Corrigé

1a. Il y en a $n-2$, car seules les 2 positions extrèmes sont inchangées. On en déduit que $k_n \leq (n-2)!$.

1b. Dans ce cas, f correspond à un décalage des chiffres d'un cran vers la gauche, le premier devenant le dernier. On en déduit que $k_{32} = 5$.

2a. Négation : $x+1$. Conjonction : xy. Ou exclusif : $x+y$. Disjonction : $xy+x+y$.

2b. Il y a $(2^q)^{2^p} = 2^{q\times 2^p}$ portes booléennes à p entrées et q sorties, et $2^p!$ portes réversibles à p entrées.

2c. En particulier, il y a $2^2 = 4$ portes booléennes à une entrée et une sortie. Or les 4 fonctions de la forme $a+bx$ avec $a, b \in \mathbf{B}$ sont clairement distinctes. Donc toutes les portes booléennes à une entrée et une sortie sont de cette forme.

2d. De même, il y a $2^4 = 16$ portes booléennes à deux entrées et une sortie. Or les 16 fonctions de la forme $a+bx+cy+dxy$ avec $a, b, c, d \in \mathbf{B}$ sont clairement distinctes. Donc toutes les portes booléennes à deux entrées et une sortie sont de cette forme.

2e. Une matrice à q lignes et p colonnes a pq coefficients. Donc il y a 2^{pq} portes booléennes linéaires à p entrées et q sorties. De même, il y a 2^q translations dans $\mathbf{B}^q$, donc il y a $2^{pq} \times 2^q = 2^{(p+1)q}$ portes booléennes affines à p entrées et q sorties.

2f. Une porte booléenne réversible linéaire est donnée par une matrice carrée d'ordre 2 inversible, ou encore une base de $\mathbf{B}^2$. Or, pour construire une base de $\mathbf{B}^2$, il faut d'abord choisir un vecteur u non nul ($2^2 - 1 = 3$ possibilités) puis un vecteur v non colinéaire à u ($2^2 - 2 = 2$ possibilités). Il y a donc $3 \times 2 = 6$ portes booléennes réversibles linéaires à deux entrées, et $6 \times 4 = 24$ portes booléennes réversibles affines à deux entrées.

2g. Il y a $2^2! = 4! = 24$ portes booléennes réversibles à deux entrées. Donc toutes sont affines.

2h. De même, il y a $(2^3-1)(2^3-2)(2^3-2^2)2^3 = 7\times 6\times 4\times 8$ portes booléennes réversibles affines à trois entrées, et $7\times 6\times 4\times 8 < 2^3! = 8!$. Donc toutes les portes booléennes réversibles à trois entrées ne sont pas affines.

3a. On a $\nu^2 = \nu$, donc ν est d'ordre 2 et $\nu^{-1} = \nu$. De même, $\sigma^2 = \sigma$, donc σ est d'ordre 2 et $\sigma^{-1} = \sigma$. Enfin, $\kappa^3 = \kappa$, donc κ est d'ordre 3, et $\kappa^{-1} = \kappa^2$ est la porte définie par $\kappa^{-1}(x, y) = (y, x+y)$.

3b. Les translations de $\mathbf{B}^2$ sont id_2, $\nu\times\mathrm{id}_1$, $\mathrm{id}_1\times\nu$, et $\nu\times\nu = (\nu\times\mathrm{id}_1)\circ(\mathrm{id}_1\times\nu)$. Donc $\{\nu\times\mathrm{id}_1, \mathrm{id}_1\times\nu\}$ engendre l'ensemble des translations de $\mathbf{B}^2$.

3c. Comme σ est d'ordre 2 et κ est d'ordre 3, l'ensemble des produits en série d'éléments de $\{\sigma, \kappa\}$ est un groupe d'ordre au moins 6. Or il n'y a que 6 portes booléennes réversibles linéaires à deux entrées. Donc $\{\sigma, \kappa\}$ engendre l'ensemble des portes linéaires réversibles à deux entrées.

3d. On en déduit que $\{\sigma, \kappa, \nu\times\mathrm{id}_1, \mathrm{id}_1\times\nu\}$ engendre l'ensemble des portes réversibles affines à deux entrées, c'est-à-dire l'ensemble des portes réversibles à deux entrées (d'après la question 2g.). Donc $\{\sigma, \kappa, \nu\times\mathrm{id}_1\}$ engendre l'ensemble des portes réversibles à deux entrées, car $\mathrm{id}_1\times\nu = \sigma\circ(\nu\times\mathrm{id}_1)\circ\sigma$.

3e. Le premier circuit correspond à la coupe *équilibrée*, c'est-à-dire par le milieu du paquet, et le second au mélange défini dans le prélude.

4a. Les matrices respectives des portes σ, κ et κ^{-1} sont $\begin{pmatrix}0&1\\1&0\end{pmatrix}$, $\begin{pmatrix}1&1\\1&0\end{pmatrix}$ et $\begin{pmatrix}0&1\\1&1\end{pmatrix}$.

