Calculer avec une mémoire remplie

Robin Milosz

IFT6370

30 novembre 2016

Plan

Calculer avec une mémoire remplie?

Calculer avec une mémoire remplie?

Calculer avec une mémoire remplie?

Ce qu'on peut faire avec 3 registres..

Bases

Anneau

- Anneau $(R, +, \times, 0, 1)$ une structure algébrique
- Exemple des entiers: $\mathbb{Z} = \ldots -2, -1, 0, 1, 2 \ldots$

Registre

- Un espace de mémoire, contenant un élément de R, (read-write)
- Exemple: $r_1 = 3, r_2 = -7, r_3 = 0, \ldots, r_m = r,\ r \in R$
- Registre d'entrée (entrée) $x_1, x_2, x_3, \ldots, x_n$ (read)

Bases

Anneau

- Anneau $(R, +, \times, 0, 1)$ une structure algébrique
- Exemple des entiers: $\mathbb{Z} = \ldots -2, -1, 0, 1, 2 \ldots$

Registre

- Un espace de mémoire, contenant un élément de R, (read-write)
- Exemple: $r_1 = 3, r_2 = -7, r_3 = 0, \ldots, r_m = r,\ r \in R$
- Registre d'entrée (entrée) $x_1, x_2, x_3, \ldots, x_n$ (read)

Modèle de calcul

Un programme: séquence d'instructions I_i (réversibles) de la forme:

$$r_j \leftarrow r_j + (r_i \times c)$$

$$r_j \leftarrow r_j - (r_i \times c)$$

$$r_j \leftarrow r_j + (r_i \times x_u)$$

$$r_j \leftarrow r_j - (r_i \times x_u)$$

$i \neq j$

Formule algébrique

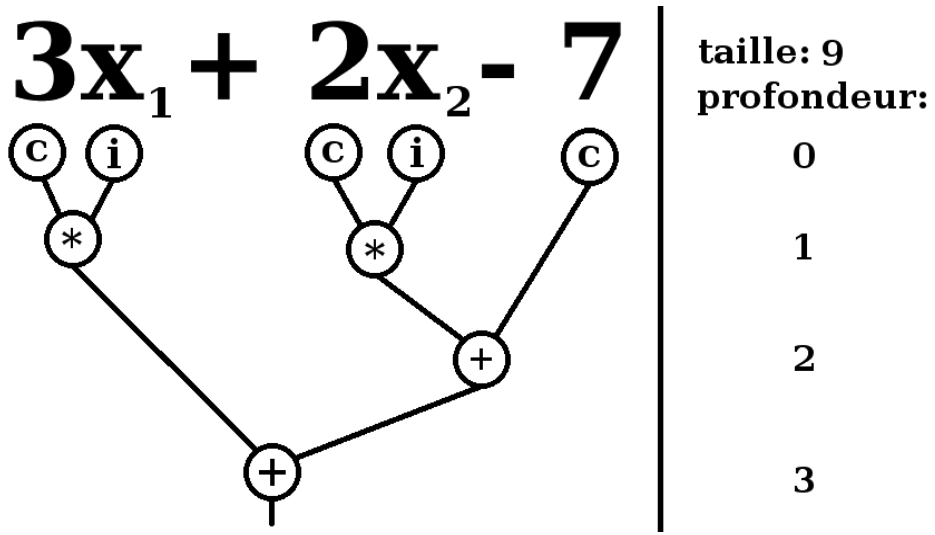


Figure: Une formule algébrique de profondeur 3 et de taille 9

Formule f de profondeur $d = 0$: entrée ou constante
Formule f de profondeur $d > 0$: $(f + g)$ ou $(f \times g)$

Théorème

Théorème

Une formule algébrique $f(x_1, x_2, \ldots, x_n)$ sur R, de profondeur d, peut être calculée avec un programme d'au plus 4^d instructions et qui utilise 3 registres.

Note

La réponse du calcul sera du type:

$$r_j \leftarrow r_j + (r_i \times f(x_1, x_2, \ldots, x_n))$$

Convention: $r_1 = 0$ et $r_2 = 1$ pour obtenir:

$$r_1 \leftarrow r_1 + (r_2 \times f(x_1, x_2, \ldots, x_n))$$

i.e

$$r_1 = f(x_1, x_2, \ldots, x_n)$$

Théorème

Théorème

Une formule algébrique $f(x_1, x_2, \ldots, x_n)$ sur R, de profondeur d, peut être calculée avec un programme d'au plus 4^d instructions et qui utilise 3 registres.

Note

La réponse du calcul sera du type:

$$r_j \leftarrow r_j + (r_i \times f(x_1, x_2, \ldots, x_n))$$

Convention: $r_1 = 0$ et $r_2 = 1$ pour obtenir:

$$r_1 \leftarrow r_1 + (r_2 \times f(x_1, x_2, \ldots, x_n))$$

i.e

$$r_1 = f(x_1, x_2, \ldots, x_n)$$

Preuve

Récursivement,
$d = 0$:
Constante

$$r_j \leftarrow r_j \pm (r_i \times c)$$

Entrée

$$r_j \leftarrow r_j \pm (r_i \times x_u)$$

Preuve

Toujours récursivement,
$d > 0$:
Addition
Si on a:

$$r_j \leftarrow r_j \pm (r_i \times f(x_1, x_2, \ldots, x_n))$$

$$r_j \leftarrow r_j \pm (r_i \times g(x_1, x_2, \ldots, x_n))$$

Alors on peut obtenir:

$$r_j \leftarrow r_j \pm (r_i \times (f + g)(x_1, x_2, \ldots, x_n))$$

Preuve

Multiplication

Si on a:

$$r_j \leftarrow r_j \pm (r_i \times f(x_1, x_2, \ldots, x_n))$$

$$r_k \leftarrow r_k \pm (r_j \times g(x_1, x_2, \ldots, x_n))$$

Alors on peut obtenir:

$$r_k \leftarrow r_k \pm (r_i \times (f \times g)(x_1, x_2, \ldots, x_n))$$

Preuve

Multiplication (suite)

$$I_1 \ : \ r_k \leftarrow r_k - (r_j \times g(x_1, x_2, \ldots, x_n))$$
$$I_2 \ : \ r_j \leftarrow r_j + (r_i \times f(x_1, x_2, \ldots, x_n))$$
$$I_3 \ : \ r_k \leftarrow r_k + (r_j \times g(x_1, x_2, \ldots, x_n))$$
$$I_4 \ : \ r_j \leftarrow r_j - (r_i \times f(x_1, x_2, \ldots, x_n))$$

