Chapitre 12.

POLYNOMES DE VERITE

L'ordinateur est un graphe boolien,

et hors souci de délai

la couleur de toute flèche issue d'un sommet de graphe boolien

est fonction (de vérité) du mot d'entrée,

ce que précise le

Théorème 12

Les fonctions de vérité sont polynômes.

Toute fonction de vérité est exprimable

par son polynôme de vérité

que nous nous proposons de prouver :

Les monômes (de vérité)

en des variables, indéterminées ou lettres

sont les produits commutatifs formels de certaines

en nombre fini et deux à deux distinctes

d'entre elles.

Les polynômes (de vérité) en ces variables

sont les sommes commutatives formelles de certains,

en nombre fini et deux à deux distincts

d'entre ces monômes.

vu wtu v I wvut sont des monômes en t u v w

yx y x I sont les quatre monômes en x y

t I sont les deux monômes en t

vut vu vt tu v u t I sont les huit monômes en t u v

Le nombre des monômes en n lettres égale
le nombre des parties de cet ensemble de n lettres

c'est-à-dire 2^n

Le nombre des polynômes en n lettres égale à son tour
le nombre des parties de l'ensemble des monômes en ces n lettres

c'est-à-dire 2^{2^n} .

Mais le nombre des fonctions de vérité en n variables,

ou fonctions $2^n \longrightarrow 2$

égale lui-même 2^{2^n}

D'où :

Le nombre des fonctions de vérité en n variables
égale
Le nombre des polynômes de vérité en n variables

Or, tout polynôme de vérité V (w ... t)

en les n variables w ... t

<u>détermine</u>

<u>sa</u> fonction de vérité

$2 \to 2^{n}$: w ... t :--> V (w ... t) .

Le théorème 12 affirme la bijectivité

de cette fonction <u>détermine</u>

dont le domaine / but est l'ensemble des polynômes / fonctions de vérité en w ... t.

<u>Domaine</u> et <u>but</u> ayant même nombre fini d'éléments,

la démonstration du théorème 12 se ramène à établir la <u>surjectivité</u> de la fonction <u>détermine</u>. Autrement dit :

Par suite de l'équipotence de domaine et but finis

pour établir que toute fonction de vérité est

exprimable par <u>son</u> polynôme de

suffit à la prouver

exprimable par <u>un</u> polynôme de vérité.

A tout seigneur, tout honneur !

Commençons par <u>polynomiser</u> l'exponentiel à n bits.

A cet effet,

pour tous mots binaires à n bits a et x

notons K (a x)

