Butlletí de la Societat Catalana de Matemàtiques
Vol. 37, núm. 1, 2022. Pàg. 5–59. DOI: 10.2436/20.2002.01.102

Autòmats de Stallings, un camí d'anada i tornada

Jordi Delgado i Enric Ventura

L'algèbre n'est qu'une géometrie écrite;
la géométrie n'est qu'une algèbre figurée.

Sophie Germain (1776–1831)

Resum: En aquest article revisem algunes de les propietats fonamentals del grup lliure i fem una exposició detallada de la teoria dels autòmats de Stallings, una interpretació geomètrica dels seus subgrups que ha estat (i segueix essent) immensament fructífera, tant com a mitjà per a entendre resultats clàssics com com a font de nous resultats. N'expliquem alguns dels més rellevants.

Paraules clau: grup lliure, subgrup, autòmat, Stallings, problema algorísmic, problema de decisió.

Classificació MSC2010: 20-02, 20E05, 20F05, 20F10, 20F65, 05C25.

1 Introducció

La relació entre l'àlgebra i la geometria és, probablement, una de les més fructíferes entre les diferents àrees matemàtiques. Val a dir que es tracta d'una relació bidireccional. Si bé inicialment l'àlgebra es va constituir com un potent recurs per a resoldre (entre d'altres) problemes geomètrics (per exemple, amb el treball d'Euclides al Llibre II dels *Elements*, molts segles més tard, de forma sistemàtica, amb el descobriment de Descartes de la geometria analítica, o, més modernament, amb el desenvolupament de la topologia algebraica), a mesura que aquesta guanyava en abstracció, i es constituïa en una disciplina matemàtica *per se*, s'ha anat configurant també una relació fructífera en sentit contrari: els arguments geomètrics i topològics han esdevingut un instrument essencial per a resoldre problemes d'origen i motivació algebraics.

Aquesta influència ha estat especialment acusada durant el darrer segle i escaig en l'àmbit de la teoria de grups infinits, on l'enfocament combinatori (basat en la idea de presentació d'un grup) ha donat pas a una explosió de mètodes i arguments geomètrics que han acabat conformant l'àrea anomenada *teoria geomètrica de grups*.

El concepte de presentació d'un grup (vegeu la definició 20) es basa en el de *grup lliure*, una mena de llenç[1] on tots els grups poden ser dibuixats. No és, per tant, gens sorprenent la rellevància que ha tingut l'estudi del grup lliure en el desenvolupament de la teoria de grups, especialment dels grups infinits. Per als no avesats, convé recordar que el grup lliure admet una interpretació molt senzilla i intuïtiva com a «conjunt de paraules» usant un conjunt predefinit de lletres (vegeu la secció 2).

La concisió de la descripció combinatòria donada per les presentacions és especialment propícia per a la formulació de qüestions algorísmiques, que, durant el darrer segle, han esdevingut un tercer ingredient estretament lligat a l'àlgebra i la geometria dels grups.

Malgrat la seva aparent simplicitat, reforçada pel fet que els seus subgrups són també lliures (teorema de Nielsen-Schreier), les relacions entre els subgrups del grup lliure són intricades i amaguen sorpreses interessants. Per exemple, veurem que —en contrast amb el que succeeix en els ambients abelians clàssics— el grup lliure de rang 2 té subgrups de qualsevol rang finit, i fins i tot de rang infinit. I estudiarem el comportament de les seves interseccions, que va donar lloc a la coneguda conjectura de Hanna Neumann, un problema obert durant més de mig segle, i resolt fa uns anys independentment per Friedman a [18] i per Mineyev a [36] (vegeu també les simplificacions remarcables de Dicks a [18, apèndix B] i [17]).

Tot i la innegable complexitat del seu reticle de subgrups, veurem que, des del punt de vista algorísmic, els grups lliures, en general, es comporten molt bé. Multitud de problemes algorísmics naturals (incloent-hi els problemes clàssics de Dehn, així com els de la pertinença,[2] la intersecció de subgrups o la finitud de l'índex) són decidibles al grup lliure $\mathbb{F}_n$; molts d'ells gràcies, precisament, a tècniques basades en els autòmats de Stallings. Vegeu [12] per a un inventari (no exhaustiu) de problemes decidibles usant autòmats de Stallings, els protagonistes d'aquest article. Cal assenyalar, però, que els comportaments díscols tampoc no estan lluny: és suficient fer un producte directe de dos grups lliures per començar a trobar problemes molt naturals que són algorísmicament indecidibles (vegeu [35]).

En aquest article començarem fent una breu introducció al grup lliure i les seves propietats principals. Tot seguit, exposem els fonaments de la teoria dels autòmats de Stallings, una interpretació geomètrica molt aclaridora dels subgrups del grup lliure que, a més, ha resultat immensament fructífera en termes d'aplicacions. A la secció 4 en revisarem algunes de les més importants.

---

1 Com veurem a la secció 2, un full d'origami, del qual sorgeixen tots els altres grups després de «plegar-lo» adequadament, és potser una metàfora més acurada.

2 En anglès, *Membership Problem* (MP).

1.1 Notació, terminologia i convenis

La major part de la notació i la terminologia utilitzades en aquest article són estàndard; tanmateix, a continuació aclarim alguns aspectes per evitar possibles confusions.

El conjunt dels números naturals, designat per $\mathbb{N}$, inclou el zero, i especifiquem condicions sobre ell mitjançant subíndexs; per exemple, designem per $\mathbb{N}_{\geq 1}$ el conjunt de números naturals estrictament positius. El cardinal d'un conjunt S es designa per $\#S$, i la notació $|\cdot|$ es reserva per a indicar longitud (en diferents contextos). Escrivim com a $[m,n] = \{k \in \mathbb{N} : m \leq k \leq n\}$ el conjunt de números naturals entre m i n (ambdós inclosos) i $[0,\aleph_0] = \mathbb{N} \cup \{\aleph_0\}$.

Designem per $\mathbb{F}$ un grup lliure genèric, mentre que les notacions $\mathbb{F}_A$ i $\mathbb{F}_\kappa$ (resp., $\mathbb{F}_n$) s'usen per a emfatitzar una base A i el rang κ (resp., n, si és finit) de $\mathbb{F}$, respectivament. Les primeres lletres de l'alfabet llatí ($a,b,c,\ldots$) s'usen normalment per a designar els símbols dels alfabets formals, mentre que les últimes ($u,v,w,\ldots$) solen designar paraules formals o elements del grup lliure.

Les funcions actuen per la dreta. És a dir, designem per $(x)\varphi$ (o simplement per $x\varphi$) la imatge de l'element x per la funció φ, i designem per $\phi\psi$ la composició $A \xrightarrow{\phi} B \xrightarrow{\psi} C$. En conseqüència, escrivim, per exemple, $g^h = h^{-1}gh$ (el conjugat de g per h) i $[g,h] = g^{-1}h^{-1}gh$ (el commutador de g i h).

Designem la conjugació (d'elements o subgrups) per $\sim$, i escrivim $H \leqslant G$, $H \trianglelefteqslant G$, $H \leqslant_{\mathsf{fg}} G$, $H \leqslant_{\mathsf{ff}} G$, $H \leqslant_{\mathsf{fi}} G$, per designar que H és subgrup, subgrup normal, subgrup finitament generat, factor lliure, i subgrup d'índex finit (de G), respectivament.

2 Grup lliure

Comencem recordant les definicions de monoide i de grup. Un *monoide* és un parell $(G,\cdot)$ on G és un conjunt arbitrari, i $\cdot\colon G \times G \to G$, $(g_1,g_2) \mapsto g_1 \cdot g_2$ és una operació associativa amb element neutre (que representarem per 1). Si, a més, tot element $g \in G$ té un (únic) invers g^{-1} (*i. e.*, tal que $g \cdot g^{-1} = g^{-1} \cdot g = 1$) diem que $(G,\cdot)$ és un *grup*. Si $A \subseteq G$, designarem per A^{-1} el conjunt d'inversos d'elements de A, *i. e.*, $A^{-1} = \{a^{-1} : a \in A\}$. Usualment ometrem el símbol per a l'operació i escriurem $g \cdot h = gh$. Si, a més, $gh = hg$ per a tot $g,h \in G$, direm que el monoide (o el grup) és *commutatiu* o *abelià*; en aquest cas l'operació se sol designar per «+» i l'element neutre per 0 (*notació additiva*).

Hi ha moltes maneres de definir els grups lliures i les seves bases: geomètriques, algebraiques, combinatòries, categòriques… La més concreta és, potser, la que adapta la noció estàndard de base de l'àlgebra lineal al context de grups, mentre que la més abstracta és probablement la categòrica.[3] Al llarg d'aquesta secció les desenvoluparem totes dues i veurem com estan relacionades. Abans, però, emfasitzem el polimorfisme del grup lliure amb dues caracteritzacions addicionals, de caràcter geomètric, que enunciem sense demostració.

3 Vegeu `https://en.wikipedia.org/wiki/Abstract_nonsense`.

TEOREMA 1. *Sigui F un grup. Aleshores, els enunciats següents són equivalents:*

(a) *F és un grup lliure;*

(b) *F és el grup fonamental d'un graf connex;*[4]

(c) *F actua lliurement i sense inversions sobre les arestes d'un arbre.*[5]

Tot i la indubtable rellevància d'aquest resultat, hem preferit fer una presentació «algebraica» del grup lliure, amb l'esperança que el lector la trobi més natural. Comencem notant que és immediat de la definició de grup que els factors trivials 1 i els productes gg^{-1} (anomenats *cancel·lacions*) són superflus en qualsevol producte $g_1 \cdots g_n$ d'elements d'un grup G (per exemple, $h1k = hk$ i $hgg^{-1}k = hk$). Un producte en el qual no apareixen factors trivials ni cancel·lacions s'anomena *producte reduït* (incloent-hi el producte buit, que representa l'element neutre —també anomenat *element trivial* en aquest context). És clar que, eliminant repetidament factors trivials i cancel·lacions, tot producte es pot convertir en un producte reduït, amb el mateix resultat dins de G.

DEFINICIÓ 2. Sigui G un grup i $A \subseteq G$. Diem que A és un subconjunt *lliure* (o *independent*) en G si dos productes reduïts diferents d'elements de $A^{\pm} = A \cup A^{-1}$ sempre donen resultats diferents de G (o, equivalentment, si el buit és l'únic producte reduït que dona l'element trivial de G). Diem que A *genera* (o que és un *conjunt de generadors* per a) G si tot element de G és igual a un producte (que podem suposar reduït) d'elements de $A^{\pm}$. Finalment, diem que A és una *base* de G i que G és un grup lliure (sobre A) si A és lliure en G i genera G. Farem servir la notació $\mathbb{F}$ per a referir-nos als grups lliures.

DEFINICIÓ 3. S'anomena *rang* d'un grup G, designat per $\operatorname{rk}(G)$, la mínima cardinalitat d'un conjunt de generadors per a G. Si un grup admet un conjunt de generadors finit, direm que és *finitament generat*.

EXEMPLE 4. Considerem el grup dels enters $\mathbb{Z}$ amb notació additiva.[6] Els conjunts $\{1\}$ i $\{-1\}$ en són bases ja que, clarament, generen $\mathbb{Z}$ i cap expressió de la forma

$$1 + 1 + \overset{n)}{\cdots} + 1 \quad \text{o bé} \quad (-1) + (-1) + \overset{n)}{\cdots} + (-1)$$

amb $n \neq 0$ dona igual a zero. En particular, $\{1\}$ és un conjunt de generadors (òbviament mínim) de $\mathbb{Z}$, i per tant $\operatorname{rk}(\mathbb{Z}) = 1$.

EXEMPLE 5. En canvi, $\{\overline{1}\} = \{1+n\mathbb{Z}\}$ *no* és una base de $\mathbb{Z}/n\mathbb{Z}$, per a $n \geq 2$, ja que, tot i ser-ne generador, no és un subconjunt lliure, degut a la *relació* $\overline{1} + \overset{n)}{\cdots} + \overline{1} = \overline{0}$. De fet, *cap* subconjunt $A \subseteq \mathbb{Z}/n\mathbb{Z}$ no és base ja que el subconjunt buit no genera, i qualsevol element $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ compleix la relació: $\overline{a} + \overset{n)}{\cdots} + \overline{a} = \overline{0}$; per tant, el grup $\mathbb{Z}/n\mathbb{Z}$ no és lliure.

4 Vegeu la definició 33 per a la definició de grup fonamental, i l'observació 50 i la proposició 54(ii) per a una reformulació en termes d'autòmats.

5 Un arbre és un graf connex sense cicles. Vegeu [6, capítol 3].

6 En notació additiva, 1 és el generador natural del grup $(\mathbb{Z}, +)$ i no pas el neutre, designat per 0.

Noteu que el grup trivial és lliure (amb base $\emptyset$ i, per tant, amb rang 0) i, com hem vist a l'exemple anterior, el grup dels enters $\mathbb{Z}$ també és lliure (i té dues bases, $\{1\}$ i $\{-1\}$). És immediat de la definició que aquests són els únics grups lliures abelians. D'altra banda, hem vist que $\mathbb{Z}/n\mathbb{Z}$ no és lliure per a cap $n \geq 2$. Amb el mateix argument es pot demostrar que cap grup finit no és lliure, excepte el trivial.

Observació 6. Si $A \subseteq \mathbb{F}$ és base d'un grup (lliure) $\mathbb{F}$, aleshores A és un sistema de generadors *minimal* de $\mathbb{F}$; és a dir, $\langle A \rangle = \mathbb{F}$, però $\langle A \setminus S \rangle \neq \mathbb{F}$ per a tot $\emptyset \neq S \subseteq A$.

Prova. Si existís un $S \neq \emptyset$ tal que $A \setminus S$ generés tot $\mathbb{F}$, aleshores, per qualsevol $s \in S$, tindríem $s \in \mathbb{F} = \langle A \setminus S \rangle$, i l'element $s \in G$ el podríem obtenir com una lletra de A i, alhora, com un producte reduït en $A \setminus S$, contradient la hipòtesi que A és una família lliure. $\square$

Tot seguit construirem grups lliures amb bases de cardinal arbitrari.

Definició 7. Sigui A un conjunt (finit o infinit), que anomenarem *alfabet*, o conjunt de *lletres* elementals. Una *paraula* sobre A és una seqüència ordenada i finita de lletres, $a_1 a_2 \cdots a_n$, on $n \geqslant 0$, i $a_i \in A$, amb possibles repeticions. El nombre total de lletres n d'una paraula s'anomena *longitud*, i escrivim $|a_1 a_2 \cdots a_n| = n$. Com a conveni, designarem per 1 l'única paraula de longitud zero, o *paraula buida*. El conjunt de totes les paraules sobre A el designem per A^*.

Observació 8. Per a tot alfabet A, el conjunt A^* és un monoide amb l'operació de concatenació, $u \cdot v = uv$, $u, v \in A^*$. A més, $|uv| = |u| + |v|$ i, per tant, l'únic element invertible és el neutre, 1.

Aprofitant la notació exponencial per a productes successius d'un element amb si mateix, $u^n = u \cdot \overset{n)}{\cdots} \cdot u$, podem abreujar les paraules de A^* tot escrivint la potència corresponent cada vegada que una lletra apareix diverses vegades consecutivament; per exemple, $aabaaabbab = a^2ba^3b^2ab$. Si fem això agrupant al màxim, cadascuna de les potències de lletres que apareixen s'anomena una *síl·laba*; per exemple, la paraula anterior té longitud $2 + 1 + 3 + 2 + 1 + 1 = 10$, i 6 síl·labes.

Observem que, sobre un alfabet d'una sola lletra, $A = \{a\}$, el monoide A^* és isomorf al dels números naturals (en efecte, $A^* = \{1, a, a^2, a^3, \ldots\}$ i $a^n \cdot a^m = a^{n+m}$, per $n, m \geqslant 0$). En canvi, sobre un alfabet A de dues o més lletres, el monoide A^* és força més complicat; en particular, com que $ab \neq ba$, no és un monoide commutatiu.

Anem en la bona direcció per aconseguir que A sigui una base de A^*: efectivament A genera A^*, i cap producte de longitud $n \neq 0$ d'elements de A no dona mai igual a 1. El problema és que A^* només és un monoide (de fet, un monoide lliure); però és molt lluny de ser un grup ja que cap element, llevat del neutre 1, no té invers. Per a convertir-lo en un grup, haurem d'introduir els inversos de tots els elements. Com veurem, serà suficient d'introduir «inversos formals» per a les lletres elementals, $A^{-1} = \{a^{-1} : a \in A\}$. És a dir, doblem l'alfabet A amb una lletra nova per cadascuna de les antigues, i el designem per $A^{\pm} = A \sqcup A^{-1} = \{a, a^{-1} \mid a \in A\}$. La notació usada suggereix que cada a^{-1} és l'invers del corresponent a, i així serà en acabar la construcció, però de moment és només una qüestió notacional: a i a^{-1} són simplement dues lletres diferents del nou alfabet $A^{\pm}$ (inverses formals, si voleu).

Considerem el monoide $(A^{\pm})^*$, és a dir, el conjunt de totes les paraules sobre l'alfabet $A^{\pm}$ amb l'operació de concatenació. Per exemple, si $A = \{a, b\}$ tindrem $A^{\pm} = \{a, a^{-1}, b, b^{-1}\}$ i $(A^{\pm})^*$ conté exactament $4^2 = 16$ paraules de longitud 2, a saber a^2, aa^{-1}, ab, ab^{-1}, $a^{-1}a$, a^{-2}, $a^{-1}b$, $a^{-1}b^{-1}$, ba, ba^{-1}, b^2, bb^{-1}, $b^{-1}a$, $b^{-1}a^{-1}$, $b^{-1}b$, i b^{-2} (on $x^{-n} = (x^{-1})^n$, per $n \geqslant 0$). Per a aconseguir que, per cada lletra $a \in A$, l'element a^{-1} sigui realment l'invers de a, cal fer alguna cosa per a forçar que $aa^{-1} = 1 = a^{-1}a$. Una manera d'aconseguir-ho és fent el conjunt quocient per la relació d'equivalència apropiada.

Definició 9. Anomenem *reducció elemental*, designada per $\rightsquigarrow$, la transformació consistent a eliminar una cancel·lació dins d'una paraula; és a dir, si $a \in A$ i $u, v \in (A^{\pm})^*$, aleshores

$$uaa^{-1}v \rightsquigarrow uv \quad \text{i} \quad ua^{-1}av \rightsquigarrow uv. \tag{1}$$

La transformació inversa l'anomenem *inserció elemental*, i la seva clausura simètrica (designada per $\leftrightsquigarrow$), *transformació elemental*. És a dir,

$$w \leftrightsquigarrow w' \quad \Leftrightarrow \quad w \rightsquigarrow w' \text{ ó } w' \rightsquigarrow w. \tag{2}$$

Òbviament, si $w \leftrightsquigarrow w'$ llavors $|w| = |w'| \pm 2$. Finalment, definim $\sim$ com la *clausura reflexotransitiva* de $\leftrightsquigarrow$; és a dir, per a tot $w, w' \in (A^{\pm})^*$

(i) $w \sim w$ i

(ii) $w \sim w' \Leftrightarrow \exists w_0 = w, w_1, \ldots, w_n = w'$ t.q. $w_0 \leftrightsquigarrow w_1 \leftrightsquigarrow \cdots \leftrightsquigarrow w_n$,

és a dir, $w \sim w'$ si es pot passar de w a w' fent una quantitat finita de reduccions i/o insercions elementals, entenent que això inclou el cas amb $n = 0$ passes. Per exemple, $a^2a^{-1}bb^{-1}a^{-2}b \sim a^2c^{-1}ca^{-3}b$ ja que

$$a^2a^{-1}bb^{-1}a^{-2}b \rightsquigarrow abb^{-1}a^{-2}b \rightsquigarrow aa^{-2}b \leftsquigarrow a^2a^{-3}b \leftsquigarrow a^2c^{-1}ca^{-3}b.$$

És immediat de la definició que $\sim$ és una relació d'equivalència al conjunt $(A^{\pm})^*$. Podem considerar, doncs, el conjunt quocient, que designem per $\mathbb{F}_A = (A^{\pm})^*/\sim$. És clar que a la classe $[w] \in \mathbb{F}_A$ hi ha precisament totes les paraules «iguals» a $w \in (A^{\pm})^*$ mòdul les igualtats elementals desitjades $aa^{-1} = 1 = a^{-1}a$, $a \in A$. Finalment, definim a $\mathbb{F}_A = (A^{\pm})^*/\sim$ una operació binària (clarament ben definida) adaptant de manera natural la concatenació de $(A^{\pm})^*$: per a tot $u, v \in (A^{\pm})^*$,

$$[u] \cdot [v] = [uv]. \tag{3}$$

Proposició 10. *El conjunt* $\mathbb{F}_A$ *amb l'operació* (3) *és un grup.*

Prova. La propietat associativa és conseqüència immediata de l'associativitat de la concatenació en $(A^{\pm})^*$; l'element neutre és $[1]$; i l'invers d'una classe $[a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n}] \in \mathbb{F}_A$ (on $\epsilon_j = \pm 1$) és la classe $[a_{i_n}^{-\epsilon_n} \cdots a_{i_1}^{-\epsilon_1}]$. Per tant, $\mathbb{F}_A$ amb l'operació (3) té estructura de grup. □

Ja tenim el grup $\mathbb{F}_A$ construït. Vegem ara que $\mathbb{F}_A$ és lliure amb base A. La manera natural de veure A dins de $\mathbb{F}_A$ és com el conjunt de classes de les paraules positives de longitud 1, és a dir, $\{[a] : a \in A\}$. Però hi ha un petit problema tècnic aquí: estem segurs que dues lletres positives diferents estan sempre en classes diferents? En altres paraules, estem segurs que l'aplicació $\iota_A \colon A \to \mathbb{F}_A$, $a \mapsto [a]$, és injectiva? Intuïtivament sembla clar que, si $a, b \in A$ són dues lletres diferents, llavors $a \not\sim b$ ja que no sembla possible transformar la lletra a en una de diferent b, simplement usant reduccions i insercions elementals. Per a demostrar-ho rigorosament usarem la proposició següent, que és important també per a altres qüestions.

Definició 11. Una paraula $w \in (A^{\pm})^*$ és *reduïda* si no conté cap parell de lletres consecutives mútuament inverses formals. És a dir, $w = a_{i_1}^{\epsilon_1} a_{i_2}^{\epsilon_2} \cdots a_{i_n}^{\epsilon_n}$ és reduïda si, sempre que dues lletres consecutives coincideixin, $a_{i_j} = a_{i_{j+1}}$, els seus signes també, $\epsilon_j = \epsilon_{j+1}$. El conjunt de paraules reduïdes en A el designarem per $R(A) \subseteq (A^{\pm})^*$.

Proposició 12. *Tota classe d'equivalència* $[w] \in \mathbb{F}_A$ *conté una i només una paraula reduïda (designada per* $\overline{w}$*).*

Prova. És clar que tota classe conté alguna paraula reduïda, ja que podem prendre un representant qualsevol $w \in [w]$ i (si no és ja reduït) reduir-lo aplicant reduccions elementals successives fins que no en quedi cap de disponible. Aquest procés sempre acaba en un nombre finit de passos, ja que $|w|$ és finit i a cada pas la longitud disminueix en dues unitats.

Per veure la unicitat, suposem que dues paraules reduïdes diferents $w, w' \in R(A)$ pertanyen a la mateixa classe i busquem una contradicció. Sigui $w = w_0 \leftrightsquigarrow w_1 \leftrightsquigarrow \cdots \leftrightsquigarrow w_{n-1} \leftrightsquigarrow w_n = w'$ una successió de transformacions elementals minimitzant $N = \sum_{i=0}^{n} |w_i|$. Com que $w \neq w'$ i ambdues són reduïdes, no pot ser ni $n = 0$, ni $n = 1$, ni $n = 2$; per tant, $n \geqslant 3$. A més, $|w_0| < |w_1|$ i $|w_{n-1}| > |w_n|$ i, per tant, hi ha un $j \in [1, n-1]$ tal que $|w_{j-1}| < |w_j| > |w_{j+1}|$. Fixem-nos ara en les reduccions elementals $w_{j-1} \leftsquigarrow w_j \rightsquigarrow w_{j+1}$, i en les dues lletres de w_j afectades per cadascuna d'aquestes reduccions. Si n'hi ha una (o dues) en comú, aleshores $w_{j-1} = w_{j+1}$ cosa que contradiu la minimalitat de N. I si els parells de lletres eliminades en ambdues reduccions són disjunts, aleshores $w_j = xa^{\epsilon}a^{-\epsilon}yb^{\delta}b^{-\delta}z$, per a certes paraules $x, y, z \in (A^{\pm})^*$, certes lletres $a, b \in A$, i certs signes $\epsilon, \delta = \pm 1$; canviant $w_{j-1} \leftsquigarrow w_j \rightsquigarrow w_{j+1}$ per $w_{j-1} = xyb^{\delta}b^{-\delta}z \rightsquigarrow xyz \leftsquigarrow xa^{\epsilon}a^{-\epsilon}yz = w_{j+1}$ ó $w_{j-1} = xa^{\epsilon}a^{-\epsilon}yz \rightsquigarrow xyz \leftsquigarrow xyb^{\delta}b^{-\delta}z = w_{j+1}$ segons convingui, reduïm el valor de N, en contradicció també amb la seva minimalitat. □

OBSERVACIÓ 13. Donat que a tota classe $[w] \in \mathbb{F}_A$ hi ha una única paraula reduïda $\overline{w} \in R(A)$ (tal que $[w] = [\overline{w}]$), podem pensar el grup $\mathbb{F}_A$, alternativament, com el conjunt de paraules reduïdes $R(A)$ amb l'operació $u \cdot v = \overline{uv}$. Sovint aplicarem aquesta interpretació i escriurem simplement $w \in \mathbb{F}_A$ per referir-nos a l'element $[w] = [\overline{w}] \in \mathbb{F}_A$.

Com que les lletres (les paraules de llargada 1, per ser precisos) són clarament reduïdes, el resultat següent és immediat de la proposició 12.

COROL·LARI 14. *L'aplicació $\iota_A \colon A \to \mathbb{F}_A$, $a \mapsto [a]$ és injectiva.* □

Ara, pensant $A \subseteq \mathbb{F}_A$ via ι_A, és clar que tota paraula reduïda és producte d'elements de $A^{\pm}$ (és a dir, A genera $\mathbb{F}_A$), i que el buit és l'únic producte reduït d'elements de $A^{\pm}$ que dona $1 \in \mathbb{F}_A$ (és a dir, A és un subconjunt lliure de $\mathbb{F}_A$).

COROL·LARI 15. *Per a tot alfabet A, el grup $\mathbb{F}_A$ és lliure amb base A.* □

Hem provat l'existència de grups lliures amb bases de qualsevol cardinal. La pregunta natural ara és quan dos d'aquests grups, $\mathbb{F}_A$ i $\mathbb{F}_{A'}$, són isomorfs (com a grups). I és força raonable pensar que serà, precisament, quan A i A' tinguin el mateix cardinal. Efectivament, així és; i per a demostrar-ho ens serà de molta utilitat la caracterització següent de «grup lliure», que, en realitat, n'és la definició estàndard en termes categòrics.

PROPOSICIÓ 16. *Siguin F un grup i $A \subseteq F$. Designem per $\iota_A \colon A \hookrightarrow F$ la inclusió natural. Aleshores, F és lliure amb base A si i només si, per a tot grup G, i tota aplicació (de conjunts) $\varphi \colon A \to G$, existeix un únic morfisme de grups $\widetilde{\varphi} \colon F \to G$ tal que $\iota_A \widetilde{\varphi} = \varphi$.*

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d, hook, "\iota_A"'] & G \\ F \arrow[ur, dashed, "\exists!\widetilde{\varphi}"'] & \end{tikzcd}$$

FIGURA 1: Definició categòrica de grup lliure F.

