Notas para los cursos de Matemática Discreta [C1 (MAD-FIQ)], y Teoría de la Computación (TCOMP-FICH)

http://www.cimec.org.ar/tcomp

Jorge D'Elia, Juan M. Giménez, Gustavo A. Ríos Rodríguez, Sergio F. Yapur
Coautores ediciones anteriores: Alejandro Cosimo, Lisandro D, Dalcin,
Juan J. Gómez Barroso, Pablo S. Rojas Fredini, Pablo A. Kler,
Ezequiel J. López, Martín A. Pucheta, Sofía S. Sarraf,
Guillermo C. Tessi

www.cimec.org.ar/tcomp
<jdelia@cimec.unl.edu.ar>

Departamento de Ingeniería Informática
Facultad de Ingeniería y Ciencias Hídricas (FICH, http://fich.unl.edu.ar)
Universidad Nacional del Litoral (UNL, http://www.unl.edu.ar)

versión 20220725

Indice

CAPÍTULO 1

Lógica y demostraciones

Nota. Estas notas siguen el texto de referencia Rosen (2004) manteniendo la numeración de las secciones y sus títulos, como una referencia adicional para el auto-estudio siguiendo ese texto.

Contents

1.1. Lógica proposicional

Definición. Una *proposición* es toda oración o enunciado que es, o bien verdadera, o bien es falsa, pero no ambas cosas a la vez. *Notación*: para las proposiciones emplearemos letras y, por convenio, empezaremos con p, q, r, s, ..., también usaremos P, Q, R, S, ..., y cuando no alcanza también con α, β, γ, ...

Definición. El Valor de Verdad (VV) de una proposición dada, o bien es verdadero si la proposición es verdadera, o bien es falsa en caso contrario. *Notación*: en el primer caso simbolizaremos con T y con F en el segundo caso.

Observación. Denotaremos "verdadero" con T, como en estas notas, aunque también se suele usar V, como en el texto de referencia (Rosen (2004)). Un motivo de la primera elección es para aminorar confusiones con el símbolo $\vee$ cuando se escribe con letra manuscrita en las evaluaciones.

Observación. También se suele simbolizar falso y verdadero con 0 y 1, respectivamente, lo cual es una notación controversial porque 0 ni 1 son valores lógicos, no obstante, su

uso se encuentra muy difundido, *e.g.* en compiladores, si bien también se utilizan otras convenciones en los compiladores, en técnicas digitales, en Sec. 2.7 del texto de referencia (Rosen (2004)), etc.

Definición. Una *proposición compuesta* es un proposición obtenida por la combinación de una o más proposiciones dadas mediante el uso de *operadores (o conectivos) lógicos*.

Definición. La Tabla de Verdad (TV) muestra en forma sistemática los valores de verdad de una proposición compuesta en función de los *todas las combinaciones posibles* de los valores de verdad de las proposiciones que la componen.

Comentario. Consideraremos 6 operadores (o conectivos) lógicos:

1) Negación (**not**)
2) Conjunción (**and**)
3) Disyunción (inclusiva) (**or**)
4) Disyunción exclusiva (**xor**)
5) Implicación (*material implication*)
6) Doble implicación o bicondicional (**eqv**)

en donde, en negrita, se destacan los conectivos lógicos de uso tan frecuente que han sido incorporados en pseudolenguajes, técnicas digitales, y en lenguajes de programación. En el libro de texto de referencia (Rosen (2004)) se emplean casi indistintamente las frases "operador lógico" y "conectivo lógico" excepto para la negación, en donde prefiere la primera (porque sólo hay una proposición p).

Definición. Sea p una proposición. El enunciado "no se cumple p" es otra proposición llamada la negación de p. *Notación*: la negación de p se denota con $\neg p$ y se lee "no p". La TV de la negación es la dada en la Tabla 1.1.

p	$\neg p$
F	T
T	F

Tabla 1.1: Negación (**not**).

Definición. Sean p y q proposiciones. La proposición compuesta "p y q" es la proposición que es verdadera cuando tanto p como q son verdaderas y es falsa en los demás casos. *Notación*: la conjunción de p y q se denota con $p \wedge q$ y se lee "p y q". La TV de la conjunción es la dada en la Tabla 1.2.

p	q	$p \wedge q$
F	F	F
F	T	F
T	F	F
T	T	T

Tabla 1.2: Conjunción (**and**).

Definición. Sean p y q proposiciones. La proposición "p ó q" es la proposición que es falsa cuando tanto p como q son falsas y es verdadera en los demás casos. La TV de la disyunción inclusiva es la Tabla 1.3. *Notación*: la disyunción de p y q se denota con $p \vee q$ y se lee "p ó q".

Observación. En ciencias jurídicas, para evitar ambiguedades, se suele emplear "p y/o q", lo cual justifica el calificativo "disyunción inclusiva", esto es, $p \vee q$ es verdadera cuando, o bien p es verdadera y q es falsa, o bien p es falsa y q es verdadera, o bien ambas p y q son verdaderas.

p	q	$p \vee q$
F	F	F
F	T	T
T	F	T
T	T	T

Tabla 1.3: Disyunción (o disyunción inclusiva, **or**).

Definición. Sean p y q proposiciones. La proposición "o bien p o bien q pero no ambas" es aquella que es verdadera cuando exactamente solo una de las proposiciones es verdadera, y es falsa en los demás casos. *Notación*: la disyunción exclusiva de p y q la denotaremos con $p \oplus q$ y se puede leer como "o bien p, o bien q". La TV de la disyunción exclusiva es la dada en la Tabla 1.4.

p	q	$p \oplus q$
F	F	F
F	T	T
T	F	T
T	T	F

Tabla 1.4: Disyunción exclusiva (**xor**).

Observación.

- En el texto de referencia (Rosen (2004)) se emplea la notación $p \oplus q$, y es la que adoptada aquí;
- En cambio, en el texto de consulta (Johnsonbaugh (2005)) se emplea la notación $p \veebar q$.

Observación. Las TV de la disyunción exclusiva $p \oplus q$ y de $(p \wedge \neg q) \vee (\neg p \wedge q)$ son las mismas, como se muestra en la Tabla 1.5.

p	q	$p \oplus q$	$(p \wedge \neg q) \vee (\neg p \wedge q)$
F	F	F	F
F	T	T	T
T	F	T	T
T	T	F	F

Tabla 1.5: Las TV de la disyunción exclusiva $p \oplus q$ y de $(p \wedge \neg q) \vee (\neg p \wedge q)$ son las mismas.

Tarea. Mostrar que las TV de la disyunción exclusiva $p \oplus q$ y de $\neg(p \wedge q) \wedge (p \vee q)$ son las mismas.

Tabla de verdad con más de dos proposiciones

- Con dos proposiciones p y q se observa que las TV tienen 4 filas, *e.g.* las correspondientes a los conectivos lógicos (excepto la negación);
- En general, la TV de una proposición obtenida por la combinación de n proposiciones, tendrá 2^n filas. Este resultado se demuestra en conteo (y suele preguntarse en el parcial 2, globalizador y finales!);
- Si bien no es importante el orden dado a las filas en una TV, sin embargo, puede ser conveniente adquirir un criterio sistemático, para no omitir alguna fila combinatoria y/o no repetir alguna (errores algo frecuentes en las evaluaciones).

Ejemplo.

- Si una proposición compuesta está formada por 2, 3, 4, y 5 proposiciones, entonces hay 4, 8, 16, y 32 filas en su TV, respectivamente, lo cual no parece tan extenso de hacer;
- Pero con 200, 300, 400, y 500 proposiciones habrán, aproximadamente, 1×10^6, 2×10^{90}, 2×10^{120}, y 3×10^{150} filas en su TV, respectivamente, lo cual es muy caro, aún computacionalmente. Adelantamos (lo verán en la asignatura AED) que leyes de crecimiento como 2^n, donde n es el tamaño del problema, son muy "malas noticias" en computación.

1.2. Equivalencias proposicionales

Definición. Sean p y q proposiciones. La implicación "si p entonces q" es la proposición que es falsa únicamente cuando p es verdadera y q es falsa, y es verdadera en los demás casos. *Notación*: la implicación "si p entonces q", se denota con $p \to q$. *Nomenclatura*: en la implicación $p \to q$, la p es la *premisa* (o *hipótesis*, o *antecedente*), y la q es la *conclusión* (o *tesis*, o *consecuente*). La TV de la implicación es la dada en la Tabla 1.6.

p	q	$p \to q$
F	F	T
F	T	T
T	F	F
T	T	T

Tabla 1.6: Implicación.

Observación.

- La definición de la implicación $p \to q$ es más general que en el lenguaje corriente, *i.e.* a diferencia del sentido común, no hay una relación "causa-efecto" entre la premisa p y la conclusión q, lo cual es sorprendente para el neófito;
- Una forma útil de entender el VV de la implicación es pensarla como un contrato legal. *Tarea*: leer el ejemplo alusivo en el libro de texto de referencia (Rosen (2004));

Observación. Hay muchas maneras de expresar la implicación $p \to q$ (todas se preguntan en las evaluaciones!). Mencionamos 12:

1) **Si** p**, entonces** q.
2) **Si** p**,** q.
3) p **es suficiente para** q.
4) q **si** p.
5) q **cuando** p.
6) **Una condición necesaria para** p **es** q.
7) p **implica** q.
8) p **sólo si** q.
9) **Una condición suficiente para** q **es** p.
10) q **siempre que** p.
11) q **es necesaria para** p.
12) q **se deduce de** p.

Observación. En los cursos de lógica se describe con más cuidado el siguiente detalle en el enunciado de la implicación "si p entonces q":

- Normalmente la palabra **si** introduce al antecedente. O sea, lo que viene a continuación de la palabra **si** es la *premisa* p;
- La excepción es cuando aparece en la frase **sólo si**, en donde se invierten los términos. O sea, lo que sigue después del **solo si** es la *conclusión* q.

Ejemplo. [por Eli Haye]. Sea p: ser santafesino (en un sentido provincial), y q: ser argentino. Se tiene:

1) Si (es santafesino), entonces (es argentino).
2) Si (es santafesino), (es argentino).
3) (Ser santafesino) es suficiente para (ser argentino).
4) (Es argentino) si (es santafesino).
5) (Es argentino) cuando (es santafesino).
6) Una condición necesaria para (ser santafesino) es (ser argentino).
7) (Ser santafesino) implica (ser argentino).
8) (Es santafesino) sólo si (es argentino).
9) Una condición suficiente para (ser argentino) es (ser santafesino).
10) (Es argentino) siempre que (sea santafesino).
11) (Ser argentino) es necesario para (ser santafesino).
12) (Ser argentino) se deduce de (ser santafesino).

Recíproca, contrapositiva (o contra-recíproca) e inversa

Definición. A partir de la implicación $p \to q$ se definen:

- La proposición $q \to p$ es la *recíproca* de $p \to q$;
- La proposición $\neg q \to \neg p$ es la *contrapositiva* (o *contra-recíproca*) de $p \to q$;
- La proposición $\neg p \to \neg q$ es la *inversa* de $p \to q$.

Observación. Las TV de la implicación $p \to q$ y de su *contrapositiva* $\neg q \to \neg p$ son las mismas, ver la Tabla 1.7.

Tarea. Mostrar que las TV de la recíproca $q \to p$ y de la inversa $\neg p \to \neg q$ de la implicación $p \to q$ son las mismas.

p	q	$p \to q$	$\neg q \to \neg p$
F	F	T	T
F	T	T	T
T	F	F	F
T	T	T	T

Tabla 1.7: Las TV de la implicación $p \to q$ y de su *contrapositiva* $\neg q \to \neg p$ son las mismas.

Doble implicación (o bicondicional)

Definición. Sean p y q proposiciones. La doble implicación (o bicondicional) de p y q es la proposición compuesta que es verdadera cuando p y q tienen los mismos valores de verdad y es falsa en los demás casos. *Notación*: la doble implicación de p y q se denota con $p \leftrightarrow q$. La TV de la doble implicación es la dada en la Tabla 1.8.

p	q	$p \leftrightarrow q$
F	F	T
F	T	F
T	F	F
T	T	T

Tabla 1.8: Doble implicación (o bicondicional **eqv**).

Observación. Hay varias maneras de expresar la doble implicación $p \leftrightarrow q$ (y se preguntan en las evaluaciones!). Mencionamos 4:

1) p **si y sólo si** q.
2) p **es necesario y suficiente para** q.
3) **Si** p **entonces** q **y recíprocamente**.
4) p **ssi** p.

Observación. La TV de la doble implicación (o bicondicional) $p \leftrightarrow q$ y de $(p \to q) \wedge (q \to p)$ son las mismas, ver la Tabla 1.9. Esto es útil en las demostraciones.

p	q	$p \leftrightarrow q$	$(p \to q) \wedge (q \to p)$
F	F	T	T
F	T	F	F
T	F	F	F
T	T	T	T

Tabla 1.9: Las TV de la doble implicación (o bicondicional) $p \leftrightarrow q$ y de $(p \to q) \wedge (q \to p)$ son las mismas.

Observación. Las TV del bicondicional $p \leftrightarrow q$ y de $(p \wedge q) \vee (\neg p \wedge \neg q)$ son las mismas, como se muestra en la Tabla 1.10.

Observación. Las TV del bicondicional $p \leftrightarrow q$ y de $\neg(p \oplus q)$ son las mismas, como se puede concluir al comparar las Tablas 1.4 y 1.8.

p	q	$p \leftrightarrow q$	$(p \wedge q) \vee (\neg p \wedge \neg q)$
F	F	T	T
F	T	F	F
T	F	F	F
T	T	T	T

Tabla 1.10: Las TV de la doble implicación (o bicondicional) $p \leftrightarrow q$ y de $(p \wedge q) \vee (\neg p \wedge \neg q)$ son las mismas.

prioridad de precedencia	operador lógico	nombre
1	$\neg$	negación
2	$\wedge$	conjunción (*and*)
3	$\vee$	disyunción (*or*)
4	$\rightarrow$	implicación (o condicional)
5	$\leftrightarrow$	doble implicación (o bicondicional)

Tabla 1.11: Reglas de precedencia de los operadores lógicos.

Reglas de precedencia de los operadores lógicos

- La proposición compuesta $(p \vee q) \wedge (\neg r)$ es la conjunción de $p \vee q$ y de $\neg r$;
- Para reducir el número de paréntesis se conviene que la negación se aplica antes que los demás operadores, *e.g.* la proposición $(\neg p) \wedge q$, se reduce a $\neg p \wedge q$, pero $(\neg p) \wedge q$ no es lo mismo que $\neg(p \wedge q)$;
- En general se acostumbra, si no hay ambiguedades, utilizar las Reglas de precedencia (RP) dadas en la Tabla 1.11. Empero, si hay dudas, entonces emplear los paréntesis;
- Ejemplo: la notación $p \vee q \rightarrow r$ quiere significar $(p \vee q) \rightarrow r$. De ningún modo equivale, por ejemplo, a $p \vee (q \rightarrow r)$, un *fatal error* en un examen;
- Las RP se usan libremente tanto en los libros como en la Guía de Trabajos Prácticos (GTP) y en las evaluaciones.

Tautología, contradicción y contingencia

Definición. Una proposición compuesta que siempre es verdadera, no importando los VV de sus proposiciones componentes, se denomina *tautología*.

Definición. Una proposición compuesta que siempre es falsa, no importando los VV de sus proposiciones componenentes, se denomina *contradicción*.

Definición. Una proposición compuesta que no es una tautología ni una contradicción se denomina *contingencia*.

Ejemplo. En la Tabla 1.12 se muestra un ejemplo de una tautología y de una contradicción.

Equivalencia lógica

Definición. Se dice que las proposiciones p y q son lógicamente equivalentes (LE), o que p y q definen una equivalencia lógica, siempre que el bicondicional $p \leftrightarrow q$ se reduce a una tautología. *Notación*: cuando p y q son LE se denota con $p \equiv q$.

p	$\neg p$	$p \vee \neg p$	$p \wedge \neg p$
F	T	T	F
T	F	T	F

Tabla 1.12: Un ejemplo de una tautología (la columna $p \vee \neg p$ siempre es T), y de una contradicción (la columna $p \wedge \neg p$ siempre es F).

Equivalencia Lógica (EL)	Ley	
$p \vee F \equiv p$ $p \wedge T \equiv p$	identidad	1
$p \vee T \equiv T$ $p \wedge F \equiv F$	dominación	2
$p \vee p \equiv p$ $p \wedge p \equiv p$	idempotencia	3
$\neg(\neg p) \equiv p$	doble negación	4
$p \vee q \equiv q \vee p$ $p \wedge p \equiv q \wedge p$	conmutativas	5
$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	asociativas	6
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	distributivas	7
$\neg(p \vee q) \equiv \neg p \wedge \neg q$ $\neg(p \wedge q) \equiv \neg p \vee \neg q$	De Morgan	8
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	absorción	9
$p \vee \neg p \equiv T$ $p \wedge \neg p \equiv F$	negación	10

Tabla 1.13: Tabla de EL de uso muy frecuente.

Observación. El símbolo $\equiv$ no es un operador (o conectivo) lógico, puesto que $p \equiv q$ no es una proposición compuesta, sino que quiere indicar que el bicondicional $p \leftrightarrow q$ se reduce a una tautología.

Ejemplo. En la Tabla 1.13se listan las equivalencias lógicas de uso muy frecuente en las evaluaciones.

Ejemplo. En las Tablas 1.14-1.15 se incluye listados de EL relacionadas con condicionales y bicondicionales, respectivamente.

Tarea. Verificar cada una de las leyes listadas en las Tablas 1.13-1.15, *e.g.* como se hace en el siguiente ejemplo.

$p \to q \equiv \neg q \to \neg p$	(c1)
$p \to q \equiv \neg p \vee q$	(c2)
$\neg(p \to q) \equiv p \wedge \neg q$	(c3 (se obtiene aplicando De Morgan en c2))
$p \vee q \equiv \neg p \to q$	(c4)
$p \wedge q \equiv \neg(p \to \neg q)$	(c5)
$(p \to q) \wedge (p \to r) \equiv p \to (q \wedge r)$	(c6)
$(p \to r) \wedge (q \to r) \equiv (p \vee q) \to r)$	(c7)
$(p \to q) \vee (p \to r) \equiv p \to (q \vee r)$	(c8)
$(p \to r) \vee (q \to r) \equiv (p \wedge q) \to r)$	(c9)

Tabla 1.14: Algunas EL relacionadas con condicionales.

$$p \leftrightarrow q \equiv (p \to q) \wedge (q \to p) \quad \text{(b1)}$$
$$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q \quad \text{(b2)}$$
$$p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q) \quad \text{(b3)}$$
$$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q \quad \text{(b4)}$$

Tabla 1.15: Otras EL relacionadas con bicondicionales.

p	q	$\overbrace{\neg(p \vee q)}^{P}$	$\overbrace{\neg p \wedge \neg q}^{Q}$	$P \leftrightarrow Q$
F	F	T	T	T
F	T	F	F	T
T	F	F	F	T
T	T	F	F	T

Tabla 1.16: Demostración mediante TV de las leyes de De Morgan para proposiciones en el caso $\neg(p \vee q)$.

Ejemplo. Leyes de De Morgan para dos proposiciones. En las Tablas 1.16-1.17 se demuestra, por medio de una TV que:

- $\neg(p \vee q) \equiv \neg p \wedge \neg q$, es decir: "no ($p$ o q) es equivalente a (*no* p) y (no q)";
- $\neg(p \wedge q) \equiv \neg p \vee \neg q$, es decir: "no ($p$ y q) es equivalente a (*no* p) o (no q)".

Ejemplo. *Consigna*: justificar, con y sin el uso de TV, si $((p \to q) \wedge (q \wedge r)) \to (p \to r)$, es una tautología, contradicción o contingencia. Solución:

- Con TV: para el hogar!
- Sin TV: considerar los pasos detallados en la Ec (1.1);
- *Comentario*: la técnica es eliminar las implicaciones, luego las negaciones, luego asociar o distribuir para obtener alguna ley conocida (*e.g.* identidad, dominación, absorción, negación, etc. Hay muchos caminos... el mejor es intentar, intentar, intentar, ...

Observación. En Tabla 1.18 se muestra un ejemplo de tautologia.

p	q	$\overbrace{\neg(p \wedge q)}^{P}$	$\overbrace{\neg p \vee \neg q}^{Q}$	$P \leftrightarrow Q$
F	F	T	T	T
F	T	T	T	T
T	F	T	T	T
T	T	F	F	T

Tabla 1.17: Demostración mediante TV de las leyes de De Morgan para proposiciones en el caso $\neg(p \wedge q)$.

p	q	r	$a = p \vee q$	$b = (\neg p \vee r)$	$c = q \vee r$	$d = a \wedge b$	$e = d \to c$
F	F	F	F	T	F	F	T
F	T	F	T	T	T	T	T
T	F	F	T	F	F	F	T
T	T	F	T	F	T	F	T
F	F	T	F	T	T	F	T
F	T	T	T	T	T	T	T
T	F	T	T	T	T	T	T
T	T	T	T	T	T	T	T

Tabla 1.18: Ejemplo de una tautologia.

$$
\begin{aligned}
A \wedge (B \vee C) =& [(p \to q) \wedge (q \to r)] \to (p \to r) && \text{uso Tabla 1.14-c1}\\
\equiv& \neg[(p \to q) \wedge (q \to r)] \vee (p \to r) && \text{uso ley de De Morgan}\\
\equiv& [\neg(p \to q) \vee \neg(q \to r)] \vee (p \to r) && \text{elimino corchetes}\\
\equiv& \neg(p \to q) \vee \neg(q \to r) \vee (p \to r) && \text{uso Tabla 1.14-c1}\\
\equiv& \neg(\neg p \vee q) \vee \neg(\neg q \vee r) \vee (\neg p \vee r) && \text{De Morgan y saco último ()}\\
\equiv& (p \wedge \neg q) \vee (q \wedge \neg r) \vee (\neg p) \vee r && \text{asocio convenientemente}\\
\equiv& [(p \wedge \neg q) \vee \neg p] \vee [(q \wedge \neg r) \vee r] && \text{uso ley distributiva}\\
\equiv& [(p \vee \neg p) \wedge (\neg q \vee \neg p)] \vee [(q \vee r) \wedge (\neg r \vee r)] && \text{uso ley de la negación}\\
\equiv& [T \wedge (\neg q \vee \neg p)] \vee [(q \vee r) \wedge T] && \text{uso ley de identidad}\\
\equiv& (\neg q \vee \neg p) \vee (q \vee r) && \text{puedo quitar paréntesis}\\
\equiv& \neg q \vee \neg p \vee q \vee r && \text{asocio convenientemente}\\
\equiv& (\neg q \vee q) \vee (\neg q \vee r) && \text{uso ley de la negación}\\
\equiv& T \vee (\neg q \vee r) && \text{uso ley de la dominación}\\
\equiv& T && \text{es una tautología.}
\end{aligned}
\tag{1.1}
$$

1.3. Predicados y cuantificadores

Definición.

- Sea $P(x)$ un enunciado que incluye a la variable $x \in D$. Se denomina Función Proposicional (FP), o predicado, al enunciado P si, para cada valor $x \in D$, se tiene que $P(x)$ es una proposición;
- Se denomina Dominio de Discurso (DD) al conjunto D del enunciado P.
- Caso con más de una variable: un enunciado de la forma $P(x_1, x_2, ..., x_n)$ es el VV de la FP P en la n-tupla $(x_1, x_2, ..., x_n)$;

Observación. Algunos conjuntos de uso frecuente:

- Enteros: $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$ (notar que el 0 no-tiene signo);
- Enteros positivos: $\mathbb{Z}^+ = \{1, 2, 3, ...\}$;
- Enteros negativos: $\mathbb{Z}^- = \{..., -3, -2, -1\}$;

- Enteros **no-negativos**: $\mathbb{Z}_0^+ = \{0, 1, 2, 3, ...\}$ (de utilidad en inducción);
- Números reales $\mathbb{R}$.

Observación. En general, el VV de una Función Proposicional $P(x)$ puede ser, o bien T, o bien F, según sea el DD, como se muestra en el siguiente ejemplo.

Ejemplo. Sea el enunciado $P(x) : \ x + 1 > 2x$, con $x \in \mathbb{Z}$. Entonces

1) si el DD es el intervalo $-\infty < x < 1$, entonces $P(x)$ es T;
2) si el DD es el intervalo $1 \leq x < \infty$, entonces $P(x)$ es F.

Cuantificador existencial

Definición. La *cuantificación existencial* de la función proposicional P con Dominio de Discurso D es la proposición: $P(x)$ es verdadera para **al menos un** valor x en el DD. *Notación*. Se denota con $\exists x, P(x)$, donde $\exists$ es el **cuantificador existencial**. *Nomenclatura*. La notación $\exists x, P(x)$ se puede leer indistintamente como sigue:

- Hay **UN** x tal que $P(x)$;
- Hay **AL MENOS UN** x tal que $P(x)$;
- Para **ALGUN** x, $P(x)$;
- **EXISTE** x tal que $P(x)$.

Observación.

- Cuando todos los elementos del DD se pueden enumerar, o sea cuando x_1, x_2, ... x_n, se tiene que
$$\exists x \ P(x) \equiv P(x_1) \vee P(x_2) \vee ... \vee P(x_n) \tag{1.2}$$
puesto que la disyunción es verdadera ssi **al menos uno** de $P(x_1)$, $P(x_2)$, ..., o $P(x_n)$ es verdadero;
- Notación: el lado derecho de la Ec. (1.2) lo abreviaremos con
$$\textbf{any}\ (P(x)) = \bigvee_{i=1}^{n} P(x_i) = P(x_1) \vee P(x_2) \vee ... \vee P(x_n) \tag{1.3}$$
- La evaluación dada por la Ec. (1.2) la ejemplificaremos en un programa demo en la Sec. 1.3, y es tan frecuente en la práctica que en algunos lenguajes de programación, e.g. Python y Fortran disponen de la función intrínseca **any()**.

Cuantificador universal

Definición. La *cuantificación universal* de la función proposicional P con Dominio de Discurso D es la proposición: $P(x)$ es verdadera para **todos** los valores x en el DD. *Notación*. Se denota con $\forall x, P(x)$, donde $\forall$ es el **cuantificador universal**. *Nomenclatura*. La notación $\forall x, P(x)$ se puede leer indistintamente como sigue:

- Para **TODO** x se cumple $P(x)$;
- Para **CUALQUIER** x se cumple $P(x)$;
- Para **CADA** x se cumple $P(x)$.

Observación.

- Cuando todos los elementos del DD se pueden enumerar, o sea cuando x_1, x_2, ..., x_n, se tiene que
$$\forall x, P(x) \equiv P(x_1) \wedge P(x_2) \wedge ... \wedge P(x_n) \tag{1.4}$$
puesto que la conjunción es verdadera ssi $P(x_1)$, $P(x_2)$, ..., $P(x_n)$ son **todas** verdaderas;
- Notación: el lado derecho de la Ec. (1.4) lo abreviaremos con
$$\textbf{all}\ (P(x)) = \bigwedge_{i=1}^{n} P(x_i) = P(x_1) \wedge P(x_2) \wedge ... \wedge P(x_n) \tag{1.5}$$
- La evaluación dada por la Ec. (1.4) la ejemplificaremos en un programa demo en la Sec. 1.3, y es tan frecuente en la práctica que en algunos lenguajes de programación, e.g. Python y Fortran disponen de la función intrínseca **all()**.

Observación. En la Tabla 1.19 se resume cuándo una sentencia cuantificada es T o F.

Observación. Enfatizamos la importancia que tiene el DD en los ejercicios: para una misma sentencia cuantificada, el resultado puede ser verdadero o falso dependiendo de cómo se haya definido el DD, como se muestra en el siguiente ejemplo.

Ejemplo. Evaluar el VV de $\forall x\ (x^2 \geq x)$ cuando: (i) $x \in \mathbb{R}$ (tema 1); y (ii) $x \in \mathbb{Z}$ (tema 2). Solución: sea $x^2 \geq x$. Restando x miembro a miembro, se tiene que $x^2 - x \geq x - x$, y sacando factor común x en el lazo izquierdo de esta última desigualdad queda $x(x-1) \geq 0$, cuyas soluciones son $x \leq 0$ o $x \geq 1$. En cuanto al intervalo $0 < x < 1$ se puede observar:

i) Cuando la variable x puede tomar valores *reales*, habrán (infinitos) valores de x en dicho intervalo pero, en ese caso, la última desigualdad es inválida (verificarlo!). Por eso, se concluye que $\forall x\ (x^2 \geq x)$ es F *cuando* $x \in \mathbb{R}$;
ii) Cuando la variable x sólo puede tomar valores *enteros*, no existen valores de x en dicho intervalo tales que hagan F la última desigualdad. Por tanto, en este caso se concluye que $\forall x\ (x^2 \geq x)$ es T *cuando* $x \in \mathbb{Z}$.

Observación. Hay que tener cuidado cuando se usan los cuantificadores $\forall x$ o $\exists x$. Por ejemplo, sean:
$$\begin{aligned} P(n) &: n \text{ es par} \\ Q(n) &: n \text{ es impar.} \end{aligned} \tag{1.6}$$
donde el DD es conjunto de los enteros $\mathbb{Z}$. Entonces:

- $\forall n\ (P(n) \vee Q(n))$, se puede enunciar como "para todo entero n, se tiene que n es par o n es impar", lo cual es T;

sentencia cuantificada	cuándo es T	cuándo es F
$\exists x, P(x)$	$P(x)$ es T para **AL MENOS UN** x	$P(x)$ es F para **TODO** x
$\forall x, P(x)$	$P(x)$ es T para **TODO** x	**Al menos un** x tal que $P(x)$ es F

Tabla 1.19: Casos cuando una sentencia cuantificada es T o F.

- Pero $(\forall n\ P(n)) \vee (\forall n\ Q(n))$, se puede enunciar como "todos los enteros n son pares, o todos los enteros n son impares", lo que es F;
- Se concluye que, en general,

$$\forall n\ (P(n) \vee Q(n)) \not\equiv (\forall n\ P(n)) \vee (\forall n\ Q(n)) \tag{1.7}$$

Negación de proposiciones cuantificadas o leyes de De Morgan generalizadas para la lógica

Teorema. Sea P una FP en un DD dado. Entonces

$$\begin{aligned} \neg(\exists x, P(x)) &\equiv \forall x \neg P(x) \\ \neg(\forall x, P(x)) &\equiv \exists x \neg P(x) \end{aligned} \tag{1.8}$$

Demostración de la primera parte (la segunda queda como tarea para el hogar):

- Suponga que $\neg(\exists x, P(x))$ es T. Eso significa que $\exists x, P(x)$ es F. Por la definición del cuantificador existencial, la proposición $\exists x, P(x)$ es F cuando $P(x)$ es F para **todo** $x \in D$. Pero si $P(x)$ es F para **todo** $x \in D$, eso significa que $\neg P(x)$ es T para **todo** $x \in D$. Por la definición del cuantificador universal, cuando $\neg P(x)$ es T para **todo** $x \in D$, la proposición $\forall x, \neg P(x)$ es T. Entonces, cuando $\neg(\exists x, P(x))$ es T, la proposición $\forall x, \neg P(x)$ también es T;
- Suponga que $\neg(\exists x, P(x))$ es F. Eso significa que $\exists x, P(x)$ es T. Por la definición del cuantificador existencial, la proposición $\exists x, P(x)$ es T cuando $P(x)$ es T para **algún** $x \in D$. Pero si $P(x)$ es T para **algún** $x \in D$, eso significa que $\neg P(x)$ es F para **algún** $x \in D$. Por la definición del cuantificador universal, cuando $\neg P(x)$ es F para **algún** $x \in D$, la proposición $\forall x, \neg P(x)$ es F. Entonces, cuando $\neg(\exists x, P(x))$ es F, la proposición $\forall x, \neg P(x)$ también es F.

Observación. Algunos lenguajes de programación preven instrucciones para los cuantificadores $\exists x$ y $\forall x$ en el caso en que todos los elementos del DD se pueden enumerar (o sea x_1, x_2, ... x_n). En particular, las instrucciones `any` y `all` están presentes en otros lenguajes, e.g. python o fortran.

1.4. Cuantificadores anidados

Veremos únicamente el caso de cuantificadores doblemente anidados, a través de un ejemplo y los ejercicios en la GTP.

Ejemplo.
Exprese en palabras y determine el VV de las siguientes proposiciones cuantificadas, en donde $x, y \in \mathbb{R}$:

- Sea $\exists x \exists y\ (x+y=17)$. En palabras: para algún x, existe un y tal que $x+y=17$. Valor de Verdad: en este caso es posible hallar, al menos, un par x, y tal que $x+y=17$ (*e.g.* sea el par $x=7$ e $y=10$). Como ambos cuantificadores son existenciales, un ejemplo es suficiente para concluir que el VV de esta proposición es T;
- Sea $\forall x \exists y\ (x+y=17)$. En palabras: para todo x, existe un y tal que $x+y=17$. Valor de Verdad: en este caso también es posible hallar, para cada x, un y tal que satisfaga la propiedad, y que está dado por $y=17-x$. Esto es, cada x tiene asegurado un y (único en cada caso) y, por eso, el VV de esta proposición es T;
- Sea $\exists x \forall y\ (x+y=17)$. En palabras: para algún x, y para todo y, debe ser $x+y=17$. Valor de Verdad: debería existir un x tan particular que sumándole cualquier y diera siempre 17. Pero eso no es posible, por lo que el VV de esta proposición es F;
- Sea $\forall x \forall y\ (x+y=17)$. En palabras: para todo x, y para todo y, debe ser $x+y=17$. Valor de Verdad: para cualquier x debería ser posible sumarle cualquier y y siempre dar 17. Otra vez, eso no es posible, por lo que el VV de esta proposición es F.

Observación.
Sin demostrarlo se tiene en general que

$$\begin{array}{ll} \exists x \exists y\ P(x,y) \equiv \exists y \exists x\ P(x,y) & \text{conmutan} \\ \forall x \forall y\ P(x,y) \equiv \forall y \forall x\ P(x,y) & \text{conmutan} \\ \forall x \exists y\ P(x,y) \not\equiv \exists y \forall x\ P(x,y) & \text{no conmutan} \end{array} \tag{1.9}$$

Negación en proposiciones con cuantificadores doblemente anidados

Para negar proposiciones con cuantificadores doblemente anidados, se emplea sucesivamente las reglas de negación para proposiciones con único cuantificador.

Ejemplo. Negar la proposición $\exists x \forall y\ (x+y=17)$, donde $x, y \in \mathbb{R}$. *Solución*:

$$\begin{array}{l} \neg(\exists x \forall y\ (x+y=17)) \\ \equiv \forall x\ \neg(\forall y\ (x+y=17)) \\ \equiv \forall x\ \exists y\ \neg(x+y=17) \\ \equiv \forall x\ \exists y\ (x+y \neq 17) \end{array} \tag{1.10}$$

Observación. Cuando todos los elementos del DD se pueden enumerar, o sea x_1, x_2, ... x_n, puede ser útil pensar a los cuantificadores anidados como recorridos anidados. Por ejemplo, para determinar si $\forall x \forall y\ P(x,y)$ es T o F, recorremos todos los valores x e y de la siguiente manera. Para cada x revisamos con un recorrido anidado todos los valores de y. Si encontramos que $P(x,y)$ es T en todos los casos, la conclusión inevitable es que $\forall x \forall y\ P(x,y)$ es T. Si por el contrario, cuando encontramos el primer par de valores x e y tal que $P(x,y)$ es F, podrían haber más de un par, es suficiente para concluir que $\forall x \forall y\ P(x,y)$ es F.

1.5. Métodos de demostración

Alguna terminología

Definición.

- **Axioma** o **postulado**: es una suposición no demostrable y que se supone verdadera. *Comentario*: en Física suele emplearse el término "principio";
- **Definición**: es una oración declarativa que describe con precisión el significado y alcance de un término (palabra, frase, u otro conjunto de símbolos);
- **Demostración**: es una serie de proposiciones conexas que definen un razonamiento. Para construir una demostración hacen falta métodos para obtener nuevas proposiciones a partir de las ya dadas, en donde estas últimas pueden incluir axiomas o lemas;

- **Reglas de inferencia**: son proposiciones compuestas tautológicas. *Comentario*: sirven para obtener conclusiones válidas a partir de la veracidad de otras afirmaciones. La Tabla 1.20 lista las más usuales;
- **Teorema**: es un enunciado escrito como una implicación que se demuestra como verdadero usando una demostración. *Comentario*: se reserva para un resultado de mayor alcance o más importante;
- **Lema**: es un teorema auxiliar (de menor alcance) que se usa para demostrar otro teorema más destacado (de mayor alcance);
- **Corolario**: es una consecuencia de un teorema ya demostrado;
- **Falacia**: es una forma de razonamiento incorrecta;
- **Paradoja**: es una inconsistencia lógica. Intuitivamente, un razonamiento es inconsistente cuando contiene una ambigüedad;
- **Conjetura**: es una proposición cuyo VV es desconocido a la fecha. A veces se logra probar que es T, otra veces que es F.

Ejemplo. Un ejemplo de una *conjetura* en computación se relaciona con el algoritmo de Collatz: se elige un entero positivo n mayor a 1. Si n es par entonces dividirlo por 2, sino multiplicarlo por 3 y sumarle 1. Luego, si el resultado es 1, entonces finalizar, sino repetir las cuentas. Este algoritmo se puede enunciar matemáticamente con la función $f(n)$ para todo entero positivo n dada por

$$f(n) = \begin{cases} n/2 & \text{si } n \bmod 2 = 0 \text{ (entero par);} \\ 3n+1 & \text{si } n \bmod 2 \neq 0 \text{ (entero impar).} \end{cases} \tag{1.11}$$

La conjetura de Collatz (o conjetura de $3n+1$) sostiene que, en esas condiciones, la función $f(n)$ *siempre* llegará al entero 1 para cualquier entero positivo n inicial. Si le tenemos fe a la conjetura, una implementación computacional de la misma es listada en la función `collatz(n)`:

```
1 def collatz(n): # conjetura de Collatz
2     while (n > 1):
3         if (n%2 == 0):    # es par
4             n = n/2
5         else:             # es impar
6             n = (3*n)+1
7     return n
```

Definición. Razonamientos (o argumentos) válidos:

- Un *razonamiento* (o argumento) es una implicación formada por n proposiciones de la forma:
$$(p_1 \wedge p_2 \wedge ... \wedge p_n) \rightarrow q \tag{1.12}$$
- Las implicaciones usadas en los razonamientos suelen escribirse en forma expandida (cuando hay lugar) de la siguiente manera:
  premisa p_1: ...
  premisa p_2: ...
  ... ...
  premisa p_n: ...
  conclusión c: / $\therefore$ ...
  en donde cada premisa p de la implicación se escribe en columna, una debajo de la otra, y la conclusión c debajo de una raya horizontal, donde el símbolo $\therefore$ se lee "por lo tanto" o "luego";
- Otra notación más compacta (usada en parciales, recuperatorios y exámenes) es ecribirlo en una línea de texto: p_1 **y** p_2 **y**, ..., **y** p_n, / $\therefore$ q;
- Se dice que *un razonamiento (o argumento) es válido si siempre que* **TODAS** *las premisas son* T, *la conclusión también lo es*;
- En consecuencia, demostrar que la conclusión q se deduce lógicamente de las premisas p_1, p_2, ..., p_n, es lo mismo que demostrar que la implicación $(p_1 \wedge p_2 \wedge ... \wedge p_n) \rightarrow q$ **siempre** es T;
- En un razonamiento (o argumento) válido, cuando **todas** las premisas son T, se llega (siempre) a que la *conclusión* que también es T;
- *Receta* (con TV): para determinar si un razonamiento (o argumento) es válido, se construye su TV y se mira **únicamente** las filas en donde **todas** las premisas p_1, p_2, ..., p_n son T, y se chequea que **siempre** se tiene una conclusión q también es T.

Tarea. Dadas las proposiciones p y q:

1) Demostrar que $(p \wedge (p \rightarrow q)) \rightarrow q$ es una tautología;
2) Analizar el razonamiento: p y $p \rightarrow q$, / $\therefore$ q.
3) Analizar el razonamiento:

premisa p_1:	p
premisa p_2:	$p \rightarrow q$
conclusión c:	$\therefore \quad q$

Ejemplo. Dadas las proposiciones r, s, t, u, analizar el razonamiento:

premisa p_1:	$r \rightarrow s$
premisa p_2:	$\neg s \vee t$
premisa p_3:	$\neg t \vee u$
premisa p_4:	$\neg u$
conclusión c:	$\therefore \quad \neg r$

Solución:

1) La única opción en p_4 para que sea T, es que u sea F;
2) Comoo u es F, la única opción en p_3 para que sea T, es que t sea F;
3) Como t es F, la única opción en p_2 para sea T, es que s sea F;

Razonamiento	Tautología	Nombre
p $\therefore p \vee q$	$p \to (p \vee q)$	adición
$p \wedge q$ $\therefore p$	$(p \wedge q) \to p$	simplificación
p q $\therefore p \wedge q$	$(p) \wedge (q) \to (p \wedge q)$	combinación
p $p \to q$ $\therefore q$	$(p \wedge (p \to q)) \to q$	*modus pones*
$\neg q$ $p \to q$ $\therefore \neg p$	$(\neg q \wedge (p \to q)) \to \neg p$	*modus tollens*
$p \to q$ $q \to r$ $\therefore p \to r$	$((p \to q) \wedge (q \to r)) \to (p \to r)$	silogismo hipotético
$p \vee q$ $\neg p$ $\therefore q$	$((p \vee q) \wedge (\neg p) \to q$	silogismo hipotético
$p \vee q$ $\neg p \vee r$ $\therefore q \vee r$	$((p \vee q) \wedge (\neg p \vee r)) \to (q \vee r)$	resolución

Tabla 1.20: Reglas de inferencia más usuales.

4) Como s es F, la única opción en p_1 para que sea T, es que r sea F, entonces $\neg r$ es T;
5) Como $\neg r$ es T, la conclusión c es T, por lo que el razonamiento es válido.

Definición.

- Muchos teoremas son implicaciones de la forma $p \to q$;
- Notar que una implicación $p \to q$ es T excepto cuando p es T y q es F;
- Cuando se demuestra que $p \to q$ es T, hay que probar que q es T cuando p lo es, o sea, no se demuestra que q sea T (en forma aislada);
- Existen diversas formas para realizar una demostración.

Definición.

- **Demostración directa** (DeD): la implicación $p \to q$ se puede probar comprobando que si p es T entonces q también lo es. *Receta*: se asume que p es T y, usando definiciones y teoremas dados, se comprueba que q también debe ser T;
- **Demostración indirecta** (DeI): como la implicación $p \to q$ es LE a su contrapositiva (o contra-recíproca) $\neg q \to \neg p$, la implicación $p \to q$ se puede probar demostrando que su contrapositiva (o contra-recíproca) es T; *Receta*: se asume que $\neg q$ es T y, usando definiciones y teoremas dados, se comprueba que $\neg p$ también debe ser T;
- **Demostración vacua** [en $p \to q$ cuando p es F]: se demuestra que la premisa (o hipótesis) es F, en ese caso la implicación es T porque tiene las formas $F \to T$ o $F \to F$, las cuales son ambas T;
- **Demostración trivial**: [en $p \to q$ cuando q es T]: se demuestra que la conclusión (o tesis) es T, en ese caso la implicación es T porque tiene las formas $F \to T$ o $T \to T$, las cuales son ambas T;

- **Demostración por contradicción** (o **por Reducción al Absurdo**) (DrA): se hace mas abajo.
- **Demostración por resolución**: para probar una implicación de la forma $(p_1 \vee p_2 ... \vee p_n) \rightarrow q$ se puede optar en emplear la EL dada por $(p_1 \vee p_2 ... \vee p_n) \rightarrow q \equiv (p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge ...(p_n \rightarrow q)$.

Demostración por contradicción (o por Reducción al Absurdo)

- (Toda la Sec. por Sergio Yapur). Intro: las demostraciones por reducción al absurdo pueden al principio causar un poco de confusión, debido a que nos ofrece mayor libertad que otras técnicas que tienen un formalismo más obvio, como ser la demostración directa, la indirecta, por casos, etc. En esas técnicas, el formalismo queda perfectamente definido en términos de las hipótesis y la conclusión a la que queremos llegar. Esto no significa que la demostración por reducción al absurdo no tenga un formalismo bien definido, sino simplemente que es un formalismo más flexible, y debido a esa flexibilidad constituye uno de los métodos más poderosos de demostración. Para entenderlo, profundicemos un poco en esta técnica.
- Formalismo:
  - Para demostrar una proposición de la forma $p \rightarrow q$ mediante la técnica por reducción al absurdo, es necesario poder construir una contradicción en el cuerpo de la demostración. Recordemos que una contradicción es una proposición que resulta siempre falsa, independientemente del valor de verdad de las proposiciones que la componen. Llamemos a esta contradicción con la letra C. Esta contradicción puede lograrse de varias formas. Enumeremos algunos ejemplos posibles:
    - Un número que sea positivo y negativo a la vez
    - Un número real que sea la raíz cuadrada de un número negativo
    - Una matriz que sea invertible pero que tenga determinante nulo
    - Una función derivable en todos lados, pero que no sea continua en un punto
  - En su forma más simple, la contradicción suele expresarse como $C = w \wedge \neg w$, que claramente es falsa independientemente de qué valor de verdad tome la proposición w. Pero tengamos en mente que no es la única forma posible (e.g. pueden haber varias proposiciones involucradas). Solo importa que sea una contradicción.
  - Ahora bien, cómo se vincula esta contradicción con lo que queremos demostrar? Observemos la siguiente definición

$$R \equiv p \wedge (p \rightarrow q) \tag{1.13}$$

  - Vemos que esta proposición es verdadera si vale la hipótesis y la implicación que tratamos de demostrar. O sea que (2) es lo que tratamos de demostrar. Desarro-

llémoslo

$$\begin{aligned} R &\equiv p \wedge (p \rightarrow q) \\ &\equiv p \wedge (\neg p \vee q) \\ &\equiv (p \wedge \neg p) \vee (p \wedge q) \\ &\equiv F \vee (p \wedge q) \\ &\equiv p \wedge q \end{aligned} \tag{1.14}$$

- Por otro lado, observemos la siguiente construcción $\neg R \rightarrow C$. Como esta construcción es una contradicción (pues $C \equiv F$), por lo que la implicación solo es verdadera1 si $\neg R \equiv F$ (es decir $R \equiv T$). Como vimos en la Ec. (1.14), esto ocurre si tanto p como q verdaderos, y por tanto $p \rightarrow q$ es verdadero.
- Qué significa todo esto? Que si negamos R y llegamos a una contradicción, la única posibilidad viable, de acuerdo a Ec. (1.13) es que la implicación $p \rightarrow q$ sea verdadera. Hablamos de posibilidad viable porque en términos lógicos, también podría ocurrir que la hipótesis sea falsa, pero este caso no nos interesa, ya que nos desvincula del teorema o resultado que queremos demostrar. Dicho de otra forma, si no vale la hipótesis p, no estamos demostrando el teorema en absoluto.

Ejemplo. Demostrar usando una DrA que $\sqrt{2}$ no es un número racional. Solución. Sea $p:$ $\sqrt{2}$ es irracional. En una DrA suponemos que $\neg p$ es T. Si $\sqrt{2}$ fuera racional, entonces existen dos enteros positivos a y b tales que $\sqrt{2} = a/b$, con $b \neq 0$, donde a y b no tienen factores comunes (i.e. no existe un entero h que divida a ambos sino simplificaríamos). A continuación hacemos

$$\begin{aligned} \sqrt{2} &= \frac{a}{b} \quad \text{con } b \neq 0 \\ 2 &= \frac{a^2}{b^2} \\ 2b^2 &= a^2 \end{aligned} \tag{1.15}$$

La forma de la Ec. (1.15) indica que a^2 es un entero par. Si a^2 es entero par, entonces a también es un entero par, i.e. $a = 2k$, con k entero. En ese caso

$$2b^2 = a^2 = (2k)^2 = 2(2k^2) = 2\tilde{k} \tag{1.16}$$

donde $\tilde{k} = 2k^2$ es otro entero. Vemos que $\neg p$ equivale, por una parte, aseverar que $\sqrt{2} = a/b$, con enteros a y b sin factores comunes pero, por otra parte, que 2 divide a los enteros a y b, llegando a una contradicción.

Ejemplo. (de parcial y de examen). Demuestre usando reducción al absurdo que los únicos enteros consecutivos no-negativos a, b, y c tales que satisfacen $a^2 + b^2 = c^2$ son 3, 4, y 5.
Solución: Antes comprobamos que los enteros dados verifican la igualdad $3^2 + 4^4 = 5^2$, o sea, $9 + 16 = 25$. A continuación negamos el enunciado, o sea, "porfiamos" en que deben existir otros enteros consecutivos (además de 3, 4, y 5), que satisfacen la igualdad dada en el enunciado, y los vamos a determinar. Para hallarlos, podemos hacer como sigue:

- Como a, b, y c deben ser enteros consecutivos podemos elegir $a = n$, $b = n + 1$, y $c = n + 2$, donde n es un entero (no-negativo) a determinar.

- Reemplazando en la igualdad del enunciado tenemos $n^2 + (n+1)^2 = (n+2)^2$
- Desarrollando los paréntesis, tenemos $n^2 + (n^2 + 2n + 1) = (n^2 + 4n + 4)$
- Agrupando términos en el lado izquierdo queda la ecuación cuadrática $n^2 - 2n - 3 = 0$
- Cuyas raíces son $n = [2 \pm \sqrt{4 - 4 \cdot 1 \cdot (-3)}]/2$, resultando $n = 3$ y $n = -1$;
- Verificación (incluirla en las evaluaciones!): $3^2 - 2 \cdot 3 - 3 = 9 - 6 - 3 = 0$, y $(-1)^2 - 2 \cdot (-1) - 3 = 1 + 2 - 3 = 0$;
- Pero la raíz negativa no-cumple la restricción del enunciado, y por eso la descartamos;
- Solo nos queda la raíz positiva $n = 3$, por lo que nuestra porfiada se "estrella contra la realidad", es decir, los enteros $a = 3$, $b = 4$, y $c = 5$ son los únicos enteros no-negativos que verifican $a^2 + b^2 = c^2$.

Ejemplo. Analizar los VV posibles de p cuando el VV de la implicación $\neg p \to (r \wedge \neg r)$ es T. Sol.: notamos que la proposición compuesta $(r \wedge \neg r)$ es una contradicción (i.e. siempre es F sin importar los VV de r). Entonces, si la implicación dada es T, el VV de p debe ser T.

Observación. Una Demostración Indirecta (DeI) puede re-pensarse (o re-escribirse) como una Demostración por Reducción al Absurdo (DrA), y viceversa.

- En una DeI de $p \to q$ es T, utilizamos una DeD aplicada a la contrapositiva $\neg q \to \neg p$, *i.e.* asumimos que $\neg q$ es T y, usando definiciones y teoremas dados, se comprueba que $\neg p$ también lo es.
- Para re-escribir una DeI de $p \to q$ como una DrA, suponemos que tanto la premisa p como la conclusión negada $\neg q$ son T.
- A continuación, usamos la DeD en $\neg q \to \neg p$ para concluir que $\neg p$ también debe ser T, lo que conduce a la contradiccón $p \wedge \neg p$.

Observación. Las TV de la implicación $p \to q$ y de $(p \wedge \neg q) \to (r \wedge \neg r)$ son las mismas, como se muestra en la Tabla 1.21.

Observación. Para probar la implicación $p \to q$:

- En una DeD no suponemos que la conclusión q fuera F, sino que asumimos a la premisa p como T, y comprobamos si la conclusión q también resulta T;
- En una DeI suponemos que la premisa p es F, y comprobamos si la contrapositiva $\neg q \to \neg p$ fuera T;
- En una DrA suponemos que la premisa p es T y que la conclusión q es F, y tratamos de llegar a alguna contradicción $r \wedge \neg r$.

Definición. Un entero n es par si existe un entero k tal que $n = 2k$. Un entero n es impar si existe un entero k tal que $n = 2k + 1$. Observación: un entero n, o bien es par, o bien es impar.

Ejemplo. Demostrar: si (n^2 es entero par), entonces (n es entero par). Solución. Sean las proposiciones $p : n^2$ es entero par, y $q : n$ es entero par. La contrapositiva es: (si n es entero impar), entonces (n^2 es entero impar). DeI: si n es un entero impar, entonces usamos la definición de entero impar para escribir $n = 2k + 1$, donde k es un entero. Elevando al cuadrado lado a lado $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2\tilde{k} + 1$, donde $\tilde{k} = 2k^2 + 2k$

p	q	r	$\alpha \equiv p \to q$	$p \wedge \neg q$	$r \wedge \neg r$	$\beta \equiv (p \wedge \neg q) \to (r \wedge \neg r)$
F	F	F	F	F	F	T
T	F	F	F	T	F	F
F	T	F	T	F	F	T
T	T	F	T	F	F	T
F	F	T	F	F	F	T
T	F	T	F	T	F	F
F	T	T	T	F	F	T
T	T	T	T	F	F	T

Tabla 1.21: Las TV de la implicación $p \to q$ y de $(p \wedge \neg q) \to (r \wedge \neg r)$ son las mismas.

es *otro entero* (no olvidar indicarlo en las evaluaciones). Se tiene que $n^2 = 2\tilde{k} + 1$, cuya forma matemática indica que n^2 es entero impar.

Ejemplo. Demostrar: si $(x + y) \geq 2$, entonces $x \geq 1 \vee y \geq 1$, para todo $x, y \in \mathbb{R}$.

Solución. Sean $p : (x + y) \geq 2$, $q : x \geq 1 \vee y \geq 1$, donde

- DeI: su contrapositiva es: si $x < 1 \wedge y < 1$, entonces $(x + y) < 2$, para todo $x, y \in \mathbb{R}$. Asumimos que $x < 1$ e $y < 1$ son ambas T, y sumamos cada desigualdad entre si obteniendo que $(x + y) < 2$ es T. Por otra parte, notar que cuando $x < 1$ e $y < 1$ son ambas F, la premisa de la contrapositiva es F, por lo que la implicación es T.
- DrA: asumimos que la premisa p y conclusión negada $\neg q$ son ambas T. Pero si $\neg q$ es T, ya vimos en el caso anterior que $\neg p$ también es T. Así llegamos a la contradicción $p \wedge \neg p$. La única chance es concluir que q es T.

Ejemplo. (demostración por casos) Probar que $|xy| = |x||y|$, con $x, y \in \mathbb{R}$, donde $|x| = x$ cuando $x \geq 0$, pero $|x| = -x$ cuando $x < 0$.

Solución. Dados los signos de x, y en los 4 cuadrantes, podemos escribir la implicación compuesta $(p_1 \vee p_2 \vee p_3 \vee p_4) \to q \equiv (p_1 \to q) \wedge (p_2 \to q) \wedge (p_3 \to q) \wedge (p_4 \to q)$, donde

a) p_1: $x \geq 0 \wedge y > 0$ (primer cuadrante). Aquí, si $x \geq 0$ e $y > 0$, entonces $xy \geq 0$, por lo que $|xy| = xy = |x||y|$;
b) p_2: $x < 0 \wedge y \geq 0$ (segundo cuadrante). Ahora, si $x < 0$ e $y \geq 0$, entonces $xy \leq 0$, por lo que $|xy| = -xy = (-x)y = |x||y|$;
c) p_3: $x < 0 \wedge y < 0$ (tercer cuadrante). Pero si $x < 0$ e $y < 0$, entonces $xy > 0$, por lo que $|xy| = xy = (-x)(-y) = |x||y|$;
d) p_4: $x \geq 0 \wedge y < 0$ (cuarto cuadrante). Finalmente, si $x \geq 0$ e $y < 0$, entonces $xy \leq 0$, por lo que $|xy| = -xy = x(-y) = |x||y|$.

Definición. Un número real x es racional si existen dos enteros p y q, con $q \neq 0$, tales que $x = p/q$. Un número real que no es racional es irracional.

Tarea. Demostrar que la implicación $((p \to q) \wedge q) \to p$ **no es** una tautología. *Comentario*: esta implicación conduce a la (conocida) falacia de "afirmar la conclusión".

Ejemplo. [posponer al parcial 2 en adelante pues requiere utilizar el teorema del binomio (o binomio de Newton)]. Demostrar que las únicas terminaciones de n^4 cuando $n = 10k + h$, donde k es un entero y $h = 0, 1, ..., 8, 9$, son 0,1,5,6. Usar una demostración por casos.

Solución: si $n > 0$ o $n < 0$, entonces $n^4 > 0$, por lo que basta el caso $n > 0$ y analizar por casos:

$$\begin{aligned}
(10k+0)^4 &= 10^4k^4 + 0^4 && \text{donde } 0^4 = 0\\
(10k+1)^4 &= 10^4k^4 + a_1k^3 + a_2k^2 + a_3k + 1^4 && \text{donde } 1^4 = 1\\
(10k+2)^4 &= 10^4k^4 + b_1k^3 + b_2k^2 + b_3k + 2^4 && \text{donde } 2^4 = 16\\
(10k+3)^4 &= 10^4k^4 + c_1k^3 + c_2k^2 + c_3k + 3^4 && \text{donde } 3^4 = 81\\
(10k+4)^4 &= 10^4k^4 + d_1k^3 + d_2k^2 + d_3k + 4^4 && \text{donde } 4^4 = 256\\
(10k+5)^4 &= 10^4k^4 + e_1k^3 + e_2k^2 + e_3k + 5^4 && \text{donde } 5^4 = 625\\
(10k+6)^4 &= 10^4k^4 + f_1k^3 + f_2k^2 + f_3k + 6^4 && \text{donde } 6^4 = 1296\\
(10k+7)^4 &= 10^4k^4 + g_1k^3 + g_2k^2 + g_3k + 7^4 && \text{donde } 7^4 = 2401\\
(10k+8)^4 &= 10^4k^4 + h_1k^3 + h_2k^2 + h_3k + 8^4 && \text{donde } 8^4 = 4096\\
(10k+9)^4 &= 10^4k^4 + i_1k^3 + i_2k^2 + i_3k + 9^4 && \text{donde } 9^4 = 6561
\end{aligned} \tag{1.17}$$

en donde observando todas las terminaciones posibles obtenidas se concluye la veracidad del enunciado.

Tarea. Demostrar que las únicas terminaciones de n^2 cuando $n = 10k + h$, donde k es un entero y $h = 0, 1, ..., 8, 9$, son 0,1,4,5,6,9.

Ejemplo. Dado un entero n cualquiera, demostrar que

(a) n es par;
(b) $n + 1$ es impar;
(c) $3n + 1$ es impar;
(d) $3n$ es par.

son equivalentes. Solución:

- Si (a), entonces (b), es decir, si (n es par), entonces ($n + 1$ es impar). Empleando una DeD: si n es par entonces, usando la definición de entero par, se tiene que $n = 2k$ donde k es algún entero. A continuación sumamos 1, lado a lado de la igualdad resultando $n + 1 = 2k + 1$, lo cual, por definición de entero impar, es entero impar.
- Si (b), entonces (c), es decir, si ($n+1$ es impar), entonces ($3n+1$ es impar). Empleando una DeD: si $n + 1$ es impar entonces, usando la definición de entero impar, se tiene que $n + 1 = 2k + 1$ donde k es entero. A continuación, multiplicamos por 3, lado a lado,

$$\begin{aligned}
3(n+1) &= 3(2k+1)\\
3n+3 &= 3\cdot 2k + 3\\
3n+1+2 &= 3\cdot 2k + 1 + 2\\
3n+1 &= 2\cdot 3k + 1\\
3n+1 &= 2\tilde{k} + 1
\end{aligned} \tag{1.18}$$

  donde $\tilde{k} = 3k$ es otro entero. Por lo cual, por definición de entero impar, $3n + 1$ es un entero impar.

- Si (c), entonces (d), es decir, si ($3n + 1$ es impar), entonces ($3n$ es par). La contrapositiva es: si ($3n$ es impar), entonces ($3n + 1$ es par). Suponemos que $3n$ es impar, o sea, $3n = 2k + 1$ donde k es un entero. A continuación sumamos 1, lado a lado, dando $3n + 1 = 2k + 1 + 1 = 2k + 2 = 2(k + 1) = 2\tilde{k}$, donde $\tilde{k} = k + 1$ es otro entero. Por lo cual, por definición de entero par, $3n + 1$ es entero par.
- Si (d), entonces (a), es decir, si ($3n$ es par), entonces (n es par). Empleando una DeI: si (n es impar), entonces ($3n$ es impar), caso que fue visto en el tercer caso.

1.6. Conjuntos

Los conjuntos se emplean para agrupar "cosas" que, generalmente, tienen propiedades parecidas, *e.g.* el conjunto de los estudiantes de una clase, un conjunto de caramelos, etc.

Definición. *Conjunto*: es una colección de *elementos*, en donde se admite la presencia de elementos repetidos y no necesariamente estar ordenados. *Elemento*: es cualquier entidad cuya naturaleza interna no interesa y puede ser cualquiera, *e.g.* letras, enteros, cadenas de caracteres, colores, figuras, personas, puntos, rectas, planos, etc. Notación: los conjuntos se representarán con letras mayúsculas, A, B, etc, y los elementos con letras minúsculas, a, b, x, y, etc.

Definición. Se dice que cada elemento **pertenece** al conjunto, y que un conjunto **contiene** a sus elementos. **Notación**: se usa $x \in A$ para denotar que el elemento x *pertenece* al conjunto A, y $x \notin A$ en caso contrario.

Definición. *Conjunto universal* U: es un conjunto especial que contiene a todos los elementos posibles bajo consideración, y cambiará según el problema considerado.

Observación. Las definiciones de conjunto y de elementos vistas aquí lo son en un sentido intuitivo y da lugar a la teoría de conjuntos "informal", en la cual se apela a la intuición para determinar como se comportan los conjuntos.

