ENSTA Paris
Information et Réseaux
Mardi 25 octobre 2022

NOM Prénom : [redacted]

Les polycopiés et les notes prises en cours sont autorisés.
Les appareils électroniques ne sont pas autorisés.

Nota :

Les 2 problèmes sont totalement indépendants.
Veuillez donc remettre deux copies séparées avec votre nom pour chacun des exercices et l' énoncé de chacun des exercices à l'intérieur de chacune de vos copies (même si cette copie est vide).

Problème 1

Rappel: $\log_2(3)$= 1.58

1/ Un canal a une entrée X qui prend des valeurs aléatoires binaires parmi les valeurs $\{x_1=1, x_2=3\}$ et une sortie Y qui peut prendre 4 valeurs aléatoires parmi $\{y_1=0, y_2=1, y_3=2, y_4=3\}$.
L'observation de ce canal permet de connaitre les probabilités conjointes :

$$P(x_1,y_1) = 1/4 \quad P(x_1,y_2) = 1/8 \quad P(x_1,y_3) = 1/8 \quad P(x_1,y_4) = 0$$
$$P(x_2,y_1) = 0 \quad P(x_2,y_2) = 1/8 \quad P(x_2,y_3) = 1/8 \quad P(x_2,y_4) = 1/4$$

Calculer les probabilités marginales p(x) et p(y) ; X et Y sont-elles indépendantes ?
Calculer H(X), H(Y), H(X,Y), H(X/Y), H(Y/X), I(X,Y).
Quelle est la redondance minimale nécessaire pour assurer une transmission avec une probabilité d'erreur arbitrairement faible ?

2/ Les valeurs aléatoires des entrées et des sorties prennent des valeurs identiques à la question précédente, mais le canal entre l'entrée et la sortie est de qualité différente et les probabilités valent à présent :

$$P(x_1,y_1) = 1/4 \quad P(x_1,y_2) = 1/4 \quad P(x_1,y_3) = 0 \quad P(x_1,y_4) = 0$$
$$P(x_2,y_1) = 0 \quad P(x_2,y_2) = 0 \quad P(x_2,y_3) = 1/4 \quad P(x_2,y_4) = 1/4$$

Calculer les probabilités marginales p(x) et p(y) ; X et Y sont-elles indépendantes ?
Calculer H(X), H(Y), H(X,Y), H(X/Y), H(Y/X), I(X,Y).
Quelle est la redondance minimale nécessaire pour assurer une transmission avec une probabilité d'erreur arbitrairement faible ?

3/ On suppose que le canal entre l'entrée et la sortie varie aléatoirement dans le temps ; il est décrit par les probabilités données dans la question 1 dans 50% des cas, et celles données dans la question 2 le reste du temps. Calculer la redondance minimale nécessaire pour assurer une transmission avec une probabilité d'erreur arbitrairement faible sur ce canal. Comparer et commenter sur la redondance relative nécessaire pour les canaux de ces 3 premières questions.

4/ Pouvez-vous proposer pour un de ces 3 canaux, un système de codage/décodage correcteur le plus simple et le plus efficace possible afin d'obtenir une probabilité d'erreur arbitrairement faible ?

ENSTA Paris
Information et Réseaux
Mardi 25 octobre 2022

NOM Prénom : [redacted]

Les polycopiés et les notes prises en cours sont autorisés.
Les appareils électroniques ne sont pas autorisés.

Nota :
Les 2 problèmes sont totalement indépendants.
Veuillez donc remettre deux copies séparées avec votre nom pour chacun des exercices et l'énoncé de chacun des exercices à l'intérieur de chacune de vos copies (même si cette copie est vide).

Problème 2

La question 4/ est totalement indépendante des questions 1/, 2/ et 3/ de ce problème.
Pour les 3 premières questions de ce problème, on considère le corps de Galois à 8 éléments engendré par le polynôme $1 + X^2 + X^3$.

1/ Donner dans un tableau à deux colonnes la liste des éléments de ce corps : dans la première colonne vous exprimerez comme puissance d'un élément primitif α (forme polaire) les différents éléments non nuls de ce corps, et dans la deuxième colonne, vous donnerez la représentation équivalente de chaque élément comme un polynôme de degré inférieur à 3 (forme cartésienne).

2/ Réaliser un circuit multipliant dans ce corps par α^4.

3/ On considère le code de Reed Solomon engendré par le polynôme générateur
$g_{RS}(X) = (X + \alpha)(X + \alpha^2)(X + \alpha^3)(X + \alpha^4)$.

a/ Préciser les caractéristiques de ce code (longueur avant et après codage, distance minimale) exprimées en symboles du corps de Galois à 8 éléments.
b/ Quelle est la longueur du paquet d'erreurs exprimée en bits que ce code de Reed Solomon garantit de corriger ?
c/ Déduire de l'étude précédente, avec le plus de précision possible, le schéma d'un circuit codeur de Reed-Solomon engendré par $g_{RS}(X)$.
d/ On reçoit le mot dont la représentation polynomiale est : $R(X) = \alpha^4 + X^2 + \alpha^6 X^4 + X^5$
Détailler avec précision les étapes de la correction de ce mot reçu.
Combien de bits ont été corrigés ? Est-ce en contradiction avec le résultat de la question 3b/ ?

4/ Un code bloc sous forme systématique transforme k=2 bits en n=6 bits. Les 4 mots codés équiprobables sont les suivants : (000000), (011001), (100110), (110111).
Quelle est la capacité de détection de ce code ? Quelle est sa capacité de correction ?
Si le canal est binaire symétrique avec une probabilité de transition p=0.01, quelle est la probabilité que le récepteur ne puisse pas détecter d'erreur, et donc pas corriger un mot reçu ?