MATHÉMATIQUES ET SCIENCES HUMAINES

G. COHEN
M. DEZA

Distances invariantes et L-cliques sur certains demi-groupes finis

Mathématiques et sciences humaines, tome 67 (1979), p. 49-69
<http://www.numdam.org/item?id=MSH_1979__67__49_0>

Math. Sci. hum. (17e année, n°67, *1979*, p.49-69)

DISTANCES INVARIANTES ET L-CLIQUES SUR CERTAINS DEMI-GROUPES FINIS[1]

G. COHEN[2] et M. DEZA[3]

INTRODUCTION

Après quelques rappels généraux sur les espaces métriques, nous nous intéressons aux ensembles finis munis d'une distance entière. Nous considérons d'abord des méthodes de constructions, d'extension et de restriction de métriques associées à des graphes. Des exemples sont donnés, principalement empruntés au contexte "Codes correcteurs d'erreurs" (pour un traitement détaillé, cf. par exemple /26/, /27/). La notion de distance invariante par translation, importante dans cette dernière discipline, est étudiée plus généralement dans les groupes et demi-groupes non abéliens ; l'invariance à droite permet de lui substituer la notion de "poids" (distance à l'unité), plus simple à manier. L'accent est mis sur certains demi-groupes de relations binaires et sur le groupe symétrique, ainsi que sur 6 distances (ou poids), notées L_1 ("city-block"), L_∞, L (lee), H (Hamming), T, I, définies en 1. et 3.4., et reliées entre elles en 5. Dans la quatrième partie, nous

---

[1] Nous remercions Bernard Monjardet, dont les conseils et suggestions nous ont beaucoup aidés dans la mise en forme de l'article.

[2] ENST (Ecole Nationale Supérieure des Télécommunications), 46 rue Barrault 75634 Paris Cedex 13.

[3] CNRS, Paris.

définissons les L-cliques maximales, ensembles de cardinalité maximale tels que les distances entre leurs éléments appartiennent à un ensemble d'entiers L. Nous proposons pour finir quelques problèmes. Il est à noter qu'une partie de la terminologie et des problèmes sont empruntés au "Codage", où l'on se pose des questions du type suivant : trouver un "code", ayant le maximum de "mots", avec une contrainte sur la distance minimale entre mots, garantissant, après une altération dûe à la transmission à travers un canal, la reconnaissance du message émis. Les L-cliques sont une généralisation de cette notion de code, à laquelle nous étendons certaines bornes de cardinalité. L'espace métrique est ensuite particularisé (ici à S_n) pour obtenir des résultats plus explicites.

1 . RAPPELS ET EXEMPLES

Soit E un ensemble fini, $(\mathbb{R},>)$ le corps ordonné des réels avec l'ordre ordinaire.

Soit une fonction $d : E \times E \to (\mathbb{R},>)$ telle que

$d(a,b) \geqslant o$ et $d(a,a) = o$, pour tout $a,b \in E$.

d a éventuellement les propriétés suivantes :

1) symétrie : $d(a,b) = d(b,a)$

2) positivité : $d(a,b) = o$ implique $a = b$

3) inégalité triangulaire : $d(a,c) \leqslant d(a,b) + d(b,c)$.

Nous appellerons une fonction d vérifiant

1) *prédistance*

1), 2) *quasi-distance*

1), 3) *écart* ("semi-metric")

1), 2), 3) *distance*.

Une quasi-distance induit une distance par *clôture triangulaire* :

$$\bar{d}_t(a,b) = \min \sum_{i=1}^{n} d(x_i, x_{i+1}) \text{ pour tout } \{x_i\},\ n$$

avec $x_1 = a$, $x_n = b$.

Un écart induit une distance sur l'espace quotient (E/R x E/R) avec

$aRb \Leftrightarrow d(a,b) = o.$

Enfin toute fonction d possède des *clôtures symétriques*

par exemple $\bar{d}_s(a,b) = \frac{(d(a,b) + d(b,a))}{2}$

ou Min (d(a,b), d(b,a)).

Certaines généralisations sont possibles où l'on remplace $(\mathbb{R},>)$ par un ensemble ordonné (A,>). Par exemple si A est une algèbre de Boole, $d : A \times A \to A$ définie par $d(a,b) = a\bar{b} + b\bar{a}$ vérifie les propriétés 1), 2), 3) et est appelée *autométrique* (/4/, Chap. 15).

Dans la suite d sera toujours *entière*, c'est à dire

$$d : E \times E \to (\mathbb{N},>).$$

Quelques distances

Soit $X, Y \in \mathcal{P}(E)$, ensemble des parties de E, alors $S(X,Y) = |X \Delta Y|$ est la distance bien connue de la différence symétrique.

Considérons maintenant $N = \{1, 2, \ldots, n\}$ muni de l'addition modulo n, et $E = N^k$. Pour $X = (x_1, \ldots, x_k)$, $Y = (y_1, \ldots, y_k)$ deux éléments quelconques de N^k. Définissons :

$$L_1(X,Y) = \sum_i |x_i - y_i|$$

$$L_\infty(X,Y) = \operatorname{Max}_i |x_i - y_i|$$

$$L(X,Y) = \sum_i \operatorname{Min} (|x_i - y_i|, n - |x_i - y_i|)$$

$$H(X,Y) = |\{i, x_i \neq y_i\}|.$$

H est la distance de Hamming, employée en transmissions ; elle s'interprète comme distance de différence symétrique, en considérant un élément X de N^k comme une partie d'un ensemble à kn éléments.

Par exemple : (2, 1, 4) → (0100 1000 0001) ; alors S = 2H.

