Pour en savoir plus sur les mathématiques du

Signal du GPS

Chaque satellite envoie au GPS un signal, composé de 0 et de 1, qui semble complètement aléatoire. Avec ce signal, le GPS calcule sa distance au satellite.

Christiane Rousseau
Université de Montréal

Le signal d'un satellite est une suite de M chiffres, 0 et 1, et il est répété périodiquement. On appelle ces chiffres des bits. Le récepteur du GPS connaît les signaux de chacun des satellites. Il génère un signal et le compare au signal reçu.

Pour comparer deux fenêtres de M bits le récepteur calcule le nombre de bits en accord moins le nombre de bits en désaccord. Cette différence est appelée *corrélation* entre les deux signaux.

Comparons les deux signaux de 15 bits suivants :

0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1
0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0

Leur corrélation est –1 car ils coïncident aux bits de même couleur, soit sur 7 positions et diffèrent aux 8 autres positions. Si la corrélation est M, soit le nombre total de bits, le récepteur conclut que les deux signaux sont les mêmes. Sinon, il translate le signal qu'il émet et recalcule la corrélation.

Il fait de même avec tous les signaux des satellites et leurs translatés jusqu'à ce qu'il trouve 4 translations des signaux de 4 satellites qui ont une corrélation de M avec 4 signaux qu'il génère. Le récepteur sait à quel instant le cycle du signal de chaque satellite commence. Il sait de combien il a dû translater le signal qu'il génère pour trouver une corrélation égale à M. C'est à partir de cette translation qu'il mesure le temps de parcours du signal d'un satellite jusqu'à lui.

Il y a toujours des erreurs dans la transmission des signaux.

Malheureusement, il y a toujours des erreurs dans la transmission des signaux et le récepteur doit pouvoir corriger les erreurs de transmission.

Pour pouvoir corriger les erreurs, les signaux reproduits par le GPS doivent être très mal corrélés entre eux et très mal corrélés avec une translation d'eux-mêmes. Ainsi, toute corrélation très proche de M va être interprétée comme le fait que le récepteur a bien identifié le signal. Par contre, dans l'exemple des deux signaux de 15 bits, s'il y a une ou deux erreurs dans la transmission d'un des signaux, il est difficile de le confondre avec l'autre.

Registre à décalage

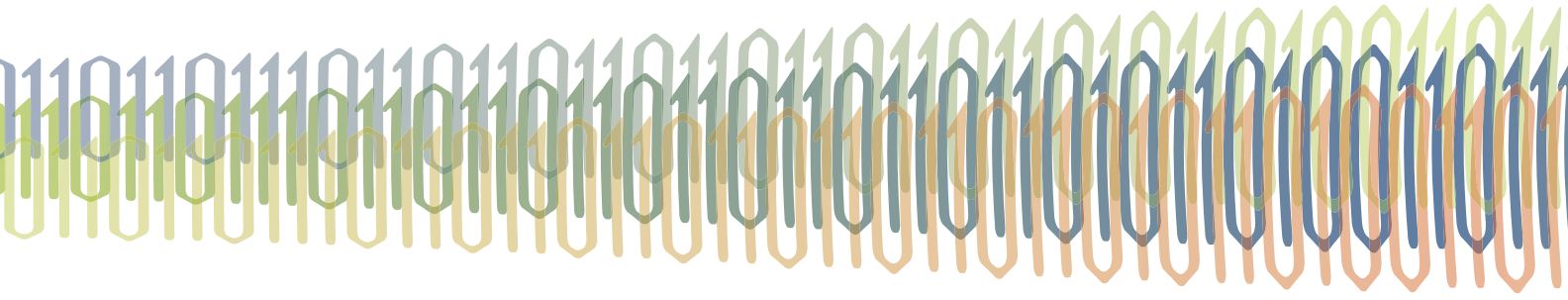
Les signaux sont générés par un registre à décalage (**figure 1**) qui fonctionne comme suit. Pour générer une suite $\{a_n\}$, on choisit d'abord des nombres $q_0, \ldots, q_{r-1}$ dans l'ensemble $\{0, 1\}$. On choisit ensuite les r premiers éléments de la suite à engendrer, soit $\{a_0, \ldots, a_{r-1}\}$, où chaque $a_i \in \{0,1\}$ et on détermine alors :

