

Jules

Plan

- I / Modèle
- II / Addition
- III / Multiplication
- IV / Exponentiation

I / ~~Expos~~Représentation des entiers de \mathbb{Z} dans une base $B \geq 2$ Complément à la base:On a $a_{n-1} \dots a_0, a_k \in [0; B-1]$

$$a_{n-1} \dots a_0 = \begin{cases} \sum_{k=0}^{n-1} a_k B^k & \text{si } a_{n-1} < \frac{B}{2} \\ \sum_{k=0}^{n-1} a_k B^k - B^n & \text{sinon} \end{cases}$$

$$\sum_{k=0}^{n-1} a_k B^k - B^n = - \sum_{k=0}^{n-1} (B-1-a_k) B^k + 1$$

Avec n chiffres: $\left[\left\lfloor -\left\lfloor \frac{B}{2} \right\rfloor B^{n-1} \right\rfloor ; \left\lfloor \frac{B}{2} \right\rfloor B^{n-1} - 1 \right]$

↳ représentation unique

Représentation signée $B \leq B \leq 2B+1$ $a_0 \dots a_{n-1} \in \left[\left\lfloor -\frac{B}{2} \right\rfloor ; \left\lfloor \frac{B}{2} \right\rfloor \right]$

$$(a_{n-1} \dots a_0)_{B,B} = \sum_{k=0}^{n-1} a_k B^k$$

Représenta° pas nécessairement unique

■

Mesure de perf:

- es de circuits élémentaires (op° 1 seul chiffre)
- circuits composés

Taille d'un circuit: nb de circuits élémentaires

Profondeur: nb max de circuits entre entrée et sortie

II / Addition (code)

Algo add° entiers en complément à la base:

Taille $\Theta(n)$, Profondeur: $\Theta(\log(n))$

Idée: si les entiers sont un chiffre, c'est immédiat.
Sinon on divise les entiers en 2:

$$a = a_{l_0} + a_{h_1} \times 2^{\lfloor \frac{n}{2} \rfloor}$$

$$b = b_{l_0} + b_{h_1} \times 2^{\lfloor \frac{n}{2} \rfloor}$$

Pour optim, on calcule $a_{h_1} + b_{h_1}$ pour toutes les retenues possibles.

[Présentation de code Python]

Add° représentation signée ($\beta > \frac{B}{2}$)

$$a_i + b_i = u_i + v_i B, u_i \in [-\beta + 1; \beta - 1]$$

$$v_i \in [-1; 1]$$

$$d_i = u_i + v_{i-1}$$

→ Taille en $\Theta(n)$, Profondeur en $\Theta(1)$

On peut calculer en //... qqch ?

III / Multiplication

Uniquement pour la représentation en chiffres signés, avec $\beta > B/2$

On veut calculer $a \times b$, $|a| = n$, $|b| = p$, $n \leq p$

$$a = a_{l_0} + a_{h_1} B^{\lfloor n/2 \rfloor}$$

$$ab = a_{l_0} \times b + a_{h_1} \times b \times B^{\lfloor n/2 \rfloor}$$

profondeur: $\Theta(\log n)$, taille: $\Theta(np)$

IV / Exponentiation

ExpRapide (a, base, exp):

si exp = 0

renvoyer 1

sinon

$r \leftarrow \text{exp mod base}$

$q \leftarrow \text{exp / base}$

renvoyer ExpRapide(base, a, q) \times base r ?

$$\text{Exp}(a, b) = \text{ExpRapide}(a, 1, b) \rightarrow a^b$$

b est en complément, a est en rep signée
 ? J'ai raté un truc?

$$\text{Profondeurs: } O(|b|) \times (\log |a| + \log |b|)$$

$$P_{|b|=1} = 1$$

$$P_k = P_{k+1} + \min(\log \dots)$$

$$\leq P_{k+1} + \log(\dots)$$

$$P_0 \leq \sum_{k=0}^{|b|-1} \log(\dots)$$

Intérêt des deux représentations: on peut les mélanger pour avoir des ~~trucs~~ algos optis