Graphes à grand tour de taille

Le tour de taille d'un graphe est la longueur du plus petit circuit. Si le graphe modélise un réseau de transmission de l'information, il est intéressant d'avoir le tour de taille le plus grand possible, afin d'éliminer les redondances. Pour un graphe régulier, un argument de comptage élémentaire montre que le tour de taille est au plus logarithmique en le nombre de sommets. Mais il existe des familles de graphes réguliers où le tour de taille croît vraiment comme le logarithme du nombre de sommets. Le but de l'article est de donner la construction de celle de ces familles qui réalise le taux de croissance du tour de taille le plus rapide, parmi tous les taux de croissance connus.

Dans cet article, il sera question de graphes finis, simples (c'est-à-dire sans boucle ni arête multiple), connexes, et k-réguliers (c'est-à-dire, tout sommet à exactement k voisins). Un exemple célèbre est donné à la figure 1 : c'est le graphe de Petersen, qui est 3-régulier.

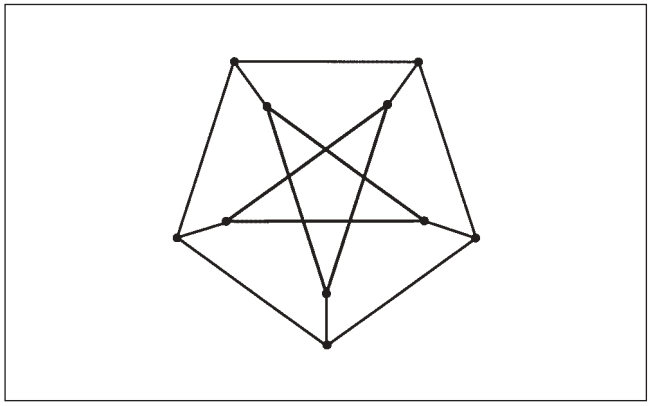

Figure 1

Le *tour de taille* d'un graphe X est la longueur du plus petit circuit de X (on dit aussi *maille*, ou *systole*[1]) : on le note $g(X)$.

Pour un graphe X k-régulier, connexe, fini, il existe une relation simple entre le tour de taille $g = g(X)$ et le nombre de sommets $|X|$. Notons $r = \left[\frac{g-1}{2}\right]$ le plus grand entier strictement inférieur à $\frac{g}{2}$. Fixons un sommet $x_0 \in X$, et considérons la boule fermée $B_{\leqslant r}(x_0)$ de centre x_0 et de rayon r. Comme $r < g/2$, cette boule ne peut pas contenir de circuit ; en d'autres termes, le graphe induit par X sur $B_{\leqslant r}(x_0)$, est un arbre (figure 2).

