Hypercubes

par Gilles DUBOIS, Lycée de L'Isle Adam

1 Introduction

L'information peut être transmise sous forme de *messages* qui sont des suites de *caractères* appartenant à un même *alphabet*, sur l'emploi duquel sont tombés d'accord a priori l'expéditeur et le destinataire du message. C'est par exemple le cas d'un texte écrit en langue française.

Un message, pour parvenir à son destinataire, emprunte un *canal*.

Pour pouvoir être porteur d'information, un alphabet doit comporter au moins deux caractères distincts. En outre, le canal *binaire* est le plus simple qu'on puisse imaginer, c'est celui qui permet la transmission de deux caractères distincts et de deux seulement. La technologie actuelle fait que le canal binaire apparaît comme simple et assez naturel, une impulsion électrique en un intervalle de temps correspondant à l'envoi d'un des caractères, l'absence d'impulsion correspondant à la transmission de l'autre caractère.

Le canal binaire permet la transmission d'un message rédigé avec les caractères de n'importe quel alphabet pourvu qu'on se mette d'accord sur un *codage* préalable des caractères dudit alphabet.

En particulier, les caractères de n'importe quel alphabet peuvent être codés en des suites de symboles binaires ; la méthode la plus simple étant la suivante : m désignant le nombre de caractères distincts de l'alphabet initial à coder (alphabet A), on détermine d'abord le plus petit entier n tel que $2^n \geqslant m$. Cela fait, on établit une bijection entre A et une partie de $B = (\mathbb{Z}/2\mathbb{Z})^n$. Un élément de B se représente comme un n-uple $b = (b_1, \ldots, b_n)$ où $b_i = 0$ ou 1, ou bien plus simplement comme un nombre entre 0 et $2^n - 1$ écrit en base *deux*.

En pratique, des canaux binaires sont utilisés *en parallèle* ; ainsi, toute machine de traitement de l'information travaillant sur 8 *bits* peut théoriquement convoyer tous les caractères d'un alphabet comportant $2^8 = 256$ caractères distincts.

Cela dit, la transmission d'un seul caractère par un tel procédé comporte trois opérations, le codage, le transport, et le décodage du caractère. Ces opérations peuvent être entachées d'*erreurs*, dues à des défaillances humaines, mécaniques ou de circuits électroniques.

Supposons que $\text{Card}(A) = m = 2^n = \text{Card}(B)$. Dans ce cas, il y a correspondance bijective entre les caractères de A et ceux de B. La moindre erreur dans la suite des opérations décrites ci-dessus fera que le caractère *reçu* ne sera pas celui qui a été effectivement *émis*.

Ainsi se pose le problème de la correction des erreurs. Celle-ci est possible lorsque l'alphabet A possède une *redondance* propre. Ainsi la

réception d'un X à la place d'un H ne passera pas inaperçue du destinataire dans un message rédigé en langue française. Mais si le message consiste en une série statistique de nombres écrits en système décimal sur lesquels le destinataire ne possède a priori aucune information, la réception du chiffre 5 au lieu du chiffre 8 passera inaperçue et cette erreur pourra avoir des conséquences fâcheuses.

Il y a un moyen d'éviter cet inconvénient ; il consiste à introduire artificiellement une redondance pour l'alphabet B en prenant l'entier n plus grand que nécessaire. Ainsi, seulement *certains* éléments de B, formant une partie, disons C, de B correspondront par convention à des éléments de A. Par définition, une bijection : $f : A \longrightarrow C \subset B$ constitue un *code* dans B pour les éléments de A.

La première idée qui vient pour détecter, voire corriger les erreurs est de prendre les éléments de C suffisamment *espacés* dans B pour une métrique que l'on précisera.