Registre	Init.	1	2	3	4
r_i	τ_i	τ_i	τ_i	τ_i	τ_i
r_j	τ_j	τ_j	$\tau_j + (\tau_i \times f)$	$\tau_j + (\tau_i \times f)$	τ_j
r_k	τ_k	$\tau_k - (\tau_j \times g)$	$\tau_k - (\tau_j \times g)$	$\tau_k + (\tau_i \times (f \times g))$ *	$\tau_k + (\tau_i \times (f \times g))$

* $\tau_k - (\tau_j \times g) + ((\tau_j + (\tau_i \times f)) \times g) = \tau_k - (\tau_j \times g) + ((\tau_j \times g) + ((\tau_i \times f) \times g)$

On a alors:

$$r_k \leftarrow r_k \pm (r_i \times (f \times g)(x_1, x_2, \ldots, x_n))$$

Preuve

Multiplication (suite)

$$I_1 \ : \ r_k \leftarrow r_k - (r_j \times g(x_1, x_2, \ldots, x_n))$$
$$I_2 \ : \ r_j \leftarrow r_j + (r_i \times f(x_1, x_2, \ldots, x_n))$$
$$I_3 \ : \ r_k \leftarrow r_k + (r_j \times g(x_1, x_2, \ldots, x_n))$$
$$I_4 \ : \ r_j \leftarrow r_j - (r_i \times f(x_1, x_2, \ldots, x_n))$$

Registre	Init.	1	2	3	4
r_i	τ_i	τ_i	τ_i	τ_i	τ_i
r_j	τ_j	τ_j	$\tau_j + (\tau_i \times f)$	$\tau_j + (\tau_i \times f)$	τ_j
r_k	τ_k	$\tau_k - (\tau_j \times g)$	$\tau_k - (\tau_j \times g)$	$\tau_k + (\tau_i \times (f \times g))$ *	$\tau_k + (\tau_i \times (f \times g))$

* $\tau_k - (\tau_j \times g) + ((\tau_j + (\tau_i \times f)) \times g)$ = $\tau_k - (\tau_j \times g) + ((\tau_j \times g) + ((\tau_i \times f) \times g)$

On a alors:

$$r_k \leftarrow r_k \pm (r_i \times (f \times g)(x_1, x_2, \ldots, x_n))$$

Preuve

Multiplication (suite)

$$I_1 \ : \ r_k \leftarrow r_k - (r_j \times g(x_1, x_2, \ldots, x_n))$$
$$I_2 \ : \ r_j \leftarrow r_j + (r_i \times f(x_1, x_2, \ldots, x_n))$$
$$I_3 \ : \ r_k \leftarrow r_k + (r_j \times g(x_1, x_2, \ldots, x_n))$$
$$I_4 \ : \ r_j \leftarrow r_j - (r_i \times f(x_1, x_2, \ldots, x_n))$$

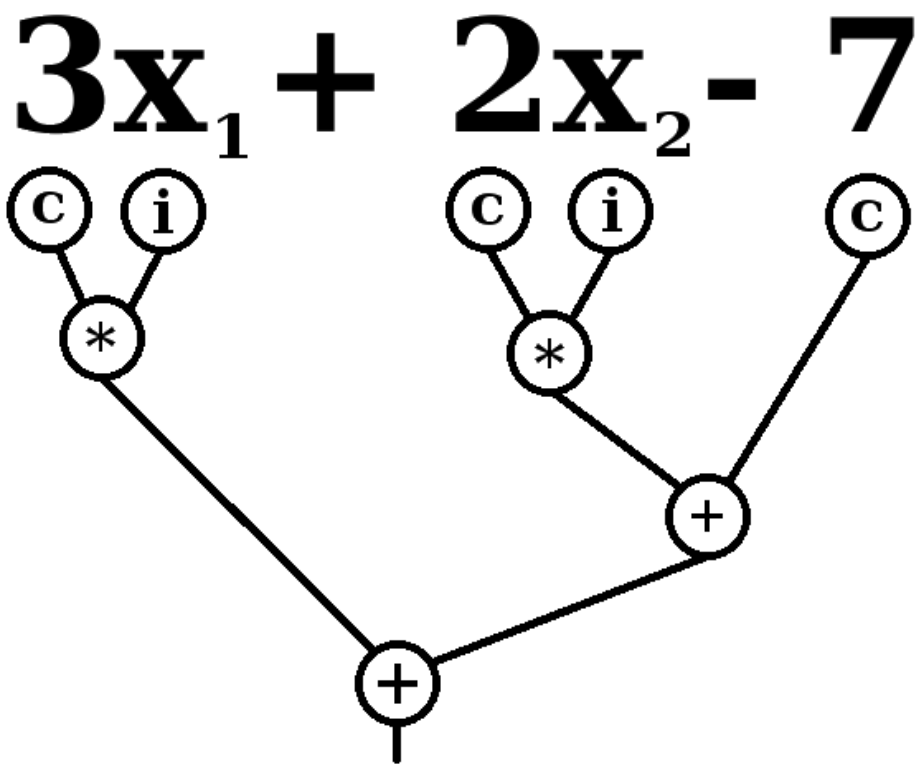
Registre	Init.	1	2	3	4
r_i	τ_i	τ_i	τ_i	τ_i	τ_i
r_j	τ_j	τ_j	$\tau_j + (\tau_i \times f)$	$\tau_j + (\tau_i \times f)$	τ_j
r_k	τ_k	$\tau_k - (\tau_j \times g)$	$\tau_k - (\tau_j \times g)$	$\tau_k + (\tau_i \times (f \times g))$ *	$\tau_k + (\tau_i \times (f \times g))$

* $\tau_k - (\tau_j \times g) + ((\tau_j + (\tau_i \times f)) \times g)$ = $\tau_k - (\tau_j \times g) + ((\tau_j \times g) + ((\tau_i \times f) \times g)$