la valeur de la flèche de sortie numérotée a

causée par l'entrée x

En vertu même de la définition de l'exponentielle,

$K\ (a\ x)$ est la <u>fonction de Kronecker</u> ou <u>équivalence logique</u>

<u>une</u> ssi a égale x

<u>nulle</u> ssi a différent de x

Posant

$$a = a_{n-1} \ldots a_0 \qquad\qquad b = b_{n-1} \ldots b_0$$

suit

$$*_i \,(I + a_i + x_i) = I$$

ssi

pour tout $i < n$: $\quad I + a_i + x_i = I$

ssi

pour tout $i < n$: $\quad a_i = x_i$

ssi

$$a = x$$

D'où

Théorème 13

La fonction de vérité de Kronecker se polynomise

$$K\ (a\ x) = *_i \,(I + a_i + x_i)$$

Comme $I + a_i + x_i$ égale $I + x_i$ ou x_i

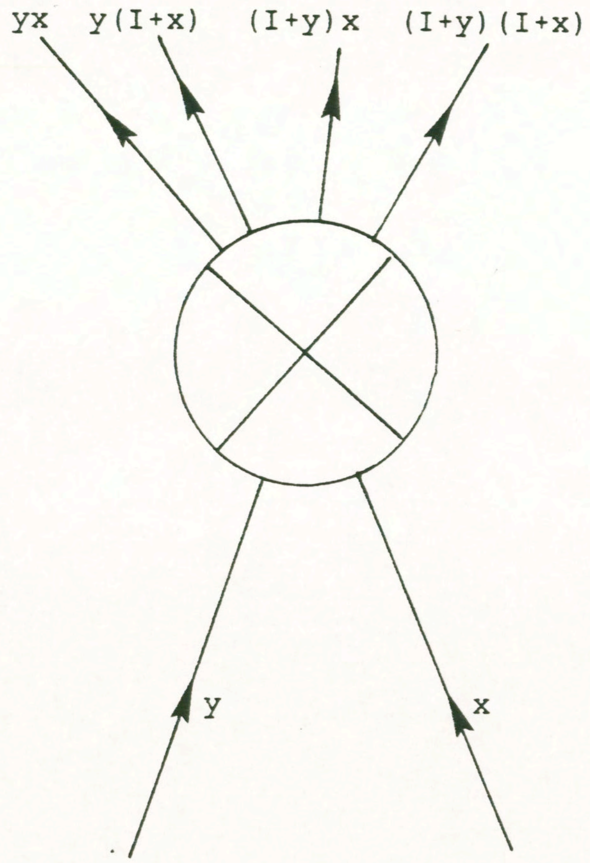
selon que a_i égale o ou I

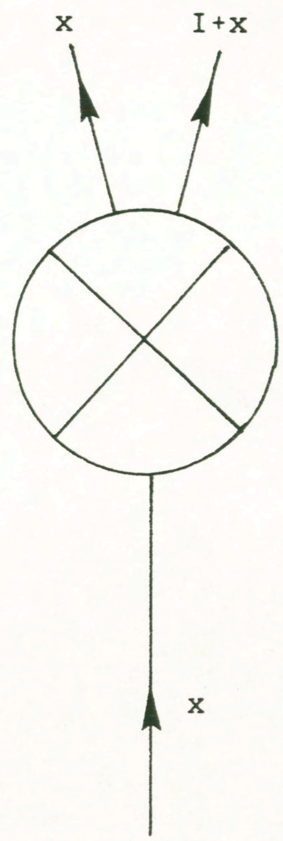
l'exponentiel se polynomise de cette manière expéditive :