PROVA. Suposem que F és lliure amb base A. Donats G i $\varphi \colon A \to G$, el morfisme $\widetilde{\varphi} \colon F \to G$ que busquem ha de complir $a\widetilde{\varphi} = a\varphi$ per a tot element $a \in A$ i, per tant, $(a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n})\widetilde{\varphi} = (a_{i_1}\widetilde{\varphi})^{\epsilon_1} \cdots (a_{i_n}\widetilde{\varphi})^{\epsilon_n} = (a_{i_1}\varphi)^{\epsilon_1} \cdots (a_{i_n}\varphi)^{\epsilon_n}$, per a tot producte reduït d'elements de A, $a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n}$. Com que A genera F, el possible morfisme $\widetilde{\varphi}$ queda completament determinat per φ, la qual cosa ens dona la unicitat. D'altra banda, com que A és un subconjunt lliure de F (*i. e.*, cap element de F no admet dues expressions diferents com a producte reduït d'elements de A) és clar que la igualtat anterior per a $\widetilde{\varphi}$ ens dona una aplicació $F \to G$ ben definida. Finalment, veiem que $\widetilde{\varphi}$ és morfisme de grups: donats $x, y \in F$, considerem les seves (úniques) expressions reduïdes,

$$x = a_{i_n}^{\epsilon_n} \cdots a_{i_2}^{\epsilon_2} a_{i_1}^{\epsilon_1} \quad \text{i} \quad y = b_{j_1}^{\delta_1} b_{j_2}^{\delta_2} \cdots b_{j_m}^{\delta_m},$$

amb $a_{i_1}, \ldots, a_{i_n}, b_{j_1}, \ldots, b_{j_m} \in A$ i $\epsilon_1, \ldots, \epsilon_n, \delta_1, \ldots, \delta_m = \pm 1$. Fixant-nos en les $0 \leq r \leq \min\{n, m\}$ cancel·lacions que apareixen en el producte xy, tenim que $a_{i_1}^{\epsilon_1} = b_{j_1}^{-\delta_1}, \ldots, a_{i_r}^{\epsilon_r} = b_{j_r}^{-\delta_r}$ i $a_{i_{r+1}}^{\epsilon_{r+1}} \neq b_{j_{r+1}}^{-\delta_{r+1}}$. En aquesta situació, l'(única) expressió reduïda per a l'element xy en termes de A és $xy = a_{i_n}^{\epsilon_n} \cdots a_{i_{r+1}}^{\epsilon_{r+1}} b_{j_{r+1}}^{\delta_{r+1}} \cdots b_{j_m}^{\delta_m}$ i tenim

$$\begin{aligned}
(xy)\tilde{\varphi} &= (a_{i_n}^{\epsilon_n} \cdots a_{i_{r+1}}^{\epsilon_{r+1}} b_{j_{r+1}}^{\delta_{r+1}} \cdots b_{j_m}^{\delta_m})\tilde{\varphi} = \\
&= (a_{i_n}\varphi)^{\epsilon_n} \cdots (a_{i_{r+1}}\varphi)^{\epsilon_{r+1}} \cdot (b_{j_{r+1}}\varphi)^{\delta_{r+1}} \cdots (b_{j_m}\varphi)^{\delta_m} = \\
&= [(a_{i_n}\varphi)^{\epsilon_n} \cdots (a_{i_{r+1}}\varphi)^{\epsilon_{r+1}}] \cdot [(a_{i_r}\varphi)^{\epsilon_r} \cdots (a_{i_1}\varphi)^{\epsilon_1}] \cdot \\
&\quad \cdot [(b_{j_1}\varphi)^{\delta_1} \cdots (b_{j_r}\varphi)^{\delta_r}] \cdot [(b_{j_{r+1}}\varphi)^{\delta_{r+1}} \cdots (b_{j_m}\varphi)^{\delta_m}] = \\
&= (a_{i_n}^{\epsilon_n} \cdots a_{i_{r+1}}^{\epsilon_{r+1}} \cdot a_{i_r}^{\epsilon_r} \cdots a_{i_1}^{\epsilon_1})\tilde{\varphi} \cdot (b_{j_1}^{\delta_1} \cdots b_{j_r}^{\delta_r} \cdot b_{j_{r+1}}^{\delta_{r+1}} \cdots b_{j_m}^{\delta_m})\tilde{\varphi} = \\
&= (x)\tilde{\varphi} \cdot (y)\tilde{\varphi}.
\end{aligned}$$

Per veure l'altra implicació, suposem certa la propietat universal per a F.

Considerem $H = \langle A \rangle \leqslant F$, el subgrup de F generat per A, i designem per $i\colon H \hookrightarrow F$ la inclusió. Aplicant la propietat universal a la inclusió $\varphi\colon A \hookrightarrow H$, obtenim un morfisme $\tilde{\varphi}\colon F \to H$ que compleix $\iota_A \tilde{\varphi} = \varphi$. Però ara tornem a aplicar la propietat universal a la composició $\iota_A = \varphi i\colon A \hookrightarrow H \hookrightarrow F$: el morfisme $\tilde{\varphi} i$ compleix $\iota_A(\tilde{\varphi} i) = (\iota_A \tilde{\varphi}) i = \varphi i$, i la identitat $\mathrm{id}_F\colon F \to F$ també ho compleix $\iota_A \,\mathrm{id}_F = \iota_A = \varphi i$. Per tant, per la unicitat, $\mathrm{id}_F = \tilde{\varphi} i$, d'on deduïm que $F = \mathrm{im}(\mathrm{id}_F) = \mathrm{im}(\tilde{\varphi} i) = \mathrm{im}\, \tilde{\varphi} \leqslant H = \langle A \rangle$ i, per tant, que A genera F.

$$\begin{tikzcd}
A \arrow[r, hook, "\varphi"] \arrow[d, hook, "\iota_A"'] & H \\
F \arrow[ur, dashed, "\tilde{\varphi}"'] &
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
A \arrow[r, hook, "\varphi"] \arrow[d, hook, "\iota_A"'] & H \arrow[r, hook, "i"] & F \\
F \arrow[urr, dashed, "\tilde{\varphi} i = \mathrm{id}_F"'] & &
\end{tikzcd}$$

Per altra banda, podem pensar en el conjunt A com un alfabet formal i construir el grup $G = \mathbb{F}_A$; aplicant la propietat universal a la inclusió $\varphi\colon A \hookrightarrow \mathbb{F}_A$, $a \mapsto [a]$, existeix un morfisme $\tilde{\varphi}\colon F \to \mathbb{F}_A$ que compleix $\iota_A \tilde{\varphi} = \varphi$, és a dir, que compleix $(a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n})\tilde{\varphi} = (a_{i_1}\varphi)^{\epsilon_1} \cdots (a_{i_n}\varphi)^{\epsilon_n} = [a_{i_1}]^{\epsilon_1} \cdots [a_{i_n}]^{\epsilon_n} = [a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n}]$, per a cada producte reduït $a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n}$ d'elements de A. Per tant, si dos productes reduïts d'elements de A, $a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n}$ i $b_{j_1}^{\delta_1} \cdots b_{j_m}^{\delta_m}$ donen el mateix resultat a F, $a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n} =_F b_{j_1}^{\delta_1} \cdots b_{j_m}^{\delta_m}$, llavors $[a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n}] =_{\mathbb{F}_A} [b_{j_1}^{\delta_1} \cdots b_{j_m}^{\delta_m}]$, i la proposició 12 ens assegura que són la mateixa expressió reduïda: $n = m$, $a_{i_1} = b_{j_1}, \ldots, a_{i_n} = b_{j_n}$, i $\epsilon_1 = \delta_1, \ldots, \epsilon_n = \delta_n$. Per tant, A és un subconjunt lliure de F. □

Proposició 17. *Siguin $\mathbb{F}$ un grup lliure amb base $A \subseteq \mathbb{F}$, $\mathbb{F}'$ un grup lliure amb base $A' \subseteq \mathbb{F}'$, i designem per ι_A i $\iota_{A'}$ les respectives inclusions. Llavors, $\mathbb{F}$ i $\mathbb{F}'$ són grups isomorfs si i només si A i A' tenen el mateix cardinal: $\mathbb{F} \simeq \mathbb{F}' \Leftrightarrow \#A = \#A'$.*

Prova. Per la implicació cap a l'esquerra, suposem $\#A = \#A'$ i prenem una aplicació bijectiva $\eta\colon A \to A'$. Aplicant la propietat universal de $\mathbb{F}$ a $\eta\iota_{A'}$ obtenim un morfisme $\alpha\colon \mathbb{F} \to \mathbb{F}'$ que compleix $\iota_A\alpha = \eta\iota_{A'}$; anàlogament, aplicant la propietat universal de $\mathbb{F}'$ a $\eta^{-1}\iota_A$, obtenim un morfisme $\beta\colon \mathbb{F}' \to \mathbb{F}$ que compleix $\iota_{A'}\beta = \eta^{-1}\iota_A$; vegeu la part superior de (4). Però ara apliquem la propietat universal de $\mathbb{F}$ a la inclusió ι_A: òbviament la identitat compleix $\iota_A\,\mathrm{id}_{\mathbb{F}} = \iota_A$; però el morfisme $\alpha\beta\colon \mathbb{F} \to \mathbb{F}' \to \mathbb{F}$ també: $\iota_A\alpha\beta = \eta\iota_{A'}\beta = \eta\eta^{-1}\iota_A = \iota_A$. Per unicitat, deduïm que $\alpha\beta = \mathrm{id}_{\mathbb{F}}$. I amb un argument simètric, $\beta\alpha = \mathrm{id}_{\mathbb{F}'}$. Per tant, $\mathbb{F} \simeq \mathbb{F}'$.

$$
\begin{tikzcd}
A \arrow[r, hook, "\eta"] \arrow[d, hook, "\iota_A"'] & A' \arrow[r, hook, "\iota_{A'}"] & \mathbb{F}' \\
\mathbb{F} \arrow[urr, dashed, "\alpha"'] & &
\end{tikzcd}
\qquad
\begin{tikzcd}
A' \arrow[r, hook, "\eta^{-1}"] \arrow[d, hook, "\iota_{A'}"'] & A \arrow[r, hook, "\iota_A"] & \mathbb{F} \\
\mathbb{F}' \arrow[urr, dashed, "\beta"'] & &
\end{tikzcd}
$$

$$
\begin{tikzcd}
A \arrow[r, hook, "\iota_A"] \arrow[d, hook, "\iota_A"'] & \mathbb{F} \\
\mathbb{F} \arrow[ur, dashed, "\alpha\beta=\mathrm{id}_{\mathbb{F}}"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
A' \arrow[r, hook, "\iota_{A'}"] \arrow[d, hook, "\iota_{A'}"'] & \mathbb{F}' \\
\mathbb{F}' \arrow[ur, dashed, "\beta\alpha=\mathrm{id}_{\mathbb{F}'}"'] &
\end{tikzcd}
\tag{4}
$$

Per a la implicació contrària farem un argument de naturalesa diferent. És fàcil veure que, si $\#A \geqslant \aleph_0$, llavors $\#\mathbb{F}_A = \#A$. Per tant, si $\#A, \#A' \geqslant \aleph_0$ el resultat és evident. Restringim-nos, doncs, al cas $\#A < \infty$.

Observeu que, per cada grup G, la propietat universal de $\mathbb{F}$ ens dona una bijecció, $\mathrm{Map}(A, G) \to \mathrm{Hom}(\mathbb{F}, G)$, $\varphi \mapsto \tilde{\varphi}$, entre el conjunt d'aplicacions de A a G, i el conjunt de morfismes de grups de $\mathbb{F}$ a G (la inversa és la restricció, $\phi_{|A} \leftarrow\!\shortmid \phi$). Per tant, aquests dos conjunts tenen el mateix cardinal, $\#\mathrm{Map}(A, G) = \#\mathrm{Hom}(\mathbb{F}, G)$. Si $\mathbb{F}$ i $\mathbb{F}'$ són grups isomorfs, llavors, mirant aplicacions i morfismes a $\mathbb{Z}/2\mathbb{Z}$, tenim

$$
\begin{aligned}
2^{\#A} &= \#\mathrm{Map}(A, \mathbb{Z}/2\mathbb{Z}) = \#\mathrm{Hom}(\mathbb{F}, \mathbb{Z}/2\mathbb{Z}) = \\
&= \#\mathrm{Hom}(\mathbb{F}', \mathbb{Z}/2\mathbb{Z}) = \#\mathrm{Map}(A', \mathbb{Z}/2\mathbb{Z}) = 2^{\#A'},
\end{aligned}
$$

d'on es dedueix que $\#A = \#A'$. $\square$

Observació 18. Un grup lliure $\mathbb{F}$, doncs, pot ser-ho sobre diversos subconjunts seus $A, A' \subseteq \mathbb{F}$; però, en aquest cas, tots hauran de tenir el mateix cardinal $\#A = \#A'$. Donat que les bases de $\mathbb{F}$ són sistemes de generadors minimals, veiem ara que, de fet, són sistemes de generadors de cardinal mínim: si A és base de $\mathbb{F}$, aleshores $\mathrm{rk}(\mathbb{F}) = \#A$. Escriurem $\mathbb{F}_\kappa$ per designar el grup lliure de rang κ (si no volem fer referència a cap base concreta).

Aquesta situació és anàloga a la de l'àlgebra lineal: un K-espai vectorial E sobre un cos K pot tenir diverses bases, però totes han de tenir sempre el mateix cardinal (la K-dimensió de E). Com ja hem vist, hi ha grups lliures de qualsevol rang, de la mateixa manera que hi ha K-espais vectorials de qualsevol dimensió. Una diferència important, però, és que en àlgebra lineal tot K-espai vectorial té bases (i, per tant, dimensió), mentre que hi ha molts grups que no tenen cap base, és a dir que *no són lliures* sobre cap subconjunt (els grups finits no trivials, per exemple).

Algebraicament, la família dels grups lliures és d'una gran rellevància. Com que, llevat d'isomorfia, n'hi ha un de sol per a cada rang κ, el designarem per $\mathbb{F}_\kappa$ si volem obviar la referència a l'alfabet concret A usat per a la seva construcció. Així tindrem:

$$\mathbb{F}_0 \simeq 1, \quad \mathbb{F}_1 \simeq \mathbb{Z}, \quad \mathbb{F}_2, \quad \mathbb{F}_3, \ldots, \mathbb{F}_{\aleph_0}, \overset{7}{\ldots}$$

Clarament, els únics grups commutatius són els dos primers, força especials dins d'aquesta família. La rellevància d'aquests grups rau en el fet que, d'alguna manera, contenen *tota* la informació possible sobre *tots* els grups possibles. Això es concreta a través del resultat clàssic següent, força senzill de demostrar, i alhora de fonamental importància per a la teoria de grups.

TEOREMA 19. *Tot grup G és quocient d'un grup lliure. És a dir, per a tot grup G existeixen un cardinal κ i un subgrup normal $N \trianglelefteq \mathbb{F}_\kappa$ tals que $G \simeq \mathbb{F}_\kappa / N$.*

PROVA. Sigui $A \subseteq G$ un conjunt de generadors de G (sempre es pot prendre $A = G$), i sigui $\kappa = \#A$ el seu cardinal. Pensem A com un conjunt abstracte, i considerem el grup lliure $\mathbb{F}_A$. Per la propietat universal aplicada a la inclusió $\varphi\colon A \to G$, existeix un (únic) morfisme de grups $\widetilde{\varphi}\colon \mathbb{F}_A \to G$ tal que $[a]\widetilde{\varphi} = a$, per a tot $a \in A$. Com que A genera G, $\widetilde{\varphi}$ és exhaustiu i, pel primer teorema d'isomorfia, $N = \ker \widetilde{\varphi}$ és un subgrup normal de $\mathbb{F}_A$ que compleix $\mathbb{F}_A / N \simeq \operatorname{Im}(\widetilde{\varphi}) = G$. □

Si al teorema 19 fixem una base per a $\mathbb{F}_\kappa$, i una família de generadors de N *com a subgrup normal* de $\mathbb{F}_\kappa$, aleshores obtenim el concepte de presentació, essencial en teoria de grups.

DEFINICIÓ 20. Sigui G un grup. Una *presentació* per a G és un parell (A, R) on A és un conjunt de símbols, R és un subconjunt de $\mathbb{F}_A$, i $G \simeq \mathbb{F}_A / \langle\langle R \rangle\rangle$.[8] Abusant lleugerament del llenguatge, se sol escriure $G = \langle A \mid R \rangle$, i es diu que els elements de A (resp., R) són els *generadors*[9] (resp., *relators*) de G donats per la presentació $\langle A \mid R \rangle$, i que $w \in (A^{\pm})^*$ és una *paraula en els generadors* de G.

COROL·LARI 21. *El grup lliure amb base A admet la presentació $\mathbb{F}_A = \langle A \mid - \rangle$.*

7 Qui vulgui que siguin… Vegeu `https://ca.wikipedia.org/wiki/Hipòtesi_del_continu`.

8 La *clausura normal* $\langle\langle R \rangle\rangle$ és el subgrup (normal) generat per tots els conjugats d'elements de R.

9 Formalment, els generadors de G donats per la presentació $G = \langle A \mid X \rangle$ són les imatges $[a]\widetilde{\varphi}$ dels elements $a \in A$ per la seqüència d'homomorfismes exhaustius $(A^{\pm})^* \twoheadrightarrow \mathbb{F}_A \twoheadrightarrow G$.

Noteu que el teorema 19 ens diu que tot grup admet una presentació —de fet, infinites presentacions. Diem que una presentació $\langle A \mid R \rangle$ és *finita* si tant A com R són conjunt finits. Es diu que un grup és *finitament presentat* si admet una presentació finita.

El teorema 19 admet dues interpretacions contraposades. Per un costat, implica que, col·lectivament, els reticles de subgrups (normals) dels grups lliures contenen tota la informació algebraica possible sobre qualsevol grup concebible; això els converteix en uns candidats naturals i molt concrets on buscar informació sobre qualsevol grup. Però, per altra banda, per aquesta mateixa raó, aquests reticles han de ser extraordinàriament complicats, i és utòpic pretendre entendre'ls completament.

Les presentacions constitueixen la manera natural de descriure els grups des del punt de vista de la teoria combinatòria i algorísmica de grups. La contrapartida geomètrica més elemental és l'anomenat *digraf de Cayley*, definit a continuació.

Definició 22. Siguin G un grup i $S \subseteq G$ un conjunt de generadors per G. Aleshores, el *digraf de Cayley de G respecte de S*, designat per $\mathsf{Cay}(G,S)$, és el graf dirigit (digraf) amb conjunt de vèrtexs G, i un arc $g \xrightarrow{s} gs$ per a cada element $g \in G$ i cada generador $s \in S^{\pm}$.

Observeu que els digrafs de Cayley (respecte a conjunts generadors) són connexos: com que $\langle S \rangle = G$, qualsevol $g \in G$ es pot escriure en la forma $g = s_{i_1}^{\epsilon_1} \cdots s_{i_k}^{\epsilon_k}$, per a certs $k \geq 0$, $s_{i_j} \in S$, i $\epsilon_j = \pm 1$ i, llavors, el camí

$$1 \xrightarrow{s_{i_1}^{\epsilon_1}} s_{i_1}^{\epsilon_1} \xrightarrow{s_{i_2}^{\epsilon_2}} s_{i_1}^{\epsilon_1} s_{i_2}^{\epsilon_2} \xrightarrow{s_{i_3}^{\epsilon_3}} \cdots \xrightarrow{s_{i_k}^{\epsilon_k}} g \tag{5}$$

connecta el vèrtex $1 \in G$ amb el vèrtex genèric $g \in G$. Per altra banda, els digrafs de Cayley són també $(2\#S)$-regulars:[10] per definició, de cada vèrtex $g \in G$ en surt exactament una aresta per cada $s \in S^{\pm}$ (que va al vèrtex $gs \in G$) i n'arriba també exactament una per cada $s \in S^{\pm}$ (que ve de $gs^{-1} \in G$); en general, algunes d'aquestes arestes poden ser paral·leles, o llaços.

Recalquem que $\mathsf{Cay}(G,S)$ depèn fortament del conjunt de generadors escollit S (vegeu figura 2). Per tant, no és un objecte geomètric canònicament associat al grup G, sinó al grup G *i a un conjunt de generadors concret S*.

Exemple 23. El digraf de Cayley del grup lliure $\mathbb{F}_{\{a\}} \simeq \mathbb{Z}$ respecte a la base $\{a\}$ (és a dir, $\{1\}$ en notació additiva) és un camí dirigit amb infinits vèrtexs consecutius, connectats cadascun al següent per una a-aresta (i a l'anterior per una (a^{-1})-aresta). A la figura 2 podeu veure dibuixats els digrafs de Cayley $\mathsf{Cay}(\mathbb{Z},\{1\})$ i $\mathsf{Cay}(\mathbb{Z},\{2,3\})$ on, com és habitual amb els digrafs involutius (vegeu la definició 32), dibuixem només els arcs positius, i assenyalem amb ◉ el vèrtex corresponent a l'element neutre.

10 Un digraf Γ és *regular* si el nombre d'arcs que entren en un vèrtex i el nombre d'arcs que en surten són independents del vèrtex $\mathsf{p} \in \mathsf{V}\Gamma$.

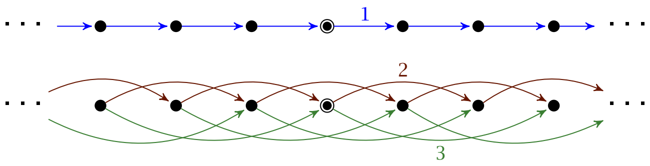


FIGURA 2: $\mathsf{Cay}(\mathbb{Z}, \{1\})$ (a dalt) i $\mathsf{Cay}(\mathbb{Z}, \{2, 3\})$ (a sota).

EXEMPLE 24. És fàcil veure que el digraf de Cayley del grup lliure $\mathbb{F}_{\{a,b\}}$ respecte de la base$\{a, b\}$ té l'aspecte de la figura 3. Per a convèncer-nos-en, només cal tenir en compte les dues observacions anteriors (es tracta d'un digraf connex, i 4-regular), juntament amb els fets d'ésser infinit ($\#\mathbb{F}_{\{a,b\}} = \aleph_0$) i d'ésser un arbre: un hipotètic camí tancat ens donaria dues expressions diferents d'un mateix element g com a producte reduït de les lletres a, a^{-1}, b, b^{-1}, contradient el fet que $\mathbb{F}_{\{a,b\}}$ és lliure en $\{a, b\}$. Anàlogament, el digraf de Cayley del grup lliure $\mathbb{F}_\kappa$ de rang κ respecte a una base és el corresponent arbre infinit 2κ-regular.

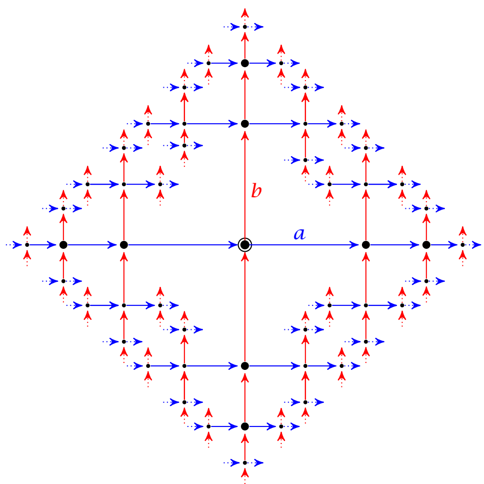


FIGURA 3: El digraf de Cayley de $\mathbb{F}_{\{a,b\}}$.

Com veurem a la secció següent, el digraf de Cayley dels grups lliures respecte a una base tindrà protagonisme en la teoria d'autòmats de Stallings. Concretament, el subgraf definit a continuació.

DEFINICIÓ 25. Sigui A un alfabet, i $a \in A^{\pm}$. Anomenem *a-branca de Cayley* de $\mathbb{F}_A$ la component connexa de $\mathsf{Cay}(\mathbb{F}_A, A) \setminus \mathsf{F}$ que conté $\odot$, on F és el conjunt d'arcs incidents a $\odot$ excepte $\odot \xrightarrow{a} \bullet$ (i el seu invers); vegeu la figura 4.

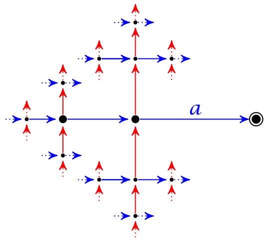


FIGURA 4: La (a^{-1})-branca de Cayley de $\mathbb{F}_{\{a,b\}}$.

Dedicarem la resta d'aquest article a fer una primera aproximació a l'estudi del reticle de subgrups de $\mathbb{F}_n$, amb $n \geqslant 2$ finit. I, tal com intuíem més amunt, ens adonarem de seguida que, efectivament, és extremadament complicat. D'entrada, presenta certs comportaments que recorden patrons de l'àlgebra lineal i suggereixen que, potser, alguns aspectes no seran tan intricats; però gairebé sempre acaba apareixent algun comportament distintiu, sovint de tipus fractal, que el distancia radicalment d'ambients algebraics més benignes.

Acabem aquesta secció proposant un parell de problemes sobre el reticle de subgrups de $\mathbb{F}_2 = \mathbb{F}_{\{a,b\}}$ indicatius de la complexitat a la qual ens referim. Es tracta de problemes molt naturals, anàlegs a problemes típics de l'àlgebra lineal, que en aquell context es resolen fàcilment plantejant i resolent sistemes d'equacions. Només cal endinsar-se una mica en ambdós problemes, com farem a continuació, per a copsar la dificultat extra que suposa el fet d'estar tractant amb grups fortament no commutatius. Convidem el lector a intentar resoldre'ls abans de continuar llegint, per tal de percebre la complexitat a què ens referim. Tot i que en un primer apropament poden semblar difícils de resoldre, veurem a la secció 4 que hi ha una manera elegant, eficient i sorprenentment senzilla de tractar-los: usar la teoria dels autòmats de Stallings, que expliquem en detall a la secció 3.

EXEMPLE 26. Sigui $\mathbb{F}_2$ el grup lliure sobre $A = \{a, b\}$ i considerem el subgrup $H = \langle v_1, v_2, v_3 \rangle \leqslant \mathbb{F}_2$ generat pels elements $v_1 = baba^{-1}$, $v_2 = aba^{-1}$, i $v_3 = aba^2$. És cert que l'element $u = b^2aba^{-1}b^7a^{-2}b^{-1}a^2 \in \mathbb{F}_2$ pertany a H? I, en cas afirmatiu, sabem expressar-lo com a producte de v_1, v_2, v_3 i els seus inversos?

Per a certes paraules, decidir la pertinença a H és fàcil. Per exemple, per a veure que a^3 pertany a H, és suficient observar que $v_2^{-1}v_3 = (ab^{-1}a^{-1})(aba^2) = a^3$. Un altre argument senzill ens permet deduir que l'element a *no* pertany a H: tant se val com multipliquem v_1, v_2, v_3 o els seus inversos, el a-exponent (és a dir, el nombre total de a obtingut sumant les d'exponent positiu i restant les d'exponent negatiu) al resultat sempre serà múltiple de 3. En efecte, els a-exponents dels generadors són $|v_1|_a = 1 - 1 = 0$, $|v_2|_a = 1 - 1 = 0$, i $|v_3|_a = 1 + 2 = 3$; com que $|w_1w_2|_a = |w_1|_a + |w_2|_a$ (ja que la possible cancel·lació entre w_1 i w_2 elimina la mateixa quantitat de a positives que de a negatives), tots els elements del subgrup $H = \langle v_1, v_2, v_3 \rangle$ han de tenir forçosament a-exponent múltiple de 3. I, com que $|a|_a = 1$ no és múltiple de 3, deduïm que $a \notin H$.