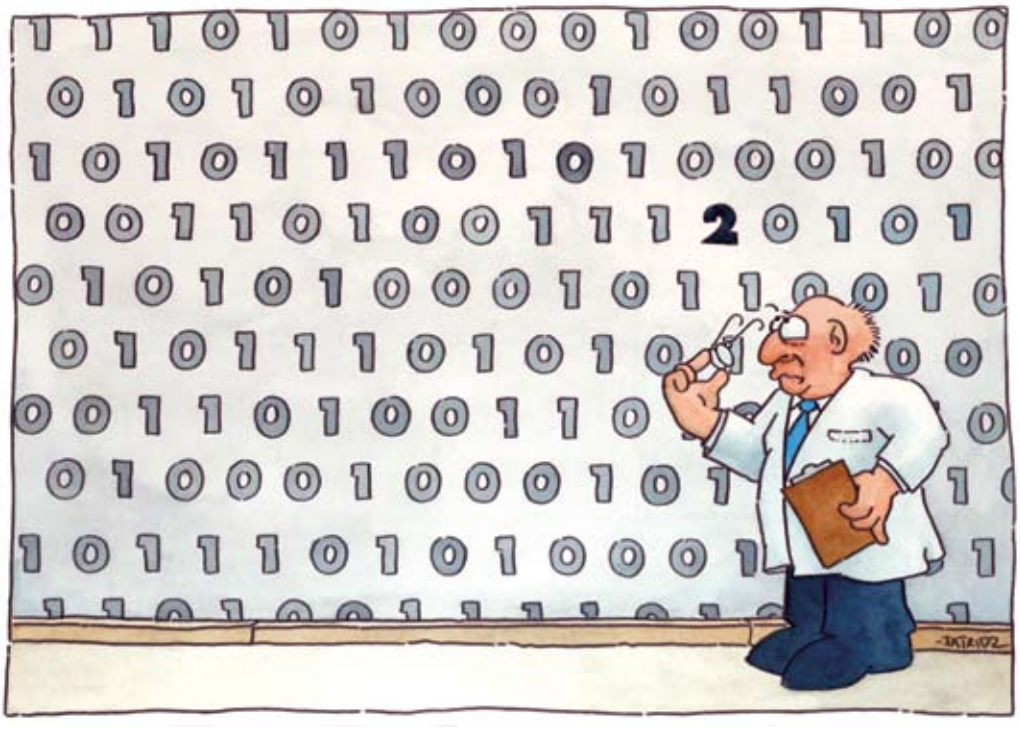
$$a_r = q_0\, a_0 + \ldots + q_{r-1}\, a_{r-1}$$

où l'addition et la multiplication sont définies à la **figure 2** et sont appelées addition et mulitiplication modulo 2.

Le registre enlève a_0, décale $a_1, \ldots, a_{r-1}$ vers la droite et inscrit a_r à gauche. On itère le procédé : si $a_{n-r}, \ldots, a_{n-1}$ sont les entrées dans le registre, alors celui-ci calcule :

$$a_n = q_0\, a_{n-r} + \ldots + q_{r-1}\, a_{n-1}$$





Copyright © Images.com/Corbis

Toute la problématique est donc de bien choisir $q_0, \ldots, q_{r-1}$ et les $a_0, \ldots, a_{r-1}$ pour obtenir des suites qui ont les propriétés recherchées, à savoir être mal corrélées entre elles et mal corrélées avec une translation d'elle-même.

Les registres à décalage bien initialisés peuvent produire des suites avec des propriétés remarquables. Examinons le résultat suivant.

Résultat :

Il existe des nombres $q_0, \ldots, q_{r-1}$ et des conditions initiales $a_0, \ldots, a_{r-1}$ tels que la suite $\{a_n\}$ générée par le registre à décalage est de période exactement $M = 2^r - 1$ et tels que la corrélation de deux fenêtres de la suite de longueur M soit exactement -1 sauf si les deux fenêtres sont espacées d'un nombre entier de périodes.

