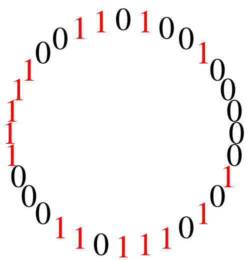
Mathémagie : cycles de de Bruijn et jeu de carte.
Fabrice ORGOGOZO

Références : [TAOCP 4A, 7.2.1.1], [TAOCP 1, exercice 2.3.4.2-23], [TAOCP 2, exercice 3.2.2-17], [Flajolet et Sedgewick 2009, exemple V.15], [Stanley 1999, 5.6.15], [Lidl et Niederreiter 1997, chap. 8] ; [Diaconis et Graham 2012, chap. 2 et 4].

1. Théorie (esquisse de)

Soient A un ensemble de cardinal a et r un entier. On appelle **suite**[1] **de de Bruijn**[2] a-aire d'ordre r une suite cyclique u, c'est-à-dire une application $\mathbb{Z}/N\mathbb{Z} \to A$ pour un entier $N \geq 1$, telle que pour chaque mot m de longueur r formé sur A, il existe un unique $i \in \mathbb{Z}/N\mathbb{Z}$ tel que $m = u_{i+1}u_{i+2}\cdots u_{i+r}$. Compte-tenu de l'unicité et du fait qu'il existe a^r mots de longueur r, on a nécessairement $N = a^r$. Les suites cycliques

et



sont des exemples de suites de de Bruijn binaires d'ordre respectivement 3 et 5 (avec respectivement $N = 8$ et 32)[3]. On peut montrer non seulement qu'il en existe toujours (pour a et r quelconques) mais aussi les compter : le nombre de suites de de Bruijn binaires d'ordre r commençant par $0\cdots0$ [r zéros] est égal à $2^{2^{r-1}-r}$.

La théorie des corps finis permet de construire de telles suites lorsque le cardinal de l'alphabet A est une puissance q d'un nombre premier. (Le cas général s'y ramène d'ailleurs, en décomposant a — donc N — en produit de facteurs premiers et en utilisant le théorème chinois.) Fixons une extension $\mathbb{F}_q \subseteq \mathbb{F}_{q^r}$ de corps de cardinaux respectifs q et q^r et considérons un générateur x de $\mathbb{F}_{q^r}^\times$, de polynôme minimal $P = T^r - c_1T^{d-1} - c_2T^{d-2}\cdots - c_{r-1}T - c_r \in \mathbb{F}_q[T]$. (Il existe $\dfrac{\varphi(q^r-1)}{r} > 1$ tels polynômes.) Considérons la suite u définie de la façon suivante : $u_1 = \cdots = u_{r-1} = 0$, $u_r = c_r$ et, pour $n \in]\!]r, q^r[\![$, définie par récurrence : $u_n = c_r u_{n-r} + \cdots + c_1 u_{n-1}$. La matrice A associée à cette *suite récurrence linéaire* est la matrice compagnon du polynôme P ; elle est diagonalisable sur $\mathbb{F}_{q^r}$, de valeurs propres x et ses conjugués, qui sont des racines primitives q^r-1-ièmes de l'unité. On se convainc alors aisément que la suite $u = u_0u_1\cdots u_{q^r-1}$, où $u_0 \coloneqq 0$, est une suite de de Bruijn : les images par A^i du vecteur non nul $(u_1, \ldots, u_r)$ parcourent $\mathbb{F}_q^r - \{0\}$ lorsque i parcourt $[\![0, q^r-1[\![$ et l'égalité $A^{q^r-1}(u_1, \ldots, u_r) = (u_1, \ldots, u_r)$ montre que la suite est bien cyclique. (Poser $u_0 = 0$ permet d'obtenir le mot nul $0\cdots0$ de longueur r.)

[1] Ou bien « cycle », « bracelet ».

[2] « də ˈbrœy̯n »

[3] Dans le premier cas, ce sont les deux seules suites, à rotation près.

