Annals of Discrete Mathematics 8 (1980) 211–216

SOME METRICAL PROBLEMS ON S_n*

G. COHEN
Ecole Nationale Supérieure des Telecommunications, Paris, France

M. DEZA
CNRS, 75007 Paris, France

We present some problems related to right- (or bi-)invariant metrics d on the symmetric group of permutations S_n. Characterizations and constructions of bi-invariant extremal (in the corresponding convex cone) metrics are given, esp. for $n \leq 5$. We also consider special subspaces of the metric space (S_n, d): unit balls, sets with prescribed distances (L-cliques), "hamiltonian" sets.

Here we give (for proofs, see [3]) some results and problems arising by analogy with extremal set systems. Related problems of coding type (with Hamming metric) are considered in [1, 4].

1. Invariance

S_n is the symmetric group of degree n whose elements (permutations) are denoted $\alpha, \beta, \gamma, \ldots$, with 1 being the identity. It is endowed with an integer metric $d: S_n \times S_n \to \mathbb{N}$ which will always be in this paper *right-invariant*, i.e. $\forall \alpha, \beta, \gamma\ d(\alpha\gamma, \beta\gamma) = d(\alpha, \beta)$. Then $d(\alpha, \beta) = d(\alpha\beta^{-1}, 1) = p_d(\alpha\beta^{-1})$ is the *weight* of $\alpha\beta^{-1}$. We will denote $d(1, \alpha)$ by $d(\alpha)$.

Examples. $H(\sigma) = |\{i: \sigma(i) \neq i\}$; $L_1(\sigma) = \sum |\sigma(i) - i|$; $L_\infty(\sigma) = \text{Max}\, |\sigma(i) - i|$; $T(\sigma) =$ min. number of transpositions t_i such that $t_i t_j \cdots \sigma = 1$. If d is also *left-invariant*, i.e. $\forall \alpha, \beta, \gamma\ d(\gamma\alpha, \gamma\beta) = d(\alpha, \beta)$, it is said to be *bi-invariant*.

Proposition 1. *The bi-invariance of d is equivalent to any of the following conditions:*

(1) $\forall \alpha, \beta\ d(\alpha\beta) = d(\beta\alpha)$,
(2) $\forall \alpha, \beta\ d(\alpha, \beta) = d(\alpha^{-1}, \beta^{-1})$,
(3) $\forall \alpha, \beta\ d(\alpha) = d(\beta\alpha\beta^{-1})$.

Calling $N_i(\sigma)$ the number of cycles of length i in σ, with $\sum iN_i(\sigma) = n$, and $\mathscr{C}_\sigma$ the conjugacy class of σ, i.e. $\mathscr{C}_\sigma = \{\alpha\sigma\alpha^{-1}, \alpha \in S_n\}$ we get

Corollary. *H and T are bi-invariant.*

* Ce travail a été effectué pendant le séjour des auteurs au Centre de Recherche de Mathématiques, Appliquées, Université de Montréal.

It comes from the fact that $H(\sigma) = n - N_i(\sigma)$, $T(\sigma) = n - \sum N_i(\sigma)$ (Cayley) and (3) of Proposition 1.

2. Graphic distance

The distance d is *graphic* if $d(\alpha, \beta)$ is the length of the shortest path joining α and β in the graph whose vertex set is S_n and edge-set $\{(\sigma, \theta): d(\sigma, \theta) = 1\}$. This is equivalent to saying: $\forall \alpha, \beta \; d(\alpha, \beta) \geq 2 \Rightarrow \exists \gamma$ between α and β, i.e. such that $d(\alpha, \beta) = d(\alpha, \gamma) + d(\gamma, \beta)$ (see [10]).

