$d-1$ of the copies of $\boldsymbol{C}^q$, the inner product $\langle v|M|v\rangle$ is constant as v ranges over the unit vectors of C. A quantum code with minimum distance d can be used to correct $[(d-1)/2]$ single-letter errors.

The *symplectic* inner product in $\mathrm{GF}(q)^{2n}$ is defined as follows:

$$((a|b),\,(a'|b')) = a\cdot b' - b\cdot a' \tag{7}$$

where

$$(a|b) = (a_1,\,\ldots,\,a_n,\,b_1,\,\ldots b_n),$$
$$(a'|b') = (a'_1,\,\ldots,\,a'_n,\,b'_1,\,\ldots b'_n), \qquad a_i,\,b_i,\,a'_i,\,b'_i \in \mathrm{GF}(q).$$

The symplectic weight w_s of a vector $(a_1,\,\ldots,\,a_n,\,b_1,\,\ldots b_n) \in \mathrm{GF}(q)^{2n}$ is defined as the number of indexes i such that at least one of a_i and b_i is nonzero. The symplectic weight w_s and Hamming weight w_h of a vector $(a|b) \in GF(q)^{2n}$ are related by

$$\frac{1}{2}\,w_h((a|b)) \le w_s((a|b)) \le w_h((a|b)). \tag{8}$$

Rains [8] showed that a quantum $((n,\,q^k,\,d))_q$ code exists provided that there is an $(n-k)$-dimensional subspace C of $\mathrm{GF}(q)^{2n}$ which is self-orthogonal with respect to the symplectic product, and such that the minimum symplectic weight of $C^\perp - C$ is at least d. If d' is the minimum weight of the nonzero elements of C, then C is said to be *pure* to weight d'. If $d' \ge d$, the code C is called *pure*.

If C is self-dual, that is, $C = C^\perp$, the resulting quantum code is pure by convention and corresponds to a single quantum state with the property that when subjected to a decoherence of $[(d-1)/2]$ coordinates, it is possible to determine which coordinates were decohered. Such codes are useful in testing whether certain storage locations of qubits are decohering faster than they should [5].

Consider now a linear $(2n,\,n)$ code $C \in \mathcal{A}$ with a generator matrix $(I,\,A)$, where A is a symmetric $n\times n$ matrix over $\mathrm{GF}(q)$: $A = A^T$. Since $(-A,\,I)$ is a generator matrix of the dual code with respect to the ordinary inner product (1), the code is formally self-dual, that is, the Hamming weight distribution of the code and its dual coincide.

Lemma 3.1: Any q-ary $(2n,\,n)$ code $C \in \mathcal{A}$ is self-dual ($C = C^\perp$) with respect to the symplectic inner product (7).

Proof: If $G = (I,\,A)$ is a generator matrix of C, the symplectic inner product of the ith and jth row of G is $a_{ij} - a_{ji}$. Since $A = A^T$, we have $a_{ij} - a_{ji} = 0$. □

Now Theorem 2.1, (6), Lemma 3.1, and (8) imply the following.

Theorem 3.2: The class of quantum-error-correcting codes of length n obtained from $(2n,\,n)$ codes from the class $\mathcal{A}$ contains codes that can correct $[(d-1)/2]$ errors where

$$\frac{d}{n} \ge P$$

and P is defined as in Theorem 2.1.

Remark 3.3: The quantum codes in Theorem 3.2 are of dimension zero, hence encode one quantum state with n qubits. A construction of nonbinary quantum codes with asymptotically nonzero rate and relative distance was recently found by Ashikhmin, Litsyn, and Tsfasman [3].

Acknowledgment

The author wishes to thank the referees for the very useful comments and suggestions.

