Un développement algébrique de l'algorithme d'exclusion et quelques problèmes géométriques en algèbre de Boole

Jean-Marie Laborde

THESE

présentée à

Université Scientifique et Médicale de Grenoble

Institut National Polytechnique de Grenoble

pour obtenir le grade de

DOCTEUR es SCIENCES

Mathématiques

par

Jean-Marie LABORDE

UN DEVELOPPEMENT ALGEBRIQUE DE L'ALGORITHME D'EXCLUSION ET QUELQUES PROBLEMES GEOMETRIQUES EN ALGEBRE DE BOOLE.

thèse soutenue le 27 janvier 1977 devant la Commission d'Examen :

Président	J. KUNTZMANN
Examinateurs	C. BENZAKEN
	M. CHEIN
	A. COLMERAUER
	R FRAÏSSE

UNIVERSITE SCIENTIFIQUE

ET MEDICALE DE GRENOBLE

Monsieur Gabriel CAU : Président
Monsieur Pierre JULLIEN : Vice-Président

MEMBRES DU CORPS ENSEIGNANT DE L'U.S.M.G.

PROFESSEURS TITULAIRES

MM.	ARNAUD Paul	Chimie
	AUBERT Guy	Physique
	AYANT Yves	Physique approfondie
Mme	BARBIER Marie-Jeanne	Electrochimie
MM.	BARBIER Jean-Claude	Physique Expérimentale
	BARBIER Reynold	Géologie appliquée
	BARJON Robert	Physique nucléaire
	BARNOUD Fernand	Biosynthèse de la cellulose
	BARRA Jean-René	Statistiques
	BARRIE Joseph	Clinique chirurgicale
	BEAUDOING André	Clinique de Pédiatrie et Puériculture
	BERNARD Alain	Mathématiques Pures
Mme	BERTRANDIAS Françoise	Mathématiques Pures
MM.	BERTRANDIAS Jean-Paul	Mathématiques Pures
	BEZES Henri	Pathologie chirurgicale
	BLAMBERT Maurice	Mathématiques Pures
	BOLLIET Louis	Informatique (IUT B)
	BONNET Georges	Electrotechnique
	BONNET Jean-Louis	Clinique ophtalmologique
	BONNET-EYMARD Joseph	Clinique gastro-entérologique
Mme	BONNIER Marie-Jeanne	Chimie générale
MM.	BOUCHERLE André	Chimie et toxicologie
	BOUCHEZ Robert	Physique nucléaire
	BOUSSARD Jean-Claude	Mathématiques Appliquées
	BOUTET DE MONTVEL Louis	Mathématiques Pures
	BRAVARD Yves	Géographie
	CABANEL Guy	Clinique rhumatologique et hydrologique
	CALAS François	Anatomie
	CARLIER Georges	Biologie végétale
	CARRAZ Gilbert	Biologie animale et pharmacodynamie
	CAU Gabriel	Médecine légale et toxicologie
	CAUQUIS Georges	Chimie organique
	CHABAUTY Claude	Mathématiques Pures
	CHARACHON Robert	Clinique Oto-rhino-laryngologique
	CHATEAU Robert	Clinique de neurologie
	CHIBON Pierre	Biologie animale
	COEUR André	Pharmacie chimique et chimie analytique
	CONTAMIN Robert	Clinique gynécologique
	COUDERC Pierre	Anatomie pathologique
Mme	DEBELMAS Anne-Marie	Matière médicale
MM.	DEBELMAS Jacques	Géologie générale
	DEGRANGE Charles	Zoologie
	DELORMAS Pierre	Pneumophtisiologie

MM.	DEPORTES Charles	Chimie minérale
	DESRE Pierre	Métallurgie
	DESSAUX Georges	Physiologie animale
	DODU Jacques	Mécanique appliquée (IUT A)
	DOLIQUE Jean-Michel	Physique des plasmas
	DREYFUS Bernard	Thermodynamique
	DUCROS Pierre	Cristallographie
	DUGOIS Pierre	Clinique de dermatologie et syphiligraphie
	GAGNAIRE Didier	Chimie physique
	GALLISSOT François	Mathématiques Pures
	GALVANI Octave	Mathématiques Pures
	GASTINEL Noël	Analyse numérique
	GAVEND Michel	Pharmacologie
	GEINDRE Michel	Electroradiologie
	GERBER Robert	Mathématiques Pures
	GERMAIN Jean-Pierre	Mécanique
	GIRAUD Pierre	Géologie
	JANIN Bernard	Géographie
	KAHANE André	Physique générale
	KLEIN Joseph	Mathématiques Pures
	KOSZUL Jean-Louis	Mathématiques Pures
	KRAVTCHENKO Julien	Mécanique
	KUNTZMANN Jean	Mathématiques Appliquées
	LACAZE Albert	Thermodynamique
	LACHARME Jean	Biologie végétale
Mme	LAJZEROWICZ Janine	Physique
MM.	LAJZEROWICZ Joseph	Physique
	LATREILLE René	Chirurgie générale
	LATURAZE Jean	Biochimie pharmaceutique
	LAURENT Pierre-Jean	Mathématiques Appliquées
	LEDRU Jean	Clinique médicale B
	LLIBOUTRY Louis	Géophysique
	LOISEAUX Pierre	Sciences nucléaires
	LONGEQUEUE Jean-Pierre	Physique nucléaire
	LOUP Jean	Géographie
Mlle	LUTZ Elisabeth	Mathématiques Pures
MM.	MALGRANGE Bernard	Mathématiques Pures
	MALINAS Yves	Clinique obstétricale
	MARTIN-NOEL Pierre	Clinique cardiologique
	MAZARE Yves	Clinique médicale A
	MICHEL Robert	Minéralogie et Pétrographie
	MICOUD Max	Clinique maladies infectieuses
	MOURIQUAND Claude	Histologie
	MOUSSA André	Chimie nucléaire
	MULLER Jean-Michel	Thérapeutique (Néphrologie)
	NEEL Louis	Physique du Solide
	OZENDA Paul	Botanique
	PAYAN Jean-Jacques	Mathématiques Pures
	PEBAY-PEYROULA Jean-Claude	Physique
	RASSAT André	Chimie systématique
	RENARD Michel	Thermodynamique
	REVOL Michel	Urologie
	RINALDI Renaud	Physique
	DE ROUGEMONT Jacques	Neuro-chirurgie
	SEIGNEURIN Raymond	Microbiologie et Hygiène
	SENGEL Philippe	Zoologie

MM.	SIBILLE Robert	Construction mécanique (IUT A)
	SOUTIF Michel	Physique générale
	TANCHE Maurice	Physiologie
	TRAYNARD Philippe	Chimie générale
	VAILLANT François	Zoologie
	VALENTIN Jacques	Physique nucléaire
	VAUQUOIS Bernard	Calcul électronique
Mme	VERAIN Alice	Pharmacie galénique
MM.	VERAIN André	Physique
	VEYRET Paul	Géographie
	VIGNAIS Pierre	Biochimie médicale
	YOCCOZ Jean	Physique nucléaire théorique

PROFESSEURS ASSOCIES

MM.	CLARK Gilbert	Spectrométrie physique
	CRABBE Pierre	CERMO
	ENGLMAN Robert	Spectrométrie physique
	HOLTZBERG Frédéric	Basses températures
	DEMBICKI Eugéniuz	Mécanique
	MATSUSHIMA Yozo	Mathématiques Pures

PROFESSEURS SANS CHAIRE

Mlle	AGNIUS-DELORD Claudine	Physique pharmaceutique
	ALARY Josette	Chimie analytique
MM.	AMBROISE-THOMAS Pierre	Parasitologie
	BELORIZKY Elie	Physique
	BENZAKEN Claude	Mathématiques Appliquées
	BIAREZ Jean-Pierre	Mécanique
	BILLET Jean	Géographie
	BOUCHET Yves	Anatomie
	BRUGEL Lucien	Energétique (IUT A)
	BUISSON René	Physique (IUT A)
	BUTEL Jean	Orthopédie
	COHEN ADDAD Pierre	Spectrométrie physique
	COLOMB Maurice	Biochimie
	CONTE René	Physique (IUT A)
	DEPASSEL Roger	Mécanique des fluides
	FONTAINE Jean-Marc	Mathématiques Pures
	GAUTHIER Yves	Sciences Biologiques
	GAUTRON René	Chimie
	GIDON Paul	Géologie et Minéralogie
	GLENAT René	Chimie organique
	GROULADE Joseph	Biochimie médicale
	HACQUES Gérard	Calcul numérique
	HOLLARD Daniel	Hématologie
	HUGONOT Robert	Hygiène et Médecine préventive
	IDELMAN Simon	Physiologie animale
	JOLY Jean-René	Mathématiques Pures
	JULLIEN Pierre	Mathématiques Appliquées
Mme	KAHANE Josette	Physique
MM.	KRAKOWIAK Sacha	Mathématiques Appliquées
	KUHN Gérard	Physique (IUT A)
	LE ROY Philippe	Mécanique (IUT A)
	LUU DUC Cuong	Chimie organique

MM.	MAYNARD Roger	Physique du solide
Mme	MINIER Colette	Physique (IUT A)
MM.	PELMONT Jean	Biochimie
	PERRIAUX Jean-Jacques	Géologie et Minéralogie
	PFISTER Jean-Claude	Physique du solide
Mlle	PIERY Yvette	Physiologie animale
MM.	RAYNAUD Hervé	M.I.A.G.
	REBECQ Jacques	Biologie (CUS)
	REYMOND Jean-Charles	Chirurgie générale
	RICHARD Lucien	Biologie végétale
Mme	RINAUDO Marguerite	Chimie macromoléculaire
MM.	ROBERT André	Chimie papetière
	SARRAZIN Roger	Anatomie et chirurgie
	SARROT-REYNAULD Jean	Géologie
	SIROT Louis	Chirurgie générale
Mme	SOUTIF Jeanne	Physique générale
MM.	STREGLITZ Paul	Anesthésiologie
	VIALON Pierre	Géologie
	VAN CUTSEM Bernard	Mathématiques Appliquées

MAITRES DE CONFERENCES ET MAITRES DE CONFERENCES AGREGES

MM.	AMBLARD Pierre	Dermatologie
	ARMAND Gilbert	Géographie
	ARMAND Yves	Chimie (IUT A)
	BACHELOT Yvan	Endocrinologie
	BARGE Michel	Neuro-chirurgie
	BARJOLLE Michel	M.I.A.G.
	BEGUIN Claude	Chimie organique
Mme	BERIEL Hélène	Pharmacodynamie
MM.	BOST Michel	Pédiatrie
	BOUCHARLAT Jacques	Psychiatrie adultes
Mme	BOUCHE Liane	Mathématiques (CUS)
MM.	BRODEAU François	Mathématiques (IUT B)
	CHAMBAZ Edmond	Biochimie médicale
	CHAMPETIER Jean	Anatomie et organogénèse
	CHARDON Michel	Géographie
	CHERADAME Hervé	Chimie papetière
	CHIAVERINA Jean	Biologie appliquée (EFP)
	CONTAMIN Charles	Chirurgie thoracique et cardio-vasculaire
	CORDONNIER Daniel	Néphrologie
	COULOMB Max	Radiologie
	CROUZET Guy	Radiologie
	CYROT Michel	Physique du solide
	DELOBEL Claude	M.I.A.G.
	DENIS Bernard	Cardiologie
	DOUCE Roland	Physiologie végétale
	DUSSAUD René	Mathématiques (CUS)
Mme	ETERRADOSSI Jacqueline	Physiologie
MM.	FAURE Jacques	Médecine légale
	FAURE Gilbert	Urologie
	GAUTIER Robert	Chirurgie générale
	GENSAC Pierre	Botanique
	GIDON Maurice	Géologie
	GROS Yves	Physique (IUT A)

MM. GUITTON Jacques	Chimie
HICTER Pierre	Chimie
IVANES Marcel	Electricité
JALBERT Pierre	Histologie
JUNIEN-LAVILLAVROY Claude	O.R.L.
KOLODIE Lucien	Hématologie
LE NOC Pierre	Bactériologie-virologie
LEROY Philippe	IUT A
MACHE Régis	Physiologie végétale
MAGNIN Robert	Hygiène et médecine préventive
MALLION Jean-Michel	Médecine du travail
MARECHAL Jean	Mécanique (IUT A)
MARTIN-BOUYER Michel	Chimie (CUS)
MICHOULIER Jean	Physique (IUT A)
NEGRE Robert	Mécanique (IUT A)
NEMOZ Alain	Thermodynamique
NOUGARET Marcel	Automatique (IUT A)
PARAMELLE Bernard	Pneumologie
PECCOUD François	Analyse (IUT B)
PEFFEN René	Métallurgie (IUT A)
PERRET Jean	Neurologie
PERRIER Guy	Géophysique - Glaciologie
PHELIP Xavier	Rhumatologie
RACHAIL Michel	Médecine interne
RACINET Claude	Gynécologie et obstétrique
RAMBAUD André	Hygiène et hydrologie
RAMBAUD Pierre	Pédiatrie
Mme RENAUDET Jacqueline	Bactériologie
MM. ROBERT Jean-Bernard	Chimie Physique
ROMIER Guy	Mathématiques (IUT B)
SHOM Jean-Claude	Chimie générale
STOEBNER Pierre	Anatomie pathologique
VROUSOS Constantin	Radiologie

MAITRE DE CONFERENCES ASSOCIES

M. COLE Antony	Sciences nucléaires

Fait à SAINT MARTIN D'HERES, AVRIL 1976.

INSTITUT NATIONAL POLYTECHNIQUE DE GRENOBLE

Président : M. Philippe TRAYNARD

Vice-Président : M. Pierre-Jean LAURENT

PROFESSEURS TITULAIRES

MM.	BENOIT Jean	Radioélectricité
	BESSON Jean	Electrochimie
	BLOCH Daniel	Physique du solide
	BONNETAIN Lucien	Chimie Minérale
	BONNIER Etienne	Electrochimie et Electrométallurgie
	BOUDOURIS Georges	Radioélectricité
	BRISSONNEAU Pierre	Physique du solide
	BUYLE-BODIN Maurice	Electronique
	COUMES André	Radioélectricité
	DURAND Francis	Métallurgie
	FELICI Noël	Electrostatique
	FOULARD Claude	Automatique
	LESPINARD Georges	Mécanique
	MOREAU René	Mécanique
	PARIAUD Jean-Charles	Chimie-Physique
	PAUTHENET René	Physique du solide
	PERRET René	Servomécanismes
	POLOUJADOFF Michel	Electrotechnique
	SILBER Robert	Mécanique des Fluides

PROFESSEUR ASSOCIE

M.	ROUXEL Roland	Automatique

PROFESSEURS SANS CHAIRE

MM.	BLIMAN Samuel	Electronique
	BOUVARD Maurice	Génie Mécanique
	COHEN Joseph	Electrotechnique
	LACOUME Jean-Louis	Géophysique
	LANCIA Roland	Electronique
	ROBERT François	Analyse numérique
	VEILLON Gérard	Informatique Fondamentale et Appliquée
	ZADWORNY François	Electronique

MAITRES DE CONFERENCES

MM.	ANCEAU François	Mathématiques Appliquées
	CHARTIER Germain	Electronique
	GUYOT Pierre	Chimie Minérale
	IVANES Marcel	Electrotechnique
	JOUBERT Jean-Claude	Physique du solide
	MORET Roger	Electrotechnique Nucléaire
	PIERRARD Jean-Marie	Mécanique
	SABONNADIERE Jean-Claude	Informatique Fondamentale et Appliquée
Mme	SAUCIER Gabrièle	Informatique Fondamentale et Appliquée

MAITRE DE CONFERENCES ASSOCIE

M. LANDAU Ioan	Automatique

CHERCHEURS DU C.N.R.S. (Directeur et Maître de Recherche)

MM. FRUCHART Robert	Directeur de Recherche
ANSARA Ibrahim	Maître de Recherche
CARRE René	Maître de Recherche
DRIOLE Jean	Maître de Recherche
MATHIEU Jean-Claude	Maître de Recherche
MUNIER Jacques	Maître de Recherche

Je tiens à exprimer ici ma reconnaissance, à

Monsieur le Professeur J. KUNTZMANN
qui me fait l'honneur de présider le jury de cette thèse ;

- que l'énergie et le talent qu'il a su déployer pour l'illustration des mathématiques appliquées et de l'informatique, à la tête du Laboratoire associé C.N.R.S. n° 7 , soient pleinement appréciés -

Monsieur R. FRAÏSSE, Professeur à
l'Université de Provence, Marseille ;

Monsieur C. BENZAKEN, Professeur à
l'Université Scientifique et Médicale de Grenoble ;

Monsieur M. CHEIN, Professeur à
l'Université Pierre et Marie Curie, Paris ;

Monsieur A. COLMERAUER, Professeur à
l'U.E.R. de Luminy, Marseille

qui ont bien voulu accepter de faire partie de ce jury.

Je remercie également Monsieur C. PAYAN de sa passion désintéressée pour les mathématiques, en particulier pour les problèmes des autres ; Mademoiselle NAUDIN, de son acharnement à dactylographier le manuscrit en temps utile ; le personnel du service Tirage, de la qualité matérielle de leur travail.

PLAN DETAILLE DE LA

PREMIERE PARTIE

I - L'ALGORITHME D'EXCLUSION

1) Notations, problème.
2) Formulation du processus algorithmique.
3) Hypothèses - Théorème de convergence.

II - DISCUSSION DES HYPOTHESES

1) D'autres conditions suffisantes.
2) Tentatives d'affaiblissement des conditions suffisantes.

III - STRUCTURES A CONSENSUS

1) L'algorithme en algèbre de Boole.
2) Une généralisation des opérations de Quine.

IV - APPLICATION A LA DEMONSTRATION AUTOMATIQUE

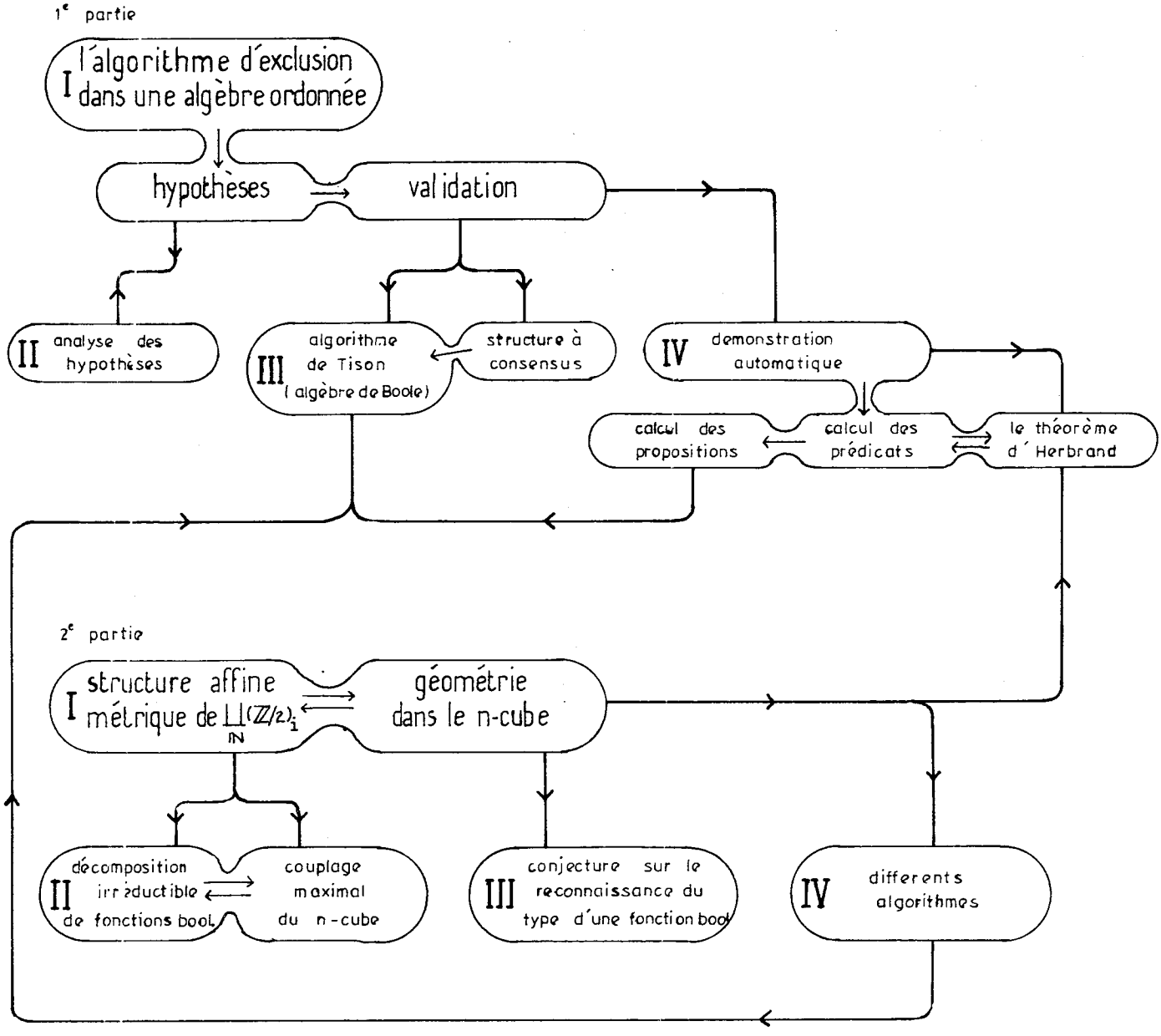
1) Le contexte général des méthodes en démonstration automatique.
2) Une autre présentation du théorème de résolution. Applications.
3) Un théorème d'algèbre de Boole et le théorème de Herbrand.

UN DEVELOPPEMENT ALGEBRIQUE DE L'ALGORITHME D'EXCLUSION ET QUELQUES PROBLEMES GEOMETRIQUES EN ALGEBRE DE BOOLE

SOMMAIRE

ARTICULATION EN "ORGANIGRAMME"

DES DIFFERENTS PARTIES ET CHAPITRES.



COMMENTAIRES

L'algorithme proposé par Tison pour la recherche de la base complète d'une fonction booléenne [KUNTZMANN 1] est abordé, dans la première partie, d'un point de vue algébrique assez général, ce qui permet différentes applications en particulier en démonstration automatique.

La deuxième partie présente un point de vue assez géométrique, pour l'étude de quelques questions classiques d'algèbre de Boole ; l'algorithme d'exclusion, dans sa version booléenne, y trouve en particulier une démonstration directe.

Note - La formulation de l'algorithme de Tison remonte à 1964 [TISON] et les différentes démonstrations qui en furent données étaient au moins incomplètes. La rédaction de la première partie est une amélioration de la première validation complète [LABORDE 1] . La validation purement booléenne de la deuxième partie est originale.

LES QUATRE CHAPITRES DE LA PREMIERE PARTIE

Le chapitre I expose le cadre algébrique, donne les hypothèses (axiomes) de la structure dans laquelle on s'est placé pour établir le théorème de convergence de l'algorithme d'exclusion.

Le chapitre II s'intéresse aux hypothèses faites au chapitre I : il en fournit des versions plus fortes (moins générales) mais plus faciles à vérifier ; par le jeu de contre-exemples on montre, d'autre part, que si l'on affaiblit les hypothèses du I, la convergence n'est plus assurée.

Au chapitre III sont exposées les applications :

- en algèbre de Boole (recherche de la base complète d'une fonction).
- dans une "structure à consensus" sur un produit quelconque de treillis distributifs.

Le chapitre IV est entièrement consacré au théorème de Herbrand [FRAÏSSE] et à la démonstration automatique fondée sur la méthode du résolvant [ROBINSON] .

On montre que dans un ensemble de clauses, l'opération multivoque de résolvant vérifie les hypothèses du I ; la démonstration d'un théorème consistant à montrer qu'un certain ensemble de clauses est insatisfaisable on obtient:

dans le cas où l'ensemble de clauses est insatisfaisable, la démonstration automatique du théorème ;
dans le cas contraire, la description de l'ensemble des réalisations.

On démontre, d'autre part, un théorème d'algèbre de Boole qui s'avère être "l'âme" du théorème d'Herbrand.

Note - En restreignant le cadre précédent du calcul des prédicats à celui des propositions, on retrouve la situation booléenne exposée au II.

LES CINQ CHAPITRES DE LA DEUXIEME PARTIE

Le chapitre I présente la structure affine métrique de $(\mathbb{Z}/_2)^n$ et les définitions "géométriques" de notions classiques d'algèbre de Boole qui constituent le support de l'ensemble des chapitres suivants. On démontre ainsi un théorème [LABORDE 2] parallèle à celui de l'inégalité triangulaire de la structure euclidienne habituelle de $\mathbb{R}^n$ et qui sera utilisé au IV.

Au chapitre II sont abordés les liens entre la notion de décomposition irréductible de coût maximum d'une fonction booléenne [KUNTZMANN 2] et celle de couplage maximal de cardinalité minimum du n-cube [FORCADE] .

La question dans [KUNTZMANN 2] sur le coût maximum est résolue ; un certain nombre de normes et de développements asymptotiques sont démontrés ou conjecturés.

Le chapitre III présente une conjecture, du genre de celle de [ULAM] pour l'isomorphisme de deux graphes qui, elle, concerne la reconnaissance du type d'une fonction booléenne. [LABORDE 3] permet une vérification pour $n \leqslant 4$ et le théorème exposé au I fournit une contribution à la résolution.

Le chapitre IV présente, à l'aide des notions du I, différents théorèmes classiques d'algèbre de Boole,dont une démonstration partant,uniquement booléenne, de la convergence de l'algorithme de Tison. Un nouvel algorithme pour la recherche de la base complète est, aussi, donné.

Annexe -

En annexe est donné un catalogue des 402 types de fonctions booléennes de quatre variables, classés lexicographiquement selon la croissance du nombre de points, du nombre de monômes premiers, de la dimension des monômes et représentés sous une forme la plus "lisible" possible.

A la suite de ce catalogue on trouve la liste des 216 codes des fonctions booléennes à examiner (cf. 2ème partie, III, 2).

Remargue - Une grande part des dessins de cette thèse a été effectués à l'aide d'un traceur Benson, en particulier le catologue des fonctions.

CHAPITRE I

L'ALGORITHME D'EXCLUSION

1) 1.1) Notations.

1.2) Problème.

2) Formulation du processus algorithmique sous forme d'une suite double.

3) Hypothèses.

3.1) Préliminaires : rappels et définitions.

3.2) Une série d'hypothèses.

- (I) de compatibilité de l'ordre et des opérations
- (II) de distributivité généralisée
- (III) d'absorption
- (IV) de finitude.

3.3) 2 lemmes, 1 corollaire.

3.4) Le théorème de convergence.

I - L'ALGORITHME D'EXCLUSION

1) - Notations, problème

1.1) - Notations

Soit $\mathcal{A} = (A, \leqslant, \{*_i\}_{i \in I})$ une structure algébrique ordonnée dont A désigne le support, $\leqslant$ la relation d'ordre et $*_i$ les opérations d'une famille indexée par I.

Soit $P \subset A$.

On note $\overline{P}$ la plus petite (pour l'inclusion) partie de A, contenant P et stable pour les $\{*_i\}_{i \in I}$: c'est l'ensemble des valeurs des formules bien formées sur le vocabulaire

$$P \cup \{(\} \cup \{)\} \cup \bigcup_{i \in I} \{*_i\}$$

On note Max P l'ensemble des éléments maximaux de P.

1.2) - Problème

Etant donné $P \subset A$, trouver Max $\overline{P}$.

2) Formulation du processus algorithmique

Définition d'une suite récurrente double (E_n, F_n) sur $\mathcal{L}(\overline{P})$.

$\mathcal{L}(\overline{P})$ dédignant l'ensemble des parties libres de $\overline{P}$, on suppose que l'on dispose d'une fonction $\mathcal{L}(\overline{P}) \to \overline{P}$ associant à toute partie x non vide de $\overline{P}$ un élément de x, et l'on appelera pointage une telle fonction.
(On rappelle qu'une partie libre L dans un ordonné E est définie par
$L \subset E$, L libre $\iff \forall \{x,y\} \subset L$ x = y ou x et y incomparables)

- terme initial $(E_o,F_o) = (\emptyset, \text{Max } P)$

- itération $(n \geq 0)$

en définissant $E'_n = E_n \cap \text{Max}(E_n \cup F_n)$

$$F'_n = F_n \cap \text{Max}(E_n \cup F_n) ,$$

si $F'_n = \emptyset$ $(E_{n+1},F_{n+1}) = (E'_n,\emptyset)$ et la suite stationne

sinon en désignant l'élément pointé de F'_n par f et par $\mathcal{F}(F)$ l'ensemble des valeurs des formules de hauteur 1 sur F admettant au moins une feuille étiquetée par f :

$$(E_{n+1},F_{n+1}) = (E'_n \cup \{f\} , F'_n - \{f\} \cup \mathcal{F}(F'_n)).$$

Exemple - Dans le cas d'opérations univoques, binaires, totales, commutatives et en nombre fini m, si $(E'_n,F'_n) = (\{e_o,\ldots,e_r\} ,\{f_o,\ldots f_s\})$ et si F'_n "pointe" sur f_o

$$(E_{n+1},F_{n+1}) = (\{e_o,\ldots,e_r,f_o\} , \{f_1,\ldots f_s,f_o \underset{1}{*} f ,\ldots f_o \underset{m}{*} f , f_{o_1} * f_1,\ldots f_{o_m} * f_s \})$$

3) - Hypothèses sur $\overline{P}$

3.1) Préliminaires

3.1.1) Ordre α sur $\mathcal{L}(\overline{P})$

Sur $\mathcal{P}(A)$ définissons une relation α par

$$P \alpha Q \iff \forall x \in P \quad \exists y \in Q \quad x \leqslant y.$$

a) Sur $\mathcal{P}(A)$ α est un préordre. En effet, d'une part $P \alpha P$ (réflexivité) et, d'autre part, pour x élément quelconque de P, si $P \alpha Q$

$$\exists y \in Q \quad x \leqslant y$$

or pour cet y si $Q \propto R$

$$\exists z \in R \quad y \leqslant z \quad \text{d'où, finalement}$$

$$\forall x \in P \quad \exists z \in R \quad x \leqslant z \quad \text{(transitivité).}$$

b) Proposition 1 - $P \propto Q$ et $Q \propto P$ et $P \neq Q \Rightarrow P$ n'est pas libre.

En effet, de $P \neq Q$ on déduit $\exists x \in P \quad x \notin Q$, or de $P \propto Q$ on tire

$$\exists y \in Q \quad x \leqslant y$$

et comme $x \notin Q$, $x \neq y$ d'où $x < y$; de $Q \propto P$ on tire

$$\exists z \in P \quad y \leqslant z$$

d'où on déduit que P contient deux éléments x et y vérifiant $x < y$. P' n'est donc pas libre, par symétrie Q non plus, c'est que :

COROLLAIRE - $\propto$ est un ordre sur $\mathcal{L}(A)$ et sa restriction à $\overline{P}$ (encore notée $\propto$) est un ordre sur $\mathcal{L}(\overline{P})$.

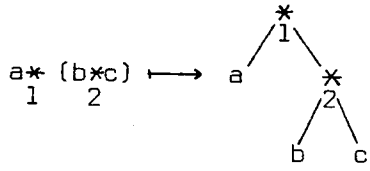
Remarque - Max P est alors la plus grande (selon α) des parties libres de P.

3.1.2) - Rappels sur l'ensemble noté $\tilde{Q}$ des formules bien formées et définies sur Q

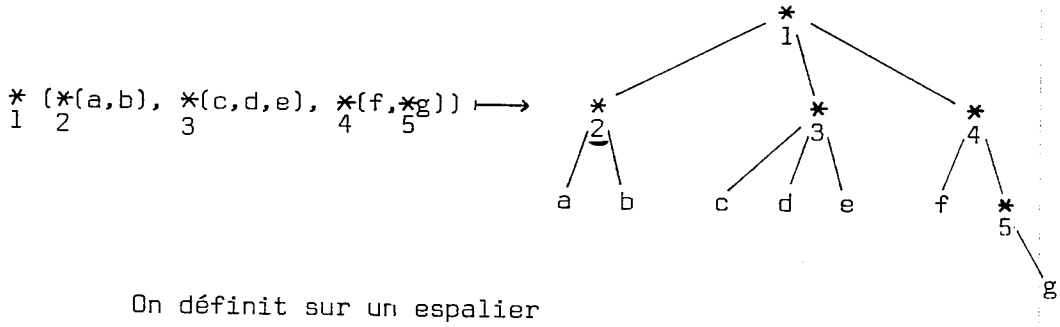
a) On peut admettre ici qu'il est possible de faire correspondre bijectivement à tout élément x de cet ensemble un espalier $\mathcal{X}$, dont les noeuds (sommets différents d'une feuille) sont étiquetés par des $*_i$ et les feuilles par des éléments de Q. Dans un tel espalier, le $\frac{1}{2}$ degré extérieur d'un noeud étiqueté par $*_i$ est égal à l'"arité" de l'opération $*_i$.

Remarque - Si la structure algébrique est commutative on oublie dans chaque espalier l'ordre transverse (ordre total sur les successeurs de chaque noeud) : l'espalier devient alors une arborescence.

Exemples - (ordre de haut en bas)



et dans le cas d'opérations non forcément binaires



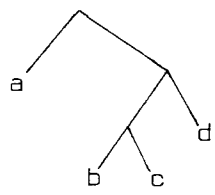
On définit sur un espalier

- la hauteur d'un sommet (feuille ou noeud) par la longueur de la chaîne joignant la racine (unique sommet sans prédécesseur) à ce sommet, calculée en faisant abstraction, dans cette chaîne, des sommets de $\frac{1}{2}$ degré extérieur (vers ces feuilles) égal à 1.

- la hauteur h(x) d'un espalier x par la hauteur maximale d'une feuille.

- la "profondeur de voisinage" d'une feuille x, différente de la racine, comme la hauteur de l'espalier terminal issu du prédécesseur de x (dorénavant on ne parlera seulement que de profondeur);

Exemple -



p(a) = 3
p(d) = 2
p(b) = 1
p(c) = 1

et si x est aussi racine p(x) = 0 .

b) Valeurs et définition d'une formule bien formée

En partant des feuilles d'un noeud, si l'opération représentée par l'étiquette du noeud est définie pour le jeu d'arguments représentés par les étiquettes des feuilles, on peut associer à ce noeud la valeur ($\in \overline{P}$) de cette opération selon ces arguments (ou, éventuellement l'ensemble des valeurs, si l'opération n'est pas univoque).

De proche en proche, si l'on peut associer à la racine d'une arborescence associée à une formule x un ensemble de valeurs v(x), on dira que cette arborescence est définie et que v(x) est son ensemble de valeurs.

c) Préordre sur $\tilde{A}$, l'ensemble des formules bien formées et définies sur A

On peut prolonger à $\tilde{A}$ l'ordre défini sur A par un préordre encore noté $\leq$

$$f \leqslant g \iff v(f) \propto v(g)$$

en effet, réflexivité $f \leqslant f$ (immédiat)

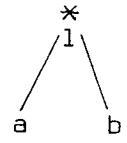
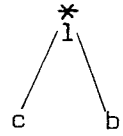
transitivité $f \leqslant g$ ou $g \leqslant h \implies f \leqslant h$ (immédiat).

3.2) Une série d'Hypothèses

3.2.1) Hypothèse (I) de compatibilité de l'ordre et des opérations

Etant donnés une formule x sur $\overline{P}$ et un ensemble Φ majorant selon α les feuilles de x (et minimal pour l'inclusion), il existe une formule y à feuilles dans Φ vérifiant

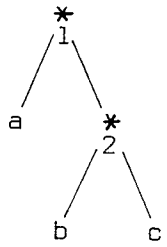
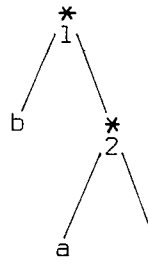
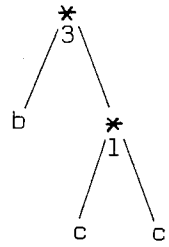
$$x \leqslant y \quad \text{avec} \quad h(x) \leqslant h(y)$$

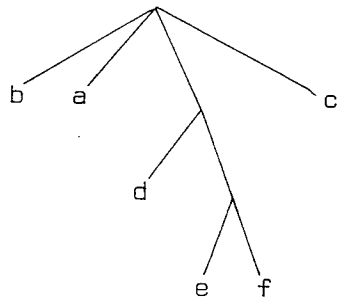
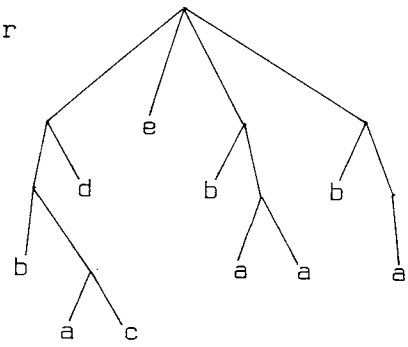
Exemple -  majorée par  ou b ou c si $c \geqslant a$

Remarque : cette hypothèse est moins forte que l'isotonie.

3.2.2) Hypothèses (II) de distributivité généralisée

- forme (II) f : Toute formule x sur $\overline{P}$, admettant une feuille d'étiquette a, est majorée par une formule y dont les feuilles ont des étiquettes prises parmi celles de x et telle qu'aucune feuille d'étiquette a ne soit de profondeur > 1.

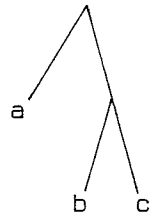
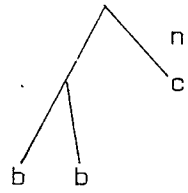
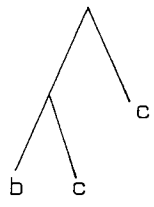
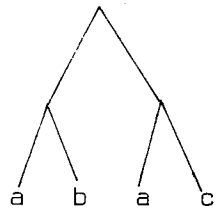
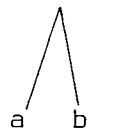
Exemple -  majorée par  ou  on a

 majorée par 

- Une forme plus forte notée (II)F peut être obtenue en imposant une condition de hauteur.

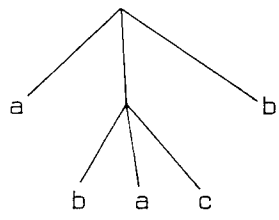
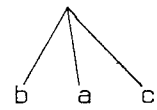
Toute formule . . . . . de profondeur > 1 et vérifiant $h(y) \leqslant h(x)$, et si x admet une feuille de hauteur 1, étiquetée par a, y vérifie $h_a(y) < h(x)$, où pour déterminer $h_a(y)$, les noeuds de y admettant une feuille d'étiquette a, sont considérés comme des feuilles.

On dira dans ce dernier cas que l'on "distribue" a sur son facteur.

Exemple -  majorée par  n'est pas acceptable, seuls sont acceptables les majorants de la forme  ou  ou  ou  ou b ou a.

3.2.3) - Hypothèse (III) d'absorption

Toute formule x sur $\bar{P}$ de hauteur 2, dont une feuille de hauteur 1 est étiquetée par a, ainsi que l'une de ses feuilles de hauteur 2, est majorée par a ou par l'un des noeuds (de hauteur 1) admettant un successeur étiqueté par a.

Exemple -  majorée par a ou 

3.2.4) - Hypothèse (IV) de finitude

$\overline{P}$ est supérieurement fini.

On rappelle qu'un ensemble ordonné E est supérieurement fini signifie :

- toute chaîne de E, possédant un élément minimal est finie (ou toute suite croissante est stationnaire).
- toute partie libre de $\overline{E}$ est finie.

Exemple - Tout ensemble ordonné fini.

Remarque générale à toutes les hypothèses formulées :

ces hypothèses ne sont pas supposées être vérifiées uniformément en $\overline{P}$.

3.3) - Démonstration de deux Lemmes et un corollaire

3.3.1) - LEMME 1 (f) -

Sous la seule hypothèse (II) faible

$$\forall F \subset \overline{P} \quad \forall x \in \tilde{F} \quad \exists y \in \{f\} \cup \widetilde{F-\{f\} \cup \mathcal{F}(F)} \quad y \geq x$$

où f est l'élément pointé de F.

En effet, cette proposition est équivalente à (II) faible.

LEMME 1 (F) -

Sous l'hypothèse (II) forte

$$\forall F \subset \overline{P} \quad \forall x \in \tilde{F} \quad \exists y \in \{f\} \cup \widetilde{F-\{f\} \cup \mathcal{F}(F)} \quad y \geq x$$

avec $h(y) \leq h(x)$ et si x admet une feuille de hauteur 1, étiquetée par f $h_f(y) < h(x)$.

En effet, cette proposition est équivalente à (II) forte.

3.3.2) LEMME 2

$$\forall n \in \mathbb{N} \quad \forall x \in \widetilde{E'_n \cup F'_n} \quad \exists y \in \widetilde{E'_n \cup F'_n} \quad y \geqslant x$$

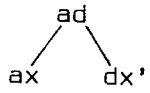
On dira d'une formule y obtenue par distribution de a sur son facteur, qu'elle est dominée par a si elle satisfait à l'hypothèse (III). On a la

Propriété 1 - Si une formule x est dominée par a, l'itération de la distribution à l'intérieur de x, de a, conduit alors en un nombre fini d'étapes (par diminution de la hauteur) à une formule stable pour la distribution de a (qui ne peut donc être que a ou une formule sans occurrence de a).

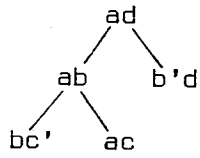
Soit alors une formule sur $E'_n \cup F'_n$, on aura développé les feuilles sur F_o, par distribution successive des différents noeuds représentant des occurrences d'éléments de E'_n et réécriture à l'aide du lemme 1. On obtient une formule maximale pour l'inclusion de ses sous-formules dominées par des éléments de E'_n (en nombre fini). La propriété 1 permet alors d'affirmer qu'on obtient en un nombre fini d'étapes une formule stable pour la distribution des éléments de E'_n, c'est-à-dire un élément de E'_n ou une formule sans occurrence dans E'_n, c'est-à-dire sur F'_n.

Remarque sur des questions de hauteurs. Considérons en algèbre de Boole et avec pour seule operation $\overset{*}{i}$ celle de consensus, la suite (E_n, F_n) :

i	E_i	F_i
0		ax cx' bc' b'd
1	ax	cx' bc' b'd / ac
2	ax cx'	bc' b'd ac / bx'
3	ax cx' bx'	bc' b'd ac / dx'
4	ax cx' bx' bc'	b'd ac dx' / c'd ab
5	ax cx' bx' bx' b'd	ac dx' c'd ab / ad
	.....	.....

Au rang 3, la formule 

n'est majorée que par une formule de hauteur au moins 2 sur F'_3 :



Ceci montre que dans l'énoncé du lemme 2 il est probablement difficile d'obtenir une condition de hauteur intéressante.

3.3.3) - COROLLAIRE 1 (du lemme 1 et du lemme 2)-

$$\forall n \qquad \text{Max } \overline{P} \subset E_n \cup \overline{F_n}$$

On raisonne par récurrence sur n en appelant M_n la propriété au rang n.

- M_o est satisfaite puisque $E_o \cup \overline{F}_o = \overline{\text{Max } P}$ et que par (I)
  $\text{Max } \overline{P} = \text{Max } \overline{\text{Max } P} \subset \overline{\text{Max } P}$
- Supposons alors M_n $(n \geq 0)$ et montrons M_{n+1} .

Sans tenir compte des questions de longueur, le lemme 2 permet d'affirmer que (compte-tenu de (I))

$$\text{Max } \overline{P} \subset E_n \cup \overline{F}_n \Rightarrow \text{Max } \overline{P} \subset E'_n \cup \tilde{F}'_n ;$$

le lemme 1(f) permet d'affirmer alors :

$$\text{Max } \overline{P} \subset E'_n \cup \overline{F'_n} \Rightarrow \text{Max } \overline{P} \subset E_{n+1} \cup \overline{F_{n+1}}$$ ce qui établit la proposition.

3.4) - Théorème de convergence de (E_n, F_n) -

Selon la topologie discrète
et sous l'hypothèse IV on a de plus $\lim_n (E_n, F_n) = (\text{Max } \overline{P}, \emptyset)$.

Démonstration - Si $\exists n \quad F_n = \emptyset$,

la suite (E_n, F_n) converge (stationne à partir d'un certain rang) et, d'après le corollaire, ce ne peut être que vers $(\text{Max } \overline{P}, \emptyset)$.

Etablissons donc que

$$\exists n \quad F_n = \emptyset.$$

Raisonnons par l'absurde et considérons la suite de parties libres $G_n = E'_n \cup F'_n$. On va montrer qu'on peut en extraire une sous-suite strictement croissante (pour α) $G_{\phi(n)}$:

1) $G_n \; \alpha \; G_{n+1}$: en effet si $x \in G_n - G_{n+1}$ alors il existe un majorant de x dans G_{n+1} et si $x \in G_n \cap G_{n+1}$, $x \in G_{n+1}$ est un majorant de x.

2) $\forall n \; \exists m > n \quad G_n \neq G_m$, en effet dans le cas contraire G_n serait stationnaire, ce qui est impossible si $\forall n \; F_n \neq \emptyset$.

On définit alors une suite de suites croissantes sur $\overline{P}$.
Soit $x_{oo} \in G_o$: $x_{n+1,o}$ est choisi dans $G_{\phi(n+1)}$ comme un majorant de $x_{n,o} \in G_{\phi(n)}$. D'après (IV) $x_{n,o}$ stationne à partir d'un certain r_o.

La $(m+1)^e$ suite est alors définie de la façon suivante (où $R_i = \sum_{j=o}^{i} r_j$) :
Si $x_{n,m}$ converge vers $x_{\infty,m}$ en stationnant à partir de r_m, il existe un élément dans $G_{\phi(R_{m+1})}$ incomparable à chacun des éléments de $G_{\phi(R_m)}$, soit $x_{o,m+1}$.

$x_{n+1,m+1}$ est alors choisi dans $G_{\phi(R_m+n+1)}$ comme un majorant de $x_{n,m+1}$.

Le fait que $\{x_{\infty,i}\}_{i\in\mathbb{N}}$ est une partie libre infinie contredit (IV).

CHAPITRE II

DISCUSSION DES HYPOTHESES

1) Conditions d'existence d'un algorithme.

1.1) Condition A.

1.2) Condition suffisante de A.

1.3) Différents jeux d'hypothèses assurant (I), (II), III) ou (IV).

2) Tentatives d'affaiblissement des conditions suffisantes.

2.1) Sur (I).

2.2) Sur (II) - Cas d'un produit de treillis (non distributifs).

2.3) Sur (III).

2.4) Sur (IV) - Définition de la notion de pointage "systématique" et un autre théorème de convergence.

II - DISCUSSION DES HYPOTHESES

1) Existence et conditions d'existence d'un algorithme pour résoudre le problème de la détermination de Max $\overline{P}$, connaissant P.

1.1) - Le théorème d'algèbre précédent n'est pas suffisant pour assurer l'existence d'un algorithme. En effet, il est nécessaire de s'assurer qu'à chaque itération du processus défini en I, il est possible de n'avoir qu'à effectuer un nombre fini d'opérations élémentaires.

Cela implique, en particulier, qu'à chaque itération E_n,F_n soient finis (ceci est d'ailleurs assuré par l'hypothèse IV).

Cela implique qu'il soit possible de n'envisager, pour passer de F'_n à F_{n+1} qu'un nombre fini d'opérations de $\{*_i\}_{i \in I}$ (condition A), dont on doit supposer qu'elles sont d'"arité" finie et que pour un jeu d'arguments elles ne fournissent qu'un ensemble fini de valeurs.

Il est immédiat que si ces conditions sont satisfaites, alors il correspond bien au processus du I, un algorithme.

1.2) - Condition suffisante pour assurer la condition A.

Introduisons la notion de partie "suffisante" de l'ensemble I, indexant l'ensemble des opérations $\{*_i\}_{i \in I}$:

Définition - $J \subset I$ est dite suffisante si, quels que soient les arguments $x_1, x_2, \ldots, x_r$ dans $\overline{P}$, des $*_i$ pour $i \in I$,

$$\exists k \in \{1,\ldots,r\} \qquad *_i(x_1,\ldots,x_r) \leqslant x_k$$

ou $$\exists j \in J \quad \exists \{y_1,\ldots,y_s\} \subset \{x_1,\ldots,x_r\} \qquad *_i(x_1,\ldots,x_r) \leqslant *_j(y_1,\ldots,y_s).$$

Les opérations indexées dans I-J sont alors dites "inutiles" car, avec des notations évidentes, et compte-tenu de (I)

$$\overline{P}^I \propto \overline{P}^J$$

et $\quad \text{Max } \overline{P}^I = \text{Max } \overline{P}^J$.

On peut alors formuler une condition B, suffisante de A:

Condition B (suffisante de A), il existe dans I, une partie suffisante finie.

Remarque - Dans la suite, les hypothèses du 1.1) autres que la Condition A, seront toujours supposées satisfaites.

1.3) - Différents jeux d'hypothèses assurant (I), (II), (III) ou (IV).

1.3.1) Sur (I) -

Montrons que pour (I) il suffit que (I) soit vraie pour les formules de hauteur 1. Raisonnons par induction sur la hauteur d'une formule quelconque x , en appelant $(I)_h$ la propriété (I) pour les formules de hauteur h. Pour x atomique $(I)_o$ est immédiate.

Supposons la propriété établie pour $h < H$ $(H \geqslant 1)$ et établissons $(I)_H$. x non atomique peut être considérée comme une formule de hauteur 1, dont les feuilles sont étiquetées par des formules de hauteur $< H$, majorées par des formules de hauteur $<H$ dont les étiquettes des feuilles sont prises dans Φ. $(I)_1$ permet alors d'affirmer $(I)_H$.

On a donc $(I) \Leftrightarrow (I)_1$.

Montrons alors que $(I)_1 \Leftrightarrow (I)_{1,1}$ où $(I)_{1,1}$ est la propriété $(I)_1$ vraie pour les seuls x et Φ tels que l'ensemble des feuilles de x et Φ ne diffèrent que d'un élément au plus.

On raisonne de même par induction sur i pour établir $\forall i\ (I)_{1,i}$ soit $(I)_1$.

Application - Dans une structure à opérations binaires, totales, commutatives (I) est conséquence de la seule hypothèse d'isotonie :

$$\forall i\ \forall x\ \forall y\ \forall z \quad x \leqslant y \Rightarrow x *_i z \leqslant y *_i z$$

1.3.2) - Sur (II)-

Comme pour (I) on peut démontrer, moyennant (I) et (III).

$$(II)_F \Leftrightarrow (II)_{F_2}$$

Démonstration de $(II)_{F_2} \Leftrightarrow (II)_F$ moyennant (I) et (III).

On raisonne par induction sur la longueur d'une formule quelconque x. Pour x atomique $(II)_{F_o}$ est immédiate,
de même $(II)_{F_1}$ et $(II)_{F_2}$ (hypothèse).

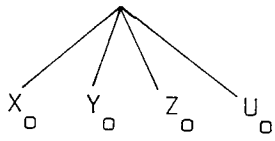
Supposons alors $(II)_{F_h}$ établie pour $h < H$ $(H \geqslant 3)$ et établissons $(II)_{F_H}$:

x de hauteur au moins 3 peut être considérée comme une formule de hauteur 1 dont les feuilles sont étiquetées par des formules de hauteur < H . Si chacun des majorants de ses feuilles, intervenant dans la formule fournie par (I), est différente de f, le problème est résolu, sinon le problème est ramené à celui portant sur une formule de longueur au plus H et admettant une feuille de hauteur 1 étiquetée par f.

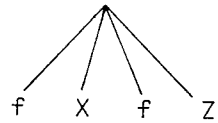
A une telle formule (dans le cas où elle est de hauteur > 1 sinon le problème est résolu) on peut appliquer $(II)_{F_2}$ en la considérant comme

une formule de hauteur 2 dont les feuilles sont étiquetées par des formules de hauteur < H (en fait < H-1). On obtient après application de $(II)_{F_2}$ puis de (I), soit une formule de hauteur < H, soit une formule donnant une solution, à moins que l'un des majorants fournis par $(II)_{F_{h<H}}$ ne soit f.

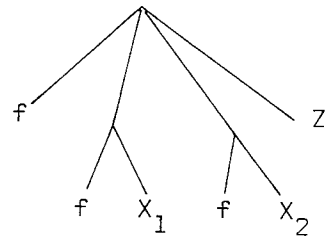
Exemple d'une telle situation :



par $(I)_{F_h}$ puis (I)



si $X=X_1X_2$ et par $(II)_{F_h}$



X_0, Y_0, Z_0, U_0 de hauteur < H

D'après (III) cette dernière formule, dominée par f, est majorée par une formule ne contenant des occurrences de f qu'au plus de profondeur 1 et satisfaisant les conditions de hauteur.

Application au cas d'opérations totales, binaires, commutatives.

(II) F_2 s'écrit

$\forall x \ \forall y \ \forall z$ $x*(y*z)$ majorée par l'un des éléments suivants

$h = 0$ { - x ; - y ; - z }

$h = 1$ { - x * { x ; y ; z } mis pour $\{x*x, x*y, x*z\}$; - y * { y ; z } ; - z*z }

$h = 3$ - (x * { x ; y ; z }) * { y ; z ; x * { x ; y ; z } }

On montrera en algèbre de Boole que le consensus s'inscrit bien dans ces possibilités car,

$x * (y*z)$ est majoré, dans le cas où $*$ représente l'opération de consensus entre deux monômes par l'un des éléments de

$$\{z,\ x*y\ ,\ x*z\ ,\ (x*y)*z\ ,\ (x*y)\ *\ (x*z)\}$$

1.3.3) Sur (III) -

Dans le cas d'opérations totales binaires, commutatives, (III) s'écrit

$\forall x\ \forall y$ $\quad x * (x*y)$ majorée par $x*y$ ou x.

1.3.4) - Sur (IV) -

On a la propriété :

Dans une structure algébrique, l'associativité et la commutativité simple impliquent (IV) si (III) (immédiat).

2) Tentatives d'affaiblissement des conditions suiffisantes

2.1) Sur (I) -

On ne peut pas supprimer toute hypothèse sur la compatibilité de l'ordre et des opérations.

En effet, considérons $E = \{-1,0,1\}$ avec $-1 < 0 < 1$ et la loi commutative idempotente définie par (et notée multiplicativement)

	0	1	-1
0	0	0	0
1	0	1	1
-1	0	1	-1

Soit A = E x E muni de l'ordre et de la loi produit T

. T est commutative idempotente.

. T ne vérifie pas (I) on a $-1 < 0$ et en multipliant par 1 on aurait $1 \leq 0$ alors que $1 > 0$.

. T vérifie $(II)_F$ puisque T est associative,

en effet, considérons a(b c)

si l'un des a, b ou c est nul alors a(bxc) = 0 = (axb)c

sinon si a=1 1xbc = 1 = (1xb)c

et pour a=-1 -1xbc = bc = (-1xb)c

. T vérifie (III)

en effet a(ab) = (aa)b = ab

. T vérifie (IV) puisque A est fini (ou encore en remarquant qu'ici (III) $\Rightarrow$ (IV)).

Pour P = {(1,0) , (0,-1) , (-1,1)} comme (1,0) > (0,-1)

Max P = {(1,0) , (-1,1)}

$(E'_o,F_o) = (\varnothing , \{(1,0) , (-1,1)\})$

$(E_1,F_1) = (\{(1,0)\} , \{(-1,1) , \{(-1,0)\}\})$

$(E'_1,F'_1) = (\{(1,0)\} , \{(-1,1)\})$

$(E'_2,F'_2) = (\{(1,0) , (-1,1)\} , \varnothing)$

alors que (0,-1) T(-1,1) =(0,1) > (-1,1) .

2.2) - Sur (II) -

On a vu $(II)_F \Leftrightarrow (II)_{F_2}$

a) Montrons que $(II)_2$ n'est pas suffisante.

Soit $A = \{a,b,c,\alpha,\pi\}$ muni de l'ordre strict vide et d'une opération

binaire, notée multiplicativement, commutative, définie par sa table :

	a	b	c	α	π
a	a	a	c	π	π
b		a	α	α	π
c			c	α	π
α				α	π
π					π

. (I) est bien vérifié puisque l'ordre strict est vide.

. Pour vérifier $(II)_2$ il suffit de vérifier que x(yz) peut s'écrire comme une formule où la profondeur de x n'est pas > 1.

Pour $x = \pi$ il vient $x(yz) = \pi = x$

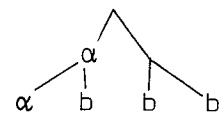
Pour y ou z valant π , il vient $x(yz) = x\pi = \pi = yz$

On peut donc se limiter à $\{x,y,z\} \subset \{a,b,c,\alpha\}$.

Pour $x = \alpha$ il vient $x(yz) = \alpha = x$ à moins que yz ne vaille π ou a. Dans le premier cas $x(yz) = \pi = yz$.

Dans le deuxième, on a les éventualités

$$x(yz) = \begin{cases} \alpha\, aa = \pi = \alpha a \\ \alpha\, ab = \alpha a \\ \alpha\, bb = \end{cases}$$



.

