Circuits et nombres 2-adiques

Gérard Berry

Chaire Algorithmes, machines et langages

Collège de France

Cours 2, le 9 avril 2013

COLLÈGE
DE FRANCE
1530

Source du cours

Ce cours reprend la théorie / pratique de Jean Vuillemin (ENS)

J. Vuillemin. *On circuits and numbers*, IEEE Trans. on Computers, 43:8:868-79, 1994.

Nombres 2-adiques

- R est une complétion de Q. Est-ce la seule?

  Non : nombres p-adiques

- Beau, mais utile ? *cf. Alain Connes / JP Changeux*
- Jean Vuillemin: les entiers 2-adiques sont le bon modèle des circuits numériques

2_Z : anneau des entiers 2-adiques

$x = {}_2x_0x_1x_2$ … poids faibles d'abord

opérations $+$ et $\times$ de gauche à droite

$0 = {}_200000\ldots = {}_2(0)$

$1 = {}_210000\ldots = {}_21(0)$ $\quad -1 = {}_211111\ldots = {}_2(1)$

$2 = {}_201000\ldots = {}_201(0)$ $\quad -2 = {}_201111\ldots = {}_20(1)$

$x = {}_2101010\ldots = {}_2(10)$

$= {}_2100000\ldots + {}_2001010\ldots$

$= 1 + 4x$

$\boxed{x = -1/3}$

$y = {}_2010101\ldots$

$x + y = -1$

$\boxed{x = -2/3}$

Anneau mais pas corps !

$\pm p/q$ existe pour p, q entiers ssi q est impair
(cf. Euclide)

1/2 n'existe pas
car la somme x_0+x_0 ne peut pas valoir 1

$2\mathbb{Z}$ comme algèbre Booléenne

- 2-adique x vu comme l'ensemble $\{ i \mid x_i = 1 \}$

  exemple: $-1/3 = {}_2101010... = \{ i \mid i \text{ pair} \}$

- Opérations Booléennes point par point

  $x \wedge y \qquad x \vee y \qquad \neg x$

  $(x \wedge y)_n = x_n \wedge y_n$ etc.

- Relation arithmético-logique fondamentale

$$\boxed{x + \neg x = -1}$$

$$\begin{array}{r} {}_2\mathtt{100011...} \\ {}_2\mathtt{011100...} \\ \hline {}_2\mathtt{111111...} \end{array}$$

Espace Métrique de Cantor

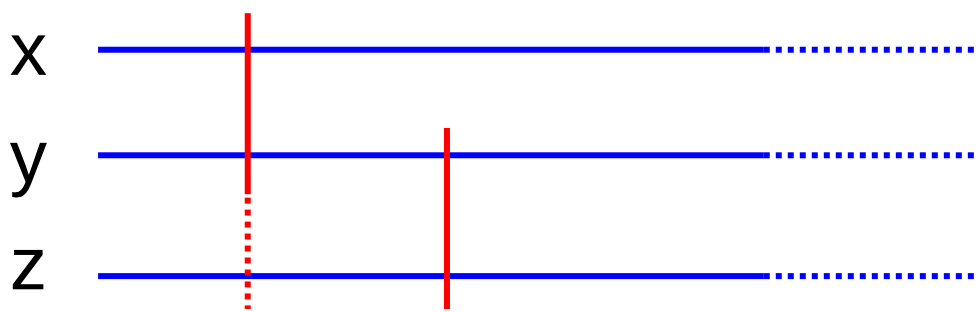
$d(x,x) = 0$

$d(x,y) = 2^{-n}$ $\quad n$ minimal tel que $x_n \neq y_n$

Exemple : $d\ ({}_2011\underline{1}1\ldots,\ {}_2011\underline{0}1\ldots = 1/8)$

- <u>Lemme :</u> 2z est ultramétrique :

$$d(x,z) \leq \max(d(x,y), d(y,z))$$

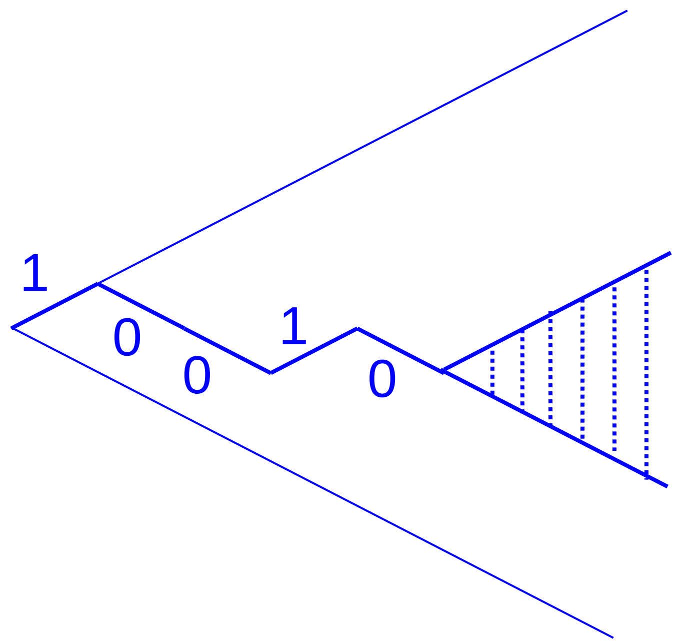


Espace Métrique de Cantor

- Base d'ouverts : préfixes finis

  $\{{}_2x_0x_1...x_ny_0y_1...y_n... \mid y \in 2z\}$

ex. ouvert de préfixe ${}_2$10010



- Compact – très différent des réels !