Definición. Descripción de un conjunto. Hay tres maneras:

- Por **extensión** (o por enumeración): se enumeran todos los elementos del conjunto colocándolo entre un par de llaves. Notación: $\{x_1, x_2, ..., x_n\}$ cuando n es finito, sino $\{x_1, x_2, ..., x_n, ...\}$ cuando hay una cantidad infinita de elementos;
- Por **notación constructiva** (o por **comprensión**): se caracteriza a los elementos por una propiedad que todos deben tener. Notación: $\{x \mid$ (propiedad que debe cumplir)$\}$.
- Mediante **diagramas de Venn**: es una representación gráfica en donde se representa al conjunto universal U con un gran rectángulo, los demás conjuntos con figuras cerradas cuasi-circulares, ubicadas dentro del universal, y los elementos, con puntos o marcas.

Ejemplo. Ejemplos de conjuntos por extensión:

- Tres caramelos de menta, cuatro de chocolate y tres de frutilla;

- El conjunto de las vocales: $\{a, e, i, o, u\}$;
- El conjunto de los enteros positivos impares menores a 10: $\{1, 3, 5, 7, 9\}$;
- Un conjunto arbitrario: $\{a, 2, \text{Alfredo}, \text{Grecia}, \alpha\}$.

Ejemplo. Ejemplos de conjuntos por comprensión:

- El conjunto de todos los caramelos: $\{x \mid x \text{ es un caramelo}\}$;
- $\{n \mid n \text{ es entero positivo impar menor a } 10\}$;
- $\{x \mid x \text{ es un número real}\}$ que es lo mismo que decir $\{x \mid x \in \mathbb{R}\}$;

Ejemplo. Ejemplos de conjuntos universales U: el conjunto de todas las letras del alfabeto español (que es finito); el conjunto de todos los enteros (con un número infinito de elementos).

Definición. Igualdad de dos conjuntos: dos conjuntos son iguales ssi tienen los mismos elementos. **Notación**: cuando dos conjuntos A y B son iguales se denota con $A = B$.

Observación. No interesa el orden ni la presencia de elementos repetidos aunque, cuando se pueda y por comodidad, se acostumbra listar el conjunto con los elementos ordenados según algún orden, y sin repetidos.

Ejemplo.

- Los conjuntos $\{1, 3, 5\}$ y $\{5, 1, 3\}$ son iguales, pues contienen los mismos elementos;
- Los conjuntos $\{1, 3, 5\}$ y $\{1, 5, 5, 5, 1, 5, 1, 1, 3, 3\}$ son iguales, pues contienen los mismos elementos;
- Los conjuntos pueden tener a otros conjuntos como elementos, e.g. $\{\emptyset, \{a\}, \{b\}, \{a, b\}\}$ y $\{x|x \text{ es un subconjunto de } \{a, b\}\}$. Notar que ambos conjuntos son iguales.

Definición. *Conjunto vacío*: es el conjunto sin elementos. **Notación**: el conjunto vacío se denota con $\emptyset$, también con $\{\ \}$ y, para evitar confusiones, evitaremos decir conjunto nulo.

Observación. El conjunto $\emptyset$ no es lo mismo que $\{\emptyset\}$, porque en el primero no hay elementos, mientras que en el segundo, es un conjunto que contiene al conjunto vacío, y por tanto hay un elemento.

Definición. *Subconjunto*: se dice que un conjunto A es subconjunto de otro conjunto B ssi, todo elemento de A pertenece a B. **Notación**: cuando A es un sunconjunto de B se denota con $A \subseteq B$. Empleando cuantificadores se tiene que $A \subseteq B$ ssi $\forall x\ (x \in A \rightarrow x \in B)$ es T.

Observación. En general $A \subseteq B$ no es lo mismo que $B \subseteq A$, como se observa en el siguiente ejemplo.

Ejemplo. Sean los conjuntos $A = \{1, 2, 3\}$, $B = \{1, 2, 3, 4, 5\}$:

- Como A y B no tienen los mismos elementos, se tiene $A \neq B$;
- Como cada elemento de A es un elemento de B, se tiene que $A \subseteq B$;
- Pero no todo elemento de B está en A, por eso $B \nsubseteq A$;

Teorema. Para cualquier conjunto A se tiene:

i) $\emptyset \subseteq A$. *Demostración*: empleando la definición de subconjuntos expresada a través cuantificadores que, en este caso, se re-escribe como $\forall x\ (x \in \emptyset \rightarrow x \in A)$ es T. Como el conjunto vacío no tiene elementos, se sigue que $x \in \emptyset$ es siempre F, con lo cual se tienen las formas $F \rightarrow F$ o $F \rightarrow T$, las cuales son ambas T. *Comentario*: este es un ejemplo de una demostración *vacua*;

ii) $A \subseteq A$. *Demostración*: empleando la defínción de subconjuntos expresada a través cuantificadores que, en este caso, se re-escribe como $\forall x\ (x \in A \rightarrow x \in A)$ es T. Cuando $x \in A$ es T se tiene la forma $T \rightarrow T$ que es T, y cuando $x \notin A$, queda la forma $F \rightarrow F$ que también T. Luego, en cualquier caso, la implicación $\forall x\ (x \in A \rightarrow x \in A)$ es T.

Definición. *Subconjunto propio*: cuando se quiere enfatizar que un conjunto A es subconjunto de otro conjunto B pero $A \neq B$, se denota con $A \subset B$, y se dice que A es un *subconjunto propio* de B.

Observación. No confundir $\in$ (pertenencia) con $\subseteq$ (inclusión). Mientras que la relación de inclusión es transitiva, i.e. si $A \subseteq B$ y $B \subseteq C$, entonces $A \subseteq C$. En cambio, la relación de pertenencia no lo es, i.e. si $\alpha \in B$ y $B \in C$, en general $\alpha \notin C$. Por ejemplo, si bien $a \in \{a, b\}$ y $\{a, b\} \in \{\{a, b\}, \{a, b, c\}\}$, pero $a \notin \{\{a, b\}, \{a, b, c\}\}$.

Observación.

- Para demostrar que dos conjuntos A y B tiene los mismos elementos, hay que probar que cada conjunto es subconjunto del otro, *i.e.* , hay que demostrar si $A \subseteq B \wedge B \subseteq A$, entonces $A = B$;
- La observación anterior equivale a: $(\forall x\ (x \in A \rightarrow x \in B)) \wedge (\forall x\ (x \in B \rightarrow x \in A))$, que equivale a $\forall x\ (x \in A \leftrightarrow x \in B)$.

Definición. *Número de elementos (o cardinal) de un conjunto*: cuando hay n elementos **distintos** en un conjunto A, donde n es un entero finito no negativo, se dice A es un conjunto finito, y que n es el cardinal de A. El cardinal de A se denota con $n = |A|$. Cuando A no es finito, entonces se dice que es un conjunto infinito.

Ejemplo.

- Como el conjunto vacío no tiene elementos, se tiene que $|\emptyset| = 0$;
- El conjunto de enteros, y el conjunto de los enteros positivos son infinitos;
- Los conjuntos $A = \{1, 3, 5\}$ y $B = \{1, 5, 5, 5, 1, 5, 1, 1, 3, 3\}$ tienen el mismo cardinal $n = |A| = |B| = 3$.

Definición. *Conjunto de partes de un conjunto (o conjunto potencia)*: dado un conjunto A, el conjunto de partes de un conjunto (o conjunto potencia), es el conjunto formado por todos los subconjuntos de A, y se denota con $\mathcal{P}(A)$.

Ejemplo.

- El conjunto de partes del conjunto $A_3 = \{a, b, c\}$ es el conjunto de subconjuntos $\mathcal{P}(A_3) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$;
- El conjunto de partes del conjunto vacío tiene exactamente 1 único elemento: el conjunto vacío, i.e. $\mathcal{P}(\emptyset) = \{\emptyset\}$;

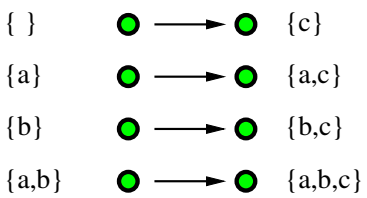

Figura 1.1: Coordinación de subconjuntos de $\{a, b, c\}$: los que contienen al elemento a (izq.), y los que no lo contienen (der.).

- El conjunto de partes del conjunto $\{\emptyset\}$ tiene exactamente 2 elementos: el conjunto vacío y el mismo conjunto $\{\emptyset\}$, i.e. $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$;
- De lo anterior se concluye que $|\mathcal{P}(\emptyset)| = 1$, y $|\mathcal{P}(\{\emptyset\})| = 2$.

Coordinación entre los elementos de dos conjuntos potencia que difieren en un elemento

Interesa ver la coordinación entre los elementos de $\mathcal{P}(A_n)$ y de $\mathcal{P}(A_{n+1})$, para lo cual antes vemos un caso simple. Por ejemplo, sea el conjunto finito $A_3 = \{a, b, c\}$, formado por tres elementos, entonces $\mathcal{P}(A_3)$ lo podemos separar en dos grupos, a saber:

- Todos los subconjuntos que no-contienen al elemento c, o sea los subconjuntos $\emptyset$, $\{a\}$, $\{b\}$, y $\{a, b\}\}$, ver Fig. 1.1 (izq.);
- Todos los subconjuntos que si-contienen al elemento c, o sea los subconjuntos $\{c\}$, $\{a, c\}$, $\{b, c\}$, y $\{a, b, c\}\}$; ver Fig. 1.1 (der.);
- Notar que el primer grupo (a la izq.) corresponde a todos los subconjuntos del conjunto $A_2 = \{a, b\}$;
- Notar que a partir del primer grupo (a la der.), al agregar el elemento c en cada caso, se obtienen los subconjuntos del segundo grupo (a la der.);
- Notar que cada subconjunto que no-contiene al elemento c, se lo puede coordinar de un modo único con un subconjunto que si lo contiene;
- Por eso, exactamente la *mitad* de los subconjuntos de $\mathcal{P}(A_3)$ contienen al elemento c, y la otra mitad no;
- Esta propiedad de coordinación entre los elementos de $\mathcal{P}(A_2)$ y $\mathcal{P}(A_3)$ es general para cualquier número finito de elementos n, y será de utilidad en el teor. 3.3 para demostrar una fórmula para el número de elementos en el conjunto potencia $\mathcal{P}(A_n)$ del conjunto A_n en función de n.

Definición. *Tupla*: la n-tupla *ordenada* $(a_1, a_2, ..., a_n)$ es la colección ordenada en la que a_1 es el primer elemento, a_2 es el segundo elemento, ..., a_n es el n-ésimo elemento.

Definición. Igualdad de dos tuplas. Las tuplas $(a_1, a_2, ..., a_n)$ y $(b_1, b_2, ..., b_n)$ son iguales ssi $a_1 = b_1$, y $a_2 = b_2$, ..., y $a_n = b_n$.

Observación. En las evaluaciones no confundir las notaciones: $\{a, c, ..., z\}$ para conjuntos, y $(a, c, ..., z)$ para tuplas.

Ejemplo.

- Las duplas (a, b) y (c, d) son iguales, ssi $a = c$ y $b = d$;

- Las duplas (a, b) y (b, a) no son iguales, a menos que $a = b$.

Definición. *Producto cartesiano* de dos conjuntos: el producto cartesiano de los conjuntos A y B se denota con $A \times B$, y es el conjunto formado por todos los pares ordenados (a, b), donde $a \in A$ y $b \in B$. En símbolos: $A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$.

Observación. Los productos cartesianos $A \times B$ y $B \times A$ no son iguales a menos que: $A = B$, o bien $A = \emptyset$, o bien $B = \emptyset$, o bien $A = B = \emptyset$.

Ejemplo. Justificar en cada caso si es T o F:

- $\emptyset \in \{\}$ (alternativas $\{\} \in \emptyset$, $\{\} \in \{\}$, $\emptyset \in \emptyset$): Sol.: como la pertenencia (símbolo $\in$) describe si un elemento pertenece (o no) a un conjunto, y como $\emptyset$ por definición no tiene elementos, se concluye que $\emptyset \in \{\}$ es F.
- $\emptyset \subseteq \{\emptyset\}$ (alternativas: $\{\} \subseteq \emptyset$, $\{\} \subseteq \{\}$, $\emptyset \subseteq \emptyset$): Sol.: como la inclusión (símbolo $\subseteq$) describe si un conjunto es (o no) un subconjunto de otro conjunto, y como $\emptyset$ es subconjunto de todo conjunto, se concluye que $\emptyset \subseteq \{\}$ es T.
- $\{\emptyset\} \subseteq \emptyset$ (alternativas: $\{\{\}\} \subseteq \emptyset$, $\{\{\}\} \subseteq \{\}$, $\{\emptyset\} \subseteq \{\}$): Sol.: como el elemento $\emptyset$ del conjunto $\{\emptyset\}$ no es un elemento del conjunto $\emptyset$, porque $\emptyset$ no tiene elementos, se concluye que $\{\emptyset\} \subseteq \emptyset$ es F;
- $\emptyset = \{\emptyset\}$: (alternativas: $\{\} = \{\emptyset\}$, $\{\} = \{\{\}\}$, $\emptyset = \{\{\}\}$): Sol.: si bien $\emptyset \subseteq \{\emptyset\}$ es T pero $\{\emptyset\} \subseteq \emptyset$ es F, por lo que $\emptyset = \{\emptyset\}$ es F;
- $A \subseteq A$: Sol.: como un conjunto A es un subconjunto de si mismo, $A \subseteq A$ es T (hay un teorema al respecto);
- $A \subset A$: Sol.: como un conjunto A no puede ser a la vez un subconjunto propio de si mismo, $A \subset A$ es F.

1.7. Operaciones con conjuntos

Definición. *Unión de dos conjuntos*: la unión de los conjuntos A y B es el conjunto que contiene los elementos que, o bien están en A, o bien están en B, o bien están en ambos. **Notación**: La unión de los conjuntos A y B se denota con $A \cup B$. **Simbología**: $A \cup B = \{x \mid (x \in A) \vee (x \in B)\}$.

Definición. *Intersección de dos conjuntos*: la intersección de los conjuntos A y B es el conjunto que contiene los elementos que están tanto en A como en B. **Notación**: La intersección de los conjuntos A y B se denota con $A \cap B$. **Simbología**: $A \cap B = \{x \mid (x \in A) \wedge (x \in B)\}$.

Definición. *Diferencia de dos conjuntos*: la diferencia de los conjuntos A y B es el conjunto que contiene los elementos que están en A pero no en B. **Notación**: La diferencia de los conjuntos A y B se denota con $A - B$. **Simbología**: $A - B = \{x \mid (x \in A) \wedge (x \notin B)\}$. $B - A = \{x \mid (x \in B) \wedge (x \notin A)\}$. Notar que, en general, $A - B \neq B - A$.

Definición. *Diferencia simétrica de dos conjuntos*: la diferencia simétrica de los conjuntos A y B es el conjunto que contiene los elementos que están en A o bien que están en B, pero no en ambos. **Notación**: La diferencia simétrica de los conjuntos A y B se denota con $A \oplus B$. **Simbología**: $A \oplus B = \{x \mid ((x \in A) \wedge (x \notin B) \vee (x \in B) \wedge (x \notin A))\}$. Tarea: probar que $A \oplus B = B \oplus A$; **Igualdad 1**: $A \oplus B = (A - B) \cup (B - A)$; **Igualdad 2**: $A \oplus B = (A \cup B) - (A \cap B)$.

Definición. *Complemento de un conjunto*. Sea U el conjunto universal. El complemento del conjunto A es la diferencia $U - A$, o sea, es el conjunto que contiene los elementos que están en U pero no están en A. **Notación**: El complemento del conjunto A se denota con $\overline{A}$. **Simbología**: $\overline{A} = \{x \mid x \notin A\}$.

Tarea. Para los conjuntos A y B, trazar los diagramas de Venn de:

- La unión $A \cup B$;
- La intersección $A \cap B$;
- Las diferencias $A - B$ y $B - A$;
- Las diferencias simétricas $A \oplus B$ y $B \oplus A$;
- Los complementos $\overline{A}$ y $\overline{B}$.

Ejemplo. Sean los conjuntos $A = \{1, 2, 3, 4\}$, $B = \{3, 4, 5, 6, 7\}$, y el universal $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 0\}$:

- Unión: $A \cup B = \{1, 2, 3, 4, 5, 6, 7\}$;
- Intersección: $A \cap B = \{3, 4\}$;
- Las diferencia $A - B = \{1, 2\}$ y $B - A = \{5, 6, 7\}$. Notar que, en general, $A - B \neq B - A$;
- Diferencias simétricas: $A \oplus B = (A - B) \cup (B - A) = \{1, 2, 5, 6, 7\}$, y $B \oplus A = (B - A) \cup (A - B) = \{1, 2, 5, 6, 7\}$. Notar que $A \oplus B = B \oplus A$.
- Diferencia simétrica (bis): $A \oplus B = (A \cup B) - (A \cap B) = \{1, 2, 5, 6, 7\}$, y $B \oplus A = (B \cup A) - (B \cap A) = \{1, 2, 5, 6, 7\}$;
- Complementos: $\overline{A} = U - A = \{5, 6, 7, 8, 9, 0\}$ y $\overline{B} = U - B = \{1, 2\}$;

Ejemplo. En la Tabla 1.22 se listan identidades de conjuntos de uso muy frecuente.

Observación. *Igualdad de dos conjuntos*: en el texto de referencia se emplean 3 métodos para probar que los conjuntos A y B son iguales, i.e. probar que $A = B$ equivale a demostrar:

a) Por *doble inclusión*, i.e. si se logra probar que $A \subseteq B$ y $B \subseteq A$, entonces $A = B$;
b) Utilizado *notación constructiva* de conjuntos;
c) Utilizando Tablas de Pertenencia (TP) (sólo en el Rosen): se toma un elemento x y se considera cada combinación de conjuntos a la que puede pertenecer, verificando que los elementos de una misma combinación pertenecen a ambos conjuntos de la identidad a comprobar. Para indicar que un elemento x pertenece a un conjunto se indica con 1, y con 0 en caso contrario. Notar que las TP son prácticamente muy similares a las TV.

Ejemplo. Probar que $A \cap (A \cup B) = A$. Solución:

	Identidad	Ley
1	$A \cup \emptyset = A$ $A \cap U = A$	identidad
2	$A \cup U = U$ $A \cap \emptyset = \emptyset$	dominación
3	$A \cup A = A$ $A \cap A = A$	idempotencia
4	$\overline{\overline{A}} = A$	doble complemento
5	$A \cup B = B \cup A$ $A \cap B = B \cap A$	conmutativas
6	$(A \cup B) \cup C = A \cup (B \cup C)$ $(A \cap B) \cap C = A \cap (B \cap C)$	asociativas
7	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	distributivas
8	$\overline{A \cup B} = \overline{A} \cap \overline{B}$ $\overline{A \cap B} = \overline{A} \cup \overline{B}$	De Morgan
9	$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	absorción
10	$A \cup \overline{A} = U$ $A \cap \overline{A} = \emptyset$	complemento

Tabla 1.22: Tabla de identidades entre conjuntos de uso muy frecuente.

a) **Por doble inclusión**. La igualdad $A \cap (A \cup B) = A$ significa que $A \cap (A \cup B) \subseteq A$ y que $A \subseteq A \cap (A \cup B)$. En ese caso:

a] Suponga que $A \subseteq A \cap (A \cup B)$. Entonces:

- Por definición de inclusión se tiene que $(x \in A) \rightarrow (x \in (A \cap (A \cup B)))$;
- Luego, por definición de intersección, se tiene que $(x \in A) \rightarrow ((x \in A) \wedge x \in (A \cup B))$;
- Luego, por definición de unión se tiene que $(x \in A) \rightarrow (x \in A) \wedge ((x \in A) \vee (x \in B))$;
- Introduciendo ahora el cambio de notación $p \equiv x \in A$, y $q \equiv x \in B$, la expresión lógica anterior se re-escribe como $p \rightarrow (p \wedge (p \vee q))$;
- Luego, por ley de absorción, se tiene que $p \rightarrow p \equiv \mathrm{T}$.

Con lo que se concluye que la implicación $(x \in A) \rightarrow [x \in (A \cap (A \cup B))]$ es una tautología) (independiente de si $x \in A$ es T o es F).

ii) Ahora, suponga que $A \cap (A \cup B) \subseteq A$. Entonces

- Por definición de inclusión se tiene que $x \in (A \cap (A \cup B)) \rightarrow (x \in A)$;
- Luego, por definición de intersección se tiene que $(x \in A \wedge x \in (A \cup B)) \rightarrow (x \in A)$;
- Luego, por definición de unión, se tiene que $(x \in A \wedge (x \in A \vee x \in B)) \rightarrow (x \in A)$;
- Introduciendo ahora el cambio de notación $p \equiv x \in A$, y $q \equiv x \in B$, la expresión lógica anterior se re-escribe como $(p \wedge (p \vee q)) \rightarrow p$;
- Luego, por ley de absorción, se tiene que $p \rightarrow p \equiv \mathrm{T}$.

Con lo que se concluye que la implicación $x \in (A \cap (A \cup B)) \rightarrow (x \in A)$ es una tautología) (independiente de si $x \in A$ es T o es F).

iii) Finalmente, como $L_I \subseteq L_D$ y $L_D \subseteq L_I$ son ambas T, entonces se concluye que

A	B	$A \cup B$	$A \cap (A \cup B)$
0	0	0	0
1	0	1	1
0	1	1	0
1	1	1	1

Tabla 1.23: Demostración de la ley de absorción $A \cap (A \cup B) = A$ para todos los conjuntos A y B mediante una tabla de pertenencia: como las columnas para A y para $A \cap (A \cup B)$ son las mismas, entonces la ley es válida.

$L_I = L_D$ es T.

b) Solución utilizando *notación constructiva* de conjuntos:

$$\begin{aligned} A \cap (A \cup B) &= \{x \mid x \in (A \cap (A \cup B))\} \\ &= \{x \mid (x \in A) \wedge x \in (A \cup B)\} \\ &= \{x \mid (x \in A) \wedge (x \in A \vee x \in B)\} \\ &= \{x \mid p \wedge (p \vee q)\} \\ &= \{x \mid (p \wedge p) \vee (p \wedge q)\} \\ &= \{x \mid p \vee (p \wedge q)\} \\ &= \{x \mid p\} \\ &= \{x \mid x \in A\} \\ &= A \end{aligned} \tag{1.19}$$

c) Solución utilizando *tablas de pertenencia*: tomamos cada combinación de conjuntos a la que puede pertenecer un elemento x, y chequeamos si los elementos de una misma combinación de conjuntos pertenecen a ambos conjuntos de la identidad. Para esto, usamos un 1 cuando un elemento pertenece a un conjunto, y un 0 cuando no pertenece, e.g. ver Tabla 1.23.

Ejemplo. Probar que $A \times (B \cup C) = (A \times B) \cup (A \times C)$. Solución (únicamente por doble inclusión):

i) Sea $(a, b) \in A \times (B \cup C)$. Entonces, por definición de producto cartesiano, $a \in A \wedge b \in (B \cup C)$. Por definición de la unión $b \in (B \cup C) \equiv b \in B \vee b \in C$. Reemplazando, $a \in A \wedge (b \in B \vee b \in C)$, haciendo distributiva $(a \in A \wedge b \in B) \vee (a \in A \wedge b \in C)$, es decir, $(a, b) \in (A \times B \vee A \times C)$. por lo que $L_I \subseteq L_D$.

ii) Sea $(a, b) \in (A \times B) \cup (A \times C)$. Entonces, por definición de unión $(a, b) \in (A \times B) \vee (a, b) \in (A \times C)$. Por definición de producto cartesiano $(a \in A \wedge b \in B) \vee (a \in A \wedge b \in C)$. Sacando factor común queda $a \in A \wedge (b \in B \vee b \in C)$. Por definición de unión $a \in A \wedge (b \in (B \cup C))$. Por definición de producto cartesiano, $(a, b) \in A \times (B \cup C)$. por lo que $L_D \subseteq L_I$.

iii) Finalmente, como $L_I \subseteq L_D$ y $L_D \subseteq L_I$ son ambas T, entonces se concluye que $L_I = L_D$ es T.

Ejemplo. Determinar el VV de

1) $A - B = B - A$;
2) $\overline{(A \cap B)} \subseteq A$;

3) $(A \cap B) \cup (B - A) = B$;

para todos los conjuntos A y B. Solución: los dos primeros ejemplos son falsos, donde un contraejemplo común es tomar $A = \{1, 2, 3\}$, $B = \{4, 5, 6\}$, y el conjunto universal $U = \{1, 2, 3, 4, 5, 6, 7\}$. En cuanto al tercer ejemplo, utilizando notación constructiva de conjuntos en el lado izquierdo queda

$$(A \cap B) \cup (B - A) = \{x \mid (x \in A \wedge x \in B) \vee (x \in B \wedge x \notin A)\} \tag{1.20}$$

Ahora sean $p : x \in A$, $q : x \in B$, entonces queda $(p \wedge q) \vee (q \wedge \neg p)$, y utilizando una tabla de verdad en esta última proposición compuesta se observa que tiene los mismos valores de verdad que q, con lo cual se concluye que la identidad propuesta es verdadera. Tarea: corroborar utilizando (i) un diagrama de Venn, y (ii) una tabla de pertenencia.

Ejemplo. Probar que $A \cap B = A - \overline{B}$. Solución:

$$\begin{aligned} A \cap B &= \{x \mid x \in A \wedge x \in B\} \\ &= \{x \mid x \in A \wedge x \notin \overline{B}\} \\ &= \{x \mid x \in (A - \overline{B})\} \\ A - \overline{B} &= \{x \mid x \in A \wedge x \notin \overline{B}\} \\ &= \{x \mid x \in A \wedge x \in B\} \\ &= \{x \mid x \in (A \cap B)\} \end{aligned} \tag{1.21}$$

Ejemplo. Probar que $A \cap (B - C) = (A \cap B) - (A \cap C)$. Solución: Introduciendo $p \equiv x \in A$, y $q \equiv x \in B$, $r \equiv x \in C$, se tiene:

i) Tomando el lado izquierdo:

$$\begin{aligned} A \cap (B - C) &= \{x \mid x \in A \cap (B - C)\} \\ &= \{x \mid x \in A \wedge x \in (B - C)\} \\ &= \{x \mid x \in A \wedge x \in B \wedge x \notin C\} \\ &= \{x \mid p \wedge q \wedge \neg r\} \end{aligned} \tag{1.22}$$

ii) Tomando el lado derecho (notar que $\{x \mid x \notin (A - C)\} = \{x \mid x \notin A \vee x \notin C\}$):

$$\begin{aligned} (A \cap B) - (A \cap C) &= \{x \mid x \in (A \cap B) \wedge x \notin (A - C)\} \\ &= \{x \mid (x \in A \wedge x \in B) \wedge (x \notin A \vee x \notin C)\} \\ &= \{x \mid (p \wedge q) \wedge (\neg p \vee \neg r)\} \\ &= \{x \mid (p \wedge q \wedge \neg p) \vee (p \wedge q \wedge \neg r)\} \\ &= \{x \mid F \vee (p \wedge q \wedge \neg r)\} \\ &= \{x \mid p \wedge q \wedge \neg r\} \end{aligned} \tag{1.23}$$

iii) Finalmente, los lados derechos de las Ecs. (1.22-1.23) son iguales, por lo que los lados izquierdos también lo son.

Definición. *Unión generalizada (de una colección de conjuntos)*: la unión de la colección finita de conjuntos A_1, A_2 ..., A_n, es el conjunto que contiene los elementos que pertenecen al menos a uno de los conjuntos de la colección. **Notación**: usamos la notación $A_1 \cup A_2 \cup ... \cup A_n = \bigcup_{i=1}^{n} A_i$.

Definición. *Intersección generalizada (de una colección de conjuntos)*: la intersección de la colección finita de conjuntos A_1, A_2 ..., A_n, es el conjunto que contiene aquellos elementos que pertenecen a todos los conjuntos de la colección. **Notación**: usamos la notación $A_1 \cap A_2 \cap ... \cap A_n = \bigcap_{i=1}^{n} A_i$.

Ejemplo. Sea $A_i = \{i, i+1, ...\}$, con entero positivo i, con infinitos elementos. Entonces:

- $\bigcup_{i=1}^{n} A_i = \bigcup_{i=1}^{n} \{i, i+1, ...\} = \{1, 2, 3, ...\}$;
- $\bigcap_{i=1}^{n} A_i = \bigcap_{i=1}^{n} \{i, i+1, ...\} = \{n, n+1, n+2, ...\}$;

Principio de inclusión-exclusión (o de la criba) [Ref.: Sec. 6.5, p. 420, Rosen]

El Principio de Inclusión-Exclusión (PIE) (o principio de la criba) es un recurso muy útil en problemas de conteo en donde intervienen conjuntos finitos. En lo que sigue seguiremos la presentación de Biggs (1998):

1) Si los conjuntos finitos A y B son *disjuntos* (o sea, $A \cap B = \emptyset$) se tiene que:

$$|A \cup B| = |A| + |B| \tag{1.24}$$

Ejemplo. Sean los conjuntos $A = \{a, b, c\}$ y $C = \{d, e\}$. En este caso $A \cup C = \{a, b, c, d, e\}$ pero $A \cap C = \emptyset$. En este caso $|A| = 3$ y $|C| = 2$, verificándose que $|A \cup C| = 3 + 2 = 5$.

2) Pero si los conjuntos finitos A y B no son disjuntos (o sea, $A \cap B \neq \emptyset$), al sumar $|A|$ y $|B|$, estamos contando dos veces los elementos que están en $A \cap B$.

Ejemplo. Sean los conjuntos $A = \{a, b, c\}$ y $B = \{b, c, d, e\}$. Ahora tenemos que $A \cap B = \{b, c\}$ y $A \cup B = \{a, b, c, d, e\}$, por lo que $|A| = 3$ y $|B| = 4$, pero $|A \cup B| = 5$.

Para corregirlo, notar que basta restar el número de elementos que fueron contados en forma doble, o sea, aquellos que están en $A \cap B$, es decir,

$$|A \cup B| = |A| + |B| - |A \cap B| \tag{1.25}$$

Ejemplo. En el caso del ejemplo anterior $|A \cap B| = 2$, y usando la Ec. (1.25) resulta que $|A \cup B| = 3 + 4 - 2 = 5$, como debe ser.

3) En el caso de tres conjuntos finitos A, B y C, al sumar $|A|$, $|B|$ y $|C|$, los elementos de $A \cap B$, $B \cap C$, y $C \cap A$ los contamos dos veces (si es que no están en los tres conjuntos simultáneamente), mientras que los elementos de $A \cap B \cap C$ los hemos contado tres veces. Para corregirlo, restamos $|A \cap B|$, $|B \cap C|$, y $|C \cap A|$. Pero al hacerlo los elementos de $A \cap B \cap C$, que inicialmente fueron contados tres veces, ahora han sido quitados

tres veces, por lo que a continuación hay que sumar $|A \cap B \cap C|$. Así se deduce la expresión

$$\begin{aligned} |A \cup B \cup C| &= \alpha_1 - \alpha_2 + \alpha_3 \\ \alpha_1 &= |A| + |B| + |C| \\ \alpha_2 &= |A \cap B| + |A \cap C| + |B \cap C| \\ \alpha_3 &= |A \cap B \cap C| \end{aligned} \tag{1.26}$$

En general, se tiene el siguiente resultado (Biggs (1998)):

Enunciado. Para n conjuntos finitos A_1, A_2, ..., A_n:

$$|A_1 \cup A_2 \cup ... \cup A_n| = \alpha_1 - \alpha_2 + \alpha_3 - ... + (-1)^{n-1}\alpha_n \tag{1.27}$$

donde α_i es la suma de los cardinales de todas las intersecciones posibles de i conjuntos, con $1 \leq i \leq n$.

Ejemplo. En el caso de cuatro conjuntos finitos A, B, C, y D se tiene:

$$\begin{aligned} |A \cup B \cup C \cup D| &= \alpha_1 - \alpha_2 + \alpha_3 - \alpha_4 \\ \alpha_1 &= |A| + |B| + |C| + |D| \\ \alpha_2 &= |A \cap B| + |A \cap C| + |A \cap D| + |B \cap C| + |B \cap D| + |C \cap D| \\ \alpha_3 &= |A \cap B \cap C| + |A \cap B \cap D| + |A \cap C \cap D| + |B \cap C \cap D| \\ \alpha_4 &= |A \cap B \cap C \cap D| \end{aligned} \tag{1.28}$$

Pregunta (para el parcial 2): cuántas combinaciones de 3 conjuntos se pueden elegir entre 4 conjuntos?

Observación. El PIE es un recurso conveniente en diversas aplicaciones. Un ejemplo es en problemas de conteo (más adelante), e.g. usando los principios de conteo y el PIE, determinar el número de cadenas de 8 bits que empiezan con 101 y/o terminan con 01.

1.8. Funciones

Definición. Sean dados los conjuntos A y B. *Función* (def. 1): una función f de A en B es una asignación de un UNICO elemento de B a CADA elemento de A. *Función* (def. 2): una función f de A en B es un subconjunto del producto cartesiano $A \times B$, tal que: cumple con dos propiedades: (a) existencia: CADA elemento $a \in A$ tiene asignado un $b \in B$; (b) unicidad: CADA elemento $a \in A$ tiene asignado un UNICO $b \in B$; **Notación**: se denota $f(a) = b$, si b es el único elemento de B asignado por la función f a cada elemento de A. Además, si f es una función de A en B, entonces escribimos $f : A \to B$. **Comentario**: las *funciones* son un caso particular de las *relaciones* (ver más adelante).

Definición. *Dominio, codominio, imagen, preimagen, rango*: si f es una función de un conjunto A en otro B, decimos que A es el *dominio* de f, B es el *codominio* de f. Si $f(a) = b$, decimos que b es la *imagen* de a, y que a es la *preimagen* de b. El *rango* (o *imagen*) de la función f es el conjunto de todas las imágenes de los elementos del dominio A. Notar que, en general, rango$(f) \subseteq B$.

Observación. Especificación de una función $f: A \to B$. Entre otras, a través de:

1) Lista de pares ordenados (caso discreto);
2) Tabla de valores (caso discreto);
3) Fórmula matemática (caso discreto o continuo);
4) Diagrama de flechas (o digrafo), caso discreto;
5) Matrices (caso discreto);

Ejemplo. Subconjuntos f_1, f_2, f_3, y f_4 del producto cartesiano $A \times B$ de los conjuntos A y B, en donde $A = \{a, b, c\}$, $B = \{\alpha, \beta, \gamma, \delta\}$. En algunos son también funciones y otros no, ver Fig. 1.2:

1) $f_1 = \{(a,\beta), (b,\delta), (c,\alpha)\}$: en este caso se cumplen las condiciones de existencia y de unicidad, por lo que el subconjunto f_1 del producto cartesiano $A \times B$ es una función. Notar que el elemento γ del codominio B no tiene preimagen alguna (no importa);
2) $f_2 = \{(a,\beta), (b,\delta), (c,\beta)\}$: también se cumplen las condiciones de existencia y de unicidad. Luego, el subconjunto f_2 del producto cartesiano $A \times B$ es una función. Notar que el elemento β del codominio B tiene dos preimágenes (no importa);
3) $f_3 = \{(a,\delta), (b,\beta), (b,\gamma), (c,\alpha)\}$: notar que el elemento b del conjunto A tiene asignado dos elementos ((b,β) y (b,γ)). Luego, no se cumple la condición de unicidad, por lo que el subconjunto f_3 del producto cartesiano $A \times B$ no es una función;
4) $f_4 = \{(a,\delta), (c,\alpha)\}$: notar que el elemento b del conjunto A no tiene asignado elemento alguno en el codominio. Luego, no se cumple la condición de existencia para todos los elementos del dominio A, por lo que el subconjunto f_4 del producto cartesiano $A \times B$ no es una función.

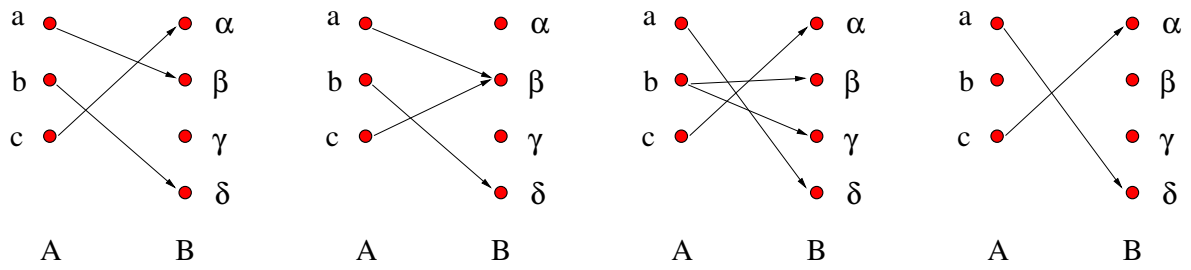

Figura 1.2: Diagramas de flechas de los subconjuntos f_1, f_2, f_3, y f_4, del producto cartesiano $A \times B$ de los conjuntos A y B. En algunos casos son funciones y en otros no.

Definición. Imagen de un subconjunto del dominio de una función (def. 4 del libro, pág. 91). Sean los conjuntos A y B, el subconjunto $C \subseteq A$, y la función f de A en B. La imagen de un subconjunto C del dominio A de la función f es el subconjunto de B formado por todas las imágenes de los elementos de C. **Notación**: $f(C) = \{f(x) \mid \forall x \in C\}$.

Función inyectiva, sobreyectiva, y biyectiva

Definición. Función inyectiva (def. 1): se dice que una función $f: A \to B$ es *inyectiva* (o *uno a uno*), si PARA CADA $b \in B$ existe A LO SUMO un $a \in A$, tal que $f(a) = b$

(o sea, podria no-existir). Función inyectiva (def. 2): se dice que una función $f: A \to B$ es *inyectiva* (o *uno a uno*), ssi $f(x) = f(y)$ implica que $x = y$, con $x, y \in A$. En otras palabras, cuando f es inyectiva: (i) si $f(x) = f(y)$, entonces $x = y$; y (ii) si $x = y$, entonces $f(x) = f(y)$, con $x, y \in A$.

Definición. Función sobreyectiva (def. 1): se dice que una función $f: A \to B$ es *sobreyectiva* (o *suryectiva*), si el rango de f es todo B. **Notación**: rango$(f) = B$ ssi f es sobreyectiva. O sea, cuando f es sobreyectiva: (i) si rango$(f) = B$, entonces f es sobreyectiva; y (ii) si f es sobreyectiva, entonces rango$(f) = B$. Función sobreyectiva (def. 2): se dice que una función $f: A \to B$ es *sobreyectiva* (o *suryectiva*), ssi para TODO elemento $y \in B$, existe un $x \in A$ tal que $f(x) = y$.

Definición. Función biyectiva (def.): una función $f: A \to B$ es *biyectiva* cuando es inyectiva y sobreyectiva simultáneamente.

Observación. Uso de la leyes de De Morgan generalizadas (o leyes De Morgan en proposiciones cuantificadas) en funciones no inyectivas ni sobreyectivas (Sec. 2.2, pp. 94-95, Johnsonbaugh).

1) Una función $f: X \to Y$ no es inyectiva cuando $\forall x_1 \forall x_2 \, ((f_1 = f_2) \to (x_1 = x_2))$ es F, donde $f_1 = f(x_1)$, y $f_2 = f(x_2)$. Luego, su negación debe ser T y hacemos

$$\begin{aligned} &\neg(\forall x_1 \forall x_2 \, ((f_1 = f_2) \to (x_1 = x_2))) \\ &\equiv \exists x_1 \neg(\forall x_2 \, ((f_1 = f_2) \to (x_1 = x_2))) \\ &\equiv \exists x_1 \exists x_2 \, \neg((f_1 = f_2) \to (x_1 = x_2)) \\ &\equiv \exists x_1 \exists x_2 \, ((f_1 = f_2) \wedge (x_1 \neq x_2)) \end{aligned} \tag{1.29}$$

   donde se usó la EL $\neg(p \to q) \equiv \neg(\neg p \vee q) \equiv p \wedge \neg q$. En palabras, la última línea de la Ec. (1.29) expresa que una función $f(x)$ no es inyectiva si existen x_1 y x_2 tales que $f(x_1) = f(x_2)$ pero $x_1 \neq x_2$.

2) Una función $f: X \to Y$ no es sobreyectiva cuando $\forall y \exists x \, (f(x) = y)$ es F, donde $x \in X$, e $y \in Y$. Luego, su negación debe ser T y hacemos

$$\begin{aligned} &\neg(\forall y \exists x \; f(x) = y) \\ &\equiv \exists y \neg(\exists x \; f(x) = y) \\ &\equiv \exists y \forall x \; \neg(f(x) = y) \\ &\equiv \exists y \forall x \; f(x) \neq y \end{aligned} \tag{1.30}$$

   En palabras, la última línea de la la Ec. (1.30) expresa que una función $f(x)$ no es sobreyectiva si existe un $y \in Y$ tal que para todo $x \in X$ se comprueba que $f(x) \neq y$.

Función inversa, y composición de dos funciones

Definición. Función inversa (def.): sea $f: A \to B$ una función biyectiva del conjunto A en otro B. La función inversa de f es la función de $B \to A$ que asigna a cada elemento de $b \in B$ el único elemento $a \in A$ tal que $f(a) = b$, y se denota con $f^{-1} = \{(b, a) \mid (a, b) = f\}$. *Comentario*: en este contexto no confundir la notación f^{-1} con $1/f$.

Definición. Composición de dos funciones (o función de función): sean los conjuntos A, B y C, y las funciones $g\colon A \to B$ y $f\colon B \to C$. La composición de la función f con g se define con $f(g(a))$, para todo $a \in A$, siempre que Imagen$(g) \subseteq$ Dominio(f), y se denota con $(f \circ g)(a) = f(g(a))$. En símbolos:

$$g\colon A \to B \quad \text{y} \quad f\colon B \to C \quad : \quad f(g(a)) = f \circ g \quad \text{si Imagen}(g) \subseteq \text{Dominio}(f) \tag{1.31}$$

Ejemplo. Sean $g\colon A \to A$ y $f\colon A \to C$, con $A = \{a, b, c\}$, y $C = \{1, 2, 3\}$, donde $g = \{(a, b), (b, c), (c, a)\}$ y $f = \{(a, 3), (b, 2), (c, 1)\}$. Como Imagen$(g) \subseteq$ Dominio(f), la composición $f \circ g$ es posible, y es: $f(g(a)) = f(b) = 2$, $f(g(b)) = f(c) = 1$, y$f(g(c)) = f(a) = 3$. Pero como Imagen$(f) \nsubseteq$ Dominio(g), no es posible hallar $g \circ f$.

Algunas funciones importantes: función piso y función techo

Definición. Función piso (o parte entera) (def.): asigna al número real x el MAYOR entero que es menor o igual que x, y se denota con $\lfloor x \rfloor$.

Definición. Función techo (o parte entera por exceso) (def.): asigna al número real x el MENOR entero que es mayor o igual que x, y se denota con $\lceil x \rceil$.

Observación. Prestar atención cuando x es positivo, cero o negativo. Se tiene:

- La función piso $\lfloor x \rfloor$ siempre asigna el entero más cercano a x "mirando hacia" $-\infty$, e.g. piso $(+2.345) = +2$ pero piso $(-2.345) = -3$;
- La función techo $\lceil x \rceil$ siempre asigna el entero más cercano a x "mirando hacia" $+\infty$, e.g. techo $(+6.789) = +7$ pero techo $(-6.789) = -6$.

Ejemplo. Sean las funciones $g\colon A \to B$ y $f\colon B \to C$. Demuestre o dé un contraejemplo en cada caso:

1) Si f y $(f \circ g)$ son sobreyectivas, entonces g >es también sobreyectiva? Rpta: es F, contraejemplo: sea los conjuntos $A = \{a\}$, $B = \{2, 3\}$, y $C = \{\delta\}$, y las funciones $g = \{(a, 2)\}$, y $f = \{(2, \delta), (3, \delta)\}$. Se tiene que $(f \circ g) = \{(a, \delta)\}$, con lo cual se tiene que f y $(f \circ g)$ son sobreyectivas pero g no lo es.
2) Si f y g son inyectivas, entonces $(f \circ g)$ >es también inyectiva? Rpta. Sean los elementos a y b distintos en A. En ese caso:
   - Como $g\colon A \to B$ es inyectiva, hay unicidad de su preimagen, por lo que $g(a)$ y $g(b)$ son elementos distintos en B;
   - Como $f\colon B \to C$ es inyectiva, hay unicidad de su preimagen, por lo que $f(g(a))$ y $f(g(b))$ son elementos distintos en C;
   - Lo anterior vale para todo $a, b \in A$, con $a \neq b$. Se concluye que $(f \circ g)$ es inyectiva cuando f y g también lo son.
3) Si f y g son sobreyectivas, entonces $(f \circ g)$ >es también sobreyectiva? Rpta. Sea un elemento $c \in C$. En ese caso:

- Como $f\colon B \to C$ es sobreyectiva, entonces para todo $c \in C$ se tiene que $c = f(b)$ para algún $b \in B$;
- Como $g\colon A \to B$ es sobreyectiva, entonces para todo $b \in B$ se tiene que $b = g(a)$ para algún $a \in A$;
- Eso significa que $c = f(b) = f(g(a))$. Esto vale para todo $c \in C$, por lo que se concluye que $(f \circ g)$ es sobreyectiva cuando f y g también lo son.

CAPÍTULO 2

Los fundam.: algor., enteros y matrices

Nota. Estas notas siguen el texto de referencia Rosen (2004) manteniendo la numeración de las secciones y sus títulos, como una referencia adicional para el auto-estudio siguiendo ese texto.

Contents

2.1. Algoritmos

Omitir (la gente de FICH lo verá en Algoritmos y Estructuras de Datos (AED), y la de FIQ en Computación / Programación (COP)).

2.2. Crecimiento de funciones

Omitir (pues la gente de FICH lo verán en AED).

2.3. Complejidad de algoritmos

Omitir (pues la gente de FICH lo verán en AED).

2.4. Enteros y división

División

Definición. Divisor (def.): sean los enteros A y D, con $D \neq 0$. Se dice que D divide al entero A si existe un entero Q tal que $A = QD$, donde A es el *dividendo*, Q es el *cociente*, y D es el *divisor*. Cuando D divide al entero A, también se dice que D es un factor (o un divisor) de A, o que D es un múltiplo de A. **Notación**: cuando el entero $D \neq 0$ divide al entero A, se denota con $D|A$, y equivale a $\exists Q\,(A = QD)$ para todos los enteros $A, D, Q \in \mathbb{Z}$, siempre que $Q \neq 0$.

Ejemplo. $3|12$ pues $12/3 = 4$, mientras que $4 \not| 11$ pues $11/4 = 2.75$.

Teorema. Sean los enteros a, b, y c. Se tiene:

$$\begin{array}{l} \text{(i) Si } a|b, \text{ y } a|c, \text{ entonces } a|(b+c) \\ \text{(ii) Si } a|b, \text{ entonces } a|(bc) \\ \text{(iii) Si } a|b, \text{ y } b|c, \text{ entonces } a|c \end{array} \tag{2.1}$$

Demostración:

(i) Suponga que $a|b$ y que $a|c$. Entonces, por definición de divisor, se tiene:

$$\begin{array}{ll} b = pa & \text{donde } p \text{ es un entero} \\ c = qa & \text{donde } q \text{ es un entero, y sumando ambas igualdades} \\ \hline b + c = (p+q)a & \text{pero } (p+q) \text{ es otro entero} \end{array} \tag{2.2}$$

y se concluye que a divide a $b + c$.

(ii) Suponga que $a|b$, entonces, por definición de divisor, se tiene que

$$\begin{array}{ll} b = ka & \text{para algún entero } k, \text{ multiplicando lado a lado por } c \\ \hline cb = c(ka) & \text{reasociando factores en el lado derecho} \\ cb = (ck)a & \text{pero } (ck) \text{ es otro entero, por lo que } a \text{ divide a } cb \end{array} \tag{2.3}$$

y se concluye que a divide a cb.

(iii) Para el hogar.

Números primos

Definición. Número primo (def.): un entero positivo p mayor a 1 es primo cuando sus únicos divisores positivos son 1 y p. **Número compuesto**: un entero mayor a 1 es compuesto cuando no es primo.

Observación. Si un entero positivo $n > 1$ es compuesto, entonces tiene al menos un divisor positivo d distinto de 1 y de sí mismo. Para verlo:

(i) Como d es positivo y $d \neq 1$, debe ser $d \geq 2$;
(ii) Como d es un divisor de n y $d \neq n$, debe ser $d < n$.

Por eso, en principio, para chequear si un entero positivo n es compuesto, habría que revisar si alguno de los enteros $2 \leq d < n$, es decir, si 2, 3, ..., $(n-1)$ dividen a n, y si no hay ninguno entonces n es primo. Pero, en realidad, el rango de enteros a revisar es más reducido, según el siguiente teorema.

Teorema. Un entero positivo n mayor a 1 es compuesto ssi n tiene un divisor d tal que $2 \leq d \leq \sqrt{n}$.

i) Si (n es un entero compuesto), entonces (n tiene un divisor d tal que $2 \leq d \leq \sqrt{n}$). Demostración. Supongamos que n es un entero compuesto, entonces, n tiene un divisor e tal que $2 \leq e < n$. Hay dos casos:

- Caso en que $e \leq \sqrt{n}$. Si así fuera, entonces n tiene un divisor e que satisface $2 \leq e \leq \sqrt{n}$;
- Caso en que $e > \sqrt{n}$. Si así fuera, como e divide a n, entonces existe un entero q tal que $n = qe$, por lo cual q también es un divisor de n. A continuación, usaremos contradicción para concluir que $q \leq \sqrt{n}$. Supongamos en contrario que fuera $q > \sqrt{n}$ (cuidado: hay un error tipográfico en el texto de Johnsonbaugh). Entonces

$$\begin{array}{ll} e > \sqrt{n} & \text{es el segundo caso} \\ q > \sqrt{n} & \text{multiplicando lado a lado ambas desigualdades} \\ \hline eq > \sqrt{n}\sqrt{n} & \text{pero el lado izquierdo es } eq = n, \text{ luego} \\ n > n & \end{array} \tag{2.4}$$

pero a última desigualdad es una contradicción. Por eso, debe ser $q \leq \sqrt{n}$.

ii) Si (n tiene un divisor d tal que $2 \leq d \leq \sqrt{n}$), entonces (n es un entero compuesto). Demostración. Si n tiene un divisor d tal que $2 \leq d \leq \sqrt{n}$ entonces, por defínción de entero compuesto, n es compuesto.

Ejemplo. (se puede omitir). Algoritmo de la criba de Eratóstenes para determinar si un entero positivo n es primo o compuesto.

```
1  import math
2  def es_primo (n):
3      """Retorna True si el entero positivo n es primo sino retorna False"""
4      # caso n < 2
5      if (n < 2): # no es primo
6          return False
7      else:
8          r = int (math.floor(math.sqrt(n)))
9          for d in range(2,r+1):
10             h = n %d
11             if (h == 0):
12                 return False
13         return True
```

Enunciado. Teorema fundamental de la aritmética: todo entero n mayor a 1 se puede expresar como el producto de primos. Si los primos se escriben en orden no decreciente, entonces la factorización es única. En símbolos, si $n = p_1 p_2 ... p_i$, donde todos son primos

tales que $p_1 \leq p_2 \leq ... \leq p_i$, y si $n = p'_1 p'_2 ... p'_j$, donde todos son primos tales que $p'_1 \leq p'_2 \leq ... \leq p'_z$, entonces $i = j = z$, y $p_k = p'_k$, para $k = 1, 2, ..., z$.

Enunciado. El número de primos es infinito.

Enunciado. Teorema de los número primos. El cociente del número z de primos menores o iguales a x y $x/\ln(x)$ tiende a 1 cuando $x \to \infty$.

Algoritmo de la división

Definición. Cociente-residuo (en lugar de "algoritmo de la división"): sea a un entero y d un entero positivo, entonces existen dos enteros q y r únicos tales que $a = qd + r$, donde $0 \leq r < d$.

Observación.

- Hay un error de tipeo en la def. dada en pág. 145 del Rosen.
- Preferimos decir "cociente-residuo" en lugar de "algoritmo de la división" pues esta última, si bien es tradicional, es conflictiva pues esta definición no es un algoritmo.

Definición. En la igualdad $a = qd + r$ definida por el algoritmo de la división, donde $0 \leq r < d$:

- Se dice que a es el *dividendo*, d es el *divisor*, q es el *cociente*, y r es el *resto*.
- Se introducen las notaciones: $q = a \text{ div } d$, $r = a \bmod d$.

Máximo común divisor y mínimo común múltiplo

Definición. Máximo común divisor (def.). Sean los enteros positivos α y β. Un divisor común de α y de β es un entero k que divide tanto a α como a β. El Máximo Común Divisor (MCD) de α y β es el divisor común positivo más grande. **Notación**: el MCD de los enteros positivos α y β se denota con $\text{mcd}(\alpha, \beta)$.

Ejemplo. Calcular el mcd (30,105).

Solución. Primero usamos la definición:

$$\begin{aligned} \text{divisores\_positivos (30)} &= \{1, 2, 3, 5, 6, 10, 15, 30\} \\ \text{divisores\_positivos (105)} &= \{1, 3, 5, 5, 7, 15, 21, 35, 105\} \\ \text{divisores\_comunes (30,105)} &= \{1, 3, 5, 15\} \\ \text{mcd (30,105)} &= \max(\text{divisores\_comunes (30,105)}) = 15 \end{aligned} \tag{2.5}$$

Por otra parte, notar que

$$\begin{aligned} \text{factorizacion\_factores\_primos (30)} &= 2 \cdot 3 \cdot 5 = 2 \cdot 3 \cdot 5 \cdot 7^0 \\ \text{factorizacion\_factores\_primos (105)} &= 3 \cdot 5 \cdot 7 = 2^0 \cdot 3 \cdot 5 \cdot 7 \\ \text{mcd (30,105)} &= 2^0 \cdot 3 \cdot 5 \cdot 7^0 = 15 \end{aligned} \tag{2.6}$$

Este segundo cómputo es un resultado general y que descripto por el enunciado del siguiente teorema:

Enunciado. Sean dos enteros α y β mayores a 1 con factorizaciones primas

$$\begin{aligned} \alpha &= p_1^{a_1} p_2^{a_2} ... p_h^{a_h} \\ \beta &= p_1^{b_1} p_2^{b_2} ... p_h^{b_h} \end{aligned} \tag{2.7}$$

en donde si el primo p_i no es factor del entero α, entonces se hace $a_i = 0$, y del mismo modo para β, mientras que h es el número total de primos juntando las factorizaciones en primos de α y de β. Entonces se cumple que

$$\text{mcd}(\alpha, \beta) = p_1^{\text{mín}\,(a_1,b_1)} p_2^{\text{mín}\,(a_2,b_2)} ... p_h^{\text{mín}\,(a_h,b_h)} \tag{2.8}$$

Ejemplo. Calcular el mcd (82 320,950 796).

Solución: usando el teorema

$$\begin{aligned} \text{factorizacion\_factores\_primos } (82\,320) &= 2^4 \cdot 3^1 \cdot 5^1 \cdot 7^3 \cdot 11^0 \\ \text{factorizacion\_factores\_primos } (950\,796) &= 2^2 \cdot 3^2 \cdot 5^0 \cdot 7^4 \cdot 11^1 \\ \text{mcd } (82\,320{,}950\,796) &= 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^3 \cdot 11^0 = 4116 \end{aligned} \tag{2.9}$$

Definición. Mínimo común múltiplo (def.). Sean los enteros positivos α y β. Un múltiplo común de α y de β es un entero k que es divisible tanto por α como por β. El Mínimo Común Múltiplo (MCM) de α y n es el divisor común positivo más pequeño. **Notación**: el MCM de los enteros positivos α y β se denota con mcm(α, β).

Ejemplo. Calcular el mcm (30,105).

Solución: primero usamos la definición

- El 105 es divisible por 105 pero no por 30;
- El que le sigue es 210 que sí es divisible tanto por 105 como por 30;
- Como 210 es el divisible común a 105 y 30 más chico, entonces mcm (30,105) = 210.

Otra vez, podemos hacer

$$\begin{aligned} \text{factorizacion\_factores\_primos } (30) &= 2 \cdot 3 \cdot 5 = 2 \cdot 3 \cdot 5 \cdot 7^0 \\ \text{factorizacion\_factores\_primos } (105) &= 3 \cdot 5 \cdot 7 = 2^0 \cdot 3 \cdot 5 \cdot 7 \\ \text{mcm } (30{,}105) &= 2^1 \cdot 3 \cdot 5 \cdot 7^1 = 210 \end{aligned} \tag{2.10}$$

Notar que la factorización prima de mcm (30,105) debe contener a los factores 2, 3, 5 para que de ese modo 30 pueda dividir a mcm (30,105). Del mismo modo, la factorización prima de mcm (30,105) también debe contener a los factores 3, 5, 7 para que de ese modo 105 pueda dividir a mcm (30,105). Este segundo cómputo es un resultado general y que descripto por el enunciado del siguiente teorema:

Enunciado. Sean dos enteros α y β mayores a 1 con factorizaciones primas

$$\begin{aligned} \alpha &= p_1^{a_1} p_2^{a_2} ... p_h^{a_h} \\ \beta &= p_1^{b_1} p_2^{b_2} ... p_h^{b_h} \end{aligned} \tag{2.11}$$

en donde si el primo p_i no es factor del entero α, entonces se hace $a_i = 0$, y del mismo modo para β, mientras que h es el número total de primos juntando las factorizaciones en primos de α y de β. Entonces se cumple que

$$\text{mcm}(\alpha,\beta) = p_1^{\text{máx}\,(a_1,b_1)} p_2^{\text{máx}\,(a_2,b_2)} ... p_h^{\text{máx}\,(a_h,b_h)} \tag{2.12}$$

Ejemplo. Calcular el mcd (82 320,950 796).

Solución: usando el teorema

$$\begin{aligned} \text{factorizacion\_factores\_primos}\ (82\ 320) &= 2^4 \cdot 3^1 \cdot 5^1 \cdot 7^3 \cdot 11^0 \\ \text{factorizacion\_factores\_primos}\ (950\ 796) &= 2^2 \cdot 3^2 \cdot 5^0 \cdot 7^4 \cdot 11^1 \\ \text{mcd}\ (82\ 320{,}950\ 796) &= 2^4 \cdot 3^2 \cdot 5^1 \cdot 7^4 \cdot 11^1 = 19\ 015\ 920 \end{aligned} \tag{2.13}$$

Ejemplo. Calcular el producto (mcd (30,105) · mcm (30,105)) y relacionarlo con los enteros 30 y 105.

Solución: haciendo las cuentas se tiene que

$$\begin{aligned} \text{mcd}\ (30{,}105) &= 15 \\ \text{mcm}\ (30{,}105) &= 210 \\ \hline \text{mcd}\ (30{,}105) \cdot \text{mcm}\ (30{,}105) &= 15 \cdot 210 = 3150 \end{aligned} \tag{2.14}$$

Pero a la vez 3150 se puede factorizar como $30 \cdot 105$ y se tiene

$$\text{mcd}\ (30{,}105) \cdot \text{mcm}\ (30{,}105) = 3150 = 30 \cdot 105 \tag{2.15}$$

Esta propiedad es un resultado general y queda descripto por el siguiente teorema:

Teorema. Para todos los enteros positivos α y β se tiene que

$$\text{mcd}(\alpha,\beta) \cdot \text{mcm}(\alpha,\beta) = \alpha \cdot \beta \tag{2.16}$$

Demostración:

i) Si $\alpha = 1$, entonces $\text{mcd}(1,\beta) = 1$, y $\text{mcm}(1,\beta) = \beta$, entonces $\text{mcd}(\alpha,\beta) \cdot \text{mcm}(\alpha,\beta) = 1 \cdot \beta = \alpha \cdot \beta$;

ii) Si $\beta = 1$, entonces $\text{mcd}(\alpha, 1) = \alpha$, y $\text{mcm}(\alpha, 1) = 1$, entonces $\text{mcd}(\alpha,\beta) \cdot \text{mcm}(\alpha,\beta) = \alpha \cdot 1 = \alpha \cdot \beta$;

iii) Por (i-ii) sólo basta analizar el caso $\alpha > 1$ y $\beta > 1$. Para eso, usando las Ecs. (2.8-2.12), y teniendo en cuenta que

$$\text{mín}(x,y) + \text{máx}(x,y) = x + y \tag{2.17}$$

se tiene que

$$\begin{aligned} \text{mcd}(\alpha,\beta) \cdot \text{mcm}(\alpha,\beta) &= \left[p_1^{\text{mín}\,(a_1,b_1)} p_2^{\text{mín}\,(a_2,b_2)} ... p_h^{\text{mín}\,(a_h,b_h)}\right] \cdot \\ &\times \left[p_1^{\text{máx}\,(a_1,b_1)} p_2^{\text{máx}\,(a_2,b_2)} ... p_h^{\text{máx}\,(a_h,b_h)}\right] \\ &= \left[p_1^{a_1} p_2^{a_2} ... p_h^{a_h}\right] \cdot \left[p_1^{b_1} p_2^{b_2} ... p_h^{b_h}\right] = \alpha \cdot \beta \end{aligned} \tag{2.18}$$

Observación. Si se tiene un algoritmo eficiente para hallar $\text{mcd}(\alpha,\beta)$, entonces se usa la Ec. (2.16) para hallar el $\text{mcm}(\alpha,\beta)$.

Aritmética modular

Intro: la aritmética modular se refiere a las cuentas en donde solo interesa los restos de las divisiones por enteros, tales como en el manejo de las horas del reloj. Por ejemplo, qué hora será dentro de 47 horas si la hora actual fuera 13 hs? Rpta: sumamos 47 a la hora actual y al resultado tomamos el resto de dividirlo por 24, o sea, (13 + 47) mod 24, resultando 12 hs.

Definición. Sean A y B enteros, y M un entero positivo. Entonces se dice que A es *congruente con B en módulo M* si M divide a la diferencia $(A - B)$, y se denota con $A \equiv B \pmod{M}$.