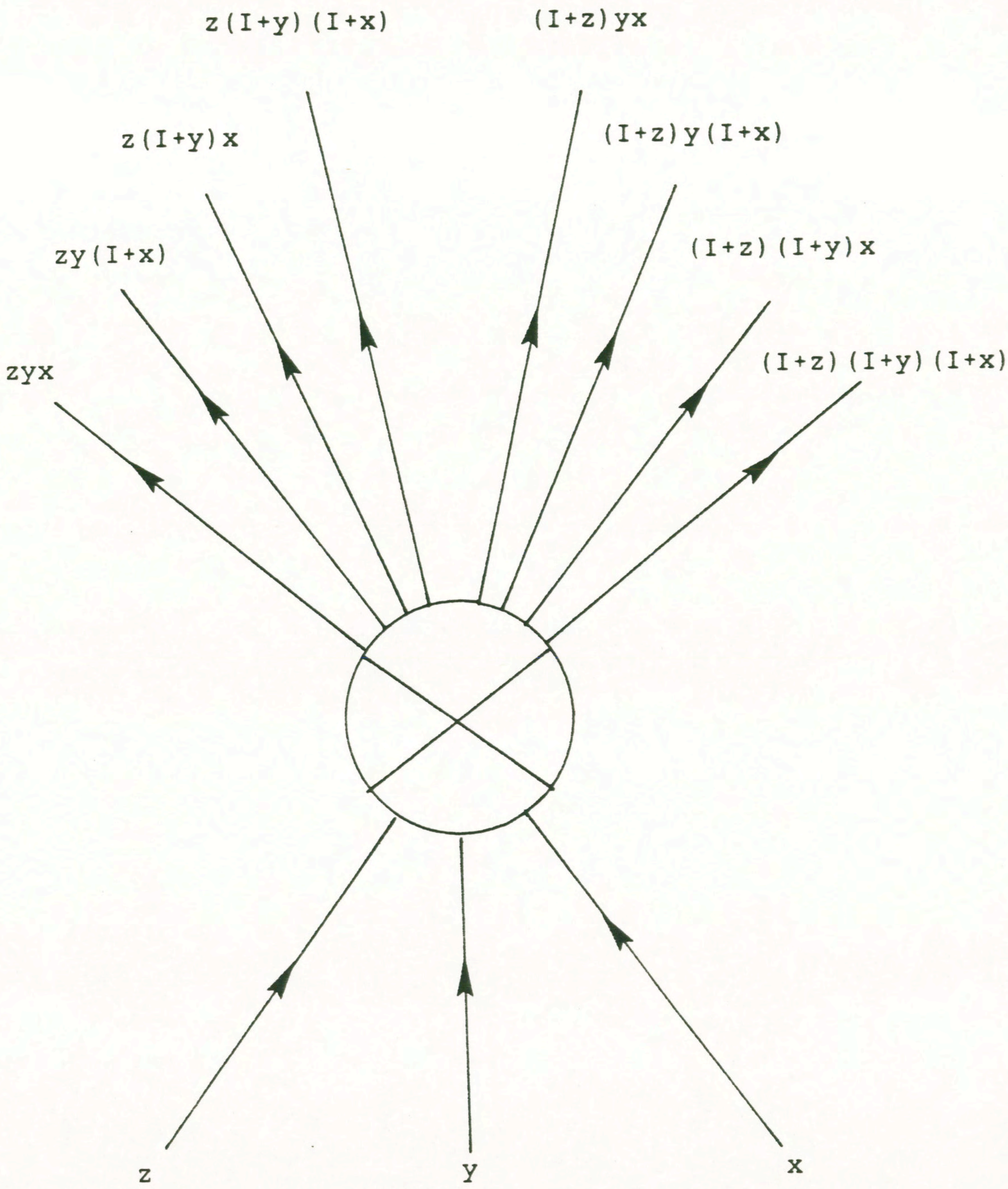
$$K \, (I \quad o \quad I \quad o \quad I \qquad x_4 x_3 x_2 x_1 x_0 \,)$$

$$= \; x_4 \, (I + x_3) \, x_2 \, (I + x_1) \, x_0$$

(où a = IoIoI)






z(I+y)(I+x)
(I+z)yx
z(I+y)x
(I+z)y(I+x)
zy(I+x)
(I+z)(I+y)x
zyx
(I+z)(I+y)(I+x)
z
y
x

Reste à prouver que

la polynomisation désormais acquise des exponentielles

entraine celle de toute fonction de vérité $V : 2^n \longrightarrow 2$

Fixant momentanément le mot binaire à n bits x :

En la somme $\underset{a}{+} K(a\,x) * V(a)$

le coefficient $K(x\,x)$ est <u>un</u>

et les autres $K(a\,x)$ sont nuls.

D'où $V(x) = \underset{a}{+} K(a\,x) * V(a)$

Les $K(a\,x)$ étant déjà polynomisés

la polynomisation de V suit :

$$\boxed{V(x) = \underset{a}{+} \underset{i}{*} (I + a_i + x_i)\, V(a)}$$

où a parcourt les mots binaires à n bits

et i parcourt les naturels $< n$

ou mieux encore

$$\boxed{V(x) = \underset{a}{+} \underset{i}{*} (I + a_i + x_i)}$$

où a parcourt les <u>uns</u> de V

et i les naturels $< n$

La fonction de vérité $V(w \dots t)$ supposée polynomisée,

les polynômes de ses niée préniée et duale

se trouvent aisément :

