Preuve et Analyse des Algorithmes

16:00–18:00
aucun document autorisé

21 juin 2016

Soit m un entier positif. On note X_m l'ensemble des 2^m entiers de taille binaire m. Pour $z \in X_m$, on note : z_i ou $(z)_i$ le i-ème bit de z, $\mathrm{wt}(z)$ le poids binaire de z et $\mathrm{dec}(z)$ la décomposition binaire de z :

$$z = \sum_{i=1}^{m} z_i 2^{i-1} \, (0 \le z_i \le 1), \quad \mathrm{wt}(z) = \sum_{i=1}^{m} z_i, \quad \mathrm{dec}(z) = (z_m \dots z_2 z_1).$$

Dans la suite, on utilise les opérateurs binaires du langage `C` : reste de la division par 2, décalage à droite de k bits, et conjonction bit à bit.

$$x \,\%\, 2 = x \,\&\, 1 = x_1, \quad \mathrm{dec}(x >> k) = (0 \dots 0 x_m \dots x_{k+1}), \quad z = (x \,\&\, y) \iff \forall i,\ z_i = x_i y_i.$$

1 Préliminaires

1. Montrer que $\mathrm{wt}(z) = \mathrm{wt}(z/2) + \mathrm{wt}(z \,\%\, 2) = \mathrm{wt}(z >> 1) + z \,\&\, 1$.
2. On suppose z est de la forme $\mathrm{dec}(z) = (* \dots * 10 \dots 0)$. Donner la décomposition binaire de $z - 1$.
3. Montrer que $1 + \mathrm{wt}(z \,\&\, (z-1)) = \mathrm{wt}(z)$.
4. Montrer par récurrence sur m que :

$$\sum_{k=0}^{m-1} k 2^k = 2^m (m-2) + 2.$$

5. Soit i un entier, $1 \le i \le m$, montrer que :

$$\sum_{x \in X_m} (x)_i = \sum_{x \in X_m} x_i = 2^{m-1}.$$

6. En déduire

$$\sum_{z \in X_m} \mathrm{wt}(z) = m 2^{m-1}, \quad \text{puis} \quad \sum_{k=0}^{m} k \mathrm{C}_m^k = m 2^{m-1}.$$

où C_m^k désigne un coefficient du binôme de Newton i.e. $\sum_{k=0}^{m} \mathrm{C}_m^k T^k = (1+T)^m$.

2 Poids Binaire Récursif

On suppose que $m = 2n$ est pair. Tout entier $z \in X_m$ se décompose sous la forme $z = x 2^n + y, \quad x, y \in X_n$, et donc, $\mathrm{wt}(z) = \mathrm{wt}(x) + \mathrm{wt}(y)$.

1. Donner la décomposition de $2^n - 1 = ((1 << n) - 1)$ sur m bits.
2. Quel décalage à droite donne x en fonction de z et n ?

3. Quel masque donne y en fonction de z et n ?
4. Ecrire une fonction récursive `int rec( ullong z, int m)` qui calcule le poids d'un entier z dont la taille m est une puissance de 2. La fonction doit élaguer l'arbre de récursion sur les noeuds vérifiant $z = 0$ ou $m = 1$.
5. Estimer le temps de calcul dans le pire des cas.
6. Estimer le temps de calcul pour un entier de poids 1.
7. Donner la décomposition de 1777 sur 16 bits.
8. Faire le graphe des appels récursifs dans le cas $z = 1777$ et $m = 16$.

3 Poids Binaire Naif

```
1 int pb( ullong z ) {
2 int r = 0;
3 while ( z ) {
4       r+= (z % 2);
5       z = z / 2;
6 }
7 return r;
8 }
```

On note $I(\gamma)$ le nombre d'itérations de la boucle de la fonction `int pb(ullong z)` pour une instance γ du paramètre z, la valeur moyenne sur X_m est :

$$\tilde{I}(m) = \frac{1}{2^m} \sum_{\gamma \in X_m} I(\gamma).$$

On applique `pb` aux instances de X_m.

1. Quel est l'ensemble des instances défavorables.
2. Quel est ensemble des entiers γ tels que $I(\gamma) = 1$?.
3. Décrire l'ensemble des entiers γ tels que $I(\gamma) = k$.
4. Préciser le cardinal de cet ensemble.
5. Donner une formule du nombre moyen d'itération.
6. Déterminer le nombre réel α tel que $\tilde{I}(m) \sim \alpha m$.

4 Poids Binaire Efficace

```
1  int wt( ullong z )
2  {
3  int r = 0;
4  while ( z ) {
5       z &= ( z-1 );
6       r++;
7       z >>=1;
8  }
9  return r;
10 }
```

On note $J(\gamma)$ le nombre d'itérations de la boucle de la fonction `int wt(ullong z)` pour une instance γ du paramètre z, la valeur moyenne sur X_m est :

$$\tilde{J}(m) = \frac{1}{2^m} \sum_{\gamma \in X_m} J(\gamma).$$

On applique `wt` aux instances de X_m.

1. Quel est l'ensemble des instances défavorables.
2. Quel est ensemble des entiers γ tels que $J(\gamma) = 1$?.
3. Décrire l'ensemble des entiers γ tels que $J(\gamma) = k$.
4. Préciser le cardinal de cet ensemble.
5. Donner une formule du nombre moyen d'itération.
6. Déterminer le nombre réel β tel que $\tilde{J}(m) \sim \beta m$.