Proposition 2. *If d is a graphic distance (connected graph), then $E_d = \{\alpha: d(\alpha) = 1\}$ generates S_n. Reciprocally, if E is a symmetric set (i.e. $e \in E \Rightarrow e^{-1} \in E$), then the distance d_E (defined by $d_E(1) = 0$, $d_E(e) = 1$ ($\forall e \in E$), $d_E(\alpha)$ is the smallest number of $e_i \in E$, such that $\alpha = e_i e_j, \ldots, d_E(\alpha) = \infty$ when such a writing is impossible) is a graph weight, finite when E generates S_n.*

Proposition 3. *d_E is bi-invariant iff E is stable by conjugacy, i.e. $E = \bigcup \mathscr{C}_{\alpha_i}$.*

Some constructions. Let d_{E_1, E_2} be graph distances as in Proposition 2. Denote:

(1) $d_{E_1} \wedge d_{E_2} = d_{E_1 \cup E_2}$,
(2) $d_{E_1} \vee d_{E_2} = d_{E_1 \wedge E_2}$,
(3) $d_{E_1} \circ d_{E_2} = d_{E_1 \circ E_2}$, where $E_1 \circ E_2 = \{\sigma_1 \sigma_2, \sigma_1 \in E_1, \sigma_2 \in E_2\}$.

They are graph weights, bi-invariant if d_{E_1} and d_{E_2} are bi-invariant. This is a partial answer to a question of [5].

3. Extremal bi-invariant metrics

Bi-invariant metrics form a convex cone over $\mathbb{R}$.

Proposition 4. *If E is exactly one conjugacy class, i.e. $E = \mathscr{C}_\alpha$, then d_E is an extreme ray of the cone of bi-invariant metrics.*

Examples. $E = \mathscr{C}_{(12)}$, the set of all transpositions; then $d_E = T$ is extremal. Let C_i denote a cycle of length i, $E_i = \{C_i\}$ generates S_n for even i. The associated distance $d_{\{C_i\}}$ is extremal. We have

$$H = T + \bigwedge_{i=2}^{\infty} d_{\{C_i\}}.$$

Thus H is not an extreme ray.

Proposition 5. *Let $E_1 = \mathscr{E}_\alpha$, $E_2 = \mathscr{E}_\beta$, then d_{E_1} and d_{E_2} are Lipschitz-isomorph, i.e.*

$$k_1^{-1} d_{E_1} \leq d_{E_2} \leq k_2 d_{E_1}$$

with $k_1 = P_{E_1}(\beta)$, $k_2 = P_{E_2}(\alpha)$ independent of n.

The characterization of extremal bi-invariant metrics (graphic or not) seems a difficult problem.

Examples. A few bi-invariant metrics on S_5 (see Table 1).

Table 1

	Cycle structure					
d	(1) (2) (3) (45)	(1) (2) (345)	(1) (2345)	(1) (23) (45)	(12345)	(12) (345)
H	2	3	4	4	5	5
T	1	2	3	2	4	3
$d_{\{C_4\}}$	3	2	1	2	2	3
$T \wedge d_{\{C_3\}}$	1	1	2	2	2	2
$\bigwedge_{i=2}^{\infty} d_{\{C_i\}}$	1	1	1	2	1	2

4. Some special subspaces of the metric space (S_n, d)

4.1. *Hamiltonian sets*

Let E be a set of transformations, then [12] (S_n, d_E) has a hamiltonian circuit if the graph G_E with vertex set $\{1, 2, \ldots, n\}$ and edge set $\{(i, j): \exists t \in E, t(i) = j, t(j) = i\}$ is connected.

Examples. $G_E = K_n$, then $d_E = T$.

G_E is the path of length n (i.e. $1, 2, \ldots, n$), then d_E is noted I.

G_E is the star with center 1, then d_E is noted U.

From $L_\infty \leq I$, one deduces that (S_n, L_∞) is also hamiltonian.

Proposition 6. *If (S_n, d_{E_1}) and (S_n, d_{E_2}) are hamiltonian, then $(A_n, d_{E_1} \circ d_{E_2})$ is hamiltonian.*

Example. $(A_n, U \circ U)$ is hamiltonian, with

$$U \circ U = d_E, \quad \text{where} \quad E = \{t_1 \circ t_j: \ t_i = (1\,i), \ t_j = (1\,j)\}.$$

That is, one can generate A_n by performing permutations which are cycles of length 3 of the form $(j\,i\,1)$. Hence $(A_n, d_{\{C_3\}})$ is hamiltonian.

