A bound on permutation codes

Jürgen Bierbrauer
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931, USA
jbierbra@mtu.edu

Klaus Metsch
Universität Gießen
Mathematisches Institut
Arndtstr. 2, D-35392 Gießen, Germany
klaus.metsch@math.uni-giessen.de

Submitted: Nov 28, 2012; Accepted: July 18, 2013; Published: July 26, 2013
Mathematics Subject Classifications: 05A05, 05B40, 51E26, 94B60

Abstract

Consider the symmetric group S_n with the Hamming metric. A **permutation code** on n symbols is a subset $C \subseteq S_n$. If C has minimum distance $\geqslant n-1$, then $|C| \leqslant n^2 - n$. Equality can be reached if and only if a projective plane of order n exists. Call C **embeddable** if it is contained in a permutation code of minimum distance $n-1$ and cardinality n^2-n. Let $\delta = \delta(C) = n^2 - n - |C|$ be the **deficiency** of the permutation code $C \subseteq S_n$ of minimum distance $\geqslant n-1$.

We prove that C is embeddable if either $\delta \leqslant 2$ or if $(\delta^2-1)(\delta+1)^2 < 27(n+2)/16$. The main part of the proof is an adaptation of the method used to obtain the famous Bruck completion theorem for mutually orthogonal latin squares.

1 Introduction

Definition 1. Consider the symmetric group S_n equipped with the Hamming distance. A **permutation code** is a subset $C \subseteq S_n$ and the **minimum distance** $d = d(C)$ is the minimum distance between two members of C.

Permutation codes are also known as permutation arrays and as permutation sets. There is a vast literature on the subject. Motivation comes from data transmission over power lines, see [7, 15, 6, 5], and the design of block ciphers [14]. A related and in some sense dual notion are uniformly t-homogeneous sets of permutations where the defining property is that there is a constant $\mu > 0$ such that for any two not necessarily different unordered t-subsets A and B of letters the number of permutations $\pi \in C$ mapping $\pi : A \mapsto B$ equals μ. Those sets have been studied in the framework of perpendicular arrays, see for example [1, 2, 11].

Clearly a permutation code $C \subseteq S_n$ of distance n has at most n codewords, with equality if and only if C is a Latin square of order n. The case of minimum distance $n-1$ leads to the following notion:

Definition 2. A permutation code $C \subseteq S_n$ is **sharply 2-transitive** if for any two pairs $(a,b),(c,d)$ of symbols such that $a \neq b, c \neq d$ there is precisely one $\pi \in C$ such that $\pi(a) = b$ and $\pi(c) = d$.

Proposition 3. *A permutation code $C \subseteq S_n$ of minimum distance $\geqslant n-1$ has size at most $n(n-1)$, with equality if and only if C is sharply 2-transitive. A 2-transitive set of permutations on n letters exists if and only if a projective plane of order n exists. This is the case if n is a prime-power.*

Proof. Most of the claims are well-known and easy to see. For the sake of completeness we sketch the proof of equivalence between projective planes and sharply 2-transitive permutation sets. Given a projective plane of order n, choose a point ∞ and two lines l_1, l_2 on ∞. Label the points $\neq \infty$ on l_1, l_2 as $P_1, \ldots, P_n$ and $Q_1, \ldots, Q_n$, respectively. To each point $R \notin l_1 \cup l_2$ associate a permutation π_R such that $\pi_R(i) = j$ if R, P_i, Q_j are collinear. The axioms of a projective plane show that this defines a sharply 2-transitive set of permutations. This proves one of the claims.

Let C be a permutation code of distance $\geqslant n-1$. Associate to C a geometry $\Pi(C)$ with $1+2n+|C|$ points and n^2+2 lines where $l_1 = \{\infty, P_1, \ldots, P_n\}$ and $l_2 = \{\infty, Q_1, \ldots, Q_n\}$ are two of the lines, each $\pi \in C$ defines a point and for each pair (i,j) where $1 \leqslant i, j \leqslant n$ the line L_{ij} contains P_i, Q_j and those $\pi \in C$ which map $\pi : i \mapsto j$. If C is sharply 2-transitive, then $\Pi(C)$ has n^2+n+1 points and n^2+2 lines and it is easy to see that it can be completed to a projective plane of order n. □

In the sequel we will restrict attention to permutation codes $C \subset S_n$ of minimum distance $\geqslant n-1$.

Definition 4. A permutation code $C \subseteq S_n$ of minimum distance $\geqslant n-1$ is **embeddable** if it is contained in a sharply 2-transitive set. Let M_n be the largest size of a permutation code $C \subseteq S_n$ of distance $\geqslant n-1$, and m_n the largest size of a non-embeddable such code.

