ÉCOLE POLYTECHNIQUE

CONCOURS D'ADMISSION 2003 FILIÈRES PSI ET PT

ÉPREUVE FACULTATIVE D'INFORMATIQUE

(Durée : 2 heures)

L'utilisation des calculatrices n'est pas autorisée pour cette épreuve.

⋆ ⋆ ⋆

Avertissements :
Le langage de programmation choisi par le candidat doit être spécifié en tête de la copie.
On attachera une grande importance à la concision, à la clarté et à la précision de la rédaction.

Codage cyclique

On se propose d'implanter plusieurs techniques de détection d'erreurs dans la transmission de données sur les moyens de communication non fiables. Les données transitant sur le réseau sont des séquences de *bits* que l'on notera 0 ou 1. Ces séquences de bits sont découpées en mots $\langle b_0, b_1, \ldots, b_{n-1}\rangle$ de longueur n ($n > 0$) où n est une constante globale, fixée une fois pour toutes. Ces mots sont représentés par des tableaux d'entiers b de longueur n dont l'élément b_i à l'indice i vaut 0 ou 1. Le nombre d'erreurs de transmission du mot b est le nombre de bits ayant changé de valeur après la transmission.

Le temps d'exécution $T(f)$ d'une fonction f de la variable b est le nombre d'opérations élémentaires (addition, soustraction, multiplication, division, affectation) nécessaires au calcul de $f(b)$. Lorsque ce temps d'exécution dépend d'un paramètre p, il sera noté $T_p(f)$. De même l'espace mémoire $E(f)$ est la somme des tailles des données intermédiaires nécessaires pour le calcul de $f(b)$. On dira que $T_p(f)$ est d'ordre $O(g(p))$ pour signifier qu'il existe $K > 0$ tel qu'on a $T_p(f) \leq K g(p)$ pour tout p.

Partie I – Bit de parité

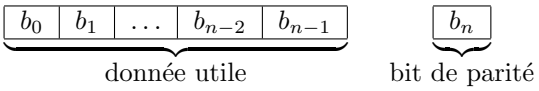
Le ou-exclusif $x \oplus y$ de deux bits x et y est défini par la table des valeurs suivante :

x \ y	0	1
0	0	1
1	1	0

On remarque qu'on a $0 \oplus x = x \oplus 0 = x$ et $x \oplus x = 0$ pour toute valeur de x. Donc x est son propre opposé pour $\oplus$.

Question 1 Écrire la fonction `ou_exclusif` qui calcule le ou-exclusif $x \oplus y$ des deux bits x et y pris comme arguments.

La technique du *bit de parité* consiste à rajouter un bit b_n (le bit de parité) aux données utiles $\langle b_0, b_1, \ldots, b_{n-1}\rangle$ de façon à ce que $\langle b_0, b_1, \ldots, b_{n-1}, b_n\rangle$ ait un nombre pair de bits à 1. Ainsi, pour $n = 7$, le bit de parité du tableau $\langle 1, 1, 0, 1, 1, 1, 0\rangle$ est 1. Le mot transmis sur le réseau est $\langle 1, 1, 0, 1, 1, 1, 0, 1\rangle$. Schématiquement, on aura :



Question 2 Écrire la fonction `bit_parite` qui calcule le bit de parité du tableau b, contenant la suite de bits $\langle b_0, b_1, \ldots, b_{n-1}\rangle$.
Question 3 Combien d'erreurs de transmission la technique du bit de parité permet-elle de détecter dans un mot b de longueur n ? Justifiez-le.

Partie II – Codage CRC

On peut considérer le tableau b de n bits $\langle b_0, b_1, \ldots, b_{n-1}\rangle$ comme les coefficients du polynôme

$$P(X) = b_0X^{n-1} + b_1X^{n-2} + \ldots + b_{n-2}X + b_{n-1}.$$

Soit $\mathbf{B}[X]$ l'ensemble des polynômes dont les coefficients sont des bits. Le degré du polynôme $P(X) = b_0X^{n-1} + b_1X^{n-2} + \ldots + b_{n-2}X + b_{n-1}$ de $\mathbf{B}[X]$ est la valeur maximale de k tel que b_{n-1-k} ne soit pas nul.
Question 4 Écrire la fonction `degre` prenant en argument un tableau b de coefficients représentant le polynôme $P(X)$ de $\mathbf{B}[X]$, et retournant le degré de P. (Par convention, le degré du polynôme nul vaudra -1).

La somme exclusive des deux polynômes $P(X)$ et $Q(X)$ de $\mathbf{B}[X]$ dont les coefficients sont les tableaux $\langle b_0, b_1, \ldots, b_{n-1}\rangle$ et $\langle c_0, c_1, \ldots, c_{n-1}\rangle$ est définie par :

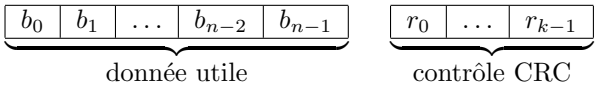
$$P(X) \oplus Q(X) = (b_0 \oplus c_0)X^{n-1} + (b_1 \oplus c_1)X^{n-2} + \ldots + (b_{n-1} \oplus c_{n-1}).$$

Remarque :
$P(X)$ est son propre opposé, puisque $P(X) \oplus P(X) = 0$ pour tout polynôme $P(X)$ de $\mathbf{B}[X]$.
Question 5 Écrire la fonction `plus` prenant comme arguments deux tableaux b et c représentant deux polynômes $P(X)$ et $Q(X)$ de $\mathbf{B}[X]$, deux indices i et j dans b et c, et une longueur l, et qui modifie le tableau b pour remplacer ses coefficients b_i, b_{i+1}, …, b_{i+l-1} par $b_i \oplus c_j$, $b_{i+1} \oplus c_{j+1}$ … $b_{i+l-1} \oplus c_{j+l-1}$.

