Feuille TD 6 - Codage de canal - Entropie - Compression

Dans un casino, on joue au 421. Le casino possède un serveur centralisé qui enregistre tous les lancers de dés effectués sur chaque table de jeu. À chaque table, un croupier transmet -par infrarouge- les séquences de dés au serveur. Le problème est de mettre en place une architecture permettant de réaliser la transmission fiable et sécurisée des informations.

Construction d'un code de Reed-Solomon adapté

La liaison infrarouge est modélisée par un canal binaire symétrique de probabilité d'erreur 0.001. On désire ici assurer des transmissions fiables sur ce canal.

1. Quelle est la probabilité p d'erreur lorsqu'on envoie un octet ?

Rappel. Soit α un élément primitif du corps $V = \mathbb{F}_q$.
On rappelle que les codes de Reed-Solomon sont des codes cycliques sur V de de longueur $n = q - 1$ dont le polynôme générateur g de degré r est de la forme :

$$g(X) = \prod_{i=s}^{s+r-1} (X - \alpha^i) .$$

Le code de Reed-Solomon ainsi obtenu est donc un code $(n = q-1, k = n-r = q-1-r)$ avec r arbitraire. Ce code est de distance $r+1$ [cf polycopié].
En choisissant r, on peut donc construire un code de distance arbitraire, donc de taux de correction arbitraire.

2. Pour remédier aux erreurs dues au canal, lorsqu'on envoie n octets, on veut garantir de corriger jusqu'à $p \times n$ erreurs. Expliquer comment construire un code correcteur de type Reed-Solomon en précisant :

a. le corps de base et la valeur choisie pour n;

b. le degré du polynôme générateur et le rendement du code.

c. le nombre maximal d'erreurs détectées;

d. la dimension d'une matrice génératrice du code. Comment s'écrit cette matrice à partir des coefficients du polynôme générateur ?

Pour $d = 3, .., 10$, les polynômes suivants à coefficients dans $\mathbb{F}_2$ sont primitifs :

degré d	Polynôme primitif
3	$1 + \alpha + \alpha^3$
4	$1 + \alpha + \alpha^4$
5	$1 + \alpha^2 + \alpha^5$
6	$1 + \alpha + \alpha^6$

degré d	Polynôme primitif
7	$1 + \alpha^3 + \alpha^7$
8	$1 + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^8$
9	$1 + \alpha^4 + \alpha^9$
10	$1 + \alpha^3 + \alpha^{10}$

e. donner le polynôme utilisé pour implémenter le corps de base et expliquer brièvement comment réaliser les opérations d'addition et de multiplication;

f. donner l'expression du polynôme générateur en fonction de α.

3. Calculer la capacité du canal. Comparer au rendement du code proposé.

Sécurisation des communications

4. Comment coder les séquences de dés pour garantir qu'il n'y ait pas de trucages sans consentement d'un croupier ?

Codage des lancers

On suppose les dés du casino non pipés. On cherche à coder les séquences de tirages sur le canal binaire :

1. Quelle est l'entropie d'un dé ?
2. Proposer un algorithme de codage où les mots de code sont de même longueur.
3. Calculer la longueur moyenne de ce codage.
4. Proposer un codage de Huffman.
5. Ce codage est-il optimal ? Si non, proposer un codage plus performant.