Fonctions continues et synchrones

- Lemme : $f : 2^{\mathbb{Z}} \rightarrow 2^{\mathbb{Z}}$ continue ssi $f(x)_n$ dépend seulement d'un nombre fini de x_m

- Définition : $f : 2^{\mathbb{Z}} \rightarrow 2^{\mathbb{Z}}$ synchrone ssi calculable par un circuit synchrone (de mémoire finie ou infinie)

- Théorème $f : 2^{\mathbb{Z}} \rightarrow 2^{\mathbb{Z}}$ est synchrone si et seulement si $f(x)_n$ dépend seulement de $x_0 x_1 \ldots x_n$

$$\boxed{\forall\, x,y.\ d(f(x),f(y)) \leq d(x,y)}$$

Preuve : « seulement si » trivial, « si » voir plus tard

Circuits de Moore et fonctions contractantes

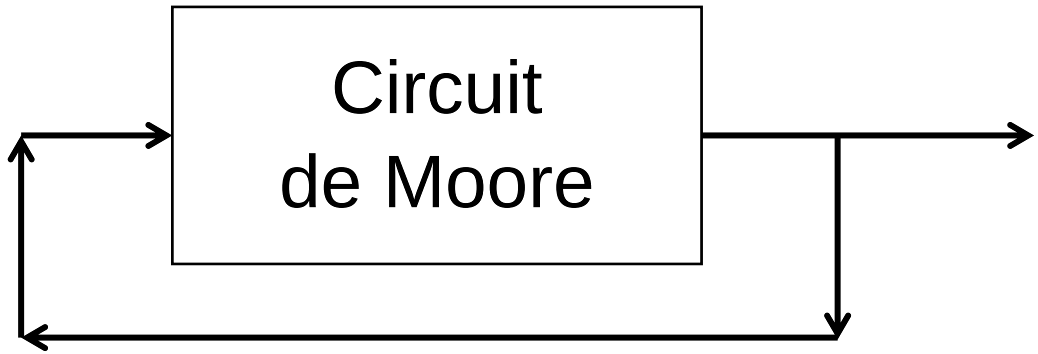
- Un circuit est de Moore ssi tout fil entre entrée et sortie passe par au moins un registre

- Une fonction $f : 2Z \rightarrow 2Z$ contractante ssi $f(x)_n$ dépend seulement de $x_0 x_1 \ldots x_{n-1}$

$$\boxed{\forall\ x,y.\ d(f(x),f(y)) < d(x,y)} \longleftarrow \text{Lifschitz}$$

- <u>Théorème :</u> une fonction est contractante ssi elle est réalisable par un circuit de Moore

Rebouclage des circuits de Moore



$$\forall\ x,y.\ d(f(x),f(y)) < d(x,y)$$

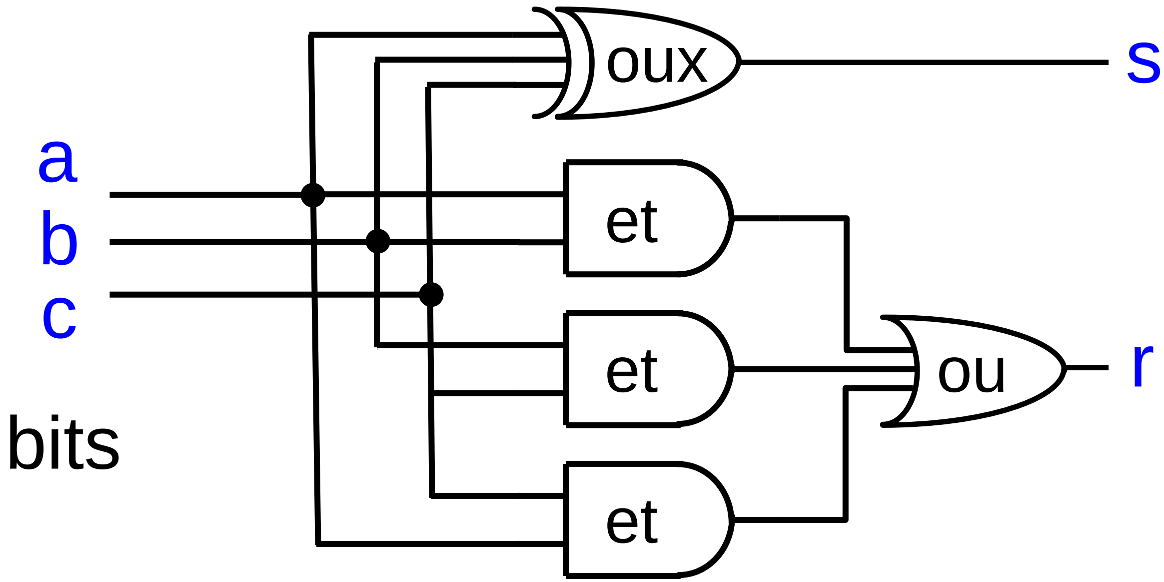
$$\Updownarrow$$

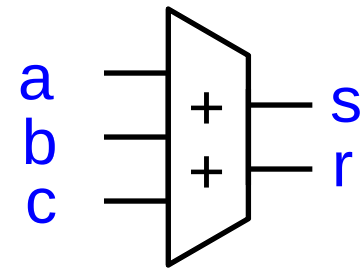
$$\boxed{\forall\ x,y.\ d(f(x),f(y)) < 0{,}6\ d(x,y)}$$

Lifschitz

<u>Théorème de Banach :</u> toute fonction Lifschitzienne sur un compact a un point fixe unique

Additionneur 3 bits (Full Adder)

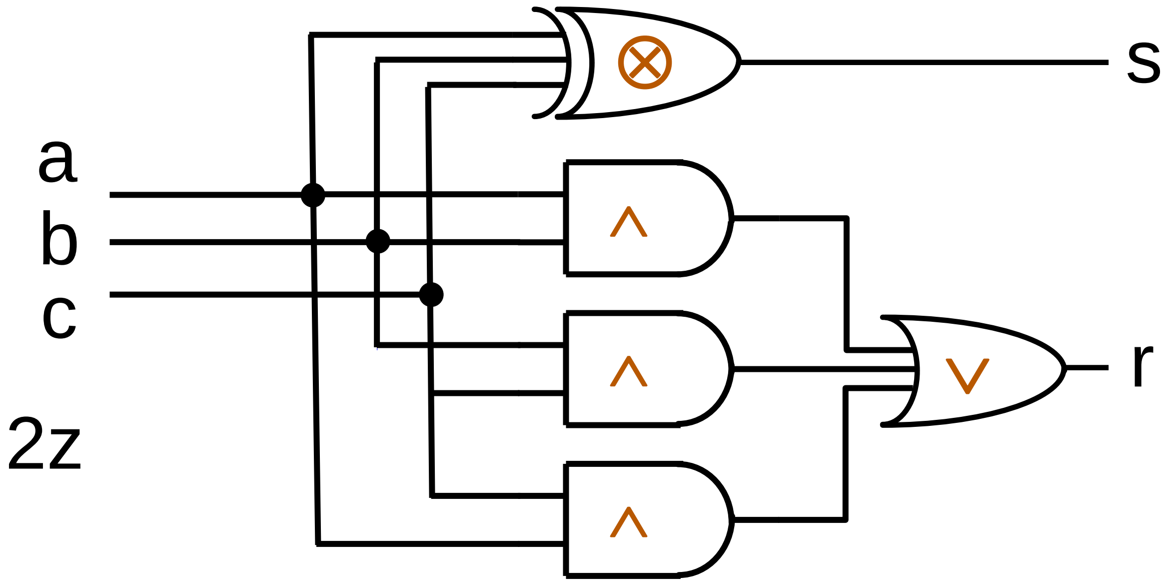


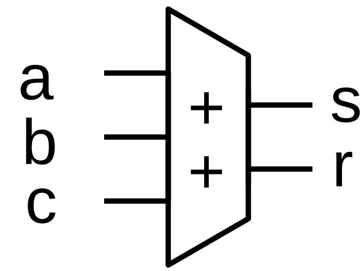


s = a oux b oux c

r = (a et b) ou (b et c) ou (c et a)