$$\overline{V}(w \dots t) = I + V(w \dots t)$$

$$\underline{V}(w \dots t) = V(I + w \dots I + t)$$

$$V^{*}(w \dots t) = I + V(I + w \dots I + t)$$

En particulier :

$$p \text{ ET } q = (\text{ET } p\, q) = pq$$

$$p \text{ OU } q = (\text{OU } p\, q) = I + (I+p)(I+q)$$

$$(\text{ET } p\, q\, r) = pqr$$

$$(\text{OU } p\, q\, r) = I + (I+p)(I+q)(I+r)$$

$$(\text{NI } p\, q\, r) = (I+p)(I+q)(I+r)$$

$$(\text{NAND } p\, q\, r) = I + pqr$$

La fonction de vérité V

est autopréniée si et seulement si

$$V(w \dots t) = V(I + w \dots I + t)$$

et autoduale si et seulement si

$$V(w \dots t) = I + V(I + w \dots I + t)$$

Les fonctions de vérité en zéro variable

sont les constantes o et I

niées mutuelles

et toutes deux autopréniées et autoduales.

Les fonctions de vérité en la seule variable <u>effective</u> x

sont les polynômes x et $I + x$

niés et préniés mutuels et tous deux autoduaux

Parmi les fonctions de vérité en les deux variables p q figurent déjà les deux constantes, les deux polynômes en p et les deux polynômes en q : o I p I+p q I+q

Restent les dix polynômes à deux variables effectives, partagés en deux quatuors et une paire

OU	NI
p + q + pq	I + p + q + pq

quatuor majeur

I + pq	pq
NAND	ET

p ===> q	p =/=> q
I + p + pq	p + pq

quatuor mineur

I + q + pq	q + pq
p <=== q	p <=/= q

disjonction exclusive	paire	équivalence logique
p + q		I + p + q

E X E R C I C E

Le calcul propositionnel polynomial que nous ont légué Boole et C.S. Peirce est une merveilleuse petite machine à penser logiquement, apte à débrouiller sans tension des situations a priori compliquées et confuses. Comme ce calcul est en soi d'une simplicité aussi extrême que le maniement de la baguette du chef d'orchestre, tout l'art réside en la mise en polynôme. Aussi, convient-il d'intégrer un certain nombre de principes simples et de reconnaître quelques repères typiques du paysage boolien, permettant une orientation aisée, et auxquels il soit possible de se fier en cas de difficulté.

1. L'addition et la multiplication des polynômes booliens sont associatives et commutatives. Le polynôme <u>un</u> I est le neutre pour la multiplication. Le polynôme nul o est le neutre pour l'addition et l' absorbant pour la multiplication. La multiplication distribue l'addition et tout polynôme de vérité vérifie $P + P = o$ et $P * P = P$.

2. Dans le cadre des nombres naturels, +1 sonne la liberté par l'envol de la litanie 0 1 2 3 4 5 6 7 ... Dans le cadre boolien, +I manifeste la volonté de liberté et d'indépendance en disant NON !

3. Tout polynome de vérité vérifie Non Non P = P

4. Comme la vérité n'admet que les deux valeurs <u>une</u> et <u>nulle</u>, non nulle est une et non une est nulle

non nul est un et non un est nul

5. La conjonction d'une suite de polynômes de vérité est leur produit boolien exprimable de multiples manières

(ET P Q R) = PQR = P ET Q ET R

ou mieux encore, mais rarement en dehors de la langue vulgaire

ET P ET Q ET R

6. La conjonction ou produit de vérité est nul(le)

si et seulement si

l'un au moins des facteurs est nul.

