A Survey on Packing and Covering Problems in the Hamming Permutation Space

Jörn Quistorff
Department 4
FHTW Berlin (University of Applied Sciences)
10313 Berlin, Germany
J.Quistorff@fhtw-berlin.de

Submitted: Mar 22, 2004; Accepted: Apr 17, 2006; Published: Apr 24, 2006
Mathematics Subject Classifications: 05B40, 20B35

Abstract

Consider the symmetric group S_n equipped with the Hamming metric d_H. Packing and covering problems in the finite metric space (S_n, d_H) are surveyed, including a combination of both.

1 Introduction

Let n be a positive integer and consider the symmetric group S_n of all permutations of the set $\{1, 2, ..., n\}$. There are several metrics on S_n, surveyed in [20]. The most important one seems to be the Hamming metric d_H. In the present paper, the finite metric space (S_n, d_H) will be called the *Hamming permutation space*. The packing and covering problems in this space are the following.

- Let d be given and determine (or estimate) the largest cardinality of a d-packing, i.e. of a subset $C \subseteq S_n$ with the property that its elements are at a distance of at least d from each other.
- Let e be given and determine (or estimate) the smallest cardinality of an e-covering, i.e. of a subset $C \subseteq S_n$ with the property that the balls of radius e around the elements of C cover the whole space.

The first papers on packing in the Hamming permutation space are [19], where Deza raised the problem in 1976, and [22]. Considerable research on covering in this space was recently started by Kézdy/Snevily [26] and Cameron/Wanless [10]. But already in 1978, a problem combining packing and covering was introduced by Deza/Vanstone [21, Section 3.4.].

Similar problems are frequently discussed in other situations. Of special interest is the classical *coding theory*, dealing with Q^n, $|Q| = q \geq 2$, equipped with the Hamming (or Lee) metric, see for example [3], [6], [7], [14], [27], [28], [36]. Recently, combinations of packing and covering problems in (Q^n, d_H) have been considered, see [29] and its references. The connection between coding theory and the corresponding problems on permutations was pointed out by Blake et al. [5] in 1979.

Packing and covering problems in *graph theory*, using the length of the shortest path as a metric, can be interpreted as generalizations of the respective problems in coding theory, but not of the respective problems on permutations. Modifying these problems one can get six closely connected extremal cardinalities. In 1978, Cockayne et al. [11] proved them to be related by a single string of inequalities. These cardinalities are now standard in graph theory, compare [24].

A common generalization of packing and covering problems in both graph theory and the Hamming permutation space, was given 2003 in [31] where the notion of a *finite metric space* is used. That paper also contains the transformation of the six extremal cardinalities mentioned above to finite metric spaces.

In coding theory, a standardization of the notations regarding packing and covering has taken place, the letters A and K (more precisely: $A_q(n, d)$ and $K_q(n, R)$) indicate the extremal cardinalities of the classical packing and covering problems. In graph theory, β and γ (more precisely: $\beta_0(G)$ and $\gamma(G)$) became standard instead. Furthermore, i (more precisely: $i(G)$) indicates an extremal number related to a problem combining packing and covering. In [31], the letters β, γ and i were transferred to finite metric spaces.

The aim of the present paper is to survey results on packing and covering problems in the Hamming permutation space, including a combination of both. This seems to be necessary since some papers are hard to trace and many different notations have been used up to now. Furthermore, the author hopes to promote the use of β, γ and i also in the Hamming permutation space.

Extremal problems concerning subgroups (instead of subsets) of S_n as well as asymptotic results will not be surveyed in this paper.

The paper is organized as follows: Section 2 recalls necessary notations and some basic results. In Section 3, bounds are given which appear if the parameters of a packing or covering problem are modified, i.e. if at least two different Hamming permutation spaces are involved. In Section 4, so-called destructive bounds are studied which destroy the hope of finding very small sets solving the covering problem and very large sets solving the packing problem. In Section 5, so-called constructive bounds arising from constructions of suitable sets of permutations are discussed. Some conjectures are mentioned in Section 6. Finally, Section 7 presents existence problems for sets which satisfy bounds with equality.

2 Notation

Let $n \in \mathbf{N}$ and S_n be the symmetric group of all permutations of the set $\{1, 2, ..., n\}$. The identity permutation is denoted by id. Clearly,

$$d_H : S_n \times S_n \to \{0, 1, 2, ..., n\}, (\pi, \pi') \mapsto |\{x \in \{1, 2, ..., n\} : \pi(x) \neq \pi'(x)\}|$$

is a metric on S_n, called the Hamming metric. The finite metric space (S_n, d_H) will be called the Hamming permutation space. Two permutations $\pi, \pi' \in S_n$ agree in exactly $n - d_H(\pi, \pi')$ positions which is also the number of fixed points of $\pi^{-1}\pi'$. Let $D(S_n) := d_H(S_n \times S_n)$ be the set of all distances which appear in S_n. Since two permutations cannot differ in exactly one position, $D(S_n) = \{0, 2, 3, 4, ..., n\}$. A ball of radius $e \in D(S_n)$ around $\pi \in S_n$ is denoted by

$$B_e(\pi) := \{\pi' \in S_n : d_H(\pi, \pi') \leq e\}.$$

Its volume depends only on the radius, not on the centre. Hence,

$$V_e := |B_e(\pi)| = \sum_{k=0}^{e} \binom{n}{k} k! \sum_{x=0}^{k} \frac{(-1)^x}{x!}$$

for all $\pi \in S_n$. To avoid formal problems in Section 4, put $B_1(\pi) := B_0(\pi) = \{\pi\}$ and $V_1 := V_0 = 1$.