Teorema. Sean A y B enteros, y M un entero positivo. Entonces $A \equiv B \pmod{M}$ si y solo si $A \bmod M = B \bmod M$. Dem.: Si $A \bmod M = B \bmod M$, eso significa que A y B dan el *mismo* resto R al dividirlos por M. Entonces

$$\begin{array}{l} A = Q_1 M + R \quad \text{con } 0 \le R < M \\ B = Q_2 M + R \quad \text{notar que es el mismo } R \\ \hline (A - B) = (Q_1 - Q_2)M \quad \therefore \quad M \mid (A - B) \end{array} \tag{2.19}$$

Teorema. Sean A y B enteros, y sea M un entero positivo. Los enteros A y B son congruentes en módulo M ssi existe un entero K tal que $A = B + KM$. Dem.: Si $A \equiv B \pmod{M}$, entonces $M \mid (A - B)$. Esto significa que existe un entero K tal que $A - B = KM$, por lo que $A = B + KM$. Recíprocamente, si existe un entero K tal que $A - B = KM$, entonces $KM = A - B$, lo que significa que M divide a $A - B$, y por eso $A \equiv B \pmod{M}$.

Teorema. Sean A, B, C, y D enteros, y sea M un entero positivo. Entonces (i) $A+C \equiv B+D \pmod{M}$, y (ii) $AC \equiv BD \pmod{M}$. Dem. de (i):

$$\begin{array}{l} \text{Si } A \equiv B \pmod{M} \quad \therefore \; B = A + SM \text{ donde } S \text{ es un entero} \\ \text{Si } C \equiv D \pmod{M} \quad \therefore \; D = C + TM \text{ donde } T \text{ es un entero} \end{array} \tag{2.20}$$

Sumando lado a lado y re-agrupando

$$\begin{array}{l} B = A + SM \\ D = C + TM \\ \hline (B + D) = (A + C) + (S + T)M \end{array} \tag{2.21}$$

Como $(S + T)$ es otro entero se concluye $(B + D) \equiv (A + C) \bmod M$.

Aplicaciones de las congruencias

- **Funciones de dispersión** (o *hashing*). Las funciones de dispersión se utilizan para asignar posiciones de memoria de modo tal que las operaciones de asignación y recuperación de la info almacenada sean rápidas. Por ejemplo, la info de cada alumno en una facu se almacena en un archivo que se localiza eligiendo alguna *clave K* que identifica de forma unívoca al archivo de cada alumno, e.g. elegir como clave al DNI

de cada estudiante. Una función de dispersión H asigna una posición de memoria $H(K)$ al archivo de clave K, y deben ser tales que sean rápidas de calcular. Además deben ser *sobreyectivas* para así aprovechar toda la memoria disponible. Existen muchos tipos de funciones de dispersión, donde una de las más comunes son las basadas en una congruencia de la forma

$$H(K) = K \bmod M \tag{2.22}$$

donde M es el número de posiciones de memoria disponibles. Este tema se verá con mayor amplitud en AED.

- **Números pseudo-aleatorios**. En muchas aplicaciones se necesita elegir números en forma aleatoria, lo cual en la compu se logra utilizando métodos sistemáticos. Pero, como todo método sistemático nunca puede ser completamente aleatorio, en realidad los números obtenidos son números pseudo-aleatorios. Un método usual se basa en *congruencias lineales* donde se eligen 4 enteros:
  - un módulo M
  - un multiplicador A, tal que $2 \leq A < M$
  - un incremento C, tal que $0 \leq C < M$
  - una semilla X_0, tal que $0 \leq X_0 < M$

  Entonces, se va generando la sucesión de pseudo-aleatorios $\{X_n\}$, con $0 \leq X_n < M$ para todo entero n, utilizando la congruencia lineal

$$X_{n+1} = (AX_n + C) \bmod M \tag{2.23}$$

  Por ejemplo, con $M = 9$, $A = 7$, $C = 4$, y $X_0 = 3$, se obtiene la sucesión de enteros $\{X_n\} = \{3, 7, 8, 6, 1, 2, 0, 4, 5, 3, 7, 8, 6, 1, 2, 0, 4, 5, 3, ...\}$, donde la sub-secuencia $\{3, 7, 8, 6, 1, 2, 0, 4, 5\}$ se repite indefinidamente.

Criptología

Criptosistema de clave privada: cifrado de Julio César

- Los mensajes simplemente son cadenas de caracteres alfanuméricos. En los métodos de cifrado de mensajes se empieza transformándolos en números enteros. Luego, cada entero asociado a un caracter se transforma en otro entero utilizando alguna transformación, típicamente por desplazamiento circular, o desplazamiento en módulo Z, donde $Z = 26$ en un alfabeto de 26 letras. En los criptosistemas de clave privada hace falta conocer la clave de cifrado. Por ejemplo, en el cifrado por traslación en modulo Z con clave (privada) K, el entero P que representa algún caracter, se cifra y descifra con el par de ecuaciones

$$\begin{aligned} C &= (P + K) \bmod Z \\ P &= (C - K) \bmod Z \end{aligned} \tag{2.24}$$

- Cuando se usa un criptosistema de clave privada, un par de personas que se comunican en secreto deben compartir una clave para poder cifrar y descifrar. Tarea: ver ejercicio(s) en GTP.

2.5. Enteros y algoritmos

Representaciones de números enteros

Intro. Es usual usar notación decimal para representar números enteros, e.g. 987 significa $9\cdot 10^2+8\cdot 10^1+7\cdot 10^0$. No obstante, a veces, conviene usar una base distinta de la decimal, en particular: binario (base 2), octal (base 8), hexadecimal (base 16). De hecho se puede usar cualquier base $B > 0$, dando lugar al enunciado del siguiente teorema.

Enunciado. Expresión de un entero positivo en una base B positiva: sea un entero positivo B mayor a 1. Si n es un entero positivo, entonces se lo puede expresar como

$$n = a_k B^k + a_{k-1}B^{k-1} + ... + a_1 B^1 + a_0 \tag{2.25}$$

de una única forma, donde k es un entero no negativo, a_0, a_1, ..., a_k son enteros no negativos menores a B, y $a_k \neq 0$.

Definición. Expresión binaria (def.): cuando se elige base $B = 2$, con lo cual bastan 2 símbolos, cada símbolo es 0 o 1. En consecuencia la expresión binaria de un entero es una cadena de bits.

Ejemplo. Obtener la expresión decimal del binario $z = (1\ 0101\ 1101)_2$.

Solución:

$$z = 1\cdot 2^8 + 0\cdot 2^7 + 1\cdot 2^6 + 0\cdot 2^5 + 1\cdot 2^4 + 1\cdot 2^3 + 1\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0 = (349)_{10} \tag{2.26}$$

Definición. Expresión hexadecimal (def.): cuando se elige base $B = 16$, con lo cual hacen falta 16 símbolos. Normalmente se emplean 0-9 y A-F, e.g. ver Tabla 2.1.

decimal	binario	hexadecimal
1	00001	1
2	00010	2
3	00011	3
4	00100	4
5	00101	5
6	00110	6
7	00111	7
8	01000	8
9	01001	9
10	01010	A
11	01011	B
12	01100	C
13	01101	D
14	01110	E
15	01111	F
16	10000	10

Tabla 2.1: Enteros desde 1 hasta 16 en base decimal, binaria, y hexadecimal.

Ejemplo. Obtener la expresión decimal del hexadecimal $z = (2AE0B)_{16}$.

Solución:

$$\begin{aligned} z &= 2\cdot 16^4 + 10\cdot 16^3 + 14\cdot 16^2 + 0\cdot 16^0 + 11\cdot 16^0 \\ &= (175\ 627)_{10} \end{aligned} \tag{2.27}$$

Ejemplo. Obtener la expresión decimal del hexadecimal $z_1 = (21)_{16}$, y $z_2 = (30)_{16}$.

Solución:

$$\begin{aligned} z_1 &= 2 \cdot 16^1 + 1 \cdot 16^0 = (33)_{10} \\ z_2 &= 3 \cdot 16^1 + 0 \cdot 16^0 = (48)_{10} \end{aligned} \tag{2.28}$$

Observación. cada dígito hexadecimal puede expresarse usando 4 bits lo cual, con experiencia, facilita las conversiones.

Ejemplo. Como $(1110)_2 = (14)_{10} = (E)_{16}$, y como $(0101)_2 = (05)_{10} = (5)_{16}$, se tiene que $(1110\ 0101)_2 = (E5)_{16}$.

Definición. Byte, palabra, octeto (def.): son cadenas de bits de longitud 8. Notar que un byte se puede representar usando 2 números hexadecimales.

En cuanto a cambios de base, lo ilustraremos con ejemplos.

Ejemplo. Calcular $z = (12\ 345)_{10}$ en octal.

Solución:

$$\begin{aligned} 12\ 345 &= 8 \cdot 1\ 543 + 1 && (1) \\ 1\ 543 &= 8 \cdot 192 + 7 && (7) \\ 192 &= 8 \cdot 24 + 0 && (0) \\ 24 &= 8 \cdot 3 + 0 && (0) \\ 3 &= 8 \cdot 0\ (\text{end}) + 3 && (3) \\ (12\ 345)_{10} &= (30\ 071)_8 \end{aligned} \tag{2.29}$$

Ejemplo. Calcular $z = (177\ 130)_{10}$ en hexadecimal.

Solución:

$$\begin{aligned} 177\ 130 &= 16 \cdot 11\ 070 + 10 && (A) \\ 11\ 070 &= 16 \cdot 691 + 14 && (E) \\ 691 &= 16 \cdot 43 + 3 && (3) \\ 43 &= 16 \cdot 2 + 11 && (B) \\ 2 &= 16 \cdot 0\ (\text{end}) + 2 && (2) \\ (177\ 130)_{10} &= (2B3EA)_{16} \end{aligned} \tag{2.30}$$

Ejemplo. Calcular $z = (241)_{10}$ en binario.

Solución:

$$\begin{aligned} 241 &= 2 \cdot 120 + 1 \\ 120 &= 2 \cdot 60 + 0 \\ 60 &= 2 \cdot 30 + 0 \\ 30 &= 2 \cdot 15 + 0 \\ 15 &= 2 \cdot 7 + 1 \\ 7 &= 2 \cdot 3 + 1 \\ 3 &= 2 \cdot 1 + 1 \\ 1 &= 2 \cdot 0\ (\text{end}) + 1 \\ (241)_{10} &= (1111\ 0001)_2 \end{aligned} \tag{2.31}$$

Algoritmos para operaciones con enteros

Omitir.

Exponenciación modular

Omitir.

El algoritmo de Euclides

Intro. El algoritmo de Euclides permite calcular rápidamente el máximo común divisor de dos enteros a y b, donde $a \geq b$, y se basa en la propiedad

$$\text{mcd}\,(a,b) = \text{mcd}\,(b,r) \qquad \text{donde } r = a \bmod b \tag{2.32}$$

Cuando $a < b$, se permutan los términos, i.e. mcd (a,b) = mcd (b,a).

Ejemplo. Calcular el mcd (30,105).

Solución: usamos reiteradamente la Ec. (2.32), resultando:

$$\begin{aligned}&\text{mcd(30,105)= mcd(105,30=mcd(30,15), pues 105 mod 30 = 15}\\&\text{mcd(30,15) = mcd(15,0), pues 30 mod 15 = 0}\\&\text{mcd (15,0) = 15, pues 15 es el mayor entero que divide a 15 y a 0}\end{aligned} \tag{2.33}$$

2.6. Aplicac. de la teor. de núm.

Algunos resultados útiles

Teorema. Si a, b, y c son enteros tales que $a|b$ y $a|c$, entonces se cumple que $a|(mb+nc)$, para todos los enteros m y n. Demostración:

- Si $a|b$ entonces, también $a|(bc)$ para todo entero c. Por eso, $a|mb$ y $a|nc$ para todos los enteros m y n;
- Si $a|mb$ y $a|nc$ entonces, también $a|(mb+nc)$, comprobando así el enunciado del corolario.

Observación. Este teorema es re-útil en los fundamentos matemáticos de la criptografía de clave pública RSA, i.e. cuando se utiliza la autenticación con clave pública para conectarse a un servidor remoto mediante el protocolo SSH, en donde se utilizan dos claves, una pública y otra privada, y que en linux se generan con `ssh-keygen -t rsa` donde `rsa` selecciona ese método.

Ejemplo. Expresar mcd(252,198) como una combinación lineal de 252 y 198. Solución. Utilizando el algoritmo de Euclides se tiene:

$$\begin{aligned}252 &= 1\cdot 198 + 54\\198 &= 3\cdot 54 + 36\\54 &= 1\cdot 36 + 18\\36 &= 2\cdot 18 + 0\end{aligned} \tag{2.34}$$

Ahora

$$\begin{aligned} 18 &= 54 - 1 \cdot 36 \\ 36 &= 198 - 3 \cdot 54 \end{aligned} \tag{2.35}$$

A continuación

$$\begin{aligned} 18 &= 54 - 1 \cdot 36 \\ &= 54 - 1 \cdot (198 - 3 \cdot 54) \\ &= 4 \cdot 54 - 1 \cdot 198 \end{aligned} \tag{2.36}$$

Por último

$$\begin{aligned} 54 &= 252 - 1 \cdot 198 \\ 18 &= 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 \\ &= 4 \cdot 252 - 5 \cdot 198 \end{aligned} \tag{2.37}$$

Teorema. Sean a, b, y c enteros positivos, tales que $\text{mcd}(a, b) = 1$ y $a|bc$, entonces $a|c$. Demostración: como $\text{mcd}(a, b) = 1$, existen dos enteros s y t tales que $sa + tb = 1$. Luego

$sa + tb = 1$	multiplicando lado a lado por c
$csa + ctb = c$	Pero:
	Por enunciado se sabe que $a\|bc$, entonces $a\|tbc$, con t entero;
	Como $a\|a$, entonces $a\|csa$, con cs entero;
	Entonces, como $a\|ctb$ y $a\|csa$, se concluye que $a\|c$.

(2.38)

- Lema 2: omitir.
- Ejemplo 2: omitir.
- Teorema 2: omitir.

Congruencias lineales

Omitir.

Teorema chino del resto

Omitir.

Aritm. comp. con núm. grandes

Omitir.

Pseudoprimos

Omitir.

Criptografía de clave pública

Omitir.

Cifrado RSA

Omitir.

Descifrado RSA

Reseña histórica de RSA (Rivest, Shamir, y Adelman): lectura optativa. Comentario: Adelman fue quien introdujo el término *virus informático*.

RSA como sistema de clave pública

Omitir.

CAPÍTULO 3

Razon. matem., inducc. y recursividad

Nota. Estas notas siguen el texto de referencia Rosen (2004) manteniendo la numeración de las secciones y sus títulos, como una referencia adicional para el auto-estudio siguiendo ese texto.

Contents

3.1. Estrategias de demostración

- Introducción: lectura.
- Estrategias de demostración:
  - Razonamiento hacia adelante y hacia atrás: lectura.
  - Ejemplo 1 (media aritmética y media geomótrica): demostrar que $(a+b)/2 > \sqrt{ab}$ cuando a y b son reales positivos distintos: re-hacerlo.
  - Ejemplo 2 (juego con piedras): omitir.
  - Demostración por casos: lectura.
  - Ejemplo 3: omitir.
  - Ejemplo 4:
    - Previo: ecuación *diofántica* (def.): es toda ecuación con coeficientes y soluciones *enteras*.
    - Demostrar que no-existen soluciones enteras x e y en la ecuación diofántica $x^2 + 3y^2 = 8$: re-hacerlo.
  - Adaptación de demostraciones conocidas: omitir.
  - Ejemplo 5: omitir.

- Conjetura y demostración:
  - Intro: lectura.
  - Ejemplo 6 (primos de Mersenne): omitir.
  - Teorema 1: omitir.
  - Ejemplo 7: omitir.
- Conjetura y contraejemplos:
  - Ejemplo 8. Es re-hecho a continuación:

    Conjetura. Sea $f(n) = n^2 + n + 41$ con $n \in \mathbb{Z}^+$. Si calculamos $f(n)$ para los primeros 39 valores de n resulta $f(n)$ es un entero primo, i.e. solo divisible por 1 y por si mismo, por lo que se podría conjeturar que $f(n)$ es un entero primo para todo $n \in \mathbb{Z}^+$. Sin embargo, cuando $n = 40$ se obtiene $f(40) = 1681$ el cual no es entero primo porque se puede expresar como $1681 = 41^2$. Se concluye entonces que esta conjetura es F.
  - Ejemplo 9: lectura.
  - Problemas abiertos: lectura.
  - Teorema de Fermat:
    - *Teorema de Fermat*: la ecuación diofántica $x^n + y^n = z^n$ no-tiene soluciones enteras x, y, z, donde $xyz \neq 0$, para ningún entero $n > 2$.
    - Observ.: la ecuación diofántica $x^2 + y^2 = z^2$ tiene infinitas soluciones enteras, dando las ternas de Pitágoras, y corresponden a las longitudes de los lados de un triángulo rectángulo con lados de longitud entera.
  - Ejemplo 10. Conjetura de Goldbach (enunciado): todo entero par n mayor a 2 es igual a la suma de dos primos.
  - Ejemplo 11: omitir.
  - Ejemplo 12 (primos gemelos):
    - Primos *gemelos* (def.): 2 primos son gemelos si difieren en 2.
    - Ejemplos: 3 y 5, 5 y 7, 11 y 13, 17 y 19, son primos gemelos.
    - Conjetura de los primos gemelos: existen infinitos primos gemelos.
  - Ejemplo 13. *Conjetura de Collatz* (o conjetura $3n + 1$, algoritmo de Hasse, problema de Kakutani, problema de Siracusa, o problema de Ulam): ya visto en el Ejemplo 1.5.
- *Problema de Turing* (o problema de la detención, o problema de la parada): de central importancia en la teoría de la computación: postergado al último cap.
- Otros métodos de demostración: omtir.

3.2. Sucesiones y sumatorias

- Sucesiones: omitir.
- Sucesiones especiales de enteros: omitir.

sumatoria	resultado	
$\sum_{k=0}^{n} k$	$\frac{n(n+1)}{2}$	Suma de Gauss
$\sum_{k=0}^{n} k^2$	$\frac{n(n+1)(2n+1)}{6}$	En inducción
$\sum_{k=0}^{n} k^3$	$\left[\frac{n(n+1)}{2}\right]^2$	Difícil!
$\sum_{k=0}^{n} Ar^k$ con $r \neq 1$	$A\frac{r^{n+1}-1}{r-1}$	Progresión geométrica

Tabla 3.1: Sumatorias frecuentes y sus valores.

Sumatorias

Intro. La sumatoria y la productoria son de utilidad en diversos temas, en particular en inducción y en AED, y se expresan como sigue:

Definición.

- Sumatoria:

$$\sum_{k=m}^{n} a_k = a_m + a_{m+1} + ... + a_m \tag{3.1}$$

- Productoria:

$$\prod_{k=m}^{n} a_k = a_m a_{m+1} ... a_m \tag{3.2}$$

Ejemplo. Cambio de índice y de límites en una sumatoria. En la sumatoria

$$A = \sum_{k=0}^{n} k r^{n-k} \tag{3.3}$$

introducir el cambio de índice $k = j - 1$. Solución: como $k = j - 1$ se tiene que, cuando $k = 0$ es $j = 1$, y cuando $k = n$ es $j = n + 1$. Por otra parte $n - k = n - j + 1$. Finalmente, reemplazando, sresulta

$$A = \sum_{j=1}^{n+1} (j-1) r^{n-j+1} \tag{3.4}$$

Ejemplo. [Un error algebraico algo frecuente en parciales] Sumar $5 \cdot 11^n + 5 \cdot 11^n$. Solución: Antes, como ya sabemos $5A + 5A = 2 \cdot (5A)$. Ahora sea $A = 11^n$, entonces $5 \cdot 11^n + 5 \cdot 11^n = 2 \cdot (5 \cdot 11^n)$.

- Ejemplo 9: omitir.
- Ejemplo 10: omitir.
- Ejemplo 11: omitir.

- Ejemplo 12: omitir.
- Ejemplo 13 (sumatorias dobles): omitir.
- Ejemplo 14: omitir.
- Ejemplo 15: omitir.
- Ejemplo 16: omitir.
- Ejemplo 17: omitir.
- Cardinal: omitir.

3.3. Inducción matemática

Inducción

Intro. El Principio de Inducción Matemática (PIM) (Sec. 3.3, p. 222, Rosen; Sec. 1.7, p. 53, Johnsonbaugh) lo usaremos para demostrar proposiciones cuantificadas de la forma $\forall n\ P(n)$, donde $P(n)$ es una FP en el entero n, mientras que el DD es el conjunto de **TODOS** los enteros a partir de algún entero n_0 dado, i.e. es el conjunto infinito $\{n_0, n_0 + 1, n_0 + 2, ...\}$.

Enunciado. Sea la proposición cuantificada de la forma $\forall n\ P(n)$, donde $P(n)$ es una FP en el entero n, mientras que el DD es el conjunto de todos los enteros $\mathbb{Z}_0^+$ a partir de un entero n_0 dado. El PIM sostiene que si se cumplen tanto el PB como el PI:

- Paso Base (PB) (cuando $n = n_0$): se comprueba que $P(n_0)$ es T;
- Paso de Inducción (PI): se demuestra que la implicación $P(k) \rightarrow P(k + 1)$ es T para algún entero $k \geq n_0$ arbitrario;

entonces $P(n)$ vale para todos los enteros $n \geq n_0$. El PIM puede simbolizarse con la regla de inferencia compuesta.

$$\begin{aligned} &[P(n_0) \wedge H(k)] \rightarrow \left[\forall n \in \mathbb{Z}_{n_0}^+ \text{se cumple } P(n)\right], \text{ donde} \\ &H(k) \equiv (P(k) \rightarrow P(k+1)) \quad \text{para algún entero } k \geq n_0 \text{ arbitrario.} \end{aligned} \tag{3.5}$$

Observación.

i) En los ejercicios frecuentemente es $n_0 = 0$, $n_0 = 1$ u, ocasionalmente, $n_0 > 1$;
ii) La frase para algún entero $k > n_0$ arbitrario en la implicación de la Ec. (3.5) es importante, i.e. hay que demostrar la veracidad de $P(k + 1)$ a través de la implicación $P(k) \rightarrow P(k + 1)$ asumiendo que $P(k)$ es T para algún $k > ge0$;
iii) El antecedente de la implicación en $H(k)$, que se asume T cuando se demuestra el PI, lo llamaremos como la Hipótesis Inductiva (HI).

Ejemplos de demostraciones por inducción

Ejemplo. [PIM con una igualdad en donde $n_0 = 1$]: *suma de Gauss*. Demostrar usando el PIM que

$$1 + 2 + 3 + ... + n = \frac{n(n+1)}{2} \tag{3.6}$$

para todos los enteros n positivos. Solución:

- PB ($n = 1$): en el lado izquierdo de la Ec. (3.6) se tiene que $I_1 = 1$ (suma reducida al primer sumando), mientras que en el lado derecho se tiene $D_1 = 1 \cdot 2/2 = 1$ (a la derecha). Como se cumple la igualdad $I_1 = D_1$, se verifica el PB.
- PI: asumimos que la HI dada por

$$\underbrace{1 + 2 + 3 + ... + k}_{I_k} = \underbrace{\frac{k(k+1)}{2}}_{D_k} \tag{3.7}$$

es T para algún entero $k \geq 1$ arbitrario. A continuación elegimos sólo uno de los lados de la Ec. (3.7), en donde conviene tomar el lado izquierdo que contiene la sumatoria, y lo planteamos para el siguiente índice $(k + 1)$:

$$\begin{aligned} I_{k+1} &= \{1 + 2 + 3 + ... + k\} + (k + 1) && \text{; introducimos la HI en } \{...\} \\ &= \frac{k(k+1)}{2} + (k + 1) && \text{; sumamos fracciones} \\ &= \frac{k(k+1) + 2(k+1)}{2} && \text{; sacamos factor común } (k + 1) \\ &= \frac{(k+1)(k+2)}{2} = D_{k+1} \end{aligned} \tag{3.8}$$

O sea, empezando por el lado izquierdo de la Ec. (3.7) pero re-escrita para el siguiente índice $(k + 1)$, se obtiene la igualdad predicha por el enunciado para el lado derecho pero re-escrito también para el siguiente índice $(k+1)$. Es decir, la implicación $P(k) \rightarrow P(k + 1)$ es T para algún entero $k \geq 1$ arbitrario.
- Finalmente, como se cumple el PB y el PI, el PIM asegura que se cumple el enunciado para todos los enteros positivos n.

Ejemplo. [PIM con una igualdad en donde $n_0 = 1$]: suma de los primeros n enteros impares. Demostrar usando el PIM que

$$1 + 3 + 5 + ... + (2n - 1) = n^2 \tag{3.9}$$

para todos los enteros n positivos. Solución:

- PB ($n = 1$): en el lado izquierdo de la Ec. (3.9) se tiene $I_1 = 1$ (suma reducida al primer sumando), mientras que en el lado derecho se tiene $D_1 = 1^2 = 1$. Como se cumple la igualdad $I_1 = D_1$, se verifica el PB.
- PI: asumimos que la HI

$$\underbrace{1 + 3 + 5 + ... + (2k - 1)}_{I_k} = \underbrace{k^2}_{D_k} \tag{3.10}$$

es T para algún entero $k \geq 1$ arbitrario. A continuación elegimos sólo uno de los lados de la Ec. (3.10), en donde conviene tomar el lado que contiene la sumatoria, y

lo planteamos para el siguiente índice $(k+1)$:

$$\begin{aligned} I_{k+1} &= \{1+3+5+...+(2k-1)\}+(2(k+1)-1) && \text{; introducimos la HI en \{...\}} \\ &= k^2+2(k+1) && \text{; prop. distributiva} \\ &= k^2+2k+2 && \text{; cuadrado del binomio} \\ &= (k+1)^2 \end{aligned} \tag{3.11}$$

O sea, empezando por el lado izquierdo de la Ec. (3.10) pero re-escrita para el siguiente índice $(k+1)$, se obtiene la igualdad predicha por el enunciado para el lado derecho pero re-escrito para el siguiente índice $(k+1)$. Es decir, la implicación $P(k) \rightarrow P(k+1)$ es T para algún entero $k \geq 1$ arbitrario.

- Finalmente, como se cumple el PB y el PI, el PIM asegura que se cumple el enunciado para todos los enteros positivos n.

Ejemplo. [PIM con una desigualdad en donde $n_0 = 1$]. Demostrar usando el PIM que

$$n < 2^n \tag{3.12}$$

para todos los enteros n positivos. Solución:

- PB $(n = 1)$: en el lado izquierdo de la Ec. (3.12) se tiene $I_1 = 1$, mientras que en el lado derecho se tiene $D_1 = 2^1 = 2$. Como se cumple la desigualdad $I_1 < D_1$, se verifica el PB.
- PI: asumimos que la HI dada por

$$\underbrace{k}_{I_k} < \underbrace{2^k}_{D_k} \tag{3.13}$$

es T para algún entero $k \geq 1$ arbitrario. A continuación elegimos sólo uno de los lados de la Ec. (3.13), en donde puede convenir tomar el lado izquierdo, y lo planteamos para el siguiente índice:

$$\begin{aligned} I_{k+1} &= \{k\}+1 && \text{; introd. HI en \{...\}} \\ &< 2^k+1 && \text{; reemplazo } 1<2^k \text{ para } k>0 \\ &< 2^k+2^k && \text{; usamos } A+A=2A \text{ (1 pera + 1 pera = 2 peras)} \\ &= 2\cdot 2^k = 2^{k+1} = D_{k+1} && \text{; pot. de igual base} \end{aligned} \tag{3.14}$$

Observando desde el inicio vemos que $I_{k+1} < D_{k+1}$, que es lo predicho por la desigualdad pero re-escrita para el siguiente índice $(k+1)$. Es decir, la implicación $P(k) \rightarrow P(k+1)$ es T para algún entero $k \geq 1$ arbitrario.

- Finalmente, como se cumple el PB y el PI, el PIM asegura que se cumple el enunciado para todos los enteros positivos n.

Ejemplo. [PIM con una desigualdad en donde $n_0 = 4$]. Demostrar usando el PIM que

$$2^n < n! \tag{3.15}$$

para todos los enteros $n \geq 4$. Solución:

- PB ($n = 4$): en el lado izquierdo de la Ec. (3.15) se tiene $I_4 = 2^4 = 16$, mientras que en el lado derecho $D_4 = 4! = 24$. Como se cumple la desigualdad $I_4 < D_4$, se verifica el PB.
- PI: asumimos que la HI dada por

$$\underbrace{2^k}_{I_k} < \underbrace{k!}_{D_k} \tag{3.16}$$

es T para algún entero $k \geq 4$ arbitrario. A continuación elegimos sólo uno de los lados de la Ec. (3.16), en donde puede convenir tomar el lado izquierdo, y lo planteamos para el siguiente índice:

$$\begin{aligned} I_{k+1} &= 2^{k+1} && \text{; potencia de igual base} \\ &= \{2^k\} \cdot 2 && \text{; introd. HI en \{...\} y permutamos} \\ &< 2 \cdot \{k!\} && \text{; dato auxiliar } 2 < k+1 \text{ para } k \geq 4 \\ &< (k+1) \cdot (k!) && \text{; usamos def. del factorial} \\ &= (k+1)! && \text{; pot. de igual base} \end{aligned} \tag{3.17}$$

Observando desde el inicio vemos que $I_{k+1} < D_{k+1}$, que es lo predicho por la desigualdad dada pero re-escrita para el siguiente índice $(k+1)$. Es decir, la implicación $P(k) \rightarrow P(k+1)$ es T para algún entero $k \geq 4$ arbitrario.
- Finalmente, como se cumple el PB y el PI, el PIM asegura que se cumple el enunciado para todos los enteros $n \geq 4$.

Ejemplo. [PIM cuando no es una igualdad ni una desigualdad]: Demostrar usando el PIM que $(n^3 - n)$ es divisible por 3 para todos los enteros positivos n. Solución:

- Previo: por ejemplo, como 8 div 4 = 2, y 8 mod 4 = 0, decimos que 8 es divisible por 4. En general decir que un entero B es divisible por otro entero positivo A, significa que B mod $A = 0$. En particular, como 0 div 3 = 0 y 0 mod 3 = 0, decimos en general que **cero es divisible por cualquier entero positivo**.
- PB ($n = 1$): tenemos $P(1) = 1^3 - 1 = 0$. Como 0 es divisible por 3, se concluye que el PB es T.
- PI: asumimos que la HI dada por:

$$P(k) : (k^3 - k) \text{ es divisible por } 3 \tag{3.18}$$

es T para algún entero $k \geq 1$ arbitrario. A continuación, nos preguntamos qué sucede cuando k pasa a $(k+1)$ en el polinomio, o sea:

$$\begin{aligned} (k+1)^3 - (k+1) = & && \text{; desarrollamos el (...)}^3 \\ &= (k^3 + 3k^2 + 3k + 1) - (k+1) && \text{; reagrupamos monomios} \\ &= \underbrace{\{(k^3 - k)\}}_{\text{por HI es divisible por 3}} + \underbrace{3(k^2 + k)}_{\text{3 veces un entero}} \end{aligned} \tag{3.19}$$

vemos que $(k+1)^3 - (k+1)$ también es divisible por 3 siempre que $k^3 - k$ lo sea, y se cumple el PI.

- Finalmente, como se cumple el PB y el PI, el PIM asegura que se cumple para todos los enteros positivos n.

Teorema. Número de elementos del conjunto potencia. Si un conjunto finito A tiene n elementos, entonces

$$|\mathcal{P}(A)| = 2^n \tag{3.20}$$

para todo entero $n \geq 0$. Demostración: (i) por PIM (en el parcial 1); y (ii) por conteo (en el parcial 2), (iii) ambos (después del parcial2, recuperatorios y finales).

- PB si $n = 0$ entonces no hay elementos, y se reduce al conjunto vacío. El único subconjunto del conjunto vacío es el conjunto vacío. Así que en el lado izquierdo $I_0 = 1$, mientras que en el lado derecho $D_0 = 2^0 = 1$, y se cumple la igualdad $I_1 = D_1$.
- PI: cuando $k \geq 0$:
  - i) Sea A_{k+1} el conjunto con $(k+1)$ elementos, y sea A_k el conjunto obtenido de A_{k+1} al eliminar un elemento cualquiera x, por lo que A_k tiene k elementos;
  - ii) Notar que cada subconjunto de $\mathcal{P}(A_{k+1})$ que contiene a un elemento genérico x, se lo puede coordinar de un modo único con un subconjunto que no lo contiene. Por eso, exactamente la mitad de los subconjuntos de $\mathcal{P}(A_{k+1})$ contienen al elemento x, y la otra mitad no lo contienen (ver Fig. 3.1 y releer la Obs. 1.6).
  - iii) Como A_k tiene k elementos, podemos utilizar la hipótesis inductiva para concluir que $|\mathcal{P}(A_k)| = 2^k$;
  - iv) Pero los subconjuntos de $\mathcal{P}(A_k)$ son los de $\mathcal{P}(A_{k+1})$ que no contienen al elemento x y su número es la *mitad*, o sea

$$|\mathcal{P}(A_k)| = \frac{|\mathcal{P}(A_{k+1})|}{2} \tag{3.21}$$

  despejando $|\mathcal{P}(A_{k+1})|$ se tiene

$$\begin{aligned} |\mathcal{P}(A_{k+1})| &= 2 \cdot |\mathcal{P}(A_k)| \\ &= 2 \cdot 2^k \\ &= 2^{k+1} \end{aligned} \tag{3.22}$$

  que es lo predicho por la HI en el lado derecho pero re-escrito para el siguiente índice $(k+1)$. Es decir, la implicación $P(k) \rightarrow P(k+1)$ es T para algún entero $k \geq 0$ arbitrario.
  - 1) Finalmente, como se cumple el PB y el PI, el PIM asegura que se cumple el enunciado para todos los enteros no-negativos n.

Ejemplo. [PIM en leyes generalizadas de De Morgan para conjuntos, en donde $n_0 = 2$]. Demostrar usando el PIM que

$$\overline{\bigcap_{j=1}^{n} A_j} = \bigcup_{j=1}^{n} \overline{A_j} \tag{3.23}$$

para todos los enteros $n \geq 2$, donde $A_1, A_2, ..., A_n$ son subconjuntos de un cierto conjunto universal U. Solución:

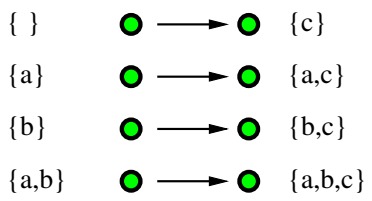

Figura 3.1: Coordinación de los subconjuntos de $A_3 = \{a, b, c\}$: los que no contienen al elemento c (izq.), y los que lo contienen (der.). Notar que los mostrados a la izq. son los elementos del conjunto potencia $A_2 = \{a, b\}$.

- PB ($n = 2$): la Ec. (3.23) cuando $n = 2$ se reduce a:

$$A_1 \cap A_2 = \overline{A_1} \cup \overline{A_2} \tag{3.24}$$

que es una de las leyes de De Morgan para 2 conjuntos, por lo que se concluye que el PB es Verdadero (por *True*) (T).

- PI: asumimos que la HI dada por

$$\underbrace{\overline{\bigcap_{j=1}^{k} A_j}}_{I_k} = \underbrace{\bigcup_{j=1}^{k} \overline{A_j}}_{D_k} \tag{3.25}$$

es T para algún entero $k \geq 2$ arbitrario. A continuación elegimos sólo uno de los lados de la Ec. (3.25). Aquí elegimos tomar el lado izquierdo, y lo planteamos para el siguiente índice $(k + 1)$:

$$\begin{aligned}
I_{k+1} &= \overline{\bigcap_{j=1}^{k+1} A_j} && \text{; expandimos intersección generalizada} \\
&= \overline{\bigcap_{j=1}^{k} A_j \cap A_{k+1}} && \text{; reemplazo } H_k = \bigcap_{j=1}^{k} A_j \\
&= \overline{H_k \cap A_{k+1}} && \text{; introducimos ley de De Morgan para 2 conj.} \\
&= \left\{\overline{H_k}\right\} \cup \overline{A_{k+1}} && \text{; por HI es } \overline{H_k} = \overline{\bigcap_{j=1}^{k} A_j} = \bigcup_{j=1}^{k} \overline{A_j} \\
&= \left\{\bigcup_{j=1}^{k} \overline{A_j}\right\} \cup \overline{A_{k+1}} && \text{; usamos propiedad asociativa} \\
&= \bigcup_{j=1}^{k+1} \overline{A_j}
\end{aligned} \tag{3.26}$$

O sea, empezando por el lado izquierdo de la Ec. (3.25) pero re-escrita para el siguiente índice $(k + 1)$, se obtiene la igualdad predicha por el enunciado para el lado derecho pero re-escrito también para el siguiente índice $(k + 1)$. Es decir, la implicación $P(k) \rightarrow P(k + 1)$ es T para algún entero $k \geq 2$ arbitrario.

- Finalmente, como se cumple el PB y el PI, el PIM asegura que se cumple el enunciado para todos los enteros positivos $n \geq 2$.

Tarea. [PIM en leyes generalizadas de De Morgan para conjuntos, y con $n_0 = 2$]. Demostrar usando el PIM que

$$\overline{\bigcup_{j=1}^{n} A_j} = \bigcap_{j=1}^{n} \overline{A_j} \tag{3.27}$$

para todos los enteros $n \geq 2$, donde A_1, A_2, ..., A_n son subconjuntos de un cierto conjunto universal U.

Ejemplo. [PIM en conjuntos, en donde $n_0 = 2$]. Demostrar usando el PIM que

$$X \cap \bigcup_{j=1}^{n} A_j = \bigcup_{j=1}^{n} (X \cap A_j) \tag{3.28}$$

para todos los enteros $n \geq 2$, donde X es un conjunto, mientras que A_1, A_2, ..., A_n son subconjuntos de un cierto conjunto universal U. Solución:

- PB ($n = 2$): la Ec. (3.28) cuando $n = 2$ se reduce a:

$$X \cap (A_1 \cup A_2) = (X \cap A_1) \cup (X \cap A_2) \tag{3.29}$$

  que es una de las leyes distributivas para 2 conjuntos, por lo que se concluye que el PB es T.
- PI: asumimos que la HI dada por

$$\underbrace{X \cap \bigcup_{j=1}^{k} A_j}_{I_k} = \underbrace{\bigcup_{j=1}^{k} (X \cap A_j)}_{D_k} \tag{3.30}$$

  es T para algún entero $k \geq 2$ arbitrario. A continuación elegimos sólo uno de los lados de la Ec. (3.30). Aquí elegimos tomar el lado izquierdo, y lo planteamos para

el siguiente índice $(k+1)$:

$$\begin{aligned}
I_{k+1} &= X \cap \bigcup_{j=1}^{k+1} A_j && \text{; expandimos unión generalizada} \\
&= X \cap \left[\bigcup_{j=1}^{k} A_j \cup A_{k+1} \right] && \text{; introducimos prop. ditributiva} \\
&= \left\{ X \cap \bigcup_{j=1}^{k} A_j \right\} \cup (X \cap A_{k+1}) && \text{; introducimos la HI en \{...\}} \\
&= \left\{ \bigcup_{j=1}^{k} (X \cap A_j) \right\} \cup (X \cap A_{k+1}) && \text{; reagrupo} \\
&= \bigcup_{j=1}^{k+1} \Big(X \cap A_j \Big)
\end{aligned} \tag{3.31}$$

O sea, empezando por el lado izquierdo de la Ec. (3.30) pero re-escrita para el siguiente índice $(k+1)$, se obtiene la igualdad predicha por el enunciado para el lado derecho pero re-escrito también para el siguiente índice $(k+1)$. Es decir, la implicación $P(k) \rightarrow P(k+1)$ es T para algún entero $k \geq 2$ arbitrario.

- Finalmente, como se cumple el PB y el PI, el PIM asegura que se cumple el enunciado para todos los enteros positivos $n \geq 2$.

Tarea. [PIM en leyes generalizadas de De Morgan para conjuntos, y con $n_0 = 2$]. Demostrar usando el PIM que

$$X \cup \bigcap_{j=1}^{n} A_j = \bigcap_{j=1}^{n} (X \cup A_j) \tag{3.32}$$

para todos los enteros $n \geq 2$, donde X es un conjunto, mientras que A_1, A_2, ..., A_n son subconjuntos de un cierto conjunto universal U. Solución: tarea para el hogar.

Ejemplo. [PIM con una matriz y $n_0 = 1$]. Sea la matriz

$$\boldsymbol{A} = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \tag{3.33}$$

demostrar usando el PIM que la potencia enésima $\boldsymbol{A}^n$ de $\boldsymbol{A}$ está dada por

$$\boldsymbol{A}^n = \begin{bmatrix} a^n & 0 \\ 0 & b^n \end{bmatrix} \tag{3.34}$$

para todo entero positivo n. Solución:

- PB $(n = 1)$: cuando $n = 1$ en el lado izquierdo de la Ec. (3.34) se tiene

$$I_1 = \boldsymbol{A}^1 = \boldsymbol{A} \tag{3.35}$$

mientras que en el lado derecho:

$$D_1 = \begin{bmatrix} a^1 & 0 \\ 0 & b^1 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \tag{3.36}$$

entonces $I_1 = D_1$ y se concluye que el PB es T.

- PI: asumimos que la HI dada por

$$\boldsymbol{A}^k = \begin{bmatrix} a^k & 0 \\ 0 & b^k \end{bmatrix} \tag{3.37}$$

es T para algún entero k positivo arbitrario. A continuación elegimos sólo uno de los lados de la Ec. (3.37). Aquí elegimos tomar el lado izquierdo, y lo planteamos para el siguiente índice $(k + 1)$:

$$\begin{aligned} I_{k+1} = \boldsymbol{A}^{k+1} &= \boldsymbol{A}^k \boldsymbol{A}^1 && \text{; introducimos la HI en el primer factor} \\ &= \begin{bmatrix} a^k & 0 \\ 0 & b^k \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} && \text{; multiplicamos matricialmente} \\ &= \begin{bmatrix} (a^k a + 0) & (0 + 0) \\ (0 + 0) & (b^k b) \end{bmatrix} && \text{; potencias de igual base} \\ &= \begin{bmatrix} a^{k+1} & 0 \\ 0 & b^{k+1} \end{bmatrix} \end{aligned} \tag{3.38}$$

O sea, empezando por el lado izquierdo de la Ec. (3.37) pero re-escrita para el siguiente índice $(k + 1)$, se obtiene la igualdad predicha por el enunciado para el lado derecho pero re-escrito también para el siguiente índice $(k + 1)$. Es decir, la implicación $P(k) \rightarrow P(k + 1)$ es T para algún entero $k \geq 2$ arbitrario.

- Finalmente, como se cumple el PB y el PI, el PIM asegura que se cumple el enunciado para todos los enteros positivos n.

Inducción fuerte

Observación.

i) El Principio de Inducción Fuerte (PIF) (Sec. 3.3, p. 232, Rosen; Sec. 1.8, p. 65, Johnsonbaugh) lo usaremos ocasionalmente para demostrar proposiciones cuantificadas de la forma $\forall n\ P(n)$, donde el DD es el conjunto de los enteros a partir de un entero n_0 dado, i.e. el conjunto $\{n_0, n_0 + 1, n_0 + 2, ...\}$.

ii) El texto de Johnsonbaugh denota a la afirmación que se va a probar por $P(n)$ en lugar de $P(n + 1)$, convención que no seguiremos aquí.

iii) Omitir la propiedad del buen orden.

Enunciado. Sea la proposición cuantificada de la forma $\forall n\ P(n)$, donde $P(n)$ es una FP en el entero n, mientras que el DD es el conjunto de los enteros a partir de un n_0 dado. El PIF sostiene que si se cumplen tanto el PB como el PI fuerte, en donde:

- PB (cuando $n = n_0$): se demuestra que $P(n_0)$ es T;

- PI fuerte: se demuestra la implicación

$$\left[\bigwedge_{j=n_0}^{k} P(j)\right] \rightarrow P(k+1) \quad \text{es T para algún entero } k \geq n_0 \text{ arbitrario;} \tag{3.39}$$

entonces $P(n)$ vale para todos los enteros $n \geq n_0$. El PIF puede simbolizarse con la regla de inferencia compuesta:

$$\begin{aligned} &[P(n_0) \wedge H(k)] \rightarrow \left[\forall n : \ P(n) \quad \text{con } n \in \mathbb{Z}_{n_0}^{+}\right] \quad \text{, donde} \\ &H(k) \equiv \left[\bigwedge_{j=n_0}^{k} P(j)\right] \rightarrow P(k+1) \quad \text{para algún } k \geq n_0 \text{ arbitrario.} \end{aligned} \tag{3.40}$$

Ejemplo. [PIF cuando no es una igualdad ni una desigualdad, y con $n_0 = 12$]: Demostrar usando el PIF que toda TP de 12 o más centavos se puede cobrar usando estampillas de 4 o 5 centavos. Solución:

- PB: aunque basta demostrar el caso $n = 12$ pero después, para invocar el PIF, necesitaremos también chequear todos los casos hasta $n = 16$ (después se entenderá mejor por qué). Tenemos:
  (a) Cuando $n = 12$ usamos 3 estamp. de 4 centavos y 0 de 5 cent.
  (b) Cuando $n = 13$ usamos 2 estamp. de 4 centavos y 1 de 5 cent.
  (c) Cuando $n = 14$ usamos 1 estamp. de 4 centavos y 2 de 5 cent.
  (d) Cuando $n = 15$ usamos 0 estamp. de 4 centavos y 3 de 5 cent.
  (e) Cuando $n = 16$ usamos 4 estamp. de 4 centavos y 0 de 5 cent.

  En particular, en el caso (a), cuando $n = 12$, se cumple el PB.
- Sea la FP

$$P(k)\text{: una TP de } k \text{ centavos se cobra usando estampillas de 4 o 5 centavos} \tag{3.41}$$

  Ahora planteamos el PIF:

$$[P(k-3) \wedge P(k-2) \wedge P(k-1) \wedge P(k)] \rightarrow P(k+1) \tag{3.42}$$

  para algún entero $k \geq 15$ arbitrario. En particular, si $k = 15$ la Ec. (3.42) se reduce a

$$[P(12) \wedge P(13) \wedge P(14) \wedge P(15)] \rightarrow P(16) \tag{3.43}$$

  Dados los valores del inciso anterior, la Ec. (3.43) es T. Además la Ec. (3.43) muestra que según el valor del entero k podemos tener estampillas de 4 y 5 centavos, o solo de 4 centavos, o solo de 5 centavos. A continuación, para un entero $k \geq 15$ arbitrario;
  i) Si habíamos usado, al menos, 1 estampilla de 4 centavos (en forma similar a los casos (a-c), entonces la reemplazamos por 1 de 5 centavos;
  ii) Pero si no habíamos usado estampillas de 4 centavos, o sea, que habían, al menos, 3 estampillas de 5 centavos (similar al caso (d) cuando $k = 15$). Luego, reemplazamos 3 estampillas de 5 centavos por 4 estampillas de 4 centavos.

En cualquier caso, podemos pasar de una TP de k centavos a la TP de $k+1$ centavos. Es decir, la implicación $(P(k-3) \wedge P(k-2) \wedge P(k-1) \wedge P(k)) \rightarrow P(k+1)$ es T para algún entero $k \geq 15$ arbitrario.
- Finalmente, como se cumple el PB y el PI, el PIF asegura que se cumple el enunciado para todos los enteros $n \geq 15$.

La propiedad del buen orden

Omitir.

3.4. Def. recurs. e inducc. estruc.

Funciones definidas recursivamente

Definición. Una función $f(n)$ cuyo dominio es el conjunto de los enteros $\mathbb{Z}^+_{n_0}$, donde n_0 es un cierto entero inicial, se puede definir en forma inductiva (o recursiva (Sec. 3.4, p. 239, Rosen)) utilizando dos etapas:

- PB ($n = n_0$): se especifica el valor de la función $f(n)$ en n_0;
- Paso Recursivo (PR): se define una regla para obtener el valor de la función $f(n)$ a partir de sus valores en los enteros anteriores a n.

Observación. Las funciones definidas en forma inductiva o recursiva frecuentemente, tienen dominio en los enteros no-negativos ($n_0 = 0$) o positivos ($n_0 = 1$).

Ejemplo. [Función factorial]. La función factorial $F(n) = n!$ con dominio en los enteros no-negativos se define como

$$F(n) = \begin{cases} nF(n-1) & \text{si } n \geq 1 \\ 1 & \text{si } n = 0 \end{cases} \tag{3.44}$$

Ejemplo. [Función potencia]. La función potencia a^n con dominio en los enteros no-negativos se define como

$$a^n = \begin{cases} aa^{(n-1)} & \text{si } n \geq 1 \\ 1 & \text{si } n = 0 \end{cases} \tag{3.45}$$

Ejemplo. [Números (o sucesión) de Fibonacci]. Los números (o sucesión) de Fibonacci f_n se define como

$$f_n = \begin{cases} f_{n-1} + f_{n-2} & \text{si } n \geq 3 \\ 1 & \text{si } n = 1 \text{ o } n = 2 \end{cases} \tag{3.46}$$

Por ejemplo, los primeros 8 valores de la sucesión de Fibonacci, definida por la Ec. (3.46), se listan en la Tabla 3.2.

Ejemplo. [Sucesión de Fibonacci y PIF, en donde $n_0 = 6$ (para finales)]. Demostrar usando el PIF que

$$\underbrace{f_n}_{I_n} > \underbrace{\left(\frac{3}{2}\right)^{n-1}}_{D_n} \tag{3.47}$$

n	1	2	3	4	5	6	7	8
f_n	1	1	2	3	5	8	13	21
$(3/2)^{n-1}$	1.0000	1.5000	2.2500	3.3750	5.0625	7.5938	11.3906	17.0859

Tabla 3.2: Los primeros 8 valores de la sucesión f_n de Fibonacci, y de la función $(3/2)^{n-1}$.

para todos los enteros $n \geq 6$, donde f_n es la sucesión de Fibonacci definida por la Ec. (3.46). Solución:

- PB: aunque basta demostrar el caso $n = 6$ pero después, para poder invocar el PIF, necesitaremos también chequear los casos $n = 7$ y $n = 8$ (después se entenderá por qué). Entonces, los primeros 8 valores de la sucesión de Fibonacci y de la desigualdad definida por la Ec. (3.47), se listan en la Tabla 3.2. De esta última, vemos que
  (a) Cuando $n = 6$: se tiene $I_6 = 8$ y $D_6 \approx 7.5938$, por lo que $I_6 > D_6$;
  (b) Cuando $n = 7$: se tiene $I_7 = 13$ y $D_7 \approx 11.3906$, por lo que $I_7 > D_7$;
  (c) Cuando $n = 8$: se tiene $I_8 = 21$ y $D_7 \approx 17.0859$, por lo que $I_8 > D_8$.

  En particular, en el caso (a), cuando $n = 6$, se cumple el PB.
- Sea la FP
$$P(n)\text{: se cumple que } f_n > (3/2)^{n-1} \tag{3.48}$$
  Ahora planteamos el PIF:
$$[P(n-1) \wedge P(n)] \rightarrow P(n+1) \tag{3.49}$$
  para algún entero $n \geq 7$ arbitrario. En particular, si $n = 7$, la Ec. (3.49) se reduce a
$$[P(6) \wedge P(7)] \rightarrow P(8) \tag{3.50}$$
  Dados los valores (a)-(c) del inciso anterior, la Ec. (3.50) es T. A continuación, para un entero $n \geq 7$ arbitrario planteamos:
$$f_{n-1} > \left(\frac{3}{2}\right)^{n-2}$$
$$f_n > \left(\frac{3}{2}\right)^{n-1}$$
$$\overline{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}$$
$$f_{n-1} + f_n > \left(\frac{3}{2}\right)^{n-2} + \left(\frac{3}{2}\right)^{n-1}$$
$$f_{n+1} > \left(\frac{3}{2}\right)^{n} \left[\left(\frac{3}{2}\right)^{-2} + \left(\frac{3}{2}\right)^{-1}\right]$$
$$f_{n+1} > \left(\frac{3}{2}\right)^{n} \left[\frac{4}{9} + \frac{2}{3}\right] = \left(\frac{3}{2}\right)^{n} \cdot \frac{10}{9} > \left(\frac{3}{2}\right)^{n} \cdot 1 = D_{n+1}$$
  donde $10/9 \approx 1.1111 > 1$, por lo que $I_{n+1} > D_{n+1}$, y se cumple el PI.

- **Conjuntos y estructuras definidas recursivamente**: omitir.
- **Inducción estructural**: omitir.

3.5. Algoritmos recursivos

Omitir.

3.6. Verificación de programas

Omitir.

CAPÍTULO 4

Recuento

Nota. Estas notas siguen el texto de referencia Rosen (2004) manteniendo la numeración de las secciones y sus títulos, como una referencia adicional para el auto-estudio siguiendo ese texto.

Contents

4.1. Fundamentos de combinatoria

Principios básicos de recuento

Definición. La regla del producto (o **principio de la multiplicación**) (PM). Si se tiene una serie de t tareas tales que se pueden hacer en t etapas sucesivas, donde

- La tarea 1 se puede hacer de n_1 maneras;
- La tarea 2 se puede hacer de n_2 maneras; etc.;
- La tarea t se puede hacer de n_t maneras;

y las tareas son compatibles dos a dos, i.e. si se hace la tarea T_i también se puede hacer la tarea T_j, con $i \neq j$, entonces, el número de opciones z para hacer toda la tarea es $z = n_1 n_2 ... n_t$.

Ejemplo. Para contar el número de opciones en el menú de un bar, o para combinar la ropa (e.g. camisa, pantalón), etc., hay que emplear el PM, ver los ejemplos del libro.

Ejemplo. Etiquetar las butacas de un auditorio con una letra y un número entero positivo menor o igual a 100 ¿De cuántas formas distintas existen para etiquetar una butaca? Considere un alfabeto de 26 letras. Solución: el proceso de etiquetar las butacas consiste

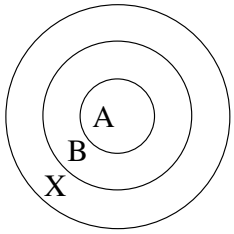

Figura 4.1: Diagrama de Venn cuando $A \subset B \subset X$.

en 2 tareas: asignar una de las 26 letras del alfabeto, y luego asignar uno de los 100 números disponibles. Usando el PM hay $z = 26 \cdot 100 = 2600$ formas distintas de etiquetar una butaca.

Ejemplo. Sean los 5 caracteres A, B, C, D, E. Hallar el número de cadenas que se pueden construir cuando:

i) De longitud 4, sin repetir caracteres: usamos el PM en 4 pasos sucesivos $z_{ABCD} = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$ opciones;
ii) De longitud 4, sin repetir caracteres, y que empiezan con B: otra vez usamos el PM en 4 pasos sucesivos $z_B = 1 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 24$ opciones;
iii) De longitud 4, sin repetir caracteres, y sin empezar con B: hay dos formas para calcularlo:
   a) Contar las opciones que empiezan con A, luego con C, luego con D, luego con E, y sumarlas. En cada uno se tiene el mismo número de opciones $z_0 = 1 \cdot 4 \cdot 3 \cdot 2 = 24$, por lo que en total habrán $z_{ACDE} = 4z_0 = 4 \cdot 24 = 96$ opciones;
   b) Hacerlo por diferencia entre los números de opciones en total y las que empiezan con B. Se tiene $z_{ACDE} = z_{ABCDE} - z_B = 120 - 24 = 96$ opciones.

Ejemplo. ¿Cuántas cadenas de bits diferentes hay de longitud 7? Solución: hay que llenar 7 casilleros, en cada uno hay 2 opciones, por lo que usando el PM hay $z = 2^7$.

Ejemplo. ¿Cuántas patentes diferentes hay si cada una consiste en una serie de 3 letras seguidas de 4 dígitos, y se permiten las repeticiones de letras o dígitos? Considere un alfabeto de 26 letras. Solución: considerando un alfabeto de 26 letras, los 10 dígitos, y usando el PM hay en total $z = 26^3 \cdot 10^4$.

Observación. Una demostración basada en un argumento combinatorio es una demostración que emplea un argumento de conteo.

Teorema. Utilizando un argumento de conteo demuestre que en un conjunto finito A de n elementos, se cumple que $|\mathcal{P}(A)| = 2^n$, donde $\mathcal{P}(A)$ es el conjunto potencia (o conjunto de partes) del conjunto A.

Demostración:

Un subconjunto del conjunto $A = \{a_1, a_2, ..., a_n\}$ se puede construir en n pasos sucesivos:

- Se elige (o no) el elemento a_1;

etapa 1: colocar elemento x_1	etapa 2: colocar elemento x_2	A	$B-A$	$X-B$	par ordenado (A,B) resultante
	en A	$\{1,2\}$	$\emptyset$	$\emptyset$	$(\{1,2\},\{1,2\})$
en A	en $B-A$	$\{1\}$	$\{2\}$	$\emptyset$	$(\{1\},\{1,2\})$
	en $X-B$	$\{1\}$	$\emptyset$	$\{2\}$	$(\{1\},\{1\})$
	en A	$\{2\}$	$\{1\}$	$\emptyset$	$(\{2\},\{1,2\})$
en $B-A$	en $B-A$	$\emptyset$	$\{1,2\}$	$\emptyset$	$(\emptyset,\{1,2\})$
	en $X-B$	$\emptyset$	$\{1\}$	$\{2\}$	$(\emptyset,\{1\})$
	en A	$\{2\}$	$\emptyset$	$\{1\}$	$(\{2\},\{2\})$
en $X-B$	en $B-A$	$\emptyset$	$\{2\}$	$\{1\}$	$(\emptyset,\{2\})$
	en $X-B$	$\emptyset$	$\emptyset$	$\{1,2\}$	$(\emptyset,\emptyset)$

Tabla 4.1: Ejemplo: cada uno de los subconjuntos A y B que verifican $A \subseteq B \subseteq X$ cuando $X = \{1,2\}$.

- Se elige (o no) el elemento a_2; etc.;
- Se elige (o no) el elemento a_n;

en donde cada etapa se puede realizar de 2 maneras por lo que, usando el PM, el número de subconjuntos posibles es $z = 2 \cdot 2 \cdot ... \cdot 2$, n veces, o sea $z = 2^n$.

Teorema. (para finales) Sea un conjunto finito X de n elementos, y los subconjuntos A y B de X. Utilizando un argumento de conteo demuestre que el número de pares ordenados (A,B) tales que $A \subseteq B \subseteq X$ es $z = 3^n$. Demostración: Sea el par ordenado (A,B) tal que $A \subseteq B \subseteq X$. Convine trazar un diagrama de Venn, ver Fig. 4.1, para ver lo siguiente: (i) Si se asigna cada elemento de X a uno de los conjuntos A, $B-A$ o $X-B$, entonces se obtendrá un par único (A,B) que satisface $A \subseteq B \subseteq X$; (ii) Recíprocamente, cada elemento del conjunto X debe estar en uno solo de los subconjuntos A, $B-A$ o $X-B$. Por eso, podemos emplear el siguiente proceso por etapas:

- Se asigna el elemento x_1 de X a alguno de los conjuntos A, $B-A$, o $X-B$;
- Se asigna el elemento x_2 de X a alguno de los conjuntos A, $B-A$, o $X-B$, etc.;
- Se asigna el elemento x_n de X a alguno de los conjuntos A, $B-A$, o $X-B$;

En cada una de estas etapas hay 3 opciones por lo que, usando el PM, el número total de opciones es $z = 3 \cdot 3 \cdot ... \cdot 3$, n veces, o sea $z = 3^n$.

Ejemplo. Sea un conjunto finito $X = \{1,2\}$, y los subconjuntos A y B de X tales que verifican $A \subseteq B \subseteq X$. Aplique el teorema anterior. Luego, liste cada uno de los pares ordenados (A,B) que verifican $A \subseteq B \subseteq X$. Solución: tenemos $n = 2$, por lo que $z = 3^2 = 9$, i.e. hay 9 pares ordenados (A,B) que verifican $A \subseteq B \subseteq X$. Cada uno está listado en la Tabla 4.1.

Ejemplo. ¿Cuántas cadenas de bits diferentes hay de longitud 6? Solución: usando el PM hay $z = 2^7$.

Ejemplo. ¿Cuántas funciones se pueden definir desde un conjunto $A = \{a_1, a_2, ..., a_m\}$ de m elementos (dominio) a otro conjunto $B = \{b_1, b_2, ..., b_n\}$ de n elementos (codominio)? Solución: una función $f: A \to B$ se corresponde con una elección de los n elementos del codominio B, para cada uno de los elementos del dominio A. Usando el PM hay $z = n \cdot n ... \cdot n$ (m veces), o sea, $z = |B|^{|A|}$, es decir, $z = |\text{codominio}|^{|\text{dominio}|}$. Notar que cuando $|A| = 1$ (o $m = 1$), se tiene que son posibles definir n funciones, aunque no serán funciones inyectivas.

Tarea. Escriba cada una de las funciones que se pueden definir entre los conjuntos A y B cuando: (i) $A = \{a\}$ y $B = \{1, 2, 3\}$; (ii) $A = \{a, b\}$ y $B = \{\delta\}$. En cada caso ¿hay inyectivas? ¿cuáles?

Ejemplo. ¿Cuántas funciones inyectivas se pueden definir desde un conjunto $A = \{a_1, a_2, ..., a_m\}$ de m elementos (dominio) a otro conjunto $B = \{b_1, b_2, ..., b_n\}$ de n elementos (codominio)? Solución:

i) Sea una función $f: A \to B$. Si $|A| > |B|$ entonces no hay unicidad de la preimagen, por lo que f no será inyectiva;
ii) Sabemos que $|A| \leq |B|$ (i.e. $m \leq n$). Si f debe ser inyectiva, entonces se la puede construir en m pasos sucesivos:
   - Elijo la imagen de a_1, para lo cual dispongo de n opciones;
   - Elijo la imagen de a_2, para lo cual dispongo de $(n-1)$ opciones;
   - Elijo la imagen de a_3, para lo cual dispongo de $(n-2)$ opciones; etc.;
   - Elijo la imagen de a_m, para lo cual dispongo de $(n-m+1)$ opciones;

   por lo que, usando el PM, en total hay

$$z = n \cdot (n-1)...(n-m+1) \tag{4.1}$$

   funciones inyectivas posibles $f: A \to B$, siempre que $|A| \leq |B|$;
ii) Caso particular: cuando $m = n$ entonces se pueden definir $n!$ funciones inyectivas.