Ainsi, si l'on convient que deux éléments de C sont toujours au moins distants de 2 unités, la réception d'un caractère de B n'appartenant pas à C, et ne correspondant donc à aucun caractère de A, signale la présence d'une erreur. Néanmoins, il n'est pas en général possible de corriger cette erreur dans la mesure où le caractère reçu peut être équidistant de deux éléments de C. Par contre, si on a pris la précaution d'éloigner les éléments de C de 3 unités au moins les uns des autres, si une erreur de codage est commise sur *un seul bit* on recevra un élément de B distant d'une unité d'un élément de C, et à une distance supérieure à 1 de tout autre élément de C. Il devient donc possible avec un tel code, non seulement de *détecter* l'erreur, mais de la *corriger*.

Ainsi, en gonflant B, et en répartissant astucieusement C dans B, il devient possible de détecter et de corriger un nombre de plus en plus grand d'erreurs. Cependant, il y a des limites, car ce faisant, les caractères de A devront être codés en des séquences de plus en plus longues et le risque de faire des erreurs grandit. Comment trouver la juste proportion ?

Un ensemble tel que B s'appelle un *hypercube n-dimensionnel* (notation H_n). Nous nous proposons ici, non pas de répondre à la question ci-dessus qui est du ressort de la théorie de l'information, mais seulement de développer quelques aspects essentiellement métriques de la géométrie des H_n en rapport avec les problèmes posés.

2 Taxi-distance

On trouvera ici une description sommaire de la taxi-géométrie sur un réseau de $\mathbf{R}^n$.

Etudions d'abord le cas du plan. Soit E le réseau constitué par les points à coordonnées entières du plan affine rapporté à un repère orthonormé. Un tel ensemble constitue un modèle mathématique du réseau

routier d'une ville moderne dont les rues se coupent à angle droit, comme il en existe tant aux Etats-Unis.

On convient de définir la distance de deux points A et B de E comme étant la plus petite des longueurs des chemins reliant A à B en se déplaçant sur le réseau par des segments de longueur unité parallèles aux axes de coordonnées, de sorte qu'au départ de chaque point il y a exactement 4 directions possibles. On peut alors définir une "droite" joignant A et B comme étant un chemin de longueur minimum.

La géométrie ainsi obtenue n'est pas euclidienne, comme on peut s'en rendre compte facilement.

Si (x,y) est un vecteur de $\mathbf{R}^2$, on peut prendre comme norme d'ordre k :

$$(|x|^k + |y|^k)^{1/k} ;$$

la distance ordinaire correspond à la norme d'ordre 2, et la taxi-distance à la norme d'ordre 1.

Tout cela se généralise naturellement en dimension n quelconque, la taxi-distance entre deux points $A=(a_1,\ldots,a_n)$ et $B=(b_1,\ldots,b_n)$ de $\mathbf{R}^n$ étant donnée par la formule :

$$d(A,B) = \sum_{1 \leqslant i \leqslant n} |a_i - b_i|$$

3 Hypercubes

Conformément aux usages, nous appellerons *hypercube n-dimensionnel* l'espace $(\mathbf{Z}/2\mathbf{Z})^n$ muni de sa structure canonique d'espace vectoriel sur le corps $\mathbf{Z}/2\mathbf{Z}$.

Les hypercubes ont donc une structure algébrique relativement riche. Ce sont avant tout des groupes finis commutatifs, donc susceptibles d'être représentés par des graphes.

L'espace H_n est en outre muni d'une base canonique :

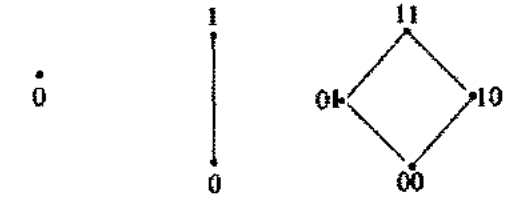
$$e_1 = 100\ldots0 \quad , \quad e_2 = 010\ldots0 \quad , \quad \ldots \quad , \quad e_n = 000\ldots01.$$

Pour des raisons de simplification d'écriture, on ne se conformera pas à l'usage pour l'écriture des n-uples, mais on écrira tout simplement un élément de H_n comme un nombre à n chiffres en système binaire.