References

[1] A. Ashikhmin, A. Barg, E. Knill, and S. Litsyn, "Quantum error detection II: Lower and upper bounds," *IEEE Trans. Inform. Theory*, pp. 789–801, May 2000.
[2] A. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes," LANL preprint quant-ph/0005008.
[3] A. Ashikhmin, S. Litsyn, and M. A. Tsfasman. Asymptotically good quantum codes. LANL preprint quant-ph/0 006 061. [Online]. Available: http://xxx.lanl.gov/abs/quant-ph/0 006 061
[4] E. R. Berlekamp, *Algebraic Coding Theory*. New York: McGraw-Hill, 1968.
[5] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF (4)," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1369–1387, July 1998.
[6] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev., A*, vol. 54, pp. 1098–1105, 1996.
[7] V. Pless and J. N. Pierce, "Self-dual codes over $GF(q)$ satisfy a modified Varshamov–Gilbert bound," *Inform. Contr.*, vol. 23, pp. 35–40, 1973.
[8] E. M. Rains, "Nonbinary quantum codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1827–1832, Sept. 1999.
[9] A. Steane, "Simple quantum error correcting codes," *Phys. Rev. Lett.*, vol. 77, pp. 793–797, 1996.
[10] V. D. Tonchev, "Error-correcting codes from graphs," *Discr. Math.*, to be published.

Constructions of Permutation Arrays

Cunsheng Ding, Fang-Wei Fu, Torleiv Kløve, *Senior Member, IEEE*, and Victor K.-W. Wei, *Fellow, IEEE*

***Abstract*—A permutation array (PA) of length n and minimum distance d is a set of permutations of n elements such that any two permutations coincide in at most $n-d$ positions. Some constructions of PAs are given.**

***Index Terms*—Code construction, permutation array (PA), permutation code.**

I. Introduction

We consider permutations of the distinct elements of some fixed set R with n elements. Let S_n denote the set of all $n!$ permutations. For example, for $n=3$ and $R=\{0,\,1,\,2\}$, we have

$$S_3 = \{012,\,021,\,102,\,120,\,201,\,210\}.$$

Manuscript received December 13, 2000; revised November 20, 2001. This work was supported in part by the National Natural Science Foundation of China under Grant 60172060, the Trans-Century Training Program Foundation for the Talents of the Education Ministry of China, and the Foundation for University Key Teacher of the Education Ministry of China, The Norwegian Research Council, and the Research Grant Council of Hong Kong under Earmarked Grant CUHK 4424/99E.

C. Ding is with the Department of Computer Science, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong (e-mail: cding@cs.ust.hk).

F.-W. Fu is with the Department of Mathematics, Nankai University, Tianjin 300071, China (e-mail: fwfu@nankai.edu.cn).

T. Kløve is with the Department of Information Engineering, The Chinese University of Hong Kong, Shatin, N.T., Hong Kong, on leave from University of Bergen, Norway (e-mail: Torleiv.Klove@ii.uib.no).

V. K.-W. Wei is with the Department of Information Engineering, The Chinese University of Hong Kong, Shatin, N.T., Hong Kong (e-mail: kwwei@ie.cuhk.edu.hk).

Communicated by S. Litsyn, Associate Editor for Coding Theory.

Publisher Item Identifier S 0018-9448(02)01934-X.

An $(n,\ d)$ *permutation array* (PA) is a subset of S_n with the property that the Hamming distance between any two distinct permutations in the array is at least d. The PA is called equidistant if the Hamming distance between any two distinct permutations in the array is exactly d. There are a number of papers on equidistant PA, see [2, pp. 326–329] and references therein. Less is known about PA in general. The main papers are [1], [3], [5], [11]. A very recent paper is [12]. Cyclic $(n, n–1)$ PA have been studied under the name circular florentine arrays, see [2, pp. 480–484]. Recently, Vinck and coauthors [4], [6]–[8] used PA in an application to data transmission over power lines. In [9] the $(6,\ 5)$ PA of maximal size 18 were classified. In [10], some constructions of $(n,\ n-1)$ PA were given. In this correspondence, we also mainly consider constructions of $(n,\ n-1)$ PA.

II. Some Known Results

Let $P_{n,\,d}$ be the maximal size of an $(n,\ d)$ PA. Reference [3] proved that for all n and d we have the following simple upper bound.

