REVUE FRANÇAISE D'INFORMATIQUE ET DE RECHERCHE OPÉRATIONNELLE, SÉRIE ROUGE

A. BIGARD

Propriétés des diagrammes de Cayley

Revue française d'informatique et de recherche opérationnelle, série rouge, tome 4, n° 2 (1970), p. 51-56.

<http://www.numdam.org/item?id=M2AN_1970__4_2_51_0>

R.I.R.O.
(4e année, R-2, 1970, p. 51-56)

PROPRIETES DES DIAGRAMMES DE CAYLEY

par A. BIGARD

Résumé. — *L'objet de cet article est d'approfondir les relations qui existent entre la notion de groupe et la notion de graphe. Dès 1873, Cayley a montré qu'on peut représenter tout groupe fini au moyen d'un graphe. Cette représentation est d'un usage courant en cristallographie. Les graphes ainsi obtenus ont des propriétés remarquables. Nous les appelons « diagrammes de Cayley ».*

C'est Cayley qui a eu le premier l'idée de représenter les groupes par des graphes en faisant correspondre un point à chaque élément du groupe et en joignant deux points par un arc si le second est multiple du premier par un générateur [1]. Cette représentation est souvent utilisée en cristallographie. Nous allons voir qu'elle permet d'établir une connexion intéressante entre la théorie des groupes et la théorie des graphes.

Dans cet article, nous traiterons uniquement du cas fini.

Soit (X, U) un graphe fini, où X est l'ensemble des sommets et $U \subseteq X \times X$ l'ensemble des arcs. On notera $|X|$ le nombre d'éléments de X.

Définition. — Nous dirons que (X, U) est un diagramme de Cayley s'il existe sur X une structure de groupe telle que $(a, b) \in U$ implique $(ax, bx) \in U$ et $(xa, xb) \in U$.

Nous poserons $U(a) = \{ b \mid (a, b) \in U \}$ et $U^{-1}(a) = \{ b \mid (b, a) \in U \}$.

D'autre part, nous noterons e l'élément neutre de X.

Proposition 1. — *Pour tout a, on a* $U(a) = aU(e) = U(e)a$;

$$U^{-1}(a) = aU^{-1}(e) = U^{-1}(e) \quad \text{et} \quad U^{-1}(a^{-1}) = [U(a)]^{-1}$$

En effet, si $x \in U(a)$, on a $(a, x) \in U$ qui est équivalent à $(e, a^{-1}x) \in U$, c'est-à-dire à $a^{-1}x \in U(e)$ ou encore $x \in aU(e)$.

De plus, $(a, x) \in U$ est aussi équivalent à $(e, xa^{-1}) \in U$ c'est-à-dire à $x \in U(e)a$.

La seconde égalité se démontre de la même manière. Par ailleurs, $x \in U^{-1}(a^{-1})$ est équivalent à $(x, a^{-1}) \in U$, donc à :

$(a, x^{-1}) = (axx^{-1}, aa^{-1}x^{-1}) \in U$, c'est-à-dire $x^{-1} \in U(a)$ ou encore $x \in [U(a)]^{-1}$.

Corollaire 1. — *Pour tout* a, $|U(a)| = |U^{-1}(a)| = |U(e)|$.

Corollaire 2. — $U(e)$ *est une partie distinguée de* $X(\forall x, xU(e) = U(e)x)$.

Proposition 2. — *Si* G *est un groupe et* K *une partie distinguée de* G, *il existe* U *tel que* (G, U) *soit un diagramme de Cayley et* $U(e) = K$. *De plus* U *est unique.*

Prenons $U = \{(a, b) \mid a^{-1}b \in K\}$. Si $(a, b) \in U$, alors

$$(ax)^{-1}(bx) = x^{-1}a^{-1}bx \in x^{-1}Kx \subseteq K$$

donc $(ax, bx) \in U$ et $(xa)^{-1}(xb) = a^{-1}x^{-1}xb = a^{-1}b \in K$, donc $(xa, xb) \in U$.