4b. La transformation $\phi \mapsto \sigma_i \circ \phi$ revient à échanger la ligne i avec la ligne $i+1$. La transformation $\phi \mapsto \kappa_i^{-1} \circ \phi$ revient à remplacer la ligne i par la ligne $i+1$ et la ligne $i+1$ par la somme des deux lignes. Les deux autres transformations correspondent aux opérations analogues sur les colonnes.

4c. La porte ϕ est de la forme $\mathrm{id}_1 \times \psi$ avec $\psi : \mathbf{B}^{p-1} \to \mathbf{B}^{p-1}$ si la première ligne et la première colonne de A sont normales.

4d. Comme A est inversible, sa dernière colonne est non nulle. Soit i l'indice du dernier coefficient non nul (c'est-à-dire égal à 1) dans cette colonne. Si $i = 1$, la colonne est normale. Supposons donc que $i > 1$. Si le coefficient précédent est nul, on applique la transformation $\phi \mapsto \sigma_{i-1} \circ \phi$, sinon on applique la transformation $\phi \mapsto \kappa_{i-1}^{-1} \circ \phi$, de sorte que l'indice du dernier coefficient non nul devient $i-1$. On continue ainsi jusqu'à ce que la dernière colonne soit normale.

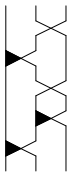
4e. On considère maintenant la première ligne : l'indice j du dernier coefficient non nul vaut alors p. Si le coefficient précédent est nul, on applique la transformation $\phi \mapsto \phi \circ \sigma_{j-1}$, sinon on applique la transformation $\phi \mapsto \phi \circ \kappa_{j-1}^{-1}$, de sorte que l'indice du dernier coefficient non nul devient $j-1$. On continue ainsi jusqu'à ce que la première ligne soit normale. On remarque que la dernière colonne est passée à la première place. Autrement dit, la première colonne est aussi normale.

4f. On a donc $\gamma \circ \phi \circ \delta = \mathrm{id}_1 \times \psi$ avec $\psi : \mathbf{B}^{p-1} \to \mathbf{B}^{p-1}$, où γ et δ sont des produits en séries de σ_i et de κ_i^{-1}. Donc $\phi = \gamma^{-1} \circ (\mathrm{id}_1 \times \psi) \circ \delta^{-1}$ où γ^{-1} et δ^{-1} sont des produits en séries de σ_i et de κ_i. On applique le même raisonnement à ψ, et par récurrence sur p, on en déduit que l'ensemble des σ_i et des κ_i engendre l'ensemble des portes linéaires réversibles à p entrées.

4g. On applique les transformations suivantes :

$$\begin{pmatrix}0&1&1\\1&0&1\\0&1&0\end{pmatrix} \to \begin{pmatrix}1&0&1\\1&1&0\\0&1&0\end{pmatrix} \to \begin{pmatrix}1&1&0\\1&0&1\\0&0&1\end{pmatrix} \to \begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix} \text{ puis } \begin{pmatrix}1&1\\0&1\end{pmatrix} \to \begin{pmatrix}0&1\\1&0\end{pmatrix} \to \begin{pmatrix}1&0\\0&1\end{pmatrix}.$$

On en déduit la décomposition suivante pour la porte ϕ :



4h. Dans le pire des cas, la longueur de la décomposition vaut $p(p-1)$ (par exemple 6 en dimension 3).

4i. À chaque étape, on a $X = ZAY$. À la fin, on a donc $\mathrm{I} = ZAY$, d'où $A^{-1} = YZ$.

5a. τ est réversible car $\tau^2 = \mathrm{id}_3$, mais elle n'est ni linéaire, ni affine (à cause du monôme xy).

5b. Toutes les portes définissables à partir de $\mathcal{P} = \{\nu, \sigma, \kappa\}$ sont affines. Donc τ n'est pas définissable à partir de $\mathcal{P}$.

5c. Si ϕ est une transposition, on voit aisément que $\phi \times \mathrm{id}_1$ est le produit de 2 transpositions. En général, si ϕ est le produit de n transpositions, alors $\phi \times \mathrm{id}_1$ est le produit de $2n$ transpositions, donc elle est paire. Idem pour $\mathrm{id}_1 \times \phi$.

5d. Si $\mathcal{P}$ est un ensemble fini de portes réversibles, et q est strictement plus grand que le nombre d'entrées de chaque porte de $\mathcal{P}$, alors toute porte à q entrées qui est définissable à partir de $\mathcal{P}$ est un produit de permutations de la forme $\phi \times \mathrm{id}_1$ ou $\mathrm{id}_1 \times \phi$, donc elle définit une permutation paire. En particulier, les transpositions de $\mathbf{B}^q$ ne sont pas définissables à partir de $\mathcal{P}$. C'est le cas, par exemple, de la porte de Toffoli si $\mathcal{P} = \{\nu, \sigma, \kappa\}$.