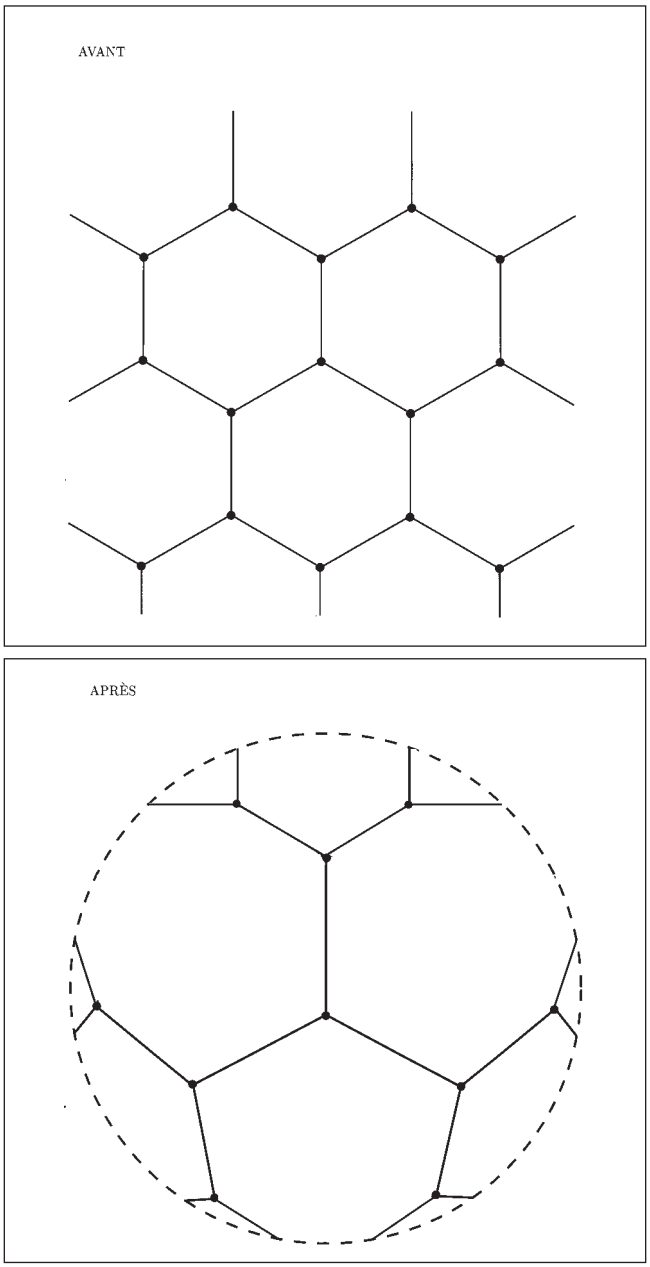

Figure 2

[1] En anglais : « girth » ; en allemand : « taillenweite ».

– Alain Valette, Institut de mathématiques, rue Émile Argand 11, CH-2007 Neuchâtel – Suisse.
alain.valette@unine.ch

Le nombre de sommets de la boule $B_{\leqslant r}(x_0)$ est facile à estimer : on additionne le nombre de sommets à distance 0 de x_0, le nombre de sommets à distance 1, le nombre de sommets à distance 2, etc. Comme le graphe X est k-régulier, cela donne :

$$|B_{\leqslant r}(x_0)| = 1 + k + k(k-1) + k(k-1)^2 + \cdots + k(k-1)^{r-1} = \frac{k(k-1)^r - 2}{k-2}.$$

Ecrivons maintenant l'inégalité [2] triviale $|B_{\leqslant r}(x_0)| \leqslant |X|$. En passant au logarithme en base $k-1$, on obtient la relation recherchée :

$$\left[\frac{g(X)-1}{2}\right] \leqslant \log_{k-1}|X| + \log_{k-1}\left[\frac{k-2+\frac{2}{|X|}}{k}\right].$$

Cette relation prend une forme particulièrement simple si, au lieu de considérer un graphe X, on considère une famille $(X_n)_{n\geqslant 1}$ de graphes k-réguliers, connexes, finis, avec $|X_n| \to +\infty$ pour $n \to \infty$:

$$g(X_n) \leqslant (2 + o(1)) \log_{k-1}|X_n| \qquad (1)$$

(ici $o(1)$ est une quantité qui tend vers 0 pour $n \to \infty$).

L'intérêt de considérer des familles de graphes vient de la théorie des circuits de communication : un graphe modélise un réseau de communication, les sommets représentant les utilisateurs (émetteurs/récepteurs d'informations), les arêtes représentant les canaux le long desquels l'information se propage. La condition $\lim_{n\to\infty} |X_n| = +\infty$ correspond au désir d'avoir des modèles de réseaux arbitrairement grands. L'exigence de k-régularité est de nature économique : en effet, le meilleur réseau de communication sur m sommets est donné par le graphe complet, où tout sommet est connecté à tout autre ; mais le nombre d'arêtes est $\frac{m(m-1)}{2}$, il est quadratique en m. En revanche, pour notre famille $(X_n)_{n\geqslant 1}$ de graphes k-réguliers, le nombre d'arêtes de X_n est $\frac{k|X_n|}{2}$; ce nombre croît donc linéairement avec $|X_n|$. Dans ce contexte, il est intéressant d'avoir le tour de taille le plus grand possible : le fait que les circuits soient longs veut dire qu'il y aura peu de retours de l'information, c'est-à-dire peu de redondances.

[2] Pour le graphe de Petersen, on a l'égalité $B_{\leqslant r}(x_0) = X$, mais c'est exceptionnel !

Définition. *Soit $(X_n)_{n\geqslant 1}$ une famille de graphes k-réguliers connexes, finis, avec $\lim_{n\to\infty} |X_n| = +\infty$. Nous dirons que $(X_n)_{n\geqslant 1}$ est une* famille à grand tour de taille *s'il existe $C > 0$ tel que*

$$g(X_n) \geqslant (C + o(1)) \log_{k-1}|X_n| \quad \textit{pour tout} \quad n \geqslant 1.$$

Par l'inégalité (1), on a nécessairement $C \leqslant 2$. Une famille est à grand tour de taille si le tour de taille est de l'ordre du logarithme du nombre de sommets. Il n'est pas du tout évident que de telles familles existent. En effet, vu l'erreur commise dans la comparaison entre $B_{\leqslant r}(x_0)$ et X, on pourrait penser que $|X|$ est en général bien plus grand que $|B_{\leqslant r}(x_0)|$. Il est donc assez surprenant que de telles familles de graphes existent bel et bien : cela a été démontré en 1962 par Erdös et Sachs : grâce à des méthodes non constructives, ils démontrent l'existence de familles $(X_n)_{n\geqslant 1}$ avec $g(X_n) \geqslant \log_{k-1}|X_n|$ (c'est-à-dire $C = 1$). Une jolie construction élémentaire, complètement explicite, a ensuite été donnée par Margulis en 1982 ; malheureusement, elle ne donne que $C = \frac{2\log 3}{3\log(1+\sqrt{2})} \simeq 0,831$. Notre but dans cet article est de présenter une preuve élémentaire[3] du résultat suivant, obtenu indépendemment en 1988 par Lubotzky, Phillips, Sarnak d'une part, et Margulis d'autre part.