Observe that $M_q = q^2 - q$ if q is a prime-power, and $M_n = m_n < n^2 - n$ provided n is not the order of a projective plane. In those cases m_n can be seen as a measure for the best possible approximation to the non-existing plane. The values of m_n are known only for $n \leqslant 6$.

Result 5. $m_4 = 7, m_5 = 15, m_6 = 18$.

In fact in cases $n = 2$ and $n = 3$ the symmetric group is sharply 2-transitive itself, so m_n is not defined in those cases. For $n = 4$ it is easy to see that $m_4 = 7$. One such maximal non-embeddable code consists of the identity permutation and the elements of order 4. The value of m_5 is found in Bogaerts [3], the determination of m_6 is due to Kløve [9, 10].

Assume a set of t mutually orthogonal Latin squares of order n exists. The representation as a dual net shows immediately that this allows the construction of a permutation code $C \subseteq S_n$ of minimum distance $\geqslant n-1$ and size tn. This generalizes a statement from Proposition 3 which corresponds to case $t = n-1$. In particular the existence of 5 mutually orthogonal Latin squares of order 12 shows $M_{12} \geqslant 60$. It is a recent result by I. Janiszczak and R. Staszewski (personal communication) that $M_{12} \geqslant 112$.

Our main results are the following:

Theorem 6. *Let $C \subseteq S_n$ be a permutation code of minimum distance $\geqslant n-1$, where $|C| = n^2 - n - \delta$.*

- *If $\delta \leqslant 2$, then C is embeddable.*
- *If $(\delta^2-1)(\delta+1)^2 < 27(n+2)/16$, then C is embeddable.*

The embeddability of a permutation code of size n^2-n-1 (case $\delta = 1$ of Theorem 6) had been shown by Quistorff [13]. Of particular interest is case $n = 10$, the smallest integer $n > 6$ for which no projective plane of order n exists. The lower bound $M_{10} \geqslant 49$ has been shown in [8]. Theorem 6 shows $M_{10} \leqslant 87$.

Our proof is an adaptation of the celebrated Bruck embedding theorem for mutually orthogonal Latin squares, see [4, 12]. In Section 2 we define a geometric representation of permutation sets. Some basic properties are proved in Section 3. The last two sections contain the proofs of the embeddability theorems.

2 A geometric setting

Definition 7. A **permutation incidence structure** of order n consists of points and lines such that

- There are n^2 points.
- Each line has precisely n points.
- Each point is on at least 2 lines.
- Two different lines meet in at most one point.

Definition 8. Let the total number of lines of a permutation incidence structure be $n^2+n-\delta$. Then δ is the **deficiency** and we write $P(n, \delta)$.

Observe that as a consequence of the last axiom, each point of a $P(n, \delta)$ is on at most $n+1$ lines. Permutation incidence structures are essentially geometric representations of permutation codes $C \subseteq S_n$. This geometry is obtained by dualizing the geometry $\Pi(C)$ used in the proof of Proposition 3. More precisely the following holds:

Proposition 9. *The following are equivalent:*

A permutation code $C \subseteq S_n$ of minimum distance$\geqslant n-1$, where $|C| = n(n-1) - \delta$.

A $P(n, \delta)$ which possesses two parallel classes of lines each of which partitions the points.

Proof. Let C be a permutation code of distance $\geqslant n-1$ and size $n(n-1)-\delta$. The corresponding $P(n,\delta)$ is obtained from $\Pi(C)$ by omitting the point ∞ and dualization: the points of the $P(n,\delta)$ are the lines L_{ij}, the lines of the $P(n,\delta)$ are the permutations and the $2n$ points P_i, Q_j on the lines l_1, l_2.

Conversely let a $P(n,\delta)$ be given. The dual structure has n^2 lines. Each point is on n lines, each line has at least 2 points and two different points are on at most one line. The additional property shows that this dual structure possesses two sets $\{P_1,\ldots,P_n\}$ and $\{Q_1,\ldots,Q_n\}$ of points with the property that each line contains exactly one of the P_i and one of the Q_j. It follows that the lines are precisely the lines L_{ij} through P_i and Q_j. Let X be one of the $n^2-n-\delta$ remaining points. Then X determines a permutation on n objects in the obvious way (the permutation maps $i\mapsto j$ if and only if $X\in L_{ij}$), The resulting permutation code C has $n^2-n-\delta$ elements and minimum distance $\geqslant n-1$. □

To sum up: each permutation code C of minimum distance $\geqslant n-1$ and size $n^2-n-\delta$ defines a $P(n,\delta)$. On the other hand it is obvious that a $P(n,\delta)$ results if we remove some δ lines from an affine plane of order n. We want to prove that for small values of δ each $P(n,\delta)$ is embeddable in an affine plane. We are going to prove this if either $\delta\leqslant 2$ (Corollary 15 and Theorem 23) or $(\delta^2-1)(\delta+1)^2 < 27(n+2)/16$ (Theorem 26). This will complete the proof of Theorem 6.