Additionneur 3 bits (Full Adder)



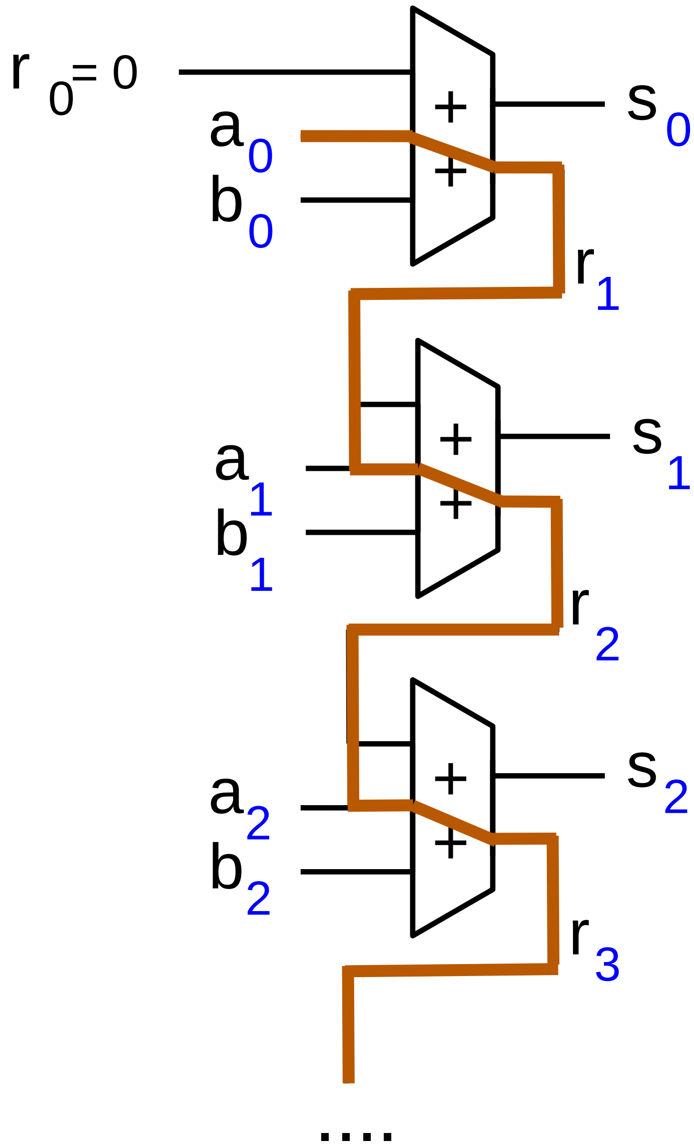


$s = a \otimes b \otimes c$

$r = (a \wedge b) \vee (b \wedge c) \vee (c \wedge a)$

$$\boxed{a + b + c = s + 2r}$$

L'addition dans l'espace



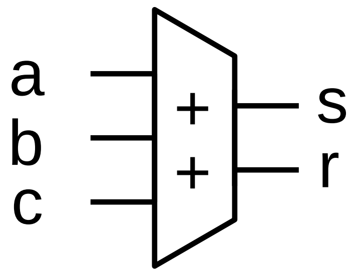
$$\boxed{s = a + b}$$

continuité:
couper à n bits
pour n bits de sortie

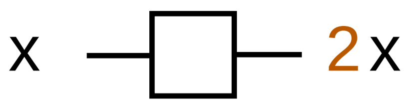
$$s \bullet 2^n = s \bmod 2^n$$

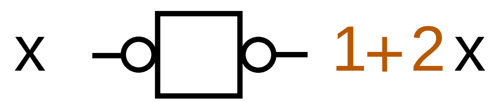
$$\boxed{s \bullet 2^n = a \bullet 2^n + b \bullet 2^n}$$

Opérateurs 2-adiques de base

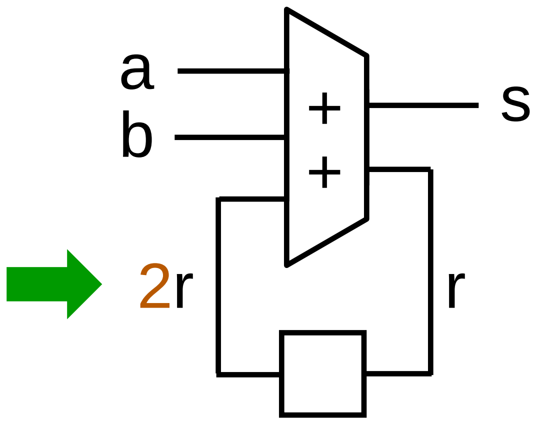


$$a+b+c = s+2r$$





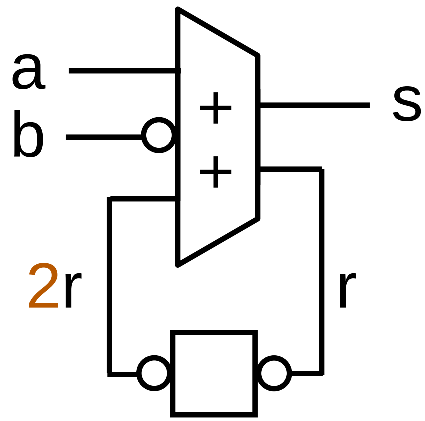
Addition et soustraction dans le temps



$$a+b\cancel{+2}r = s\cancel{+2}r$$

$$\boxed{s = a+b}$$

même équation
que dans l'espace !