Théorème 1. *Soient p, q des nombres premiers impairs distincts, avec $p \equiv 1$ (mod. 4) et $\left(\frac{p}{q}\right) = -1$ (c'est-à-dire que p n'est pas un carré* modulo q*). Il existe une famille $(X^{p,q})$, construite explicitement, de graphes $(p+1)$-réguliers sur $q(q^2-1)$ sommets, avec $g(X^{p,q}) \geqslant \left(\frac{4}{3} + o(1)\right) \log_p |X^{p,q}|$.*

Les graphes $X^{p,q}$ seront des graphes de Cayley du groupe fini $\mathrm{PGL}_2(q)$, d'ordre $\frac{q(q-1)}{2}$, par rapport à une partie génératrice à $p+1$ éléments construite à partir du théorème des quatre carrés de Jacobi.

A notre connaissance, la constante $C = \frac{4}{3}$ du théorème 1 détient le record du monde. La preuve ci-dessous est tirée d'un travail en commun avec Davidoff et Sarnak.

[3] La preuve originale utilisait les groupes algébriques sur les adèles, en particulier le théorème d'approximation forte de Kneser.

RAPPELS

Graphes de Cayley

Les graphes que nous construirons seront des graphes de Cayley. Rappelons rapidement cette notion.

Soit Γ un groupe (fini ou infini) et S une partie *finie* de Γ. Nous supposons que S ne contient pas le neutre 1 de Γ et que S est symétrique, c'est-à-dire stable par le passage à l'inverse. Le *graphe de Cayley* $\mathcal{G}(\Gamma, S)$ est le graphe dont l'ensemble des sommets est Γ et dont l'ensemble des arêtes est formé des paires $\{x, y\}$ pour lesquelles il existe $s \in S$ tel que $y = xs$. Notons que cette relation d'adjacence est symétrique (car $S = S^{-1}$) et que le graphe $\mathcal{G}(\Gamma, S)$ est simple (car $1 \notin S$).

La figure 3 donne différents exemples de graphes de Cayley du groupe additif $\Gamma = \mathbb{Z}/6\mathbb{Z}$ (groupe cyclique d'ordre 6).

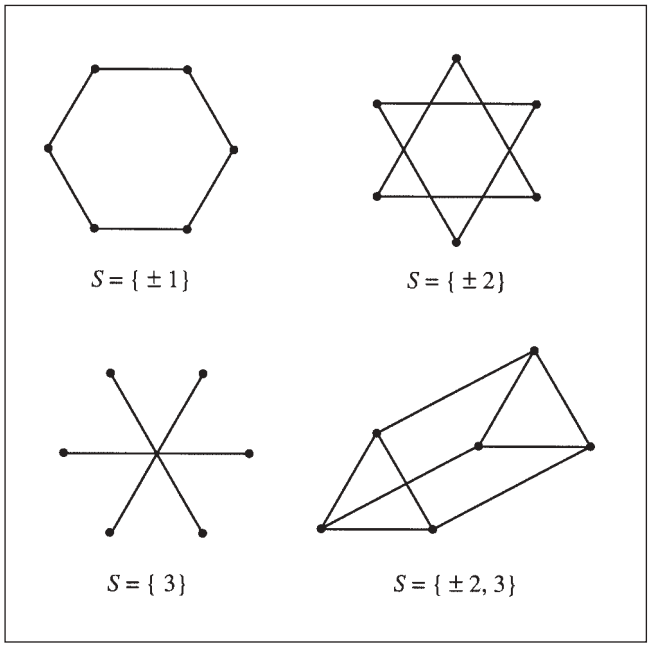

Figure 3

Les propriétés principales d'un graphe de Cayley sont les suivantes :

- $\mathcal{G}(\Gamma, S)$ est k-régulier, avec $k = |S|$;
- Γ agit par automorphismes sur $\mathcal{G}(\Gamma, S)$, transitivement sur les sommets (grâce aux multiplications gauches de Γ) ;
- $\mathcal{G}(\Gamma, S)$ est connexe si et seulement si S engendre Γ (en effet : $\mathcal{G}(\Gamma, S)$ est connexe si et seulement si tout sommet peut être relié au sommet $1 \in \Gamma$, si et seulement si tout élément de Γ s'écrit comme un produit d'éléments de S).