Consider now a subset C of the symmetric group S_n. Its packing radius is denoted by

$$p(C) := \max\{e' \in D(S_n) : B_{e'}(\pi) \cap B_{e'}(\pi') = \emptyset \, \forall \pi, \pi' \in C \text{ with } \pi \neq \pi'\}.$$

If C contains at least two permutations,

$$d(C) := \min\{d_H(\pi, \pi') \in D(S_n) : \pi, \pi' \in S_n \text{ with } \pi \neq \pi'\}$$

is called the minimum distance of C. In contrast to the situation in coding theory, the inequality $2p(C) + 1 \leq d(C)$ might fail: Take for example

$$C = \left\{ \text{id}, \begin{pmatrix} 1234 \\ 2341 \end{pmatrix} \right\} \subseteq S_4$$

implying $p(C) = 2$ and $d(C) = 4$. If C is nonempty then its covering radius is denoted by

$$t(C) := \max\{\min\{d_H(\pi, \pi') \in D(S_n) : \pi' \in C\} : \pi \in S_n\}$$

and $\Delta(C) := \max\{d_H(\pi, \pi') \in D(S_n) : \pi, \pi' \in C\}$ is called its diameter. Clearly, C is e-covering iff $t(C) \leq e$. Since $e, e' \in D(S_n)$ with $e > e'$ imply $B_e(\pi) \setminus B_{e'}(\pi) \neq \emptyset$, the inequality $p(C) \leq t(C)$ follows.

If the length of the shortest path joining two vertices of a finite (undirected loop-free) graph (V, E) is used as a metric on V, then another finite metric space is generated. In the graph theoretical literature concerning that space, an e-covering is called e-domination. Furthermore, a subset C is called e-independent iff its elements are at a distance $> e$

from each other. Hence, the connection to d-packings is obvious. In the following, only the notions of independent subsets and covering subsets will be used. Furthermore, only $e \in D(S_n)$ is considered, other cases like $e = 1$ are dull.

Clearly, every subset of an e-independent set is also e-independent. Furthermore, every superset of an e-covering is also e-covering. The only minimal e-independent subset of S_n is the empty set, the only maximal e-covering subset is S_n itself. The determination of maximal e-independent subsets and of minimal e-covering subsets in case of $e \in D(S_n) \setminus \{0, n\}$ is nontrivial while the situation $e \in \{0, n\}$ is again trivial. Clearly, a subset is maximal e-independent iff it is simultaneously e-independent and e-covering.

Let $\gamma_n(e)$ denote the smallest cardinality of a minimal e-covering subset of S_n. Let $i_n(e)$ and $\beta_n(e)$ denote the smallest and the largest cardinality of a maximal e-independent subset of S_n, respectively. The words *minimal* in the definition of $\gamma_n(e)$ and *maximal* in the definition of $\beta_n(e)$ can be omitted. Up to now, nearly nothing has been shown about the largest cardinality of minimal e-covering subsets of S_n.

The smallest cardinality $f(n, s)$ of a subset of S_n with a covering radius $\leq n - s$ is considered in [10]. Hence, $\gamma_n(e) = f(n, n - e)$. In [33], $U(S_n, d_H, e)$ is used instead.

The largest cardinality of a d-packing in S_n is denoted in [35] by $M(n, d)$. In [30] and [33], $u(n, d)$ and $u(S_n, d_H, d)$ are used instead. The maximal cardinality of a subset of S_n with the property that any two distinct permutations agree in at most λ positions is denoted in [19] and [22] by $R(n, \leq \lambda)$. Hence, $\beta_n(e) = M(n, e + 1) = R(n, \leq n - e - 1)$.

In [30], the smallest cardinality of a maximal d-packing in S_n is denoted by $v(n, d)$. In [21] and [10], the smallest cardinality of a maximal subset of S_n with the property that any two distinct permutations agree in at most k positions is denoted by $R_{\mathrm{minmax}}(n, \leq k)$ and $m(n, k)$, respectively. Hence, $i_n(e) = v(n, e+1) = m(n, n-e-1) = R_{\mathrm{minmax}}(n, \leq n-e-1)$.

Clearly,

$$1 \leq \gamma_n(e) \leq i_n(e) \leq \beta_n(e) \leq n! \tag{1}$$

holds true in analogy to the result of Cockayne et al. [11]. As mentioned above, the situation $e \in \{0, n\}$ is trivial since $\gamma_n(0) = n!$ and $\beta_n(n) = 1$.