Les métriques, L_1, L_∞ sont les analogues pour r = 1, r = ∞, λ_i = 1 des distances de Minkowski-Hölder associées aux normes $||x|| = (\Sigma \lambda_i |x_i|^r)^{1/r}$ définies sur les espaces vectoriels. L_1 est encore appelée "Manhattan", "Taxicab", "city-block", "Grill", "écart absolu" ...

2 . DISTANCES DE GRAPHE : d_G

Soit G un graphe simple (c'est à dire non orienté, sans boucle ni arête multiple). On note S(G) l'ensemble de ses sommets, A(G) l'ensemble de ses arêtes. La distance d_G entre sommets de G est celle du "plus court chemin" (chaîne) entre ces sommets.

(E,d) sera dit *graphique* si ses points peuvent être mis en bijection avec les sommets d'un graphe G de façon que les distances dans E et G soient égales. Alors d sera notée d_G.

Définition : Soient x, a, b ∈ E , a ≠ x ≠ b. Alors x est *entre* a et b si

$$d(a,b) = d(a,x) + d(x,b).$$

PROPOSITION /16/ : (E,d) est graphique ssi :

$$\forall\ a, b \in E\ ,\ d(a,b) \geq 2 \Rightarrow \exists\ x \text{ entre } a \text{ et } b.$$

Distance d'ordre $d_>$

Soit E un ensemble partiellement ordonné par >. Son graphe de *couverture* non orienté $G_c(E)$ est défini ainsi : a, b ∈ E sont liés par une arête ssi a *couvre* b (qu'on note a ⋗ b) ou b couvre a, c'est à dire si a > b ou b > a et s'il n'existe pas d'élément x de E entre a et b. La longueur du plus court chemin entre 2 points de $C_c(E)$ est une distance dite *d'ordre*, notée $d_>$.

Distance de rang d_r

Un rang sur E est une application de $(E,\gtrdot)$ dans $\mathbb{N}$ telle que $\forall x,y \in E$, $x \gtrdot y \Longrightarrow r(x) = r(y) + 1$. Si E est un treillis modulaire, r(x) définie comme longueur de l'intervalle $[\tilde{o},x]$ est un rang vérifiant $r(x) + r(y) = r(x \vee y) + r(x \wedge y)$ et on définit une distance dite de *rang*, notée d_r, par :

$$d_r(x,y) = r(x \vee y) - r(x \wedge y).$$

La relation $d_r(x,y) = 2r(x \vee y) - r(x) - r(y) = r(x) + r(y) - 2r(x \wedge y)$ rend possible une généralisation et caractérisation pour les sup. et inf. demi-treillis /23/.

On établit facilement la chaîne irréversible suivante :

PROPOSITION : $d = d_r \Longrightarrow d = d_> \Longrightarrow d = d_G$.

2.1. Construction de distances graphiques

Soient E un ensemble fini,

T un ensemble d'opérations sur E, i.e. d'applications $t : E \to E$,

T^* le monoïde libre engendré par T, i.e. ensemble des produits finis d'éléments de T.

Définition : $$d_T(e_1,e_2) = \min_{i,j} (i + j)$$

$$\text{tel que } t_1.t_2 \ldots t_i\,(e_1) = t'_1.t'_2 \ldots t'_j\,(e_2) \qquad (1)$$

et $d_T(e_1,e_2) = \infty$ si l'écriture (1) est impossible.

PROPOSITION : d_T est une distance graphique.

Preuve : d_T satisfait les axiomes d'une distance, et son graphe associé G_T est le suivant :

$S(G_T) = E$, $A(G_T) = \{(e,f) \in E \times E \ ; \ \exists\, t \in T,\ t(e) = f \text{ ou } t(f) = e\}$.

Inversement, soit d_G une distance de graphe, on lui associe un ensemble d'opérateurs T_G de la façon suivante : soient $i,j \in S(G)$, avec $(i,j) \in A(G)$; on pose $t_{ij}(i) = j$, $t_{ij}(j) = i$ et $t_{ij}(k) = k$ pour tout $k \neq i,j$, enfin $T_G = \{t_{ij}, (i,j) \in A(G)\}$.

Remarques : d_T est finie ssi G_T est connexe, ou encore ssi $T^*(E) = E$.
En codage, les éléments de T sont appelés *bruits élémentaires* et ceux de T^* *bruits*.
Lorsque T s'identifie à une partie de E, ses éléments s'appellent en codage *erreurs élémentaires* (de poids 1) et ceux de T^* *erreurs* . Dans /10/, T^* est appelé bruit additif arbitraire.

Exemples :

1) $E = N = \{1, 2, \ldots n\}$.

   Appelons translation sur N une application t_a de N dans N définie par $t_a(i) = i + a$ (modulo n), et identifions t_a et a.

   a) $T = \{t_i, i \in N\} \simeq E$, $G_T = K_n$, le graphe complet à n sommets, $d_T = H$ (distance de Hamming).

   b) $T = \{t_1\}$, G_T est un chemin : $S(G) = N$, $A(G) = \{(j,j+1), 0 \leqslant j \leqslant n-1\}$, $d_T = L_1$.

   c) $T = \{t_1, t_{n-1}\}$, G_T est un cycle : $S(G) = N$, $A(G) = \{(j,j+1) \text{ modulo } n\}$ $d_T = L$.

2) En Linguistique, $E = N^*$ est l'ensemble des mots sur l'alphabet N. On prend pour T l'ensemble des opérateurs suivants : insertion, enlèvement, substitution d'une lettre quelconque de l'alphabet dans le mot. Alors d_T est la métrique de Levenstein /24/, considérée en codage et indépendamment en Biologie dans /2/ comme métrique de mutations dans les chaînes d'ADN.