In [9] a similar question is investigated. Ring n bells in a "good" way, which may be restated as follows: find a hamiltonian circuit in (S_n, L_∞) with the extra condition that $\varphi(\sigma_i\sigma_{i+1}^{-1}) \cap \varphi(\sigma_{i+1}\sigma_{i+2}^{-1}) = \emptyset$, where $\varphi(\alpha)$ is the set of fixed points of α, and σ_i, σ_{i+1}, σ_{i+2} are any three consecutive nodes of the circuit.

4.2. *Metric basis and symmetries*

A *d-metric basis* B is a set $B \subset S_n$ such that $\forall \sigma, \pi \in S_n$, if $\forall \beta \in B \quad d(\sigma, \beta) = d(\pi, \beta)$, then $\sigma = \pi$.

It is shown in [5] that $1 \cup \{C_2\} \cup \{C_3\}$ is a H-metric basis and this is used to prove that G_H, the group of isometries of (S_n, H) has order $2(n!)^2$ and contains as normal subgroup $F = \{f_{\sigma\pi}\colon f_{\sigma\pi}(\alpha) = \sigma\alpha\pi^{-1}\}$. For any bi-invariant d, it is easy to see that $G_d \supset G_H$. It would be interesting to find minimal d-metric basis for other d's.

4.3. *Spheres and balls*

Let $S(d, n, r) = \{\sigma \in S_n\colon d(\sigma) = r\}$, $B(d, n, r) = \{\sigma \in S_n\colon d(\sigma) \leq r\}$ then

$$|S(H, n, r)| = \binom{n}{r} r! \sum_{i=0}^{r} \frac{(-1)^i}{i!} \simeq e^{-1} \binom{n}{r} r!,$$

$$|S(T, n, r)| = \sum_{\substack{(t_1 \cdots t_n) \in \{1, 2, \ldots, n\}^n \\ \Sigma t_i = n - r}} \frac{n!}{1^{t_1} t_1! \cdots n^{t_n} \cdot t_n!}, \text{ (see [2])}$$

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

$$|B(L_\infty, n, 2)| = 2\,|B(L_\infty, n-1, 2)| + 2\,|B(L_\infty, n-3, 2)| - |B(L_\infty, n-5, 2)|, \quad \text{(see [11])}$$

$$|S(I, n, r)| = \sum_{i=0}^{n-1} |S(I, n-1, r-i)|.$$

5. *L*-cliques in (S_n, d)

Let d be a right-invariant distance on S_n. Let L be a subset of $\{1, 2, \ldots, n\}$. We call a subset A of S_n a *L-clique* (denote $\mathcal{A}(L)$) if $d(x, y) \in L$ for any $x, y \in A$, $x \neq y$. We call $\mathcal{A}(L)$ *l-code* if $L = \{l, l+1, \ldots, n\}$, *$l$-anticode* if $L = \{1, 2, \ldots, l-1\}$, *$l$-equidistant code* if $L = \{l\}$ for some integer l. Let us fix a L-clique A.

For any subset $S \subseteq S_n$ denote $\mathcal{A}_S(L)$ any subset $B \subseteq S$ such that B is a L-clique.

Proposition 7. *Let $S \subseteq S_n$, then*

$$|A| \leq \max |\mathcal{A}_S(L)| \cdot \frac{n!}{|S|}$$

if either d is bi-invariant or A is symmetric.

Proposition 7 follows from *density bound*

$$\frac{|A|}{|S_n|} \leqslant \frac{|\mathscr{A}_S(L)|}{|S|}.$$

Let $q(\alpha, \beta)$ be a right-invariant function $q: S_n \times S_n \to \mathbb{R}$ such that
(a) matrix $(q(\alpha, \beta))$ of order $n!$ has only nonnegative eigenvalues and
(b) $q(\alpha, \beta) \leqslant 0$ whenever $d(\alpha, \beta) \in L$.