Since $\gamma_n(e), i_n(e), \beta_n(e) \in \mathbf{N}$, every real lower bound α' on one of these desired values implies the lower bound $\lceil \alpha' \rceil$ and every real upper bound α'' implies the upper bound $\lfloor \alpha'' \rfloor$. These rounding rules can be applied to all of the following estimations.

3 Modifications

Clearly, γ_n and β_n are monotonously decreasing functions. If the parameter n is modified, some estimations can be proved.

Theorem 1 *Let $n, \check{n} \in \mathbf{N}$ and $e \in D(S_n)$ as well as $\check{e} \in D(S_{\check{n}})$.*

(i) $\frac{1}{n+1}\gamma_{n+1}(e) \leq \gamma_n(e) \leq \gamma_{n+1}(e)$ *and* $\gamma_{n+1}(e + 2) \leq \gamma_n(e)$ *if* $e \leq n - 1$.

(ii) $\frac{1}{n+1}\beta_{n+1}(e) \leq \beta_n(e) \leq \beta_{n+1}(e)$ *and* $\beta_{n+1}(e + 3) \leq \beta_n(e)$ *if* $0 < e \leq n - 2$.

(iii) $\min\{\beta_n(e), \beta_{\check{n}}(\check{e})\} \leq \beta_{n+\check{n}}(e + \check{e} + 1)$.

Proof: Let $y \in \{1, 2, ..., n\}$. Denote by $\tau_{y,n}$ the unique transposition in S_n with $\tau_{y,n}(y) = n$ and $\tau_{y,n}(n) = y$, if $y < n$. Otherwise put $\tau_{n,n} := \mathrm{id}$. If $\pi \in S_n$ then denote the extension of π to a permutation of $\{1, 2, ..., n+1\}$ with a fixed point $n+1$ by $\bar{\pi}$. If $\pi \in S_n$ with $\pi(n) = n$ then denote the restriction of π to a permutation of $\{1, 2, ..., n-1\}$ by $\mathrm{res}(\pi)$. If π is an arbitrary permutation in S_n then put $\pi' := \mathrm{res}(\tau_{\pi(n),n} \circ \pi) \in S_{n-1}$. Let $\rho : \{1, 2, ..., \breve{n}\} \to \{n+1, n+2, ..., n+\breve{n}\}, x \mapsto n+x$. Denote the concatenation of $\pi \in S_n$ and $\breve{\pi} \in S_{\breve{n}}$ with $x \mapsto \pi(x)$ if $x \le n$ and $x \mapsto \rho\breve{\pi}\rho^{-1}(x)$ if $x > n$ by $\pi \oplus \breve{\pi} \in S_{n+\breve{n}}$.

(i) Let $C \subseteq S_{n+1}$ be e-covering with $|C| = \gamma_{n+1}(e)$. Put $C' := \{\pi' \in S_n : \pi \in C\}$. Let $\sigma \in S_n$ then $\exists \pi \in C$ with $d_H(\bar{\sigma}, \pi) \le e$. Since $d_H(\sigma, \pi') \le d_H(\bar{\sigma}, \pi)$ also $C' \subseteq S_n$ is e-covering and $|C'| \le |C|$ holds true. This proves the second estimation.
Let $C \subseteq S_n$ be e-covering with $|C| = \gamma_n(e)$. Put $\bar{C} := \{\bar{\pi} \in S_{n+1} : \pi \in C\}$ and $\tilde{C} := \bigcup_{y=1}^{n+1} \{\tau_{y,n+1} \circ \bar{\pi} \in S_{n+1} : \pi \in C\}$. Let $\sigma \in S_{n+1}$ then $\exists \pi \in C$ with $d_H(\sigma', \pi) \le e$. Since $d_H(\sigma, \bar{\pi}) \le d_H(\sigma', \pi) + 2$ and $d_H(\sigma, \tau_{\sigma(n+1),n+1} \circ \bar{\pi}) = d_H(\sigma', \pi)$ it follows that $\bar{C} \subseteq S_{n+1}$ is $(e+2)$-covering and $\tilde{C}$ is e-covering. Finally, $\left|\bar{C}\right| = |C|$ and $\left|\tilde{C}\right| = (n+1)|C|$ prove the third and the first estimation, respectively.

(ii) Let $C \subseteq S_{n+1}$ be e-independent with $|C| = \beta_{n+1}(e)$. Then $C_y := \{\pi' \in S_n : \pi \in C$ and $\pi(n+1) = y\}$ is also e-independent $\forall y \in \{1, 2, ..., n+1\}$. Furthermore, $\exists y$ with $|C_y| \ge \frac{1}{n+1}|C|$. This proves the first estimation.
Let $C \subseteq S_n$ be e-independent with $|C| = \beta_n(e)$. Then $\bar{C} := \{\bar{\pi} \in S_{n+1} : \pi \in C\}$ is also e-independent and $|\bar{C}| = |C|$ holds true. This proves the second estimation.
Let $C \subseteq S_{n+1}$ be $(e+3)$-independent with $|C| = \beta_{n+1}(e+3)$. Then $C' := \{\pi' \in S_n : \pi \in C\}$ is e-independent and $|C'| = |C|$ holds true. This proves the third estimation.