Il est clair que $U(e) = K$ et l'unicité résulte de la proposition 1.

Si (X, U) est un diagramme de Cayley, considérons le préordre $\tilde{U}$ associé à U : $(a, b) \in \tilde{U}$ si et seulement si $a = b$ ou il existe une suite $(x_i)_{0 \leqslant i \leqslant n}$ telle que $x_0 = a$, $x_n = b$ et $(x_i, x_{i+1}) \in U$ pour tout $i < n$.

On voit immédiatement que $(X, \tilde{U})$ est un diagramme de Cayley.

Lemme. — $(a, b) \in U$ *implique* $(b, a) \in \tilde{U}$.

Considérons d'abord le cas où $a = e$. Désignons par N l'ordre de X.

On a certainement $b^N = e$. Or $(e, b) \in \tilde{U}$ implique successivement $(b, b^2) \in \tilde{U}$, $(b^2, b^3) \in \tilde{U}$, ..., $(b^{N-1}, e) \in \tilde{U}$. Comme $\tilde{U}$ est transitif, il en résulte $(b, e) \in \tilde{U}$. Revenons au cas général : $(a, b) \in \tilde{U}$ entraîne $(e, a^{-1}b) \in \tilde{U}$ donc $(a^{-1}b, e) \in \tilde{U}$ c'est-à-dire $(b, a) \in \tilde{U}$.

Si nous appelons stable par U tout sous-groupe S tel que $a \in S$ implique $U(a) \subseteq S$, alors on a le théorème suivant :

Théorème 1. — *Dans un diagramme de Cayley,* $\tilde{U}(e)$ *est :*

1° *la composante connexe de* e,

2° *le sous-groupe engendré par* $U(e)$,

3° *l'intersection des sous-groupes stables par* U.

Désignons respectivement par A, B, C ces trois ensembles.

On a évidemment $\tilde{U}(e) \subseteq A$. Inversement, soit $a \in A$.

On a alors une chaîne $(x_i)_{i \geqslant n}$ reliant e à a. Raisonnons par récurrence sur n. Comme $x_{n-1} \in A$, on a $x_{n-1} \in \tilde{U}(e)$. si $(x_{n-1}, a) \in U$ alors $(e, a) \in \tilde{U}$. Si $(a, x_{n-1}) \in U$, on a $(a, x_{n-1}) \in \tilde{U}$ donc d'après le lemme $(x_{n-1}, a) \in \tilde{U}$

ce qui donne encore $(e, a) \in \tilde{U}$ par transitivité. On a donc $A = \tilde{U}(e)$. On va montrer que $\tilde{U}(e) \subseteq C \subseteq B \subseteq \tilde{U}(e)$.

Si S est stable par U, il l'est aussi par $\tilde{U}$ donc $\tilde{U}(e) \subseteq S$. Par suite, on a bien $\tilde{U}(e) \subseteq C$.

Pour prouver que $C \subseteq B$, il suffit de vérifier que B est stable. Si $a \in B$ et $x \in U(a)$, on a $a^{-1}x \in U(e) \subseteq B$ donc $x \in B$.

Enfin, $\tilde{U}(e)$ est un sous-groupe distingué car, d'après le lemme, $\tilde{U}$ est une relation d'équivalence compatible avec la structure de groupe. Comme $\tilde{U}(e)$ contient $U(e)$, il contient aussi B qui est engendré par $U(e)$.

Corollaire 1. — *Dans un diagramme de Cayley, les composantes connexes sont fortement connexes et toutes isomorphes.*

Comme l'application $x \to ax$ est un automorphisme du graphe, la composante connexe de a est $a\tilde{U}(e) = \tilde{U}(a)$.