On a alors:

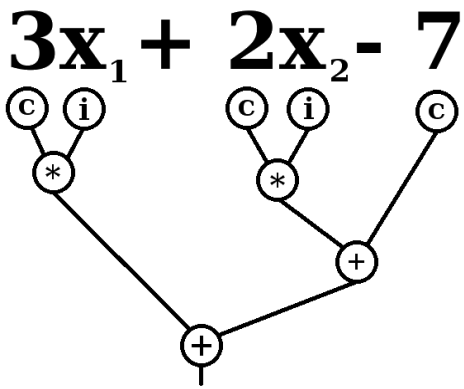
$$r_k \leftarrow r_k \pm (r_i \times (f \times g)(x_1, x_2, \ldots, x_n))$$

Exemple



Écrire les intructions et trouver la valeur de la formule sur entrée $x_1 = 2, x_2 = 4$

Exemple

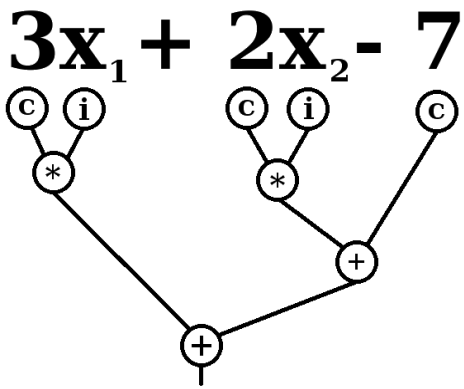


$$I_1 : r_1 \leftarrow r_1 - (r_3 \times [x_1])$$
$$I_2 : r_3 \leftarrow r_3 + (r_2 \times [c = 3])$$
$$I_3 : r_1 \leftarrow r_1 + (r_3 \times [x_1])$$
$$I_4 : r_3 \leftarrow r_3 - (r_2 \times [c = 3])$$

$$I_5 : r_1 \leftarrow r_1 - (r_3 \times [x_2])$$
$$I_6 : r_3 \leftarrow r_3 + (r_2 \times [c = 2])$$
$$I_7 : r_1 \leftarrow r_1 + (r_3 \times [x_2])$$
$$I_8 : r_3 \leftarrow r_3 - (r_2 \times [c = 2])$$

$$I_9 : r_1 \leftarrow r_1 - (r_2 \times [c = -7])$$

Exemple

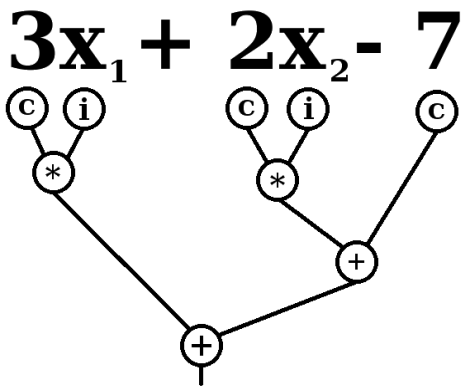


$$
\begin{aligned}
I_1 &: r_1 \leftarrow r_1 - (r_3 \times [x_1]) \\
I_2 &: r_3 \leftarrow r_3 + (r_2 \times [c = 3]) \\
I_3 &: r_1 \leftarrow r_1 + (r_3 \times [x_1]) \\
I_4 &: r_3 \leftarrow r_3 - (r_2 \times [c = 3])
\end{aligned}
$$

$$
\begin{aligned}
I_5 &: r_1 \leftarrow r_1 - (r_3 \times [x_2]) \\
I_6 &: r_3 \leftarrow r_3 + (r_2 \times [c = 2]) \\
I_7 &: r_1 \leftarrow r_1 + (r_3 \times [x_2]) \\
I_8 &: r_3 \leftarrow r_3 - (r_2 \times [c = 2])
\end{aligned}
$$

$$
I_9 : r_1 \leftarrow r_1 - (r_2 \times [c = -7])
$$

Exemple

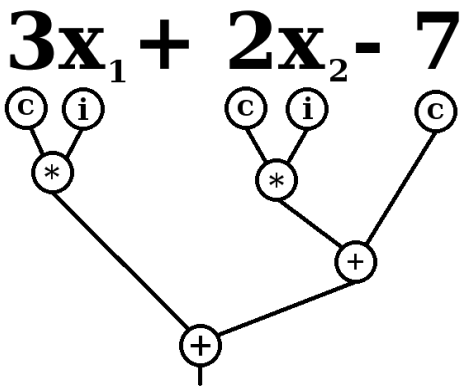


$$
\begin{aligned}
I_1 &: r_1 \leftarrow r_1 - (r_3 \times [x_1]) \\
I_2 &: r_3 \leftarrow r_3 + (r_2 \times [c = 3]) \\
I_3 &: r_1 \leftarrow r_1 + (r_3 \times [x_1]) \\
I_4 &: r_3 \leftarrow r_3 - (r_2 \times [c = 3])
\end{aligned}
$$

$$
\begin{aligned}
I_5 &: r_1 \leftarrow r_1 - (r_3 \times [x_2]) \\
I_6 &: r_3 \leftarrow r_3 + (r_2 \times [c = 2]) \\
I_7 &: r_1 \leftarrow r_1 + (r_3 \times [x_2]) \\
I_8 &: r_3 \leftarrow r_3 - (r_2 \times [c = 2])
\end{aligned}
$$

$$I_9 : r_1 \leftarrow r_1 - (r_2 \times [c = -7])$$

Exemple

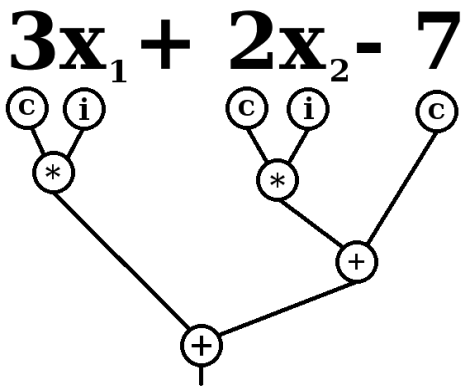


$$
\begin{aligned}
l_1 &: r_1 \leftarrow r_1 - (r_3 \times [x_1]) \\
l_2 &: r_3 \leftarrow r_3 + (r_2 \times [c = 3]) \\
l_3 &: r_1 \leftarrow r_1 + (r_3 \times [x_1]) \\
l_4 &: r_3 \leftarrow r_3 - (r_2 \times [c = 3])
\end{aligned}
$$