(iii) Let $C = \{\pi_1, \pi_2, ..., \pi_{\beta_n(e)}\} \subseteq S_n$ be e-independent and let $\breve{C} = \{\breve{\pi}_1, \breve{\pi}_2, ..., \breve{\pi}_{\beta_{\breve{n}}(\breve{e})}\} \subseteq S_{\breve{n}}$ be $\breve{e}$-independent. Put $\tilde{C} := \{\pi_j \oplus \breve{\pi}_j \in S_{n+\breve{n}} : 1 \le j \le \min\{\beta_n(e), \beta_{\breve{n}}(\breve{e})\}\}$. By construction, $\tilde{C}$ is $(e+e'+1)$-independent and $\left|\tilde{C}\right| = \min\left\{|C|, \left|\breve{C}\right|\right\}$ holds true. □

The first estimation of part (i) is due to Cameron/Wanless [10]. The first and second estimation of part (ii) are given by Deza [19]. The third estimations of part (ii) as well as part (iii) are due to the present author [30]. The remaining two estimations of part (i) seem to be new.

4 Destructive Bounds

In this section, lower bounds on $\gamma_n(e)$ and $i_n(e)$ as well as upper bounds on $\beta_n(e)$ are surveyed. In general, one may say that these bounds destroy the hope of finding e-covering sets of very small cardinality as well as e-independent sets of very large cardinality. Hence, they will be called destructive in this paper. A first trivial example is $\gamma_n(e) \ge 2$ if $0 < e < n$.

The following additional definitions are useful in this context. Let $C \subseteq S_n$. The set of all distances appearing in C will be denoted by $D(C)$. If the subset C is nonempty with diameter $\Delta(C) \leq e \in D(S_n)$, it will be called an e-antiset. If $S_n = \biguplus_{j \in J} C_j$ is a decomposition of the symmetric group into e-antisets, $\beta_n(e) \leq |J|$ holds true. Frankl/Deza [22] proved in 1977 a fundamental statement using antisets:

Theorem 2 (Set-Antiset Bound) *Let $C, C' \subseteq S_n$ with $D(C) \cap D(C') \subseteq \{0\}$. Then*

$$|C| \cdot |C'| \leq n!. \tag{2}$$

If C is an e-antiset then

$$\beta_n(e) \leq \frac{n!}{|C|}.$$

Proof: Let $\pi, \sigma \in C$ and $\pi', \sigma' \in C'$ with $\pi \circ \pi' = \sigma \circ \sigma'$. Then $d_H(\pi, \sigma) = d_H(\pi \circ \pi', \sigma \circ \pi') = d_H(\sigma \circ \sigma', \sigma \circ \pi') = d_H(\sigma', \pi') \in D(C) \cap D(C')$. Hence, $\pi = \sigma$ and $\pi' = \sigma'$. Consequently, $|C| \cdot |C'| = |C \circ C'| \leq |S_n| = n!$. □

In [13], inequality (2) is called the duality bound. In coding theory [1], an analogous theorem is called the code-anticode bound. It refers to the theory of association schemes due to Delsarte [16].

Theorem 2 motivates the search for large e-antisets in S_n, started in [19] and [22]. The following construction was presented in general by the present author [31] in 2003, while special cases were already given by Frankl/Deza [22] in 1977.

Put

$$I_k(\pi, \sigma) := \{x \in \{1, 2, ..., k\} : \pi(x) \neq \sigma(x)\}$$

for $k \in \{0, 1, ..., n\}$ and $\pi, \sigma \in S_n$. The number of permutations in S_n differing from a given permutation $\sigma \in S_n$ in all of the first k components does not depend on σ. Hence, put

$$F_k(n) := |\{\pi \in S_n : \{1, 2, ..., k\} = I_k(\pi, \sigma)\}| = \sum_{x=0}^{k} (-1)^x \binom{k}{x} (n-x)!$$

for $k \in \{0, 1, ..., n\}$ and an arbitrary $\sigma \in S_n$.

Theorem 3 *If $e \in D(S_n)$ and $j \in \left\{0, 1, ..., \left\lfloor \frac{e}{2} \right\rfloor\right\}$ as well as $\sigma \in S_n$ then*

$$C_e^{(j)}(\sigma) := \{\pi \in S_n : j \geq |I_{n-e+2j}(\pi, \sigma)|\} \supseteq B_j(\sigma)$$

is an e-antiset with

$$\left| C_e^{(j)}(\sigma) \right| = \sum_{k=0}^{j} \binom{n-e+2j}{k} \cdot F_k(e - 2j + k) \geq V_j.$$