Notons qu'on obtient une généralisation de ces métriques en pondérant les opérateurs de T (ou les arêtes de G_T). Des exemples sont donnés dans /24/.

2.2. Extension et restriction des métriques graphiques

Soient (E_i, d_i) des espaces métriques graphiques, πE_i leur produit cartésien, et définissons une application de πE_i dans $\mathbb{N}$ par :

$$\otimes_f d_i ((x_i), (y_i)) = f (\{d_i (x_i, y_i)\}).$$

PROPOSITION : $(\pi E_i, \otimes_f d_i)$ est un espace métrique graphique pour

$$f = \Sigma_i \ , \ f = \mathrm{Max}_i .$$

Remarquons qu'à partir d'une autre fonction, l'entropie, on obtient la distance non entière de Shannon-Fitingof-Goppa, ...

Exemples 1) $\forall i$, $E_i = E$, $d_i = d$, $f = \Sigma$

alors $\otimes_\Sigma d(X,Y) = \sum_{i=1}^{n} d(x_i,y_i)$, où $X = (x_i)$, $Y = (y_i) \in E^n$.

Dans ce cas on identifie $\otimes_\Sigma d$ et d.

2) $E_i = E$, $d_i = L_1$, $f = \mathrm{Max}$, $\otimes_{\mathrm{Max}} L_1 = \mathrm{Max}$ (c'est la norme L_∞ des espaces hilbertiens).

3) Somme pondérée : $E_i = E$, $d_i = H$, $A(X,Y) = \sum_i 2^i H(x_i,y_i)$ est la distance arabique /5/, adaptée aux erreurs arithmétiques /21/.

Restriction d'un métrique graphique

PROPOSITION : Soit $S \subset E$, d_T restreinte à S est graphique ssi S stable par T.

3 . DISTANCES INVARIANTES SUR UN GROUPE OU UN DEMI-GROUPE

Soit G un groupe fini (généralement non abélien) avec unité 1 ; on note ab le "produit" de deux éléments a et b de G, a^{-1} l'inverse de a.

3.1. Poids associés aux distances

Définitions : Soit d une prédistance

- d sera dite *invariante à droite* (resp. *à gauche*) sur G si :

  $\forall$ a, b, c $\in$ G, d(a,b) = d(ac,bc), (resp. d(a,b) = d(ca,cb)).

  si d possède ces 2 propriétés, elle sera dite *bi-invariante*.

- On dira q'une application p : G $\to$ $\mathbb{N}$ est un *prépoids* si p(1) = 0

  et $\forall$ a $\in$ G, $p(a^{-1}) = p(a)$, un *quasi-poids* si de plus p(a) = 0 $\Rightarrow$ a = 1,

  un *poids* enfin si de plus $p(ab) \leqslant p(a) + p(b)$, $\forall$ a, b $\in$ G.

PROPOSITION : L'application $\emptyset$: d $\to$ p_d, définie par $p_d(a) = d(a,1)$ est une bijection entre l'ensemble des distances (resp. prédistances, quasi-distances) invariantes à droite et celui des poids (resp. prépoids, quasi-poids) sur G.

Preuve : $\emptyset^{-1}$ est l'application : d $\to$ d_p, où $d_p(a,b) = p(ab^{-1})$; d et p_d seront donc identifiés dans la suite.

Toutes les métriques que nous considérons seront invariantes à droite. Alors $d(a,b) = d(ab^{-1}, 1) = d(ab^{-1})$, $d(a) = d(a^{-1}) = d(a,1)$. On aura ainsi l'équicardinalité de toutes les boules d'un rayon donné, agréable dans les problèmes de Codage.

Les notions d'invariance s'étendent aux demi-groupes, mais les caractérisations de la bi-invariance données dans les paragraphes suivants ne seront plus valables.

3.2. Les demi-groupes R_n, TP_n, T_n, P_n, S_n

Une *relation binaire* (sur N) est un sous-ensemble de N x N.

Une *transformation partielle* (sur N) est une application d'une partie de N dans une autre.

Une *transformation* (sur N) est une application de N dans N.

Une *permutation partielle* (sur N) est une bijection entre deux parties de N.

Une *permutation* (sur N) est une bijection de N sur lui-même.

Nous noterons R_n, TP_n, T_n, P_n, S_n respectivement les ensembles de toutes les relations binaires, transformations partielles, transformations, permutations partielles, et permutations. Il est évident que $S_n = T_n \cap P_n$, $T_n \cup P_n \subset TP_n \subset R_n$ et $|S_n| = n!$, $|T_n| = n^n$, $|P_n| = \sum_{i=o}^{n} i!\binom{n}{i}^2$,

$$|TP_n| = \sum_{i=1}^{n} \binom{n}{i} n^i, \quad |R_n| = 2^{n^2}.$$

Chaque transformation partielle peut s'écrire comme un N-uple d'éléments de $N \cup \{\infty\}$. Exemple ; $N = \{1, 2, 3, 4\}$; la relation $a = \{(1,2), (3,3), (4,3)\} = \{(i, a(i)), i = 1, 3, 4\}$ est un élément de TP_4, c'est à dire une application de $\{1, 3, 4\}$ dans $\{2,3\}$ et se représente comme $a = (2, \infty, 3, 3)$. Chaque permutation partielle s'interprète comme une transformation sur $N \cup \{\infty\}$.