$$
\begin{aligned}
l_5 &: r_1 \leftarrow r_1 - (r_3 \times [x_2]) \\
l_6 &: r_3 \leftarrow r_3 + (r_2 \times [c = 2]) \\
l_7 &: r_1 \leftarrow r_1 + (r_3 \times [x_2]) \\
l_8 &: r_3 \leftarrow r_3 - (r_2 \times [c = 2])
\end{aligned}
$$

$$l_9 : r_1 \leftarrow r_1 - (r_2 \times [c = -7])$$

Exemple



$$
\begin{aligned}
I_1 &: r_1 \leftarrow r_1 - (r_3 \times [x_1 = 2]) \\
I_2 &: r_3 \leftarrow r_3 + (r_2 \times [c = 3]) \\
I_3 &: r_1 \leftarrow r_1 + (r_3 \times [x_1 = 2]) \\
I_4 &: r_3 \leftarrow r_3 - (r_2 \times [c = 3])
\end{aligned}
$$

$$
\begin{aligned}
I_5 &: r_1 \leftarrow r_1 - (r_3 \times [x_2 = 4]) \\
I_6 &: r_3 \leftarrow r_3 + (r_2 \times [c = 2]) \\
I_7 &: r_1 \leftarrow r_1 + (r_3 \times [x_2 = 4]) \\
I_8 &: r_3 \leftarrow r_3 - (r_2 \times [c = 2])
\end{aligned}
$$

$$I_9 : r_1 \leftarrow r_1 - (r_2 \times [c = -7])$$

Exemple - simulation des intructions

$$I_1 \ : \ r_1 \leftarrow r_1 - (r_3 \times [x_1 = 2])$$
$$I_2 \ : \ r_3 \leftarrow r_3 + (r_2 \times [c = 3])$$
$$I_3 \ : \ r_1 \leftarrow r_1 + (r_3 \times [x_1 = 2])$$
$$I_4 \ : \ r_3 \leftarrow r_3 - (r_2 \times [c = 3])$$

$$I_5 \ : \ r_1 \leftarrow r_1 - (r_3 \times [x_2 = 4])$$
$$I_6 \ : \ r_3 \leftarrow r_3 + (r_2 \times [c = 2])$$
$$I_7 \ : \ r_1 \leftarrow r_1 + (r_3 \times [x_2 = 4])$$
$$I_8 \ : \ r_3 \leftarrow r_3 - (r_2 \times [c = 2])$$

$$I_9 \ : \ r_1 \leftarrow r_1 - (r_2 \times [c = -7])$$

Registre	Init.	I_1	I_2	I_3	I_4	I_5	I_6	I_7	I_8	I_9
r_1	0									
r_2	1									
r_3	2									

Exemple - simulation des intructions

$$I_1 \ : \ r_1 \leftarrow r_1 - (r_3 \times [x_1 = 2])$$
$$I_2 \ : \ r_3 \leftarrow r_3 + (r_2 \times [c = 3])$$
$$I_3 \ : \ r_1 \leftarrow r_1 + (r_3 \times [x_1 = 2])$$
$$I_4 \ : \ r_3 \leftarrow r_3 - (r_2 \times [c = 3])$$

$$I_5 \ : \ r_1 \leftarrow r_1 - (r_3 \times [x_2 = 4])$$
$$I_6 \ : \ r_3 \leftarrow r_3 + (r_2 \times [c = 2])$$
$$I_7 \ : \ r_1 \leftarrow r_1 + (r_3 \times [x_2 = 4])$$
$$I_8 \ : \ r_3 \leftarrow r_3 - (r_2 \times [c = 2])$$

$$I_9 \ : \ r_1 \leftarrow r_1 - (r_2 \times [c = -7])$$

Registre	Init.	I_1	I_2	I_3	I_4	I_5	I_6	I_7	I_8	I_9
r_1	0	-4								
r_2	1	1								
r_3	2	2								

Exemple - simulation des intructions

$$I_1 \ : \ r_1 \leftarrow r_1 - (r_3 \times [x_1 = 2])$$
$$I_2 \ : \ r_3 \leftarrow r_3 + (r_2 \times [c = 3])$$
$$I_3 \ : \ r_1 \leftarrow r_1 + (r_3 \times [x_1 = 2])$$
$$I_4 \ : \ r_3 \leftarrow r_3 - (r_2 \times [c = 3])$$

$$I_5 \ : \ r_1 \leftarrow r_1 - (r_3 \times [x_2 = 4])$$
$$I_6 \ : \ r_3 \leftarrow r_3 + (r_2 \times [c = 2])$$
$$I_7 \ : \ r_1 \leftarrow r_1 + (r_3 \times [x_2 = 4])$$
$$I_8 \ : \ r_3 \leftarrow r_3 - (r_2 \times [c = 2])$$

$$I_9 \ : \ r_1 \leftarrow r_1 - (r_2 \times [c = -7])$$

Registre	Init.	I_1	I_2	I_3	I_4	I_5	I_6	I_7	I_8	I_9
r_1	0	-4	-4							
r_2	1	1	1							
r_3	2	2	5							

Exemple - simulation des intructions

$$I_1 \ : \ r_1 \leftarrow r_1 - (r_3 \times [x_1 = 2])$$
$$I_2 \ : \ r_3 \leftarrow r_3 + (r_2 \times [c = 3])$$
$$I_3 \ : \ r_1 \leftarrow r_1 + (r_3 \times [x_1 = 2])$$
$$I_4 \ : \ r_3 \leftarrow r_3 - (r_2 \times [c = 3])$$

$$I_5 \ : \ r_1 \leftarrow r_1 - (r_3 \times [x_2 = 4])$$
$$I_6 \ : \ r_3 \leftarrow r_3 + (r_2 \times [c = 2])$$
$$I_7 \ : \ r_1 \leftarrow r_1 + (r_3 \times [x_2 = 4])$$
$$I_8 \ : \ r_3 \leftarrow r_3 - (r_2 \times [c = 2])$$

$$I_9 \ : \ r_1 \leftarrow r_1 - (r_2 \times [c = -7])$$

Registre	Init.	I_1	I_2	I_3	I_4	I_5	I_6	I_7	I_8	I_9
r_1	0	-4	-4	6						
r_2	1	1	1	1						
r_3	2	2	5	5						