If e is even then $C_e^{(\frac{e}{2})}(\sigma) = B_{\frac{e}{2}}(\sigma)$ and, hence, $\left| C_e^{(\frac{e}{2})}(\sigma) \right| = V_{\frac{e}{2}}$. Otherwise

$$C_e^{(\frac{e-1}{2})}(\sigma) = B_{\frac{e-1}{2}}(\sigma) \uplus \left\{ \pi \in S_n : \frac{e-1}{2} = |I_{n-1}(\pi, \sigma)| \text{ and } \pi(n) \neq \sigma(n) \right\}$$

and, hence,

$$\left|C_e^{(\frac{e-1}{2})}(\sigma)\right| \;=\; V_{\frac{e-1}{2}} + \binom{n-1}{\frac{e-1}{2}} \cdot F_{\frac{e+1}{2}}\left(\frac{e+1}{2}\right).$$

The use of $C_e^{(0)}(\pi)$ proves the analog of the (Joshi-)Singleton bound

$$\beta_n(e) \leq \frac{n!}{e!}. \tag{3}$$

Additionally to (3),

$$i_n(e) \neq \frac{n!}{e!} - 1 \neq \beta_n(e)$$

was proved in [30, p. 116, p. 102]. Using Hall's condition, $i_n(n-1) \geq n$ can easily be shown. A combination with (1) and (3) yields

$$i_n(n-1) = \beta_n(n-1) = n.$$

Furthermore, the sphere packing bound (or Hamming bound)

$$\beta_n(e) \leq \frac{n!}{V_{\lfloor \frac{e}{2} \rfloor}}, \tag{4}$$

which is given in the Hamming permutation space by Deza [19], turns out to be another corollary of Theorem 3. The simple direct proof of (4) uses the fact that $\biguplus_{\pi \in C} B_{\lfloor \frac{e}{2} \rfloor}(\pi) \subseteq S_n$ is a disjoint union if C is e-independent. In case of e even, the application of $C_e^{(\frac{e}{2})}(\sigma)$ gives exactly (4). Otherwise, the application of $C_e^{(\frac{e-1}{2})}(\sigma)$ is an improvement of (4). Frankl/Deza [22] already showed (3) and this improvement of (4). As an example beyond [22], one can find in [31] the application of $C_5^{(1)}(\sigma)$ for $n = 10$ with

$$\left|C_5^{(1)}(\sigma)\right| = 132 > \left|C_5^{(0)}(\sigma)\right| = 120 > \left|C_5^{(2)}(\sigma)\right| = 118.$$

Tarnanen [35] showed in 1999 that the theory of association schemes can be applied in order to find powerful upper bounds on $\beta_n(e)$ in particular cases if the character table of S_n is available. He tabulated results for $7 \leq n \leq 10$ and $3 \leq e \leq 6$, for example $\beta_7(3) \leq 543$ instead of 720 by Theorem 2 and 3.

A common generalization of an e-independent set and an e-antiset is the notion of an L-clique: For a given $L \subseteq D(S_n)$, a set $C \subseteq S_n$ is called an L-clique if $D(C) \subseteq L$. Two sophisticated bounds on L-cliques and, hence, also on $\beta_n(e)$ are mentioned in [13]: The density bound, due to Cohen/Deza [12], can be interpreted as a common generalization of inequality (2) and the first estimation of Theorem 1 (ii). The very general averaging bound is due to Gabidulin/Sidorenko [23].

Dual to (4), the sphere covering bound

$$\gamma_n(e) \geq \frac{n!}{V_e} \tag{5}$$

is also easy to prove since $\bigcup_{\pi\in C} B_e(\pi) = S_n$ if C is e-covering. The combination of (4) and (5) gives $\beta_n(2e) \le \gamma_n(e)$. Both sphere bounds can be slightly improved in certain cases by a proper decomposition of S_n: In [33], the method in general is discussed and $S_n = \biguplus_{k=1}^{n}\{\pi \in S_n : \pi(1) = k\}$ is applied. In [10], a special case is presented for $\gamma_5(2) \ge 12$. It leads to the application of $S_n = A_n \uplus (S_n \setminus A_n)$ with the alternating group A_n. Both decompositions prove for example

$$\beta_n(4) + \left\lceil \frac{\beta_n(4)}{n} \right\rceil \binom{n-1}{2} \le (n-1)!$$

and

$$\left\lfloor \frac{\beta_n(4)}{2} \right\rfloor + \left\lceil \frac{\beta_n(4)}{2} \right\rceil \binom{n}{2} \le \frac{n!}{2}$$

as well as

$$\gamma_n(2) + \left\lfloor \frac{\gamma_n(2)}{n} \right\rfloor \binom{n-1}{2} \ge (n-1)!$$

and

$$\left\lceil \frac{\gamma_n(2)}{2} \right\rceil + \left\lfloor \frac{\gamma_n(2)}{2} \right\rfloor \binom{n}{2} \ge \frac{n!}{2}.$$

Computer proofs of $i_5(3) \ge 7$ and $\beta_6(4) \le 18$ are mentioned in [10] and [21], respectively. This section is finished by giving some more lower bounds on $\gamma_n(e)$.

Theorem 4 *Let $n \ge 3$.*

(i) $\gamma_n(n-1) \ge \left\lfloor \frac{n}{2} \right\rfloor + 1$.

(ii) $\gamma_n(n-2) \ge \left\lfloor \frac{n}{2} \right\rfloor + 2$.