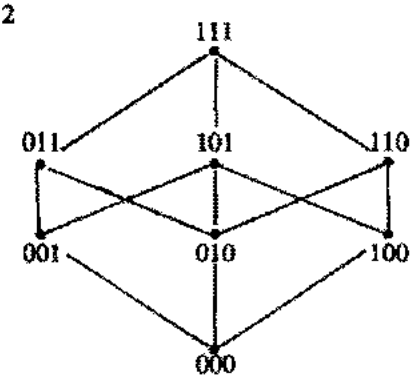
Ajoutons qu'il sera commode, pour nos besoins particuliers, d'identifier $\mathbf{Z}/2\mathbf{Z}$ avec la partie $\{0,1\}$ de $\mathbf{R}$, étant entendu qu'il s'agit d'une identification purement ensembliste et que les structures algébriques ne sont pas concernées. Cela permet d'identifier H_n à une partie de $\mathbf{R}^n$; cependant H_n n'est pas un sous groupe de $\mathbf{R}^n$ et encore moins un sous-espace vectoriel.

Diverses représentations planes de H_n sont possibles. Certaines mettent en évidence la structure de groupe additif, d'autres mettent en évidence l'aspect métrique, consistant à relier entre eux par un segment deux points voisins (distants d'une unité) de l'hypercube.

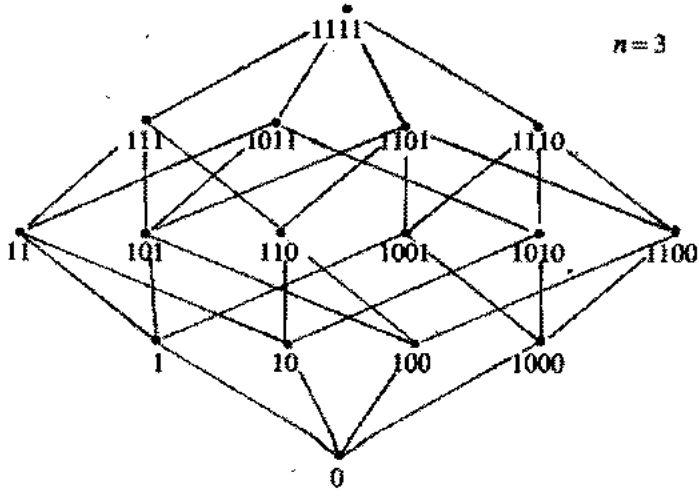
Les schémas obtenus sont alors les suivants :