La technique dite **CRC** (*Cyclic Redundancy Check*) ajoute plus de bits de contrôle à chaque mot transmis que la méthode du bit de parité. Elle considère un polynôme générateur $G(X)$, bien choisi dans $\mathbf{B}[X]$, de degré k ($0 < k \leq n$), donné une fois pour toutes ; et elle construit, pour tout mot b correspondant au polynôme $P(X)$, le reste $R(X)$ de la division euclidienne de $P(X) \cdot X^k$ par $G(X)$.

$$R(X) = P(X) \cdot X^k \bmod G(X)$$

où mod est l'opération modulo. Si $\langle r_0, r_1, \ldots, r_{k-1}\rangle$ sont les coefficients de $R(X)$, la donnée transmise $\langle b_0, b_1, \ldots, b_{n-1}, r_0, r_1, \ldots, r_{k-1}\rangle$ correspondra à un polynôme multiple de $G(X)$. Graphiquement, on a :



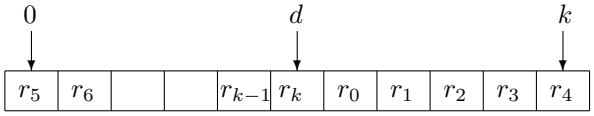
Pour calculer le reste $R(X)$ de la division de $P(X) \cdot X^k$ par $G(X)$, on utilise l'algorithme classique de la division. On aligne les bits valant 1 les plus à gauche du dividende et du diviseur, puis on retranche le diviseur du dividende (grâce à l'opération $\oplus$). Le degré du résultat strictement inférieur à celui du dividende. Et on recommence la division en prenant le résultat comme nouveau dividende, jusqu'à ce que son degré soit strictement inférieur à k. Ainsi, par exemple, pour les tableaux $b = \langle 0, 1, 1, 1, 0, 1\rangle$ et $g = \langle 0, 1, 0, 1\rangle$ (et donc $k = 2$), les étapes successives de la division donnent :

$\langle 0,1,1,1,0,1,0,0\rangle$
$\langle 0,0,1,0,0,1,0,0\rangle$
$\langle 0,0,0,0,1,1,0,0\rangle$
$\langle 0,0,0,0,0,1,1,0\rangle$
$\langle 0,0,0,0,0,0,1,1\rangle$

D'où la valeur $\langle 1,1\rangle$ pour le CRC.

Question 6 Écrire la fonction `crc` prenant en argument deux tableaux b et g et qui retourne le tableau de bits correspondant aux coefficients du CRC du mot représenté par b par rapport au polynôme générateur représenté par le tableau g. (La valeur de l'argument b ne doit pas être modifiée). Donner un ordre de grandeur du temps et de l'espace mémoire pris par `crc` en fonction de la longueur n de b et du degré k de g.

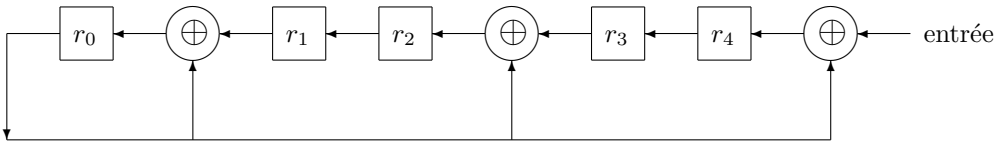
Pour réduire l'espace mémoire utilisé, on peut ranger les résultats partiels du reste (dans le calcul de la division) dans un registre circulaire de $k+1$ bits. Ce registre est représenté par un tableau r de bits de taille $k+1$, et une variable d indique l'emplacement de son bit le plus significatif. Plus exactement le registre est organisé comme suit :



Question 7 Écrire une nouvelle version `crc1` de la fonction `crc`, qui ne prend qu'un espace mémoire en $O(k)$. (La valeur de l'argument b doit toujours être inchangée).

Les polynômes générateurs habituels utilisés pour le CRC sont $X^{16}+X^{15}+X^2+1$ (CRC-16), $X^{32}+X^{26}+X^{23}+X^{22}+X^{16}+X^{12}+X^{11}+X^{10}+X^8+X^7+X^5+X^4+X^2+X+1$ (CRC-Ethernet), etc. On réalise des circuits pour calculer rapidement les valeurs du CRC.

Question 8 Expliquer le circuit suivant de calcul du CRC avec $G(X)=X^5+X^4+X^2+1$ comme polynôme générateur. (Initialement, tous les r_i sont nuls ; les bits du mot b d'entrée arrivent sur la droite, suivis de 4 bits valant 0 ; le circuit est synchronisé par une horloge globale qui à chaque tranche de temps décale tous les r_i d'un cran vers la gauche ; le résultat est le tableau de bits $\langle r_0,r_1,r_2,r_3,r_4\rangle$ une fois que tous les bits d'entrée ont été lus).



On peut montrer que la technique du bit de parité est un cas particulier de la méthode de détection d'erreurs par CRC.

Question 9 Quel est le polynôme générateur correspondant à la méthode du bit de parité ?

⋆ ⋆
⋆