(iii) $\gamma_n(n-2) \ge 6$ *for $n \ge 5$.*

The three parts of this theorem are due to Kézdy/Snevily [26], Cameron/Wanless [10] and the present author [30, p. 117-119], respectively. The proof of each part uses Hall's condition. As an example, $\gamma_7(5) \ge 6$ is shown in the following.

Proof: Consider $C \subseteq S_7$ with $2 \le |C| \le 5$ and use $C(x) := \{\pi(x) : \pi \in C\}$. There are distinct y_3, y_4 and an x_1 as well as $\pi_1, \pi_2 \in C$ with $\pi_1(x_1) = y_3$ and $\pi_2(x_1) = y_4$. Put $x_2 := \pi_2^{-1}(y_3) \ne x_1$. Hence, $y_3, y_4 \in C(x_1)$ and $y_3 \in C(x_2)$. Hall's condition gives distinct $y_1 \notin C(x_1)$ and $y_2 \notin C(x_2)$. Furthermore, there are distinct x_3, x_4 with $y_3 \notin C(x_3)$ and $y_4 \notin C(x_4)$ as well as $x_4 \ne x_2$. Hence, $|\{x_1, x_2, x_3, x_4\}| = 4$. Put $C' := \{\sigma \in S_7 : \sigma(x_j) = y_j \text{ for } 1 \le j \le 4\}$. Then $|C'| = 6$ and for every $\pi \in C$ there is at most one $\sigma \in C'$ with $d_H(\pi, \sigma) \le 5$. This implies the existence of the desired $\sigma \in C'$ with $d_H(\pi, \sigma) > 5$ for all $\pi \in C$. $\square$

5 Constructive Bounds

In this section, upper bounds on $\gamma_n(e)$ and $i_n(e)$ as well as lower bounds on $\beta_n(e)$ are given which arise from explicit constructions or at least existence proofs of proper subsets of S_n. In these constructions, Latin squares are frequently used. Many details about them can be found for example in [4], [15], [17], [18].

A very general bound is given in [25] with a reference to [2]. Its application to the Hamming permutation space proves

$$\gamma_n(e) \le n! \frac{1 + \ln V_e}{V_e}$$

for $e > 0$. The analog of the Gilbert bound

$$\beta_n(e) \ge \frac{n!}{V_e} \tag{6}$$

is due to Deza [19]. Because of the material of the above sections, (6) does not need to be proved by a construction any more. It turns out to be a corollary of (1) and (5) which seems to be a new insight. Let $\pi \in S_e$, then $\{\pi \oplus \breve{\pi} \in S_n : \breve{\pi} \in S_{n-e}\}$ shows $\gamma_n(2e) \le (n-e)!$. (For the concatenation $\pi \oplus \breve{\pi}$ see the proof of Theorem 1.) In [30], it is proved that $i_n(2) \le \frac{n!}{2} - 2$ for $n \ge 4$.

If there is a Latin square of order n without a transversal then

$$\gamma_n(n-2) \le i_n(n-2) \le n. \tag{7}$$

In case of n even, the cyclic group gives such a Latin square and (7) is valid.

A construction [26] using a Latin square of order $\left\lfloor \frac{n}{2} \right\rfloor + 1$ shows

$$\gamma_n(n-1) \le \left\lfloor \frac{n}{2} \right\rfloor + 1$$

and, hence, equality follows from Theorem 4. Some constructions [10, Theorem 9] using Latin squares with certain subsquares prove

$$\gamma_{4k+1}(4k-1) \le 5k + 2$$

and

$$\gamma_n(n-2) \le n + 2 \left\lceil \frac{1}{2} \left\lceil \frac{n+1}{3} \right\rceil \right\rceil$$

for $n \ge 8$.

Every system of k mutually orthogonal Latin squares of order n implies $\beta_n(n-2) \ge kn$, see for example [30]. The construction of certain finite nets due to Bruck [9, Theorem 5] or mutually orthogonal Latin squares (see [18, p. 25]) gives

$$i_n(n-2) \le n(\hat{n} - 1) \le \beta_n(n-2)$$

with $\hat{n} := \min\{p_j^{m_j} : j \in J\}$ if $\prod_{j\in J} p_j^{m_j}$ is the prime factorization of n, also compare [30].

The alternating group A_n implies $\beta_n(2) \geq \frac{n!}{2}$ and the analog of the Singleton bound (3) gives equality. Other well-known subgroups of S_n, see for example [8], prove

$$\beta_n(n-2) \geq n(n-1)$$

and

$$\beta_{n+1}(n-2) \geq (n+1)n(n-1)$$

if n is a prime power as well as $\beta_{11}(7) \geq \frac{11!}{7!}$ and $\beta_{12}(7) \geq \frac{12!}{7!}$. Again, bound (3) gives equality in all cases.

Some constructions in particular cases show $\gamma_5(3) \leq 6$, $i_5(3) \leq 7$, $\beta_6(4) \geq 18$, $\gamma_7(5) \leq 8$, $\gamma_9(7) \leq 10$, $\beta_{10}(8) \geq 32$ with equality in the first three cases, see [10], [21, Section 3.3.].