Observación. El PM en términos de conjuntos finitos. Por una parte, si $A_1, A_2, ..., A_n$ son conjuntos finitos, entonces el número de elementos del producto cartesiano $A_1 \times A_2 ... \times A_n$ es igual al producto del números de elementos de cada conjunto. Por otra parte, la tarea de elegir un elemento del producto cartesiano $A_1 \times A_2 ... \times A_n$ consiste en elegir un elemento de A_1, un elemento de A_2, ..., un elemento de A_n. Luego, utilizando el PM se tiene que $|A_1 \times A_2 ... \times A_n| = |A_1||A_2|...|A_n|$.

Definición. La regla de la suma (o **principio de la suma**) (PS) (enunciado). Si se tiene una serie de t tareas tales que:

- La tarea 1 se puede hacer de n_1 maneras;
- La tarea 2 se puede hacer de n_2 maneras; etc.;
- La tarea t se puede hacer de n_t maneras;

y las tareas son incompatibles dos a dos, i.e. si se hace la tarea T_i no se hace la tarea T_j, con $i \neq j$, entonces el número de opciones z para hacer toda la tarea es $z = n_1 + n_2 + ... + n_t$.

Ejemplo. Un alumno puede elegir un tema proyecto entre 3 listas de temas. Si cada lista tiene 23, 17 y 13 propuestas, entonces ¿cuántas opciones dispone el alumno para elegir? Solución:

- De la primera lista dispone de 23 opciones;
- De la segunda lista dispone de 17 opciones; etc.;
- De la tercera lista dispone de 13 opciones.

Como las tareas incompatibles dos a dos entonces, por el PS, el alumno dispone de $z = 23 + 17 + 13 = 53$ opciones.

Observación. El PS en términos de conjuntos finitos. Por una parte, si A_1, A_2, ..., A_n son conjuntos finitos disjuntos dos a dos, i.e. $A_i \cap A_j = \emptyset$ cuando $i \neq j$, entonces el número de elementos de la unión $A_1 \cup A_2 ... \cup A_n$ es igual a la suma del números de elementos de cada conjunto. Por otra parte, sea T_i la tarea de elegir un elemento del conjunto A_i, para $i = 1, 2, ..., n$. Como las tareas son incompatibles dos a dos, el número de formas de elegir un elemento de la unión, que coincide con el número de elementos de la unión, es la suma $z = |A_1| + |A_2| + ... + |A_n|$.

Problemas de recuento más complicados

Lectura optativa.

El principio de inclusión-exclusión

Observación. El PIE en conteo. Cuando algunas tareas se pueden hacer simultáneamente, no se puede usar el PS para hallar el número de opciones de hacer toda la tarea pues estamos contando 2 veces las tareas que se pueden hacer simultáneamente. Una forma de resolverlo, es sumando el número de maneras de realizar cada una de las tareas, y luegos restamos el número de opciones de realizar las tareas que se pueden hacer simultáneamente, es decir, aplicamos el PIE.

Ejemplo. ¿Cuántas cadenas de 8 bits comienzan con 1 o terminan con 10? Solución. Usamos el PIE para 2 conjuntos:

$$\begin{aligned} |A \cup B| &= |A| + |B| - |A \cap B| \\ z_{A \cup B} &= z_A + z_B - z_{A \cap B} \end{aligned} \tag{4.2}$$

a) Tarea A: el número de cadenas de 8 bits que empiezan con 1 es $z_A = 1 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^7$;
b) Tarea B: el número de cadenas de 8 bits que terminan con 10 es $z_B = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 1 \cdot 1 = 2^6$;
iii) Tarea $A \cap B$: el número de cadenas de 8 bits que empiezan con 1 y terminan con 10 es $z_2 = 1 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 1 \cdot 1 = 2^5$;
iv) Tarea $A \cup B$: entonces $z_{A \cup B} = z_A + z_B - z_{A \cap B} = 2^7 + 2^6 - 2^5 = 128 + 64 - 32 = 160$ opciones. Notar que, en general, $z \geq 0$.

Diagrama en árbol

Intro.

- Algunos problemas de conteo se pueden resolver usando un Diagrama en Arbol (DA);
- Un digrama en árbol está formado por una raíz, un cierto número de ramas que parte de la raíz y, quizás, por otras ramas que empiezan en los extremos libres de las ramas, y así sucesivamente, hasta llegar a las hojas, las cuales son los extremos de las ramas en donde no empieza otra rama;
- Si utilizamos un árbol para contar, entonces usamos las ramas para representar cada posible elección. Los resultados posibles están en las hojas.

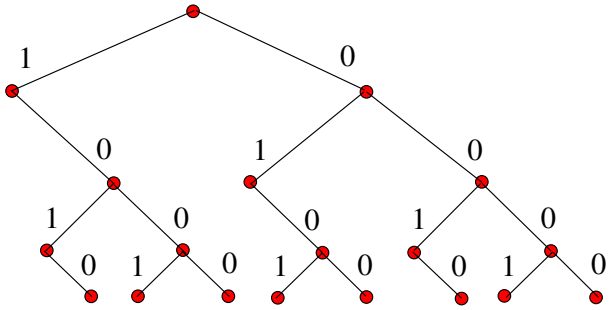

Figura 4.2: Diagrama en árbol para hallar el número de cadenas de 4 bits sin dos unos consecutivos.

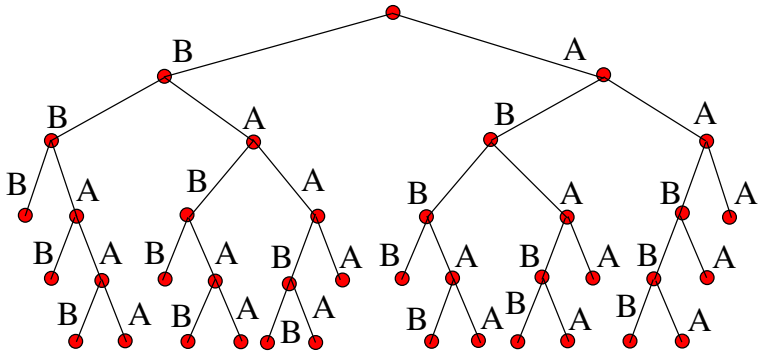

Figura 4.3: Eliminatoria entre 2 equipos con no más de 5 partidos, en donde el primero que gane 3 partidos es el campeón.

Ejemplo. ¿Cuántas cadenas de 4 bits sin dos unos consecutivos hay, y cuáles son? Solución: hay 8 cadenas que se muestran en el diagrama en árbol de la Fig. 4.2.

Ejemplo. Una eliminatoria entre 2 equipos con, a lo más, 5 partidos, en donde el primero que gane 3 partidos es el campeón ¿Cuáles son las posibles historias de la eliminatoria. Solución: los posibles historiales se muestran en el diagrama en árbol de la Fig. 4.3.

Ejemplo. ¿Cuántas opciones hay para elegir 2 libros de temas diferentes de la siguiente lista de libros: 5 de Computación (C), 3 de Matemática (M), y 2 de Arte (A), donde todos son libros distintos. Solución. Hay que elegir 2 libros de temas diferentes. Primero contamos las opciones por separado con 2 temas usando el PM. Tenemos:

- Computación-Matemática $z_{CM} = 5 \cdot 3 = 15$;
- Computación-Arte $z_{CA} = 5 \cdot 2 = 10$;
- Matemática-Arte $z_{MA} = 3 \cdot 2 = 6$;

Estas selecciones son incompatibles entre si, i.e. corresponden a conjuntos ajenos entre si, por lo que usamos el PS resultando $z = z_{CM} + z_{CA} + z_{MA} = 15 + 10 + 6$.

4.2. Principios del palomar

Teorema. El principio del PP (o principo de Dirichlet). Suponga que $(k + 1)$ o más palomas vuelan a k palomares. entonces algún palomar debe contener, al menos, 2 palomas.

Dem. por contradicción: supongamos que ninguno de los palomares contienen más de una paloma, entonces el número total de palomas es, como máximo, k, lo cual contradice que hay al menos $(k + 1)$ palomas.

Observación.

- En la demostración en el texto de Rosen: hay un error de tipeo.
- En la presentación en el texto de Johnsonbaugh: hay un error de tipeo en la expresión matemática donde aparece la función piso en lugar de la función techo.
- El PP, en cualquiera de sus formas, no dice cómo localizar el palomar con al menos dos palomas, solo asegura su existencia.
- Para usar el PP hay que decidir quiénes son las palomas y quiénes son los palomares.
- Entre otras aplicaciones el PP es empleado en teoría de juegos.

El principio del palomar generalizado

Teorema. El principio del PP **generalizado**. Si N palomas vuelan hacia k palomares, entonces existe al menos un palomar que contiene por lo menos techo(N/k) palomas. Dem. por contradicción: supongamos que ninguno de los palomares contienen más de techo$(N/k) - 1$ palomas, entonces el número total Z de palomas es, como máximo, $Z = k\,(\lceil N/k \rceil - 1)$. Pero,

$$\begin{aligned} k\,(\lceil N/k \rceil - 1) &< k\,[(N/k + 1) - 1] \\ Z &< N \end{aligned} \tag{4.3}$$

desigualdad que contradice que hay, al menos, N palomas, donde se tuvo en cuenta la desigualdad $\lceil N/k \rceil < N/k + 1$.

Ejemplo. Hay 10 personas con los nombre Germán (G), Javier (J), Luciana (L), y los apellidos Aimar (A), Ciaraviglio, y Mascherano (M). Probar que, al menos, 2 personas tienen el mismo nombre y apellido. Solución: vemos que hay $3 \cdot 3 = 9$ nombres completos para las 10 personas (e.g. tres posibles son LA, GC, y JM). En este caso, las palomas son las personas $N = 10$, y los palomares son los nombres completos $k = 9$. Entonces, usando el PP, algún mismo nombre completo se asigna, al menos, a techo $(10/9) = 2$ personas.

Observación. Sean los conjuntos finitos X e Y, con $m = |X|$ y $n = |Y|$, y una función $f\colon X \to Y$. Cuando el número de elementos del dominio es mayor al del codominio (i.e. $m > n$), entonces la función $f(x)$ no es inyectiva pues $y = f(x_i) = f(x_j)$ para, al menos un par de elementos $x_i, x_j \in X$, con $x_i \neq x_j$, indica que la preimagen de y no es única.

Ejemplo. Demostrar que en cualquier grupo de 6 personas o más hay, al menos, 3 personas que mutuamente, o bien se conocen, o bien no se conocen.
Solución: sean las 6 personas P_1, P_2, ..., P_6. Hay 5 pares posibles (P_1, P_2), (P_1, P_3), (P_1, P_4), (P_1, P_5), (P_1, P_6), que, o bien se conocen, o bien no se conocen. Empleando el PP generalizado hay $\lceil 5/2 \rceil = 3$ pares de personas (P_1, P_i), (P_1, P_j), (P_1, P_k) con un mismo valor (o bien se conocen, o bien no se conocen). Ahora ubicamos a esos 3 pares de personas en 2 habitaciones:

- En la habitación A ubicamos a las 3 personas P_i, P_j, P_k que conocen a P_1:

  - Si, al menos, un par entre P_i, P_j, P_k se conocen entre si, entonces, ese par más P_1 constituye un grupo de 3 personas que se conocen;
  - En caso contrario, P_i, P_j, P_k no se conocen entre si, por lo que ahora tenemos un grupo de 3 personas que no se conocen entre si.
- En la habitación B ubicamos a las 3 personas P_i, P_j, P_k que no conocen a P_1:
  - Si, al menos, un par entre P_i, P_j, P_k no se conocen entre si, entonces, ese par más P_1 constituye un grupo de 3 personas que no se conocen;
  - En caso contrario, P_i, P_j, P_k se conocen entre si, por lo que otra vez tenemos 3 pares de personas que se conocen entre si.

4.3. Permutaciones y combinaciones

Permutaciones

Definición. Permutación (o **n-permutación**). Una permutación (o n-permutación) de n elementos DISTINTOS x_1, x_2, ..., x_n es un ordenamiento de sus n elementos. Notación: el número de permutaciones de n elementos tomados de un conjunto de n elementos distintos lo denotamos con $P(n)$ (o con $P(n, n)$).

Ejemplo. Encuentre todas las permutaciones posibles de las letras A, B, C. Solución: se tienen 6 posibilidades

- ABC, BCA, CAB (obtenida con permutaciones circulares);
- ACB, BAC, CBA (fija la primera letra del caso anterior y una permutación de las 2 restantes).

Teorema. El número de permutaciones con n elementos tomados de un conjunto de n elementos distintos está dado por $P(n) = n!$
Demostración: Usamos el PM para construir una permutación en n etapas sucesivas:

- Se elige el 1er elemento, para lo cual hay n opciones;
- Se elige el 2do elemento, para lo cual quedan $(n - 1)$ opciones;
- Se elige el 3er elemento, para lo cual quedan $(n - 2)$ opciones; etc.;
- Se elige el último elemento, para lo cual queda 1 opción;

por lo que, usando el PM, el número de permutaciones posibles es

$$P(n, n) = n(n - 1)(n - 2)...2 \cdot 1 = n! \tag{4.4}$$

Ejemplo. Sean las 6 letras $ABCDEF$. Determine el número de permutaciones que contienen:

- La subcadena DEF. Solución: hay que contar todas las permutaciones de los caracteres A, B, C, y DEF (fija). Vemos que para el conteo tenemos 4 cadenas efectivas, por lo que se tiene $z = 4!$
- Las letras DEF juntas pero en cualquier orden. Solución: a la solución del caso anterior hay que agregarle las permutaciones de los caracteres D, E, y F, lo cual agrega $3!$ por lo que en total se tiene $z = 4! \cdot 3! = 6 \cdot 24 = 144$.

Ejemplo. Sean 6 personas distinguibles (i.e. no gemelos ni clones). Determine el número de opciones para sentarlas alrededor de una mesa circular. Solución: notar que los arreglos obtenidos por rotación se consideran iguales porque una vez sentados en alguna forma, los podemos correr a todos juntos sin cambiar la disposición relativa. En este caso, sentamos a A en cualquier lugar, luego sentamos a las $5 = 6 - 1$ personas restantes en alguna forma, para lo cual hay $(6 - 1)!$ opciones.

Observación. En general, $P(n, \text{arreglo lineal}) = n!$ y $P(n, \text{arreglo circular}) = (n - 1)!$

Definición. Permutación de r elementos (**r-permutación**). Una permutación de r elementos (o r-permutación) tomados de entre n elementos DISTINTOS x_1, x_2, ... x_n, es un ordenamiento de r elementos, donde $0 \leq r \leq n$. Notación: el número de permutaciones de r elementos tomados de un conjunto de n elementos distintos, con $0 \leq r \leq n$, lo denotamos con $P(n, r)$.

Ejemplo. Determine todas las permutaciones con 2 elementos tomados del conjunto $\{A, B, C, D\}$. Solución. Por fuerza bruta obtenemos:

- AB, AC, AD (la 1ra con la 2da, con la 3ra, etc.);
- BC, BD (la 2da con la 3ra, con la 4ta, etc.);
- CD (la 3ra con la 4ta, con la 5ta, etc.);
- BA, CA, DA, CB, DB, DC (todas las permutaciones de los casos anteriores).

con un total de 12 alternativas.

Teorema. El número de permutaciones con r elementos tomados de un conjunto de n elementos distintos, con $0 \leq r \leq n$, está dado por $P(n, r) = n \cdot (n - 1)....(n - r + 1)$. *Demostración*: Usamos el PM para construir una permutación con r elementos tomados de un conjunto de n elementos, donde $0 \leq r \leq n$, lo hacemos en r etapas sucesivas:

- Se elige el elemento 1, para lo cual hay n opciones;
- Se elige el elemento 2, para lo cual hay $(n - 1)$ opciones;
- Se elige el elemento 3, para lo cual hay $(n - 2)$ opciones; etc.;
- Se elige el elemento r, para lo cual hay $(n - r + 1)$ opciones;

por lo que, usando el PM, el número de permutaciones posibles con r elementos es

$$P(n, r) = n(n - 1)(n - 2)...(n - r + 1) \tag{4.5}$$

Notar que si $r = n$, entonces se recupera el caso anterior.

Ejemplo. Determine el número de permutaciones con 2 elementos tomados del conjunto $\{A, B, C, D\}$. Solución: tenemos $n = 4$ y $r = 2$, por lo que $n - r + 1 = 4 - 2 + 1 = 3$, y el número de permutaciones posibles de 2 elementos tomados de un conjunto de 4 elementos es $P(4, 2) = 4 \cdot 3 = 12$, cada una de las cuales fueron listadas en el ejemplo anterior.

Observación. Fórmula alternativa de cómputo para $P(n, r)$. Notar que:

$$\begin{aligned} P(n, r) &= n(n - 1)(n - 2)...(n - r + 1) \\ &= \frac{n(n - 1)(n - 2)...(n - r + 1)(n - r)(n - r - 1)...2 \cdot 1}{(n - r)(n - r - 1)...2 \cdot 1} \\ &= \frac{n!}{(n - r)!} \end{aligned} \tag{4.6}$$

Ejemplo. Determine el número de opciones para ubicar alrededor de una mesa (rectangular) a 7 Marcianos (M) y a 5 Venusianos (V), donde todos son distinguibles (i.e. no hay gemelos ni clones), si 2 V no-pueden sentarse juntos. Solución. Una sentada la podemos hacer en 2 etapas:

i) Sentamos primero a los 7 de Marte dejando un lugar libre por medio, para lo cual hay $z_M = P(7) = 7!$ opciones. Notar que de este modo se generaron 7+1=8 lugares libres, i.e. _M1_M2_M3_M4_M5_M6_M7_;
ii) Luego sentamos a los 5 de Venus en esos 8 lugares libres, para lo cual hay $z_V = P(8, 5)$ opciones;

Finalmente, usando el PM, se tienen $z = z_M z_V = P(7)P(8, 5) = 7!P(8, 5)$ opciones.

Combinaciones

Definición. Combinación. Una combinación de r elementos tomados de entre n elementos DISTINTOS x_1, x_2, ... x_n, es una selección NO-ORDENADA de r elementos, donde $0 \leq r \leq n$. Notación: el número de combinaciones de r elementos tomados de un conjunto de n elementos distintos, con $0 \leq r \leq n$, lo denotamos tanto con $\binom{n}{r}$ (notación de Newton), como con $C(n, r)$.

Ejemplo. Determine todas las combinaciones con 2 elementos tomados del conjunto $\{A, B, C, D\}$. Solución. Por fuerza bruta obtenemos 6 posibilidades:

- AB, AC, AD (la 1ra con la 2da, con la 3ra, etc.);
- BC, BD (la 2da con la 3ra, con la 4ta, etc.);
- CD (la 3ra con la 4ta, con la 5ta, etc.);

Teorema. El número de combinaciones con r elementos tomados de un conjunto A de n elementos distintos, con $0 \leq r \leq n$, está dado por

$$C(n, r) = \frac{n!}{r!(n-r)!} \tag{4.7}$$

Demostración. Podemos construir las permutaciones con r elementos tomados de un conjunto de n elementos, con $0 \leq r \leq n$, en 2 etapas sucesivas:

- Construimos todas las combinaciones con r elementos tomados de un conjunto de n elementos;
- Para cada combinación con r elementos obtenemos todas sus permutaciones posibles.

Luego, usando el PM, el número de permutaciones con r elementos es igual al producto del número de combinaciones con r elementos tomados de una conjunto de n elementos,

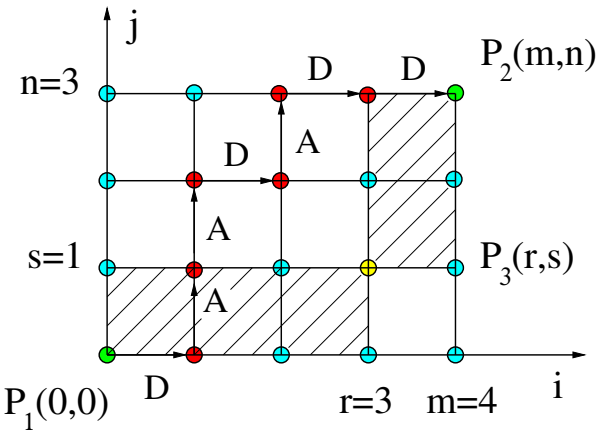

Figura 4.4: Grilla rectangular entre los vértices $P_1(0,0)$ y $P_2(m,n)$. Incluye un vértice intermedio $P_3(r,s)$, y la ruta *DAADADD*.

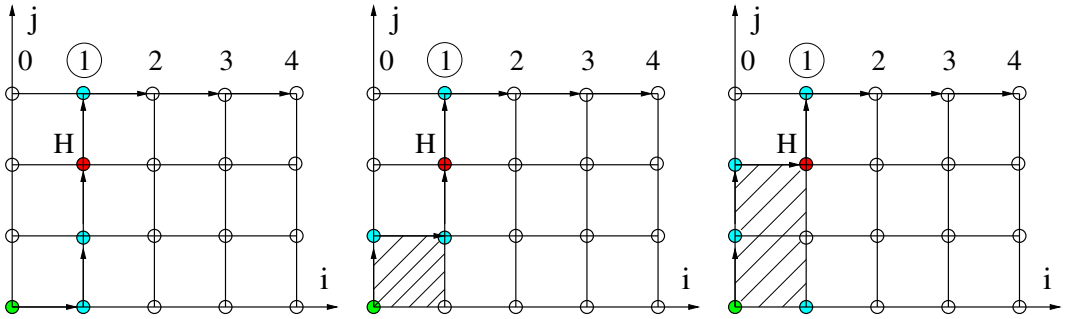

Figura 4.5: La clase de las rutas que llegan al borde superior por primera vez en la posición $i = 1$ en la grilla $n = 3 \times m = 4$.

por el número de sus permutaciones, i.e.

$$\begin{aligned} P(n,r) &= C(n,r)P(r) \\ \therefore \quad C(n,r) &= \frac{P(n,r)}{P(r)} \\ &= \frac{n(n-1)(n-2)...(n-r+1)}{r(r-1)...1} \\ &= \frac{n!}{r!(n-r)!} \end{aligned} \tag{4.8}$$

Ejemplo. Si $\{A,B,C,D\}$, y $r = 2$, tendremos

- AB, AC, AD, BC, BD, CD (todas las combinaciones con 2 elementos);
- BA, CA, DA, CA, DB, DC (todas las permutaciones de las combinaciones anteriores);
- Aqui tenemos $P(4,2) = 12$ y $P(2) = 2! = 2$, con lo que $C(4,2) = P(4,2)/P(2) = 12/2 = 6$, y que ya fueron listadas.

Ejemplo. Si $\{A,B,C,D\}$, y $r = 2$, tendremos

- AB, AC, AD, BC, BD, CD (todas las combinaciones con 2 elementos);
- BA, CA, DA, CA, DB, DC (todas las permutaciones de las combinaciones anteriores);

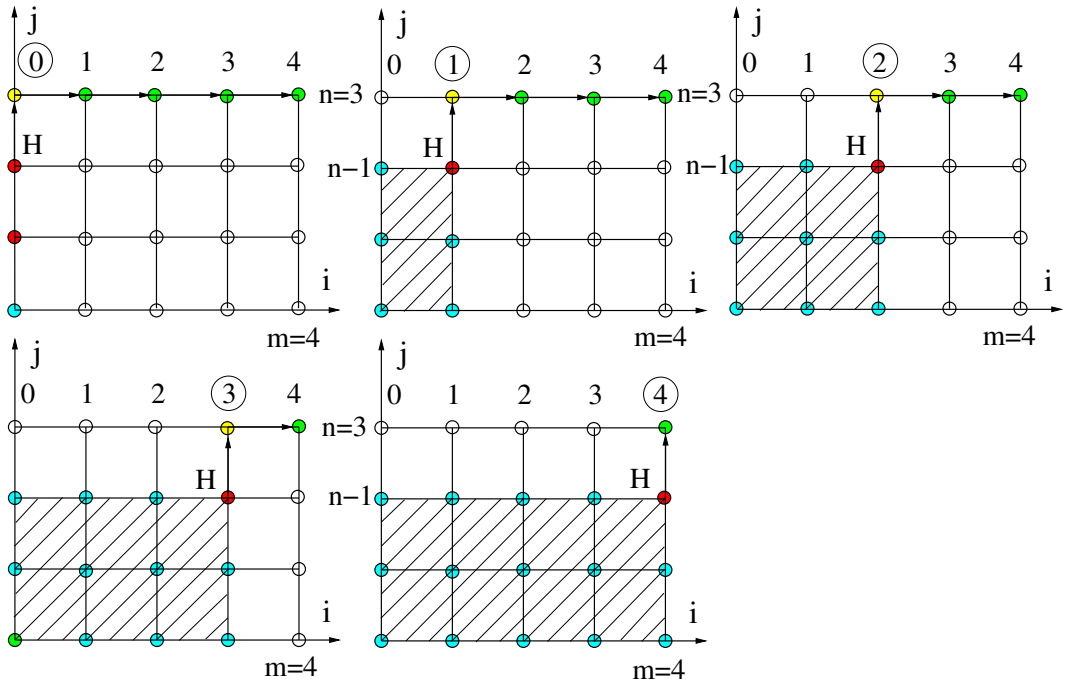

Figura 4.6: División de las rutas en clases según la primera vez que tocan el borde superior. Una ruta toca al borde superior por primera vez en cualquiera de las líneas verticales $i = 0, 1, 2, 3, 4$.

- Aquí tenemos $P(4,2) = 12$ y $P(2) = 2! = 2$, con lo que $C(4,2) = P(4,2)/P(2) = 12/2 = 6$, y que ya fueron listadas.

Definición. Identidad combinatoria. Una identidad combinatoria es una identidad que involucra coeficientes binomiales.

Observación. Usualmente las identidades combinatorias se demuestran utilizando dos estrategias:

- Mediante un argumento de conteo en conjuntos finitos;
- Mediante manipulaciones algebraicas basadas en la definición del coeficiente binomial $C(m,n)$.

Ejemplo. El teorema de Pascal en combinatoria es un primer ejemplo de una identidad combinatoria relativa a los coeficientes binomiales.

Ejemplo. Conteo de rutas posibles en una grilla rectangular entre vértices $P_1(0,0)$ y $P_2(m,n)$ dados, y posiblemente un vértice intermedio $P_3(r,s)$, con $0 \leq r \leq m$ y $0 \leq s \leq n$. Demuestre, incluyendo el uso de argumentos de conteo, que:

i) Existen $\binom{m+n}{m}$ rutas para ir desde el vértice $P_1(0,0)$ hacia el $P_2(m,n)$, yendo siempre hacia la Derecha (D) y hacia arriba (A);

ii) Se verifican las *identidades combinatorias*

$$\begin{aligned}\binom{m+n}{m} &= \binom{m+n}{n} \\ \binom{m+n}{m} &= \sum_{k=0}^{m} \binom{k+(n-1)}{k}\end{aligned} \tag{4.9}$$

Solución:

i) Cada ruta desde $P_1(0,0)$ hacia $P_2(m,n)$ se puede representar como una cadena de $(m+n)$ letras A (hacia Arriba) y D (hacia a la Derecha). Por ejemplo, en la Fig. 4.4 se muestra el caso $m = 4$ y $n = 3$, en donde la cadena de cualquier ruta tiene 7 caracteres, e.g. en la dicha figura se ha marcado la ruta $DAADADD$, con 4 letras D y 3 letras A. Entonces, contar el números de rutas en esas condiciones equivale al número de cadenas que se pueden construir, para lo cual hay 2 opciones:

- Elegimos primero las m posiciones para las letras D, en cualquier orden, entre los $(m+n)$ lugares en la cadena, y luego completamos las posiciones restantes con las letras D. Luego, el número total de rutas posibles debe ser $\binom{m+n}{m}$;
- Elegimos primero las n posiciones para las letras A, en cualquier orden, entre los $(m+n)$ lugares en la cadena, y luego completamos las posiciones restantes con letras A. Luego, el número total de rutas posibles debe ser $\binom{m+n}{n}$;
- El resultado de los conteos anteriores debe ser el mismo, por lo que $\binom{m+n}{m} = \binom{m+n}{n}$.

Observaciones:

- Las posiciones elegidas para las letras A y D se pueden distinguir, por eso, no incide que las letras sean indistinguibles;
- La primera Ec. (4.9) también se puede comprobar usando la definición de número combinatorio y un poco de álgebra:

$$\begin{aligned}\binom{m+n}{m} &= \frac{(m+n)!}{m!(m+n-m)!} = \frac{(m+n)!}{m!n!} \\ \binom{m+n}{n} &= \frac{(m+n)!}{n!(m+n-n)!} = \frac{(m+n)!}{n!m!}\end{aligned} \tag{4.10}$$

ii)
- Dividimos las rutas en clases basándonos en la primera vez que tocan el borde superior. Una ruta puede tocar el borde superior por primera vez en cualquiera de las $m+1$ líneas verticales;
- Notar que (i) las clases son ajenas porque una ruta no puede llegar al borde superior por primera vez en más de una ocasión; y (ii) cada ruta pertenece a alguna clase;
- Es decir, esas clases definan una partición del conjunto de rutas, por lo cual podemos emplear el PS, según el cual la suma del número de rutas en cada clase es igual al número total de rutas, pues (i) ninguna ruta se cuenta 2 veces (porque están en clases disjuntas); y (ii) cada ruta pertenece a alguna clase;

- Por ejemplo, en la Fig. 4.5 se muestran las 3 rutas que existen para llegar al borde superior por primera vez en la línea vertical $i = 2$. Notar que las rutas alternativas se dan antes de llegar al vértice H marcado, i.e. una vez llegado a H sólo hay una forma de terminar la ruta: subiendo un cuadro (una A). Por eso basta contar el número de rutas en la subgrilla sombreada 1×2 y, por el inciso anterior, se obtiene $z_2 = \binom{1+2}{1} = \binom{3}{1} = 3$, valor ya obtenido;
- Haciendo lo mismo en cada una de las líneas verticales $i = 0, 1, 2, 3, 4$, ver Fig. (4.6), se tiene

$$\begin{aligned}
\text{en } i = 0: &\quad \binom{0+2}{0} = \binom{2}{0} = 1 \\
\text{en } i = 1: &\quad \binom{1+2}{1} = \binom{3}{1} = 3 \\
\text{en } i = 2: &\quad \binom{2+2}{2} = \binom{4}{2} = 6 \\
\text{en } i = 3: &\quad \binom{3+2}{3} = \binom{5}{3} = 10 \\
\text{en } i = 4: &\quad \binom{4+2}{4} = \binom{6}{4} = 15
\end{aligned} \tag{4.11}$$

  cuya suma z_D es el lado derecho de la Ec. (4.9) y es igual al lado izquierdo z_I de la misma ecuación

$$\begin{aligned}
z_D &= 1 + 3 + 6 + 10 + 15 = 35 \\
z_I &= \binom{4+3}{3} = \binom{7}{3} = 35
\end{aligned} \tag{4.12}$$

- Generalizando la ley que se va generando en la Ec. (4.11) se tiene

$$\begin{aligned}
z_D &= \sum_{k=0}^{m} \binom{k + (n-1)}{k} \\
z_I &= \binom{m+n}{m}
\end{aligned} \tag{4.13}$$

  y como debe ser $z_I = z_D$, se obtiene la segunda identidad de la Ec. (4.9).

4.4. Coeficientes binomiales

Ejemplo. Evaluar $(a + b)^3$ a partir de un desarrollo algebraico directo.
Solución:

selección en el 1er factor $(a+b)$	selección en el 2do factor $(a+b)$	selección en el 3er factor $(a+b)$	producto
a	a	a	$aaa = a^3$
a	a	b	$aab = a^2b$
a	b	a	$aba = a^2b$
a	b	b	$abb = ab^2$
b	a	a	$baa = a^2b$
b	a	b	$bab = ab^2$
b	b	a	$bba = ab^2$
b	b	b	$bbb = b^3$

Tabla 4.2: Tarea de selección de los símbolos a y b, en cualquier orden y permitiendo las repeticiones.

$$\begin{aligned}(a+b)^3 &= (a+b)(a+b)(a+b)\\ &= (a+b)(aa+ab+ba+bb)\\ &= (aaa+aab+aba+abb)(baa+bab+bba+bbb)\\ &= a^3+a^2b+a^2b+ab^2+a^2b+ab^2+ab^2+b^3\\ &= a^3+3a^2b+3ab^2+b^3\end{aligned} \tag{4.14}$$

Pero este resultado se lo puede repensar como una tarea de selección de símbolos a o b, en cualquier orden, permitiendo las repeticiones, tarea que se muestra en la Tabla 4.2, cuya generalización conduce al teorema de Newton (o teorema de binomio).

Teorema de Newton (o teorema de binomio)

Teorema. Teorema de Newton (o teorema de binomio). Si $a, b \in \mathbb{R}$ y n es un entero positivo, entonces

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k \tag{4.15}$$

i) Demostración 1 (usando un argumento de conteo):

- En el desarrollo de $(a+b)^n$, un término de la forma $a^{n-k}b^k$ surge de elegir b en k factores, y elegir a en $(n-k)$ factores adicionales;
- Pero esto se puede hacer de $C(n,k)$ modos pues $C(n,k)$ cuenta el número de opciones para elegir k elementos de entre n disponibles;
- Entonces $a^{n-k}b^k$ debe aparecer $C(n,k)$ veces. Esto vale para $0 \leq k \leq n$ y, aplicando el PS,

$$(a+b)^n = \binom{n}{0}a^nb^0 + \binom{n}{1}a^{n-1}b^1 + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{n}a^0b^n \tag{4.16}$$

ii) Demostración 2 (usando inducción): para alumnos libres.

Tarea. Re-hacer ejemplos 6.7.2, 6.7.3, y 6.7.5.

Observación. Los coeficientes binomiales son los números combinatorios.

Ejemplo. Encontrar el coeficiente de a^5b^4 de $(a+b)^9$.
Solución: con $n = 9$, y $k = 4$ en el binomio de Newton se tiene que $C(n,k)a^{n-k}b^k = C(9,5)a^5b^4 = 126a^5b^4$.

Triángulo de Pascal (o de Tartaglia)

El triángulo de Pascal (o de Tartaglia) permite obtener rápidamente los coeficientes binomiales construyendo la siguiente disposición de enteros en la forma de un esquema triangular:

$n = 0$: 1
$n = 1$: 1 1
$n = 2$: 1 2 1
$n = 3$: 1 3 3 1
$n = 4$: 1 4 6 4 1

En esta construcción se pueden identificar

fila horizontal n: $\binom{n}{k-1}$ $\binom{n}{k}$
fila horizontal $(n+1)$: $\binom{n+1}{k}$
diagonal $(k-1)$ diagonal k

Teorema. El triángulo de Pascal se justifica mediante el teorema (o identidad) de Pascal en combinatoria:

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k} \quad \text{para todos los enteros positivos } n \text{ y } k \text{ tales que } 1 \leq k \leq n \tag{4.17}$$

el cual es un ejemplo de una *identidad combinatoria*.

i) Demostración (usando un argumento de conteo):
   - Sea un conjunto A con n elementos. Al agregarle un nuevo elemento x, entonces el número de subconjuntos de k elementos que se pueden formar a partir del conjunto $B = A \cup \{x\}$ está dado por $C(n+1,k)$.
   - Los subconjuntos de k elementos de B se pueden dividir en 2 clases ajenas, a saber, los de la clase 1, dados por los subconjuntos de B que no contienen al elemento x, y los de la clase 2, que sí lo contienen.
   - Cada subconjunto de la clase 1 es un conjunto de k elementos tomados del conjunto A, por lo que hay $C(n,k)$ opciones;
   - Cada subconjunto de la clase 2 consiste en la unión de un subconjunto de $k-1$ elementos de A, y el conjunto $\{x\}$, formado por el elemento x, por lo que hay $C(n,k-1)$ opciones;
   - Luego, usando el PS, se tiene que $C(n+1,k)$ debe ser igual a la suma $C(n,k) + C(n,k-1)$.

ii) Demostración 2 (usando la definición): es un ejercicio en la GTP.

Ejemplo. Demostrar que para todo entero n positivo se tiene la identidad combinatoria:

$$\sum_{k=1}^{n} \binom{n}{k} = 2^n \tag{4.18}$$

Solución:

i) Demostración 1 (usando un argumento de conteo):

- Dado un conjunto A de n elementos, hay $C(n,k)$ subconjuntos de k elementos, y la suma de todos ellos cuenta el número de subconjuntos posibles de A;
- Por otra parte, se sabe que hay 2^n subconjuntos posibles de un conjunto A de n elementos;
- Dado que se trata de la misma tarea, ambas expresiones deben ser iguales.

ii) Demostración 2 (usando inducción). A partir de:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \tag{4.19}$$

si $a = b = 1$, entonces se obtiene la Ec. 4.18.

Ejemplo. Demostrar que para todo entero n positivo se tiene la identidad combinatoria

$$\sum_{i=k}^{n} \binom{i}{k} = \binom{n+1}{k+1} \tag{4.20}$$

Solución:

- Re-escribimos la identidad de Pascal

$$\binom{i}{k} = \binom{i+1}{k+1} - \binom{i}{k+1} \qquad \text{donde } 1 \le k \le n \tag{4.21}$$

- Antes hacemos el caso particular

$$\begin{aligned} \sum_{i=3}^{6} \binom{i}{3} &= \binom{3}{3} + \binom{4}{3} + \binom{5}{3} + \binom{6}{3} \\ &= \binom{3}{3} + \left[\binom{5}{4} - \binom{4}{4}\right] + \left[\binom{6}{4} - \binom{5}{4}\right] + \left[\binom{7}{4} - \binom{6}{4}\right] \\ &= \binom{3}{3} - \binom{4}{4} + \binom{7}{4} = \binom{7}{4} \end{aligned} \tag{4.22}$$

- Ahora, en general,

$$\begin{aligned}\sum_{i=k}^{n}\binom{i}{k} &= \binom{k}{k}+\binom{k+1}{k}+...+\binom{n}{k}\\ &= 1+\left[\binom{k+2}{k+1}-\binom{k+1}{k+1}\right]\\ &+\left[\binom{k+3}{k+1}-\binom{k+2}{k+1}\right]+...\\ &+\left[\binom{n+1}{k+1}-\binom{n}{k+1}\right]\\ &=\binom{n+1}{k+1}\end{aligned} \tag{4.23}$$

Ejemplo. Demostrar que para todo entero n positivo se tiene la identidad combinatoria

$$\binom{1}{1}+\binom{2}{1}+...+\binom{n}{1}=\frac{n+1}{2} \tag{4.24}$$

Solución:

$$\binom{n+1}{2}=\frac{(n+1)!}{2!(n-1)!}=\frac{(n+1)n(n-1)!}{2(n-1)!}=\frac{n(n+1)}{2} \tag{4.25}$$

$$\binom{n+1}{1}=\frac{n!}{1!(n-1)!}=\frac{n(n-1)!}{1(n-1)!}=n \tag{4.26}$$

Teorema. Teorema multinomial (caso $m = 3$. Si $a, b, c \in \mathbb{R}$ y n es un entero positivo, entonces

$$(a+b+c)^n=\sum_{i+j+k=n}\binom{n}{i\ j\ k}a^ib^jc^k \tag{4.27}$$

Demostración:

- Antes, para concretar, primero evaluemos $(a + b + c)^{17}$. En ese caso, hay que evaluar $(a + b + c)^{17} = (a + b + c)...(a + b + c)$, con 17 factores idénticos. Entre otros estará el término $a^4b^6c^7$ pues la suma de esos exponentes es $4 + 6 + 7 = 17$, de donde

$$\begin{aligned}&\text{Como } a \text{ puede ser elegido en 4 de los 17 factores:}\\ &\text{Como } b \text{ puede ser elegido en 6 de los 17 factores:}\\ &\text{Como } c \text{ puede ser elegido en 7 de los 17 factores:}\end{aligned} \tag{4.28}$$

  tendremos

$$\binom{17}{4}\binom{13}{6}\binom{7}{7}=\frac{17!}{4!13!}\frac{13!}{6!7!}\frac{7!}{7!0!}=\frac{17!}{4!6!7!} \tag{4.29}$$

  entonces, en el desarrollo de $(a + b + c)^{17}$ está el el término

$$\frac{17!}{4!6!7!}a^4b^6c^7 \tag{4.30}$$

número de solución	i	j	k
1	3	0	0
2	0	3	0
3	0	0	3
4	2	1	0
5	2	0	1
6	1	2	0
7	0	2	1
8	0	1	2
9	1	0	2
10	1	1	1

Tabla 4.3: Valores de i, j, k tales que $i + j + k = 3$.

Lo que se está haciendo es calcular el número de formas de ordenar las 17 letras *aaaabbbbbbccccccc*. Se concluye que el desarrollo de $(a + b + c)^{17}$ es la suma de todos los términos de la forma

$$\frac{17!}{i!\,j!k!}a^i b^j c^k \tag{4.31}$$

donde i, j, k recorren todos los posibles enteros no-negativos tales que $i + j + k = 17$.

- En general, se tiene

$$(a + b + c)^n = \sum_{i+j+k=n} \binom{n}{i\ j\ k} a^i b^j c^k \tag{4.32}$$

Ejemplo. Evaluar $(x + y + z)^3$. Solución:

$$(x + y + z)^3 = \sum_{i+j+k=3} \binom{3}{i\ j\ k} x^i y^j z^k \tag{4.33}$$

donde el número de soluciones de $i + j + k = 3$ se obtiene con el teorema del pelotero con $k = 3$ y $t = 3$, resultando $z = C(k + (t-1), (t-1)) = C(3 + 2, 2) = C(5, 2) = 10$ sumandos. Los valores i, j, k son mostrados en la Tabla 4.3. Tenemos

$$\begin{aligned}(x + y + z)^3 = {} & \frac{3!}{3!0!0!}x^3y^0z^0 + \frac{3!}{0!3!0!}x^0y^3z^0 + \frac{3!}{0!0!3!}x^0y^0z^3 \\ & + \frac{3!}{2!1!0!}x^2y^1z^0 + \frac{3!}{2!0!1!}x^2y^0z^1 + \frac{3!}{1!2!0!}x^1y^2z^0 \\ & + \frac{3!}{0!2!1!}x^0y^2z^1 + \frac{3!}{0!1!2!}x^0y^1z^2 + \frac{3!}{1!0!2!}x^1y^0z^2 + \frac{3!}{1!1!1!}x^1y^1z^1\end{aligned} \tag{4.34}$$

operando y simplificando

$$\begin{aligned}(x + y + z)^3 = {} & x^3 + y^3 + z^3 \\ & + 3x^2y^1 + 3x^2z^1 + 3x^2y^2 \\ & + 3y^2z^1 + 3y^1z^2 + 3x^1z^2 + 6x^1y^1z^1\end{aligned} \tag{4.35}$$

4.5. Permutaciones y combinaciones generalizadas

Permutaciones con repetición

Ejemplo. Encuentre todas las cadenas que se pueden formar usando todas las letras de la palabra MISSISSIPPI. Solución: tenemos $n = 11$ letras pero, como hay letras repetidas, la respuesta no es $z = (11 \cdot 10...2 \cdot 1) = 11! = 39\,916\,800$, sino que son muchas menos. Notar que

- Hay $C(11, 2)$ lugares para las 2 letras P, y pierdo 2 lugares;
- Hay $C(11 - 2, 4) = C(9, 4)$ lugares para las 4 letras S, y pierdo 4 lugares;
- Hay $C(9 - 4, 4) = C(5, 4)$ lugares para las 4 letras I, y pierdo 4 lugares;
- Hay $C(5 - 4, 1) = C(1, 1)$ lugares para la letra M (una sola);

y usando el PM se tiene

$$\begin{aligned} z &= \binom{11}{2} \cdot \binom{9}{4} \cdot \binom{5}{4} \cdot \binom{1}{1} \\ &= \frac{11!}{2!9!} \cdot \frac{9!}{4!5!} \cdot \frac{5!}{4!1!} \cdot \frac{1!}{1!0!} \\ &= \frac{11!}{2!4!4!1!} = 34\,650 \end{aligned} \tag{4.36}$$

y que es mucho-mucho menor (en una relación 1152 a 1) con respecto a una permutación de 11 elementos distinguibles.

Teorema. El número de permutaciones de n elementos tomados de una colección con:

- n_1 elementos idénticos del tipo 1;
- n_2 elementos idénticos del tipo 2; etc.
- n_t elementos idénticos del tipo t;

tal que hay $n = n_1 + n_2 + ... + n_t$ elementos en total, está dado por

$$z = \frac{n!}{n_1!n_2!...n_t!} \qquad \text{con } n = n_1 + n_2 + ... + n_t \tag{4.37}$$

Demostración: Hay que asignar las posiciones a cada uno de los n elementos, en donde

- Para los n_1 elementos idénticos del tipo 1, hay $C(n, n_1)$ opciones, y se pierden n_1 lugares;
- Para los n_2 elementos idénticos del tipo 2, hay $C(n - n_1, n_2)$ opciones, y se pierden otros n_2 lugares;
- Para los n_3 elementos idénticos del tipo 3, hay $C(n-n_1-n_2, n_3)$ opciones, y se pierden otros n_3 lugares; etc.

por lo que, usando el PM, el número total de permutaciones posibles es

$$\begin{aligned} z &= C(n, n_1) \cdot C(n - n_1, n_2) \cdot C(n - n_1 - n_2, n_3) \; ... \; C(n - n_1 - n_2... - n_{t-1}, n_t) \\ &= \frac{n!}{n_1!(n - n_1)!} \cdot \frac{(n - n_1)!}{n_2!(n - n_1 - n_2)!} \cdots \frac{(n - n_1 - n_2... - n_{t-1})!}{n_t!} \\ &= \frac{n!}{n_1!n_2!...n_t!} \end{aligned} \tag{4.38}$$

Combinaciones con repetición

Ejemplo. Se tienen libros de Computación (C), Física (F), e Historia (H), con al menos 6 copias idénticas (clones) de cada uno. Determine el número de opciones para elegir 6 libros. Solución:

- Hay que elegir, en cualquier orden, 6 libros del conjunto $\{C, F, H\}$ con 3 clases, o **colores**;
- Una selección queda definida indicando el número de libros de cada tipo, para lo cual conviene un esquema con círculos $\circ$ para los libros de cada clase (o de cada color), posiblemente repetidos, y 2 rectángulos $\square$ como **separadores** que separan a las 3 clases de libros, e.g.

Computación (C)		Física (F)		Historia (H)		
$\circ\circ\circ$	$\square$	$\circ\circ$	$\square$	$\circ$	3 de C, 2 de F, 1 de H	(4.39)
	$\square$	$\circ\circ\circ\circ$	$\square$	$\circ\circ$	0 de C, 4 de F, 2 de H	

- Notar que para separar las 3 clases de libros (o colores), hacen falta 2 separadores $\square$, i.e. es el número de clases (o de colores) menos 1;
- Cada ubicación de 6 círculos y 2 separadores $\square$ define una selección, en donde hay 8 símbolos en total (entre círculos y rectángulos);
- Notar que basta definir la ubicación de los 2 separadores, por lo que tendremos $z = C(8, 2) = 28$ formas para elegir 6 libros de C, F e H.

Teorema. "Teorema del pelotero". El número de opciones para elegir una combinación de k elementos posiblemente repetidos (y en cualquier orden) tomados de un conjunto con t clases (o colores, asumidos ditinguibles), está dado por

$$z = \binom{k + (t-1)}{t-1} \tag{4.40}$$

Además

$$\binom{k + (t-1)}{t-1} = \binom{k + (t-1)}{k} \tag{4.41}$$

Demostración:

- Sea el conjunto de las t clases (o colores) asumidos como distinguibles;
- Consideremos k círculos (para los elementos) y $t-1$ separadores (para los colores). En total tenemos $k + (t-1)$ símbolos;
- Cada distribución de estos símbolos define una combinación;
- El número de símbolos hasta encontrar al separador 1, define una selección de elementos de la clase (o color) 1;
- El número de símbolos entre los separadores 1 y 2, define una selección de elementos de la clase (o color) 2; etc.
- Como hay $C(k + (t-1), t-1)$ opciones para elegir las posiciones de los separdores, también habrán $z_1 = C(k + (t-1), t-1)$ selecciones;
- Como hay $C(k + (t-1), k)$ opciones para elegir las posiciones de los círculos, también habrán $z_2 = C(k + (t-1), k)$ selecciones;

i	j	k
0	0	0
1	0	0
1	1	0
1	1	1

Tabla 4.4: Valores de i, j, k en el algoritmo de 3 lazos anidados, con $n = 2$ y $k = 3$.

- Como es la misma tarea se concluye que $z_1 = z_2$.

Ejemplo. Hay 3 pilas de pelotas: Rojas (R), Verde (V), y Amarillas (A). Cada pila tiene al menos 6 pelotas. Determine el número de opciones para:

- Elegir 8 pelotas, sin restricciones;
- Elegir 8 pelotas con al menos una de cada color.

Solución:

- Es una elección de $k = 8$ elementos, posiblemente repetidos, en cualquier orden, por lo que podemos aplicar el "teorema del pelotero", con $t = 3$ clases (los 3 colores de las pelotas), resultando $z = C(8 + (3 - 1), (3 - 1) = C(10, 2) = 45$;
- Primero elegimos 1 pelota de cada color y, para completar, hay que agregar las que falta, i.e. $k = 8 - 3 = 5$ pelotas de cualquier color, i.e. $z = C(5 + (3 - 1), (3 - 1) = C(7, 2) = 21$.

```
1 def cuantas_veces(n):
2     for i in range (n):
3         for j in range (i):
4             for k in range (j):
5                 print (i,j,k)
6             #end k
7         #end j
8     #end i
9     return
```

Ejemplo. Determine el número de veces en que se ejecuta la impresión de la túpla (i, j, k) en el algoritmo dado.
Solución:

- Cada `print` muestra los valores de los enteros (i, j, k), donde $0 \leq i \leq j \leq k \leq (n-1)$;
- Cada sucesión de los tres enteros i, j, k satisface dicha desigualdad. Hay que contar el número de opciones de elegir 3 enteros, permitiendo las respeticiones, tomados del conjunto $\{0, 1, ..., n - 1\}$, por lo que el número de clases (colores) distinguibles es $t = n$, mientras que la cantidad de elementos en cada selección es $k = 3$, es decir, $z = C(k + (t - 1), (t - 1)) = C(n + 2, n - 1)$
- Por ejemplo, si $n = 2$ es $z = C(2 + 2, 2 - 1) = C(4, 1) = 4$ se tienen los valores i, j, k mostrados en la Tabla 4.4.

Ejemplo. Contar el número de soluciones de la ecuación diofántica

$$x_1 + x_2 + x_3 + x_4 = 29 \tag{4.42}$$

sujeta a las siguientes restricciones:

i) Cuando $x_1, x_2, x_3, x_4 \geq 1$. Solución: es equivalente a elegir 29 elementos x_i de tipo i, con $i = 1, 2, 3, 4$. En este caso, el número de clases (colores) es $t = 4$, y el número de elementos en cada selección es $k = 29$ (la suma de k valores uno). Se tiene $z_1 = C(k + (t-1), (t-1) = C(29 + (4-1), (4-1) = C(32, 3) = 4960$

ii) Cuando $x_1 > 0$, $x_2 > 1$, $x_3 > 2$, $x_4 \geq 0$. Solución: es equivalente a elegir 29 elementos con, al menos, 1 elemento del tipo 1, 2 elementos del tipo 2, y 3 elementos del tipo 3. Después hay que completar eligiendo $k = 29 - 1 - 2 - 3 = 23$ elementos adicionales. Escribimos:

$$\begin{gathered}(x_1 - 1) + (x_2 - 2) + (x_3 - 3) + (x_4 - 0) = 29 - 1 - 2 - 3 - 0 \\ y_1 + y_2 + y_3 + y_4 = 23\end{gathered} \tag{4.43}$$

donde $y_1, y_2, y_3, y_4 \geq 0$, y ahora puede aplicarse el teorema del pelotero con los nuevos valores: $z_2 = C(23 + (4-1), (4-1) = C(26, 3) = 2600$

Ejemplo. Contar el número de soluciones de la ecuación diofántica

$$x_1 + x_2 + x_3 + x_4 = 12 \tag{4.44}$$

con $0 \leq x_1 \leq 4$, $0 \leq x_2 \leq 5$, $0 \leq x_3 \leq 8$, $0 \leq x_4 \leq 9$. Solución:

- Introducimos los conjuntos
  - X: conj. de enteros no negativos, sin otras restricciones, es el conjunto universal;
  - A: conj. de enteros $0 \leq x_1 \leq 4$;
  - B: conj. de enteros $0 \leq x_2 \leq 5$;
  - C: conj. de enteros $0 \leq x_3 \leq 8$;
  - D: conj. de enteros $0 \leq x_4 \leq 9$;
- Entonces, el conjunto solución es

$$I = A \cap B \cap C \cap D \tag{4.45}$$

cuya cantidad de elementos $z_I = |I|$ es la respuesta pedida, pero haremos un rodeo para hallarlo, empezando con el conjunto universal

$$U = I \cup \overline{I} \tag{4.46}$$

donde

$$\overline{I} = \overline{A \cap B \cap C \cap D} \tag{4.47}$$

Como I e $\overline{I}$ son conjuntos disjuntos se tiene que

$$|U| = |I| + |\overline{I}| \qquad \therefore \qquad |I| = |U| - |\overline{I}| \tag{4.48}$$

Por otro lado, usando una de las leyes de De Morgan

$$\overline{I} = \overline{A} \cup \overline{B} \cup \overline{C} \cup \overline{D} \tag{4.49}$$

pero

$$\begin{aligned}\overline{A} &= U - A \\ \overline{B} &= U - B \\ \overline{C} &= U - C \\ \overline{D} &= U - D\end{aligned} \tag{4.50}$$

en donde

$$\begin{aligned} &U - A\text{: conjunto con } x_1 \geq 5 \text{ y } x_2, x_3, x_4 \geq 0; \\ &U - B\text{: conjunto con } x_2 \geq 6 \text{ y } x_1, x_3, x_4 \geq 0; \\ &U - C\text{: conjunto con } x_3 \geq 9 \text{ y } x_1, x_2, x_4 \geq 0; \\ &U - D\text{: conjunto con } x_4 \geq 10 \text{ y } x_1, x_2, x_3 \geq 0; \end{aligned} \tag{4.51}$$

por lo que

$$\begin{aligned} |I| &= |U| - |\overline{A} \cup \overline{B} \cup \overline{C} \cup \overline{D}| \\ |I| &= |U| - |(U - A) \cup (U - B) \cup (U - C) \cup (U - D)| \\ z_I &= z_0 - (z_1 + z_2 + z_3 + z_4) \end{aligned} \tag{4.52}$$

donde

$$\begin{aligned} z_0 &= |U|; \\ z_1 &= |U - A|; \\ z_2 &= |U - B|; \\ z_3 &= |U - C|; \\ z_4 &= |U - D|; \end{aligned} \tag{4.53}$$

- Conteo para el conjunto U: la ecuación es

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= 12 \quad \text{con } x_1, x_2, x_3, x_4 \geq 0. \\ z_0 &= \binom{12+3}{3} = \binom{15}{3} = 455 \end{aligned} \tag{4.54}$$

- Conteo para el conjunto $U - A$: la ecuación es

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= 12 \quad \text{con } x_1 \geq 5 \text{ y } x_2, x_3, x_4 \geq 0. \\ (x_1 - 5) + x_2 + x_3 + x_4 &= (12 - 5) \\ y_1 + x_2 + x_3 + x_4 &= 7 \quad \text{con } y_1, x_2, x_3, x_4 \geq 0. \\ z_1 &= \binom{7+3}{3} = \binom{10}{3} = 120 \end{aligned} \tag{4.55}$$

- Conteo para el conjunto $U - B$: la ecuación es

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= 12 \quad \text{con } x_2 \geq 6 \text{ y } x_1, x_3, x_4 \geq 0. \\ x_1 + (x_2 - 6) + x_3 + x_4 &= (12 - 6) \\ x_1 + y_2 + x_3 + x_4 &= 6 \quad \text{con } x_1, y_2, x_3, x_4 \geq 0. \\ z_2 &= \binom{6+3}{3} = \binom{9}{3} = 84 \end{aligned} \tag{4.56}$$

- Conteo para el conjunto $U - C$: la ecuación es

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= 12 \quad \text{con } x_3 \geq 9 \text{ y } x_1, x_2, x_4 \geq 0. \\ x_1 + x_2 + (x_3 - 9) + x_4 &= (12 - 9) \\ x_1 + x_2 + y_3 + x_4 &= 3 \quad \text{con } x_1, x_2, y_3, x_4 \geq 0. \\ z_3 &= \binom{3+3}{3} = \binom{6}{3} = 20 \end{aligned} \tag{4.57}$$

- Conteo para el conjunto $U - D$: la ecuación es

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= 12 \quad \text{con } x_4 \geq 10 \text{ y } x_1, x_2, x_3 \geq 0. \\ x_1 + x_2 + x_3 + (x_4 - 10) &= (12 - 10) \\ x_1 + x_2 + x_3 + y_4 &= 2 \quad \text{con } x_1, x_2, x_3, y_4 \geq 0. \\ z_4 &= \binom{2+3}{3} = \binom{5}{3} = 10 \end{aligned} \tag{4.58}$$

- Juntando resultados parciales

$$\begin{aligned} z_I &= z_0 - (z_1 + z_2 + z_3 + z_4) \\ &= 455 - (120 + 84 + 20 + 10) = 221 \end{aligned} \tag{4.59}$$

Ejemplos usando principios de conteo

Ejemplo. ¿De cuántas maneras puede un fotógrafo de boda ordenar un grupo de 6 (seis) personas si:

a) Los novios deben salir juntos en la foto;
b) Los novios deben salir separados en la foto;
c) La novia debe salir en algún puesto a la izquierda del novio.

Solución.

a) Los ordenamientos posibles se pueden representar con el siguiente esquema:

n_1	n_2	_	_	_	_	fila 1
_	n_1	n_2	_	_	_	fila 2
_	_	n_1	n_2	_	_	fila 3
_	_	_	n_1	n_2	_	fila 4
_	_	_	_	n_1	n_2	fila 5

en donde n_1 denota a la novia y n_2 al novio (se pueden distinguir), y _ es un lugar para las restantes 6-2=4 personas. Cada fila representa una ubicación con los dos novios juntos. En cada fila hay 2! opciones para ubicar a los 2 novios juntos (o bien n_1n_2, o bien n_2n_1), y otras 4! opciones para ubicar a las demás personas, por lo que, usando el PM, se tienen $2! \cdot 4!$ opciones en cada fila. El número total de opciones para dicha foto será la suma de todos estos casos que, por ser sumandos iguales, se reduce al producto del número de opciones en cada fila por el número de filas. Lo que falta es determinar el número de filas posibles sin tener que hacer este esquema. Para ese fin, notar que la fila 1 es una cadena de la forma $n_1n_2x_3...x_6$, donde n_1n_2 son los novios que van juntos, mientras que x_3, ..., x_6 son las restantes $6-2=4$ personas. La fila 2 se puede obtener de la 1 desplazando un lugar hacia la derecha, la fila 3 se puede obtener de la fila 2 desplazando un lugar hacia la derecha, etc. Para llegar hasta el final, hay que hacer $6-2=4$ desplazamientos hacia la derecha. El número total de filas es igual al número total de desplazamientos hacia la derecha más la fila 1, o sea $6-2+1=5$. Finalmente, el número total de opciones para dicha foto es $z = 2! \cdot (6-2)! \cdot (6-2+1)$ y, sacando cuentas, $z = 2! \cdot 4! \cdot 5 = 240$.

b) Para el hogar.
c) Para el hogar.
d) Para el hogar.

Ejemplo. Consigna: elegir una delegación de 4 personas de entre un total de 12 estudiantes para asistir a un congreso. Hallar:

a) De cuántas maneras se puede elegir la delegación? (sin restricciones);

b) Idem pero considerando que hay 2 estudiantes que quieren ir pero se niegan a estar en la delegación simultáneamente;

c) Idem pero considerando que hay 2 estudiantes que asistirán al congreso sólo si van juntos;

d) Idem pero considerando que hay 2 estudiantes que no les preocupa mucho asistir pero, si van, se niegan a estar en la delegación simultáneamente.

Solución:

a) Se tiene $z_a = C(12, 4) = 495$;
b) Sean los estudiantes A y B que quieren ir pero se niegan a estar juntos. Hacemos 2 etapas. Primero incluimos al estudiante A en la delegación y excluimos al estudiante B. Entonces restan elegir 4 - 1 = 3 delegados de un total de 12 - 1 (pues A que ya está) - 1 (pues a B lo echamos), o sea, $z_1 = C(10, 3) = 120$. Ahora incluimos al estudiante B en la delegación y excluimos al estudiante A. Es lo mismo que antes por lo que $z_2 = C(10, 3) = 120$. Finalmente usando el Principio de la Suma (PS), el total de opciones es $z_b = z_1 + z_2 = 2C(10, 3) = 240$.
c) Sean los estudiantes A y B los que solo irán si van juntos. Hacemos 2 etapas. Primero, si incluimos a ambos estudiantes A y B en la delegación, entonces sólo restan elegir a otros 2 delegados de un total de 12-2=10 (porque A y B que ya están), lo que da $z_3 = C(10, 2) = 45$ opciones. Luego excluimos a ambos estudiantes A y B en la delegación, por lo que hay que elegir a 4 delegados de un total de 12-2=10 (porque A y B fueron excluidos), lo que se agregan otras $z_4 = C(10, 4) = 210$ opciones. Finalmente, usando el PS, el total es $z_c = z_3 + z_4 = C(10, 2) + C(10, 4) = 45 + 210 = 255$.
d) Sean los estudiantes A y B que no les preocupa mucho asistir pero, si van, se niegan a estar en la delegación simultáneamente. Una manera de resolver esto es usar el PIE, *i.e.* considerar el total de las combinaciones sin restricciones (inciso-a), es decir, $z_a = C(12, 4) = 495$, y a ese total le restamos el número de delegaciones en las que A y B aparecen juntos, dado por $z_3 = C(10, 2) = 45$ ya hallado. Con todo esto se obtiene $z_d = 495 - 45 = 450$. Verificación: otro razonamiento es sumar el número de opciones cuando A y B quieren ir pero se niegan a estar juntos (inciso-b) con el número de opciones cuando excluimos A y B de la delegación, o sea, $z'_d = z_b + z_4 = 2C(10, 3) + C(10, 4) = 240 + 210 = 450$, y se llega al mismo resultado.