Corollaire 2. — *Un diagramme de Cayley (X, U) est connexe si et seulement si X est engendré par $U(e)$.*

D'après la proportion 1, si $U(e)$ a n éléments $U(a) = aU(e)$ a également n éléments. Il en est de même de $U^{-1}(a) = [U(a^{-1})]^{-1}$. D'après un résultat bien connu (cf. [2], chap. 17, théorème 2) on a :

Proposition 3. — *Un diagramme de Cayley connexe admet un circuit eulérien.*

On remarquera que tout circuit eulérien passe exactement n fois par chaque sommet.

Posons $U(e) = \{ t_1, ..., t_n \}$ et soit $V_i = \{ (a, b) \mid a^{-1}b = t_i \}$. On a ainsi une partition de U : $U = V_1 \cup ... \cup V_n$ ou, si l'on préfère, un coloriage des arcs. Le graphe a donc la propriété suivante que nous appellerons propriété de l'arc-en-ciel : De tout sommet part et arrive un arc de chaque couleur et un seul.

Proposition 4. — *Soit (X, U) un diagramme de Cayley connexe. Pour que X soit commutatif, il faut et il suffit qu'il vérifie la propriété suivante :*

(c) Si $(a, b) \in V_i$ et $(b, c) \in V_j$, il existe d avec $(a, d) \in V_j$ et $(d, c) \in V_i$.

Intuitivement, tout chemin de longueur deux donne naissance à un parallélogramme dont les côtés opposés sont de même couleur.

La condition est nécessaire car on a : $a^{-1}b = t_i$, $b^{-1}c = t_j$. Posons $d = at_j$. On a $c = bt_j = at_it_j = at_jt_i = dt_i$.

La condition est suffisante : Si t_i et t_j sont deux générateurs, on a $(e, t_i) \in V_i$ et $(t_i, t_it_j) \in V_j$.

Soit d tel que $(e_i\, d) \in V_j$ et $(d, t_i t_j) \in V_i$. On a $d = t_j$ et $t_i t_j = dt = t_i t_j$, donc les générateurs de X commutent.

La propriété (*c*) sera dite propriété du parallélogramme.

Théorème 2. — *Soit (X, U) un graphe connexe. Pour qu'il existe sur X une structure de groupe commutatif qui fasse de (X, U) un diagramme de Cayley, il faut et il suffit qu'il existe un coloriage des arcs pour lequel il a la propriété de l'arc-en-ciel et la propriété du parallélogramme.*

On a vu que ces conditions sont nécessaires. Montrons qu'elles sont suffisantes.

Soit n le nombre de couleurs du coloriage et soit L le groupe abélien libre à n générateurs $(g_1, ..., g_n)$. Prenons une origine arbitraire 0 sur le graphe.

Si $g = \lambda_1 g_1 + ... + \lambda_n g_n$ est un élément de L, g définit un chemin sur le graphe, de la façon suivante. On part de 0 et on suit λ_1 arcs de couleurs g_1 dans le sens positif si $\lambda_1 \geqslant 0$ ou négatif si $\lambda_1 \leqslant 0$. On parvient ainsi à un sommet a_1. De a_1 on suit λ_2 arcs de couleur g_2 dans le sens positif si $\lambda_2 \geqslant 0$ et négatif si $\lambda_2 \leqslant 0$, etc. Soit $\varphi(g)$ l'extrémité du chemin défini par g.

1) Montrons que l'application φ est surjective.

Comme X a la propriété de l'arc-en-ciel, il existe un circuit eulérien donc il est fortement connexe. Soit $x \in X$. Considérons un chemin joignant 0 à x : $u_0 = 0, u_1, ..., u_n = x$.

Sur ce chemin les couleurs se succèdent dans un certain ordre, qui n'est pas nécessairement l'ordre canonique.