Theorem 1: For all $n \geq 1$ we have

$$P_{n,\,d} \leq \frac{n!}{(d-1)!}.$$

In particular, $P_{n,\,n-1} \leq n(n-1)$.

Proof: We include the easy proof here. Let C be an $(n,\ d)$ PA. There are $n!/(d-1)!$ sequences in R^{n-d+1} having distinct elements. For any such sequence there is at most one permutation in C starting with this sequence since two distinct such permutations would have distance at most $n-(n-d+1)=d-1$. QED

Reference [3] also showed the following.

Proposition 1: If n is a prime power, then

$$P_{n,\,n-1} = n(n-1).$$

Reference [10] generalized the construction and the bound. We repeat the results and proofs here.

Theorem 2: Let R be a ring (commutative with unity) of size n. Let U be the set of (multiplicative) units in R. Let V be a subset of U such that $v-v' \in U$ for all distinct $v,\ v' \in V$. Let

$$C = \{(v \cdot x + y | x \in R)\,|\, v \in V,\ y \in R\}.$$

Then C is an $(n,\ n-1)$ PA of size $n \cdot |V|$.

Proof: We first note that $(v \cdot x + y | x \in R)$ is a permutation of R since $vx+y = vx'+y$ implies $v(x-x')=0$ and so $x-x' = v^{-1}\cdot 0 = 0$. Next, if $v \cdot x + y = v' \cdot x + y'$ where $v \neq v'$ (and $v,\ v' \in V$), then

$$x = (y'-y)\cdot(v-v')^{-1}$$

that is, x is uniquely determined. QED

For an integer $n>1$, let $n = \prod_{i=1}^{u} p_i^{e_i}$ be the standard factorization of n, and let

$$\theta(n) = \min\{p_i^{e_i} | 1 \leq i \leq u\}.$$

Theorem 3: For all $n > 1$ we have

$$P_{n,\,n-1} \geq n\,(\theta(n)-1)\,.$$

Proof: Let

$$R = \mathrm{GF}\,(p_1^{e_1}) \times \mathrm{GF}\,(p_2^{e_2}) \times \cdots \times \mathrm{GF}\,(p_u^{e_u})$$

(direct product). For $1 \leq i \leq u$, let γ_{ij}, $j = 1,\ 2,\ \ldots,\ \theta(n)-1$ be distinct nonzero elements of GF $(p_i^{e_i})$. Let

$$V = \{(\gamma_{1j},\ \gamma_{2j},\ \ldots,\ \gamma_{uj}) | 1 \leq j \leq \theta(n)-1\}\,.$$

Then the conditions of Theorem 2 are satisfied and so Theorem 2 gives an array of size $n(\theta(n)-1)$. QED

As usual, we get an equivalent code if we permute the positions or permute the elements of the set R. For example, if $\pi_1,\ \pi_2$ are permutations of the ring R of Theorem 2, the theorem gives the following $(n,\ n-1)$ PA:

$$C = \{(\pi_2\,(v \cdot \pi_1(x) + y)\,|x \in R)\,|v \in V,\ y \in R\}\,.$$

III. Some Terminology

Let C be a PA over R of size M. We list the permutations of C as rows of an $M \times n$ array which we also denote by C. We introduce some terminology.

We say that C is r-**bounded** if no element of R appears more than r times in any column of C.

We say that C is r-**balanced** if each element of R appears exactly r times in each column of C.

We say that C is r-**separable** if it is the disjoint union of r $(n,\ n)$ PA of size n.

We say that C is **cyclic** if any cyclic shift of a row in C is a gain a row in C.

These concepts are related. An r-separable PA is r-balanced. An r-balanced PA is r-bounded. Further, an r-bounded $(n,\ n-1)$ PA has size at most rn and it has size exactly rn if and only if it is r-balanced. Finally, a cyclic PA is r-separable for some r.