Teorema. [Rosen: ejemplo 16 (pág. 444), y Problema 45 (pág. 448), **re-re-clásico en evaluaciones**]. Conteo en relaciones: ver teorema 7.1 en la Sec. 7.1.

relacioón R	matriz $M(R)$	reflexiva	simétrica	antisimétrica
$R_1 = \emptyset$	$M_1 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$	-	1	1
$R_2 = \{(a,a)\}$	$M_2 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$	-	2	2
$R_3 = \{(a,b)\}$	$M_3 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$	-	-	3
$R_4 = \{(b,a)\}$	$M_4 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$	-	-	4
$R_5 = \{(b,b)\}$	$M_5 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$	-	3	5
$R_6 = \{(a,a),(a,b)\}$	$M_6 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$	-	-	6
$R_7 = \{(a,a),(b,a)\}$	$M_7 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$	-	-	7
$R_8 = \{(a,a),(b,b)\}$	$M_8 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	1	4	8
$R_9 = \{(a,b),(b,a)\}$	$M_9 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	-	5	-
$R_{10} = \{(a,b),(b,b)\}$	$M_{10} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$	-	-	9
$R_{11} = \{(b,a),(b,b)\}$	$M_{11} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$	-	-	10
$R_{12} = \{(a,a),(a,b),(b,a)\}$	$M_{12} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$	-	6	-
$R_{13} = \{(a,a),(a,b),(b,b)\}$	$M_{13} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	2	-	11
$R_{14} = \{(a,a),(b,a),(b,b)\}$	$M_{14} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$	3	-	12
$R_{15} = \{(a,b),(b,a),(b,b)\}$	$M_{15} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$	-	7	-
$R_{16} = \{(a,a),(a,b),(b,a),(b,b)\}$	$M_{16} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$	4	8	-

Tabla 4.5: Todas las relaciones R posibles sobre el conjunto $A = \{a, b\}$ y su clasificación.

Ejemplo. Sea R una relación definida en el conjunto $A = \{a\}$. Aplique las fórmulas de conteo del ejemplo anterior, y obtenga cada relación posible.

Solución.

- El número de relaciones posibles R es $z_1 = 2^{1^2} = 2^1 = 2$, y están dadas por $R_1 = \emptyset$, $R_2 = \{(a,a)\}$;
- El número de relaciones R reflexivas es $z_2 = 2^{(1^2-1)} = 2^{1-1} = 2^0 = 1$;
- El número de relaciones R simétricas es $z_3 = 2^1 \cdot 2^{(1^2-1)/2} = 2 \cdot 2^{0/2} = 2$;
- El número de relaciones R antisimétricas es $z_4 = 2^1 \cdot 3^{(1^2-1)/2} = 2 \cdot 3^{0/2} = 2$.

Ejemplo. Sea R una relación definida en el conjunto $A = \{a, b\}$. Aplique las fórmulas de conteo del ejemplo anterior, y obtenga cada relación posible.

Solución.

- El número de relaciones R que se pueden definir en el conjunto A dado es $z_1 = 2^{2^2} = 2^4 = 16$;
- El número de relaciones R reflexivas que se pueden definir en el conjunto A dado es $z_2 = 2^{(2^2-2)} = 2^{4-2} = 2^2 = 4$;

- El número de relaciones R simétricas que se pueden definir en el conjunto A dado es $z_3 = 2^2 \cdot 2^{(2^2-2)/2} = 4 \cdot 2^{(4-2)/2} = 4 \cdot 2^1 = 8$;
- El número de relaciones R antisimétricas que se pueden definir en el conjunto A dado es $z_4 = 2^2 \cdot 3^{(2^2-2)/2} = 4 \cdot 3^{(4-2)/2} = 4 \cdot 3^1 = 12$.

Finalmente, cada una de la relaciones posibles que se pueden definir en el conjunto $A = \{a, b\}$ se listan en la Tabla 4.5.

CAPÍTULO 5

Probabilidad discreta

Nota. Estas notas siguen el texto de referencia Rosen (2004) manteniendo la numeración de las secciones y sus títulos, como una referencia adicional para el auto-estudio siguiendo ese texto.

Omitir todo el cap.

CAPÍTULO 6

Técnicas avanzadas de recuento

Nota. Estas notas siguen el texto de referencia Rosen (2004) manteniendo la numeración de las secciones y sus títulos, como una referencia adicional para el auto-estudio siguiendo ese texto.

Contents

6.1. Relaciones de recurrencia (RR)

Intro a las RR

Lectura.

Relaciones de recurrencia

Definición. Relación de Recurrencia (RR) y Condiciones Iniciales (CI). Una RR para la sucesión a_0, a_1, ... a_n, ... es una ecuación que relaciona el término genérico con un cierto número de términos predecesores. Para que la RR sea unívoca, se debe especificar las CI dadas por un número finito de términos de la sucesión conocidos expliícitamente.

Observación.

i) A veces el término genérico es a_n, en ese caso sus predecesores son a_{n-1}, a_{n-2}, ..., etc;
ii) Otras veces el término genérico es a_{n+1}, por lo que sus predecesores son a_n, a_{n-1}, ..., etc;

Ejemplo. La RR y las CI para la sucesión de Fibonacci se puede escribir en diversas formas, e.g.:

$$\begin{aligned} f_n &= f_{n-1} + f_{n-2} \quad \text{para } n = 3, 4, ... \\ f_1 &= f_2 = 1 \end{aligned} \tag{6.1}$$

que puede re-escribirse como

$$f_n = \begin{cases} f_{n-1} + f_{n-2} & \text{para } n = 3, 4, ... \\ 1 & \text{para } n = 1 \text{ o } n = 2 \end{cases} \tag{6.2}$$

y que puede resescribirse como

$$\begin{aligned} f_{n+1} &= f_n + f_{n-1} \quad \text{para } n = 2, 3, ... \\ f_1 &= f_2 = 1 \end{aligned} \tag{6.3}$$

Modelos con relaciones de recurrencia

Ejemplo. Sea A_n la cantidad de dinero al final de n años, y suponga una persona que invierte $A_0 = 1000$ al 12 % anual compuesto. Escriba una RR y un algoritmo para obtener la cantidad de dinero al cabo de n años. Solución.

- Sea $t = 12/100$ la tasa tanto por 1. Tenemos

$$\begin{aligned} &A_n = A_{n-1} + tA_{n-1} = (1 + t)A_{n-1} = pA_{n-1} \\ &A_n = pA_{n-1} \quad \text{con todo entero } n \geq 1 \text{ y } A_0 = 1000 \end{aligned} \tag{6.4}$$

- Resolviendo por iteración:

$$\begin{aligned} &A_n = pA_{n-1} = p(pA_{n-2}) = p^2A_{n-2} = ... = p^nA_0 \\ &A_n = p^nA_0 \end{aligned} \tag{6.5}$$

Ejemplo. Hallar una RR y las CI para el número de subconjuntos de un conjunto de n elementos. Solución: sea S_n el número de subconjuntos de un conjunto de n elementos. Como al pasar de un conjunto de $(n - 1)$ elementos a otro conjunto de n elementos se duplica el número de subconjuntos disponibles (pues $|\mathbb{P}(\mathbb{X})| = 2^n$, con $n = |X|$), obtenemos la RR

$$S_n = 2S_{n-1} \quad \text{con } n \geq 1 \text{ y } S_0 = 1 \tag{6.6}$$

Ejemplo. Hallar una RR y las CI para el número on de cadenas de n bits que no contienen la subcadena 111. Solución: sea S_n el número de cadenas de n bits que no contienen la subcadena 111. La cadena de n bits que no contiene la subcadena 111 puede provenir de las subcadenas:

- Con $(n - 1)$ bits tales que terminan en 0, 1;
- Con $(n - 2)$ bits tales que terminan en 00, 01, 10;
- Con $(n - 3)$ bits tales que terminan en 000, 001, 010, 100, 101, 110;

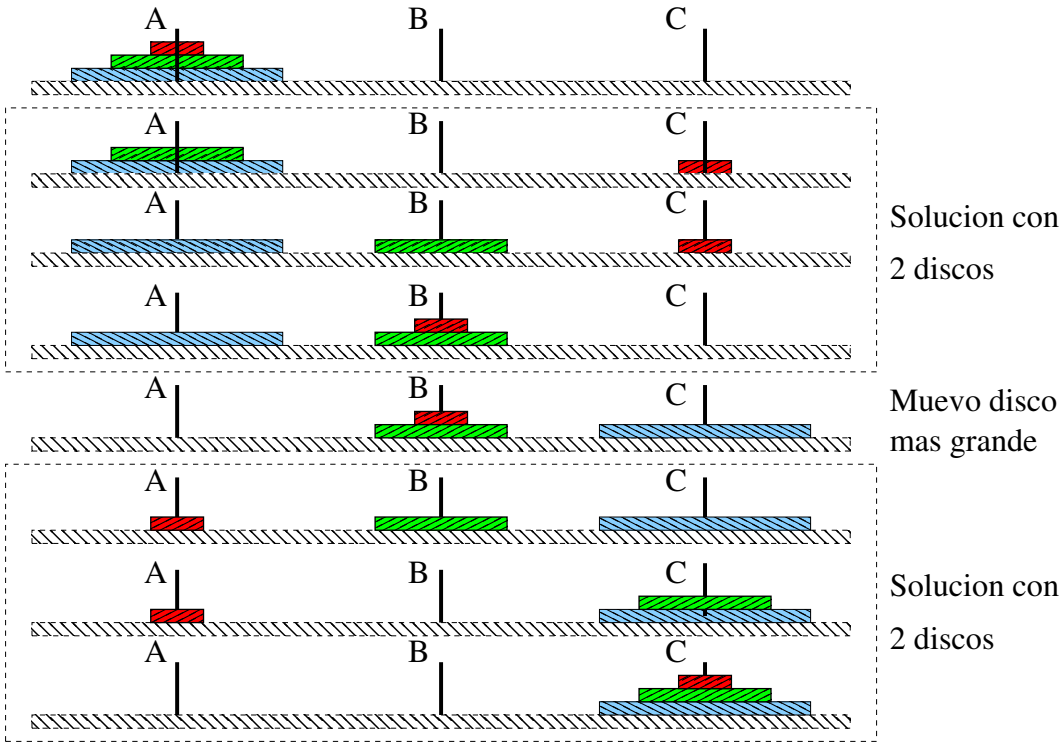

Figura 6.1: Movimientos en el juego de las TH con $n = 3$ discos.

- Usando el PS obtenemos la RR y las CI dadas por

$$\begin{aligned} S_n &= S_{n-1} + S_{n-2} + S_{n-3} \quad \text{con } n \geq 4 \\ S_1 &= 2 \quad \text{son 0 y 1} \\ S_2 &= 3 \quad \text{son 00, 01, 10} \\ S_3 &= 5 \quad \text{son 000, 001, 010, 100, 101} \end{aligned} \tag{6.7}$$

Ejemplo. Torres de Hanoi. Encontrar la RR y la CI para el número de movimientos H_n que resuelve el problema del juego de las Torres de Hanoi (TH) con n discos, con al menos un disco. Solución:

- Consigna: mover los discos, de a uno por vez, desde la estaca A hacia la C, pero nunca colocando un disco más grande sobre otro más pequeño, usando la estaca B como auxiliar;
- Por ejemplo, en la Fig. 6.1 se muestran los movimientos para resolver este juego con $n = 3$ discos;
- Si hay un disco ($n = 1$), el juego se resuelve con un movimiento, por lo que $c_1 = 1$;
- Si hay más de un disco, $n > 1$, el juego se divide en 3 etapas: (i) se pasan $n - 1$ discos de la estaca A hacia la auxiliar B, lo cual involucra H_{n-1} movimientos; (ii) luego se mueve el disco más grande de manera explíta a la estaca C (con un movimiento); y (iii) se vuelven a pasar los $n - 1$ discos de la estaca auxiliar B hacia la C, lo cual involucra otros H_{n-1} movimientos. Sumando, se tiene la RR y la condición inicial

$$\begin{aligned} H_n &= 2H_{n-1} + 1 \quad \text{con } n \geq 2 \\ H_1 &= 1 \end{aligned} \tag{6.8}$$

6.2. Resolución de las RR

Intro

Ejemplo. Resolver la RR dada por $a_n = a_{n-1} + 3$, para todo entero $n \geq 2$, con la CI dada por $a_1 = 2$. Solución:

$$\begin{aligned} a_n &= a_{n-1} + 3 \quad \text{con } n \geq 2 \\ a_{n-1} &= a_{n-2} + 3 \\ a_n &= (a_{n-1}) + 3 = ((a_{n-2} + 3) + 3) = (a_{n-3} + 3) + 3 + 3 = a_{n-4} + (3 + 3 + 3 + 3) \end{aligned} \tag{6.9}$$

Para hallar k hacemos

$$\begin{aligned} n - k = 1 \quad &\therefore \quad k = n - 1 \\ a_n &= a_1 + 3(n-1) \\ a_n &= 2 + 3(n-1) \quad \text{con } n \geq 1 \end{aligned} \tag{6.10}$$

Resolución de RRL de CC homogéneas

Definición. Una Relación de Recurrencia Homogénea, Lineal, de Coeficientes Constantes (RRHLCC), de orden k, es una relación de recurrencia de la forma

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + ... + c_k a_{n-k} \quad \text{con, al menos, } c_k \neq 0 \tag{6.11}$$

en donde la unicidad se logra definiendo k condiciones iniciales

$$a_0 = c_0 \quad a_1 = c_1 \quad ... \quad a_k = c_k \tag{6.12}$$

Ejemplo. Clasificar cada una de las siguientes RR.

- $s_n = 2s_{n-1}$: es una RRHLCC, de orden 1;
- $f_n = f_{n-1} + f_{n-2}$ (Fibonacci): es una RRHLCC, de orden 2;
- $a_n = 3a_{n-1}a_{n-2}$: es una RRH no-lineal, de CC, de orden 2;
- $a_n - a_{n-1} = 2n$: es una RR lineal, no-homogénea, de CC, y de orden 1;
- $a_n = 3na_{n-1}$: es una RR lineal, homogénea, y de coeficientes no-constantes.

Ejemplo. Procedimiento básico para resolver una RRHLCC. Resolver la RRHLCC dada por $a_n = 5a_{n-1} - 6a_{n-2}$, para todo entero $n \geq 2$, con las CI particulares $a_0 = 7$ y $a_1 = 16$. Solución: Sea $a_n = r^n$, donde r se asume como una constante real. Reemplazando

$$\begin{aligned} r^n &= 5r^{n-1} - 6r^{n-2} \\ r^n - 5r^{n-1} + 6r^{n-2} &= 0 \\ r^{n-2}(r^2 - 5r + 6) &= 0 \quad \text{si } r^{n-2} \neq 0, \text{ debe ser } (r^2 - 5r + 6) = 0 \\ \therefore \quad r_{1,2} = \frac{5 \pm \sqrt{25 - 24}}{2} \quad &\therefore \quad r_1 = 2 \quad , \quad r_2 = 3 \end{aligned} \tag{6.13}$$

entonces hay 2 soluciones linealmente independientes $S_n = r_1^n$ y $T_n = r_2^n$, por lo que la solución general es una combinación lineal de ambas soluciones

$$\begin{aligned} a_n &= \alpha S_n + \beta T_n \\ &= \alpha r_1^n + \beta r_2^n \\ &= \alpha 2^n + \beta 3^n \end{aligned} \tag{6.14}$$

donde α y β son constantes a determinar a partir de las condiciones iniciales

$$\begin{aligned} a_0 &= \alpha 2^0 + \beta 3^0 = 7 \\ a_1 &= \alpha 2^1 + \beta 3^1 = 16 \end{aligned} \tag{6.15}$$

con lo que se tiene un sistema lineal de dos ecuaciones para las incógnitas α y β

$$\begin{aligned} \alpha + \beta &= 7 \\ 2\alpha + 3\beta &= 16 \end{aligned} \tag{6.16}$$

cuya solución da $\alpha = 5$ y $\beta = 2$. Finalmente, la solución particular es $a_n = 5 \cdot 2^n + 2 \cdot 3^n$ para $n = 0, 1, 2, ...$

Teorema. Sea $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ una RRHL de segundo orden. Se cumple que:

- Si S y T son soluciones, entonces $U = \alpha S + \beta T$ también es solución;
- Si r es una raíz de $t^2 - c_1 t - c_2 = 0$, entonces r^n es solución, para $n = 0, 1$;
- Si $\{a_n\}$ es la sucesión $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ tal que $a_0 = c_0$, $a_1 = c_1$, y si r_1, r_2 son raíces reales y distintas, i.e. $r_1 \neq r_2$, entonces existen constantes α y β tales que $a_n = \alpha r_1^n + \beta r_2^n$, para $n = 0, 1, ...$;

Demostración:

- Como S y T son soluciones de la RR, debe ser

$$\begin{aligned} S_n = c_1 S_{n-1} + c_2 S_{n-2} \quad &\therefore \quad \alpha S_n = \alpha(c_1 S_{n-1} + c_2 S_{n-2}) \\ T_n = c_1 T_{n-1} + c_2 T_{n-2} \quad &\therefore \quad \beta T_n = \beta(c_1 T_{n-1} + c_2 T_{n-2}) \end{aligned} \tag{6.17}$$

  sumando ambas ecuaciones

$$\begin{aligned} U_n &= \alpha S_n + \beta T_n \\ &= c_1(\alpha S_{n-1} + \beta T_{n-1}) + c_2(\alpha S_{n-2} + \beta T_{n-2}) \\ &= c_1 U_{n-1} + c_2 U_{n-2} \end{aligned} \tag{6.18}$$

  por lo que U también es una solución.
- Si r es una raíz de la EC dada por $t^2 - c_1 t - c_2 = 0$, entonces se cumple $r^2 = c_1 t + c_2$, y hacemos

$$c_1 r^{n-1} + c_2 r^{n-2} = r^{n-2}(c_1 r + c_2) = r^{n-2} r^2 = r^n \tag{6.19}$$

  por lo que la sucesión r^n, con $n = 0, 1, ...$, verifica la EC;
- Sea $U_n = \alpha r_1^n + \beta r_2^n$, entonces U es solución y para cumplir con las CI dadas, planteamos

$$\begin{aligned} U_0 &= \alpha r_1^0 + \beta r_2^0 = C_0 \\ U_1 &= \alpha r_1^1 + \beta r_2^1 = C_1 \end{aligned} \tag{6.20}$$

es decir,

$$\begin{aligned} \alpha + \beta &= C_0 \\ \alpha r_1 + \beta r_2 &= C_1 \end{aligned} \tag{6.21}$$

Para igualar el primer término de ambas ecuaciones hacemos

$$\begin{aligned} r_1\alpha + r_1\beta &= r_1 C_0 \\ r_1\alpha + r_2\beta &= C_1 \end{aligned} \tag{6.22}$$

restando lado a lado se obtiene $(r_1 - r_2)\beta = r_1 C_0 - C_1$, y sólo cuando $r_1 \neq r_2$ se puede obtener $\beta = (r_1 C_0 - C_1)/(r_1 - r_2)$, y luego $\alpha = C_0 - \beta$.

Teorema. Sea $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ una RRHL de segundo orden. Si $\{a_n\}$ es la sucesión $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ tal que $a_0 = c_0$, $a_1 = c_1$, y si ambas raíces de $r^2 - c_1 r - c_2 = 0$ son iguales a r_0, entonces existen constantes α y β tales que $a_n = \alpha r_0^n + \beta n r_0^n$, con $n = 0, 1, ...$;
Demostración:

- El teorema anterior prueba que la sucesión r_0^n, para $n = 1, 2, ...$, es solución de la RR;
- Por lo que resta demostrar que la sucesión nr_0^n, para $n = 1, 2, ...$, también es una solución de la RR.
- Como r_0 es la única solución real de la EC, se tiene

$$r^2 - c_1 r - c_2 = (r - r_0)(r - r_0) = (r - r_0)^2 \tag{6.23}$$

Las raíces x_1 y x_2 de la ecuación cuadrática general $ax^2 + bx + c = 0$ verifican las propiedades $x_1 + x_2 = -b/a$ y $x_1 \cdot x_2 = c/a$. Dichas propiedades en este caso se re-expresan como $c_1 = 2r_0$ y $c_2 = -r_0^2$, por lo que

$$\begin{aligned} a_n &= c_1 a_{n-1} + c_2 a_{n-2} \\ &= c_1(n-1)r_0^{n-1} + c_2(n-2)r_0^{n-2} \\ &= 2r_0(n-1)r_0^{n-1} - r_0^2(n-2)r_0^{n-2} \\ &= r_0^n[2(n-1) - (n-2)] \\ &= nr_0^n \end{aligned} \tag{6.24}$$

entonces la sucesión nr_0^n es solución.

Ejemplo. Resolver $a_n = 4a_{n-1} - 4a_{n-2}$ para todo entero $n \geq 2$, con $a_0 = 1$ y $a_1 = 1$.
Solución: Sea $a_n = r^n$, donde r se asume como una constante real no nula. Reemplazando

$$\begin{aligned} r^n - 4r^{n-1} + 4r^{n-2} &= 0 \\ r^{n-2}(r^2 - 4r + 4) &= 0 \quad \text{si } r^{n-2} \neq 0, \text{ debe ser } (r^2 - 4r + 4) = 0 \\ \therefore \quad r_{1,2} &= \frac{4 \pm \sqrt{16 - 16}}{2} \qquad \therefore \quad r_1 = r_2 = r_0 = 2 \end{aligned} \tag{6.25}$$

entonces las 2 soluciones linealmente independientes son $S_n = r_0^n$ y $T_n = n \cdot r_0^n$, por lo que la solución general es una combinación lineal de ambas soluciones de la forma:

$$\begin{aligned} a_n &= \alpha S_n + \beta T_n \\ &= \alpha r_0^n + \beta n r_0^n \\ &= \alpha 2^n + \beta n 2^n \end{aligned} \tag{6.26}$$

donde α y β son constantes a determinar a partir de las condiciones iniciales

$$\begin{aligned} a_0 &= \alpha 2^0 + \beta \cdot 0 \cdot 2^0 = 1 \\ a_1 &= \alpha 2^1 + \beta \cdot 1 \cdot 3^1 = 1 \end{aligned} \tag{6.27}$$

con lo que se tiene un sistema lineal de dos ecuaciones para las constantes α y β

$$\begin{aligned} \alpha &= 1 \\ 2\alpha + 2\beta &= 1 \end{aligned} \tag{6.28}$$

cuya solución da $\alpha = 1$ y $\beta = -1/2$. Finalmente, la solución particular es $a_n = 2^n - \frac{1}{2}n2^n$ para $n = 0, 1, 2, ...$

Resolución de RRL de CC no-homogéneas

Ejemplo. Resolver la RR que resuelve el número mínimo de movimientos para resolver el juego de las TH, dada por $H_n = 2H_{n-1} + 1$, para todo entero $n \geq 2$, con la CI para un disco $H_1 = 1$. Solución: por iteración (en donde el último valor de k está dado cuando $n - k = 1$, por lo que $k = n - 1$)

$$\begin{aligned} H_n &= 2H_{n-1} + 1 \quad \text{con } n \geq 2 \\ &= 2(2H_{n-2} + 1) + 1 \\ &= 2^2(H_{n-2}) + 2 + 1 \\ &= 2^2(2H_{n-3} + 1) + 2 + 1 \\ &= 2^3 H_{n-3} + 2^2 + 2^1 + 2^0 \\ &= 2^3(2H_{n-4} + 1) + 2^2 + 2^1 + 2^0 \\ &= 2^4 H_{n-4} + 2^3 + 2^2 + 2^1 + 2^0 = ... \\ &= 2^k(2H_{n-k} + 1) + 2^{k-1} + ... + 2^1 + 2^0 \\ &= 2^{n-1} H_1 + 2^{n-2} + ... + 2^1 + 2^0 = ... \\ &= 2^{n-1} + 2^{n-2} + ... + 2^1 + 2^0 \end{aligned} \tag{6.29}$$

que es una forma particular de la serie geométrica

$$a + ar + ar^2 + ... + ar^m = \frac{a(r^{m+1} - 1)}{r - 1} \quad \text{con } r \neq 1 \tag{6.30}$$

cuando $r = 2$, $a = 1$, y $m = n - 1$, resulta

$$1 + 2 + 4 + 8 + ... + 2^{n-1} = \frac{1 \cdot (2^n - 1)}{2 - 1} \tag{6.31}$$

por lo que la solución no-recursiva es

$$H_n = 2^n - 1 \tag{6.32}$$

6.3. Algoritmos de divide y vencerás

Omitir (la gente de FICH lo verá en AED).

6.4. Funciones generatrices

Omitir.

6.5. Principio de inclusión-exclusión (PIE)

Ya visto en el Cap. Conjuntos.

6.6. Aplicaciones del PIE

Ver GTP y el Cap. Conjuntos.

CAPÍTULO 7

Relaciones

Nota. Estas notas siguen el texto de referencia Rosen (2004) manteniendo la numeración de las secciones y sus títulos, como una referencia adicional para el auto-estudio siguiendo ese texto.

Contents

7.1. Relaciones y sus propiedades

Intro

Definición. Sean dos conjuntos A y B. *Relación Binaria* (RB): una relación binaria R de A en B es un subconjunto del producto cartesiano $A \times B$. **Notación**: $R = \{(a, b) \mid (a, b) \in A \times B\}$, donde $a \in A$ y $b \in B$. Se denota aRb cuando $(a, b) \in R$, y se dice que el elemento a está relacionado con el elemento b mediante R. En caso contrario, se denota con $a \not R b$ cuando $(a, b) \notin R$.

Funciones como relaciones

Observación. Una función $f : A \to B$ es un caso especial de una RB, en donde R asigna exactamente **un** elemento $b \in B$ a **cada** elemento $a \in A$.

Relación en un conjunto

Definición. *Relación* (def.): una relación en un conjunto A es una RB de A en A, i.e. $R = \{(a, b) \mid (a, b) \in A \times A\}$, donde $a, b \in A$.

Relación reflexiva, simétrica, antisimétrica, e inversa

Definición. Relación reflexiva (def.): una relación R en un conjunto A es reflexiva si todos los pares ordenados de la forma (a, a) pertenecen a la relación R. **Notación**: una relación R en un conjunto A es reflexiva si $(a, a) \in R$, para todo $a \in A$.

Ejemplo. Como $n|n$ para cada entero positivo n, se concluye que la relación "divide a" en el conjunto de los enteros positivos es reflexiva.

Definición. Relación simétrica (def.): una relación R en un conjunto A es simétrica si $(a, b) \in R$, entonces $(b, a) \in R$, para todo $a, b \in A$. **Notación**: una relación R en un conjunto A es simétrica si $(a, b) \in R \rightarrow (b, a) \in R$, para todo $a, b \in A$. **Observación**: en una relación simétrica no importan la presencia o ausencia de los pares con elementos iguales (a, a).

Definición. Relación antisimétrica (def. 1): una relación R en un conjunto A es antisimétrica si $(a, b) \in R \wedge a \neq b$, entonces $(b, a) \notin R$, para todos $a, b \in A$. **Relación antisimétrica** (def. 2): una relación R en un conjunto A es antisimétrica si $(a, b) \in R \wedge (b, a) \in R$, entonces $a = b$, para todo $a, b \in A$. **Observación**: en una relación antisimétrica no importan la presencia o ausencia de los pares con elementos iguales (a, a). **Notación**: una relación R en un conjunto A es antisimétrica si $((a, b) \in R \wedge (b, a) \in R) \rightarrow a = b$, para todo $a, b, c \in A$.

Ejemplo. Como $n|n$ para cada entero positivo n, se concluye que la relación "x divide a y" es reflexiva cuando x, y pertenecen al conjunto de los enteros positivos.

Observación.

a) Los términos simétrico y antisimétrico no son opuestos entre si. Una relación R en un conjunto A puede tener simultáneamente ambas propiedades (poco frecuente), o carecer de ambas (bastante más frecuente);
b) Si una relación R en un conjunto A contiene algún par ordenado (a, b) tal que $a \neq b$, entonces no puede se simétrica y antisimétrica a la vez.

Ejemplo. Analizar las siguientes relaciones R en el conjunto $A = \{a, b, c\}$ dadas por la Ec. (7.1):

$$\begin{aligned}
R_1 &= \{(a,a),(b,b),(c,c)\} : \text{es reflexiva, es simétrica, y es antisimétrica;} \\
R_2 &= \{(a,a),(b,b)\} : \text{no es reflexiva, es simétrica, y es antisimétrica;} \\
R_3 &= \{(a,a),(a,b)\} : \text{no es reflexiva, no es simétrica, y es antisimétrica;} \\
R_4 &= \{(a,a),(a,b),(b,a)\} : \text{no es reflexiva, es simétrica, pero no es antisimétrica.}
\end{aligned} \tag{7.1}$$

Teorema. Conteo en Relaciones . [Rosen: ejemplo 16 (pág. 444), y Problema 45 (pág. 448), **re-re-clásico en evaluaciones**]. Sea R una relación en un conjunto finito A de n elementos. Utilice un argumento de conteo para demostrar que el número máximo de:

- relaciones $z_1 = 2^{n^2}$;

- relaciones reflexivas $z_2 = 2^{(n^2-n)}$;
- relaciones simétricas $z_3 = 2^n \cdot 2^{(n^2-n)/2}$;
- relaciones antisimétricas $z_4 = 2^n \cdot 3^{(n^2-n)/2}$.

Demostración:

- La base 2 surge porque cada par ordenado (x, y) del producto cartesiano $A \times A$ tiene 2 posibilidades en una relación dada, o bien estar, o bien no estar. Como hay $n \cdot n$ pares ordenados en el producto cartesiano $A \times A$, se concluye que hay 2^{n^2} opciones;
- En una relación R en un conjunto A de n elementos, los pares ordenados que tienen componentes iguales (de la forma (x, x)) son n, y los restantes serán $(n^2 - n)$. Al formar todas las relaciones reflexivas posibles, esos pares remanentes pueden o no estar y por eso hay $2^{(n^2-n)}$ opciones;
- En una relación R en un conjunto A de n elementos, los pares ordenados que tienen componentes iguales (de la forma (x, x)) son n, estos pueden (o no) estar en una relación simétrica, por lo que tenemos un factor 2^n. Los restantes pares ordenados que se pueden formar de $A \times A$ son $(n^2 - n)$. Al contar todas las relaciones simétricas posibles, si un par ordenado $(x, y) \in R$, con $x \neq y$, entonces también hay que incluir al par simétrico (y, x). Luego, sólo disponemos de la mitad de los pares iniciales, i.e. $(n^2 - n)/2$, los cuales pueden (o no) estar. En total tenemos $2^n \cdot 2^{(n^2-n)/2}$ opciones;
- Por empezar, podemos (o no) incluir los pares con elementos iguales (x, x)en una relación antisimétrica, por lo que tenemos un factor 2^n. En los restantes pares ordenados (x, y), con $x \neq y$, hay 3 opciones: o bien colocar (x, y) sólo, o bien colocar (y, x) sólo, o bien no colocar (x, y) ni (y, x). En total tenemos $2^n \cdot 3^{(n^2-n)/2}$ opciones.

Ejemplo. Contrapositiva de la definición de relación antisimétrica. Escriba la contrapositiva de: una relación R en un conjunto A es antisimétrica si $(a, b) \in R \wedge (b, a) \in R$, entonces $a = b$, para todo $a, b \in A$.

Solución: una relación R en un conjunto A es antisimétrica si $a \neq b$, entonces $(a, b) \notin R \vee (b, a) \notin R$, para todo $a, b \in A$.

Definición. Relación inversa. Sea una relación R de un conjunto A en otro B. La relación inversa se denota con R^{-1} y es la relación de B en A definida por $R^{-1} = \{(b, a) \mid (a, b) \in R\}$, con $a \in A$ y $b \in B$.

Ejemplo. Sean los conjuntos $A = \{2, 3, 4\}$ y $B = \{3, 4, 5, 6, 7\}$, y las relaciones:

a) $R = \{(a, b) \mid$ si a divide a $b\}$. En este caso queda $R =$ { (2,4), (2,6), (3,3), (3,6), (4,4) }.
b) $R^{-1} = \{(b, a) \mid$ si b es divisible por $a\}$. Ahora $R^{-1} =$ { (4,2), (6,2), (3,3), (6,3), (4,4) }.

Relación transitiva

Definición. Relación transitiva: una relación R en un conjunto A es transitiva, si $(a, b) \in R$ y $(b, c) \in R$, entonces se tiene también $(a, c) \in R$, para todo $a, b, c \in A$. **Notación**: una relación R en un conjunto A es transitiva si $((a, b) \in R \wedge (b, c) \in R) \rightarrow (a, c) \in R$, para todo $a, b, c \in A$.

Ejemplo. Sea la relación $R = \{(a, b) \mid a \text{ divide a } b \text{ para todo } a, b \in \mathbb{Z}$. Se tiene:

i) Si a divide a b, usando la definición de divide se tiene: como aRb, entonces $b = \alpha a$, con $\alpha \in \mathbb{Z}$;
ii) Si b divide a c, usando la definición de divide se tiene: como bRc, entonces $c = \beta b$, con $\beta \in \mathbb{Z}$;
iii) Reemplazando $c = \beta b = \beta\alpha a = \gamma a$, o sea, $c = \gamma a$, es decir, c divide a a, donde $\gamma = \alpha\beta$, con $\gamma \in \mathbb{Z}$;
iv) Eso ocurre para todo aRb y bRc, por lo que la relación "a divide a b" es transitiva en $\mathbb{Z}$.

Ejemplo. Sean R y S relaciones en un conjunto A. Demuestre o dé un contraejemplo en cada caso:

1) Si R y S son transitivas, entonces ¿es $R \cup S$ transitiva? Rpta: es F, contraejemplo: sea el conjunto $A = \{1, 2, 3\}$, y las relaciones transitivas $R = \{(1, 2)\}$ y $S = \{(2, 3)\}$. Se tiene $R \cup S = \{(1, 2), (2, 3)\}$ que no es transitiva.
2) Si R y S son transitivas, entonces ¿es $R \cap S$ transitiva?
3) Si R y S son transitivas, entonces ¿es $R \circ S$ transitiva?
4) Si R es transitiva, entonces ¿es R^{-1} transitiva? Solución. Para todo $a, b, c \in A$ se tiene:
   - Si $aR^{-1}b$ y $bR^{-1}c$, entonces, por definición de R^{-1}, debe ser bRa y cRb, o sea, cRb y bRa;
   - Como R es transitiva, debe ser cRa;
   - Por definición de relación inversa, debe ser $aR^{-1}c$;
   - Se concluye que toda vez que $aR^{-1}b$ y $bR^{-1}c$, debe ser $aR^{-1}c$, por lo que R^{-1} también es transitiva.
5) Si R es reflexiva, entonces ¿es R^{-1} reflexiva? Rpta. Para todo $a \in A$ se tiene:
   - Si R es reflexiva, entonces aRa para todo $a \in A$. Por definición de R^{-1}, debe ser $aR^{-1}a$ para todo $a \in A$, por lo que $R \subseteq R^{-1}$;
   - Si R^{-1} es reflexiva, entonces $aR^{-1}a$ para todo $a \in A$. Por definición de R^{-1}, debe ser aRa para todo $a \in A$, por lo que $R^{-1} \subseteq R$. Por eso, $R = R^{-1}$;
   - Por último, si R es reflexiva, entonces aRa para todo $a \in A$. Y como $R = R^{-1}$, debe ser $aR^{-1}a$ para todo $a \in A$.
6) Si R y S son reflexivas, entonces ¿es $R \cup S$ reflexiva? Rpta. Para todo $a, b \in A$ se tiene:
   - Si $R \cup S$ es reflexiva, entonces $(a, a) \in (R \cup S)$ para todo $a \in A$;
   - Por definición de la unión se tiene $(a, a) \in R \vee (a, a) \in S$ para todo $a \in A$;
   - Como R y S son reflexivas, cada una es T;
7) Si R y S son reflexivas, entonces ¿es $R \cap S$ reflexiva? Rpta. Para todo $a, b \in A$ se tiene:
   - Si $R \cap S$ es reflexiva, entonces $(a, a) \in (R \cap S)$ para todo $a \in A$;
   - Por definición de la intersección se tiene $(a, a) \in R \wedge (a, a) \in S$ para todo $a \in A$;
   - Y como R y S son reflexivas, cada una es T;
8) Si R y S son reflexivas, entonces ¿es $R \circ S$ reflexiva? Rpta. Para todo $a \in A$ se tiene:

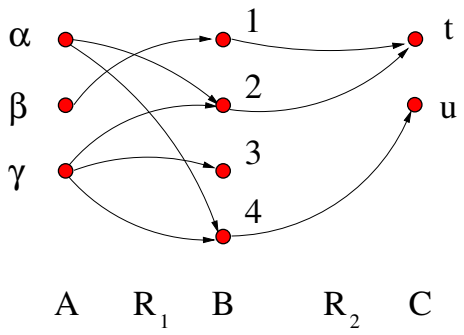

Figura 7.1: Diagramas de flechas de las relaciones R_1, R_2, y de la composición $R_2 \circ R_1$.

- Como R es reflexiva, entonces $(a, a) \in R$ para todo $a \in A$;
- Como S es reflexiva, entonces $(a, a) \in S$ para todo $a \in A$;
- En esas condiciones, $R \circ S$ se reduce a $\{(a, a) \mid \forall a \in A$, por lo que $R \circ S$ también es reflexiva.

Composición de relaciones

Definición. Composición de dos relaciones. Sean los conjuntos A, B, y C, y sean las relaciones R_1, de A hacia B, y R_2, de B hacia C. La composición de R_1 y R_2 se denota con $R_2 \circ R_1$, y es la relación de A hacia C definida con $R_2 \circ R_1 = \{(a, c) \mid (a, b) \in R_1 \wedge (b, c) \in R_2\}$, con $a \in A$, $b \in B$, y $c \in C$.

Ejemplo. Sean los conjuntos $A = \{\alpha, \beta, \gamma\}$, $B = \{1, 2, 3, 4\}$, y $C = \{t, u\}$, y las relaciones: $R_1 = \{(\alpha, 2), (\alpha, 4), (\beta, 1), (\gamma, 2), (\gamma, 3), (\gamma, 4)\}$, $R_2 = \{(1, t), (2, t), (4, u)\}$. En este caso, resulta la composición $R_2 \circ R_1 = \{(\alpha, t), (\alpha, u), (\beta, t), (\gamma, t), \gamma, u)\}$, ver Fig. 7.1.

7.2. Relaciones n-arias y sus aplicaciones

Omitir.

7.3. Representación de relaciones

Representación de relaciones usando matrices

Definición. *Matriz de una relación binaria*. Sean los conjuntos finitos A y B, donde $m = |A|$ y $n = |B|$. La matriz de una relación binaria R de A en B es la matriz de bits $\boldsymbol{M}(R)$ de $m \times n$ definida por la Ec. (7.2).

$$[\boldsymbol{M}]_{i,j} = \begin{cases} 1 & \text{si } (a_i, b_j) \in R; \\ 0 & \text{si } (a_i, b_j) \notin R; \end{cases} \tag{7.2}$$

para $i = 1, 2, ..., m$, y $j = 1, 2, ..., n$.

Observación.

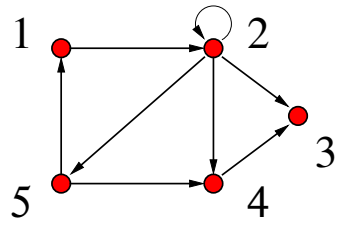

Figura 7.2: Diagrafo asociado a la relación R del ejemplo 7.3.

- Las filas de $\boldsymbol{M}$ se corresponden con los elementos del conjunto A en algún orden arbitrario pero fijo;
- Las columnas de $\boldsymbol{M}$ se corresponden con los elementos del conjunto B en algún orden arbitrario pero fijo;
- En general la matriz $\boldsymbol{M}$ de una relación binaria es rectangular excepto en una relación R definida sobre un conjunto A.

Ejemplo. Sea los conjuntos $A = \{\beta, \gamma, \delta\}$ y $B = \{a, b, c, d\}$, y la relación binaria $R = \{(\beta, b), (\beta, d), (\gamma, b), (\gamma, d)\}$, entonces la matriz de la relación binaria está dada por la Ec. (7.3).

$$\boldsymbol{M} = \begin{array}{c} \\ \beta \\ \gamma \\ \delta \end{array} \begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{array} \tag{7.3}$$

Definición. *Matriz de una relación en un conjunto* (def.). Sea una relación R en un conjunto finito A de n elementos. La matriz de la relación R es la matriz de bits $\boldsymbol{M}$, cuadrada de $n \times n$, dada por la Ec. (7.4).

$$[\boldsymbol{M}]_{i,j} = \begin{cases} 1 & \text{si } (a_i, a_j) \in R; \\ 0 & \text{en caso contrario;} \end{cases} \tag{7.4}$$

donde $i, j = 1, 2, ..., n$, y los elementos $a_i, a_j \in A$.

Repres. de relaciones usando digrafos

Nota: preferimos emplear “digrafo” en lugar de “grafo dirigido”.

Definición. Digrafo asociado a una relación finita. Sea R una relación en un conjunto finito A. El digrafo G asociado con la relación R se traza de la siguiente manera: (i) se representa cada elemento a de A con un vértice (o punto); (ii) para cada par ordenado $(a, b) \in R$ se traza una flecha (lado o arco orientado) desde el vértice a hacia el b, con $a, b \in A$.

Definición. Trayectoria. Sea R una relación en un conjunto A. Una trayectoria (o camino, o ruta) de longitud n en R desde el elemento a hacia el b es una sucesión finita P :

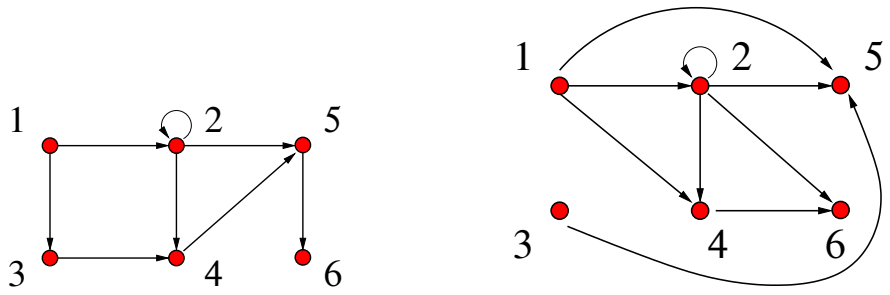

Figura 7.3: Digrafos asociados a las relaciones R y R^2 del ejemplo 7.3.

$a, x_1, x_2, ..., x_{n-1}, b$ que empieza en a, termina en b, y tal que $aRx_1 \wedge x_1Rx_2... \wedge x_{n-1}Rb$.
Ciclo: es una trayectoria que empieza y termina en un mismo vértice.

Observación. Una ruta de longitud n involucra $(n + 1)$ elementos de A aunque no necesariamente distintos.

Ejemplo. Sea el conjunto $A = \{1, 2, 3, 4, 5\}$, y la relación $R = \{(1, 2), (2, 2), (2, 3), (2, 4), (4, 3), (5, 1), (5, 4)\}$, ver Fig. 7.2. Tres trayectorias cualesquiera en R son: P_1: 1, 2, 5, 4, 3, P_2: 1, 2, 5, 1, y P_3: 2,2, donde $|P_1| = 4$, $|P_2| = 3$, y $|P_3| = 1$.

Observación. Las trayectorias de longitud 1 están asociadas con los pares ordenados $(a, b) \in R$. Las trayectorias en una relación R permiten definir nuevas relaciones a partir de R.

Definición. Relación R^n sobre un conjunto finito A. La relación R^n, con entero positivo n está formada con los pares ordenados $(a, b) \in R^n$, en donde aR^nb indica que existe una trayectoria de longitud n entre los elementos a y b pertenecientes al conjunto A.

Para obtener R^n puede ser más cómodo hacerlo a través de la matriz $\boldsymbol{M}(R^n)$ asociada, la cual se obtiene mediante la potencia n de la matriz $\boldsymbol{M}(R)$ dada por

$$\boldsymbol{M}(R^n) = \underbrace{\boldsymbol{M}(R) \odot \boldsymbol{M}(R)... \odot \boldsymbol{M}(R)}_{n \text{ factores}} \tag{7.5}$$

realizada con n factores, en donde $\odot$ denota el producto matricial de bits (o producto matricial booleano) definido a continuación.

Definición. Producto matricial de bits (o producto matricial booleano). Sean los conjuntos finitos A, B y C, con p, q y r elementos, respectivamente, las relaciones R_1 de A en B, y R_2 de B en C, respectivamente, y las matrices de relaciones $\boldsymbol{M}(R_1)$ de $p \times q$ y $\boldsymbol{B}(R_2)$ de $q \times r$, se define el producto matricial de bits $\boldsymbol{M}(R_1 \circ R_2) = \boldsymbol{M}(R_1) \odot \boldsymbol{M}(R_2)$ a la matriz obtenida realizando primero el producto matricial usual, y a continuación reemplazar cada entrada no nula de $\boldsymbol{M}(R_1 \circ R_2)$ por 1, mientras que las entradas nulas siguen siendo nulas.

Ejemplo. Sea el conjunto $A = \{1, 2, 3, 4, 5, 6\}$, y la relación R = { (1,2), (1,3), (2,2), (2,4), (2,5), (3,4), (4,5), (5,6) }, ver Fig. 7.3. Calculando $R^2 = R \circ R$ mediante la definición se obtiene: R^2 = { (1,2), (1,4), (1,5), (2,2), (2,4), (2,5), (2,6), (3,5), (4,6) }, y que son todas

las trayectorias de longitud 2 en A obtenidas a partir de R, verlo en la Fig. 7.3. Tarea: obtener R^2 mediante el producto matricial de bits $\boldsymbol{M}(R^2) = \boldsymbol{M}(R) \odot \boldsymbol{M}(R)$.

En la Tabla 7.1 se resumen recetas prácticas para chequear en una relación R en un conjunto finito A de n elementos las propiedades: reflexiva, simétrica, antisimétrica, y transitiva, en donde

$$\begin{aligned} I_A &= \{(x_1, x_1), (x_1, x_1)..., (x_n, x_n)\} && \text{relación identidad en } A; \\ R^2 &= R \circ R && \text{composición de } R \text{ con } R; \\ R^{-1} &= \{(y, x) \mid (x, y) \in R\} && \text{relación inversa de } R; \end{aligned} \tag{7.6}$$

propiedad	como conjunto	en la matriz de R
R es reflexiva	$I_A \subseteq R$	$\boldsymbol{M}(I_A) \leq \boldsymbol{M}(R)$
R es simétrica	$R = R^{-1}$	$\boldsymbol{M}(R) = \boldsymbol{M}(R^{-1})$
R es antisimétrica	$R \cap R^{-1} \subseteq I_A$	$\boldsymbol{M}(R) \odot \boldsymbol{M}(R^{-1}) \leq \boldsymbol{M}(I_A)$
R es transitiva	$R^2 \subseteq R$	$\boldsymbol{M}(R^2) \leq \boldsymbol{M}(R)$

Tabla 7.1: Recetas para chequear algunas propiedades de una relación R en un conjunto A.

Ejemplo. Sea el conjunto $A = \{a, b, c\}$ y la matriz de la relación R dada por la Ec. (7.7). Usar el producto matricial de bits (o producto booleano) para decidir si R es transitiva (o no).

$$\boldsymbol{M}(R) = \begin{array}{c} \\ a \\ b \\ c \end{array} \begin{array}{c} \begin{array}{ccc} a & b & c \end{array} \\ \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \end{array} \tag{7.7}$$

Solución. Calculando:

$$\boldsymbol{M}(R^2) = \begin{array}{c} \\ a \\ b \\ c \end{array} \begin{array}{c} \begin{array}{ccc} a & b & c \end{array} \\ \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{array} \tag{7.8}$$

A partir de las Ecs. (7.7-7.8) se concluye que no se cumple que $\boldsymbol{M}(R^2) \leq \boldsymbol{M}(R)$, por lo que R no es transitiva.

Ejemplo. Sea el conjunto $A = \{a, b, c\}$ y la matriz de la relación R dada por la Ec. (7.9). Usar el producto matricial de bits (o producto booleano) para decidir si R es transitiva (o no).

$$\boldsymbol{M}(R) = \begin{array}{c} \\ a \\ b \\ c \end{array} \begin{array}{c} \begin{array}{ccc} a & b & c \end{array} \\ \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \end{array} \tag{7.9}$$

Solución. Calculando:

$$M(R^2) = \begin{array}{c} \\ a \\ b \\ c \end{array} \begin{array}{c} \begin{array}{ccc} a & b & c \end{array} \\ \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \end{array} \tag{7.10}$$

A partir de las Ecs. (7.9-7.10) se concluye que se cumple que $M(R^2) \leq M(R)$, por lo que R es transitiva.

Observación. [omitir] Implementaciones de tests para determinar si una relación R en un conjunto A es: reflexiva, simétrica, antisimétrica, transtiva, relación de equivalencia, relación de orden parcial, o ninguna, analizando la matriz M asociada a R, son mostradas a continuación.

```
def es_reflexiva (M):
    n = len(M)
    for i in range (n):
        if not M[i,i]:
            return False
    return True
```

```
def es_simetrica_vainilla (M):
    n = len (M)
    for i in range (n):
        for j in range (n):
            if (M[i,j] and not M[j,i]):
                return False
    return True
```

```
def es_simetrica(M):
    n = len (M)
    for i in range (n):
        for j in range (i+1,n):
            if (M[i,j] and not M[j,i]):
                return False
            if (M[j,i] and not M[i,j]):
                return False
    return True
```

```
def es_antisimetrica (M):
    n = len (M)
    for i in range (n):
        for j in range (i+1,n):
            if (M[i,j] and M[j,i]):
                return False
    return True
```

```
def es_transitiva (M):
    n = len (M)
    for k in range (n):
        for i in range (n):
            for j in range (n):
                if ((M[i,k] and M[k,j]) and not M[i,j]):
                    return False
    return True
```

```
def es_relacion_de_equivalencia (M):
    return (es_reflexiva (M) and
            es_simetrica (M) and
            es_transitiva(M))
```

```
def es_relacion_de_orden_parcial (M):
    return (es_reflexiva     (M) and
            es_antisimetrica(M) and
            es_transitiva    (M))
```

7.4. Cierre de relaciones

Para el hogar:

- Cierre reflexivo, relación diagonal: definiciones y ejemplos;
- Cierre simétrico: definición y ejemplos;
- Cierre transitivo, relación de conexión, y matriz boolena del cierre transitivo:
  - Definición 2 (pág. 466);
  - Enunciados de los teoremas 2 y 3 (págs. 466 y 468);
  - Re-hacer Ejemplo 7 (pág. 468);
  - Omitir el algoritmo de Roy-Warshall.

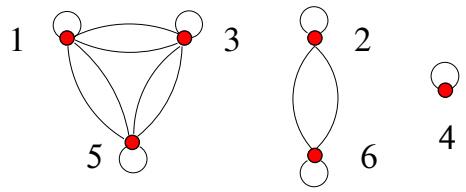

Figura 7.4: La relación R es una RE.

7.5. Relaciones de equivalencia

Intro

Definición. *Relación de Equivalencia*: es una relación R sobre un conjunto A que es reflexiva, simétrica, y transitiva.

Ejemplo. Sea el conjunto $A = \{1, 2, 3, 4, 5, 6\}$ y la Relación de Equivalencia (RE) dada por la Ec. (7.11). Se tiene que esta R es una RE. Verlo más rápidamente analizando la Fig. 7.4.

$$\begin{aligned} R = \{&(1,1),(1,3),(1,5),(2,2),(2,6),(3,5),\\ &(4,4),(5,5),(6,6),(3,1),(5,1),(6,2),(5,3)\} \end{aligned} \tag{7.11}$$

Definición. *Partición* (def.): una partición $\mathcal{S}$ de un conjunto A es una colección de n subconjuntos A_k para $k = 1, 2, ..., n$, llamados también como bloques, tales que: (i) cada bloque A_k es no vacío; (ii) los bloques son disjuntos dos a dos; y (iii) la unión de todos los bloques recupera al conjunto A.

Notación: los subconjuntos (bloques) A_k definen la partición

$$S = \{A_k \mid \text{para } k = 1, 2, ..., n\}$$

con n entero positivo, cuando

$$\begin{cases} A_k \neq \emptyset & \text{para } k = 1, 2, ..., n; \\ A_i \cap A_j = \emptyset & \text{con } i \neq j, \text{ para } i, j = 1, 2, ..., n; \\ \bigcup_{k=1}^{n} A_k = A & . \end{cases} \tag{7.12}$$

Ejemplo. Sea el conjunto $A = \{a, b, c, d, e, f, g, h, i, j\}$, con $|A| = 10$, y los subconjuntos (bloques) $A_1 = \{a, b, c\}$, $A_2 = \{d, e\}$, $A_3 = \{f\}$, y $A_4 = \{g, h, i, j\}$. Como se cumplen las tres condiciones

- Cada bloque A_k es no vacío, para $k = 1, 2, 3, 4$;
- Todas las intersecciones de los bloques de a pares son vacías, i.e. $A_1 \cap A_2 = A_1 \cap A_3 = A_1 \cap A_4 = \emptyset$, $A_2 \cap A_3 = A_2 \cap A_4 = \emptyset$, y $A_3 \cap A_4 = \emptyset$;
- $A_1 \cup A_2 \cup A_3 \cup A_4 = A$;

entonces la colección de conjuntos (bloques) A_1, A_2, A_3, y A_4, define una partición $\mathcal{S}$ del conjunto A.

Clases de equivalencia y particiones

Observación. Si $\mathcal{S}$ es una partición de un conjunto A, entonces se la puede emplear para construir una RE en el conjunto A.

Ejemplo. Sea el conjunto de 6 pelotas $A = \{1, 2, 3, 4, 5, 6\}$, numeradas y pintadas con los colores rojo (*red*, pelotas 1, 3, 5), verde (*green*, pelotas 2,6), y amarillo (*yellow*, pelota 4). Si las separamos en los bloques obtenemos la Ec. (7.13). entonces la colección $S = \{A_1, A_2, A_3\}$ define una partición de A, donde la relación aRb indica que las pelotas a y b son del mismo color, donde R está dada por la Ec. (7.14). Se observa que R es una RE. Verlo quizás más rápidamente analizando la Fig. 7.4.

$$\begin{aligned} A_1 &= \{x \mid x \text{ es una pelota roja }\} \\ A_2 &= \{x \mid x \text{ es una pelota verde }\} \\ A_3 &= \{x \mid x \text{ es una pelota amarilla}\} \end{aligned} \tag{7.13}$$

$$R = \{(1,1),(1,3),(1,5),(2,2),(2,6),(3,5),(4,4),(5,5),(6,6),(3,1),(5,1),(6,2),(5,3)\} \tag{7.14}$$

Teorema. (teor. 3.2.1, pág. 125 Johnsonbaugh). Sea $\mathcal{S}$ una partición en un conjunto A. Se define la relación R en A como sigue: aRb si y solo si los elementos a y b pertenecen a un mismo bloque A_k de la partición $\mathcal{S}$. En esas condiciones, la relación R es una RE. *Demostración*:

- Sea un elemento $a \in A$. Por la definición de partición $\mathcal{S}$, un elemento a debe pertenecer a algún conjunto A_k de la partición $\mathcal{S}$, por lo que aRa. Además, se observa que eso ocurre para todo elemento $a \in A$. Por eso, la relación R es reflexiva;
- Suponga que aRb. Eso significa que ambos elementos a y b están en un mismo bloque A_k de la partición $\mathcal{S}$. Por eso, se concluye que también bRa. Otra vez, eso vale para todo $a, b \in A$, por lo que la relación R es simétrica;
- Suponga que aRb y que bRc. En el primer caso, significa que ambos elementos a y b pertenecen a un mismo bloque A_i de la partición $\mathcal{S}$, mientras que en el segundo caso significa que los elementos b y c pertenecen a algún otro bloque A_j, posiblemente con $i \neq j$. Pero el elemento b pertenece exactamente a un bloque de la partición $\mathcal{S}$, por lo que debe ser $i = j$. En consecuencia, ambos elementos a y c estarán en el mismo bloque A_i y, por ende, aRc. Otra vez, esto vale para todo $a, b, c \in A$, por lo que la relación R es transitiva.

Si $\mathcal{S}$ es una partición de un conjunto A, y R es una RE determinada por $\mathcal{S}$, entonces los bloques de la partición $\mathcal{S}$ pueden ser descriptos en términos de la RE expresada por R. Si A_k es un bloque genérico de la partición $\mathcal{S}$, y $a \in A_k$ le pertenece, entonces, por definición de partición, se tiene que A_k consta de todos los elementos x que están relacionados con a.

Definición. *Conjunto relativo en una* RE *de un elemento*: sea R una RE sobre un conjunto A, y un elemento p de A. El conjunto relativo en R del elemento p de A es el conjunto formado por todos los elementos $x \in A$ tales que xRp, y se denota con la Ec. (7.15).

$$[p] = \{x \mid xRp\} \tag{7.15}$$

Definición. *Clases de Equivalencia*: sea R una RE sobre un conjunto A. Los conjuntos relativos $[a]$ definidos por la partición $\mathcal{S}$ asociada con R se llaman las CE sobre el conjunto A.

Ejemplo. En el ejemplo de las pelotas numeradas y pintadas con los colores rojo (*red*, pelotas 1, 3, 5), verde (*green*, pelotas 2,6), y amarillo (*yellow*, pelota 4), tenemos la tres CE dadas en la Ec. (7.16). En general, los números de elementos en cada CE son diferentes entre si. Sugerencia: omitir el ter. 3.2.15 por inducir a confusión.

$$\begin{aligned} C_1 &= \{1, 3, 5\} = [1] = [3] = [5] \\ C_2 &= \{2, 6\} = [2] = [6] \\ C_3 &= \{4\} = [4] \end{aligned} \tag{7.16}$$

Teorema. Se R una RE en el conjunto A. Las afirmaciones listadas en la Ec. (7.17) son equivalentes.

$$\begin{aligned} &\text{(i)} && aRb && ; \\ &\text{(ii)} && [a] = [b] && ; \\ &\text{(iii)} && [a] \cap [b] \neq \emptyset && ; \end{aligned} \tag{7.17}$$

Demostración:

1) (i) $\rightarrow$ (ii) Suponga que aRb. Para probar que $[a] = [b]$ mostraremos que $[a] \subseteq [b]$ y que $[b] \subseteq [a]$. Para eso hacemos:
   - Sea $x \in [a]$, entonces, por la definición de $[a]$, se concluye que xRa;
   - Como xRa, aRb, y R es transitiva, debe ser xRb, por lo que $x \in [b]$;
   - Como $x \in [a]$ y $x \in [b]$, para todo $x \in [a]$, debe ser $[a] \subseteq [b]$;
   - Al revés, sea $z \in [b]$, entonces, por la definición de $[b]$, se tiene que zRb;
   - Como R es simétrica, si aRb debe ser bRa;
   - Como zRb, bRa, y R es transitiva, debe ser zRa, con lo que $z \in [a]$;
   - Como $z \in [b]$ y $x \in [a]$, para todo $z \in [b]$, debe ser $[b] \subseteq [a]$;
   - Se concluye que $[a] = [b]$.
2) (ii) $\rightarrow$ (iii) Suponga que $[a] = [b]$. Como R es reflexiva, se tiene que aRa para todo $a \in A$. En ese caso, como $[a]$ es no vacia, se concluye $[a] \cap [b] \neq \emptyset$;
3) (iii) $\rightarrow$ (i) Suponga que $[a] \cap [b] \neq \emptyset$. Entonces existe un elemento c tal que $c \in [A] \wedge c \in [b]$, es decir, aRc y bRc. Por simetría, si bRc debe ser cRb. Entonces tenemos aRc, cRb, y R transitiva, por lo que debe ser aRb;
4) Como se cumplen (i) $\rightarrow$ (ii), (ii) $\rightarrow$ (iii), y (iii) $\rightarrow$ (i), las 3 afirmaciones son equivalentes.

7.6. Ordenes parciales

Relación de orden parcial

Definición. se dice que una relación R en un conjunto A es una Relación de Orden Parcial (ROP) si es reflexiva, antisimétrica, y transitiva.

Relación de orden total

Definición. Elementos comparables e incomparables. Sea una ROP R sobre un conjunto A, y sean los elementos $a, b \in A$. Se denota con $a \preceq b$ para indicar que $(a, b) \in R$, notación que sugiere interpretar a la ROP R como un ordenamiento de los elementos de A. Si en una ROP R en un conjunto A se verifica que $a \preceq b$ o bien $b \preceq a$, entonces se dice que los elementos a y b de A son comparables y, en el caso contrario se dice que son elementos incomparables.

Definición. Relación de orden total: una relación R en un conjunto A es una Relación de Orden Total (ROT) cuando todos los elementos de A son comparables.

Ejemplo.

1) **Ejemplo de orden total**: la relación $\leq$ en los enteros positivos es una ROT, pues para todos los enteros $a, b \in \mathbb{Z}$ se tiene, o bien $x \leq y$, o bien $y \leq x$;
2) **Ejemplo de orden parcial**: la relación $a|b$ en los enteros positivos es una ROP porque tiene elementos tanto comparables como incomparables, e.g. 3 y 6 son comparables (pues 3 divide a 6), pero 2 y 3 son incomparables (pues 2 no divide a 3).

CAPÍTULO 8

Grafos

Nota. Estas notas siguen el texto de referencia Rosen (2004) manteniendo la numeración de las secciones y sus títulos, como una referencia adicional para el auto-estudio siguiendo ese texto.

Contents

8.1. Introducción a los grafos

Lectura para el hogar.

Tipos de grafos

Definición.