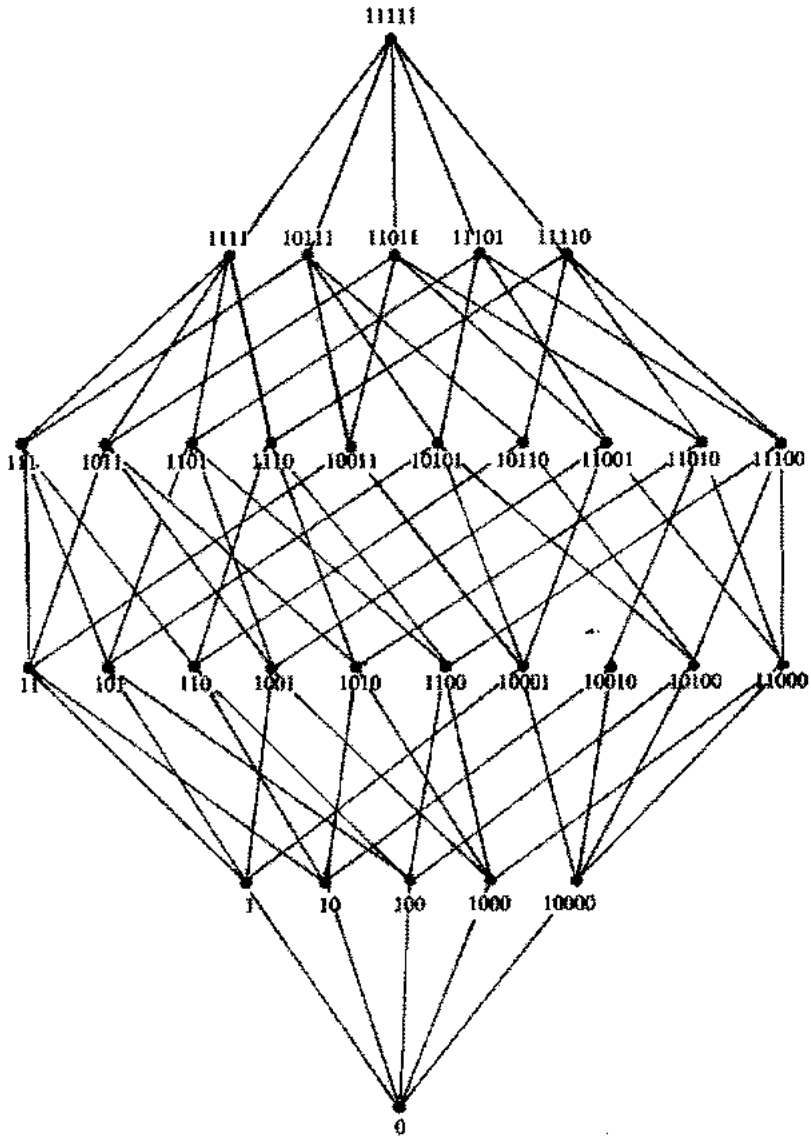
$n=0$ $n=1$ $n=2$



$n=3$



$n=4$



$n = 5$

4 Propriétés particulières à la métrique des H_n

Remarquons tout de suite que H_n est muni d'une structure naturelle d'espace affine sur le corps $\mathbb{Z}/2\mathbb{Z}$. Le choix d'une origine permet

d'identifier les vecteurs à des points et il nous arrivera de parler des "sommets" de l'hypercube.

Il sera aussi commode d'introduire la notion de "norme" sur H_n, bien qu'habituellement ce terme soit réservé à des espaces réels ou complexes. Si on note d_1 la taxi-distance et $\|\ \|_1$ la norme associée, on a entre les deux les relations usuelles :

$$\|x\|_1 = d_1(x,0) \qquad d_1(x,y) = \|x-y\|_1$$

et si l'on identifie les éléments de H_n à des points

$$d_1(A,B) = \|\overrightarrow{AB}\|_1$$

Cela dit, si d_2 et $\|\ \|_2$ désignent les restrictions à H_n des normes et distances euclidiennes sur $\mathbf{R}^n$ (lorsqu'on identifie H_n à une partie de $\mathbf{R}^n$), il y a un lien très simple entre d_1 et d_2 ; on a : $d_2 = \sqrt{d_1}$, plus précisément $\|x\|_2 = \sqrt{\|x\|_1}$ pour tout x de H_n ; car si $x = (x_1,\ldots,x_n)$, on a $x_i^2 = x_i$ pour tout i tel que $1 \leqslant i \leqslant n$, puisque $x_i = 0$ ou $x_i = 1$; donc

$$\Sigma\, x_i^2 = \Sigma\, |x_i| = \Sigma\, x_i$$

Cette remarque bien simple a des conséquences intéressantes et curieuses.

Tout d'abord, les taxi-boules et les taxi-sphères de H_n seront les intersections avec H_n des boules et sphères euclidiennes de $\mathbf{R}^n$ et nous pourrons alors utiliser notre "vision" euclidienne pour des problèmes taxi-géométriques.

Ainsi le problème de l'intersection des sphères résolu dans $\mathbf{R}^n$ sera-t-il "résolu" dans H_n, avec cependant quelques mauvaises surprises, car on peut trouver comme intersection de deux sphères un ensemble situé sur une sphère euclidienne de dimension moindre que n, de diamètre moindre que le diamètre de chacune d'elles et dont le centre n'appartient pas à H_n. Un exemple simple de cette situation s'obtient en considérant le cas de l'intersection de deux cercles centrés sur deux sommets opposés d'un carré, qui se coupent donc en les deux autres sommets du carré si le rayon de chaque cercle est pris égal à 1. L'intersection est alors une sphère de dimension 1 (deux points) centrée au centre de gravité du carré, qui n'est pas lui-même un sommet du carré.

