

Un code correcteur d'erreurs

Roland Gillard

13 novembre 2000

On considère une suite de quinze octets. En lui associant une suite de seize octets, on montre qu'il est possible de détecter et de corriger *une* erreur de transmission sur la suite de seize octets, de façon à pouvoir reconstituer la suite initiale de quinze octets. Ce système est utilisé pour les transmissions par minitel.

1 Description de la méthode

On représente les suites d'octets par des polynômes à coefficients dans $\mathbb{F}_2[X]$. On part d'un polynôme de degré inférieur à 119 (correspondant à une suite de 15 octets). On lui associe un polynôme de degré inférieur ou égal à 126 par la formule

$$T(X) = X^7 P(X) + R(X) ,$$

où $R(X)$ désigne le reste de la division de $X^7 P(X)$ par $A(X) = X^7 + X^3 + 1$: c'est le polynôme qu'on transmet. Comme $R(X) + R(X) = 0$ dans $\mathbb{F}_2[X]$, on obtient:

Lemme 1.1 *Le reste de la division de $T(X)$ par $A(X)$ est nul.*

Supposons l'existence d'une *unique* erreur sur $T(X)$: ainsi $T(X)$ est remplacé par $T'(X) = T(X) + X^m$ avec $0 \leq m \leq 126$ et le reste de la division du polynôme $T'(X)$ par $A(X)$ est égal d'après le lemme au reste de X^m .

Théorème 1.2 *L'application qui, à m vérifiant $0 \leq m \leq 126$, associe le reste de la division de X^m par $X^7 + X^3 + 1$ est injective.*

Ainsi s'il y a 0 ou 1 erreur dans la transmission de $T(X)$, on peut rétablir la valeur initiale de $T(X)$ et récupérer $P(X)$ en effectuant la division par X^7 . Il est facile (exercice!) d'écrire un programme pour déterminer m connaissant le reste de la division de X^m par $X^7 + X^3 + 1$.

2 Démonstration du théorème

Proposition 2.1 *Le polynôme $A(X) \in \mathbb{F}_2[X]$ est irréductible. Le groupe multiplicatif de $\mathbb{F}_2[X]/(A(X))$ est cyclique engendré par la classe x de X .*

Le théorème en résulte immédiatement. Il suffit de montrer le premier point car $2^7 - 1 = 127$ est premier.

2.1 Démonstration de la proposition

Soit x une racine de $A(X)$ dans une extension convenable de \mathbb{F}_2 . Si $X^7 + X^3 + 1$ est réductible et si x a été bien choisi, x engendre une extension de degré 1, 2 ou 3. On a donc $x^m = x$ avec $m = 2, 4$ ou 8. Ainsi les polynômes $A(X)$ et $X^m - 1$ ($m = 1, 3$ ou 7) ont un facteur commun dans $\mathbb{F}_2[X]$; en utilisant l'algorithme d'Euclide, on vérifie très rapidement que ce n'est pas le cas.