Intégration des codes correcteurs

Durée : 1 heure 30. Tous documents et calculatrices autorisés.

Exercice A. Entrelacement de 2 codes

On s'intéresse à la construction d'un code permettant de corriger des rafales d'erreurs avec une faible probabilité de de mauvaise correction sur un canal de communication où les blocs sont de 64 octets (512 bits).

Pour cela, on entrelace deux codes C_1 et C_2, en choisissant $C_2(64, 60, 5)$ sur $\mathbb{F}_{256}$.

1. Comment peut-on construire un tel code $C_2(64, 60, 5)$?

2. Expliquer rapidement comment l'utilisation en séquence des deux codes C_1 et C_2 permet de limiter la probabilité de mauvaise correction.

3. Quelles caractéristiques choisissez-vous pour C_1 ?

4. Quels profondeur et retard choisissez-vous pour la table d'entrelacement ?

5. Donner la longueur (en nombre de bits) des rafales qui peuvent être garanties corrigées.

6. Décrire rapidement les étapes du codage.

7. Décrire rapidement les étapes du décodage avec correction.

Exercice B. Codes convolutifs

On considère le code convolutif de générateur: $g_1 = X + 1$ et $g_2 = X^2 + 1$.

1. Dessiner l'automate associé.

2. Dessiner deux étages du diagramme en treillis.

3. Quelle est la séquence codée associé à la séquence $1111\ldots$?

4. Quelle séquence source correspond à la séquence codée 00 00 00 00 ?

5. En déduire qu'un nombre fini d'erreurs sur le canal peut entraîner un nombre infini d'erreurs de décodage.

Remarque *Ce phénomène est appelé "propagation catastrophique d'erreurs". Il apparaît en particulier quand il existe un autre état que l'état initial qui est son propre successeur par la transition "0". Cependant, il peut être éviter en choisissant des polynômes générateurs sans facteurs communs.*

C. Système de McEliece - Niederreiter

On rappelle le protocole de Mac Eliece. Alice choisit en secret trois matrices carrées arbitraires à coefficients dans $\mathbb{F}_2$:

- M la matrice d'un code linéaire de Goppa (n, k) qui est $t = \frac{n-k}{m}$ correcteur.
- S de dimension $k \times k$ et inversible;
- P une matrice de permutation de dimension $n \times n$.

Alice publie $N = SMP$ et t comme clef publique et garde S, M et P secrets.
Pour envoyer un message $w \in \mathbb{F}_2^k$ à Alice, Bob utilise le protocole suivant :

- Bob choisit un vecteur $b \in \mathbb{F}_2^n$ avec exactement t composantes égales à 1;
- Bob calcule $c = w.N + b$ et envoie c à Alice.

1. Comment Alice déchiffre-t-elle c pour retrouver w ?

2 Majorer le coût pour Alice de ce déchiffrement en fonction de n, k et t.

3. Pourquoi ce système est-il considéré comme robuste ?

4. A n fixé, quel est le compromis entre le choix de t et le choix de k ?

5. On propose d'utiliser pour M un code raccourci du code de Goppa. Qu'en pensez-vous ?