EPFL - Information, Calcul et Communication - Partie théorique

Série 6

1 Nombre de bits

a) En 2025, combien de bits sont nécessaires pour représenter les informations suivantes?

1. le nombre d'étudiants inscrits au cours ICC en GC et MX à l'EPFL
2. le nombre total d'étudiants inscrits à l'EPFL
3. le nombre de vues d'une vidéo sur Youtube
4. le nombre d'habitants sur la planète Terre

b) Seul un certain nombre des 250 étudiants inscrits à un cours se présentent à un examen. Combien de bits sont nécessaires pour enregistrer les informations suivantes?

1. le nombre d'étudiants présents lors de l'examen
2. la liste des étudiants présents à l'examen
   (en supposant qu'on dispose déjà de la liste complète des noms des étudiants)

2 Conversion de décimal en binaire

Ecrire un algorithme qui prenne en entrée une liste L de n chiffres représentant un nombre entier positif en écriture décimale (par exemple: $L = (1, 9, 8, 4)$, représentant 1984) et dont la sortie soit une autre liste M de m bits représentant le même nombre en binaire (dans l'exemple, on voudrait donc $M = (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$). Quelle est la complexité temporelle de votre algorithme? (exprimée en fonction de n, avec la notation $\Theta(\cdot)$)

3 Utiliser la décomposition binaire

a) L'algorithme suivant (qui remonte à l'Egypte ancienne!) n'utilise que des opérations d'addition et de soustraction, ainsi que des multiplications et divisions par 2, très faciles à exécuter avec la représentation binaire. Mais que fait-il exactement? (essayer avec $x = 7$ et $y = 5$)

devinette

entrée : *x, y deux nombres entiers positifs*
sortie : *???*

```
z ⟵ 0
Tant que y ≥ 1
    Si y est pair
        x ⟵ 2 · x
        y ⟵ y/2
    Sinon
        z ⟵ z + x
        y ⟵ y − 1
Sortir : z
```

b) Si x et y sont des nombres nécessitant chacun n bits en représentation binaire, quelle est la complexité temporelle de l'algorithme ci-dessus? (utiliser la notation $\Theta(\cdot)$)

4 10 rats pour 1'000 bouteilles

Vous organisez un mariage et avez commandé à cette occasion 1'000 bouteilles d'un excellent vin. Manque de chance, il semble qu'un horrible individu a introduit dans une (et une seule) de ces bouteilles un poison incolore, insipide et inodore, dont les effets sont mortels, mais au bout de 24h *environ*. Pour trouver la bouteille empoisonnée, vous disposez de 10 rats testeurs. Votre problème: nous sommes vendredi à 14h, et le mariage a lieu demain samedi à 15h. Comment allez-vous procéder pour être en mesure de pouvoir servir les 999 bouteilles non-empoisonnées au mariage ?

Indication: Pour commencer à réfléchir au problème, on peut penser à la situation où on a seulement 4 bouteilles à tester et 2 rats à disposition.

Note: La résolution de ce problème n'est pas seulement utile aux organisateurs de mariages! L'algorithme de Hamming, basé sur ce principe, permet de localiser des erreurs de transmission dans de très longs messages, en utilisant un petit nombre de bits de parité pour coder les messages envoyés.

5 Pour le plaisir: nombres premiers de Mersenne, nombres parfaits*

Les nombres premiers sont un sujet qui fascine depuis toujours... La fameuse conjecture de Riemann, par exemple, qui date de 1859, peut être reformulée en une hypothèse sur la distribution des nombres premiers. Elle reste non-résolue jusqu'à aujourd'hui, malgré plus de 150 de travaux sur le sujet !

Un autre thème lié est la recherche de (très) grands nombres premiers qui, comme nous le verrons vers la fin de ce cours, a trouvé une application majeure dans les systèmes de cryptographie modernes dits à clé publique. A ce propos, c'est un moine français du 17e siècle, Marin Mersenne, qui a proposé une méthode efficace pour trouver de grands nombres premiers, en suggérant de chercher parmi les nombres de la forme $N = 2^p - 1$, où p est lui-même un nombre premier.

a) Comment s'écrit $N = 2^p - 1$ en binaire ?

En observant le début de la séquence ainsi formée, on trouve

$$2^2 - 1 = 3, \quad 2^3 - 1 = 7, \quad 2^5 - 1 = 31, \quad 2^7 - 1 = 127, \quad \ldots$$

qui sont effectivement tous des nombres premiers.

b) Pour autant, est-il vrai que tout nombre de Mersenne $N = 2^p - 1$, avec p premier, est un nombre premier ?

Si $N = 2^p - 1$ est un nombre premier de Mersenne, alors Euclide a montré déjà au 4e siècle avant J.-C. que $M = N(N+1)/2 = 2^{p-1}(2^p - 1)$ est un nombre *parfait*, en ce sens que M est la somme de ses diviseurs (hormis lui-même). Les premiers nombre parfaits (sans jeu de mot!) sont $M = 6$, 28, 496, $8'192$.

c) Qu'est-ce qui caractérise la décomposition binaire d'un nombre parfait ?

A l'heure actuelle, on ne connaît que 51 nombres premiers de Mersenne; le plus grand d'entre eux, qui est aussi le plus grand nombre premier connu, est composé d'environ 25 millions de chiffres !

d) De manière correspondante, quel est approximativement le nombre de chiffres qui composent le plus grand nombre parfait connu ?