La conjonction à un seul facteur égale donc ce facteur,

ce qui s'écrit

ET x = x

Sans facteur,

la conjonction de l'ensemble vide est sans facteur nul

et se trouve donc <u>une</u>

ce qui s'écrit plaisamment

(ET) = I

et dit, qu'en calcul boolien, tout produit de zéro facteur est <u>un</u>

ce que traduit encore la formule insidieuse

$$X^{0} = I$$

aux particularisations perverses

$$o^{0} = I \qquad\qquad I^{0} = I$$

non nul est un et non un est nul

5. La conjonction d'une suite de polynômes de vérité est leur produit boolien exprimable de multiples manières

(ET P Q R) = PQR = P ET Q ET R

ou mieux encore, mais rarement en dehors de la langue vulgaire

ET P ET Q ET R

6. La conjonction ou produit de vérité est nul(le)

si et seulement si

l'un au moins des facteurs est nul.

La conjonction à un seul facteur égale donc ce facteur,

ce qui s'écrit

ET x = x

Sans facteur,

la conjonction de l'ensemble vide est sans facteur nul

et se trouve donc <u>une</u>

ce qui s'écrit plaisamment

(ET) = I

et dit, qu'en calcul boolien, tout produit de zéro facteur est <u>un</u>

ce que traduit encore la formule insidieuse

$$X^{0} = I$$

aux particularisations perverses

$$o^{0} = I \qquad\qquad I^{0} = I$$

7. Le produit boolien de tout nombre fini non nul n

de facteurs égaux

égale ce facteur :

$$X^n = X$$

8. L'observation commune

NI R NI Q NI P

= ET NON R ET NON Q ET NON P

déjà traduite

Conjonction et Exclusion sont préniées mutuelles

s'exprime encore

NI P NI Q NI R

= (NI P Q R)

= (I + P) (I + Q) (I + R)

= I + P + Q + R + PQ + PR + QR + PQR

L'exclusion d'une suite de fonctions de vérité

est leur polynôme boolien complet.

(NI X Y Z) = I + X + Y + Z + XY + XZ + YZ + XYZ

(NI X Y) = I + X + Y + XY

(NI X) = I + X

(NI) = I

9. La disjonction OU , le vel des Anciens Romains ,

est la disjonction non exclusive.

La disjonction	est	une	ssi l'un au moins de ses termes est un
L' exclusion		nulle	

Disjonction et exclusion sont niées mutuelles.

Des usagers de la langue anglaise ont traduit ce fait en nommant l'exclusion NOR = Not OR et nous fîmes comme eux.

En français : NI = NON OU ou encore OU = NON NI

En polynôme : OU = I + NI

Sachant NI polynôme complet suit :

OU est le est polynôme complet amputé du terme constant

(OU X Y Z) = X + Y + Z + XY + XZ + YZ + XYZ

(OU X Y) = X + Y + XY

(OU X) = X

(OU) = o

10. L'incompatbilité de Sheffer est la négation de la conjonction

à l'anglaise nommée NAND

(NAND X Y Z) = I + XYZ

(NAND X Y) = I + XY

(NAND X) = I + X

(NAND) = I + I = o

11. (ET) = I = (NI)

(OU) = o = (NAND)

12. Conjonction et disjonction sont duales mutuelles

ce que traduit la langue polynôme boolienne

(ET X Y Z) = X . Y . Z

(OU X Y Z) = I + (I + X) (I + Y) (I + Z)

13. L'exclusion NI et l'incompatibilité NAND

sont duales mutuelles

ce que confirment les développements polynômiaux booliens

(NAND X Y Z) = I + X Y Z

(NI X Y Z) = I + I + (I + X) (I + Y) (I + Z)

14. La négation ou NON est indifféremment

l' exclusion ou l'incompatibilité

à entrée unique

(NON X) = (NI X) = (NAND X) = I + X

Comme exclusion et incompatibilitté viennent de se montrer

duales mutuelles

la négation NON se trouve autoduale,

ce dont voici vérification directe triviale

I + X

= I + I + I + X

15. Selon la philosophie boolienne

adoptée en catimini par l'ordinateur,

```
:---  Le principe  ---:                  :--- le principe ---:
:                     :                  :                   :
:  de contradiction   :       et         :  du tiers exclu   :
:                     :                  :                   :
:---------------------:                  :-------------------:
```

verticalement énoncés :

```
                         La

                         :
     conjonction         :          disjonction
                         :

 d'une proposition et de sa négation est toujours

                         :
        fausse           :             vraie
                         :
```

sont duaux mutuels.