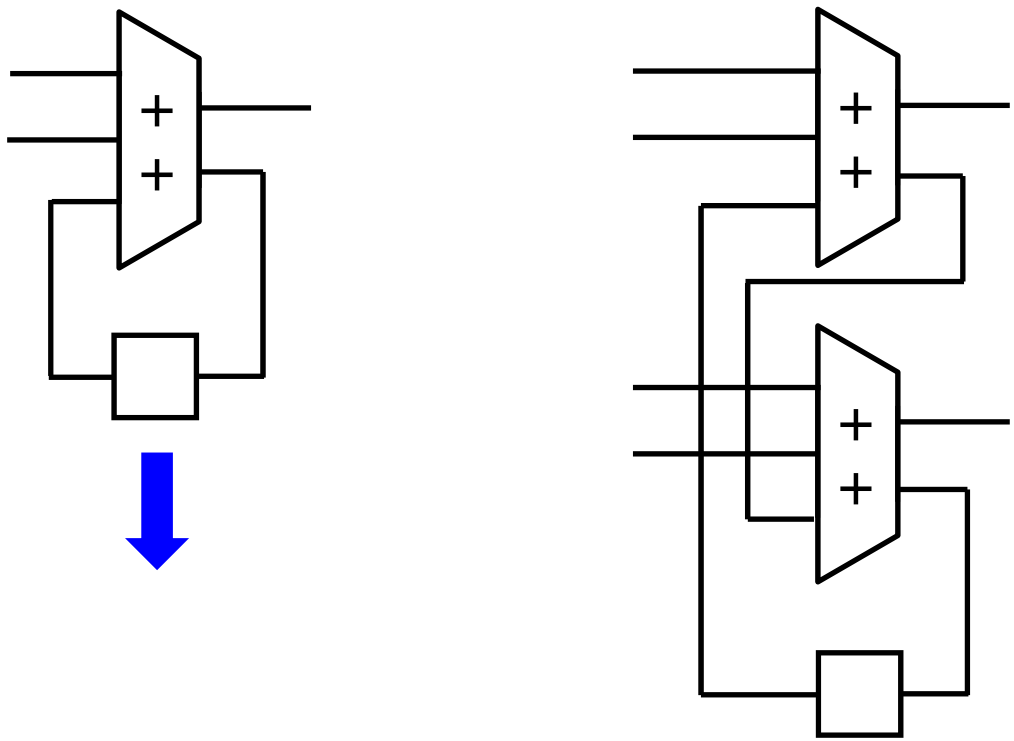
$$a+\neg b+1\cancel{+2}r = s\cancel{+2}r$$

$$b+\neg b = -1$$

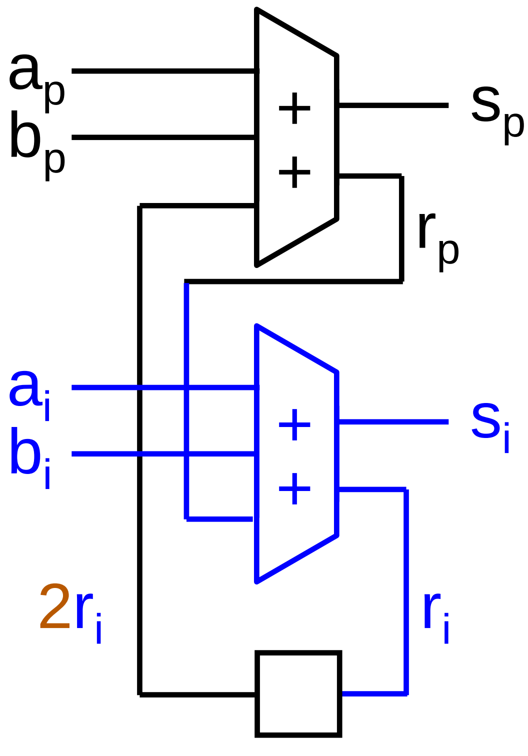
$$\neg b+1 = -b$$

$$\boxed{s = a-b}$$

Addition mixte espace / temps



Addition mixte espace / temps



$$x \odot y = {}_2x_0y_0x_1y_1\ldots$$

$$a = a_p \odot a_i$$

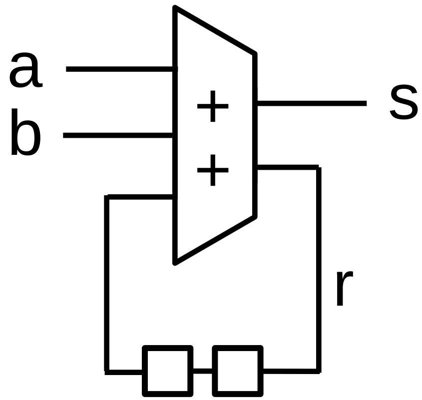
$$b = b_p \odot b_i$$

$$s = s_p \odot s_i$$

$$\boxed{s = a + b}$$

toujours la
même équation !

