TD 4 : Détection d'erreurs

1 Détection d'erreurs

Exercice 1 (RIB)

1. Vérifiez que la clé de votre RIB personnel est bien correcte selon le critère décrit sur les transparents.
2. Soit $B = 42912, G = 81837, N = TM951PRV36X$. Calculez une / la clé de RIB correspondante.
3. Pour B, G, N donnés, est-ce que la clé C est déterminée de manière unique, ou est-ce que plusieurs C avec la propriété souhaitée sont acceptables ?

Voici le tableau de traduction pour calculer $S(N)$ (attention, discontinuité entre R et S) :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	1	2	3	4	5	6	7	8	9	2	3	4	5	6	7	8	9

Exercice 2 (RIB : Analyse) Analysons la méthode de vérification du RIB plus en détail, pour mieux motiver la vérification "$R \mod 97$", sans pourtant faire une analyse entièrement formelle.

Nous compareron trois méthodes de vérification :

— M_{13} : $R \mod 13$ doit être 0
— M_{97} (celle utilisée par le RIB) : $R \mod 97$ doit être 0
— M_{99} : $R \mod 99$ doit être 0

Considérons les cas suivants :

1. Supposez que les erreurs sont distribuées de manière uniforme lors de la saisie de R. Cela veut dire : il est aussi probable de saisir n'importe quel autre nombre R' à 23 chiffres que le nombre R souhaité. Quelle proportion des erreurs n'est pas détectée par la méthode M_{13} (respectivement M_{97} / M_{99}) ? Quelle méthode est donc préférable ?
2. L'hypothèse faite sous (1) n'est pas réaliste. Lors d'une saisie manuelle, certaines classes d'erreurs sont plus fréquentes que d'autres. On peut supposer que la permutation de chiffres, et surtout une transposition (permutation de deux chiffres voisins, par exemple 4529 au lieu de 4259) est particulièrement fréquente.
   (a) Étant donné un nombre R, démontrez que tout nombre R^π issu de la permutation des chiffres de R a le même reste de division par 3. Par exemple, $4529 \mod 3 = 2 = 4259 \mod 3$.
   (b) Exagérons un peu et supposons que les erreurs de permutation sont les seules qui peuvent apparaître lors de la saisie de R. Pour un R donnée et n'importe quelle permutation R^π de R, quelle est la probabilité que $R \mod 99 = R^\pi \mod 99$ *sachant que* $R \mod 3 = R^\pi \mod 3$? Même question pour $R \mod 97 = R^\pi \mod 97$. Sous cet angle, laquelle des méthodes M_{97} et M_{99} est préférable ?

Exercice 3 (Caractéristiques RIB)

1. Donnez les caractéristiques du code RIB : (n, k)-code pour quels n, k ? Rendement ?
2. Montrez que le code est 1-détecteur. (Considérez uniquement des RIB composés de chiffres, négligez le codage des lettres.)
3. Montrez que le code n'est pas 2-détecteur (il suffit de donner un exemple).

Exercice 4 (Codage et décodage avec CRC) Soient $G_1(X) = X^3 + X + 1$ et $G_2(X) = X^5 + X^3 + 1$ des polynômes générateurs.

Utilisez ces polynômes pour

1. coder les messages [110100111] et [001110110]
2. décoder le message [001110110110] avec G_1
3. décoder le message [001100111110] avec G_1

Exercice 5 (Bit de parité et CRC) Démontrez que le CRC avec polynôme générateur $G(X) = X + 1$ correspond exactement à une vérification avec un bit de parité (quelle variante : paire ou impaire ?).

Exercice 6 Cet exercice a pour but de montrer que les polynômes générateurs $G'(X)$ multiples de X (où $G'(X) = G(X) * X$) ne sont pas très utiles et qu'il vaut mieux utiliser directement le polynome $G(X)$.

1. Pour avoir une intuition du phénomène, prenez le polynôme $G'(X) = X^3 + X = G(X) * X$, où $G(X) = X^2 + 1$ est l'exemple utilisé en cours. Codez le message $M(X) = X^5 + X^3 + X + 1$ avec G et G'. Qu'est-ce que vous observez ?
2. Démontrez, en vous référant à la définition de l'opération mod sur les polynômes, que $(A(X) * X)$ mod $(B(X) * X) = (A(X) \mod B(X)) * X$
3. Généralisez l'observation de (1) à tout polynôme $G(X)$ et $G'(X) = G(X) * X$ et montrez que le codage avec $G'(X)$ présente une redondance inutile (dans quel sens ?).

Exercice 7 Nous parlons de *deux erreurs isolées de distance d* si lors de la transmission d'un message, exactement deux bits sont inversés, et ceci à des positions i et j dans le message avec $i > j$ et $i - j = d$. Par exemple, les erreurs entre le message envoyé $Env = [11011100]$ et le message reçu $Rec = [10011110]$ se trouvent aux positions $i = 6$ et $j = 1$ (la position 0 est la plus à droite). Il s'agit donc de deux erreurs isolées de distance 5.

Démontrez la propriété suivante : Pour qu'un code CRC avec un polynôme générateur $G(X)$ détecte deux erreurs isolées de distance d, il suffit que $G(X)$ ne divise pas le polynôme $X^d + 1$.

NB : Nous excluons des polynômes générateurs $G(X)$ qui sont des multiples de X, voir exercice 6.

Exercice 8 Nous nous intérssons aux générateurs $G(X)$ qui sont des monômes, qui sont donc de la forme X^n, pour $n \geq 0$.

1. Prenons le monôme $G(X) = X^0 = 1$. Pour un message $M(X)$, quel est son codage $Env(X)$? Quelles erreurs sont donc détéctées par ce monôme ?
2. Combinez ce résultat avec le résultat de l'exercice 6 pour évaluer l'utilité des générateurs X^n pour $n > 0$.

Maintenant, vous comprenez pourquoi les générateurs CRC utilisés en dans la pratique sont tous de la forme $X^{n+1} + \cdots + 1$.

Exercice 9 Une perturbation électrique a souvent pour conséquence qu'une séquence de bits consécutifs d'un message est altérée lors d'un transmission, tandis que le reste du message n'est pas affecté. Une telle séquence de bits est appelée *burst*. (*N.B. : ce ne sont pas forcément tous les bits du burst qui sont modifiés.*)

1. Soit $G_1(X) = X^2 + X + 1$ un générateur, $Env_1 = [101111011001]$ le message envoyé et $Rec_1 = [101001101001]$ le message reçu. Calculez le polynôme d'erreur $Err_1(X)$. Quel est la longueur b_1 du burst ? Montrez que $G_1(X)$ ne permet pas de détecter l'erreur ; ceci découle du fait que $Err_1(X)$ est de la forme $G_1(X) * P_1(X) * X^i$, pour un $P_1(X)$ qui n'est pas multiple de X. Indiquez $P_1(X)$ et i.

2. Plus en général, soit $G(X) = X^n + \cdots + 1$ un générateur. Soit $Err(X)$ un polynôme d'erreur qui contient un burst. Montrez que $Err(X)$ est toujours de la forme $B(X) * X^j$, pour un $B(X)$ non multiple de X. Quel est le rapport entre $B(X)$ et la longueur b du burst ? Montrez que si $b \leq n$, alors une erreur de transmission est sûrement détectée.
3. Sur cette base, proposez un générateur $G_2(X)$ qui aurait pu détecter l'erreur de (1).