Però en el cas de l'element $u = b^2aba^{-1}b^7a^{-2}b^{-1}a^2$, el a-exponent total és $|u|_a = 0$, per tant, no podem descartar-lo usant l'argument anterior. Òbviament, això tampoc no ens assegura que hi hagi de pertànyer: no tenim, *a priori*, cap indicació de com podem multiplicar entre si les paraules v_1, v_2, v_3 i els seus inversos, per tal d'aconseguir u; ni de si això és realment possible, o no. Si els elements v_1, v_2, v_3 commutessin, el problema es reduiria a decidir si u és de la forma $v_1^{\alpha}v_2^{\beta}v_3^{\gamma}$ amb $\alpha, \beta, \gamma \in \mathbb{Z}$, és a dir, si u és una *combinació lineal* de v_1, v_2, v_3 amb coeficients enters. Com es pot percebre, però, la no commutativitat dels elements v_1, v_2, v_3 complica molt el plantejament i la resolució d'aquest problema.

La resposta en aquest cas és afirmativa, però trobar un producte adequat (que doni u) ja no és tan fàcil a simple vista:

$$v_1v_2^{-1}v_1(v_1v_2^{-1})^7v_3^{-1}v_2^{-1}v_3 =$$

$$= baba^{-1}(aba^{-1})^{-1}baba^{-1}(baba^{-1}(aba^{-1})^{-1})^7(aba^2)^{-1}(aba^{-1})^{-1}aba^2 =$$

$$= baba^{-1}ab^{-1}a^{-1}baba^{-1}(baba^{-1}ab^{-1}a^{-1})^7a^{-2}b^{-1}a^{-1}ab^{-1}a^{-1}aba^2 =$$

$$= b\,baba^{-1}b^7a^{-2}b^{-1}a^2 = b^2aba^{-1}b^7a^{-2}b^{-1}a^2 = u.$$

Evidentment, fer els càlculs per comprovar si un determinat producte dels generadors dona u és fàcil. Però trobar, o més encara, decidir l'existència d'un producte de $v_1^{\pm 1}$, $v_2^{\pm 1}$, $v_3^{\pm 1}$ que doni la paraula candidata u, no ho sembla tant.[11] És fàcil adonar-se que la complicació deriva de com de recargolada sigui l'eventual expressió *(de llargada finita però arbitràriament gran)* del candidat u en termes dels generadors. A la subsecció 4.2 explicarem una manera sistemàtica de resoldre aquest problema.

Preguntes afins amb una evident importància algebraica són: és aquesta l'única manera d'obtenir u a partir de v_1, v_2, v_3? Si n'hi ha d'altres, podem descriure-les totes? Podem calcular la paraula més curta (potser no única) que doni u?…

Observeu que el problema anàleg en àlgebra lineal seria del tipus següent: «pertany el vector $(1, 2, 3)$ al subespai vectorial $\langle(-1, 2, 1), (0, 1, -3)\rangle$ de $\mathbb{R}^3$?». Per a respondre, només hem de mirar si el sistema d'equacions $(1, 2, 3) = \alpha(-1, 2, 1) + \beta(0, 1, -3)$ té o no solucions a $\mathbb{R}$. En l'ambient no commutatiu en què ens trobem no coneixem, de moment, cap eina que pugui fer un paper semblant al que fan els sistemes d'equacions en l'àlgebra lineal. Com veurem a continuació, en el cas dels grups lliures, els autòmats de Stallings faran aquest paper.

Per acabar la secció, us proposem un altre problema que involucra interseccions de subgrups del grup lliure.

11 Almenys a la majoria dels humans (vegeu `https://ca.wikipedia.org/wiki/P_versus_NP`).

EXEMPLE 27. Sigui $\mathbb{F}_2$ el grup lliure sobre $A = \{a, b\}$, i considerem els subgrups $H = \langle u_1, u_2, u_3 \rangle \leqslant \mathbb{F}_2$ i $K = \langle v_1, v_2, v_3 \rangle \leqslant \mathbb{F}_2$ donats per les paraules $u_3 = a^{-1}bab^{-1}a$, i $v_1 = ab$, $v_2 = a^3$, i $v_3 = a^{-1}ba$, $u_1 = b$, $u_2 = a^3$. Com veurem al corol·lari 66, els subgrups del grup lliure no tenen per què ser finitament generats. Ho és la intersecció $H \cap K$? I, en tal cas, podeu calcular-ne un conjunt de generadors?

A simple vista ja es veu que l'element a^3 és present a ambdós subgrups: $a^3 = v_2 \in H$, i $a^3 = u_2 \in K$. També se'n veu fàcilment un altre:

$$H \ni u_1^{-1}u_2u_1 = b^{-1}a^3b = v_1^{-1}v_2v_1 \in K.$$

I amb una mica més d'imaginació (o de treball de càlcul) aquí tenim un tercer element de la intersecció:

$$H \ni u_3^3 = a^{-1}ba^3b^{-1}a = v_3v_2v_3^{-1} \in K.$$

Com que $H \cap K$ és un subgrup de $\mathbb{F}_2$, deduïm que $\langle a^3, b^{-1}a^3b, a^{-1}ba^3b^{-1}a \rangle$ està contingut a $H \cap K$. Seguir trobant nous elements a simple vista no sembla fàcil; però la pregunta contrària encara sembla més complicada: és cert que $H \cap K = \langle a^3, b^{-1}a^3b, a^{-1}ba^3b^{-1}a \rangle$? O cal trobar i afegir-hi més generadors?

El lector interessat pot provar de respondre totes aquestes preguntes per si sol. Nosaltres, de moment, ho deixarem aquí, i tornarem a tractar aquests exemples a la secció 4, on ja disposarem d'eines adequades per a respondre totes aquestes preguntes… i més!

3 Autòmats de Stallings

DEFINICIÓ 28. Sigui A un alfabet. Un *A-autòmat* Γ (o simplement *autòmat*, si l'alfabet és clar pel context) és un graf dirigit amb els arcs etiquetats en A i un vèrtex distingit; més formalment, és una tupla $\Gamma = (\mathsf{V}, \mathsf{E}, \iota, \tau, \ell, ⊙)$, on V i E són conjunts, $\iota, \tau\colon \mathsf{E} \to \mathsf{V}$ i $\ell\colon \mathsf{E} \to A$ són funcions, i $⊙ \in \mathsf{V}$. Els conjunts $\mathsf{V} = \mathsf{V}\Gamma$ i $\mathsf{E} = \mathsf{E}\Gamma$ s'anomenen conjunt de *vèrtexs* i d'*arcs* (o *arestes dirigides*) de Γ, respectivament, i les funcions ι, τ i ℓ assignen a cada arc $\mathsf{e} \in \mathsf{E}$ el seu *origen* $\iota(\mathsf{e}) \in \mathsf{V}$, el seu *final* $\tau(\mathsf{e}) \in \mathsf{V}$, i la seva *etiqueta* $\ell(\mathsf{e}) \in A$, respectivament. Si $\iota\mathsf{e} = \mathsf{p}$, $\tau\mathsf{e} = \mathsf{q}$ i $\ell(\mathsf{e}) = a$, aleshores diem que e és un *a-arc de* p *a* q, i escrivim $\mathsf{e} \equiv \mathsf{p} \xrightarrow{a} \mathsf{q}$. El vèrtex distingit $⊙$ s'anomena *vèrtex base* o *punt base* del A-autòmat. El *digraf subjacent* d'un A-autòmat Γ és el digraf resultat d'ignorar-ne la funció ℓ i el punt base $⊙$.

Observeu que, segons la nostra definició, un autòmat no és necessàriament connex, i admet la possibilitat tant d'arcs amb el mateix origen i final (*llaços*), com també de múltiples arcs amb el mateix origen i el mateix final (*arcs paral·lels*).

DEFINICIÓ 29. Sigui Γ un A-autòmat. Un vèrtex p de Γ s'anomena *saturat* si per a cada lletra $a \in A$ hi ha (almenys) un a-arc amb origen p. En cas contrari, diem que p és insaturat (o *a-deficient*, si volem referir-nos a l'etiqueta que falta). El *a-dèficit* de Γ, designat per $\mathrm{def}_a(\Gamma)$, és el nombre (cardinal) de vèrtexs a-deficients a Γ. Un A-autòmat Γ s'anomena *saturat* si tots els seus vèrtexs ho són, *i. e.*, si $\mathrm{def}_a(\Gamma) = 0$ per a tot $a \in A$.

Definició 30. Un *camí (dirigit)* en un A-autòmat Γ és una seqüència alternada finita $\gamma = \mathsf{p}_0\mathsf{e}_1\mathsf{p}_1 \cdots \mathsf{e}_l\mathsf{p}_l$, on $\mathsf{p}_i \in \mathsf{V}\Gamma$, $\mathsf{e}_i \in \mathsf{E}\Gamma$, $\iota\mathsf{e}_i = \mathsf{p}_{i-1}$, i $\tau\mathsf{e}_i = \mathsf{p}_i$ per a $i = 1, \ldots, l$. Aleshores, p_0 i p_l s'anomenen *origen* i *final* de γ respectivament, i escrivim $\mathsf{p}_0 = \iota(\gamma)$ i $\mathsf{p}_l = \tau(\gamma)$. Diem que γ és un camí de p_0 a p_l, i ho designem per $\gamma\colon \mathsf{p}_0 \rightsquigarrow \mathsf{p}_l$. Si l'origen i el final de γ coincideixen, diem que γ és un *camí tancat*. Un camí tancat de p a p s'anomena p-*camí*. La *longitud* d'un camí γ, designada per $|\gamma|$, és el nombre d'arcs a γ (comptant possibles repeticions). Els camins de longitud 0 s'anomenen *camins trivials* i corresponen als vèrtexs de Γ.

Recordem que $A^{\pm} = A \sqcup A^{-1}$, on A^{-1} és el conjunt d'inversos formals de A.

Definició 31. Un *A-autòmat involutiu* és un $A^{\pm}$-autòmat amb una involució $\mathsf{e} \mapsto \mathsf{e}^{-1}$ als seus arcs tal que si $\mathsf{e} \equiv \mathsf{p} \xrightarrow{a} \mathsf{q}$ aleshores $\mathsf{e}^{-1} \equiv \mathsf{p} \xleftarrow{a^{-1}} \mathsf{q}$. Aleshores, diem que (l'arc etiquetat) e^{-1} és l'*invers* de e. Observeu que $(\mathsf{e}^{-1})^{-1} = \mathsf{e}$; és a dir, en un autòmat involutiu, els arcs etiquetats apareixen aparellats amb els seus respectius inversos (vegeu la figura 5).

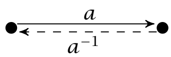


Figura 5: Un arc en un autòmat involutiu amb el seu invers puntejat.

Definició 32. Un arc en un A-autòmat involutiu Γ es diu *positiu* (resp., *negatiu*) si la seva etiqueta pertany a A (resp., A^{-1}). S'anomena *part positiva* de Γ, designada per Γ^+, l'autòmat obtingut després d'eliminar de Γ tots els arcs negatius. És clar que tot autòmat involutiu queda determinat per la seva part positiva, que habitualment farem servir per a descriure l'autòmat, amb el conveni tàcit que els arcs positius $\mathsf{p} \xrightarrow{a} \mathsf{q}$ es poden travessar cap enrere (*i. e.*, de q a p) llegint la lletra inversa a^{-1}. Observeu que, identificant els parells d'arcs mútuament inversos (en una *aresta*, no dirigida), recuperem la noció estàndard de graf *no dirigit*, que anomenarem *graf (no dirigit) subjacent* de Γ. Farem servir aquesta correspondència per a traslladar a l'àmbit dels autòmats algunes nocions bàsiques de teoria de grafs. Per exemple, direm que un autòmat Γ és *connex* si ho és el seu graf subjacent, direm que T és un *arbre generador*[12] de Γ si ho és del seu graf subjacent, i definirem el *grau* d'un vèrtex p, designat per $\deg(\mathsf{p})$, com el nombre d'arestes incidents a p en el graf subjacent, i el *rang* de Γ, designat per $\mathrm{rk}(\Gamma)$, com el rang del seu graf subjacent (vegeu la definició 33). En particular, si Γ és un autòmat involutiu, connex i finit, aleshores $\mathrm{rk}(\Gamma) = 1 - \#\mathsf{V}\Gamma + \#\mathsf{E}\Gamma^+$.

12 En anglès, *spanning tree*.

Si Γ és un A-autòmat involutiu, aleshores el $A^{\pm}$-etiquetatge de Γ s'estén de forma natural a un $(A^{\pm})^*$-etiquetatge dels camins, tot concatenant les corresponents etiquetes: si $\gamma = \mathsf{p}_0\mathsf{e}_1\mathsf{p}_1 \cdots \mathsf{e}_l\mathsf{p}_l$ és un camí, definim la seva *etiqueta*, i la seva *etiqueta reduïda* com $\ell(\gamma) = \ell(\mathsf{e}_1)\cdots\ell(\mathsf{e}_l) \in (A^{\pm})^*$, i $\overline{\ell}(\gamma) = \overline{\ell(\gamma)} \in \mathbb{F}_A$, respectivament. En ambdós casos, s'entén que l'etiqueta d'un camí trivial és l'element trivial 1. Si $\ell(\gamma) = w \in (A^{\pm})^*$ diem que el camí γ *llegeix* w, o que la paraula w *etiqueta* el camí γ, i escrivim $\gamma\colon \mathsf{p}_0 \overset{w}{\rightsquigarrow} \mathsf{p}_l$.

Es diu que un camí presenta *retrocés*[13] si té dos arcs successius inversos l'un de l'altre. Un camí sense retrocés es diu *camí reduït*. És obvi que, si $\ell(\gamma)$ és una paraula reduïda, aleshores el camí γ ha de ser reduït, però el recíproc no és cert en general, ja que es poden donar les situacions (no deterministes) de la figura 6. Observeu també que, si T és un arbre generador d'un A-autòmat connex Γ, aleshores per a cada parell de vèrtexs p, q a Γ existeix un únic camí *reduït* de p a q usant només arcs de T; l'anomenem T-geodèsica de p a q, i el designem per $\gamma_T[\mathsf{p},\mathsf{q}]$, o simplement per $\mathsf{p} \overset{T}{\rightsquigarrow} \mathsf{q}$.

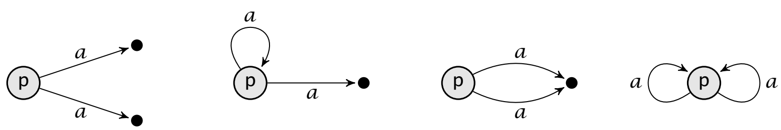


FIGURA 6: Situacions no deterministes al vèrtex p.

Si $\gamma = \mathsf{p}_0\mathsf{e}_1\mathsf{p}_1 \cdots \mathsf{e}_l\mathsf{p}_l$ és un camí en un A-autòmat involutiu Γ (llegint $\ell(\gamma) = \ell(\mathsf{e}_1)\cdots\ell(\mathsf{e}_l)$), aleshores s'anomena *camí invers* de γ a $\gamma^{-1} = \mathsf{p}_l\mathsf{e}_l^{-1}\mathsf{p}_{l-1}\cdots\mathsf{e}_1^{-1}\mathsf{p}_0$ (llegint $\ell(\gamma)^{-1} = \ell(\mathsf{e}_l)^{-1}\cdots\ell(\mathsf{e}_0)^{-1}$). És clar que, també, $\overline{\ell}(\gamma^{-1}) = \overline{\ell}(\gamma)^{-1}$.

És el moment de començar a relacionar els A-autòmats amb els grups. Potser la manera més natural de fer-ho és a través de la idea topològica de grup fonamental d'un graf. Com veurem, si admetem etiquetes a les arestes, aquesta idea desemboca en la de subgrup reconegut, que, com es mostra a continuació, és un subgrup concret de $\mathbb{F}_A$, en lloc d'un grup abstracte.

DEFINICIÓ 33. Siguin Γ un graf no dirigit i connex, i $\mathsf{p} \in \mathsf{V}\Gamma$. El *grup fonamental de* Γ *al vèrtex* p, designat per $\pi_{\mathsf{p}}(\Gamma)$, és el conjunt de classes de p-camins a Γ mòdul retrocés, o mòdul reducció de camins (que, en el cas dels grafs vistos com a espais topològics, equival a dir mòdul homotopia), juntament amb l'operació de concatenació de p-camins. És ben sabut que, independentment del vèrtex p triat, $\pi_{\mathsf{p}}(\Gamma)$ és un grup lliure de rang igual al nombre (cardinal) d'arestes fora d'un arbre generador T de Γ; a aquest valor, que no depèn de l'arbre T, l'anomenem el *rang (gràfic)* de Γ, designat per $\mathrm{rk}(\Gamma)$; és fàcil veure que, si Γ és finit, aleshores

$$\mathrm{rk}(\Gamma) - 1 = \#\mathsf{E}\Gamma - \#\mathsf{V}\Gamma = \frac{1}{2}\sum\nolimits_{\mathsf{q}\in\mathsf{V}\Gamma}(\deg(\mathsf{q}) - 2), \tag{6}$$

on $\#\mathsf{V}\Gamma$ és el nombre de vèrtexs i $\#\mathsf{E}\Gamma$ el nombre d'arestes (no dirigides) de Γ.

13 En anglès, *backtracking*.

DEFINICIÓ 34. Sigui Γ un A-autòmat involutiu i connex, i $\mathsf{p} \in V\Gamma$. És fàcil veure que el conjunt d'etiquetes reduïdes de p-camins a Γ,

$$\langle\Gamma\rangle_{\mathsf{p}} = \{\overline{\ell}(\gamma) : \gamma \colon \mathsf{p} \rightsquigarrow \mathsf{p}\}, \tag{7}$$

és un subgrup de $\mathbb{F}_A$; l'anomenem *subgrup reconegut per* Γ *al vèrtex* p. El subgrup $\langle\Gamma\rangle_{\circledcirc}$ el designem simplement per $\langle\Gamma\rangle$.

OBSERVACIÓ 35. En general, el subgrup reconegut per un A-autòmat Γ i el grup fonamental de (el subgraf subjacent de) Γ en un vèrtex p són conceptes diferents, però estretament lligats per l'aplicació *llegir etiquetes reduïdes*:

$$\begin{aligned} \widetilde{\ell}_\Gamma \colon \pi_{\mathsf{p}}(\Gamma) &\twoheadrightarrow \langle\Gamma\rangle_{\mathsf{p}} \leqslant \mathbb{F}_A \\ [\gamma] &\mapsto \overline{\ell}(\gamma). \end{aligned} \tag{8}$$

És clar que $\widetilde{\ell}_\Gamma$ està ben definit i és un homomorfisme de grups exhaustiu *i no injectiu, en general*. Més endavant veurem una condició sobre Γ, sota la qual $\widetilde{\ell}_\Gamma$ serà injectiu.

La definició 34 (prenent $\mathsf{p} = \circledcirc$) determina l'aplicació següent, que relaciona els A-autòmats amb el reticle de subgrups de $\mathbb{F}_A$:

$$\begin{aligned} \{\text{(classes d'isomorfia de) } A\text{-autòmats}\} &\to \{\text{subgrups de } \mathbb{F}_A\} \\ \Gamma &\mapsto \langle\Gamma\rangle. \end{aligned} \tag{9}$$

És fàcil veure que aquesta aplicació és exhaustiva; és a dir, tot subgrup $H \leqslant \mathbb{F}_A$ és el subgrup reconegut per algun A-autòmat. En efecte, si $S = \{w_i\}_{i\in I} \subseteq \mathbb{F}_A$ és un conjunt de paraules reduïdes que generen H, aleshores considerem, per a cada $w_i = a_{i_1}a_{i_2}\cdots a_{i_l} \in S$ ($a_j \in A^{\pm}$), el cicle orientat llegint w_i (ó w_i^{-1} en direcció contrària); anomenat *pètal* associat a w_i, i designat per $\mathsf{Fl}(w_i)$ (vegeu la figura 7).

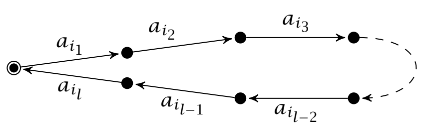


FIGURA 7: El pètal $\mathsf{Fl}(w_i)$.

A continuació definim l'*autòmat flor* $\mathsf{Fl}(S)$ com l'autòmat obtingut després d'identificar els punts base dels pètals associats als elements de S (vegeu la figura 8).

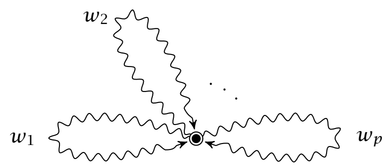


FIGURA 8: L'autòmat flor $\mathsf{Fl}(w_1, w_2, \ldots, w_p)$.

És clar que les etiquetes reduïdes dels $\odot$-camins de $\mathsf{Fl}(S)$ descriuen precisament el subgrup H; *i. e.*, $\langle \mathsf{Fl}(S) \rangle = \langle S \rangle = H \leqslant \mathbb{F}_A$. Per tant, l'aplicació (9) és exhaustiva. Observeu també que (9) està lluny de ser injectiva ja que, per exemple, diferents famílies de generadors per a H proporcionen diferents autòmats flor, tots preimatge de H per (9).

El resultat clau de Stallings a [50] ens diu que es pot eliminar tota la redundància de la representació donada per (9) (i assolir un únic representant Γ per a cada subgrup $H \leqslant \mathbb{F}_A$) simplement imposant un parell de condicions força naturals sobre els autòmats involucrats: ésser determinista, i ésser cor.

DEFINICIÓ 36. Un A-autòmat Γ es diu *determinista* si de cap dels seus vèrtexs no surten dos arcs diferents amb la mateixa etiqueta; és a dir, si per a cada vèrtex $\mathsf{p} \in \mathsf{V}\Gamma$, i per a cada parell d'arcs e, e' sortint de p, $\ell(\mathsf{e}) = \ell(\mathsf{e}')$ implica $\mathsf{e} = \mathsf{e}'$. (Noteu que un autòmat involutiu és determinista si i només si de cap vèrtex no surten i a cap vèrtex no arriben arcs diferents amb la mateixa etiqueta positiva.)

DEFINICIÓ 37. Un autòmat involutiu es diu *cor*[14] si tot vèrtex (i, per tant, tot arc) apareix en algun $\odot$-camí reduït. El *cor d'un autòmat involutiu* Γ, designat per $\mathrm{core}(\Gamma)$, és el màxim subautòmat cor de Γ que conté el punt base. És clar que $\mathrm{core}(\Gamma)$ és un subautòmat induït,[15] de Γ (de fet, de la component connexa de Γ que conté $\odot$), connex, i que reconeix el mateix subgrup, *i. e.*, $\langle \mathrm{core}(\Gamma) \rangle = \langle \Gamma \rangle$.

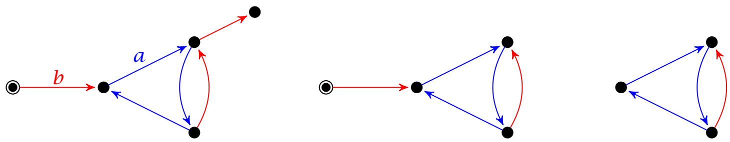
Observeu que $\mathrm{core}(\Gamma)$ pot tenir encara un vèrtex de grau 1 que, en cas d'existir, ha de ser necessàriament el punt base a l'*extrem d'un «pèl» penjant de* $\mathrm{core}(\Gamma)$. Eliminant aquest eventual pèl obtenim el que anomenem *cor restringit* de Γ, designat per $\mathrm{core}^*(\Gamma)$ (formalment, el digraf etiquetat obtingut després d'eliminar successivament tots els vèrtexs de grau 1 de $\mathrm{core}(\Gamma)$ i ignorar el vèrtex base).

OBSERVACIÓ 38. És fàcil veure que $\mathrm{rk}(\mathrm{core}^*(\Gamma)) = \mathrm{rk}(\mathrm{core}(\Gamma)) = \mathrm{rk}(\Gamma)$ (vegeu la subsecció 4.6), i que $\langle \mathrm{core}^*(\Gamma) \rangle_{\mathsf{p}}$ és conjugat a $\langle \mathrm{core}(\Gamma) \rangle = \langle \Gamma \rangle$, per a tot $\mathsf{p} \in \mathsf{V}(\mathrm{core}^*(\Gamma))$ (vegeu la subsecció 4.4).

DEFINICIÓ 39. Un A-autòmat involutiu es diu *reduït* si és determinista i cor.

14 En anglès, *core*.
15 Un subautòmat és *induït* si conté tots els arcs (de l'autòmat original) incidents als seus vèrtexs.

EXEMPLE 40. Principals variants d'autòmat involutiu i determinista:



Γ $\quad$ $\mathrm{core}(\Gamma)$ $\quad$ $\mathrm{core}^*(\Gamma)$

FIGURA 9: D'esquerra a dreta, un autòmat determinista no reduït Γ (amb dos pèls), el seu cor $\mathrm{core}(\Gamma)$, i el seu cor restringit $\mathrm{core}^*(\Gamma)$.

Per veure que cada fibra de (9) admet un únic representant reduït adaptarem un resultat clàssic de teoria de llenguatges.

DEFINICIÓ 41. Siguin $\Gamma = (\mathsf{V}, \mathsf{E}, \iota, \tau, \ell, \odot)$ i $\Gamma' = (\mathsf{V}', \mathsf{E}', \iota', \tau', \ell', \odot')$ A-autòmats. Un *homomorfisme (de A-autòmats)* de Γ a Γ' és una funció $\theta\colon \mathsf{V} \to \mathsf{V}'$ que envia el punt base al punt base ($\odot\theta = \odot'$) i tal que, per a cada $\mathsf{p}, \mathsf{q} \in \mathsf{V}$ i cada $a \in A$, si $\mathsf{p} \xrightarrow{a} \mathsf{q}$ aleshores $\mathsf{p}\theta \xrightarrow{a} \mathsf{q}\theta$. Habitualment, abusem lleugerament del llenguatge i el designem per $\theta\colon \Gamma \to \Gamma'$.

PROPOSICIÓ 42. *Siguin Γ i Γ' A-autòmats reduïts. Aleshores, $\langle\Gamma\rangle \leqslant \langle\Gamma'\rangle$ si i només si existeix un homomorfisme $\Gamma \to \Gamma'$ i, en aquest cas, l'homomorfisme és únic.*

PROVA. La unicitat és conseqüència del determinisme de Γ'. En efecte, suposem que $\theta_1, \theta_2\colon \Gamma \to \Gamma'$ són homomorfismes, i $\mathsf{p} \in \mathsf{V}\Gamma$ un vèrtex tal que $\mathsf{p}\theta_1 \neq \mathsf{p}\theta_2$. Aleshores les imatges per θ_1 i θ_2 de qualsevol camí $\gamma\colon \odot \rightsquigarrow \mathsf{p}$ a Γ seran camins a Γ' amb el mateix origen, $\odot'$, i la mateixa etiqueta, $\ell(\gamma)$, però diferent final, $\mathsf{p}\theta_1 \neq \mathsf{p}\theta_2$, en contradicció amb el determinisme de Γ'.