2. Tour de magie

Considérons un jeu de $32 = 2^5$ cartes triées de la façon suivante :

$$8\clubsuit,\ A\clubsuit,\ 2\clubsuit,\ 4\clubsuit,\ A\spadesuit,\ 2\diamondsuit,\ 5\clubsuit,\ 3\spadesuit,\ 6\diamondsuit,\ 4\spadesuit,\ A\heartsuit,\ 3\diamondsuit,\ 7\clubsuit,\ 7\spadesuit,\ 7\heartsuit,\ 6\heartsuit, \ldots$$
$$\ldots, 4\heartsuit,\ 8\heartsuit, A\diamondsuit,\ 3\clubsuit,\ 6\clubsuit,\ 5\spadesuit,\ 3\heartsuit,\ 7\diamondsuit,\ 6\spadesuit,\ 5\heartsuit,\ 2\heartsuit,\ 5\diamondsuit,\ 2\spadesuit,\ 4\diamondsuit,\ 8\spadesuit,\ 8\diamondsuit.$$

Le lien avec la suite de de Bruijn binaire d'ordre 5 ci-dessus (lue dans le sens trigonométrique positif) — associée au polynôme $T^5 - T^2 - 1$, c'est-à-dire à la relation de récurrence $u_n = u_{n-5} + u_{n-3}$ dans $\mathbb{F}_2$ — est le suivant : à un 5-uplet de bits, on peut associer une couleur (le bit dominant : 0↔noir ; 1↔rouge), majeur ou pas (bit suivant : 0↔♣, ♢; 1↔♡, ♠), et un nombre entre 1 et 8 (trois derniers bits, avec la convention que 000↔8). Par exemple, le « mot » 00000 correspond au 8♣, le mot 00001 à $A\clubsuit$, etc. En pratique, on demande à des spectateurs de couper le jeu à tour de rôle (ce qui ne change rien à l'ordre des cartes à rotation près) et on demande aux 5 derniers de prendre chacun la carte sur le dessus. On leur demande de se concentrer sur la carte et de nous envoyer par « télépathie » la valeur de leur carte. Sous prétexte d'interférences ou variante, on demande à ceux qui ont une carte rouge de se mettre en avant. On peut alors immédiatement trouver la première carte : c'est celle correspondant par le codage précédent au mot CCCCC, où les C sont les couleurs des cartes des 5 spectateurs (avec rappelons-le la convention rouge↔1, **noir**↔0). Après avoir annoncé quelle est cette carte, on peut demander au premier spectateur de la montrer pour confirmer que l'on a correctement « reçu le message ». Reste à trouver les 4 cartes suivantes. La relation de récurrence étant particulièrement simple ici — après abcde, on a bcde(a+c mod. 2) [sauf pour 00000] —, il n'est pas nécessaire de connaître par cœur l'ordre du jeu : la valeur de la carte suivant une carte de valeur x est $2x$ sauf si la carte est un petit rouge ou un gros noir, auquel cas c'est $2x+1$. (Convention : « petit » : $8 = 0, 1, 2, 3$; « gros » : $4, 5, 6, 7$.) Enfin, la carte suivante, dont on connaît déjà la couleur, est une carte en majeur (c'est-à-dire cœur ou pique) si la dernière carte visible est grosse. Exception : on ne passe pas du 8↔10000 au A♣↔00001 mais on intercale 8♣↔00000 entre les deux. (L'application linéaire étant injective, on n'obtient jamais 00000 en itérant à partir d'un vecteur non nul.)

Pour d'autres applications ludiques des corps finis, cf. p. ex. [Madore 2015a], [Madore 2015b].

Références

The art of computer programming

TAOCP 1 Donald E. Knuth (1997). *The art of computer programming. Vol. 1. Fundamental algorithms.* 3e éd. Addison-Wesley, xx+650 pages.

TAOCP 2 Donald E. Knuth (1998). *The art of computer programming. Vol. 2. Seminumerical algorithms.* 3e éd. Addison-Wesley, xiv+762 pages.

TAOCP 4A Donald E. Knuth (2011). *The art of computer programming. Vol. 4A. Combinatorial algorithms, part 1.* Addison-Wesley, xvi+883 pages.

Diaconis, Persi et Ron Graham (2012). *Magical mathematics.* The mathematical ideas that animate great magic tricks. Princeton University Press, xiv+244 pages.

Flajolet, Philippe et Robert Sedgewick (2009). *Analytic combinatorics.* Cambridge University Press, xiv+810 pages. ☞.

Lidl, Rudolf et Harald Niederreiter (1997). *Finite fields.* 2e éd. Encyclopedia of Mathematics and its Applications **20**. Cambridge University Press, xiv+755 pages.

Madore, David A. (2015a). *Le jeu de cartes Dobble et la géométrie projective expliquée aux enfants.* Blog. ☞.

– (2015b). *Comment faire un jeu de* Tribble. Blog. ☞.

Stanley, Richard P. (1999). *Enumerative combinatorics. Vol. 2.* Cambridge Studies in Advanced Mathematics **62**. Cambridge University Press, xii+581 pages.