Pour y ou z valant α , par exemple, $y = \alpha$ il vient

$$x(yz) = x(\alpha z) = x\alpha = xy$$

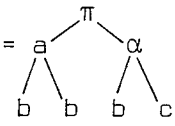
à moins que z ne vaille π ou α .

Le premier cas a déjà été envisagé, dans le deuxième

$$x(\alpha a) = x\pi = \pi = \alpha a = yz$$

On peut donc, finalement, se limiter aux seules vérifications correspondant à $\{x,y,z\} \subset \{a,b,c\}$.

Les différentes possibilités correspondent alors, à :

$\otimes$ $a(a\alpha) = a$	$b\ aa = a$	$c\ aa = ca$
$\otimes$ $a(ab) = a$	$b\ ab = ab$	$c\ ab = ca$
$\otimes$ $a(ac) = ac$	$b\ ac = bc$	$\otimes$ $c\ ac = cc = c$
$a\ bb = a$	$\otimes$ $b\ bb = a = bb$	$c\ bb = ca = c$
$a\ bc = \pi$ = 	$\otimes$ $b\ bc = b\alpha = \alpha = bc$	$\otimes$ $c\ bc = c\alpha = \alpha = bc$
$a\ cc = ac$	$b\ cc = bc$	$\otimes$ $c\ cc = c$

. $(II)_F$ n'est pas vérifiée, pour $a(bc)$, par exemple ;

. (III) est vérifiée, comme le montrent les précédentes égalités (précédées du signe $\otimes$), ainsi que $\pi(\pi x) = \pi$

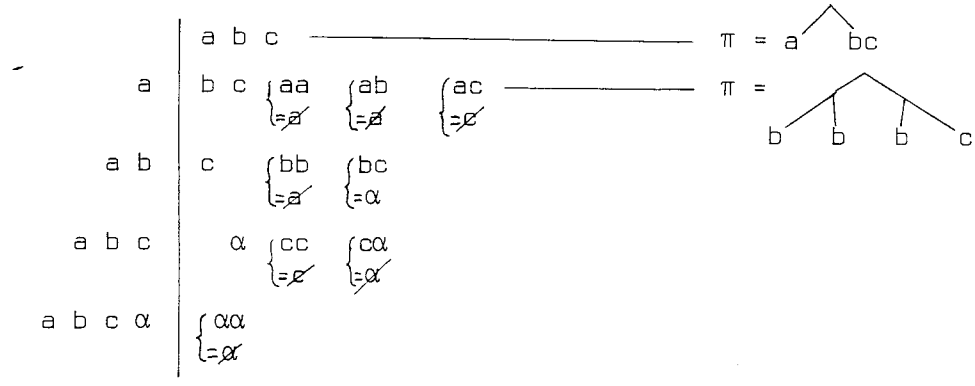
et $\alpha(\alpha x) = \alpha$ à moins que $x = \pi$ ou $x = a$:

dans le premier cas $\alpha(\alpha\pi) = \alpha\pi$;

dans le deuxième cas $\alpha(\alpha a) = \alpha\pi = \pi = \alpha a$;

. (IV) est vérifiée puisque A est fini.

Pour $P = \{a,b,c\}$ le processus algorithmique donne

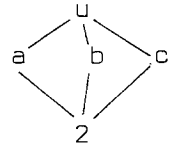


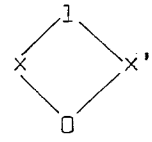
On a écrit dans le prolongement des lignes, une formule de valeur π , tant que cela a été possible.

b) Cas d'un produit de treillis -

Pour les opérations de consensus de Quine sur un produit de treillis, la distributivité des $\underset{i}{*}$ est équivalente à celles de chacun des treillis (voir structure de consensus sur un produit de treillis).

Montrons que si, pour un treillis du produit, seule la modularité est assurée, le processus ne fournit plus Max $\bar{F}$.

Soit $A = T_1 \times T_2$ avec T_1 = 

et T_2 = 

(I) et (IV) sont vérifiées (immédiat).

Vérifions (III), on a :

$$u \underset{1}{*} (u \underset{1}{*} v) = (u_1 \vee (u_1 \vee v_1) \,,\, u_2 \wedge (u_2 \wedge v_2)) = u \underset{1}{*} v$$

$$u \underset{1}{*} (u \underset{2}{*} v) = (u_1 \vee (u_1 \wedge v_1) \,,\, u_2 \wedge (u_2 \vee v_2)) = (u_1, u_2) = u$$

$$u \underset{2}{*} (u \underset{1}{*} v) = u_1 \wedge (u_1 \vee v_1) \,,\, u_2 \vee (u_2 \wedge v_2) = (u_1, u_2) = u$$

Pour P = {bx', cx, ax} le processus algorithmique donne

	bx' cx ax
bx'	cx ax u0 zl ~~u0~~ ~~zl~~
bx' ~~cx~~	~~ax~~ ~~u0~~ zl ux ~~zx~~ ~~u0~~ ~~cx~~ ~~cx~~ ~~zl~~
bx' zl	ux ~~ux~~ zl
bx' zl ux	

or $bx' \underset{2}{*} (cx \underset{1}{*} ax) = bx' \underset{2}{*} ux = bl$

et {zl, ux , $\boxed{bl}$} est libre.

2.3) Sur (III) -

Montrons qu'on ne peut pas supprimer toute hypothèse d'absorption.

Soit $A = T_x \times T_y \times T_z \times T_t$ le produit des quatre treillis distributifs isomorphes où T_x est le treillis de Boole à 2 atomes x et x', et muni de l'ordre produit. Sur A, soient les deux opérations $\underset{1}{*}$ et $\underset{2}{*}$ définies par

$$(a\ b\ c\ d) \underset{1}{*} (\alpha\ \beta\ \gamma\ \delta) = (a \vee \alpha\ ,\ b \vee \beta\ ,\ c \wedge \gamma\ ,\ d \wedge \delta)$$
$$(a\ b\ c\ d) \underset{2}{*} (\alpha\ \beta\ \gamma\ \delta) = (a \vee \alpha\ ,\ b \wedge \beta\ ,\ c \vee \gamma\ ,\ d \wedge \delta)\ .$$

Les hypothèses (I), $(II)_F$, (IV) sont vérifiées comme conséquence d'un résultat plus général (voir structure de consensus sur un produit de treillis distributifs)

Soit $P = \{a,b\}$ avec $a = x\ y\ z\ t$, $b = x'y'z't'$.

(III) n'est pas vérifié, par exemple $c = a \underset{2}{*} (a \underset{1}{*} b) = a \underset{2}{*} (1100) = 1yz0$

or $a \underset{1}{*} a = a \underset{2}{*} a = a$, $a \underset{1}{*} b = 1100$ et $a \underset{2}{*} b = 1010$.

Le processus algorithmique donne

	xyzt x'y'z't'
xyzt	x'y'z't' 1100 1010
xyzt x'y'z't'	1100 1010 1100 1y'00 1y'z'0 1010
xyzt x'y'z't' 1100	1010 1y'z'0 1100 1010 1100 1y'z'0
xyzt x'y'z't' 1100 1010	1y'z'0
xyzt x'y'z't 1100 1010 1y'z'0	

or $\{a,b,1100,1010,1y'z'0,\boxed{1yz0}\}$ est libre.

Remarque - Ceci constitue un contre-exemple à une démonstration de la convergence de l'algorithme d'exclusion, due à [Pichat] . En effet, les

hypothèses faites pour assurer la démonstration, sont satisfaites dans l'exemple précédent, sans entraîner toujours, comme on le voit, la convergence de l'algorithme vers (Max $\overline{P}$, Ø).

2.4) - Sur (IV) -

a) Montrons que toute chaîne à élément minimal est finie, n'est pas conséquence de toute partie libre de $\overline{P}$ est finie, même compte tenu de Max P fini, (I), $(II)_F$ et (III).

Soit $\mathcal{A} = (\mathbb{N}, \leqslant, (x*y) = \inf(x,y)+1$. Sont vérifiés :

(I) : de $x \leqslant y$ on déduit $\inf(x,z) \leqslant \inf(y,z)$ soit $x*z \leqslant y*z$,

$(II)_F$: considérons $x * (y*z)$

si $y > z$ $\quad y*z = z*z = z+1 \leqslant y$

d'où $x * (y*z) \leqslant x*y$;

sinon $y \leqslant z$ et $y*z = y+1$

$x * (y*z) = x * (y+1)$

- si $x > y$ $\quad x * (y+1) = y+2 \leqslant x+1 = x*x$

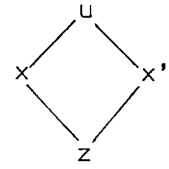
- sinon $x \leqslant y$ et $x * (y+1) = x+1 = x*x$;

et (III) : pour $x = y$ il vient

si $x > z$ $\quad x * (x*z) \leqslant x*x$

sinon $x \leqslant z$ et $x * (x*z) \leqslant x*x$

Pour $P = \{0\}$, $\overline{P} = \mathbb{N}$ une partie libre non-vide est un singleton, donc finie, et il existe pourtant une chaîne à élément minimal, non finie :
$0 < 1 < 2 \ldots . n < n+1 \ldots .$

a bis) - Soit alors $\mathcal{B}$ le treillis booléen à deux atomes 

, et $\mathcal{A} + \mathcal{B}$ la structure de

- support : somme (union disjointe) S des supports de $\mathcal{A}$ et $\mathcal{B}$.
- ordre : union des relations d'ordre avec en plus $\forall n \in \mathbb{N} \quad n \leqslant u$.
- opération : union des ensembles de triplets de $\mathcal{A}$ et $\mathcal{B}$ (l'opération ainsi définie est partielle).

(I), $(II)_F$ et (III) étant vérifiées séparément dans $\mathcal{A}$ et $\mathcal{B}$, elles le sont aussi dans $\mathcal{A} + \mathcal{B}$ puisque l'adjonction de couples à l'ordre ne pourrait être que "favorable" à la satisfaction de ces hypothèses.

Pour $P \subset S$, $P = \{0,x,x'\}$, $\text{Max } P = \{0,x,x'\}$, $u \in \overline{P}$, $\text{Max } \overline{P} = \{u\}$. $\text{Max } \overline{P} \neq \emptyset$ est fini, or pourtant, il existe une chaîne à élément minimal infinie, dans $\overline{P}$: $\mathbb{N}$ (ici les parties libres non vides sont les singletons de $\mathbb{N}$, ainsi que $\{z,n\},\{x,n\},\{x',n\}$ et $\{x,x',n\}$ quel que soit $n \in \mathbb{N}$). On remarque ainsi que l'affirmation du a) subsiste même si l'on suppose $\text{Max } \overline{P} \neq \emptyset$.

b) Montrons que $\text{Max } \overline{P}$ fini , n'est pas conséquence de toute chaîne à élément minimal est finie, même compte-tenu de Max P fini, (I), $(II)_F$ et (III).

Soit $\mathcal{U} = (\mathbb{N}$, ordre strict vide, $xy = \inf(x,y)+1)$. Sont vérifiées :

- (I): de $x \leqslant y$ (soit $x = y$) on déduit $x\,z \leqslant y\,z$;

(II): si $x(yz)$ défini, alors $x = y+1 = z+1$ et $x(yz) = x+1 = xx$;

et (III): $x(xy)$ n'est jamais défini, donc (III) est vérifiée.

Il vient pour $P = \{0\}$ $\text{Max } P = \{0\}$ $\overline{P} = \mathbb{N}$ $\text{Max } \overline{P} = \mathbb{N}$.
$\text{Max } \overline{P}$ est infini bien qu'il n'existe pas de chaîne infinie puisqu'une chaîne maximale ne peut être qu'un singleton.

c) Donnons un cas où (I), $(II)_F$, (III) sont satisfaites, où Max P et Max $\overline{P}$ sont finis et où toute chaîne à élément minimal est finie, bien qu'il existe une partie libre infinie.

On considère $\mathcal{U} + \mathcal{B}$ où l'opération + est la même qu'en abis), pour $\mathcal{A} + \mathcal{B}$. Ici, pour P = {0,x,x'} , Max P = {0,x,x'} , Max $\overline{P}$ = {u} , $\mathbb{N}$ est une partie libre infinie et si l'on définit un pointage, choisissant dans une partie de $\overline{P}$ d'intersection non vide avec $\mathbb{N}$, un des éléments de $\mathbb{N}$, le processus algorithmique ne converge pas :

	1xx'
1	xx'2
12	xx'3
..	....
12....n	xx'n+1
.....	.....

d) Notion de pointage systématique ; le pointage naturel.

On peut cependant améliorer le résultat du[3), en restreignant la classe des pointages. Un pointage sera dit systématique (notion non uniforme) s'il assure que tout élément apparaissant dans F_n finit par en être "exclu". C'est le cas du pointage "naturel" défini de la manière suivante :

on écrit les éléments de F_n en file, ceux de F'_n sont écrits en respectant l'ordre de F_n, F_{n+1} est alors une file dont les premiers éléments sont ceux de F'_n hormis f_o élément de tête de F'_n et sur lequel "pointe" F'_n.

Pour un pointage systématique, démontrons alors le

COROLLAIRE 2 - (des Lemmes 1 et 2, compte-tenu de (I), $(II)_F$, (III) et $(IV)_I$).

Soit n arbitraire et pour $x \in$ Max $\overline{P}$, x arbitraire, une formule y de

valeur x, alors

$$h(y) > 0 \Rightarrow \exists m > n \quad \exists z \in E_m \cup \tilde{F}_m \quad v(z) = x \text{ et } h(z) < h(y)$$

On raisonne par induction sur la hauteur de y en appelant D_ℓ la propriété pour les x admettant une formule de hauteur ℓ (propriété universelle sur n).

. Pour h = 1: Au cours de réductions de F_r à F'_r ($r \geq n$) si une des étiquettes des feuilles de y est éliminée par un élément de E'_n alors le problème est résolu d'après le lemme 2. Si l'une des feuilles est exclue le problème est encore résolu.

Compte-tenu que tout élément apparaissant dans un F_r finit par être exclu (hypothèse sur le pointage), l'hypothèse qu'il n'existe pas de rang où y soit majorée par un atome de F_r ($r \geq n$) implique qu'il existe au moins une chaîne à élément minimal (x) infinie, ce qui est contraire à l'hypothèse de finitude de $(IV)_I$.

. Supposons D_ℓ établie pour $\ell < L$ ($L > 1$).

y peut s'écrire comme une formule de hauteur 1 à feuilles f_i, $i=1,\ldots P$, de hauteur $< L$. D_ℓ pour $\ell < L$ fournit des formules de hauteur $< L-1$ sur E_n pour $m = \underset{i=1,\ldots P}{\text{Max}} \{m_i\}$, et finalement par (I) on a bien D_L.

De ce corollaire on déduit que tout élément maximal de $\overline{P}$, finit par figurer dans un F_n. Max P étant alors supposé être fini, il existe donc un rang tel que $\text{Max } \overline{P} \subset E_n$ et, par conséquent, $\text{Max } \overline{P} = E'_n$.

Remarquons que si un ordonné E vérifie la propriété des suites croissantes, tout élément admet un majorant dans Max E (qui n'est donc pas vide) puisque si $x \in E$ n'est pas maximal, x est majoré par $y > x$, y lui-même jouant alors le rôle x on en déduirait une suite croissante non stationnaire.

Si $\overline{P}$ vérifie la 1ère partie de IV si $\mathrm{Max}\ \overline{P} \subset E_n$ on a donc, nécessairement $F'_n = \emptyset$. On a donc établi le

THEOREME - Si $\overline{P}$ satisfait

- (I), $(II)_F$, (III)

$(IV)_f$ {
- Max P et Max $\overline{P}$ finis
- toute suite croissante de $\overline{P}$ est stationnaire

alors, pour un pointage systématique

$$\lim_n (E_n, F_n) = (\mathrm{Max}\ \overline{P}, \emptyset)$$

Application à l'exemple du 3).

Pour le pointage naturel, le processus est un algorithme, les étapes successives en sont :

	1 x x'
1	x x' 2
~~1 x~~	~~x' 2~~ u
U	

Remarque générale aux contre-exemples 1 bis) et 3).

Les opérations envisagées n'étaient que partielles; ceci n'est pas une hypothèse pour assurer l'existence de ces contre-exemples.

En effet, on peut toujours, dans le cas d'opérations partielles sur $\mathcal{A}$, associer à $\mathcal{A}$, $\mathcal{A}'$ une structure à opérations totales définie par :

- support A' = A $\cup$ {A} ; l'élément {A} ($\notin$ A) sera noté O.
- l'ordre sur A' est celui de A auquel on adjoint les couples de

$\{0\} \times A'$.

- l'ensemble des multiplets correspondants aux opérations $\overset{'}{*}_i$ est celui de ceux correspondant aux $*_i$, auquel on adjoint les multiplets de la forme (symbole opératoire, arguments, résultats) $(\overset{'}{*}_i, m, 0)$ si $*_i$ n'est pas défini pour $m \in A$, ou si 0 figure parmi les arguments.

Si $\mathcal{A}$ vérifie l'une des hypothèses (I), $(II)_f$, $(II)_F$, (III), $(IV)_f$ ou (IV), il en est de même de $\mathcal{A}'$ et réciproquement.

D'autre part, pour $P \neq \{0\}$ les deux suites $(E'_n, F'_n)_{\mathcal{A}}$ et $(E'_n, F'_n)_{\mathcal{A}'}$ sont égales.

CHAPITRE III

STRUCTURE A CONSENSUS

1) L'algorithme de Tison en algèbre booléenne.

1.1) Rappel d'un théorème.

1.2) Vérification des hypothèses.

1.3) Exemple.

2) Structure générale de consensus.

2.1) Présentation du cadre : un produit de treillis distributifs.

2.2) Conditions suffisantes pour satisfaire (III).

III - STRUCTURE A CONSENSUS

1)-Algorithme de Tison pour déterminer les monômes premiers d'une fonction booléenne (un monôme premier est un monôme maximal pour l'ordre sur les fonctions booléennes).

1.1) - Rappel d'un théorème d'algèbre booléenne.

On note $\overline{m}$ le monôme m "effectué". Sur B, l'ensemble des monômes booléens, ordonné par la restriction de l'ordre sur les fonctions booléennes, on définit une opération binaire partielle, commutative :

$m*n$ = consensus de m et de n, si il existe.

On rappelle une CNS d'existence du consensus de m et n :
il existe une et une seule lettre a apparaissant sous une forme dans $\overline{m}$ et sous la forme complémentée dans $\overline{n}$; le consensus est alors le produit des lettres de m et n, en omettant la lettre a.

On démontre en algèbre booléenne, le

THEOREME - $\text{Max } \overline{\{m_1, m_2, \ldots . m_p\}}^{*} = \{\text{Monômes premiers de } f = \sum_{1}^{p} m_i\}$

1.2) - Vérification des hypothèses (I), $(II)_F$, (IV).

- (I) Soit, m,n et p, supposés effectués, vérifiant :

$m \leqslant n$ (c'est-à-dire $m = \mu n$)

et $m*p$ défini (m et p admettant un consensus suivant a $\geqslant$ m)

si a figure dans n on peut écrire $m*p = \mu(n*p) \leqslant n*p$

sinon $m*p \leqslant \frac{m}{a} \leqslant n$

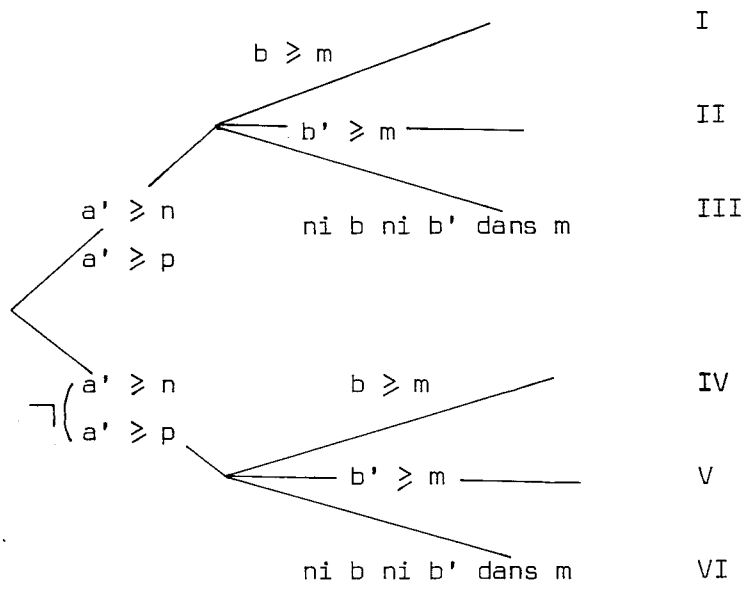
d'où l'on déduit que (I) est bien vérifiée.

- $(II)_F$ Soit, m,n et p supposés effectués, vérifiant

$m * (n*p)$ défini (m et $n*p$ consensus suivant $a \geqslant m$, n et p suivant $b \geqslant n$).

Remarque - Certainement $a \neq b$.

Suivant que a' figure dans n et p ou dans l'un des deux seulement (et, dans ce cas, quitte à un changement de notation, on peut supposer qu'il s'agit de n) et que b ou b' ou ni l'un ni l'autre figure dans m, on a les six possibilités suivantes :



- Si μ, ν , π représentent des monômes ne contenant ni a ou b, ni a' ou b', et respectivement diviseurs maximaux de m, n, p pour cette propriété, on peut schématiser les différentes possibilités par

$$m*(n*p) = \frac{m}{\mu} *\left(\frac{n}{\nu}*\frac{p}{\pi}\right)\times\mu\nu\pi = a\begin{cases} b \\ b' \\ 1 \\ b \\ b' \\ 1 \end{cases} *\left\{a'b*\begin{cases} a \\ a' \\ a' \\ 1 \quad b' \\ 1 \\ 1 \end{cases}\right\}\times\mu\nu\pi = \begin{cases} b \\ b' \\ 1 \\ \\ b \\ b' \\ 1 \end{cases} \times\mu\nu\pi \begin{cases} \leqslant b\mu\nu & = m*n \\ \leqslant b'\mu\nu & = m*p \\ = \mu\nu\pi & = (m*n)*(m*p) \\ & \\ \leqslant b\mu\nu & = m*n \\ \leqslant b'\pi & = p \\ = \mu\nu\pi & = (m*n)*p \end{cases}$$

- (III) est immédiatement vérifié puisqu'une formule $x * (x*y)$ n'est jamais définie.
- (IV) Pour Max P fini soit V l'ensemble (fini) des lettres primées ou non, apparaissant dans les monômes de Max P.

De Card $\overline{P}$ < Card $\mathcal{P}(V)$ on déduit que $\overline{P}$ est fini.

1.3) Exemple d'application de l'algorithme

	abc	abd'	acde	bcd	bcd'
abc	abd'	acde	bcd	bcd'	
abc abd'	acde	bcd	bcd' / abce	abc	
abc abd'acde	bcd	bcd' / abce			
abc abd'acde bcd	bcd' / bc				
abd' acde bc					

2) - Structure générale de consensus

2.1) - Etant donné un produit non vide de treillis $T = \prod_{i \in I} T_i$ ordonné par l'ordre produit, considérons un ensemble d'opérations binaires, totales, univoques, défini par une famille Φ d'éléments de $\mathcal{P}(I)$ selon :

à tout $J \in \Phi$ $(J \subset I)$ on associe

$x \underset{J}{*} y = (z_i)_{i \in I}$ avec z_i = si $i \in J$ alors $x_i \vee y_i$ sinon $x_i \wedge y_i$.

Les $(\overset{*}{J})_{J \in \Phi}$ sont commutatives, associatives, idempotentes, isotones : cela découle immédiatement de la structure de treillis des T_i.

Proposition 1 - La distributivité des T_i implique celle des $\overset{*}{J}$.

En effet, soit $x \overset{*}{J} (y \overset{*}{K} z) = (t_i)_{i \in I}$

il vient $t_i =$ si $i \in K-J$ alors $x_i \wedge (y_i \vee z_i) = (x_i \wedge y_i) \vee (x_i \wedge z_i)$

sinon

si $i \in J-K$ alors $x_i \vee (y_i \wedge z_i) = (x_i \vee y_i) \wedge (x_i \vee z_i)$

sinon

si $i \in J \cap K$ alors $x_i \vee (y_i \vee z_i) = (x_i \vee y_i) \vee (x_i \vee y_i)$

sinon $x_i \wedge (y_i \wedge z_i) = (x_i \wedge y_i) \wedge (x_i \wedge y_i)$.

Or $(x \overset{*}{J} y) \overset{*}{K} (x \overset{*}{J} z) = (\mathcal{C}_i)_{i \in I}$ avec

$\mathcal{C}_i =$ si $i \in K-J$ alors $(x_i \wedge y_i) \vee (x_i \wedge z_i)$

sinon

si $i \in J-K$ alors $(x_i \vee y_i) \wedge (x_i \vee z_i)$

sinon

si $i \in J \cap K$ alors $(x_i \vee y_i) \vee (x_i \vee z_i)$

sinon $(x_i \wedge y_i) \wedge (x_i \wedge z_i)$.

On a donc bien $\forall i \in I \quad t_i = \mathcal{C}_i$ les $\overset{*}{J}$ sont des distributives.

$\mathcal{A} = (T, \leqslant, \{\overset{*}{J}\}_{J \in \Phi})$ vérifie donc (I) et $(II)_F$ (uniformément en $\overline{P}$ pour $P \subset T$).

2.2) - Problème - Sous quelles conditions sur Φ, (III) est-elle satisfaite ?

Soit $x \underset{J}{*} (x \underset{K}{*} y) = (z_i)_{i \in I}$, il vient

z_i = si $i \in K-J$ alors $x_i \wedge (x_i \vee y_i) = x_i$

sinon

si $i \in J-K$ alors $x_i \vee (x_i \wedge y_i) = x_i$

sinon

si $i \in J \cap K$ alors $x_i \vee (x_i \vee y_i) = x_i \vee y_i$

sinon $x_i \wedge (x_i \wedge y_i) = x_i \wedge y_i$

On en déduit deux conditions suffisantes, pour que (III)

- CS_1 $\forall \{J,K\} \subset \Phi$ $J=K$ ou $J \cap K = \emptyset$

En effet, il vient alors

pour $J = K$ $x \underset{J}{*} (x \underset{J}{*} y) = x \underset{J}{*} y$

pour $J \neq K$ $x \underset{J}{*} (x \underset{K}{*} y) \leqslant x$

Cas particulier où CS_1 est satisfaite $\forall J \in \Phi$ $J = \{j\}$
($\mathcal{A}$ est alors une structure à, au plus, $\bar{\bar{I}}+1$ opération).

- CS_2 $\forall \{J,K\} \subset \Phi$ $J \cap K = \emptyset$ ou $J \cup K \in \Phi$

en effet, il vient alors, si $J \cap K \neq \emptyset$, $x \underset{J}{*} (x \underset{K}{*} y) \leqslant x \underset{J \cup K}{*} y$

sinon $x \underset{J}{*} (x \underset{K}{*} y) \leqslant x$

En remarquant que l'ensemble des éléments maximaux (pour l'inclusion) de Φ est une partie suffisante, on se ramène à une seule condition

CS	l'ensemble des éléments maximaux de Φ vérifie la condition d'intersection vide 2 à 2 (prépartition de I).

2.3) - Si on définit le support d'un élément de T, comme l'ensemble des indices tel que x_i ne soit pas maximal dans T_i, on a la

Proposition 2 -

P vérifie Max P est un ensemble fini d'éléments à support fini $\Rightarrow$ Cond. B.

En effet, une partie suffisante finie est formée par la réunion (finie) des supports des éléments de Max P.

Finalement, grâce à V (IV)

Dans T, si Max P est un ensemble fini d'éléments à support fini, on peut appliquer l'algorithme d'exclusion pour trouver Max $\overline{P}$, dès que

- l'ensemble des éléments maximaux de Φ forment une prépartition de I.

CHAPITRE IV

1) LA DEMONSTRATION AUTOMATIQUE FONDEE SUR UNE FORME DU THEOREME DE HERBRAND

1.1) Le cadre du calcul des prédicats du 1er ordre.

1.2) La mise d'un problème sous forme clausale.

1.3) Le principe de résolution [ROBINSON].

2) UNE AUTRE PRESENTATION DU THEOREME DE RESOLUTION

2.0) Rappels.

2.1) Etude de la subsomption en tant que préordre.

2.2) Une caractérisation du préordre lié à la subsomption.

2.3) Décomposition du préordre.

2.4) Un principe dual de la subsomption.

2.5) Définition de l'opération de résolution et le théorème de résolution sous la forme: S insatisfaisable $\Leftrightarrow \{ \square \} = \text{Max } \bar{S}^{\mathcal{R}}$.

2.6) Mise en oeuvre de l'algorithme d'exclusion pour calculer $\text{Max } \bar{S}^{\mathcal{R}}$.

3) INTERPRETATION BOOLEENNE DU THEOREME DE HERBRAND ET UN NOUVEL ALGORITHME DE DEMONSTRATION AUTOMATIQUE

3.0) Un théorème de compacité en algèbre de Boole et son corollaire.

3.1) Le théorème de Herbrand.

3.2) Retour sur la subsomption.

3.3) Un nouvel algorithme de démonstration automatique.

3.4) Conjugaison de la méthode d'exclusion avec celle du support. Exemple.

Remarque préliminaire - Ce chapitre est divisé en trois parties : la première, intitulée "la démonstration automatique fondée sur le théorème de Herbrand", présente le cadre général de la majorité des méthodes modernes utilisées en démonstration automatique. On n'y trouvera rien de très nouveau par rapport à d'autres exposés, et elle ne sert que de référence à la deuxième partie, intituée "une autre présentation du théorème de résolution". Il est donc possible, pour le lecteur familiarisé avec la démonstration automatique, de se rendre directement en tête de la deuxième partie.

1) LA DEMONSTRATION AUTOMATIQUE FONDEE SUR UNE FORME DU THEOREME DE HERBRAND, LE THEOREME DE RESOLUTION DÛ A ROBINSON (1965)

1.1) On a l'habitude de considérer qu'un théorème (de mathématique) se présente sous la forme d'un énoncé affirmant que, sous un certain nombre d'hypothèses, on est assuré de telle ou telle propriété.

Exemple - Un théorème d'algèbre, élémentaire par les notions qui le sous-tendent, mais pas forcément facile à démontrer ...

Supposons que dans une structure algébrique à une opération binaire associative les équations (en x) $ux = v$ et $xu = v$ admettent chacune une solution, alors nécessairement l'opération admet au moins un élément neutre, à droite par exemple.

Le langage des prédicats du ler ordre permet de formuler un grand nombre de problèmes sous la forme

$$\{F_1, F_2, \ldots, F_p\} \vdash F$$

où F et les F_i sont des formules du calcul des prédicats du ler ordre et où le symbolisme $A \vdash B$ veut dire et se lit, B est conséquence syntaxique de A.

En introduisant la notion (sémantique) de modèle, on dira qu'une formule F_1 (du CP_1) est conséquence logique d'un ensemble de formules $\{F_1, F_2, \ldots, F_p\}$[1] et l'on écrira

$$\{F_1, F_2, \ldots, F_p\} \models F$$

si toute réalisation satisfaisant (ou modèle) de l'ensemble de formules $F_1, F_2, \ldots, F_p$ satisfait aussi F.

---

[1] *Si cet ensemble est vide, l'écriture $\emptyset \models A$ (ou $\models A$) signifiera donc que A est satisfaite dans toute réalisation, on dira alors que A est valide et, dans le cas contraire, on dira que A est insatisfaisable.*

On a les(meta)théorèmes

$$\vdash F \Leftrightarrow \models F \quad \begin{cases} \Rightarrow & \text{th. de consistance} \quad \_ \text{ facile} \\ \Leftarrow & \text{th. de complétude} \quad \_ \text{ difficile:Gödel(1935)} \end{cases}$$

On a aussi pour un ensemble de formules $F_1, F_2, \ldots F_p$

$$F_1, F_2, \ldots, F_p \models F \Leftrightarrow F_1 \wedge F_2 \wedge \cdots \wedge F_p \wedge \neg F \text{ insatisfaisable.}$$

Compte-tenu de ces (meta)théorèmes, on peut ramener le problème de la démonstration (au sens classique de ce mot) de nombreuses propriétés mathématiques au problème de prouver qu'une formule du CP_1 (calcul des prédicats du 1er ordre) est insatisfaisable.

On montre encore qu'une formule quelconque F peut être transformée algorithmiquement en une formule équivalente F'[1] F' s'écrivant

$$Q_1 x_1 \; Q_2 x_2 \cdots Q_p x_p F''$$

où les symboles Q_i sont à remplacer par $\forall$ ou $\exists$ et où F" est une formule sans quantificateur. F' est alors dite une forme prénexe de F.

D'autre part, et quitte à augmenter l'ensemble des symboles fonctionnels du langage correspondant à une formule F, d'un certain nombre(fini) d'éléments appelés "fonctions de Skolem", on peut transformer algorithmiquement la formule F, supposée prénexe, en une formule F' ne contenant, au plus, que des quantificateurs universels, telle que

F est insatisfaisable si et seulement si F' insatisfaisable.

Remarquons enfin que toute formule peut être transformée algorithmi-

---

[1] *C'est-à-dire que F et F' sont simultanément satisfaites ou non dans toute réalisation ou encore* $\vdash F \sim F'$.

quement en une formule de forme normale conjonctive, c'est-à-dire du type

$$C_1 \wedge C_2 \wedge \cdots \wedge C_p$$

où chacun des C_i, appelés clauses, s'écrit

$$C_i = L_{i_1} \vee L_{i_2} \vee \cdots \vee L_{i_q}$$

où les L_j, appelés littéraux, sont des formules atomiques ou la négation de telles formules.

En définitive, la majeure partie des problèmes peut donc se ramener à montrer qu'un ensemble de clauses n'admet pas de modèle (de réalisation les satisfaisant toutes) où finalement, on peut considérer que :

- une clause est un ensemble[1] fini de littéraux ;
- un littéral est un atome ou la négation d'un atome ;
- un atome est un prédicat suivi de n-termes si le prédicat est à n-places[1] ;
- un terme est soit une variable, soit une fonction suivie de n termes si la fonction est à n places ;[1]
- l'alphabet d'un problème est un ensemble (généralement fini) de symboles de
  - variables : u, v, w, x, y, z ....;
  - fonctions : a, b, c, f, g, h ....;
    (à chaque symbole de fonction est attaché un entier : son nombre de places) ;
  - prédicats : P, Q, R .....
    (à chaque symbole de prédicat est attaché un entier : son nombre de places) ;
  - et négation : $\neg$.

---

[1] *Conformément à l'usage concernant les notations, on se permet, si aucune confusion n'est à craindre, de supprimer les parenthèses et virgules dans l'écriture des clauses, littéraux, prédicats et termes.*

On dira que deux littéraux de la forme P et $\neg$ P constituent une paire complémentaire.

1.2) On montre que, dans ce cadre, la notion générale de modèle peut être très simplifiée.

Tout d'abord, comme ensemble de base d'une réalisation, il suffit de ne considérer que la base constituée de l'ensemble des termes constants.

Cet ensemble dit"univers de Herbrand" ne devant pas être vide, on ajoute une constante (fonction à 0 place) arbitraire, au vocabulaire de tout problème qui n'en comprendrait pas déjà.

La notion de modèle peut alors se ramener aux notions suivantes :

Un modèle d'un ensemble Σ de clauses constantes (ne faisant pas intervenir de symboles de variables) est simplement un ensemble M, de littéraux constants, ne contenant pas de paire complémentaire et tel que

$$\forall C \in \Sigma \quad \exists L \in M \quad L \in C$$

(un modèle d'un ensemble non vide de clauses ne peut donc être vide).

Un modèle d'un ensemble de clauses Σ quelconques sera un modèle de l'ensemble des clauses de Σ , rendues constantes en substituant de toutes les façons possibles les symboles de variables par les éléments de l'univers de Herbrand de Σ .

(dans une même clause on fait évidemment correspondre à deux occurrences d'une même variable, le même terme de l'univers de Herbrand).

Exemple - Considérons l'ensemble $\{C_1, C_2\} = \{P(x)\ Q(a),\ \neg P(x)\ R(b)\}$.
L'univers de Herbrand associé est $\{a,b\}$. On peut déterminer l'ensemble des modèles minimaux en développant selon des lois immédiates

$$(P_a + Q_a)\ (P_b + Q_a)\ (\neg P_a + R_b)\ (\neg P_b + R_b)$$

$$= P_a P_b R_b + Q_a \neg P_a \neg P_b + Q_a R_b$$

soit trois modèles minimaux

$$\{P_{(a)}, P(b), R(b)\}\ \{\neg P(a), \neg P(b), Q(a)\}\quad \{Q(a), R(b)\}$$

- Considérons un ensemble de clauses contenant la clause vide (celle qui ne contient aucun littéral), souvent notée $\square$.

D'après la relation $\forall C \in \Sigma \quad \exists L \in M \quad L \in C$, appliquée à $C = \square$ on voit que

un ensemble de clauses contenant la clause vide n'admet pas de modèle.

Dans le cas du théorème d'algèbre indiqué plus haut, le passage du problème à sa forme clausale peut se faire de la façon suivante :

On introduit le prédicat à trois places :

P(x,y,z) qui signifie que z est un produit de x et y.

Il faut alors traduire les hypothèses concernant la structure algébrique à une cpération binaire, ainsi que la conclusion qu'il existe un élément neutre à droite.

On peut exprimer l'associativité du produit par

$$F_1 : \forall x \forall y \forall z \forall u \forall v \forall w \quad (P(x,y,u) \wedge P(y,z,v)) \supset (P(x,v,w) \sim P(u,z,w))$$

$$\left\{ \text{si } u \in \{xy\} \quad \text{et} \quad v \in \{yz\} \quad \text{alors} \quad w \in \{x(yz)\} \Longleftrightarrow w \in \{(xy)z\} \right\} .$$

On peut exprimer l'existence des solutions des équations de division par

F_2 : $\forall x \; \forall y \; \exists g \qquad P(g,x,y)$ (solution à gauche)

F_3 : $\forall x \; \forall y \; \exists d \qquad P(x,d,y)$ (solution à droite) .

La conclusion peut s'écrire

F_4 : $\exists x \; \forall k \qquad P(k,x,k)$.

Le problème revient donc à montrer qu'est insatisfaisable la formule $F_1 \wedge F_2 \wedge F_3 \wedge \neg F_4$ où l'on a pris soin de changer les noms des variables communes aux différents F_i.

La partie sans quantificateur de F_1 se transforme suivant

$$\neg P_{xyu} \vee \neg P_{yzv} \vee \left[(P_{xvw} \supset P_{uzw}) \wedge (P_{uzw} \supset P_{xvw})\right]$$

$$(\neg P_{xgu} \vee \neg P_{yzv} \vee \neg P_{xvw} \vee P_{uzw}) \wedge (\neg P_{xyu} \vee \neg P_{yzw} \vee \neg P_{uzw} \vee P_{xvw})$$

et apparaît comme la conjonction de deux clauses (le travail avance vite!).
La "skolemisation" de F_2 donne $\forall x \; \forall y \quad P(g(x,y),x,y)$
et de même F_3 donne $\forall x \; \forall y \quad P(x,d(x,y),y)$.
La négation de F_4 s'écrit $\forall x \; \exists k \; \neg P(k,x,k)$ dont la skolémisée est
$\forall x \quad \neg P(k(x),x,k(x))$.

La forme clausale du théorème est donc

$C_1 = \{ \neg P(x,y,u) \; , \; \neg P(y,z,v) \; , \; \neg P(x,v,w) \; , \; P(u,z,w)\}$
$C_2 = \{ \neg P(x,y,u) \; , \; \neg P(y,z,v) \; , \; \neg P(u,z,w) \; , \; P(x,v,w)\}$
$C_3 = \{ P(g(x,y) \; , \; x, \; y)\}$
$C_4 \quad \{ P(x,d(x,y), \; y)\}$
$C_5 = \{ \neg P(k(x) \; , \; x, \; k(x)\}$

Remarque - Dans une telle écriture, deux variables de même nom mais apparaissant dans deux clauses différentes ne représentent pas le même objet ; on pourrait dire que dans chaque clause il y a mutification des variables.

Le théorème d'Herbrand peut s'énoncer:

Si S est ensemble (fini) de clauses, H son univers de Herbrand, alors S est insatisfaisable $\Longleftrightarrow$ $\exists P \subset H$ P fini tel que l'ensemble des clauses de S rendues constantes sur P est insatisfaisable.

Si l'on sait énumérer l'univers de Herbrand (ce qui est immédiat) on dispose donc d'une procédure semi-décidable en ce qui concerne l'insatisfaisabilité de S.

Les tentatives de Gilmore (1960) et Davis-Putman (1960) relèvent de cette dernière idée.

Mais la croissance très rapide du nombre de développements à calculer, en vue de déterminer les modèles sur les différentes parties finies de H, ne permet pas d'envisager la démonstration automatique de théorèmes autres que vraiment très simples, beaucoup plus simples que celui auquel on vient de s'intéresser.

1.3) Une autre version du théorème de Herbrand, dûe à Robinson, est fondée sur le principe de résolution.

L'opération Résolution de deux clauses.

La définition suivante de l'opération de résolution , et que l'on trouve actuellement le plus souvent, [Chang et Lee] est différente de celle initialement proposée par Robinson mais lui est équivalente.

Notion d'Unification d'un ensemble de littéraux.

On dira qu'un ensemble $\{L_1, \ldots\ldots, L_p\}$ est unifiable, s'il existe une substitution σ de variables en termes telle que

$$\sigma L_1 = \sigma L_2 = \ldots = \sigma L_p \quad ;$$ [1]

σ est alors un unificateur de $\{L_1, \ldots L_p\}$.

Exemple - $\{P(x,t,x)\ ,\ P(f(y)\ ,\ t,\ z)\ ,\ P(x,y,f(t)\}$

est unifiable par la substitution

$$x \longmapsto f(t)$$
$$y \longmapsto t$$
$$z \longmapsto f(t)$$

le résultat commun est $P(f(t)\ ,\ t\ ,\ f(t))$.

Un unificateur de A, σ sera dit plus général que σ' s'il existe une substitution σ'' telle que pour chacun des littéraux L de A.

$$\sigma'' \circ \sigma L = \sigma' L$$

Il est facile de montrer, en exhibant un algorithme d'unification, qu'il existe un unificateur maximal pour cette propriété qui sera plus grand unificateur (p.g.u.).

Notion de facteur d'une clause.

Si une partie d'une clause C possède un plus grand unificateur σ alors la clause σC est dite facteur de C (ou obtenue par factorisation de C). Le nombre des facteurs d'une clause est évidemment fini.

Exemple - $P(a,x,y) \neg P(a,b,y)\ P(y,b,y)\ Q(x)$ ainsi que
$P(a,b,a) \neg P(a,b,a)\ Q(b)$ sont des facteurs de
$P(a,x,y) \neg P(z,b,t)\ P(t,b,t)\ Q(x)$.

Remarque - Dans le dernier exemple, la clause initiale possède des facteurs

---

[1] *Dans la littérateure spécialisée c'est plutôt le symbolisme* $L\sigma$ *qui est employé pour désigner le résultat de la substitution* σ *sur le littéral* L .

présentant une paire complémentaire constante. Une telle clause sera appelée une tautologie et l'on montre facilement que si une clause T d'un problème S est une tautologie

S insatisfaisable $\Longleftrightarrow$ S-T insatisfaisable.

Résolvants binaires de deux clauses C_1 et C_2.

En supposant que les variables de C_1 sont $x_1, x_2, \ldots x_p$
et celles de C_2 $y_1, y_2, \ldots y_q$,

si C_1 et C_2 possèdent une paire de littéraux complémentaires $L_1 \subset C_1$ et $\neg L_1 \subset C_2$, unifiable par un p.g.u., σ, alors la clause

$\sigma(C_1 - \{L_1\}) \cup \sigma(C_2 - \{\neg L_1\})$ sera dite résolvant binaire de C_1 et C_2 (sur L_1).

Deux clauses peuvent présenter 0,1 ou plusieurs (en nombre fini) résolvants binaires.

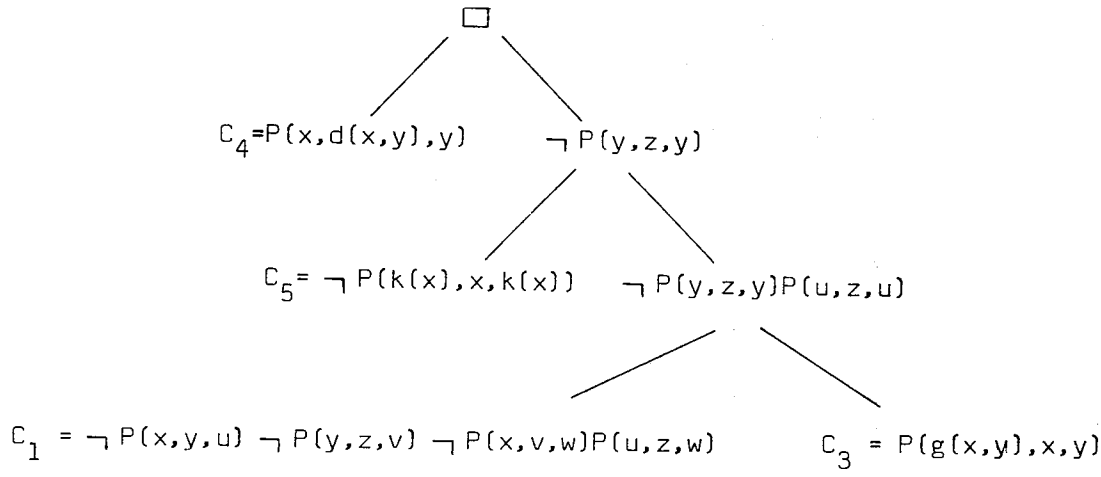
Résolvants de deux clauses.

L'ensemble des résolvants de deux clauses C_1 et C_2 sera alors l'ensemble (éventuellement vide) des résolvants binaires des facteurs de C_1 avec ceux de C_2.

On peut alors énoncer le théorème de Résolution (Robinson 1965),

S est insatisfaisable $\Longleftrightarrow$ $\square$ appartient à la fermeture de S pour l'opération de résolution.

Dans l'exemple du problème cité plus haut



Commentaires -

. Par la substitution $\begin{cases} v \mapsto y \\ w \mapsto u \end{cases}$, C_1 se factorise en

$$\neg P(x,y,u)\ \neg P(y,z,y)\ P(u,z,u)$$

dont un résolvant avec C_3 est $\neg P(y,z,y)\ P(u,z,u)$.

. Le théorème d'algèbre admet la démonstration directe suivante, en désignant par E l'ensemble support de la structure à une opération binaire : si E n'est pas vide, soit $a \in E$ et x tel que $xa=a$.

Alors $\forall c$ $ac = (xa)\ c = x(ac)$

d'où l'on déduit que x est neutre sur aE.

Or $aE = E$ puisque $\forall b \quad \exists x\ ax = b$

. Une analyse plus fine de la démonstration obtenue à l'aide de la forme clausale montre que le théorème démontré est plus général que celui qu'on avait annoncé : on a, en fait, très exactement démontré :

Si une opération binaire sur un ensemble non vide, pas forcément univoque ni même partout définie (hypergroupoïde [Lévy-Bruhl]) vérifie

- l'axiome des quotients, à gauche et à droite
- la semi-associativité à droite :

$$\{x(y\ z)\} \subset \{(xy)z\}^{(1)},$$

alors il existe un élément neutre à droite.

---

(1) $\{x(y\ z)\}$ *désigne l'ensemble des résultats de* x *composé avec l'ensemble des résultats de* y *composé avec* z.

2) UNE AUTRE PRESENTATION DU THEOREME DE RESOLUTION

Le théorème d'Herbrand, en indiquant qu'il existe, dès qu'un ensemble fini de clauses est insatisfaisable, un ensemble fini de leurs instances constantes insatisfaisable, fournit une procédure pour la semi-décidabilité du CP_1. Dans la réalité, quand on essaye "d'implémenter" un algorithme relevant directement du théorème de Herbrand, on s'aperçoit qu'il manque un "démon de la preuve" qui serait d'abord chargé de déterminer en un temps raisonnable un des fameux ensembles finis dont le théorème d'Herbrand affirme l'existence.

De ce point de vue, Robinson fait remarquer que le théorème de résolution qui dérive de celui de Herbrand, nous dispense des services du "démon de la preuve."

Nous allons, maintenant, donner une démonstration directe du theorème de résolution (généralisé à un ensemble dénombrable de clauses) dont on verra que le théorème de Herbrand est un corollaire.

Pour cela, nous allons travailler non pas sur des clauses, mais sur des classes d'ensembles de clauses pour une certaine relation d'équivalence, et introduire une autre opération de résolution dont on montrera qu'elle est équivalente à celle de Robinson.

Considérons un ensemble dénombrable Σ de clauses.

2.0) Rappels - On définit l'"univers de Herbrand" de Σ ,H, comme l'ensemble des schémas fonctionnels[1] sur le vocabulaire (dénombrable) des symboles fonctionnels apparaissant dans Σ (si Σ ne comporte pas de symboles fonctionnels à 0 place on en ajoute 1 arbitraire).

Cet ensemble de termes constants est encore dénombrable puisque borné en cardinal par le cardinal de l'ensemble des suites finies sur un ensemble au plus dénombrable.

On appellera instance d'une clause, le résultat de la substitution aux mêmes symboles de variable de cette clause, des mêmes termes.

On appelle modèle d'un ensemble de clause $S \subset \Sigma$

tout ensemble M de littéraux constants, ne contenant pas de littéraux complémentaires[2], et tel que dans toute instance constante d'une clause de S on puisse trouver un littéral qui soit aussi dans M :

$$\forall\ C \in H(S)\ \ \exists L \in M \quad L \in C$$

où H(S) désigne l'ensemble des instances constantes des clauses de S.

2.1) Etude de la subsomption en tant que préordre -

Définition - On dira, de la façon habituelle, que la clause C est subsumée[3] par la clause D et l'on écrira CsD s'il existe une instance de D, $\sigma D \subset C$.

---

[1] *Sur la définition de l'ensemble des schémas fonctionnels, voir par exemple* [*Kreisel Krivine*].

[2] *Deux littéraux sont dits complémentaires et forment alors une paire complémentaire si l'un est la négation de l'autre, i.e obtenu en le faisant précéder du symbole* $\neg$

[3] *Du latin subsumere, prendre parmi d'autres.*

On peut noter par le symbole S la relation duale :

$C \; s \; D \Leftrightarrow D \; S \; C$ et nous lirons indifféremment C s D ou D S C

C est subsumée (ou sous-impliquée) par D

D subsume (ou sous-implique) C

Propriété - La relation de subsomption (sous-implication) est un préordre sur l'ensemble des instances des clauses de Σ .

En effet, il est évident que $X \; s \; X$ puisque $X \subset X$

et, de plus, $X \; s \; Y$ et $Y \; s \; Z$ implique $X \; s \; Z$

puisque $\sigma Y \subset X$ et $\sigma' Z \subset Y$ implique $\sigma \circ \sigma' \; Z \subset X$.

Remargue - Cette notion est bien classique dans la littérature, bien qu'il n'en soit jamais fait un usage explicite en tant que préordre.

Exemples - $P(a)Q(a) \; s \; P(a)P(x)Q(x) \; s \; P(a)Q(x) \; s \; P(x)Q(y)$

mais $P(a)Q(x)$ et $P(x)Q(x)$ sont incomparables selon s.

2.2) Une caractérisation du préordre s - Soit deux clauses telles que $X \; s \; Y$. Considérons un modèle M, d'une clause Y. M contient un littéral de toute clause constante de X, puisqu'une telle clause est aussi une clause constante de Y. On en déduit le

THEOREME 2 — X s Y $\Longrightarrow$ tout modèle de Y est un modèle de X.

Nous allons nous intéresser à la réciproque. Tout d'abord, on remarque qu'une condition nécessaire pour assurer la réciproque est que H soit infini puisque, par exemple pour H = {a}, P(a) et P(x) ont même ensemble de modèles (i.e. {P(a)}) bien que P(a) ne **subsume pas** P(x)).

Avant d'énoncer et de démontrer la réciproque dans le cas où H est infini, démontrons le

LEMME 2- Soit deux clauses dont l'une C est obtenue à partir de l'autre D, par instanciation d'un ensemble D' $\subset$ D, de littéraux sur une partie D" $\subset$ D. Alors C et D ont même ensemble de modèles.

Exemple - C = P(a)Q(a)P(y) et D = P(a)P(x)Q(a)Q(x)R(z)
vérifient les conditions du Lemme ;
C = P(a)Q(a)R(y) et D = P(a)P(x)Q(z)R(z)
ne les vérifient pas.

En effet, il est immédiat (cf. dernier théorème) que tout modèle de D est un modèle de C puisque C s D. D'autre part, si M est un modèle de C, comme toute clause constante de D est une clause constante de C, M est aussi un modèle de D, ce qui finit d'établir le lemme.

Nous allons, maintenant, démontrer la RECIPROQUE DU THEOREME 2.

Si H est infini, alors tout modèle de Y est un modèle de X $\Longrightarrow$ X s Y

Démonstration - Tout d'abord, remplaçons éventuellement Y par Y' $\subset$ Y, Y' minimal pour l'inclusion et telle que Y' et Y vérifient les conditions du lemme précédent ; d'après ce lemme Y' et Y ont même ensemble de modèles.

Soit alors P un symbole de littéral[1] de Y' et l'on désignera par $P(x_1,\ldots,x_n)$ une de ses occurrences dont les symboles de variables sont $x_1,\ldots,x_n$.

$M = \{P(t_1,\ldots,t_n)\}_{(t_1,\ldots,t_n) \in H^n}$ est un modèle minimal de Y ; toute clause constante de X contient l'un des $P(t_1,\ldots t_n)$. Le symbole P apparaît donc dans X.

Supposons qu'aucune de ses occurrences dans X ne soit sous forme d'une instance $\sigma P(x_1,\ldots x_n)$. Alors il existe, puisque H est infini et que le nombre d'occurrences de P dans X est fini, au moins une instance constante de P dont M n'est pas un modèle, non plus que de X.

Pour tout littéral de Y' il existe donc dans X une instance de ce littéral.

Nous allons montrer que les différentes substitutions correspondant aux différents littéraux de Y' sont compatibles, c'est-à-dire qu'il n'existe pas deux de ces substitutions transformant, l'une le symbole x vers le terme t_1 et l'autre vers $t_2 \neq t_1$. En effet, dans ce cas, supposons que la transposition $x \longmapsto t_1$ corresponde à $P(\ldots,x,\ldots)$ et $x \mapsto t_2$ à $Q(\ldots,x,\ldots)$ (il n'est pas impossible que P = Q).

On peut alors construire un modèle minimal de Y' contenant

$$\{P(\ldots,t_2,\ldots) \ , \ Q(\ldots,t_1,\ldots)\}$$

ne contenant pas $\{P(\ldots,t_1,\ldots),Q(\ldots,t_2,\ldots)\}$ qui ne sera donc pas un modèle de X.

(Exemple, supposons $Y = P(x)Q(x)$ et $X = P(a)\ Q(b)$, $\{P(b),Q(a)\}$ est un modèle de Y et pas de X).

---

[1] *On appellera symbole de littéral, la quantité P (resp. $\neg P$), si le littéral est une formule atomique (resp. la négation d') commençant par P.*

2.3) Décomposition du préordre (équivalence et ordre sur les classes).

On dispose maintenant des outils nécessaires à la décomposition du préordre en une relation d'équivalence et un ordre sur ses classes.

En effet, considérons la relation d'équivalence

$$X \text{ eq } Y \iff X \text{ s } Y \text{ et } Y \text{ s } X$$

Dans le cas H infini[1], X s Y et Y s X s'exprime grâce à la caractérisation en termes de modèle, par

X et Y ont même ensemble de modèles.

Cette relation d'équivalence induit sur les parties de l'ensemble des instances de clauses de Σ , une relation qui n'est autre que l'équivalence $\sim$ puisque l'on a

S et S' ont même ensemble de modèles $\iff$ $S \sim S'$[2].

On désignera par $\dot{A}$ la classe de A.

On peut encore énoncer la propriété :

S et S' ont même ensemble de clauses constantes $\iff$ $S \sim S'$.

En effet, la définition d'un modèle fait, d'un modèle de S, un modèle de ses clauses constantes.

Exemple - En particulier $\{A(x)\} \sim \{A(i)\}_{i \in H}$

---

[1] *Dorénavant, nous supposerons H infini comme implicite, sauf indication contraire ; dans le cas contraire, on se ramène facilement, en fait, du calcul des prédicats au calcul propositionnel, i.e. à une structure isomorphe à l'algèbre de Boole.*

[2] *Ici, il conviendrait de remplacer S et S' par les formules du CP_1 qui leur correspondent, si l'on tient à conserver le même symbole $\sim$.*

La réciproque, dans le cas où S est satisfaisable, s'obtient par l'absurde en utilisant la caractérisation de la subsomption :

THEOREME - Si S est satisfaisable, alors $S \sim S' \iff$ S et S' ont même ensemble de clauses constantes.