Exemple - simulation des intructions

$$I_1 \ : \ r_1 \leftarrow r_1 - (r_3 \times [x_1 = 2])$$
$$I_2 \ : \ r_3 \leftarrow r_3 + (r_2 \times [c = 3])$$
$$I_3 \ : \ r_1 \leftarrow r_1 + (r_3 \times [x_1 = 2])$$
$$I_4 \ : \ r_3 \leftarrow r_3 - (r_2 \times [c = 3])$$

$$I_5 \ : \ r_1 \leftarrow r_1 - (r_3 \times [x_2 = 4])$$
$$I_6 \ : \ r_3 \leftarrow r_3 + (r_2 \times [c = 2])$$
$$I_7 \ : \ r_1 \leftarrow r_1 + (r_3 \times [x_2 = 4])$$
$$I_8 \ : \ r_3 \leftarrow r_3 - (r_2 \times [c = 2])$$

$$I_9 \ : \ r_1 \leftarrow r_1 - (r_2 \times [c = -7])$$

Registre	Init.	I_1	I_2	I_3	I_4	I_5	I_6	I_7	I_8	I_9
r_1	0	-4	-4	6	6					
r_2	1	1	1	1	1					
r_3	2	2	5	5	2					

Exemple - simulation des intructions

$$I_1 \ : \ r_1 \leftarrow r_1 - (r_3 \times [x_1 = 2])$$
$$I_2 \ : \ r_3 \leftarrow r_3 + (r_2 \times [c = 3])$$
$$I_3 \ : \ r_1 \leftarrow r_1 + (r_3 \times [x_1 = 2])$$
$$I_4 \ : \ r_3 \leftarrow r_3 - (r_2 \times [c = 3])$$

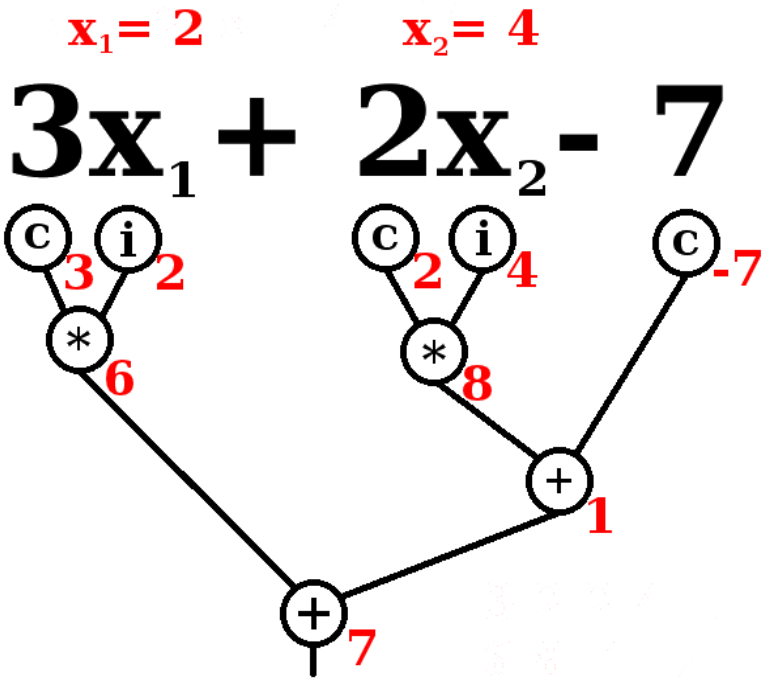
$$I_5 \ : \ r_1 \leftarrow r_1 - (r_3 \times [x_2 = 4])$$
$$I_6 \ : \ r_3 \leftarrow r_3 + (r_2 \times [c = 2])$$
$$I_7 \ : \ r_1 \leftarrow r_1 + (r_3 \times [x_2 = 4])$$
$$I_8 \ : \ r_3 \leftarrow r_3 - (r_2 \times [c = 2])$$

$$I_9 \ : \ r_1 \leftarrow r_1 - (r_2 \times [c = -7])$$

Registre	Init.	I_1	I_2	I_3	I_4	I_5	I_6	I_7	I_8	I_9
r_1	0	-4	-4	6	6	-2	-2	14	14	7
r_2	1	1	1	1	1	1	1	1	1	1
r_3	2	2	5	5	2	2	4	4	2	2

Exemple - ”vérification”

Registre	Init.	I_1	I_2	I_3	I_4	I_5	I_6	I_7	I_8	I_9
r_1	0	-4	-4	6	6	-2	-2	14	14	7
r_2	1	1	1	1	1	1	1	1	1	1
r_3	2	2	5	5	2	2	4	4	2	2



Classes NC^1 et $\#NC^1$

NC^i : classe de fonctions calculées par des circuits booléens en max $log(n)^i$ profondeur et utilisant des portes standard *NOT*, *OR* et *AND*.

$\#NC^i(R)$: classe de fonctions calculées par des circuits algébriques en max $log(n)^i$ profondeur et utilisant des portes *SUM* et *MULT* sur un anneau R.

