TD9

Exercice 1. *Algorithme de Freivalds modifié*

On rappelle que pour vérifier un produit de matrices $A \cdot B = C$, l'algorithme de Freivalds tire un vecteur $r \in \{0,1\}^n$ aléatoire puis vérifie l'égalité $A \cdot B \cdot r = C \cdot r$.
On le modifie de la manière suivante : au lieu de tirer r dans $\{0,1\}^n$, on le tire dans S^n où S est un ensemble fixé à l'avance.

1. Montrer que la probabilité d'erreur de l'algorithme modifié est bornée par $1/|S|$.
2. Supposons que la source d'aléa dont on dispose ne fournit que des bits aléatoires. Comparer le nombre de bits nécessaires pour appliquer l'algorithme de Freivals original et sa version modifiée.
3. En déduire le nombre total de bits aléatoires à tirer pour obtenir une probabilité de succès p dans chacune des deux variantes.
4. On suppose qu'un bit aléatoire s'obtient en temps $O(1)$ et qu'on vise une probabilité de succès p. Quelle version de l'algorithme faut-il préférer ?

Exercice 2. *Évaluation modulaire d'un polynôme*

Pour que le test d'identité polynomiale soit efficace, il faut évaluer le polynôme *modulo* un nombre premier.

1. Soit f un polynôme, x un entier et p un nombre premier choisi aléatoirement $\leq N$. Borner la probabilité $\Pr[f(x) = 0 \bmod p | f(x) \neq 0]$, en fonction de $|f(x)|$.
2. Montrer que si f est de degré d et que ces coefficients sont tous inférieurs ou égaux à M en valeur absolue, alors $|f(x)| \leq Mx^{d+1}$ pour tout $x \geq 2$.
3. En déduire que si on tire aléatoirement un nombre premier $p \leq 4(d+1)\log(kM)\ln(4(d+1)\log(kM))$ et qu'on évalue un polynôme f de degré d dont les coefficients sont bornés par M en valeur absolue en un point $x \in \{2, \dots, k\}$, $\Pr[f(x) = 0 \bmod p | f(x) \neq 0] \leq 1/2$.
4. En déduire un algorithme probabiliste de complexité $O(d \log^2(dM))$ pour le problème suivant : étant donné trois polynômes f, g, et h, tels que $\deg(f) + \deg(g) = \deg(h) = d$ et dont les coefficients sont bornés par M en valeur absolue, déterminer si $h = fg$. Donner les garanties de succès de l'algorithme.

Exercice 3. *Comparaison des techniques*

1. Démontrer la correction de l'algorithme de Freivalds à l'aide du lemme de Schwartz-Zippel.

Soit EvalMod un algorithme d'*évaluation modulaire*, c'est-à-dire que EvalMod(f, x, p) calcule $f(x) \bmod p$.

2. Exprimer l'algorithme de test d'égalité d'entiers à l'aide d'EvalMod, où le point d'évaluation x est fixé.
3. Donner un autre algorithme de test d'égalité d'entiers basé sur EvalMod, où x n'est plus fixé.
4. Donner un troisième algorithme de test d'égalité d'entiers basé sur EvalMod, où cette fois x et p sont fixés.