3 Basic properties of permutation incidence structures

In the sequel let $(\mathcal{P},\mathcal{L})$ be a $P(n,\delta)$.

Definition 10. Let r_P (the **degree** of P) be the number of lines on the point P and $\delta_P = n+1-r_P\geqslant 0$ the **deficiency** of P. For a line l define $\delta_l=\sum_{P\in l}\delta_P$, the **deficiency** of l. A point P is **exceptional** if $\delta_P>0$. Let E be the set of exceptional points. Lines l, g are **parallel** if either $l=g$ or $l\cap g=\emptyset$. Let $i(l_1,l_2,\ldots)$ be the number of lines which are parallel to $l_1,l_2,\ldots$ and different from $l_1,l_2,\ldots$.

Lemma 11. *Let P be a point and l a line. The following hold:*

- *We have $r_P\leqslant n+1$ with equality if and only if P is joined to all remaining points.*
- *If $P\notin l$ and P non-exceptional, then P is on precisely one line which is parallel to l.*
- *$\delta_l\geqslant 0$ with equality if and only if each $P\in l$ is non-exceptional.*
- *$i(l)=n-\delta-1+\delta_l$ for each line l.*

Proof. The first statement is obvious (as $1+(n+1)(n-1)=n^2$). For the second statement observe that by the first P is on precisely n lines that are not parallel to l. It follows that precisely one line through P must be parallel to l. The third claim follows from the first.

As for the last claim, it is easier to count the lines which are not parallel to l. This number is $1+\sum_{P\in l}(r_P-1)=1+\sum_{P\in l}(n-\delta_P)=1+n^2-\delta_l$. Subtracting this from the total number $n^2+n-\delta$ of lines yields the result. □

Lemma 12. *We have $|E|\leqslant\sum_{P\in\mathcal{P}}\delta_P=\delta n$, with equality on the left if and only if all points have deficiency $\leqslant 1$.*

Proof. Double counting of point-line incidences shows

$$n(n^2+n-\delta)=n|\mathcal{L}|=\sum_{P\in\mathcal{P}}r_P=\sum_{P\in\mathcal{P}}(n+1-\delta_P)=n^2(n+1)-\sum_{P\in\mathcal{P}}\delta_P.$$

The equality follows by comparison, the inequality is an obvious consequence. □

In particular $\delta\geqslant 0$ and $P(n,0)$ is an affine plane. We can assume $\delta>0$ in the sequel. Here is a refinement of the preceding lemma:

Lemma 13. *For each line l the following hold:*

- *$|E\cap l|\leqslant\delta_l$, with equality if all points on l have deficiency $\leqslant 1$.*
- *$|E\setminus l|\leqslant\sum_{Q\in E\setminus l}\delta_Q=\delta n-\delta_l$ with equality if all points off l have deficiency $\leqslant 1$.*

Proof. Let $e_l=|E\cap l|$. The number of lines meeting l in a point equals $\sum_{P\in l}(n-\delta_P)=n^2-\delta_l$. On the other hand this number is $\leqslant(n-e_l)n+e_l(n-1)=n^2-e_l$. It follows $e_l\leqslant\delta_l$ with equality if every exceptional point of l has deficiency one. The remaining statements are implied by Lemma 12. □

Lemma 14. *We have $\delta_P\leqslant\delta$ for all P. Equality holds if and only if all points collinear with P are non-exceptional and all remaining points except P have deficiency 1.*

Proof. Let P be an exceptional point. It is not collinear with $\delta_P(n-1)$ points and those points are exceptional. Let l be a line on P. By Lemma 13 we have

$$\delta_P(n-1)\leqslant|E\setminus l|\leqslant\delta n-\delta_l\leqslant\delta n-\delta_P.$$

Comparison shows $\delta_P\leqslant\delta$. Equality holds if and only if all three inequalities above are met with equality. □

Corollary 15. *Each $P(n,1)$ can be embedded in an affine plane.*

Proof. There is an exceptional point P. By Lemma 14 there are precisely $1+n-1=n$ exceptional points and those are pairwise not collinear. Their union can be used as an additional line which completes the $P(n,1)$ to an affine plane. □

In the sequel we may assume $\delta\geqslant 2$.