En outre, la relation classique *d'orthogonalité*

$$d_2(B,C)^2 = d_2(A,B)^2 + d_2(A,C)^2$$

devient

$$d_1(B,C) = d_1(A,B) + d_1(A,C)$$

qui est plutôt une relation d'"*alignement*" taxi-géométrique.

A propos des sphères et des boules, les problèmes de dénombrement sont faciles à résoudre :

Désignons par $S(x,r)$, $B(x,r)$, $B'(x,r)$ respectivement la sphère, la boule ouverte et la boule fermée de rayon r et de centre x. Il suffit dans le cas de H_n de considérer les valeurs de r entières et inférieures ou égales à n. On constate alors que :

$$B(x,r) = B'(x,r-1) \qquad \text{et que} \qquad B'(x,r) = \bigcup_{0 \leqslant t \leqslant r} S(x,t)$$

de sorte qu'il suffit de savoir dénombrer les points des sphères. Nous sommes dans un espace affine, nous pouvons donc en utilisant les translations constater que le cardinal de $S(x,r)$ ne dépend que de r. Il suffit donc de savoir calculer le cardinal de $S(0,r)$ qui comporte exactement C_n^r éléments, car c'est le nombre de sommets ayant exactement r coordonnées parmi n étant égales à 1, les autres étant toutes nulles.

En particulier $\text{Card}(S(x,n)) = 1$. Il existe donc un élément et un seul, soit $\bar{x}$, de H_n à distance maximale n de x, que nous désignerons par l'*antipode* de x.

La relation :

$$2^n = \sum_{0 \leqslant i \leqslant n} C_n^i = \sum_{0 \leqslant i \leqslant h} C_n^i + \sum_{h+1 \leqslant i \leqslant n} C_n^i$$

est une façon d'exprimer que le complémentaire d'une boule de centre x et de rayon h est une boule de centre $\bar{x}$ et de rayon $n-1-h$ et que H_n est la réunion de $n+1$ sphères disjointes.

Bien que nous ayons affaire avec les H_n à des espaces finis et discrets, il sera commode d'utiliser quelques termes empruntés à la géométrie différentielle.

Définition : Appelons *géodésique* d'extrémités A,B dans H_n une suite de points $P_1, P_2, \ldots, P_k$ vérifiant :

$$P_1 = A \quad , \quad P_k = B \quad , \quad k - 1 = d_1(A,B) \quad , \quad d_1(P_i, P_{i+1}) = 1 \quad .$$

Cette notion de géodésique correspond bien à celle de plus court chemin d'un point à un autre. Si $P_1, \ldots, P_k$ est une telle géodésique, la figure formée par trois points consécutifs quelconques P_{i-1}, P_i, P_{i+1} est toujours un triangle rectangle. En outre, en général il n'existe pas une seule géodésique liant deux points donnés dans H_n. Le comptage du nombre de géodésiques liant A à B, en fonction de k et n, est assez simple.

Notons qu'on aurait pu utiliser le mot "droite" au lieu de "géodésique", mais il y aurait alors eu risque de confusion avec les droites affines de H_n, lesquelles comportent toujours exactement deux points.

5 Variétés linéaires

Le fait que H_n ne soit pas un sous-espace vectoriel de $\mathbf{R}^n$ apparaît de la façon la plus claire (et la plus déroutante) sous l'aspect barycentrique.

Ainsi, les droites n'ont que deux points qui n'ont pas de milieu. Le lecteur verra qu'on peut, en fait, ne considérer que les systèmes pondérés pour lesquels tous les points ont la masse unité, autrement dit il n'y a que des isobarycentres, et encore ces isobarycentres n'existent-ils que si le nombre de points est impair. Ainsi, dans l'hypercube de dimension 2 (carré), l'isobarycentre de trois sommets quelconques est le quatrième sommet.