L'opération ordinaire ab de composition des applications a,b munit P_n, T_n, TP_n d'une structure de demi-groupe unitaire, l'élément unité étant la permutation identité $1 = (1, 2, \ldots, n)$. Plus précisément P_n est un *demi-groupe inversif*, c'est à dire que tout élément a de P_n admet un unique élément "inverse" a^{-1} tel que $a\,a^{-1}\,a = a$ et $a^{-1}\,a\,a^{-1} = a^{-1}$. En fait S_n devient même un groupe, dit groupe symétrique. On peut généraliser la composition pour 2 relations de R_n (comme produit booléien des matrices binaires d'incidence ou autrement dit produit des graphes associés à ces relations) ; R_n devient ainsi un demi-groupe unitaire, /5/.

On sait qu'on peut définir sur R_n deux autres opérations, notées $\vee$ et $\wedge$, correspondant à l'union et l'intersection dans N x N. Avec $\tilde{0} = \emptyset$ et $\tilde{1} = N \times N$, P_n devient un treillis de Boole à n^2 *atomes* (i.e. éléments a tels

que $b < a$ ssi $b = \tilde{0}$). $(P_n, \wedge, \tilde{0})$ est un inf demi-treillis ayant $\tilde{1}$ pour unité, et même un *treillis partiel*, c'est à dire que 2 éléments quelconques de P_n ayant un majorant commun admettent un supremum (l'ordre étant classiquement défini par $a < b \iff a \wedge b = a$).

L'importance théorique de ces demi-groupes résulte des théorèmes de plongement suivants :

Le Théorème de Cayley "tout groupe fini est isomorphe à un sous-groupe d'un groupe symétrique" admet par exemple les généralisations :

a) tout demi-groupe fini est isomorphe à un sous demi-groupe de transformations /9/.

b) tout demi-groupe fini est isomorphe à un sous demi-groupe de relations binaires de *type* 1 ("1-fold") c'est à dire tel que 2 éléments quelconques aient une intersection vide /6/.

c) tout demi-groupe inversif fini est isomorphe à un sous demi-groupe inversif de permutations partielles (/15/ p. 139).

En combinant a) et b) nous obtenons

d) tout demi-groupe fini régulier (tel que $ab = ac$ implique $b = c$) est isomorphe à un sous demi-groupe de transformations de type 1.

3.3. Métriques invariantes à droite sur les demi-groupes R_n, TP_n, P_n, T_n, S_n

Les métriques L_1, L_∞, L, H, introduites au paragraphe 1, sont invariantes à droite sur TP_n. Les poids p(a) associés, où, $a = \{(i, a(i))\} \in TP_n$ sont :

- $\sum_i |a(i) - i|$ pour L_1,
- $\max_i |a(i) - i|$ pour L_∞,
- $\sum_i \min(|a(i) - i|, n - |a(i) - i|)$ pour L,
- $|\{i, a(i) \neq i\}|$ pour H.

Définition : Nous appellerons *support* $\hat{a}$ d'un élément a de TP_n

$$\hat{a} = \{i,\ (i,\ a(i)) \in a\}.$$

Alors on peut définir sur TP_n l'écart H_1 par $H_1(a,b) = |\hat{a} \Delta \hat{b}|$. Sur S_n, $H_1 = 0$.

$\mathcal{R}_n$ étant un treillis avec rang r ($r(a) = |a|$) possède une distance

$H_2(a,b) = r(a) + r(b) - 2r(a \wedge b)$. En remarquant que sur P_n, $r(a) = |\hat{a}|$ et que $|a \hat{\wedge} b| = \varphi(ab^{-1})$ (nombre de points fixes de ab^{-1}) on obtient :

$$H_2(a,b) = |\hat{a}| + |\hat{b}| - 2\varphi(ab^{-1}).$$

D'où sur S_n $\quad H_2 = 2H = S$.

Sur TP_n on peut considérer également H_3 comme l'habituelle distance de Hamming sur $N \cup \{\infty\}$.

Exemple : Soient dans R_4 $a = \{(1,2), (3,3), (4,3)\} = (2, \infty, 3, 3)$, $1 = \{(1,1), (2,2), (3,3), (4,4)\} = (1,2,3,4)$. Alors $\hat{a} = \{1,3,4\}$, $\hat{1} = \{1,2,3,4\}$, $H_1(a,1) = 1$, $H_2(a,1) = 5$, $H_3(a,1) = 3$.

3.4. Construction de distances graphiques invariantes à droite

PROPOSITION : Soit T un ensemble d'opérateurs sur l'ensemble fini E. Si T est identifiable à une partie de E, d_T est invariante à droite.

Démonstration : Par définition (paragraphe 1)

$$d_T(e_1, e_2) = \min (i+j) \text{ tel que } t_1\ t_2 \ldots t_i\ e_1 = t'_1 \ldots t'_j\ e_2$$

d'où pour tout e de E $t_1 \ldots t_i\ e_1\ e = t'_1 \ldots t'_j\ e_2\ e$ et $d_T(e_1, e_2) = d_T(e_1\ e, e_2\ e)$.

Ici d_T est finie ssi T génère $E(T^* = E)$.

Exemples pour $E = S_n$

a) T = {transpositions}, d_T est noté T

b) $T = \{\text{transpositions adjacentes } t_i = (i, i+1)\}$, d_T est noté I.

On construit ainsi deux nouveaux poids ; $T(\sigma)$ (resp. $I(\sigma)$) est le nombre minimal de transpositions (resp. transpositions adjacentes) t_i telles que $t_i\, t_j \ldots t_e \sigma = 1$. Il est bien connu (Cayley) que $T(\sigma) = n$ - nombre de cycles de σ (cf. 3.6.).

3.5. Caractérisations de la bi-invariance [dans un groupe (non-abélien) G].

Soit f une prédistance invariante à droite, a, b, des éléments quelconques de G.