Lemma 16. *Let lines l,h meet in an exceptional point. Then $i(l,h)\leqslant\delta_l+\delta_h-(1+\delta)$.*

Proof. We know $i(l)$. As h contains at least $n - \delta_h$ non-exceptional points and each of those is on a line parallel to l, the number in question is bounded by the difference $i(l) - (n - \delta_h) = \delta_l + \delta_h - 1 - \delta$. □

Lemma 17. *Let lines $l \neq h$ be parallel, $\delta_l, \delta_h > 0$. Then $i(l,h) \geqslant n-1-\delta-(\delta_l-1)(\delta_h-1)$.*

Proof. Start from the $i(l)$ lines parallel to l and different from l. How many of those intersect h? Each of the $\geqslant n - \delta_h$ non-exceptional points on h contributes only h itself, and each of the $\leqslant \delta_h$ exceptional points, being collinear with the non-exceptional points on l, contributes at most δ_l such lines one of which is h. It follows that the number in question is $\geqslant i(l) - 1 - \delta_h(\delta_l - 1)$. □

Lemma 18. *If h and h' meet, are both parallel to l and $\delta_l, \delta_h, \delta_{h'} > 0$, then $n + 1 \leqslant \delta_l(\delta_h + \delta_{h'} - 1)$.*

Proof. $h \cap h'$ is an exceptional point as it is on two lines parallel to l. We have

$$i(l) \geqslant 2 + i(l,h) + i(l,h') - i(l,h,h').$$

We know $i(l)$, have lower bounds on $i(l,h), i(l,h')$ and an upper bound on $i(l,h,h') \leqslant i(h,h') - 1$. Comparing the extremes of these inequalities yields the claim. □

Definition 19. For each line l, let $\Pi(l)$ the set of lines parallel to l.

We know from Lemma 11 that $\Pi(l)$ is a family of $n + \delta_l - \delta$ lines.

Lemma 20. *Suppose l is a line with at least $n - 1$ non-exceptional points. Then $\Pi(l)$ consists of mutually parallel lines, and $\delta_g \geqslant \delta_l$ for all $g \in \Pi(l)$.*

Proof. Let $l \neq g \in \Pi(l)$. We know that each non-exceptional point of g is on precisely one line which is parallel to l. The presence of $n - 1$ non-exceptional points on l shows that the same is true for each exceptional point of g. It follows that the lines in $\Pi(l)$ are mutually parallel and therefore $\Pi(l) \subseteq \Pi(g)$. This implies $\delta_l \leqslant \delta_g$. □

4 Special cases

Proposition 21. *Each $P(n, \delta)$ containing a line of deficiency 0 and such that $n \geqslant \delta(2\delta - 1)$ is embeddable.*

Proof. Let $\delta_l = 0$. Then $|\Pi(l)| = n - \delta$. Each point covered by a line from $\Pi(l)$ is on $n + 1$ lines and therefore non-exceptional. It follows that those points are precisely the non-exceptional points. Each point outside is exceptional. Lemma 12 implies that the points not covered by $\Pi(l)$ form the set E of exceptional points, each of deficiency $\delta_Q = 1$. This implies that every line $l' \in \Pi(l)$ satisfies $\delta_{l'} = 0$ and hence $\Pi(l') = \Pi(l)$. Let $g \notin \Pi(l)$. Then g has precisely $n - \delta$ non-exceptional points, and therefore $\delta_g = \delta$. Hence, every line has deficiency 0 or δ.

Let $Q \in E$ and $U \subset E$ the n-set consisting of Q and all points not collinear with Q. Assume some two points of U are collinear on a line h. Then Q is on some two different lines both of which are parallel to h. As all lines involved have deficiency δ, then Lemma 18 yields a contradiction. This shows that U can be added to the list of lines resulting in a $P(n, \delta - 1)$ which still contains a line of deficiency 0. We are done by induction. □

Proposition 22. *If $\delta > 0$ and $n \geqslant (\delta - 1)(2\delta - 3)$, then each $P(n, \delta)$ containing a point of deficiency δ is embeddable.*

Proof. Let $\delta_{P_0} = \delta$. We are in the situation of Lemma 14 when equality holds. The bundle of lines $l_1, \ldots, l_{n+1-\delta}$ on P_0 covers P_0 and the $(n + 1 - \delta)(n - 1)$ non-exceptional points. The complement is the set N of $\delta(n - 1)$ points of deficiency 1. We have $E = \{P_0\} \cup N$.

As $|\Pi(l_i)| = n$ it follows from Lemma 20 that the lines of $\Pi(l_i)$ partition the point set into n lines. As each $g \in \Pi(l_i)$ satisfies $\delta_g \geqslant \delta$ (Lemma 20) and $\sum_{g \in \Pi(l_i)} \delta_g = \sum_{P \in \mathcal{P}} \delta_P = \delta n$ it follows that $\delta_g = \delta$ and therefore $\Pi(g) = \Pi(l_i)$. Each of the remaining lines meets each of the l_i, each line parallel to l_i and has deficiency $\delta - 1$.