- *Grafo*: un grafo se denota con la dupla $G = (V, E)$, y está formado por un conjunto V de *vértices* (o nodos), y de un conjunto E de *aristas*, tal que cada arista $e \in E$ se asocia a un par no-ordenado de vértices;
- Si existe una *única* arista e asociada a los vértices u y v se escribe $e = (u, v)$ o $e(v, u)$ en donde, en este contexto, (u, v) no-representa un par ordenado;
- Supondremos (suposición más frecuente en literatura) que el conjunto de vértices V es no-vacío, el de aristas E puede ser vacío, y que ambos son finitos;
- Se dice que dos o más aristas son *aristas paralelas* cuando están asociadas a un mismo par de vértices;
- *Lazo* (o *bucle*): es una arista incidente en un mismo vértice;

- Vértice *aislado*: es un vértice que no incide en ninguna arista;
- Un *grafo simple* es un grafo $G = (V, E)$ *sin lazos ni aristas paralelas*;
- *Multigrafo*: un multigrafo $G = (V, E)$ consta de un conjunto de vértices V, un conjunto de aristas E, y una función f de E en $\{\{u, v\} \mid u, v \in V,\ u \neq v\}$. Se dice que las aristas e_1 y e_2 son aristas múltiples (o paralelas) si $f(e_1) = f(e_2)$;
- *Pseudografo*: un pseudografo $G = (V, E, f)$ consta de un conjunto de vértices V, un conjunto de aristas E, y una función f de E en $\{\{u, v\} \mid u, v \in V\}$. Se dice que una arista e es un *lazo* (o *bucle*) si $f(e) = \{u, u\}$ para algún $u \in V$.

Teorema. [en el texto de Rosen: *teorema de los apretones de manos* **reclásico en evaluaciones**]. Sea $G = (V, E)$ un grafo con $n = |V|$ vértices y $m = |E|$ aristas. Se cumple que

$$\sum_{k=1}^{n} \delta(v_k) = 2m \tag{8.1}$$

En particular, la suma de los grados de todos los vértices de un grafo es un número par. Demostración: cada arista contribuye en 2 unidades a la suma de los grados de los vértices, pues cada arista incide en 2 vértices, posiblemente iguales. Eso significa que la suma de los grados de todos los vértices, debe ser igual al doble del número de aristas.

Teorema. [en el texto de Johnsonbaugh figura como un corolario del teorema anterior **reclásico en evaluaciones**]. Todo grafo $G = (V, E)$ tiene un número par de vértices de grado impar. Demostración: sean V_P y V_I los conjuntos de vértices de grado par e impar, respectivamente, de G. Descomponemos la suma de los grados de todos los vértices en 2 sumas:

$$\sum_{v \in V_P} \delta(v) + \sum_{v \in V_I} \delta(v) = 2m \tag{8.2}$$

- Como $\delta(v)$ es par si $v \in V_P$, la primera sumatoria es la suma de números pares, por lo que es un número par.
- Además la suma de ambas sumatorias es otro número par, e igual a $2m$. En consecuencia la segunda sumatoria debe ser otro número par.
- Pero todos los términos en la segunda sumatoria son números impares, por lo que la única chance es que debe haber un número par de sumandos. En definitiva, debe haber un número par de vértices de grado impar.
- Observ.: notar que este teor. se cumple, por ejemplo, incluso en los siguientes casos particulares:
  - Cuando $G(V, E)$ tiene un vértice y sin aristas:
  - Cuando $G(V, E)$, conexo o desconexo, tiene únicamente vértices de grado par, con lo que el número de vértices de grado impar es cero. Pero como cero es un entero par, otra vez, se verifica el enunciado.

Familias distinguidas de grafos simples

Definición.

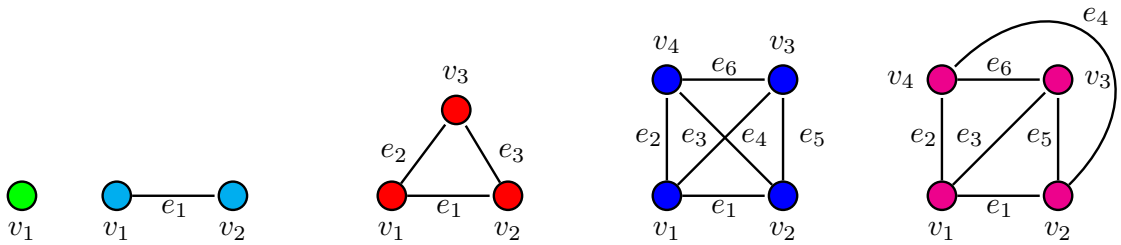

Figura 8.1: Los grafos completos K_1, K_2, K_3, y K_4, en donde K_4 graficado de dos maneras.

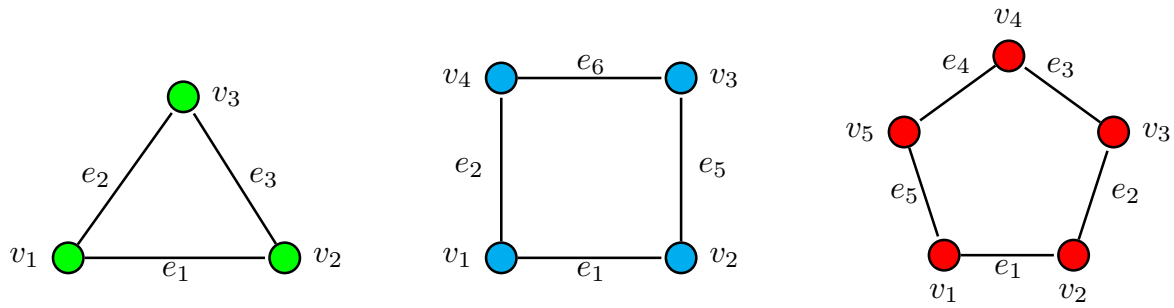

Figura 8.2: Los grafos ciclo C_3, C_4, y C_5.

- Grafo *completo*: el grafo completo de n vértices, con $n \geq 1$, es el grafo *simple* que contiene exactamente una arista entre cada par de vértices distintos. Se denota con K_n.
- *Grafo ciclo*: el grafo ciclo para $n \geq 3$ vértices es un grafo simple que consta de n vértices $\{v_1, v_2, v_3, ..., v_n\}$, y las aristas $\{(v_1, v_2), (v_2, v_3), ..., (v_{n-1}, v_n)\}$. Se denota con C_n.
- *Grafo rueda* (*wheel*): el grafo rueda es el grafo simple que se obtiene cuando se agrega un vértice adicional al ciclo C_n y lo conectamos con cada uno de los vértices de C_n. Se denota con W_n.
- *Grafo n-cubo* (o hipercubo): el cubo n dimensional es el grafo simple que tiene 2^n vértices, el grado de cada vértice es n, cuyos vértices representan a las 2^n cadenas de bits de longitud n, de modo tal que dos vértices son adyacentes si las cadenas de bits a las que representan difieren exactamente en un bit. Se denota con Q_n. Para construir en forma *recursiva* de Q_{n+1} a partir de Q_n: se hacen dos copias de Q_n, anteponiendo un 0 a cada una de las etiquetas de los vértices de una de las copias de Q_n, anteponiendo un 1 a cada una de las etiquetas de los vértices de la otra copia, y agregando aristas que conectan 2 vértices cuyas etiquetas difieran únicamente en el primer bit.

Ejemplo. Los grafos completos K_1, K_2, K_3, y K_4 se muestran en la Fig. 8.1.

Ejemplo. Los grafos ciclo C_3, C_4, y C_5 se muestran en la Fig. 8.2.

Ejemplo. Los grafos rueda W_3, W_4, y W_5 se muestran en la Fig. 8.3.

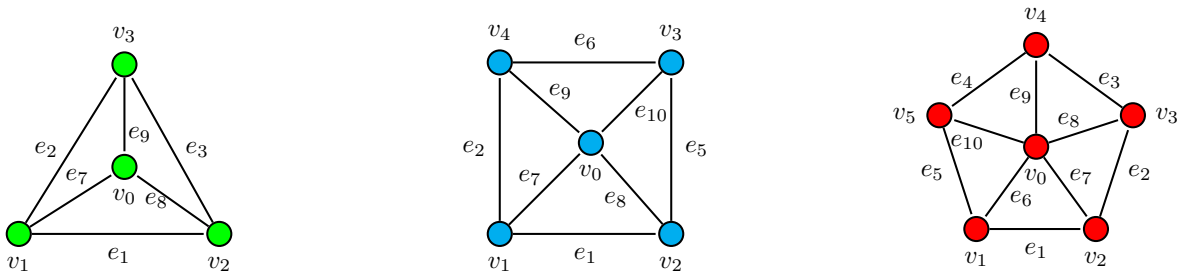

Figura 8.3: Los grafos rueda W_3, W_4, y W_5.

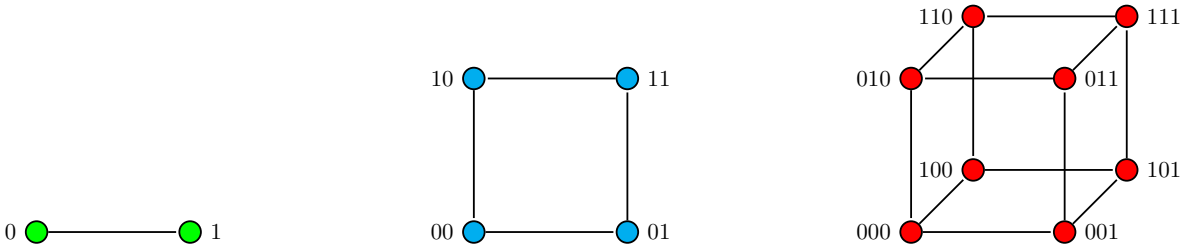

Figura 8.4: Los hipercubos Q_1, Q_2, y Q_3.

Ejemplo. Los hipercubos Q_1, Q_2, y Q_3, obtenidos en forma recursiva, se muestran en la Fig. 8.4.

Tarea. Obtener: el hipercubo Q_2 a partir de Q_1, y el hipercubo Q_3 a partir de Q_2, en forma recursiva.

Ejemplo. Utilizando un argumento de conteo determine el número de aristas de K_n y de Q_n. Solución:

- El grafo completo K_n tiene n vértices y el grado de cada vértice es $(n-1)$. Eso se repite en todos los n vértices, y utilizando el principio de la multiplicación el número de aristas sería $n(n-1)$, pero notar que en el conteo las aristas se cuentan dos veces: la arista e_{ij} se cuenta una vez como arista incidente en el vértice i y otra vez como arista incidente en el vértice j, por lo tanto el número total de aristas en K_n es la mitad, o sea $n(n-1)/2$.
- El hipercubo Q_n tiene 2^n vértices y el grado de cada vértice es n. Eso se repite en todos los 2^n vértices, y utilizando el principio de la multiplicación el número de aristas sería $n2^n$, pero otra vez en el conteo las aristas se cuentan dos veces: la arista e_{ij} se cuenta una vez como arista incidente en el vértice i y otra vez como arista incidente en el vértice j, por lo tanto el número total de aristas en Q_n es la mitad, o sea $n2^n/2$, es decir, $n2^{n-1}$.

Grafos bipartitos

Definiciones.

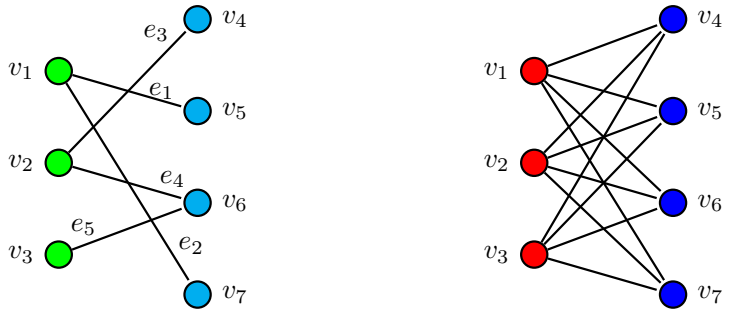

Figura 8.5: Un grafo bipartito $G_{3,4}$, y el grafo bitartito completo $K_{3,4}$.

- Grafo *bipartito*: un grafo $G = (V, E)$ es bipartito si es un grafo simple en donde existen dos conjuntos de vértices V_1 y V_2 de V, cualesquiera posiblemente vacío, tales que $V_1 \cap V_2 = \emptyset$, y $V_1 \cup V_2 = V$, y donde cada arista de E es incidente en un vértices de V_1 y en un vértice de V_2. En particular, el grafo completo K_1 es bipartito: donde V_1 es el conjunto que contiene al único vértice, y V_2 es el conjunto vacío, donde cada arista, en realidad ninguna, incide en un vértice de V_1 y en un vértice de V_2;
- Grafo *bipartito completo*: un grafo $G = (V, E)$ es bipartito completo si es un grafo simple tal que: (i) el conjunto de vértices admite una partición en V_1 con m vértices y en V_2 con n vértices; y (ii) el conjunto de aristas E consiste en *todas* las aristas de la forma (v_i, v_j), con $v_i \in V_1$ y $v_j \in V_2$. Se denota con $K_{m,n}$.

Ejemplo. En la Fig. 8.5 se muestran un grafo bipartito $G_{3,4}$, y el grafo bitartito completo $K_{3,4}$.

Algunas aplicaciones de tipos especiales de grafos

Lectura optativa:

- Ejemplo 12: redes de área local;
- Ejemplo 13: redes en cálculo paralelo.

Grafos definidos a partir de otros

Definiciones.

- *Subgrafo*: se dice que $G' = (V', E')$ es un subgrafo del grafo $G = (V, E)$ si $V' \subseteq V$ y $E' \subseteq E$;
- *Unión de dos grafos*: la union de dos grafos simples $G_1 = (V_1, E_1)$ y $G_2 = (V_2, E_2)$ es el grafo simple $G = (V, E)$ donde $V = V_1 \cup V_2$ y $E = E_1 \cup E_2$.

8.2. Representaciones e isomorfismo en grafos

Representaciones de grafos

Sea un grafo $G = (V, E)$ sin aristas múltiples. Dos representaciones de grafos comprenden: (i) enumerar todas las aristas de G; (ii) utilizar listas de adyacencia, i.e. listar los vértices que son adyacentes a cada vértice de G.

Matrices de adyacencia

Definiciones.

- Matriz de *adyacencia* en grafos simple: Sea un grafo simple $G = (V, E)$, con $n = |V|$ vértices y $m = |E|$ aristas, con un orden arbitrario en los vértices y en las aristas. la matriz de adyacencia $\boldsymbol{A}$ de G tiene n filas y n columnas, siguiendo el orden dado a los vértices, y con valores enteros según:

$$[\boldsymbol{A}]_{i,j} = \begin{cases} 1 & \text{si la arista } (v_i, v_j) \in E, \text{ con } i \neq j \\ 0 & \text{en otro caso} \end{cases} \tag{8.3}$$

- Matriz de *adyacencia* en grafos con bucles y aristas paralelas: Sea un grafo $G = (V, E)$ con lazos o con aristas paralelas, con $n = |V|$ vértices y $m = |E|$ aristas, con un orden arbitrario en los vértices y en las aristas. la matriz de adyacencia $\boldsymbol{A}$ de G tiene n filas y n columnas, siguiendo el orden dado a los vértices, y con valores enteros según:

$$[\boldsymbol{A}]_{i,j} = \begin{cases} k & \text{si hay } k \text{ aristas paralelas } (v_i, v_j), \text{ con } i \neq j \\ 2z & \text{si hay } z \text{ lazos } (v_i, v_i) \\ 0 & \text{en otro caso} \end{cases} \tag{8.4}$$

- La matriz de adyacencia $\boldsymbol{A}$ es cuadrada y simétrica;
- La suma de la fila o de la columna del vértice v_i es igual al grado $\delta(v_i)$;
- La matriz de adyacencia depende del ordenamiento dado a los vértices, y como hay $n!$ formas de enumerar los vértices, hay $n!$ matrices de adyacencia distintas para mismo un grafo G dado de n vértices.

Matrices de incidencia

Definición. Sea un $G = (V, E)$, con $n = |V|$ vértices y $m = |E|$ aristas, con un orden arbitrario en los vértices y en las aristas, tal vez con lazos o con aristas paralelas. La matriz de *incidencia* $\boldsymbol{I}$ de G tiene n filas y m columnas, siguiendo el orden dado, y con valores enteros según:

$$[\boldsymbol{I}]_{i,j} = \begin{cases} 1 & \text{si el vértice } v_i \text{ es incidente en la arista } e_j \\ 0 & \text{en otro caso} \end{cases} \tag{8.5}$$

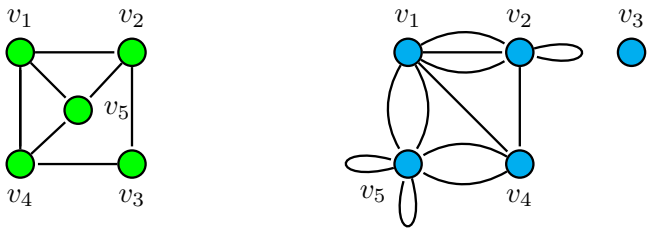

Figura 8.6: G_1: grafo simple (sin lazos ni aristas paralelas) (izq.). G_2: grafo no-simple (con lazos o aristas paralelas) (der).

Ejemplo. En los grafos trazados en la Fig. 8.6:

- En el grafo simple G_1 (izq.):

$$\boldsymbol{A} = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \\ \delta(v_i) \end{array} \begin{array}{c} \begin{array}{ccccc} v_1 & v_2 & v_3 & v_4 & v_5 \end{array} \\ \left[\begin{array}{ccccc} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{array}\right] \\ \begin{array}{ccccc} 3 & 3 & 2 & 3 & 3 \end{array} \end{array} \begin{array}{c} \delta(v_i) \\ \\ 3 \\ 3 \\ 2 \\ 3 \\ 3 \end{array} \tag{8.6}$$

- En el grafo no-simple G_2 (der.):

$$\boldsymbol{A} = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \\ \delta(v_i) \end{array} \begin{array}{c} \begin{array}{ccccc} v_1 & v_2 & v_3 & v_4 & v_5 \end{array} \\ \left[\begin{array}{ccccc} 0 & 3 & 0 & 1 & 2 \\ 3 & 2 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 2 \\ 2 & 0 & 0 & 2 & 4 \end{array}\right] \\ \begin{array}{ccccc} 6 & 6 & 0 & 4 & 8 \end{array} \end{array} \begin{array}{c} \delta(v_i) \\ \\ 6 \\ 6 \\ 0 \\ 4 \\ 8 \end{array} \tag{8.7}$$

  Observar la fila y columna nulas del vértice v_3.

Isomorfismo de grafos (nociones)

Definiciones.

- Los grafos G_1 y G_2 son *isomorfos* si existe una dupla de funciones (f, g) *biyectivas*, en donde la función f mapea los vértices de G_1 a los vértices de G_2, y la función g mapea las aristas de G_1 a las aristas de G_2, de modo tal que una arista e es incidente en los vértices u y v de G_1 si la arista $g(e)$ es incidente en $f(u)$ y en $f(v)$ en G_2.
- La tupla de funciones (f, g) definen el *isomorfismo* de G_1 en G_2.

Ejemplo. En la Fig. 8.7 se muestran los grafos G_1 (izq.) y G_2 (der.):

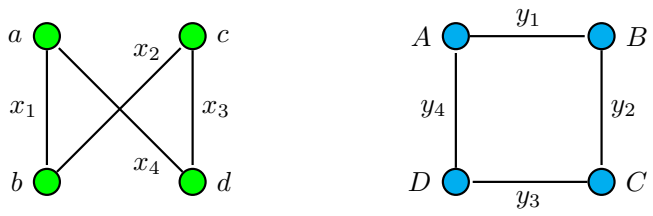

Figura 8.7: Los grafos G_1 (izq.) y G_2 son isomorfos.

- El grafo G_1 tiene los 4 vértices: a, b, c, d, y las 4 aristas: (a, b), (b, c), (c, d), y (d, a);
- El grafo G_2 tiene los 4 vértices: A, B, C, D, y las 4 aristas: (A, B), (B, C), (C, D), y (D, A).
- Los grafos G_1 y G_2 son isomorfos, en donde el isomorfismo es descripto por la tupla de funciones:

$$\begin{array}{cccc} f(a) = A & f(b) = B & f(c) = C & f(d) = D \\ g(x_1) = y_1 & g(x_2) = y_2 & g(x_3) = y_3 & g(x_4) = y_4 \end{array} \tag{8.8}$$

Observación.

- En general, la matriz de adyacencia de un grafo cambia cuando se modifica el orden de los vértices.
- No obstante, los grafos $_1$ y G_2 resultan isomorfos si para algún orden de sus vértices, sus matrices de adyacencia son iguales.

Teorema. Sean los grafos G_1 y G_2 ambos de n vértices. Entonces, G_1 y G_2 son isomorfos si, para algún orden de sus vértices, sus matrices de adyacencia $\boldsymbol{A}_1$ y $\boldsymbol{A}_2$ son iguales. Demostración:

- Suponemos que G_1 y G_2 son isomorfos, por lo que existe una tupla de funciones biyectivas (f, g), con una función f de los vértices de G_1 a los de G_2, y una función g de las aristas de G_1 a las de G_2, de modo tal que una arista e incide en los vértices u y v si la arista $g(e)$ incide en $f(u$ y en $f(v)$ en G_2;
- Sea $u_1, u_2, ..., u_n$ un orden de los vértices de G_1, y $\boldsymbol{A}_1$ la matriz de adyacencia de G_1 relativa a dicho orden;
- Sea $\boldsymbol{A}_2$ la matriz de adyacencia de G_2 relativa al orden $f(u_1), f(u_2), ..., f(u_n)$ de los vértices de G_2;
- Supongamos que la entrada i, j (fila i, columna j, con $i \neq j$) de $\boldsymbol{A}_1$ es igual k. Entonces existen k aristas $e_1, e_2, ...e_k$ incidentes en u_i y en u_j;
- En ese caso, hay otras k aristas $g(e_1), ..., g(e_k)$ incidentes en $f(u_i)$ y en $f(u_j)$ en G_2;
- Por eso, la entrada i, j en $\boldsymbol{A}_2$, que cuenta el número de aristas que inciden en $f(u_i)$ y en $f(u_j)$ también es igual k;
- Un razonamiento similar muestra que las entradas diagonales de $\boldsymbol{A}_1$ y $\boldsymbol{A}_2$ también son iguales;
- Por lo que debe ser $\boldsymbol{A}_1 = \boldsymbol{A}_2$.

Enunciado. Sean los grafos $G_1 = (V_1, E_1)$ y $G_2 = (V_2, E_2)$ isomorfos. Entonces las siguientes enunciados son equivalentes:

- G_1 y G_2 son isomorfos;
- Existe una función biyectiva f de V_1 a V_2 en donde: los vértices u y v son adyacentes en G_1, si los los vértices $f(u)$ y $f(v)$ son adyacentes en G_2.

Ejemplo. Para los grafos G_1 y G_2 mostrados en la Fig. 8.7 (izq. y der.) se tiene que la matriz de adyacencia de G_1 relativa al orden a, b, c, d es

$$\boldsymbol{A}_1 = \begin{array}{c} \\ a \\ b \\ c \\ d \end{array} \begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \end{array} \tag{8.9}$$

y que es igual a la matriz de adyacencia de G_2, relativa al orden A, B, C, D, i.e.

$$\boldsymbol{A}_2 = \begin{array}{c} \\ A \\ B \\ C \\ D \end{array} \begin{array}{c} \begin{array}{cccc} A & B & C & D \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \end{array} \tag{8.10}$$

por lo que G_1 y G_2 son grafos isomorfos.

Definición. Invariante: sean dos grafos G_1 y G_2 isomorfos. Se dice que la propiedad P es un *invariante* si G_1 tiene la propiedad P, entonces G_2 también tiene la propiedad P.

Observación. Si G_1 y G_2 son isomorfos, entonces G_1 y G_2 tienen:

- Un mismo número de vértices, por lo que la propiedad "tiene n vértices" es un invariante, con $n \geq 0$;
- Un mismo número de aristas, por lo que la propiedad "tiene e aristas" es un invariante, con $e \geq 0$;
- La misma cantidad de vértices de igual grado, por lo que la propiedad "tiene un vértice de grado k" es un invariante, con $k \geq 0$;
- La misma cantidad de ciclos simples de longitud k, por lo que la propiedad "tiene un ciclo simple de longitud k" es un invariante, con $k \geq 3$;
- Nota: hay muchos otros invariantes que no veremos.

Ejemplo. En la Fig. 8.8 se muestran los grafos G_1 (izq.) y G_2 (der.), en donde:

- Ambos tienen 6 vértices cada uno;
- Ambos tienen 10 aristas cada uno;
- G_1 no tiene vértices de grado 3, pero G_2 tiene 2, por lo que G_1 y G_2 no son isomorfos.

Ejemplo. En la Fig. 8.9 se muestran los grafos G_1 (izq.) y G_2 (der.), en donde:

- Ambos tienen 8 vértices cada uno;
- Ambos tienen 16 aristas cada uno;
- Cada vértice en G_1 y en G_2 tiene grado 4;
- Los ciclos simples en G_1 son de longitud 3, pero en G_2 los ciclos simples son de longitud 4, por lo que G_1 y G_2 no son isomorfos.

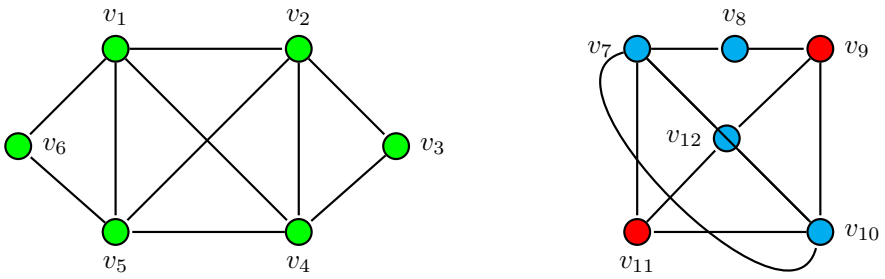

Figura 8.8: Los grafos G_1 (izq.) y G_2 tienen 6 vértices y 10 aristas cada uno, pero G_1 no tiene vértices de grado 3 mientras que G_2 tiene 2 (en rojo), por lo que no son isomorfos.

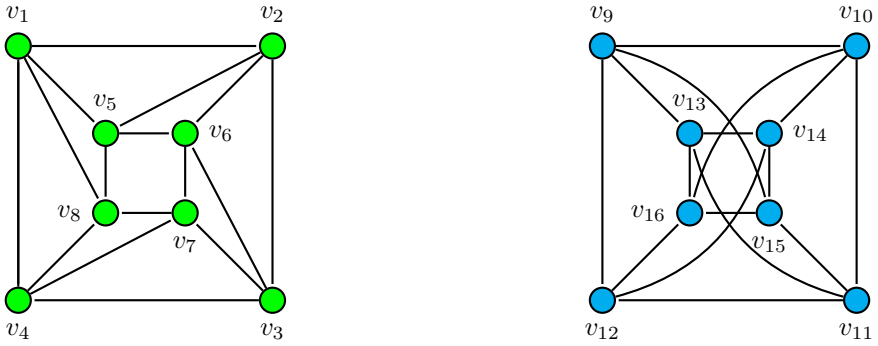

Figura 8.9: Los grafos G_1 (izq.) y G_2 tienen 8 vértices, 16 aristas, y 8 vértices de grado 4 cada uno, pero G_1 tiene ciclos simples de longitud 3 mientras que G_2 no, por lo que no son isomorfos.

8.3. Conexión

Caminos

Definiciones. Sea un grafo $G = (V, E)$, dos vértices u y v de G, y n es un entero no-negativo. Entonces:

- *Camino* (o trayectoria o ruta): Un *camino* de longitud n de u a v en G, es una secuencia de n aristas e_1, e_2, ..., e_n de G tal que $f(e_1) = \{x_0, x_1\}$, $f(e_2) = \{x_1, x_2\}$, ..., $f(e_n) = \{x_{n-1}, x_n\}$, donde $x_0 = u$ y $x_n = v$. Si G en particular es simple, entonces denotamos ese camino por su secuencia de vértices $x_0, x_1, ..., x_n$ (pues al enumerar esos vértices el camino es único);
- *Circuito* (o ciclo): cuando el camino empieza y termina en el mismo vértice, i.e. $u \equiv v$, y tiene longitud mayor a cero;
- Se dice que el camino o el circuito *pasa por* los vértices $x_0, x_1, ..., x_n$;
- Se dice que el camino o el circuito *recorre* las aristas $e_1, e_1, ..., e_n$;
- Camino *simple* (o trayectoria simple, o ruta simple): cuando no-repite aristas.
- Circuito *simple*: cuando no-repite aristas.

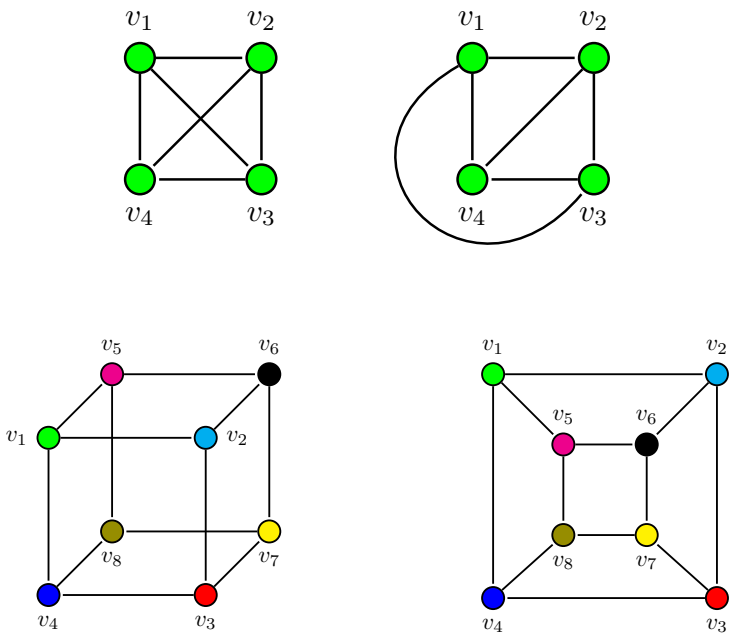

Figura 8.10: El grafo completo K_4 (arriba, izq. y der.), y el hipercubo Q_3 (abajo, izq. y der.) son grafos planos.

Definición. *Grafo conexo*: Un grafo $G = (V, E)$ es conexo si exite al menos un camino entre cada par de vértices distintos de G.

Enunciado. Sea $G = (V, E)$ un grafo conexo. Existe un camino simple entre cada par de vértices distintos.

Definición.

- *Componente* (o *componente conexa*). Sea un grafo conexo $G = (V, E)$ y un vértice u en G. El subgrafo G' de G formado por todas las aristas y vértices de G que están contenidos en algún camino que comienza en el vértice u se llama *componente* (o *componente conexa*) de G que contiene a u;
- *Vértice de articulación*. Sea un grafo conexo $G = (V, E)$ y un vértice u en G. Un vértice v en G es un vértice de articulación si al eliminar v y todas las aristas incidentes en v, se desconecta G;
- *Arista puente*. Sea un grafo conexo $G = (V, E)$ y un vértice u en G. Una arista e en G es una arista puente si la eliminación de e (pero conservando los vértices incidentes en e), desconecta a G.

Ejemplo. El grafo $G = (V, E)$ trazado en la Fig. 8.11 es un grafo conexo porque existe, al menos, un camino entre cada par de vértices en G. Por eso, se puede listar las rutas sin las aristas. Por ejemplo, la ruta $T_1 = (v_8, e_{12}, v_5, e_8, v_2, e_5, v_3, e_7, v_4, e_3, v_1)$, o la ruta $T_2 = (v_8, e_{12}, v_5, e_8, v_2, e_4, v_3, e_7, v_4, e_1, v_1)$, ambas de longitud 5. Además, la ruta $T_3 = (v_8, e_{12}, v_5, e_6, v_1)$, de longitud 3, y la $T_4 = (v_6)$ de longitud 0.

Ejemplo. El grafo $G = (V, E)$ trazado en la Fig. 8.12 es un grafo simple (sin lazos ni aristas paralelas), y también es conexo (existe al menos una ruta entre cada par de vértices

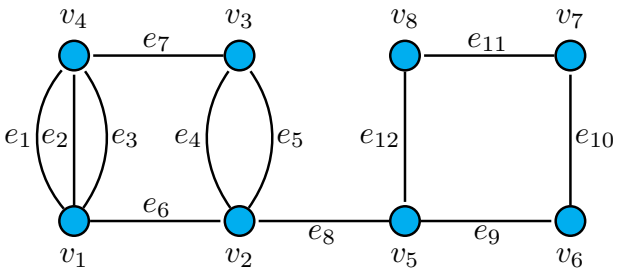

Figura 8.11: El grafo $G = (V, E)$ es conexo porque existe, al menos, una ruta entre cada par de vértices de G, pero no es un grafo simple porque tiene las aristas paralelas e_1, e_2, e_3 y e_4, e_5.

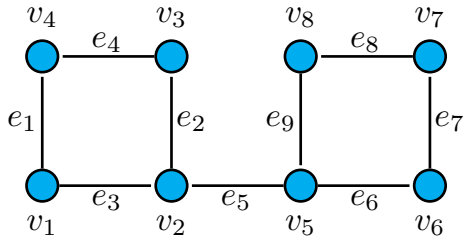

Figura 8.12: Un grafo conexo $G = (V, E)$ porque tiene, al menos, una ruta entre cada par de vértices de G. Además, no es un grafo simple porque tiene las aristas paralelas e_1, e_2, e_3 y e_4, e_5.

de G). En particular, entre los vértices v_8 y v_1 se pueden listar las rutas sin incluir las aristas, e.g. $T_1 = (v_8, v_5, v_2, v_3, v_4, v_1)$ de longitud 5, y la $T_2 = (v_8, v_5, v_2, v_1)$, de longitud 3.

Ejemplo. El grafo $G = (V, E)$ trazado en la Fig. 8.13 no es conexo porque entre otros, por ejemplo, no hay una ruta entre los vértices v_8 y v_1.

Ejemplo. El grafo conexo $G = (V, E)$ trazado en la Fig. 8.14 (arriba, izquierda o derecha) particionado mediante: las aristas puente e_4 y e_8 (mitad-izq.), o con los vértices de articulación v_4 y v_9 (mitad-der.), la elección de los mismos es arbitraria, resultando dos componentes conexas (abajo-izq. y abajo-der.).

Ejemplo. En el grafo conexo $G = (V, E)$ trazado en la Fig. 8.14 (izq. o der.):

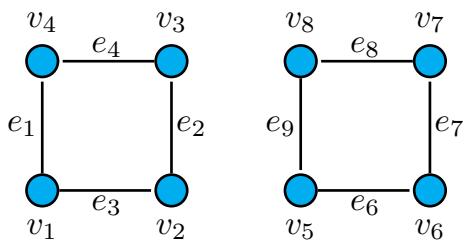

Figura 8.13: Un grafo $G = (V, E)$ que no es conexo porque, por ejemplo, no hay una ruta entre los vértices v_8 y v_1.

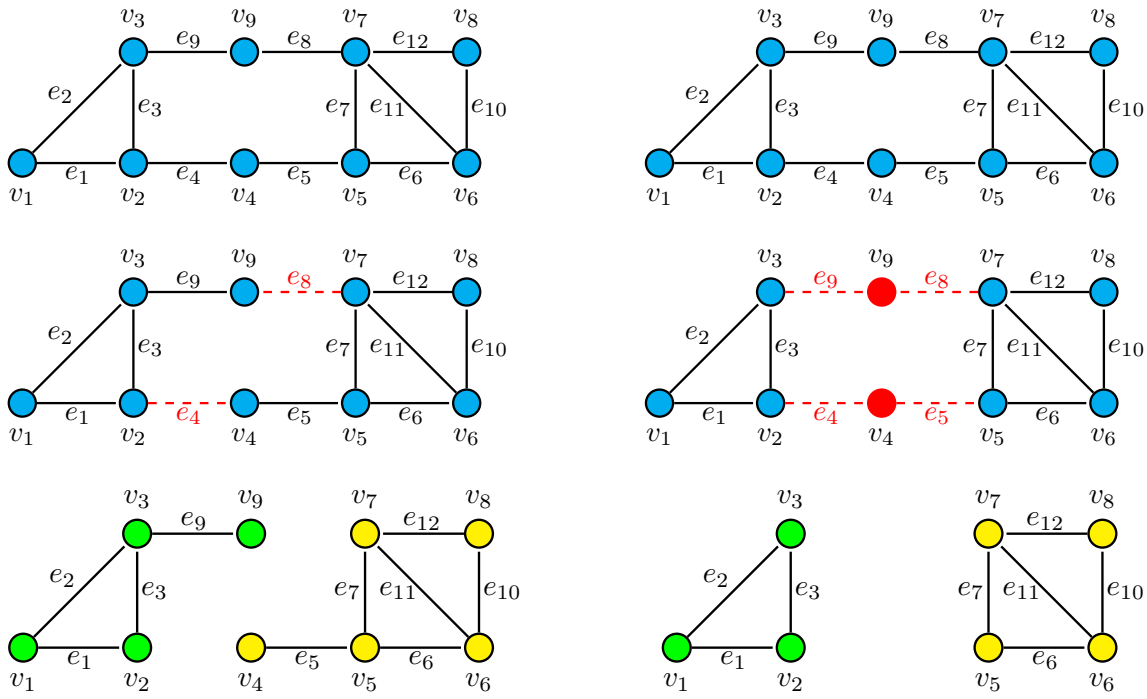

Figura 8.14: Un grafo conexo $G = (V, E)$ (arriba, izq. o der.) particionado mediante: las aristas puente e_4 y e_8 (mitad-izq.), o los con los vértices de articulación v_4 y v_9 (la elección de los mismos es arbitraria), resultando dos componentes conexas (abajo-izq. y abajo-der.).

- $T_1 = (v_4, v_5, v_7, v_6, v_8, v_7, v_9)$: no es una ruta simple, tampoco un ciclo, ni un ciclo simple;
- $T_2 = (v_4, v_5, v_7, v_9)$: sí es una ruta simple, pero no es un ciclo, ni un ciclo simple;
- $T_3 = (v_7, v_6, v_8, v_7, v_9, v_3, v_2, v_4, v_5, v_7)$: no es una ruta simple, sí es un ciclo, pero no un ciclo simple;
- $T_4 = (v_7, v_9, v_3, v_2, v_4, v_5, v_7)$: no es una ruta simple, sí es un ciclo, y sí es un ciclo simple;
- $T_5 = (v_7)$: sí es una ruta simple, pero no es un ciclo, ni un ciclo simple.

Caminos e isomorfismo

Omitir.

El número de caminos entre dos vértices

Teorema. [**Conteo de caminos de longitud** p **en un grafo** G]: sea $G = (V, E)$ un grafo *simple* de n vértices, y la matriz de adyacencia $\boldsymbol{A}$ asociada a G, con respecto a un orden dado. Se cumple que: la entrada ij (en la fila i y columna j) de la potencia $\boldsymbol{A}^p$ es igual al número de caminos de longitud p entre los vértices i y j, para $p = 1, 2, ...$ Demostración (por inducción sobre p).

- Paso Base ($p = 1$): si $p = 1$, $\boldsymbol{A}^1$ se reduce a $\boldsymbol{A}$. La entrada ij es 1 si hay una arista de i a j, lo cual representa un camino de longitud 1, y 0 en otro caso, entonces se verifica

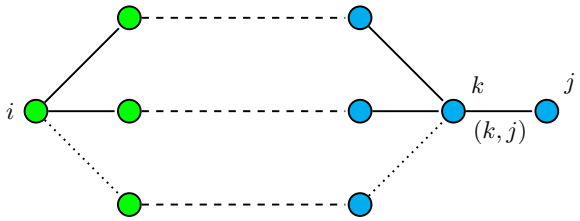

Figura 8.15: Un camino de i a j de longitud $p+1$ cuyo penúltimo vértice es k consiste en un camino de longitud p de i a k, seguida de la arista (k, j). Si hay B_{ik} caminos de longitud p de i a k, y A_{kj} vale 1 si está la arista (k, j) y 0 en otro caso, entonces la suma de $s_k t_k$ sobre toda k da el número de caminos de longitud $p+1$ de i a j.

el PB.

- Paso Inductivo: suponemos que el teorema es cierto para algún entero p, positivo y arbitrario pero fijo, y vemos qué sucede con $p+1$. Además, sea $\boldsymbol{A}^p = \boldsymbol{B}$. Calculamos $\boldsymbol{A}^{p+1}$ con el producto matricial $\boldsymbol{A}^{p+1} = \boldsymbol{A}^p \boldsymbol{A}$, i.e. la entrada ij en $\boldsymbol{A}^{p+1}$ se obtiene al multiplicar por pares los elementos en la fila i de $\boldsymbol{A}^p$ por los elementos de la columna j de $\boldsymbol{A}$, y después sumamos:

$$\text{fila } i \text{ de } \boldsymbol{A}^p = \boldsymbol{B}: \quad \begin{bmatrix} B_{i1} & B_{i2} & \dots & B_{ik} & \dots & B_{in} \end{bmatrix} \times \overset{\text{columna } j \text{ de } \boldsymbol{A}}{\begin{bmatrix} A_{i1} \\ A_{i2} \\ \vdots \\ A_{ik} \\ \vdots \\ A_{in} \end{bmatrix}} \tag{8.11}$$

$$= B_{i1}A_{1j} + B_{i2}A_{2j} + \dots + B_{ik}A_{kj} + \dots + B_{in}A_{nj}$$
$$= \text{entrada } ij \text{ de } \boldsymbol{A}^{p+1}$$

Por la HI, B_{ik} es el número de caminos de longitud p de i a k en el grafo G. Como la última arista es (k, j), Fig. 8.15, y A_{kj} vale 0 o 1:

- Si $A_{kj} = 0$ no hay arista (k, j), por lo que hay $B_{ik}A_{kj} = B_{ik} \cdot 0 = 0$ caminos de longitud $p+1$ de i a j;
- Si $A_{kj} = 1$, hay una arista (k, j). Como hay B_{ik} caminos de longitud p del vértice i al k, entonces hay $B_{ik}A_{kj} = B_{ik} \cdot 1 = B_{ik}$ caminos de longitud $p+1$ de i a j;
- Al sumar sobre k se cuentan todas las caminos de longitud $p+1$ de i a j. Entonces, la entrada ij en $\boldsymbol{A}^{p+1}$ es igual al número de caminos de longitud $p+1$ de i a j, y se prueba el paso inductivo.

Circuitos y circuitos simples

Teorema. Sea $G = (V, E)$ un grafo, y un vértice u cualequiera de G. El grafo G contiene un circuito de u a u, entonces G contiene un circuito simple de u a u. Demostración: sea el ciclo (verlo en el dibujo) $C = (v_0, e_1, v_1, \dots, e_i, v_i, e_{i+1}, \dots, e_j, v_j, e_{j+1}, \dots, e_n, v_n)$ de u a u, donde $u = v_0 = v_n$, ver Fig. 8.16. Si C no es un circuito simple, entonces $v_i = v_j$ para algún $i < j < n$. Se sustituye C por el circuito (verlo en el dibujo)

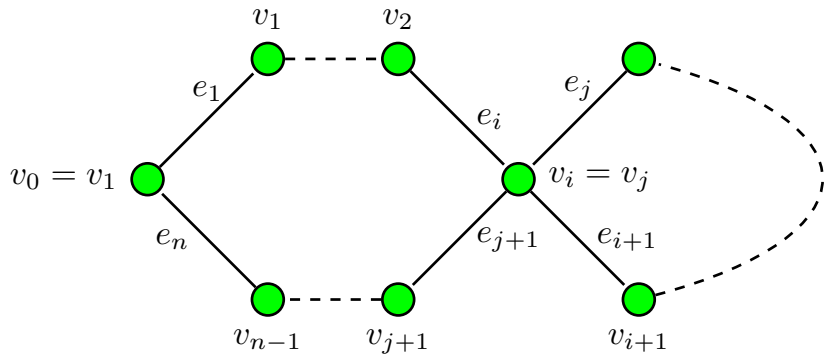

Figura 8.16: Un circuito C que, o bien es simple, o bien se puede reducir a un circuito simple.

$C' = (v_0, e_1, v_1, ..., e_i, v_i, e_{j+1}, ..., e_n, v_n)$. Si C' no resulta un circuito simple de v a v, entonces se repite este procedimiento recursivamente hasta obtener un circuito simple de u a u.

8.4. Caminos eulerianos y hamiltonianos

Caminos y circuitos de Euler

Definiciones. Sea un grafo $G = (V, E)$ y un vértice v cualquiera de G:

- *Circuito de Euler* (o *ciclo de Euler*) [CE]: un circuito de Euler en un grafo G es un circuito SIMPLE (circuito sin aristas repetidas de longitud mayor a cero), y que contiene a TODAS las aristas del grafo G;
- *Camino de Euler*: un camino de Euler es un camino SIMPLE (sin aristas repetidas) que contiene a TODAS las aristas de G.

Observación. Entre los textos de Johnsonbaugh (2005) y de Rosen (2004): hay diferencias sutiles en las definiciones, e.g. trayectoria, ciclo, trayectoria simple, ciclo simple, circuito de Euler, etc. De todos modos, cada libro es consistente pero atención cuando se interconsultan ambos textos.

Ejemplo. En la Fig. 8.17 se muestra el grafo G que describe el problema de los siete puentes de Königsberg, donde G no tiene un circuito de Euler ni un camino de Euler.

Ejemplo. En los grafos conexos trazados en la Fig. 8.18:

- En el grafo G_1 (izq.): un circuito de Euler es $C_1 = (v_1, v_5, v_3, v_2, v_5, v_4, v_1)$;
- En el grafo G_2 (med.): no tiene un circuito de Euler ni un camino de Euler;
- En el grafo G_3 (der.): no tiene un circuito de Euler, pero si un camino de Euler, e.g. $T_3 = (v_5, v_2, v_3, v_4, v_2, v_5, v_4)$.

Teorema. Sea $G = (V, E)$ un grafo, y los vértices u y v arbitrarios en G. Entonces (G tiene un circuito de Euler (CE)), ssi (G es conexo y todo vértice tiene grado par).
Demostración. Sean:

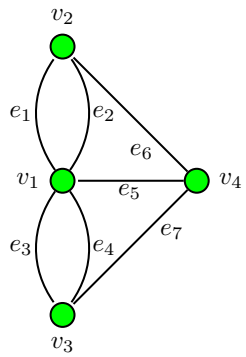

Figura 8.17: Grafo para el problema de los siete puentes de Königsberg: no tiene un circuito de Euler ni un camino de Euler.

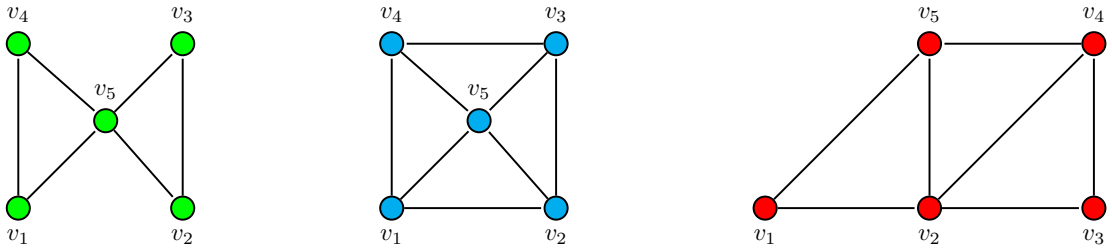

Figura 8.18: Grafo G_1 (izq.): con un circuito de Euler; grafo G_2 (med.): no tiene un circuito de Euler ni un camino de Euler; grafo G_3 (der.): no tiene un circuito de Euler, pero si un camino de Euler.

- p: el grafo $G = (V, E)$ tiene un Circuito de Euler (CE);
- q: el grafo $G = (V, E)$ es conexo y todo vértice tiene grado par.

(i) Si p entonces q:

- Suponga que G tiene un CE que empieza en un vértice u y continúa con una arista (u, x) incidente en u;
- La arista (u, x) contribuye con 1 al grado de u. Cada vez que el circuito pasa por un vértice subsiguiente v contribuye en 2 al grado de ese vértice, pues el circuito entra a v por una arista y sale por otra arista incidentes en v;
- Cuando el circuito vuelve al vértice inicial u, contribuye con otro 1 al grado de u. Por eso el grado $\delta(u)$ tiene que ser par puesto el circuito contribuye con 1 cuando comienza, con 1 cuando finaliza, y con 2 cada vez vez que pasa por u, si es que lo hace;
- Los demás vértices x tienen grado par porque el circuito contribuye con 2 en $\delta(x)$ cada vez que el circuito pasa por x;
- En definitiva, si G es conexo y tiene un CE, entonces todos sus vértices tienen grado par.

(ii) Si q entonces p:

- Suponga que G es un grafo conexo y que el grado de cada vértice es par;
- La tarea es formar un circuito simple C_0 a partir de un vértice arbitrario u de G, se elige una arista (u, x) adyacente a u arbitraria, continuamos construyendo un

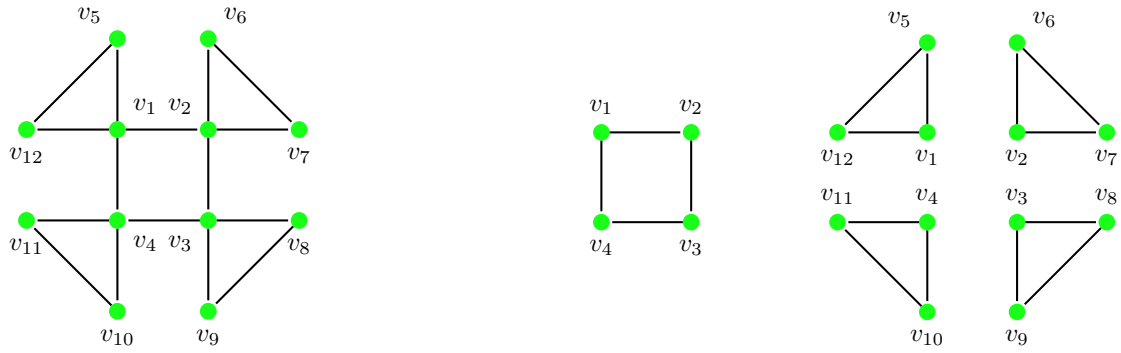

Figura 8.19: Un grafo $G(V, E)$ conexo donde todo vértice tiene grado par (izq.), puede descomponerse en $G = G_0 \cup H$, donde: (i) el subgrafo G_0 (centro) se obtiene con un circuito (arbitrario) $C_0 = (v_1, v_2, v_3, v_4$ a partir de un vértice (también arbitrario v_1, centro); y (ii) el subgrafo H (der.) que contiene la diferencia $G - G_0$. En general H resulta desconexo, como en este ejemplo con 4 circuitos: $C_1 = (v_1, v_{12}, v_5, v_1)$, $C_2 = (v_2, v_6, v_7, v_2)$, $C_3 = (v_3, v_8, v_9, v_3)$, y $C_4 = (v_4, v_{10}, v_{11}, v_4)$. Empero, la unión $C_0 \cup C_1 \cup C_2 \cup C_3 \cup C_4$ conduce a un circuito de Euler en G.

circuito simple (sin aristas repetidas), tomando todas las aristas que se puedan, e.g. $u = v_1$ en la Fig. 8.19;

- El circuito C_0 tiene que ser finito pues G tiene un número finito de aristas, comienza en una arista (u, x), y termina en otra arista (y, u), donde cada vez que el camino atraviesa un vértice, utiliza una arista cuando entra, otra arista cuando sale (que debe existir pues el grado de cada vértice es par);
- Tal vez el circuito C_0 hace uso de todas de las aristas o tal vez no, e.g. la Fig. 8.19 es un ejemplo en que no;
- Si se usaron todas las aristas, entonces se obtiene un CE, en caso contrario, se considera el subgrafo H obtenido de G al eliminar todas las aristas utilizadas en C_0 y los vértices no-incidentes en las aristas que sobreviven;
- Como G es conexo, entonces H tiene al menos un vértice w en común con el circuito eliminado C_0;
- Todos los vértice de H tienen grado par (pues todos los vértices de G son de grado par y en cada uno se eliminaron aristas por parejas para formar H). Tal vez H no resulte conexo, e.g. en la Fig. 8.19 se muestra un ejemplo en que no;
- En H se construye un circuito simple empezando en w eligiendo todas las aristas que se puedan, e.g. en la Fig. 8.19 con $w = v_1$ se obtiene un circuito C_1;
- Luego, formamos un circuito simple contatenando los circuitos C_0 y C_1, lo cual puede hacerse pues el vértice w es compartido por C_0 y por C_1;
- El proceso se repite hasta utilizar todas las aristas de G. Por ejemplo, en la Fig. 8.19 se obtienen sucesivamente los circuitos C_2, C_3, y C_4. Después, la unión de C_0, C_1, C_2, C_3, y C_4 conduce a un CE en G.

Teorema. Sea $G = (V, E)$ un grafo y dos vértices u y v cualesquiera de G, con $u \neq v$. Entonces (el grafo G tiene un camino euleriano entre u y v que contiene a todas las aristas y vértices), ssi (G es conexo y los únicos vértices de grado impar son u y v).
Demostración. Sean:

- p: el grafo G tiene un camino euleriano entre u y v que contiene a todas las aristas y

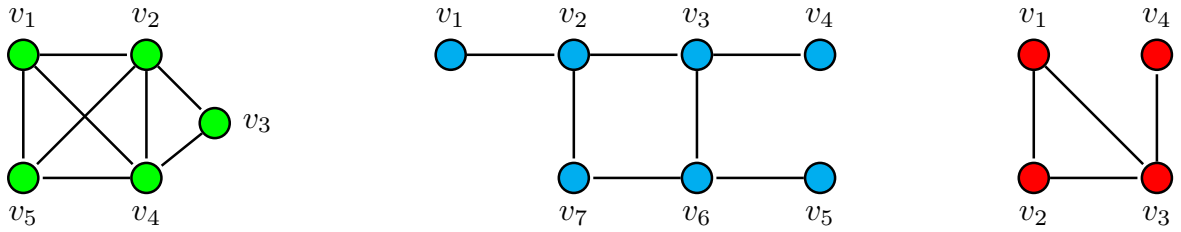

Figura 8.20: Grafo G_1 (izq.): con un circuito de Hamilton y con un camino de Hamilton; grafo G_2 (med.): no tiene un circuito de Hamilton ni un camino de Hamilton; grafo G_3 (der.): no tiene un circuito de Hamilton, pero si un camino de Hamilton.

vértices;
- q: el grafo G es conexo y los únicos vértices de grado impar son u y v;

Demostración:

(i) Si p entonces q:
- Suponemos que G tiene un camino euleriano P (todas las aristas sin repetir) de u a v que contiene a todas las aristas y vértices, por eso G debe ser conexo;
- Si se agrega una arista (u, v) se obtiene el grafo G' el cual admite un circuito de Euler uniendo el camino P junto con la arista agregada (u, v);
- Por teorema de Euler cada vértice tiene grado par, por lo que al eliminar la arista agregada solo afecta a los grados de u y v, que se reducen en 1;
- Por eso, en el camino original los vértices u y v tienen grado impar y los demás otros tienen grado par.

(ii) Si q entonces p:
- Suponemos que el grafo G es conexo y tiene exactamente dos vértices u y v de grado impar;
- Provisoriamente se agrega la arista $e = (u, v)$ resultando el grafo G' que es conexo donde cada vértice tiene grado par;
- Por teorema de Euler G' tiene un CE. Luego, al eliminar la arista e de este CE, se obtiene un camino simple (sin aristas repetidas) de u a v que contiene todas las aristas y vértices de G.

Caminos y circuitos de Hamilton

Definición. Sea un grafo $G = (V, E)$, y un vértice u cualquiera de G:

- *Circuito de Hamilton* (o ciclo de Hamilton) [CH]: un circuito de Hamilton es un circuito simple (circuito sin aristas repetidas de longitud mayor a cero), que contiene a TODOS los vértices de G;
- *Camino de Hamilton* [TH]: es un camino que pasa por cada vértice de G exactamente sólo una vez.

Ejemplo. En los grafos conexos trazados en la Fig. 8.20:

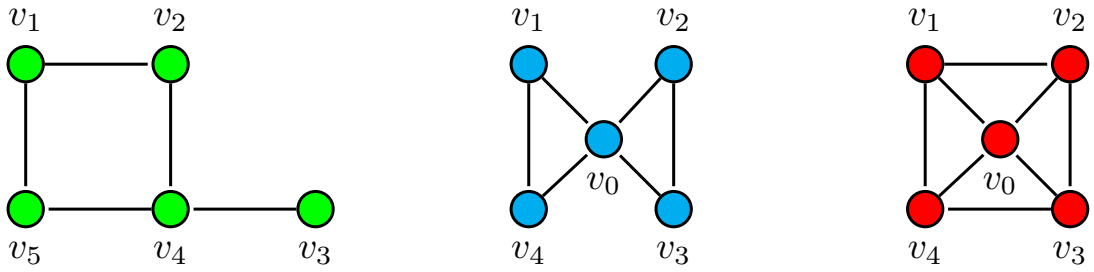

Figura 8.21: Grafo G_1 (izq.) y grafo G_2 (cen.): ninguno tiene un circuito de Hamilton. Pero el grafo G_3 (der.) sí tiene un circuito de Hamilton.

- En el grafo G_1 (izq.): un circuito de Hamilton es $C_1 = (v_1, v_2, v_3, v_4, v_5, v_1)$, y un camino de Hamilton es $T_3 = (v_1, v_2, v_3, v_4, v_5)$;
- En el grafo G_2 (med.): no tiene circuito de Hamilton, ni camino de Hamilton;
- En el grafo G_3 (der.): no tiene un circuito de Hamilton, pero si un camino de Hamilton, e.g. $T_3 = (v_1, v_2, v_3, v_4)$.

Observación. Sobre la existencia de los circuitos de Hamilton:

- No se conoce una manera sencilla de determinar si un grafo G tiene un circuito o un camino de Hamilton, lo cual contrasta fuertemente con la tarea de determinar si un grafo tiene un circuito de Euler porque ahí, simplemente, aplicamos el teorema de Euler. Es decir, para determinar la existencia de los circuitos de Hamilton en G no se conocen criterios simples (necesarios y suficientes);
- Sin embargo, se conocen diversos resultados parciales que dan condiciones suficientes para la existencia de los circuitos de Hamilton;
- Por otra parte, ciertas propiedades pueden usarse para mostrar que un grafo G no tiene un circuito de Hamilton. Por ejemplo:
  - Un grafo con un vértice de grado 1 no puede tener un circuito de Hamilton, porque en un circuito de Hamilton cada vértice es incidente en otros dos vértices del circuito;
  - Si un vértice en el grafo G tiene grado 2, entonces ambas aristas que inciden con ese vértice deben ser parte de cualquier circuito de Hamilton;
  - Cuando se va construyendo un circuito de Hamilton y el mismo ha pasado a través de un vértice, entonces todas las aristas incidentes en ese vértice que no se usaron (distintas de las dos utilizados en el circuito que se intenta construir), pueden ser eliminadas en la subsiguiente búsqueda;
  - Un circuito de Hamilton no puede contener otro circuito de Hamilton más pequeño dentro del mismo.

Ejemplo. En los grafos conexos trazados en la Fig. 8.21:

- En el grafo G_1 (izq.): no tiene un circuito de Hamilton porque G_1 tiene un vértice de grado 1;
- En el grafo G_2 (cen.): los vértices v_1, v_2, v_3, v_4 tienen grado 2, por lo que las aristas incientes en esos vértices deben ser parte del circuito de Hamilton, pero entonces

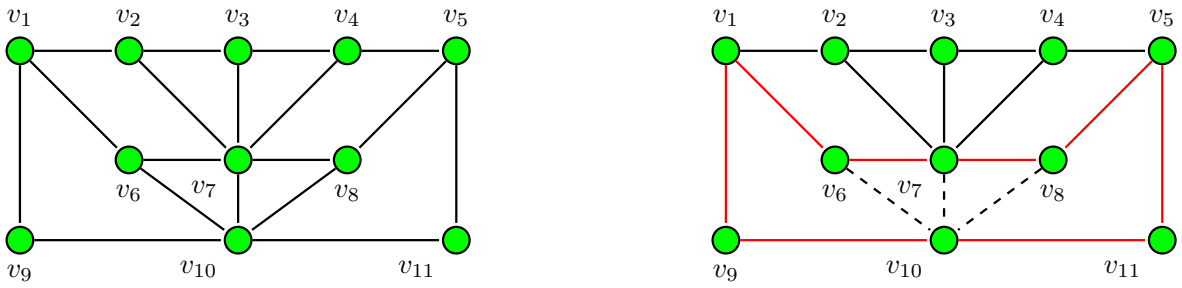

Figura 8.22: Grafo G (izq.). Se traza un circuito C en G (en rojo a la der.): todos sus vértices tienen grado 2, pero al intentar agregar una arista algún vértice v pasa a $\delta(v) > 2$, por lo que G no tiene un CH.

todo CH debe tener las 4 aristas incidentes en v_0, entonces hay que pasar dos veces por v_0. Por eso, G_2 tampoco tiene un circuito de Hamilton;
- En cambio, en el grafo G_3 (der.): un circuito de Hamilton es $C_1 = (v_1, v_2, v_3, v_4, v_0, v_1)$.

Ejemplo. En el grafo conexo G trazado en la Fig. 8.22 (izq.):

- Como v_9 tiene grado 2, sus aristas incidentes (v_9, v_1) y (v_9, v_{19}) son parte del CH que se intenta trazar, marcadas en rojo en la Fig. 8.22 (der.);
- Como v_{11} tiene grado 2, sus aristas incidentes (v_{11}, v_{10}) y (v_{11}, v_5) también son parte del CH que se intenta trazar, marcadas en rojo en la Fig. 8.22 (der.);
- Dado las dos aristas ocupadas en v_{10}, las restantes aristas incidentes en v_{10} no pueden estar en el CH que se intenta trazar, marcado en punteado en la Fig. 8.22 (der.);
- Entonces, las aristas (v_1, v_6), (v_6, v_7), y (v_7, v_8), (v_8, v_5), también deben estar en el CH, con lo que resulta el circuito C trazado en la Fig. 8.22 (der.);
- Ahora, al intentar alguna arista adicional a C, se obtiene un circuito con algún vértice v con grado $\delta(v) > 2$, lo que no es posible en un CH. Por eso, este grafo no tiene un CH.