[$\Leftarrow$] la implicació cap a l'esquerra és certa sense cap hipòtesi addicional sobre Γ, Γ': si $\theta\colon \Gamma \to \Gamma$ és un homomorfisme d'autòmats, aleshores la imatge de qualsevol $\odot$-camí a Γ és un $\odot'$-camí a Γ' amb la mateixa etiqueta, i per tant, la mateixa etiqueta reduïda; per tant, $\langle\Gamma\rangle \leqslant \langle\Gamma'\rangle$.

[$\Rightarrow$] Suposem ara que Γ i Γ' són A-autòmats reduïts amb $\langle\Gamma\rangle \leqslant \langle\Gamma'\rangle$ i construïm un homomorfisme $\theta\colon \Gamma \to \Gamma'$. Òbviament, prenem $\odot\theta = \odot'$. Per a tot vèrtex $\mathsf{p} \neq \odot$, considerem un $\odot$-camí reduït γ a Γ que passi per p:

$$\gamma\colon \odot \overset{u}{\rightsquigarrow} \mathsf{p} \overset{v}{\rightsquigarrow} \odot$$

(sabem que n'existeix almenys un perquè Γ és cor). A més, com que Γ és també determinista, tenim que tant u com v són paraules reduïdes, i sense cancel·lació entre elles. En particular, $uv \in \langle\Gamma\rangle$ i per tant $uv \in \langle\Gamma'\rangle$. Això vol dir que uv és l'etiqueta reduïda d'un $\odot'$-camí a Γ' i, com que Γ' és determinista, uv és també l'etiqueta d'un $\odot'$-camí reduït γ' a Γ', que podem descompondre com a

$$\gamma'\colon \odot' \overset{u}{\rightsquigarrow} \mathsf{p}' \overset{v}{\rightsquigarrow} \odot'.$$

Definim $\mathsf{p}\theta = \mathsf{p}'$. Per veure que està ben definit, sigui $\odot \overset{w}{\rightsquigarrow} \mathsf{p} \overset{z}{\rightsquigarrow} \odot$ un altre $\odot$-camí reduït de Γ que passa per p, considerem $\odot' \overset{w}{\rightsquigarrow} \mathsf{p}'' \overset{z}{\rightsquigarrow} \odot'$ el corresponent $\odot'$-camí reduït a Γ', i vegem que $\mathsf{p}' = \mathsf{p}''$. Observeu que $\odot \overset{u}{\rightsquigarrow} \mathsf{p} \overset{z}{\rightsquigarrow} \odot$ és un $\odot$-camí a Γ *amb possible retrocés a* p; si anomenem q el vèrtex on acaba aquest retrocés, aleshores tenim

$$\begin{tikzcd}
 & \mathsf{q} \arrow[d, rightsquigarrow, "u_2"', "z_1^{-1}"] \arrow[dr, rightsquigarrow, "z_2"] & \\
\odot \arrow[ur, rightsquigarrow, "u_1"] \arrow[dr, rightsquigarrow, "w"'] & \mathsf{p} \arrow[r, phantom] & \odot, \\
 & \mathsf{p} \arrow[ur, rightsquigarrow, "v"'] &
\end{tikzcd}$$

on $u = u_1u_2$, $z = z_1z_2$, $u_2 = z_1^{-1}$, i el camí $\odot \overset{u_1}{\rightsquigarrow} \mathsf{q} \overset{z_2}{\rightsquigarrow} \odot$ és reduït. Per tant, $uv = u_1u_2v$, $wz = wz_1z_2$ i u_1z_2 han de ser llegibles (sense cancel·lació entre síl·labes) com a etiquetes de $\odot'$-camins reduïts a Γ':

$$\begin{tikzcd}
 & \mathsf{q}' \arrow[r, rightsquigarrow, "u_2"] & \mathsf{p}' \arrow[dr, rightsquigarrow, "v"] & \\
\odot \arrow[ur, rightsquigarrow, "u_1"] \arrow[r, rightsquigarrow, "u_1"] \arrow[dr, rightsquigarrow, "w"'] & \mathsf{q}''' \arrow[rr, rightsquigarrow, "z_2"] & & \odot' \\
 & \mathsf{p}'' \arrow[r, rightsquigarrow, "z_1"'] & \mathsf{q}'' \arrow[ur, rightsquigarrow, "z_2"'] &
\end{tikzcd}$$

Finalment, pel determinisme de Γ', és clar, primer que $\mathsf{q}' = \mathsf{q}''' = \mathsf{q}''$, i després (tenint en compte que $u_2 = z_1^{-1}$) que $\mathsf{p}' = \mathsf{p}''$, tal com reclamàvem. Per tant, $\theta\colon \mathsf{V}\Gamma \to \mathsf{V}\Gamma'$ està ben definit.

Per acabar, vegem que θ és un homomorfisme d'autòmats entre Γ i Γ'. En efecte, com que Γ és cor, donat un arc $\mathsf{e} \equiv \mathsf{p} \xrightarrow{a} \mathsf{q}$ a Γ, sabem que existeix un $\odot$-camí reduït a Γ que usa l'arc e:

$$\odot \overset{u}{\rightsquigarrow} \mathsf{p} \xrightarrow{a} \mathsf{q} \overset{v}{\rightsquigarrow} \odot.$$

Per tant, $uav \in \langle \Gamma \rangle \leqslant \langle \Gamma' \rangle$ (sense cancel·lació entre síl·labes). I, per la definició de θ, a Γ' hi tenim el $\odot'$-camí reduït

$$\odot' \overset{u}{\rightsquigarrow} \mathsf{p}\theta \xrightarrow{a} \mathsf{q}\theta \overset{v}{\rightsquigarrow} \odot'.$$

En particular, tenim un arc $\mathsf{p}\theta \xrightarrow{a} \mathsf{q}\theta$ a Γ', i per tant, θ és un homomorfisme d'autòmats de Γ a Γ', tal com volíem demostrar. □

Els corol·laris següents són immediats, i capturen exactament la propietat que perseguim.

COROL·LARI 43. *Si* Γ *és un autòmat reduït, aleshores l'únic homomorfisme* $\Gamma \to \Gamma$ *és la identitat.* □

COROL·LARI 44. *Si dos A-autòmats reduïts reconeixen el mateix subgrup, aleshores són isomorfs. És a dir, si* Γ *i* Γ' *són A-autòmats reduïts, aleshores*

$$\langle \Gamma \rangle = \langle \Gamma' \rangle \Leftrightarrow \Gamma \simeq \Gamma'.$$

Per tant, d'entre tots els A-autòmats que reconeixen un cert subgrup $H \leqslant \mathbb{F}_A$, serà suficient triar-ne un de reduït per tal d'obtenir un representant únic, i restringir (9) a una bijecció. Vegem a continuació que aquest representant reduït sempre existeix, i com es relaciona amb un altre autòmat naturalment associat al subgrup H corresponent.

DEFINICIÓ 45. Siguin G un grup, H un subgrup de G, i $S \subseteq G$ un conjunt de generadors per a G. Aleshores, l'*autòmat de Schreier (per la dreta) de H respecte a S*, designat per $\mathsf{Sch}_G(H,S)$, és el S-autòmat amb conjunt de vèrtexs $H\backslash G$ (el conjunt de classes laterals per la dreta de G mòdul H), un arc $Hg \xrightarrow{s} Hgs$ per a cada classe lateral $Hg \in H\backslash G$ i cada element $s \in S^{\pm}$, i la classe lateral H com a vèrtex base.

OBSERVACIÓ 46. Noteu que, si $H \trianglelefteq G$, llavors $\mathsf{Sch}_G(H,S) = \mathsf{Cay}(G/H,S)$. En particular, $\mathsf{Sch}_G(1,S) = \mathsf{Cay}(G,S)$.

Donat que d'ara endavant sempre considerarem $G = \mathbb{F}_A$, prendrem habitualment la base A com a conjunt de generadors i escriurem simplement $\mathsf{Sch}_{\mathbb{F}_A}(H,A) = \mathsf{Sch}(H,A)$. El A-autòmat $\mathsf{Sch}(H,A)$ té les propietats següents.

PROPOSICIÓ 47. *Sigui H un subgrup de $\mathbb{F}_A$. Aleshores,*

(i) $\mathsf{Sch}(H,A)$ *és un A-autòmat involutiu, determinista i saturat;*
(ii) $\mathsf{Sch}(H,A)$ *és connex;*
(iii) $\langle \mathsf{Sch}(H,A) \rangle = H$*;*
(iv) cada arc e *no pertanyent a* $\operatorname{core}(\mathsf{Sch}(H,A))$ *és un pont de* $\mathsf{Sch}(H,A)$*; és a dir,* $\mathsf{Sch}(H,A) \setminus \{\mathsf{e}\}$ *té dues components connexes i, a més, la que no conté* $\circledcirc$ *és un arbre infinit i saturat* excepte al vèrtex incident a e*;*
(v) $\mathsf{Sch}(H,A)$ *no és necessàriament cor.*

PROVA. L'apartat (i) és immediat de la definició d'autòmat de Schreier (definició 45). La connexió de $\mathsf{Sch}(H,A)$ és conseqüència directa del fet que tot vèrtex Hw està connectat amb el punt base: en efecte, posant $w = a_{i_1}^{\epsilon_1} a_{i_2}^{\epsilon_2} \cdots a_{i_l}^{\epsilon_l}$ com a paraula en $A^{\pm}$, tenim el camí

$$\gamma\colon \circledcirc \xrightarrow{a_{i_1}^{\epsilon_1}} Ha_{i_1}^{\epsilon_1} \xrightarrow{a_{i_2}^{\epsilon_2}} Ha_{i_1}^{\epsilon_1} a_{i_2}^{\epsilon_2} \xrightarrow{a_{i_3}^{\epsilon_3}} \cdots \xrightarrow{a_{i_l}^{\epsilon_l}} Hw. \tag{10}$$

Això demostra (ii). L'apartat (iii) se segueix del fet que el camí (10) és tancat si i només si $Hw = \circledcirc = H$, és a dir, si i només si $\ell(\gamma) = w \in H$.

Per veure (iv) considerem un arc e de $\mathsf{Sch}(H,A)$ no pertanyent a $\operatorname{core}(\mathsf{Sch}(H,A))$. Si hi hagués camins, i per tant camins reduïts, γ i η a $\mathsf{Sch}(H,A) \setminus \{\mathsf{e}\}$, de $\circledcirc$ a $\iota\mathsf{e}$, i de $\circledcirc$ a $\tau\mathsf{e}$, respectivament, llavors $\gamma\mathsf{e}\eta^{-1}$ seria un $\circledcirc$-camí reduït, cosa que contradiu que e no forma part del cor. Per tant, e és un pont a $\mathsf{Sch}(H,A)$. Canviant e per e^{-1} si cal, podem suposar que hi ha un camí γ de $\circledcirc$ a $\iota\mathsf{e}$, que no passa per l'arc e. Llavors, si la component connexa de $\mathsf{Sch}(H,A) \setminus \{\mathsf{e}\}$ que conté $\tau\mathsf{e}$ no fos arbre, hi hauria un $\tau\mathsf{e}$-camí reduït no trivial ξ, i $\gamma\mathsf{e}\xi\mathsf{e}^{-1}\gamma^{-1}$

seria un $\circledast$-camí reduït que passa per e i contradiu un altre cop el fet que e no pertany al cor. Per tant, la component connexa de $\mathsf{Sch}(H, A) \setminus \{\mathsf{e}\}$ que conté $\tau\mathsf{e}$ és un arbre; i haurà de ser forçosament infinit ja que si no, tindria vèrtexs de grau 1, cosa que contradiria el fet que $\mathsf{Sch}(H, A)$ és saturat. Com que cada vèrtex és saturat, aquest arbre és necessàriament una branca de Cayley (vegeu la figura 10).

Finalment, per a veure (v) només cal observar l'autòmat $\mathsf{Sch}(\langle b \rangle, \{a, b\})$, dibuixat a la figura 10: un b-llaç al punt base $\circledast$, i dues branques de Cayley naixent dels dos arcs disponibles al punt base. $\square$

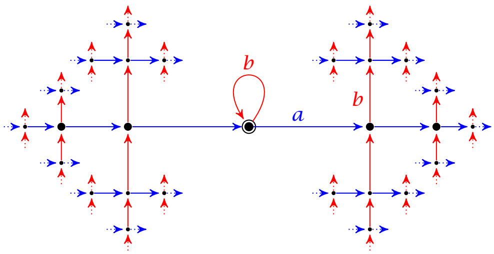


FIGURA 10: L'autòmat de Schreier de $\langle b \rangle \leqslant \mathbb{F}_{\{a,b\}}$.

De la proposició 47 és clar que la propietat d'ésser cor és l'única que li falta a $\mathsf{Sch}(H, A)$ per a ser un autòmat reduït que reconeix H.

DEFINICIÓ 48. Sigui H un subgrup de $\mathbb{F}_A$. Anomenem *autòmat de Stallings* de H respecte a A, designat per $\mathsf{St}(H, A)$, el cor de $\mathsf{Sch}(H, A)$; és a dir $\mathsf{St}(H, A) = \mathrm{core}(\mathsf{Sch}(H, A))$. També definim l'*autòmat restringit de Stallings* de H respecte a A com el digraf $\mathsf{St}^*(H, A) = \mathrm{core}^*(\mathsf{St}(H, A))$. Si la base de referència A és clara pel context, habitualment l'ometrem i escriurem simplement $\mathsf{Sch}(H)$, $\mathsf{St}(H)$, i $\mathsf{St}^*(H)$.

EXEMPLE 49. (La part positiva de) l'autòmat de Stallings $\mathsf{St}(\mathbb{F}_A, A)$ té un únic vèrtex i un llaç etiquetat per cada $a \in A$. Aquest autòmat s'anomena *rosa* (de $\#A$ pètals), i es designa per $\mathcal{B}_A$ o $\mathcal{B}_n$, on $n = \#A$:

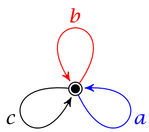


FIGURA 11: $\mathcal{B}_3$, una rosa de tres pètals.

OBSERVACIÓ 50. És clar que, per a qualsevol cardinal n, el grup fonamental de la rosa de n pètals és el grup lliure de rang n; és a dir, $\pi_{\circledast}(\mathcal{B}_n) \simeq \mathbb{F}_n$.

A continuació resumim les propietats principals de l'autòmat de Stallings i la seva relació amb el de Schreier.

PROPOSICIÓ 51. *Sigui H un subgrup de $\mathbb{F}_A$. Aleshores,*

(i) $\mathsf{St}(H, A)$ *és un A-autòmat involutiu, determinista, i cor (per tant, reduït);*

(ii) $\langle \mathsf{St}(H, A) \rangle = H$*;*

(iii) $\mathsf{St}(H, A)$ *és saturat* $\Leftrightarrow \mathsf{St}(H, A) = \mathsf{Sch}(H, A) \Leftrightarrow \mathsf{Sch}(H, A)$ *és cor;*

(iv) $\mathsf{St}(H, A)$ *no és necessàriament saturat;*

(v) $\mathsf{Sch}(H, A)$ *consisteix en* $\mathsf{St}(H, A)$ *amb una a-branca de Stallings adjacent a cada vèrtex a-deficient de* $\mathsf{St}(H, A)$*, on $a \in A^{\pm}$;*

(vi) l'índex $|\mathbb{F}_A : H|$ *és finit si i només si* $\mathsf{St}(H, A)$ *és saturat i* $\# \mathsf{V}\, \mathsf{St}(H, A) < \infty$*.*

PROVA. L'apartat (i) és immediat de la definició d'autòmat de Stallings (definició 48), mentre que (ii) se segueix de la mateixa definició i l'observació 38.

Per a veure (iii) només cal recordar que $\mathsf{Sch}(H)$ és sempre saturat, $\mathsf{St}(H)$ és sempre cor, i $\mathsf{St}(H) = \operatorname{core}(\mathsf{Sch}(H))$. Per tant, (iv) és conseqüència de la proposició 47(v).

(v) Si p és un vèrtex a-deficient de $\mathsf{St}(H)$, l'arc de $\mathsf{Sch}(H)$ llegint a des de p no pertany a $\mathsf{St}(H)$ i aleshores el resultat reclamat no és més que una reinterpretació de la proposició 47(iv).

(vi) Recordem que $|\mathbb{F}_A : H| = \# \mathsf{V}\, \mathsf{Sch}(H, A)$. Si $\mathsf{St}(H)$ és saturat i té un nombre finit de vèrtexs, aleshores $|\mathbb{F}_A : H| = \# \mathsf{V}\, \mathsf{Sch}(H, A) = \# \mathsf{V}\, \mathsf{St}(H, A) < \infty$, on hem usat l'apartat (iii) a la segona igualtat. Recíprocament, suposem $|\mathbb{F}_A : H| < \infty$: per una banda $\# \mathsf{V}\, \mathsf{St}(H, A) \leq \# \mathsf{V}\, \mathsf{Sch}(H, A) = |\mathbb{F}_A : H| < \infty$; i per una altra, si $\mathsf{St}(H, A)$ fos insaturat, (v) implicaria que $\mathsf{Sch}(H, A)$ té arbres infinits penjant de tots els vèrtexs insaturats, cosa que contradiu que $\# \mathsf{V}\, \mathsf{Sch}(H, A) = |\mathbb{F}_A : H| < \infty$. □

És convenient tenir present que, com a conseqüència de la teoria desenvolupada, les propietats (i) i (ii) de la proposició 47, i la propietat (i) de la proposició 51, caracteritzen, de fet, els respectius tipus d'autòmats.

COROL·LARI 52. *Sigui Γ un A-autòmat involutiu i determinista. Aleshores:*

(i) si Γ és saturat i connex, aleshores $\Gamma \simeq \mathsf{Sch}(\langle \Gamma \rangle, A)$*;*

(ii) si Γ és cor, aleshores $\Gamma \simeq \mathsf{St}(\langle \Gamma \rangle, A)$. □

Disposem ja de tots els ingredients necessaris per a establir la bijecció que buscàvem entre A-autòmats i subgrups de $\mathbb{F}_A$, tot restringint (9) al domini adequat.

TEOREMA 53 (J. R. STALLINGS [50]). *La funció*

$$\begin{array}{rcl} \{\textit{(classes d'isomorfia de) } A\textit{-autòmats reduïts}\} & \to & \{\textit{subgrups de } \mathbb{F}_A\} \\ \Gamma & \mapsto & \langle \Gamma \rangle \end{array} \tag{11}$$

és una bijecció, amb inversa $\mathsf{St}(H, A) \leftarrow\!\shortmid H$.

Prova. Les dues aplicacions estan ben definides: en efecte, per a tot Γ, $\langle\Gamma\rangle$ és un subgrup de $\mathbb{F}_A$; i, gràcies a la proposició 51(i), per a tot subgrup $H \leqslant \mathbb{F}_A$, $\mathsf{St}(H, A)$ és un A-autòmat reduït. I són una inversa de l'altra: per la proposició 51(ii), $\langle \mathsf{St}(H, A)\rangle = H$ i, com que Γ és reduït, $\mathsf{St}(\langle\Gamma\rangle, A) = \Gamma$, a conseqüència del corol·lari 44. $\square$

El pas següent és garantir el caràcter computacional de la bijecció (11), que serà fonamental per als nostres interessos. Veurem que els subgrups *finitament generats* corresponen precisament als A-autòmats reduïts *finits* i que la conversió entre ambdós és algorísmica. Trobarem mètodes eficients per a computar les dues direccions de la bijecció (11): (a) donat un A-autòmat reduït i finit Γ, calcularem explícitament un sistema de generadors finit de $\langle\Gamma\rangle$ (millor encara, en calcularem una base, i demostrarem de passada que $\langle\Gamma\rangle$ sempre torna a ser un grup lliure); i (b) donat un sistema de generadors finit de $\langle\Gamma\rangle$, construirem el seu autòmat (finit) de Stallings $\mathsf{St}(H, A)$.

Proposició 54. *Sigui* Γ *un A-autòmat involutiu i connex, sigui T un arbre generador de* Γ*, i considerem*

$$S_T = \{w_{\mathsf{e}} : \mathsf{e} \in \mathsf{E}^+\Gamma \setminus \mathsf{E}T\} \subseteq \langle\Gamma\rangle \leqslant \mathbb{F}_A, \tag{12}$$

on $w_{\mathsf{e}} = \overline{\ell}(\circledcirc \overset{T}{\rightsquigarrow} \bullet \xrightarrow{\mathsf{e}} \bullet \overset{T}{\rightsquigarrow} \circledcirc)$. *Llavors,*

(i) S_T *és un sistema de generadors per* $\langle\Gamma\rangle$*;*

(ii) si Γ *és determinista, aleshores* $\langle\Gamma\rangle$ *és un grup lliure i* S_T *n'és una base; en particular, el rang algebraic* $\mathrm{rk}(\langle\Gamma\rangle)$ *i el rang gràfic* $\mathrm{rk}(\Gamma)$ *coincideixen;*

(iii) si Γ *és reduït, aleshores* $\langle\Gamma\rangle$ *és finitament generat si i només si* Γ *és finit; i en aquest cas,* $\mathrm{rk}(\langle\Gamma\rangle) = 1 - \#\mathsf{V}\Gamma + \#\mathsf{E}^+\Gamma$.

Prova. (i) Sigui $w \in \langle\Gamma\rangle$, i expressem-lo com a $w = \overline{\ell}(\gamma)$, per a cert $\circledcirc$-camí reduït γ a Γ. Si distingim les visites de γ a arcs fora de T, podem escriure

$$\gamma\colon \circledcirc \overset{T}{\rightsquigarrow} \bullet \xrightarrow{\mathsf{e}_1^{\epsilon_1}} \bullet \overset{T}{\rightsquigarrow} \bullet \xrightarrow{\mathsf{e}_2^{\epsilon_2}} \bullet \overset{T}{\rightsquigarrow} \bullet \cdots \bullet \overset{T}{\rightsquigarrow} \bullet \xrightarrow{\mathsf{e}_l^{\epsilon_l}} \bullet \overset{T}{\rightsquigarrow} \circledcirc,$$

on $\mathsf{e}_1, \ldots, \mathsf{e}_l \in \mathsf{E}^+\Gamma \setminus \mathsf{E}T$ (amb possibles repeticions) i $\epsilon_j = \pm 1$. Observem ara que γ té la mateixa etiqueta reduïda que el camí ampliat

$$\gamma'\colon \circledcirc \overset{T}{\rightsquigarrow} \bullet \xrightarrow{\mathsf{e}_1^{\epsilon_1}} \bullet \overset{T}{\rightsquigarrow} \circledcirc \overset{T}{\rightsquigarrow} \bullet \xrightarrow{\mathsf{e}_2^{\epsilon_2}} \bullet \overset{T}{\rightsquigarrow} \circledcirc \cdots \circledcirc \overset{T}{\rightsquigarrow} \bullet \xrightarrow{\mathsf{e}_l^{\epsilon_l}} \bullet \overset{T}{\rightsquigarrow} \circledcirc. \tag{13}$$

Per tant, $w = \overline{\ell}(\gamma) = \overline{\ell}(\gamma') = w_{\mathsf{e}_1}^{\epsilon_1} w_{\mathsf{e}_2}^{\epsilon_2} \cdots w_{\mathsf{e}_l}^{\epsilon_l} \in \langle S_T\rangle$.

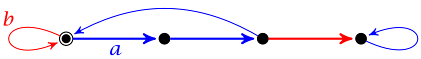
(ii) Suposem ara, a més, que Γ és determinista. Demostrarem que S_T és, de fet, una base de $\langle\Gamma\rangle$ i que, per tant, $\langle\Gamma\rangle$ és un grup lliure. És suficient veure que qualsevol paraula reduïda no buida en S_T representa un element no trivial de $\mathbb{F}_A$. En efecte, sigui $w = w_{\mathsf{e}_1}^{\epsilon_1} w_{\mathsf{e}_2}^{\epsilon_2} \cdots w_{\mathsf{e}_l}^{\epsilon_l}$, amb $l \geq 1$, $\mathsf{e}_1, \ldots, \mathsf{e}_l \in \mathsf{E}^+\Gamma \setminus \mathsf{E}T$ (amb possibles repeticions), i tal que no hi ha dos factors successius inversos l'un de l'altre, *i. e.*, $\mathsf{e}_i = \mathsf{e}_{i+1}$ implica $\epsilon_i = \epsilon_{i+1}$. Aleshores,

$$\begin{aligned}
\overline{w} &= \overline{w_{\mathsf{e}_1}^{\epsilon_1} w_{\mathsf{e}_2}^{\epsilon_2} \cdots w_{\mathsf{e}_l}^{\epsilon_l}} \\
&= \overline{\ell}(\circledcirc \overset{T}{\rightsquigarrow} \bullet \xrightarrow{\mathsf{e}_1^{\epsilon_1}} \bullet \overset{T}{\rightsquigarrow} \circledcirc \overset{T}{\rightsquigarrow} \bullet \xrightarrow{\mathsf{e}_2^{\epsilon_2}} \bullet \overset{T}{\rightsquigarrow} \circledcirc \cdots \circledcirc \overset{T}{\rightsquigarrow} \bullet \xrightarrow{\mathsf{e}_l^{\epsilon_l}} \bullet \overset{T}{\rightsquigarrow} \circledcirc) \\
&= \overline{\ell}(\circledcirc \overset{T}{\rightsquigarrow} \bullet \xrightarrow{\mathsf{e}_1^{\epsilon_1}} \bullet \overset{T}{\rightsquigarrow} \bullet \xrightarrow{\mathsf{e}_2^{\epsilon_2}} \bullet \overset{T}{\rightsquigarrow} \bullet \cdots \bullet \overset{T}{\rightsquigarrow} \bullet \xrightarrow{\mathsf{e}_l^{\epsilon_l}} \bullet \overset{T}{\rightsquigarrow} \circledcirc).
\end{aligned}$$

Però aquest últim $\circledcirc$-camí és no buit ($l \geq 1$), i reduït (donat que els arcs $\mathsf{e}_i^{\epsilon_i}$ estan tots fora de T, i dos de consecutius mai no presenten retrocés). Com que Γ és determinista, això significa que $\overline{w} \neq 1$, com volíem demostrar. Per tant, S_T és una base de $\langle \Gamma \rangle$ i el rang algebraic i el rang gràfic coincideixen, $\mathrm{rk}(\langle \Gamma \rangle) = \# S_T = \mathrm{rk}(\Gamma)$.

(iii) Finalment, suposem que Γ és reduït. Si Γ és finit, llavors $\#(\mathsf{E}^+\Gamma \setminus \mathsf{E}T) < \infty$ i $\langle \Gamma \rangle$ és finitament generat. Recíprocament, si $\Gamma = \mathrm{core}(\Gamma)$ té rang finit, aleshores és finit (ja que, afegint un nombre finit d'arcs a un arbre infinit, no resulta mai un cor). I en aquest cas, $\mathrm{rk}(\langle \Gamma \rangle) = \mathrm{rk}(\Gamma) = 1 - \#\mathsf{V}\Gamma + \#\mathsf{E}^+\Gamma$. La demostració està completa. $\square$

Exemple 55. Considereu l'autòmat determinista següent, i l'arbre generador T format pels arcs horitzontals (representats amb traç més gruixut).



D'acord amb la proposició 54(ii), el subgrup $\langle \Gamma \rangle$ reconegut per Γ és lliure amb base el conjunt $S_T = \{b, a^3, a^2bab^{-1}a^{-2}\}$ i, per tant, de rang 3.

El següent resultat fonamental, demostrat primer per J. Nielsen, per a subgrups finitament generats, i uns anys més tard per O. Schreier, amb total generalitat, se segueix ara de manera transparent de la teoria de Stallings.