Si $(u_{\alpha-1}, u_\alpha) \in V_i$ et $(u_\alpha, u_{\alpha+1}) \in V_j$ avec $j < i$ on remplace u_α par u'_α tel que $(u_{\alpha-1}, u'_\alpha) \in V_j$ et $(u'_\alpha, u_{\alpha+1}) \in V_i$. Ces transformations permettent d'obtenir un chemin « canonique » provenant d'un élément de L par le procédé indiqué.

2) Montrons que $\varphi(g) = \varphi(g')$ implique $\varphi(s + g) = \varphi(s + g')$. Il est clair qu'on peut se ramener, par récurrence, au cas où s est un générateur g_i. Si $a = \varphi(g) = \varphi(g')$, $\varphi(g_i + g)$ et $\varphi(g_i + g')$ coïncident avec l'unique b tel que $(a, b) \in V_i$.

La relation $\varphi(g) = \varphi(g')$ est donc une relation d'équivalence $\mathcal{R}$ compatible avec la structure du groupe L. Il existe une bijection entre $L/\mathcal{R}$ et X. Il suffit maintenant de transporter sur X la structure de groupe de $L/\mathcal{R}$.

Si $\mathcal{C} = (u_1, ..., u_n)$ est un chemin, nous noterons $x\mathcal{C}$ le chemin $(xu_1, ..., xu_n)$. Si $\mathcal{C}$ est un chemin hamiltonien, $x\mathcal{C}$ est un chemin hamiltonien. Par suite si (X, U) admet un chemin hamiltonien, tout sommet est l'origine d'un chemin hamiltonien.

Théorème 3. — *Soit (X, U) un diagramme de Cayley commutatif. Pour qu'il admette un chemin hamiltonien, il faut et il suffit qu'il soit connexe.*

La condition est évidemment nécessaire. Montrons qu'elle est suffisante. On pose $U(e) = \{ t_1, ..., t_n \}$. Nous allons raisonner par récurrence sur n.

Si $n = 1$, alors G est cyclique d'ordre N et $(e, t_1, t_1^2, ..., t_1^{N-1})$ est un chemin halmitonien.

Soit S le sous-groupe engendré par $\{ t_2, ..., t_n \}$. Le sous-groupe engendré S admet un chemin hamiltonien $\mathcal{C}$. On peut supposer que $\mathcal{C} = (e, ..., b)$. Soit k l'index de S. Si xS est une classe modulo S, on remarque que $x\mathcal{C}$ est un chemin hamiltonien de xS. On obtient alors un chemin hamiltonien de X de la façon suivante :

$$(\mathcal{C}, t_1 b\mathcal{C}, t_1^2 b^2 \mathcal{C}, ..., t_1^{k-1} b^{k-1} \mathcal{C})$$

La proposition suivante fournit un critère assez simple pour que (X, U) soit commutatif.

Proposition 5. — *Soit (X, U) un diagramme de Cayley connexe.*

$$\text{Si } |X| = p_1^{\alpha_1} ... p_r^{\alpha_r}$$

(décomposition en facteurs premiers) et si $|U(e)| \leqslant \inf (p_i - 1)$, X est commutatif.

Comme $U(e)$ est distingué, X opère dans $U(e)$ par les automorphismes intérieurs. On considère la décomposition de $U(e)$ en classes de transitivité. Chaque classe a un ordre de la forme $p_1^{\beta_1} ... p_r^{\beta_r}$ avec $\beta_i \leqslant \alpha_i$. Par suite de la condition imposée sur $|U(e)|$ les β_i sont nuls. Donc chaque classe de transitivité se réduit à un seul élément. Par suite, $U(e)$ est contenu dans le centre.

Comme $U(e)$ engendre X, il en résulte que X est commutatif.

Rappelons qu'un graphe de tournoi est un graphe (X, U) sans boucle tel que pour $a \neq b$, U contient (a, b) ou (b, a) mais pas les deux.