8.5. Algoritmo de Dijkstra

Caminos de longitud mínima

- Algoritmo de Dijkstra (o caminos de longitud mínima). El Algoritmo de Dijkstra (AD) permite encontrar un camino de menor peso (o Ruta de Peso Mínimo (RPM)) entre dos vértices v_A y v_Z cualesquiera en un grafo ponderado $G = (V, E, W)$, donde V es el conjunto de vértices, V es el conjunto de aristas, y W es el conjunto de los pesos de las aristas (números no-negativos);
- Contiene una modificación simple al algoritmo básico admite grafos G no-conexos (ver mas abajo, es ejercicio de la GTP, y re-clásica pregunta en examen), resultando un Algoritmo de Dijkstra Modificado (ADM);
- El ADM asigna una etiqueta $L(v)$ a cada vértice v. En cada iteración, algunos vértices tienen etiquetas *temporales* y otros tienen etiquetas *permanentes*;

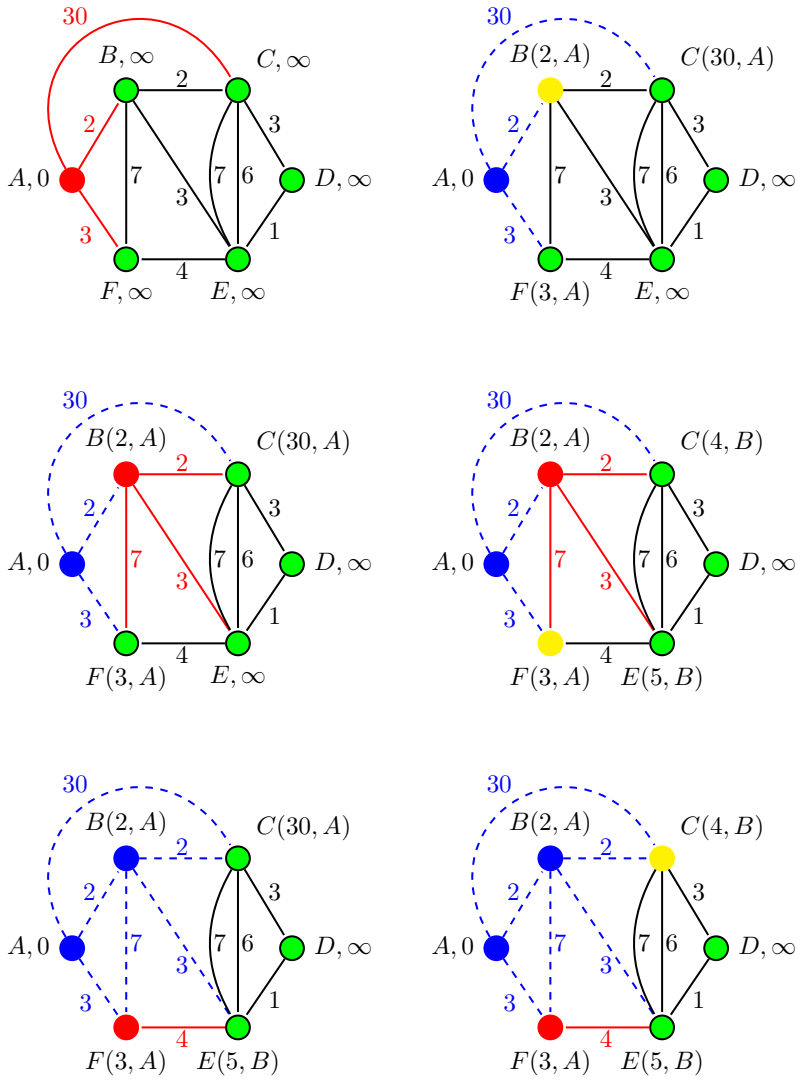

Figura 8.23: El AD para hallar una RPM desde el vértice A hacia el D. Vértice de peso mínimo u elegido y aristas adyacentes a u (en rojo) [izq.]. Eventual cambio de los pesos de los vértices adyacentes a u, y siguienteo vértice de peso mínimo (en amarillo) [der.].

- Sean S es el conjunto de vértices con etiquetas *permanentes*;
- Se puede demostrar que si $L(v)$ es la etiqueta permanente del vértice v, donde $v \in S$, entonces $L(v)$ es la longitud de una RPM desde v_A hacia v;
- Al inicio, como *condición inicial* para todo el grafo, el vértice de partida v_A tiene etiqueta temporal 0, y los demás vértices tienen etiquetas temporales ∞;
- En el caso en que los vértices de partida v_A y de llegada v_Z están en una misma componente conexa, el AD terminará cuando el vértice de llegada v_Z se le asigne una etiqueta *permanente*. Cuando eso ocurre, $L(v_Z)$ es la longitud de una RPM desde v_A hacia v_Z. En ese caso, como verificación en examen, $L(v_Z)$ debe coincidir con la suma de los pesos de todas las aristas de la RPM hallada.
- El algoritmo dado en Rosen para la búsqueda a lo ancho puede re-escribirse como:

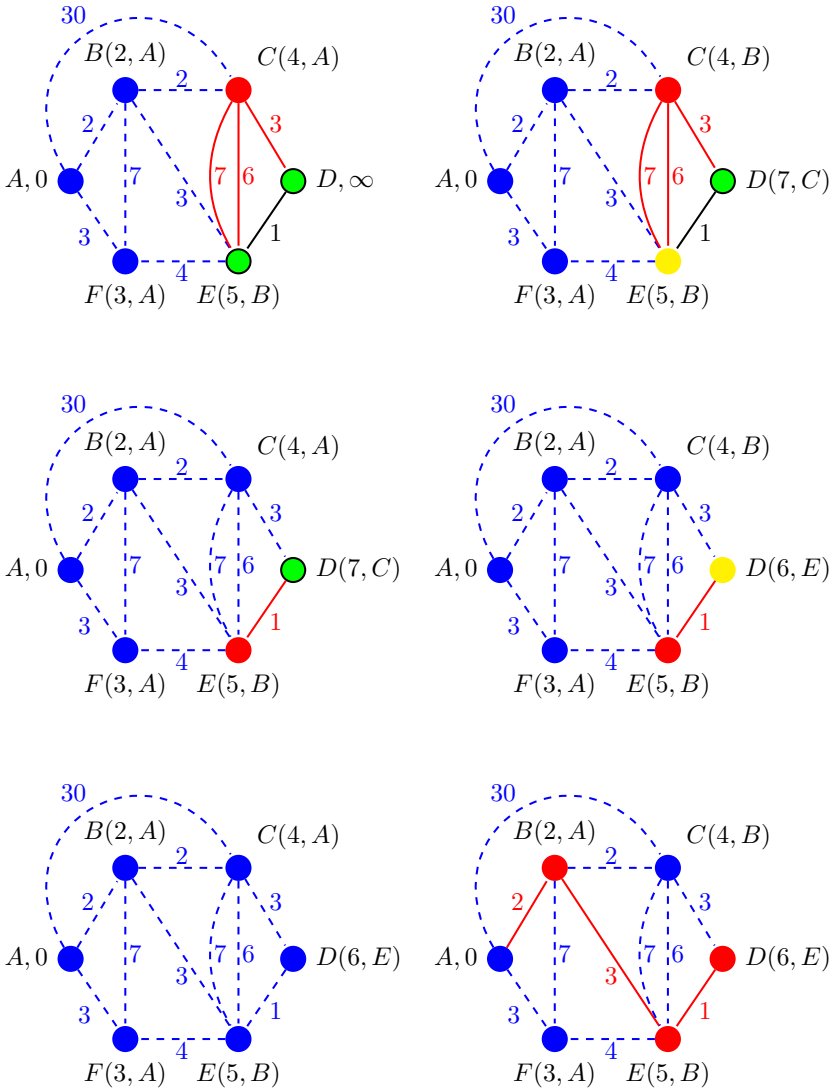

Figura 8.24: El AD para hallar una RPM desde el vértice *A* hacia el *D*: continuación de la Fig. 8.23.

```
1  def dijkstra (G, v_A, v_Z):      # grafo ponderado G(V,E,W),
2     # inicializa                  # vertice de partida v_A, y
3     for u := 1 to n:             # vertice de llegada v_Z
4        L (u) := infinito         # todos los vertices
5     #end for                     # con peso infinito
6     L (v_A) := 0                 # peso 0 en vertice de partida v_A
7     S       := vacio             # lista de vertices de peso minimo
8     while (True):
9        #busca un vertice de peso minimo
10       elije un vertice u de peso L (u) minimo
11       if   (u == infinito):     # no hay ruta entre v_A y v_Z
12          return error           # aborta
13       elif (u == v_Z):          # llega al vertice de llegada v_Z
14          return (S,L)           # termina OKI
15       #end if
16       #agrega vertice en S
17       agregar_vertice (u,S)     # agrega u en S
```

```
18        L := V - S                  # vertices que no-estan en S
19        for v en L:                 # recorre solo esos vertices
20            cta := L(u) + W(u,v)    # peso vertice u min + peso arista
21            if (test < L(v)):       # es menor
22                L(v) := cta         # actualiza
23            #end if                 # y que no-forme ciclo
24        #end for
25    #end while
26 #end dijkstra
```

En cada iteración del ADM se cambia el estado de alguna etiqueta de vértice de temporal a permanente de la siguiente manera:

- En el grafo iterado se busca el vértice temporal u con peso $L(u)$ mínimo y se lo pasa a S, (como vértice con peso permanente, en color rojo en la Fig. del ejemplo siguiente);
- Si $u = v_Z$, entonces fin del ADM, retornando $L(v_Z)$ y S con la RPM;
- En cambio, si el peso del vértice u es $L(u) = \infty$, entonces se aborta;
- En otro caso, para todos los vértices v que no-están en S se hace la cuenta test

$$L_{\text{test}}(v) = L(u) + L[(u, v)] \tag{8.12}$$

  y, solo si es menor que el peso actual $L(v)$, entonces se cambia $L(v)$ con el peso test $L_{\text{test}}(v)$;
- Además, para recordar de donde provino el cambio del peso y poder re-construir la RPM, se recuerda en el vértice v al vértice u que ocasionó el decremento mediante la dupla $(L_{\text{test}}(v), u)$.

En el caso cuando el $L(u)$ mínimo resulta infinito se tiene:

- Dado que existe al menos un camino entre cada par de vértices ubicados dentro de una misma Componente Conexa (CC), el test de la Ec. (8.12) siempre dispondrá de vértices adyacentes, y cambiará gradualmente los pesos iniciales ∞ de algunos vértices por otros valores menores;
- Si los vértices de partida v_A y de llegada v_Z están en una misma CC, entonces existe al menos un camino entre v_A y v_Z, por lo que siempre habrán vértices adyacentes disponibles para el test de la Ec. (8.12);
- Como entre CC diferentes no hay aristas que las vinculen, el test de la Ec. (8.12) no-podrá cambiar los pesos temporales de los vértices ubicados en otras CC;
- Cuando todos los vértices disponibles en la CC del vértice de partida v_A se eligieron como vértices de peso mínimo, y ninguno corresponde al de llegada v_Z, en la siguiente iteración se elegirá un vértice ubicado en otra CC;
- Pero, como no hay conexión entre la CC del v_A y las restantes CC, entonces todos los vértices temporales de las restantes CC mantuvieron el peso inicial ∞;
- Entonces, cuando se elige un vértice u con peso $L(u) = \infty$, se está eligiendo por primera vez un vértice ubicado en otra componente conexa, y por eso no será posible continuar.

Ejemplo. En el grafo conexo G trazado en la Fig. 8.23 (arriba-izq.), encontrar una RPM desde el vértice A hacia el D. Solución: el desarrollo del AG se muestra con los grafos trazados en las Figs. 8.23-8.24. Luego de finalizar, una RPM es $R = (D, G, B, A)$, y su

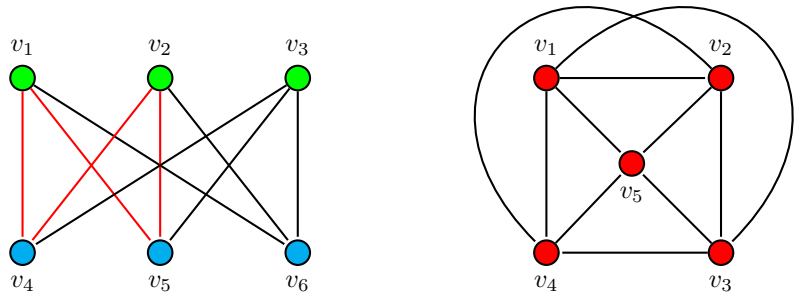

Figura 8.25: El grafo bipartito completo $K_{3,3}$ (izq.) y el completo K_5 (der.) no son grafos planos.

peso es $L(D) = 5$, y se marca en rojo en la Fig. 8.24 (abajo-derecha). Se verifica que $L(D) = 1 + 3 + 2 = 5$, i.e. es igual a la suma de los pesos $L[(D, E)]$, $L[(E, B)]$, y $L[(B, A)]$ de esas aristas.

Nota. En los ejercicios con algoritmos de grafos:

- Use orden alfabético cada vez que se pueda, utilizado en estas notas, y que es el criterio empleado en el texto de Johnsonbugh pero ausente en el de Rosen;
- Se admiten 3 alternativas:
  1) Un dibujo del grafo por cada iteración que precise el orden en que se van eligiendo las aristas o los vértices, e.g. como se hizo en las Figs. 8.23-8.24;
  2) Un único gran dibujo del grafo, ocupando toda la página, empleando el etiquetado dado en las prácticas:
     - En cada iteración k y en cada vértice v se indica la etiqueta $(p, e)_k$, donde p es el peso del vértice v desde el cual se llega, e es la etiqueta del vértice desde el cual proviene, y el subíndice k es la iteración;
     - Las etiquetas se escriben incluso cuando el peso p con el que llegan al vértice v en la iteración k no es menor, en cuyo caso se escribe la etiqueta $(p, e)_k$ y después se la tacha, excepto aquella etiqueta con el menor peso para llegar al vértice en cuestión;
  3) Una tabla completa, en el estilo de los textos de Johnsonbaugh y Rosen, que liste cada iteración.

  Puede haber cierta preferencia por la alternativa 1 en parte porque puede resultar más rápida de trazar y de revisar por eventuales errores antes de entregar. Sólo hay que lograr cierta soltura en dibujar en forma expeditiva.

El problema del viajante

Omitir (alumnos de FICH lo verá en AED, y los de FIQ quizás nunca).

8.6. Grafos planos (nociones)

Definición.

Figura 8.26: Subdivisión elemental: de izq. a der.; suavizado (o alisado): de der. a izq.

Figura 8.27: Los grafos G_1 (izq.) y G_2 (der.) son homomorfos: G_2 puede obtenerse de G_1 con 2 subdisiones elementales, y G_1 puede obtenerse de G_2 con 2 suavizados.

- Grafo *plano*: un grafo $G = (V, E)$ conexo y simple (simple: no hay lazos ni aristas paralelas), es un grafo *plano* si puede trazarse sobre una superficie sin que se crucen sus aristas;
- *Cara* o *región* f: es cada una de las regiones contiguas en que queda dividida una superficie por un grafo plano (incluyendo la región no-acotada), y queda delimitada por el ciclo de frontera;
- Cara exterior (o región exterior): está definida por la región no-acotada;
- Grado de una cara G_f (o región G_r): es igual al número de aristas que hay en el ciclo de frontera;
- En un grafo plano, cada arista pertenece al menos a 2 ciclos frontera (e.g. verlo en K_3);
- *Fórmula de Euler* (FE) para un grafo plano: si G es un grafo conexo, simple, y plano, tiene v vértices, e aristas, y f caras, entonces se verifica que:

$$f = (e - v) + 2 \tag{8.13}$$

  esto es: todas las representaciones planares de un grafo dividen al plano en un mismo número de regiones.

Ejemplo. Los grafos G_1 y G_2 mostrados en la Fig. 8.27 son homomorfos porque mediante subdisiones elementales se reducen a G'.

Observación.

- El grafo completo K_4 (Fig. 8.10, arriba), y el hipercubo Q_3 (Fig. 8.10, abajo), son grafos planos;
- El grafo bipartito completo $K_{3,3}$ no es plano. Demostración:
  - Los ciclos en el grafo bipartito completo $K_{3,3}$ tienen al menos longitud 4, e.g. ver ciclo (v_1, v_3, v_2, v_1) trazado en color rojo en Fig. 8.25 (izq.);
  - Entonces cada cara en $K_{3,3}$ estará delimitada al menos por 4 aristas, y el número e_f de aristas que acotan las caras debe ser $e_f \geq 4f$;

- En un grafo plano, cada arista contribuye en 2 al grado de cada cara, por lo que $e_f = 2e$ (donde e es el número total de aristas en G);
- *Suponiendo* que $K_{3,3}$ *fuera* plano, podemos introducir la FE dada por la Ec. (8.13):

$$\begin{aligned} e_f &\geq 4f \\ e_f &= 2e \end{aligned} \quad \therefore \quad 2e \geq 4f = 4(e - v + 2) \tag{8.14}$$

Como en $K_{3,3}$ hay $v = 6$ vértices, y $e = 9$ aristas, resulta

$$\begin{aligned} 2(9) &\geq 4(9 - 6 + 2) \\ 18 &\geq 20 \end{aligned} \tag{8.15}$$

lo que no es posible, por lo que $K_{3,3}$ debe ser un grafo no-plano;

- También se puede demostrar que el grafo completo K_5 tampoco es plano, ver Fig. 8.25;
- Además, si un grafo G contiene a $K_{3,3}$ o a K_5 como subgrafos, entonces G no puede ser un grafo plano.

Definiciones.

- Aristas *en serie*: si un grafo $G = (V, E)$ tiene un vértice v de grado 2, y aristas (v, v_1) y (v, v_2), con $v_1 \neq v_2$, se dice que las aristas (v, v_1) y (v, v_2) están en *serie*;
- *Subdivisión elemental* (en Rosen) o *reducción de una serie* (en Johnsonbaugh): consiste en eliminar el vértice v, y sustitur las aristas (v, v_1) y (v, v_2), con (v_1, v_2), ver Fig. 8.26, yendo de izq. a der.;
- *Suavizado* (o *alisado*): es la operación inversa de la anterior, i.e. introducir el vértice v, y sustitur la arista (v_1, v_2) con (v, v_1) y (v, v_2), ver Fig. 8.26, yendo de der. a izq.;
- Se dice que los grafos G_1 y G_2 son un *homomorfismo* si G_1 y G_2 se pueden obtener mediante una serie de subdivisiones elementales.

Teorema de Kuratowski: un grafo G no-es plana, ssi G contiene un subgrafo homomorfo a $K_{3,3}$ o a K_5.

CAPÍTULO 9

Arboles

Nota. Estas notas siguen el texto de referencia Rosen (2004) manteniendo la numeración de las secciones y sus títulos, como una referencia adicional para el auto-estudio siguiendo ese texto.

Contents

9.1. Intro a árboles

Definiciones.

- *Arbol*: un árbol T (por *Tree*) es un grafo $G = (V, E)$ simple (sin lazos ni aristas paralelas), que además es conexo y sin circuitos;
- *Arbol con raíz*: un árbol con raíz es un árbol T en donde un vértice cualquiera ha sido designado como vértice raíz (o simplemente raíz), de modo tal que todas las aristas se miran desde la raíz.

Teorema. (Un grafo $T = (V, E)$ es un árbol) ssi (existe un UNICO camino entre cada par de vértices).

Demostración. El ssi se desdobla en 2 implicaciones. Sean: p : el grafo T es un árbol, y q : existe un único camino entre cada par de vértices, con lo que:

(i) Si T es un árbol, entonces T es un grafo conexo sin circuitos. Sean los vértices u y v. Puesto que T es conexo, entonces existe al menos un camino entre u y v. Si hubiera un segundo camino, entonces combinando el primer camino de u a v, y el segundo camino de v a u, entonces se obtendría un circuito, lo que implica que habría

un circuito en T, pero eso no es posible, por eso se concluye que: si T es un árbol, entonces existe un único camino entre cada par de vértices;

(ii) Si existe un único camino entre cada par de vértices u y v de T, entonces T no puede tener un circuito ¿Por qué? Rpta: porque si T tuviera un circuito que contuviera a los vértices u y v, entonces habría un camino de u a v, y otro camino de v a u, con lo que se tendrían dos caminos entre u y v.

Definiciones. Sean T un árbol con vértice raíz v_0, v es un vértice de T distinto de v_0. Entonces:

- Vértice *padre*: el vértice *padre* de v es el UNICO vértice u de T tal que existe una arista entre u y v;
- Vértice *hijo*: cuando u es el vértice *padre* de v, se dice que v es el vértice *hijo* de u;
- Vértices *hermanos*: los vértices *hermanos* son TODOS los vértices con un mismo vértice padre u;
- Vértices *antecesores*: los vértices *antecesores* de un vértice v distinto del vértice raíz v_0, son TODOS los vértices del único camino a la raíz v_0, excluyendo al vértice v e incluyendo a la raíz v_0 (i.e. los antecesores de v es el padre de v, y el padre del padre, y así sucesivamente hasta llegar a la raíz);
- Vértices *descendientes*: los vértices *descendientes* de un vértice v son todos los vértices tales que v es un antecesor;
- Vértice *hoja*: es un vértice sin hijos;
- Vértice *interno*: es un vértice con hijos. Obs.: si el vértice raíz v_0 tiene hijos, entonces también es un vértice interno, sino es un vértice hoja;
- *Subárbol*: si u es un vértice de T, entonces el subárbol con vértice raíz u que contiene al vértice u, a todos sus descendientes, y a las aristas incidentes en los mismos, es el *subárbol* con vértice raíz u;
- *Arbol con raíz m-ario*: un árbol con raíz m-ario es un árbol con raíz donde todos sus vértices internos tienen, a lo sumo, m hijos;
- *Arbol binario*: un árbol binario es un árbol con raíz m-ario donde $m = 2$;
- *Arbol con raíz m-ario completo*: un árbol con raíz m-ario completo es un árbol con raíz m-ario donde todos sus vértices internos tienen exactamente m hijos;
- *Arbol ordenado con raíz*: un árbol ordenado con raíz en el que los hijos están ordenados. Se los dibujan de modo tal que los hijos de cada vértice interno se colocan ordenados de izquierda a derecha. Obs.: lo anterior implícitamente define un orden para las aristas;
- *Hijo izquierdo e hijo derecho*, y *subárbol izquierdo y subárbol derecho*: en un árbol binario ordenado (usualmente denominado simplemenente árbol binario) si cada vértice interno tiene dos hijos, entonces el primer hijo es el hijo izquierdo, y el segundo hijo es el hijo derecho. El subárbol con raíz en el hijo izquierdo es el *subárbol izquierdo*, y el subárbol con raíz en el hijo derecho es el *subárbol derecho*, y Obs.: un árbol binario puede faltar uno de los hijos.

Arboles como modelos

Lectura optativa:

- Ejemplo 5: hidrocarburos saturados y árboles.
- Ejemplo 6: representaciones de organizaciones.
- Ejemplo 7: sistema de archivos en una compu.
- Ejemplo 8: micros en cómputo paralelo conectados en árboles.

Propiedades de los árboles

Teorema. Un árbol de n vértices tiene $(n-1)$ aristas, para cualquier entero n positivo. Demostración. Usando PIM se tiene:

- PB ($n = 1$): un árbol con un vértice no tiene aristas. Por otro lado: si $n = 1$ entonces $n - 1 = 0$, con lo cual se verifica el PB.
- PI. Asumimos que la HI: un árbol con k vértices tiene $(k-1)$ aristas, es T para algún entero k positivo. Sea T árbol con $(k+1)$ vértices, y sean v una hoja cualquiera de T (que existe si T es finito), y w es su padre. Al eliminar de T tanto a la hoja v como a la arista (v, w) se obtiene un subárbol T' de k vértices, conexo y acíclico. Por HI, T' tiene $(k-1)$ aristas. Como T tiene una arista más que T', i.e. la arista eliminada (v, w), se tiene que T tiene k aristas.
- Finalmente, como se cumple el PB y el PI, el PIM asegura que se cumple el enunciado para todos los enteros $n > 0$.

Propiedades de los árboles m-arios completos

Teorema. Sea un árbol m-ario completo T con I vértices internos, M hijos en cada vértice interno, entonces tiene $N = MI + 1$ vértices en total. Demostración:

- Todo vértice excepto la raíz es hijo de algún vértice interno;
- Cada uno de los I vértices internos tiene M hijos, por lo que hay MI vértices sin contar la raíz,
- Agregando la raíz, en total hay $MI + 1$ vértices.

Obs.: cuando en un árbol m-ario completo T se conoce alguno de los enteros N (vértices), I (vértices internos), M (hijos en cada vértice interno), L (hojas), entonces los otros dos quedan definidos. Para hallarlos:

Teorema. Sea T un árbol m-ario completo:

1) Si se sabe que tiene N vértices, entonces tiene

$$\begin{aligned} I &= (N-1)/M && \text{vértices internos} \\ L &= [(M-1)N+1]/M && \text{hojas} \end{aligned} \tag{9.1}$$

2) Si se sabe que tiene I vértices internos, entonces tiene

$$\begin{aligned} N &= NM+1 && \text{vértices} \\ L &= [(M-1)I+1 && \text{hojas} \end{aligned} \tag{9.2}$$

3) Si tiene L hojas, entonces tiene

$$\begin{array}{ll} N = (ML-1)/(M-1) & \text{vértices} \\ I = (M-1)/(L-1) & \text{vértices internos} \end{array} \tag{9.3}$$

Demostración:

1) Del teor. anterior se sabe que cuando T es un árbol m-ario completo T con I vértices internos, y M hijos en cada vértice interno, entonces tiene $N = MI + 1$ vértices en total. Además, como cada vértice es, o bien una hoja, o bien un vértice interior, se tiene $N = L + I$. Luego

$$\begin{array}{lll} N = MI + 1 & \therefore & I = (N-1)/M \\ N = L + I & \therefore & L = N - I \\ L = N - (N-1)/M & \therefore & L = ((M-1)N + 1)/M \end{array} \tag{9.4}$$

2) Para el hogar;
3) Para el hogar.

Definiciones. Sean T un árbol con vértice raíz v_0, mientras que v es un vértice de T distinto de v_0. Entonces:

- *Nivel*: el nivel de un vértice v es la longitud del único camino desde la raíz v_0 a v. Obser.: la raíz v_0 tiene nivel 0;
- *Altura*: la altura de un árbol T con raíz v_0, es el máximo nivel;
- *Arbol equilibrado (o balanceado)*: un árbol con raíz v_0 y altura H está equilibrado (o balanceado) cuando todas sus hojas están en los niveles H o $H-1$.

Teorema. Un árbol m-ario de altura H tiene, a lo sumo, $L = M^H$ hojas, para cualquier entero H positivo. Demostración. Usando PIM en la altura k, se tiene:

- PB ($k = 1$): un árbol m-ario de altura 1, que es un árbol con una sola raíz con, a lo suma, M hijos, los cuales todos son hojas. Por eso, no hay más de $L = M^1$ hojas en un árbol m-ario de altura 1.
- PI. Asumimos que la HI: un árbol m-ario de altura k tiene, a lo sumo, M^k hojas. es T para un entero k positivo, arbitrario pero fijo. Sea T árbol m-ario de altura $k+1$. Las hojas de T son las hojas de los subárboles de T obtenidos al eliminar las aristas que conectan la raíz de T con los vértices del nivel 1. Cada uno de los subárboles de T tiene altura menor o igual a k. Por la HI, cada uno, tiene a lo sumo, M^k hojas. Pero, a lo sumo, hay M de estos subárboles, cada uno con un máximo de M^k hojas, hay M^{k+1} hojas como máximo en el árbol m-ario de altura $k+1$;
- Finalmente, como se cumple el PB y el PI, el PIM asegura que se cumple el enunciado para todos los enteros $H > 0$.
- Corolario 1: si un árbol m-ario de altura H tiene L hojas, entonces $H \geq \lceil \log_M(L) \rceil$. Caso especial: cuando $M = 2$ (árbol binario) es $H \geq \lceil \log 2(L) \rceil$;
- Corolario 2: si un árbol m-ario de altura H es completo y equilibrado y tiene L hojas, entonces $H = \lceil \log_M(L) \rceil$.

9.2. Aplicaciones de los árboles

Arboles binarios de búsqueda

Omitir (la gente de FICH lo verá en AED, y la de FIQ en COP (quizás o nunca).

Arboles de decisión

Omitir (la gente de FICH algo verá en AED).

Códigos de Huffman (o códigos instantáneos)

Es la antesala de los *zipeadores* (o compresores): omitir pues la gente de FICH lo verá en AED.

Arboles de juegos

Es la antesala de ciertos tipos de juegos: omitir!

9.3. Recorridos en árboles

Observación. La "forma práctica" (con lápiz y papel) bastará en las evaluaciones para todos los algoritmos. En particular:

- Listado preorden;
- Listado inorden (o enorden, o entreorden);
- Listado postorden.

Sistema de rotulado universal

Para recorrer todos los vértices de un árbol ordenado con raíz necesitamos ordenar todos los hijos. En el papel los hijos se dibujan de izquierda a derecha pero, en general, hace falta rotular (o etiquetar) todos los vértices. Para tal fin utilizamos el siguiente esquema recursivo:

1) Rotulamos la raíz con el entero 0. Luego, rotulamos sus k hijos (del nivel 1), de izquierda a derecha, con los enteros 1, 2, 3, ..., k;
2) Para cada vértice v del nivel n con etiqueta A, rotulamos sus k_v hijos, de izquierda a derecha, como $A.1$, $A.2$, ..., $A.k_v$.

Algoritmos de recorrido

Los recorridos sistemáticos de todos los vértices de un árbol ordenado con raíz se llaman algoritmos de recorrido de un árbol, los cuales son recursivos. Mencionamos 4 recorridos: en preorden, en inorden (o enorden, o entreorden), en postorden, y por niveles. Omitiremos el cuarto pues la gente de FICH lo verá en AED, mientras que los de FIQ nunca, así nos restringiremos a los 3 primeros. Primero daremos una "forma práctica" (con lápiz y

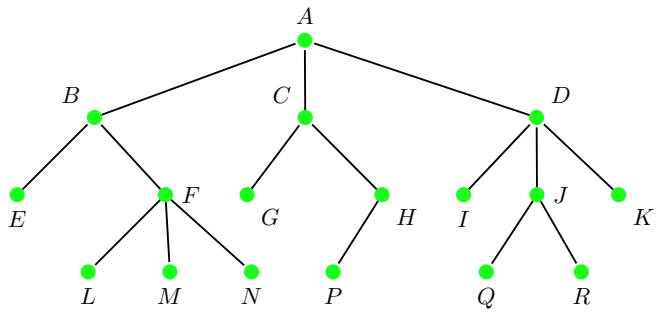

Figura 9.1: Un árbol m-ario ordenado $T = (V, E)$ con raíz en el vértice A. Los recorridos preorden, inorden, y postorden son dados en el texto.

papel), que bastará en las evaluaciones y, a continuación, las definiciones recursivas y los algoritmos de cada uno.

Observación. Listados preorden, inorden, y postorden: una "forma práctica" (con lápiz y papel) es listar los vértices del árbol ordenado T con raíz r de la siguiente manera:

- Listado *preorden*: empezar en el vértice raíz r de T, si es hoja entonces listarlo, sino recorrer T siguiendo sus ramas **de izquierda a derecha**, y listar cada vértice v la **primera** vez que se lo visita;
- Listado *inorden* (o *enorden* o *entreorden*): empezar en el vértice raíz r de T, si es hoja entonces listarlo, sino recorrer T siguiendo sus ramas **de izquierda a derecha**, y listar cada vértice v la **segunda** vez que se lo visita;
- Listado *postorden*: empezar en el vértice raíz r de T, si es hoja entonces listarlo, sino recorrer T siguiendo sus ramas **de derecha a izquierda**, y listar cada vértice v la **primera** vez que se lo visita.

Observación. En libros de texto es más frecuente la siguiente forma del *postorden*:

- Listado *postorden* (versión alternativa): empezar en el vértice raíz r de T, si es hoja entonces listarlo, sino recorrer T siguiendo sus ramas **de izquierda a derecha**, y listar cada vértice v la **última** vez que se lo visita;
- Notar que es completamente equivalente a la versión anterior.

Ejemplo. [lo usual en evaluaciones] En el árbol m-ario ordenado $T = (V, E)$ con raíz r trazado en la Fig. 9.1 listar todos sus vértices utilizando los recorridos: preorden, inorden, y postorden. Solución: a partir de la Fig. 9.1 se tiene:

$$\begin{aligned} L_{\text{preorden}} &= \{A, B, E, F, L, M, N, C, G, H, P, D, I, J, Q, R, K\} \\ L_{\text{inorden}} &= \{E, B, L, F, M, N, A, G, C, P, H, I, D, Q, J, R, K\} \\ L_{\text{postorden}} &= \{E, L, M, N, F, B, G, P, H, C, I, Q, R, J, K, D, A\} \end{aligned} \tag{9.5}$$

Definición. Recorrido en preorden. Sea T un árbol ordenado con raíz r. Entonces:

- Si T consta sólo de r, entonces r es el recorrido en preorden de T;
- En otro caso, sean $T_1, T_2, ..., T_p$ los p subárboles de r, listados de izquierda a derecha, en T. El recorrido en preorden comienza visitando r, continúa recorriendo T_1 en

preorden, luego recorre T_2 en preorden, y así sucesivamente hasta recorrer T_p en preorden.

Un algoritmo para el recorrido en preorden es el siguiente:

```
def preorden (T):       # subarbol T(u)
   u := raiz (T)        # la raiz de T(u)
   tarea (u)            # tarea sobre u, e.g. imprimirlo
   L := hijos (u)       # todos los hijos de u
   for c in L:          # para cada hijo c de u, de izq. a der.
      preorden (T(c)) # recorre subarbol de c
   # end for
   return
```

Definición. Recorrido en inorden. Sea T un árbol ordenado con raíz r. Entonces:

- Si T consta sólo de r, entonces r es el recorrido en inorden de T;
- En otro caso, sean $T_1, T_2, ..., T_p$ los p subárboles de r, listados de izquierda a derecha, en T. El recorrido en inorden comienza recorriendo T_1 en inorden, continúa visitando r, luego recorre T_2 en inorden, y así sucesivamente hasta recorrer T_p en inorden.

Un algoritmo para el recorrido en inorden es el siguiente:

```
def inorden (T):                  # subarbol T(u)
   u := raiz (T)                  # la raiz de T(u)
   if (u == hoja):                # cuando u no-tiene hijos
      tareasobre (u)              # tarea sobre u, e.g. imprimirlo
   else:
      p := hijo_mas_izquierdo (u) # primer hijo de u
      inorden (T(p))              # recursion sobre p
      tareasobre (u)              # tarea sobre u, e.g. imprimirlo
      L := hermanos_derechos (p)  # todos los hermanos derechos de p
      for c in L:                 # cada hermano c de p, de izq. a der.
         inorden (T(c))           # recorre subarbol de c
      # end for
   # end if
   return
```

Definición. Recorrido en postorden. Sea T un árbol ordenado con raíz r. Entonces:

- Si T consta sólo de r, entonces r es el recorrido en postorden de T;
- En otro caso, sean $T_1, T_2, ..., T_p$ los p subárboles de r, listados de izquierda a derecha, en T. El recorrido en postorden comienza recorriendo T_1 en postorden, luego recorre T_2 en postorden, y así sucesivamente hasta recorrer T_p en postorden, y finaliza visitando r.

Un algoritmo para el recorrido en postorden es el siguiente:

```
def postorden (T):      # subarbol T(u)
   u := raiz (T)        # la raiz de T(u)
   L := hijos (u)       # todos los hijos de u
   for c in L:          # para cada hijo c de u, de izq. a der.
      postorden (T(c)) # recorre subarbol de c
   # end for
   tarea (u)            # tarea sobre u, e.g. imprimirlo
   return
```

Notación infija, prefija, y posfija

Omitir: la gente de FICH lo verá en AED, y la de FIQ: nunca! Comentario: la notación prefija (o notación polaca, o RPN (por *Reverse Polish Notation*)) se ha usado en calculadoras comerciales (e.g. la HP-15C).

9.4. Arbol de expansión

Intro

Definición. *Arbol de expansión*. un árbol de expansión (o árbol generador) de un grafo simple $G = (V, E)$ es un árbol que contiene a TODOS los vértices de G.

Teorema. (Un grafo SIMPLE es conexo) ssi (si tiene un árbol expansión). Demostración: omitir.

Ejemplo 2. **Redes con Protocolo de Internet** (redes IP): lectura para el hogar.

Observación. La "forma práctica" (con lápiz y papel) bastará en las evaluaciones para todos los algoritmos. En particular:

- Búsqueda en profundidad (o búsqueda en retroceso);
- Búsqueda a lo ancho.

Búsqueda en profundidad

Dado un grafo conexo $G(V, E)$ se puede encontrar un árbol de expansión $T(V, E')$, donde $E' \subseteq E$, utilizando el algoritmo de la búsqueda en profundidad (también denominado búsqueda en retroceso).
El algoritmo dado en Rosen para la búsqueda en profundidad (o búsqueda en retroceso) puede re-escribirse como:

```
1  def busca_en_profundidad (G):      # grafo conexo G(V,E), V={v1,..,vn}
2     T := inicia_arbol (v1)          # inicia arbol T(V',E') con v1
3     visita (v1,G)                   # es la llamada semilla
4     # ..............................................................
5     def visita (u,G,T):             # recibe un vertice generico u de G
6        L := vecinos (u)             # en L los vecinos de u
7        for c in L and c not in T:   # cada vecino c que NO-ESTA en T
8           agrega (c,u,T)            # agrega c y arista (c,u) en T
9           visita (c,G,T)            # visita al vertice adyacente de
10       #end for
11    #end visita
12    # ..............................................................
13 #end busca_en_profundidad
```

Ejemplo. En el grafo conexo $G = (V, E)$ trazado en la Fig. 9.2 encontrar un árbol de expansión $T(V, E')$ utilizando la Búsqueda en Profundidad (BP), y el orden alfabético ante igualdades de elección. Solución: el desarrollo de la BP se muestra con los grafos trazados en la Fig. 9.3, donde las aristas en trazo continuo son las aristas del árbol en construcción. El árbol T obtenido se dibuja aparte en la Fig. 9.4.

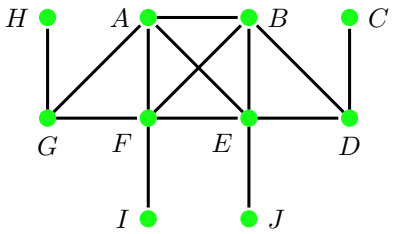

Figura 9.2: Ejemplo de un grafo conexo $G = (V, E)$ a utilizar en búsqueda en profundidad y en búsqueda a lo ancho.

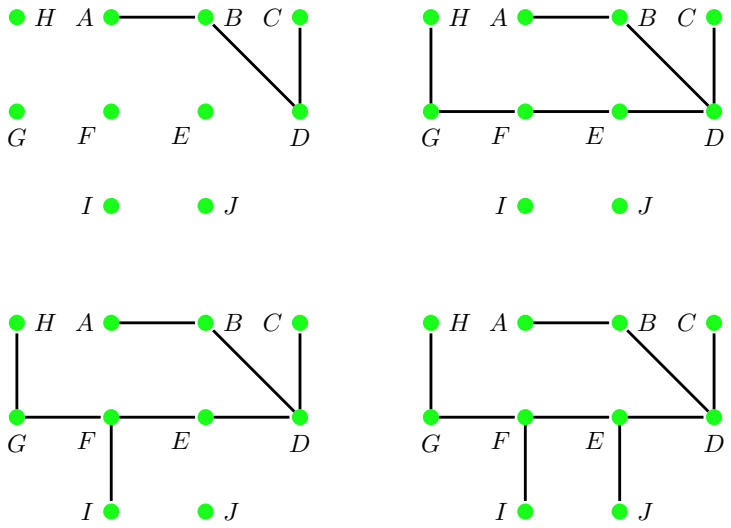

Figura 9.3: Iteraciones en la búsqueda en profundidad en el grafo conexo $G = (V, E)$ de la Fig. 9.2, donde cada subgrafo iterado (cada dibujo) es el obtenido *antes* de tener que hacer un *retroceso*. El árbol de expansión $T = (V, E')$ de $G(V, E)$ es el último dibujado con todos los vértices de G.

Búsqueda a lo ancho

Dado un grafo conexo $G(V, E)$ se puede encontrar un árbol de expansión $T(V, E')$, donde $E' \subseteq E$, utilizando el algoritmo de la búsqueda a lo ancho. El algoritmo dado en Rosen para la búsqueda a lo ancho puede re-escribirse como:

```
1  def busca_a_lo_ancho (G):          # grafo conexo G(V,E), V={v1,..,vn}
2     T := inicia_arbol (v1)          # inicia arbol T(V',E') con v1
3     C := []                         # inicia cola (del cajero) auxiliar
4     agrega (v1,C)                   # agrega vertice v1 a la cola C
5     while not vacia (C):            # mientras no esta vacia
6        u := frente_cola (C)         # el primero y lo quita de la cola
7        L := vecinos (u)             # en L los vecinos de u
8        for c in L:                  # cada vecino c que NO-ESTA en T
9           if c not in C and c not in T: # vec c NO-ESTA en C ni en T
10             agrega (c,u,T)        # agrega c y arista (c,u) en T
11             encola (c,Q)          # encola c en C
12          #end if
13       #end for
14    #end while
15 #end busca_a_lo_ancho
```

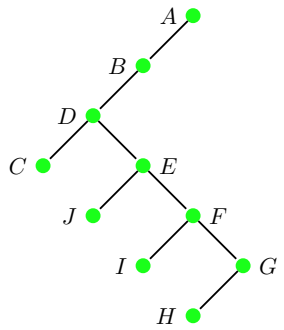

Figura 9.4: Arbol $T = (V, E)$ con raíz en el vértice A obtenido con búsqueda en profundidad.

Ejemplo. En el grafo conexo $G = (V, E)$ trazado en la Fig. 9.2 encontrar un árbol de expansión $T(V, E')$ utilizando la Búsqueda a lo Ancho (BA), utilizando el orden alfabético ante igualdades de elección. Solución: el desarrollo de la búsqueda a lo ancho se muestra con los grafos trazados en la Fig. 9.5, donde las aristas en trazo continuo son las aristas del árbol en construcción. El árbol T obtenido se dibuja aparte en la Fig. 9.6,

Aplicaciones de la búsqueda en profundidad

- Ejemplo 6. **Coloración** en grafos: lectura.
- Ejemplo 7. El problema de las n reinas: opcional.
- Ejemplo 8. Suma de subconjuntos: omitir.

Búsqueda en profundidad en digrafos (arañas web)

- Ejemplo 9: opcional.
- Ejemplo 10: **arañas web**, e.g. buscadores en internet, e.g. Google: lectura.

9.5. Arbol de expansión mínimo

Intro

Definición. *Arbol de expansión mínimo*: un árbol de expansión mínimo (o árbol generador mínimo) de un grafo ponderado $G = (V, E, W)$ es un árbol generador tal que la suma de los pesos de todas sus aristas es la mínima posible.

Observación. La "forma práctica" (con lápiz y papel) bastará en las evaluaciones para todos los algoritmos. En particular:

- Algoritmo de Prim;
- Algoritmo de Kruskal.

Algoritmo de Prim

Idea del algoritmo de Prim:

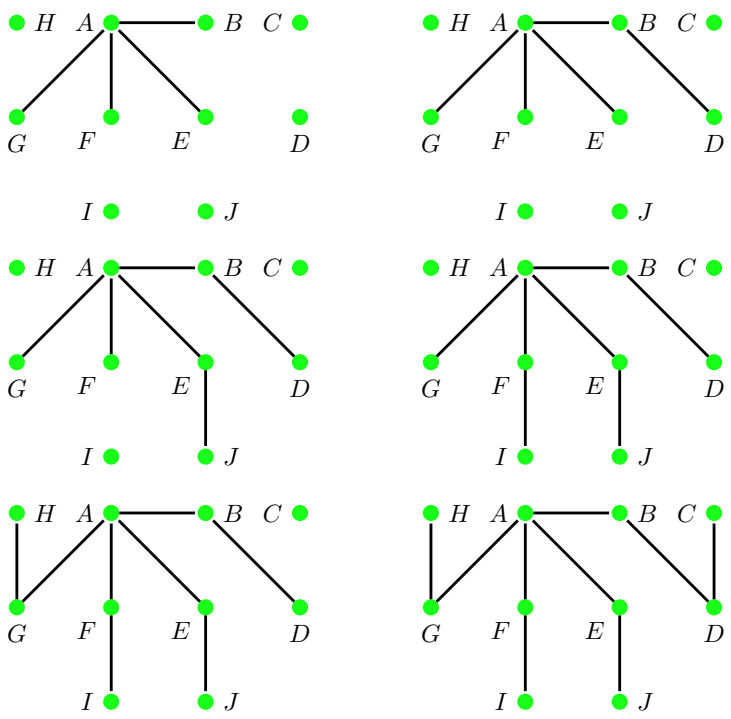

Figura 9.5: Iteraciones en la búsqueda a lo ancho en el grafo conexo $G = (V, E)$ de la Fig. 9.2, donde cada subgrafo iterado es el obtenido al agregar todos los vértices c adyacentes al vértice u quitado del frente de la cola C en cada iteración (tal que no se formen circuitos). El árbol de expansión $T = (V, E')$ de $G(V, E)$ es el último dibujado con todos los vértices de G.

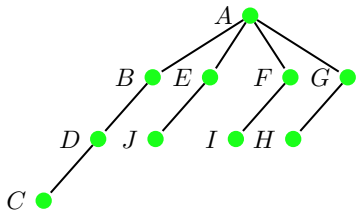

Figura 9.6: Arbol $T = (V, E)$ con raíz en el vértice A obtenido con búsqueda a lo ancho.

- Elegimos un orden arbitrario para los vértices;
- Elegimos una arista $e = (u, v)_w$ de peso w tal que sea mínimo. Esta arista será la primera arista del árbol T;
- Agregamos sucesivamente aristas al árbol T de entre las de peso mínimo disponibles, tal que sean incidentes con un vértice u que ya está en el árbol T y un vértice v que aún no está en T, y siempre que no formen un ciclo;
- Finalizamos cuando se agregaron $(n - 1)$ aristas.

El algoritmo de Prim puede describirse con:

```
1  def prim (G):                    # grafo ponderado G(V,E,W)
2     T := vacio                    # inicia T(V',E')
3     for k := 1 to (n-1):          # E' tiene (n-1) aristas, con n=|V|
4        if (k == 1):               # si es la primera arista
5           elegir arista e_min     # arista e de peso min
6        else:                      # las que siguen
```

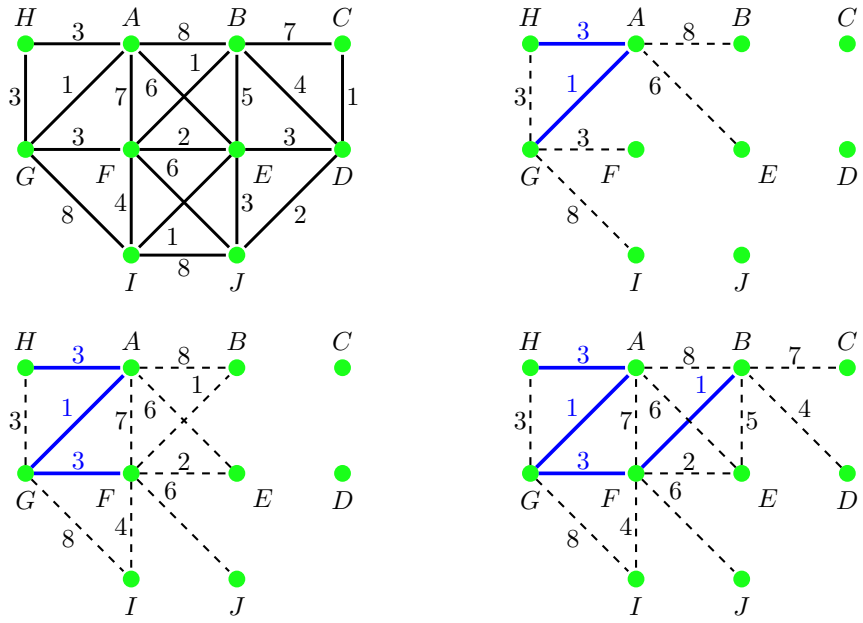

Figura 9.7: Iteraciones en el algoritmo de Prim en el grafo conexo $G = (V, E)$ de n vértices (arriba-izq.), donde cada subgrafo iterado T_k es el árbol parcial obtenido al agregar la arista adyacente a T_k de peso menor (tal que no se formen circuitos).

```
7           elegir arista (u,v)_min # con u en V' y v en V con w_min
8       #end if                     # y que no-forme ciclo
9       agregar (u,v) en T          # agrega arista (u,v) en E'
10    #end for
11  #end prim
```

Observación.

- La elección de la arista $e = (u, v)_w$ de vértice $u \in T'$, y vértice $v \in T$, de peso w tal que sea mínimo, puede (o suele) no-ser unívoca;
- Aquí optamos por elegir aquella con vértice $u \in T'$ menor según un orden predefinido para los vértices, típicamente el orden alfanumérico.

Ejemplo. En el grafo conexo ponderado $G = (V, E, W)$ trazado en la Fig. 9.7 (arriba-izquierda), encontrar un árbol de expansión mínimo $T(V, E', W')$ utilizando el algorimo de Prim (AP), utilizando el orden alfabético ante igualdades de elección en cada iteración. Solución: el desarrollo del AP se muestra con los grafos trazados en la Figs. 9.7-9.8, donde las aristas en trazo continuo son las aristas del árbol en construcción.

Algoritmo de Kruskal

Idea del algoritmo de Kruskal:

- Elegimos un orden arbitrario para los vértices;
- Elegimos una arista $e = (u, v)_w$ de peso w mínimo, y que será la primera arista de T;
- Agregamos sucesivamente aristas al árbol T de entre las de peso mínimo disponibles, siempre que no formen un ciclo;

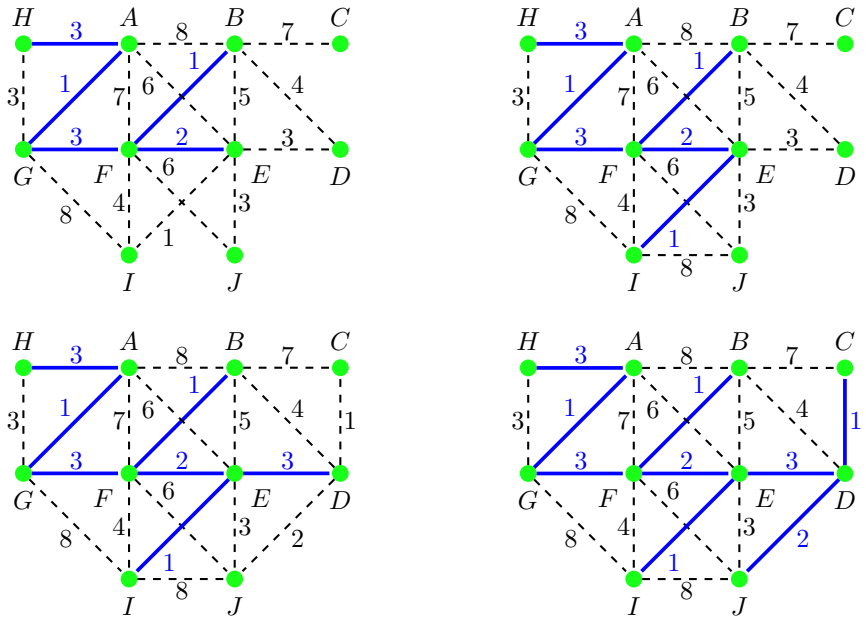

Figura 9.8: Iteraciones sucesivas en el algoritmo de Prim (continuación de la Fig. 9.7). El árbol de expansión mínimo $T = (V, E', W')$ de $G(V, E, W)$ es el último dibujado y que tiene $(n-1)$ aristas de G, i.e. $n = 10$ vértices, 9 aristas, y $w_{\min} = 17$.

- Finalizamos cuando se agregaron $(n-1)$ aristas.

El algoritmo de Kruskal puede describirse con:

```
1 def kruskal (G):                  # grafo ponderado G(V,E,W)
2    T := vacio                     # inicia T(V',E')
3    for k := 1 to (n-1):           # E' tiene (n-1) aristas, con n=|V|
4       elegir arista (u,v)_min     # pero que no-forme un ciclo
5       agrega arista (u,v) en T    # agrega arista (u,v) en E'
6    #end for
7 #end kruskal
```

Ejemplo. En el grafo conexo ponderado $G = (V, E, W)$ trazado en la Fig. 9.9 encontrar un árbol de expansión mínimo $T(V, E', W')$ utilizando el algoritmo de Kruskal (AK), utilizando el orden alfabético ante igualdades de elección en cada iteración. Solución: el desarrollo del AK se muestra con los grafos trazados en la Fig. 9.9, donde las aristas en trazo continuo son las aristas del árbol en construcción.

Observación. No-unicidad del árbol de expansión mínimo. En un grafo conexo ponderado $G = (V, E, W)$ pueden haber más de un árbol de expansión con un mismo peso mínimo pero con diferentes conjuntos de arsitas. Por ejemplo, en la Fig. 9.10 se muestran dos árboles de expansión mínimos $T_1(V, E', W')$ (izq.) y $T_2(V, E'', W'')$ (der.), ambos de igual peso mínimo $w_{\min} = 17$.

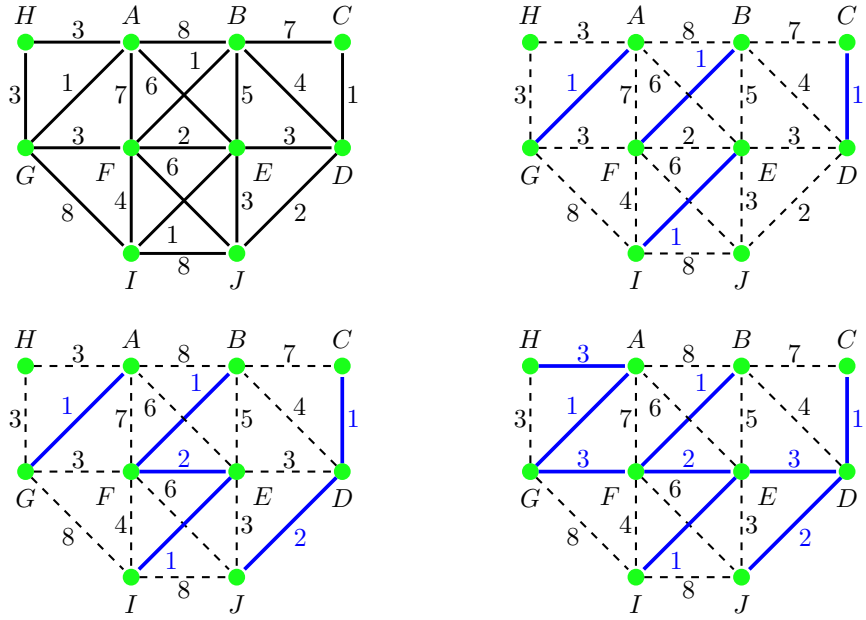

Figura 9.9: Iteraciones sucesivas en el algoritmo de Kruskal en el grafo conexo $G = (V, E)$ de n vértices (arriba-izq.), donde cada subgrafo iterado T_k es el árbol parcial obtenido al agregar todas las aristas de menor peso (tal que no formen circuitos) empezando con las de menor peso, i.e.: todas las de peso: 1 (arriba, der.), 2 (abajo, izq.), y 3 (abajo, der.). El árbol de expansión mínimo $T = (V, E', W')$ de $G(V, E, W)$ es el último dibujado y que tiene $(n-1)$ aristas de G, i.e. $n = 10$ vértices, 9 aristas, y $w_{\min} = 17$.

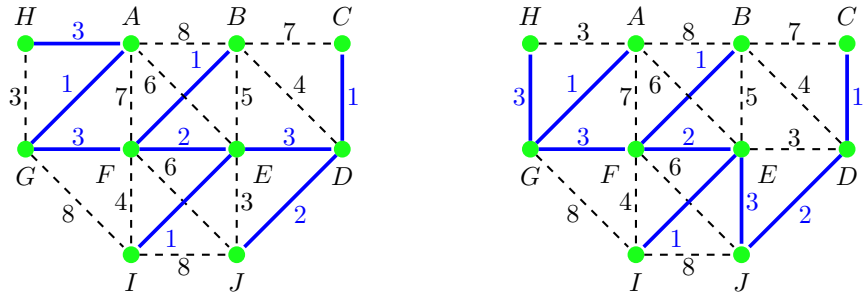

Figura 9.10: Dos árboles de expansión mínimos $T_1(V, E', W')$ (izq.) y $T_2(V, E'', W'')$ (der.), con $n = 10$ vértices, 9 aristas, donde ambos son diferentes pero tienen igual peso mínimo $w_{\min} = 17$.

CAPÍTULO 10

Algebra de Boole

Nota. Estas notas siguen el texto de referencia Rosen (2004) manteniendo la numeración de las secciones y sus títulos, como una referencia adicional para el auto-estudio siguiendo ese texto.

Omitir todo el cap.

CAPÍTULO 11

Modelos de computación

Nota. Estas notas siguen el texto de referencia Rosen (2004) manteniendo la numeración de las secciones y sus títulos, como una referencia adicional para el auto-estudio siguiendo ese texto. Por otra parte, para interesados en este tema, puede resultar de interés consultar, además del texto de Johnsonbaugh (2005), las presentaciones dadas en Aho et al. (1998, 2008); Hopcroft et al. (2008) ("libros del dragón" (rojo, verde, púrpura, etc.) en la jerga de los *hackers*), o en Alfonseca Moreno et al. (2006).

Contents

11.1. Lenguajes y gramáticas

Intro informal

- **Palabra**: una palabra en las gramáticas más clásicas es una unidad con algún significado que está separada de otras unidades mediante pausas en el habla o bien con blancos en la escritura;
- **Frase** (u **oración**): es una combinación de palabras;
- **Gramática**: define una serie de reglas precisas para una construcción correcta de las oraciones. Por ejemplo, según la gramática española, la frase *el perro explica pacientemente*, está compuesta por un sujeto *el perro*, formado a su vez por el artículo *el* y el nombre *perro*, y un predicado *explica pacientemente*, formado a su vez por el verbo *explica* y el adverbio *pacientemente*;
- **Sintaxis**: predefine reglas para un orden correcto para construir una oración con una forma válida, e.g. una regla para un orden correcto en una oración es: sujeto + verbo

+ predicado, e.g. la frase *el perro explica pacientemente* es aceptable, en cambio la frase *pacientemente perro explica el* no tiene una forma válida;
- **Semántica**: analiza el significado de las oraciones, e.g. la frase *el perro explica pacientemente*, en general, no tiene mayor realidad para el sentido común excepto en situaciones especiales como en literatura, e.g. en las fábulas de Esopo;
- **Lenguaje natural**: abarca al lenguaje hablado entre personas en los diferentes idiomas, e.g. ordenados por el número de (i) hablantes: inglés, chino mandarín, hindi, español, francés, etc.; (ii) hablantes nativos: chino mandarín, español, inglés, hindi, francés, etc.. Empero, un gran problema es que tienen sintaxis extremadamente elaboradas como para formalizarlas matemáticamente;
- **Lenguaje formal** (primera aproximación): un lenguaje formal queda definido con un conjunto de reglas precisas bien definidas. Es mucho más restringido comparado con el lenguaje natural, pero de gran utilidad tanto en la traducción automatizada como en los lenguajes de programación.

Ejemplo. Una gramática rudimentaria ("de juguete") para un subconjunto del idioma español queda descripta con la siguiente serie de definiciones:

1) **frase** (u oración): compuesta por un **sujeto** seguido por un **predicado**;
2) Un **sujeto**: compuesto por, o bien un **artículo** seguido de un **nombre**, o bien un **artículo** seguido de un **nombre** y luego seguido de un **adjetivo**;
3) Un **predicado**: compuesto por, o bien un **verbo** seguido de un **adverbio**, o bien un **verbo**;
4) Un **artículo** es alguna de las palabras: *un*, *el*;
5) Un **adjetivo** es alguna de las palabras: *nuevo*, *agudo*;
6) Un **nombre** es alguna de las palabras: *coronavirus*, *geólogo*;
7) Un **verbo** es alguna de las palabras: *explora*, *contagia*;
8) Un **adverbio** es alguna de las palabras: *rápidamente*, *globalmente*.

junto con las reglas de **sustituciones**:

- **frase**
- **sujeto predicado**
- (**artículo nombre adjetivo**) **predicado**
- **artículo nombre adjetivo verbo adverbio**

las cuales permiten obtener diferentes frases eligiendo sustituciones permitidas en forma sucesiva hasta que no se puedan aplicar más reemplazos. Por ejemplo, una posible secuencia de sustituciones es:

- **frase**
- (**sujeto**) **predicado**
- **artículo nombre adjetivo** (**predicado**)
- **artículo nombre adjetivo verbo adverbio**
- *el* **nombre adjetivo verbo adverbio**
- *el coronavirus* **adjetivo verbo adverbio**
- *el coronavirus nuevo* **verbo adverbio**

- *el coronavirus nuevo contagia* **adverbio**
- *el coronavirus nuevo contagia rápidamente*

Entonces, e.g. son frases válidas *un geólogo agudo contagia globalmente*, o *un geólogo nuevo explora minuciosamente*, pero no lo es *nuevo un globalmente contagia geólogo*.

Gramática con estructura de frases

Definiciones.

- Un *vocabulario* (o *alfabeto*) V es un conjunto finito y no-vacío cuyos elementos se denominan *símbolos*;
- Una *palabra* sobre un alfabeto V es una cadena finita de elementos de V;
- La *palabra vacía* (o *cadena vacía*) es la cadena sin símbolos, y se denota con λ;
- El *conjunto de todas las palabras finitas* sobre V se denota con V^*;
- Un *lenguaje (formal)* L sobre un alfabeto V es un subconjunto de V^*;

Observación.

