Graphe associé au corps $F_5[x]/(1 + 3x + x^2 + 3x^3 + x^4)$

Gaëtan Kuhn

Qui suis-je ? Un ancien étudiant de l'Université de Genève ayant fini son master de mathématiques en février 2020. Pour mon mémoire, j'ai étudié les liens qui existent entre les structures algébriques et les graphes. Par la suite, mon superviseur Anders Karlsson et moi-même avons coécrit un article concernant un tout nouveau type de graphe associé à des corps finis.

Que voit-on sur cette image ? Il s'agit d'un graphe, c'est à dire un objet composé de sommets (points) et d'arêtes (liens entre deux sommets). En l'occurrence, ce graphe possède 625 sommets et 4996 arrêtes. Les graphes sont des objets combinatoires qui peuvent se révéler utiles dans différents domaines des mathématiques. Ce que vous voyez est l'une de ses réalisations géométriques.

Dans quel contexte ce graphe apparaît ? Comme mentionné ci-dessus, les graphes peuvent être utilisés dans différents domaines des mathématiques. Celui-ci appartient à une famille de graphes, utilisée en algèbre générale pour distinguer différents modèles d'un corps fini. Il représente l'un des modèles de $GF(5^4)$: le quotient $F_5[x]/(1 + 3x + x^2 + 3x^3 + x^4)$.

À quoi ça sert de distinguer différents modèles de corps finis ? Commençons par mettre un peu de lumière autour de cette notion de corps. Un corps fini est une structure mathématique à p^n éléments, équipée de deux opérations (une somme et un produit) compatibles. Le nombre p doit être un nombre premier et n un entier positif. Pour chaque paire (p, n), il n'existe « qu'un seul corps fini à isomorphisme près ». Derrière cette dénomination quelque peu indigeste, se cache l'idée suivante : deux corps ayant le même nombre d'éléments ont des opérations équivalentes. Pourtant, le choix d'un modèle se révèle important lorsque l'on fait des (gros) calculs, plus particulièrement lorsque ces objets sont implémentés dans des algorithmes. Certains sont plus efficaces et plus rapides que d'autres. Cela peut sembler en contradiction avec ce qui a été dit dans le paragraphe précédent, mais ce n'est pas le cas. Afin d'illustrer cela, faisons une analogie. Considérons l'addition et la multiplication telles que nous les connaissons. Ensuite, prenons les systèmes de numération arabe et romain comme deux « modèles » pour représenter nos éléments, les nombres. Si je vous demande de calculer la somme de quarante-trois avec cent trente-deux, vous conviendrez qu'il est plus commode de faire le calcul avec le modèle numérique arabe (43 + 132), plutôt qu'avec le modèle romain (XLIII + CXXXII). Ainsi la nature de l'opération reste la même, mais les modèles sont différents et pour le calcul, l'un est plus pratique que l'autre.

Je veux plus de détails ! Un graphe de cette famille se construit comme une superposition de deux graphes de Cayley (du groupe additif et du groupe multiplicatif), avec comme générateurs les racines du polynôme qui construit notre modèle. Ces graphes ont été pensés de façon à ce qu'un automorphisme de corps soit un automorphisme de graphe.

La partie orange correspond à un graphe de Cayley du groupe ${C_5}^n$. Ce n'est pas étonnant d'avoir une forme très régulière liée à 5. Pour la partie cyan par contre, c'est un peu plus chaotique ! Il y a néanmoins une tendance : pour de très grands corps se dessine une épicycloïde à $p \pm 1$ pétales. C'est un phénomène que l'on peut retrouver dans des graphes plus simples, associés aux tables de multiplication usuelles (c.f. références de [2] à [5]).

Pour ce qui est des invariants classiques de graphes, les graphes de cette familles sont connexes avec un diamètre borné par : $((2p-1)(2n+1)-3)$. Des simulations informatiques tendent à nous montrer que ce diamètre serait en réalité bien inférieur, ce qui rendrait cette famille de graphes d'autant plus intéressante ! Sa maille est de 2, les cycles en question se situent autour de $x^{p^k}(x^{p^k}-1)^{-1}$. C'est une propriété qui vient directement de la structure des corps que nous étudions. D'autres propriétés concernant les racines du polynôme, comme le fait d'être un élément normal ou primitif, se matérialisent également sur le graphe. Quelques valeurs propres ont été trouvées, mais l'essentiel de son spectre demeure pour le moment inconnu. Si vous souhaitez avoir plus de détails, vous pouvez lire l'article [1].

Références

[1] Anders Karlsson add Gaëtan Kuhn *A natural graph of finite fields distinguishing between models*. Submitted, 2020.

[2] Simon Plouffe *La forme de b^n mod p*. Non publié, 2020.

[3] Simon Plouffe *The reflection of light rays in a cup of coffee* Non publié, 2020.

[4] Times Tables, Mandelbrot and the Heart of Mathematics - Mathologer, `https://www.youtube.com/watch?v=qhbuKbxJsk8`

[5] The Dancing Mandala : Multiplication Tables Plotted on a Unit Circle, `https://www.youtube.com/watch?v=13be44CqrrI`