Addition stéréo



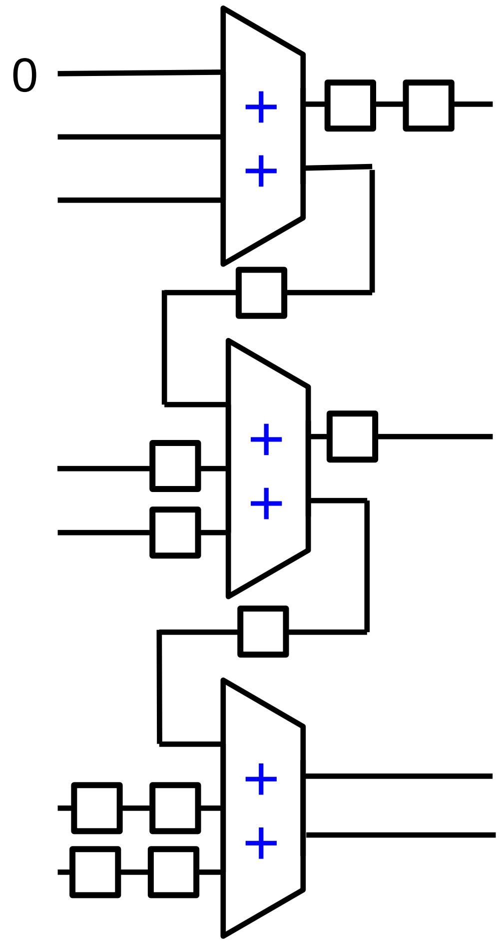
additionneur
bègue

$a = a_p \odot a_i$

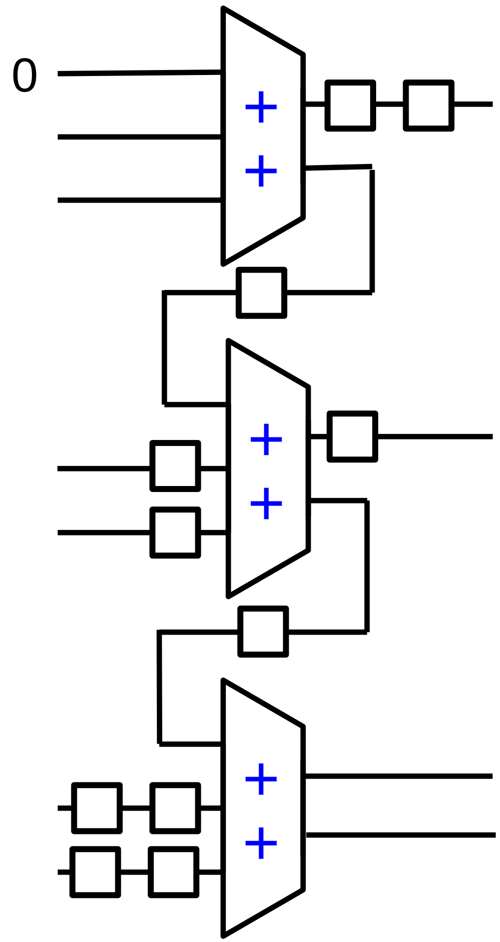
$b = b_p \odot b_i$

$$\boxed{\begin{aligned} s &= s_p \odot s_i \\ s_p &= (a_p + b_p) \\ s_i &= (a_i + b_i) \end{aligned}}$$

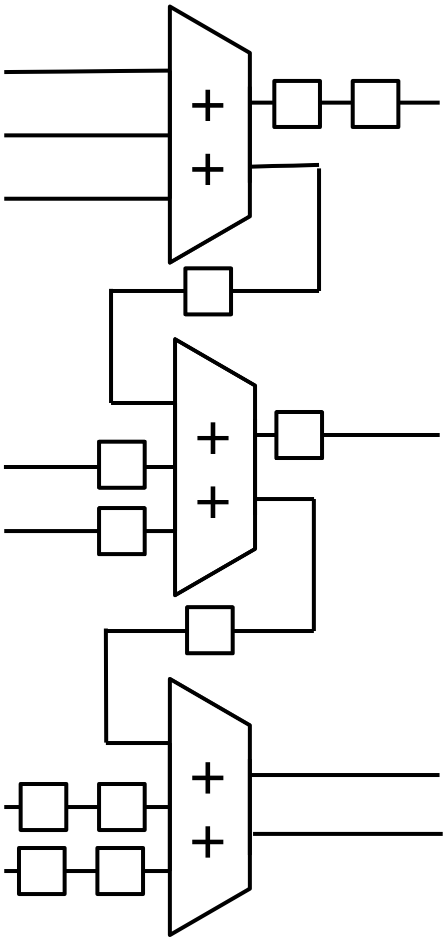
Quelques beaux additionneurs



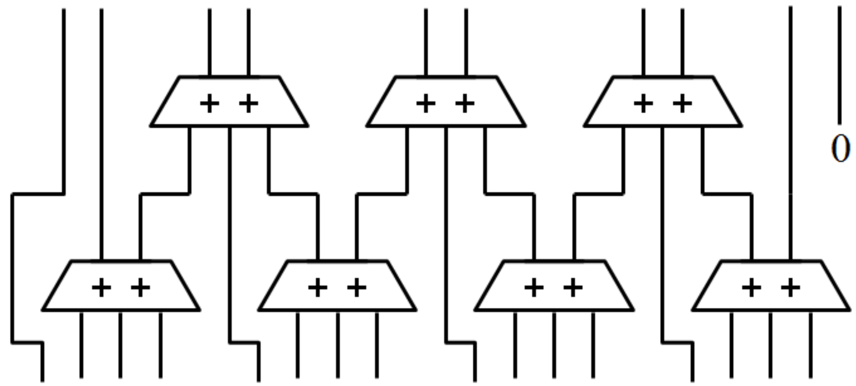
Quelques beaux additionneurs



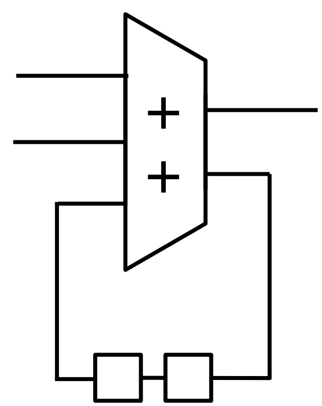
Additionneurs divers



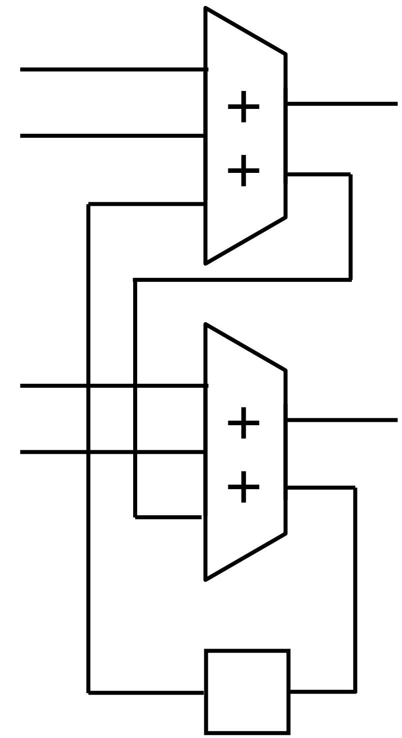
pipeline



sans retenue

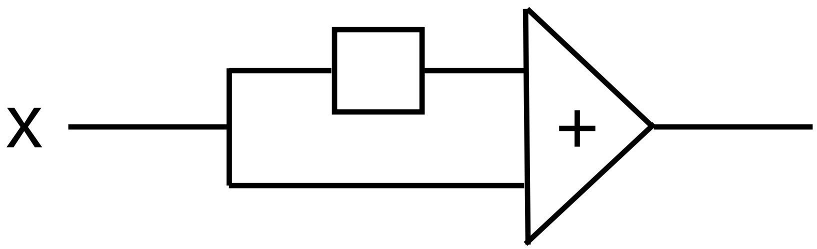


stéréo

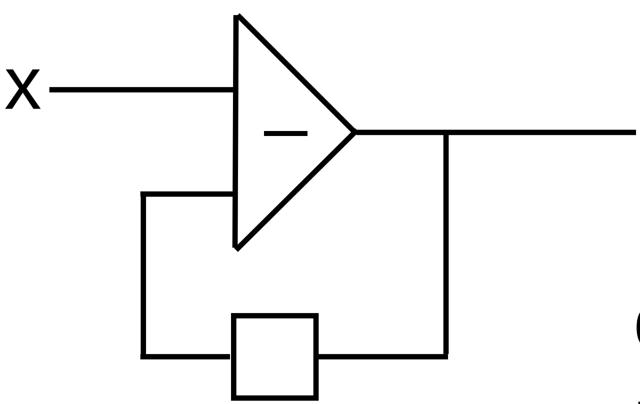


2 par 2

Multiplication et division par des constantes



$x + 2x = 3x$



$x \div 3$

$$\boxed{x \div 3 = x - 2\,(x \div 3)}$$

division seulement
par des entiers impairs!