Example 1: The PA given by the construction in Theorem 2 is $|V|$-separable

$$C = \bigcup_{v \in V} C_v, \qquad \text{where } C_v = \{(v \cdot x + y | x \in R) | y \in R\}\,.$$

Example 2: Let C be a cyclic $(n,\ n-1)$ PA of size rn. Then

$$C = \bigcup_{i=1}^{r} C_i$$

where the C_i are cyclic $(n,\ n)$ PA. Each C_i contains a row from C and all its cyclic shifts. In particular, C is r-separable. An $r \times n$ array containing one row from each C_i is known as a circular florentine array, see [2, pp. 480–484].

From the proof of Theorem 1 and the definition of r-balanced, we immediately get the following result.

Proposition 2: Any $(n,\ n-1)$ PA of size $n(n-1)$ is $(n-1)$-balanced.

Let $B_{n,\,r}$ denote that maximal size of an r-bounded $(n,\ n-1)$ PA. Clearly,

$$B_{n,\,r} \leq rn \tag{1}$$

and

$$n = B_{n,\,1} \leq B_{n,\,2} \leq \cdots \leq B_{n,\,n-1} = P_{n,\,n-1} \tag{2}$$

where the last equality follows from the fact that an element of R can appear at most $n-1$ times in a column of an $(n,\ n-1)$ PA.

Proposition 3: For $1 \leq r \leq \theta(n)-1$, we have $B_{n,\,r} = nr$.

Proof: The C used to prove Theorem 3 is $(\theta(n)-1)$-separable. Taking a suitable subset of this C we can get an r-separable $(n,\ n-1)$ PA for any $r \leq \theta(n)-1$. QED

Remark 1: For q a prime power, Theorem 3 gives a $(q-1)$-separable $(q, q-1)$ PA of size $q(q-1)$; the construction in this case is essentially due to [3]. Properties (1) and (2) immediately gives the following result.

Proposition 4: If q is a prime power, then $B_{q,q-1} = q(q-1)$.

Example 3: There exists a circular florentine 4×15 array, see [2, Table 48.17]. Hence $B_{15,4} = 60$.

IV. A New Construction

We will now introduce a method to combine two arrays to make a larger array.

Let $C = (c_{ij})$ be an $(n, n-1)$ array of size M (the elements are assumed to be from $\{0, 1, \ldots, n-1\}$).

Define $f(i, j)$ as follows: if $c_{ij} = \alpha$ and this is the tth appearance of α in column j, counting from the top, then $f(i, j) = t$. From this definition we see that

$$\text{if } c_{i_1 j} = c_{i_2 j} \text{ and } i_1 \neq i_2, \text{ then } f(i_1, j) \neq f(i_2, j). \tag{3}$$

Further, C is r-bounded if and only if $f(i, j) \leq r$ for all i and j.

Let $C = (c_{ij})$ be r-bounded and let

$$\Gamma = \Gamma_1 \cup \Gamma_2 \cup \cdots \cup \Gamma_s$$

be an s-separable $(m, m-1)$ array (of size sm and elements from $\{0, 1, \ldots, m-1\}$) where $s \geq r$ and the Γ_u are (m, m) PA. Denote the permutations (rows) of Γ_u by $\boldsymbol{g}_{u,v}$, $v = 1, 2, \ldots, m$.

Define $C * \Gamma$ as the $mM \times mn$ matrix containing $M \times n$ blocks where block (i, j) is the $m \times m$ matrix

$$\Gamma_{f(i,j)} + mc_{i,j}J$$

where J is the all–1 matrix.

We can now give the main result of this correspondence.

Theorem 4: If C is an r-bounded $(n, n-1)$ PA and Γ is an s-separable $(m, m-1)$ PA where $s \geq r$, then $C * \Gamma$ is an r-bounded $(mn, mn-1)$ PA of size $m|C|$. Moreover, if C is r-balanced, then $C * \Gamma$ is r-balanced.