L'ordre sur les classes est défini par

$$\dot{A} \leq \dot{B} \iff A \; s \; B$$

On a encore les

Propriété 1 - Soit S un ensemble de clauses (parmi les instances des clauses de Σ), alors

$$\forall \, C \in S \quad C \; s \; \square \; ^{(1)} \; ;$$

la clause vide est un élément maximum ou encore un élément universel. (Démonstration évidente car $\forall X \quad \varnothing \subset X$).

Propriété 2 - Si T est une tautologie, c'est-à-dire une clause contenant une paire complémentaire (ici constante ou non) :

$$\forall \, C \in S \quad \left.\begin{array}{l} T \text{ et } C \text{ sont comparables} \\ C \text{ non tautologique} \end{array}\right\} \Longrightarrow \; T \; s \; C \; .$$

On peut considérer que cette propriété "rapproche" les tautologies du statut d'éléments minimaux de l'ensemble des clauses non tautologiques.

Ces deux propriétés sont à rapprocher de ce qu'en algèbre de Boole

- le monôme 1 (rôle dual de $\square$ à cause de la correspondance $\begin{array}{l} \wedge \mapsto + \\ \vee \mapsto \cdot \end{array}$) majore tous les monômes, il est "universel".

---

(1) *Le symbole $\square$ désigne la clause vide (l'ensemble vide), de même que 0 est aussi une autre écriture de $\varnothing$.*

- un monôme contenant le produit xx' est le monôme nul, qui est un "zéro".

Remarquons, d'après la démonstration du théorème 2 et du lemme 2 que si C s D, C est aussi subsumée par les clauses D', ayant même modèle que D et telles que D et D' satisfassent les conditions de ce lemme.

Ceci nous conduit à envisager :

2.4) Un principe dual de la subsomption.

Le principe de subsomption, utilisé au moins partiellement par de nombreuses méthodes de démonstration automatique, consiste à ne retenir, d'un ensemble de clauses, que celles qui ne sont pas subsumées par d'autres (le théorème 2 fournit une justification à ce principe).

Ce principe revient à ne conserver que les clauses, en un certain sens les plus générales : on préfère P(x)Q(y) à P(x)Q(x) à P(a)Q(a).

En revanche, d'après le lemme 2 deux clauses C et D, dont l'une, C est obtenue à partir de D par instanciation d'un ensemble D' $\subset$ D, de littéraux sur une partie D" $\subset$ D, admettent le même ensemble de modèles.

On peut donc, pour déterminer l'ensemble des modèles d'un ensemble de clauses, remplacer une clause C par une clause D, telle que C et D vérifient les conditions du lemme. Ce remplacement revient, sous certaines conditions, à ne conserver à l'intérieur d'une clause, que les littéraux les moins généraux : on préfère P(a) à P(a) P(x). Ce principe est donc dual du principe de subsomption, nous l'appelerons principe de simplification des clauses.

On peut énoncer le

THEOREME - Toute clause C est équivalente à une clause simplifiée, minimale pour l'inclusion, unique et donc minimum.

La partie existence est évidente, seule pose problème, l'unicité. Or cette dernière résulte de ce que si D est une solution minimale, tout autre solution minimale D' contient une instance de tout littéral de D. Si cette instance est stricte[1], D contient elle-même une instance stricte d'un de ces littéraux. On en déduit que D n'est pas minimale, en considérant l'ensemble des littéraux de D' affectés par l'instanciation telle que $\sigma D \subset D'$.

D'un point de vue algorithmique on peut donc, en vue de trouver la version la plus simplifiée d'une clause, utiliser n'importe quelle construction exhaustive, par exemple, par fermeture progressive d'un ensemble $D'' \subset D$, vers lequel peut s'instancier une partie de D, $D' \supset D''$.

Exemple - $P(a)P(b)P(x)Q(x,y,z)Q(a,t,t)Q(b,u,v)$

Si l'on essaie $x \mapsto a$

nécessairement $Q(x,y,z) \mapsto Q(a,t,t)$

par $y \mapsto t$

$z \mapsto t$

Reste $P(a)P(b)Q(a,t,t)Q(b,u,v)$ minimal.

Si l'on essaie $x \mapsto b$ il vient de même nécessairement

$y \mapsto u$

$z \mapsto v$

et il reste la même clause.

---

[1] *On appellera instance stricte, une instance qui ne soit pas une simple variante, c'est-à-dire obtenue par une substitution ne faisant intervenir que des symboles de variables.*

2.5) - Définition de l'opération résolution de deux clauses

2.5.1) - On définit tout d'abord, de la façon habituelle, un résolvant de deux clauses constantes C et D, comme une clause s'écrivant

$$(C-\{L\}) \cup (D-\{M\})$$

dans le cas où C et D contiennent les deux littéraux complémentaires L et M.

L'opération de résolution fait alors correspondre à deux clauses quelconques l'ensemble des résolvants de leurs instances constantes.

Exemple 1 - $C = P(x,y)Q(x)$

$D = \neg P(x,a)R(b)$

Pour chaque $i \in H$, $P(i,a)Q(i)$ et $\neg P(i,a)R(b)$ sont deux instances constantes de C et D, admettant $Q(i)R(b)$ pour résolvant.

La résolution de C et D fournit donc l'ensemble de clauses $\{Q(i)R(b)\}_{i \in H}$ équivalent au singleton $\{Q(x)R(b)\}$.

Exemple 2 - $C = P(x,y)Q(y)$

$D = \neg P(y,a) \neg P(b,z)$

L'ensemble des instances constantes de C et D peut être décrit comme

$$\{P(i,j)Q(j)\}_{(i,j) \in H^2} \cup \{\neg P(i,a) \neg P(b,j)\}_{(i,j) \in H^2}$$

L'ensemble des résolvants de C et D est donc

$$\{Q(a) \neg P(b,j)\}_{j \in H} \cup \{Q(j) \neg P(i,a)\}_{(i,j) \in H^2} \cup \{Q(a)\}$$

équivalent à

$$\{Q(a),\ Q(a) \neg P(b,y)\ ,\ Q(x) \neg P(y,a)\}\ .$$

Remarque - Deux clauses constantes peuvent admettre plusieurs résolvants :

$P(a)Q(b)Q(c)$ et $\neg P(a)\ \neg Q(b)R(d)$ peuvent être résolus en

$Q(b)\ \neg Q(b)Q(c)R(d)$ et $P(a)\ \neg P(a)Q(c)R(d)$; mais on montre facilement que si deux clauses constantes admettent plusieurs résolvants, chacun d'entre eux est, en fait, une tautologie.

Démontrons alors le

LEMME - Soit S un ensemble de clauses, contenant les clauses C et D, dont R(C,D) désigne l'ensemble des résolvants, alors

$$M \text{ est un modèle de } S \iff M \text{ est un modèle de } S \cup R(C,D)$$

La partie $(\Longleftarrow)$ est évidente puisque $S \subset (S \cup R(C,D))$

Etablissons la partie $(\Longrightarrow)$.

Pour cela, considérons un élément (constant) R de R(C,D) résolvant les instances C' et D' de C et D :

Supposons donc que $R = (C'-\{L\}) \cup (D'-\{M\})$ où L et M sont complémentaires. Puisque M est un modèle de S, l'un des deux littéraux L ou M, n'appartient pas à M ; supposons que ce soit L. L'un des littéraux de $C'-\{L\}$ appartient donc à M, ce qui prouve que M est aussi un modèle de R donc de $S \cup \{R\}$ et finalement de $S \cup R(C,D)$.

On peut alors énoncer le

2.5.2) - THEOREME DE RESOLUTION

Soit S un ensemble (dénombrable) de clauses, on peut écrire
S insatisfaisable $\iff$ $\square \in \overline{S}^{\mathcal{R}}$ où $\square$ désigne la clause vide et $\overline{S}^{\mathcal{R}}$ désigne la fermeture de S pour l'opération de résolution.

En effet ($\Leftarrow$) résulte du lemme précédent. Pour établir ($\Rightarrow$) nous allons montrer, en adaptant l'idée de [Robinson], que si $\square \notin \overline{S}^{\mathcal{R}}$, $\overline{S}^{\mathcal{R}}$ est satisfaisable ainsi, donc, que $S \subset \overline{S}^{\mathcal{R}}$.

Supposons en effet que $\square \notin \overline{S}^{\mathcal{R}}$ et soit $A = (A_i)_{i \in \mathbb{N}}$ l'ensemble des formules atomiques intervenant dans les instances constantes de S. Nous allons construire un modèle de $\overline{S}^{\mathcal{R}}$ réécrit, éventuellement, sous forme équivalente de clauses constantes.

Considérons pour cela la suite récurrente

$$M_0 = \varnothing$$
$$M_{i+1} = M_i \cup \{A_i\}$$

à moins qu'il existe une clause de $\overline{S}^{\mathcal{R}}$ dont tous les littéraux soient complémentaires de littéraux de $M_i \cup \{A_i\}$, auquel cas

$$M_{i+1} = M_i \cup \{\neg A_i\} .$$

Soit alors $M = \bigcup_{i \in \mathbb{N}} M_i$

M est un modèle de $\overline{S}^{\mathcal{R}}$; en effet, dans le cas contraire, il existerait un plus petit entier $j > 0$ tel qu'une certaine clause C ne possède que des littéraux complémentaires de ceux de M_j (car une clause constante est un ensemble <u>fini</u> de littéraux).

M_j doit donc s'écrire $M_{j-1} \cup \{\neg A_i\}$ et comme j est minimal C contient A_i. Il existe d'après la forme de M_j une autre clause, D, ne possédant que des littéraux complémentaires de $M_{j-1} \cup \{A_i\}$. Si D ne contenait pas $\neg A_i$, j-1 serait lui-même un entier tel qu'une clause (à savoir D) ne possède que des littéraux complémentaires de ceux de M_{j-1}. Comme j est minimal pour cette propriété D contient $\neg A_i$.

La clause $(C-\{A_i\}) \cup (D-\{\neg A_i\})$ ne possède que des littéraux complé-

mentaires de littéraux de M_{j-1}, à moins qu'elle ne soit vide. Or le premier cas est exclu puisque j est minimal, de même que le deuxième puisque $\square \notin \overline{S}^{\mathcal{R}}$.

2.5.3) - Equivalence des deux définitions de l'opération de résolution

La définition de l'opération de résolution donnée par Robinson fait intervenir la notion de clé triple et se prête assez mal à une manipulation abstraite. On rappelle que la définition de l'ensemble des résolvants, comme l'ensemble des résolvants binaires de facteurs des clauses parents (voir p. 54 , plus haut), lui est équivalente .

Appelons $R_R(C,D)$ l'ensemble des résolvants de deux clauses C et D selon la définition de Robinson, $R_F(C,D)$ selon la définition à l'aide de la notion de facteurs d'une clause, et $R_E(C,D)$ selon la définition donnée ici.

On a bien

$$\dot{R}_E(C,D) \sim \dot{R}_F(C,D) \quad (=\dot{R}_R(C,D)) \qquad (E)$$

puisque l'ensemble des instances constantes de $R_F(C,D)$ est justement $R_E(C,D)$.

Compte tenu de ce théorème de résolution et du théorème caractérisant la subsomption,

> l'ensemble des modèles d'une famille (dénombrable) S de clauses est caractérisé par
>
> $$\mathrm{Max}\ \overline{S}^{\mathcal{R}} \ (1)$$

(1) *A proprement parler, cette notation relève d'un abus de langage, puisque l'opérateur Max est relatif à l'ordre des classes et non au préordre sur les clauses.*

et en particulier

$$S \text{ est insatisfaisable} \Leftrightarrow \{ \square \} = \text{Max } \overline{S}^{\mathcal{R}} \quad .$$

Enfin, la relation (E) devient Max $R(C,D) = R_F(C,D)$. De ces deux dernières relations on déduit immédiatement le théorème d'Herbrand sous sa forme classique:

> S insatisfaisable $\Leftrightarrow$ il existe une partie finie de H, sur laquelle S est insatisfaisable.

Remarque sur l'élimination des tautologies.

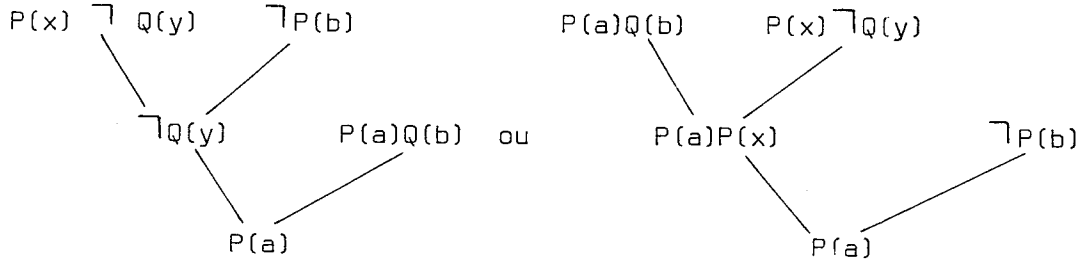
En remarquant que si $T \subset S$ est une tautologie, on peut toujours prolonger un modèle de S-T en un modèle de S, on peut

- dans le cas où l'on cherche effectivement à déterminer Max $\overline{S}^{\mathcal{R}}$, abandonner les tautologies (d'origine ou produites par résolution), à condition d'en conserver cependant une liste.
- dans le cas où l'on cherche seulement à montrer que l'on peut effectivement générer la clause vide, alors on peut tout simplement éliminer toutes les tautologies.

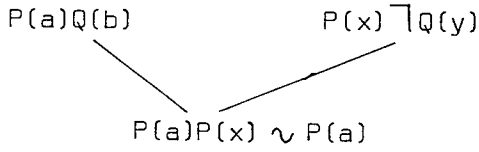
2.5.4) - on a intérêt, pour éviter de retarder l'apparition de certaines clauses, à prendre pour ensemble de résolvants, l'ensemble de leurs éventuels simplifiés :

Exemple - Dans $S = \{P(x) \neg Q(y) , P(a)Q(b) , \neg P(b)\}$

la clause P(a) ne peut s'écrire à l'aide du résolvant classique que comme formule de hauteur au moins 2 sur S :



tandis qu'à l'aide de résolvant "réduit" P(a) est une formule de hauteur 1 :



Remarque - La condition $\sigma C' \subset C$ dans la définition est indispensable. Considérons en effet P(a,x)P(y,b). Cette clause n'a pas le même ensemble de modèles, par exemple sur l'univers {a,b} que P(a,b).

En effet, l'ensemble des instances constantes est

P(a,a)P(a,b)
P(a,a)P(b,a)
P(a,b)
P(a,b)P(b,a)

dont les modèles minimaux sont :

{P(a,a)P(a,b) , P(a,b)P(b,a)}

alors que P(a,b) admet pour seul modèle minimal {P(a,b)}.

2.6) - Application de l'algorithme d'exclusion pour calculer Max $\overline{S}^{\mathcal{R}}$ (y compris dans le cas S dénombrable).

2.6.1) - Vérification des hypothèses

Hypothèse de compatibilité de l'ordre avec l'opération de résolution

Soit C et D, 2 clauses admettant un résolvant R, et une clause $C' \geq C$. Pour assurer l'hypothèse (1), il est suffisant de montrer que si C' et D sont résolubles, ils admettent un résolvant $R' \geq R$.

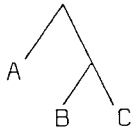
Or ceci est une conséquence presqu'immédiate du

LEMME de relèvement (p. 85, Chang et Lee, Symbolic Logic and Mechanical Theorem Proving):

Si C'_1 et C'_2 sont des instances de C_1 et C_2 respectivement et si C' est un résolvant de C'_1 et C'_2 alors il existe un résolvant C de C_1 et C_2, dont C' est une instance.

Hypothèse de distributivité.

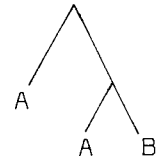
En regardant l'ensemble des résolvants comme l'ensemble des résolvants de leurs instances constantes, on vérifie immédiatement que l'opération de résolvant satisfait aux mêmes conditions que le consensus en algèbre de Boole (voir p. 40), permettant de transformer toute formule



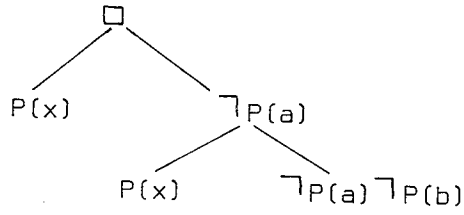
en une formule de hauteur au plus 2 et n'admettant pas de feuille étiquetée par A, de profondeur 1.

Hypothèse d'absorption.

Contrairement au cas booléen il arrive qu'une formule



puisse être définie, comme par exemple



formule qui ne peut pas s'écrire comme formule de hauteur 1 au plus, sur les feuilles $\{P(x)\ ,\ \neg P(a)\ \neg P(b)\}$.

Il est possible de tourner la difficulté en modifiant la définition : sans changer les propriétés précédentes, on peut remplacer l'ensemble initial des résolvants par la famille des résolvants itérés.

Pour cette version de la définition de l'opération de résolution on a

$$\text{Max}\ R(P(x)\ ,\ \neg P(a)\ \neg P(b)) = \{\ \square\ \}\ .$$

Hypothèse de finitude

Dans le cas de l'insatisfaisabilité, en reprenant la notion de pointage systématique introduite au II.2), il vient

$\text{Max}\ \overline{S}^{\mathcal{R}} = \{\ \square\ \}$ (hypothèse d'insatisfaisabilité)

$\Rightarrow$

Pour tout pointage systématique $\lim_{n\to\infty} (E_n, F_n) = (\ \square\ , \emptyset)$.

En effet, d'après le corollaire 2, pour un pointage systématique, tout élément maximal de $\overline{S}^{\mathcal{R}}$, finit par figurer dans un F_n soit

$$\exists n \quad (E'_n, F'_n) = (E_n, \square\ )$$

soit $\quad (E_{n+1}, F_{n+1}) = (\ \square\ , \emptyset)$.

Dans le cas où l'on ne sait rien de l'insatisfaisabilité, en général, on ne

sait pas vérifier la propriété $\overline{S}^{R}$ supérieurement fini : on ne sait pas si l'algorithme converge (se "termine");ceci correspond bien à la notion de procédure de semi-décision pour le calcul des prédicats du 1er ordre.

Remarques-

Dans le cas où l'ensemble de clauses initiales serait infini dénombrable, on peut toujours, au moins théoriquement, développer l'algorithme successivement sur chacune des parties finies de S : nous retrouvons une situation où un "démon de la preuve" serait apprécié pour fournir, dans le cas de l'insatisfaisabilité, en un temps raisonnable, une des parties finies insatisfaisables (dont on sait qu'elles existent).

Dans le cas où l'opération de résolution, modifiée en son ensemble d'itérées, conduirait à une infinité de résolvants, on peut toujours, au moins théoriquement, se ramener à un cas fini, en développant l'algorithme successivement sur des ensembles de clauses dont on borne (par une suite croissante) le degré d'imbrication.

3) Interprétation booléenne du théorème de Herbrand et un nouvel algorithme de démonstration automatique

3.0) Un théorème de compacité en algèbre de Boole

Une partie de ce qui va suivre utilise certaines notions ou résultats qui ne seront exposés qu'au premier chapitre de la deuxième partie. Pour des raisons d'unité de l'exposé touchant à la logique, nous avons préféré ne pas reporter cette partie.

Considérons $F = \prod_{i \in \mathbb{N}} (\mathbb{Z}/2)_i$ et soit $A \subset F$ une partie quelconque de F, pas forcément finie comme en algèbre de Boole habituelle.

On peut, de la même façon qu'en 2,I (p. 96) introduire les notions de structure affine, de monômes, monômes premiers, de consensus. On va démontrer le

THEOREME

Si une famille de monômes $(M_i)_{i \in I \subset \mathbb{N}}$ admet un monôme premier m, dont tous les points sont couverts au moins par un monôme de longueur finie[1], alors m appartient à la fermeture des M_i pour l'opération de consensus.

Ce théorème énonce donc une propriété de compacité en ce sens qu'il exprime que de tout recouvrement d'une partie (infinie) de $\prod_{i \in \mathbb{N}} (\mathbb{Z}/2)_i$, par des monômes (de longueur finie) on peut déduire un recouvrement fini.

---

[1] *On appellera longueur d'un monôme, le nombre de lettres (éventuellement infini) correspondant à son écriture (i.e intervenant dans le système d'équations le définissant).*

Remarquons ensuite que l'énoncé de ce théorème, dans le cas où I est une partie finie, se ramène à un résultat bien classique d'algèbre de Boole que, d'ailleurs, la convergence de l'algorithme d'exclusion, dans le cas booléen classique, se trouve établir.

Il est immédiat que ce théorème admet le

COROLLAIRE - Si la fermeture,pour l'opération de consensus,d'une famille (dénombrable) de monômes de longueur finie, n'est pas son enveloppe convexe (i.e. contient plus d'1 élément), c'est qu'il existe des points de cette enveloppe qui ne sont pas couverts par la famille.

On établit la contra-posée du théorème, c'est-à-dire qu'en supposant que m n'appartienne pas à la fermeture, nous allons construire un point de m qui n'est couvert par aucun des monômes de la famille.

On suppose que $\mathbb{N}^*$ est la famille d'indices indexant les lettres $\{a_i\}_{i\in\mathbb{N}^*}$ [1] correspondant aux différentes directions de m ; m est donc représenté par le produit des lettres qui ne sont pas dans $\{a_i\}_{i\in\mathbb{N}^*}$.

Nous allons construire un point (i.e un monôme de dimension zéro, c'est-à-dire contenant toutes les lettres sous une seule de leurs deux formes) n'appartenant pas à la fermeture de la famille, a fortiori à la famille.

Partant du monôme

$m_0 = m$ on construit par récurrence

$m_{i+1} = m_i \cdot a_{i+1}$ $(i \geq 0)$ à moins qu'il n'existe

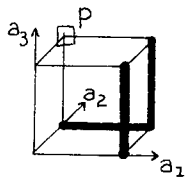
---

[1] *Le cas où cette famille est finie correspond évidemment au cas où il ne s'agit, en fait, que d'algèbre booléenne finie.*

un monôme de la fermeture qui contienne $m_i \cdot a_{i+1}$ auquel cas

$$m_{i+1} = m_i \cdot a'_{i+1}$$

$p = \prod_{i \in \mathbb{N}} m_i$ représente un point de m .

Exemple 

$m = 1$ $\quad M_1 = a_1 a'_2 \quad M_2 = a_1 a_2 \quad M_3 = a_2 a'_3$

$m_1 = a'_1$

$m_2 = a'_1 a_2$

$m_3 = a'_1 a_2 a_3$.

Montrons que p n'appartient à aucun monôme de la fermeture.

Dans le cas contraire il existerait un monôme de la fermeture (dont chaque monôme présente un nombre fini de lettres), contenant m_{i+1} et pas m_i ; soit alors, i le plus petit entier tel que m_i n'est pas inclus dans un monôme de la fermeture et que m_{i+1} le soit (i.e soit inclus dans μ) ; par hypothèse $i \geqslant 1$. m_{i+1} s'écrit $m_i \cdot a'_{i+1}$ et μ contient la lettre a'_{i+1} (car i est minimal). Si $m_{i+1} = m_i \cdot a'_{i+1}$ il existe un monôme ν contenant $m_i \cdot a_{i+1}$ et ν contient la lettre a_{i+1} sinon i ne serait pas minimal (i-1 conviendrait relativement à ν).

Le consensus de μ et ν ne devant alors contenir que des lettres de m_i, contrairement au fait que i est minimal, c'est que i = 0 contrairement à l'hypothèse ; ce qui établit donc la propriété.

Remarque 1 -

Les éléments de la fermeture étant de longueur finie, il se trouve que l'on a établi qu'il n'est donc pas possible qu'une famille quelconque de monômes de longueur finie admette un monôme premier de longueur infinie ; résultat loin d'être, a priori, évident.

Remarque 2 -

On notera le parallèle de cette démonstration avec celle de la p.68 .

J'ai vainement recherché une démonstration "géométrique" du théorème ou de son corollaire, s'appuyant sur la caractérisation (donnée p. 98) de l'opération de consensus. Si cette démonstration pouvait être trouvée, on obtiendrait finalement une démonstration "purement géométrique" de ce qu'on montrera être l'"âme" du théorème de Herbrand.

Remarque 3 -

Il est évident que c'est bien la propriété de longueur finie qui est à l'origine de la propriété exprimée par le théorème ou son corollaire.

En effet, considérons la famille des

$$m_o = \prod_{i \in \mathbb{N}^*} a_i$$

et pour $i \geqslant 1$ $\quad m_i = a'_i$.

Tous les points sont couverts par m_o ou un des m_i. Pourtant la fermeture, qui ne contient en plus des $\{m_i\}_{i \in \mathbb{N}}$ que des monômes présentant un nombre infini de lettres, ne contient pas le monôme 1.

3.1) Le théorème de Herbrand

Etant donné un ensemble (dénombrable) de clauses S et son univers de Herbrand, considérons l'ensemble dénombrable

$$A = \{A_i\} i \in P \subset \mathbb{N}$$

des atomes intervenant dans l'ensemble S_c des instances constantes (sur H) des clauses de S.

A une clause constante, on fait correspondre un monôme booléen de longueur finie dans

$$\prod_{i \in A} (\mathbb{Z}/2)_i$$

suivant $C = \{L_i\}_{i \in I \text{ (fini)}} \longmapsto \prod_{i \in I} \tilde{A}_i$ où $\tilde{A}_i = A_i$ si $L_i = A_i$
$\tilde{A}_i = A'_i$ si $L_i = \neg A_i$.

A une clause quelconque faisons correspondre l'ensemble des monômes représentant ses instances constantes. Rappelons qu'un modèle de S est un modèle de S_c c'est-à-dire un ensemble de littéraux constants sans paire complémentaire, contenant un littéral de chaque clause de S_c. Il vient alors immédiatement, si l'on fait correspondre à S l'union des monômes représentant ses clauses :

Propriété 1 - Un modèle d'un ensemble de clauses S est représenté par un multiple d'un monôme premier de la fonction duale de celle représentant S, et réciproquement.

En effet, cela découle

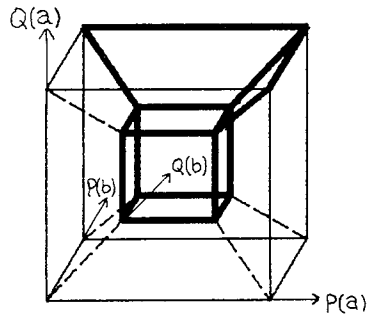
- de la définition d'un modèle, qu'on vient de rappeler ;
- de la propriété du produit de deux monômes premiers de fonctions booléennes, d'être multiple d'un monôme premier du produit des deux fonctions.

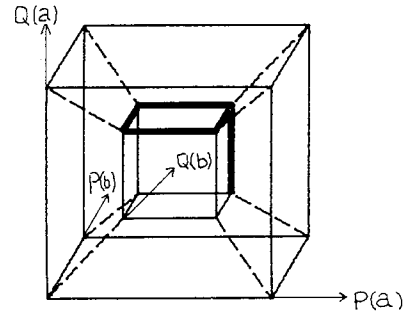
Exemple - $S = \{P(x)\ Q(a),\ Q(b)\}$, $H = \{a,b\}$
$A = \{P(a), P(b),\ Q(a),\ Q(b)\}$
$S_c = \{P(a)\ Q(a),\ P(b)\ Q(a),\ Q(b)\}$.

Les modèles de S sont obtenus en développant

$$(P_a + Q_a)(P_b + Q_a)Q_b = P_a P_b Q_b + Q_a Q_b$$

S est représenté par: et ses modèles minimaux par :





.

Il vient alors

Propriété 2 - Un ensemble (dénombrable) de clauses S est insatisfaisable (n'admet pas de modèles) $\Longleftrightarrow$

La fonction qui le représente est la fonction 1.

La duale de cette fonction est alors, en effet, la fonction nulle.

D'après le corollaire p.76, la fermeture des monômes représentant S, pour l'opération de consensus, contient la fonction 1 (qui représente la clause vide) et l'on a donc

S insatisfaisable

$\Longleftrightarrow$ Il existe une génération finie de la fonction 1 à partir d'un ensemble fini de monômes, représentant des clauses constantes de S.

$\Longleftrightarrow$ Il existe une partie finie de H sur laquelle S est insatisfaisable (les termes constants intervenant dans l'ensemble, ci-dessus, de clauses constantes).

Le dernier énoncé est l'une des formes du théorème de Herbrand.

Remarque - La méthode, ci-dessus, fournit donc le théorème de Herbrand, dans le cas habituel où S est fini, ce qui correspond à une formule initiale du CP_1, elle-même finie, mais aussi dans le cas où la formule initiale mise sous forme prénexe normale conjonctive, purement universelle par "skolémisation" serait infinie, à la seule condition qu'aucune de ses sous-formules sans symbole $\wedge$ ne soit de longueur infinie (ce qui implique, en particulier, qu'une telle sous-formule ne contient qu'un nombre fini de $\vee$ et ne contient pas non plus de termes de longueur infinie).

Cette condition sur les symboles $\vee$ est d'ailleurs nécessaire, comme le montre l'exemple suivant

$$\phi = \forall x \neg P(x) \wedge \bigvee_{i \in \mathbb{N}} P(\underbrace{f(f(f\ldots f}_{i \text{ fois}}(a)\ldots)$$

Son univers de Herbrand est $H = \{a, f(a), ffa\ldots, ffff\ldots fa, \ldots\}$.
ϕ est évidemment insatisfaisable, bien que sur toute partie finie $P \subset H$, et avec des notations évidentes, $\phi(P)$ ne soit pas une antithèse.

Remarque 1 sur le théorème d'interpolation (de Craig) -

On a donné p.75 l'énoncé d'un théorème d'algèbre de Boole et non pas seulement son corollaire qui était suffisant pour démontrer le théorème de Herbrand. En effet, le théorème lui-même, traduit au moins une partie du théorème de Craig :

Pour une certaine classe de formule du CP_1, la relation $A \supset B$ se traduit par le fait que l'ensemble représentatif A' de A contient B', celui de B.

Une formule d'interpolation entre A et B peut alors être obtenue (au problème des quantificateurs près) par une formule correspondant à l'ensemble des monômes premiers de A' d'intersection non-vide avec ceux de

B', monômes qui ne contiennent que des symboles de prédicats communs à A et B.

Remarque 2 - Partant d'une formule du CP_1 valide (en symbole $\models A$), la formule $\neg A$ est insatisfaisable, de même que $\widehat{\neg A}$ la formule purement universelle associée.

Si $\widehat{\neg A}$ s'écrit sous forme clausale

$$\widehat{\neg A} = C_1 \wedge C_2 \wedge \cdots \wedge C_n$$

alors, en remarquant que la résolution correspond à un modus ponens, il vient

$$C_1, \ldots, C_n \vdash F \qquad \text{(F désigne la constante "Faux")}$$

et par le théorème de déduction

$$C_1, \ldots, C_{n-1} \vdash \neg C_n \vee F$$

soit $\vdash \neg C_1 \vee \neg C_2, \ldots \vee \neg C_n \vee F$

soit $\vdash \neg(\widehat{\neg A}) \vee F$

soit $\vdash \neg(\widehat{\neg A})$;

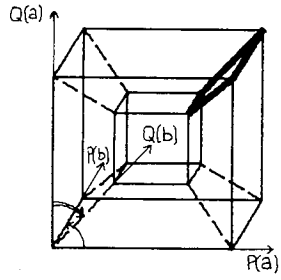
c'est-à-dire, finalement $\models A$ implique $\vdash \check{A}$ où $\check{A}$ désigne la formule du CP_1 purement existentielle associée à A.

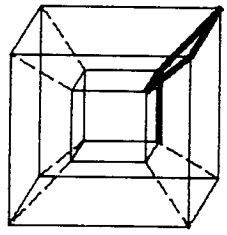
3.2) Retour sur la subsomption

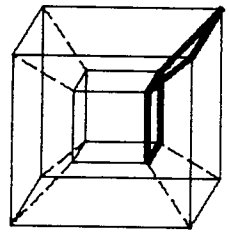
Dans le formalisme actuel, C est subsumée par D, s'écrit tout simplement :

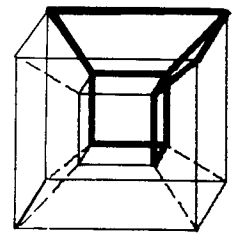
l'ensemble représentatif de C est inclus dans celui qui représente D.

Exemple - en prenant H = {a,b}, voici la représentation de quatre clauses croissantes :







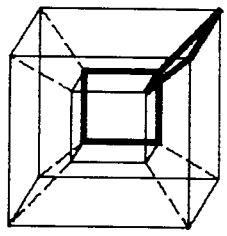


P(a)Q(a)

P(a)Q( ) } P(a)P(x)Q(x)
P(a)P(b)Q(b) }

P(a)Q(a) } P(a)Q(x)
P(a)Q(b) }

P(a)Q(a) }
P(b)Q(a) }
P(a)Q(b) } P(x)Q(y)
P(b)Q(b) }

et  qui n'est pas comparable aux deux précédentes .

P(a)Q(a) }
P(b)Q(b) } P(x)Q(x)

On obtient donc immédiatement le résultat déjà indiqué p.62 :

C subsume D }
et D subsume C } $\Longleftrightarrow$ C et D ont même ensemble de modèles.

3.3) Un nouvel algorithme de démonstration automatique

Etant donné un ensemble de clauses insatisfaisable, considérons une des parties finies, P de H, dont le théorème de Herbrand affirme l'existence et telle que

S(P) soit insatisfaisable.

S(P) couvre donc tous les points de l'hypercube de dimension finie, dont les directions sont indexées par les atomes (en nombre fini) intervenant dans S(P).

Sans enlever la propriété de couvrir l'unité (i.e tous les points de l'hypercube) on peut remplacer dans S(P) une clause constante non vide C, par l'ensemble des consensus selon une direction arbitraire représentée par une lettre de C qu'elle admet avec les autres éléments de S(P), (opération E).

En effet, ceci n'est autre qu'une conséquence du fait que le consensus de deux monômes est l'union des arêtes réalisant leur distance 1 : si donc un point P' n'est couvert que par m, soit Q un point à distance 1 de P suivant la direction choisie et qui ne soit pas dans m (il en existe, à moins que m ne couvre l'unité lui-même). Q appartient donc à un autre monôme m' ≠ m et l'arête PQ (a fortiori le point P), appartient au consensus de m et m'[1].

La répétition de l'opération E, en ne conservant à chaque étape que des éléments incomparables 2 à 2 (pour l'inclusion) finit par produire en un nombre fini d'étapes, la clause vide, puisque sinon, il devrait exister une infinité de monômes distincts possédant un nombre fini de lettres[2].

Grâce au lemme de relèvement assurant que si deux clauses,C et D, sont des instances de C' et D' et admettent un résolvant E, alors il existe un résolvant de C' et D', dont E est une instance, nous déduisons un algorithme, différent de celui de la page 73 , et surtout plus facile à mettre en oeuvre.

---

[1] *Cette propriété est déjà indiquée dans [Tison] avec une démonstration plus longue.*

[2] *Ceci constitue, dans le cas particulier de l'insatisfaisabilité, une démonstration directe de la convergence de l'algorithme d'exclusion.*

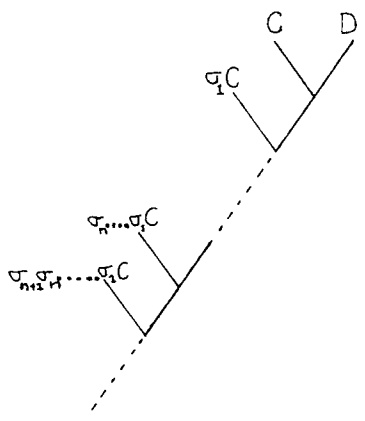
Si S est un ensemble de clauses insatisfaisable, l'ensemble S' où l'on a remplacé une clause C par l'ensemble de ses résolvants avec les autres clauses de S sur un même littéral de C, est encore insatisfaisable, du moins s'il n'existe pas de possibilité de résoudre C avec les clauses de S' ou avec C elle-même suivant ce même littéral.

En effet, chaque point d'un monôme représentant une clause constante C est encore couvert après le remplacement (l'exclusion) de la clause qui a généré C, du moins si les points à distance 1 sont couverts par certaines clauses constantes ne provenant pas de C.

Dans cette dernière situation, deux cas peuvent se produire suivant que la suite des itérées de la résolution de C avec une clause est infinie ou non, que l'on peut distinguer grâce au

LEMME - Si une clause C admet une infinité de résolvants itérés avec une autre clause D, alors C est auto résolvable.

Démonstration - Les littéraux de D étant en nombre fini, l'existence d'une suite infinie implique que certaines résolutions se fassent sur un littéral $L \in C$ et $\neg L \in C$.



Il s'ensuit l'algorithme suivant, semi-décidable, pour le problème de l'insatisfaisibilité d'un ensemble de clauses:

Etant donné un ensemble de clauses S, insatisfaisable, la répétition de l'opération d'exclusion suivante, à condition qu'à terme elle porte successivement sur chacune des clauses initiales (de S) ou nouvellement produites, engendre la clause vide :

dans l'ensemble S' de clauses, obtenues après un certain nombre d'étapes, considérant une clause C

- si elle est autorésolvable, on remplace S' par son union avec l'ensemble des résolvants, (suivant un littéral arbitraire de C), de C avec les autres clauses de S';
- sinon on remplace dans S', C par l'ensemble (fini) de ses résolvants itérés suivant l'un de ses littéraux avec les autres clauses de S'.

Enfin, il est toujours possible de remplacer tout ensemble de clauses par l'ensemble de ses éléments maximaux, selon le préordre associé à la subsomption et de supprimer les tautologies.

Remarque - Cet algorithme inclut

- le principe de pureté selon lequel on peut toujours supprimer une clause qui contiendrait un littéral pur L, c'est-à-dire telle qu'aucune résolution ne puisse se faire sur lui.
- le principe d'instanciation permettant de remplacer une clause C, qui contiendrait un littéral unifiable avec un nombre fini de littéraux complémentaires, suivant les unifications $\sigma_1,\ldots,\sigma_r$, par $\{\sigma_1 C,\ldots,\sigma_p C\}$.

3.4) Conjugaison de la méthode d'exclusion avec celle du support

Rappelons que la méthode du support consiste à utiliser un ensemble $T \subset S$ tel que S-T soit un ensemble de clauses satisfaisables et à ne considérer de résolvants qu'entre des clauses dont l'une, au moins, "a le support" et où la propriété "avoir le support" signifie pour une clause C :

$C \in S$,

où C est un résolvant de 2 clauses dont l'une, au moins, "a le support".

Cette méthode est bien connue. Donnons-en cependant, une justification très facile. Pour cela, il suffit de montrer qu'un point quelconque de l'hypercube fini correspondant au théorème de Herbrand, finit, au cours du calcul de la fermeture, par appartenir à un monôme "ayant le support":

Validation de la méthode du support -

En effet, soit P un point qui n'aurait pas cette propriété, il est à distance minimale d, d'un point "ayant le support". La distance d ne peut être que 1, sinon d ne serait pas minimale ; ceci implique que P appartient au consensus de deux monômes dont l'un "a le support" contrairement à l'hypothèse faite.

Q.E.D.

Considérons alors le processus algorithmique suivant, consistant à conjuguer la méthode du support et la méthode de l'exclusion selon :
à une étape donnée, seule est susceptible d'être considérée pour une opération d'exclusion, une clause ayant le support.

Pour montrer que ce processus engendre la clause vide, il suffit de remarquer que toute clause initiale de S-T, finit par disparaître (par subsomption) ; or ce dernier point est immédiat d'après la validation de la méthode du support.

Remarque - Il n'est pas possible d'envisager la combinaison brutale des deux méthodes, qui reviendrait à éliminer "d'entrée", purement et simplement, les clauses à distance >1 du support.

Exemple -

$S = \{\neg P\ \neg Q\ ,\ \neg PQ\ ,\ P\ \neg Q\ ,\ PQ\}$ avec $T = \{PQ\}$

On serait conduit à remplacer S insatisfaisable, par

$\{\neg PQ\ ,\ P\ \neg Q\ ,\ PQ\}$ qui lui, est satisfaisable.

Exemple d'application :

$S = \{C_1, C_3, C_4, C_5\}$ (voir page 51)

$T = \{C_5\}$

Il vient successivement les ensembles de clauses :

S

$C_1C_3C_4$ $\underline{C_5 * C_1}$ $= \{\neg Pxy\ kx'\ \neg P\ yx'v\ \neg P\ xv\ kx'\} = \underline{\{C_6\}}$

$C_1C_3C_4$ $\underline{C_6 * C_1}$ $= \{\ \ldots.\ \}$ $\underline{C_6 * C_3} = \{\ \ldots, \underline{C_9} = \neg Pv\ x'v, \ldots\ \}$ $\underline{C_6 * C_4} = \{\ldots\}$

$C_1C_3C_4$ .... $\underline{C_9 * C_1}$ $\underline{C_9 * C_3}$ $\underline{C_9 * C_4} = \{\ \square\ \}$

$\underline{\square}$

(On a souligné les clauses (ou ensemble de)"ayant le support").

PLAN DETAILLE DE LA

DEUXIEME PARTIE

I - QUELQUES NOTIONS GEOMETRIQUES EN ALGEBRE DE BOOLE

1) Structure affine métrique sur $\coprod_{i \in \mathbb{N}} (\mathbb{Z}/2)_i$.
2) Structure affine métrique et monômes premiers.
3) L'inégalité triangulaire dans $(\mathbb{Z}/2)^n$ et ses conséquences.

II - UNE QUESTION D'ALGEBRE DE BOOLE SUR LES FONCTIONS IRREDUCTIBLES ET LE COUPLAGE MIN MAX DU N-CUBE

1) Problème.
2) Quelques résultats sur le couplage du n-cube.
3) Un encadrement de I_n et ses conséquences.
4) Sur l'existence d'un 23-couplage du 6-cube.
5) Justification de deux conjectures sur M_n et I_n .

III - PRESENTATION ET RESOLUTION PARTIELLE D'UNE CONJECTURE SUR LE TYPE DES FONCTIONS BOOLEENES

1) Présentation de la conjecture.
2) Fonctions d'au plus quatre variables.
3) Fonction d'au plus quatre points.

IV - PRESENTATION GEOMETRIQUE DE DIFFERENTS ALGORITHMES D'ALGEBRE DE BOOLE

1) L'algorithme d'exclusion en algèbre de Boole.
2) Conséquences en ce qui concerne deux algorithmes classiques.
3) Un nouvel algorithme de recherche de la base complète.

CHAPITRE I

QUELQUES NOTIONS GEOMETRIQUES EN ALGEBRE DE BOOLE

1) Structure affine métrique sur $\coprod_{i \in \mathbb{N}} (\mathbb{Z}/2)_i$

1.1) Une norme.

1.2) La linéarité des isométries.

1.3) Forme des matrices orthogonales.

2) Structure affine métrique et monômes premiers

2.1) Représentation des fonctions booléennes.

2.2) Représentation des monômes.

2.3) Le problème de la recharche de la base complète.

2.3.1) définition du consensus général

2.3.2) relations du consensus général avec le consensus ordinaire

2.4) La méthode de la double duale.

3) L'inégalité triangulaire dans $(\mathbb{Z}/2)^n$; ses conséquences

3.1) Cas du bipoint.

3.2) Cas du triangle.

3.3) Cas du tétraèdre.

I - QUELQUES NOTIONS GEOMETRIQUES EN ALGEBRE DE BOOLE

1) - Structure affine métrique sur $\coprod_{i \in \mathbb{N}} (\mathbb{Z}/2)_i$

1.1) - Une norme

On considère l'espace vectoriel sur le corps $\mathbb{Z}/2$, somme d'une famille indéxée par $\mathbb{N}$ d'exemplaires de $\mathbb{Z}/2$; ainsi que sa structure affine naturelle :

à $(x,y) \in E \times E$ correspond l'opérateur $\vec{z} = z = y-x$

à $(x,\vec{y})$ $E \times E$ correspond alors $x+\vec{y} = x+y$.

Remargue -

. $\mathbb{Z}/2$ est un corps valué par $\begin{cases} |0| = 0 \in \mathbb{R}^+ \\ |1| = 1 \in \mathbb{R}^+ \end{cases}$.

En effet - $x = 0 \Rightarrow |x| = 0$ et $|x| = 0 \Rightarrow x = 0$;

$-|x.y| = |x|.|y|$;

il suffit de vérifier, si $x = 0$, $0 = 0.|y|$

sinon $x = 1$, $|y| = |y|$;

$- |x+y| \leqslant |x| + |y|$

il suffit de vérifier

si $x+y = 0$ $\qquad 0 \leqslant |x| + |y|$

sinon $x+y = 1$ et $|x| + |y| \geqslant 1$ puisque l'un des deux x ou y n'est pas nul.

. Il s'agit d'ailleurs de la seule valuation de $\mathbb{Z}/2$, car du deuxième axiome pour $x = y = 1$ on tire $|1| = |1|.|1|$ qui n'admet dans $\mathbb{R}^+$

que les solutions $|1| = 0$ ou $|1| = 1$, la première solution conduisant à $1 = 0$.

On peut énoncer le

THEOREME - L'application $\coprod_{i\in\mathbb{N}} (\mathbb{Z}/2)_i \to \mathbb{R}^+ ; x \longmapsto \|x\| = \Sigma\, |x_i|$ [1] où les x_i sont les composantes de x dans la base canonique est une norme.

En effet - $x = 0 \iff \forall i\ x_i = 0 \iff \|x\| = 0$

- $\|\lambda x\| = \Sigma|\lambda x_i| = \Sigma\, |\lambda|\,|x_i| = |\lambda|\,\Sigma\,|x_i| = \lambda\,\|x\|$

- $\|x+y\| = \Sigma\, |x_i+y_i| \leqslant \Sigma\, |x_i| + |y_i| = \|x\| + \|y\|$

Remarque - Comme dans le cas des espaces vectoriels réels $\mathbb{R}^n$, on pourrait montrer qu'en dimension finie toutes les normes sont équivalentes. (En effet, la sphère unité, finie, est certainement compacte). En dimension infinie elles ne le sont pas :

la suite $u_n = \sum_{i=1}^{n} e_i$ vérifie $\lim_{n\to\infty} \|u_n\| = \infty$ alors $\lim_{n\to\infty} N(u_n) = 1$

où $N(x)$ désigne la norme du sup.

Bien que cette norme ne se déduise pas d'un produit scalaire, on va montrer que, comme dans le cas $\mathbb{R}^n$ espace vectoriel sur $\mathbb{R}$, toute isométrie de E est une application linéaire.

Montrons d'abord que la norme ne se déduit pas d'un produit scalaire. Pour cela on va utiliser le lemme connu :

LEMME - Si une norme d'un espace vectoriel V sur le corps valué $\mathbb{K}$, se déduit d'un produit scalaire, l'ensemble

$$\{M\ ,\ M \in V \quad \|MA\| = \|MB\|\}$$

---

[1] *Le symbole Σ représente une sommation finie puisqu'un élément de la somme des espaces $\mathbb{Z}/2$, ne comporte qu'un nombre fini de composantes non nulles.*

où A et B sont deux points distincts de V est de codimension 1.

Démonstration - en introduisant l'origine O il vient

$$\|MO + OA\|^2 = \|MO + OB\|^2$$

soit $\|MO\|^2 + 2\ MO.OA + \|OA\|^2 = \|MO\|^2 + 2\ MO.OB + \|OB\|^2$

soit $OM.AB = \dfrac{\|OB\|^2 - \|OA\|^2}{2}$ Q.E.D. .

Or ici, par exemple, pour A = O et B = e_1 (1er vecteur de la base canonique)

$\{M\ ,\ \|MA\| = \|MB\|\} = \varnothing$ n'est certainement pas de codimension 1.

1.2) - La linéarité des isométries

Considérons maintenant la forme: ExE $\to$ $\mathbb{R}$

$$(x,y) \mapsto \langle x,y\rangle = \Sigma\ |x_i|.|y_i| .$$

C'est une forme bilinéaire symétrique pour laquelle le système constitué de la base canonique vérifie $\langle e_i,e_j\rangle = \delta_{ij}$ ce qui permet d'écrire si $x = \Sigma\ x_i e_i$

$$|x_i| = \langle x,e_i\rangle \text{ puisque } \langle \Sigma\ x_j e_j, e_i\rangle = \Sigma\ x_j\ \langle e_j,e_i\rangle = |x_i|$$

Soit alors une isométrie u. Le système des $u(e_i)$ vérifie encore

$$\langle u(e_i)\ ,\ u(e_j)\rangle = \delta_{ij}\ ;$$

pour l'établir il suffit de remarquer qu'une isométrie est injective et que l'image par u, d'un vecteur de la base canonique, ne peut être qu'un vecteur de cette base (ce sont les seuls vecteurs de norme 1). De $u(e_i) = u(e_j) \Leftrightarrow e_i = e_j$ on déduit alors $\langle u(e_i),\ u(e_j)\rangle = \delta_{ij}$.

On peut donc écrire $u(x) = \Sigma\, y_i\, u(e_i)$ où $|y_i| = \langle u(x), u(e_i)\rangle$. Reste donc à démontrer, pour établir le théorème annoncé, que

$$\langle u(x), u(e_i)\rangle = \langle x, e_i\rangle \quad \text{car l'on aura alors}$$

$u(x) = \Sigma\, x_i\, u(e_i)$ ce qui établit la $\mathbb{Z}/2$ linéarité.

Démonstration de $\langle u(x), u(e_i)\rangle = \langle x, e_i\rangle$.

Supposons d'abord $\langle x, e_i\rangle = 0$, c'est donc que x est dans l'espace engendré par les $\{e_j\}_{j\in\mathbb{N}} - \{e_i\}$.

Or, si l'on avait $\langle u(x), u(e_i)\rangle \neq 0$, $u(x) + u(e_i)$ serait dans l'espace engendré par $\{u(e_j)\}_{j\in\mathbb{N}} - \{u(e_i)\}$, ce qui est impossible puisque pour $x = 0$ on aurait $\|u(x)\| \geqslant 1$.

De la même façon, on démontre par l'absurde que si $\langle x, e_i\rangle = 1$ alors $\langle u(x), u(e_i)\rangle = 1$.

On peut donc énoncer le

THEOREME - Toute isométrie de $\coprod_{i\in\mathbb{N}} (\mathbb{Z}/2)_i$ pour la norme $\|x\| = \Sigma\, |x_i|$ est $\mathbb{Z}/2$-linéaire.

COROLLAIRE - Les isométries de $\coprod_{i\in\mathbb{N}} (\mathbb{Z}/2)_i$ sont représentées par les matrices de permutations des axes (un 1 et un seul 1 dans chaque ligne et chaque colonne, les autres coefficients étant nuls). Ceci est, en effet, une conséquence immédiate de la remarque ayant servi à établir $\langle u(e_i), u(e_j)\rangle = \delta_{ij}$.

1.3) - Un problème

On peut cependant se poser la question de savoir (en dimension finie)

quelles sont les matrices orthogonales au sens

$$AA^t = I \iff \langle e_i \cdot e_j \rangle_{\mathbb{Z}/2} = \delta_{ij} \quad \in \mathbb{Z}/2 \ ?$$

Si V est un vecteur ne comportant que des 1, il vient

$$(V^tV + I)^t = V^tV + I$$

d'où pour la matrice $A = V^tV + 1$

$$A^tA = (V^tV+I)(V^tV+I) = V^tVV^tV + \underbrace{V^tV+V^tV}_{J} + I$$

et si la dimension de V est paire, VV^t est le scalaire nul d'où

$$A^tA = 0 \times V^tV + I = I$$

On peut donc générer par ce procédé une famille de solutions, à l'aide de vecteurs de dimension paire et de la matrice unité.

Par exemple pour $V_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, $V_2 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$ on peut obtenir

$$\begin{bmatrix} 0 & 1 & & & & \\ 1 & 0 & & 0 & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & 0 & 1 & 1 & 1 \\ & 0 & & & 1 & 0 & 1 & 1 \\ & & & & 1 & 1 & 0 & 1 \\ & & & & 1 & 1 & 1 & 0 \end{bmatrix} .$$

Toutes les solutions sont-elles de ce type ?

2) - Structure affine métrique et monômes premiers

On peut considérer une fonction booléenne comme la donnée d'une partie finie de $E = \coprod_{i \in \mathbb{N}} (\mathbb{Z}/2)_i$. Il existe alors, étant donnée une fonction booléenne, un plus petit produit $\prod_{i=1}^{n} (\mathbb{Z}/2)_i \approx (\mathbb{Z}/2)^n$ contenant la partie finie représentative de la fonction et la quantité n est son nombre de variables.

2.1) - Représentation des fonctions booléennes

Si F est une fonction, on peut la "décomposer" au sens de l'union, en une famille finie de variétés affines de E. Or, parmi ces variétés, il en existe de remarquables ; ce sont les variétés d'étendue[1] égale à 1, qu'on appellera monômes.

Propriété - Toute fonction booléenne admet une décomposition (appelée base) en un nombre fini de monômes.

Immédiat : un point est un monôme et une fonction F peut toujours s'écrire $F = \bigcup_{x \in F} \{x\}$.

De façon habituelle, on définit aussi une base première comme une décomposition en monômes premiers, c'est-à-dire maximaux pour l'inclusion dans F ; une base irrédondante comme une base $F = \bigcup_{i \in I} M_i$ satisfaisant

$$\forall i \quad F \neq \bigcup_{j \in I-\{i\}} M_j$$

la base complète comme la base formée de tous les monômes premiers.

---

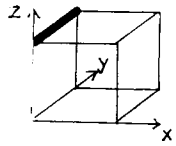
[1] *On peut, par exemple, définir l'étendue d'une variété comme le produit Min* $\prod \|x_i\|$ *où les* x_i *forment une base de la variété : en ce sens, les points, correspondant à un produit vide, seront considérés eux aussi comme étant d'étendue* 1. *L'étendue de*  *est alors Min* {1x2, 1x3} = 2 ; *l'étendue de la clé de parité à 3 variables est Min* {2x2} = 4.

2.2) - Représentation des monômes

On établit facilement qu'un monôme peut s'écrire comme intersection de monômes de dimensions supérieures et, en particulier, comme intersection de monômes de codimension 1.

On peut donc représenter un monôme comme un système d'équation $\{x_i = \lambda_i\}_{i \in I}$ où $\lambda \in \mathbb{Z}/_2$ que l'on codera par le produit des noms des variables indéxées par I, sous forme directe si $\lambda_i = 1$ et sous forme accentuée si $\lambda_i = 0$.

Exemple - Pour les variables $(x_1, x_2, x_3) = (x, y, z)$ le monôme représenté sur la figure correspond aux équations $x = 0$ et $z = 1$ que l'on représente par x'z.

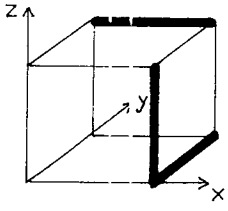


2.3) - Un problème important en algèbre de Boole, la recherche de la base complète

2.3.1) - Définition d'une opération de consensus général d'un ensemble des monômes.

Si M est un ensemble de monômes, le consensus général de M est défini comme l'ensemble des monômes premiers de la fonction représentée par M diminué de M lui-même.

Exemple -



Consensus Gen$(\{xy', yz\}) = \{xy', yz, xz\} - \{xy', yz\} = \{xz\}$
Consensus Gen$(\{xy', yz, xz'\}) = \{x\}$

On a, évidemment

M + Consensus Gen M ⊃ Base complète de M.

Aspect géométrique de cette définition, dans le cas de deux monômes.

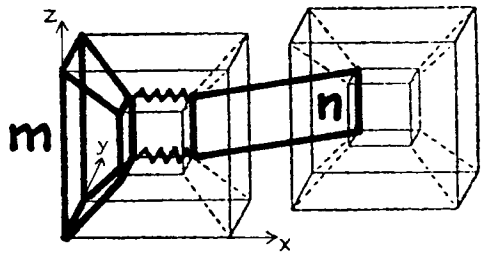
On va montrer le

THEOREME - Si m et n sont deux monômes, pour qu'ils admettent un consensus général non vide, il est nécessaire et suffisant qu'ils soient à distance[1] 1 ; leur consensus est alors constitué d'un seul monôme, l'union des arêtes réalisant la distance 1.

Exemple -

$m = x'u'$

$n = xyt$



en ∿∿ les deux arêtes, constituant un monôme de dimension 2.

Démonstration -

Une condition nécessaire pour que $CG(\{m,n\})$ ne soit pas vide est que $m \cup n$ contienne des variétés d'étendue 1, en particulier des arêtes, qui ne soient pas incluses dans m ou n. La distance de m à n est donc $\leqslant 1$.

Si cette distance est nulle, considérons l'intersection alors non vide de m et n qui, elle aussi, est d'étendue 1. Si $a \in m$ et $b \in n$ sont deux points, on peut toujours réaliser leur distance par un chemin passant par l'intersection de m et n. Deux tels points, s'ils vérifient $a \notin n$ et $b \notin n$ sont donc nécessairement à distance au moins 2 et $m \cup n$ ne peut admettre d'autres monômes que des monômes inclus dans m ou n, c'est-à-dire qu'alors $CG(\{m,n\}) = \emptyset$.