Sommes de 4 carrés

Partons du théorème des 4 carrés de Jacobi (voir Weil et Davidoff, Sarnak et Valette pour les preuves élémentaires) : si p est premier, il y a $8(p+1)$ manières d'écrire p comme somme de 4 carrés d'entiers :

$$|\{(x_0, x_1, x_2, x_3) \in \mathbb{Z}^4 : x_0^2 + x_1^2 + x_2^2 + x_3^2 = p\}| = 8(p+1).$$

Supposons dorénavant $p \equiv 1 \pmod 4$. En réduisant $x_0^2 + x_1^2 + x_2^2 + x_3^2 = p$ *modulo* 4, et en se rappelant que les carrés *modulo* 4 sont 0 et 1, on voit qu'exactement un des x_i est impair et les autres pairs. Ainsi

$$|\{(x_0, x_1, x_2, x_3) \in \mathbb{Z}^4 : x_0^2 + x_1^2 + x_2^2 + x_3^2 = p\,,\ x_0 \text{ impair},\ x_0 > 0\}| = p + 1\,. \quad (2)$$

Quaternions

Si R est un anneau commutatif à unité, nous noterons $\mathbb{H}(R)$ l'anneau des *quaternions de Hamilton* à coefficients dans R

$$\mathbb{H}(R) = \{a_0 + a_1 i + a_2 j + a_3 k : a_0, a_1, a_2, a_3 \in R\}$$

où les symboles i, j, k sont soumis aux relations usuelles :

$$i^2 = j^2 = k^2 = -1\,,\ ij = -ji = k,$$
$$jk = -kj = i\,,\ ki = -ik = j.$$

Si $\alpha = a_0 + a_1 i + a_2 j + a_3 k$ est un quaternion, nous définissons le *quaternion conjugué* $\overline{\alpha} = a_0 - a_1 i - a_2 j - a_3 k$, ainsi que la *norme* :

$$N(\alpha) = \overline{\alpha}\,\alpha = \alpha\,\overline{\alpha} = a_0^2 + a_1^2 + a_2^2 + a_3^2.$$

Notons $\mathbb{F}_q$ le corps fini à q éléments (q impair). Rappelons que, dans $\mathbb{F}_q$, l'équation $1 + x^2 + y^2 = 0$ possède toujours au moins une solution (pour le voir, posons $A_+ = \{1 + x^2 : x \in \mathbb{F}_q\}$, $A_- = \{-y^2 : y \in \mathbb{F}_q\}$: ces deux sous-ensembles de $\mathbb{F}_q$ ont tous deux $\dfrac{q+1}{2}$ éléments, soit plus de la moitié des éléments de $\mathbb{F}_q$, donc leur intersection est non vide : il existe donc $x, y \in \mathbb{F}_q$ tels que $1 + x^2 = -y^2$).

L'anneau de quaternions $\mathbb{H}(\mathbb{F}_q)$ est isomorphe à l'anneau $M_2(\mathbb{F}_q)$ des matrices 2×2 à coefficients dans $\mathbb{F}_q$. Cet isomorphisme n'est pas canonique, mais dépend du choix des deux éléments x, y tels que $1 + x^2 + y^2 = 0$ dans $\mathbb{F}_q$. Choisissons ces éléments une fois pour toutes, et posons

$$\psi_q : \mathbb{H}(\mathbb{F}_q) \to M_2(\mathbb{F}_q) :$$
$$a_0 + a_1 i + a_2 j + a_3 k$$
$$\mapsto \begin{pmatrix} a_0 + a_1 x + a_3 y & -a_1 y + a_2 + a_3 x \\ -a_1 y - a_2 + a_3 x & a_0 - a_1 x - a_3 y \end{pmatrix}.$$

On vérifie que ψ_q est un isomorphisme d'anneaux, tel que

$$\det \psi_q(\alpha) = N(\alpha) \qquad (\alpha \in \mathbb{H}(\mathbb{F}_q)) \tag{3}$$

De plus $\psi_q(\alpha\,\overline{\alpha}) = \psi_q(\overline{\alpha}\,\alpha)$ est une matrice scalaire.

Groupes finis

Notons $\mathrm{GL}_2(q)$ le groupe des matrices 2×2, inversibles, à coefficients dans $\mathbb{F}_q$. L'ordre de $\mathrm{GL}_2(q)$ est

$$|\mathrm{GL}_2(q)| = q(q-1)(q^2-1)$$

(en effet, on peut choisir de q^2-1 façons la première colonne d'une matrice inversible et de $q^2 - q = q(q-1)$ façons sa deuxième colonne, linéairement indépendante de la première).