Instructions = $M_{3\times3}$

$$I_1 \ : \ r_2 \leftarrow r_2 - (r_1 \times x_u)$$

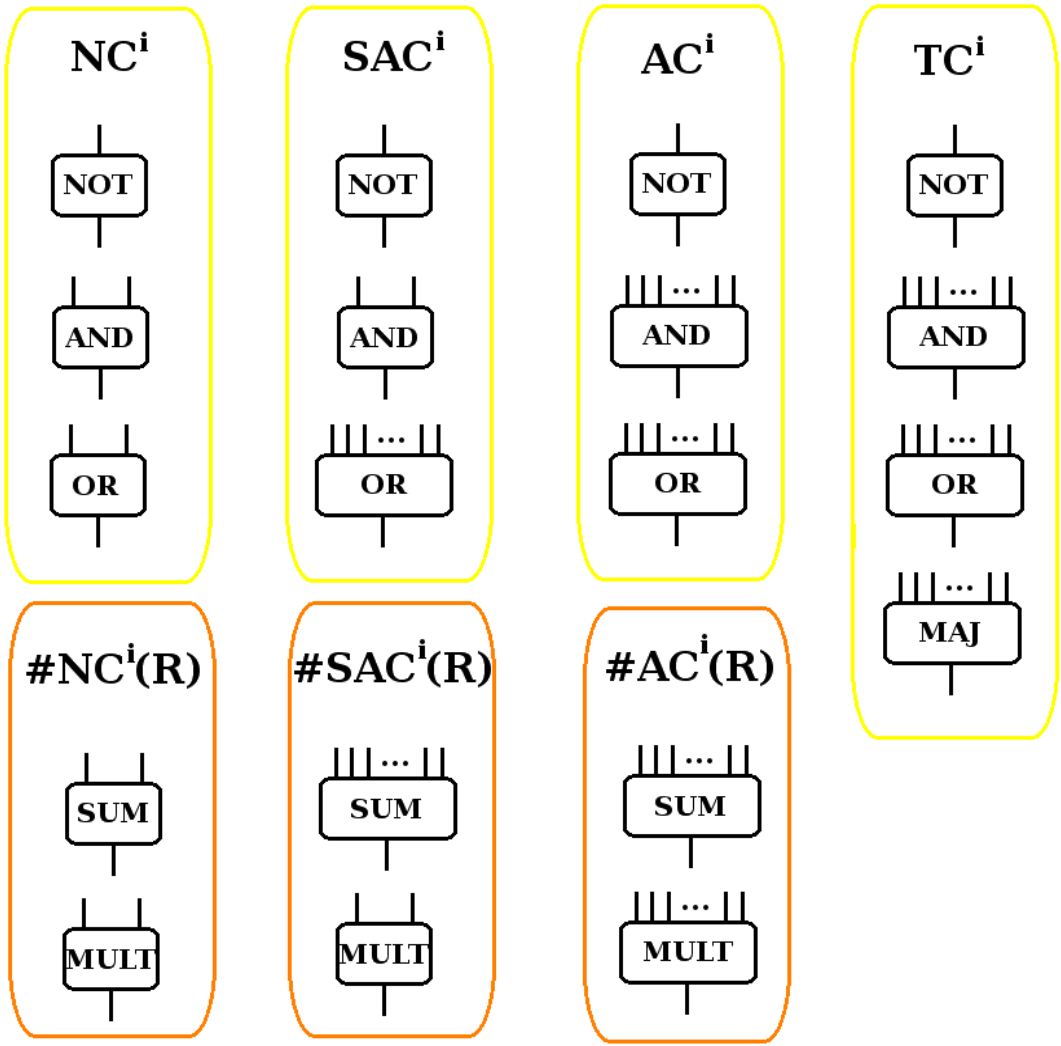
Équivalent à:

$$I_1 = \begin{pmatrix} 1 & 0 & 0 \\ x_u & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Ce qu'on peut faire avec plusieurs registres..
(espace catalytique)

Classes de circuits

Circuits booléens et circuits algébriques de profondeur max $log(n)^i$



Modèle de calcul: Instructions

Instruction

$$r_i \leftarrow r_i \pm (u \times v)$$

où u et $v \in \{constantes,\ x_k,\ r_j\}$, $i \neq j$

"Skew instruction" quand au moins u ou v est une constante ou entrée.

Un programme: séquence d'instructions I_i (réversibles):

Programme $P = I_1, I_2, \ldots, I_l$

Modèle de calcul: Calcul transparent

Fonction $f(x)$ calculé de façon transparente

Programme P sur registres $r_1, r_2, \ldots, r_m$ avec valeurs $\tau_1, \tau_2, \ldots, \tau_m$ et entrée $(x_1, x_2, \ldots, x_n)$ résulte en $r_i = \tau_i + f(x_1, x_2, \ldots, x_n)$, peut-importe les autres registres.

Vecteur de fonctions $(f_1(x), f_2(x), \ldots, f_k(x))$ calculé de façon transparente

Programme P sur registres $r_1, r_2, \ldots, r_m$ avec valeurs $\tau_1, \tau_2, \ldots, \tau_m$ et entrée $(x_1, x_2, \ldots, x_n)$ résulte en $r_{i_j} = \tau_{i_j} + f_j(x_1, x_2, \ldots, x_n)$, $\forall i \in \{1, 2, \ldots, k\}$, peut-importe les autres registres.

Modèle de calcul: Calcul transparent

Fonction $f(x)$ calculé de façon transparente

Programme P sur registres $r_1, r_2, \ldots, r_m$ avec valeurs $\tau_1, \tau_2, \ldots, \tau_m$ et entrée $(x_1, x_2, \ldots, x_n)$ résulte en $r_i = \tau_i + f(x_1, x_2, \ldots, x_n)$, peut-importe les autres registres.

Vecteur de fonctions $(f_1(x), f_2(x), \ldots, f_k(x))$ calculé de façon transparente

Programme P sur registres $r_1, r_2, \ldots, r_m$ avec valeurs $\tau_1, \tau_2, \ldots, \tau_m$ et entrée $(x_1, x_2, \ldots, x_n)$ résulte en $r_{i_j} = \tau_{i_j} + f_j(x_1, x_2, \ldots, x_n)$, $\forall i \in \{1, 2, \ldots, k\}$, peut-importe les autres registres.