Une autre curiosité est que la boule fermée de rayon r et de centre x est en fait la réunion (non disjointe) de toutes les variétés linéaires de dimension r passant par x, ce qui contraste beaucoup avec le cas des espaces réels normés où une boule ne peut jamais contenir une variété linéaire de dimension supérieure ou égale à 1.

Considérons une variété linéaire V de dimension m dans H_n ; alors V est munie d'une structure d'espace affine sur $\mathbb{Z}/2\mathbb{Z}$ et comporte 2^m points ; en outre V est munie d'une distance qui est la restriction de la taxi-distance de H_n. Si V admet pour système de vecteurs directeurs une partie de la base canonique $(e_1,\ldots,e_n)$, V s'identifie à un hypercube de dimension m. Nous dirons alors que V est un *sous-hypercube* de H_n.

Lorsque $n=3$, le sous-espace engendré par $e_1=100$ et $e_2=010$ est un sous-hypercube de dimension 2, mais il n'en est pas de même de la variété linéaire, de dimension 2 également, engendrée par 001 et 110.

6 Ensembles convexes

On dit que $E \subset H_n$ est *faiblement convexe* si, quels que soient les points A et B appartenant à E, il existe une géodésique reliant A à B dans E. On dit que E est *fortement convexe* si toutes les géodésiques reliant A à B sont dans E.

Ainsi une variété linéaire n'est, en général, ni faiblement convexe, ni à plus forte raison, fortement convexe, contrairement au cas des espaces normés réels. Une boule est faiblement convexe sans être fortement convexe.

Tout sous-ensemble de H_n se sépare en un nombre fini de composantes convexes ; à l'intérieur de chacune de ces composantes on a une propriété de connexité par les géodésiques.

L'intersection de convexes étant évidemment convexe, on a immédiatement la notion de convexe engendré par une partie donnée de H_n. Il est utile de constater que, dans le cas d'une paire $P = \{x,y\}$, le convexe engendré par P est le plus petit sous-hypercube de H_n contenant x et y, et que sa dimension est exactement $d_1(x,y)$, la taxi-distance entre x et y.

7 Distance d'un point à un sous-ensemble

Soit E une partie de H_n et x un élément de H_n ; on pose comme à l'accoutumée :

$$d_1(x,E) = \inf_{y\in E} d_1(x,y)$$

et on appelle ce nombre la distance de x à E.

Remarquons que, puisque nous avons ici affaire à des ensembles finis, il existe effectivement au moins un $y\in E$ tel que $d_1(x,E)=d_1(x,y)$, cet élément n'étant pas nécessairement unique. On remarquera, par exemple, que si $x\in H_n$, si $\bar{x}$ est son antipode et si $E=B'(x,1)$, on a $d_1(\bar{x},E)=n-1$ et la distance est atteinte en exactement n points de E qui sont les extrémités des droites d'origine x.

Par contre, si E est un sous-hypercube de H_n, il est facile de montrer l'existence d'un *unique* $y\in E$ tel que $d_1(x,y)=d_1(x,E)$; cette propriété s'étend, en fait, à tous les ensembles fortement convexes et on a un analogue du théorème de la projection orthogonale sur les fermés convexes dans les espaces de Hilbert.

8 Isométries

a) *Isométries vectorielles*

On considère H_n muni de sa structure d'espace vectoriel sur $\mathbb{Z}/2\mathbb{Z}$; on appelle *isométrie* de H_n toute application linéaire $u: H_n \to H_n$ vérifiant

$$d_1(u(x),u(y)) = d_1(x,y) \qquad \forall x,y\in H_n .$$

La condition ci-dessus équivaut à : $\|u(x)\|_1 = \|x\|_1 \qquad \forall x\in H_n$, de sorte que si u est une isométrie vectorielle, nous voyons que la matrice de u relativement à la base canonique $(e_1,\dots,e_n)$ s'obtient nécessairement en permutant les colonnes de la matrice carrée unité d'ordre n. D'autre part, il est clair que si σ est un élément du groupe symétrique S_n, c'est-à-dire une permutation des entiers $\{1,\dots,n\}$, alors l'application linéaire $u_\sigma : H_n \to H_n$ caractérisée par $u_\sigma(e_i) = e_{\sigma(i)}$ est une isométrie vectorielle.