Proof: The rows of $C * \Gamma$ are clearly permutations of $\{0, 1, \ldots, mn-1\}$. Let $\boldsymbol{x}, \boldsymbol{y}$ be distinct rows of $C * \Gamma$. Then

$$\boldsymbol{x} = \left(\boldsymbol{g}_{f(i_1,j),l_1} + c_{i_1,j}\boldsymbol{m}\right)_{j=1,2,\ldots,n}$$
$$\boldsymbol{y} = \left(\boldsymbol{g}_{f(i_2,j),l_2} + c_{i_2,j}\boldsymbol{m}\right)_{j=1,2,\ldots,n}$$

where $\boldsymbol{m} = (m, m, \ldots, m)$ (of length m). Hence,

$$d_H(\boldsymbol{x}, \boldsymbol{y}) = \sum_{j=1}^{n} d_H\left(\boldsymbol{g}_{f(i_1,j),l_1} + c_{i_1,j}\boldsymbol{m}, \boldsymbol{g}_{f(i_2,j),l_2} + c_{i_2,j}\boldsymbol{m}\right).$$

We consider three cases.

Case I, $i_1 = i_2 = i$: Then $c_{i_1,j} = c_{i_2,j}$ for all j, and $l_1 \neq l_2$. Since $\Gamma_{f(i,j)}$ is an (m, m) PA, we have

$$d_H\left(\boldsymbol{g}_{f(i_1,j),l_1} + c_{i_1,j}\boldsymbol{m}, \boldsymbol{g}_{f(i_2,j),l_2} + c_{i_2,j}\boldsymbol{m}\right) = d_H\left(\boldsymbol{g}_{f(i,j),l_1}, \boldsymbol{g}_{f(i,j),l_2}\right) = m$$

for all j and so $d_H(\boldsymbol{x}, \boldsymbol{y}) = mn$.

Case II, $i_1 \neq i_2$, but $c_{i_1,j} = c_{i_2,j}$. (This can be the case for at most one value of j since C is an $(n, n-1)$ PA): By (3), $f(i_1, j) \neq f(i_2, j)$. Hence,

$$d_H\left(\boldsymbol{g}_{f(i_1,j),l_1} + c_{i_1,j}\boldsymbol{m}, \boldsymbol{g}_{f(i_2,j),l_2} + c_{i_2,j}\boldsymbol{m}\right) = d_H\left(\boldsymbol{g}_{f(i_1,j),l_1}, \boldsymbol{g}_{f(i_2,j),l_2}\right) \geq m-1.$$

Case III, $c_{i_1,j} \neq c_{i_2,j}$: The elements of $\boldsymbol{g}_{f(i_1,j),l_1} + c_{i_1,j}\boldsymbol{m}$ belong to the set

$$\{mc_{i_1,j}, mc_{i_1,j}+1, \ldots, mc_{i_1,j}+m-1\}$$

and the elements of $\boldsymbol{g}_{f(i_2,j),l_1} + c_{i_2,j}\boldsymbol{m}$ belong to

$$\{mc_{i_2,j}, mc_{i_2,j}+1, \ldots, mc_{i_2,j}+m-1\}.$$

Since these sets are disjoint, we have

$$d_H\left(\boldsymbol{g}_{f(i_1,j),l_1} + c_{i_1,j}\boldsymbol{m}, \boldsymbol{g}_{f(i_2,j),l_2} + c_{i_2,j}\boldsymbol{m}\right) = m.$$

Combining Cases II and III, we see that if $i_1 \neq i_2$, then $d_H(\boldsymbol{x}, \boldsymbol{y}) \geq mn-1$. Hence, we have shown that $C * \Gamma$ is an $(mn, mn-1)$ code.

By the definition of $C * \Gamma$, each column of $C * \Gamma$ is a column of the matrix

$$\begin{bmatrix} \Gamma_{f(1,j)} + mc_{1,j}J \\ \vdots \\ \Gamma_{f(M,j)} + mc_{M,j}J \end{bmatrix} \tag{4}$$

for some j with $0 \leq j \leq n-1$. Since the $\Gamma_{f(i,j)}$ are (m, m) PA, each column of $\Gamma_{f(i,j)}$ is a permutation of $\{0, 1, \ldots, m-1\}$. Hence, for any fixed $x \in \{0, 1, \ldots, m-1\}$, the element $x + my$ appears in some fixed column of (4) the same number of times that y appears in the jth column of C. Hence $C * \Gamma$ is r-bounded (respectively, r-balanced) if and only if C is r-bounded (respectively, r-balanced). QED.