$x \div 2 =$ prédiction du prochain bit

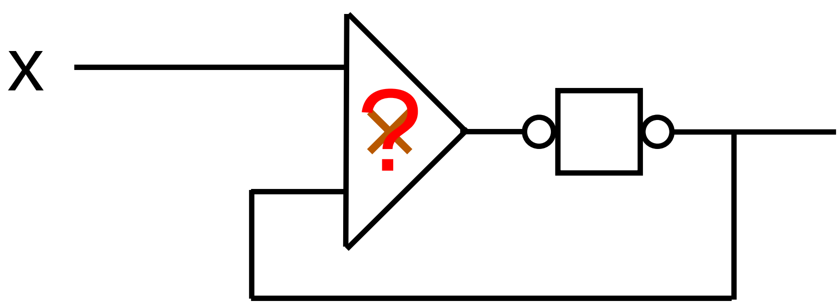
non synchrone !

Quasi-inverse

$$y = 1 \div (1-2x)$$

$$y - 2xy = 1$$

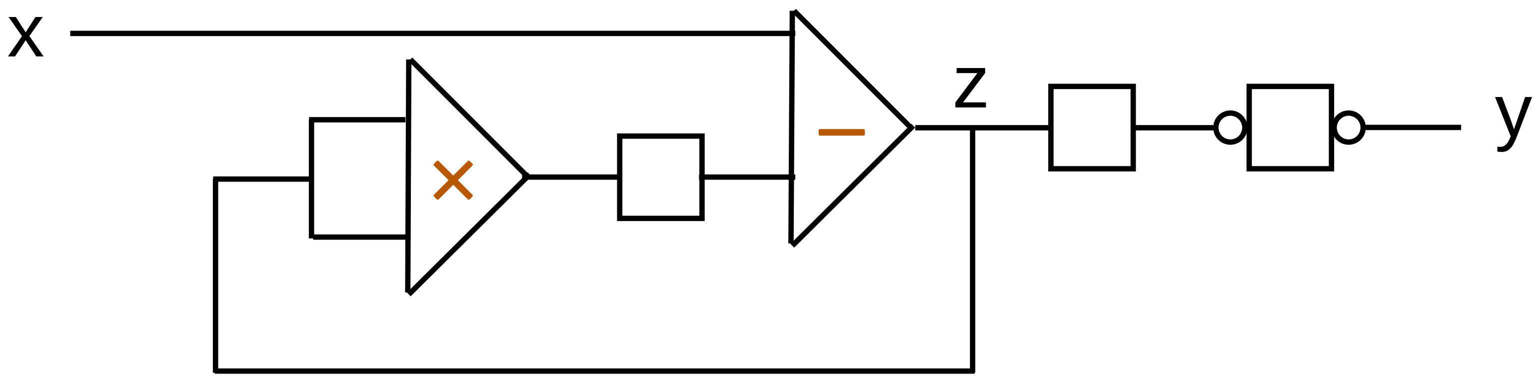
$$y = 1 + 2xy$$



$$y = 1 \div (1-2x)$$

Quasi-racine carrée

$$y = \sqrt{1+8x}$$



$$y = 1+4z$$

$$y^2 = 1+8z+16z^2$$

$$z = x-2z$$

$$y^2 = 1+8x-\cancel{16}z^2+\cancel{16}z^2$$

Forme normale SDD de f : 2z→2z

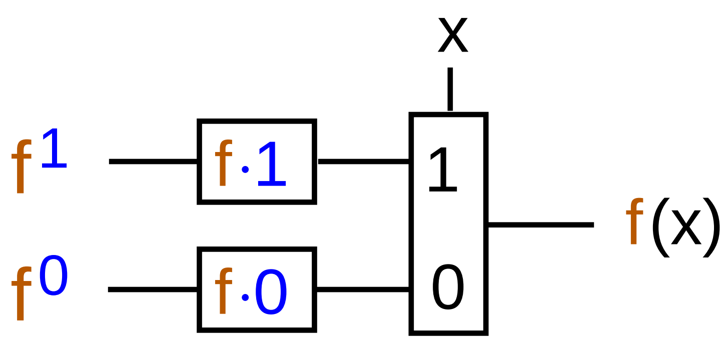
$f{\cdot}0$ = premier bit sorti par f pour l'entrée 0...

$f{\cdot}1$ = ... 1...