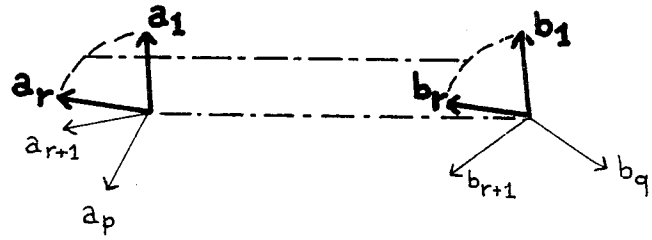
---

[1] *La distance de deux variétés (monômes) est le minimum de la distance de deux points dont l'un appartient à la première variété (monôme) et l'autre à la seconde.*

Dans le cas où la distance de m à n vaut 1
montrons que l'union des arêtes réalisant cette distance est une variété d'étendue 1, ce qui finira d'établir le théorème.

Soit a ∈ m et b ∈ n une paire de points réalisant la distance 1, m est engendréepar une famille $(a_i)_{i=1...p}$ de vecteurs unitaires issus de a et de même n par une famille $(b_i)_{i=1...q}$.

Considérons alors les vecteurs $\{a_i\}$ correspondant à l'intersection des vecteurs libres associés aux a_i et aux b_i ; on pourra supposer que ce sont les r-premiers :



On établit facilement que les extrémités de toutes les combinaisons linéaires homologues de vecteurs de $\{a_i\}_{i=1,...,r}$ et de $\{b_i\}_{i=1,...,r}$ sont des couples de points réalisant la distance 1 et que ce sont les seuls.

Cette famille de couples étant une variété affine d'origine a, engendré par les $\{a_i\}_{i=1,...,r}$ et ab, d'étendue 1, on a bien établi le théorème.

2.3.2) - Relations de cette notion avec celle de consensus

On rappelle qu'on peut définir [Kuntzmann 5] le consensus de deux monômes m et n, s'il existe une variable v figurant sous formes opposées dans m et n, comme le produit des lettres de m et n, différentes de v ou v' ; le consensus d'un ensemble de monômes est alors, s'il existe, le résultat de la composition de plusieurs opérations de consensus

portant sur deux monômes et utilisant, au total, tous les monômes initiaux (on montre qu'un tel consensus, s'il existe, est unique).

Démontrons alors la

Propriété 1 -

Si m et n sont deux monômes

$$\text{Consensus Gen}(\{m,n\}) = \{\text{Consensus}(m,n)\}$$

cette écriture sous-entendant que le cas où le consensus ordinaire de m et n n'existe pas, correspond à

$$\text{Consensus Gen}(\{m,n\}) = \emptyset .$$

- Inclusion $\supset$

Celle-ci est immédiate si le consensus de m et n n'existe pas. S'il existe, on démontre que c'est un monôme premier de la fonction m+n, ce qui établit l'inclusion.

- Inclusion $\subset$

Si le consensus général est vide , c'est que m+n n'admet pas d'autres monômes premiers que m et n et qu'alors le consensus ordinaire n'existe pas.

Sinon, en se référant au théorème précédent, la direction des arêtes réalisant la distance 1, correspond à une variable figurant sous une forme dans m et sous la forme opposée dans n. m peut donc s'écrire

$$m = PQx$$

de même $n = PRx'$, en représentant par P l'ensemble des lettres communes à m et n, par Q celles de m qui ne sont pas dans n, et par R celles de n non

dans m.

Selon chacune des deux définitions, le consensus sera

{PQR} et PQR ce qui établit la propriété.

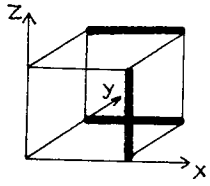
On démontrerait facilement, de même, la

Propriété 2 -

Si M, ensemble de monômes, admet un consensus, alors

Consensus Gen(M) ⊃ {Consensus (M)}

Exemple 1 -

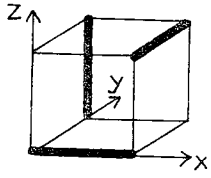


M = {xy' , yz' , yz}

Consensus (M) = x = Consensus (xy', Consensus (yz',yz))

Consensus Gen(M) = {y,x}

Exemple 2 -



M = {y'z' , xz , x'y}

Le consensus ordinaire de M n'existe pas et l'on a

Consensus Gen(M) = {xy' , x'z' , yz}

2.4) - Un théorème classique d'algèbre de Boole, sur les monômes premiers d'un produit ; la méthode de la double duale.

On montre en algèbre de Boole que

THEOREME - On obtient les monômes premiers d'un produit en faisant le produit des monômes premiers des facteurs, avec suppression éventuelle des multiples.

Pour cela, il suffit de montrer qu'aucun consensus ne peut donner de résultats nouveaux [Kuntzmann 3].

Avec la définition de monôme premier que nous avons adoptée, le théorème est absolument immédiat et l'on rappelle qu'il en découle la méthode de la double duale pour obtenir la base complète d'une fonction : en effet, dans une écriture

$$\prod_{i=1}^{P} \left(\sum_{1}^{q_i} a_{ij} \right)$$

chaque décomposition $\Sigma\, a_{ij}$ constitue une décomposition suivant la base complète de $\Sigma\, a_{ij}$.

De nombreux theorèmes d'algèbre de Boole peuvent ainsi s'obtenir très facilement ; on verra d'autres exemples au chapitre IV.

3) - L'inégalité triangulaire dans $(\mathbb{Z}/2)^n$; ses conséquences.

Le problème qui va nous intéresser dans ce paragraphe est le suivant :

Quels sont les graphes des distances d'un bipoint, d'un triangle, d'un tétraèdre, qui correspondent effectivement à un bipoint, un triangle, un tétraèdre de $(\mathbb{Z}/2)^n$ pour la distance correspondant à la norme $\Sigma\, |x_i|$? On montrera, en particulier, que

pour que le graphe des distances d'un tétraèdre corresponde à un tétraèdre de $(\mathbb{Z}/2)^n$, il est nécessaire et suffisant que les quatre sous-graphes triangulaires correspondent à un triangle de $(\mathbb{Z}/2)^n$, théorème qui n'admet pas d'équivalent dans le cas réel (i.e. espace sur $\mathbb{R}$).

3.1) - Cas du bipoint

Ce cas est évident, on peut écrire le

THEOREME 1 - a entier est la longueur d'un bipoint inscrit dans un n-cube [1] $a \leqslant n$.

3.2) - Cas du triangle

On va démontrer le

THEOREME 2 - a, b, c, quantités entières, sont les longueurs des côtés d'un triangle inscrit dans un n-cube

$$\Leftrightarrow (0) \begin{cases} |b-c| \leqslant a \leqslant b+c & (I) \\ a+b+c \text{ pair} \\ \operatorname{Sup}(a,b,c) \leqslant n \\ a+b+c \leqslant 2n \quad . \end{cases}$$

Remarque - La condition (I) d'allure non symétrique peut être remplacée par

$$\text{les trois relations symétriques (II)} \begin{cases} a \leqslant b+c \\ b \leqslant a+c \\ c \leqslant a+b \end{cases}$$

$$\text{ou même (III)} \begin{cases} |b-c| \leqslant a \\ |c-a| \leqslant b \\ |a-b| \leqslant c \quad . \end{cases}$$

En effet, si $b \geqslant c$, ce qu'on peut toujours supposer, $|b-c| = b-c$ et de $b-c \leqslant \underline{a \leqslant b+c}$ on déduit $\underline{b \leqslant a+c}$

$$\text{et} \quad 2b-c \leqslant a+b$$
$$\text{soit} \quad 2(b-c) + c \leqslant a+b$$
$$\text{d'où} \quad \underline{c \leqslant a+b}$$

ce qui établit entièrement (I) $\Rightarrow$ (II) .

---

[1] *Le terme n-cube sera souvent employé pour désigner* $(\mathbb{Z}/_2)^n$, *en particulier lorsque l'on n'a pas précisé d'origine particulière.*

$$\text{De } \begin{cases} b \leqslant a+c \\ c \leqslant a+b \end{cases} \quad \text{on déduit} \quad \begin{cases} b-c \leqslant a \\ c-b \leqslant a \end{cases} \quad \text{soit} \quad |b-c| \leqslant a$$

ce qui établit par symétrie (II) $\Rightarrow$ (III).

De $|a-b| \leqslant c$ on déduit en particulier $a-b \leqslant c$, ce qui, avec $|b-c| \leqslant a$ établit (III) $\Rightarrow$ (I).

3.2.1) - Etablissons maintenant la partie " $\Rightarrow$ " du théorème (condition nécessaire).

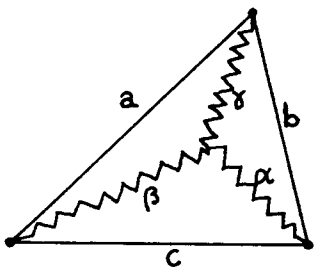
Si a,b,c sont les longueurs des côtés d'un triangle, il existe trois vecteurs $\vec{a},\vec{b},\vec{c}$ de normes a,b,c tels que $\vec{a} = \vec{b}+\vec{c}$.

On a donc $\|\vec{a}\| \leqslant \|\vec{b}\| + \|\vec{c}\|$ soit $a \leqslant b+c$

et $\|\vec{b}+\vec{c}-\vec{c}\| \leqslant \|\vec{b}+\vec{c}\| + \|c\| = a+c$ soit $b-c \leqslant a$; on établirait de même $c-b \leqslant a$ ce qui donne finalement (I). Le n-cube ne possédant que des cycles de longueur paire, la quantité a+b+c doit nécessairement être paire.

Par le théorème 1, il est aussi nécessaire qu'on ait $\sup(a,b,c) \leqslant n$.

Enfin, soit γ l'ensemble des directions communes à a et b,
β l'ensemble des directions de a non dans b,
α l'ensemble des directions de b non dans a.



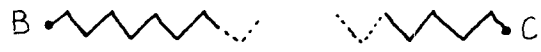
Il vient $a = \gamma + \beta$
$b = \gamma + \alpha$
$c \leqslant \beta + \alpha$
d'où $a+b+c \leqslant 2(\alpha+\beta+\gamma) < 2n$.

3.2.2) - Reste à établir la partie "$\Leftarrow$"

Soit a,b,c, trois entiers vérifiant les conditions (0) et supposons,

par exemple, $a \geqslant b \geqslant c$.

Considérons alors, dans le n-cube, deux points B et C, à distance a, et une chaîne de a arêtes de directions distinctes reliant B à C.



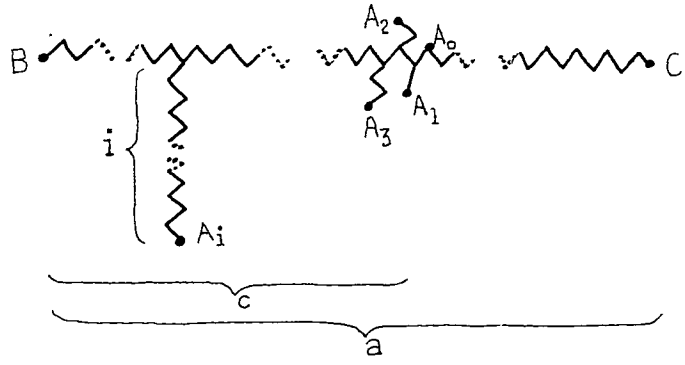
Puisque $c \leq a$, on peut trouver un point A à distance C de B, de différentes façons :

A_o sur la chaîne BC avec $A_oC = a-c$;

A_1 à distance 1 d'un point de la chaîne, lui-même à distance C-1 de B avec $A_1C = a-c+2$;

A_i à distance i d'un point de la chaîne, lui-même à distance c-i de B avec $A_iC = a-c+2i$;

et ceci est possible tant que $i \leqslant n-a$.



L'application $f : [0,\ldots,n-a] \to \mathbb{N}$

$$i \mapsto f(i) = \|A_iC\|$$

est strictement croissante de a-c à a-c+2n-2a = 2n-(a+c) et ceci de 2 en 2. Comme b = a-c (modulo 2) et que $a-c \leqslant b \leqslant 2n-(a+c)$ on en déduit qu'il existe un triangle ABC admettant des côtés de longueur a,b,c.

Remarque 1 - dans le cas a = n il vient $b+c \geqslant a = n$ ainsi que $b+c \leqslant 2n-n = n$ d'où $b+c = n$.

Remarque 2 - La démonstration du théorème précédent montre, de plus, qu'à une isométrie près, le triangle ABC est unique, ce qui n'avait, a priori, rien d'évident : l'homologue de cette propriété dans $\mathbb{R}^n$ s'appelle le 3^e cas d'égalité des triangles.

3.3) - Cas du tétraèdre

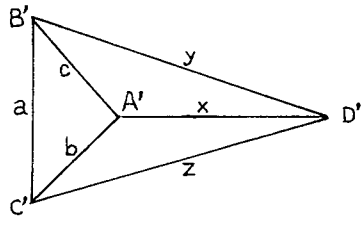
On va démontrer le théorème

> Pour que le graphe des distances d'un tétraèdre représente effectivement un tétraèdre du n-cube, il est nécessaire et suffisant que chacun des quatre graphes triangulaires représente effectivement un triangle du n-cube.

La condition nécessaire est évidente.

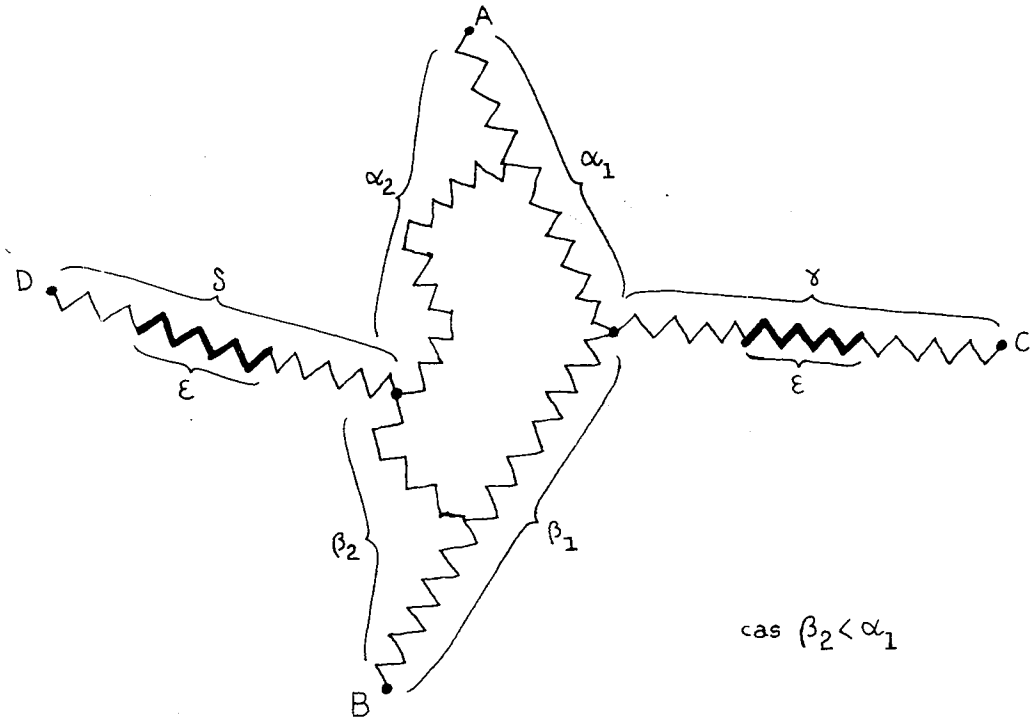
3.3.1) - Démonstration de la condition suffisante

Soit A',B',C',D' les sommets d'un graphe des distances tel que les triangles A'B'C' , A'B'D' , A'C'D' , B'C'D' correspondent aux triangles ABC, ABD , ACD , BCD d'un n-cube :



Soit α_1, β_1,γ le nombre de directions communes à AB et AC, BA et BC, CA et CB, on a :

$$\begin{cases} \alpha_1+\beta_1 = c \\ \alpha_1+\gamma = b \\ \beta_1+\gamma = a \end{cases} \qquad \text{d'où} \qquad \begin{cases} \alpha_1 = \dfrac{b+c-a}{2} \\ \beta_1 = \dfrac{a+c-b}{2} \\ \gamma = \dfrac{a+b-c}{2} \end{cases}$$



Considérons (ci-dessus) un point D réalisant le triangle ABD conformément au graphe des distances A'B'D'. On va montrer que parmi tous les choix possibles de D il en existe au moins un tel que la distance DC soit z. Pour cela calculons les distances réalisables minimale et maximale de C à D.

a) Distance minimale

Soit α_2 et β_2 les quantités homologues à α_1 et β_1, mais relativement à ABD. On peut toujours , quitte à échanger les noms de A et B, supposer $\alpha_2 \leqslant \alpha_1$. La distance minimale est alors

$$\alpha_1-\alpha_2 = \frac{b+c-a}{2} - \frac{x+c-y}{2} = \frac{b-x}{2} + \frac{y-a}{2}$$

Or, dans le triangle A'C'D', $b-x \leqslant z$ et de même dans B'C'D' $y-a \leqslant z$

b) Distance maximale

Elle est obtenue en rendant la distance δ de D à la chaîne de directions du triangle ABD, aussi grandeque possible. Or, cette distance est au plus $\delta = n-\alpha_1-\beta_1-\gamma+\varepsilon$ où ε est le nombre de directions communes à cette chaîne et à la chaîne joignant C à la chaîne AB dans le triangle ABC.

On a donc, en supposant par exemple $\beta_2 \leqslant \alpha_1$

$$DC \leqslant (n-\alpha_1-\beta-\gamma) + (\beta_1+\beta_2) + (\gamma-\varepsilon)$$

$$DC \leqslant 2(n-\alpha_1-\beta_1) + \beta_1+\beta_2 - \gamma-\delta$$

$$DC \leqslant 2n-b-c+a-a-c+b+ \frac{a+c-b}{2} + \frac{y+c-x}{2} + \frac{c-a-b}{2} + \frac{c-x-y}{2}$$

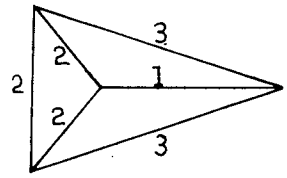
$$DC \leqslant 2n-b-x \ .$$

Dans le cas où l'on n'aurait pas $\beta_2 \leqslant \alpha_1$ c'est que $\alpha_2 < \beta_1$, en remplaçant $\beta_1 + \beta_2$ par $\alpha_2 + \alpha_1$ il vient

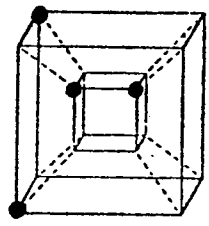
$$DC \leqslant 2n-a-y$$

Or dans le triangle A'D'C' $b+x+z \leqslant 2n$, et de même dans B'C'D' $a+y+z \leqslant 2n$. On en déduit que $z \in [DC_{Min}, DC_{Max}]$. Il y a deux façons de faire varier la distance C, soit en modifiant ε , soit en modifiant la chaîne AB correspondant au triangle ABD. Dans un cas comme dant l'autre, la variation est de 2. En remarquant que $x+b+z \equiv 0 \pmod 2 \Rightarrow z \equiv 2n-b-x \pmod 2$ et donc, de même $z \equiv 2n-a-y \pmod 2$, on finit d'établir le théorème.

Exemple -

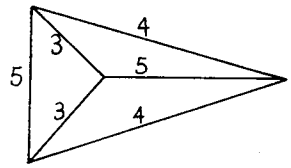


3 triangles peuvent être construits dans $(\mathbb{Z}/2)^3$, les triangles de côtés (2,2,2), (3,2,1) et (3,2,1) puisque la somme de leurs côtés vaut 6 = 2x3. Le dernier (3,3,2) de somme 8 ne peut être construit qu'au moins dans $(\mathbb{Z}/2)^4$. La figure suivante donne une réalisation du tétraèdre dans $(\mathbb{Z}/2)^4$:

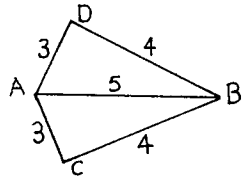


3.3.2) Contre-exemple dans $\mathbb{R}^n$

Considérons le graphe



Les quatre triangles peuvent être construits dans $\mathbb{R}^2$. Considérons la réalisation des deux triangles (3,4,5) selon la figure



La distance maximale de D à C sera obtenue en rendant les deux triangles ABC et ADB coplanaires. Dans ce cas

$$DC = 2\sqrt{\frac{9x16}{25}} = \frac{24}{5} < 5$$

Ce qui rend impossible la réalisation du tétraèdre dans $\mathbb{Z}/2^n$, du moins selon la norme euclidienne.

3.3.3) - Définition -

Nous appellerons périmètre d'une partie de $\coprod_{\mathbb{N}} \mathbb{Z}/2$, la somme éventuellement infinie des longueurs de ses bipoints.

On a vu que le périmètre p d'un triangle de $(\mathbb{Z}/2)^n$ vérifie $p \leqslant 2n$. On en déduit la propriété

Propriété - Le périmètre p d'un tétraèdre de $(\mathbb{Z}/2)^n$ vérifie $p \leqslant 4n$.
En effet, si l'on considère le tétraèdre représenté par la figure

$$a+b+c \leqslant 2n$$
$$a+y+z \leqslant 2n$$
$$x+b+z \leqslant 2n$$
$$x+y+c \leqslant 2n$$

d'où $2p \leqslant 4 \times 2n$.

On peut remplir certaines cases du tableau suivant, donnant en fonction de la dimension de l'espace et du nombre de points d'une partie, la valeur maximale des différents périmètres :

Dimension → / n ↓	1	2	3	4	5	6	7	8
0	0	-	-	-	-	-	-	-
1	0	1	-	-	-	-	-	-
2	0	2	4	8	-	-	-	-
3	0	3	6	12	18	27	36	48
4	0	4	8	16	24	36	48	64
Formule	0	n	2n	4n	6n?	9n?	12n?	16n?

On notera les conjectures Max p(5) = 6n , Max p(6) = 9n,
Max p(7) = 12n et Max p(8) = 16n .

Sur les valeurs du tableau des "périmètres généralisés"

Le chapitre sur l'inégalité triangulaire et ses conséquences, fournit les formules générales $\Pi(1)=0$, $\Pi_n(2)=n$, $\Pi_n(3)=2n$, $\Pi(4)=4n$.

On établit d'autre part facilement

$$\Pi_n(2^n) = \frac{1}{2}\left(2^n(n+2C_n^2+\ldots+nC_n^n\right) = \frac{1}{2}\,2^n \sum_{i=0}^{n} iC_n^i = n\,2^{2(n-1)}$$

et encore

$$\Pi_n(2^n-1) = \frac{1}{2}\left(C_n^1(n2^{n-1}) + C_n^2(n2^{n-2})+\ldots+C_n^n(n2^{n-n})\right)$$

$$= n2^{n-1}(2^n-1) - n2^{n-1} = n2^{n-1}(2^{n-1}-1) \quad ;$$

de même

$$\Pi_n(2^n-2) = \frac{1}{2}\left(C_n^1(n2^{n-1}-(n-1)) +\ldots C_n^p\left(n2^{n-p}-(n-p)\right)+\ldots C_n^{n-1}\left(n2^{n-(n-1)}-1\right)\right)$$

$$= n2^{n-1}(2^{n-1}-1)-n(2^{n-1}-1) = n(2^{n-1}-1)^2$$

et enfin

$$\Pi_n(2^{n-1}) = \frac{1}{2}\,2^{n-1}(0+2C_n^2 +\ldots 2pC_n^{2p} +\ldots) = n2^{2(n-2)} \quad ;$$

soit

$$\Pi_n(2^n) = n2^{\,2(n-1)}$$

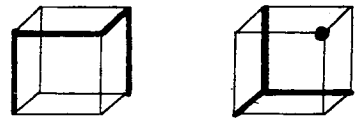
$$\Pi_n(2^n-1) = n2^{n-1}(2^{n-1}-1) = \Pi(2^n)\left(1 - \sqrt{\frac{n}{\Pi(2^n)}}\right)$$

$$\Pi_n(2^n-2) = n(2^{n-1}-1)^2 = \frac{\Pi^2(2^n-1)}{n2^{2(n-1)}}$$

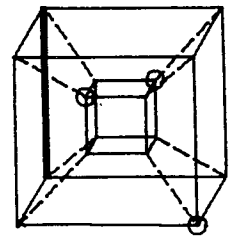
$$\Pi_n(2^{n-1}) = n2^{2(n-2)} = \frac{\Pi(2^n)}{4}$$

on détermine enfin :

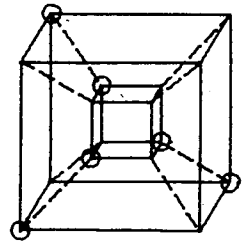
$\Pi_3(5) = 18$ pour les fonctions



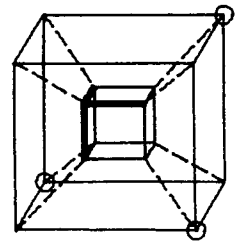
$\Pi_4(5) = 24$ par exemple pour



$\Pi_4(6) = 36$ par exemple pour



$\Pi_4(7) = 48$ par exemple pour



Remarque-

Les conjectures de la page 110. s'inscrivent dans les deux formules générales, compatibles avec celles de la page précedente :

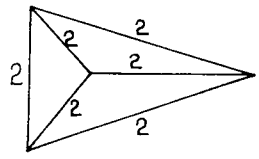
$$\begin{cases} p \text{ pair} & \Pi_n(p) = \frac{p^2}{4} n \\ p \text{ impair} & \Pi_n(p) = \frac{p^2 - 1}{4} n \end{cases}$$

Enfin on peut démontrer le

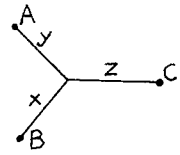
THEOREME - Deux tétraèdres non isomorphes (isométriques) de graphe de distances données sont de dimensions différentes, où la dimension d'un tétraèdre est le plus petit entier n tel que ce tétraèdre soit inclus dans une partie isomorphe à $(\mathbb{Z}/2)^n$.

En effet, en revenant à la figure p.107, deux tétraèdres non isomorphes, correspondent à des valeurs de ε différentes. Le théorème est alors établi si l'on remarque que la dimension d'un tétraèdre est le nombre de directions différentes intervenant dans une décomposition du type de celles de la figure

Exemple 1 -

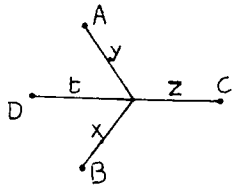


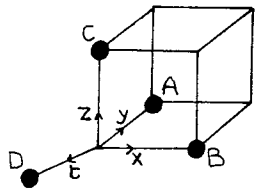
Considérons la décomposition de l'un des triangles



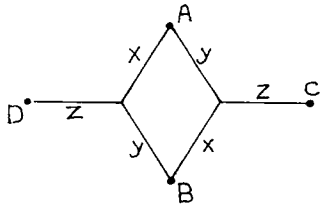
.

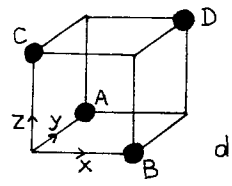
On obtient deux décompositions différentes de ABCD qui sont





dimension 4

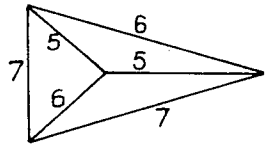




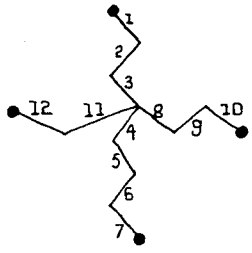
dimension 3

.

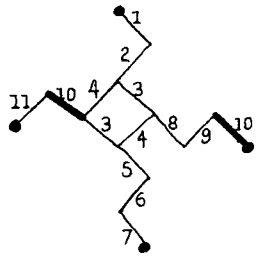
Exemple 2 -



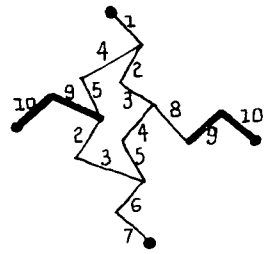
Voici les trois décompositions non isomorphes des tétraèdres admettant le graphe de distances ci-contre.



n = 12



n = 11



n = 10

CHAPITRE II

UNE QUESTION D'ALGEBRE DE BOOLE SUR LES FONCTIONS IRREDUCTIBLES ET LE COUPLAGE MIN-MAX DU N-CUBE

1) - Présentation du problème.

1.1) Une question d'algèbre de Boole.

1.2) Ses relations avec le couplage du n-cube.

2) - Quelques résultats sur le couplage du n-cube.

3) - Un encadrement de I_n et ses conséquences.

4) - Sur l'existence d'un 23-couplage du 6-cube (conséquence de la conjecture C1 de Forcade).

4.1) Couplages maximaux vérif. C1.

4.2) Un programme de recherche des couplages maximaux.

4.3) Sur les stables complémentaires.

4.4) Résultats en dimension 6.

- non-existence d'un 23-couplage et infirmation de C1.

4.5) Résultats en dimension 5 - Notion de type réduit de couplage indécomposable.

- existence de 9 types réduits de couplage à 12 arêtes et indécomposables.

5) - Sur la possibilité de resserrer l'encadrement $1+\frac{1}{3n} < \frac{3M_n}{2^n} < 1+\sqrt{\frac{2}{\pi n}} + o(\frac{1}{\sqrt{n}})$

5.1) Etude du gain possible.

5.2) Proposition de la conjecture $\frac{3M_n}{2^n} = 1+\frac{1}{3n} + o(\frac{1}{n})$.

Annexes -

1 - $\sum_{i=0}^{n} C^i_{2i} = \frac{4^{n+1}}{3\sqrt{\pi n}}\left(1+\frac{1}{24n}+\varepsilon\right)$ avec $0 < \varepsilon < \frac{1}{5n^2}$ (pour $n \geqslant 9$) .

2 et 3 - un majorant de C^{3k+1}_{6k+3} et le calcul d'une perturbation .

4 - Sur les groupes d'automorphismes de certains couplages.

II - UNE CONJECTURE D'ALGEBRE DE BOOLE SUR LES FONCTIONS IRREDUCTIBLES ET LE COUPLAGE MIN-MAX DU N-CUBE

1) - Présentation du problème

1.1) Une question d'Algèbre de Boole

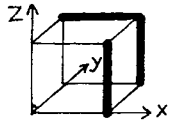
Considérons une décomposition δ d'une fonction booléenne f de n-variables, c'est-à-dire un ensemble de monômes, tel que

$$\sum_{0 \leqslant i \leqslant p} m_i = f \qquad \text{avec} \qquad \forall i \, \forall j \; m_i m_j = 0$$

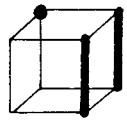
(Dans une telle décomposition les hyperfaces représentatives, dans le n-cube des différents monômes sont 2 à 2 disjoints).

Une décomposition est dite irréductible si elle ne comporte pas d'hyperfaces parallèles, de même dimension, et à distance 1 (i.e. s.s.i. on ne peut pas effectuer de réduction du type $ma + ma' \longmapsto m$).

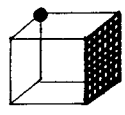
Exemple - Soit la fonction booléenne mise sous la forme non-remarquable



xy' + xy + yz ,



xy' + xy + x'yz en est une décomposition,



x + x'yz en est une décomposition irréductible.

Remargue - Partant d'une fonction booléenne mise sous une forme quelconque, on peut en déduire une décomposition (disjointe) en itérant le processus (non déterministe) suivant :

si m_1 et m_2 sont deux monômes non-disjoints et en supposant dim $m_1 \geq$ dim m_2

$$\{m_1, m_2\} \quad \text{par} \quad \{m_1,\ m_1 - m_2\}^{(1)}$$

De même, on peut passer d'une décomposition quelconque à une décomposition irréductible en effectuant toutes les "réductions"possibles.

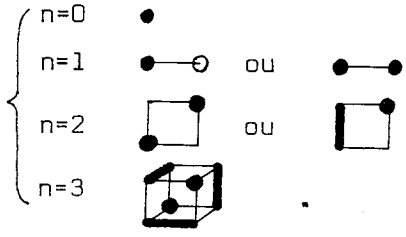
Le problème [Kuntzmann2] se pose alors, ne serait-ce que pour déterminer l'encombrement de certains algorithmes, de connaître :

$$I_n = \underset{\delta \in D_n}{\text{Max Card}}\ \delta$$

D_n : ensemble des décomposition irréductibles de fonctions booléennes de n-variables.

C'est le nombre maximum de monômes entrant dans une décomposition irréductible d'une fonction booléenne de n-variables.

On détermine facilement $I_o=1$, $I_1=1$, $I_2=2$, $I_3=5$



On connait la conjecture

$$n \geq 3 \quad I_n = 5 \times 2^{n-3} \quad ?$$

correspondant, pour n=3 à la décomposition de la fonction l donnée plus haut, et en général, à la décomposition

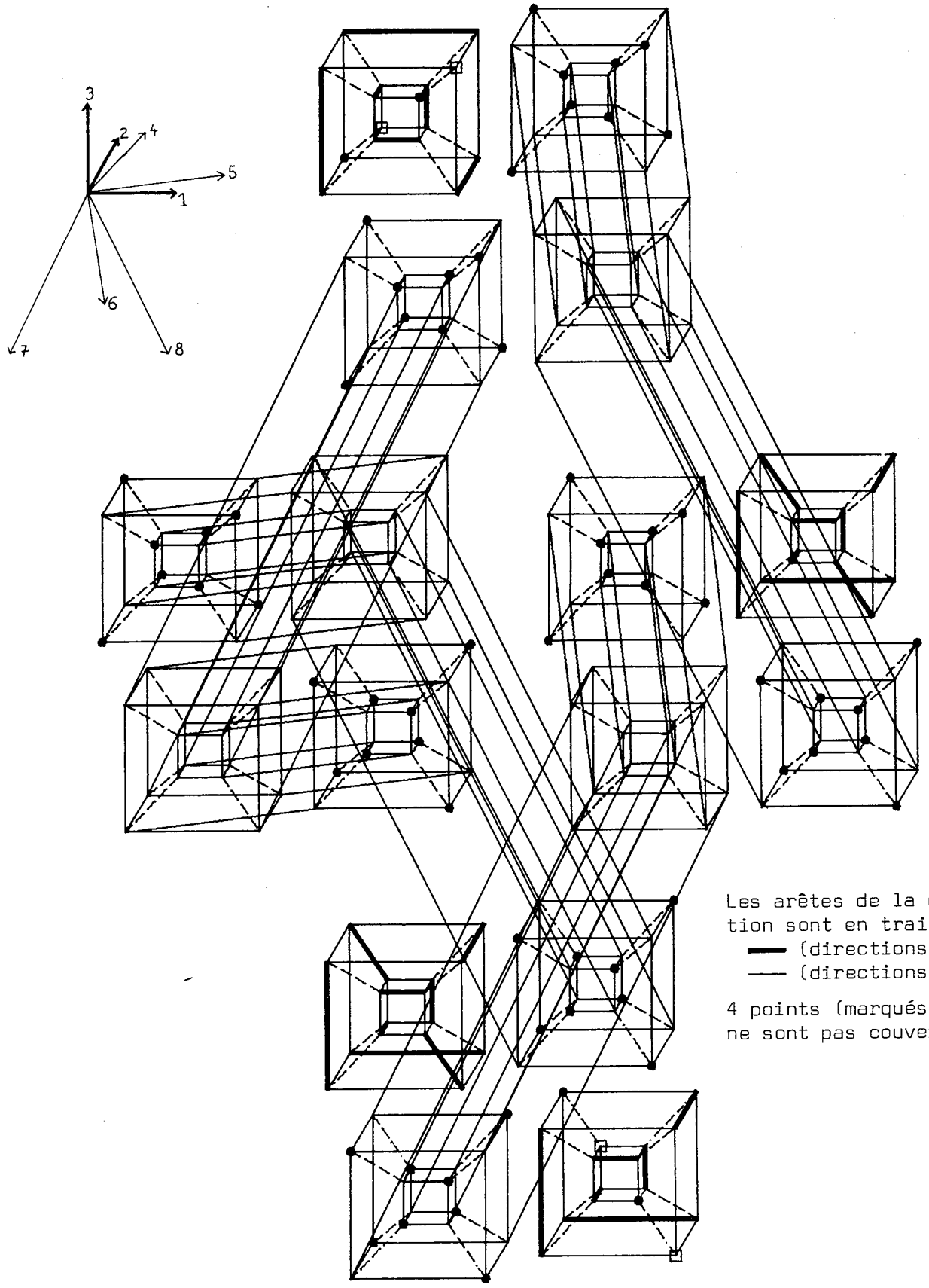
$$l(a,b,c,x_1,..,x_{n-3}) = P_{n-3}(x_1,..,x_{n-3}) \times (abc+a'b'c'+ac'+cb'+ba') + P'_{n-3}(x_1,..,x_{n-3}) \times (abc'+a'b'c+bc+c'a'+ab')$$

} Décomposition (D)

où P_m représente la fonction dite clé de parité de m variables (points d'affixe paire).

Remarque - Il existe des décompositions irréductibles de cardinal $5 \times 2^{n-3}$ sans, pour autant, couvrir tous les points de HC_n. Par exemple, en dimension 8 :

(1) *$m_1 - m_2$ représente la différence ensembliste de l'ensemble des points de m_1 et de m_2.*



Les arêtes de la décomposition sont en traits
▬ (directions 1,2,3,4)
—— (directions 5,6,7,8)

4 points (marqués □) ne sont pas couverts.

Décomposition irréductible d'une fonction de 8 variables différente de la fonction 1, et présentant $5 \times 2^{n-3} = 160$ composants:
64+4 points et 64+16+12 arêtes .

1.2) - Relation avec le problème du couplage min-max du n-cube

Associons à toute décomposition irréductible, une décomposition éventuellement non-irréductible, en remplaçant toute hyperface de dimension $\geqslant 2$ par un couplage parfait[1] de cette hyperface.

En définissant I'_n de façon analogue à I_n, mais relativement à des décompositions selon des hyperfaces de dimension au plus un (points ou arêtes) et irréductibles seulement en ce qui concerne les points, on a, évidemment,

$$I_n \leqslant I'_n .$$

On peut supposer qu'une telle décomposition couvre tous les points de HC_n car, si un point n'est pas couvert, en l'ajoutant on ne peut diminuer le cardinal de la décomposition, car l'ajout du point, soit implique une réduction, mais le cardinal ne change pas, soit augmente le cardinal de 1.

L'ensemble des arêtes d'une telle décomposition est alors un couplage maximal de HC_n.

Soit i'_n le cardinal d'une décomposition et m_n le cardinal du couplage maximal, on doit avoir

$$i'_n = m_n + (2^n - 2m_n) = 2^n - m_n .$$

On a donc $I_n \leqslant I'_n = 2^n - Mn$

où M_n est le cardinal minimum d'un couplage maximal de HC_n.

---

[1] *Rappel - Dans un graphe, un couplage est un ensemble d'arêtes disjointes ; un couplage parfait est un couplage couvrant tous les points. Ici, on identifie une hyperface H à son graphe d'ensemble de sommets, ceux de H, d'ensemble d'arêtes, celles de H (les hyperfaces de dimension 1). Une hyperface admet toujours un couplage parfait trivial.*

2) - Quelques résultats sur le couplage du n-cube

Forcade, en 1972, a publié le résultat suivant : [FORCADE]

$$\lim_{n\to\infty} \frac{M_n}{2^n} = \frac{1}{3}$$, et proposé deux conjectures

C_1 $\quad M_n = \left\lceil 2^n \frac{n}{3n-1} \right\rceil$ [1]

C_2 $\quad M_n = 2^n \frac{n}{3n-1}$ pour n de la forme $n = \frac{1+2^{2p+1}}{3}$ $(p \in \mathbb{N})$

Remargue - On établit facilement

$$2^n \frac{n}{3n-1} \in \mathbb{N} \iff n = 0 \quad \text{ou} \quad n = \frac{1+2^{2p+1}}{3} \quad \text{avec } p \in \mathbb{N}$$

En effet, $2^n \frac{n}{3n-1} \in \mathbb{N} \iff \exists \ell \quad n2^n = (3n-1)\ell$

Or, n et 3n-1 sont premiers entre eux puisque 3(n) - (3n-1) = 1, d'où n divise ℓ , soit $\ell = pn$. Il vient alors , si $n \neq 0$ $2^n = (3n-1)p$, i.e. $3n-1 = 2^k$. La propriété sera donc établie si l'on établit $2^k+1 \underset{3}{\equiv} 0 \Leftrightarrow k \underset{2}{\equiv} 1$. [2]

1) Etablissons l'implication $\Rightarrow$

Si l'on suppose k = 2p (p > 0), en écrivant $2^{2p}+1 = 4 \times (2^{2(p-1)}+1) - 3$ et avec l'hypothèse que cette quantité est multiple de 3, on arriverait à 2^0+1 multiple de 3.

2) Etablissons l'implication $\Leftarrow$

Si l'on suppose k = 2p+1 (p $\geqslant$ 0), l'écriture $2^{2p+1}+1 = 4 \times (2^{2(p-1)+1}+1) - 3$ permet de déduire que $2^k+1 \underset{3}{\equiv} 0$ puisque $2^1+1 \underset{3}{=} 3 \equiv 0$.

---

[1] *Le symbolisme* $\lceil x \rceil$ *désigne l'entier immédiatement superieur ou égal à* x.

[2] *Le symbolisme* $x \underset{n}{\equiv} y$ *est mis pour* x-y *multiple de* n (x=y modulo n).

La conjecture C_1 est vraie, évidemment, pour $n \in \{0,1,2\}$ car $M_0 = 0$, $M_1=1$, $M_2=2$. Pour $n \in \{3,4,5\}$ la décomposition (D) confirme encore la conjecture ($M_3=3$, $M_4=6$, $M_5=12$).

Pour n=6 (D) donne un couplage à 24 arêtes et C_1 affirme $M_6=23$; l'existence ou non d'un couplage à 23 arêtes du cube de dimension 6 confirmerait ou infirmerait C_1. Quant à C_2, on n'est assuré de sa justesse que pour $p \in \{0,1\}$ correspondant à n=1 et n=3 : dès p=2, $n = \frac{1+2^5}{3} = 11$: le problème est ouvert.

2.1) <u>Amélioration du résultat</u> $\lim_{n\to\infty} \frac{M_n}{2^n} = \frac{1}{3}$ (1)

Forcade établit (1) à l'aide de trois lemmes

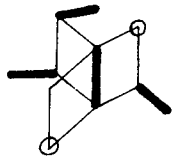
lemme 1 $\quad M_{n+1} \leqslant 2\, M_n$

lemme 2 $\quad M_n \geqslant 2^n \frac{n}{3n-1}$

lemme 3 $\quad \overline{\lim_{n\to\infty}} \; M_{6n} \leqslant \frac{2^{6n}}{3}$ ($\overline{\lim}$ mis pour limite superieure)

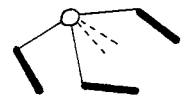
On peut donner une démonstration beaucoup plus courte que celle de Forcade, du lemme 2.

En effet, il suffit de remarquer que par une arête d'un couplage maximal passent, au plus, n-1 faces carrées contenant un point non couvert. En décomptant de 2 façons ces points non couverts, on établit



$$m_n(n-1) \geqslant n(2^n - m_n)$$

soit $\quad m_n \geqslant 2^n \frac{n}{3n-1}$

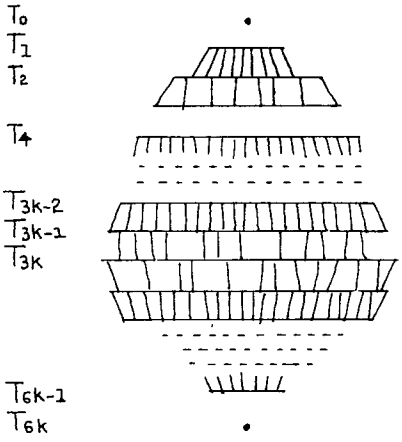


Pour établir son troisième lemme, Forcade exhibe un couplage de HC_{6n} dont il majore le cardinal par une quantité admettant $\frac{2^{6n}}{3}$ pour partie principale. Nous allons reprendre cette idée en améliorant le décompte.

Une origine de HC_n étant choisie, considérons les T_p ($0 \leqslant p \leqslant n$) ensemble des points de HC_n à distance p de son origine. Un point de T_p est relié à n-p points T_{p+1}, chacun d'eux étant relié à p+1 points de T_p. Pour $\frac{p+1}{n-p} \leqslant 1$, soit $2p \leqslant n-1$, il existe donc d'après un corollaire bien connu du théorème de Hall, un couplage de T_p vers T_{p+1}.

Partant de p=1 et successivement pour chacun des p égaux à 1 modulo 3, on construit un couplage de T_p vers T_{p+1}, ainsi que son symétrique par rapport au centre du cube, tant que c'est possible. On obtient ainsi un couplage de HC_n saturant certains T_p. On le rend alors maximal par adjonction de nouvelles arêtes.

En dimension 3, on trouve le couplage bien connu "demi-tour du cube" Pour n multiple de 6, on obtient, par exemple, un couplage que l'on peut "schématiser" ainsi :



et on a la majoration

$$m_{6k} \leqslant 2\,(C_{6k}^{2} + C_{6k}^{5} + \ldots + C_{6k}^{3k-1}) \quad .$$

Calcul de $s_k = 2\left(C_{6k}^{2} + C_{6k}^{5} + \ldots + C_{6k}^{3k-1}\right)$:

2.2) Une réduction combinatoire -

On peut écrire, pour $k \geqslant 1$

$$C_{6k}^{2}+\ldots+C_{6k}^{3i+2}\ldots+C_{6k}^{3k-1} = C_{6k-1}^{1}+C_{6k-1}^{2}+\ldots+C_{6k-1}^{3i+1}+C_{6k-1}^{3i+}+\ldots+C_{6k-1}^{3k-2}+C_{6k-1}^{3k-1}$$

d'où

$$C_{6k}^{2}+\ldots+C_{6k}^{3i+2}+\ldots+C_{6k}^{3k-1}+C_{6k-1}^{o}+C_{6k-1}^{3}+\ldots C_{6k-1}^{3i}+\ldots+C_{6k-1}^{3k-3} = 2^{6k-1-1} = 2^{6k-2};$$

de même la deuxième partie du premier membre

$$C_{6k-1}^{o}+\ldots C_{6k-1}^{3i}+\ldots C_{6k-1}^{3k-3}+C_{6k-2}^{1}+\ldots+C_{6k-2}^{3i+1}+\ldots+C_{6k-2}^{3k-2} = 2^{6k-3} - \frac{1}{2}\,C_{6k-2}^{3k-1}$$

et successivement

$$C_{6k-2}^{1}+\ldots\ldots+C_{6k-2}^{3k-2}+C_{6k-3}^{2}+\ldots\ldots+C_{6k-3}^{3k-4}=2^{6k-4}$$

$$C_{6k-3}^{2}+\ldots\ldots+C_{6k-3}^{3k-4}+C_{6k-4}^{o}+\ldots\ldots+C_{6k-4}^{3k-3}=2^{6k-5}-\frac{1}{2}C_{6k-4}^{3k-2}$$

$$C_{6k-4}^{o}+\ldots\ldots+C_{6k-4}^{3k-3}+C_{6k-5}^{1}+\ldots\ldots+C_{6k-4}^{3k-5}=2^{6k-6}$$

$$C_{6k-5}^{1}+\ldots\ldots+C_{6k-5}^{3k-5}+C_{6k-6}^{2}+\ldots\ldots+C_{6k-6}^{3k-4}=2^{6k-7}-\frac{1}{2}C_{6k-6}^{3k-3}\ .$$

On en déduit la récurrence linéaire

$$s_k=s_{k-1}-2^{6k-6}+2^{6k-5}-\ldots.+2^{6k-1}+C_{6k-6}^{3k-3}+C_{6k-6}^{3k-2}+C_{6k-4}^{3k-2}+C_{6k-2}^{3k-1}$$

$$s_{k-1}=s_{k-2}-2^{6k-12}\,\frac{(-2)^6-1}{-2-1}+C_{6k-12}^{3k-6}+C_{6k-10}^{3k-5}+C_{6k-8}^{3k-4}$$

avec $s_1=0+2^o\,\frac{2^6-1}{3}+C_o^o+C_2^1+C_4^2$ puisque $30=0+21+1+2+6$;

soit, finalement

$$s_k=\frac{2^6-1}{3}\,2^o+\ldots.+2^{6(k-1)}+\sum_{i=0}^{3k-1}C_{2i}^{i}$$

$$s_k=\frac{2^6-1}{3}\,\frac{2^{6k}-1}{2^6-1}+\sum_{i=0}^{3k-1}C_{2i}^{i}\ ,$$

$$\boxed{s_k=\frac{2^{6k}-1}{3}+\sum_{i=0}^{3k-1}C_{2i}^{i}}$$

Remarque - On établirait de même, à l'aide des égalités :

$$C_{6k+3}^{1}+\ldots\ldots+C_{6k+3}^{3k+1}+C_{6k+2}^{2}+\ldots.+C_{6k+2}^{3k-1}=2^{6k+1}+\frac{1}{2}C_{6k+2}^{3k+1}$$

et $2\,C_3^1=6=3+C_o^o+C_2^1$,

$$2\left(C^{1}_{6k+3}+\dots+C^{3k+1}_{6k+3}\right)=\frac{2^{6k+3}+1}{3}+\sum_{i=0}^{3k+1}C^{i}_{2i}\quad;$$

ainsi qu'à l'aide de :

$$C^{2}_{6k+3}+\dots+C^{3k-1}_{6k+3}+C^{0}_{6k+2}+C^{3}_{6k+2}+\dots+C^{3k}_{6k+2}=2^{6k+1}-\frac{1}{2}C^{3k+1}_{6k+2}$$

et $2C^{2}_{9}=72=3+2^{3}\frac{2^{6}-1}{3}-C^{0}_{0}-C^{1}_{2}-C^{2}_{4}-C^{3}_{6}-C^{4}_{8}$;

$$2\left(C^{2}_{6k+3}+\dots+C^{3k-1}_{6k+3}\right)=\frac{2^{6k+3}+1}{3}-\sum_{i=0}^{3k+1}C^{i}_{2i}\quad.$$

2.3) Une borne supérieure pour M_n et un encadrement -

A l'aide de la relation $\sum_{i=0}^{n}C^{i}_{2i}=\frac{4^{n+1}}{3\sqrt{\pi n}}\left(1+\frac{1}{24n}+\varepsilon\right)$ avec $0<\varepsilon<\frac{1}{5n^{2}}$ $(n\geqslant 9)$

(voir calcul annexe 1), il vient

$$s_k=\frac{2^{6k}-1}{3}+\frac{4^{3k}}{3\sqrt{\pi(3k-1)}}\left(1+\frac{1}{24(3k-1)}+\varepsilon\right)$$

où $\varepsilon<\frac{1}{5(3k-1)^{2}}$;

soit $M_{6k}<\frac{2^{6k}}{3}\left(1+\sqrt{\frac{2}{\pi 6k}}\,\frac{1+\frac{1}{12(6k-2)}+\varepsilon}{\sqrt{1-\frac{2}{6k}}}\right)$.

En remarquant alors (lemme 1 de Forcade) que $\frac{M_{n+1}}{2^{n+1}}\leq\frac{M_n}{2^n}$ [1], on peut écrire

$$0\leqslant i<6\qquad M_{6k+i}<\frac{2^{6k+i}}{3}\left(1+\sqrt{\frac{2}{\pi(6k+i)}}\,\frac{1+\frac{1}{12(6k-2)}+\varepsilon}{\sqrt{1-\frac{i}{6k+i}}\,\sqrt{1-\frac{2}{6k}}}\right)\quad.$$

---

[1] *Pour cela il suffit de plonger un couplage maximal de HC_n, dans HC_{n+1} et de le compléter par le couplage symétrique par rapport au centre de HC_{n+1}, pour obtenir un couplage maximal de HC_{n+1}.*

L'inégalité

$$\frac{1+\frac{1}{12(6k-2}+\frac{4}{5(6k-2)^2}}{\sqrt{1-\frac{5}{6k+5}}\sqrt{1-\frac{2}{6k}}} < 1+\frac{3}{6k+5} \quad \text{valable dès } k=3, \text{ permet donc}$$

d'écrire

$$\boxed{\forall\, n \geqslant 18 \qquad M_n < \frac{2^n}{3}\left(1+\sqrt{\frac{2}{\pi n}}+\varepsilon\right) \text{ où } \quad \varepsilon < \sqrt{\frac{2}{\pi n}} \times \frac{3}{n} = o\left(\frac{1}{n}\right)} \quad ;$$

l'inégalité $1+\frac{1}{3n} < 1+\frac{1}{3n-1} = \frac{3n}{3n-1}$ fournit alors l'encadrement annoncé

$$\boxed{1+\frac{1}{3n} < \frac{3M_n}{2^n} < 1+\sqrt{\frac{2}{\pi n}}+o\left(\frac{1}{n}\right)} \quad .$$

3) Un encadrement de I_n

3.1) Considérons le couplage proposé au début de ce chapitre, dans le cas particulier $n \equiv_6 3$.

Un tel couplage constitue une décomposition disjointe, pas forcément irréductible. Nous allons montrer qu'en fait, une telle décomposition n'est que "peu" réductible. On utilise, pour cela, le

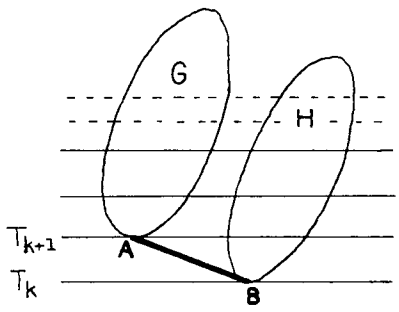
LEMME - Une hyperface de dimension p intercepte exactement p+1 ensembles T_i consécutifs : T_{i+j} $\quad 0 \leqslant j \leqslant p$.

Ce lemme s'établit immédiatement par récurrence.

Il est vrai pour les hyperfaces de dimension 0 : les points.

Supposons-le vrai en dimension $p < n$ et considérons une hyperface F de dimension p+1, immergée dans HC_n. En tant qu'ensemble de points F est la réunion de G et H de dimension p, on va montrer que H et G n'interceptent pas les mêmes p ensembles T_i.

En effet, soit A un point de G réalisant le minimum de la distance des points de G à l'origine de HC. L'arête joignant A au point B de H, suivant la direction supplémentaire de F, ne peut être incluse dans un T_i car les points d'un même T_i sont à des distances paires. L'extrémité de cette arête ou de sa symétrique, par rapport au centre de F, fournit alors un[(1)] point B de H appartenant à un ensemble T_k, différent de ceux interceptés par G.



D'autre part, si F interceptait plus de p+2 ensembles T_K, il existerait alors dans F deux points à distance au moins p+2, ce qui est impossible puisque dim F = p+1.

On peut, pour $n \equiv 3$ supposer que le couplage est symétrique par rapport au centre de HC_n et donc ne s'intéresser qu'à la configuration correspondant aux T_i avec $0 \leqslant i \leqslant 3k+2$. Le lemme permet d'affirmer que les réductions ne peuvent produire, au plus, que des carrés. On obtient alors la minoration suivante, du nombre j_n des éléments non ponctuels d'une décomposition disjointe irréductible maximale de HC_n (pour $n \equiv 3$)

$$2\,(C^1_{6k+3} + C^4_{6k+3} + \dots C^{3k-2}_{6k+3}) + C^{3k+1}_{6k+3} \leqslant j_{6k+3}$$

Or $i_{6k+3} = j_{6k+3} + (2^{6k+3} - 2m_{6k+3})$ et finalement

$$i_{6k+3} > 2(C^1_{6k+3} + C^4_{6k+3} + \dots + C^{3k-2}_{6k+3}) + C^{3k+1}_{6k+3} + 2^{6k+3} - 2\,m_{6k+3}$$

---

(1) *Un tel point est unique, mais ici, cela importe peu.*

où $m_{6k+3} = 2\,(C^{2}_{6k+3} + \quad + C^{3k-1}_{6k+3}) + C^{3k+1}_{6k+3}$.