- Notar que λ es diferente del conjunto vacío $\emptyset$;
- El conjunto $\{\lambda\}$ contiene exactamente una palabra: la palabra vacía.

Especificaciones de un lenguaje

Los lenguajes se pueden especificar de varias formas:

- Enumerando todas las palabras que pertenecen al lenguaje;
- Definiendo criterios para que una palabra pertenezca al lenguaje;
- Definiendo una gramática G, como en el ejemplo de la gramática rudimentaria ("de juguete"), y que se describe a continuación.

Definición. Una *Gramática con Estructura de Frases* (GEF, o simplemente *gramática*) es la tupla $G = (V, T, N, P, s_0)$, en donde:

- **Vocabulario** (o **alfabeto**) V: es un conjunto finito y no-vacío formado por todos los símbolos utilizados en el lenguaje;
- Símbolos **terminales** T: es un subconjunto del vocabulario V cuyos elementos no pueden reemplazarse por otros símbolos;
- Símbolos **no-terminales** N: es el subconjunto de los elementos del vocabulario V que pueden reemplazarse por otros elementos, y está dado por $N = V - T$. Obs.: el vocabulario V es la unión de T y N, donde T y N son disjuntos, i.e. $V = N \cup T$, con $N \cap T = \emptyset$;
- **Símbolo inicial** s_0: es un símbolo no-terminal arbitrario por el cual se empieza;
- **Producción** P: es el conjunto de las producciones de la gramática G. Una producción en la gramática G es toda regla que define como reemplazar una cadena del conjunto V^* (de todas las palabras finitas) por otra cadena, y se denota por $z_0 \to z_1$, la producción en donde z_0 puede reemplazarse por z_1.

Ejemplo. En el ejemplo introductorio de una gramática rudimentaria ("de juguete") tenemos:

- Conjunto de símbolos terminales

$$T = \Big\{un,\ el,\ coronavirus,\ geólogo,\ explora,\ contagia,\ rápidamente,\ globalmente\Big] \tag{11.1}$$

- Conjunto de símbolos no-terminales

$$N = \Big\{\textbf{frase},\ \textbf{sujeto},\ \textbf{predicado},\ \textbf{adjetivo},\ \textbf{artículo},\ \textbf{nombre},\ \textbf{verbo},\ \textbf{adverbio}\Big\} \tag{11.2}$$

- Símbolo inicial s_0 = **frase**;
- Producciones P: las primeras producciones pueden escribirse como:

$$\begin{aligned} \textbf{frase} &\rightarrow \textbf{sujeto predicado} \\ \textbf{sujeto} &\rightarrow \textbf{artículo nombre} \\ &\rightarrow \textbf{artículo nombre adjetivo} \\ \textbf{predicado} &\rightarrow \textbf{verbo} \\ &\rightarrow \textbf{predicado adverbio} \\ \textbf{frase} &\rightarrow \textbf{sujeto predicado} \end{aligned} \tag{11.3}$$

Gramáticas con estructura de frases

Definición. Consideremos la gramática con estructura de frases $G(T, N, P, s_0)$, y sean las cadenas $w_0 = hz_0r$ y $w_1 = hz_1r$ sobre V (la concatenación de hz_0r). Se tiene:

- Si $z_0 \rightarrow z_1$ es una producción de G, entonces decimos que la cadena w_1 se *deriva directamente* de w_0 (o que es *directamente derivable*), y se escribe $w_0 \Rightarrow w_1$.
- Si $w_0, w_1, ..., w_n$ son cadenas sobre V tales que $w_0 \Rightarrow w_1$, $w_1 \Rightarrow w_2$, ..., $w_{n-1} \Rightarrow w_n$, decimos que w_n es derivable de w_0, y se denota con $w_0 \overset{*}{\Rightarrow} w_n$. La secuencia de pasos utilizada para obtener w_n a partir de w_0 se llama derivación.

Ejemplo. Sean: el vocabulario $V = \{a, b, A, B, s_0\}$, los terminales $T = \{a, b\}$, los no-terminales $N = \{A, B, s_0\}$, el símbolo inicial s_0, y las producciones

$$\begin{aligned} P = \{s_0 &\rightarrow ABa \\ A &\rightarrow BB \\ B &\rightarrow ab \\ AB &\rightarrow b\} \end{aligned} \tag{11.4}$$

Entonces, la tupla $G(T, N, P, s_0)$ define una gramática con estructura de frases.

Ejemplo. En la gramática $G(T, N, P, s_0)$ del ejemplo anterior: (i) la cadena $Aaba$ se deriva directamente de ABa porque $B \rightarrow ab$ es una producción de G; y (ii) la cadena

abababa se deriva de *ABa* en base a las producciones:

$$\begin{aligned} A(B)a &\Rightarrow A(ab)a \\ (A)aba &\Rightarrow (BB)aba \\ (B)(B)aba &\Rightarrow (ab)(ab)aba \end{aligned} \tag{11.5}$$

Definición. Sea $G = (V, T, N, P, s_0)$ una gramática con estructura de frases. El *lenguaje generado* por G es el conjunto $L(G)$ de todas las cadenas de terminales que se derivan del estado inicial s_0. En símbolos

$$L(G) = \{w \in T^* \mid s_0 \overset{*}{\Rightarrow} w\} \tag{11.6}$$

Ejemplo. Sea la gramática con estructura de frases $G = (V, T, N, P, s_0)$ con el vocabulario $V = \{a, b, A, s_0\}$, los terminales $T = \{a, b\}$, los no-terminales $N = \{A, s_0\}$, el símbolo inicial s_0, y las producciones

$$\begin{aligned} P = \{s_0 &\to aA \\ s_0 &\to b \\ A &\to aa\} \end{aligned} \tag{11.7}$$

Encuentre el lenguaje $L(G)$ generado por la gramática G.
Solución:

$$\begin{aligned} s_0 &\to aA \\ s_0 &\to b \\ aA &\to aaa \end{aligned} \tag{11.8}$$

Como no-puede derivarse ninguna otra palabra con las producciones P dadas, se concluye que el lenguaje generado por G es $L(G) = \{b, aaa\}$.

Ejemplo. Sea la gramática con estructura de frases $G = (V, T, N, P, s_0)$ con el vocabulario $V = \{0, 1, s_0\}$, los terminales $T = \{0, 1\}$, los no-terminales $N = \{s_0\}$, el símbolo inicial s_0, y las producciones

$$\begin{aligned} P = \{s_0 &\to 11s_0 \\ s_0 &\to 1\} \end{aligned} \tag{11.9}$$

Encuentre el lenguaje $L(G)$ generado por la gramática G. Solución:

$$\begin{aligned} s_0 &\to 0 \\ s_0 &\to 11s_0 \\ 11s_0 &\to 110 \\ 11s_0 &\to 1111s_0 \\ 1111s_0 &\to 11110 \\ 1111s_0 &\to 111111s_0 \\ 111111s_0 &\to 1111110 \\ 111111s_0 &\to 11111111s_0 \end{aligned} \tag{11.10}$$

Se observa que, en cualquier etapa, se puede agregar dos unos al final de la cadena y, o bien continuar derivando, o bien finalizarla con un cero, por lo que se concluye que el lenguaje generado por G es de la forma $L(G) = \{0, 110, 11110, 1111110, ...\}$.

Ejemplo. Construya una gramática con estructura de frases $G = (V, T, N, P, s_0)$ tal que genere el lenguaje $L(G) = \{0^n 1^n\}$ para $n = 0, 1, 2, ...$ Solución: La gramática G puede obtenerse anteponiendo un 0 y posponiendo un 1 a la cadena inicial, siendo la cadena inicial λ (la cadena vacía), resultando: el vocabulario $V = \{0, 1, s_0\}$, los terminales $T = \{0, 1\}$, los no-terminales $N = \{s_0\}$, el símbolo inicial λ (la cadena vacía), y las producciones

$$\begin{aligned} P = \{&s_0 \to 0 s_0 1 \\ &s_0 \to \lambda\} \end{aligned} \tag{11.11}$$

Ejemplo. Construya una gramática con estructura de frases $G = (V, T, N, P, s_0)$ tal que genere el lenguaje $L(G) = \{0^m 1^n\}$ para $m, n = 0, 1, 2, ...$
Solución 1: La gramática G puede obtenerse, o bien anteponiendo un 0, o bien posponiendo un 1 a la cadena inicial, siendo la cadena inicial λ (la cadena vacía), resultando: el vocabulario $V = \{0, 1, s_0\}$, los terminales $T = \{0, 1\}$, los no-terminales $N = \{s_0\}$, el símbolo inicial λ (la cadena vacía), y las producciones

$$\begin{aligned} P = \{&s_0 \to 0 s_0 \\ &s_0 \to s_0 1 \\ &s_0 \to \lambda\} \end{aligned} \tag{11.12}$$

Solución 2: otra G es con el vocabulario $V = \{0, 1, s_0, A\}$, los terminales $T = \{0, 1\}$, los no-terminales $N = \{s_0, A\}$, el símbolo inicial λ (la cadena vacía), y las producciones

$$\begin{aligned} P = \{&s_0 \to 0 s_0 \\ &s_0 \to 1A \\ &s_0 \to 1 \\ &s_0 \to \lambda \\ &A \to 1A \\ &A \to 1\} \end{aligned} \tag{11.13}$$

Tipos de gramática con estructura de frases

tipo	restricciones en las producciones $w_1 \to w_2$
0	sin restricciones
1	$\text{len}(w_1) < \text{len}(w_2)$ o $w_2 = \lambda$
2	$w_1 = A$, donde A es un no-terminal
3	$w_1 = A$ y $w_2 = aB$, o $w_2 = a$, siendo $A, B \in N$ (no-terminal), y $a \in T$ (terminal), o $s_0 \to \lambda$

Tabla 11.1: Tipos de gramáticas.

Definiciones. Clasificación de las gramáticas de Chomsky (ver Tabla 11.1):

- **Gramática de tipo 0**. No se impone restricción alguna a las producciones. Por eso se dice que una gramática de tipo 0 es también una gramática sin restriciones;
- **Gramática de tipo 1**. Cuando las producciones son de las formas:

$$\begin{aligned} &w_1 \to w_2 \quad \text{si } \text{len}(w_2) > \text{len}(w_1) \\ &w_1 \to \lambda \end{aligned} \tag{11.14}$$

Cuando se tiene una producción de la forma $\alpha w_1 \beta \rightarrow \alpha w_2 \beta$ (pero no de la forma $w_2 \rightarrow w_1$), la w_1 se puede reemplazar por w_2 únicamente cuando w_1 está entre las cadenas α y β, es decir, cuando w_1 está en el contexto de α y β. Por eso se dice que una gramática de tipo 1 es también una Gramática Sensible al Contexto (GSC) (o una gramática dependiente del contexto);

- **Gramática de tipo 2**. Cuando las producciones son de la forma:

$$w_1 \rightarrow w_2 \text{ donde } w_1 \text{ es un único no-terminal} \tag{11.15}$$

En una gramática de tipo 2 las producciones tienen un no-terminal únicamente en su lazo izquierdo, y además se puede sustituir un no-terminal a la izquierda de una producción independientemente de lo que figure en la cadena (siempre que aparezca en la misma). Por eso se dice que una gramática de tipo 2 también es una gramática libre de contexto;

- **Gramática de tipo 3**. Cuando las producciones son de la forma:

$$\begin{aligned} &w_1 \rightarrow w_2 \quad \text{con } w_1 = A, \text{ y } w_2 = aB \text{ o } w_2 = a \\ &\quad \text{con } A \text{ y } B \text{ no-terminales, pero } a \text{ es un terminal} \\ &w_1 \rightarrow w_2 \quad \text{con } w_1 = s_0, \text{ y } w_2 = \lambda \end{aligned} \tag{11.16}$$

Una gramática de tipo 3 tiene reglas de sustitución sencillas: se reemplaza un no-terminal por,

- o bien un terminal;
- o bien un terminal seguido de otro no-terminal;
- o bien por la cadena vacía.

Por eso se dice que una gramática de tipo 3 es tambíen una Gramática Regular (GR).

Observación. Notar que (e.g. ver Fig. 11.1):

- toda gramática de tipo 3 es también una gramática de tipo 2;
- toda gramática de tipo 2 es también una gramática de tipo 1;
- toda gramática de tipo 1 es también una gramática de tipo 0.

Observación.

- Las gramáticas de tipo 2 (o libres de contexto) se utilizan para definir la sintaxis en casi todos los lenguajes de programación;
- Las gramáticas de tipo 3 (o regulares) se emplean internamente en los compiladores para el análisis sintáctico, donde ingresa una cadena y retorna sus componentes léxicos (**lexemas**, o *tokens*).

Definición. Un lenguaje L es sensible al contexto (respectivamente, libre de contexto, regular) si existe una gramática G sensible al contexto (respectivamente, libre de contexto, regular), tal que $L = L(G)$.

Ejemplo.

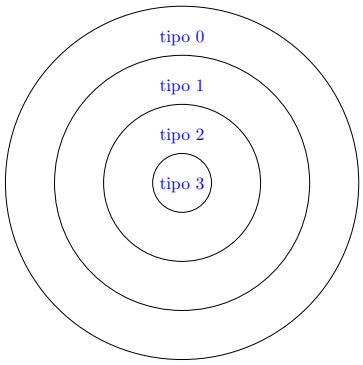

Figura 11.1: Clasificación de Chomsky de las gramáticas, tipos: 0 (con estructura de frases), 1 (dependiente del contexto), 2 (independiente del contexto), y 3 (regular).

- El lenguaje $L(G) = \{0^m 1^n \mid m, n = 1, 2, ...\}$ es un lenguaje regular porque admite una gramática regular G;
- El lenguaje $L(G) = \{0^n 1^n \mid n = 1, 2, ...\}$ es un lenguaje libre de contexto porque las producciones son $s_0 \to 0 s_0 1$ y $s_0 \to \lambda$.

Arboles de derivación

Definición. Un árbol de derivación es un árbol con raíz ordenado que representa todas las derivaciones posibles en un lenguaje generado por una gramática libre de contexto, donde la raíz del árbol representa al símbolo inicial, los nodos internos representan los símbolos no-terminales, mientras que las hojas representan los símbolos terminales. Si la producción $A \to w$ es parte de una derivación, donde w es una palabra, entonces el nodo del árbol que contiene al símbolo A tiene como hijos a todos los nodos que representan a todos los símbolos de w, ordenados de izquierda a derecha.

Observación. El problema de determinar si una frase w dada pertenece (o no) a un lenguaje generado por una GLC aparece en la construcción de compiladores, cuya solución admite dos enfoques posibles:

- **Análisis descendente**: se empieza en el símbolo inicial s_0, y se van aplicando producciones sucesivamente hasta llegar a la palabra dada w;
- **Análisis ascendente**: se empieza en la palabra dada w y se van aplicando producciones sucesivamente hasta llegar al símbolo inicial s_0.

Ejemplo. Un árbol de derivación para la frase *el coronovirus nuevo contagia rapidamente* es mostrada en la Fig. 11.2.

Ejemplo. Determine si la palabra *cbab* pertenece al lenguaje generado por la gramática $G = (V, T, s_0, P)$, con vocabulario $V = \{a, b, c, A, B, C, S\}$, terminales $T = \{a, b, c\}$, no-

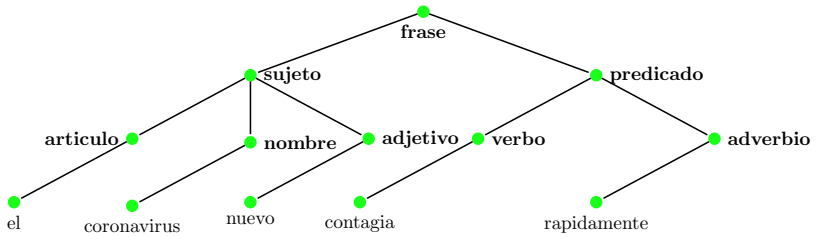

Figura 11.2: Un árbol de derivación para la frase *el coronovirus nuevo contagia rapidamente*.

terminales $N = \{A, B, C, S\}$, símbolo inicial s_0, y las producciones

$$\begin{aligned} P = \{ & s_0 \to AB \\ & A \to Ca \\ & B \to Ba \\ & B \to Cb \\ & B \to b \\ & C \to cb \\ & C \to b\} \end{aligned} \tag{11.17}$$

Solución:

- **Análisis descendente**: empezamos en símbolo inicial s_0 e intentamos derivar la palabra *cbab* usando las producciones disponibles. Se tiene:

$$s_0 \to (A)B \to (Ca)B = (C)aB \to (cb)aB = cba(B) \to cbab \tag{11.18}$$

- **Analisis ascendente**: empezamos en la cadena dada *cbab* analizada y otra vez se van aplicando producciones sucesivamete. Se tiene:

$$(cb)ab \to (C)ab = (Ca)b \to (A)b = A(b) \to AB \to s_0 \tag{11.19}$$

La forma de Backus-Naur

La forma de Backus-Naur suele utilizarse para especificar una gramática de tipo 2, e.g. para la sintaxis de lenguajes de programación tales como C, Java, Pascal, Fortran, LISP (e.g. en los manuales de los compiladores de IBM), lenguajes de bases de datos tales como SQL, o lenguajes de marcas, como XML.
La forma de Backus-Naur se define como sigue:

- Las producciones en una gramática de tipo 2 tienen un único símbolo no-terminal en el lazo izquierdo;
- Las producciones aparecen en el lado derecho en una misma línea separadas por barras | verticales;
- El símbolo $\to$ se reemplaza con ::=
- Los símbolos no-terminales se rodean con $\langle ... \rangle$, mientras que los símbolos terminales con nada.

Por ejemplo, el conjunto de producciones

$$P = \{(A \to Aa), (A \to a), (A \to AB)\} \tag{11.20}$$

se re-escriben con

$$\langle A \rangle ::= \langle A \rangle a \mid a \mid \langle A \rangle \mid \langle B \rangle \tag{11.21}$$

Ejemplo. Hallar la forma de Backus-Naur para la gramática rudimentaria "de juguete" dada en el inicio del cap.
Solución: está dada por la Ec. (11.22):

$$\begin{aligned}
\langle frase \rangle &::= \langle sujeto \rangle \langle predicado \rangle \\
\langle sujeto \rangle &::= \langle articulo \rangle \langle nombre \rangle \langle adjetivo \rangle \mid \langle articulo \rangle \langle nombre \rangle \\
\langle predicado \rangle &:: \langle verbo \rangle \mid \langle adverbio \rangle \mid \langle verbo \rangle \\
\langle articulo \rangle &:: un \mid el \\
\langle adjetivo \rangle &:: nuevo \mid agudo \\
\langle nombre \rangle &:: coronavirus \mid geologo \\
\langle verbo \rangle &:: explora \mid contagia \\
\langle adverbio \rangle &:: rapidamente \mid globalmente
\end{aligned} \tag{11.22}$$

Ejemplo. Hallar la forma de Backus-Naur para la producción de enteros con signo en notación decimal.
Solución: está dada por la Ec. (11.23):

$$\begin{aligned}
\langle enteroconsigno \rangle &::= \langle signo \rangle \langle entero \rangle \\
\langle signo \rangle &::= + \mid - \\
\langle entero \rangle &::= + \mid - \langle digito \rangle \mid \langle digito \rangle \langle entero \rangle \mid \\
\langle digito \rangle &:: 0 \mid 1 \mid 2 \mid 3 \mid 4 \mid 5 \mid 6 \mid 7 \mid 8 \mid 9
\end{aligned} \tag{11.23}$$

Ejemplo. Hallar la forma de Backus-Naur de un identificador válido en programación (las variables de usuario cuando se programa), definido como una cadena de caracteres alfanuméricos que debe empezar con una letra.
Solución: la forma de Backus-Naur en este caso está dada en la Ec. (11.24):

$$\begin{aligned}
\langle identificador \rangle &::= \langle letra \rangle \mid \langle identificador \rangle \langle letra \rangle \mid \langle identificador \rangle \langle digito \rangle \\
\langle letra \rangle &::= a \mid b \mid c \mid ... \mid x \mid \mid y \mid z \\
\langle digito \rangle &::= 0 \mid 1 \mid 2 \mid 3 \mid 4 \mid 5 \mid 6 \mid 7 \mid 8 \mid 9
\end{aligned} \tag{11.24}$$

11.2. Máquinas de estado finito con salida

Intro

Las Máquinas de Estado Finito (MEF) son la base de diversos dispositivos/software, e.g. máquinas expendedoras (de jugo, café, etc.), correctores ortográficos y gramaticales, indexadores, reconocimiento de voz, protocolos de comunicación entre compus, etc.

	estado siguiente f					función de salida g				
estado	5	10	25	N	R	5	10	25	N	R
s_0	s_1	s_2	s_3	s_0	s_0	n	n	n	n	n
s_1	s_2	s_3	s_6	s_1	s_1	n	n	n	n	n
s_2	s_3	s_4	s_6	s_2	s_2	n	n	5	n	n
s_3	s_4	s_5	s_6	s_3	s_3	n	n	10	n	n
s_4	s_5	s_6	s_6	s_4	s_4	n	n	15	n	n
s_5	s_6	s_6	s_6	s_5	s_5	n	5	20	n	n
s_6	s_6	s_6	s_6	s_0	s_0	5	10	25	N	M

Tabla 11.2: Estados posibles en una máquina expendedora de jugos.

Ejemplo. Describir una máquina expendedora de jugos que acepta monedas de 5, 10, y 25 pesos. Cuando un cliente ingresa 30 pesos o más, la máquina da vuelto a todo ingreso superior a 30 pesos y, a continuación, el cliente opta por pulsar, o bien un botón naranja (N) para obtener un jugo de naranja, o bien un botón rojo (R) para obtener un jugo de manzana.

Solución:

- Para describir el funcionamiento de esta máquina expendedora de jugos hay que:
  - Definir todos sus estados posibles;
  - Determinar cómo cambia de un estado dado a otro cuando recibe una moneda;
  - La salida para cada combinación posible de entrada y estado inicial;
- Según las monedas ingresadas, la máquina expendedora puede estar en alguno de 7 estados s_k posibles, con $k = 0, 1, ..., 6$, donde s_k es el estado cuando la máquina expendedora ha recaudado $5k$ pesos;
- La máquina expendedora empieza en el estado s_0, con 0 pesos recaudados, mientras que las posibles entradas son: 5, 10, o 25 pesos, el botón naranja N, y el botón rojo R;
- Las posibles salidas son: nada (n), 5, 10, 15, 20, o 25 pesos, un jugo de naranja, o un jugo de manzana;
- Por ejemplo, si un cliente introduce 10 pesos seguido de 25 pesos, entonces la máquina expendedora le devuelve 5 pesos, y luego el cliente selecciona apretar, o bien el botón N, o bien el botón R. En este ejemplo tenemos:
  - La máquina expendeora empieza en el estado s_0 (0 pesos);
  - La primera entrada es 10 pesos, que hace cambiar el estado de la máquinaa expendedora de s_0 a s_2 pero no devuelve nada;
  - La segunda entrada es 25 pesos, que ahora hace cambiar el estado de s_2 a s_6, donde dá un vuelto de 5 pesos;
  - La siguiente entrada es el botón N que cambia el estado de s_6 a s_0 y produce la salida que es el jugo de naranja N;
- La Tabla 11.2 muestra todos los cambios de estados y salidas posibles en esta máquina expendedora.

Máquinas de estado finito con salida

Definición. Una Máquina de Estado Finito (MEF) con salida es la túpla $\mathcal{M} = (I, O, S, f, g, s_0)$ que tiene:

. Un alfabeto finito I de *entradas* (o *inputs*);
. Un conjunto finito O de *salidas* (o *outputs*);
. Un conjunto finito S de *estados* (o *states*);
. Una función f de *transición* (o función *estado siguiente*), que asigna a cada tupla (estado, entrada) el estado siguiente, en símbolos $f : S \times I \to S$;
. Una función g de *salida* que asigna a cada tupla (estado, entrada) una nueva salida, en símbolos $g : S \times I \to O$;
. Un *estado inicial* s_0.

Observación. Para representar los valores de las funciones f y g se puede emplear:

. Una *Tabla de Estados* (TE) y una *Tabla de Transición* (TT), que listan todas tuplas (entrada,estado) posibles;
. Un *Diagrama de Estado* (DE): es un digrafo con aristas etiquetadas, donde cada estado se representa con un círculo, mientras que las aristas se etiquetan con la tupla (entrada, salida) de cada transición;

Definición. Función de salida en una MEF con salida para una cadena de entrada. Sea una Máquina de Estado Finito (MEF) con salida $\mathcal{M} = (I, O, S, f, g, s_0)$, en donde una cadena de entrada $x = x_1x_2...x_k$ va ingresando símbolo a símbolo, de izquierda a derecha. La función de salida g de una cadena de entrada $x = x_1x_2...x_k$ genera la cadena de salida $y = y_1y_2...y_k$ tal que $y = g(x)$, donde cada símbolo de entrada va llevando a la MEF de un estado a otro, y a su vez va generando la salida en la forma sucesiva:

. De s_0 a s_1 donde $s_1 = f(x_1, s_0)$ y $y_1 = g(x_1, s_0)$;
. De s_1 a s_2 donde $s_2 = f(x_2, s_1)$ y $y_2 = g(x_2, s_1)$;
. etc.
. De s_{k-1} a s_k donde $s_k = f(x_k, s_{k-1})$ y $s_k = g(x_k, s_{k-1})$.

En literatura también se suelen distinguir las siguientes:

Definiciones.

a) MEF con salida de Mealy: aquellas MEF donde la salida depende de las transiciones entre estados;
b) MEF con salida de Moore: aquellas MEF donde la salida depende sólo del estado;
c) MEF sin salida (o Autómata de Estado Finito (AEF)): aquellas MEF donde hay un conjunto final de estados y reconocen una cadena ssi llevan el estado inicial al estado final.

Ejemplo. Trace el diagrama de estados de la MEF descripta por la tabla de estados listada en la Tabla 11.3. Solución: el diagrama de estados para la Tabla 11.3 es trazado en la Fig. 11.3.

	estado siguiente f		función de salida g	
estado	0	1	0	1
s_0	s_1	s_0	1	0
s_1	s_3	s_0	1	1
s_2	s_1	s_2	0	1
s_3	s_2	s_1	0	0

Tabla 11.3: Tabla de estados de la MEF de la Fig. 11.3.

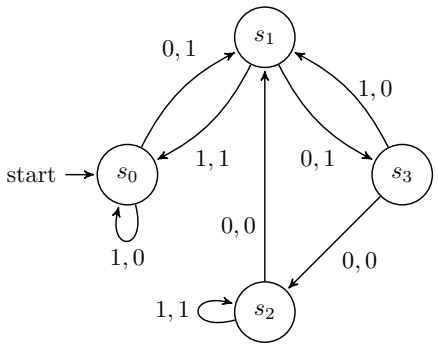

Figura 11.3: Diagrama de estados de la MEF descripta por la tabla de estados listada en Tabla 11.3.

Ejemplo. Dado el diagrama de estados mostrado en la Fig. 11.4 de una MEF con salida, obtenga la tabla de estados. Solución: la tabla de estados asociado al diagrama de estados de la Fig. 11.4 está dada en la Tabla 11.4.

Ejemplo. Hallar la cadena de salida generada por la MEF de la Fig. 11.3 cuando la cadena de entrada es $x = 101011$. Solución: los sucesivos estados y salidas se listan en la Tabla 11.5.

Ejemplo. Construir una MEF que retarde una cadena de bits en un símbolo, i.e. cuando la cadena de entrada es $x_1x_2...x_k$, la cadena de salida debe ser $0x_1x_2...x_{k-1}$. Solución: la MEF tiene que admitir las entradas 0 y 1, y tiene que tener un estado inicial s_0. Como además tiene que recordar la entrada previa si ha sido un 0 o un 1, hacen falta dos estados s_1 y s_2 tales que está en el estado s_1 si la entrada anterior fue un 1, y en el estado s_2 si fue un 0. En la transición inicial desde s_0 se tiene que producir la salida 0. Cada transición desde s_1 produce la salida 1, y cada transición desde s_2 produce la salida 0. La salida a la

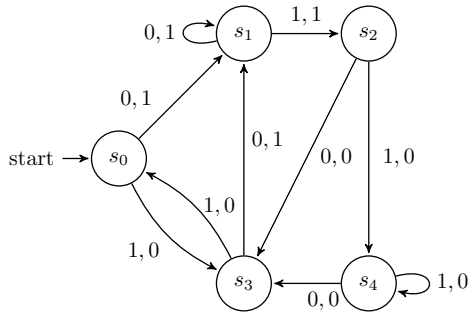

Figura 11.4: Diagrama de estados de la MEF descripta por la tabla de estados listada en Tabla 11.4.

	estado siguiente f		función de salida g	
estado	0	1	0	1
s_0	s_1	s_3	1	0
s_1	s_1	s_2	1	1
s_2	s_3	s_4	0	0
s_3	s_1	s_0	0	0
s_4	s_3	s_4	0	0

Tabla 11.4: Tabla de estados de la MEF de la Fig. 11.4.

entrada x	1	0	1	0	1	1	–
estado f	s_0	s_3	s_1	s_2	s_3	s_0	s_3
salida y	0	0	1	0	0	0	–

Tabla 11.5: Sucesivos estados y salidas con la cadena de entrada x y la MEF de la Fig. 11.4.

entrada $x_1x_2...x_k$ es la cadena que empieza en 0, seguida de x_1, seguida de x_2, ..., y finaliza con x_{k-1}. El diagrama de estados de esta MEF se muestra en la Fig. 11.3.

Ejemplo. Describir una MEF que retorna un 1 ssi la cadena de entrada x contiene tres unos consecutivos al final. Solución: la MEF pedida tiene que tener 3 estados:

- El estado s_0 recuerda que la entrada previa no es 1, si es que existe;
- El estado s_1 recuerda que la entrada previa ha sido 1 pero la entrada anterior a la previa era un 0;
- El estado s_2 recuerda que las dos entradas previas han sido un 1.

Entonces,

- Una entrada de 1 lleva de s_0 a s_1 porque se ha leído un único 1, y no dos unos consecutivos;
- Si se leen dos unos consecutivos, entonces se pasa del estado s_1 al s_2, y del s_2 a s_2, porque se han leído al menos dos unos consecutivos;
- La entrada 0 lleva de cualquier estado al s_0 porque interrumpe cualquier secuencia de unos;
- Cuando se lee un 1 estando en s_2 se queda en s_2, pues se han aparecido tres unos consecutivos;
- Esta MEF es un ejemplo de un **reconocedor de lenguajes**, porque retorna un 1 sólo cuando la cadena de entrada tiene una determinada propiedad.

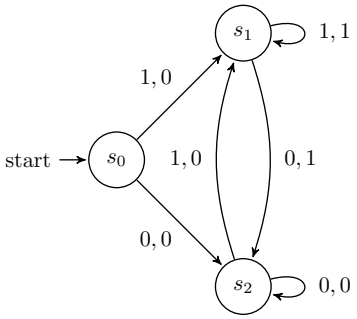

Figura 11.5: Diagrama de estados de una MEF que atrasa la entrada $x_1x_2...x_k$ en un símbolo, resultando la salida $0x_1x_2...x_{k-1}$.

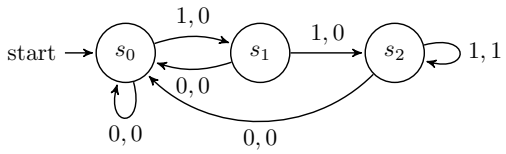

Figura 11.6: Diagrama de estados de una MEF que retorna un 1 ssi la cadena de entrada x contiene tres unos consecutivos.

El diagrama de estados de esta MEF se muestra en la Fig. 11.6.

11.3. Máquinas de estado finito sin salida

Intro

Una de las aplicaciones de los MEF es el reconocimiento de lenguajes con un correlato en los compiladores. En la Sec. anterior se mostró un ejemplo de MEF con salida para reconocer un lenguaje dando la salida 1 cuando la cadena tiene una determinada propiedad, o 0 en caso contrario. En otro tipo de MEF, en lugar de dar salidas a través de la función g, producen sólo estados finales, donde la cadena ingresada es reconocida ssi una transición del estado inicial a uno de los estados finales.

Conjunto de cadenas

Definiciones. Sean V un alfabeto, y A y B subconjuntos de V^*.

- La *concatenación* de A y B se denota con AB y es el conjunto de todas las cadenas de la forma xy, donde x es una cadena de A e y es una cadena de B;
- La n-concatenación de A se denota con A^n, con $n = 0, 1, 2, ...$ y esta dado por $A^0 = \{\lambda\}$, y $A^{n+1} = A^n A$, con $n = 0, 1, 2, ...$;
- El *cierre* de Kleene de A se denota con A^* y está dado por la unión de todos los subconjuntos con cualquier concatenación de las cadenas de A $A^* = \bigcup_{k=0}^{\infty} A^k$.

Ejemplo. Sean los conjuntos $A = \{0, 11\}$ y $B = \{1, 10, 110\}$. Hallar las concatenaciones AB y BA. Solución: $AB = \{01, 010, 0110, 11, 110, 1110\}$, y $BA = \{10, 100, 1100, 11, 101, 1101\}$.

Ejemplo. Sea el conjunto $A = \{1, 00\}$. Hallar A^n para $n = 0, 1, 2$. Solución: $A^0 = \{\lambda\}$, $A^1 = A^0 A = \{\lambda\} = \{1, 00\}$, $A^2 = A^1 A = \{11, 100, 001, 0000\}$.

Ejemplo. Hallar el Cierre de Kleen (CK) de los conjuntos $A = \{0\}$, $B = \{0, 1\}$, y $C = \{11\}$. Solución:

. $A = \{0\}$, el CK (A) es la concatenación de la cadena 0 consigo mismo un número arbitrario de veces, luego $A^* = \text{CK}(A) = \{0^n\}$, con $n = 0, 1, 2, ...$;
. $B = \{0, 1\}$, el CK (B) es la concatenación de las cadenas 0 y 1 consigo mismo un número arbitrario de veces, luego $B^* = \text{CK}(B) = V^*$

. $C = \{11\}$, el CK (C) es la concatenación de la cadena 11 consigo mismo un número arbitrario de veces, resultando un número par de unos, luego $C^* = \text{CK}(C) = \{1^{2n}\}$, con $n = 0, 1, 2, ...$

Definiciones.

- **Autómata de Estado Finito Determinista** (AEF determinista): es una MEF sin salida dada por la 5-túpla $\mathcal{A} = (S, I, f, s_0, F)$, donde:
  - Un conjunto finito S de *estados*;
  - Un conjunto finito I de símbolos de *entrada*;
  - Una función de transición $f : S \times I \to S$, que asigna a cada par (estado,entrada) un **único** estado siguiente;
  - Un estado inicial s_0;
  - Un subconjunto F de S de estados *finales* (o estados de aceptación);
- Función de transición en un AEF: sea una cadena $x_1x_2...x_k$ una cadena de I^*, entonces $f(s, x)$ es el estado obtenido al tomar sucesivamente como entrada a cada símbolo de la cadena x, de izquierda a derecha, comenzando en el estado inicial s_0:
  . De s_0 a s_1 donde $s_1 = f(x_1, s_0)$;
  . De s_1 a s_2 donde $s_2 = f(x_2, s_1)$;
  . etc.
  . De s_{k-1} a s_k donde $s_k = f(x_k, s_{k-1})$.
- *Cadena reconocida* o *cadena aceptada* por un AEF: si transforma el estado inicial s_0 en algunas estado final, i.e. $f(s_0, x)$ es un estado de f;
- *Lenguaje reconocido* o *lenguaje aceptado* por un AEF: es el conjunto de todas las cadenas reconocidas por la tupla $\mathcal{A}$;
- *AEF equivalentes*: dos AEF son equivalentes si ambos reconocen un mismo lenguaje.

Observación.

- En un AEF el conjunto de salida es $O = \{0, 1\}$, y todas las aristas que *llegan* a cada vértice tienen una misma etiqueta (ver el siguiente ejemplo);
- Diagrama de Estado de un AEF: es similar al de una MEF pero se lo simplifica eliminando los rótulos de las salidas, mientras que los estados de *aceptación* **se marcan con círculos dobles**.

Ejemplo. Trace el diagrama de estados del AEF descripto por la tupla $\mathcal{A} = (S, I, f, s_0, F)$, con los estados $S = \{s_0, s_1, s_2, s_3\}$, las entradas $I = \{0, 1\}$, los estados finales $F = \{s_0, s_3\}$, y la función de transición f listada en Tabla 11.6. Solución: el diagrama de estados asociado es trazado en la Fig. 11.7.

Ejemplo. Encontrar los lenguajes reconocidos por los AEF deterministas $\mathcal{A}_1$, $\mathcal{A}_2$, y $\mathcal{A}_3$ trazados en la Fig. 11.8. Solución: en cada caso:

. En $\mathcal{A}_1$: el único estado final es s_0. Las cadenas que transforman s_0 en s_0 son la cadena vacía y cualquier cadena vacía y cualquier cadena de unos. Entonces, el lenguaje es $L(M_1) = \{1^n \mid n = 0, 1, 2, ...\}$;

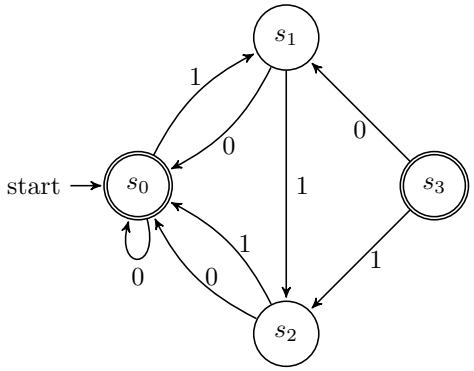

Figura 11.7: Diagrama de estados para el AEF descripto por la tabla de estados 11.6.

	estado siguiente f	
estado	0	1
s_0	s_0	s_1
s_1	s_0	s_2
s_2	s_0	s_0
s_3	s_2	s_1

Tabla 11.6: Tabla de estados del AEF de la Fig. 11.7.

. En $\mathcal{A}_2$: el único estado final es s_2. Las únicas cadenas que transforman s_0 en s_1 son 1 y 01. Entonces, el lenguaje es $L(M_2) = \{1, 01\}$;
. En $\mathcal{A}_3$: los estados finales son s_0 y s_3. Las únicas cadenas que transforman s_0 en s_0 son λ, 0, 00, 000, ... Las únicas cadenas que transforman s_0 en s_3 son las que empiezan con cero o mas ceros consecutivos, seguidos de la cadena 10, seguidos por cualquier cadena. Entonces, el lenguaje es $L(M_3) = \{0^n, 0^n 10x\}$, donde $n = 0, 1, 2, ...$ y x es cualquier cadena.

Definición. **Autómata de Estado Finito No-Determinista** (AEF-ND): es una MEF sin salida dada por la 5-túpla $\mathcal{A} = (S, I, f, s_0, F)$, donde:

- Un conjunto finito S de *estados*;
- Un conjunto finito I de símbolos de *entrada*;
- Una función de transición $f : S \times I \to S$, que asigna a cada par (estado,entrada) un conjunto $P(S)$ de estados siguientes;
- Un estado inicial s_0;
- Un subconjunto F de S de estados *finales*.

Observación.

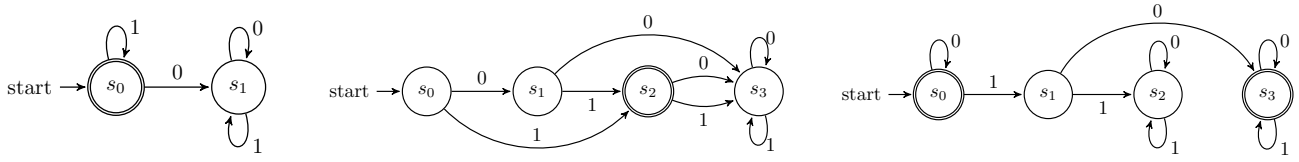

Figura 11.8: Diagrama de estados de los AEF deterministas $\mathcal{A}_1$, $\mathcal{A}_2$, y $\mathcal{A}_3$.

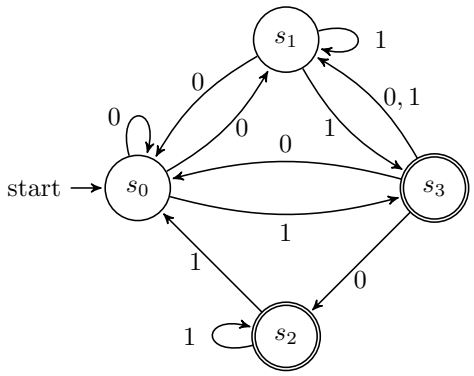

Figura 11.9: Diagrama de estados para el AEF no-determinista descripto por la tabla de estados 11.7.

- En el AEF no-determinista, la función de transición f ya no es unívoca, como en el caso anterior, es decir, se tiene más de una chance para elegir el estado siguiente;
- Es fácil darse cuenta de la no-unicidad mirando la tabla de estados porque para cada tupla (estado,entrada), en lugar de un estado siguiente, ahora hay una lista de estados siguientes;
- También es fácil darse cuenta de la no-unicidad mirando el diagrama de estados porque hay una flecha desde cada estado a todos los posibles estados siguientes.

Definiciones.

- *Cadena reconocida* o *cadena aceptada* por un AEF-ND. Cuando la cadena $x = x_1x_2...x_k$ es ingresada en un AEF-ND se tiene:
  - El símbolo x_1 transforma el estado inicial s_0 en un conjunto de estados S_1;
  - El símbolo x_2 transforma cada uno de los estados de S_1 en otros conjuntos de estados cuya unión es S_2;
  - Se continua iterando hasta el último símbolo k incluyendo en cada iteración todos los estados obtenidos en la iteración previa y el símbolo de entrada analizado.
- Se dice que el AEF-ND *reconoce* o *acepta* la cadena x si en el conjunto de todos los estados hay un estado final al que se llega desde s_0 utilizando x;
- *Lenguaje reconocido* o *lenguaje aceptado* por un AEF $\mathcal{A}$ no-determinista es el conjunto de todas las cadenas reconocidas por $\mathcal{A}$.

Ejemplo. Trace el diagrama de estados del AEF no-determinista descripto por la tupla $\mathcal{A} = (S, I, f, s_0, F)$, donde: $S = \{s_0, s_1, s_2, s_3\}$, $I = \{0, 1\}$, $F = \{s_2, s_3\}$, y la función de transición f listada en Tabla 11.7. Solución: el diagrama de estados asociado es trazado en la Fig. 11.9.

Ejemplo. Dado el diagrama de estados del AEF no-determinista mostrada en la Fig. 11.10, y tabla de transición en Tabla 11.8. obtenga el lenguaje reconocido L por este AEF. Solución: Los estados s_0 y s_4 son los estados finales. Cualquier cadena de entrada desde el estado s_0 tal que está en el conjunto de estados que pueden alcanzarse desde s_0, es una cadena reconocida por el lenguaje. Las únicas que lo verifican son constan de cero o más ceros consecutivos seguidos por 01 o 11. Entonces $L = \{0^n, 0^n01, 0^n11\}$, para $n = 0, 1, 2, ...$

	estado siguiente f	
estado	0	1
s_0	s_0, s_1	s_3
s_1	s_0	s_1, s_3
s_2		s_0,s_2
s_3	s_0, s_1, s_2	s_1

Tabla 11.7: Tabla de estados del AEF no-determinista de la Fig. 11.8.

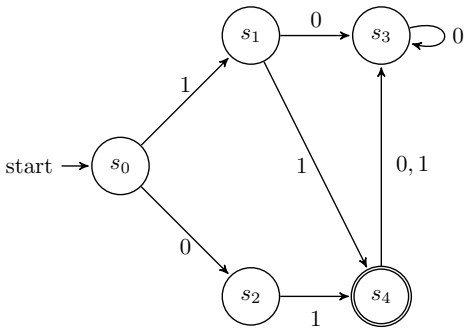

Figura 11.10: Diagrama de estados del AEF-ND descripto por la tabla de estados listada en Tabla 11.8.

Enunciado. Si el lenguaje L es reconocido por un AEF no-determinista $\mathcal{A}_0$, entonces L también es reconocido por AEF determinista $\mathcal{A}_1$.

Enunciado. Receta para obtener un AEF determinista $\mathcal{A}_1$ que reconoce a L a partir de un AEF no-determinista $\mathcal{A}_0$:

- El alfabeto de $\mathcal{A}_1$ es el mismo de $\mathcal{A}_0$;
- Cada estado de $\mathcal{A}_1$ está formado por un conjunto de estados de $\mathcal{A}_0$;
- El símbolo inicial de $\mathcal{A}_1$ es $\{s_0\}$, o sea, el conjunto que contiene al estado inicial de $\mathcal{A}_0$;
- Dado un estado $\{S_{i_1}, S_{i_2}, ..., S_{i_k}\}$ de $\mathcal{A}_1$, el símbolo de entrada x transforma ese estado en el conjunto unión de los conjuntos $f(s_{i_1})$, $f(s_{i_2})$, ..., $f(s_{i_k})$;
- Los estados de $\mathcal{A}_1$ son todos los subconjuntos del conjunto S con los estados de $\mathcal{A}_0$ obtenidos;
- Los estados finales de $\mathcal{A}_1$ son todos los conjuntos que contienen un estado final de $\mathcal{A}_0$.

Ejemplo. Obtener un AEF determinista que reconozca el mismo lenguaje L que el AEF no-determinista mostrado en la Fig. 11.10. Solución:

	estado siguiente f	
estado	0	1
s_0	s_0, s_2	s_1
s_1	s_3	s_4
s_2		s_4
s_3	s_3	
s_4	s_3	s_3

Tabla 11.8: Tabla de estados del AEF no-determinista de la Fig. 11.10.

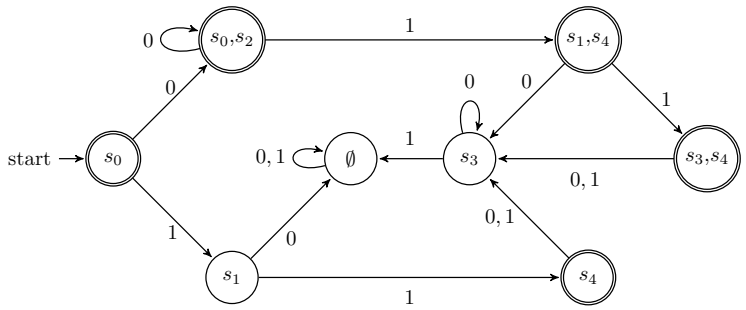

Figura 11.11: Un AEF determinista que es equivalente al no-determinista de la Fig. 11.8 obtenido con la receta del texto.

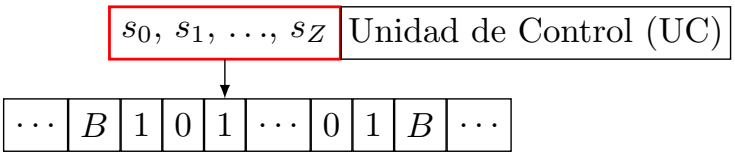

Figura 11.12: Esquema tradicional de una Máquina de Turing (MT).

- Los estados buscados de $\mathcal{A}_1$ son subconjuntos del conjunto de todos los estados de $\mathcal{A}_0$;
- El estado siguiente de un subconjunto y un símbolo de entrada es el subconjunto de todos los estados siguientes de $\mathcal{A}_0$. En este caso:
  - Para la entrada 0, como $f(s_0, 0) = \{s_0, s_2\}$, entonces el conjunto $\{s_0\}$ se transforma en $\{s_0, s_2\}$;
  - Para la entrada 1, como $f(s_0, 1) = \{s_1\}$ y $f(s_2, 1) = \{s_4\}$, entonces el conjunto $\{s_0, s_2\}$ se transforma en $\{s_1, s_4\}$;
  - Para la entrada 0, como $f(s_1, 0) = \{s_3\}$ y $f(s_4, 0) = \{s_3\}$, entonces el conjunto $\{s_1, s_4\}$ se transforma en $\{s_3\}$;
  - El conjunto vacío es uno de los estados de $\mathcal{A}_1$ porque es el conjunto que contiene todos los estados siguientes a $\{s_3\}$ con entrada 1;
  - El estado inicial es $\{s_0\}$;
  - El conjunto de todos los estados finales está formado por todos aquellos que incluyen a s_0 o s_4.

11.4. Reconocimiento de lenguajes

Omitir.

11.5. Máquina de Turing (MT)

Intro

- Las MEF, incluyendo los AEF, no se pueden usar como modelos generales de computación debido a diversas restricciones que tienen, e.g.
  - Las MEF no pueden reconocer a todos los conjuntos regulares, incluso los de fácil descripción, e.g. el conjunto $\{0^n 1^n\}$ con $n = 0, 1, 2, ...$ que las compus si reconocen empleando memoria;
  - Las MEF no pueden calcular todas las funciones, incluso funciones relativamente simples, e.g. el producto de dos enteros.
- La Máquina de Turing (MT) supera todas esas deficiencias, es más potente que las MEF, AEF, o las compus reales, porque tiene memoria infinita.

Definición de la Máquina de Turing (MT)

Definiciones.

- Función siguiente parcial: una función siguiente parcial $f(s, x)$ puede no estar definida para algún par (estado,símbolo) pero, para aquellos estados en que sí lo está, entonces es única. Es decir, la túpla (estado, símbolo, siguiente), si existiera, es único;
- Una máquina de Turing queda definida por la túpla $T = (S, I, f, s_0)$ y que consiste de:
  - Un conjunto finito de estados S;
  - Un alfabeto de símbolos de entrada I y que incluye al símbolo especial espacio en blanco B;
  - Una función siguiente parcial $f : S \times I \to S \times I \times \{L, R\}$;
  - Un símbolo inicial s_0.

Funcionamiento: para pasar de la definición matemática a una máquina (idealizada) sean (ver Fig. 11.12):

- Una *Unidad de Control* (UC), y una *cinta* dividida en celdas en un número infinito en ambos sentidos tal que, en cada paso, existe un número finito de símbolos no-blancos. Notar que la cinta representa una memoria y es infinita;
- Al comenzar la MT esta un estado inicial s_0, y que la UC está sobre el símbolo no-blanco ubicado más a la izquierda, lugar que define la posición inicial. Caso especial: si todos los símbolos son blancos, entonces la UC puede estar en cuaquier celda;
- La acción de la MT depende en cada paso del valor que toma la función parcial $f(s_i, x_j)$ en el estado s_i y el símbolo x_j;
- En cada paso, la unidad de control UC lee un símbolo x en la cinta;
- Si la MT está en un estado s y la tupla de la función parcial $f(s, x) = (s', x', d)$ está definida, entonces la UC:
  - Pasa del estado s al estado s';
  - Escribe el símbolo x' en la celda actual, borrando el anterior x;
  - La UC se mueve una celda o bien hacia la derecha si $d = R$ (*Right*), o bien hacia la izquierda si $d = L$ (*Left*);

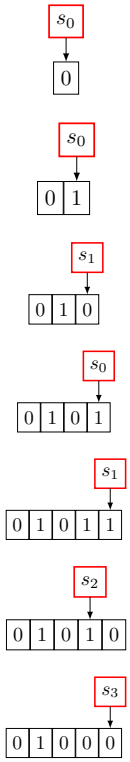

Figura 11.13: Funcionamiento de una MT dados por 7 estados.

Estas operaciones se simbolizan con la 5-tupla s, x, s', x', d');

- Pero si la función parcial $f(s, x)$ no está definida, entonces la MT se **detiene**.

Entonces, una manera habitual de representar una MT es dar un conjunto de 5-tuplas s, x, s', x', d'), quedando implícitos los conjuntos de estados y el alfabeto de entrada.

Ejemplo. Muestre el funcionamiento de la MT definida por las tuplas:

$$\begin{aligned} T_1 &:(s_0, 0, s_0, 0, R) \\ T_2 &:(s_0, 1, s_1, 1, R) \\ T_3 &:(s_1, 0, s_0, 0, R) \\ T_4 &:(s_0, 1, s_1, 1, R) \\ T_5 &:(s_1, 1, s_2, 0, L) \\ T_6 &:(s_2, 1, s_3, 0, R) \\ T_7 &:(s_2, 1, s_3, 0, R) \end{aligned} \tag{11.25}$$

Solución: la MT empieza con el estado inicial s_0 y con la UC en su posición inicial, se producen los cambios listados en la Tabla 11.9 y representados en la Fig. 11.13 donde, en el paso 7, con la tupla $(s_2, 1, s_3, 0, R)$ no hay en las tuplas dato alguna que comience con $(s_3, 0)$, por eso esta MT se detiene. Notar que la acción de esta MT es cambiar el primer par de unos consecutivos por ceros, y luego se detiene.

paso	tupla	lee	UC pasa	escribe	mov.
1	$(s_0, 0, s_0, 0, R)$	0	s_0	0	der.
2	$(s_0, 1, s_1, 1, R)$	1	s_1	1	der.
3	$(s_1, 0, s_0, 0, R)$	0	s_0	0	der.
4	$(s_0, 1, s_1, 1, R)$	1	s_1	1	der.
5	$(s_1, 1, s_2, 0, L)$	1	s_2	0	izq.
6	$(s_2, 1, s_3, 0, R)$	1	s_3	0	der.
7	$(s_2, 1, s_3, 0, R)$				

Tabla 11.9: Funcionamiento de una MT dados por 5-tuplas.

Uso de las MT para reconocer conjuntos

Definiciones. Sea una máquina de Turing (MT) definida por la tupla $T = (S, I, f, s_0)$, y sea V un subconjunto del alfabeto I, entonces:

- *Estado final* en una MT: es un estado que no es el primer estado de ninguna de las 5-tuplas que definen a la MT. Ejemplo, el estado s_3 en el ejemplo anterior;
- La máquina de Turing *reconoce* a una cadena x de V^* ssi, comenzando desde la posición inicial de T, se detiene en un estado final habiendo escrito la cadena x en la cinta. Además, la MT reconoce a un subconjunto A de V^* si x es reconocido por la MT, donde x pertenece al suconjunto A;
- La máquina de Turing *no reconoce* a una cadena x de V^* cuando, o bien T no se detiene, o bien se detiene en un estado que no sea un estado final.
- Observ.: para reconocer un subconjunto A de V^* se pueden emplear símbolos que no están en V, es decir, el alfabeto de entrada I puede incluir símbolos que no están en V, los cuales típicamente se utilizan como marcadores.

Ejemplo. Defina una MT que reconozca las cadenas de bits que tiene un 1 como segundo bit, es decir, el conjunto regular $(0 \cup 1)1(0 \cup 1)$.
Solución:

- Empezar en el primer no-blanco de la cinta (desde la izquierda);
- Moverse un lugar hacia la derecha y leer el segundo símbolo;
- Si el segundo símbolo es un 1, entonces moverse hacia un estado final;
- Pero si el segundo símbolo no es un 1 entonces, o bien detenerse, o bien pasar a otro estado que no sea un estado final;

Las operaciones anteriores se logran con las tuplas listadas en la Tabla 11.10 con las cuales:

- La MT termina en un estado final s_3 ssi la cadena de bits tiene al menos 2 bits y el segundo es un 1;
- Pero si la cadena tiene, o bien menos de dos bits, o bien el segundo bit no es un 1, entonces la MT termina en el estado s_2 que no es un estado final.

Cálculo de funciones con MT

Omitir.

paso	tupla	
T_1	$(s_0, 0, s_1, 0, R)$	
T_2	$(s_0, 1, s_1, 1, R)$	T_1 y T_2 para leer el 1er símbolo
T_3	$(s_1, 0, s_2, 0, R)$	
T_4	$(s_1, 1, s_3, 1, R)$	T_3 y T_4 para leer el 2do símbolo donde s_3 es un estado final
T_5	$(s_2, 0, s_2, 0, R)$	para no-reconocer cadenas cuyo 2do bit es 0 donde s_2 no es un estado final
T_6	$(s_0, B, s_2, 0, R)$	T_6 y T_7 para no reconocer cadenas
T_7	$(s_1, B, s_2, 0, R)$	vacías ni cadenas de un bit

Tabla 11.10: Definición de una MT con 5-tuplas.

Diferentes tipos de MT

Lectura para el hogar.

La tesis de Church-Turing

Enunciado.

- **Tesis de Church-Turing**: todo *problema resoluble con un algoritmo efectivo* admite una Máquina de Turing que también lo resuelve.
- Observ.: se dice *tesis* (en vez de *teorema*) porque la idea de un *problema resoluble con un algoritmo efectivo* es informal e imprecisa, a diferencia de un *problema resoluble con una máquina de Turing* la cual es una idea precisa;
- Comentario 1: derivados de las MT: la teoría de Turing y el cálculo lambda (de Church);
- Comentario 2: el cálculo lambda (de Church) → programación funcional → lenguajes de prgramación: Lisp, Scheme, Haskell, etc.

Nomenclatura

Indice alfabético

APÉNDICE A

Acrónimos y abreviaturas empleadas

A.1. Lista de acrónimos

AED Algoritmos y Estructuras de Datos

CE Clases de Equivalencia

COP Computación / Programación

CI Condiciones Iniciales

DA Diagrama en Arbol

DD Dominio de Discurso

DeD Demostración Directa

DeI Demostración Indirecta

DrA Demostración por Reducción al Absurdo

EC Ecuación Característica

EL Equivalencia Lógica

F Falso (por *False*)

FP Función Proposicional

GTP Guía de Trabajos Prácticos

HI Hipótesis Inductiva

LE lógicamente equivalentes

MCD Máximo Común Divisor

MCM Mínimo Común Múltiplo

PB Paso Base

PIE Principio de Inclusión-Exclusión

PIF Principio de Inducción Fuerte

PIM Principio de Inducción Matemática

PI Paso de Inducción

PR Paso Recursivo

PS Principio de la Suma

PP Principio del Palomar

PM Principio de la Multiplicación

RB Relación Binaria

RP Reglas de precedencia

RE Relación de Equivalencia

ROP Relación de Orden Parcial

ROT Relación de Orden Total

RPM Ruta de Peso Mínimo

RR Relación de Recurrencia

RRHLCC Relación de Recurrencia Homogénea, Lineal, de Coeficientes Constantes

T Verdadero (por *True*)

TH Torres de Hanoi

TV Tabla de Verdad

TP Tablas de Pertenencia

VV Valor de Verdad

V Verdadero

A.2. Lista de abreviaturas

i.e. es decir, o esto es, del latín *id est*

e.g. por ejemplo, del latín *exempli gratia*

Bibliografía

Aho, A. V., Lam, M. S., Sethi, R., and Ullman, J. D. (2008). *Compiladores: principios, técnicas y herramientas*. Pearson, Addison-Wesley Iberoamericana, 2 edition.

Aho, A. V., Sethi, R., and Ullman, J. D. (1998). *Compiladores: principios, técnicas y herramientas*. Addison-Wesley Iberoamericana, 1 edition.

Alfonseca Moreno, M., De la Cruz Echeandia, M., Ortega de la Puente, A., and Pulido Canabate, E. (2006). *Compiladores e intérpretes: teoría y práctica*. Pearson Education.

Biggs, N. (1998). *Matemática discreta*. Ediciones Vicens Vives, S.A., España, 2 edition.

Hopcroft, J. E., Motwani, R., and Ullman, J. D. (2008). *Introducción a la teoría de autómatas, lenguajes y computación*. Pearson, Addison-Wesley Iberoamericana, 3 edition.

Johnsonbaugh, R. (2005). *Matemáticas discretas*. ISBN 9789702606376. Prentice Hall, Mexico, 6 edition.

Rosen, K. H. (2004). *Matemática Discreta y sus Aplicaciones*. ISBN 9788448140731. Mc Graw Hill, Colombia, 5 edition.

APÉNDICE B

GNU Free Documentation License

Version 1.1, March 2000

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA.

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other written document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.
This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.
We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you".

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.
A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (For example, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.
The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License.
The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License.
A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, whose contents can be viewed and edited directly and straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup has been designed to thwart or discourage subsequent modification by readers is not Transparent. A copy that is not "Transparent" is called "Opaque".
Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML designed for human modification. Opaque formats include PostScript, PDF, proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML produced by some word processors for output purposes only.
The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or non-commercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical

measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.
You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies of the Document numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.
If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.
If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a publicly-accessible computer-network location containing a complete Transparent copy of the Document, free of added material, which the general network-using public has access to download anonymously at no charge using public-standard network protocols. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.
It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any,

be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has less than five).
- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- H. Include an unaltered copy of this License.
- I. Preserve the section entitled "History", and its title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K. In any section entitled "Acknowledgements" or "Dedications", preserve the section's title, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M. Delete any section entitled "Endorsements". Such a section may not be included in the Modified Version.

- N. Do not retitle any existing section as "Endorsements" or to conflict in title with any Invariant Section.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.
You may add a section entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties–for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.
You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.
The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice.
The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.
In the combination, you must combine any sections entitled "History" in the various original documents, forming one section entitled "History"; likewise combine any sections entitled "Acknowledgements", and any sections entitled "Dedications". You must delete all sections entitled "Endorsements."

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various docu-

ments with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.
You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, does not as a whole count as a Modified Version of the Document, provided no compilation copyright is claimed for the compilation. Such a compilation is called an "aggregate", and this License does not apply to the other self-contained works thus compiled with the Document, on account of their being thus compiled, if they are not themselves derivative works of the Document. If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one quarter of the entire aggregate, the Document's Cover Texts may be placed on covers that surround only the Document within the aggregate. Otherwise they must appear on covers around the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License provided that you also include the original English version of this License. In case of a disagreement between the translation and the original English version of this License, the original English version will prevail.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.
Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies

to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

> *Copyright (c) YEAR YOUR NAME. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.1 or any later version published by the Free Software Foundation; with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST. A copy of the license is included in the section entitled "GNU Free Documentation License".*

If you have no Invariant Sections, write "with no Invariant Sections" instead of saying which ones are invariant. If you have no Front-Cover Texts, write "no Front-Cover Texts" instead of "Front-Cover Texts being LIST"; likewise for Back-Cover Texts. If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.