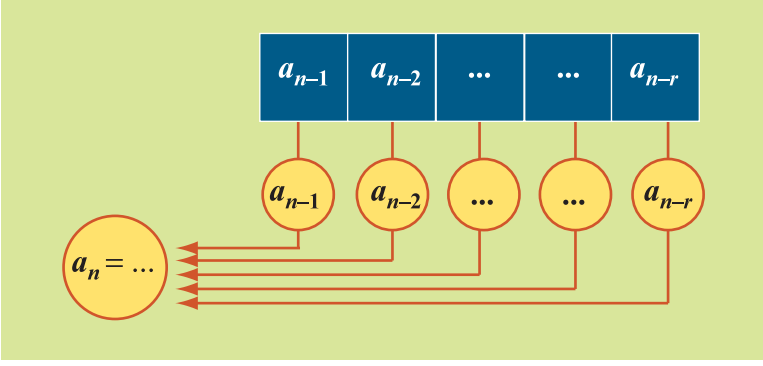


Figure 1 : *Un registre à décalage*

Addition	Multiplication
$0+0=0$	$0\times 0=0$
$0+1=1$	$0\times 1=0$
$1+0=1$	$1\times 0=0$
$1+1=0$	$1\times 1=1$

Figure 2 : *Opérations en binaire*

Signification du résultat :

Le théorème affirme que le registre bien initialisé va produire une suite périodique de période impaire $M = 2^k - 1$. Deux fenêtres de longueur M diffèrent sur exactement 2^{k-1} entrées (sauf si elles sont décalées d'un nombre entier de périodes). C'est un résultat très fort! Si M est grand, les chances sont en effet pratiquement nulles pour qu'on puisse confondre une suite avec une de ses translatées. Quant à la génération de deux suites différentes attachées à deux satellites différents, il n'existe pas encore de méthode aussi performante mais la recherche se poursuit. La preuve du résultat fait appel aux corps finis; nous ne la présenterons pas.

Comment construit-on les nombres $q_0, \ldots, q_{r-1}$ et les conditions initiales $a_0, \ldots, a_{r-1}$ qui garantissent une suite très mal corrélée avec elle-même? Nous allons expliquer les idées de la construction, sans toutefois donner la justification. Nous choisissons un polynôme

$$Q(x) = x^r + q_{r-1}\, x^{r-1} + \ldots + q_1\, x - q_0$$

dont les coefficients, c'est-à-dire les nombres $q_0, \ldots, q_{r-1}$, sont toujours, soit 0, soit 1. Sur $\{0, 1\}$ nous introduisons l'addition et la multiplication modulo 2. Nous avons donc les règles d'addition et de multiplication de la **figure 2**.

La condition sur $q_0, \ldots, q_{r-1}$ est que le polynôme $Q(x)$ soit irréductible, i.e. qu'il ne puisse se factoriser comme produit de deux polynômes de degré plus petit que r. Attention ! Dans la multiplication de deux polynômes on utilise toujours l'addition et la multiplication définies à la **figure 2**.

Voyons quels sont les polynômes irréductibles de degré 1, 2, 3.

Polynômes de degré 1 :

$$x,$$
$$x + 1$$

Ils sont tous deux irréductibles;

Polynômes de degré 2 :

$$x^2,$$
$$x^2 + 1,$$
$$x^2 + x,$$
$$x^2 + x + 1$$

Enlevons de ce groupe les polynômes réductibles, à savoir :

$$x \cdot x = x^2,$$
$$x \cdot (x + 1) = x^2 + x,$$
$$(x + 1) \cdot (x + 1) = x^2 + x + x + 1$$
$$= x^2 + x(1 + 1) + 1 = x^2 + 1$$

Il ne reste plus que $x^2 + x + 1$, qui est le seul polynôme irréductible de degré 2.

Polynômes de degré 3 :

$$x^3,$$
$$x^3 + 1,$$
$$x^3 + x,$$
$$x^3 + x + 1,$$
$$x^3 + x^2,$$
$$x^3 + x^2 + 1,$$
$$x^3 + x^2 + x,$$
$$x^3 + x^2 + x + 1$$

Enlevons de ce groupe les polynômes réductibles en étant un peu astucieux : si le polynôme est un produit de deux polynômes de degré plus petit, nécessairement l'un des deux est un polynôme de degré 1, soit x ou $x + 1$. Si x divise le polynôme celui-ci n'a pas de terme constant. Donc les polynômes x^3, $x^3 + x$, $x^3 + x^2$, $x^3 + x^2 + x$ sont réductibles. Parmi les quatre polynômes restants on doit enlever ceux qui sont divisibles par $x + 1$. Mais $x + 1$ a pour racine 1 car $1 + 1 = 0$. Donc les polynômes restants sont réductibles s'ils s'annulent en $x = 1$. C'est le cas de $x^3 + 1$, $x^3 + x^2 + x + 1$. Il nous reste donc deux polynômes irréductibles de degré 3 : $x^3 + x + 1$ et $x^3 + x^2 + 1$.