Teorema 56 (Teorema de Nielsen-Schreier, [40, 45]). *Tot subgrup d'un grup lliure és lliure.*

Prova. Pel teorema 53, tot subgrup $H \leqslant \mathbb{F}_A$ és de la forma $H = \langle \mathsf{St}(H, A) \rangle$; i, per la proposició 54, és lliure. $\square$

Finalment, situem-nos en el cas finit, i busquem un algorisme eficient per computar els dos sentits de la bijecció (11). El càlcul d'una base del subgrup reconegut per un A-autòmat reduït i finit Γ és directe de la proposició anterior: calculem un arbre generador T de Γ i, per a cada arc $\mathsf{e} \in \mathsf{E}^+\Gamma \setminus \mathsf{E}T$ (n'hi ha un nombre finit), calculem la paraula reduïda $w_{\mathsf{e}} = \overline{\ell}(\circledcirc \overset{T}{\rightsquigarrow} \bullet \xrightarrow{\mathsf{e}} \bullet \overset{T}{\rightsquigarrow} \circledcirc)$. Per la proposició 54(ii), $S_T = \{w_{\mathsf{e}} : \mathsf{e} \in \mathsf{E}^+\Gamma \setminus \mathsf{E}T\}$ és una base de $\langle \Gamma \rangle \leqslant \mathbb{F}_A$.

Per a computar la direcció contrària, donat un subgrup $H \leqslant \mathbb{F}_A$ (mitjançant una família finita S de generadors, que podem suposar paraules reduïdes), hem de trobar una manera efectiva de calcular $\mathsf{St}(H, A)$; o, el que és el mateix, una manera de calcular un A-autòmat Γ que sigui involutiu, reduït, finit, i que reconegui $\langle \Gamma \rangle = H$. Ja coneixem un A-autòmat, molt fàcil de construir, i que gairebé compleix totes aquestes condicions: l'autòmat flor $\mathsf{Fl}(S)$ és involutiu, cor, finit, reconeix $\langle \mathsf{Fl}(S) \rangle = \langle S \rangle = H$, i és determinista *excepte potser al vèrtex base* $\circledcirc$ (ja que els diferents elements de S poden començar o acabar amb la mateixa lletra de $A^{\pm}$). Per a «reparar» l'eventual no determinisme de $\mathsf{Fl}(S)$, necessitem un procediment que converteixi un A-autòmat finit en determinista (sense perdre les altres propietats); el desenvolupem a continuació.

DEFINICIÓ 57. Sigui Γ un A-autòmat involutiu; i siguin e_1 i e_2 dos arcs de Γ que violen el determinisme, *i. e.*, que compleixen $\iota\mathsf{e}_1 = \iota\mathsf{e}_2$, $\ell(\mathsf{e}_1) = \ell(\mathsf{e}_2)$, però $\mathsf{e}_1 \neq \mathsf{e}_2$. Anomenem *plegament (elemental) de Stallings*,[16] i el designem per $\Gamma \curvearrowright \Gamma'$, la transformació consistent a identificar els arcs e_1 i e_2 (i els seus corresponents inversos) a Γ. Si els arcs e_1 i e_2 no són paral·lels (*i. e.*, si $\tau\mathsf{e}_1 \neq \tau\mathsf{e}_2$), direm que és un *plegament obert*; i en cas contrari, direm que és un *plegament tancat* (vegeu la figura 12).

FIGURA 12: Un plegament obert (esquerra) i un de tancat (dreta).

Un senzill recompte de vèrtexs i arcs proporciona el resultat següent, que serà rellevant més endavant.

OBSERVACIÓ 58. Si Γ és finit i $\Gamma \curvearrowright \Gamma'$ és un plegament elemental de Stallings, aleshores:

$$\operatorname{rk}(\Gamma') = \begin{cases} \operatorname{rk}(\Gamma) & \text{si } \Gamma \curvearrowright \Gamma' \text{ és obert,} \\ \operatorname{rk}(\Gamma) - 1 & \text{si } \Gamma \curvearrowright \Gamma' \text{ és tancat.} \end{cases} \tag{14}$$

És clar que els plegaments de Stallings no modifiquen el subgrup reconegut.

LEMA 59. *Si* $\Gamma \curvearrowright \Gamma'$ *és un plegament de Stallings, aleshores* $\langle \Gamma' \rangle = \langle \Gamma \rangle$. □

Llavors, si Γ és un A-autòmat involutiu, finit, reconeixent H, el *procés de Stallings* per a convertir Γ en determinista és com segueix: si Γ ja és determinista, no cal fer res; en cas contrari, detectem successivament possibles plegaments (oberts o tancats) i els realitzem fins que no en quedi cap de disponible, és a dir, fins a obtenir un autòmat determinista. Observeu que realitzant un plegament podem provocar-ne de nous i fins i tot *augmentar* el nombre de plegaments visibles a fer. Malgrat això, està garantit que arribarem a una situació determinista amb un nombre finit de passes ja que l'autòmat inicial Γ és finit, i en cada plegament el nombre d'arcs decreix exactament en una unitat. Un cop arribem a un A-autòmat determinista, prenem el cor i designem per Γ' el A-autòmat reduït resultant. Observeu que, pel lema 59 i l'observació 38, $\langle \Gamma' \rangle = \langle \Gamma \rangle$. I pel corol·lari 44, Γ' ha de ser (isomorf a) l'autòmat de Stallings $\mathsf{St}(H, A)$. El procés descrit s'anomena (una) *seqüència de plegaments de Stallings* per a Γ:

$$\Gamma = \Gamma_0 \overset{\phi_1}{\curvearrowright} \Gamma_1 \overset{\phi_2}{\curvearrowright} \cdots \overset{\phi_p}{\curvearrowright} \Gamma_p \overset{\text{core}}{\curvearrowright} \operatorname{core}(\Gamma_p) \simeq \mathsf{St}(H, A).$$

16 En anglès, *stallings folding.*

Observeu que hi pot haver, en principi, diferents plegaments —i per tant, diferents seqüències de plegaments— disponibles a Γ. Ara bé, com que l'autòmat final és reduït, el corol·lari 44 ens garanteix que l'objecte final obtingut serà sempre el mateix (mòdul isomorfisme), *independentment de la seqüència de plegaments seguida*.

Construint una seqüència de plegaments de Stallings per a l'autòmat flor $\mathsf{Fl}(S)$, obtenim una manera efectiva de calcular $\mathsf{St}(H,A)$ a partir de qualsevol conjunt de generadors finit S per a H. No és difícil demostrar que, en aplicar una seqüència de plegaments de Stallings a l'autòmat flor $\mathsf{Fl}(S)$ d'un conjunt S de paraules *reduïdes*, cap dels plegaments de la seqüència no trenca el caràcter cor de l'autòmat inicial i, per tant, no és necessari realitzar el pas final de prendre el cor:

$$\mathsf{Fl}(S) = \Gamma_0 \overset{\phi_1}{\curvearrowright} \Gamma_1 \overset{\phi_2}{\curvearrowright} \cdots \overset{\phi_p}{\curvearrowright} \Gamma_p = \mathsf{St}(H,A).$$

Observeu finalment que el resultat de la seqüència de plegaments, $\mathsf{St}(H,A)$, depèn canònicament del subgrup H i, per tant, *també és independent del sistema de generadors finit S* de H amb què haguem començat el procés (mentre que $\mathsf{Fl}(S)$ en depèn fortament). Això conclou la computació de la bijecció (11).

Incorporant a l'enunciat del teorema 53 els resultats que acabem de demostrar, obtenim el teorema principal d'aquesta secció.

Teorema 60 (J. R. Stallings [50]). *La funció*

$$\begin{array}{rcl} \mathsf{St}\colon \{\textit{subgrups de } \mathbb{F}_A\} & \to & \{\textit{(classes d'isomorfia de) } A\textit{-autòmats reduïts}\} \\ H & \mapsto & \mathsf{St}(H,A) \end{array} \tag{15}$$

és una bijecció, amb inversa $\langle\Gamma\rangle \leftarrow\!\shortmid \Gamma$. A més, els subgrups finitament generats corresponen precisament als autòmats reduïts finits i, en aquest cas, la bijecció és computable en ambdós sentits. □

Exemple 61. Siguin $\mathbb{F}_2$ el grup lliure sobre $A = \{a,b\}$, $S = \{u_1,u_2,u_3\} \subseteq \mathbb{F}_2$ i $H = \langle S\rangle \leqslant \mathbb{F}_2$ el subgrup generat pels elements $u_1 = a^3$, $u_2 = abab^{-1}$, i $u_3 = a^{-1}bab^{-1}$. Per obtenir una base (i, per tant, el rang) de H, calcularem primer $\mathsf{St}(H,A)$. Comencem construint l'autòmat flor $\Gamma_0 = \mathsf{Fl}(S)$, i anem fent plegaments fins a obtenir l'autòmat de Stallings $\mathsf{St}(H,A)$: a la figura 13 teniu una possible seqüència de Stallings $\Gamma_0 \curvearrowright \Gamma_1 \curvearrowright \Gamma_2 \curvearrowright \Gamma_3 \curvearrowright \Gamma_4 \curvearrowright \Gamma_5 \curvearrowright \Gamma_6 = \mathsf{St}(H)$, tot indicant, en cada pas, amb traç gruixut, els arcs que es pleguen al pas següent (observeu que el primer pas són en realitat tres plegaments fets simultàniament):

Finalment, prenent $\odot \xrightarrow{b} \bullet$ com a arbre generador de $\mathsf{St}(H)$, la proposició 54(ii) ens diu que $\{a, bab^{-1}\}$ és una base del subgrup H; en particular, $\mathrm{rk}(H) = 2$.

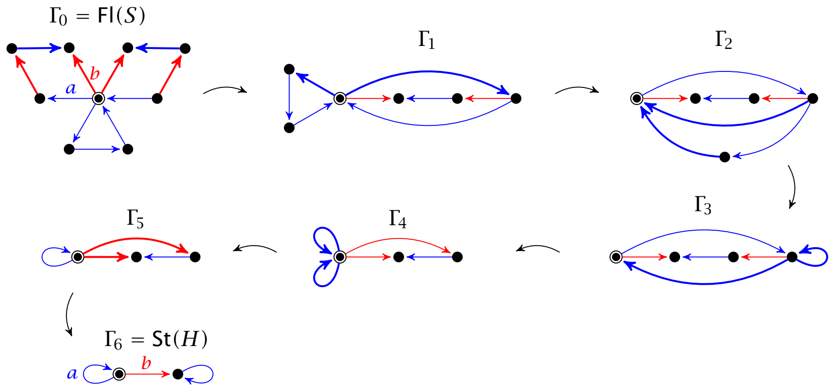


FIGURA 13: Una seqüència de plegaments de Stallings pel subgrup $H = \langle a^3, abab^{-1}, a^{-1}bab^{-1}\rangle \leqslant \mathbb{F}_{\{a,b\}}$.

Tornem per un moment al morfisme $\widetilde{\ell}_\Gamma$ definit a (8). Dèiem més amunt que no era un morfisme injectiu, en general. I, efectivament, pel A-autòmat $\Gamma_0 = \mathsf{Fl}(S)$ de l'exemple anterior (al vèrtex base $\odot$) no ho és ja que $\pi_\odot(\Gamma_0)$ és un grup lliure de rang $\operatorname{rk}(\Gamma_0) = 1 - \#\mathsf{V}\Gamma_0 + \#\mathsf{E}^+\Gamma_0 = 1 - 9 + 11 = 3 = \#S$, mentre que $\langle \Gamma_0 \rangle = \langle S \rangle = H$ és un (sub)grup (de $\mathbb{F}_A$) lliure de rang 2. Això vol dir que els tres generadors inicials u_1, u_2, u_3 de H *no* són base de H, és a dir, no són independents; per tant, hi ha d'haver un producte reduït i no buit d'ells i els seus inversos que doni l'element trivial, $w(u_1, u_2, u_3) = 1$. Això és, exactament, la contrapartida algebraica del fet gràfic que $\widetilde{\ell}_\Gamma$ no sigui injectiu: hi ha un element $1 \neq [\gamma] \in \pi_\odot(\Gamma_0)$ (*i. e.*, un $\odot$-camí reduït i no buit al A-autòmat flor Γ_0) tal que $\overline{\ell}(\gamma) = 1$ (*i. e.*, que llegeixi l'etiqueta reduïda trivial). Fent càlculs veiem, per exemple, $u_2u_3^{-1}u_1^{-1}u_2u_3^{-1}u_1^{-1}u_2u_3^{-1} = 1$. Podem anar encara una mica més enllà en aquest paral·lelisme entre àlgebra i geometria, i quantificar la no injectivitat del morfisme $\widetilde{\ell}_\Gamma \colon \pi_\odot(\Gamma) \twoheadrightarrow \langle \Gamma \rangle \leqslant \mathbb{F}_A$, $[\gamma] \mapsto \overline{\ell}(\gamma)$, des dels dos punts de vista: una manera algebraica de fer-ho és mirant el nombre mínim de generadors de $\ker(\widetilde{\ell}_\Gamma)$ com a subgrup normal de $\pi_\odot(\Gamma)$; com veurem a continuació, la contrapartida gràfica és el nombre de plegaments tancats que apareixen en una (i, per tant, en qualsevol) seqüència de plegaments de Stallings de Γ a $\mathsf{St}(H, A)$.

OBSERVACIÓ 62. Si Γ és determinista, llavors $\widetilde{\ell}_\Gamma$ és injectiu. □

És clar que la pèrdua de rang gràfic en qualsevol seqüència de Stallings per un A-autòmat finit Γ és precisament el nombre de plegaments tancats, ja que els plegaments oberts no alteren el rang, i els tancats el redueixen en una unitat (vegeu l'observació 58). Es pot usar un argument geomètricalgebraic per a demostrar que aquest nombre també coincideix amb la quantitat mínima de generadors de $\ker(\widetilde{\ell}_\Gamma)$ com a subgrup normal de $\pi_\odot(\Gamma)$ (per raons d'espai, ometem els detalls tècnics d'aquesta demostració).

Proposició 63. *Sigui* Γ *un* A*-autòmat involutiu, connex, i finit, que reconeix el subgrup* $H \leqslant \mathbb{F}_A$*, i sigui*

$$\Gamma \xrightarrow{\phi_1} \Gamma_1 \xrightarrow{\phi_2} \cdots \xrightarrow{\phi_p} \Gamma_p \xrightarrow{\text{core}} \operatorname{core}(\Gamma_p) = \mathsf{St}(H, A) \tag{16}$$

una seqüència de plegaments de Stallings per a Γ*. Aleshores, els tres nombres següents coincideixen:*

(a) *el nombre de plegaments tancats a* (16)*;*

(b) $\operatorname{rk}(\Gamma) - \operatorname{rk}(\mathsf{St}(H, A))$*;*

(c) *el nombre mínim de generadors de* $\ker(\widetilde{\ell}_\Gamma)$ com a subgrup normal *de* $\pi_{\circledcirc}(\Gamma)$.

Per tant, aquest nombre és independent de la seqüència concreta de plegaments i només depèn de Γ*.*

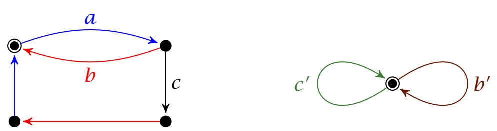
Aquest valor —independent de la seqüència concreta de plegaments i només dependent de Γ— s'anomena la *pèrdua* de Γ, designada per $\operatorname{loss}(\Gamma)$. Podem ampliar aquesta definició per a cobrir A-autòmats infinits de la manera següent:

Definició 64. Sigui Γ un A-autòmat involutiu i connex. Definim la *pèrdua* de Γ, designada per $\operatorname{loss}(\Gamma)$, com el suprem (que pot ser ∞, si Γ és infinit) del nombre de plegaments tancats, pres sobre el conjunt de totes les seqüències (finites) de plegaments de Stallings començant a Γ.

Observeu que si Γ és finit les tals seqüències de llargada maximal són, precisament, les que acaben en un Γ_p determinista; i com que $\operatorname{core}(\Gamma_p) = \mathsf{St}(\langle\Gamma\rangle)$, totes elles tenen el mateix nombre de plegaments tancats, per la proposició 63. Per tant, en el cas finit, el suprem a la definició de $\operatorname{loss}(\Gamma)$ és un màxim, i es pren sobre totes les seqüències de plegaments de Stallings començant a Γ.

Acabem la secció amb un exemple per a il·lustrar que el canvi de la base de referència pot canviar dràsticament l'aspecte de l'autòmat de Stallings. De fet, entendre com es comporta la funció $\mathsf{St}(H, A) \mapsto \mathsf{St}(H, B)$ (on A, B són bases de $\mathbb{F}$) és un dels grans reptes encara per aclarir de la teoria de Stallings.

Exemple 65 (Exemple 2.2 a [34]). Sigui $\mathbb{F}_3$ un grup lliure amb base $A = \{a, b, c\}$ i sigui $H = \langle ab, acba \rangle$. És fàcil veure que $B = \{a', b', c'\}$ és també una base de $\mathbb{F}_3$, on $a' = a$, $b' = ab$, i $c' = acba$. Els autòmats de Stallings de H respecte de A i B estan representats a la figura següent.



4 Aplicacions

En aquesta secció presentem algunes de les aplicacions més rellevants de la teoria dels autòmats de Stallings, desenvolupada a la secció 3. Començarem amb alguns teoremes clàssics sobre els subgrups del grup lliure que emergeixen de forma natural —de vegades com a simples reinterpretacions— dels resultats de la teoria de Stallings, i anirem progressant cap a aplicacions més elaborades, com ara el problema de la intersecció, font d'una de les qüestions més famoses del darrer segle en teoria geomètrica de grups.

4.1 Estructura dels subgrups

Tal com hem vist a la secció 3, una de les primeres aplicacions del teorema de Stallings (teorema 60) és el teorema de Nielsen-Schreier (teorema 56). Fixeu-vos que la bijecció (15) ens permet no només garantir que tots els subgrups d'un grup lliure són, de nou, lliures, sinó també descriure exactament (les classes d'isomorfia de) els subgrups d'un grup lliure donat: com que d'autòmats de Stallings sobre un alfabet de dues lletres n'hi ha de qualsevol rang fins a numerable (inclòs), la descripció següent se segueix immediatament.

Corol·lari 66. *Sigui $\mathbb{F}_\kappa$ el grup lliure de rang $\kappa \in [2, \aleph_0]$. Aleshores, per a tot cardinal $\mu \in [0, \aleph_0]$ existeix un subgrup $H \leqslant \mathbb{F}_\kappa$ tal que $H \simeq \mathbb{F}_\mu$.* □

En particular, subgrups de qualsevol rang finit i, fins i tot, de rang infinit numerable poden aparèixer com a subgrups de $\mathbb{F}_2$; a continuació presentem dos exemples clàssics d'aquest fet. Aquest és un comportament radicalment diferent del de l'àlgebra lineal (un K-espai vectorial de dimensió n *només* conté subespais de dimensions $0, 1, \ldots, n$), que confereix al reticle de subgrups d'un grup lliure un cert caràcter fractal.

Exemple 67. Sigui $\mathbb{F}_{\{a,b\}} = \langle a, b \mid - \rangle$ un grup lliure de rang 2. Aleshores, la clausura normal de b, designada per $\langle\langle b \rangle\rangle$, és un subgrup de $\mathbb{F}_{\{a,b\}}$ de rang infinit amb autòmat de Stallings (de rang infinit) $\mathsf{St}(\langle\langle b \rangle\rangle)$ representat a la figura 14. Prenent com a arbre generador el marcat amb traç gruixut (de fet, l'únic possible) obtenim la base $\{a^k b a^{-k} : k \in \mathbb{Z}\}$.

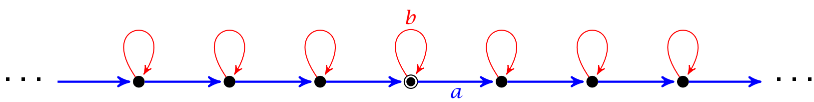


Figura 14: L'autòmat de Stallings de $\langle\langle b \rangle\rangle \leqslant \mathbb{F}_{\{a,b\}}$.

Exemple 68. Un altre exemple típic és el commutador $H = [\mathbb{F}_{\{a,b\}}, \mathbb{F}_{\{a,b\}}] \trianglelefteq \mathbb{F}_{\{a,b\}}$, *i. e.*, el subgrup normal de $\mathbb{F}_{\{a,b\}}$ generat per tots els elements de la forma $[v, w] = v^{-1}w^{-1}vw$, amb $v, w \in \mathbb{F}_{\{a,b\}}$. El subgrup H té rang infinit ja que, com tots els subgrups normals, el seu autòmat de Stallings $\mathsf{St}(H) = \mathsf{Sch}(H)$ és el digraf de Cayley del grup quocient $\mathbb{F}_{\{a,b\}}/H \simeq \mathbb{Z}^2$, respecte dels generadors $\{[a], [b]\}$, *i. e.*, respecte de la base canònica de $\mathbb{Z}^2$: la graella bidimensional infinita, amb els arcs horitzontals etiquetats per a, i els arcs verticals etiquetats per b; vegeu la figura 15. Proposem al lector descriure una base del commutador H a partir del vostre arbre generador preferit.

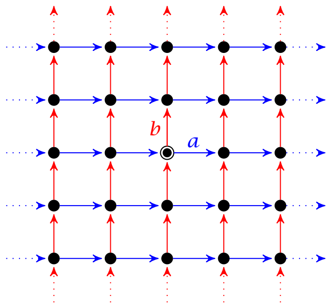


FIGURA 15: L'autòmat de Stallings del commutador $[\mathbb{F}_{\{a,b\}}, \mathbb{F}_{\{a,b\}}]$.

4.2 El problema de la pertinença

En aquesta secció estudiarem el problema de la pertinença en grups lliures i hi donarem una solució general. A continuació l'enunciem en general per a un grup finitament presentat $G = \langle A \mid R \rangle$.

PROBLEMA DE LA PERTINENÇA A $G = \langle A \mid R \rangle$, $\mathsf{MP}(G)$. *Donada una família finita $u, v_1, \ldots, v_k$ de paraules en els generadors de G, decidir si (l'element $g \in G$ representat per) u pertany al subgrup $\langle v_1, \ldots, v_k \rangle_G \leqslant G$; i, en cas afirmatiu, trobar una expressió per a u com a producte dels $v_i^{\pm}$.*

Situem-nos al grup lliure $\mathbb{F}_A$; els elements $u, v_1, \ldots, v_k$ són paraules (que podem suposar reduïdes, ja que la reducció és trivialment algorísmica) en l'alfabet A, i hem de decidir si $u \in H = \langle v_1, \ldots, v_k \rangle$.

A tal efecte, primer calculem l'autòmat de Stallings $\mathsf{St}(H)$ tal com hem vist a la secció anterior: construïm l'autòmat flor, $\mathsf{Fl}(S)$, de pètals $S = \{v_1, \ldots, v_k\}$, i anem fent plegaments successius (en qualsevol ordre) fins a obtenir $\mathsf{St}(H)$,

$$\mathsf{Fl}(S) = \Gamma_0 \curvearrowright \Gamma_1 \curvearrowright \cdots \curvearrowright \Gamma_{p-1} \curvearrowright \Gamma_p = \mathsf{St}(H). \tag{17}$$

Per les propietats (i) i (ii) a la proposició 51, sabem que $\mathsf{St}(H)$ és un autòmat determinista que reconeix el subgrup H. Per tant, $u \in \langle H \rangle$ si i només si podem llegir la paraula reduïda u com a etiqueta d'algun $\circledcirc$-camí a $\mathsf{St}(H)$. Però, gràcies al determinisme de $\mathsf{St}(H)$, això és molt fàcil de comprovar: començant a $\circledcirc$, anem resseguint l'únic possible camí etiquetat amb les lletres consecutives de $u = a_{i_1}^{\epsilon_1} a_{i_2}^{\epsilon_2} \cdots a_{i_l}^{\epsilon_l}$; si en un determinat punt no podem llegir la lletra següent, deduïm que $u \notin H$; si podem completar la lectura de u amb un camí que no acaba a $\circledcirc$, deduïm igualment que $u \notin H$; i finalment, si completem la lectura de u mitjançant un camí tancat que retorna a $\circledcirc$ (*i. e.*, un $\circledcirc$-camí), concloem que $u \in H$. Donat que aquest procediment cobreix tots els desenllaços possibles, això ens permet decidir algorísmicament si $u \in H$.

La segona part de l'algorisme consisteix a suposar que la resposta és afirmativa (*i. e.*, que $u \in H$ i tenim aquesta paraula realitzada com l'etiqueta d'un $\odot$-camí reduït γ a l'autòmat $\mathsf{St}(H)$), i buscar una manera efectiva d'expressar u en termes dels generadors originals $v_1, \ldots, v_k$. De passada, entendrem quan aquesta expressió és única i quan no. La idea és la següent: anomenem $\gamma_p = \gamma$ i l'anem *elevant enrere*, plegament a plegament, al llarg de la seqüència de plegaments usada per a calcular $\mathsf{St}(H)$, fins a obtenir un $\odot$-camí reduït γ_0 a l'autòmat flor $\mathsf{Fl}(S) = \Gamma_0$:

$$\begin{array}{ccccccccc} \mathsf{Fl}(S) = \Gamma_0 & \curvearrowright & \Gamma_1 & \curvearrowright & \cdots & \curvearrowright & \Gamma_{p-1} & \curvearrowright & \Gamma_p = \mathsf{St}(H) \\ \gamma_0 & \hookleftarrow & \gamma_1 & \hookleftarrow & \cdots & \hookleftarrow & \gamma_{p-1} & \hookleftarrow & \gamma_p = \gamma. \end{array} \tag{18}$$

Per una banda, gràcies a la forma de l'autòmat $\mathsf{Fl}(S)$, aquest últim camí γ_0 no és res més que una successió de pètals o pètals inversos, és a dir, un camí reduït amb etiqueta no necessàriament reduïda a $(A^{\pm})^*$, *però igual a una paraula reduïda en* $v_1^{\pm 1}, \ldots, v_k^{\pm 1}$. Per altra banda, farem l'elevació $\gamma_{i+1} \mapsto \gamma_i$ a través de cada plegament elemental de manera que el resultat sigui un camí reduït amb etiqueta $\ell(\gamma_i) = u_i$ no necessàriament reduïda, però tal que $\overline{u_i} = \overline{u}$; és a dir, representant el mateix element que u a $\mathbb{F}_A$. Per tant, el procés d'elevació de γ produirà una seqüència de paraules $u = u_p, u_{p-1}, \ldots, u_1, u_0 \in (A^{\pm})^*$, totes amb etiqueta reduïda igual a $\overline{u} \in \mathbb{F}_A$, introduint una o diverses cancel·lacions a cada pas, de manera que u_0 sigui l'etiqueta d'un $\odot$-camí reduït de $\mathsf{Fl}(S)$, és a dir, un cert producte dels $v_i^{\pm 1}$, que és el que estem buscant.

Fixem-nos, doncs, en un dels plegaments elementals $\Gamma_i \curvearrowright \Gamma_{i+1}$ de la seqüència (17), considerem un $\odot$-camí reduït γ_{i+1} a Γ_{i+1} (amb $u_{i+1} = \ell(\gamma_{i+1}) \in (A^{\pm})^*$), i estudiem com fer-ne l'elevació a Γ_i. Permutant i invertint lletres de A si cal, podem suposar que el plegament elemental en qüestió consisteix en la identificació de dos arcs diferents, diguem-ne e_1 i e_2, tals que $\iota\mathsf{e}_1 = \iota\mathsf{e}_2$ i $\ell(\mathsf{e}_1) = \ell(\mathsf{e}_2) = a$; vegeu la figura 12.

