1 Prélude

On mélange un jeu de n cartes (n est pair) de la façon suivante :
- On le coupe d'abord en deux paquets de même taille : le *paquet inférieur* et le *paquet supérieur* ;
- On intercale les cartes du paquet inférieur avec celles du paquet supérieur en commençant par la carte inférieure du paquet inférieur et en respectant strictement l'alternance des paquets. On termine donc nécessairement par la carte supérieure du paquet supérieur.

On numérote les positions de 0 (pour la carte inférieure) à $n-1$ (pour la carte supérieure) et on note f_n la permutation de $\{0,\dots,n-1\}$ définie par ce mélange : la carte qui se trouvait à la position i se retrouve à la position $f_n(i)$. On note k_n l'*ordre* de la permutation f_n, c'est-à-dire le plus petit entier $k > 0$ tel qu'en appliquant k fois ce mélange à un paquet donné, on retrouve la configuration initiale du paquet.

a. Combien y a-t-il de positions i telles que $f_n(i) \neq i$? En déduire une majoration de k_n.

Dans le cas d'un jeu de 32 cartes, on code les positions en binaire sur 5 bits, avec la convention habituelle : bit de poids fort à gauche.

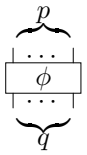
b. Décrire l'action de la permutation f_{32} pour ce codage des positions. En déduire la valeur de k_{32}.

2 Portes réversibles

On note $\mathbf{B}$ le corps fini à 2 éléments, c'est-à-dire l'ensemble $\{0,1\}$ muni de l'addition $x, y \mapsto x+y \bmod 2$ et de la multiplication $x, y \mapsto xy$. On rappelle que, dans ce corps, on a toujours $x^2 = x$. On identifie 0 avec le booléen *faux*, et 1 avec le booléen *vrai*.

a. Exprimer les connecteurs logiques habituels (*non*, *et*, *ou*) ainsi que le *ou exclusif* en utilisant l'addition et la multiplication de $\mathbf{B}$.

Une *porte booléenne à p entrées et q sorties* est la donnée d'une application $\phi : \mathbf{B}^p \to \mathbf{B}^q$ que l'on représente ainsi :



Cette porte est dite *réversible* si elle définit une bijection : dans ce cas, on a nécessairement $p = q$, et on note $\phi^{-1} : \mathbf{B}^p \to \mathbf{B}^p$ la porte *inverse* (ou *réciproque*). En particulier, on a la *porte identité* $\mathrm{id}_p : \mathbf{B}^p \to \mathbf{B}^p$ définie par $\mathrm{id}_p(x_1,\dots,x_p) = (x_1,\dots,x_p)$, que l'on représente ainsi :

b. Combien existe-t-il de portes booléennes à p entrées et q sorties, et de portes réversibles à p entrées ?

c. Exprimer chacune des portes booléennes à une ou deux entrées et une sortie comme un polynôme en une ou deux variables.

Si la porte $\phi : \mathbf{B}^p \to \mathbf{B}^q$ est de la forme $\phi(x_1,\dots,x_p) = (f_1(x_1,\dots,x_p),\dots,f_q(x_1,\dots,x_p))$ où $f_1,\dots,f_q$ sont des polynômes de degré ≤ 1, on dit qu'elle est *affine*. Si de plus, les polynômes $f_1,\dots,f_q$ sont sans terme constant, on dit qu'elle est *linéaire* : ϕ est alors définie par une matrice à q lignes et p colonnes à coefficients dans $\mathbf{B}$. Enfin, dans le cas où $\phi(x_1,\dots,x_p) = (x_1+a_1,\dots,x_p+a_p)$ (avec $a_1,\dots,a_p \in \mathbf{B}$), on dit que ϕ est une *translation de* $\mathbf{B}^p$.

d. Combien existe-t-il de portes booléennes linéaires (respectivement affines) à p entrées et q sorties ?

e. Combien existe-t-il de portes booléennes réversibles linéaires (respectivement affines) à deux entrées ?