Let $X \in N$ and U the set consisting of X and the points not collinear with X. Clearly $P_0 \in U$. As $\delta_X = 1$ we have $|U| = n$. Assume a line h contains two points from U. As X has degree n, it is on at least two lines parallel to h. The first part of the proof shows that h and the two lines on X parallel to h have deficiency $\delta - 1$. Lemma 18 yields a contradiction. It follows that U can be added as a line to produce a $P(n, \delta - 1)$, in which P_0 is a point of deficiency $\delta - 1$. We are done by induction. □

Theorem 23. *Each $P(n, 2)$ is embeddable.*

Proof. For $n \leqslant 6$ this is known. Assume therefore $n > 6$. Because of Proposition 21 and Proposition 22 it can be assumed that all lines have positive deficiency (equivalently: contain at least one exceptional point) and $\delta_P \leqslant 1$ for all P. The latter implies $|E| = \sum_{P \in \mathcal{P}} \delta_P = 2n$. As the removal of two lines from an affine plane of order n produces a $P(n, 2)$ which either has a line of deficiency 0 or has a point of deficiency 2, we expect a contradiction.

Considering the distribution of the $2n$ exceptional points on the bundle of lines on a non-exceptional point P, we see that P is on a line l of deficiency 1. We have $|\Pi(l)| = n-1$. Lemma 20 shows that the lines of $\Pi(l)$ are parallel. They cover $n(n - 1)$ points. As the n exceptional points covered by $\Pi(l)$ distribute on the $n - 1$ lines of this partial parallel class, there is precisely one line $g \in \Pi(l)$ of deficiency 2. We have $\Pi(l') = \Pi(l)$ for each line l' parallel to l which is different from g. As $|\Pi(g)| = n$, it follows that there is precisely one line h parallel to g which is not in $\Pi(l)$. Let $l' \in \Pi(l), l' \neq g, l$. Then h meets l' and $Q = h \cap l'$ is exceptional as Q is on two different parallels to g. It follows that Q is the unique exceptional point on l'. Similarly $h \cap l$ is the unique exceptional point of l. This is impossible as it implies that Q is on $n + 1$ lines, namely the line h and l' and the $n - 1$ lines that join Q to the non-exceptional points of l. □

5 Continuing with the general case

In this final section we complete the proof of Theorem 6. It follows from Theorem 23 and Propositions 21,22 that the following assumptions can be made: $\delta \geqslant 3, \delta_l > 0$ for each line l and $\delta_P < \delta$ for each point P. We start from the following:

Theorem 24. *Assume l is a line such that $\delta_l \leqslant \delta$ and $(\delta^2-1)(\delta+1)^2 < 27(n+2)/16$. Then the following hold:*

- *The lines of $\Pi(l)$ are pairwise parallel. They all have the same deficiency $\epsilon = \delta_l$ and $\Pi(l) = \Pi(h)$ for all $h \in \Pi(l)$.*

Proof. Observe $|\Pi(l)| = n - (\delta - \epsilon) \leqslant n$. Use induction on $\epsilon = \delta_l \geqslant 0$. Case $\epsilon = 0$ follows from Proposition 21 and its proof. Assume $\epsilon > 0$ in the sequel. Consider the partition $\Pi(l) = \Pi_1 \cup \Pi_2$ where Π_1 consists of l and the lines $h \neq l$ parallel to l which satisfy $\delta_h < (n+1+\epsilon)/(2\epsilon)$. Lemma 18 implies that the lines of Π_1 are pairwise parallel. The induction hypothesis implies $\delta_h \geqslant \delta_l$ for all $h \in \Pi_1$. The next major claim is that Π_2 is empty.

In order to prove this, let M be the set of points covered by lines of $\Pi(l)$ and N the complement of M. Then $|N| \geqslant n(\delta - \epsilon)$ and Lemma 11 shows that N consists of exceptional points. Let $D \subset M$ be the set of points which are on more than one line of $\Pi(l)$. Clearly points of D are exceptional. For $X \in D$, let $d_X \geqslant 2$ be the number of lines of $\Pi(l)$ on X, and $d = \sum_{h\in\Pi_2} |h \cap D|$. We have

$$n|\Pi(l)| - |M| = \sum_{X\in D}(d_X - 1) \geqslant \frac{1}{2}\sum_{X\in D} d_X = \frac{1}{2}\sum_{h\in\Pi}|h\cap D| \geqslant d/2 \tag{1}$$

and

$$\begin{aligned} \sum_{h\in\Pi_2}\sum_{P\in h\setminus D}\delta_P &= \sum_{h\in\Pi_2}(\delta_h - \sum_{P\in h\cap D}\delta_P) \\ &\geqslant \sum_{h\in\Pi_2}(\delta_h - |h\cap D|(\delta-1)) \\ &\geqslant |\Pi_2|(n+1+\epsilon)/(2\epsilon) - d(\delta-1). \end{aligned} \tag{2}$$

