C35211

3è ANNÉE

INFORMATIQUE I

DURÉE : 5 HEURES

Aucun document n'est autorisé

L'usage de toute calculatrice est interdit.

Ce sujet comporte 5 parties. On peut les traiter dans le désordre, en se reportant aux définitions données dans les parties précédentes, et on peut toujours admettre le résultat d'une question précédente.

On aborde ici une théorie combinatoire et algébrique des circuits booléens classiques réversibles.

1 Prélude

Soit un paquet de n cartes (n est pair) dont les positions sont numérotées de 0 (pour la carte inférieure) à $n-1$ (pour la carte supérieure). On le mélange de la façon suivante :

- On le coupe d'abord en deux paquets de même taille : le *paquet inférieur* et le *paquet supérieur* ;
- On intercale ensuite 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 note f_n la permutation de $\{0,\ldots,n-1\}$ 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 paquet 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}.

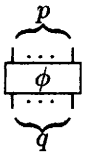
Tournez la page S.V.P.

2 Portes réversibles

On note $\mathbf{B}$ l'ensemble $\{0,1\}$ muni de l'addition $x, y \mapsto x + y \bmod 2$ et de la multiplication $x, y \mapsto xy$. Notez que $\mathbf{B}$ est un corps, et que $x^2 = x$ pour tout $x \in \mathbf{B}$. 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 $\phi : \mathbf{B}^p \to \mathbf{B}^q$. On la 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 $\mathrm{id}_p(x_1, \ldots, x_p) = (x_1, \ldots, x_p)$, 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. Montrer que les portes booléennes à une entrée et une sortie sont de la forme $a + bx$ avec $a, b \in \mathbf{B}$.

d. Montrer que les portes booléennes à deux entrées et une sortie sont de la forme $a + bx + cy + dxy$ avec $a, b, c, d \in \mathbf{B}$.

Si la porte $\phi : \mathbf{B}^p \to \mathbf{B}^q$ est de la forme $\phi(x_1, \ldots, x_p) = (f_1(x_1, \ldots, x_p), \ldots, f_q(x_1, \ldots, x_p))$ où $f_1, \ldots, f_q$ sont des polynômes de degré ≤ 1, on dit qu'elle est *affine*. Si de plus, les polynômes $f_1, \ldots, f_q$ 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 $\phi(x_1, \ldots, x_p) = (x_1 + a_1, \ldots, x_p + a_p)$ avec $a_1, \ldots, a_p \in \mathbf{B}$, on dit que ϕ est une *translation de* $\mathbf{B}^p$.

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

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

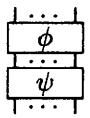
g. En déduire que toutes les portes booléennes réversibles à deux entrées sont affines.

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

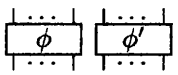
3 Circuits réversibles

Les portes booléennes se composent de deux manières différentes (*en série* ou *en parallèle*) :

- 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 ainsi :



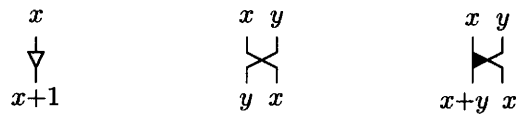
- à partir de $\phi : \mathbf{B}^p \to \mathbf{B}^q$ et $\phi' : \mathbf{B}^{p'} \to \mathbf{B}^{q'}$, on construit la porte $\phi \times \phi' : \mathbf{B}^{p+p'} \to \mathbf{B}^{q+q'}$ telle que $\phi \times \phi'\,(x_1, \ldots, x_p, x'_1, \ldots, x'_{p'}) = (y_1, \ldots, y_q, y'_1, \ldots, y'_{q'})$ 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 ainsi :



Notez qu'on peut *séquentialiser* la composition parallèle : $\phi \times \phi' = (\mathrm{id}_q \times \phi') \circ (\phi \times \mathrm{id}_{p'})$.

Soit $\mathcal{P}$ un ensemble de portes à p entrées et p sorties. On dit que $\mathcal{P}$ *engendre* $\mathcal{Q}$ si $\mathcal{Q}$ est l'ensemble des produits en série d'éléments de $\mathcal{P}$. On a alors $\mathrm{id}_p \in \mathcal{Q}$, car id_p est un produit (vide) d'éléments de $\mathcal{P}$.