Proposition 8.

$$|A| \leqslant (n!)^2 \frac{\max_{\alpha \in S_n} q(\alpha, \alpha)}{\sum_{\alpha, \beta \in S_n} q(\alpha, \beta)}.$$

Proposition 8 follows from *averaging bound* [8]

$$\frac{\sum_{\alpha, \beta \in S_n} q(\alpha, \beta)}{|S_n|^2} \leqslant \frac{\sum_{\alpha, \beta \in A} q(\alpha, \beta)}{|A|^2}$$

Denote $\bar{L} = \{1, 2, \ldots, n\} - L$.

Proposition 9.

$$|A| \leqslant \frac{n!}{\max |\mathscr{A}(\bar{L})|}$$

if either d is bi-invariant or A is symmetric.

Proposition 9 follows from *duality bound* [7]

$$|\mathscr{A}(L)| \cdot |\mathscr{A}(\bar{L})| \leqslant |S_n|.$$

We give now two applications of Proposition 9 for the case $L = \{l, l+1, \ldots, n\}$, i.e. L-clique A is a l-code.

Denote $A_1 = B(d, n, \lfloor \frac{1}{2}(l-1) \rfloor)$. Of course, A_1 is a symmetric l-anticode. Denote A_2 the stabilizator of a smallest subset $M \subseteq \{1, 2, \ldots, n\}$ such that this stabilizator is a $\bar{L}$-clique (i.e. l-anticode); of course, A_2 is symmetric.

Corollary. *For* $L = \{l+1, l+2, \ldots, n\}$
(i) $|A| \leqslant n!/|A_1|$,
(ii) $|A| \leqslant n!/|A_2|$.

Explicit values for some $|A_1|$ are derivable from Section 4.3. For (ii) one obviously has $|A_2| = (n - |M|)!$ but a general relation between $|M|$ and l is complicated (see [2]).

Two well-known upper bounds for codes in $(\mathbb{F}_q)^n$ with Hamming distance (Hamming–Rao and Singelton's bounds) corresponds to (i), (ii). For $d = H$: we have equality in (ii) iff A is a sharply $(n - l + 1)$-transitive subset of S_n; equality in (i) will give the analog of perfect codes.

References

[1] I.F. Blake, G. Cohen and M. Deza, Coding with permutations, Information and Control 43 (1) (1979) 1–19.

[2] G. Cohen, Some metrics on the symmetric group, Rapport ENST-C-78010 (1978).

[3] G. Cohen and M. Deza, Distances invariantes et L-cliques sur certains demi-groupes finis, Math. Sci. Humaines 67 (1979) 49–69.

[4] G. Cohen and M. Deza, Décodage des codes de permutations, Coll. Int. CRNS No. 276, Théorie de l'information (July 1977) Cachan, France, 203–207.

[5] P. Diaconis and R.L. Graham, Spearman's footrule as a measure of disarray, J. Roy. Statist. Soc., Ser. B 39-2 (1977) 262–268.

[6] H. Farahat, The symmetric group as metric space, J. London Math. Soc. 35 (1960) 215–220.

[7] P. Frankl and M. Deza, On the maximum number of permutations with given maximal on minimal distance, J. Combin. Theory 22 (3) (1977) 352–360.

[8] E.M. Gabidulin and Y.R. Sidorenko, One general bound for code volume, Problemy Peredači Informacii 12 (4) (1976) 266–269.

[9] B. Jaulin, Sur l'art de sonner les cloches, Math. Sci. Humaines 60 (1977) 5–20.

[10] D. Kay and G. Chartrand, A characterization of certain ptolemaic graphs, Can. J. Math. 17 (1965) 342–346.

[11] R. Lagrange, Quelques résultats dans la métrique des permutations, Ann. Sci. Ecole Norm. Sup. 79 (1962a).

[12] J. Slater, Generating all permutations by graphical transpositions, Ars Combinatoria 5 (1978) 219–225.