6 Conjectures

Some closely connected conjectures have been made concerning transversals and partial transversals in Latin squares on the one hand, $i_n(n-2)$ and $\gamma_n(n-2)$ on the other hand:

(i) (Ryser, cf. [17, p. 32])
Every Latin square of odd order has a transversal.

(ii) (Brualdi, cf. [17, p. 103])
Every Latin square of order n has a partial transversal of size $n-1$.

(iii) (Quistorff [30, p. 125])
$i_n(n-2) \geq n$. If n is odd then $i_n(n-2) \geq n+1$.

(iv) (Kézdy/Snevily [26])
If n is even then $\gamma_n(n-2) = n$. If n is odd then $\gamma_n(n-2) \geq n+1$.

Clearly, (iv) is equivalent to

(iv)′ $\gamma_n(n-2) \geq n$. If n is odd then $\gamma_n(n-2) \geq n+1$.

since (7) is valid if n is even.

Theorem 5 (iv) $\Rightarrow$ (iii) $\Rightarrow$ (i),(ii).

Proof: (iv)$\Rightarrow$(iii) follows from (1) and (iii)$\Rightarrow$(i) from (7). In order to verify (iii)$\Rightarrow$(ii), observe that every given Latin square of order n induces an $(n-1)$-independent $C \subseteq S_{n+1}$ with $|C| = n$ and $\pi(n+1) = n+1 \,\forall \pi \in C$. Because of (iii), C is not $(n-1)$-covering, implying the existence of a $\sigma \in S_{n+1} \setminus \bigcup_{\pi\in C} B_{n-1}(\pi)$. Then there are at least $n-1$ positions x_j with $1 \leq x_j \leq n$ and $\sigma(x_j) \leq n$. This proves the existence of a partial transversal of size $n-1$ in the given Latin square. $\square$

7 Satisfying Bounds with Equality

Fascinating existence problems appear if one searches for sets which satisfy some of the destructive bounds with equality. Let $e \in D(S_n)$. Due to Ahlswede et al. [1], a subset $C \subseteq S_n$ is called e-diameter perfect if there is an e-antiset $C' \subseteq S_n$ with $|C| \cdot |C'| = n!$. This notion is a generalization of e-perfect sets, discussed below. Situations where bound (3) or (4) are satisfied with equality (without using integer roundings) are of a special interest.

An e-independent set $C \subseteq S_n$ of cardinality $\frac{n!}{e!}$ is called a sharply $(n-e)$-transitive set of permutations. It is e-diameter perfect and can also be characterized by the following property: Given distinct $x_1, x_2, ..., x_{n-e}$ and distinct $y_1, y_2, ..., y_{n-e}$, there is exactly one $\pi \in C$ with $\pi(x_j) = y_j$ for all $j \in \{1, 2, ..., n-e\}$. The existence problem is trivial if $e \in \{0, 2, n-1, n\}$. Sharply multiply transitive sets of permutations are surveyed in [8], [30]. A recent nonexistence result, using Theorem 2 and (implicitly) Theorem 3 is given in [32].

A set $C \subseteq S_n$ with the property that the balls of radius e around the elements of C are disjoint and exhaust the whole space, i.e. $\biguplus_{\pi \in C} B_e(\pi) = S_n$, is called an e-perfect set. C is e-perfect iff it is an e-covering set of cardinality $\frac{n!}{V_e}$. Hence, it is e-diameter perfect. Furthermore, every $(2e)$-independent set of cardinality $\frac{n!}{V_e}$ is e-perfect. The existence problem of e-perfect sets is trivial if $e = 0$. Clearly, a necessary condition is $\frac{n!}{V_e} \in \mathbf{N}$. The nonexistence of certain 2-perfect sets, including the case $n = 11$, was proved in [34] using another metric. No further results concerning this problem are known (to the author).

References

[1] Ahlswede, R. / Aydinian, H.K. / Khachatrian, L.H.: On Perfect Codes and Related Concepts, *Des. Codes Cryptogr.*, 22 (2001), 221-237.

[2] Alon, N.: Transversal Numbers of Uniform Hypergraphs, *Graphs Comb.*, 6 (1990), 1-4.

[3] Berlekamp, E.R.: *Algebraic Coding Theory*, McGraw-Hill, New York, 1968.

[4] Beth, T. / Jungnickel, D. / Lenz, H.: *Design Theory*, Second Edition, Cambridge University Press, Cambridge, 1999.

[5] Blake, I.F. / Cohen, D. / Deza, M.: Coding with Permutations, *Inform. Control*, 43 (1979), 1-19.

[6] Bogdanova, G.T. / Brouwer, A.E. / Kapralov, S.N. / Östergård, P.R.J.: Error-Correcting Codes over an Alphabet of Four Elements, *Des. Codes Cryptogr.*, 23 (2001), 333-342.

[7] Bogdanova, G.T. / Östergård, P.R.J.: Bounds on Codes over an Alphabet of Five Elements, *Discrete Math.*, 240 (2001), 13-19.