Un diagramme de Cayley (X, U) est un graphe de tournoi si et seulement si $U(e) \cap U^{-1}(e) = \varnothing$ et $X = e \cup U(e) \cup U^{-1}(e)$.

Proposition 6. — *Soit X un groupe commutatif. Pour qu'on puisse le munir d'une structure de graphe de tournoi, il faut et il suffit que $|X|$ soit impair.*

La condition est nécessaire car $|U(e)| = |U^{-1}(e)|$, donc $|X| = 2|U(e)| + 1$.

Inversement, supposons X d'ordre impair. Prenons $T \subseteq X \times X$ maximal parmi les S tels que $S \cap S^{-1} = \varnothing$. Montrons que $X = e \cup T \cup T^{-1}$.

Soit $a \notin e \cup T \cup T^{-1}$. Si on pose $S = T \cup a$, on a nécessairement $S \cap S^{-1} \neq \varnothing$ d'après la maximalité de T. Si $x \in S \cap S^{-1}$, on a certainement $x = a = a^{-1}$. $|X|$ est divisé par l'ordre de a, qui est égal à 2, d'où une contradiction.

Soient (X_1, U_1) et (X_2, U_2) deux diagrammes de Cayley. On définira leur somme directe comme le diagramme (X, U) avec $X = X_1 \times X_2$ et

$$U(e) = (U_1(e) \times \{ e \}) \cup (\{ e \} \times U_2(e)).$$

Proposition 7. — *La somme de deux diagrammes est connexe si et seulement si ces diagrammes sont connexes.*

C'est pratiquement immédiat, si l'on tient compte du corollaire 2 du théorème 1.

Parmi les diagrammes de Cayley, les plus simples sont ceux engendrés par un élément t avec $U(e) = \{ t \}$. Nous les dirons « cycliques ». Ils méritent doublement ce nom, à la fois comme groupes et comme graphes.

Le théorème suivant caractérise les diagrammes décomposables en diagrammes cycliques.

Théorème 4. — *Pour qu'un diagramme de Cayley soit isomorphe à une somme directe de diagrammes cycliques, il faut et il suffit qu'il soit connexe, commutatif et que deux chemins qui ont les mêmes extrémités aient au moins une couleur commune* (dans le coloriage choisi).

Supposons que (X, U) est la somme des $(X_i, U_i)_{1 \leqslant i \leqslant n}$, avec $U_i(e) = t_i$.

On a donc $U(e) = \{ t_1, ..., t_n \}$.

X est connexe d'après la proposition 7 et commutatif car les X_i sont commutatifs. Soient $\mathcal{C}_1$ et $\mathcal{C}_2$ deux chemins joignant x à y $(x \neq y)$. $\mathcal{C}_1$ (resp. $\mathcal{C}_2$ utilise λ_i (resp. μ_i) arcs de couleur t_i. On a

$$y = t_1^{\lambda_1} \dots t_n^{\lambda_n} x = t_1^{\mu_1} \dots t_n^{\mu_n} x, \quad \text{d'où} t_i^{\lambda_i} = t_i^{\mu_i}.$$

Il existe un i tel que $t_i^{\lambda_i} \neq e$. Alors $\mathcal{C}_1$ et $\mathcal{C}_2$ utilisent effectivement la couleur t_i.

Réciproquement, posons $U(e) = \{ t_1, ..., t_n \}$ et soit X_i le sous-groupe de X engendré par t_i. On a $X = \sum_{i=1}^{n} X_i$. Montrons que cette somme est directe. Si on avait $e \neq t_i^{\lambda_i} = \prod_{s \neq i} t_s^{\lambda_s} = a$, on aurait deux chemins joignant e à a et n'ayant aucune couleur commune.

BIBLIOGRAPHIE

[1] CAYLEY, « The Theory of groups : graphical representation », *American Journal of Mathematics* 1 (1878).

[2] C. BERGE, *Théorie des graphes et ses applications*, Dunod, 2e éd., 1967.