

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 , $\text{wt}(z)$ le poids binaire de z et $\text{dec}(z)$ la décomposition binaire de z :

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

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.

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

1 Préliminaires

1. Montrer que $\text{wt}(z) = \text{wt}(z/2) + \text{wt}(z \% 2) = \text{wt}(z \gg 1) + z \& 1$. En effet, le quotient de z par 2 est $(0z_m \dots z_2)$ et z_1 est le reste.
2. On suppose z est de la forme $\text{dec}(z) = (* \dots * 10 \dots 0)$. Donner la décomposition binaire de $z - 1$.

$$\text{dec}(z - 1) = (* \dots * 01 \dots 1)$$

3. Montrer que $1 + \text{wt}(z \& (z - 1)) = \text{wt}(z)$.

$$\text{dec}(z \& (z - 1)) = (* \dots * 00 \dots 0)$$

il suit que pour $z > 0$ les poids de $z \& (z - 1)$ et z diffèrent de 1.

4. Montrer par récurrence sur m que :

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

La propriété est vrai pour $m = 1$ car $2^1(1 - 2) + 2 = -2 + 2 = 0 = \sum_{k=0}^0 k 2^k$. L'induction est une conséquence du calcul

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

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

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

La moitié des m -uplets binaires sont pairs !

6. En déduire

$$\sum_{z \in X_m} \text{wt}(z) = m2^{m-1}, \quad \text{puis} \quad \sum_{k=0}^m kC_m^k = m2^{m-1}.$$

où C_m^k désigne un coefficient du binôme de Newton i.e. $\sum_{k=0}^m C_m^k T^k = (1+T)^m$. Il s'agit de compter la somme des poids des mots de X_m de deux façons différentes. Il y a C_m^k mots binaires de poids k .

2 Poids Binaire Récursif

On suppose que $m = 2n$ est pair. Tout entier $z \in X_m$ se décompose sous la forme $z = x2^n + y$, $x, y \in X_n$, et donc, $\text{wt}(z) = \text{wt}(x) + \text{wt}(y)$.

1. Donner la décomposition de $2^n - 1 = ((1 \ll n) - 1)$ sur m bits.

$$\underbrace{00 \cdots 0}_{m \text{ bits}} \underbrace{11 \cdots 1}_{m \text{ bits}}$$

2. Quel décalage à droite donne x en fonction de z et n ?

$$z \gg n$$

3. Quel masque donne y en fonction de z et n ?

$$y = (1 \ll n) - 1$$

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 $m = 1$.

```

1
2 int wt( int z, int m )
3 {
4   if ( m == 1 || z == 0 ) return z;
5   m = m / 2;
6   return wt( z >> m, m ) + wt( z & ((1<<m)-1), m );
7 }
```

5. Estimer le temps de calcul dans le pire des cas. Le pire des cas correspond à l'instance $2^m - 1$ qui ne produit aucun élagage. Le temps de calcul est proportionnel au nombre de noeuds d'un arbre binaire équilibré de hauteur m :

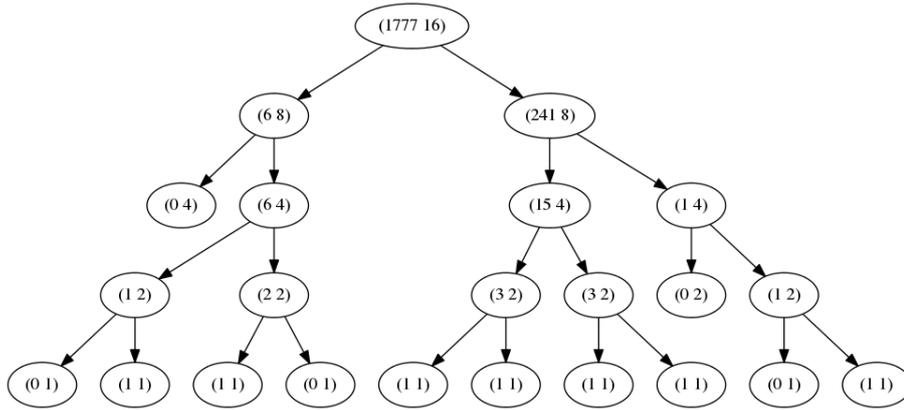
$$\sum_{k=0}^m 2^k = 2^{m+1} - 1$$

6. Estimer le temps de calcul pour un entier de poids 1. Pour une profondeur donnée, il y a au plus 1 appel récursif, ce qui conduit à un temps au plus linéaire en m .

7. Donner la décomposition de 1777 sur 16 bits.

$$0000011011110001$$

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. Il s'agit des mots dont le bit significatif est 1.

$$(1 * \dots *)$$

2. Quel est ensemble des entiers γ tels que $I(\gamma) = 1$?. Il y a une seule instance :

$$(0 \dots 01)$$

3. Décrire l'ensemble des entiers γ tels que $I(\gamma) = k$.

$$(0..01 \underbrace{* \dots *}_{k-1 \text{ bits}})$$

4. Préciser le cardinal de cet ensemble.

$$2^{k-1}$$

5. Donner une formule du nombre moyen d'itération.

$$\tilde{I}(m) = 2^{-m} \sum_{k=0}^m k 2^{k-1} = 2^{-m-1} \sum_{k=0}^m k 2^k$$

6. Déterminer le nombre réel α tel que $\tilde{I}(m) \sim \alpha m$.

$$2^{-m-1}(2^{m+1}(m-1) + 2) \sim m, \quad \alpha = 1.$$

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. Une seule instance défavorable

$$(1 \dots 1)$$

2. Quel est ensemble des entiers γ tels que $J(\gamma) = 1$? Tous les mots de poids 1.
3. Décrire l'ensemble des entiers γ tels que $J(\gamma) = k$. Tous les mots de poids k .
4. Préciser le cardinal de cet ensemble.

$$C_m^k$$

5. Donner une formule du nombre moyen d'itération.

$$\tilde{J}(m) = 2^{-m} \sum_{k=0}^m k C_m^k$$

6. Déterminer le nombre réel β tel que $\tilde{J}(m) \sim \beta m$.

$$\tilde{J}(m) = 2^{-m} \sum_{k=0}^m k C_m^k = m 2^{m-1} 2^{-m} \sim \frac{m}{2}, \quad \beta = \frac{1}{2}.$$