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



a. Donner l'ordre et l'inverse de chacune de ces 3 permutations.

b. Montrer que $\{\nu \times \mathrm{id}_1, \mathrm{id}_1 \times \nu\}$ engendre l'ensemble des translations de $\mathbf{B}^2$.

c. Montrer que $\{\sigma, \kappa\}$ engendre l'ensemble des portes linéaires réversibles à deux entrées.

d. En déduire que $\{\sigma, \kappa, \nu \times \mathrm{id}_1\}$ engendre l'ensemble des portes réversibles à deux entrées.

Un *circuit booléen réversible* est une porte réversible $\phi : \mathbf{B}^p \to \mathbf{B}^p$ décomposée comme un produit en série de portes $\mathrm{id}_i \times \alpha \times \mathrm{id}_j$ où chaque α est dans un ensemble donné $\mathcal{P}$ de portes réversibles, par exemple $\mathcal{P} = \{\nu, \sigma, \kappa\}$. On dit alors que la porte réversible ϕ est *définissable à partir de* $\mathcal{P}$.

Un tel circuit peut être interprété comme une permutation d'un paquet de 2^p cartes (voir le prélude).

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



4 Cas linéaire

On rappelle qu'une porte linéaire est définie par une matrice à coefficients dans $\mathbf{B} = \{0, 1\}$.

a. Quelles sont les matrices respectives des portes σ, κ et κ^{-1} définies dans la partie précédente ?

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. Si $1 \leq i \leq p - 1$, on pose $\sigma_i = \mathrm{id}_{i-1} \times \sigma \times \mathrm{id}_{p-i-1}$ et $\kappa_i = \mathrm{id}_{i-1} \times \kappa \times \mathrm{id}_{p-i-1}$. On les représente ainsi :



b. Quelles opérations élémentaires sur les lignes ou les colonnes de A définissent les transformations suivantes ?

$$\phi \mapsto \sigma_i \circ \phi, \qquad \phi \mapsto \kappa_i^{-1} \circ \phi, \qquad \phi \mapsto \phi \circ \sigma_i, \qquad \phi \mapsto \phi \circ \kappa_i^{-1}.$$

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 $\mathrm{id}_1 \times \psi$ avec $\psi : \mathbf{B}^{p-1} \to \mathbf{B}^{p-1}$?

d. Montrer qu'en appliquant des transformations du type $\phi \mapsto \sigma_i \circ \phi$ et $\phi \mapsto \kappa_i^{-1} \circ \phi$, on peut obtenir une matrice dont la dernière colonne est normale.

e. Montrer qu'en appliquant ensuite des transformations du type $\phi \mapsto \phi \circ \sigma_i$ et $\phi \mapsto \phi \circ \kappa_i^{-1}$, on peut obtenir une matrice dont la première ligne et la première colonne sont normales.

f. En déduire que l'ensemble des σ_i et des κ_i engendre l'ensemble des portes linéaires réversibles à p entrées.

g. En déduire une décomposition de la porte $\phi : \mathbf{B}^3 \to \mathbf{B}^3$ définie par la matrice suivante :

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

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

Cette décomposition suggère aussi un algorithme non déterministe pour inverser une matrice carrée A à coefficients dans $\mathbf{B}$. Cet algorithme utilise trois variables de matrices X, Y, Z.

- Initialement, X vaut A et Y, Z valent I (matrice identité à p lignes et p colonnes) ;
- On applique successivement des opérations élémentaires sur les colonnes ou les lignes de X ;
- À chaque fois qu'on applique une opération élémentaire sur des colonnes de X, on applique la même opération élémentaire aux colonnes de Y ;
- À chaque fois qu'on applique une opération élémentaire sur des lignes de X, on applique la même opération élémentaire aux lignes de Z ;
- On s'arrête lorsque X vaut I.

i. Exprimer A^{-1} en fonction de Y et Z à la fin d'un tel calcul.

5 Cas général

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

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

b. Montrer qu'elle n'est pas définissable à partir de $\mathcal{P} = \{\nu, \sigma, \kappa\}$.

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 $\mathcal{P}$.

FIN DE L'ÉPREUVE