Notons $\mathrm{SL}_2(q)$ le sous-groupe des matrices de déterminant 1. On a donc $\mathrm{SL}_2(q) = \mathrm{Ker}\,[\det : \mathrm{GL}_2(q) \to \mathbb{F}_q^\times]$ et par conséquent

$$|\mathrm{SL}_2(q)| = q(q^2-1)\,.$$

Notons enfin $\mathrm{PGL}_2(q)$ le quotient de $\mathrm{GL}_2(q)$ par son centre, formé des matrices scalaires. On a donc

$$|\mathrm{PGL}_2(q)| = q(q^2-1).$$

Notons $\varphi_q : \mathrm{GL}_2(q) \to \mathrm{PGL}_2(q)$ l'application-quotient, et posons $\mathrm{PSL}_2(q) = \varphi_q(\mathrm{SL}_2(q))$. On a donc

$$|\mathrm{PSL}_2(q)| = \begin{cases} q(q^2-1) & \text{si } q \text{ est pair} \\ \dfrac{q(q^2-1)}{2} & \text{si } q \text{ est impair} \end{cases}$$

Remarquons que, pour $A \in \mathrm{GL}_2(q)$, on a $\varphi_q(A) \in \mathrm{PSL}_2(q)$ si et seulement si $\det A$ est un carré dans $\mathbb{F}_q$.

LES GRAPHES $X^{p,q}$

Comme en (2), considérons les $p+1$ solutions de

$$x_0^2 + x_1^2 + x_2^2 + x_3^2 = p\,, \quad x_0 \text{ impair},\ x_0 > 0\,.$$

A chacune de ces solutions, associons le quaternion entier

$$x_0 + x_1 i + x_2 j + x_3 k\,.$$

Cela fournit un ensemble S_p de $p+1$ quaternions dans $\mathbb{H}(\mathbb{Z})$. Considérons la réduction *modulo* q

$$\tau_q : \mathbb{H}(\mathbb{Z}) \to \mathbb{H}(\mathbb{F}_q)$$

composée avec l'isomorphisme

$$\psi_q : \mathbb{H}(\mathbb{F}_q) \to M_2(\mathbb{F}_q).$$

On a, pour $\alpha \in S_p$:

$$\det(\psi_q(\tau_q(\alpha))) \equiv N(\alpha) = p \pmod{q}\,,$$

donc $\psi_q(\tau_q(S_p))$ est contenu dans le groupe $\mathrm{GL}_2(q)$ des matrices inversibles de $M_2(\mathbb{F}_q)$. Notons que S_p est stable par le passage au conjugué $\alpha \mapsto \overline{\alpha}$. Comme $\psi_q(\tau_q(\overline{\alpha}\,\alpha))$ est une matrice scalaire, cela suggère de passer au quotient par les matrices scalaires, donc de travailler dans le quotient $\mathrm{PGL}_2(q)$.

On a alors, pour $\alpha \in S_p$:

$$\varphi_q \circ \psi_q \circ \tau_q\,(\alpha\,\overline{\alpha}) = 1$$

ce qui montre que $S_{p,q} = (\varphi_q \circ \psi_q \circ \tau_q)(S_p)$ est une partie symétrique de $\mathrm{PGL}_2(q)$. Il est facile de voir que, si q est assez grand par rapport à p (c'est-à-dire $q > 2\sqrt{p}$), alors $(\varphi_q \circ \psi_q \circ \tau_q)\,|_{S_p}$ est injective et $1 \notin S_{p,q}$.

Si $\left(\dfrac{p}{q}\right) = 1$ (c'est-à-dire si p est un carré *modulo* q), alors $S_{p,q} \subseteq \mathrm{PSL}_2(q)$. Nous posons $X^{p,q} = \mathcal{G}(\mathrm{PSL}_2(q), S_{p,q})$: c'est un graphe $(p+1)$-régulier, à $\dfrac{q(q^2-1)}{2}$ sommets.

Si $\left(\dfrac{p}{q}\right) = -1$ (c'est-à-dire si p n'est pas un carré *modulo* q), alors $S_{p,q} \subseteq \mathrm{PGL}_2(q) \backslash \mathrm{PSL}_2(q)$, et nous posons $X^{p,q} = \mathcal{G}(\mathrm{PGL}_2(q), S_{p,q})$: c'est un graphe $(p+1)$-régulier à $q(q^2-1)$ sommets.

Nous devons maintenant montrer que $X^{p,q}$ est connexe, c'est-à-dire montrer que $S_{p,q}$ engendre

$$\begin{cases} \mathrm{PSL}_2(q) & \text{si} \quad \left(\dfrac{p}{q}\right) = 1 \\ \mathrm{PGL}_2(q) & \text{si} \quad \left(\dfrac{p}{q}\right) = -1 \end{cases}$$

Après cela, il nous restera à estimer le tour de taille de $X^{p,q}$. Pour traiter ces deux problèmes, nous allons construire une famille de graphes $Y^{p,q}$, connexes par construction, et les comparer aux $X^{p,q}$.