Observeu que els autòmats Γ_i i Γ_{i+1} són idèntics excepte en els dos arcs e_1 i e_2 (que són diferents a Γ_i i estan identificats a Γ_{i+1}), i excepte potser en els vèrtexs $\mathsf{q}_1 = \tau\mathsf{e}_1$ i $\mathsf{q}_2 = \tau\mathsf{e}_2$ (que són iguals a Γ_{i+1}, i *potser* diferents de Γ_i). Si $\mathsf{q}_1 \neq_{\Gamma_i} \mathsf{q}_2$ el plegament és obert, i en cas contrari tancat. Això és independent del fet que el vèrtex $\mathsf{p} = \iota\mathsf{e}_1 = \iota\mathsf{e}_2$ coincideixi o no amb q_1 i/o amb q_2 (és a dir, que e_1 i/o e_2 siguin o no llaços); aquesta possibilitat complica la visualització del procediment que farem, però no afecta els arguments. Distingim dos casos.

- *Cas 1:* $\Gamma_i \curvearrowright \Gamma_{i+1}$ *és obert (*i. e.*,* $\mathsf{q}_1 \neq_{\Gamma_i} \mathsf{q}_2$*).* Sigui $k \geq 0$ el nombre de visites del camí reduït γ_{i+1} al vèrtex identificat $\mathsf{q}_1 = \mathsf{q}_2$; cadascuna d'aquestes visites s'anomena *crítica* si γ_{i+1} arriba a $\mathsf{q}_1 = \mathsf{q}_2$ per un arc incident a q_1 en Γ_i i en surt per un d'incident a q_2 (o viceversa). És evident que cada segment γ de γ_{i+1} entre visites crítiques consecutives a $\mathsf{q}_1 = \mathsf{q}_2$ s'eleva al camí idèntic γ de Γ_i (entenent que cada visita a l'arc plegat $\mathsf{e}_1 = \mathsf{e}_2$ cal substituir-la per e_1 o e_2 segons quins siguin els arcs adjacents a γ_{i+1}; observeu que només hi ha una possibilitat). Això ens dona una elevació de γ_{i+1} a un «$\odot$-camí» de Γ_i amb la mateixa etiqueta u_{i+1}, però amb una discontinuïtat (saltant de q_1 a q_2, o viceversa) per cada visita crítica de γ_{i+1} al vèrtex $\mathsf{q}_1 = \mathsf{q}_2$. Aquest problema el podem resoldre fàcilment intercalant el segment $\mathsf{e}_1^{-1}\mathsf{e}_2$ (ó $\mathsf{e}_2^{-1}\mathsf{e}_1$) per cadascuna de les visites crítiques, i obtenim així el $\circledast$-camí reduït γ_i a Γ_i. A més, com que l'etiqueta d'aquests segments afegits és sempre $a^{-1}a$, l'etiqueta $u_i = \ell(\gamma_i)$ serà $\ell(\gamma_{i+1}) = u_{i+1}$ amb k' segments $a^{-1}a$ intercalats en les posicions de les $k' \leq k$ visites crítiques a $\mathsf{q}_1 = \mathsf{q}_2$; en particular, $\overline{u_i} = \overline{u_{i+1}} \in \mathbb{F}_A$.

Cal esmentar una possibilitat degenerada que pot ocórrer quan $\circledast = \mathsf{q}_1 = \mathsf{q}_2$ a Γ_{i+1} (i, posem per cas, $\circledast = \mathsf{q}_1$ a Γ_i). En aquesta situació, el $\circledast$-camí γ_{i+1} pot començar (resp., acabar) amb un arc e incident a q_2: en aquests casos, cal afegir el segment $\mathsf{e}_1^{-1}\mathsf{e}_2$ (resp., $\mathsf{e}_2^{-1}\mathsf{e}_1$) al començament (resp., final) de γ_i per tal que l'elevació realment comenci (resp., acabi) a $\circledast \in \Gamma_i$.

- *Cas 2:* $\Gamma_i \curvearrowright \Gamma_{i+1}$ *és tancat (i. e.,* $\mathsf{q}_1 =_{\Gamma_i} \mathsf{q}_2$*).* La noció de visita crítica al vèrtex $\mathsf{q}_1 = \mathsf{q}_2$ no té sentit ja que ara $\mathsf{q}_1 = \mathsf{q}_2$ també a Γ_i, i l'elevació de γ_{i+1} es pot fer d'una tirada (com si tot γ_{i+1} fos un sol segment entre visites crítiques): només cal considerar el mateix $\circledast$-camí a Γ_i utilitzant només un qualsevol dels arcs plegats. És més, hi ha infinites possibles elevacions de γ_{i+1} (a $\circledast$-camins reduïts de Γ_i llegint $\overline{\ell}(\gamma_{i+1})$): per cada factorització $\gamma_{i+1} = \gamma'\mathsf{r}\gamma''$, i per cada camí reduït γ''' de r a $\mathsf{p} = \iota\mathsf{e}_1 = \iota\mathsf{e}_2$ (resp., a $\mathsf{q} = \tau\mathsf{e}_1 = \tau\mathsf{e}_2$), podem elevar γ_{i+1} com a $\gamma'\mathsf{r}\gamma'''\mathsf{p}(\mathsf{e}_1\mathsf{q}\mathsf{e}_2^{-1})^k\mathsf{p}(\gamma''')^{-1}\mathsf{r}\gamma''$ (resp., $\gamma'\mathsf{r}\gamma'''\mathsf{q}(\mathsf{e}_1^{-1}\mathsf{p}\mathsf{e}_2)^k\mathsf{q}(\gamma''')^{-1}\mathsf{r}\gamma''$), on $k \in \mathbb{Z} \setminus \{0\}$. Es pot veure que aquesta és la família de totes les elevacions possibles de γ_{i+1} a $\circledast$-camins reduïts de Γ_i llegint $\overline{u_{i+1}} \in \mathbb{F}_A$.

Tot aquest procediment demostra el resultat següent.

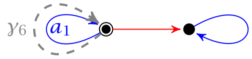
TEOREMA 69. *El problema de la pertinença per a grups lliures,* $\mathsf{MP}(\mathbb{F}_A)$*, és resoluble.* □

Podeu veure il·lustrat aquest mètode gràfic amb la resolució de l'exemple següent. Proposem al lector el seguiment d'aquest mateix mètode per deduir la paraula $v_1v_2^{-1}v_1(v_1v_2^{-1})^7v_3^{-1}v_2^{-1}v_3$, que a l'exemple 26 ens ha permès d'expressar u en termes de v_1, v_2, v_3 (sense explicar-ne l'origen).

EXEMPLE 70. Sigui $\mathbb{F}_2$ el grup lliure sobre $A = \{a, b\}$ i considerem el subgrup $H = \langle v_1, v_2, v_3 \rangle \leqslant \mathbb{F}_2$ generat pels elements $v_1 = a^3$, $v_2 = abab^{-1}$, i $v_3 = a^{-1}bab^{-1}$. Decidiu si l'element $u = a \in \mathbb{F}_2$ pertany a H i, en cas afirmatiu, expresseu-lo en termes de v_1, v_2, v_3.

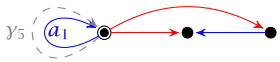
Per començar, construïm l'autòmat $\mathsf{St}(H)$, a partir del conjunt de generadors $\{v_1, v_2, v_3\}$; això està fet a l'exemple 61; vegeu la figura 13. Observeu que el primer pas $\mathcal{F} \curvearrowright \Gamma_1$ són en realitat tres plegaments elementals simultanis (no ens caldrà distinguir-los entre ells). Noteu també que tots els plegaments d'aquesta seqüència són oberts excepte un, $\Gamma_4 \curvearrowright \Gamma_5$, que és tancat perquè identifica dos a-llaços en un de sol. D'aquest procés deduïm que $H = \langle v_1, v_2, v_3 \rangle = \langle a, bab^{-1} \rangle$; o, millor encara, que $\{a, bab^{-1}\}$ és una base de H (corresponent a l'arbre maximal $\circledast \rightarrow \bullet$ de Γ_6).

D'aquí veiem clarament que $a \in H$, ja que és l'etiqueta del $\circledcirc$-camí $\gamma_6 = a_1$ de $\Gamma_6 = \mathsf{St}(H)$, assenyalat al dibuix amb una línia discontínua de color gris:

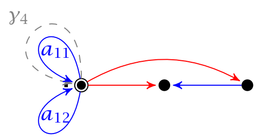


Al a-llaç incident a $\circledcirc$ (*i. e.*, l'únic arc travessat per γ_6) l'hem anomenat a_1; ens referirem als diversos arcs dels autòmats Γ_i de la seqüència de plegaments amb la lletra de les seves respectives etiquetes (a per a les blaves, i b per a les vermelles) i uns certs subíndexs que anirem definint dinàmicament; als arcs no usats no els assignarem cap nom.

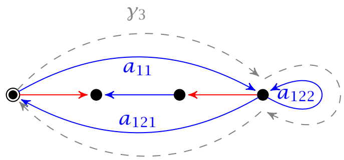
Com a primer pas, elevem el camí γ_6 a través de l'últim plegament $\Gamma_5 \curvearrowright \Gamma_6$: com que γ_6 no visita el vèrtex identificat, s'eleva al $\circledcirc$-camí $\gamma_5 = a_1$ de Γ_5 (on, amb un petit abús de llenguatge, tornem a dir a_1 a l'arc corresponent de Γ_5):



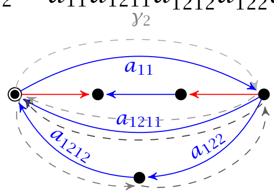
Observeu ara el plegament $\Gamma_4 \curvearrowright \Gamma_5$, que és tancat; per mantenir una notació coherent, anomenem a_{11} i a_{12} els dos a-llaços de Γ_4 que es pleguen en a_1. Per elevar γ_5 a l'autòmat Γ_4, la manera més senzilla és usant un dels dos a-llaços plegats, per exemple, $\gamma_4 = a_{11}$:



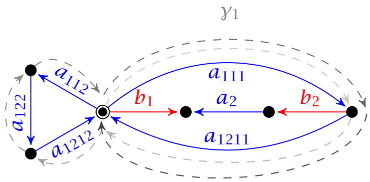
(Hi ha, però, altres maneres de fer-ho, $\gamma_4 = a_{12}$, $\gamma_4 = a_{11}a_{12}a_{11}^{-1}$, $\gamma_4 = a_{11}a_{12}^{-1}a_{11}$, etc). El pas següent és l'elevació a Γ_3: designem per a_{121} i a_{122} els dos a-arcs de Γ_3 que es pleguen sobre a_{12}, i elevem el camí γ_4 a $\gamma_3 = a_{11}a_{122}^{-1}a_{121}$:



Anomenant a_{1211} i a_{1212} els dos arcs de Γ_2 que es pleguen sobre a_{121}, el camí γ_3 s'eleva a Γ_2 com a $\gamma_2 = a_{11}a_{1211}a_{1212}^{-1}a_{122}^{-1}a_{1211}$:

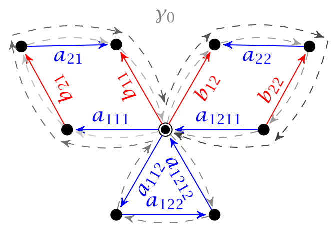


El pas següent és elevar γ_2 a Γ_1 com a $\gamma_1 = a_{111}a_{1211}a_{1212}^{-1}a_{122}^{-1}a_{112}^{-1}a_{111}a_{1211}$:



Finalment, si designem per a_2, b_1, i b_2 els arcs de Γ_1 encara no usats, i mantenim el conveni de notació per als arcs corresponents de $\Gamma_0 = \mathcal{F}$, podem elevar γ_1 a

$$\gamma_0 = a_{111}b_{21}a_{21}b_{11}^{-1}b_{12}a_{22}^{-1}b_{22}^{-1}a_{1211}a_{1212}^{-1}a_{122}^{-1}a_{112}^{-1}a_{111}b_{21}\cdot \\ \cdot\, a_{21}b_{11}^{-1}b_{12}a_{22}^{-1}b_{22}^{-1}a_{1211}.$$



Assenyalant amb parèntesis les visites completes a cada pètal o pètal invers (marcades per les visites de γ_0 a ◉) obtenim l'expressió desitjada de $u = a$ en termes de v_1, v_2, v_3:

$$a = (abab^{-1})(ba^{-1}b^{-1}a)(a^{-1}a^{-1}a^{-1})(abab^{-1})(ba^{-1}b^{-1}a) = \\ = v_2v_3^{-1}v_1^{-1}v_2v_3^{-1}.$$

Com hem comentat més amunt, les elevacions a través de plegaments oberts són úniques, però l'elevació de γ_5 a través del plegament tancat $\Gamma_4 \rightsquigarrow \Gamma_5$ té diverses possibilitats (que acabaran en resultats diferents, *i. e.*, en expressions alternatives de $u = a$ en termes de $v_1^{\pm 1}$, $v_2^{\pm 1}$, $v_3^{\pm 1}$). Convidem el lector a prendre $\gamma_4 = a_{12}$ en lloc de $\gamma_4 = a_{11}$, i a calcular la seva elevació fins a Γ_0 per obtenir la nova expressió $a = (a^{-1}bab^{-1})(ba^{-1}b^{-1}a^{-1})(aaa) = v_3v_2^{-1}v_1$.

El fet de poder obtenir a en termes de $v_1^{\pm 1}$, $v_2^{\pm 1}$, $v_3^{\pm 1}$ de *dues maneres diferents*, $v_2v_3^{-1}v_1^{-1}v_2v_3^{-1} = a = v_3v_2^{-1}v_1$, ens confirma el fet que $\{v_1, v_2, v_3\}$ generen H, però *no són un conjunt lliure* (vegeu la definició 2). Dit d'una altra manera, $v_2v_3^{-1}v_1^{-1}v_2v_3^{-1}v_1^{-1}v_2v_3^{-1} = 1$ és una relació no trivial entre els tres generadors v_1, v_2, v_3 de H.

4.3 Generadors, bases i rang

Comencem recordant que la proposició 54 garanteix la computabilitat d'una base per qualsevol subgrup de $\mathbb{F}_A$ a partir d'un conjunt *finit* de generadors.

Corol·lari 71. *Si S és un conjunt finit d'elements d'un grup lliure $\mathbb{F}_A$, aleshores una base (i, per tant, el rang) de $\langle S\rangle \leqslant \mathbb{F}_A$ és computable. Més concretament,* $\mathrm{rk}(\langle S\rangle) = 1 - \#\mathsf{V}\Gamma + \#\mathsf{E}^{+}\Gamma$*, on* $\Gamma = \mathsf{St}(\langle S\rangle)$.

Molts altres resultats fonamentals sobre bases de (subgrups de) grups lliures es deriven fàcilment de la construcció de Stallings. L'observació següent ens portarà a la important propietat de hopfianitat dels grups lliures.

Sigui Γ un A-autòmat involutiu, finit, i connex, i sigui $\Gamma \overset{\phi}{\rightsquigarrow} \Gamma'$ un plegament elemental. El corresponent morfisme d'autòmats $\phi\colon \Gamma \to \Gamma'$ indueix un morfisme exhaustiu de grups $\phi\colon \pi_{\circledast}(\Gamma) \twoheadrightarrow \pi_{\circledast}(\Gamma')$, $[\gamma] \mapsto [\gamma\phi]$ tal que $\phi\widetilde{\ell}_{\Gamma'} = \widetilde{\ell}_{\Gamma}$. A més, és fàcil veure que, si el plegament és obert, llavors ϕ és bijectiu, mentre que si és tancat (posem per cas, amb $\mathsf{e}_1, \mathsf{e}_2 \in \mathsf{E}\Gamma$ els dos arcs que s'identifiquen a Γ', $\mathsf{p} = \iota\mathsf{e}_1 = \iota\mathsf{e}_2$, $\mathsf{q} = \tau\mathsf{e}_1 = \tau\mathsf{e}_2$, i $\ell(\mathsf{e}_1) = \ell(\mathsf{e}_2) \in A^{\pm}$), llavors $\ker\phi$ està generat, com a subgrup normal de $\pi_{\circledast}(\Gamma)$, per l'element $[\eta\mathsf{p}\mathsf{e}_1\mathsf{q}\mathsf{e}_2^{-1}\mathsf{p}\eta^{-1}]$, on η és un camí qualsevol a Γ de $\circledast$ a p.

L'enunciat següent mostra com la teoria desenvolupada captura geomètricament els dos ingredients (algebraics) de la definició elemental de base (definició 2).

Proposició 72. *Sigui $S \subseteq \mathbb{F}_A$. Aleshores,*

(i) S genera $\mathbb{F}_A$ si i només si $\mathsf{St}(\langle S\rangle) = \mathcal{B}_A$*;*

(ii) S és una família lliure de $\mathbb{F}_A$ si i només si $\mathrm{loss}(\mathsf{Fl}(S)) = 0$*; i, en aquest cas,* $\mathrm{rk}(\langle S\rangle) = \#S$.

Ambdues condicions són algorísmicament decidibles si S és finit.

Prova. L'apartat (i) és clar ja que $\mathsf{St}(\mathbb{F}_A) = \mathcal{B}_A$.

Per veure l'apartat (ii) distingim dos casos. Si S és finit, considerem l'autòmat flor $\mathsf{Fl}(S)$, i una seqüència qualsevol de plegaments elementals fins a obtenir $\mathsf{St}(\langle S\rangle)$,

$$\mathsf{Fl}(S) = \Gamma_0 \overset{\phi_1}{\rightsquigarrow} \Gamma_1 \overset{\phi_2}{\rightsquigarrow} \cdots \overset{\phi_{p-1}}{\rightsquigarrow} \Gamma_{p-1} \overset{\phi_p}{\rightsquigarrow} \Gamma_p = \mathsf{St}(\langle S\rangle).$$

Component els corresponents morfismes obtenim el diagrama commutatiu

$$\begin{tikzcd}
\pi_{\circledast}(\Gamma_0) \arrow[r, two heads, "\phi_1"] \arrow[drr, two heads, "\widetilde{\ell}_0"'] & \pi_{\circledast}(\Gamma_1) \arrow[r, two heads, "\phi_2"] \arrow[dr, two heads, "\widetilde{\ell}_1"] & \cdots \arrow[r, two heads, "\phi_{p-1}"] & \pi_{\circledast}(\Gamma_{p-1}) \arrow[r, two heads, "\phi_p"] \arrow[dl, two heads, "\widetilde{\ell}_{p-1}"'] & \pi_{\circledast}(\Gamma_p) \arrow[dll, two heads, "\widetilde{\ell}_p"] \\
& & \langle S\rangle & &
\end{tikzcd} \tag{19}$$

on $\mathrm{rk}(\pi_{\circledast}(\Gamma_0)) = \#S$, amb (les classes de) els pètals com a base; i on $\widetilde{\ell}_p$ és bijectiu ja que Γ_p és determinista. Si $\mathrm{loss}(\mathsf{Fl}(S)) = 0$, tots els plegaments són oberts, cadascun dels morfismes $\phi_1, \ldots, \phi_p$ és bijectiu i concloem que $\widetilde{\ell}_0 = \phi_1 \cdots \phi_p \widetilde{\ell}_p$ és també bijectiu; per tant, $\langle S\rangle$ està lliurement generat per les etiquetes dels pètals de $\mathsf{Fl}(S)$, és a dir, per S. Recíprocament, si S és una família lliure d'elements de $\mathbb{F}_A$, llavors S és base de $\langle S\rangle \leqslant \mathbb{F}_A$, i el morfisme $\widetilde{\ell}_0$ és bijectiu; la commutativitat del diagrama anterior implica aleshores que $\phi_1, \dots, \phi_p$ són tots bijectius i, per tant, tots els plegaments de la seqüència són oberts; en conseqüència, $\operatorname{loss}(\mathsf{Fl}(S)) = 0$.

Finalment, suposem que S és infinit. Si S no és una família lliure, llavors existeix un subconjunt finit $S_0 \subset S$ que tampoc no és lliure i, aplicant el cas finit, deduïm que $\operatorname{loss}(\mathsf{Fl}(S)) \geq \operatorname{loss}(\mathsf{Fl}(S_0)) \geq 1$. Recíprocament, si S és una família lliure, tota subfamília finita $S_0 \subseteq S$ també és lliure i, aplicant el cas finit, $\operatorname{loss}(\mathsf{Fl}(S_0)) = 0$; per tant, cap seqüència finita de plegaments elementals començant a $\mathsf{Fl}(S)$ (que involucrarà forçosament un nombre finit de pètals) no pot contenir un plegament tancat; és a dir, $\operatorname{loss}(\mathsf{Fl}(S)) = 0$. $\square$

Noteu que d'aquest resultat se'n segueix una prova alternativa per a la proposició 17: si B és una base de $\mathbb{F}_A$, aleshores $\operatorname{loss}(\mathsf{Fl}(B)) = 0$ i $\mathsf{St}(\langle B\rangle, A) = \mathcal{B}_A$; per tant, $\#B = \operatorname{rk}(\mathsf{Fl}(B)) = \operatorname{rk}(\mathsf{St}(\langle B\rangle, A)) = \operatorname{rk}(\mathcal{B}_A) = \#A$. També en podem deduir la important propietat de hopfianitat dels grups lliures finitament generats:

TEOREMA 73. *El grup lliure $\mathbb{F}_n$ és* hopfià*: tot endomorfisme $\varphi\colon \mathbb{F}_n \to \mathbb{F}_n$ exhaustiu és automàticament injectiu. (Equivalentment, $S \subseteq \mathbb{F}_n$ és base de $\mathbb{F}_n$ si i només si $\langle S\rangle = \mathbb{F}_n$ i $\#S = n$.)*

PROVA. De nou, la demostració és immediata de la teoria de Stallings: si $\langle S\rangle = \mathbb{F}_n$ i $\#S = n$, aleshores $\mathsf{St}(\langle S\rangle) = \mathcal{B}_n$, i $\operatorname{rk}(\mathsf{Fl}(S)) = n$. Per tant,

$$\operatorname{loss}(\mathsf{Fl}(S)) = \operatorname{rk}(\mathsf{Fl}(S)) - \operatorname{rk}(\mathsf{St}(\langle S\rangle)) = n - n = 0 \tag{20}$$

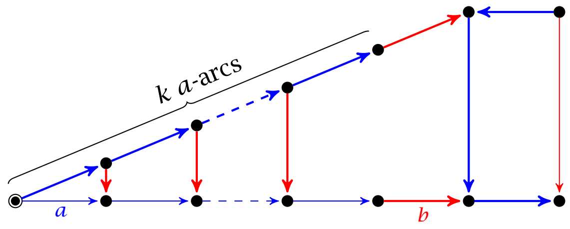
i, per la proposició 72(ii), tenim que S és una família lliure; per tant, S és base de $\mathbb{F}_n$. $\square$

D'acord amb l'observació 6, i tal com succeeix als K-espais vectorials, les bases de grups lliures $\mathbb{F}$ són sempre conjunts minimals de generadors. El recíproc —també cert als K-espais vectorials— és fals als grups lliures, fins a la màxima degeneració possible.

LEMA 74. *Existeixen conjunts de generadors minimals de $\mathbb{F}_n$, $n \geq 1$, de qualsevol cardinalitat finita $m \geq n$.*

PROVA. Aquest comportament ja es pot observar a $\mathbb{Z} = \mathbb{F}_1$ per raons purament aritmètiques: considerem un conjunt de números primers $\{p_1, \dots, p_m\}$ diferents dos a dos, i prenem $S = \{\prod_{i\neq j} p_i : j = 1, \dots, m\}$; clarament $\operatorname{mcd}(S) = 1$ i, per tant, $\langle S\rangle = \mathbb{Z}$. Però $\operatorname{mcd}(S \setminus \{\prod_{i\neq j} p_i\}) = p_j$ i, per tant, $\langle S \setminus \{\prod_{i\neq j} p_i\}\rangle = p_j\mathbb{Z} \neq \mathbb{Z}$.

Usant la teoria de Stallings podem construir exemples més sofisticats. Per exemple, al grup $\mathbb{F}_{\{a,b\}}$ considereu la família d'autòmats involutius Γ_k, $k \geq 2$, representada a continuació:



Prenent com a arbre generador el donat pels arcs representats en traç gruixut obtenim el conjunt de generadors:

$$S_k = \{aba^{-1},\ a^kbab^{-1}a^{-1}b^{-1}a^{k-1},\ a^kba^{-1}ba^{-2}b^{-1}a^{-k}\}\cup \\ \cup \{a^iba^{-1}b^{-1}a^{-(i-1)} : i \in [2, k-1]\}$$

(de cardinal $k+1$) per a $\langle\Gamma_k\rangle$. Observem, però, que Γ_k no és determinista (ho seria sense un dels dos a-arcs sortint de $\odot$) i que, fent-li plegaments de Stallings, col·lapsa fins a la rosa $\mathcal{B}_{\{a,b\}}$. Per tant, $\langle S_k\rangle = \langle\Gamma_k\rangle = \mathbb{F}_{\{a,b\}}$ i, per a tot $k \geq 2$, S_k és una família de $k+1$ generadors de $\mathbb{F}_{\{a,b\}}$. Ara bé, si eliminem un qualsevol dels generadors de S_k (equivalentment, si eliminem de Γ_k l'arc corresponent fora de l'arbre generador), el procés de plegaments queda bloquejat justament a l'arc eliminat i s'obté un A-autòmat determinista diferent de $\mathcal{B}_{\{a,b\}}$. Per tant, S_k és un sistema de generadors *minimal* de $\mathbb{F}_{\{a,b\}}$, de cardinal $k+1$. □

Fixeu-vos, finalment, que la família S_k també serveix com a contraexemple al grup lliure de la propietat fonamental en àlgebra lineal que tota família de generadors conté una base.

4.4 Conjugació i normalitat

Un dels conceptes fonamentals en teoria de grups és el de *conjugació*: si G és un grup, es diu que dos elements $g, g' \in G$ (resp., subgrups $H, H' \leqslant G$) són conjugats, i escrivim $g \sim g'$ (resp., $H \sim H'$) si existeix un element $z \in G$ tal que $z^{-1}gz = g'$ (resp., $z^{-1}Hz = H'$). Aleshores diem que g' (resp., H') és g (resp., H) *conjugat per* z, i escrivim $g' = g^z = z^{-1}gz$ (resp., $H' = H^z = z^{-1}Hz$).

La teoria de Stallings permet caracteritzar la conjugació de subgrups de forma molt transparent.

Lema 75. *Siguin H un subgrup de $\mathbb{F}_A$, i $w \in \mathbb{F}_A$. Aleshores,* $\mathsf{St}(H^w, A)$ *és el cor de l'autòmat* $\mathsf{Sch}_{Hw}(H, A)$ *obtingut canviant el punt base de* $\mathsf{Sch}(H, A)$ *per* Hw.

Prova. És clar de la proposició 47 i la definició 34 que $\mathsf{Sch}_{Hw}(H, A)$ és un A-autòmat involutiu, determinista, saturat i connex que reconeix el subgrup H^w. El resultat se segueix immediatament del corol·lari 52(ii). □

Com a conseqüència del lema anterior obtenim la següent caracterització gràfica de la conjugació de subgrups al grup lliure, que és òbviament decidible en cas que els subgrups siguin finitament generats.

PROPOSICIÓ 76. *Siguin H i K dos subgrups de $\mathbb{F}_A$. Aleshores, H i K són conjugats si i nomes si* $\mathsf{St}^*(H) = \mathsf{St}^*(K)$.

PROVA. Observeu que, per construcció, $\mathsf{St}(H)$ coincideix amb $\mathsf{St}^*(H)$ reintroduint el pèl (eventualment buit) fins a $\odot_H$.