Un calcul analogue à celui de s_k permet d'écrire

$$2(C^{1}_{6k+3} + C^{4}_{6k+3} + \ldots + C^{3k+1}_{6k+3}) = \frac{2^{6k+3}+1}{3} + \sum_{i=0}^{3k+1} C^{i}_{2i}$$

et de même

$$2(C^{2}_{6k+3} + C^{5}_{6k+3} + \ldots + C^{3k-1}_{6k+3}) = \frac{2^{6k+3}+1}{3} - \sum_{i=0}^{3k+1} C^{i}_{2i}$$

ce qui conduit à :

$$i_{6k+3} > \frac{2^{6k+3}+1}{3} + \sum_{i=0}^{3k+1} C^{i}_{2i} - C^{3k+1}_{6k+3} + 2^{6k+3} - \frac{2}{3}(2^{6k+3}+1) + 2\sum_{i=0}^{3k+1} C^{i}_{2i} - 2C^{3k+1}_{6k+3}$$

$$> \frac{2}{3}(2^{6k+3}-1) + 3\left(\sum_{i=0}^{3k+1} C^{i}_{2i} - C^{3k+1}_{6k+3}\right) .$$

Or, on a $\sum_{i=0}^{3k+1} C^{i}_{2i} = \frac{4^{3k+2}}{3\sqrt{\pi(3k+1)}}\left(1 + \frac{O(1)}{k}\right) = \frac{2^{6k+3} \times 2\sqrt{2}}{3\sqrt{\pi(6k+3)}}\left(1+\frac{O(1)}{K}\right)$

$$C^{3k+1}_{6k+3} = 2^{6k+3}\sqrt{\frac{2}{\pi(6k+3)}}\left(1 + \frac{O(1)}{k}\right) \qquad \text{(Calculs annexes 1 et 2)};$$

d'où $$\sum_{i=0}^{3k+1} C^{i}_{2i} - C^{3k+1}_{6k+3} = -\frac{2^{6k+3}}{3}\sqrt{\frac{2}{\pi(6k+3)}}\left(1 + \frac{O(1)}{k}\right)$$

$$i_{6k+3} > \frac{2}{3}\,2^{6k+3}\left(1 - \frac{3}{\sqrt{2\pi(6k+3)}} + o\left(\frac{1}{k}\right)\right) \quad \text{car} \quad \frac{1}{\sqrt{k}}\,\frac{O(1)}{k} = o\left(\frac{1}{k}\right)$$

et finalement, comme $1 - \frac{1}{3}\left(1 + \frac{1}{3n}\right) = \frac{2}{3}\left(1-\frac{1}{6n}\right)$

$$\text{pour } n \geq 3 \quad 1 - \frac{3}{\sqrt{2\pi n}} + o\left(\frac{1}{n}\right) < \frac{3I_n}{2^{n+1}} < 1 - \frac{1}{6n}$$

3.2) Au lieu d'un calcul asymptotique on peut écrire (c.f. calculs annexes 1 et 2) :

$$\sum_{i=0}^{3k+1} C_{2i}^{i} - C_{6k+3}^{3k+1} > \frac{2}{3}\, 2^{6k+3}\sqrt{\frac{2}{\pi(6k+2)}}\left(1+\frac{1}{24(3k+1)}\right) - 2^{6k+3}\sqrt{\frac{2}{\pi(6k+3)}}\left(1-\frac{5}{7(6k+3)}\right)$$

$$> \frac{2^{6k+3}}{3}\sqrt{\frac{2}{\pi(6k+3)}}\left(2+\frac{7}{6(6k+3)} - 3 + \frac{15}{7(6k+3)}\right)$$

$$> -\frac{2^{6k+3}}{3}\sqrt{\frac{2}{\pi(6k+3)}}\left(1-\frac{139}{42(6k+3)}\right)$$

d'où $i_{6k+3} > \frac{2}{3}\, 2^{6k+3}\left(1-\frac{3}{\sqrt{2\pi\,(6k+3)}}\left(1-\frac{139}{42(6k+3)}\right)\right)$

On peut donc affirmer que la conjecture initiale est certainement infirmée au moins pour k vérifiant :

$$\frac{2}{3}\, 2^{6k+3}\left(1 - \frac{3}{\sqrt{2\pi(6k+3)}}\left(1-\frac{139}{4\,(6k+3)}\right)\right) > \frac{5}{8}\; 2^{6k+3}$$

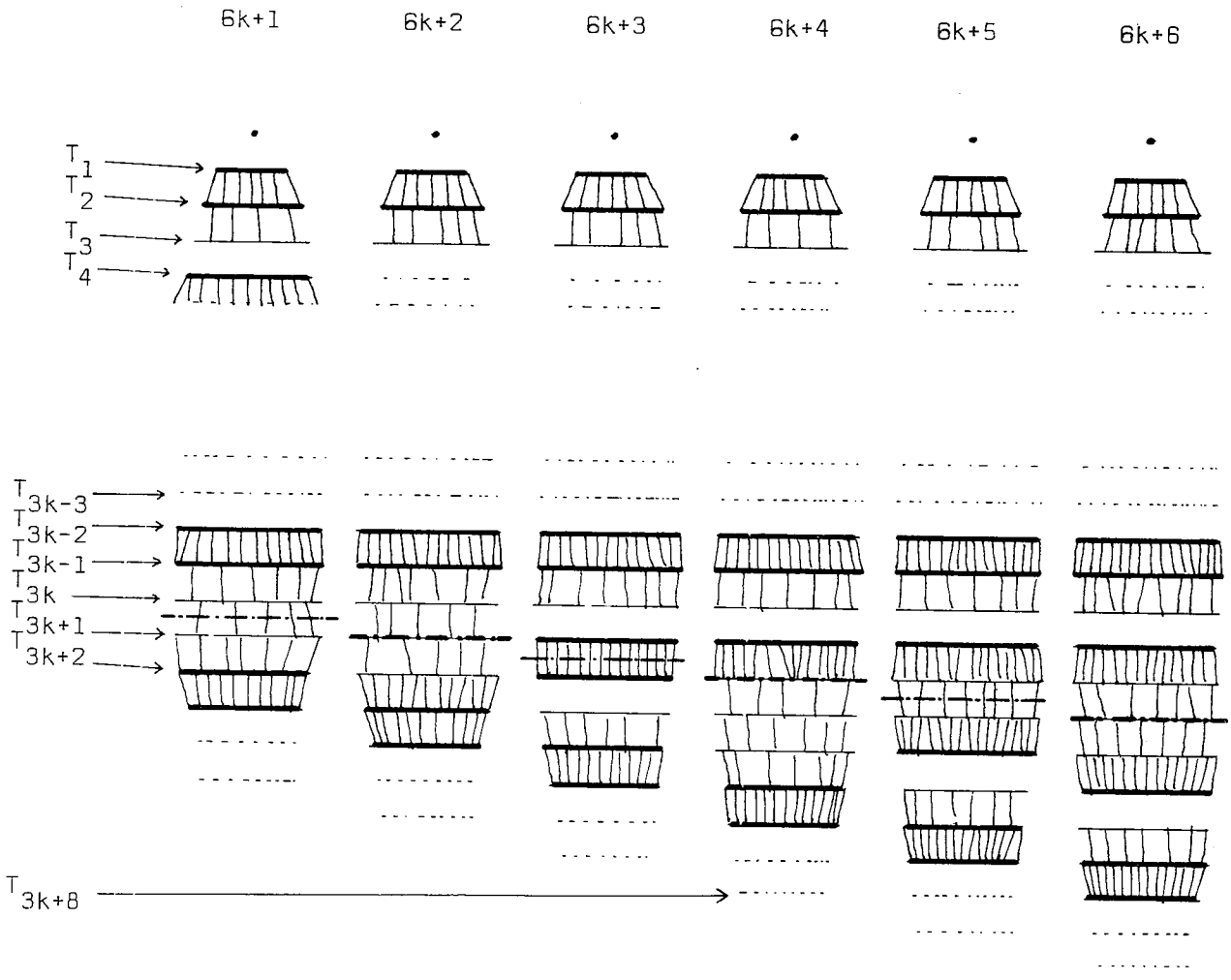
soit $$16 - \frac{48}{\sqrt{2\pi(6k+3)}}\left(1-\frac{139}{42(6k+3)}\right) > 15$$

$$1-\frac{139}{42(6k+3)} < \frac{\sqrt{2\pi(6k+3)}}{48}$$

Or, la plus petite valeur satisfaisant la dernière inégalité est k = 60. La conjecture est au moins infirmée pour n = 363.

3.3) Il ne semble pas facile de démontrer que $\frac{I_n}{2^n}$ soit une fonction croissante (pour autant que cette propriété soit vraie) ; ceci empêche de conclure directement quant à un encadrement du type précédent quelque soit n. On est alors conduit à reprendre le même principe de calcul pour les valeurs de n s'écrivant 6k+1, 6k+2, 6k+4, 6k+5, 6k+6.

Reprenons alors la représentation schématique des couplages:



en ——— les couches T_k saturées

en —·—·— l'hyperplan de symétrie

Le calcul donne alors les minorations suivantes :

$$2(C^{1}_{6k+1}+\ldots+C^{3k+1}_{6k+1}) - 2\,C^{3k+1}_{6k+1} - C^{3k-2}_{6k+1} \leq j_{6k+1}$$

$$m_{6k+1} \leq 2(C^{2}_{6k+1}+\ldots+C^{3k-1}_{6k}) + C^{3k}_{6k}\ ;$$

$$2(C^{1}_{6k+2}+\dots+C^{3k+1}_{6k+2}) - 2\,C^{3k+1}_{6k+2} - C^{3k-2}_{6k+2} \leqslant j_{6k+2}$$

$$m_{6k+2} \leqslant 2(C^{2}_{6k+2}+\dots+C^{3k-1}_{6k}) + C^{3k+1}_{6k} \quad ;$$

$$2(C^{1}_{6k+4}+\dots+C^{3k+1}_{6k+4}) - 2\,C^{3k+1}_{6k+1} \leqslant j_{6k+4}$$

$$m_{6k+4} \leqslant 2(C^{2}_{6k+4}+\dots+C^{3k-1}_{6k+4}) + 2\,C^{3k+1}_{6k} \quad ;$$

$$2(C^{1}_{6k+5}+\dots+C^{3k+1}_{6k+5}) - C^{3k+1}_{6k+5} \leqslant j_{6k+5}$$

$$m_{6k+5} \leqslant 2(C^{2}_{6k+5}+\dots+C^{3k+2}_{6k+5}) \quad ;$$

$$2(C^{1}_{6k+6}+\dots+C^{3k+1}_{6k+6}) - C^{3k+1}_{6k+6} \leqslant j_{6k+6}$$

$$m_{6k+6} \leqslant 2(C^{2}_{6k+6}+\dots+C^{3k+2}_{6k+6}) \quad .$$

Il vient alors, par $i_n = j_n + (2^n - 2m_n)$

$$i_{6k+1} = \frac{2^{6k+1}}{3}\left(1+\underbrace{(2+2)}\sqrt{\frac{2}{\pi(6k+1)}}\ \underbrace{-9}\sqrt{\frac{2}{\pi(6k+1)}}+3-2-2\underbrace{(1+5-3)}\sqrt{\frac{2}{\pi(6k+1)}}+o(\frac{1}{k})\right)$$

et pour les valeurs suivantes, en évaluant les quantités placées au-dessus des $\underbrace{\quad}$:

$$i_{6k+2} = \underbrace{\quad\quad}(2+1)\ \underbrace{\quad\quad}\ -9\ \underbrace{\quad\quad\quad}(1+4-3)\ \underbrace{\quad\quad\quad}$$

$$i_{6k+3} = \underbrace{\quad\quad}(2+0)\ \underbrace{\quad\quad}\ -3\ \underbrace{\quad\quad\quad}(1+3-3)\ \underbrace{\quad\quad\quad}$$

$$i_{6k+4} = \underbrace{\quad\quad}(2-1)\ \underbrace{\quad\quad}\ -6\ \underbrace{\quad\quad\quad}(1+2-0)\ \underbrace{\quad\quad\quad}$$

$$i_{6k+5} = \underbrace{\quad\quad}(2-2)\ \underbrace{\quad\quad}\ -3\ \underbrace{\quad\quad\quad}(1+1-0)\ \underbrace{\quad\quad\quad}$$

$$i_{6k+6} = \underbrace{\quad\quad}(2-3)\ \underbrace{\quad\quad}\ -3\ \underbrace{\quad\quad\quad}(1+0-0)\ \underbrace{\quad\quad\quad}$$

Soit

$$i_{6k+1} = \frac{2}{3}\,2^{6k+1}\left(1 - \frac{11}{2}\sqrt{\frac{2}{\pi(6k+1)}} + o\left(\frac{1}{k}\right)\right)$$

$$i_{6k+2} = \text{——————} - 5 \text{——————}$$

$$i_{6k+3} = \text{——————} - \frac{3}{2} \text{——————}$$

$$i_{6k+4} = \text{——————} - \frac{11}{2} \text{——————}$$

$$i_{6k+5} = \text{——————} - \frac{7}{2} \text{——————}$$

$$i_{6k+6} = \text{——————} - 3 \text{——————}$$

On peut donc affirmer[1]

$$1 - \frac{11}{\sqrt{2\pi n}} + o\left(\frac{1}{n}\right) < \frac{3I_n}{2^{n+1}} < 1 - \frac{1}{6n}$$

4) Sur l'existence d'un couplage à 23 arêtes du cube de dimension 6

Nous rappelons qu'une conséquence de la conjecture C1 serait l'existence d'un tel couplage alors que les seuls couplages connus possèdent 24 arêtes, en particulier ceux fournis par la décomposition (D).

Il faut se rendre compte que ce problème est extrêmement "explosif." En supposant qu'il n'existe que peu de ces couplages et en considérant

---

[1] *Le calcul précédent montre pourquoi nous avions choisi*

$n \equiv 0 \pmod 6$ *pour le calcul de* M_n

et $n \equiv 3 \pmod 6$ *pour le calcul de* I_n.

qu'un couplage est équivalent au choix d'un certain ensemble d'arêtes, on peut considérer que le problème revient à examiner les C_{192}^{23} extrémités d'un certain arbre de choix.

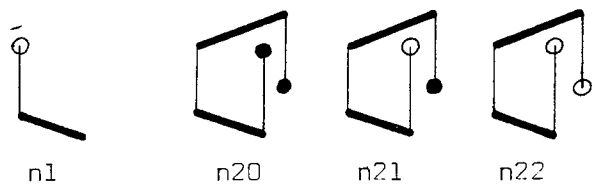
On a $$C_{192}^{23} > \frac{1}{\sqrt{2\pi}} \left(\frac{192}{169}\right)^{169} \left(\frac{192}{23}\right)^{23} \sqrt{\frac{192}{23.169}} > 3.22\ 10^{29} .$$

En examinant plus d'un million de cas à la seconde, il faudrait cependant un temps de 10^{16} années, soit 2 millions de fois l'âge de la terre, ou encore 4000 fois l'âge de la terre en fixant d'office trois arêtes.

En conséquence, il est tout à fait exclu d'espérer conclure, sans utiliser des propriétés réduisant puissamment l'ordre de choix.

4.1) Une propriété des couplages maximaux vérifiant C1.

Soit un couplage maximal du n-cube, nous allons distinguer les arêtes du cube qui ne sont pas dans le couplage. Celles-ci sont, en effet, de deux types, suivant qu'elles touchent le couplage en 1 ou 2 points. Celles du deuxième type peuvant encore se séparer en trois catégories selon le schéma suivant :



○ représente 1 point non touché par le couplage

● représente 1 point touché par le couplage.

(le symbole n_i représentera aussi bien le nom d'un type que son cardinal). Les arêtes parallèles à distance 1, conduisant à des réductions, sont du type n_{20}.

On peut écrire :

$$n_1 + n_{20} + n_{21} + n_{22} = n\times 2^{n-1} - m_n$$ (en décomptant l'ensemble des arêtes) ;

$$n_1 = n(2^n - 2m_n)$$ (en décomptant les points extérieurs au couplage, à l'aide des arêtes du 1er type) ;

$$n_{21} + 2n_{22} = n(2^n - 2m_n)$$ (en décomptant les points extérieurs au couplage à l'aide des arêtes du 2e type).

(C'est la 3° égalité qui traduit la maximalité du couplage).
Il vient, par la combinaison linéaire 2, -2, -1

$$2n_{20} + n_{21} = n\,2^n(1-2-1) + m_n(-2+4n+2n)$$

soit

$$\boxed{2n_{20}+n_{21} = 2((3n-1)m_n - n\,2^n)} \quad (1)^{(1)} .$$

De même, par la combinaison -1, 1, +1

$$\boxed{n_{22} = 3n\,2^{n-1} - (4n-1)m_n + n_{20}} \quad (II) .$$

(I) est intéressante car elle donne en particulier une borne pour n_{20}

$$n_{20} \leq (3n-1)m_n - n\,2^n$$

pour les premières valeurs de n et en admettant C1

---

(1) *Cette quantité devant être positive, on retrouve* $m_n > 2^n \frac{n}{3n-1}$.

n	max n_{20}	min n_{22}	$\left\lceil \frac{\min n_{22}}{3} \right\rceil$
1	0	0	0
2	2	-2 ($\Rightarrow n_{20}=2$)	0
3	0	3	1
4	2	6	2
5	8	12	4
6	7	47	16
7	4		
8	22		
9	20		
10	26		
11	0		
12	23		

On établit ainsi la propriété

$$M_n = \left\lceil 2^n \frac{n}{3n-1} \right\rceil \Rightarrow I_n = 2^n \frac{2n-1}{3n-1} - 3\theta n \quad \text{avec} \quad \theta \in [0,1[$$

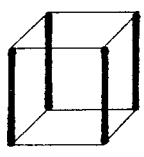
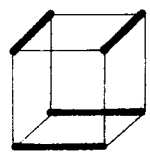
On démontre aussi qu'une solution possède au plus,

en dimension 4, 1 carré (2 arêtes parallèles à distance 1)

en dimension 5, 4 carrés

en dimension 6, 3 carrés.

En dimension 6, un couplage à 23 arêtes ne peut donc contenir un sous-couplage parfait du cube

 ou  , qui nécessite au moins 8 arêtes du type n_{20} .

(II) fournit des indications sur la présence dans un couplage de " $\frac{1}{2}$ tours du cube", ou plutôt de sous-couplage du cube selon le couplage minimal du 3cube :

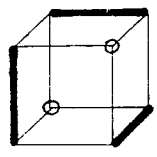


figure x .

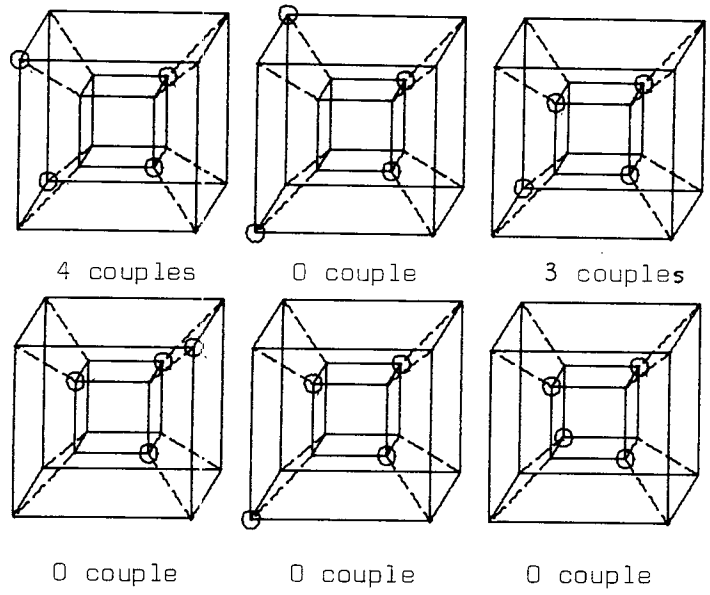
En effet, la présence d'un tel couplage nécessite que l'application canonique des arêtes de type n_{22}, sur les couples de points à distance 3, extérieurs au couplage, ne soit pas injective.

On en déduit une borne inférieure $\left\lceil \min \frac{n_{22}}{3} \right\rceil$ du nombre de couples de points à distance 3 du complémentaire d'un couplage (contrainte CT).

De même l'absence de la configuration de la figure x dans un couplage, implique la présence d'au moins min n_{22} couples à distance trois dans son complémentaire.

En dimension 4, on peut facilement décompter le nombre maximum de couples à distance 3 des différents types de 4-stables (au nombre de 6):

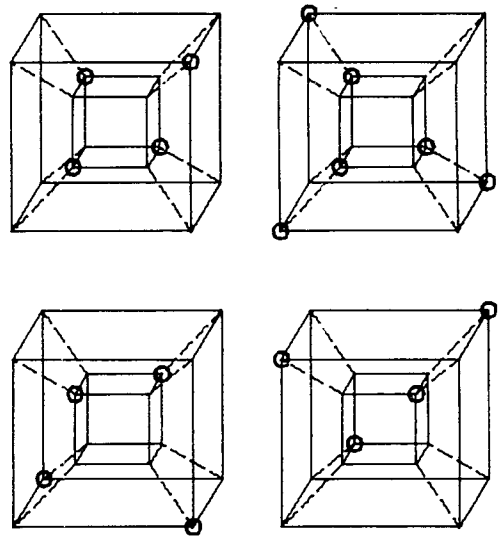
Nombre de couples de points à distance 3 des différents stables .



Ce nombre vaut $4 < 6$: un couplage minimal du 4-cube admet donc au moins une configuration du type de la figure x.(Ce résultat , vrai aussi en dimension 3, mais c'est alors évident, ne l'était pas tout à fait en dimension 4).

En dimension 5, on ne peut pas établir un tel résultat ; et, pour cause, comme le montrera la fin du chapitre .

En dimension 6, il existe "malheureusement" un (et, du reste, un seul) 18-stable du 6-cube, possédant au moins 47 (ici 48) couples de points à distance 3, ce qui empêche, du moins à ce niveau, de conclure sur la nécessité de la présence d'une configuration du type de la figure dans un 23-couplage.



Stable de 18 points du cube de dimension 6
présentant 48 couples de points à distance 3.

4.2) Un programme de recherche des couplages minimaux

L'étude précédente permet d'écrire un programme d'ordinateur, recherchant exhaustivement les couplages à 23 arêtes du 6-cube.

On emploie une méthode de back-tracking ; l'exploration de l'arbre de choix étant interrompue, soit quand la quantité $2n_{20}+n_{21}$ atteint la valeur 14, soit après le choix d'une 20^{e} arête.

Remarque : on ne construit pas les couplages décomposables, où l'on appelle décomposable, un couplage du n-cube, qui est l'union de deux couplages du n-1-cube. En dimension 3, le $\frac{1}{2}$ tour du cube est indécomposable; en dimension 4, les couplages sont tous décomposables.

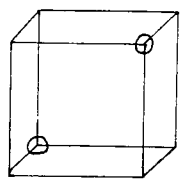
Ce programme a effectivement été écrit, malheureusement l'évolution du calcul, au début de l'exécution, ne permet pas d'envisager son déroulement complet en moins de plusieurs milliers d'heures !

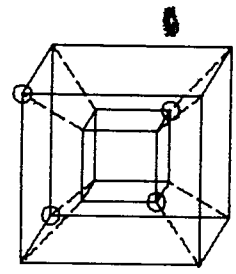
Il est bien évident que l'échec d'un tel programme provient, pour l'essentiel, de la grande symétrie du n-cube, alors que le programme n'élimine pas les différentes constructions isomorphes qu'il génère.

4.3) Introduction du stable complémentaire d'un couplage

Pour prendre en compte la notion d'isomorphisme, un moyen détourné consiste, puisque le complémentaire d'un couplage est un stable, à déterminer l'ensemble des types[1] de couplages à 2^n-2m_n points, et ensuite, pour chaque type, à tenter de construire un couplage dont on connaît le complémentaire en tenant compte des mêmes principes que plus haut.

On aurait pu espérer que le stable complémentaire d'un couplage minimal soit un stable maximal, comme c'est le cas en dimension 3 et 4:

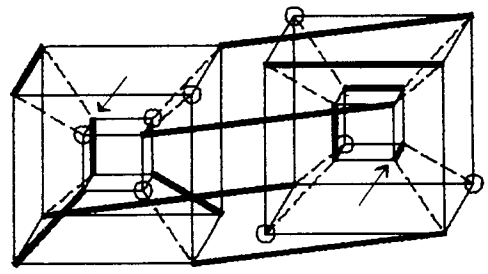




---

[1] *2 stables sont du même type s'il existe un isomorphisme de HC_n appliquant l'un sur l'autre.*

En dimension 5 il existe, en revanche, un contre-exemple:

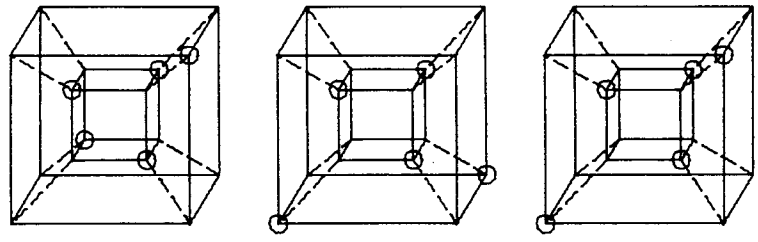


couplage minimal (12 arêtes) dont le complémentaire n'est pas un stable maximal (points marqués d'une flèche).

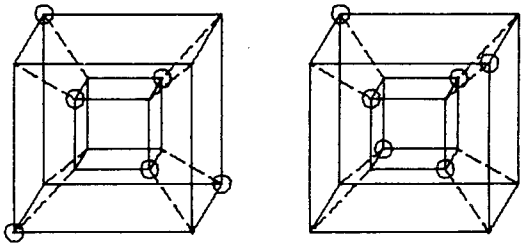
Pour déterminer les stables à 18 points du 6-cube, on remarque que le 6-cube doit contenir un stable du 5-cube à, au moins, 9 points, lui-même contenant un stable du 4-cube à, au moins, 5 points.

Ces derniers sont, en type[1] , au nombre de 7 dont

3 de 5 points :



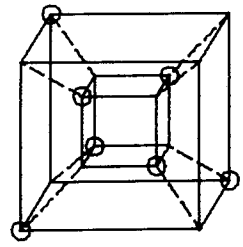
2 de 6 points :



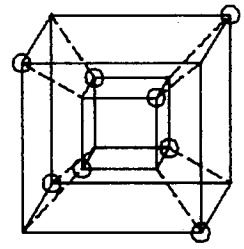
---

[1] *Pour cela, on peut consulter un catalogue des types de fonction booléenne à 4 variables. (voir l' Annexe)*

1 de 7 points :



et 1 de 8 points :



Un premier programme détermine combinatoirement en partant successivement de chacun des sept types de stables à au moins cinq points, les stables du 5-cube à au moins 9 points:

4.4) Résultats

On peut donner le tableau statistique suivant :

		Nombre total de points du stable du 5-cube								
nombre de stables contenant des stables du 4-cube d' au plus p points		9	10	11	12	13	14	15	16	
	5	12(51)	1							
	6	24(89)	19(110)	5(36)	2(5)					
	7	11(32)	18(62)	20(79)	12(41)	4(10)				
	8	1	2	2	4	2	2	1	1	
Total		48	40	27	18	6	2	1	1	143

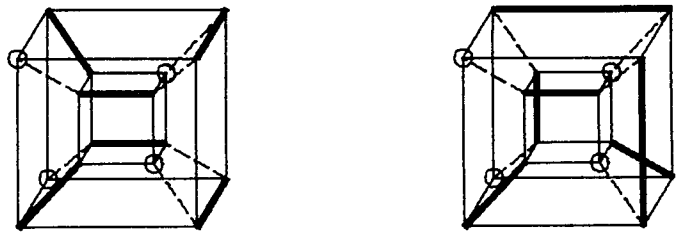
Répartition cardinale des types de stables du 5-cube à au moins 9 points (entre ( ) sont indiqués les nombres avant réduction par isomorphisme).

Un deuxième programme très semblable au premier détermine alors les stables à 18 points du 6-cube, satisfaisant à la contrainte (CT)[1]. Ces stables sont alors fournis en données à un troisième programme qui tente de construire un couplage dans le complémentaire de chacun des stables.

Le résultat définitif est le suivant, obtenu pour un total de calcul d'une vingtaine de minutes sur un programme de 2200 cartes, (FORTRAN IBM 360):

Il n'existe pas de couplage du 6-cube, à 23 arêtes.

En dimension 4, le programme retrouve les 2 types de couplages, que l'on pouvait facilement obtenir "à la main", et qui correspondent au même 4-stable :



2 types de 6-couplage du 4-cube, décomposables et de même type réduit (cf. plus loin).

---

[1] *Ces stables, nombreux, sont pourtant difficiles à fabriquer "à la main".*

4.5) Résultats en dimension 5 - Notion de type réduit de couplage indécomposable

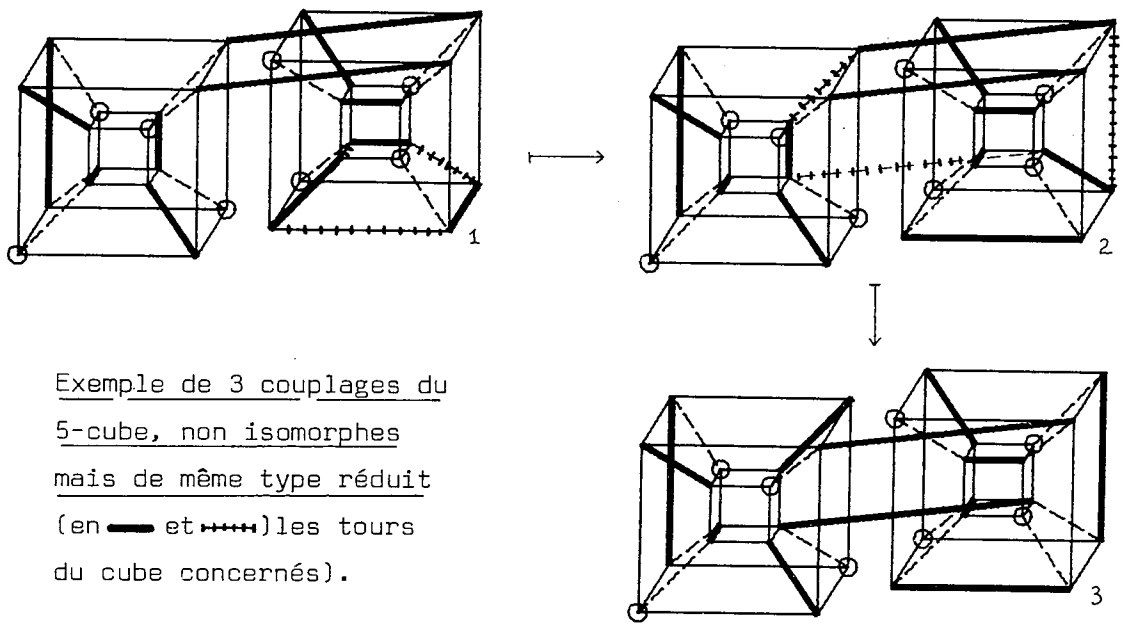
En dimension 5, le programme de génération des stables fournit 61 stables vérifiant la contrainte (CT), que l'on réduit, par isomorphisme, à 17.

Le programme de génération des couplages fournit, pour quatre d'entre eux, respectivement 56, 80, 60 et 60 couplages indécomposables.

Chacun de ces ensembles de solutions est alors divisé par l'équivalence relative à l'isomorphisme, après détermination du groupe d'automorphisme de chacun des stables. On obtient ainsi, respectivement, 16, 7, 7 et 9 types de couplages.

Introduisons enfin la notion de "type réduit" de couplage. Deux couplages sont de même type réduit, si l'on peut passer de l'un à l'autre par une suite (finie, évidemment) de permutations selon des $\frac{1}{2}$ tours du cube, consistant à échanger un $\frac{1}{2}$ tour du cube avec son complémentaire.

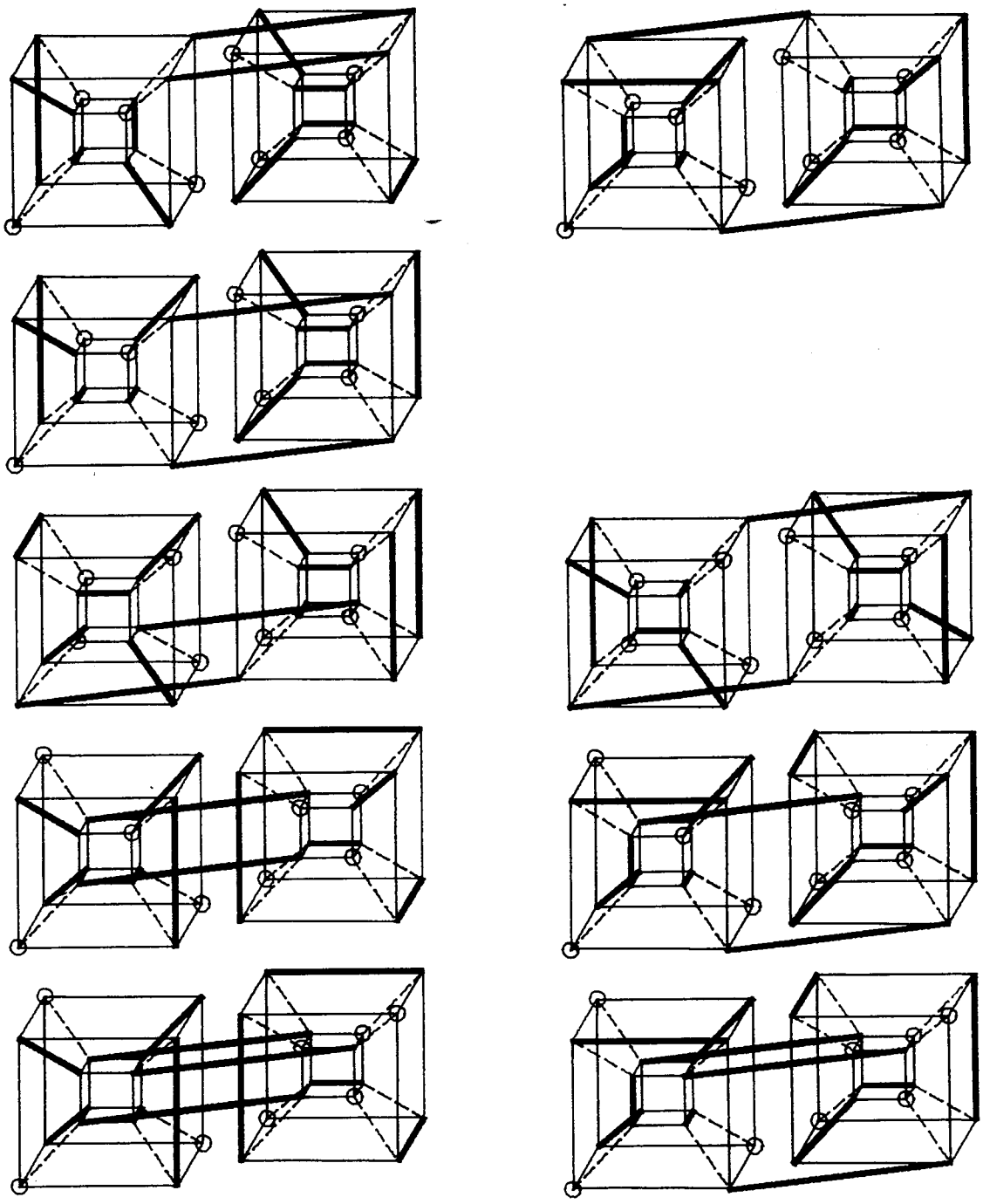
Echange de deux $\frac{1}{2}$ tours du cube complémentaires.



Exemple de 3 couplages du 5-cube, non isomorphes mais de même type réduit (en ▬ et ┅ les tours du cube concernés).

Il est immédiat que cette relation est une relation d'équivalence, stable pour la notion d'indécomposabilité.

Si l'on divise à nouveau l'ensemble des types de couplages par cette relation, on obtient 3, 2, 2 et 2 types réduits, soit au total 9 types réduits, de couplages indécomposables (cf. calcul annexe 4) :



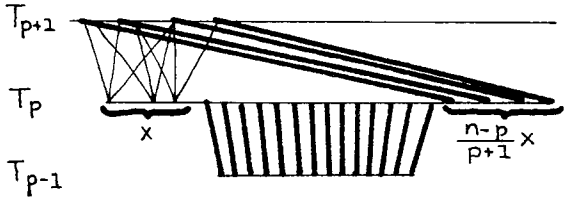
Ce faible nombre (9) montre sans doute qu'il n'est pas étonnant de ne pas avoir trouvé de solution au problème du 23-couplage du 6-cube. On constate, d'autre part, qu'il existe en dimension 5, quatre 12-couplages ne contenant pas de $\frac{1}{2}$ tour du cube (et donc, nécessairement, indécomposables).

5) Sur la possibilité de resserrer l'encadrement

$$1+\frac{1}{3n} < \frac{3M_n}{2^n} < 1+\sqrt{\frac{2}{\pi n}} + o\left(\frac{1}{\sqrt{n}}\right) \qquad \text{(III)}$$

5.1) On rappelle qu'un couplage repose sur la construction d'un couplage d'un $T_{p-1 (p\geqslant 1)}$ vers T_p, puis la saturation des points de T_p par des arêtes reliant T_p à T_{p+1}.

Pour décompter les arêtes du couplage, on a alors majoré le nombre de points de T_p atteints par des arêtes du couplage, par le cardinal de T_p. En fait, on peut certainement "s'arranger" pour ne pas couvrir tous les points de T_p. Nous allons déterminer le minimum des points couverts de T_p par un couplage



Soit x le nombre de points de T_p non couverts. Les images de ces points (par la relation du graphe) doivent être couvertes ; on peut donc écrire

$$x + \frac{n-p}{p+1}x + C_n^{p-1} \leqslant C_n^p$$

en remarquant que les demi-degrés extérieur et intérieur[1] des points de T_p sont n-p et p.

Il vient alors

$$C_n^p - x \geqslant C_n^p \left(1-(1-\frac{C_n^{p-1}}{C_n^p})\frac{p+1}{n+1} \right) = C_n^p \left(1-(1-\frac{p}{n-p+1})\frac{p+1}{n+1} \right)$$

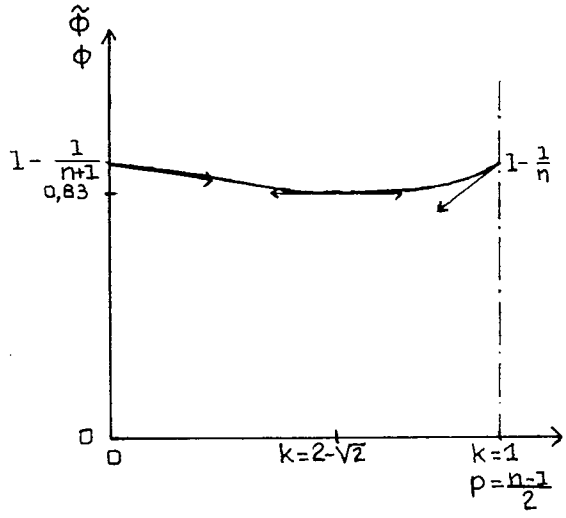
La construction la plus avantageuse conduirait donc à remplacer dans le calcul de m_n chacun des

$$C_n^p \quad \text{par} \quad C_n^p \, \phi_n(p) \quad \text{où} \quad \phi_n(p) = 1-\frac{(n-2p+1)(p+1)}{(n-p+1)(n+1)}$$

---

[1] *Pour une orientation du graphe suivant les distances à l'origine, croissantes.*

5.2) Etude du gain qu'il est ainsi possible de réaliser



Posons $p=\frac{kn}{2}$ $\qquad k \in [0,1[$

$$\tilde{\phi}_n(k)=\phi_n(p)=1-\frac{(1-k+\frac{1}{n})(\frac{k}{2}+\frac{1}{n})}{(1-\frac{k}{2}+\frac{1}{n})(1+\frac{1}{n})}$$

au voisinage de 0 il vient :

$$\tilde{\phi}_n(k) = 1-\frac{1}{n}-\frac{k}{2}+o(\frac{1}{n})+o(k)$$

et au voisinage de 1 :

$$\tilde{\phi}_n(1-u) = 1-\frac{1}{n}-u+o(\frac{1}{n})+\frac{2u^2}{1+u}.$$

Au voisinage de ∞ (pour n), $\tilde{\phi}$ admet une tangente horizontale pour

$\frac{d}{dk}\frac{(1-k)k}{(1-\frac{k}{2})} = 0$ soit $(1-2k)(1-\frac{k}{2})+(1-k)\frac{k}{2}=0$ et donc $k^2-4k+2=0$

et finalement $k = 2-\sqrt{2}$; et l'on a $\tilde{\phi}_n(2-\sqrt{2}) \sim 2(\sqrt{2}-1) \simeq 0,8284$.

Nous allons chercher une approximation de

$$K = \frac{C_{6k}^2\,\phi_{6k}(2)+C_{6k}^5\,\phi_{6k}(5)+\ldots\ldots+C_{6k}^{3k-1}\,\phi_{6k}(3k-1)}{C_{6k}^2+C_{6k}^5+\ldots\ldots+C_{6k}^{3k-1}}\ .$$

5.3) Par une méthode[1] qui rappelle l'approximation de la fonction de répartition de la loi normale par celle d'une loi binômiale, on montre que

$$K = 1-\sqrt{\frac{2}{\pi 6k}}+0(\frac{1}{k})\ .$$

---

[1] *cf. calcul annexe 3 .*

On obtient alors pour les couplages du type (T)

$$\frac{3m_n}{2^n} < \left(1+\sqrt{\frac{2}{\pi n}} + \left(\frac{1}{n}\right)\right)\left(1-\sqrt{\frac{2}{\pi n}} + O\left(\frac{1}{n}\right)\right)$$

soit $$\frac{3m_n}{2^n} < 1 + O\left(\frac{1}{n}\right)$$

Ce résultat, éliminant remarquablement la quantité $\sqrt{\frac{2}{\pi n}}$, permet d'envisager la construction d'un couplage du type (T) assurant la conjecture

$$\boxed{\frac{3M_n}{2^n} = 1 + \frac{1}{3n} + o\left(\frac{1}{n}\right)}$$

proposée en remplacement de celle de Forcade et qui correspond, en ce qui concerne les fonctions irréductibles, à

$$\frac{3I_n}{2^{n+1}} = 1 - \frac{1}{6n} + o\left(\frac{1}{n}\right)$$

ANNEXE

DU CHAPITRE II

1) Une évaluation de $u_n = \sum_{i=o}^{n} C_{2n}^{n}$

2) Une majoration de C_{6k+3}^{3k+1}

3) Une évaluation de $K = \dfrac{C_{6k}^{2}\phi_{6k}(2)+C_{6k}^{5}\phi_{6k}(5)+\ldots.+C_{6k}^{3k-1}\phi_{6k}(3k-1)}{C_{6k}^{2} + C_{6k}^{5} +\ldots.+C_{6k}^{3k-1}}$

4) Sur les groupes d'automorphismes de 4 stables du 5-cube.

1) Une évaluation de $u_n = \sum_{i=o}^{n} C_{2n}^n$

Evaluons d'abord C_{2n}^n à l'aide de la formule de Stirling

$$n! = \left(\frac{n}{e}\right)^n \sqrt{2\pi n}\left(1+\frac{1}{12n}+\varepsilon\right) \qquad 0<\varepsilon<\frac{1}{288n^2}$$

Il vient

$$C_{2n}^n = \frac{(2n)!}{(n!)^2} = \frac{\left(\frac{2n}{e}\right)^{2n}}{\left(\frac{n}{e}\right)^{2n}} \frac{\sqrt{2\pi 2n}}{2\pi n} \frac{1+\frac{1}{24n}+\varepsilon_1}{\left(1+\frac{1}{12n}+\varepsilon_2\right)^2} = \frac{4^n}{\sqrt{\pi n}} K \begin{cases} 0<\varepsilon_1<\frac{1}{288\times 4n^2} \\ 0<\varepsilon_2<\frac{1}{288n^2} \end{cases}$$

où

$$\left(1+\frac{1}{24n}\right)\left(1+\frac{1}{12n}+\frac{1}{288n^2}\right)^{-2} < K < \left(1+\frac{1}{24n}+\varepsilon_1\right)\left(1-\frac{1}{12n}+\frac{1}{144n^2}\right)^2 ;$$

or

$$\frac{1}{\left(1+\frac{1}{12n}+\frac{1}{288n^2}\right)^2} > 1-\frac{1}{6n}+\frac{1}{144n^2} ,$$

d'où

$$1-\frac{1}{8n} < K < \left(1+\frac{1}{24n}+\frac{1}{4\times 288n^2}\right)\left(1-\frac{1}{6n}+\frac{1}{48n^2}-\frac{1}{144n^3}\left(\frac{1}{6}+\frac{1}{144n}\right)\right) ;$$

soit

$$1-\frac{1}{8n} < K < 1-\frac{1}{8n}+\frac{1}{n^2}\left(\frac{1}{4\times 288}-\frac{1}{6\times 24}+\frac{1}{48}\right)-\varepsilon_3 \quad \text{avec } \varepsilon_3 > 0 .$$

Finalement

$$\forall\, n \geqslant 1 \quad C_{2n}^n = \frac{4^n}{\sqrt{\pi n}}\left(1-\frac{1}{8n}+\varepsilon\right) \quad 0 < n^2\varepsilon < \frac{17}{9\times 128} < \frac{1}{64}$$

Remargue - Le calcul asymptotique conduirait, en ce qui concerne le terme en $\frac{1}{n^2}$ à $\frac{1}{128n^2}$. On montre, d'autre part, que le facteur $\frac{17}{9\times 128}$ est le meilleur possible si l'on ne suppose rien de plus sur ε_1 et ε_2.

Pour évaluer u_n nous allons déterminer deux suites décroissantes : k_n et k'_n, vérifiant

$$k_n < \frac{\sqrt{n}}{4^n} u_n < k'_n \qquad (1)$$

On peut écrire :

$$k_n \frac{4^n}{\sqrt{\pi n}} + \frac{4^{n+1}}{\sqrt{\pi(n+1)}}\left(1 - \frac{1}{8(n+1)}\right) < u_{n+1} = u_n + C_{2n+2}^{n+1} < k'_n \frac{4^n}{\sqrt{n}} + \frac{4^{n+1}}{\sqrt{\pi(n+1)}}\left(1 - \frac{1}{8(n+1)} + \frac{1}{28(n+1)^2}\right).$$

Pour assurer (1), il est donc suffisant que

$$k_{n+1} \leqslant \frac{k_{n+1}}{4}\sqrt{\frac{n+1}{n}} + \frac{1 - \frac{1}{8n+1}}{\sqrt{\pi}} < \frac{\sqrt{n+1}}{4^{n+1}} u_{n+1} < \frac{k'_n}{4}\sqrt{\frac{n+1}{n}} + \frac{1 - \frac{1}{8(n+1)} + \frac{1}{28(n+1)^2}}{\sqrt{\pi}} \leqslant k'_{n+1}.$$

La première inégalité donne

$$4 \leqslant \sqrt{\frac{n+1}{n}} + 4\,\frac{1 - \frac{1}{8(n+1)}}{k_{n+1}\sqrt{\pi}} \quad \text{et comme} \quad \sqrt{1+\frac{1}{n}} > 1 + \frac{1}{2n} - \frac{1}{8n^2}$$

$$\text{et} \quad \frac{1}{1+\frac{1}{n}} < 1 - \frac{1}{n} + \frac{1}{n^2}$$

il vient :

$$k_{n+1} \leqslant \frac{4\left(1 - \frac{1}{8n} + \frac{1}{8n^2} - \frac{1}{8n^3}\right)}{3\sqrt{\pi}\left(1 - \frac{1}{6n} + \frac{1}{24n^2}\right)}$$

$$k_{n+1} \leqslant \frac{4}{3\sqrt{\pi}}\left(1 - \frac{1}{8n} + \frac{1}{6n} + \frac{1}{8n^2} - \frac{1}{24n^2} - \frac{1}{8n^3}\right)$$

soit

$$k_n \leqslant \frac{4}{3\sqrt{\pi}}\left(1 + \frac{1}{24n}\right) \quad \text{pour} \quad n \geqslant 4 \quad \text{puisque, alors} \quad \frac{1}{12n^2} > \frac{1}{8n^3} + \frac{1}{24(n+1)n}$$

La dernière inégalité, de même, permet d'écrire

$$4 \geqslant \sqrt{\frac{n+1}{n}} + 4\,\frac{1 - \frac{1}{8(n+1)} + \frac{1}{28(n+1)^2}}{k'_n\sqrt{\pi}} \quad \text{et comme} \quad \sqrt{1+\frac{1}{n}} < 1 + \frac{1}{2n} \text{ et } \frac{1}{n+1} > \frac{1}{n} - \frac{1}{n^2}$$

$$4 \geqslant 1+\frac{1}{2n}+\frac{4\left(1-\frac{1}{8n}+\frac{1}{8n^2}+\frac{1}{28n^2}\right)}{k'_n\sqrt{\pi}}$$

$$k'_n \geqslant \frac{4}{3\sqrt{\pi}}\,\frac{1-\frac{1}{8n}+\frac{1}{6n^2}}{1-\frac{1}{6n}}$$

$$k'_n \geqslant \frac{4}{3\sqrt{\pi}}\left(1-\frac{1}{8n}+\frac{1}{6n^2}\right)\left(1+\frac{1}{6n}+\frac{1\times 12}{36n^2\times 11}\right)$$

$$k'_n \geqslant \frac{4}{3\sqrt{\pi}}\left(1+\frac{1}{24n}+\frac{1}{6n^2}+\frac{1}{33n^2}-\frac{1}{48n^2}-\frac{1}{8\times 33n^3}+\frac{1}{36n^3}+\frac{1}{6\times 33n^4}\right)$$

$$k'_n \geqslant \frac{4}{3\sqrt{\pi}}\left(1+\frac{1}{24n}+\frac{1}{n^2}\left(\frac{1}{6}+\frac{1}{33}-\frac{1}{48}+\frac{7}{8\times 36\times 2}+\frac{1}{24\times 33}\right)\right)$$

soit $$k'_n \geqslant \frac{4}{3\sqrt{\pi}}\left(1+\frac{1}{24n}+\frac{1}{5n^2}\right) .$$

Finalement on peut écrire :

$$\text{pour } n \geqslant 9 \quad C_0^0+C_2^1+\ldots+C_{2n}^n = \frac{4^{n+1}}{3\sqrt{\pi n}}\left(1+\frac{1}{24n}+\varepsilon\right) \text{ avec } 0<\varepsilon<\frac{1}{5n^2} ,$$

car, à partir de n=9 :

$$\left(1+\frac{1}{24n}+\frac{1}{5n^2}\right)\sqrt{\frac{n+1}{n}}+3\left(1-\frac{1}{8(n+1)}+\frac{1}{64(n+1)^2}\right) \leqslant 4\left(1+\frac{1}{24(n+1)}+\frac{1}{5(n+1)^2}\right) .$$

Remarque - La valeur asymptotique correspond à $\frac{59}{384} < \frac{1}{5}$.

2) Détermination d'un majorant de C_{6k+3}^{3k+1}

$$C_{6k+3}^{3k+1} = \frac{\left(\frac{6k+3}{e}\right)^{6k+3}}{\left(\frac{3k+1}{e}\right)^{3k+1}\left(\frac{3k+2}{e}\right)^{3k+2}} \frac{\sqrt{2\pi(6k+3)}}{\sqrt{2\pi(3k+1)2\pi(3k+2)}} \frac{\left(1+\frac{1}{12(6k+3)}+\varepsilon_3\right)}{\left(1+\frac{1}{12(3k+1)}+\varepsilon_1\right)\left(1+\frac{1}{12(3k+2)}+\varepsilon_1\right)}$$

avec $\quad 0 < \varepsilon_i < \frac{1}{288(6k+i)^2}$

On obtient :

$$C_{6k+3}^{3k+1} < \frac{(6k+3)^{6k+3}}{(3k+1)^{3k+1}(3k+2)^{3k+2}\sqrt{2\pi}} \sqrt{\frac{6k+3}{(3k+1)(3k+2)}} \frac{1+\frac{1}{12(6k+3)}+\frac{1}{288(6k+3)^2}}{\left(1+\frac{1}{12(3k+1)}\right)\left(1+\frac{1}{12(3k+2)}\right)}$$

$$< \frac{1}{2\pi(6k+3)} \frac{1}{\left(\frac{3k+1}{6k+3}\right)^{3k+\frac{3}{2}}} \frac{1}{\left(\frac{3k+2}{6k+3}\right)^{3k+\frac{5}{2}}} \times B = 2^{6k+3}\sqrt{\frac{2}{\pi(6k+3)}} \times A \times B ,$$

où $\quad A = \frac{1}{\left(1-\frac{1}{6k+3}\right)^{3k+\frac{3}{2}}} \times \frac{1}{\left(1+\frac{1}{6k+3}\right)^{3k+\frac{5}{2}}}$ et $\quad B = \frac{1+\frac{1}{12(6k+3)}+\frac{1}{288(6k+3)^2}}{\left(1+\frac{1}{12(3k+1}\right)\left(1+\frac{1}{12(3k+2)}\right)}$;

pour $k \geq 3$: $\quad \ell nB = \frac{6k+3}{2}\ell n\left(1-\frac{1}{6k+3}\right) - \frac{6k+3}{2}\ell n\left(1+\frac{1}{6k+3}\right) - \ell n\left(1+\frac{1}{6k+3}\right)$

$$\ell nB < \frac{6k+3}{2}\left(\frac{1}{(6k+3)^2}+\frac{1}{2(6k+3)^4}\frac{1}{1-\frac{1}{(6k+3)^2}}\right) - \frac{1}{6k+3}+\frac{1}{2(6k+3)^2}$$

$$< -\frac{1}{2(6k+3)}+\frac{1}{2(6k+3)^2}\left(1+\frac{1}{42}\frac{21^2}{21^2-1}\right) ;$$

et par $e^x < 1 + x + \frac{x^2}{2}\frac{1}{1-\frac{x}{3}}$:

$$B < 1-\frac{1}{2(6k+3)}+\frac{1}{2(6k+3)^2}\times\frac{41}{40}+\frac{1}{2\times4(6k+3)^2}\times\underbrace{\frac{1}{1+\frac{1}{6(6k+3)}-\frac{1}{6(6k+3)^2}\frac{41}{40}}}_{>1}$$

$$B < 1-\frac{1}{2(6k+3)}+\frac{1}{(6k+3)^2}\frac{51}{80} .$$

En posant $n = 6k+3$ (pour $n \geqslant 21$) :

- $$\frac{1}{1+\frac{1}{12(3k+1)}} < \frac{1}{1+\frac{1}{6(6k+3)}\left(1+\frac{1}{6k+3}\right)} < 1-\frac{1}{6n}-\frac{1}{6n^2}+\frac{1}{6^2n^2}\left(1+\frac{1}{n}\right)^2$$

$$\leqslant 1-\frac{1}{6n}-\frac{5}{6^2n^2}+\frac{2}{6^2n^2}+\frac{1}{6^2n^4} < 1-\frac{1}{6n}-\frac{4,9}{36n^2} \quad ;$$

- $$\frac{1}{1+\frac{1}{12(3k+2)}} < \frac{1}{1+\frac{1}{6n}\left(1-\frac{1}{n}\right)} < 1-\frac{1}{6n}+\frac{1}{6n^2}+\left(\frac{1}{6n}-\frac{1}{6n^2}\right)^2$$

$$< 1-\frac{1}{6n}+\frac{7}{36n^2}-\frac{2}{36n^3}+\frac{1}{36n^4} < 1-\frac{1}{6n}+\frac{7}{36n^2} \quad ;$$

soit

$$A < \left(1+\frac{1}{12n}+\frac{1}{288n^2}\right)\left(1-\frac{1}{3n}+\frac{1}{n^2}\left(-\frac{4,9}{36}+\frac{7}{36}+\frac{1}{36}\right)+\frac{1}{n^3}\left(\frac{4,9}{6^3}-\frac{7}{6^3}\right)-\frac{1}{n^4}\,\frac{7\times 4,9}{64}\right)$$

$$< \left(1+\frac{1}{12n}+\frac{1}{288n^2}\right)\left(1-\frac{1}{3n}+\frac{3,1}{36n^2}\right) < 1-\frac{1}{4n}+\frac{0,0621}{n^2} \quad ;$$

enfin :

$$AB < 1-\frac{3}{4n}+\frac{1}{n^2}\left(0,0621+\frac{51}{80}+\frac{1}{8}\right)+\frac{1}{n^3}\left(-\frac{51}{320}-\frac{0,0621}{2}\right)+\frac{1}{n^4}\,\frac{51\times 0,0621}{80}$$

$$AB < 1-\frac{3}{4n}+\frac{1}{n^2}\left(0,0621+\frac{61}{80}\right) < 1-\frac{3}{4n}+\frac{1}{n^2}\,0,825 \quad ;$$

or

$$-\frac{3}{4}+\frac{0,825}{n} < -\frac{5}{7} \iff -21n + 28 \times 0,825 < -20n$$

soit $n > 23,1$;

ce qui établit, quitte à vérifier

$$C_{21}^{10} = 352716 < 352720 < 2^{21}\sqrt{\frac{2}{\pi\times 21}}\left(1-\frac{5}{7\times 21}\right) :$$

$$\boxed{\forall k \geqslant 3 \quad C_{6k+3}^{3k+1} < 2^{6k+3}\sqrt{\frac{2}{\pi(6k+3)}}\left(1-\frac{5}{7(6k+3)}\right)} \quad .$$

Remarque - la valeur asymptotique correspond à $\frac{3}{4}$ au lieu de $\frac{5}{7}$.