Définition : $(a|b)_f = (a|b) = \dfrac{f(a) + f(b) - f(a,b)}{2}$.

Propriétés de $(a|b)$:

$$(a|a) = f(a)$$

$$(a|b) = (b|a)$$

$$(a,b) = (a|a) + (b|b) - 2\,(a|b).$$

De plus si f vérifie l'inégalité triangulaire :

$$(a|b) \geqslant 0 \text{ et } f(a,b) = 0 \Longleftrightarrow 1 \text{ entre a et b } (f(a,b) = f(a,1) + f(1,b))$$

$$(a|a) \geqslant (a|b) \text{ avec égalité ssi a entre 1 et b.}$$

Remarquons que $(.|.)$ a des propriétés analogues à celle d'une corrélation, ou d'une quantité d'information conditionnelle.

Réciproquement : Soit $(.|.)$ une application symétrique de $G \times G \to \mathbb{N}$ ayant les 2 propriétés suivantes :

1) $\forall a, b \in G \quad (a|a) \geqslant (a|b)$ avec égalité ssi a est entre 1 et b

2) $\forall a, b, c \in G \; (a|a) + (b|c) \geqslant (a|b) + (a|c)$

Alors d définie par $d(a,b) = (a|a) + (b|b) - 2\,(a|b)$ est une distance.

PROPOSITION : Pour toute prédistance f invariante à droite les 5 propriétés

suivantes sont équivalentes :

1) $\forall a, b, c \quad (ab|cb)_f = (ba|bc)_f$

2) $\forall a, b \quad f(ab) = f(ba)$

3) f est invariante à gauche (donc bi-invariante), c'est à dire

$f(ca,cb) = f(a,b)$

4) $\forall a, b \quad f(a,b) = f(a^{-1}, b^{-1})$

5) $\forall a, b \quad f(a) = f(bab^{-1})$

Preuve :

1) $\Longrightarrow$ 2) faire a = c .

2) $\Longrightarrow$ 3) $f(ca,cb) = f(cab^{-1}c^{-1}) = f(b^{-1}c^{-1}ca) = f(b^{-1}a)$

$= f(ab^{-1}) = f(a,b)$.

3) $\Longrightarrow$ 4) $f(a,b) = f(a^{-1}a, a^{-1}b) = f(a^{-1}b) = f(a^{-1}, b^{-1})$.

4) $\Longrightarrow$ 5) $f(bab^{-1}) = f(ba,b) = f(a^{-1}b^{-1}, b^{-1}) = f(a^{-1}) = f(a)$.

5) $\Longrightarrow$ 2) $f(ab) = f(a^{-1}aba) = f(ba)$.

2) $\Longrightarrow$ 1) 2) $\Longrightarrow$ 3), et 3) + 2) $\Longrightarrow$ 1).

Corollaire :

Il y a isomorphisme entre l'ensemble des distances bi-invariantes de G et celui des poids de G vérifiant $\forall a,b \quad p(ab) = p(ba)$ ou $p(a) = p(bab^{-1})$.

3.6. Exemple d'application : cas de S_n

Soit $\sim$ la relation de conjugaison sur S_n ($\sigma \sim \pi$ ssi $\exists \alpha, \sigma = \alpha \pi \alpha^{-1}$).

Notons $\dot{\sigma}$ la classe de σ. On a :

$$S_{n/\sim} = \{\dot{\sigma}\} \simeq \{\{N_1(\sigma), N_2(\sigma) \ldots N_n(\sigma)\}, \Sigma\, i\, N_i(\sigma) = n\} \qquad (2)$$

où $N_i(\sigma)$ est le nombre des cycles de longueur i de σ.

Soit $F : S_{n/\sim} \to \mathbb{N}$ telle que $F(\dot{1}) = 0$, alors

PROPOSITION : $f : S_n \times S_n \to \mathbb{N}$ définie par

$$f(\sigma,\pi) = F(\widehat{\sigma\pi^{-1}}) = f(\sigma\pi^{-1})$$

est une prédistance bi-invariante. Si de plus $F^{-1}\{0\} = \dot{1}$ (c'est à dire $F(\dot{\sigma}) = 0 \Leftrightarrow \sigma = 1$), f est une quasi-distance et $\bar{f}_t$ (clôture transitive de f) est une distance bi-invariante.

Preuve : f est symétrique ($\dot{\sigma\pi}^{-1} = \dot{\pi\sigma}^{-1}$), nulle sur la diagonale ($F(\dot{1}) = 0$), invariante à droite par construction, donc à gauche d'après la condition 5) de la proposition précédente. Si $F^{-1}\{0\} = \dot{1}$, alors $f(\sigma,\pi) = 0 \Rightarrow \sigma\pi^{-1} = 1$, donc f est une quasi-distance. D'autre part on vérifie que la bi-invariance est héréditaire par clôture transitive, donc $\bar{f}_t$ est bi-invariante.

Construction de quasi-distances bi-invariantes sur S_n

Pour $\sigma \in S_n$, posons $f_i(\sigma) = n - \sum_{j=1}^{i} N_j(\sigma)$.

Propriétés : 1) $f_1 = H$ (distance de Hamming)

2) $f_n = T$ (définie en 3.4.)

3) $\left\lfloor \frac{n}{i+1} \right\rfloor \geqslant f_i - f_{i+1} \geqslant 0$

4) $2T \geqslant H$.

Preuves : 1), 2), résultent des définitions

$$f_i(\sigma) - f_{i+1}(\sigma) = N_{j+1}(\sigma) \geqslant 0$$

et par (2) $N_{i+1}(\sigma) \leqslant \frac{n}{i+1}$ d'où 3).