We want to lower bound $\sum_{X\in\mathcal{P}}\delta_X$. As points of N are exceptional and therefore have deficiency $\geqslant 1$ and because of Equation (1) we have

$$\sum_{X\in N}\delta_X \geqslant n^2 - |M| \geqslant (n(n-|\Pi|) + d/2 = n(\delta-\epsilon) + d/2.$$

Together with the points covered by Π_1 this yields the a priori lower bound

$$\delta n = \sum_{X\in\mathcal{P}}\delta_X \geqslant |\Pi_1|\epsilon + n(\delta-\epsilon) + d/2.$$

which we use to obtain a weak upper bound on d :

$$d/2 \leqslant \epsilon(n - |\Pi_1|) = \epsilon(\delta - \epsilon + |\Pi_2|) \tag{3}$$

Collect now the three contributions to $\sum \delta_X$ that we have to obtain a lower bound:

$$\delta n = \sum_{X \in \mathcal{P}} \delta_X \geqslant \epsilon|\Pi_1| + \underbrace{(n(\delta - \epsilon) + d/2)}_{contribution\ of\ N} + \underbrace{|\Pi_2|(n + 1 + \epsilon)/(2\epsilon) - d(\delta - 1)}_{from\ (2)}.$$

Equivalently

$$\delta n \geqslant |\Pi_2|((n + 1 + \epsilon)/(2\epsilon) - \epsilon) + \epsilon(n - \delta + \epsilon) + n(\delta - \epsilon) - (d/2)(2\delta - 3).$$

Substitute inequality (3) for $d/2$. After simplification this yields

$$\delta n \geqslant |\Pi_2|((n + 1 + \epsilon)/(2\epsilon) - 2\epsilon(\delta - 1)) + \delta n - 2\epsilon(\delta - 1)(\delta - \epsilon).$$

Because of the hypothesis in Theorem 24 the coefficient of $|\Pi_2|$ is positive. Assume $|\Pi_2| \geqslant 1$. Then

$$n + 1 + \epsilon \leqslant 4(\delta - 1)\epsilon^2(\delta - \epsilon + 1).$$

The left is $\geqslant n + 2$, the right side is maximized by $\epsilon = 2(\delta + 1)/3$ as a function of ϵ. This yields $n + 2 \leqslant (16/27)(\delta^2 - 1)(\delta + 1)^2$ contradicting the hypothesis.

Now $\Pi = \Pi_1$ consists of $n - \delta + \epsilon$ parallel lines, each of deficiency $\geqslant \epsilon$.

Finally we prove that $\Pi(l) = \Pi(h)$ for all $h \in \Pi(l)$, equivalently: each line in $\Pi(l)$ has deficiency ϵ. The situation is: $\Pi(l)$ has $n - \delta + \epsilon$ lines. They are pairwise parallel, have deficiency $\geqslant \epsilon$. Since the $n(\delta - \epsilon)$ points not covered by the lines of $\Pi(l)$ have positive deficiency, then global counting shows

$$\delta n = \sum_{P \in \mathcal{P}} \delta_P \geqslant \epsilon(n - \delta + \epsilon) + n(\delta - \epsilon)$$

which shows that at most $z = \epsilon(\delta - \epsilon) \leqslant \delta^2/4$ lines of $\Pi(l)$ have deficiency $> \epsilon$. Clearly $\Pi(l) = \Pi(h)$ for all $h \in \Pi(l)$ of deficiency ϵ.

Assume there is some $g \in \Pi(l)$ of deficiency $> \epsilon$. Then g is parallel to some line h which is not in $\Pi(l)$. Let $l = l_1, \ldots, l_c$ be the lines of $\Pi(l)$ of deficiency ϵ. We saw above that

$$c \geqslant |\Pi| - z = n - (\delta - \epsilon)(\epsilon + 1) \geqslant n - (\delta + 1)^2/4.$$

Then h meets each of the l_j.

Each point of h is exceptional. Indeed, if point X of h lies on no line of $\Pi(l)$ it is exceptional for this reason, and if X is on a line of $\Pi(l)$, then it lies on two parallels to g and is therefore exceptional.