$f{\cdot}w$ = dernier bit sorti par f pour le mot fini w

f^0 = 0-prédicteur : $f^0{\cdot}w = f{\cdot}(w0)$ pour tout mot w

f^1 = 1-prédicteur : $f^1{\cdot}w = f{\cdot}(w1)$



$$\boxed{f(x) = \mathrm{mux}(x,\ f{\cdot}1+2f^1(x),\ f{\cdot}1+2f^1(x))}$$

Forme normale SDD de f : 2z→2z

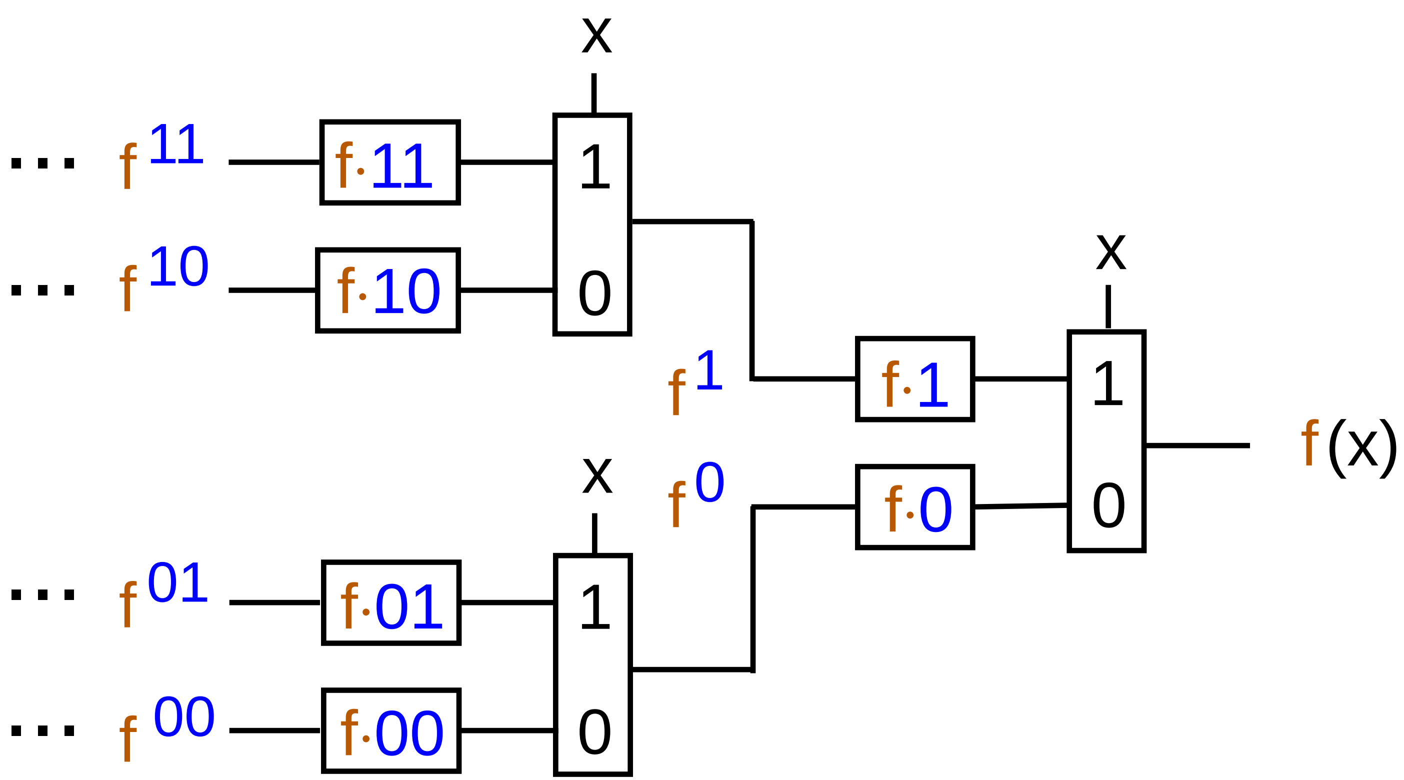
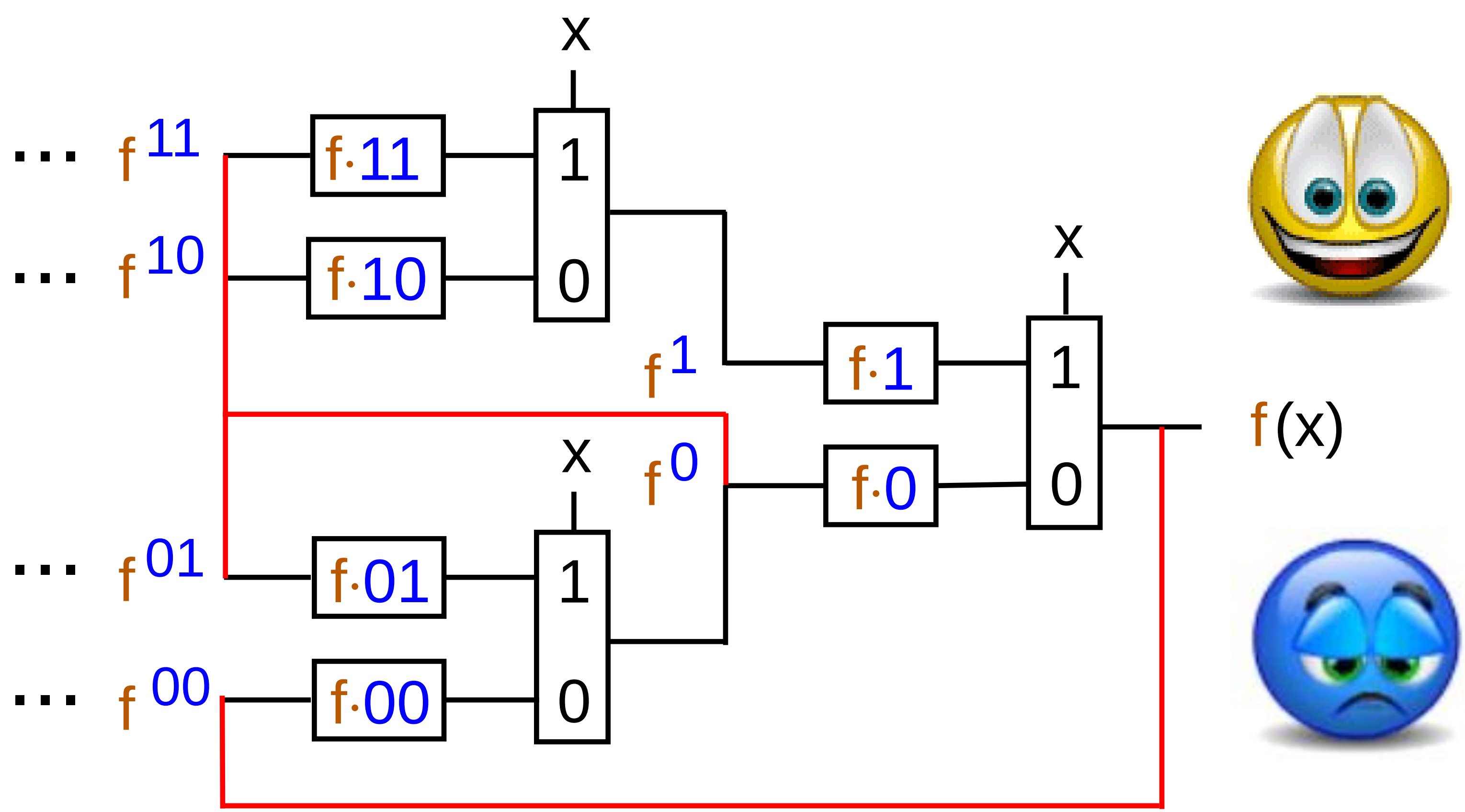