D'autre part, par (2)

$$N_1 + 2 \sum_{j\neq 1} N_j \leqslant n, \text{ d'où}$$

$$2T = 2(n - \sum_{j=1}^{n} N_j) = n - N_1 + (n - N_1 - 2 \sum_{j\neq 1} N_i)$$

$$\geqslant n - N_1 = H, \text{ i.e. 4).}$$

Nous donnons ainsi une réponse partielle à une question de /11/ : construire des métriques bi-invariantes.

Généralisation :

La notion de cycle existe sur T_n /9/. Par suite les f_i s'étendent à ce

demi-groupe et fournissent des quasi-distances invariantes à droite.

4. L-CLIQUES MAXIMALES

Soit (E,d) un ensemble muni d'une métrique entière. $A \subset E$ est une *L-clique* si $\forall x, y \in A$, $x \neq y$, $d(x,y) \in L$, avec $L \subset \mathbb{N}$.
L'ensemble des L-cliques est noté $\mathcal{A}(L)$.

Exemples : Pour L = {e, e+1, ... }, les éléments de $\mathcal{A}(L)$ sont les *e-codes*, pour L = {1,2, ... , e-1}, on obtient des *e-anticodes*, pour L = {e} des *e-codes équidistants* (cf. introduction).

Par analogie avec la théorie des graphes, on pose $\omega_L(E) = \max_A |A|$, $A \in \mathcal{A}(L)$. Dans cette section nous cherchons des bornes pour $\omega_L(E)$ (le cas $E = S_n$, $d = H$ est étudié dans /12/). $A \in \mathcal{A}(L)$ est dite *maximale* si $\forall g \in E-A$, $A \cup \{g\} \notin \mathcal{A}(L)$. Une famille d'ensembles T_i, $1 \leqslant i \leqslant t$ est appelée *ℓ-recouvrement* (resp. *ℓ-pavage*) de E si tout élément de E appartient à au moins (resp. au plus) ℓ-ensembles T_i. On a :

$$\sum_{i=1}^{t} |T_i| \geqslant \ell|E| \text{ pour tout } \ell\text{-recouvrement,}$$

$$\sum_{i=1}^{t} |T_i| \leqslant \ell|E| \text{ pour tout } \ell\text{-pavage.}$$

Donnons maintenant une borne inférieure pour $\omega_L(E)$, utilisant les 1-recouvrements.

Soit $A \in \mathcal{A}(L)$, prenons $T_i = \{b \in E,\ d(a_i,b) \notin L\}$, alors A est maximale ssi $\bigcup_{a_i \in A} T_i = E$, soit ssi $\{T_i\}_{a_i \in A}$ est un 1-recouvrement de E, d'où :

PROPOSITION : $$\omega_L(E) \geqslant \frac{|E|}{\max |T_i|}.$$

Supposons désormais que E soit un groupe, soient $A,B \subset E$, on dit que (A,B) est *bruit-code correcteur* /10/ si $\forall a, a' \in A$, $b, b' \in B$, $ab \neq a'b'$. En codage cette condition assure qu'un message "a" affecté d'un bruit "b",

(ici multiplicatif) ne sera pas confondu avec un message "a'" affecté d'un bruit "b'", et pourra donc être décodé sans ambiguïté. Remarquons que pour (A,B) bruit-code correcteur $\{T_i\} = \{a_i B\}_{a_i \in A}$ est un 1-pavage donc $\Sigma\ |T_i| = |A|.|B| \leqslant |E|$. Posant $\bar{L} = \{k \in \mathbb{N},\ k \notin L, \exists\, x, y \in E$ tels que $d(x,y) = k\}$ on en déduit le

LEMME : Si $A \in \mathcal{A}(L)$, $\bar{A} \in \mathcal{A}(\bar{L})$ et $(A,\bar{A})$ est un bruit-code correcteur, on a

$$|A| \leqslant \frac{|E|}{|\bar{A}|}\ .$$

Une borne analogue pour les schémas d'association est donnée dans /8/.

Soit $S \subset E$, notons $S^{-1} = \{s^{-1},\ s \in S\}$ et appelons S *symétrique* si $S = S^{-1}$.

PROPOSITION : Chacune des conditions suivantes est suffisante pour que $(A,\bar{A})$ soit bruit-code correcteur.

i) d invariante à droite et A ou $\bar{A}$ est symétrique

ii) d est bi-invariante.

Preuve : Supposons $a, a' \in A$, $b, b' \in \bar{A}$ et $ab = a'b'$. Alors

$$(a')^{-1} a = b'b^{-1} \text{ et } d((a')^{-1}, a^{-1}) = d(b',b).$$

i) Si A est symétrique $(a')^{-1}, a^{-1} \in A$ donc $d((a')^{-1}, a^{-1}) \in L$;

ii) Si d est bi-invariante $d((a')^{-1}, a^{-1}) = d(a',a) \in L$.

Dans les 2 cas on obtient une contradiction, car $d(b',b) \in \bar{L}$.

Corollaire (borne de dualité) : Si d est bi-invariante sur le groupe E, on a :

$$\omega_L(E) \leqslant \frac{|E|}{\omega_{\bar{L}}(E)}\ .$$

Supposons à partir de maintenant d invariante à droite. Soit $A \in \mathcal{A}(L)$ maximale, $S \subset E$ et A/S une L-clique maximale dans S. Alors :

LEMME : Si (A, A/S) est bruit-code correcteur, on a

$$\frac{|A|}{|E|} \leqslant \frac{|A/S|}{|S|}\ .$$

Preuve : $\{S^{-1}a_i\}_{a_i \in A}$ est un $|A/S|$-pavage de E.