It follows in particular $\delta_h \geqslant n$. Line h is parallel to $n - 1 - \delta + \delta_h \geqslant 2n - 1 - \delta$ other lines. At most z of those are in $\Pi(l)$. Let $s = 2n - 1 - \delta - z \geqslant 2n - (\delta + 2)^2/4$ and $h_1, \ldots, h_s$ lines parallel to h which are not in $\Pi(l)$. Count the ordered pairs of different

h_i. There are $s(s-1)$ such ordered pairs. Consider the lines $l_j \in \Pi(l), j = 1, \dots c$. Each l_j contains $m_j \leqslant \epsilon - 1 \leqslant \delta - 1$ exceptional points not on h and $n - 1 - m_j$ non-exceptional points. The non-exceptional points of l_j lie on at most one line parallel to h and thus on at most one line h_i; thus at least $s - (n - 1 - m_j)$ lines h_i must meet l_j in one of the m_j exceptional points not on h. The Cauchy-Schwartz inequality shows that the number of pairs of different h_i meeting in a point of l_j is at least

$$m_j \frac{s-n+1+m_j}{m_j}(\frac{s-n+1+m_j}{m_j} - 1) \geqslant \frac{(s-n+1)^2}{\delta - 1}.$$

We obtain the inequality

$$c(s-n+1)^2 \leqslant (\delta - 1)s(s-1).$$

Let us create a factor of s on the left side: as $s \leqslant 2(n-1)$ we obtain $(n-1)^2 \geqslant (n-1)s/2$ and $(s-(n-1))^2 = s^2 - 2(n-1)s + (n-1)^2 \geqslant s(s - 2(n-1) + (n-1)/2)$. The major inequality simplifies after factoring s :

$$c(s - 3(n-1)/2) \leqslant (\delta - 1)(s-1) < (\delta - 1)2n.$$

Using the lower bounds:

$$(\delta - 1)2n > (n - (\delta + 1)^2/4)((n+3)/2 - (\delta + 2)^2/4),$$

after multiplying out on the right, forgetting the terms not dependent on n and canceling the factor $n : 2(\delta+2)^2 + (\delta+1)^2 + 16(\delta-1) > 4n$ which clearly contradicts the hypothesis. □

Theorem 25. *Let $(\delta^2 - 1)(\delta + 1)^2 < 27(n+2)/16$. Then every line has deficiency $\leqslant \delta$.*

Proof. Pick a non-exceptional point P_0 and its bundle of $n+1$ lines $l_1, \dots, l_{n+1}$. Let $\delta_i = \delta_{l_i}$ and $\epsilon_i = \delta - \delta_i$. We want to show that $\epsilon_i \geqslant 0$ for all i. As every line is parallel to one of the lines l_i, the preceding theorem then implies the statement.

Assume therefore that some of the ϵ_i are negative. As $\sum \epsilon_i = \delta$ and at least one negative ϵ_i is present, we can find some positive ϵ_i that sum to at least $\delta + 1$. As $\epsilon_i \leqslant \delta$ for all i we can choose them such that the sum is at most 2δ. Choose therefore the lines $l_1, \dots, l_s$ such that $\epsilon_i \geqslant 0$ for $i \leqslant s$ and $z = \sum_{i=1}^{s} \epsilon_i$ satisfies $\delta + 1 \leqslant z \leqslant 2\delta$. Use the result of the preceding theorem: let $\Pi_i = \Pi(l_i)$ for $i \leqslant s$ and recall that Π_i consists of $n - \epsilon_i$ parallel lines each of which has deficiency δ_i. Let M_i be the set of points covered by the lines of Π_i and N_i its complement. We have $|M_i| = n(n - \epsilon_i)$ and $|N_i| = n\epsilon_i$. Also, let $N = \cup_{i=1}^{s} N_i$. Observe that N consists of exceptional points. Recall also from Theorem 24 that lines $l \in \Pi_i, g \in \Pi_j$ for $i < j \leqslant s$ must meet. This has the following evident consequences: if $l \in \Pi_i$ and $i \neq j$, then $|l \cap M_j| = n - \epsilon_j$ and $|l \cap N_j| = \epsilon_j$. It follows $|N_i \cap N_j| = \epsilon_i \epsilon_j$.

Here is a first lower bound on $|N|$: observe at first that $|N| \geqslant \sum_{i=1}^{s} |N_i| - \sum_{i<j\leqslant s} |N_i \cap N_j|$. In fact, the right side does count elements of N. If $P \in N$ occurs in precisely $t \geqslant 1$ of

the N_i, then the contribution of P to the right side is $t - \binom{t}{2} \leqslant 1$. The inequality follows. Continuing on the right side we obtain

$$|N| \geqslant \sum_{i=1}^{s} \epsilon_i n - \frac{1}{2} \sum_{i,j=1}^{s} \epsilon_i \epsilon_j = zn - (1/2)z^2 \tag{4}$$