En résumé, le groupe des isométries vectorielles de H_n est isomorphe au groupe symétrique S_n.

b) *Isométries affines*

On considère maintenant H_n muni de sa structure affine canonique. La définition d'une isométrie affine est évidente. Signalons, parmi les isométries affines, en premier lieu, les translations. Les translations forment un groupe isomorphe à H_n et engendré par les n translations $t_{\vec{e}_i}$ $1\leqslant i\leqslant n$. Remarquons que, du point de vue des transformations de la géométrie euclidienne classique, $t_{\vec{e}_i}$, la translation de vecteur $\vec{e}_i$, n'est rien d'autre que la restriction à H_n de la symétrie orthogonale par rapport à l'hyperplan d'équation $x_i = \frac{1}{2}$ de l'espace $\mathbb{R}^n$.

Toute isométrie affine s'écrit de manière unique $f = u \circ t$ où u est une isométrie vectorielle et où t est une translation. Il en résulte que le groupe des isométries affines de H_n est un groupe d'ordre $n! \times 2^n$ admettant un système de $2n-1$ générateurs. Ayant étudié de manière exhaustive le groupe affine de H_n, il devient possible de caractériser les éléments de symétrie d'une figure en étudiant le sous-groupe laissant cette figure globalement invariante.

9 Codes correcteurs

On appelle *code d'ordre* k dans H_n toute partie E de H_n telle que tout point de E se trouve à une distance au moins égale à k de tout autre point de E. En outre, un tel code est qualifié d'*optimal* si son nombre d'élements est maximal.

Le cas $k=1$ est trivial ; un tel code ne permet pas la détection, et encore moins la correction, d'erreurs. Dans le cas $k=2$, on a un code permettant de détecter une erreur sans toutefois pouvoir la corriger. Nous verrons comment construire des codes optimaux dans ce cas particulier.

Un des buts de cet article est de donner un sens précis à des locutions du genre "codes correcteurs équivalents" qui traînent dans la littérature spécialisée avec des définitions très vagues.

Le groupe des isométries affines de H_n opère évidemment sur l'ensemble des codes d'ordre k. Deux tels codes seront dits *équivalents* s'ils sont conjugués par cette opération, autrement dit s'il existe une isométrie transformant l'un en l'autre.

En outre, certaines affirmations qu'on trouve dans des démonstrations anciennes du type "on peut toujours supposer que le code contient l'origine" deviendront maintenant tout à fait claires ; on se ramène à l'origine par une translation.

Le lecteur s'aperçoit donc que, partant d'un code optimal, il peut construire tous les codes équivalents, lesquels sont au nombre maximum de $n! \times 2^n$ qui est le cardinal du groupe des isométries ; cependant, il n'est pas établi que ce groupe opère transitivement sur les codes optimaux, de sorte qu'a priori subsiste la possibilité d'existence de codes optimaux non équivalents.

D'une façon générale, nous désignerons par $N(k,n)$ le nombre d'éléments d'un code optimal d'ordre k dans H_n. Nous nous proposons d'encadrer ce nombre.

Etudions d'abord le cas $k=2$. Considérons donc un code optimal d'ordre 2 dans H_n. Il est possible de trouver dans H_n deux sous-hypercubes parallèles, d'ordre $n-1$, l'un passant par l'origine et l'autre par son antipode, tous deux de direction engendrée par $e_1,\ldots,e_{n-1}$.