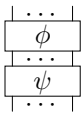
f. En déduire que toutes les portes booléennes réversibles à deux entrées sont affines.

g. En est-il de même pour les portes booléennes réversibles à trois entrées ?

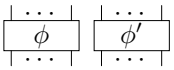
3 Circuits réversibles

Les portes booléennes se composent de deux manières différentes :

- *en série* : à partir de $\phi : \mathbf{B}^p \to \mathbf{B}^q$ et $\psi : \mathbf{B}^q \to \mathbf{B}^r$, on construit la porte $\psi \circ \phi : \mathbf{B}^p \to \mathbf{B}^r$ telle que $\psi \circ \phi\,(x_1, \ldots, x_p) = \psi(y_1, \ldots, y_p)$ où $(y_1, \ldots, y_p) = \phi(x_1, \ldots, x_p)$). On la représente par le *circuit booléen* suivant :

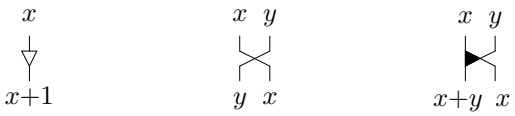


- *en parallèle* : à partir de $\phi : \mathbf{B}^p \to \mathbf{B}^q$ et $\phi' : \mathbf{B}^{p'} \to \mathbf{B}^{q'}$, on construit la porte $\phi \times \phi' : \mathbf{B}^{p+p'} \to \mathbf{B}^{q+q'}$ telle que $\phi \times \phi'\,(x_1, \ldots, x_p, x'_1, \ldots, x'_{p'}) = (y_1, \ldots, y_q, y'_1, \ldots, y'_{q'})$ où $(y_1, \ldots, y_q) = \phi(x_1, \ldots, x_p)$ et $(y'_1, \ldots, y'_{q'}) = \phi'(x'_1, \ldots, x'_{p'})$. On la représente par le circuit booléen suivant :



Si $\mathcal{P}$ est un ensemble de portes à p entrées et p sorties, l'ensemble $\mathcal{P}^*$ des produits en série d'éléments de $\mathcal{P}$ s'appelle le *monoïde engendré par* $\mathcal{P}$. On dit aussi que les éléments de $\mathcal{P}$ *engendrent* ceux de $\mathcal{P}^*$.

On considère la translation $\mathrm{N} : \mathbf{B} \to \mathbf{B}$ définie par $\mathrm{N}(x) = x + 1$ et les deux portes réversibles linéaires $\mathrm{H}, \mathrm{K} : \mathbf{B}^2 \to \mathbf{B}^2$ définies par $\mathrm{H}(x, y) = (y, x)$ et $\mathrm{K}(x, y) = (x + y, x)$. On les représente ainsi :



a. Quel est l'ordre et l'inverse de chacune de ces permutations ?

b. Montrer que H et K engendrent les permutations linéaires de $\mathbf{B}^2$.

c. Montrer que $\mathrm{N} \times \mathrm{id}_1$ et $\mathrm{id}_1 \times \mathrm{N}$ engendrent les translations de $\mathbf{B}^2$.

d. En déduire que H, K et $\mathrm{N} \times \mathrm{id}_1$ engendrent les permutations de $\mathbf{B}^2$.

Une porte réversible $\phi : \mathbf{B}^p \to \mathbf{B}^p$ peut être interprétée comme une permutation d'un jeu de 2^p cartes (voir le prélude).

e. Donner l'interprétation des circuits booléens suivants en termes de mélange d'un jeu de 32 cartes :

4 Cas linéaire

On rappelle qu'une porte linéaire $\phi : \mathbf{B}^p \to \mathbf{B}^q$ est définie par une matrice à q lignes et p colonnes à coefficients dans $\mathbf{B}$.

a. Quelles sont les matrices respectives de H, K et K^{-1} ?