Consider again a point $X \in N$. It is exceptional and therefore on at most n lines. Let X be in N_i for $i \leqslant t$ and in M_i for $t < i \leqslant s$. The number of points of N which are collinear with X is bounded by

$$\sum_{i=1}^{t} n(\epsilon_i - 1) + \sum_{i=t+1}^{s} n\epsilon_i = nz - nt.$$

Together with Equation (4) this shows that the number of points of N which are not collinear with X is $\geqslant |N| - 1 - nz + nt \geqslant nt - 1 - z^2/2$. As $z \leqslant 2\delta$ it follows that the number of points in N not collinear with X is $\geqslant tn - 1 - 2\delta^2$ and therefore $> (t-1)n$. We conclude $\delta_X \geqslant t$. Finally $\sum_{X \in N} \delta_X$ is lower bounded by the number of pairs (i, X) where $i \leqslant s$ and $X \in N_i$. This number is $\sum_{i=1}^{s} |N_i| = \sum \epsilon_i n > \delta n$. As $\sum_{X \in N} \delta_X \leqslant \delta n$ by Lemma 12, this is a contradiction. □

We are ready for the final step.

Theorem 26. *Each $P(n, \delta)$ is embeddable provided $(\delta^2 - 1)(\delta + 1)^2 < 27(n+2)/16$.*

Proof. Assume $(\delta^2 - 1)(\delta + 1)^2 < 27(n+2)/16$. We need to show that $P(n, \delta)$ can be embedded in a $P(n, \delta - 1)$. As before start from a non-exceptional point P and its bundle of lines. As $\sum \delta_i = \delta n$ it follows that there is some line l_1 on P whose deficiency is $d < \delta$. Let $\Pi = \Pi(l_1)$, a parallel class of $n - \delta + d$ lines, each of deficiency d. Let M be the set of points covered by Π, and N the complement of M. Assume all $X \in N$ satisfy $\delta_X \geqslant 2$. An obvious count yields the contradiction $\delta n = \sum_Q \delta_Q \geqslant d(n - \delta + d) + 2n(\delta - d)$, equivalently $(n - d)(\delta - d) \leqslant 0$. It follows that there is some $X \in N$ such that $\delta_X = 1$. Let U be the union of X and the $n - 1$ points not collinear with X. Assume some line l contains at least two points of U. Let $t = |l \cap U| \geqslant 2$. Then there are some two lines on X which are both parallel to l. We are in the situation of Lemma 18 which, in conjunction with Theorem 25, implies $n + 1 \leqslant \delta(2\delta - 1)$. This contradiction shows that U can be used as a new line which together with the lines of the $P(n, \delta)$ forms a $P(n, \delta - 1)$. This completes the proof. □

References

[1] J. Bierbrauer, S. Black and Y. Edel: Some t-homogeneous sets of permutations, *Designs, Codes and Cryptography* **9** (1996), 29-38.

[2] J. Bierbrauer and Y. Edel: Theory of perpendicular arrays, *Journal of Combinatorial Designs* **6** (1994), 375-406.

[3] M. Bogaerts: Isometries and construction of permutation arrays, *IEEE IT Transactions* **56** (2010), 3177-3179.

[4] R. H. Bruck: Finite nets II. Uniqueness and embedding, *Pacific J. Math.* **13** (1963), 421-457.

[5] W. Chu, C. Colbourn, P. Dukes: Constructions for permutation codes in powerline communications, *Designs, Codes and Cryptography* **32** (2004), 51-64.

[6] H.C. Ferreira, A.J.H. Vinck: Inference cancellation with permutation trellis arrays, *Proc. IEEE Vehtcular Technology Conf.* 2000, 2401-2407.

[7] S. Huczynska: Powerline communication and the 36 officers problem, *Phil. Trans.R. Soc.A* **364** (2006), 3199-3214.

[8] I. Janiszczak, R. Staszewski: An improved bound for permutation arrays of length 10, manuscript.

[9] T. Kløve, Classification of permutation codes of length 6 and minimum distance 5, *Internat. Symposium on Info. Theory and its Applications,* Honolulu 2000, 465-468.

[10] T. Kløve: A combinatorial problem motivated by a data transmission application, Chapman and Hall/ CRC Press 2004.

[11] Bill Martin and B.E. Sagan: A new notion of transitivity for groups and sets of permutations, *Journal of the London Mathematical Society* **73** (2006), 1-13.

[12] K. Metsch: Improvement of Bruck's completion theorem, *Designs, Codes and Cryptography* **1** (1991), 99-116.

[13] J. Quistorff: A survey on packing and covering problems in the Hamming permutation space, *Electron. J. Comb.* (2006), A1.

[14] D.R. de la Torre, C.J. Colbourn, A.C.H. Ling: An application of permutation arrays to block ciphers, *Congr. Numer.* **145** (2000), 5-7.

[15] A.J. Han Vinck: Codes modulation for powerline communications, *AE Internat. Journal of Electronics and Commun.* **54** (2000), 45-49.