Suposem que $\mathsf{St}^*(H) = \mathsf{St}^*(K)$. Reintroduïm a $\mathsf{St}^*(H) = \mathsf{St}^*(K)$ els dos pèls fins als vèrtexs $\odot_H$ i $\odot_K$ i sigui w l'etiqueta d'un camí reduït qualsevol de $\odot_H$ a $\odot_K$. És fàcil veure que $H^w = K$; per tant, H i K són conjugats.

Recíprocament, suposem que $H^w = K$ per alguna paraula (reduïda) $w \in \mathbb{F}_A$. Sigui γ l'únic camí possible a $\mathsf{St}(H)$ començant a $\odot_H$ i llegint w: la unicitat és clara pel determinisme de $\mathsf{St}(H)$; i si no n'existeix cap, afegim a $\mathsf{St}(H)$ el pèl necessari per a poder completar γ. Declarem $\tau\gamma$ com a nou punt base, i designem per Γ l'autòmat obtingut. Per construcció, $\mathrm{core}^*(\Gamma) = \mathrm{core}^*(\mathsf{St}(H)) = \mathsf{St}^*(H)$ és determinista, i $\langle\Gamma\rangle = w^{-1}\langle\mathsf{St}(H)\rangle w = H^w = K$. Per tant, $\mathrm{core}^*(\Gamma) = \mathrm{core}^*(\mathsf{St}(K)) = \mathsf{St}^*(K)$, d'on deduïm $\mathsf{St}^*(H) = \mathsf{St}^*(K)$. □

Observeu que, en cas que H i K siguin finitament generats i conjugats, la demostració anterior proporciona, a més, un mètode per a calcular efectivament un conjugador w. Això demostra que

COROL·LARI 77. *El problema de la conjugació de subgrups* $\mathsf{SCP}(\mathbb{F})$ *és decidible per a grups lliures: existeix un algoritme que, donats dos subconjunts finits $S_1, S_2 \subseteq \mathbb{F}$, decideix si els corresponents subgrups generats són conjugats i, en cas afirmatiu, retorna un element conjugador.* □

Recordem que un subgrup H d'un grup G es diu *normal* (a G), designat $H \trianglelefteq G$, si i només si $H^g = H$, per a tot $g \in G$. Del lema 75 també se segueix fàcilment una caracterització gràfica de normalitat en el grup lliure (i la seva decidibilitat en el cas finitament generat).

PROPOSICIÓ 78. *Sigui $H \neq 1$ un subgrup de $\mathbb{F}_A$. Aleshores, els enunciats següents són equivalents:*

(a) H és normal a $\mathbb{F}_A$;
(b) $\mathsf{Sch}(H)$ *és vèrtex-transitiu;*[17]
(c) $\mathsf{Sch}(H)$ *és vèrtex-transitiu i cor;*
(d) $\mathsf{St}(H)$ *és vèrtex-transitiu i saturat.*

PROVA. L'equivalència entre (a) i (b) se segueix clarament de les definicions a través del lema 75. Concretament, per a tot $w \in \mathbb{F}_A$:

$$H^w = H \Leftrightarrow \mathsf{Sch}(H^w) = \mathsf{Sch}(H) \Leftrightarrow \mathsf{Sch}_{Hw}(H) = \mathsf{Sch}(H).$$

La interpretació de l'esquerra correspon a la normalitat de H, mentre que la de la dreta correspon a la vèrtex-transitivitat de $\mathsf{Sch}(H)$.

17 Un A-autòmat Γ és *vèrtex-transitiu* si per a qualsevol parell de vèrtexs, p, q de Γ, existeix un automorfisme *de A-digrafs etiquetats* (és a dir, *respectant les etiquetes de les arestes* i *ignorant el punt base*) de Γ que envia p a q. (Informalment, si «Γ té el mateix aspecte vist des de qualsevol vèrtex»).

Per veure l'equivalència entre (b) i (c) és suficient veure que (b) implica (c). En efecte, si $\mathsf{Sch}(H)$ és vèrtex-transitiu, aleshores ha de ser cor ja que, clarament, no existeix cap automorfisme de A-autòmats Γ enviant un vèrtex del cor de Γ (i, per tant, pertanyent a un $\circledast$-camí reduït de Γ) a un vèrtex fora del cor de Γ (i, per tant, no pertanyent a cap $\circledast$-camí reduït de Γ).

Finalment, l'equivalència entre (c) i (d) és conseqüència immediata de la proposició 51(iii). $\square$

OBSERVACIÓ 79. Tot i que per decidir si un subgrup finitament generat $H \leqslant \mathbb{F}_A$ és normal, n'hi ha prou de comprovar si els conjugats dels generadors per les lletres de $A^{\pm}$ tornen a pertànyer a H (un nombre finit d'instàncies del problema de la pertinença), la proposició anterior ens dona una caracterització gràfica molt natural per a la normalitat, que també es pot usar per a donar un algorisme alternatiu per decidir la normalitat de H.

4.5 El problema de l'índex

Recordem que, si H és un subgrup d'un grup G, aleshores G sempre admet una partició $G = \bigsqcup_{i \in I} Hg_i$, on $g_i \in G$. Els conjunts Hg_i s'anomenen *classes laterals (per la dreta)* de H a G; el cardinal del conjunt de classes laterals $H \backslash G = \{Hg_i : i \in I\}$ s'anomena *índex* de H en G, i es designa per $|G : H|$; es diu també que $\{g_i\}_{i \in I}$ és una *família de representants* (o *transversal*) de les classes laterals (per la dreta) de H en G.

En aquesta secció usarem els autòmats de Stallings per a estudiar qüestions relatives a l'índex dels subgrups dels grups lliures, i resoldrem el problema de la finitud de l'índex, que enunciem en general a continuació.

PROBLEMA DE LA FINITUD DE L'ÍNDEX A $G = \langle A \mid R \rangle$, $\mathsf{FIP}(G)$. *Donada una família finita $v_1, \ldots, v_k$ de paraules en els generadors de G, decidir si el subgrup $\langle v_1, \ldots, v_k \rangle \leqslant G$ és d'índex finit a G i, en cas afirmatiu, calcular aquest índex i una família de representants de les corresponents classes laterals.*

Recordem (definició 45) que els vèrtexs de l'autòmat de Schreier $\mathsf{Sch}(H)$ són precisament les classes laterals per la dreta de H a $\mathbb{F}$, és a dir, $|\mathbb{F} : H| = \#\mathsf{VSch}(H)$; i observem que l'apartat (vi) de la proposició 51 pren la forma següent per a subgrups finitament generats.

COROL·LARI 80. *Sigui H un subgrup finitament generat d'un grup lliure $\mathbb{F}$. Aleshores, l'índex $|\mathbb{F} : H|$ és finit si i només si $\mathsf{St}(H)$ és saturat; en aquest cas, $|\mathbb{F} : H| = \#\mathsf{VSt}(H)$.* $\square$

Com a primera conseqüència podem deduir que $\mathbb{F}_n$ té una quantitat finita de subgrups d'un índex finit k donat (vegeu [21] per a una fórmula recurrent que compta aquest nombre de subgrups). D'aquí es dedueix fàcilment el mateix resultat per a qualsevol grup G finitament generat.

COROL·LARI 81. *Sigui G un grup finitament generat. Per a tot $k \geq 1$, G conté una quantitat finita de subgrups d'índex k.*

Exemple 82. A continuació representem els autòmats de Stallings dels 13 subgrups d'índex 3 de $\mathbb{F}_2 = \langle a, b \mid - \rangle$ (amb les corresponents classes de conjugació encerclades en gris). Òbviament, els subgrups normals corresponen a les classes amb un únic representant.

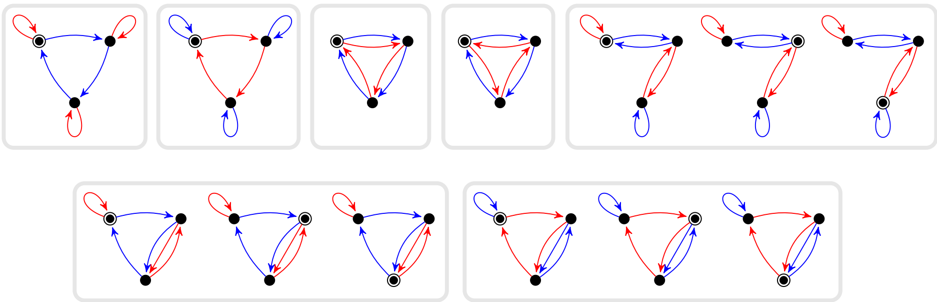


Figura 16: Els 13 subgrups d'índex 3 de $\mathbb{F}_2 = \langle a, b \mid - \rangle$.

Del corol·lari 80 se segueix immediatament el resultat següent.

Teorema 83. *El problema de la finitud de l'índex per a grups lliures,* $\mathsf{FIP}(\mathbb{F})$*, és computable.*

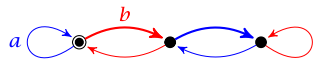
Prova. La decidibilitat de $\mathsf{FIP}(\mathbb{F})$ és conseqüència del corol·lari 80 i de la computabilitat de $\mathsf{St}(H)$ en el cas finitament generat.

Suposem ara que $\mathsf{St}(H)$ és saturat i finit. Per a calcular una família de representants de les classes per la dreta mòdul H, només hem d'observar que, a l'autòmat $\mathsf{St}(H) = \mathrm{core}(\mathsf{Sch}(H)) = \mathsf{Sch}(H)$, qualsevol camí γ amb inici $\odot$ té la forma (13) i, per tant, compleix $\tau\gamma = Hw$, on $w = \ell(\gamma) \in \mathbb{F}_A$. Per tant, podem formar una família de representants de les classes laterals per la dreta mòdul H simplement prenent un camí qualsevol del punt base $\odot$ a cadascun dels vèrtexs de $\mathsf{St}(H)$. Una manera sistemàtica de fer-ho és calcular un arbre generador T de $\mathsf{St}(H)$, i prendre les etiquetes de les T-geodèsiques de $\odot$ a cada vèrtex: $\{\ell(T[\odot, p]) \mid \mathsf{p} \in \mathsf{VSt}(H)\}$ és una família de representants de les classes laterals per la dreta mòdul H, és a dir,

$$H \backslash \mathbb{F}_A = \bigsqcup_{\mathsf{p} \in \mathsf{VSt}(H)} H\ell(T[\odot, p]). \tag{21}$$

Òbviament, l'índex $|\mathbb{F} : H|$ és el cardinal (finit) d'aquest conjunt. Això resol completament el problema de la finitud de l'índex per a grups lliures. (Si volem representants de les classes per l'esquerra, només hem d'invertir les paraules obtingudes, ja que $(Hw)^{-1} = w^{-1}H^{-1} = w^{-1}H$.) $\square$

Exemple 84. Sigui $\mathbb{F}_2$ el grup lliure sobre $A = \{a, b\}$ i considerem el subgrup $H = \langle v_1, v_2, v_3, v_4 \rangle \leqslant \mathbb{F}_2$ generat pels elements $v_1 = a$, $v_2 = b^2$, $v_3 = ba^2b^{-1}$, i $v_4 = baba^{-1}b^{-1}$. Per decidir si H és d'índex finit a $\mathbb{F}_2$ calculem $\mathsf{St}(H)$ a partir de l'autòmat flor $\mathsf{Fl}(\{v_1, v_2, v_3, v_4\})$, tal com hem explicat al teorema 53. El resultat és l'autòmat següent:



Com que els tres vèrtexs de $\mathsf{St}(H)$ tenen un a-arc entrant i un de sortint, i un b-arc entrant i un de sortint, l'autòmat $\mathsf{St}(H)$ és saturat i, per tant, H és d'índex finit a $\mathbb{F}_2$, concretament d'índex $\#\mathsf{VSt}(H) = 3$. Prenent com a arbre generador el donat pels dos arcs dibuixats amb traç gruixut, obtenim $\{1, b, ba\}$ com a conjunt de representants de les classes per la dreta mòdul H, és a dir, $\mathbb{F}_2 = H \sqcup Hb \sqcup H(ba)$.

Com veiem a continuació, la coneguda fórmula de Schreier, que relaciona l'índex d'un subgrup d'índex finit amb el seu rang, també es dedueix de forma transparent de la teoria de Stallings.

Teorema 85 (Fórmula de Schreier). *Sigui $\mathbb{F}_\kappa$ el grup lliure de rang κ, i sigui $H \leqslant \mathbb{F}_\kappa$ un subgrup d'índex finit. Aleshores,* $\operatorname{rk}(H) - 1 = |\mathbb{F}_\kappa : H|(\kappa - 1)$. *En particular, un subgrup d'índex finit és finitament generat si i només si el rang ambient κ és finit.*

Prova. Per la proposició 51(vi), si H és d'índex finit, llavors $\mathsf{St}(H)$ és 2κ-regular i $\#\mathsf{VSt}(H) < \infty$. Per tant, $\operatorname{rk}(\mathsf{St}(H)) < \infty$ (*i. e.*, hi ha un nombre finit d'arcs fora de qualsevol arbre generador) si i només si $\kappa < \infty$. En particular, si $\kappa = \infty$ llavors $\operatorname{rk}(H) = \infty$ i ja hem acabat.

Suposem ara $\kappa < \infty$. Sabem que H és finitament generat i, per tant, $\mathsf{St}(H)$ és finit. Sigui T un arbre generador de $\mathsf{St}(H)$; tal com s'ha demostrat al final de la prova del teorema 53, H té una base de $\#(\mathsf{E}^+\mathsf{St}(H) \setminus \mathsf{E}T)$ elements; per tant,

$$\begin{aligned}\operatorname{rk}(H) - 1 &= \#(\mathsf{E}^+\mathsf{St}(H) \setminus \mathsf{E}T) - 1 = \#\mathsf{E}^+\mathsf{St}(H) - \#\mathsf{E}T - 1 = \\ &= \#\mathsf{E}^+\mathsf{St}(H) - \#\mathsf{V}T = \kappa\#\mathsf{VSt}(H) - \#\mathsf{VSt}(H) = \\ &= |\mathbb{F}_\kappa : H|(\kappa - 1),\end{aligned}$$

on la penúltima igualtat prové de $2\kappa\,\#\mathsf{VSt}(H) = 2\,\#\mathsf{E}^+\mathsf{St}(H)$, obtingut sumant els graus de tots els vèrtexs. □

Combinant les caracteritzacions gràfiques d'índex finit (corol·lari 80) i normalitat (proposició 78), arribem a una mena de recíproc del lema de Schreier per a subgrups normals no trivials del grup lliure.

Corol·lari 86. *Un subgrup normal no trivial H de $\mathbb{F}_n$ és finitament generat si i només si té índex finit.* □

COROL·LARI 87. *Un subgrup normal no trivial H de $\mathbb{F}_{\aleph_0}$ té sempre rang infinit.* □

Acabem aquesta secció amb una demostració gràfica particularment neta d'un resultat clàssic de Marshall Hall, Jr., que mostra especialment bé la potència de l'enfocament geomètric per obtenir resultats algebraics.

Recordem que, donats H i K subgrups d'un grup lliure $\mathbb{F}$, es diu que H és *factor lliure* de K, i ho designem per $H \leqslant_{\mathsf{ff}} K$, si una base (i, per tant, totes les bases) de H es pot ampliar a una base de K. Observeu també que, si Δ és un subautòmat de Γ, aleshores $\langle \Delta \rangle$ és un factor lliure $\langle \Gamma \rangle$ (ampliant un arbre generador de Δ a un arbre generador de Γ).

Un resultat ben sabut d'àlgebra lineal diu que, donat un espai vectorial E i un subespai seu $F \leqslant E$, tota base de F es pot ampliar a una base de E (tècnicament, això correspon al fet que F és un sumand directe de E, noció de la qual els factors lliures són la generalització a ambients no commutatius). El resultat corresponent en un grup lliure és fals: sabem que $\mathbb{F}_n$ té subgrups H de rang superior a n (fins i tot de rang infinit) que, clarament, no en seran factors lliures, $H \not\leqslant_{\mathsf{ff}} \mathbb{F}_n$. El clàssic teorema de Marshall Hall, Jr. ens diu que un resultat d'aquesta naturalesa sí que és cert, si ens restringim a subgrups finitament generats, i canviem $\mathbb{F}_n$ per un subgrup d'índex finit adequat.

TEOREMA 88 (M. HALL, JR. [22]). *Si H és un subgrup finitament generat de $\mathbb{F}_A$, aleshores H és un factor lliure d'un subgrup d'índex finit de $\mathbb{F}_A$; és a dir:*

$$H \leqslant_{\mathsf{fg}} \mathbb{F} \Rightarrow \exists K : H \leqslant_{\mathsf{ff}} K \leqslant_{\mathsf{fi}} \mathbb{F}. \tag{22}$$

PROVA. Si H ja és d'índex finit a $\mathbb{F}_A$, el resultat és obvi. En cas contrari, sabem que $\mathsf{St}(H)$ és un A-autòmat finit i insaturat. Ara és suficient adonar-se del següent fet purament geomètric:[18] en un A-autòmat involutiu i finit, per a tot $a \in A$, $\mathrm{def}_a(\Gamma) = \mathrm{def}_{a^{-1}}(\Gamma)$. Per tant, només caldrà saturar $\mathsf{St}(H)$ aparellant, per cada $a \in A$, els vèrtexs a-deficients amb els (a^{-1})-deficients, i afegint un a-arc dels primers als segons. L'autòmat Γ obtingut és finit i saturat (per tant, reconeix un subgrup d'índex finit) i conté $\mathsf{St}(H)$ com a subautòmat. Per tant, $H = \langle \mathsf{St}(H) \rangle \leqslant_{\mathsf{ff}} \langle \Gamma \rangle$, tal com volíem demostrar. Noteu que l'aparellament de vèrtexs deficients de $\mathsf{St}(H)$ es pot fer, en general, de diverses maneres i, per tant, el subgrup obtingut K no és únic, en general. □

EXEMPLE 89. Sigui $H = \langle a^{-1}b, ab^2, a^{-2}b^4, a^{-2}baba^{-1}b^{-1}a^2 \rangle \leqslant \mathbb{F}_{\{a,b\}}$. Per a obtenir un subgrup d'índex finit de $\mathbb{F}_{\{a,b\}}$ del qual H sigui factor lliure, és suficient calcular $\mathsf{St}(H)$ (en traç continu a la figura 17) i completar-lo a un autòmat saturat (per exemple, tal com s'indica amb traç discontinu). L'autòmat obtingut reconeix un subgrup K d'índex 6 a $\mathbb{F}_{\{a,b\}}$ que conté H com a factor lliure.

18 Es tracta d'una adaptació natural del ben conegut *handshaking lemma*.

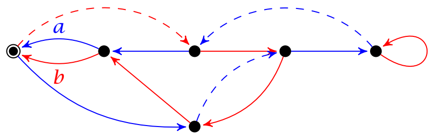


FIGURA 17: Exemple del teorema 88 (Marshall Hall, Jr.).

4.6 El problema de la intersecció

En aquesta darrera secció usarem els autòmats de Stallings per a resoldre el problema proposat a l'exemple 27: el problema de la intersecció de subgrups. Recordem que existeixen grups G que contenen parelles de subgrups $H, K \leqslant G$ finitament generats amb intersecció $H \cap K$ no finitament generada (a [9] i [14] trobareu exemples relativament senzills de grups d'aquest tipus; analitzats, a més, usant generalitzacions de les tècniques gràfiques que expliquem en aquesta secció). A. G. Howson va estudiar aquest fenomen en el grup lliure i el seu nom s'usa per a referir-se als grups que no tenen aquest comportament «estrany»: un grup G es diu que té la *propietat de Howson* (o que és *Howson*) si la intersecció de qualssevol dos subgrups finitament generats $H, K \leqslant G$ és sempre finitament generada (per inducció, el mateix és cert llavors per a interseccions d'una quantitat finita de subgrups). Per a un grup qualsevol $G = \langle A \mid R \rangle$ té sentit, doncs, plantejar-se el problema de decisió següent:

PROBLEMA DE LA INTERSECCIÓ DE SUBGRUPS A $G = \langle A \mid R \rangle$, $\mathsf{SIP}(G)$. *Donades dues famílies finites de paraules en els generadors de G, $u_1, \ldots, u_k; v_1, \ldots, v_l \in (A^{\pm})^*$, decidir si la intersecció dels corresponents subgrups generats $\langle u_1, \ldots, u_k \rangle \cap \langle v_1, \ldots, v_l \rangle$ (a G) és finitament generada i, en cas afirmatiu, calcular-ne un sistema de generadors.*

A l'article [23], Howson va demostrar que els grups lliures satisfan la propietat que porta el seu nom. A continuació, veurem com els autòmats de Stallings aporten una demostració gràfica molt neta i transparent (i, a més, constructiva!) d'aquest fet remarcable: de la mateixa demostració en sortirà una manera efectiva de calcular una base per a la intersecció, i una fita superior per al rang de $H \cap K$ en termes dels rangs de H i de K: la famosa conjectura de Hanna Neumann, resolta recentment, de la qual parlarem al final de la secció.

DEFINICIÓ 90. Siguin $\Gamma_1 = (\mathsf{V}_1, \mathsf{E}_1, \iota_1, \tau_1, \ell_1, \circledast_1)$ i $\Gamma_2 = (\mathsf{V}_2, \mathsf{E}_2, \iota_2, \tau_2, \ell_2, \circledast_2)$ dos A-autòmats. El *producte*[19] de Γ_1 i Γ_2, designat per $\Gamma_1 \times \Gamma_2$, és el A-autòmat amb:

- conjunt de vèrtexs el producte cartesià $\mathsf{V}_1 \times \mathsf{V}_2$;
- un arc $(\mathsf{p}_1, \mathsf{p}_2) \xrightarrow{a} (\mathsf{q}_1, \mathsf{q}_2)$ per a cada parell d'arcs $\mathsf{p}_1 \xrightarrow{a} \mathsf{q}_1$ a Γ_1, i $\mathsf{p}_2 \xrightarrow{a} \mathsf{q}_2$ a Γ_2 amb la mateixa etiqueta $a \in A$;

19 O *pull-back*, en terminologia categòrica.

- les funcions naturals ι, τ, ℓ com a funcions d'incidència i d'etiquetatge;
- vèrtex base $\circledast = (\circledast_1, \circledast_2)$;

vegeu la figura 18.

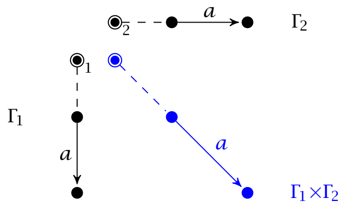


FIGURA 18: Esquema del producte (en blau) de dos A-autòmats (en negre).

Per tant, $\Gamma_1 \times \Gamma_2$ no és res més que el producte tensorial o categòric[20] de Γ_1 i Γ_2, *respectant les etiquetes dels arcs* (*i. e.*, no aparellant mai arcs amb etiquetes diferents). Amb un exemple s'entén clarament el funcionament d'aquesta operació ben natural entre A-autòmats.

EXEMPLE 91. Considerem els subgrups $H=\langle b, a^3, a^{-1}bab^{-1}a\rangle$ i $K=\langle ab, a^3, a^{-1}ba\rangle$ de $\mathbb{F}_{\{a,b\}}$. A la figura 19 podem veure l'autòmat $\mathsf{St}(H)$ dibuixat a la part esquerra (en format vertical), l'autòmat $\mathsf{St}(K)$ dibuixat a la part superior (en format horitzontal), i el producte $\mathsf{St}(H) \times \mathsf{St}(K)$ a la part central (i reorganitzat, a la dreta).

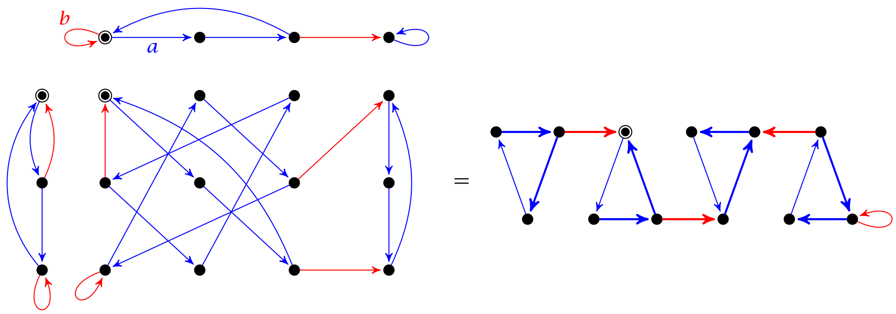


FIGURA 19: Producte dels autòmats $\mathsf{St}(H)$ i $\mathsf{St}(K)$.

La proposició següent recull les propietats principals d'aquest producte d'autòmats, que el relacionen molt de prop amb la intersecció de subgrups.

PROPOSICIÓ 92. *Siguin* $\Gamma_1 = (\mathsf{V}_1, \mathsf{E}_1, \iota_1, \tau_1, \ell_1, \circledast_1)$ *i* $\Gamma_2 = (\mathsf{V}_2, \mathsf{E}_2, \iota_2, \tau_2, \ell_2, \circledast_2)$ *dos* A*-autòmats. Aleshores,*

20 Vegeu `https://en.wikipedia.org/wiki/Graph_product`.

(i) *per a tot* $(\mathsf{p},\mathsf{q}) \in \Gamma_1 \times \Gamma_2$, *tenim* $0 \leqslant \deg(\mathsf{p},\mathsf{q}) \leqslant \min\{\deg(\mathsf{p}),\, \deg(\mathsf{q})\}$;

(ii) *si* Γ_1 *i* Γ_2 *són deterministes, llavors* $\Gamma_1 \times \Gamma_2$ *també és determinista, i, en tal cas,* $\langle \Gamma_1 \times \Gamma_2 \rangle = \langle \Gamma_1 \rangle \cap \langle \Gamma_2 \rangle$;

(iii) *encara que* Γ_1 *i* Γ_2 *siguin connexos,* $\Gamma_1 \times \Gamma_2$ *pot no ser connex;*

(iv) *encara que* Γ_1 *i* Γ_2 *siguin cor,* $\Gamma_1 \times \Gamma_2$ *pot no ser cor.*

PROVA. (i). És clar de la definició 90, ja que tot a-arc sortint de $(\mathsf{p},\mathsf{q}) \in \mathsf{V}(\Gamma_1 \times \Gamma_2)$ correspon a un a-arc sortint tant de $\mathsf{p} \in \mathsf{V}\Gamma_1$ com de $\mathsf{q} \in \mathsf{V}\Gamma_2$.

(ii). Que el producte d'autòmats deterministes és, de nou, determinista és clar de la definició. Suposem que Γ_1 i Γ_2 són deterministes; aleshores, si $w \in \langle \Gamma_1 \times \Gamma_2 \rangle$, hi ha un $\odot$-camí reduït a $\Gamma_1 \times \Gamma_2$ amb etiqueta w; projectant-lo a la primera i a la segona coordenades, obtenim $\odot$-camins reduïts a Γ_1 i a Γ_2, respectivament, llegint igualment w; per tant, $w \in \langle \Gamma_1 \rangle \cap \langle \Gamma_2 \rangle$. I, recíprocament, si $w \in \langle \Gamma_1 \rangle \cap \langle \Gamma_2 \rangle$, aleshores hi ha $\odot$-camins reduïts a Γ_1 i a Γ_2, respectivament, ambdós llegint la paraula w; «cosint-los» arc per arc, obtenim un $\odot$-camí reduït a $\Gamma_1 \times \Gamma_2$ que llegeix w i, per tant, $w \in \langle \Gamma_1 \times \Gamma_2 \rangle$.

