Transformation de Walsh

19 novembre 2013

Résumé

Dans le cours, nous avons décrit une méthode de décodage basée sur la transformation de Walsh. Il s'agit de l'implanter et de tester ses limites.

1 Transformées de Fourier-Hadamard-Walsh

Soit m un entier positif. On rappelle que le coefficient de Walsh en $a \in \{0,1\}^m$ d'une fonction booléenne f est :

$$f^\star(a) = \sum_{x \in \{0,1\}^m} (-1)^{f(x)+a.x}$$

Plus généralement, le coefficient de Fourier-Hadamard-Walsh en $a \in \{0,1\}^m$ d'une application complexe F est :

$$\hat{F}(a) = \sum_{x \in \{0,1\}^m} F(x)(-1)^{a.x}$$

Pour $(a,b) \in \{0,1\}^m \times \{0,1\}$, on note $\phi_{a,b}$ la fonction affine :

$$\phi_{a,b}(x) = a.x + b = a_1x_1 + \cdots + a_mx_m + b.$$

les opérations sont faites modulo 2.

1. Implanter le calcul de la transformée de Fourier-Hadamard `void FH(int *f, int n)` d'une application intégrale.
2. Implanter le calcul `int* walsh(int *t, int n)` de la la transformation de Walsh d'une application booléenne.
3. Implanter `int scal(x,y)` pour calculer $x.y$ dans $\{0,1\}^m$, puis `int* phi(int a, int b, ...)` qui calcule la table de vérité de $\phi_{a,b}$.
4. Vérifier le bon fonctionnement en appliquant la transformation de Walsh aux fonctions $\phi_{a,b}$.
5. Vérifier le bon fonctionnement en utilisant le caractère involutif de la transformation de Fourier-Hadamard.

2 Codage-Décodage

Les vecteurs de $m+1$ bits sont codés par des mots de 2^m bits par l'application

$$(a, b) \mapsto [ax + b]_{0 \leq x < 2^m}$$

qui envoie (a, b) sur la table de vérité de $\phi_{a,b}$. Il s'agit du codage de Reed-Müller affine utilisé notamment dans les années 70 par la sonde Mariner.

1. Ecrire un programme de codage de fichiers textes.
2. Un simulateur canal bruité symétrique binaire de probabilité de transition donnée.
3. Ecrire un décodeur basé sur la transformation de Walsh..
4. Tester la chaine codage/bruit/décodage au moyen d'un tube `unix`.

```
cat file | code -cm5 | canal -p0.01 | code -dm5
```

5. Faire une expérience analogue avec les fichiers bitmaps.

3 Forme algébrique

Soit $u \in \{0, 1\}^m$, on note :

$$X^u : x \mapsto x^u := \prod_{i=0}^{m-1} x_i^{u_i}$$

Toute application booléennes possède une et une seule représentattion polynomiale, la forme algébrique normale :

$$f(x) = \sum_u a_u X^u, \quad a_u \in \{0, 1\}^m.$$

1. Ecrire une fonction `void anf(int *f,int n)` qui calcule les coefficients de la représentation polynomiale de f.
2. L'application est involutive, vérifier le bon fonctionnement de l'implantation.

4 Décodage linéaire

Le décodage basé sur la transformation de Walsh est de complexité $\mathrm{O}(n \log n)$, il n'est pas optimal ! Utiliser l'algorithme de décodage linéaire décrit sur le site acrypta de Robert Rolland.