En effet supposons que $e \in E$ s'écrive

$$e = s_1^{-1} a_1 = s_2^{-1} a_2 = \ldots = s_\ell^{-1} a_\ell,\ a_i \in A,\ s_i \in S,$$

alors $\forall i,j \leqslant \ell,\ i \neq j\ \ d(a_i,a_j) = d(s_i,s_j) \in L$, donc $\ell \leqslant |A/S|$.

Par suite $\sum_{a_i \in A} |S^{-1}a_i| = |S|.|A| \leqslant |A/S|.|E|$, d'où

PROPOSITION (borne de densité) : Soient d invariante à droite sur le groupe E, $S \subset E$ et (A,A/S) bruit-code correcteur, alors

$$\omega_L(E) \leqslant \omega_L(S).\ \frac{|E|}{|S|}\ .$$

Un exemple d'application de la borne de dualité au codage.

E est le groupe S_n et d invariante à droite. Soit C un e-code ($C \in \mathcal{C}(L)$ avec $L = \{e, e+1, \ldots\}$), $\bar{L} = \{1, 2, \ldots e-1\}$. Nous obtenons deux bornes supérieures en considérant les deux e-anticodes suivants :

$A_1 = \{a \in E,\ d(a) \leqslant \lfloor \frac{e-1}{2} \rfloor\}$ (boule de rayon $\lfloor \frac{e-1}{2} \rfloor$).

A_1 est symétrique, donc pour tout C, (C,A_1) est bruit-code correcteur.

Il vient : $|C| \leqslant |E|.|A_1|^{-1}$

Un code réalisant l'égalité $|C| = |E|.|A_1|^{-1}$ est dit *parfait*.

Le deuxième anticode est lié à la notion de stabilisateur.

Soit d_{max} la fonction $i \to d_{max}(i) = \underset{\sigma \in S_i}{\text{Max}} \{d(\sigma)\}$

et d_{max}^{-1} définie par $d_{max}^{-1}(j) = \max \{i,\ d_{max}(i) \leqslant j\}$,

alors $A_2 = \{\sigma \in S_n,\ \wp(\sigma) \geqslant n - d_{max}^{-1}(e-1)\} \in \mathcal{C}(\bar{L})$.

$|A_2| = (d_{max}^{-1}(e-1))!$ et A_2 symétrique d'où :

$$|C| \leqslant \frac{n!}{(d_{max}^{-1}(e-1))!}\ .$$

Par exemple pour d = H, $H_{max}(i) = H_{max}^{-1}(i) = i$, il vient $|C| \leqslant \frac{n!}{(e-1)!}$, l'égalité étant réalisée s'il existe un ensemble exactement $(n - e+1)$ fois transitif /3/. Pour d = H, $E = (\mathbf{F}_q)^n$, la borne correspondante est celle bien connue de Singleton : $|C| \leqslant q^{n - e+1}$.

5. QUELQUES PROBLEMES DANS S_n

1) Propriétés statistiques des poids

La valeur maximale, la moyenne, la variance et la convergence vers la loi normale quand $n \to \infty$ sont étudiées dans /11/, /25/, pour T, L_1, I. Diaconis (communication privée) remarque que H est asymptotiquement normale. Des caractérisations analogues seraient intéressantes pour certaines classes de distances (bi-invariantes par exemple).

2) Relations entre poids

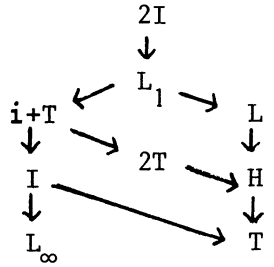
Rappelons les définitions des différents poids sur un exemple pris dans S_6. Soit $\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 4 & 5 & 3 & 1 \end{pmatrix}$, notée (6 2 4 5 3 1) ou encore par ses cycles (16) (2) (345). Alors

$H(\theta) = |\{i,\ i \neq \theta(i)\}| = 5$; $L_1(\theta) = \Sigma|\theta(i) - i| = 14$;

$L_\infty(\theta) = \text{Max}|\theta(i) - i| = 5$; $L(\theta) = \Sigma\ \text{Min}(|\theta(i) - i|, 6-|\theta(i) - i|) = 6$;

$T(\theta) = 6-|\{\text{cycles}\}| = 3$; $I(\theta) = |\{\text{minimal de transpositions } t_i = (i, i+1)$ telles que $t_i t_j \ldots t_\ell\ \theta = 1\}|$, soit $I(\theta) = 11$.

Soient d_1, d_2 deux poids. Disons que $d_1 \geqslant d_2$ ssi $\forall \sigma \in S_n$, $d_1(\sigma) \geqslant d_2(\sigma)$ et notons $d_1 \to d_2$ cet ordre entre poids. On obtient alors le diagramme suivant, reliant les 6 poids L_1, L_∞, L, H, T et I :



Pour $2I \geqslant L_1 \geqslant I+T$ cf /11/, $2T \geqslant H \geqslant T$ (voir 3.6.) ; les autres inégalités résultent des définitions. Un problème plus général est d'établir des isomorphismes "lipschitziens" entre distances, c'est à dire pour

2 distances d_1 et d_2, de trouver λ et μ indépendants de n tels que

$\lambda d_1 \geqslant d_2 \geqslant \mu d_1$.

3) Cardinal des boules

Soit $S(d,n,r) = |\{\sigma \in S_n,\ d(\sigma) = r\}|$ le cardinal d'une sphère de rayon r et $B(d,n,r) = |\{\sigma \in S_n,\ d(\sigma) \leqslant r\}|$ celui d'une boule de rayon r.