L'un au moins de ces deux hypercubes contient au minimum $N(2,n)/2$ éléments du code optimal. En répétant cet argument $n-2$ fois, on s'aperçoit qu'il existe un sous-hypercube d'ordre 2 de H_n contenant au moins $N(2,n)/2^{n-2}$ éléments du code optimal initial. Or, il est clair que dans un hypercube d'ordre 2, un code optimal ne peut contenir que 2 éléments. On a donc $N(2,n)/2^{n-2} \leqslant 2$, ce qui donne l'inégalité $N(2,n) \leqslant 2^{n-1}$. Il est facile de voir que l'on a en fait l'égalité en construisant effectivement un code optimal d'ordre 2 ayant 2^{n-1} éléments, à savoir l'ensemble des sommets de l'hypercube ayant toujours un nombre pair de chiffres 1 dans leur écriture en système binaire.

Le cas intéressant est lorsque $k = 2h + 1$ est un nombre impair, car alors un code d'ordre k est un code capable de corriger jusqu'à h erreurs de codage. Il est bien entendu que ce code est inefficace dans le cas d'une erreur d'émission d'un caractère de l'alphabet A. Les résultats qui suivent sont dus, en partie, à W. Hamming.

Théorème 1 : $$N(2h+1,n) \leqslant \frac{2^n}{\sum\limits_{0 \leqslant r \leqslant h} C_n^r}$$

En effet, les boules fermées de rayon h et ayant pour centres les points du code optimal sont deux à deux sans points communs. Il suffit d'exprimer que leur réunion a un cardinal inférieur à celui de H_n pour obtenir l'inégalité du théorème 1.

Théorème 2 : $$N(2h+1,n) \geqslant \frac{2^n}{\sum\limits_{0 \leqslant r \leqslant 2h} C_n^r}$$

Preuve : Prenons au hasard un élément x_1 de H_n. Le nombre d'éléments de H_n distants de x_1 de plus de $2h$ a pour cardinal

$$2^n - \sum_{0 \leqslant r \leqslant 2h} C_n^r$$

Prenons un élément de cet ensemble, soit x_2. Le nombre d'éléments de H_n distants de x_1 et de x_2 de plus de $2h$ a au moins pour cardinal

$$2^n - 2 \sum_{0 \leqslant r \leqslant 2h} C_n^r$$

On construit ainsi une suite $x_1, x_2, \ldots, x_s$ de points de H_n telle que x_s est à une distance supérieure à $2h$ de $x_1, \ldots, x_{s-1}$. On continue ce processus ; tant que

$$2^n - s \sum_{0 \leqslant r \leqslant 2h} C_n^r > 0$$

on est sûr de pouvoir trouver un x_{s+1}. On arrête donc le processus à un indice s tel que

$$2^n - s \sum_{0 \leqslant r \leqslant 2h} C_n^r \leqslant 0 \quad \text{de sorte que} \quad s \geqslant \frac{2^n}{\sum_{0 \leqslant r \leqslant 2h} C_n^r}$$

mais bien sûr, on a peut-être mal choisi les x_i et un meilleur choix aurait peut-être permis d'aller plus loin.

D'où $N(2h + 1,n) \geqslant s$, qui assure le résultat.

Bibliographie

Taxi-Cab Geometry, d'Eugène Krause. Addison Wesley. 1975.

Taxi-Cab Geometry — a non euclidean geometry of lattice points (The mathematics teacher, vol. 64, n° 5, pp. 418-422. Mai 1971).

Cours de Calcul Informationnel, par G. Cullmann, M. Denis Papin et A. Kaufmann. Editions Albin Michel. 1970.

Error detecting and error correcting codes, par R.W. Hamming. Bell System Tech J. 31, 504-522. 1952.

Binary codes with specified minimum distance, par M. Plotkin. Univ. of Penna. Moore School Research Division Report 51-20. 1951.

Math'Festival, par Martin Gardner. Belin. 1981. Ch. 14 (La courbe du dragon) § 5 (Les 3 pièces).

La logique quantique, par R. Hughes. Revue "Pour la Science", n° 50, décembre 1981.