(iii) i (iv). Els subgrups $H = \langle a^2, b \rangle$ i $K = \langle b, aba^{-1} \rangle$ de $\mathbb{F}_{\{a,b\}}$ serveixen de contraexemple (deixem al lector el càlcul dels respectius autòmats de Stallings, i del seu producte). □

COROL·LARI 93. *Per* $H, K \leqslant F_A$, *tenim* $\mathsf{St}(H \cap K) = \operatorname{core}(\mathsf{St}(H) \times \mathsf{St}(K))$. □

Combinat amb la proposició 54, això ens demostra la propietat de Howson, la fita de Hanna Neumann, i ens resol el problema de la intersecció per a grups lliures. Definim el *rang reduït* d'un grup lliure $\mathbb{F}_n$ com $\widetilde{\operatorname{rk}}(\mathbb{F}_n) = \max\{0, n-1\}$, és a dir, $\widetilde{\operatorname{rk}}(\mathbb{F}_n) = n-1$ excepte per al grup trivial, per la qual cosa posem $\widetilde{\operatorname{rk}}(1) = 0$ (en lloc de -1).

TEOREMA 94 (HOWSON, [23]; H. NEUMANN, [38]). *Els grups lliures* $\mathbb{F}$ *(de qualsevol rang) són Howson. A més, si* $H, K \leqslant_{\mathsf{fg}} \mathbb{F}$, *aleshores* $\widetilde{\operatorname{rk}}(H \cap K) \leq 2\widetilde{\operatorname{rk}}(H)\widetilde{\operatorname{rk}}(K)$.

PROVA. Observeu que, com que la propietat de Howson només involucra subgrups finitament generats, és suficient demostrar-la quan l'ambient $\mathbb{F}$ és de rang finit, cosa que assumirem durant la demostració. Si $H, K \leqslant \mathbb{F}_n$ són finitament generats, aleshores $\mathsf{St}(H)$ i $\mathsf{St}(K)$ són finits, i per tant, $\mathsf{St}(H) \times \mathsf{St}(K)$ també serà finit, d'on (per la proposició 92(ii)) es dedueix que $H \cap K$ torna a ser finitament generada. En conseqüència, $\mathbb{F}_n$ (i, per tant, tot grup lliure) és Howson.

Per veure la desigualtat, observem primer que, si Γ és un graf connex i finit, i Δ és el graf obtingut després d'eliminar successivament vèrtexs de grau 1 (i les corresponents arestes incidents), aleshores $\operatorname{rk}(\Delta) = \operatorname{rk}(\Gamma)$. D'altra banda, per la proposició 92(i), si $\deg(\mathsf{p}) \geq 2$ i $\deg(\mathsf{q}) \geq 2$, aleshores

$$\deg(\mathsf{p},\mathsf{q}) - 2 \leq (\deg(\mathsf{p}) - 2)(\deg(\mathsf{q}) - 2). \tag{23}$$

És clar que ens podem restringir al cas $H, K, H \cap K \neq \{1\}$. Siguin ara $\Gamma_H = \mathsf{St}(H)$, $\Gamma_K = \mathsf{St}(K)$, Γ la component connexa de $\Gamma_H \times \Gamma_K$ que conté el punt base, i Γ_H^*, Γ_K^* i $\Gamma^* \subseteq \Gamma_H^* \times \Gamma_K^*$ els respectius cors reduïts. Com que Γ^* té tots els vèrtexs (p, q) de grau 2 o superior (i, per tant, p i q també), usant les observacions anteriors, l'equació 6 i les propietats del cor reduït obtenim:

$$\begin{aligned}
\mathrm{rk}(H \cap K) - 1 &= \mathrm{rk}(\Gamma^*) - 1 = \\
&= \tfrac{1}{2} \textstyle\sum_{(\mathsf{p},\mathsf{q}) \in \mathsf{V}\Gamma^*} (\deg(\mathsf{p}, \mathsf{q}) - 2) \leq \\
&\leq \tfrac{1}{2} \textstyle\sum_{(\mathsf{p},\mathsf{q}) \in \mathsf{V}\Gamma^*} (\deg(\mathsf{p}) - 2)(\deg(\mathsf{q}) - 2) \leq \\
&\leq \tfrac{1}{2} \textstyle\sum_{(\mathsf{p},\mathsf{q}) \in \mathsf{V}(\Gamma_H^* \times \Gamma_K^*)} (\deg(\mathsf{p}) - 2)(\deg(\mathsf{q}) - 2) = \\
&= \tfrac{1}{2} (\textstyle\sum_{\mathsf{p} \in \mathsf{V}\Gamma_H^*} (\deg(\mathsf{p}) - 2))(\textstyle\sum_{\mathsf{q} \in \mathsf{V}\Gamma_K^*} (\deg(\mathsf{q}) - 2)) = \\
&= 2(\mathrm{rk}(H) - 1)(\mathrm{rk}(K) - 1). \qquad \square
\end{aligned}$$

Amb una demostració una mica més tècnica es pot veure una desigualtat més forta, que va demostrar Walter Neumann a [39]:

$$\textstyle\sum_{w \in H \backslash \mathbb{F}_A / K} \widetilde{\mathrm{rk}}(H^w \cap K) \leq 2\widetilde{\mathrm{rk}}(H)\widetilde{\mathrm{rk}}(K), \tag{24}$$

on $H^w = w^{-1}Hw$, i el sumatori recorre tots els w d'un transversal qualsevol del conjunt de classes laterals dobles $H \backslash \mathbb{F}_A / K = \{HwK \mid w \in \mathbb{F}_A\}$ (es pot veure que els sumands no nuls es corresponen bijectivament amb les components connexes no arbre i no cícliques del producte $\mathsf{St}(H) \times \mathsf{St}(K)$).

Arribats a aquest punt, és obligat mencionar que Hanna Neumann primer (sobre la desigualtat al teorema 94) i Walter Neumann més tard (sobre la desigualtat (24)) van conjecturar que el factor «2» es pot eliminar de les fites respectives. Aquestes són les famoses «conjectura de Hanna Neumann» i «conjectura forta de Hanna Neumann»,[21] demostrades (independentment i quasi simultània) fa pocs anys per J. Friedman i I. Mineyev; vegeu [18], [36], i les remarcables simplificacions obtingudes per W. Dicks, a [18, apèndix B] i a [17], respectivament.

TEOREMA 95 (J. FRIEDMAN [18] I I. MINEYEV [36]). *Sigui $\mathbb{F}$ un grup lliure i H, K subgrups finitament generats de $\mathbb{F}$. Aleshores,*

$$\textstyle\sum_{w \in H \backslash \mathbb{F}_A / K} \widetilde{\mathrm{rk}}(H^w \cap K) \leq \widetilde{\mathrm{rk}}(H)\widetilde{\mathrm{rk}}(K).$$

Com ja hem justificat, la tècnica del producte d'autòmats també ens permet resoldre el problema de la intersecció.

TEOREMA 96. *El problema de la intersecció de subgrups per a grups lliures, $\mathsf{SIP}(\mathbb{F})$, és resoluble.* $\square$

21 En anglès, *Hanna Neumann conjecture* i *Strenghtened Hanna Neumann conjecture.*

EXEMPLE 97. Com a exemple, acabem el càlcul començat a l'exemple 27. Es tractava de calcular la intersecció de $H = \langle u_1, u_2, u_3\rangle \leqslant$ i $K = \langle v_1, v_2, v_3\rangle$ donats per les paraules $u_1 = b$, $u_2 = a^3$, $u_3 = a^2bab^{-1}a$, $v_1 = ab$, $v_2 = a^3$, i $v_3 = a^{-1}ba$, com a subgrups de $\mathbb{F}_A$, $A = \{a, b\}$. A simple vista ja hem trobat els elements $a^3, b^{-1}a^3b, a^{-1}ba^3b^{-1}a \in H \cap K$; però no quedava gens clar si aquests tres elements generen $H \cap K$, o en falten de més complicats per descobrir.

A l'exemple 91 hem calculat $\mathsf{St}(H)$, $\mathsf{St}(K)$ i $\mathsf{St}(H) \times \mathsf{St}(K)$. Com que aquest últim ja és connex i cor, el corol·lari 93 ens diu que $\mathsf{St}(H \cap K) = \mathsf{St}(H) \times \mathsf{St}(K)$. Prenent com a arbre maximal T l'indicat amb arcs en traç gruixut a la figura 19, obtenim la base

$$S_T = \{b^{-1}a^3b,\ a^3, a^{-1}ba^3b^{-1}a,\ a^{-1}bab^{-1}a^3ba^{-1}b^{-1}a,\\ a^{-1}bab^{-1}aba^{-1}ba^{-1}b^{-1}a\}$$

per a la intersecció $H \cap K$.

A més, com que cadascun dels cinc generadors a S_T és l'etiqueta d'un $\circledcirc$-camí reduït a $\mathsf{St}(H)\times\mathsf{St}(K)$, el podem projectar a la primera i a la segona coordenades, respectivament, i, usant el mètode de la secció 4.2, podem reescriure'l com a paraula en $\{u_1, u_2, u_3\}$ i en $\{v_1, v_2, v_3\}$:

$$\begin{aligned}
H \ni u_1^{-1}u_2u_1 &= b^{-1}a^3b &&= v_1^{-1}v_2v_1 \in K,\\
H \ni u_2 &= a^3 &&= v_2 \in K,\\
H \ni u_3^3 &= a^{-1}ba^3b^{-1}a &&= v_3v_2v_3^{-1} \in K,\\
H \ni u_3u_2u_3^{-1} &= a^{-1}bab^{-1}a^3ba^{-1}b^{-1}a &&= v_3v_1^{-1}v_2v_1v_3^{-1} \in K,\\
H \ni u_3u_1u_3^{-1} &= a^{-1}bab^{-1}aba^{-1}ba^{-1}b^{-1}a &&= v_3v_1^{-1}v_2v_3v_2^{-1}v_1v_3^{-1} \in K.
\end{aligned}$$

OBSERVACIÓ 98. Tal com succeeix amb el problema de la pertinença (vegeu [35]), no és difícil demostrar que el problema de la intersecció és també indecidible per a productes directes de grups lliures (vegeu [14, corol·lari 2.3]), fet que confirma la indocilitat algorísmica d'aquesta família, en cert sentit propera al grup lliure.

Per acabar, vegem que la mateixa idea és útil també per a resoldre el problema de la intersecció de classes laterals en un grup lliure. Recordem que, si G és un grup qualsevol, $u, v \in G$ dos elements, i $H, K \leqslant G$ dos subgrups, llavors les classes laterals Hu i Kv o bé són disjuntes, o bé s'intersequen exactament en una classe lateral de $H \cap K$, *i. e.*, $Hu \cap Kv = (H \cap K)w$.

PROBLEMA DE LA INTERSECCIÓ DE CLASSES LATERALS A $G = \langle A \mid R\rangle$, $\mathsf{CIP}(G)$. *Donades dues famílies finites de paraules $u, u_1, \ldots, u_k; v, u_1, \ldots, u_l \in (A^{\pm})^*$, decidir si la intersecció $\langle u_1, \ldots, u_k\rangle u \cap \langle v_1, \ldots, v_l\rangle v \subseteq G$ és buida, i, en cas negatiu, calcular-ne un representant.*

TEOREMA 99. *El problema de la intersecció de classes laterals per a grups lliures, $\mathsf{CIP}(\mathbb{F})$, és resoluble.*

PROVA. Donades paraules reduïdes $u, u_1, \ldots, u_k; v, v_1, \ldots, v_l \in \mathbb{F}_A$, calculem els autòmats de Stallings de $H = \langle u_1, \ldots, u_k \rangle$ i $K = \langle v_1, \ldots, v_l \rangle$. Ara intentem seguir un camí reduït a $\mathsf{St}(H)$ començant a $\circledast_H$ i llegint $u = a_{i_1} \cdots a_{i_n}$ (on $a_{i_1}, \ldots, a_{i_n} \in A^{\pm}$). Si no és possible, perquè després de llegir a_{i_j} arribem a un vèrtex $(a_{i_{j+1}})$-deficient r, ampliem l'autòmat $\mathsf{St}(H)$ tot afegint el *pèl*

$$\mathsf{r} \xrightarrow{a_{i_{j+1}}} \bullet \xrightarrow{a_{i_{j+2}}} \bullet \xrightarrow{a_{i_{j+3}}} \cdots \xrightarrow{a_{i_n}} \mathsf{p} \tag{25}$$

(per poder completar la lectura de u com a etiqueta d'un camí de $\circledast_H$ a, diguem-ne p) i designem per $\mathsf{St}_u(H)$ l'autòmat resultant. Anàlogament, construïm $\mathsf{St}_v(K)$ (assegurant-nos que conté un camí llegint v, de $\circledast_K$ a, diguem-ne q) i calculem el producte $\Gamma = \mathsf{St}_u(H) \times \mathsf{St}_v(K)$.

Ara, si $(\circledast_H, \circledast_K)$ i (p, q) estan a la mateixa component connexa de Γ, prenem un camí γ de $(\circledast_H, \circledast_K)$ a (p, q), i el projectem a $\mathsf{St}_u(H)$ i a $\mathsf{St}_v(K)$, respectivament. Com que ambdues projeccions tenen etiqueta $w = \overline{\ell}(\gamma)$, i van de $\circledast_H$ a p, i de $\circledast_K$ a q, respectivament, concloem que $Hu = Hw$ i $Kv = Kw$; per tant, $w \in Hu \cap Hv$.

Recíprocament, si $(\circledast_H, \circledast_K)$ a (p, q) són a components connexes diferents, no hi ha cap parella de camins reduïts, de $\circledast_H$ a p (a $\mathsf{St}_u(H)$) i de $\circledast_K$ a q (a $\mathsf{St}_v(K)$), compartint la mateixa etiqueta. Per tant, $Hu \cap Kv \neq \emptyset$ si i només si $(\circledast_H, \circledast_K)$ i (p, q) són a la mateixa component connexa de $\mathsf{St}_u(H) \times \mathsf{St}_v(K)$. Això completa la demostració. □

Per acabar d'il·lustrar la utilitat d'aquesta tècnica del producte de A-autòmats, donem un argument força curt i elegant per demostrar, en l'àmbit dels grups lliures, un resultat sobre subgrups força conegut i vàlid en general (la prova del cas general requereix eines algebraiques més sofisticades, com pot ser el teorema del subgrup de Kurosh).

PROPOSICIÓ 100. *Sigui G un grup i siguin H, K, H', K' subgrups de G. Si $H \leqslant_{ff} K$ i $H' \leqslant_{ff} K'$, llavors $H \cap H' \leqslant_{ff} K \cap K'$.*

PROVA. (Fem la demostració només en el cas que G és un grup lliure, $G = \mathbb{F}$.)

Veurem primer que, si $H \leqslant_{\mathsf{ff}} K \leqslant \mathbb{F}$, i $L \leqslant \mathbb{F}$, llavors $H \cap L \leqslant_{\mathsf{ff}} K \cap L$. Considerem una base A de K que estengui una base de H, i observem que $\mathsf{St}(H, A)$ és simplement una rosa d'uns quants pètals (precisament, els etiquetats pels elements de A pertanyents a H). Considerem $\mathsf{St}(K \cap L, A)$ i calculem $H \cap L = H \cap (K \cap L)$ fent el producte d'aquests dos A-autòmats: clarament, $\mathsf{St}(H, A) \times \mathsf{St}(K \cap L, A)$ és el A-subautòmat de $\mathsf{St}(K \cap L, A)$ determinat pels arcs amb etiqueta a H. Per tant, $H \cap L \leqslant_{\mathsf{ff}} K \cap L$, tal com volíem.

Aplicant aquest fet dues vegades, obtenim $H \cap H' \leqslant_{\mathsf{ff}} K \cap H' \leqslant_{\mathsf{ff}} K \cap K'$ i, per tant, $H \cap H' \leqslant_{\mathsf{ff}} K \cap K'$, tal com volíem demostrar. □

5 Per saber-ne més

La teoria dels autòmats de Stallings és un tema molt conegut i ben representat a la literatura. A més de l'article original de Stallings [50] (d'orientació més aviat topològica), existeixen diverses revisions amb un punt de vista més proper al que s'ha usat en aquest article (vegeu *e. g.* [2, 12, 25]). Els articles que fan servir la teoria de Stallings per a resoldre altres problemes específics són innombrables i continuen apareixent amb regularitat. Podeu trobar-ne alguns exemples a [1, 3, 4, 10, 15, 31, 33, 34, 43, 49, 52].

Arran de l'èxit immens de la teoria de Stallings per al grup lliure, també hi ha hagut múltiples extensions d'aquesta idea a àmbits més generals, per exemple: grafs de grups [19, 20, 26, 44, 46, 47, 51]; monoides i semigrups [16, 30, 31, 53]; grups que satisfan certes propietats de petita cancel·lació[22] [1]; grups totalment residualment lliures [28, 37, 41]; productes lliures[24]; amalgames de grups finits [32]; grups que actuen lliurement a $\mathbb{Z}^n$-arbres [42]; grups virtualment lliures [48]; subgrups quasiconvexos [27]; productes directes i semidirectes de grups lliures amb grups lliure-abelians [8, 11, 13]; complexos cúbics CAT(0) [5]; grups relativament hiperbòlics [29]; i grups de Coxeter d'angle recte[23] [7], entre d'altres.

Agraïments

Els autors agraïm el suport parcial rebut de l'Agencia Estatal de Investigación, a través del projecte de recerca MTM2017-82740-P (AEI/FEDER, UE). El primer autor va realitzar la primera part d'aquest treball a la Universitat del País Basc (UPV/EHU) amb suport parcial del MINECO a través del projecte PID2019-107444GA-I00, i del Govern basc amb el projecte IT974-16.

Agraïm als revisors i editors l'acurada lectura d'aquest text i els pertinents comentaris i suggeriments realitzats.

Referències

[1] Arzhantseva, G. N.; Ol'shanskii, A. Yu. «The class of groups all of whose subgroups with lesser number of generators are free is generic». *Math. Notes*, 59 (4) (1996), 350–355.

[2] Bartholdi, L.; Silva, P. V. «Rational subsets of groups». A: *Handbook of Automata Theory. Vol. II. Automata in Mathematics and Selected Applications*. Berlín: EMS Press, 2021, 841–869.

[3] Bassino, F.; Martino, A.; Nicaud, C.; Ventura, E.; Weil, P. «Statistical properties of subgroups of free groups». *Random Structures Algorithms*, 42 (3) (2013), 349–373.

[4] Bassino, F.; Nicaud, C.; Weil, P. «Random generation of finitely generated subgroups of a free group». *Internat. J. Algebra Comput.*, 18 (2) (2008), 375–405.

22 En anglès, *small cancellation*.
23 En anglès, *right-angled Coxeter groups*.

[5] Beeker, B.; Lazarovich, N. «Stallings' folds for cube complexes». *Israel J. Math.*, 227 (1) (2018), 331–363.

[6] Clay, M.; Margalit, D. (ed.). *Office Hours with a Geometric Group Theorist*. Princeton, Nova Jersey: Princeton University Press, 2017.

[7] Dani, P.; Levcovitz, I. «Subgroups of right-angled Coxeter groups via Stallings-like techniques». *J. Comb. Algebra*, 5 (3) (2021), 237–295.

[8] Delgado, J. «Extensions of free groups: algebraic, geometric, and algorithmic aspects». Tesi doctoral. Universitat Politècnica de Catalunya, 2017.

[9] Delgado, J.; Roy, M.; Ventura, E. «Intersection configurations in free and free times free-abelian groups». Preprint (2022). [Disponible en línia a: `arXiv:2107.12426`]

[10] Delgado, J.; Silva, P. V. «On the lattice of subgroups of a free group: complements and rank». *J. Groups Complex. Cryptol.*, 12 (1) (2020), article núm. 1, 24 p.

[11] Delgado, J.; Ventura, E. «Algorithmic problems for free-abelian times free groups». *J. Algebra*, 391 (2013), 256–283.

[12] Delgado, J.; Ventura, E. «A list of applications of Stallings automata». *Trans. Comb.*, 11 (2022), 181–235.

[13] Delgado, J.; Ventura, E. «Stallings automata for free-times-abelian groups: intersections and index». *Publ. Mat.*, 66 (2) (2022), 789–830. `DOI: 10.5565/PUBLMAT6622209`.

[14] Delgado, J.; Ventura, E.; Zakharov, A. «Intersection problem for Droms RAAGs». *Internat. J. Algebra Comput.*, 28 (7) (2018), 1129–1162.

[15] Delgado, J.; Ventura, E.; Zakharov, A. «Relative order and spectrum in free and related groups». *Commun. Contemp. Math.* (per aparèixer). [Disponible en línia a: `arXiv:2105.03798`]

[16] Delgado, M.; Margolis, S.; Steinberg, B. «Combinatorial group theory, inverse monoids, automata, and global semigroup theory». *Internat. J. Algebra Comput.*, 12 (1-2) (2002), 179–211.

[17] Dicks, W. «Simplified Mineyev's proof of Hanna Neumann conjecture». Preprint (2011).

[18] Friedman, J. «Sheaves on graphs, their homological invariants, and a proof of the Hanna Neumann conjecture: with an appendix by Warren Dicks». *Mem. Amer. Math. Soc.*, 233 (1100) (2015), 106 p.

[19] Guirardel, V. «Approximations of stable actions on $\mathbf{R}$-trees». *Comment. Math. Helv.*, 73 (1) (1998), 89–121.

[20] Guirardel, V. «Reading small actions of a one-ended hyperbolic group on $\mathbf{R}$-trees from its JSJ splitting». *Amer. J. Math.*, 122 (4) (2000), 667–688.

[21] Hall, M., Jr. «Subgroups of finite index in free groups». *Canad. J. Math.*, 1 (1949), 187–190.

[22] Hall, M., Jr. «A topology for free groups and related groups». *Ann. of Math. (2)*, 52 (1950), 127–139.

[23] Howson, A. G. «On the intersection of finitely generated free groups». *J. London Math. Soc.*, 29 (1954), 428–434.

[24] Ivanov, S. V. «On the intersection of finitely generated subgroups in free products of groups». *Internat. J. Algebra Comput.*, 9 (5) (1999), 521–528.

[25] Kapovich, I.; Myasnikov, A. «Stallings foldings and subgroups of free groups». *J. Algebra*, 248 (2) (2002), 608–668.

[26] Kapovich, I.; Weidmann, R.; Miasnikov, A. «Foldings, graphs of groups and the membership problem». *Internat. J. Algebra Comput.*, 15 (1) (2005), 95–128.

[27] Kharlampovich, O.; Miasnikov, A.; Weil, P. «Stallings graphs for quasiconvex subgroups». *J. Algebra*, 488 (2017), 442–483.

[28] Kharlampovich, O. G.; Myasnikov, A. G.; Remeslennikov, V. N.; Serbin, D. E. «Subgroups of fully residually free groups: algorithmic problems». A: *Group Theory, Statistics, and Cryptography*. Providence, RI: Amer. Math. Soc., 2004, 63–101. (Contemp. Math.; 360)

[29] Kharlampovich, O.; Weil, P. «On the generalized membership problem in relatively hyperbolic groups». A: *Fields of Logic and Computation. III*. Cham: Springer, 2020, 147–155. (Lecture Notes in Comput. Sci.; 12180)

[30] Margolis, S. W.; Meakin, J. C. «Free inverse monoids and graph immersions». *Internat. J. Algebra Comput.*, 3 (1) (1993), 79–99.

[31] Margolis, S.; Sapir, M.; Weil, P. «Closed subgroups in pro-**V** topologies and the extension problem for inverse automata». *Internat. J. Algebra Comput.*, 11 (4) (2001), 405–445.

[32] Markus-Epstein, L. «Stallings foldings and subgroups of amalgams of finite groups». *Internat. J. Algebra Comput.*, 17 (8) (2007), 1493–1535.

[33] Martino, A.; Ventura, E. «On automorphism-fixed subgroups of a free group». *J. Algebra*, 230 (2) (2000), 596–607.

[34] Miasnikov, A.; Ventura, E.; Weil, P. «Algebraic extensions in free groups». A: *Geometric Group Theory*. Basel: Birkhäuser, 2007, 225–253. (Trends Math.)

[35] Mihaĭlova, K. A. «The occurrence problem for direct products of groups». *Dokl. Akad. Nauk SSSR*, 119 (1958), 1103–1105. [En rus]

[36] Mineyev, I. «Submultiplicativity and the Hanna Neumann conjecture». *Ann. of Math. (2)*, 175 (1) (2012), 393–414.

[37] Myasnikov, A. G.; Remeslennikov, V. N.; Serbin, D. E. «Fully residually free groups and graphs labeled by infinite words». *Internat. J. Algebra Comput.*, 16 (4) (2006), 689–737.

[38] Neumann, H. «On the intersection of finitely generated free groups». *Publ. Math. Debrecen*, 4 (1956), 186–189.

[39] Neumann, W. D. «On intersections of finitely generated subgroups of free groups». A: *Groups—Canberra 1989*. Berlín: Springer, 1990, 161–170. (Lecture Notes in Math.; 1456)

[40] Nielsen, J. «Om Regning med ikke-kommutative Faktorer og dens Anvendelse i Gruppeteorien». *Mat. Tidsskr. B* (1921), 77–94.

[41] Nikolaev, A. V.; Serbin, D. E. «Finite index subgroups of fully residually free groups». *Internat. J. Algebra Comput.*, 21 (4) (2011), 651–673.

[42] Nikolaev, A.; Serbin, D. «Membership problem in groups acting freely on $\mathbb{Z}^n$-trees». *J. Algebra*, 370 (2012), 410–444.

[43] Puder, D. «Primitive words, free factors and measure preservation». *Israel J. Math.*, 201 (1) (2014), 25–73.

[44] Rips, E.; Sela, Z. «Cyclic splittings of finitely presented groups and the canonical JSJ decomposition». *Ann. of Math. (2)*, 146 (1) (1997), 53–109.

[45] Schreier, O. «Die Untergruppen der freien Gruppen». *Abh. Math. Sem. Univ. Hamburg*, 5 (1) (1927), 161–183. [En alemany]

[46] Sela, Z. «Acylindrical accessibility for groups». *Invent. Math.*, 129 (3) (1997), 527–565.

[47] Sela, Z. «Diophantine geometry over groups. I. Makanin-Razborov diagrams». *Publ. Math. Inst. Hautes Études Sci.*, 93 (2001), 31–105.

[48] Silva, P. V.; Soler-Escrivà, X.; Ventura, E. «Finite automata for Schreier graphs of virtually free groups». *J. Group Theory*, 19 (1) (2016), 25–54.

[49] Silva, P. V.; Weil, P. «On an algorithm to decide whether a free group is a free factor of another». *Theor. Inform. Appl.*, 42 (2) (2008), 395–414.

[50] Stallings, J. R. «Topology of finite graphs». *Invent. Math.*, 71 (3) (1983), 551–565.

[51] Stallings, J. R. «Foldings of G-trees». A: *Arboreal Group Theory*. Nova York: Springer, 1991, 355–368. (Math. Sci. Res. Inst. Publ.; 19)

[52] Stallings, J. R.; Wolf, A. R. «The Todd-Coxeter process, using graphs». A: *Combinatorial Group Theory and Topology*. Princeton, NJ: Princeton Univ. Press, 1987, 157–161. (Ann. of Math. Stud.; 111)

[53] Steinberg, B. «Inverse automata and profinite topologies on a free group». *J. Pure Appl. Algebra*, 167 (2-3) (2002), 341–359.

Departament de Matemàtiques
Universitat Politècnica de Catalunya (UPC)
Escola Politècnica Superior d'Enginyeria de Manresa (EPSEM)
Av. de les Bases de Manresa, 61, 73, 08242 Manresa (Barcelona)
{jorge.delgado,enric.ventura}@upc.edu