3) Evaluation de $K = \dfrac{C_{6k}^{2}\phi_{6k}(2)+C_{6k}^{5}{}_{6k}(5)+\ldots.+C_{6k}^{3k-1}\phi_{6k}(3k-1)}{C_{6k}^{2} + C_{6k}^{5} +\ldots.+ C_{6k}^{3k-1}}$

En prolongeant C_n^p défini sur $I \subset \mathbb{N}$ par $C_n^x = \dfrac{\Gamma(n+1)}{\Gamma(x+1)\Gamma(n-x+1)}$ défini sur $[0,n] \subset \mathbb{R}$

considérons

$$C_n^{\frac{n}{2}(1-\frac{1}{\ln n})} = \frac{(\frac{n}{e})^n \sqrt{2\pi n}}{\left(\frac{n}{2e}(1-\frac{1}{\ln n})\right)^{\frac{n}{2}(1-\frac{1}{\ln n})}\left(\frac{n}{2e}(1+\frac{1}{\ln n})\right)^{\frac{n}{2}(1+\frac{1}{\ln n})}\sqrt{2\pi\frac{n}{2}(1-\frac{1}{\ln n})2\pi\frac{n}{2}(1+\frac{1}{\ln n})}}$$

$$\sim \frac{2^{n+1}}{\sqrt{2\pi n}}\,\frac{1}{A}$$

où $A = (1-\frac{1}{\ln n})^{\frac{n}{2}(1-\frac{1}{\ln n})}(1+\frac{1}{\ln n})^{\frac{n}{2}(1+\frac{1}{\ln n})}$.

$$\ln A = \frac{n}{2}\frac{1}{\ln n}\left(-1-\frac{1}{2\ln n}+\frac{1}{\ln n}+1-\frac{1}{2\ln n}+\frac{1}{\ln n}+o(\frac{1}{\ln n})\right)$$

$$= \frac{n}{2}\frac{1}{\ln n}\left(1+o(1)\right)$$

d'où

$$\boxed{\forall r \geq 0 \quad \frac{\sqrt{2\pi n}}{2^{n+1}}\,C_n^{\frac{n}{2}(1-\frac{1}{\ln n})} = o(\frac{1}{n^r})} \qquad (1)$$

(1) permet donc d'écrire

$$\forall r \geq 0 \quad K = \frac{\sum_{i=\lfloor 3k(1-\frac{1}{\ln 6k})\rfloor}^{3k-1} C_{6k}^{i}\,\phi_{6k}(i)}{\sum_{i=\lfloor 3k(1-\frac{1}{\ln 6k})\rfloor}^{3k-1} C_{6k}^{i}}\left(1+o(\frac{1}{k^r})\right) \qquad (2)$$

Or, dans le calcul de $2(C_{6k}^{2}+\dots.C_{6k}^{3k-1}) = \frac{2^{6k}}{3}\left(1+\sqrt{\frac{2}{\pi 6k}} + o(\frac{1}{k})\right)$

et de $2(C_{6k-1}^{2}+\dots.+C_{6k-1}^{3k-1}) = \frac{2^{6k-1}}{3}\left(1+2\sqrt{\frac{2}{\pi(6k-1)}} + o(\frac{1}{k})\right)$

on peut interpréter le remplacement de l'indice 6k par l'indice 6k-1 comme la multiplication de

C_{6k}^{P} par $(1-\frac{P}{6k})$ pour obtenir C_{6k-1}^{P} .

En posant $1-u = \frac{2P}{6k}$ il vient $1-\frac{P}{6k} = 1-\frac{1}{2}+\frac{u}{2} = \frac{1}{2}(1+u)$;

d'où, finalement, l'apparition d'une "fonction de correction" :

$\phi'(1-u) = \frac{1}{2}(1+u)$, alors que dans le problème initial

$\tilde{\phi}_n(1-u) = 1 - \frac{1}{n} + o(\frac{1}{n}) - u + \frac{2u^2}{1+u}$.

La correction suivant ϕ' s'est traduite par le facteur $\frac{1}{2}\left(1+\sqrt{\frac{2}{\pi(6k)}} + O(\frac{1}{k})\right)$;

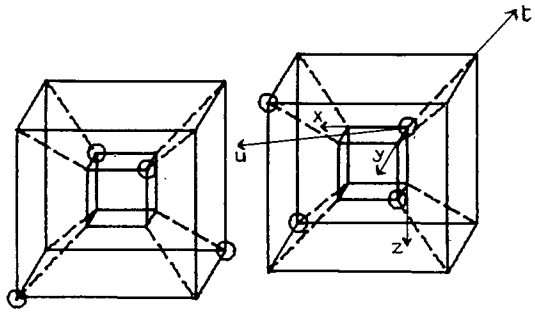
celle suivant $\tilde{\phi}_n$ se traduira grâce à (2), par

$$\left(1-\sqrt{\frac{2}{\pi 6k}} + O(\frac{1}{k})\right)\left(1+\frac{2}{\ln 6k(1+\frac{1}{\ln 6k})}\Theta\right) \quad \text{où } \Theta \in]0,1[$$

soit, finalement

$$\boxed{K = 1-\sqrt{\frac{2}{\pi 6k}} + O(\frac{1}{k})}$$

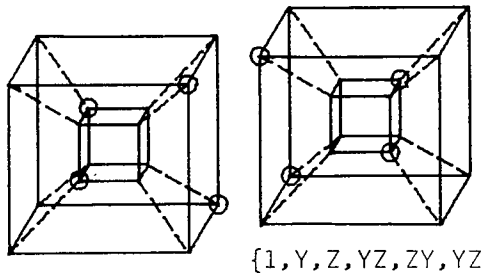
4) Sur les groupes d'automorphisme de 4 parmi les 8-stables du 5-cube



Si X représente l'automorphisme[1] (xy)y'u' (relativement au système d'axes indiqué sur la figure) et Y l'automorphisme x' z' t', alors le groupe des automorphismes du stable ci-contre admet la présentation[2]

$\langle X,Y;X^2,Y^2,XY = YX\rangle$;

c'est le groupe commutatif à quatre éléments, dit de Klein.



De la même façon, le groupe du stable ci-contre, est engendré par les trois automorphismes

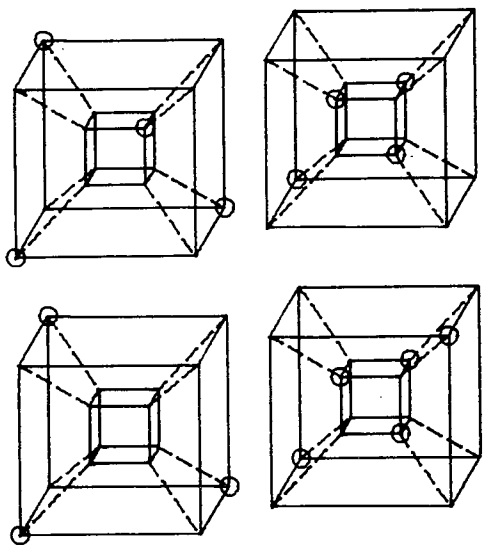
X=x'u'
Y=(yz)
Z=x'y't' et admet la présentation

$\langle X,Y,Z;X^2,Y^2,Z^2,XY=YX,XZ=ZX,YZYZ=ZYZY\rangle$;

c'est un groupe non commutatif de 16 éléments.

{1,Y,Z,YZ,ZY,YZY,ZYZ,YZYZ, X,XY,XZ,XYZ,XZY,XYZY,XZYZ,XYZYZ}.

(X est dans le centre).



Les deux derniers groupes admettent chacun, 4 générateurs X=(y'z')
Y=(zx)
Z=(x'y')

plus T_1=x'y'z't'u' pour le 1er et T_2=x'y'z'(t'u') pour le 2e ; ils ont la même présentation :

$\langle X,Y,Z,T;X^2,Y^2,Z^2,T^2,XT=TX,YT=TY,ZT=TZ,XY=YZ=ZX,YX=XZ=ZY\rangle$;il s'agit d'un groupe non commutatif de 12 éléments

{1,X,Y,Z,XY,YX,T,TX,TY,TZ,TXY,TYX}

(T est dans le centre).

---

[1] *Pour les notations voir Algèbre de Boole, [KUNTZMANN 4]*

[2] *Voir, par exemple, [MAGNUS, KARRASS, SOLITAR]*

CHAPITRE III

PRESENTATION ET RESOLUTION PARTIELLE

D'UNE CONJECTURE SUR LE TYPE DES FONCTIONS BOOLEENNES

1) Présentation de la conjecture.

2) Les fonctions d'au plus quatre variables.

2.1) 1 variable.

2.2) 2 variables.

2.3) 3 variables.

2.4) 4 variables : 216 cas à examiner.

3) Les fonctions d'au plus quatre points.
(ou d'au moins 2^n-4 points).

3.1) au plus 1 point.

3.2) 2 points .

3.3) 3 points .

3.4) 4 points

a) aucun {triangle, point} dans le code

b) au moins un {triangle, point} dans le code.

III - PRESENTATION ET RESOLUTION PARTIELLE D'UNE CONJECTURE SUR LE TYPE DES FONCTIONS BOOLEENNES

1) Présentation du problème

On se place dans $\coprod_{i\in\mathbb{N}} (\mathbb{Z}/2)_i$ muni de sa structure affine métrique. A une fonction booléenne de $n \geqslant 1$ variables, considérée comme une partie de $(\mathbb{Z}/2)^n$ on associe les n-paires de fonctions de n-1 variables, déterminées par intersection avec les n-paires d'hyperplans coordonnées ($x_i = 0$ ou $x_i = 1$ pour $i = 1,\ldots,n$).

Ceci détermine une application $C : \mathcal{P}(\mathbb{Z}/2)^n \to \mathcal{F}$ où $\mathcal{F}$ est l'ensemble des parties à au plus n éléments pris parmi les paires de fonctions booléennes de n-1 variables.

Rappelons que s'il existe une isométrie[1] transformant une fonction f en une fonction g on dit que f et g sont du même type, ce qui détermine une relation d'équivalence.

Considérons l'injection t qui, à une fonction booléenne, associe son type et l'application naturelle $\mathcal{C}$ qui en découle sur $\mathcal{F}$, telle qu'on ait

$$\mathcal{C}(\{a_1,b_1\},\ldots..\{a_n,b_n\}) = \{\{t(a_1),t(b_1)\},\ldots..,\{t(a_n),t(b_n)\}\}$$

L'application C "passe" aux ensembles de types, en ce sens, qu'il existe une application $\mathcal{C}$ rendant commutatif le diagramme

$$\begin{array}{ccc} \mathcal{P}(\mathbb{Z}/2)^n & \xrightarrow{C} & \mathcal{F} \\ \downarrow t & & \downarrow \mathcal{C} \\ T_n & \xrightarrow{\mathcal{C}} & \mathcal{P}_n^2(T_{n-1}) \end{array}$$

---

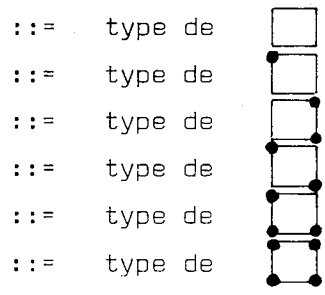
[1] *au lieu d'isometries, on pourait parler ici de déplacements (espace affine) et de rotations (espace vectoriel), puisque dans* $\mathbb{Z}/_2$: $-1 = 1$.

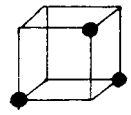
où T_n désigne l'ensemble des types de fonctions de n variables, $\mathcal{P}_n^2(T_{n-1})$ désigne l'ensemble des parties d'au plus n-éléments pris parmi les paires de types de fonctions de n-1 variables.

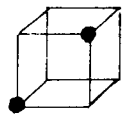
En effet, à deux fonctions f et g de même type t(f) = t(g), $\mathcal{C}_o$C associe le même élément.

Exemple - Si t_o ou même O désigne le type de la fonction vide à 2 variables, et si, de façon générale, O, 1, 21, 22, 1', O' sont les six types de fonctions à deux variables suivant :

O ::= type de
1 ::= type de
21 ::= type de
22 ::= type de
1' ::= type de
O' ::= type de



$\mathcal{C}ot$ () ={{22,1},{1,22},{1,22} = {{1,22}}

$\mathcal{C}ot$ () = {{1,1},{0,22},{1,1 } = {{0,22} , {11}}

Le problème est, alors, le suivant :

> L'application $\mathcal{C}$ est-elle injective ?

ou encore, en termes de reconstruction :

> Est-il **possible, étant donné un ensemble de n-paires** de fonctions booléennes, correspondant à ses intersections avec les hyperplans-coordonnées, de reconstruire de plusieurs façons non-isomorphes (isométriques) une fonction initiale ?

Sous cette forme, le problème s'apparente donc au problème de la reconstruction d'un graphe à partir de ses n-1 sous-graphes de n-1 points. La conjecture d'[Ulam] affirme que la reconstruction, à un isomorphisme près, est unique dès que n > 2. (Les deux graphes •—• et • • admettent la même "déconstruction" : {•,•}).

Remargue - La conjecture proposée porte sur l'affirmation de l'injectivité de l'application $\mathcal{C}$. Si l'on se permet de "compliquer" l'ensemble d'arrivée, en conservant davantage d'informations, on obtient des formes plus faibles de la conjecture. C'est le cas, par exemple, si l'on conserve le fait que, dans une "déconstruction", telle paire apparaît plusieurs fois ou même, exactement, "tant" de fois.

L'injectivité de $\mathcal{C}$ permettrait de considérer qu'elle constitue un code pour le type d'une fonction, en exprimant le type d'une fonction booléenne par composition de fonctions $\mathcal{C}$, et en considérant les types de fonctions à 3 (6 types) ou 2 (3 types) variables, comme des termes primitifs. On disposerait alors, à l'aide de ce code, d'un algorithme facile à mettre en oeuvre et efficace[1] pour la reconnaissance du type d'une fonction ainsi que pour le problème de l'équivalence en type de deux fonctions.

On va démontrer la conjecture dans deux cas particuliers :

- les fonctions de moins de 5 variables
- les fonctions ayant un ensemble représentatif de moins de 5 points (ou complémentaires d'-).

---

(1) *En effet, en travaillant sur la fonction elle-même, si la fonction est plutôt "creuse", ou son complémentaire, si elle est plutôt "pleine", on obtient rapidement, parmi l'ensemble des paires, des fonctions vides ou presque vides et donc facilement reconnaissables.*

2) Les fonctions d'au plus 4 variables

2.1) Fonctions d'1 variable

Il existe 3 types de fonctionsd'1 variable dont les codes, suivant les 2 types de fonctionsde 0 variable, sont tous distincts :

$\mathcal{C}$ () = {0,0} = {0} type 0

$\mathcal{C}$ () = {1,0} type m

$\mathcal{C}$ () = {1,1} = {1} type 2

2.2) Fonctions de 2 variables

Il existe 6 types de fonctions de 2 variables dont les codes, suivant les 3 types de fonctions de 2 variables, sont tous distincts :

$\mathcal{C}$ () = {{0,0},{0,0} = {{0}} type 0

$\mathcal{C}$ () = {{1,0},{1,0} = {{1,0}} type 1

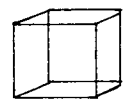
$\mathcal{C}$ () = {{2,0},{1,1}} type 21

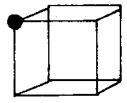
$\mathcal{C}$ () = {{1,1},{1,1}} = {{1}} type 22 ;

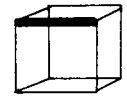
les deux types suivants s'obtiennent par passage au complémentaire et seront désignés par 0' = t () et 1' = t ().

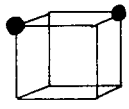
2.3) Fonctions de 3 variables

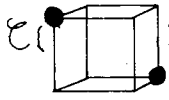
Il existe 22 types de fonctions de 3 variables, mais on peut se limiter grâce à la complémentarité aux 14 types de fonctions d'au plus 4 variables, et même, parmi ceux-ci, aux seuls 8 types propres (types de fonctions non incluses dans un hyperplan-coordonnée ou, encore, dépendant effectivement de l'ensemble des variables).

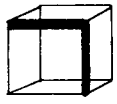

Type impropre 0
(compl. 0')

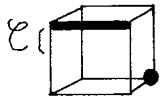

Type impropre 1
(compl. 1')

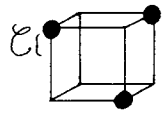

Type impropre 21
(compl. 21')

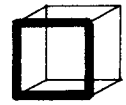

Type impropre 22
(compl. 22')

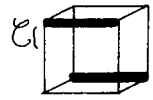

= {{1}}
Type 23
(compl.23')

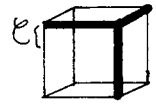

Type impropre 31
(compl. 31)

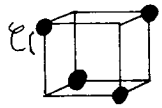

= {{21,1},{22,1}}
(compl.32')

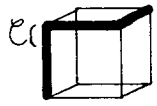

= {{22,1}}
Type 33
(compl.33')

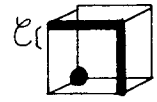

type impropre 41


={{21},{22}}
Type 42


= {1',1}
Type 43


={{22}}
Type 44


= {{21},{1',1}}
Type 45


={{21,22},{1'1}}
Type 46

2.4) Fonctions de 4 variables

Par les mêmes limitations qu'en dimension trois, on est amené à examiner les codes de 216 types propres [1] sur les 380 types propres (pour un total de 402 types).

On trouvera en annexe un catalogue des 402 types de fonctions booléennes de 4 variables, écrit pour l'occasion, à la suite duquel sont indiqués les 216 codes distincts des 216 types propres à examiner, classés lexicographiquement.

Remarque - A 5 variables, c'est plus de 600 000 types propres (sur un total de 1 228 158 types) qu'il faudrait examiner . Il semble qu'un tel examen soit possible en un temps raisonnable à l'aide d'un ordinateur et d'un programme écrit en LISP, par exemple, qui se prête bien au traitement des listes imbriquées que constituent les codes.

---

[1] *Ce nombre 216 est obtenu, comme la somme des nombres de types à moins de 8 points, soit 1+1+4+6+19+27+50+56+74 diminué du nombre de types de fonctions de 3 variables d'au plus 8 points, c'est-à-dire du nombre de types de fonctions de 3 variables, soit 22.*

3) Les fonctions d'au plus 4 points dans leur ensemble représentatif

3.1) Fonctions d'au plus 1 point

Dans ces deux cas, fonction vide ou réduite à 1 point, la propriété est évidente..

3.2) Fonction de 2 points

Par récurrence sur le nombre n de variables.

Si la distance des deux points est a < n, on est ramené à un plus petit nombre de variables puisque le bi-point est inclus dans un certain hyperplan et l'on est assuré, d'autre part, de la propriété pour n=1.

Sinon, la distance est n, le bi-point est alors constitué d'un couple de points opposés dans le n-cube, ce qui établit la propriété.

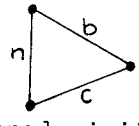
3.3) Fonction de 3 points, constituant un triangle de côtés a,b,c.

On raisonne encore par récurrence.

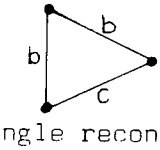
Si le triangle est inclus dans un hyperplan, on est ramené à un plus petit nombre de variables, sinon l'un des côtés, a par exemple, est de longueur n.

Les 2 autres côtés vérifient alors b < n et c < n.

Un autre triangle de même code, s'il est différent, ne peut que correspondre à la répétition de l'un des côtés < n du triangle initial, par exemple b :



triangle initial



triangle reconstruit .

Or, de $b+c = n$ (théorème du I.4) et $b < n$, on déduit $2b+c < 2n$.

De plus, $2b+c$ devant être pair (théorème du I.4), $2b+c \leqslant 2(n-1)$, le triangle reconstruit est donc inclus dans un hyperplan et ne peut donc avoir le même code que le triangle initial.

3.4) Fonction de 4 points

On utilise encore un raisonnement par récurrence et les résultats obtenus au chapitre I sur les tétraèdres de $(\mathbb{Z}/2)^n$.

Il suffit d'examiner le cas d'un tétraèdre non inclus dans un hyperplan et l'on trouvera ci-dessous l'ensemble des différents cas à envisager, divisé en deux catégories principales, suivant qu'il existe ou non dans le tétraèdre initial un triangle inclus dans un hyperplan.

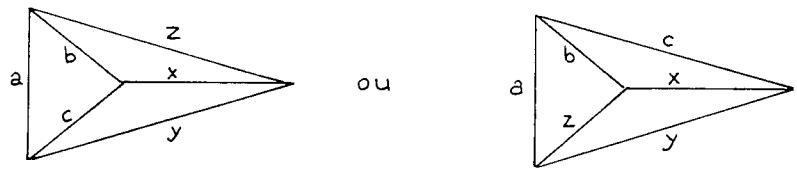
Remargue - [Simoes Pereira] a étudié une conjecture apparentée à celle proposée ici, qui consiste à envisager la décomposition d'une fonction suivant ses intersections avec les hyperplans-coordonnées, mais suivant ses différentes projections.

Nous pensons que le codage proposé ici est plus "séparateur" que celui suivant les projections.

On raisonne par récurrence sur la dimension du n-cube, et on va montrer que deux tétraèdres ayant même code, ont même graphe des distances, ce qui établit bien, d'après le théorème p.113, la propriété annoncée.

Le propriété est trivialement vérifiée pour n=0.

a) Supposons d'abord qu'il n'existe aucune direction découpant la fonction suivant un triangle et un point. C'est que les couples intervenant dans le code sont de la forme $a|x$, $b|y$ et $c|z$, où a, par exemple, représente la fonction constituée de deux points à distance a (on ne suppose pas forcément $a|x \neq b|y$, $a|x \neq c|z$). Le graphe des distances correspondant ne peut être, à une renotation éventuelle près, que



qui ne sont distincts qu'au moins si $c \neq z$.

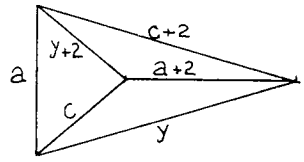
On peut supposer $z = c+h$ et il vient

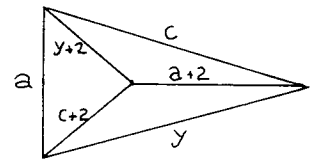
$$\underbrace{a+b+c}_{\geqslant 2n+1} + \underbrace{x+y+c}_{\geqslant 2n-1} + h \leqslant 4n \quad \text{d'où} \quad 0 < h \leqslant 2 \ .$$

Or $h \equiv 0 \pmod 2$ d'où la seule possibilité $h = 2$.

De même, si $a = x$ ou $b = y$, il y a isomorphisme . Restent donc à étudier les cas $a \neq x$ et $b \neq y$. On peut supposer $a < x$ ce qui conduit à $x = a+2$. Nous allons montrer que dans les deux cas $y < b$ ou $y > b$, l'existence des deux graphes de distances n'est pas simultanément possible.

• De $y < b$ on déduit encore $b = y+2$





il vient $2(a+y+c) + 6 \leqslant 4n$ or, $a+y+c \geqslant 2n-1$

• Dans le cas $y > b$ on est conduit à

$$2(a+b+c) + 6 \leqslant 4n \quad \text{avec} \quad a+b+c \geqslant 2n-1$$

b) Reste donc à étudier le cas où il existe une décomposition du tétraèdre en un triangle (par exemple de côtés a,b,c) et un point.

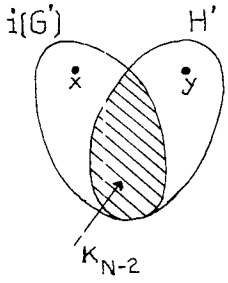
Remarquons d'abord que si deux tétraèdres sont isomorphes et qu'un triangle du premier est isomorphe à un triangle du second, alors il existe un isomorphisme des deux triangles se prolongeant en un isomorphisme des deux tétraèdres.

Cette propriété relève d'un énoncé plus général, à savoir que,

lemme pour $n \geq 1$, s'il existe un isomorphisme (de graphe marqué) de G, graphe marqué de support K_n, sur H graphe marqué de même support et que l'on connaisse un isomorphisme d'une partie $G' \subset G$ de support K_{n-1}, sur $H' \subset H$, alors il existe un isomorphisme de G sur H, appliquant G' sur H'.

La propriété est immédiate pour n=1. Supposons-la établie pour $n \leqslant N$ ($N \geqslant 1$) et établissons-la pour N+1.

Dans l'isomorphisme $i:G \to H$, si $i(G') = H'$ alors le résultat est immédiat ; sinon c'est qu'il existe dans H' deux points x et y tels que



$$x \in i(G') \quad \text{et} \quad x \notin H'$$

$$y \in H' \quad \text{et} \quad y \notin i(G')$$

- $i(G'$ est un graphe marqué de support K_N

  H' est un graphe marqué de support K_N

- $i(G')$ et H' sont isomorphes (au sens des graphes marqués)

- il existe un isomorphisme (l'identité) de $i(G') \cap H' \subset i(G')$ sur $i(G') \cap H' \subset H'$;

il existe donc un isomorphisme de $i(G')$ sur H') conservant globalement $i(G') \cap H'$ (de support K_{N-2}). Cet isomorphisme ne peut donc qu'échanger x et y, ce qui fournit, par composition, un isomorphisme de G sur H, appliquant G' sur H'.

Q.E.D.

Montrons alors que la reconstruction d'un tétraèdre dont le coce comporte un triangle, est unique. En effet, deux reconstructions éventuelles sont isomorphes, au moins en ce qui concerne le triangle (a,b,c) et le théorème p. 113 sur la décomposition des tétraèdres T et T' utilisant toutes les directions du n-cube , montre qu'elles sont alors isomorphes compte tenu de leurs décompositons (cf. page 107.) relativement au triangle (a,b,c).

CHAPITRE IV

PRESENTATION GEOMETRIQUE DE DIFFERENTS ALGORITHMES D'ALGEBRE DE BOOLE

1) L'algorithme d'exclusion en algèbre de Boole
(une démonstration directe de).

1.1) Un lemme.

1.2) Le théorème de convergence.

2) Conséquences en ce qui concerne deux algorithmes classiques de recherche de la base complète d'une fonction.

2.2) L'algorithme à tour de consensus.

2.3) Un autre algorithme [Kuntzmann 3].

3) Un nouvel algorithme de recherche de la base complète.

- Exemples en dimension 3 et 4.

1) L'algorithme d'exclusion en algèbre de Boole

On se reportera à la 1ère partie pour le cadre et les notations propres à cette question.

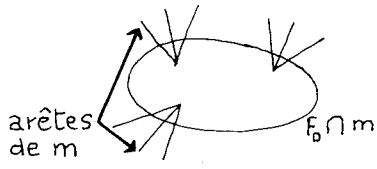
Démontrons d'abord le

1.1) LEMME

Si au rang n, un monôme premier m est couvert par des monômes de la partie droite (F_n), il en est de même au rang n+1 (F'_{n+1}), à moins que m ne figure parmi les monômes de la partie gauche (E'_{n+1}).

Démonstration - Si le monôme exclus f_o est d'intersection vide avec m, alors m est couvert par des $f_i (i \geq 1)$ c'est-à-dire par des éléments de F'_{n+1}.

Sinon, à moins que f_o ne soit m lui-même, auquel cas le problème est résolu, les consensus de f_o avec les $f_i (i \geq 1)$, et éventuellement certains $f_i (i \geq 1)$ contiennent (dans leur ensemble) toute arête de m issue d'un point de $f_o \cap m$ et ceci grâce au théorème du chapitre 1 p.98 indiquant qu'un consensus est une union d'arêtes réalisant les distances 1.



Si en chacun des points de $f_o \cap m$ ce ne sont pas toutes les arêtes de m qui sont absorbées dans la simplification transformant F_{n+1} en F'_{n+1}, alors le problème est résolu.

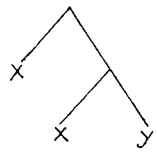
Supposons donc qu'il existe un point $a \in f_o \cap m$, tel que chacune des arêtes de m, issues de a, soit absorbée et que, de plus, aucun des f_i, $i \geq 1$ ne couvre a. Alors, à ce stade, c'est qu'au moins un majorant (déjà exclu) de l'une de ces arêtes est indispensable pour construire m.

Il existe donc un premier monôme exclu μ , d'intersection non vide avec m, dont la présence sera indispensable à la construction de m, au cours des étapes ultérieures du processus d'exclusion.

Nous allons montrer qu'en fait μ n'est pas indispensable, ce qui entraînera une contradiction et donc la non existence d'un point tel que a.

$m \cap f_o \cap \mu$ n'est pas vide puisque μ contient au moins un point tel que a. Les arêtes issues des points de $m \cap \mu$ ne sont certainement pas absorbées par des monômes déjà exclus, d'après le caractère minimal de μ . Or, ces arêtes ou certains de leur consensus, après exclusion, couvrent chacun des points de $\mu \cap f$, au cours de toutes les étapes ultérieures, à moins que l'on en vienne à exclure m lui-même ; ce qui fait que μ ne saurait être indispensable.

Remarque - La fin de la démonstration montrant qu'un monôme, après son exclusion, n'est certainement pas indispensable à la construction d'un monôme premier, n'est pas sans rappeler la propriété d'absorption du consensus (cf. I^{ère} partie, II):



non défini ou plutôt, de façon générale,

majoré par x ou par 

.

On peut alors énoncer le théorème suivant :

1.2) THEOREME

Selon la topologie discrète,

$$\lim_{n\to\infty} (E_n, F_n) = (\text{Ensemble des monômes premiers de } F_o, \emptyset) \ ;$$

c'est-à-dire la convergence de l'algorithme de Tison (en un nombre fini de pas) vers l'ensemble des monômes premiers de la fonction représentée par lesmonômes de la partie droite initiale.

En effet, au rang 0, tout monôme premier est bien couvert par des monômes de la partie droite. D'autre part, en un nombre fini de pas on arrive à $F_n = \emptyset$, sinon cela nécessiterait l'existence d'un nombre infini de monômes distincts dans le cube $(\mathbb{Z}/2)^r$ où r est le nombre de variables intervenant dans les monômes de F_o.

2) De ce théorème on déduit le, très classique,

COROLLAIRE - L'ensemble des éléments maximaux (pour l'inclusion) de la fermeture d'un ensemble de monômes F pour l'opération de consensus binaire, est constitué de l'ensemble des monômes premiers de la fonction représentée par F.

Considérons en effet l'algorithme des tours de consensus [Kuntzmann 3]

$$F_o = \text{Max } F$$
$$F_1 = \text{Max } F_o \cup \mathcal{C}_2(F_o)$$

$$F_{n+1} = \text{Max } F_n \cup \mathcal{C}_2(F_n)$$

où $\mathcal{C}_2(A)$ représente l'ensemble des consensus binaires de monômes pris dans A.

Les $E_n \cup F_n$ de l'algorithme d'exclusion sont, en effet, tous inclus dans certains des F_i de l'algorithme d'exclusion, ce qui établit

d'une part

- la convergence de l'algorithme des tours de consensus vers l'ensemble des monômes premiers ;

d'autre part

- le corollaire annoncé.

De la même façon, par référence à l'algorithme d'exclusion, on établit la convergence vers l'ensemble des monômes premiers de l'algorithme intéressant, suivant [Kuntzmann 3]:

$$F_o = \mathfrak{Max}\ F\ ,$$

et pour $i \geq 0$, en posant $F_i = (m_o, m_1, m_2, \ldots, m_j)$

si $j \leq i$ F_i stationne

sinon $$F_{i+1} = \mathfrak{Max}\left(F_i \oplus \bigoplus_{k=0}^{i} \text{consensus}\ (m_k, m_{i+1})\right)\ ^{(1)}.$$

---

(1) *Dans cette notation $\oplus$ désigne le symbole de concaténation de files et $\mathfrak{Max}$ désigne l'opérateur de file, transformant une file en la file de ses éléments maximaux à la même place, dans le même ordre.*

3) Un nouvel algorithme de recherche de la base complète

Etant données une fonction booléenne f et a, l'une de ses variables, les monômes premiers de f sont de 3 types :

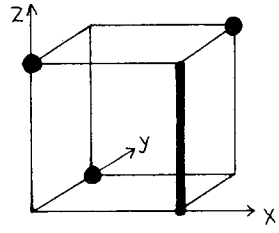
- ceux qui sont dans a=1 (multiples de a)
- ceux qui sont dans a=0 (multiples de a')
- les autres, qui sont l'union d'un certain nombre d'arêtes de direction a, l'intersection des monômes premiers de f(a=0) avec ceux de f(a=1).[1]

On peut donc définir, pour déterminer la base complète d'une fonction, l'algorithme récursif suivant :

> Etant donnée une fonction de n variables parmi lesquelles a, on détermine les bases complètes B de f(a=1) et B' de f(a=0), fonctions de n-1 variables ; la base complète de f est alors représentée schématiquement par
>
> $$(B \cap B') \cup aB \cup a'B' \quad ;$$
>
> avec la condition initiale : la base complète d'une fonction de 0 variable est réduite à l'ensemble vide ou au monôme unitaire, suivant que la fonction est nulle ou non.

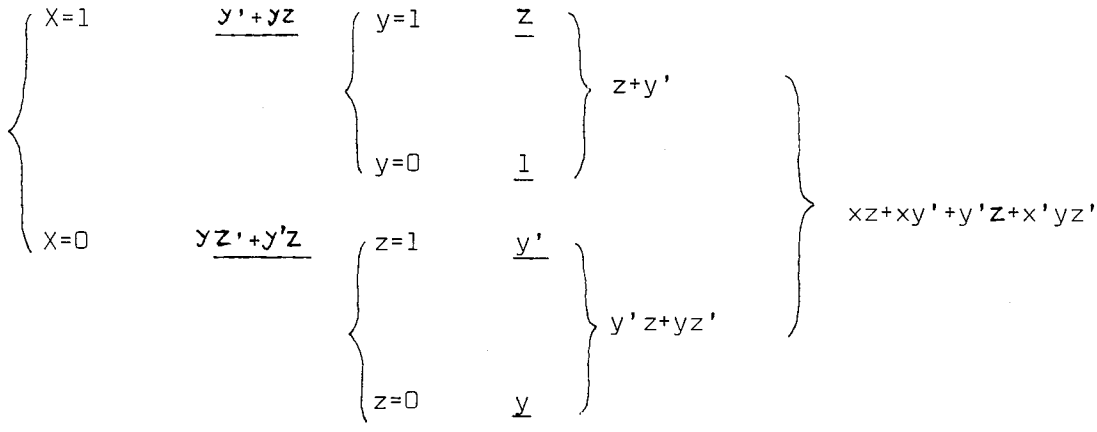
- exemple à trois variables :

$$f = xy' + x'yz' + x'y'z + xyz$$



---

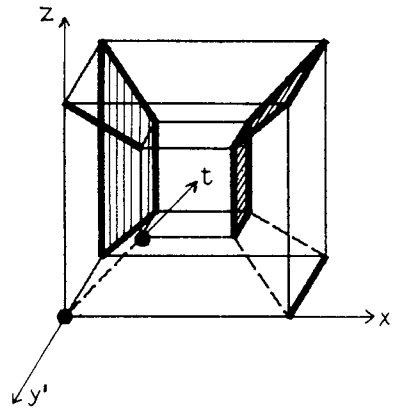
[1] *Le symbolisme f(a=1), par exemple, représente la fonction booléenne f où l'on a remplacé a par 1.*

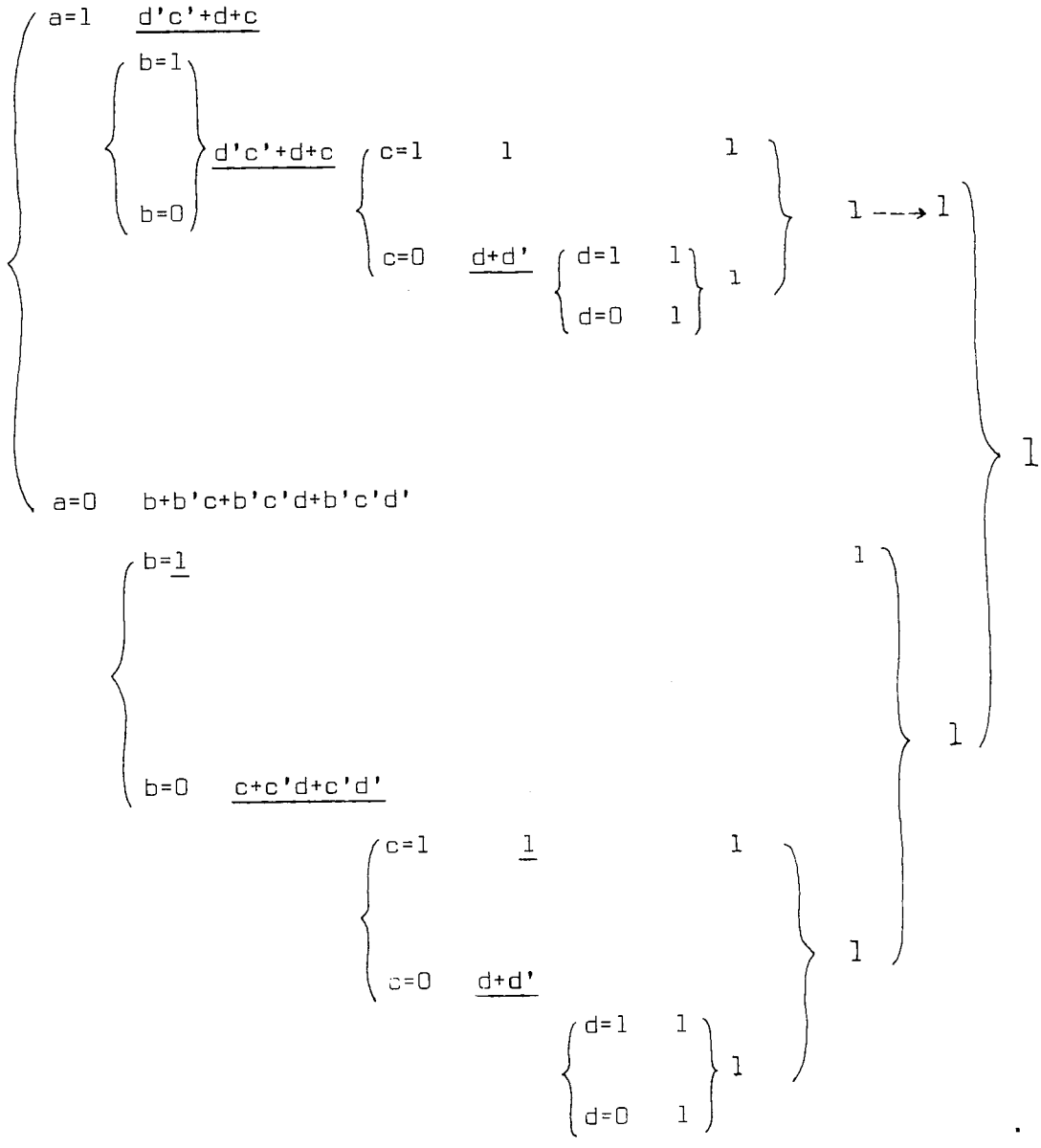


Sur une même verticale sont représentés des niveaux de récursion de même profondeur ; l'ensemble des monômes premiers figure (sous forme de somme) à l'extrême droite.

- exemple à 4 variables où la fonction couvre l'unité :

f = ad'c' + ad + ac + a'b + a'b'c + a'b'c'd + a'b'c'd'




a=1 d'c'+d+c
b=1
b=0
d'c'+d+c
c=1 1 1
c=0 d+d'
d=1 1
d=0 1
1
1 → 1
a=0 b+b'c+b'c'd+b'c'd'
b=1
b=0 c+c'd+c'd'
c=1 1 1
c=0 d+d'
d=1 1
d=0 1
1
1
1

ANNEXE

Catalogue des 402 types de fonctions booléennes de quatre variables.

Remarques -

- à chaque changement du nombre de points (N:=N+1), on indique, par une suite de la forme

$$X_1\ Y_1 \qquad X_2\ Y_2 \cdots\cdots$$

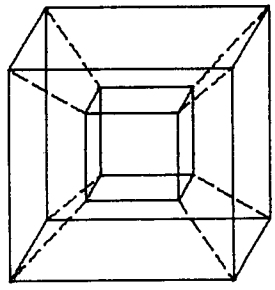
- le nombre (Y_i) de types de fonctions de X_i monômes premiers présentant N+1 points.
- les variations dans les intervalles entre les différents 4-cube, correspondent en général à une séparation entre classes d'équivalences différentes pour le préordre adopté :

croissance
- du nombre de points
- du nombre de monômes premiers
- de la dimension des monômes.

TYPES DES FONCTIONS BOOLEENNES DE 4 VARIABLES

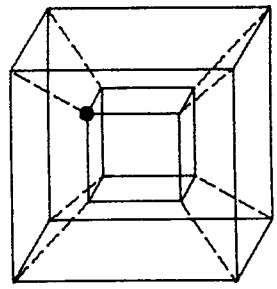
CLASSES SELON LE PREORDRE LEXICOGRAPHIQUE DE LA CROISSANCE
DES NOMBRES DE POINTS ET DE MONOMES PREMIERS, ET DE LA DIMENSION DES MONOMES

