

Devoir Surveillé du 03/03/2008
Durée 3h. Documents et calculatrices interdits

Exercice 1 – [QUESTIONS DIVERSES]

- 1) Montrer que le nombre de chiffres d'un entier $N \geq 1$ en base 2 est $\lfloor \log_2 N \rfloor + 1$.
- 2) On considère un algorithme opérant sur des données de taille $\leq N$ et dont le coût d'exécution est majoré par $T(N)$, où $T : \mathbb{R}^+ \rightarrow \mathbb{R}^+$ est une fonction croissante vérifiant $T(x) \leq 2T(x/2) + x$. Prouver que le coût de l'algorithme est un $O(N \ln N)$.
- 3) Construire explicitement des corps finis de cardinal 27 et 16.

Exercice 2 – [CODES DE REED-SOLOMON]

Soient \mathbb{F}_q un corps fini de cardinal q et deux entiers k et n tels que $1 \leq k \leq n$. On fixe des éléments distincts $x_1, \dots, x_n \in \mathbb{F}_q$ et on note \mathcal{P}_k l'ensemble des $P \in \mathbb{F}_q[X]$ de degré $\leq k-1$. L'ensemble Γ des $(P(x_1), \dots, P(x_n)) \in (\mathbb{F}_q)^n$ pour P parcourant \mathcal{P}_k est un *code de Reed-Solomon* sur \mathbb{F}_q . Un « mot » est un élément de $(\mathbb{F}_q)^n$.

- 1) Montrer que Γ est un sous-espace vectoriel de $(\mathbb{F}_q)^n$ de dimension k .
- 2) On transmet de l'information sous forme de mots de Γ . On considère un mot $m = (m_1, \dots, m_n) \in \Gamma$ que l'on envoie, on note $r = (r_1, \dots, r_n) \in (\mathbb{F}_q)^n$ le mot reçu, $e = (e_1, \dots, e_n) := r - m$ « l'erreur » et $t := \lfloor (n - k)/2 \rfloor$.
 - a) Prouver qu'il existe un $Q \in \mathbb{F}_q[X, Y] - \{0\}$ de la forme $Q(X, Y) = Q_0(X) + YQ_1(X)$ tel que $\forall i \in \{1, \dots, n\}$, $Q(x_i, r_i) = 0$, $\deg Q_0 \leq n - 1 - t$ et $\deg Q_1 \leq n - 1 - t - (k - 1)$. [Les coefficients de Q_0, Q_1 doivent vérifier un système linéaire.]
 - b) On fait l'hypothèse (*) : le nombre d'erreurs de transmission (i.e. le nombre de e_i non nuls) est $\leq t$. Soit $P \in \mathcal{P}_k$ tel que $m = (P(x_1), \dots, P(x_n))$. En considérant son nombre de racines dans \mathbb{F}_q , montrer que $Q(X, P(X)) = 0$. En déduire que Q_1 divise Q_0 et que $P = -Q_0/Q_1$, en justifiant le fait que $Q_1 \neq 0$.
 - c) Expliquer comment calculer m à partir de r (décodage de r) si l'on suppose (*). Prouver que le coût en opérations dans \mathbb{F}_q de la détermination de m est un $O(n^3)$.
- 3) On prend $q = 5$, $n = 4$, $k = 2$, $(x_1, x_2, x_3, x_4) = (1, 2, 3, 4)$ et $r = (0, 4, 3, 0)$. On suppose que r contient au plus une erreur. Trouver le mot transmis m .

Exercice 3 – [ALGORITHME DE BERLEKAMP]

Soient p un nombre premier et $P \in \mathbb{F}_p[X]$ sans facteur carré et non constant. On note P_1, \dots, P_k les facteurs irréductibles distincts de P dans $\mathbb{F}_p[X]$ et $n > 0$ le degré de P .

- 1) Montrer que la \mathbb{F}_p -algèbre $A := \mathbb{F}_p[X]/(P)$ est isomorphe à $\mathbb{F}_p[X]/(P_1) \times \dots \times \mathbb{F}_p[X]/(P_k)$ et que $\mathbb{F}_p[X]/(P_i)$ est un corps fini de cardinal $p^{\deg P_i}$ pour $i \in \{1, \dots, k\}$.

- 2) On note Φ l'endomorphisme du \mathbb{F}_p -espace vectoriel A tel que $\Phi(Q \bmod P) = (Q^p - Q) \bmod P$. En utilisant 1), prouver que $\text{Ker}(\Phi) \simeq (\mathbb{F}_p)^k$. En déduire que $k = n - \text{rg}(\Phi)$.
- 3) On suppose que $k > 1$ et on choisit $Q \in \mathbb{F}_p[X]$ tel que $Q \bmod P \in \text{Ker}(\Phi) - \mathbb{F}_p$.
- Montrer que $Q^p - Q = \prod_{a \in \mathbb{F}_p} (Q - a)$.
 - En remarquant que P divise $(Q^p - Q)$, prouver qu'il existe $a \in \mathbb{F}_p$ tel que $\text{pgcd}(P, Q - a)$ est un diviseur non trivial de P .
- 4) Expliquer comment calculer efficacement k en utilisant une \mathbb{F}_p -base simple de A . Évaluer en fonction de n et de p le coût en opérations dans \mathbb{F}_p du calcul de k et, lorsque $k > 1$, d'un facteur non trivial de P .