LES GRAPHES $Y^{p,q}$

Soit $\Lambda'(2)$ le sous-ensemble suivant de $\mathbb{H}(\mathbb{Z})$:

$$\Lambda'(2) = \{\alpha = a_0 + a_1\, i + a_2\, j + a_3\, k \in \mathbb{H}(\mathbb{Z}) : N(\alpha) = p^r\ (r \in \mathbb{N})\,,\ \alpha \text{ impair}\}.$$

Remarquons que $\Lambda'(2)$ est un monoïde multiplicatif contenant S_p. En particulier $\Lambda'(2)$ contient les mots sur l'alphabet S_p. Nous dirons qu'un tel mot est réduit s'il ne contient aucun sous-mot de la forme $\alpha\,\overline{\alpha}$ ou $\overline{\alpha}\,\alpha$ ($\alpha \in S_p$).

Théorème 2 (Dickson 1922). *Écrivons* $S_p = \{\alpha_1, \ldots, \alpha_{\frac{p+1}{2}}, \overline{\alpha_1}, \ldots, \overline{\alpha_{\frac{p+1}{2}}}\}$. *Tout élément* $\alpha \in \Lambda'(2)$, *avec* $N(\alpha) = p^r$, *s'écrit de façon unique* $\alpha = \pm\, p^\ell\, w_m$, *où* w_m *est un mot réduit sur* S_p *et* $2\ell + m = r$.

Pour une preuve de ce résultat, voir Dickson (1922) et Davidoff, Sarnak et Valette.

Le théorème de Dickson voit pointer un groupe libre, plus exactement le groupe libre sur les $\dfrac{p+1}{2}$ générateurs $\alpha_1, \ldots, \alpha_{\frac{p+1}{2}}$. Pour faire apparaître celui-ci explicitement, passons au quotient $\Lambda'(2)$ par une relation d'équivalence : pour $\alpha, \beta \in \Lambda'(2)$: $\alpha \sim \beta$ s'il existe des naturels m, k tels que $p^m\, \alpha = \pm\, p^\ell\, \beta$. Notons $[\alpha]$ la classe de α. Le théorème de Dickson se reformule en disant que $\Lambda(2) = \Lambda'(2)/\sim$ est le groupe libre $\mathbb{L}_{\frac{p+1}{2}}$ sur les générateurs $[\alpha_1], \ldots, [\alpha_{\frac{p+1}{2}}]$.

La réduction τ_q *modulo* q envoie $\Lambda'(2)$ dans le groupe multiplicatif $\mathbb{H}(\mathbb{F}_q)^\times$ de $\mathbb{H}(\mathbb{F}_q)$. Notons $Z(\mathbb{H}(\mathbb{F}_q)^\times)$ le centre de $\mathbb{H}(\mathbb{F}_q)^\times$. L'homomorphisme de monoïdes $\tau_q : \Lambda'(2) \to \mathbb{H}(\mathbb{F}_q)^\times$ induit par passage au quotient un homomorphisme de groupes

$$\Pi_q : \Lambda(2) \to \mathbb{H}(\mathbb{F}_q)^\times / Z(\mathbb{H}(\mathbb{F}_q))^\times\,.$$

A nouveau $\Pi_q\,|_{S_p}$ est injectif si q est assez grand par rapport à p ($q > 2\sqrt{p}$ marche) et nous définissons $Y^{p,q}$ comme le graphe de Cayley de l'image de Π_q par rapport à S_p :

$$Y^{p,q} = \mathcal{G}(\operatorname{Im}\Pi_q, S_p)\,.$$

Par construction, $Y^{p,q}$ est un graphe $(p+1)$-régulier connexe. Comparons la construction de $X^{p,q}$ et celle de $Y^{p,q}$ au moyen d'un diagramme commutatif. Pour cela, remarquons que l'isomorphisme $\psi_q : \mathbb{H}(\mathbb{F}_q)^\times \to \mathrm{GL}_2(q)$ envoie $Z(\mathbb{H}(\mathbb{F}_q)^\times)$ sur les matrices scalaires et induit donc un isomorphisme

$$\Psi_q : \mathbb{H}(\mathbb{F}_q)^\times / Z(\mathbb{H}(\mathbb{F}_q)^\times) \to \mathrm{PGL}_2(q)\,.$$

On a alors le diagramme commutatif :

$$\begin{array}{ccccc} \Lambda'(2) \supset S_p & \xrightarrow{\tau_q} & \mathbb{H}(\mathbb{F}_q)^\times & \xrightarrow{\psi_q} & \mathrm{GL}_2(q) \\ \downarrow & & \downarrow & & \downarrow \varphi_q \\ \Lambda(2) & \xrightarrow{\Pi_q} & \mathbb{H}(\mathbb{F}_q)^\times / Z(\mathbb{H}(\mathbb{F}_q)^\times) & \xrightarrow{\Psi_q} & \mathrm{PGL}_2(q) \supseteq Q_{p,q}. \end{array}$$

Ce diagramme montre déjà que $Y^{p,q}$ est une composante connexe de $X^{p,q}$. L'inconvénient de $Y^{p,q}$ est que nous ne connaissons pas *a priori* son nombre de sommets (contrairement à $X^{p,q}$). Mais il a l'avantage d'être donné comme quotient d'un arbre (l'arbre du groupe libre $\Lambda(2) \simeq \mathbb{L}_{\frac{p+1}{2}}$) d'avoir ainsi un tour de taille facile à estimer.