Table de vérité dans l'espace et le temps
La moitié des bits disparaît à chaque cycle

SDD partagé de f : 2z→2z à mémoire finie



f à mémoire finie $\Rightarrow$ nb fini de prédicteurs f^{w} distincts

f à n registres $\Rightarrow$ SDD(f) peut avoir 2^{2^n} registres

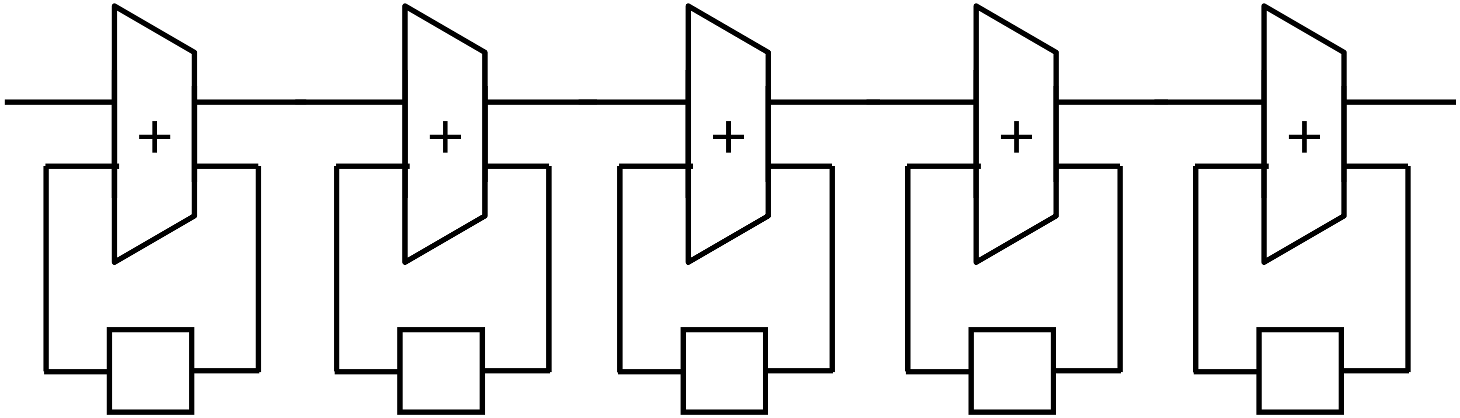
Fonctions continues et circuits

$$x = {}_2x_0x_1x_2\ \ldots \rightarrow\ x \div 2 = {}_2x_1x_2x_3$$

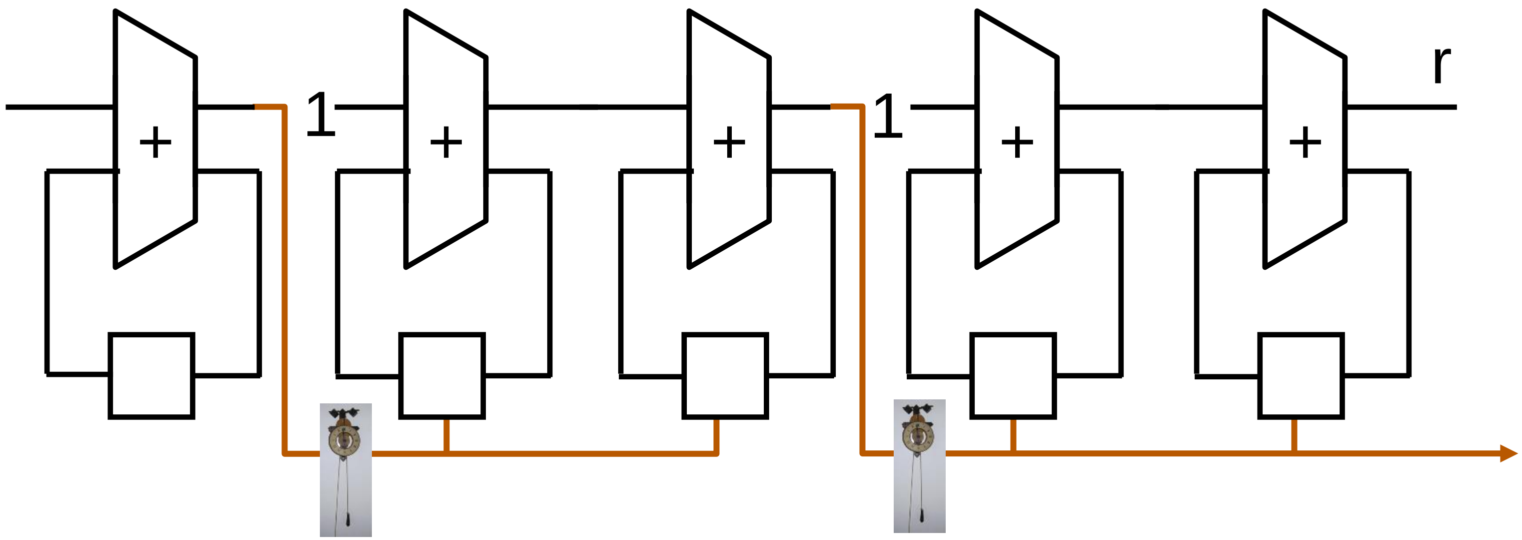
continue mais pas synchrone !
$\Rightarrow$ ralentir le temps

nombre 2-adique : < valeur, validité >

0	0	1	0	1	1	0	1	1	1	0	0	...
0	1	1	0	0	1	1	0	0	1	1	0	...
	0	1			1	0			1			



compteur lent



compteur ultra-rapide en log*(n)

tranches 1, $2^{1} = 2$, $2^{1+2} = 8$, $2^{1+2+8} = 2048$, $2^{1+2+8+2048}$!!

Trace d'une fonction synchrone

$\mathrm{Tr}(f) =_2 f{\cdot}0\ f{\cdot}1\ f{\cdot}00\ f{\cdot}01\ f{\cdot}11\ f{\cdot}000\ \ f{\cdot}001\ f{\cdot}010\ \ldots$

$= f{\cdot}0 + 2\, f{\cdot}1 + 4\ (\mathrm{Tr}(f^0) \odot \mathrm{Tr}(f^1))$

Série formelle sur Z/2Z : $S(f) = \Sigma_n\ \mathrm{Tr}(f)_n\ z^n$

Théorème:
$f : 2z \rightarrow 2z$ est de mémoire finie
ssi S(f) est algébrique dans Z/2Z