On considère maintenant le cas d'une porte réversible linéaire $\phi : \mathbf{B}^p \to \mathbf{B}^p$ définie par la matrice carrée A. On va décomposer ϕ en utilisant une variante de l'algorithme de Gauss. Pour $1 \leq i \leq p - 1$, on pose $\mathrm{H}_i = \mathrm{id}_{i-1} \times \mathrm{H} \times \mathrm{id}_{p-i-1}$ et $\mathrm{K}_i = \mathrm{id}_{i-1} \times \mathrm{K} \times \mathrm{id}_{p-i-1}$.

b. À quelles opérations élémentaires sur les lignes ou les colonnes de A correspondent les transformations suivantes ?

$$\phi \mapsto \mathrm{H}_i \circ \phi, \qquad \phi \mapsto \mathrm{K}_i^{-1} \circ \phi, \qquad \phi \mapsto \phi \circ \mathrm{H}_i, \qquad \phi \mapsto \phi \circ \mathrm{K}_i^{-1}.$$

On dit qu'une colonne (ou une ligne) est *normale* si son premier coefficient vaut 1 et les autres sont nuls.

c. À quelles conditions sur la matrice A la porte ϕ est-elle de la forme $\mathrm{id}_1 \times \phi'$ avec $\phi' : \mathbf{B}^{p-1} \to \mathbf{B}^{p-1}$?

d. Montrer qu'en appliquant des transformations du type $\phi \mapsto \mathrm{H}_i \circ \phi$ et $\phi \mapsto \mathrm{K}_i^{-1} \circ \phi$, on obtient une matrice B dont la dernière colonne est normale.

e. Montrer qu'en appliquant ensuite des transformations du type $\phi \mapsto \phi \circ \mathrm{H}_i$ et $\phi \mapsto \phi \circ \mathrm{K}_i^{-1}$, on obtient une matrice C dont la première ligne et la première colonne sont normales.

f. En déduire que les H_i et les K_i engendrent les permutations linéaires de $\mathbf{B}^p$.

g. Donner la décomposition sous forme d'un circuit booléen pour la porte réversible linéaire $\phi : \mathbf{B}^4 \to \mathbf{B}^4$ définie par la matrice suivante :

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

h. En général, quelle est la longueur de la décomposition de A (dans le pire des cas) ?

Cette décomposition suggère un algorithme pour inverser une matrice carrée A. Pour cela, on introduit trois variables de matrices X, Y, Z.

- Initialement, X vaut A et Y, Z valent I (matrice identité à p lignes et p colonnes) ;
- à chaque fois qu'on applique une transformation élémentaire aux colonnes de la matrice X, on applique la même transformation à Y ;
- à chaque fois qu'on applique une transformation élémentaire aux lignes de la matrice X, on applique la même transformation à Z ;
- à la fin de la décomposition, X vaut I.

i. Exprimer A^{-1} en fonction de Y et Z (à la fin du calcul).

5 Cas général

Soit $\mathcal{P}$ un ensemble de portes booléennes. On dit qu'une porte est *définissable à partir de* $\mathcal{P}$ si c'est la composée (en série) de portes de la forme $\mathrm{id}_i \times \phi \times \mathrm{id}_j$ avec $\phi \in \mathcal{P}$.

On considère la *porte de Toffoli* $\mathrm{T} : \mathbf{B}^3 \to \mathbf{B}^3$ définie par $\mathrm{T}(x, y, z) = (x, y, xy + z)$.

a. Cette porte est-elle réversible, linéaire, affine ?

b. Montrer qu'elle n'est pas définissable à partir de N, H et K.

On rappelle qu'une permutation est *paire* si elle se décompose en un nombre pair de transpositions. Cette définition ne dépend pas de la décomposition.

c. Montrer que pour toute porte réversible ϕ, les permutations $\phi \times \mathrm{id}_1$ et $\mathrm{id}_1 \times \phi$ sont paires.

d. En déduire que si $\mathcal{P}$ est un ensemble fini de portes réversibles, il existe une porte réversible qui n'est pas définissable à partir de $\mathcal{P}$.