Notons $\Lambda(2q)$ le noyau de l'homomorphisme Π_q. On peut penser à $\Lambda(2q)$ comme à un sous-groupe de congruence dans $\Lambda(2)$. Il est facile de vérifier que

$$\Lambda(2q) = \{[\alpha] \in \Lambda(2) : \alpha = a_0 + a_1\, i + a_2\, j + a_3\, k,\ q \text{ divise } a_1, a_2, a_3\}. \tag{4}$$

Proposition 1. $g(Y^{p,q}) \geqslant 2\log_p q$; *de plus, si* $\left(\dfrac{p}{q}\right) = -1$, *alors* $g(Y^{p,q}) \geqslant 4\log_p q - \log_p 4$.

Preuve. Notons g pour $g(Y^{p,q})$. Soient $x_0, x_1, \ldots, x_g = x_0$ les sommets d'un circuit de longueur g dans $Y^{p,q}$. Comme $Y^{p,q}$ est un graphe de Cayley, nous pouvons (quitte à translater dans $\operatorname{Im}\Pi_q$) supposer que $x_0 = 1$. En relevant ce chemin en un chemin issu de l'origine dans l'arbre de Cayley de $\Lambda(2)$, nous voyons que

$$g = \min\{|[\alpha]|_{S_p} : [\alpha] \in \Lambda(2q)\,,\ [\alpha] \neq 1\}\,,$$

où $|\cdot|_{S_p}$ désigne la longueur des mots par rapport à S_p dans le groupe libre $\Lambda(2)$. Soit donc $\alpha = a_0 + a_1 i + a_2\, j + a_3\, k \in \Lambda'(2)$, tel que $[\alpha] \in \Lambda(2q)$ et $|[\alpha]|_{S_p} = g$. En prenant les normes, on a

$$p^g = a_0^2 + a_1^2 + a_2^2 + a_3^2$$

et au moins un des nombres a_1, a_2, a_3 est non nul, car $[\alpha] \neq 1$. D'autre part, q divise a_1, a_2, a_3 par (4). Donc $p^g \geqslant q^2$, c'est-à-dire $g \geqslant 2\log_p q$.

Si $\left(\dfrac{p}{q}\right) = -1$, comme $p^g \equiv a_0^2 \pmod q$, on voit d'abord que g est pair, disons $g = 2h$. Remarquons que l'on a en fait

$$p^{2h} \equiv a_0^2 \pmod{q^2}$$

ce qui implique (pas complètement trivialement, car on travaille *modulo* q^2) :

$$p^h \equiv \pm a_0 \pmod{q^2}.$$

D'autre part, $a_0^2 \leqslant p^g$, donc $|a_0| \leqslant p^h$. Supposons par l'absurde $g < 4\log_p q - \log_p 4$, c'est-à-dire $p^h < \frac{q^2}{2}$. Alors $|p^h \mp a_0| < q^2$. De la congruence précédente, nous tirons $p^h = \pm a_0$. Alors $p^g = a_0^2$, ce qui implique $a_1 = a_2 = a_3 = 0$: c'est la contradiction désirée.

Notons que cette proposition, jointe à l'inégalité (1), donne la borne inférieure

$$|Y^{p,q}| = |\mathrm{Im}\,\Pi_q| \geqslant q\,. \tag{5}$$

PREUVE DU THÉORÈME 1

Le théorème 1 résulte de la proposition suivante :

Proposition 2. *Si $q > \sqrt{2}\,p^8$, alors $X^{p,q}$ est connexe [et donc $X^{p,q} \simeq Y^{p,q}$, et :*

$$si\ \left(\frac{p}{q}\right) = 1\ :\quad g(X^{p,q}) \geqslant \frac{2}{3}\log_p |X^{p,q}|$$

$$si\ \left(\frac{p}{q}\right) = -1\ :\quad g(X^{p,q}) \geqslant \left(\frac{4}{3} + o(1)\right)\log_p |X^{p,q}|]\,.$$

Preuve. Nous devons montrer que $S_{p,q}$ engendre

$$\begin{cases} \mathrm{PSL}_2(q) & \text{si } \left(\frac{p}{q}\right) = 1 \\ \mathrm{PGL}_2(q) & \text{si } \left(\frac{p}{q}\right) = -1\,. \end{cases}$$