Modèle de calcul: Réversibilité

Instruction et instruction inverse

$I : r_i \leftarrow r_i \pm (u \times v)$
$I^{-1} : r_i \leftarrow r_i \mp (u \times v)$

Programme et programme inverse

Programme $P = I_1, I_2, \ldots, I_l$
Programme $P^{-1} = I_l^{-1}, I_{l-1}^{-1}, \ldots, I_1^{-1},$
$P, P^{-1} = I$

Programme propre

Programme $P' = r \leftarrow r - r_i, P, r \leftarrow r + r_i, P^{-1}$

Modèle de calcul: Réversibilité

Instruction et instruction inverse

$I : r_i \leftarrow r_i \pm (u \times v)$
$I^{-1} : r_i \leftarrow r_i \mp (u \times v)$

Programme et programme inverse

Programme $P = I_1, I_2, \ldots, I_l$
Programme $P^{-1} = I_l^{-1}, I_{l-1}^{-1}, \ldots, I_1^{-1},$
$P, P^{-1} = I$

Programme propre

Programme $P' = r \leftarrow r - r_i, P, r \leftarrow r + r_i, P^{-1}$

Modèle de calcul: Réversibilité

Instruction et instruction inverse

$I : r_i \leftarrow r_i \pm (u \times v)$
$I^{-1} : r_i \leftarrow r_i \mp (u \times v)$

Programme et programme inverse

Programme $P = I_1, I_2, \ldots, I_l$
Programme $P^{-1} = I_l^{-1}, I_{l-1}^{-1}, \ldots, I_1^{-1},$
$P, P^{-1} = I$

Programme propre

Programme $P' = r \leftarrow r - r_i, P, r \leftarrow r + r_i, P^{-1}$

classe *TP*

$TP(R, s, m)$

Classe des fonctions calculées de façon transparente sur R, avec au plus s instructions et utilisant au plus m registres.
$TP(R) = TP(R, polynome(entre), polynome(entree))$

$SkewTP(R, s, m)$

Même chose mais utilisant des ”instructions skew”.
$SkewTP(R) = \#NC^1(R)$

Uniformité

Classe uniforme de circuits algébrique $\Rightarrow$ $TP(R)$ uniforme.

classe *TP*

$TP(R, s, m)$

Classe des fonctions calculées de façon transparente sur R, avec au plus s instructions et utilisant au plus m registres.
$TP(R) = TP(R, polynome(entre), polynome(entree))$

$SkewTP(R, s, m)$

Même chose mais utilisant des ”instructions skew”.
$SkewTP(R) = \#NC^1(R)$

Uniformité

Classe uniforme de circuits algébrique $\Rightarrow$ $TP(R)$ uniforme.

classe *TP*

TP(R, s, m)

Classe des fonctions calculées de façon transparente sur R, avec au plus s instructions et utilisant au plus m registres.
$TP(R) = TP(R, polynome(entre), polynome(entree))$

SkewTP(R, s, m)

Même chose mais utilisant des ”instructions skew”.
$SkewTP(R) = \#NC^1(R)$

Uniformité

Classe uniforme de circuits algébrique $\Rightarrow$ $TP(R)$ uniforme.

Ou'est-ce qu'on peut faire?

Produit binaire

Si P: $r_1 \leftarrow \tau_1 + f_1(x)$ et $r_2 \leftarrow \tau_2 + f_2(x)$, alors:

$r_0 \leftarrow r_0 + r_1 \times r_2 + r_1 \times r_4 + r_2 \times r_3$

P

$r_3 \leftarrow r_3 + r_1$

$r_4 \leftarrow r_4 + r_2$

$r_0 \leftarrow r_3 + r_1 \times r_2$

P^{-1}

$r_0 \leftarrow r_0 - r_1 \times r_4 - r_2 \times r_3$

Donne:

$r_0 \leftarrow \tau_0 + f_1(x) \times f_2(x)$

Ou'est-ce qu'on peut faire?

Somme itérée

Si P: $r_i \leftarrow \tau_i + f_i(x), \forall i \in \{1, 2, \ldots, k\}$, alors:

$r_0 \leftarrow r_0 - r_i, \forall i \in \{1, 2, \ldots, k\}$
P
$r_0 \leftarrow r_0 + r_i, \forall i \in \{1, 2, \ldots, k\}$

Donne:
$r_0 \leftarrow \tau_0 + \sum_{i=1}^{k} f_i(x)$

On a maintenant la classe $\#SAC^1(R) \subseteq TP(R)$!

Ou'est-ce qu'on peut faire?

Somme itérée

Si P: $r_i \leftarrow \tau_i + f_i(x), \forall i \in \{1, 2, \ldots, k\}$, alors:

$r_0 \leftarrow r_0 - r_i, \forall i \in \{1, 2, \ldots, k\}$
P
$r_0 \leftarrow r_0 + r_i, \forall i \in \{1, 2, \ldots, k\}$

Donne:
$r_0 \leftarrow \tau_0 + \sum_{i=1}^{k} f_i(x)$

On a maintenant la classe $\#SAC^1(R) \subseteq TP(R)$!

Aller plus loin

Produit itérée

m_i: entrée, constante ou registre, alors:

$r_i \leftarrow r_i - r_{i-1} \times m_i, \forall i \in \{k, k-1, \ldots, 2\}$
$r_1 \leftarrow r_1 + m_1$
$r_i \leftarrow r_i + r_{i-1} \times m_i, \forall i \in \{2, 3, \ldots, k\}$

Donne:
$r_i \leftarrow \tau_i + \prod_{i=1}^{k} m_i$

Aller plus loin

Puissance

Formule pour la puissance:

$$x^k = (a+x)^k + \sum_{i=1}^{k} (-1)^i \binom{k}{i} a^i (a+x)^{k-i}$$

Aller plus loin

Puissance

Si P: $r \leftarrow \tau + f(x)$, alors:

$c_i = (-1)^i \binom{k}{i}$ constantes

$r_0 \leftarrow r_0 + c_i \times r_i \times r^{k-i}, \forall i \in \{1, 2, \ldots, k\}$

P

$r_i \leftarrow r_i + r^i, \forall i \in \{1, 2, \ldots, k\}$

$r_0 \leftarrow r_0 + r^k$

P^{-1}

$r_0 \leftarrow r_0 - c_i \times r_i \times r^{k-i}, \forall i \in \{1, 2, \ldots, k\}$

Donne:

$r \leftarrow \tau + [f(x)]^k$

Aller plus loin

Valeur exacte (not)

Petit Théorème de Fermat:

Sur un anneau $R = \mathbb{Z}_p$, p premier, $x \neq 0$, $x \in R$ alors

$$x^{p-1} = 1 \ \ (mod\ p)$$

Pour nous:

$$(\sum_{i=1}^{k} f_i(x) - s)^{p-1} = 1 \ \text{ si } \ \sum_{i=1}^{k} f_i(x) \neq s, \ \ 0 \text{ sinon}$$