Polynômes de degré supérieur :

On peut utiliser un ordinateur pour nous aider à les trouver. Dans le cas du polynôme $x^4 + x + 1$ on vérifie facilement qu'il est irréductible car il ne s'annule pas en 0 et 1, donc il n'a pas de facteur de degré 1, et il ne s'écrit pas comme $(x^2 + x + 1)^2$, la seule décomposition possible en un produit de deux polynômes irréductibles de degré 2.

Il faut maintenant choisir les $a_0, \ldots, a_{r-1}$. Plusieurs suites conviennent dont la plus simple est la suite dont les $r - 1$ premiers termes sont des 0 et le r^e terme est 1 (**figure 3**).

$$\underbrace{0, 0, 0, \ldots,}_{r-1 \text{ bits}} 1$$

Figure 3 : *Les conditions initiales.*

Exemple :

Regardons la suite générée avec le polynôme $x^4 + x + 1$, soit $(q_0, q_1, q_2, q_3) = (1, 1, 0, 0)$ et les conditions initiales $a_0 = 0$, $a_1 = 0$, $a_2 = 0$, $a_3 = 1$. Vous pouvez vérifier que ceci génère la suite périodique de période $15 = 2^4 - 1$:

$$\underbrace{0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1,}_{15 \text{ bits}} 0, 0, 0, 1, 0, 0, 1, \ldots$$

Même si nous générons une suite infinie nous ne regardons que des fenêtres de longueur 15. Nous allons maintenant faire les 14 translations de cette fenêtre et calculer la corrélation dans chaque cas.

Translation de 1 :

C'est comme si on avait envoyé le premier 0 à la fin :

$$0, \underbrace{0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0,}_{15 \text{ bits}} 0, 0, 1, 0, 0, 1, \ldots$$

On voit que les deux fenêtres diffèrent aux positions : 3, 4, 6, 8, 9, 10, 11, 15, soit en 8 positions et concordent aux 7 positions restantes, soit une corrélation de –1, telle que prédite par le résultat.

Translation de 2 :

C'est comme si on avait envoyé les deux premiers 0 à la fin :

$$0, 0, \underbrace{0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0,}_{15 \text{ bits}} 0, 1, 0, 0, 1, \ldots$$

Ici encore la suite diffère en 8 positions de la suite initiale et concorde en 7 positions, soit une corrélation de –1.

Pour calculer la corrélation avec les autres fenêtres on écrit directement ces fenêtres en dessous de la première fenêtre (**figure 4**).

Dans chaque cas on vérifie que la corrélation entre chaque ligne et la première ligne est –1. En fait, il se trouve que la corrélation entre deux lignes quelconques est également –1.

Remarque : si l'on regarde ce qu'on a fait on aurait pu utiliser chacune des fenêtres de longueur 4 de notre suite comme conditions initiales au lieu de $a_0 = 0$, $a_1 = 0$, $a_2 = 0$, $a_3 = 1$, c'est-à-dire n'importe quelle suite de longueur 4, sauf la suite 0, 0, 0, 0. Ceci est vrai en général et pas seulement dans notre exemple : c'est une conséquence du résultat que nous venons de voir disant que la période est exactement $2^r - 1$.

0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1
0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0
0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0,	0
1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0,	0,	0
0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0,	0,	0,	1
0,	1,	1,	0,	1,	0,	1,	1,	1,	1,	0,	0,	0,	1,	0
1,	1,	0,	1,	0,	1,	1,	1,	1,	0,	0,	0,	1,	0,	0
1,	0,	1,	0,	1,	1,	1,	1,	0,	0,	0,	1,	0,	0,	1
0,	1,	0,	1,	1,	1,	1,	0,	0,	0,	1,	0,	0,	1,	1
1,	0,	1,	1,	1,	1,	0,	0,	0,	1,	0,	0,	1,	1,	0
0,	1,	1,	1,	1,	0,	0,	0,	1,	0,	0,	1,	1,	0,	1
1,	1,	1,	1,	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0
1,	1,	1,	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1
1,	1,	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1
1,	0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1
0,	0,	0,	1,	0,	0,	1,	1,	0,	1,	0,	1,	1,	1,	1

Figure 4 : *Les suites obtenues par translation. Les bits de couleur rouge sont ceux en désaccord avec la suite de la première ligne.*