Et comme ce calcul élémentaire

$$P \cdot (I + P) = P + P = o$$

prouve le Principe de contradiction d'Aristote,

on en conclut que

l'optique boolienne affirme à la fois

le Principe de contradiction et le Principe du tiers exclu.

16. Calcul à partir d'une des définitions de l'implication :

$P \Longrightarrow Q \quad = \quad \text{NON } P \text{ OU } Q \quad = \quad I + P \text{ OU } Q$

$= \quad I + P + Q + (I + P) \cdot Q \quad = \quad I + P + Q + Q + PQ$

$= \quad I + P + PQ \quad = \quad I + P (I + Q)$

$= \quad \text{NON } P \text{ ET NON } Q$

12. 16

17. Sur la formule

$$P \Longrightarrow Q \quad = \quad I + P\,(I + Q)$$

se lit :

prénier $P \Longrightarrow Q$ c'est échanger P Q

ou mieux encore

prénier une implication c'est la retourner,

reformulation, à la hussarde, du principe de contraposition :

la préniée d'une implication est sa retournée

$$P \Longrightarrow Q \quad = \quad \text{NON } Q \Longrightarrow \text{NON } P$$

18. Prouver (ou Calculer !)

$$P \Longrightarrow P \quad = \quad I$$

$$P \Longrightarrow Q \ \text{ ET } \ Q \Longrightarrow R \quad \Longrightarrow \quad P \Longrightarrow R \qquad = \qquad I$$

19. L'addition de vérité à nombre impair de termes est autoduale

sa niée égale sa préniée

L'addition de vérité à nombre pair de termes est autopréniée

sa niée égale sa duale

La duale $I + p + q$ de l'addition de vérité $p + q$

est l'équivalence logique, ou fonction de Kronecker encore notée

$$p \Longleftrightarrow q \quad = \quad I + p + q$$

20. Prouver

$$p \Longrightarrow q \ \text{ ET } \ q \Longrightarrow p \quad = \quad p \Longleftrightarrow q$$

21. Conjonction et disjonction à deux entrées

se distribuent mutuellement :

Par dualité suffit à prouver que

conjonction distribue disjontion

p ET q OU r = p ET q OU p ET r :

p ET q OU r = p (q + r + qr) = pq + pr + pqr

p ET q OU p ET r = pq + pr + pqpr = pq + pr + pqr

22. Prouver

(X <==> Y) = I SSI X = Y SSI X + Y = o

23. La conjonction p ==> q ET q ==> r

égale le produit (I + p + pq) (I + q + qr)

qui sans monôme pr

ne peut égaler I + p + pr = p ==> r

La conjonction p ==> q ET q ==> r

n'égale donc PAS l'implication p ==> q.

24. Prouver

p ==> qr = p ==> q ET p ==> r

p OU q ==> r = p ==> r ET q ==> r

25. Les sorties des deuzaines et des unités

de l'additionneur naturel à trois bits d'entrée z y x

sont les polynômes booliens symétriques élémentaires

zy + zx + yx et z + y + x

26. Les sorties des deuzaines et des unités de l'additionneur naturel à deux bits d'entrée $y\ x$ sont les polynômes booliens symétriques élémentaires

$$yx \qquad \text{et} \qquad y + x$$

27. Les sorties des quatraines, des deuzaines et des unités de l'additionneur naturel à quatre bits d'entrée $t\ z\ y\ x$ sont les polynômes booliens symétriques élémentaires

$$tzyx \qquad tz + ty + tx + zy + zx + yx \qquad t + z + y + x$$

28. Toute valeur de vérité vérifie $v^v = I$

et donc aussi $v^v = v$ SSI $v = I$