Notation:

$$[\![\sum_{i=1}^{k} f_i(x) \neq s]\!]$$

Aller plus loin

Valeur exacte (not)

Petit Théorème de Fermat:

Sur un anneau $R = \mathbb{Z}_p$, p premier, $x \neq 0$, $x \in R$ alors

$$x^{p-1} = 1 \pmod{p}$$

Pour nous:

$$(\sum_{i=1}^{k} f_i(x) - s)^{p-1} = 1 \text{ si } \sum_{i=1}^{k} f_i(x) \neq s, \text{ 0 sinon}$$

Notation:

$$[\![\sum_{i=1}^{k} f_i(x) \neq s]\!]$$

Aller plus loin

Valeur exacte (not)

Petit Théorème de Fermat:

Sur un anneau $R = \mathbb{Z}_p$, p premier, $x \neq 0$, $x \in R$ alors

$$x^{p-1} = 1 \ \ (mod\ p)$$

Pour nous:

$$(\sum_{i=1}^{k} f_i(x) - s)^{p-1} = 1 \ \text{ si } \ \sum_{i=1}^{k} f_i(x) \neq s, \ \ 0 \text{ sinon}$$

Notation:

$$[\![\sum_{i=1}^{k} f_i(x) \neq s]\!]$$

Aller plus loin

Majorité

Si $b_1, b_2, \ldots, b_k$ bits, alors:

$$[\![\sum_{j=\frac{k}{2}+1}^{k} [\![\sum_{i=1}^{k} b_i \neq j]\!] \neq \frac{k}{2}]\!]$$

Donne:

$MAJ(b_1, b_2, \ldots, b_k)$

On a maintenant la classe $TC^1 \subseteq TP(\mathbb{Z}_p)$!
...grand premier p

Aller plus loin

Majorité

Si $b_1, b_2, \ldots, b_k$ bits, alors:

$$[\![\sum_{j=\frac{k}{2}+1}^{k} [\![\sum_{i=1}^{k} b_i \neq j]\!] \neq \frac{k}{2}]\!]$$

Donne:

$MAJ(b_1, b_2, \ldots, b_k)$

On a maintenant la classe $TC^1 \subseteq TP(\mathbb{Z}_p)$!
...grand premier p

Espace catalytique

Catalyseur

Substance qui augmente la vitesse d'une réaction chimique sans paraître participer à cette réaction. (Larousse)

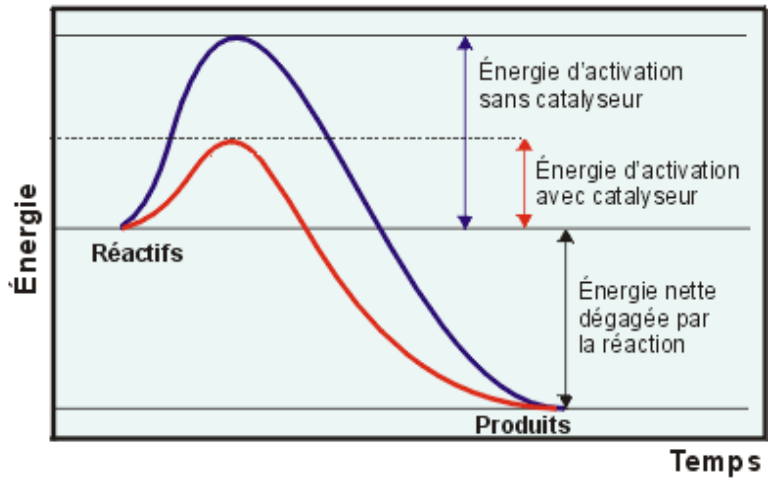


Figure: Réaction chimique avec ou sans catalyseur

Machine de Turing

$CSPACE(s(n), s_a(n))$

Classe des langages décidables par une machine de Turing utilisant $s(n)$ espace sur sa bande de travail et $s_a(n)$ espace sur sa bande auxiliaire qui doit être remise en état intial à la fin sur entrée de longueur n.

$CSPACE(s(n))$

$CSPACE(s(n)) = CSPACE(s(n), 2^{O(s(n))})$

Machine de Turing

$CSPACE(s(n), s_a(n))$

Classe des langages décidables par une machine de Turing utilisant $s(n)$ espace sur sa bande de travail et $s_a(n)$ espace sur sa bande auxiliaire qui doit être remise en état intial à la fin sur entrée de longueur n.

$CSPACE(s(n))$

$$CSPACE(s(n)) = CSPACE(s(n), 2^{O(s(n))})$$

CSPACE($log(n)$)

Idée : simuler les circuits TC^1 à l'aide d'une machine de Turing.

CSPACE

- $TC^1 \subseteq CSPACE(log(n))$
- $NC^1 \subseteq SAC^1 \subseteq AC^1 \subseteq TC^1$
- $NC^1 \subseteq L \subseteq NL \subseteq SAC^1$
- $SAT \notin CSPACE(O(n))$ avec l'hypothèse du exponential-time

Conclusion

Alors une mémoire supplémentaire remplie et incomprésible augmente la puissance d'un ordinateur!

CSPACE

- $TC^1 \subseteq CSPACE(log(n))$
- $NC^1 \subseteq SAC^1 \subseteq AC^1 \subseteq TC^1$
- $NC^1 \subseteq L \subseteq NL \subseteq SAC^1$
- $SAT \notin CSPACE(O(n))$ avec l'hypothèse du exponential-time

Conclusion

Alors une mémoire supplémentaire remplie et incomprésible augmente la puissance d'un ordinateur!

Merci

Références

- H. Buhrman, R, Cleve, M. Koucky, B. Loff, F. Speelman, *Computing with a full memory : catalytic space*, Symposium on Theory of Computing (STOC 2014), pp.857–866 url = http ://doi.acm.org/10.1145/2591796.2591874
- M. Ben-Or and R. Cleve, *Computing algebraic formulas using a constant number of registers*, SIAM Journal on Computing, 21(1):54–58, 1992.