On a $B(d,n,r) = \sum_{i=1}^{r} S(d,r,i)$

et $\quad d_1 \geqslant d_2 \Longrightarrow B(d_1,n,r) \leqslant B(d_2,n,r)$.

Les cardinaux de certaines boules et sphères sont connus, par exemple

$$S(H,n,r) = \binom{n}{r}\, r!\, \sum_{i=o}^{r} \frac{(-1)^i}{i!} \sim e^{-1} \binom{n}{r}\, r!.$$

On peut montrer /7/ que

$$S(T,n,r) = \sum_{\substack{(t_1 \ldots t_n) \in N^n \\ \Sigma t_i = n-r}} \frac{n!}{1^{t_1}.t_1! \ldots n^{t_n}.t_n!}$$

$$B(L_\infty,n,1) = B(L_\infty,n-1,1) + B(L_\infty,n-2,1)$$

$$= F_n \text{(nombres de Fibonacci) avec } F_0 = F_1 = 1.$$

La preuve est évidente, contrairement à celle du résultat suivant /19/ :

$B(L_\infty,n,2) = 2B(L_\infty,n-1,2) + 2B(L_\infty,n-3,2) - B(L_\infty,n-5,2)$.

Enfin $S(I,n,r) = \sum_{i=o}^{n-1} S(I,n-1,r-i)$ se montre par récurrence /25/. Pour une formule explicite cf. /18/ p. 16.

Les expressions d'autres S(d,n,r) ou B(d,n,r) ne nous sont pas connues.

BIBLIOGRAPHIE

/1/ ASSAOUD P., DEZA M., "Isometric embedding in L_1 and related problems", à paraître.

/2/ BEYER W.A., STEIN M.L., ULAM S.M., "Metric in Biology, an Introduction", Preprint LA-4973,Univ. of Calif., Los Alamos (1972).

/3/ BLAKE I.F., COHEN G., DEZA M., "Coding with Permutations", Inf. and Control, à paraître.

/4/ BLUMENTHAL L.M., "Theory and applications of distance geometry", Chelsea Publ. Co., New York (1970).

/5/ BIRKHOFF G., "Lattice Theory" Coll. Publ. Vol XXV, AMS, Prov. 1967.

/6/ BREDEHIN D.A., SCHEIN B.M., "Representations of ordered Semigroups and Lattices by Binary Relations", Colloq. Math. Vol 39 (1978), 1-12.

/7/ COHEN G., "Some Metrics on the Symmetric Group", Rapport interne ENST-C-78010, (1978).

/8/ DELSARTE P., "An Algebraic Approach to the Association Schemes of Coding Theory", Philips Res. Rep. Suppl., n° 10 (1973).

/9/ DENES J., "Connections between Transformation Semigroups and Graphs", in Théorie des Graphes, Rome, Dunod, Juillet 1966, 93-102.

/10/ DEZA M., "Correction of Arbitrary and Worst Noise", Probl. Per. Inf., Vol 4 (1968), 26-31.

/11/ DIACONIS P., GRAHAM R.L., "Spearman's Footrule as a Measure of Disarray", J. Royal Stat. Soc., ser.B, Vol. 39-2 (1977), 262-268.

/12/ FRANKL P., DEZA M., "On the Maximum Number of Permutations with Given Maximal on Minimal Distance", J. Comb. Th., Vol 22, n° 3 (1977), 352-360.

/13/ GABIDULIN E.M., "Combinatorial Metrics in Coding Theory", in 2nd Int. Symp. on Inf. Th., Budapest, Akadimiai Kaido, (1973), 169-176.

/14/ GABIDULIN E.M., SIDORENKO Y.R., "One General Bound for Code Volume", Prob. Per. Inf., Vol-12, n° 4 (1976), 266-269.

/15/ HOWIE Y.M., "An Introduction to Semigroup Theory", L.M.S. Monographs 7, Acad. Press, London (1976).

/16/ KAY D.C., CHARTRAND G., "A characterization of certain Ptolemaic Graphs", Canad. J. Math. 17 (1965), 342-346.

/17/ KELLY J.B., "Hypermetric Spaces", in The Geometry of Metric and Linear Spaces, Lecture Notes in Math., 490, Springer-Verlag (1975), 17-31.

/18/ KNUTH D.E., "The Art of Computer Programming", Vol 3, Reading, Addison-Wesley, 1973.

/19/ LAGRANGE R., "Quelques résultats dans la métrique des permutations", Ann. Sci. ENS. 79 (1962 a).

/20/ LAL S.N., SINGH A.K., "An Analog of Banach's Contraction Principle for 2-Metric Spaces", Bull. Austral. Math. Soc., Vol 18 (1978), 137-143.

/21/ LEVENSTEIN V.I., "Methods for obtaining Bounds in Metric Problems of Coding Theory", in 1975 IEEE-USSR Worksop on Inf. Th., Publ. IEEE.

/22/ MENGER K., "Statistical Metrics", Proc. Nat. Acad. Sci. USA., Vol 28 (1942), 535-537.

/23/ MONJARDET B., "Caractérisations métriques des ensembles ordonnés semi-modulaires", Math. et Sci. Hum., n° 56 (1976), 77-87.

/24/ TANAKA E., KASAI T., "Synchronization and Substitution Error-Correcting Codes for the Levenstein Metric", IEEE-IT, Vol 22-2, March 1976.

/25/ KENDALL M.G., "Rank Correlation Methods", 4ième Ed, Griffin, 1970.

/26/ BLAKE I.F., MULLIN R.C., "The Mathematical Theory of Coding", Academic Press, 1975.

/27/ MAC WILLIAMS F.J., SLOANE N.J.A., "The Theory of Error-Correcting Codes, I, II", North-Holland, 1977.