0 POINT



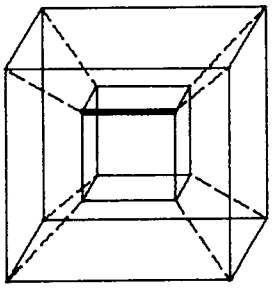
1 POINT

1 MONOME

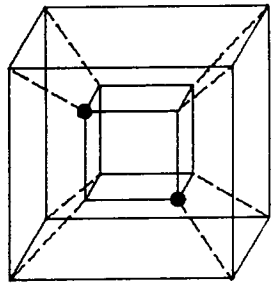


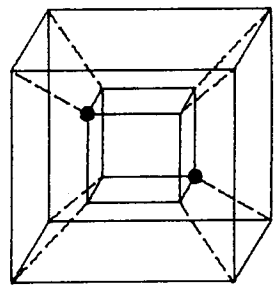
2 POINTS 1_1 2_3

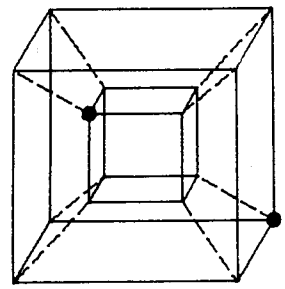
1 MONOME



2 MONOMES

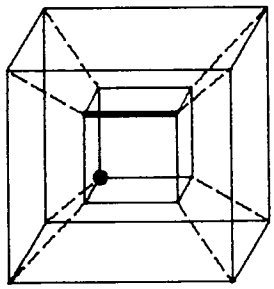


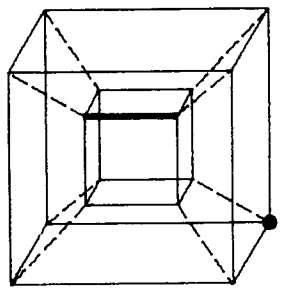


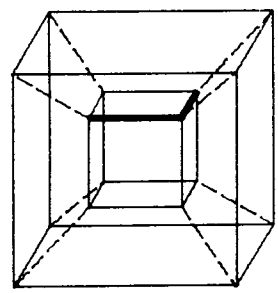


3 POINTS 2_3 3_3

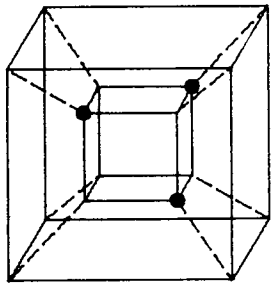
2 MONOMES

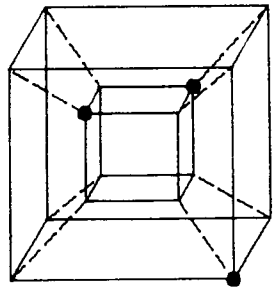


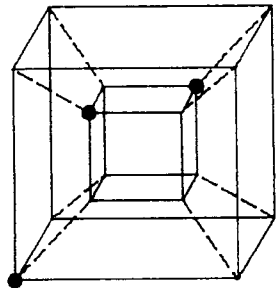




3 MONOMES

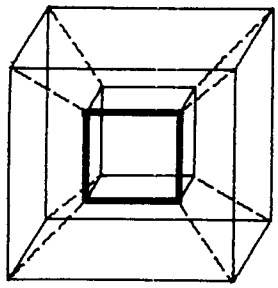




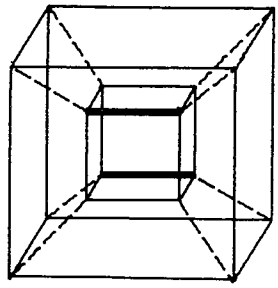


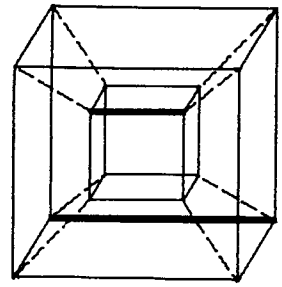
4 POINTS 1_1 2_3 3_9 4_6

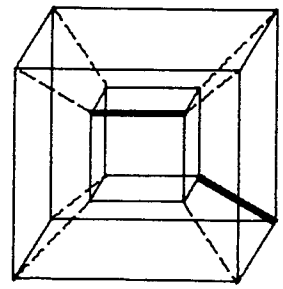
1 MONOME



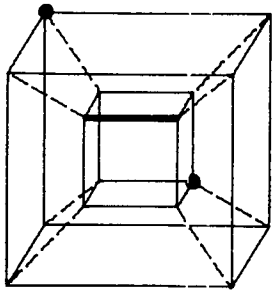
2 MONOMES

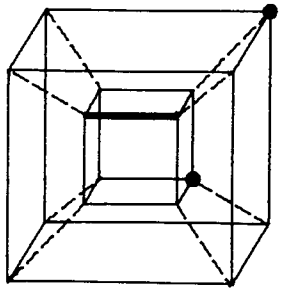


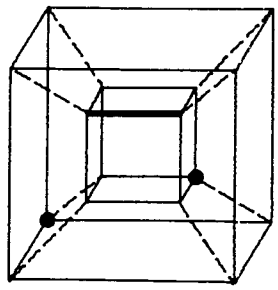


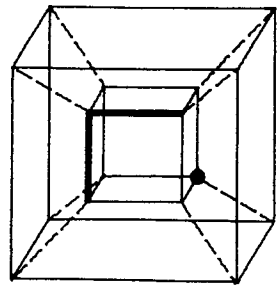


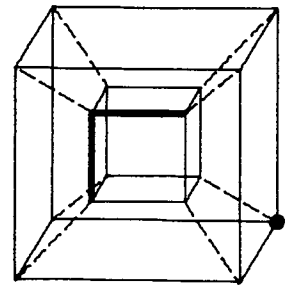
3 MONOMES

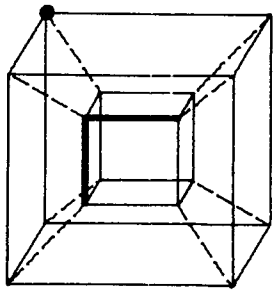


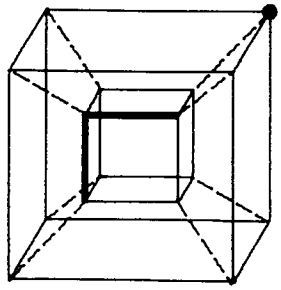


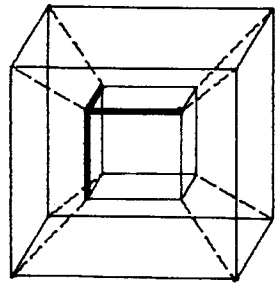


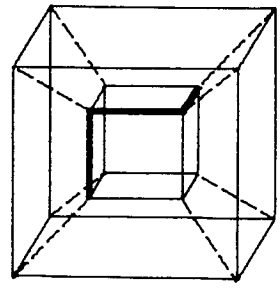




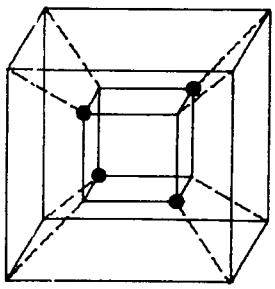


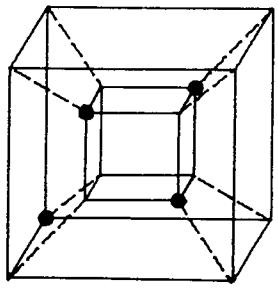


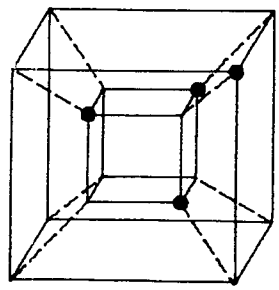


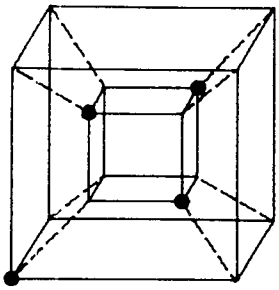


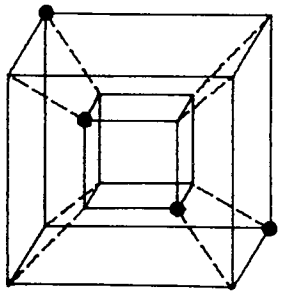
4 MONOMES

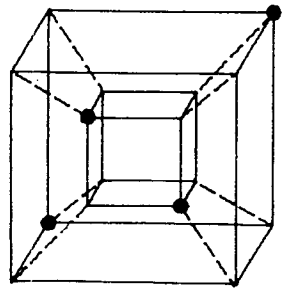






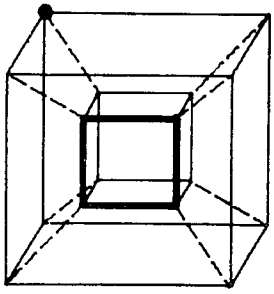


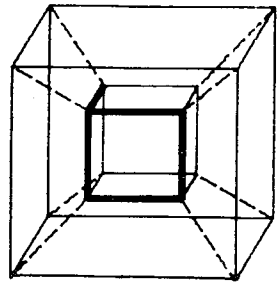




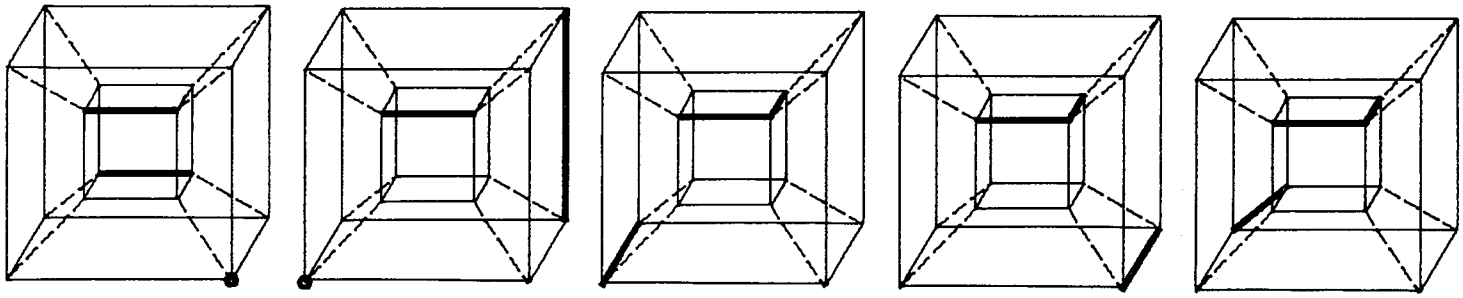
5 POINTS 2_2 3_5 4_{17} 5_3

2 MONOMES

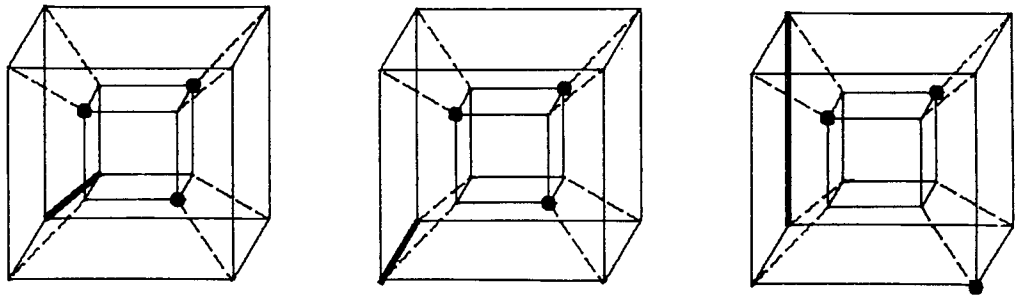


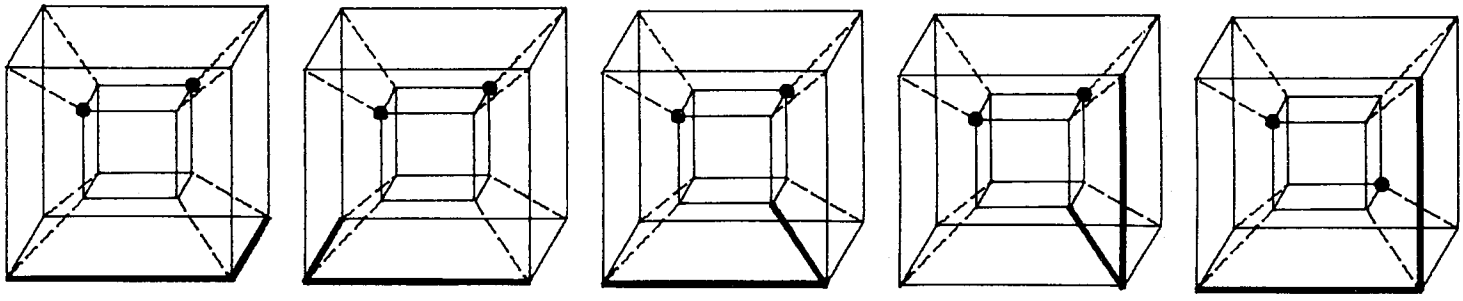


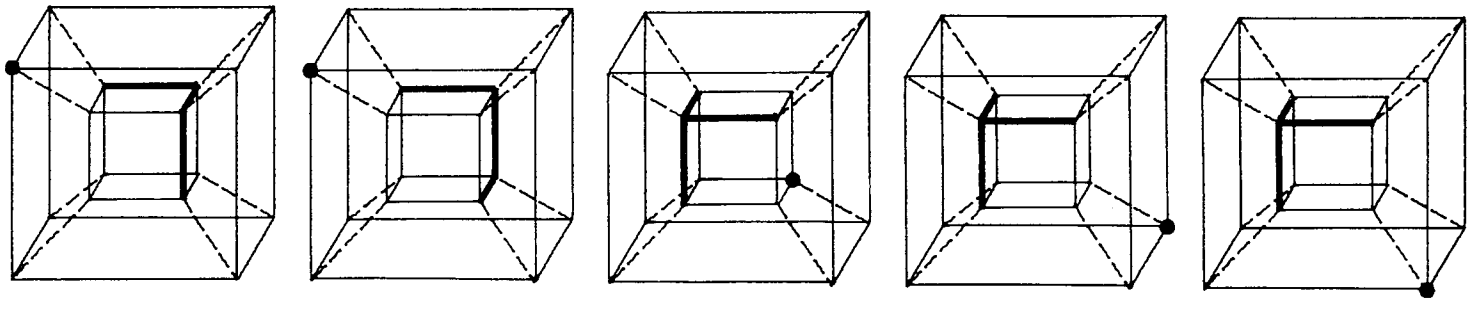
3 MONOMES

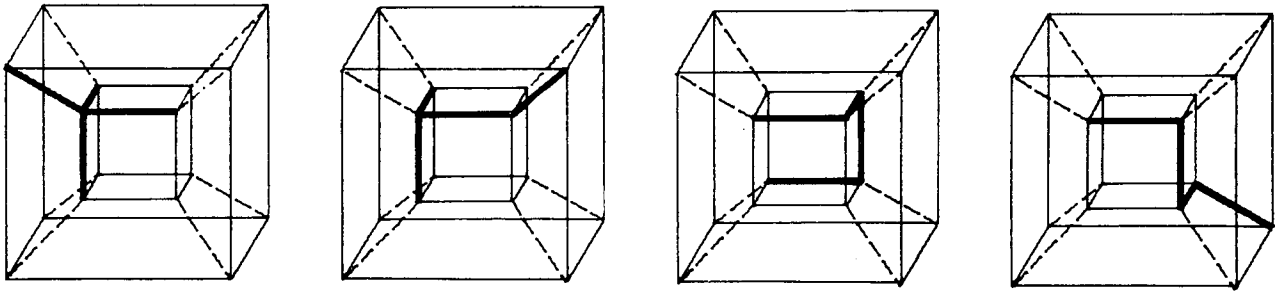


4 MONOMES

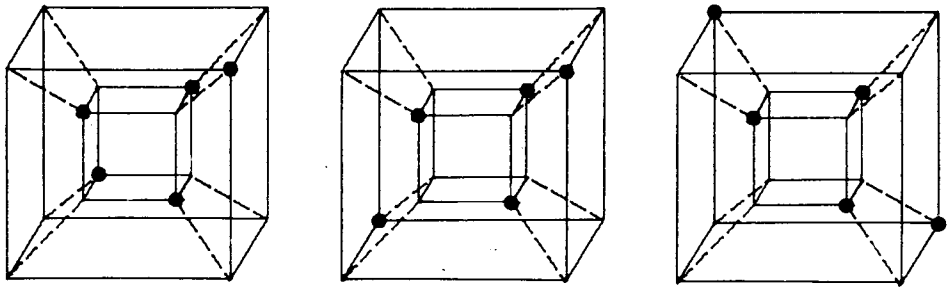






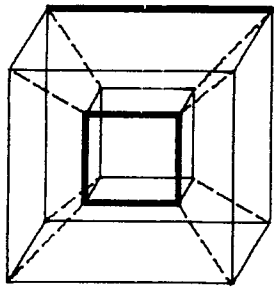


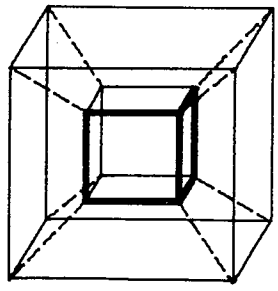
5 MONOMES



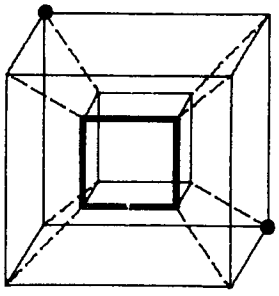
6 POINTS 2_2 3_9 4_{14} 5_{22} 6_3

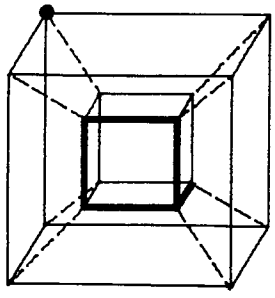
2 MONOMES

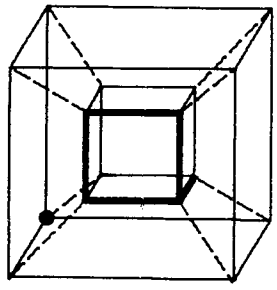


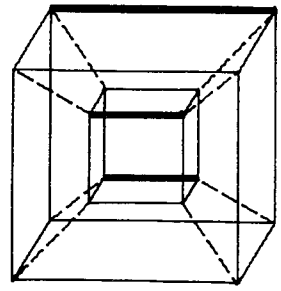


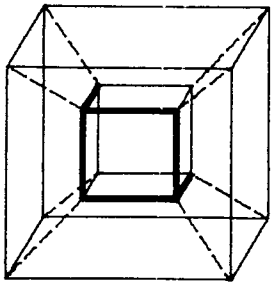
3 MONOMES

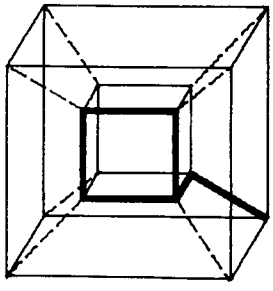


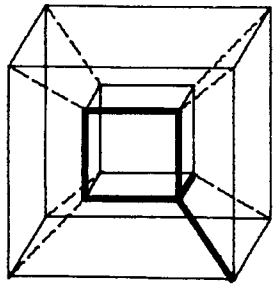


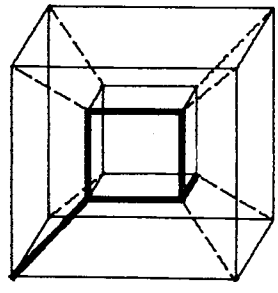


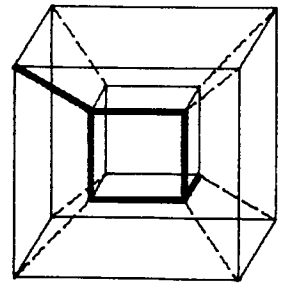




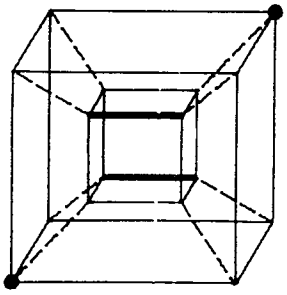


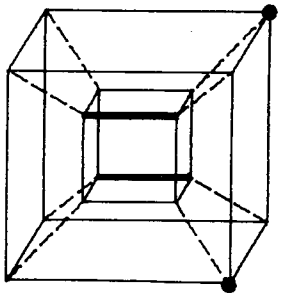


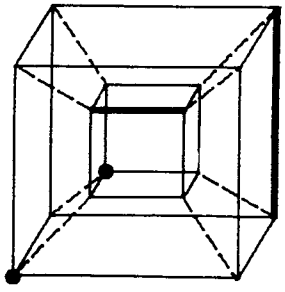


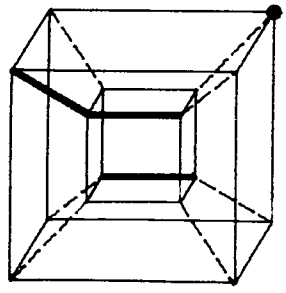


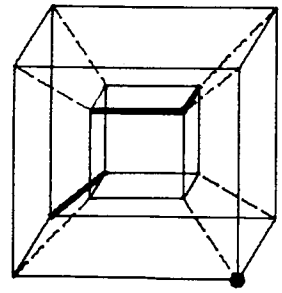
4 MONOMES

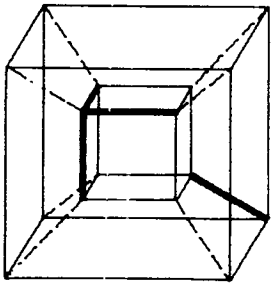


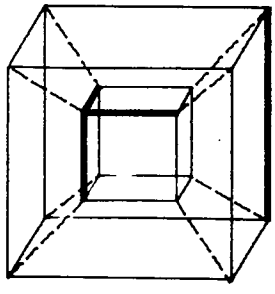


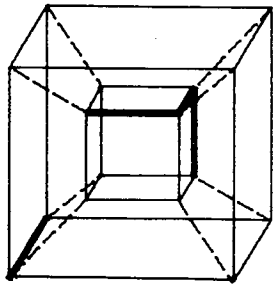


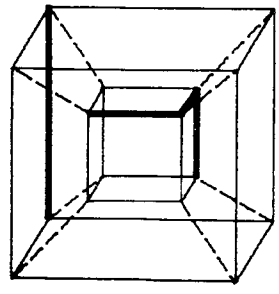


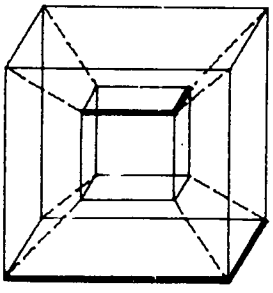


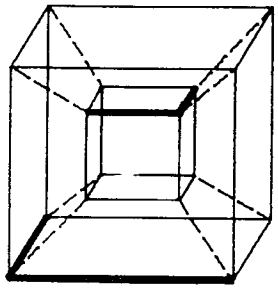


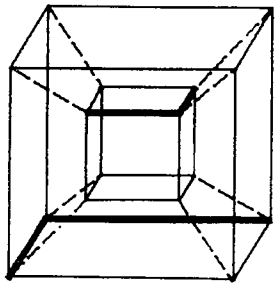


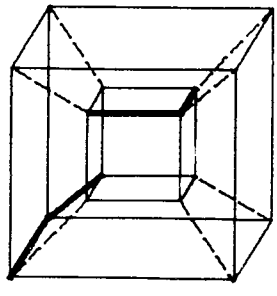


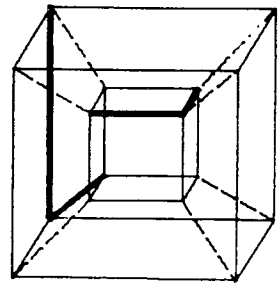




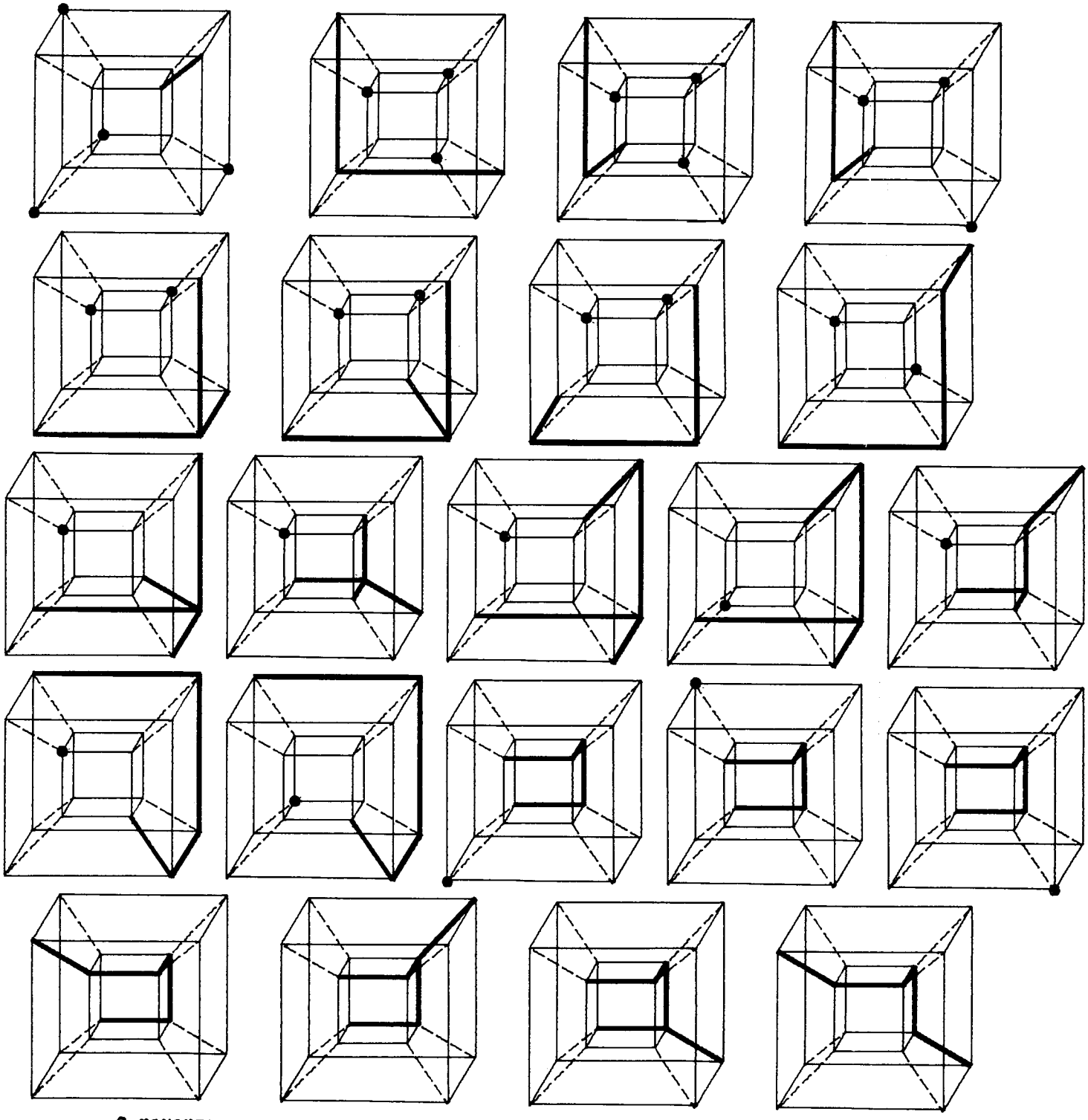




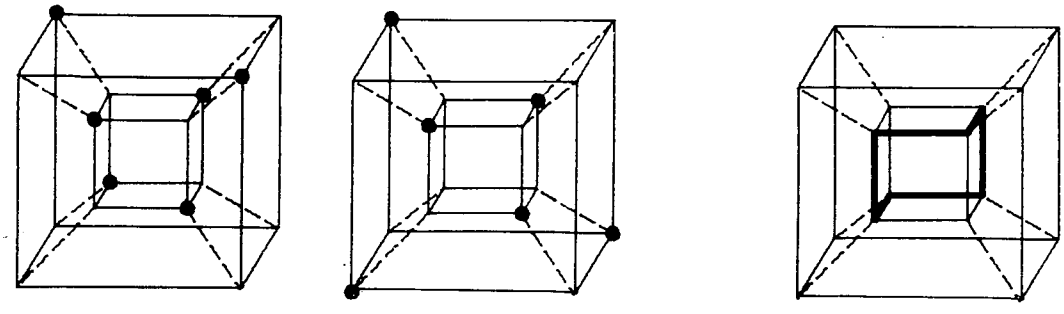




5 MONOMES

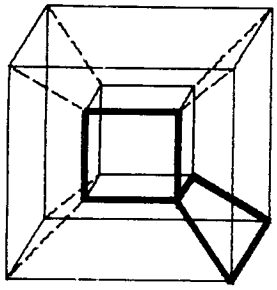


6 MONOMES

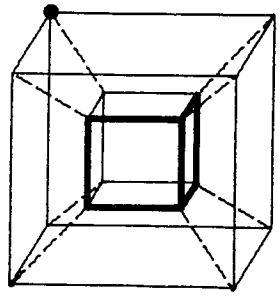


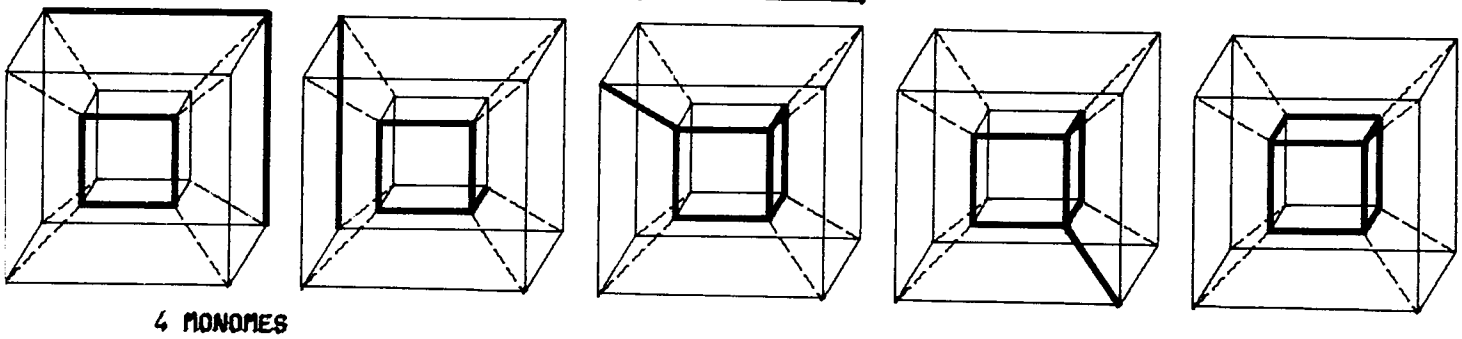
7 POINTS 2_1 3_6 4_{14} 5_{11} 6_{21} 7_3

2 MONOMES

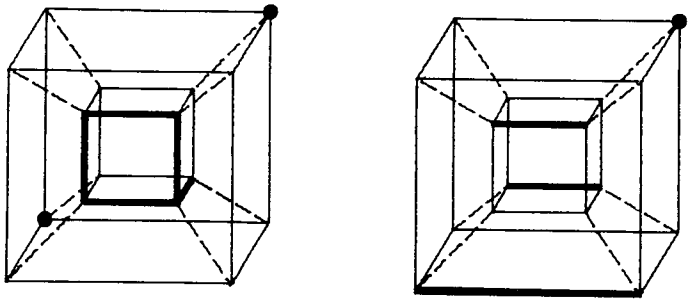


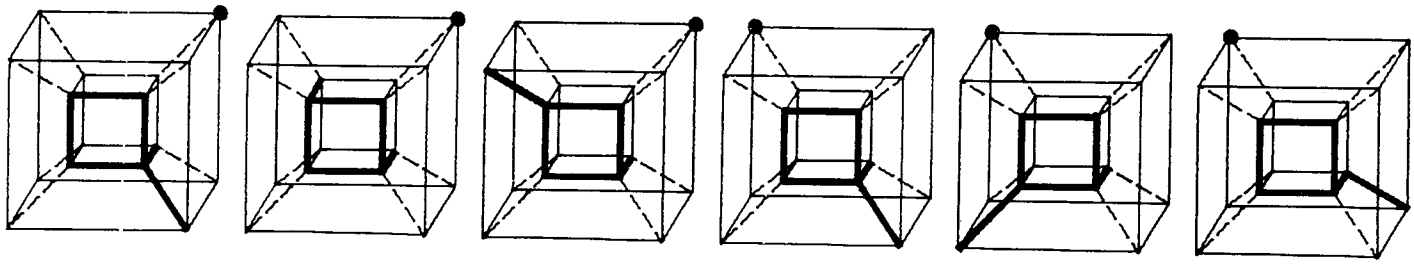
3 MONOMES

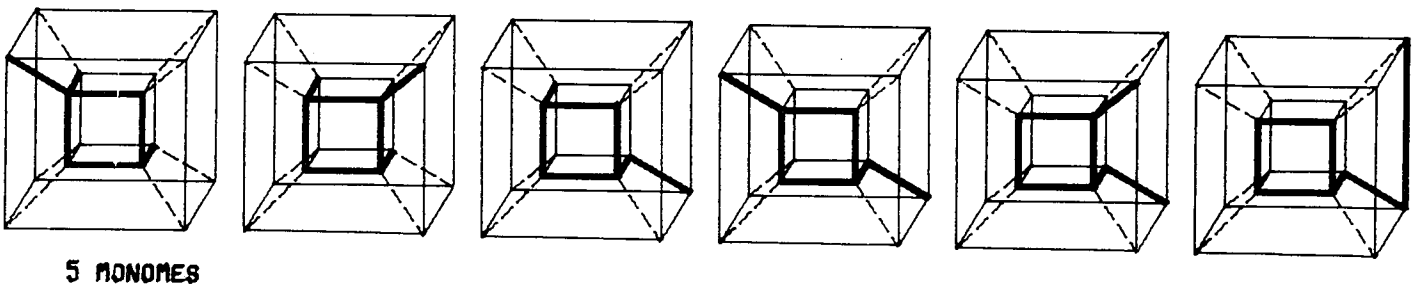




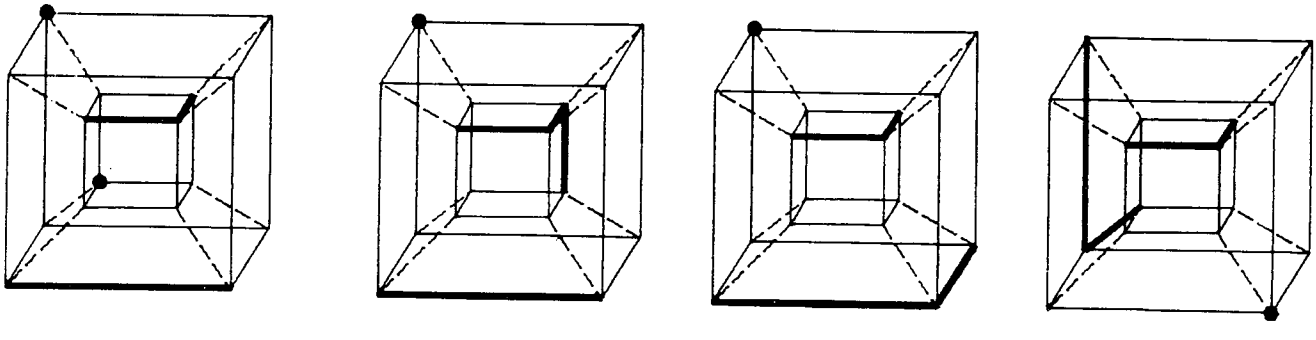
4 MONOMES

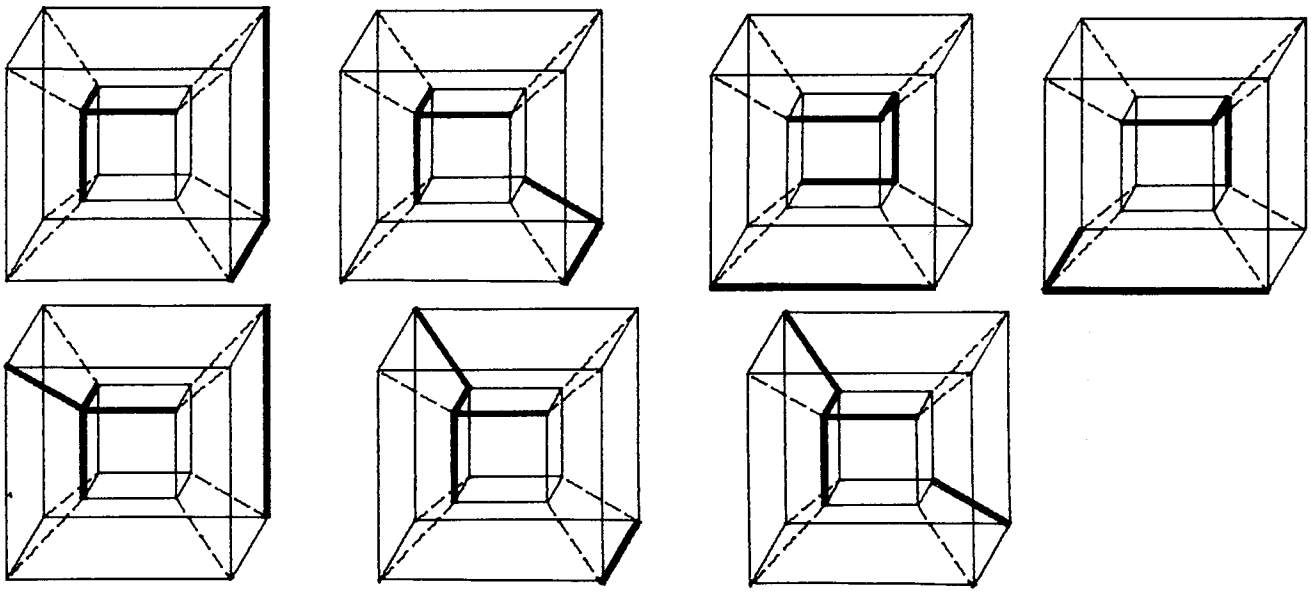




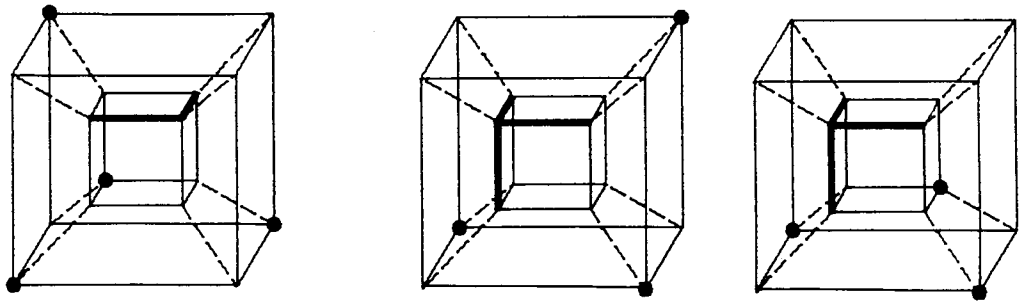


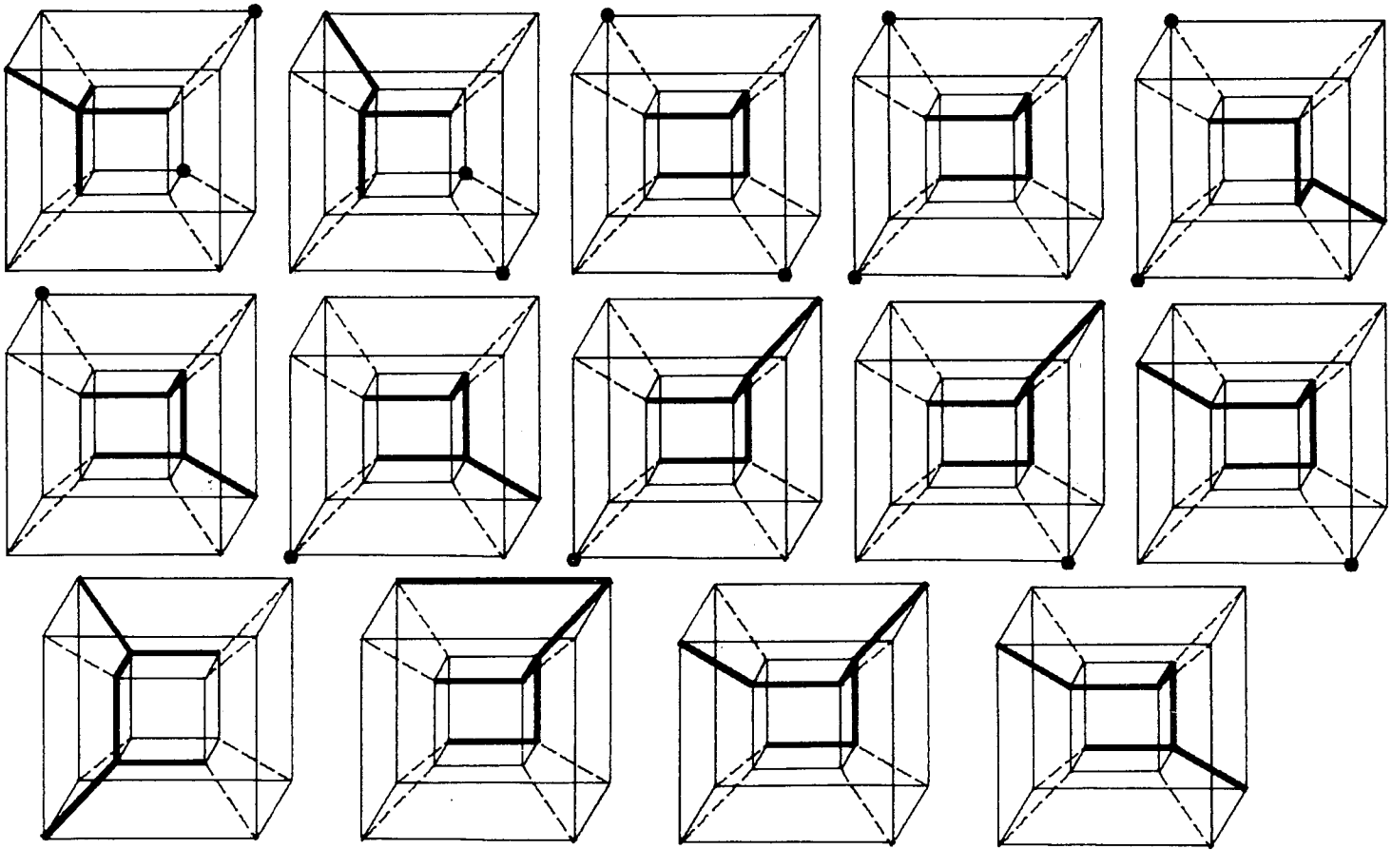
5 MONOMES

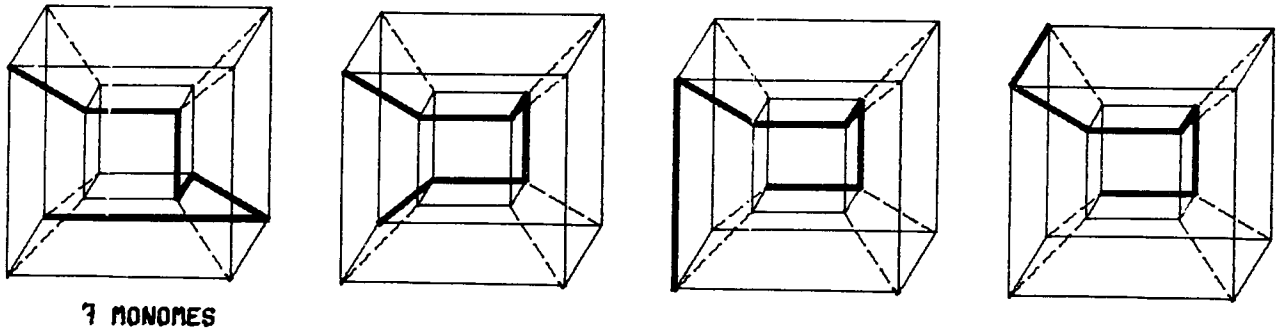




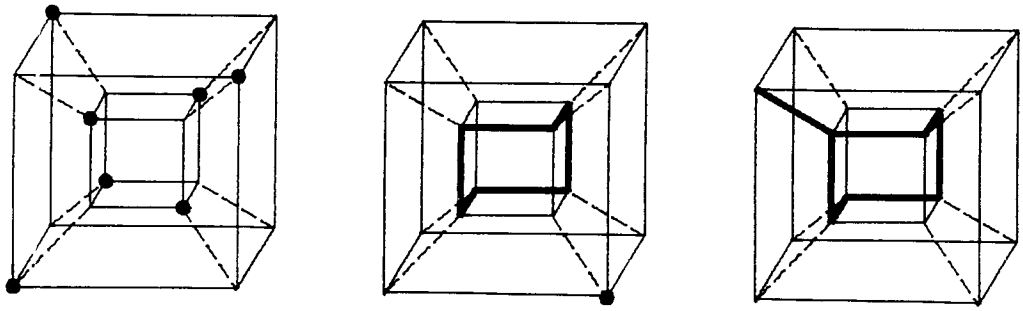
6 MONOMES







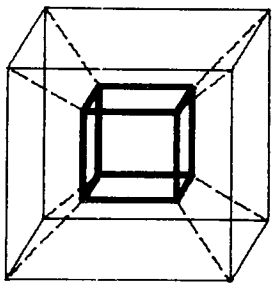
7 MONOMES



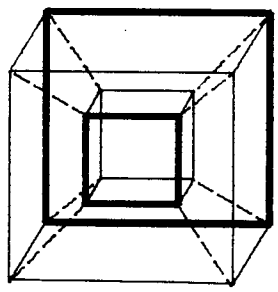
8 POINTS

1_1 2_1 3_6 4_{15} 5_{18} 6_9 7_{15} 8_9

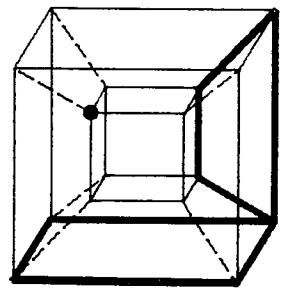
1 MONOME

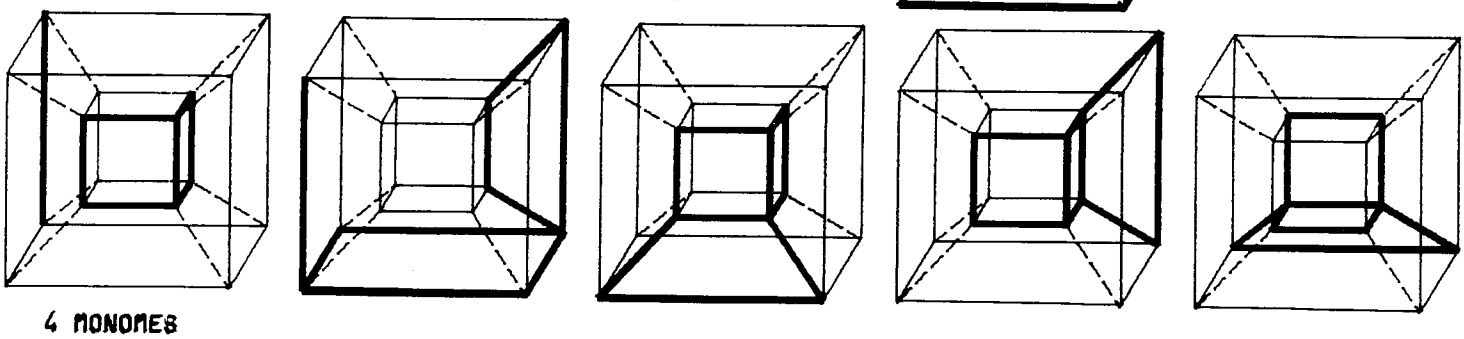


2 MONOMES

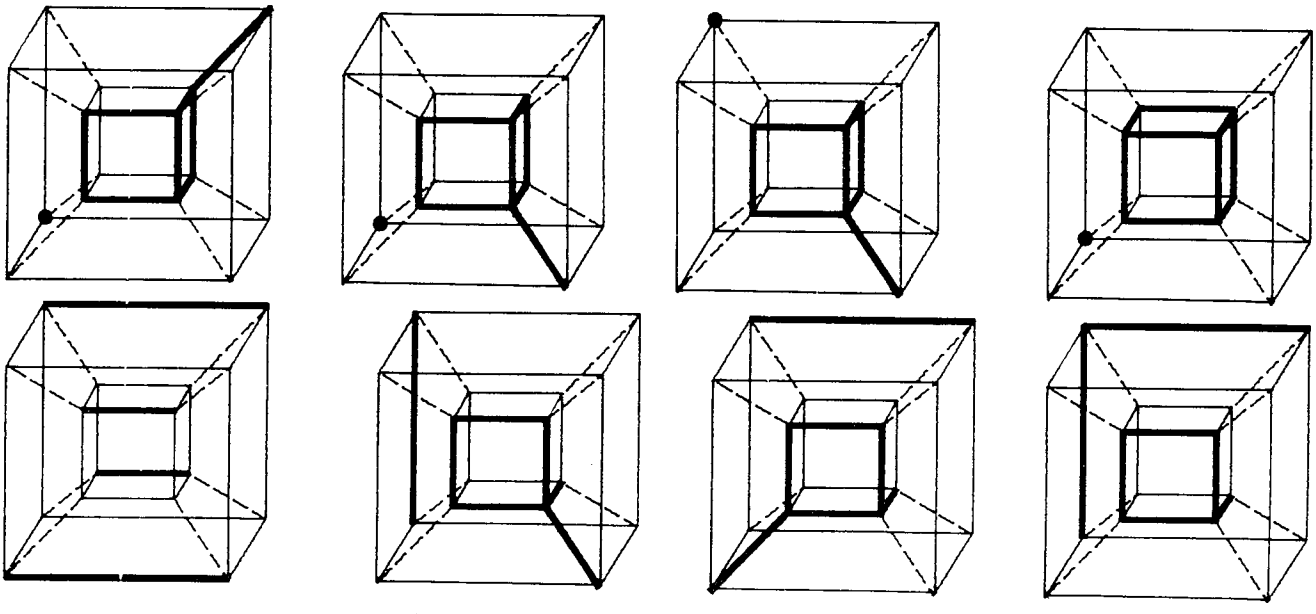


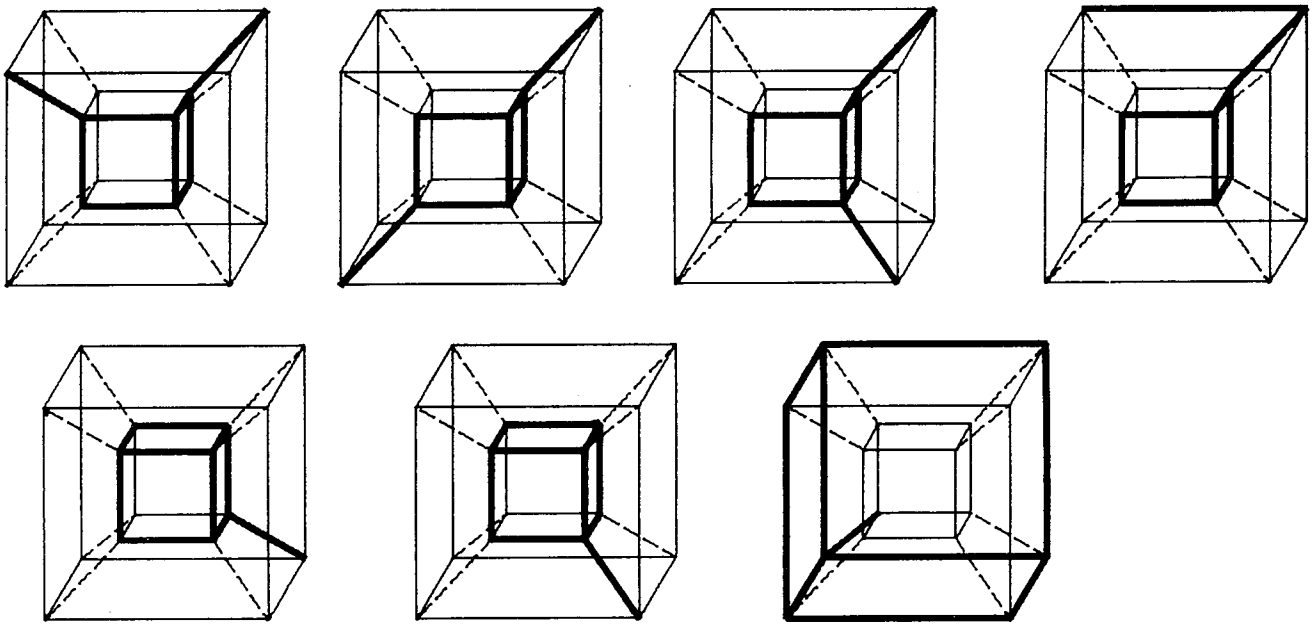
3 MONOMES



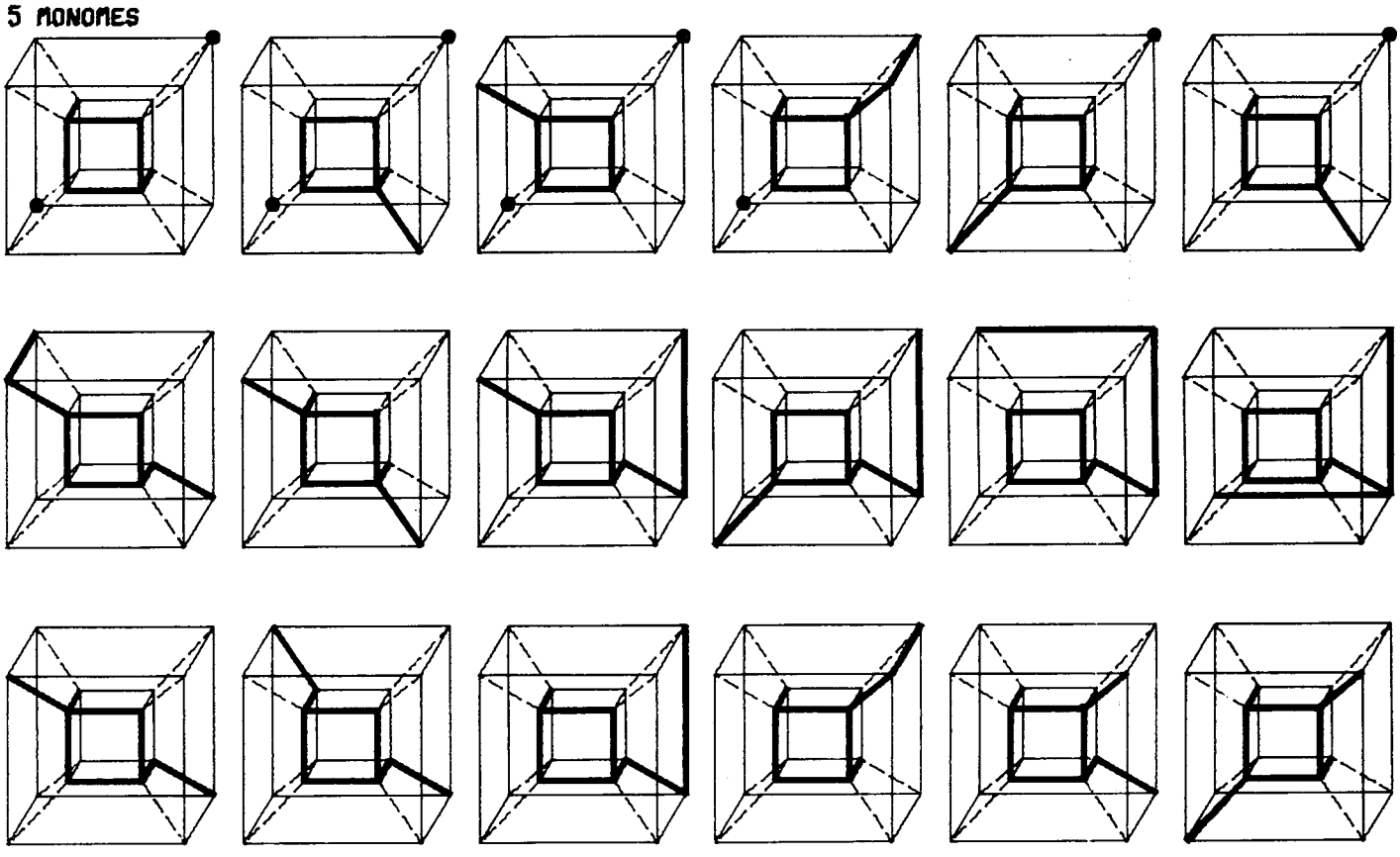


4 MONOMES

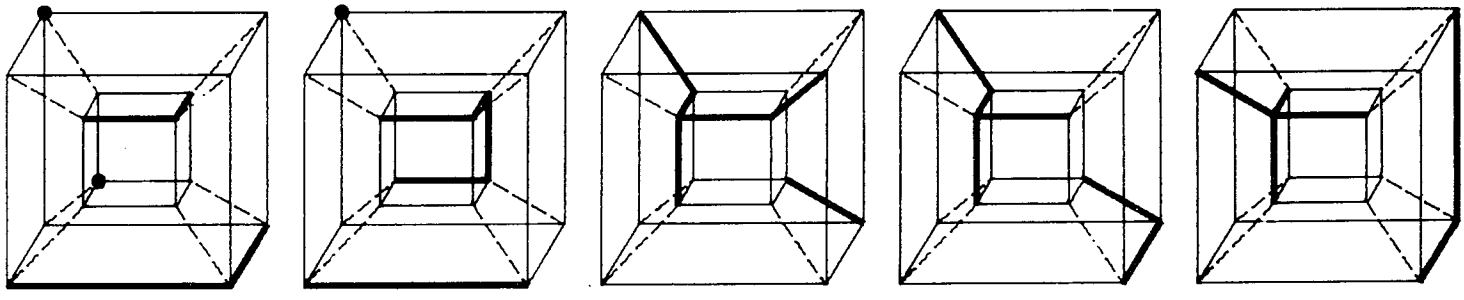


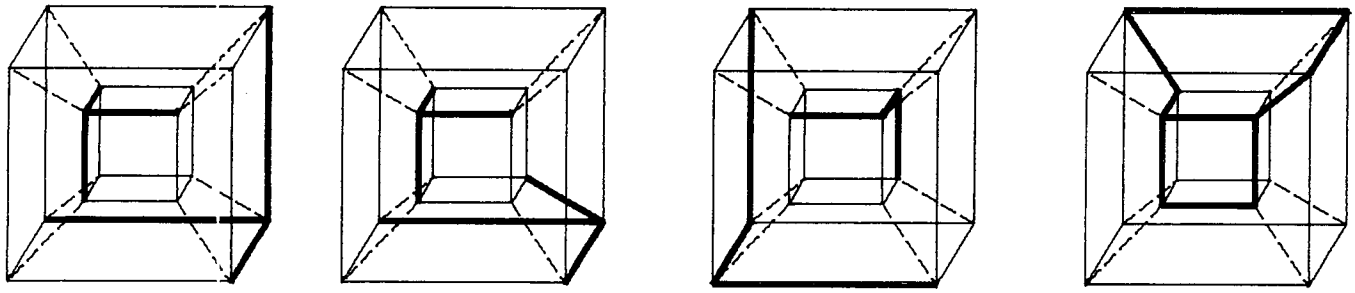


5 MONOMES

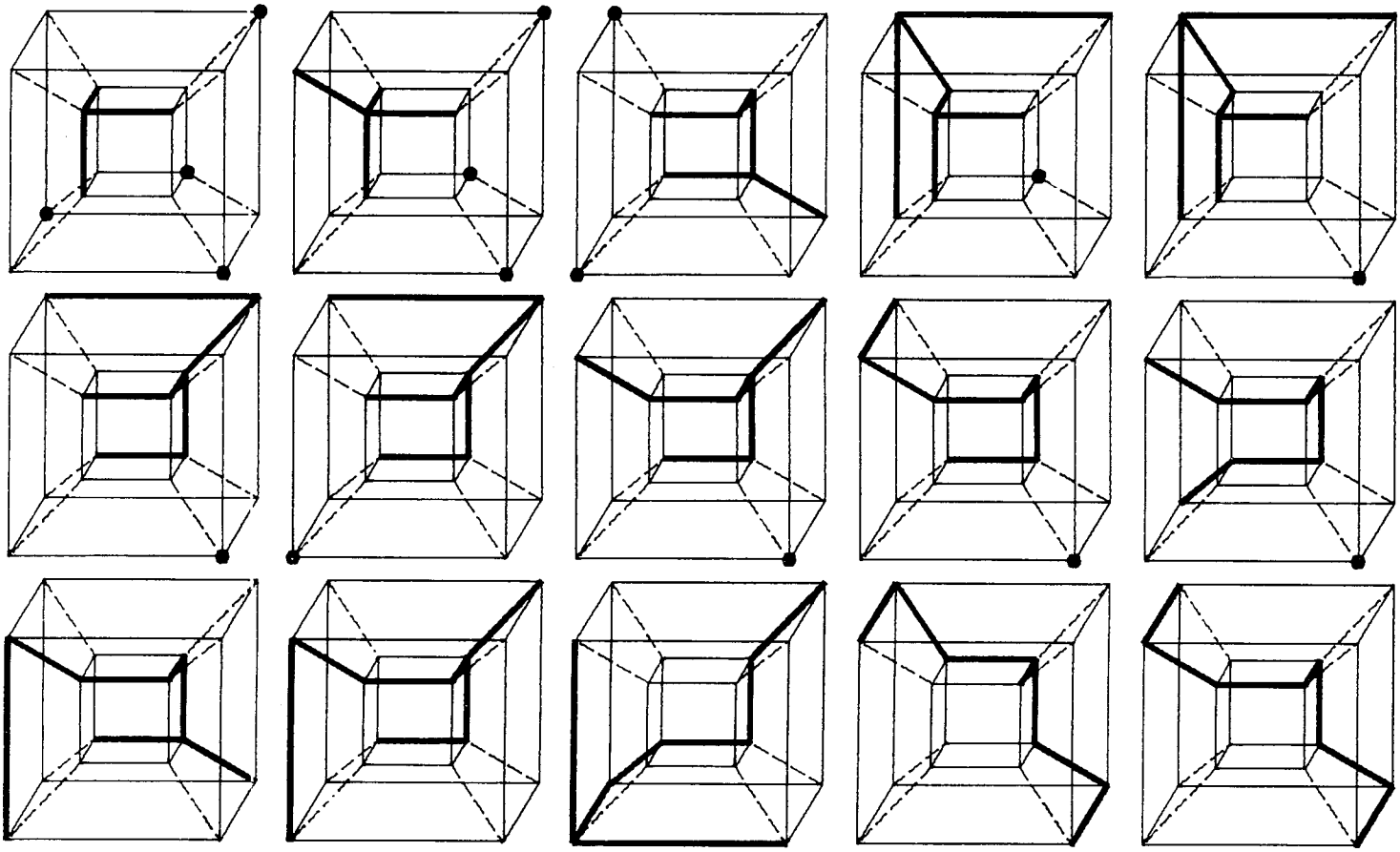


6 MONOMES

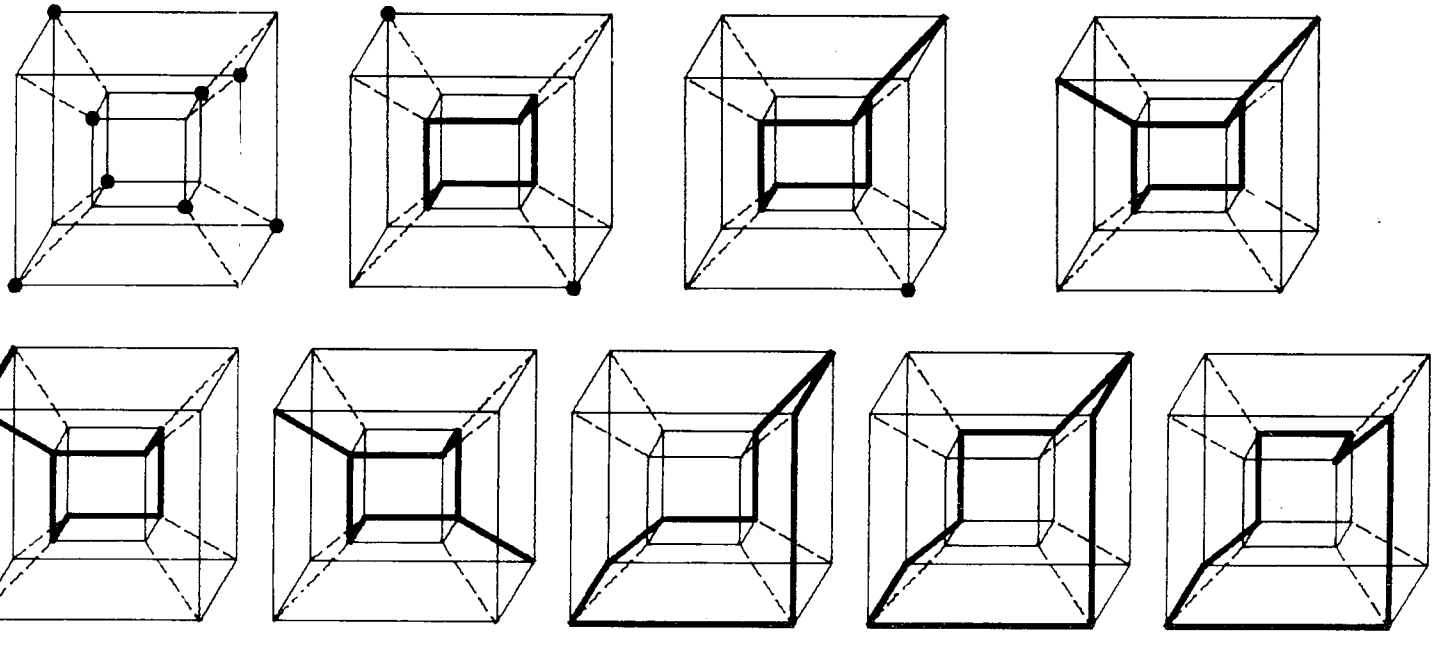




7 MONOMES

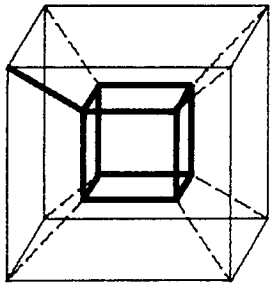


8 MONOMES

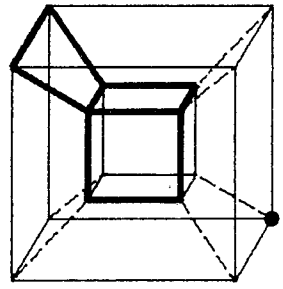


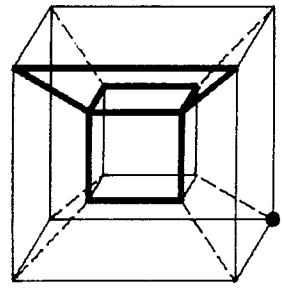
9 POINTS 2_1 4_{12} 5_{14} 6_{11} 7_6 8_5 9_6 10_1

