Codage de Hamming

La transmission d'informations numériques par ligne téléphonique, fibre optique, etc... se fait par l'envoi successif de bits égaux à 0 ou 1. Cette transmission peut être parasitée ce qui conduit à une inversion de certains bits (le taux d'erreur est de l'ordre de 10^{-5} sur une ligne téléphonique et de 10^{-11} en fibre optique) Sans contrôle, l'information est alors irrémédiablement altérée. Voyons différents schémas transformant un message donné en un message «contrôlé» permettant de détecter la présence d'erreurs, voire de corriger celles-ci.

Bit de parité

On sectionne l'information à transmettre en paquets de n bits, correspondant aux messages. A un message donné on forme le message contrôlé en ajoutant un $n+1$ ème bit de sorte qu'il y ait en tout un nombre de pair de 1. Cet $n+1$ème bit est appelé bit de parité. Concrètement :

$0\ \ 1\ \ 0\ \ 1\ \ 1\ \ 1\ \ 0$ devient $0\ \ 1\ \ 0\ \ 1\ \ 1\ \ 1\ \ 0 \mid 0$ et

$1\ \ 0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0$ devient $1\ \ 0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0 \mid 1$.

L'émetteur transmet alors le message contrôlé puis le récepteur vérifie la parité du message reçu.

Si lors de la transmission une erreur survient, la parité du message reçu est incorrecte et le récepteur décèle l'existence d'une erreur sans pour autant être capable de la localiser. Il demande alors une nouvelle émission du message.

Si lors de la transmission deux erreurs surviennent, la parité du message reçu est correcte, les erreurs ne sont pas décelées...

Tableau de parité

L'information à transmettre est ici découpée en paquets de n^2 bits que l'on organise sous la forme d'un tableau à n lignes et n colonnes. Ce tableau constitue notre message. Pour le contrôler, on y ajoute une $n+1$ème ligne et une $n+1$ème colonne de sorte que chaque ligne et chaque colonne présentent un nombre pair de 1. Ainsi les n premiers coefficients de la dernière ligne (resp. colonne) contrôlent la parité de la colonne (resp. ligne) qui lui correspond. Le dernier coefficient, quant à lui, contrôle à la fois la parité de la $n+1$ème ligne et de la $n+1$ème colonne (en fait, il contrôle même la parité du tableau initial).

Concrètement : $\begin{array}{ccc} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{array}$ devient $\begin{array}{ccc|c} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ \hline 0 & 0 & 1 & 1 \end{array}$

Si lors de la transmission du message ainsi contrôlé une erreur survient, le récepteur détecte une erreur de parité en ligne et une erreur de parité en colonne. Le bit erroné est alors repéré et il suffit alors de l'inverser pour le corriger. Notons que ceci fonctionne même si c'est l'un des bits de parité qui est erroné.

Si deux erreurs de transmission sont commises, il y aura, selon leur positionnement, deux ou quatre erreurs de parité. L'existence d'erreurs est détectée, mais on ne pourra pas les corriger.

Si trois erreurs sont commises, on peut détecter encore leur présence par la parité globale.

Si quatre erreurs sont commises et si celles-ci sont malicieusement positionnées sur deux même lignes et deux même colonnes on ne les détecte pas.

Codage de Hamming

Le message contrôlé comporte ici 2^n bits. Concrètement nous allons prendre $n=3$, même si une valeur supérieure paraît nécessaire pour percevoir l'efficacité de la méthode. Nous allons donc transmettre un octet dont les bits seront numérotés de 0 à 7 en allant de droite à gauche.

Le bit 0 va contrôler la parité de l'octet.

Les bits $1,2,4$ (correspondant aux puissances de 2) seront les bits de contrôle de notre message.

Les bits $3,5,6,7$ (les autres) seront les bits contenant l'information transmise. On décompose leur numéro en puissance de 2 : $3 = 2 + 1, 5 = 4 + 1, 6 = 4 + 2$ et $7 = 4 + 2 + 1$. Ensuite, on détermine les bits de contrôles $1,2,4$ de sorte que chacun complète la parité de l'ensemble des bits d'information où ils apparaissent dans la décomposition en puissance de 2.

Concrètement, on veut transmettre $1 \quad 1 \quad 0 \quad 1$.

On forme d'abord : $\dfrac{7 \quad 6 \quad 5 \quad 4 \quad 3 \quad 2 \quad 1 \quad 0}{1 \quad 1 \quad 0 \qquad\ 1 \qquad\qquad\quad}$

Puis on détermine le bit 1 de la manière suivante : 1 apparaît dans la décomposition des nombres $3,5$ et 7, il va donc contrôler la parité de ces trois bits et ici valoir 0.

De même le bit 2 contrôle $3,6$ et 7, il vaut donc ici 1, etc...

Finalement le message contrôlé est $\dfrac{7 \quad 6 \quad 5 \quad 4 \quad 3 \quad 2 \quad 1 \quad 0}{1 \quad 1 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 0}$.

Si lors de la transmission, une erreur est commise, on en détecte l'existence par l'imparité du message transmis, on contrôle ensuite la parité des bits $1,2$ et 4.

Par exemple si l'erreur est commise sur le bit 5, les bits 1 et 4 sont incorrects. Or $1 + 4 = 5$. C'est donc le bit 5 qui est faux.

Si l'erreur est commise sur le bit 2, seule la parité de celui-ci est incorrecte.

Si l'erreur est commise sur le bit 0, aucun bit de contrôle n'est incorrect.

A chaque fois la somme des numéros des bits de contrôles incorrects donne le bit erroné. Il ne reste alors plus qu'à l'inverser.

Si deux erreurs sont commises, la parité du message reçu est correcte mais assurément 1 ou plusieurs bits de contrôle ne le sont pas. L'existence d'erreur est détectée. Notons qu'une erreur sur les bits 1 et 2 ou sur les bits 5 et 6 conduisent aux même erreurs de parité. On ne saura donc pas corriger.

Efficacité

Etudions le rapport entre les tailles de l'information transmise et de l'information de contrôle.

Tableau de parité : $(2n+1)\big/(n+1)^2$.

Codage de Hamming : $(n+1)\big/2^n$ (les bits de contrôles correspondent aux puissances de 2 strictement inférieure à 2^n : il y en a n, on y ajoute aussi le bit de parité).

Pour une transmission de 128 bits, le tableau de parité nécessite 31 bits de contrôle contre 9 au codage de Hamming.