[8] Bonisoli, A. / Quattrocchi, P.: Existence and Extension of Sharply k-Transitive Permutation Sets: A Survey and some New Results, *Ars Comb.*, 24A (1987), 163-173.

[9] Bruck, R.H.: Finite Nets, I. Numerical Invariants, *Can. J. Math.*, 3 (1951), 94-107.

[10] Cameron, P.J. / Wanless, I.M.: Covering Radius for Sets of Permutations, *Discrete Math.*, 293 (2005), 91-109.

[11] Cockayne, E.J. / Hedetniemi, S.T. / Miller, D.J.: Properties of Hereditary Hypergraphs and Middle Graphs, *Cand. Math. Bull.*, 21 (1978), 461-468.

[12] Cohen, G. / Deza, M.: Distances invariantes et L-cliques sur certains demi-groupes finis, *Math. Sci. Hum.*, 67 (1979), 49-69.

[13] Cohen, G. / Deza, M.: Some Metrical Problems on S_n, *Annals of Discrete Math.*, 8 (1980), 211-216.

[14] Cohen, G. / Honkala, I. / Litsyn, S. / Lobstein, A.: *Covering Codes*, North-Holland, Amsterdam, 1997.

[15] Colbourn, C.J. / Dinitz, J.H. (eds.): *The CRC Handbook of Combinatorial Designs*, CRC Press, Boca Raton, New York, London, Tokyo, 1996.

[16] Delsarte, P.: An Algebraic Approach to the Association Schemes of Coding Theory, *Phillips Res. Rep. Suppl.*, 10 (1973).

[17] Dénes, J. / Keedwell, A.D.: *Latin Squares and their Applications*, Akadémiai Kiadó, Budapest, 1974.

[18] Dénes, J. / Keedwell, A.D.: Latin Squares - New Developments in the Theory and Applications, *Annals of Discrete Math.*, 46 (1991).

[19] Deza, M.: Matrices Dont Deux Lignes Quelconque Coïncident dans un Nombre Donne de Positions Communes, *J. Comb. Th., Ser. A*, 20 (1976), 306-318.

[20] Deza, M. / Huang, T.: Metrics on Permutations, a Survey, *J. Comb. Inf. Sys. Sci.*, 23 (1998), 173-185.

[21] Deza, M. / Vanstone, S.: Bounds for Permutation Arrays, *J. Stat. Plann. Inference*, 2 (1978), 197-209.

[22] Frankl, P. / Deza, M.: On the Maximum Number of Permutations with Given Maximal or Minimal Distance, *J. Comb. Th., Ser. A*, 22 (1977), 352-360.

[23] Gabidulin, É.M. / Sidorenko, V.R.: One General Bound for Code Volume, *Probl. Pered. Inform.*, 12 (1976), 31-35. *Probl. Inform. Transm.*, 12 (1976), 266-269.

[24] Haynes, T.W. / Hedetniemi, S.T. / Slater, P.J.: *Fundamentals of Domination in Graphs*, Marcel Dekker, New York, 1998.

[25] Jukna, S.: *Extremal Combinatorics*, Springer, Berlin, Heidelberg, New York, 2001.

[26] Kézdy, A.E. / Snevily, H.S.: Private communication and unpublished material cited in [10].

[27] van Lint, J.H.: *Introduction to Coding Theory*, Third Edition, Springer, Berlin, Heidelberg, New York, 1999.

[28] MacWilliams, F.J. / Sloane, N.J.A.: *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, New York, Oxford, 1977.

[29] Östergård, P.R.J. / Quistorff, J. / Wassermann, A.: New Results on Codes with Covering Radius 1 and Minimum Distance 2, *Des. Codes Cryptogr.*, 35 (2005), 241-250.

[30] Quistorff, J.: *Simultane Untersuchung mehrfach scharf transitiver Permutationsmengen und MDS-Codes unter Einbeziehung ihrer Substitute*, Habilitationsschrift, Univ. Hamburg, 1999. Shaker Verlag, Aachen, 2000.

[31] Quistorff, J.: Extremale Mengen in endlichen metrischen Räumen - ein grundlegender Überblick, *Hamb. Beitr. Math.*, 180 (2003).

[32] Quistorff, J.: A New Nonexistence Result for Sharply Multiply Transitive Permutation Sets, *Discrete Math.* 288 (2004), 185-186.

[33] Quistorff, J.: Improved Sphere Bounds in Finite Metric Spaces, *Bull. Inst. Combin. Appl.*, 46 (2006), 69-80.

[34] Rothaus, O. / Thompson, J.G.: A Combinatorial Problem in the Symmetric Group, *Pac. J. Math.*, 18 (1966), 175-178.

[35] Tarnanen, H.: Upper Bounds on Permutation Codes via Linear Programming, *Europ. J. Comb.*, 20 (1999), 101-114.

[36] Vaessens, R.J.M. / Aarts, E.H.L. / van Lint, J.H.: Genetic Algorithms in Coding Theory - a Table for $A_3(n,d)$, *Discrete Appl. Math.*, 45 (1993), 71-87.