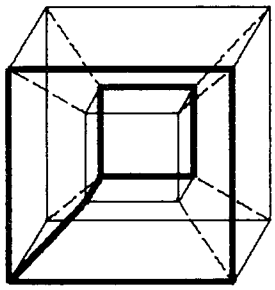
2 MONOMES

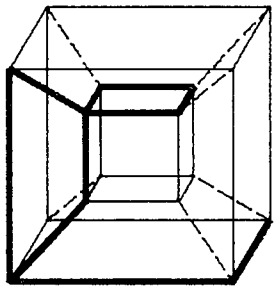


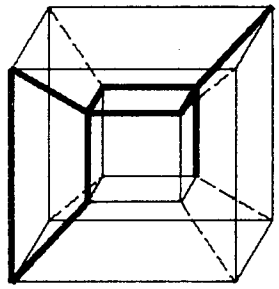
4 MONOMES

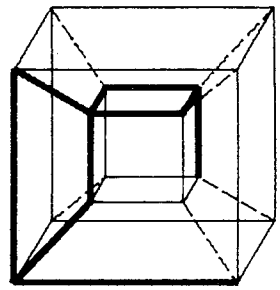


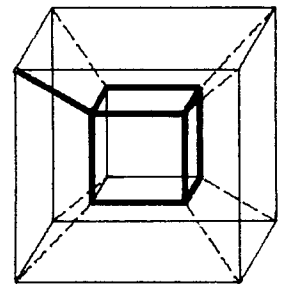


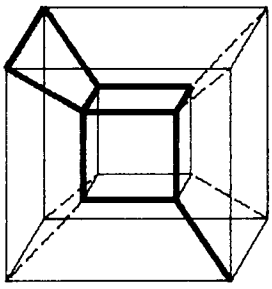


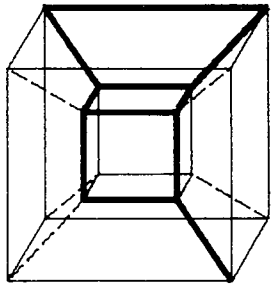


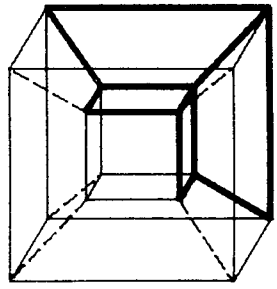


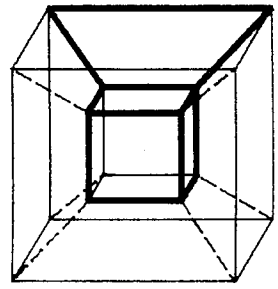


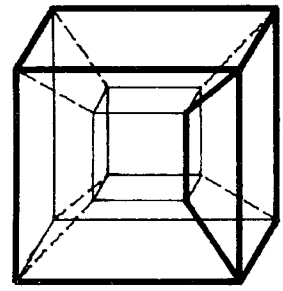




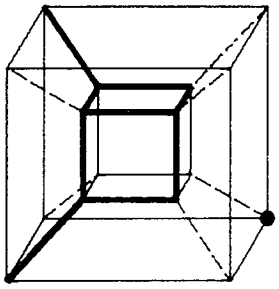


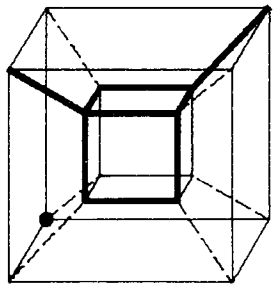


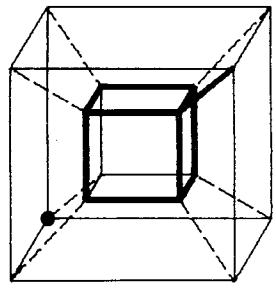


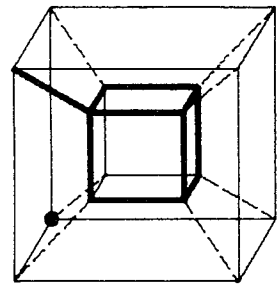


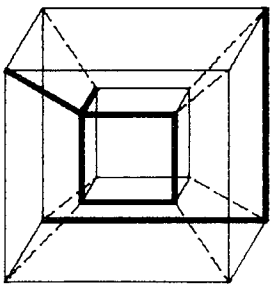
5 MONOMES

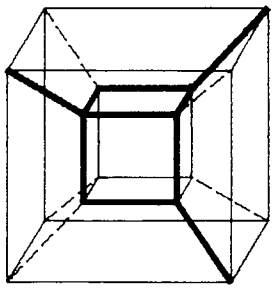


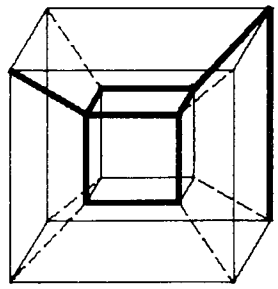


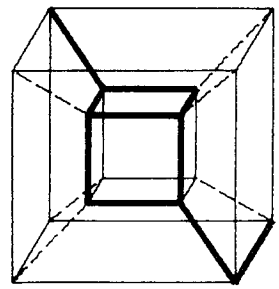


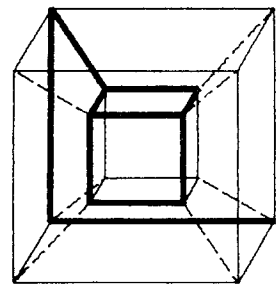


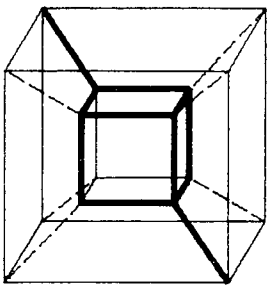


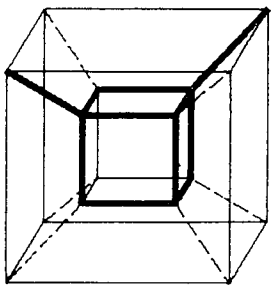


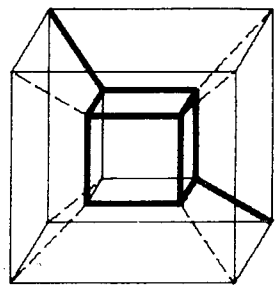


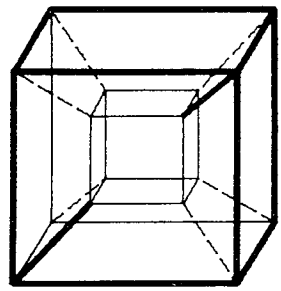


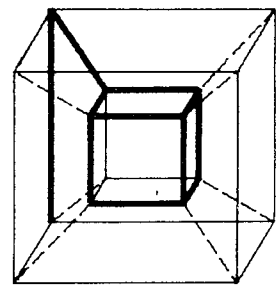




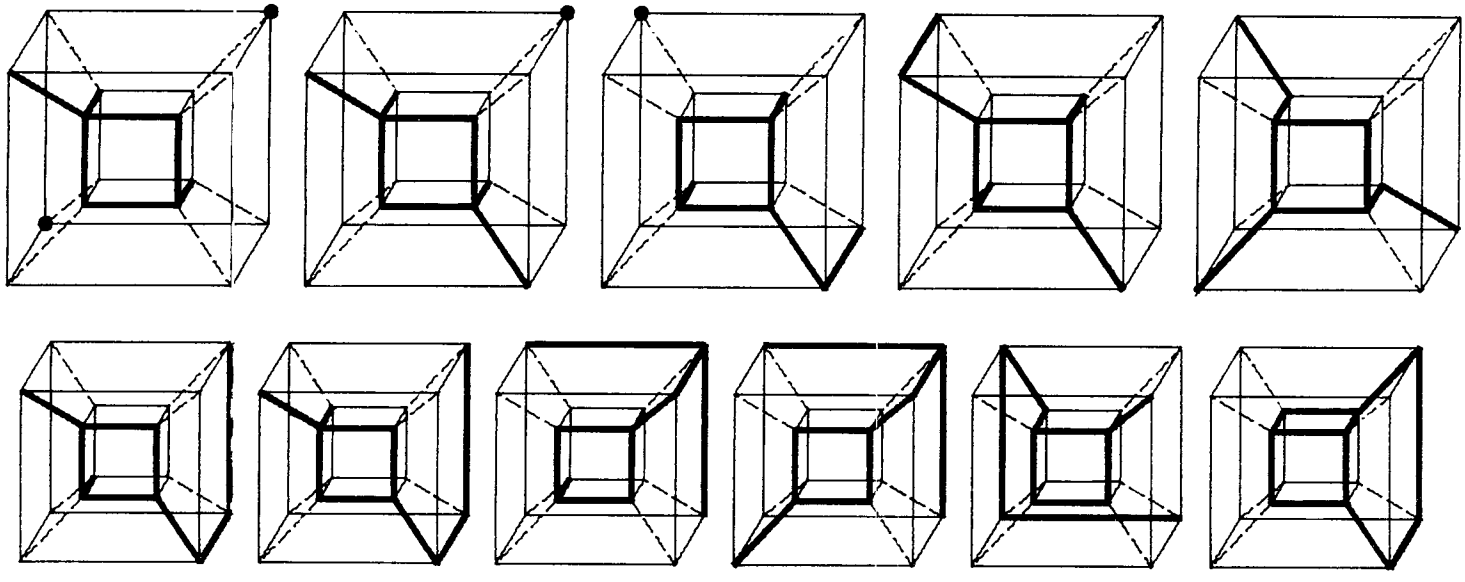




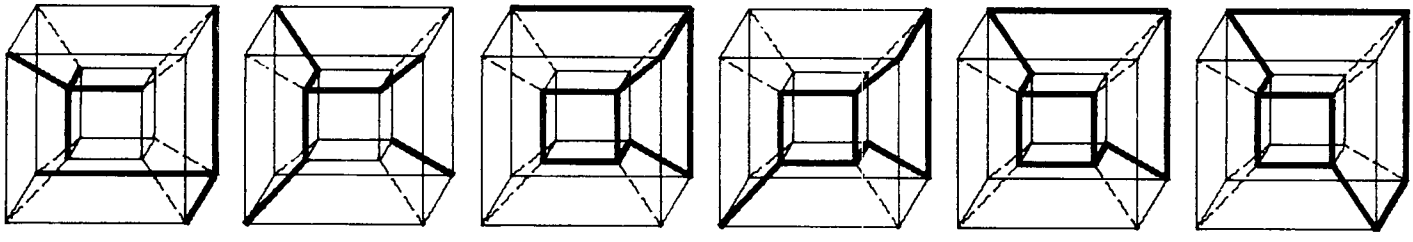




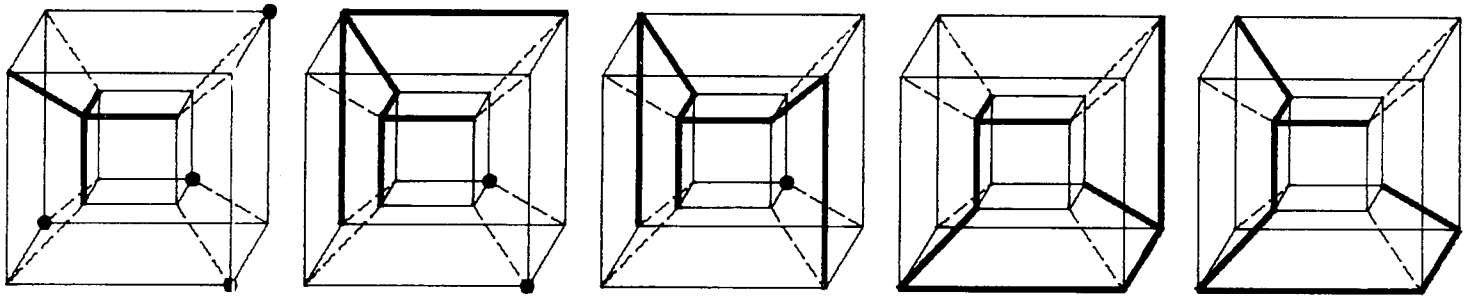
6 MONOMES



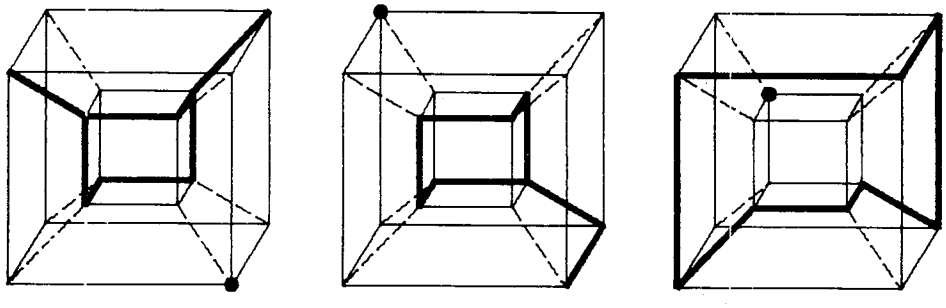
7 MONOMES



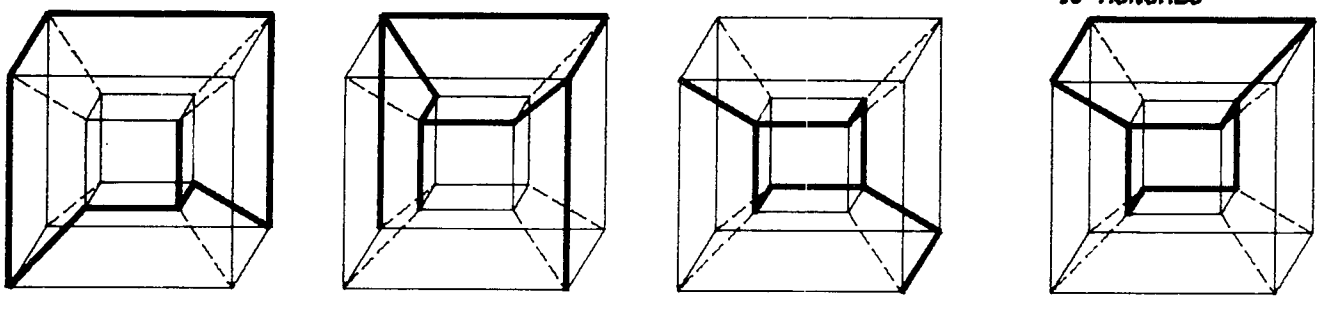
8 MONOMES



9 MONOMES

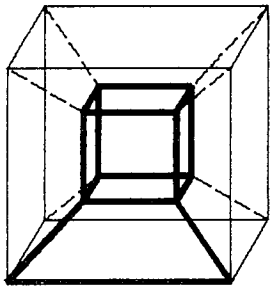


10 MONOMES

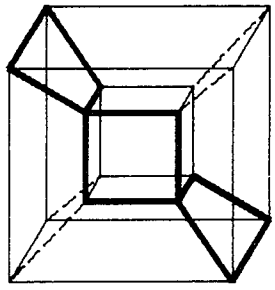


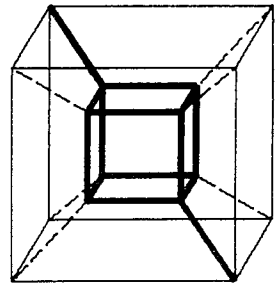
10 POINTS 2_1 3_3 4_2 5_{14} 6_{13} 7_7 8_4 9_1 10_3 11_1 12_1

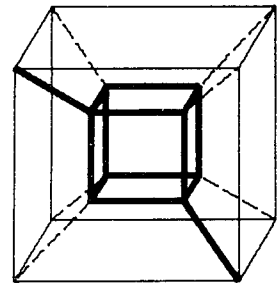
2 MONOMES



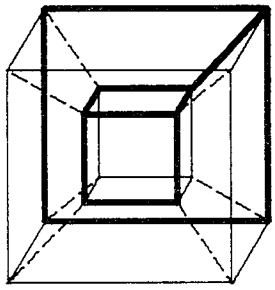
3 MONOMES

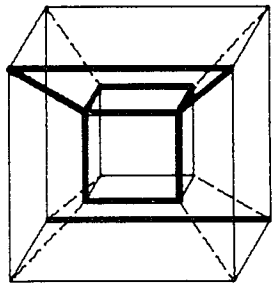




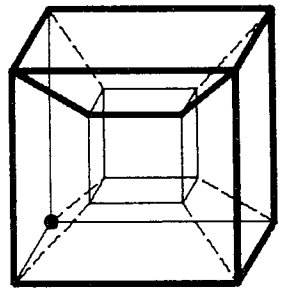


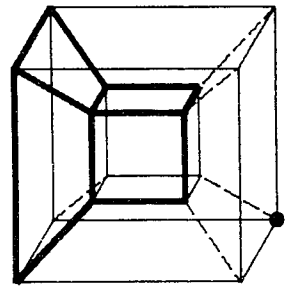
4 MONOMES

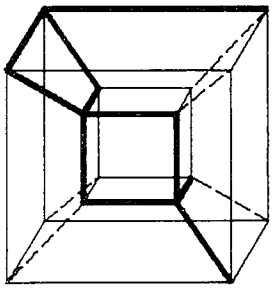


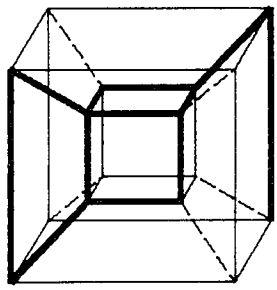


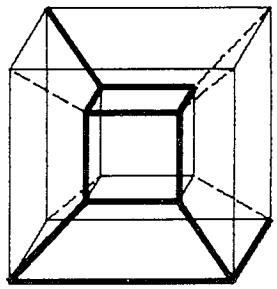
5 MONOMES

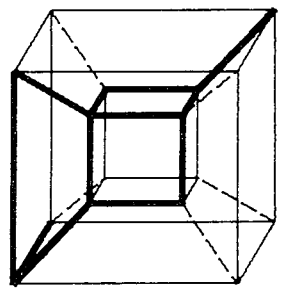


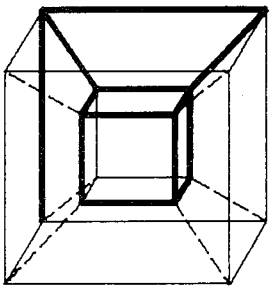


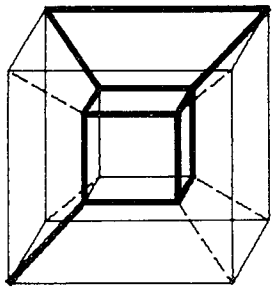


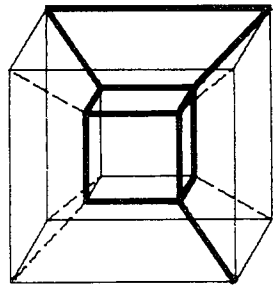


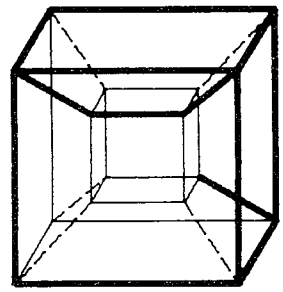


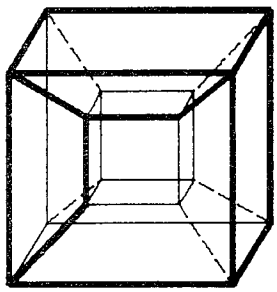


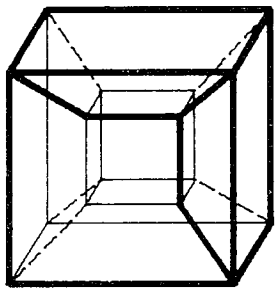


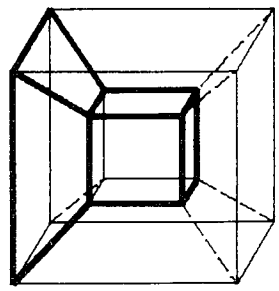


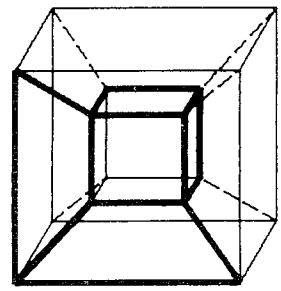




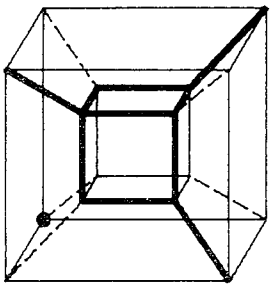


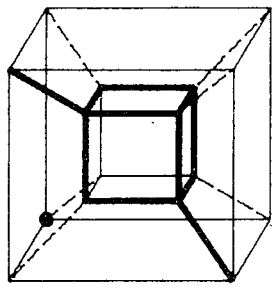


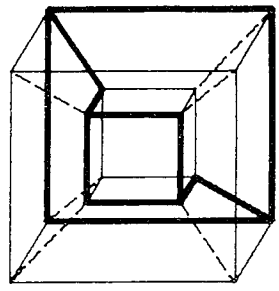


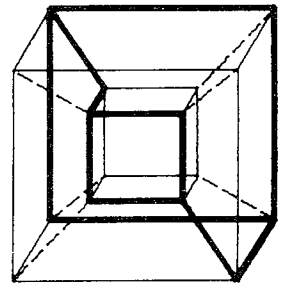


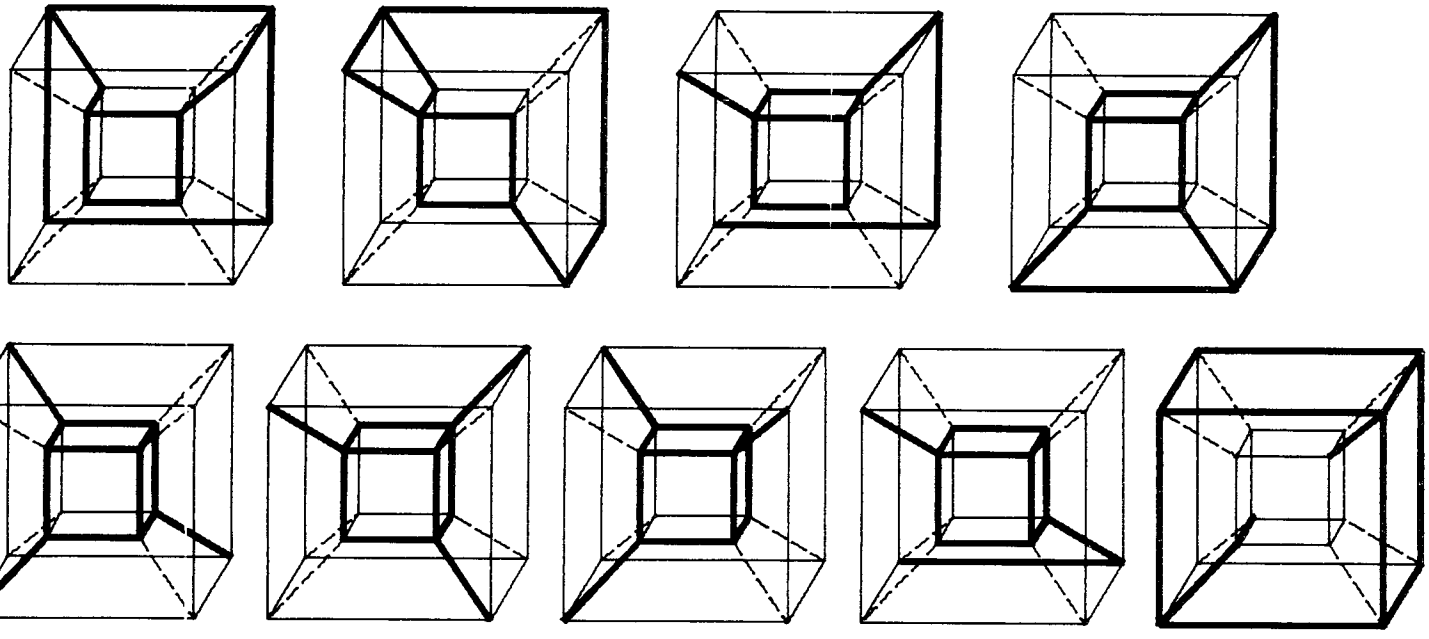
6 MONOMES



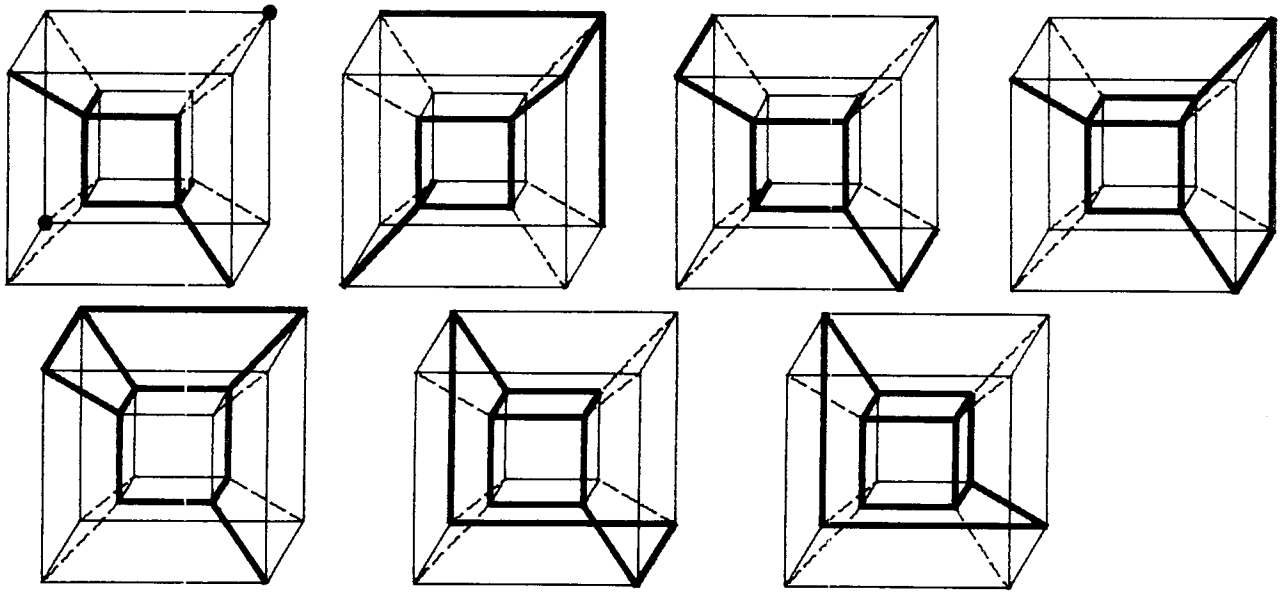






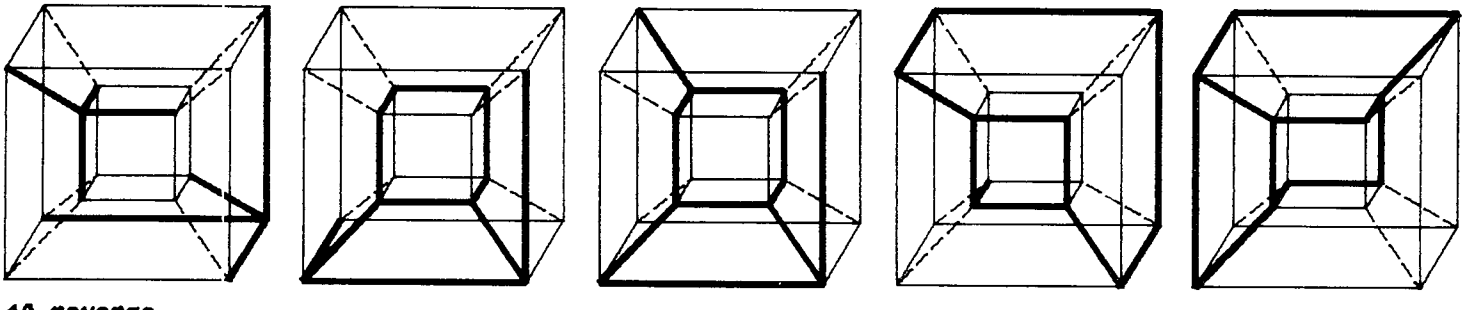


7 MONOMES



8 MONOMES

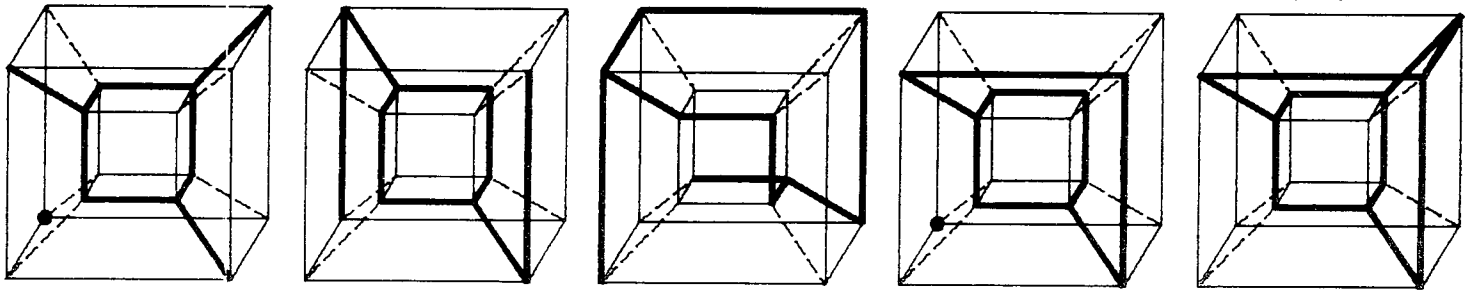
9 MONOMES



10 MONOMES

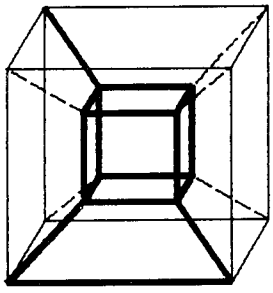
11 MONOMES

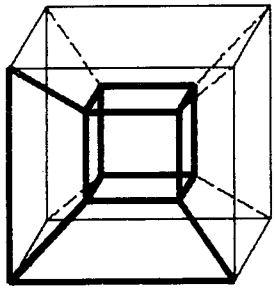
12 MONOMES



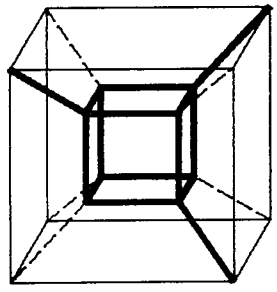
11 POINTS 3_2 4_1 5_2 6_{12} 7_4 8_3 9_1 10_1 13_1

3 MONOMES

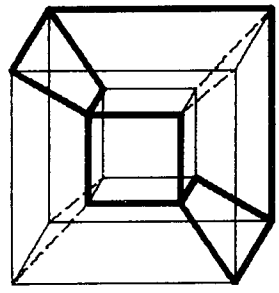


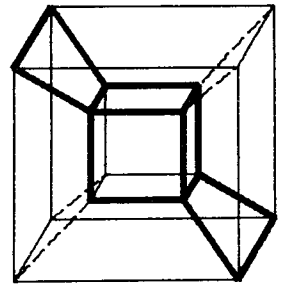


4 MONOMES

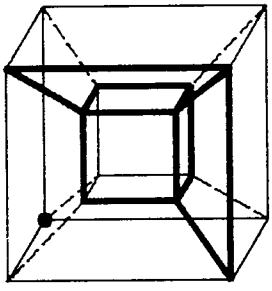


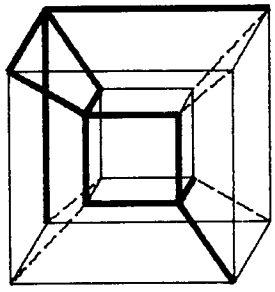
5 MONOMES

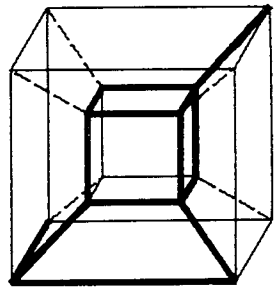


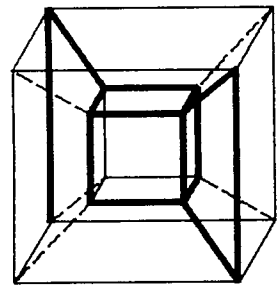


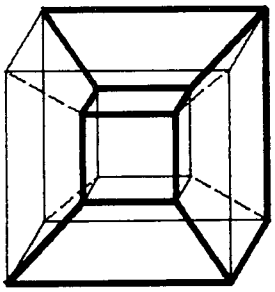
6 MONOMES

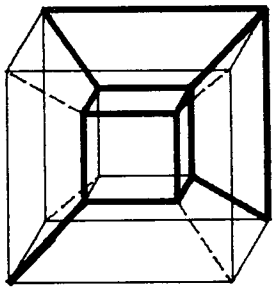


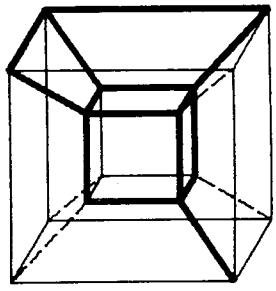


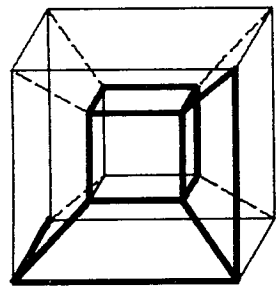


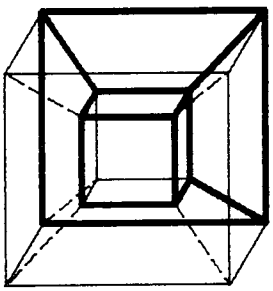


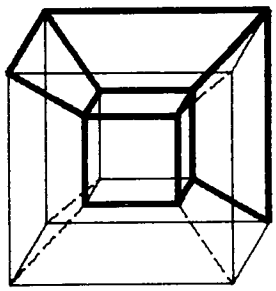


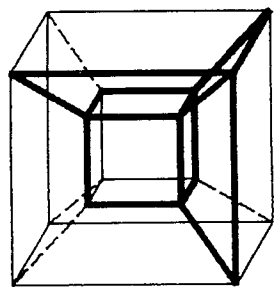


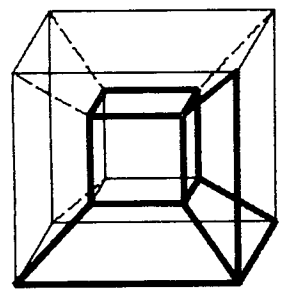




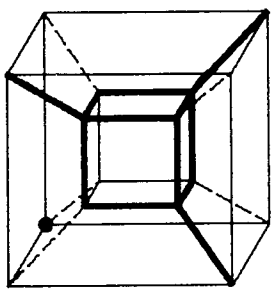


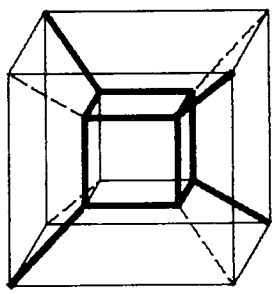


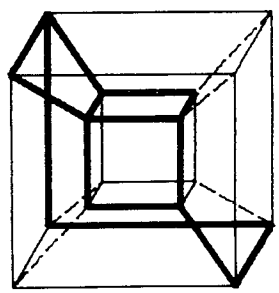


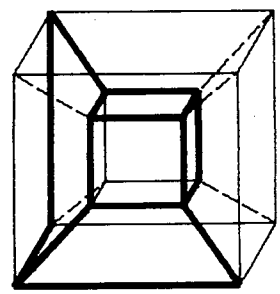


7 MONOMES

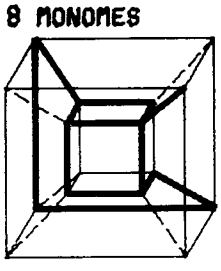


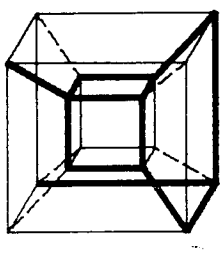


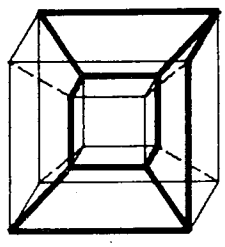




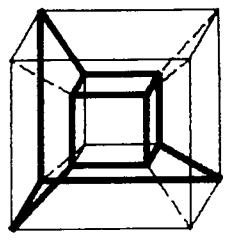
8 MONOMES



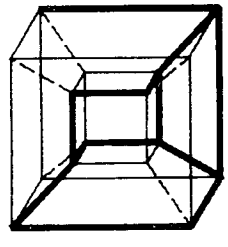




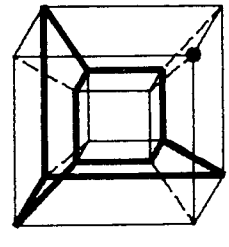
9 MONOMES



10 MONOMES

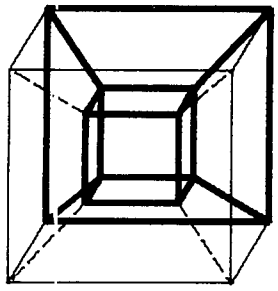


13 MONOMES

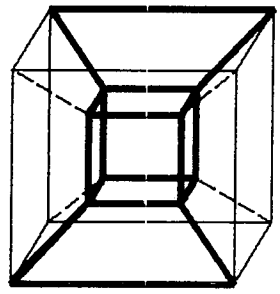


12 POINTS 2_1 3_1 4_4 5_1 6_1 7_7 8_2 10_2

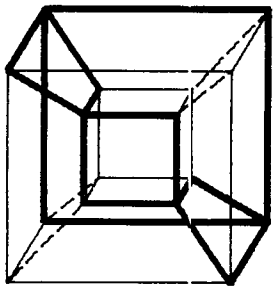
2 MONOMES

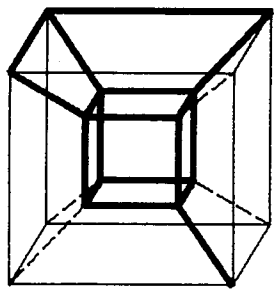


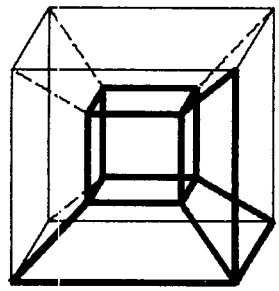
3 MONOMES

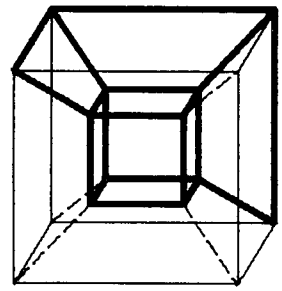


4 MONOMES

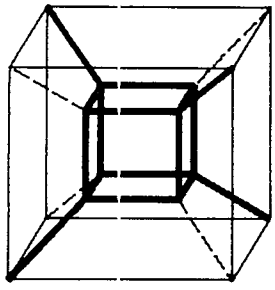




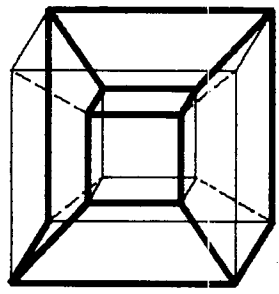




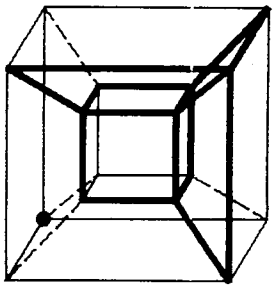
5 MONOMES

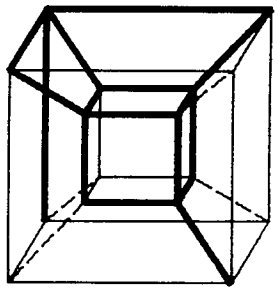


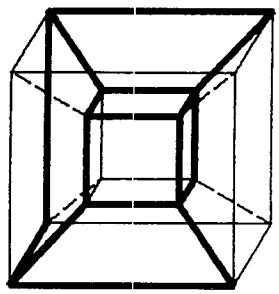
6 MONOMES

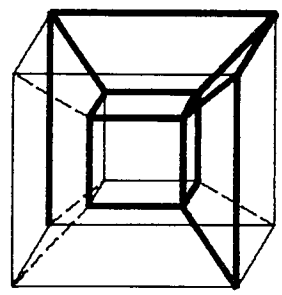


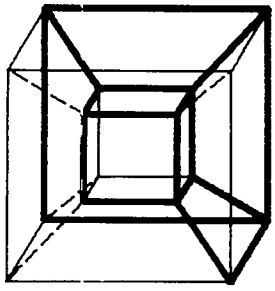
7 MONOMES

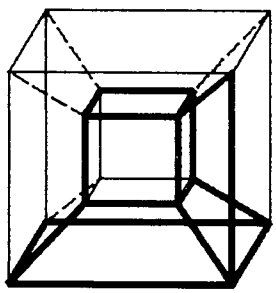


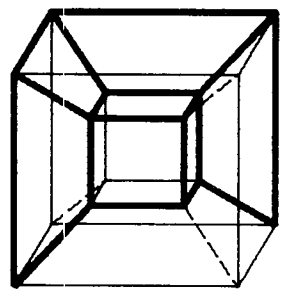




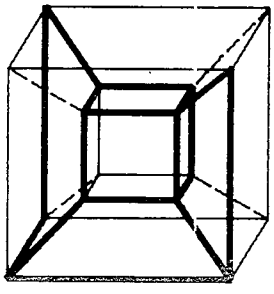


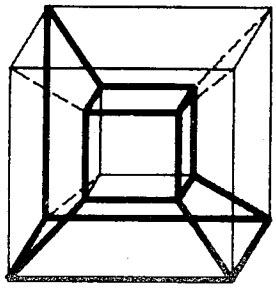




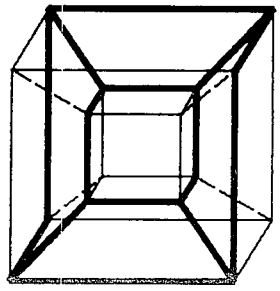


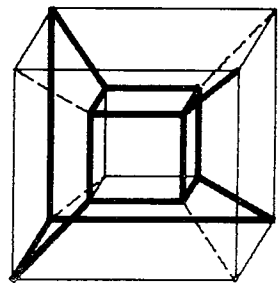
8 MONOMES





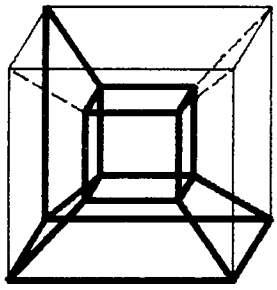
10 MONOMES



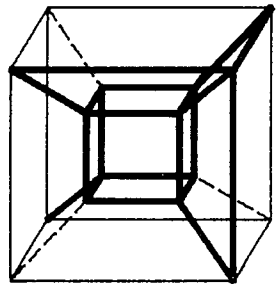


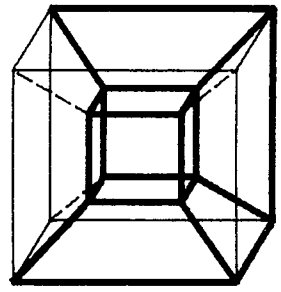
13 POINTS 3_1 5_2 8_1 9_2

3 MONOMES

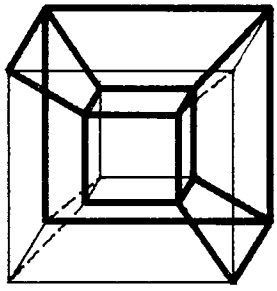


5 MONOMES

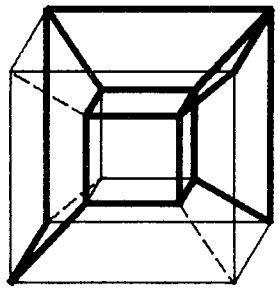


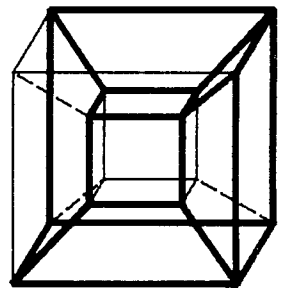


8 MONOMES



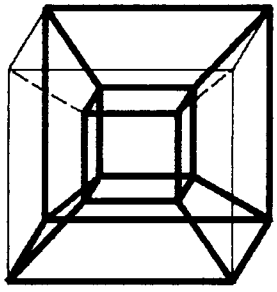
9 MONOMES



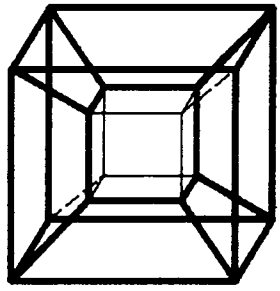


14 POINTS 3_1 4_1 7_1 12_1

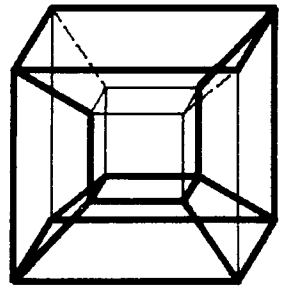
3 MONOMES



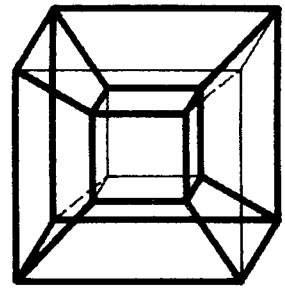
4 MONOMES



7 MONOMES

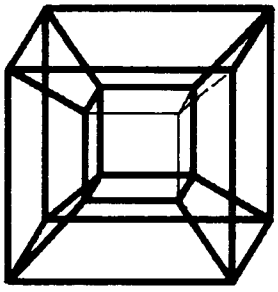


12 MONOMES



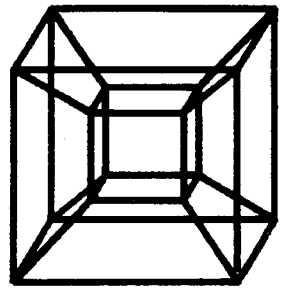
15 POINTS

4 MONOMES



16 POINTS

1 MONOME



Liste de 216 codes de fonctions de 4 variables.

Les codes sont donnés selon l'ordre lexicographique n < n+1... < n'.
Un exposant indique un facteur de répétition (dont on a fait abstraction dans le classement) , s'il vaut 1 ou 4 il n'est pas indiqué.
Enfin, l'indication $A_B C$ signifie que le code de la même ligne correspond à la Ce fonction du catalogue, de A points et B monômes premiers.

1

(1 21)^3 (1 23)

(1 22)

(1 22)^2 (1 23)^2

(1 31)^2 (1 32)^2

(1 31)^2 (1 32) (21 22)

(1 31)^2 (21 23)^2

(1 32)^2 (1 33) (21 22)

(1 32)^2 (21 21)^2

(1 32) (21 22)^2 (22 23)

(1 32)^2 (21 23) 22

(1 33)

(1 33)^2 22^2

(1 33) (22 23)^3

(1 41)^2 (21 32)^2

(1 42) (21 31)^2 (22 32)

(1 42) (21 32)^2 (22 33)

(1 43)

(1 43) (1 45)^2 (21 31)

(1 43) (1 46) (22 31)^2

(1 43) (23 31)^3

(1 44) (22 32)^3

(1 44) (22 33)^3

(1 45) (1 46) (21 32) (22 31)

(1 45)^2 (21 31)^2

(1 45) (21 32) (22 31) (23 31)

(1 46) (21 31) (21 32)^2

(1 46)^2 (21 33)^2

(1 46) (21 33) (22 31) (22 32)

(1 46) (22 32)^2 (23 31)

(1 1') (31 31')^3

(1 1') (31 31')^2(41 43)

(1 1') (31 31') (41 45)^2

(1 1') (41 46)^3

(1 21') (21 31') (31 41) (31 45)

(1 21') (21 31')^2(31 43)

(1 21') (32 41)^2 (31 46)

(1 22') (22 31') (31 43)^2

(1 22') (22 31') (31 45)^2

(1 22') (31 45)^2 (32 41)

(1 22') (31 46)^2 (33 41)

(1 23') (31 43) (31 45)^2

(1 23') (31 46)^3

(1 31') (21 41) (21 45)^2

(1 31')^2 (21 43)^2

(1 31') (21 45) (22 41) (31 32)

(1 31')^2 (21 45) 31

(1 31') (23 41) (31 32)^2

(1 31')^2 31^2

(1 32') (21 43) (22 45) 31

(1 32') (21 45)^2 (22 43)

(1 32') (21 45) 31 (31 32)

(1 32') (21 46)^2 (31 33)

(1 32') (22 46) (31 32)^2

(1 32') (31 32)^2 (31 33)

(1 33') (22 43)^3

(1 33') (22 45)^2 (31 32)

(1 33') (22 46) (31 33)^2

(1 33') (31 32)^3

21^3 23

(21 31)^2 (21 32) (23 32)

(21 32)^2 (22 32)^2

(21 33) (22 32)^2 (23 33)

(21 41)^2 (21 42) (32 32)

(21 42) (21 45) (22 46) (31 32)

(21 42)^3 33

(21 43) (22 46) (31 32)^2

(21 44) (22 46)^2 (32 33)

(21 45)^2 (23 45) 31

(21 45) (31 32)^2 32

(21 46)

(21 46) (22 42) (31 32) (32 33)

(21 46)^2 (22 45)^2

(21 46) (22 45)^2 (23 43)

(21 46)^2 31 32

(21 21')^2(31 31')^2

(21 21') (31 32') (32 31') (41 45)

(21 21')^2 41 45

(21 21') (41 42)^2 46

(21 21')^3 43

(21 22') (22 21') (31 31') (43 45)

(21 22') (31 31')^2(32 31')

(21 22') (31 32')^2(33 31')

(21 22') (31 32') (41 46) (45 46)

(21 23') (31 31')^2 45

(21 23') (31 32')^2(43 46)

(21 31')

(21 31') (21 32') (22 31') (31 45)

(21 31') (21 32') (31 41) (32 45)

(21 31') (23 31') (31 45)^2

(21 31') (31 42) (32 41) (32 46)

(21 32') (22 32') (31 45) (32 43)

(21 32') (31 42)^2 (33 46)

(21 32') (31 45) (31 46) (32 45)

(21 32')^2(31 46)^2

(21 32')^2(33 43)^2

(21 33') (22 31')^2(32 43)

(21 33') (22 32') (31 46) (33 45)

(21 33') (31 46)^2 (32 46)

22

2_2 3

3_2 2

3_3 3

3_3 2

4_3 6

4_3 7

4_3 5

4_3 2

4_2 3

4_3 3

4_3 1

4_4 3

4_4 4

4_4 2

5_2 1

5_3 4

5_3 1

5_4 14

5_4 15

5_4 13

5_4 12

5_4 1

5_5 1

5_4 9

5_4 17

5_4 10

5_3 3

5_4 7

5_4 6

5_4 8

8_4 15

8_4 14

8_4 13

8_4 4

7_3 4

7_3 5

7_3 1

7_4 9

7_4 10

7_4 11

7_4 4

7_3 3

7_3 2

6_3 6

6_3 7

6_3 3

6_3 8

6_3 2

6_3 9

6_5 21

6_5 20

6_5 19

6_5 17

6_5 18

6_5 16

6_5 9

6_5 13

6_5 6

6_4 6

4_2 2

5_3 3

5_3 2

5_4 2

6_2 1

6_4 9

6_3 4

6_4 7

6_5 3

6_5 22

6_4 8

6_4 14

6_4 4

6_5 15

6_5 12

8_4 13

8_3 4

8_4 12

8_3 5

8_3 3

8_3 6

8_4 11

8_3 3

8_5 16

8_5 15

8_6 9

8_8 5

7_2 1

7_4 13

7_4 14

7_4 12

7_3 3

7_6 16

7_5 7

7_6 21

7_6 20

7_6 15

7_4 3

7_6 9

7_5 6

4_4 5

22^2 23^2	4_4 6
$(22\ 31)^2$ $(22\ 32)^2$	5_4 4
$(22\ 31)^2$ $(23\ 32)^2$	5_4 5
$(22\ 32)$ $(22\ 33)$ $(23\ 32)^2$	5_4 3
$(22\ 33)$	5_5 3
$(22\ 41)^2$ 32^2	6_3 1
$(22\ 42)$ $(22\ 44)$ 32^2	6_4 2
$(22\ 42)^2$ 31^2	6_4 10
$(22\ 43)$ $(22\ 46)^2$ $(31\ 33)$	6_5 5
$(22\ 43)$ $(23\ 45)^2$ $(31\ 32)$	6_5 11
$(22\ 44)^2$ 33^2	6_6 1
$(22\ 45)$ $(23\ 46)$ $(31\ 33)$ 32	6_5 7
$(22\ 45)^2$ $(31\ 32)^2$	6_5 14
$(22\ 46)^2$ $(23\ 45)$ 32	6_5 8
$(22\ 46)$ $(31\ 32)$ 32^2	6_4 5
$(22\ 46)$ $(31\ 33)$ $(32\ 33)^2$	6_5 2
$(22\ 21')$ $(31\ 31')^2(31\ 32')$	8_4 9
$(22\ 21')$ $(31\ 33')$ $(32\ 31')^2$	8_4 2
$(22\ 21')$ $(32\ 31')$ $(41\ 46)$ $(45\ 46)$	8_4 1
$(22\ 22')$ $(31\ 32')$ $(32\ 31')$ 45	8_5 17
$(22\ 22')$ $(31\ 33')$ $(33\ 31')$ $(43\ 46)$	8_5 6
$(22\ 22')$ $(41\ 42)$ 45^2	8_5 14
$(22\ 22')$ $(41\ 44)$ 46^2	8_5 1
$(22\ 22')^2(43\ 45)^2$	8_5 8
$(22\ 22')^2$ 45^2	8_5 18
$(22\ 23')$ $(31\ 32')$ $(43\ 45)^2$	8_8 4
$(22\ 23')$ $(31\ 33')$ $(45\ 46)^2$	8_8 3
$(22\ 31')$ $(23\ 31')$ $(31\ 46)$ $(32\ 45)$	7_4 7
$(22\ 31')^2(31\ 46)^2$	7_4 5
$(2\ 31')^2$ $(32\ 41)$ $(32\ 45)^2$	7_4 8
$(22\ 31')$ $(32\ 46)^2$ $(33\ 41)$	7_4 1
$(22\ 32')$ $(22\ 33')$ $(32\ 45)^2$	7_6 12
$(22\ 32')$ $(31\ 42)$ $(31\ 45)^2$	7_6 19
$(22\ 32')^2(31\ 43)^2$	7_6 14
$(22\ 32')$ $(31\ 44)$ $(32\ 46)^2$	7_6 7
$(22\ 32')$ $(31\ 46)$ $(32\ 43)$ $(33\ 45)$	7_6 10
$(22\ 32')$ $(31\ 46)$ $(32\ 45)$ $(32\ 46)$	7_6 13
$(22\ 33')$ $(31\ 42)$ $(32\ 45)^2$	7_5 11
$(22\ 33')$ $(31\ 44)$ $(33\ 46)^2$	7_6 2
$(23\ 33)$	5_5 2
$(23\ 42)$ 31^2 32	6_4 11
$(23\ 42)$ 32^2 33	6_4 1
$(23\ 43)$	6_5 10
$(23\ 44)$ $(32\ 33)^3$	6_5 1
$(23\ 46)^2$ $(32\ 33)^2$	6_5 4
$(23\ 21')$ $(31\ 31')^2$ 45	8_4 10
$(23\ 21')$ $(32\ 31')^2(43\ 46)$	8_4 3
$(23\ 22')$ $(32\ 31')$ $(43\ 45)^2$	8_5 13
$(23\ 22')$ $(33\ 31')$ $(45\ 46)^2$	8_5 5
$(23\ 23')$ 43 45^2	8_8 6
$(23\ 23')$ 46^3	8_8 2
$(23\ 31')^2(32\ 43)^2$	7_4 6
$(23\ 32')$ $(31\ 43)$ $(31\ 45)$ $(32\ 45)$	7_6 17
$(23\ 32')$ $(32\ 45)^2$ $(33\ 43)$	7_6 11
$(23\ 32')$ $(32\ 46)^2$ $(33\ 46)$	7_6 6
$(23\ 33')$ $(22\ 43)^3$	7_5 9
$(23\ 33')$ $(32\ 46)$ $(33\ 45)^2$	7_6 5
$(22\ 33')^2(33\ 43)^2$	7_6 4

31^2 32^2	6_4 12
$(31\ 41)^2$ $(32\ 42)^2$	7_3 2
$(31\ 43)$ $(31\ 46)$ $(32\ 46)^2$	7_5 5
$(31\ 45)$ $(31\ 46)$ $(32\ 42)$ $(32\ 46)$	7_5 8
$(31\ 45)^2$ $(32\ 45)^2$	7_6 18
$(31\ 46)^2$ $(33\ 42)^2$	7_5 3
$(31\ 31')$ $(31\ 32')$ $(32\ 31')$ $(32\ 32')$	8_5 10
$(31\ 31')$ $(31\ 32')$ $(32\ 31')$ $(45\ 46)$	8_5 9
$(31\ 31')$ $(32\ 32')^2(41\ 43)$	8_5 12
$(31\ 31')$ $(32\ 32')$ $(41\ 45)$ $(42\ 45)$	8_5 11
$(31\ 31')$ $(41\ 46)$ $(42\ 46)^2$	8_4 8
$(31\ 32')$	8_8 7
$(31\ 32')$ $(31\ 33')$ $(32\ 32')$ $(45\ 46)$	8_7 13
$(31\ 32')^2(33\ 32')$ $(42\ 43)$	8_7 14
$(31\ 32')^2(42\ 45)$ 46	8_7 15
$(31\ 32')^3(43\ 44)$	8_7 7
$(31\ 32')^2$ 45^2	8_8 8
$(31\ 33')^2(33\ 32')^2$	8_7 14
$(31\ 33')^2$ 46^2	8_6 7
32^2 $(32\ 33)^2$	6_4 3
32 $(33\ 31')^2$ 46	8_5 3
$(32\ 42)$ $(32\ 45)$ $(32\ 46)$ $(33\ 46)$	7_5 2
$(32\ 42)^3$ $(33\ 44)$	7_4 2
$(32\ 43)$ $(32\ 45)^2$ $(32\ 46)$	7_5 10
$(32\ 44)$ $(32\ 46)^2$ $(33\ 42)$	7_5 1
$(32\ 44)^2$ $(33\ 46)^2$	7_6 1
$(32\ 46)$	7_5 4
$(32\ 46)^2$ $(33\ 45)^2$	7_6 8
$(32\ 31')$	8_3 1
$(32\ 31')$ $(32\ 32')$ $(33\ 31')$ $(45\ 46)$	8_5 4
$(32\ 31')$ $(32\ 33')^2(42\ 43)$	8_4 6
$(32\ 31')^2(42\ 45)$ 46	8_4 7
$(32\ 31')^2$ 45^2	8_5 7
$(32\ 32')$ $(32\ 33')$ $(33\ 32')$ $(45\ 46)$	8_7 8
$(32\ 32')^3(33\ 33')$	8_7 6
$(32\ 32')$ $(33\ 33')$ $(42\ 45)^2$	8_6 3
$(32\ 32')$ $(42\ 46)^2$ $(44\ 46)$	8_6 2
$(32\ 32')^2$ 46^2	8_7 9
$(32\ 32')$ $(43\ 45)$ $(45\ 46)^2$	8_7 11
$(32\ 32')^2(43\ 46)$ 45	8_7 12
$(32\ 33')^2(33\ 31')^2$	8_5 2
$(32\ 33')$ $(33\ 32')$ $(44\ 45)$ 46	8_7 3
$(32\ 33')$ $(42\ 46)$ $(45\ 46)^2$	8_6 4
$(32\ 33')^2(43\ 46)^2$	8_6 5
33	6_6 7
$(33\ 44)$	7_7 1
$(33\ 44)$ $(33\ 46)^3$	7_6 2
$(33\ 32')$ $(42\ 46)$ $(45\ 46)^2$	8_7 10
$(33\ 32')^2(43\ 46)^2$	8_7 5
$(33\ 33')^3(43\ 44)$	8_7 2
$(33\ 33')$ $(44\ 46)^3$	8_7 1
41^2 42^2	8_2 1
42 45 46^2	8_6 8
42^3 44	8_4 5
$(42\ 44)^2$ 46^2	8_6 1
43 46^3	8_6 6
44	8_8 1
45	8_8 9

REFERENCES BIBLIOGRAPHIQUES


60984 81800

REFERENCES BIBLIOGRAPHIQUES

CHANG, C.L., LEE, C.T., "Symbolic Logic and Mechanical Theorem Proving" Academic Press, N.Y. (1973).

FORCADE, R., "Smallest Maximal Matching in the Graph of the d-Dimensional Cube", Journal of Combinatorial Theory (B) 14, p. 153-156 (1973).

FRAÏSSE, R., "Cours de logique mathématique", Gauthier-Villars, 2e édit. Paris (1971).

KREISEL, G., KRIVINE, J.L., "Eléments de logique mathématique - Théorie des modèles", Dunod édit. Paris (1967).

KUNTZMANN, J.,
- 1 "Algèbre de Boole", IV-24, p. 118 Dunod édit. Paris (1968).
- 2 "Algèbre de Boole", II-62, p. 72
- 3 "Algèbre de Boole", IV-11, p. 104
- 4 "Algèbre de Boole", V-17, p. 165
- 5 "Algèbre de Boole", VI-5, p. 95.

LABORDE, J.M.,
- 1 "Généralisation de l'algorithme d'exclusion", C.R.A.S. T. 273, p. 215-218 (1971).
- 2 "Type de fonction booléenne", Séminaire d'algèbre et combinatoire, U.S.M.Grenoble, séance du 17.3.75.
- 3 "Catalogue des 402 types de fonctions booléennes à 4 variables, classées suivant le poids des fonctions et le nombre de leurs monômes premiers", Bibliothèque des Mathématiques Appliquées, U.S.M. Grenoble (1975).
- 4 "Une question d'algèbre de Boole sur les fonctions irréductibles et le couplage Min-Max du n-cube", 1er Colloque International C.N.R.S. de Théorie des Graphes - Orsay (1976).

LEVY-BRUHL, J., "Introduction aux structures algébriques", Dunod édit. Paris (1968).

MAGNUS, W., KARRASS, A., SOLITAR, D., "Combinatorial Group Theory", Interscience, N.Y. (1966).

PICHAT, E., "Contribution à l'algorithmique non-numérique dans les ensembles ordonnés", Thèse Grenoble (1970).

ROBINSON, J.A., "A Machine-oriented Logic based on the Resolution principle", Journal of the A.C.M., 12, n° 1, p. 23-41 (1965).

SIMOES PEREIRA, J.M.S., (Universidade de Coïmbra - Portugal). " A note on finite Topologies and switching Functions", (article à paraître aux Discrete Mathematics).

TISON, P., "Théorie de consensus ; algorithme de recherche des bases premières", 25-29, Colloque d'algèbre de Boole de Grenoble, Janvier 1965.

ULAM, S.M., "Collection of Mathematical Problems", 29, N.Y. (1960).

dernière page de la thèse

AUTORISATION DE SOUTENANCE

VU les dispositions de l'article 5 de l'arrêté du 16 Avril 1974,

VU les rapports de M. ....Benzaken.....

M. .....Cheiss.....

M. .....Colmerauer.....

M. ...LABORDE.....Jean-Marie..... est autorisé à présenter une thèse en soutenance pour l'obtention du grade de DOCTEUR D'ETAT ES SCIENCES.

Fait à GRENOBLE, le

Le Président de l'U.S.M.G.

Le Président de l'I.N.P.G.

P.M. TR...