Notons $\langle S_{p,q}\rangle$ le sous-groupe engendré par $S_{p,q}$, et posons

$$H = \langle S_{p,q}\rangle \cap \mathrm{PSL}_2(q)\,.$$

Pour $g, h \in \mathrm{PSL}_2(q)$, notons $[g,h] = g\,h\,g^{-1}\,h^{-1}$ le commutateur de g et h. Nous allons utiliser une propriété des sous-groupes de $\mathrm{PSL}_2(q)$, encore due à Dickson :

Théorème 3 (Dickson 1901). *Soit q un nombre premier, $q \geqslant 7$. Soit H un sous-groupe propre de* $\mathrm{PSL}_2(q)$. *Si $|H| > 60$, alors H est* métabélien, *c'est-à-dire $[[g_1, g_2], [g_3, g_4]] = 1$ pour tous $g_1, g_2, g_3, g_4 \in H$.*

Pour une preuve de ce résultat, voir Dickson (1958) et Davidoff, Sarnak et Valette. La preuve du théorème 1 continue alors comme suit. Supposons par l'absurde que $S_{p,q}$ n'engendre pas ce qu'il doit engendrer, ce qui revient à dire que H est un sous-groupe propre de $\mathrm{PSL}_2(q)$. Remarquons que $|H| \geqslant q > 60$, par (5). Nous avons vu d'autre part que le graphe de Cayley $\mathcal{G}(\langle S_{p,q}\rangle, S_{p,q})$ est isomorphe à $Y^{p,q}$. Considérons deux cas :

a) Si $\left(\frac{p}{q}\right) = 1$, alors la relation $[[g_1, g_2], [g_3, g_4]] = 1$, appliquée à quatre éléments de $S_{p,q}$, fournit un circuit de longueur 16 dans $Y^{p,q}$. Nous obtenons, grâce à la proposition 1 :

$$2\log_p q \leqslant g(Y^{p,q}) \leqslant 16$$

c'est-à-dire $q \leqslant p^8$, une contradiction.

b) Si $\left(\frac{p}{q}\right) = -1$, alors la relation $[[g_1, g_2], [g_3, g_4]] = 1$, appliquée à quatre carrés d'éléments de $S_{p,q}$, fournit un circuit de longueur 32 dans $Y^{p,q}$. Nous obtenons, par la proposition 1 :

$$4\log_p q - \log_p 4 \leqslant g(Y^{p,q}) \leqslant 32$$

c'est-à-dire $q \leqslant \sqrt{2}\,p^8$, à nouveau une contradiction.

Remarques. 1) Dans les articles originaux de Lubotzky, Phillips et Sarnak et de Margulis (1988) la connexité de $X^{p,q}$ est démontrée pour $q > 2\sqrt{p}$, ce qui est évidemment meilleur que notre hypothèse de la proposition 2.

2) Si $\left(\frac{p}{q}\right) = -1$, Biggs et Boshier ont démontré en 1992 que $g(X^{p,q}) \leqslant 4\log_p q + \log_p 4 + 2$, de sorte que la constante $C = \frac{4}{3}$ du théorème 1 (ou de la proposition 2) est optimale.

POUR EN SAVOIR PLUS

Biggs (N.-L.), Boshier (A.-G.), Note on the girth of Ramanujan graphs, *J. Comb. Theory*, Ser. B **49**, n°2, 1990, 190-194.

Davidoff (G.), Sarnak (P.), Valette (A.), Elementary number theory, group theory and Ramanujan graphs, Cambridge Univ. Press, London Math. Soc. Student Texts 55, 2003.

Dickson (L.-E.), Arithmetic of quaternions, *Proc. London Math. Soc.*, (2) **20**, 1922, 225-232.

Dickson (L.-E.), *Linear groups with an exposition of the Galois field theory*, Dover Publications, New York, 1958.

Erdös (P.), Sachs (H.), Reguläre Graphen gegebener Taillenweite mit minimaler Knollenzahl, *Wiss. Z. Univ. Halle-Willenberg Math. Nat. R.*, **12,** 1963, 251-258.

Lubotzky (A.), Phillips (R.), Sarnak (P.), Ramanujan graphs, *Combinatorica*, **8**, 1988, 261-277.

Margulis (G.-A.), Explicit constructions of graphs without short cycles and low density codes, *Combinatorica*, **2**, 1982, 71-78.

Margulis (G.-A.), Explicit group-theoretical constructions of combinatorial schemes and their application to the design of expanders and concentrators, *J. Probl. Inf. Transm.*, **24**, n°1, 1988, 39-46.

Weil (A.), Sur les sommes de trois et quatre carrés (1974), Œuvres scientifiques Vol. III, Springer-Verlag, 1979.