We illustrate the theorem with a couple of simple examples.

Example 4: Let

$$C = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\Gamma_1 = \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix}, \qquad \Gamma_2 = \begin{bmatrix} 0 & 2 & 1 \\ 2 & 1 & 0 \\ 1 & 0 & 2 \end{bmatrix}, \qquad \Gamma = \Gamma_1 \cup \Gamma_2.$$

We see that C is a 1-balanced $(2, 1)$ PA and $f(i, j) = 1$ for all i and j. We get

$$C * \Gamma = \begin{bmatrix} \Gamma_1 & \Gamma_1 + 3J \\ \Gamma_1 + 3J & \Gamma_1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 0 & 4 & 5 & 3 \\ 2 & 0 & 1 & 5 & 3 & 4 \\ 3 & 4 & 5 & 0 & 1 & 2 \\ 4 & 5 & 3 & 1 & 2 & 0 \\ 5 & 3 & 4 & 2 & 0 & 1 \end{bmatrix}.$$

We note that Γ_2 is not used since C is 1-balanced. Hence $C * \Gamma = C * \Gamma_1$. Further, we see that $C * \Gamma$ is 1-balanced.

Example 5: Let

$$C = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 0 & 2 & 3 & 1 \\ 1 & 3 & 0 & 2 \\ 1 & 2 & 0 & 3 \end{bmatrix}$$

and let Γ be the same PA as in the previous example. We see that C is a 2-bounded (but not 2-balanced) $(4, 3)$ PA. Further, $f(2, 1) = 2$, $f(4, j) = 2$ for $j = 1, 2, 3, 4$, and $f(i, j) = 1$ in all other cases. Hence, we get

$$C * \Gamma = \begin{bmatrix} \Gamma_1 & \Gamma_1 + 3J & \Gamma_1 + 6J & \Gamma_1 + 9J \\ \Gamma_2 & \Gamma_1 + 6J & \Gamma_1 + 9J & \Gamma_1 + 3J \\ \Gamma_1 + 3J & \Gamma_1 + 9J & \Gamma_1 & \Gamma_1 + 6J \\ \Gamma_2 + 3J & \Gamma_2 + 6J & \Gamma_2 & \Gamma_2 + 9J \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 1 & 2 & 0 & 4 & 5 & 3 & 7 & 8 & 6 & 10 & 11 & 9 \\ 2 & 0 & 1 & 5 & 3 & 4 & 8 & 6 & 7 & 11 & 9 & 10 \\ 0 & 2 & 1 & 6 & 7 & 8 & 9 & 10 & 11 & 3 & 4 & 5 \\ 2 & 1 & 0 & 7 & 8 & 6 & 10 & 11 & 9 & 4 & 5 & 3 \\ 1 & 0 & 2 & 8 & 6 & 7 & 11 & 9 & 10 & 5 & 3 & 4 \\ 3 & 4 & 5 & 9 & 10 & 11 & 0 & 1 & 2 & 6 & 7 & 8 \\ 4 & 5 & 3 & 10 & 11 & 9 & 1 & 2 & 0 & 7 & 8 & 6 \\ 5 & 3 & 4 & 11 & 9 & 10 & 2 & 0 & 1 & 8 & 6 & 7 \\ 3 & 5 & 4 & 6 & 8 & 7 & 0 & 2 & 1 & 9 & 11 & 10 \\ 5 & 4 & 3 & 8 & 7 & 6 & 2 & 1 & 0 & 11 & 10 & 9 \\ 4 & 3 & 5 & 7 & 6 & 8 & 1 & 0 & 2 & 10 & 9 & 11 \end{bmatrix}.$$

This is a 2-bounded (but not 2-balanced) $(12, 11)$ PA.

The following corollary follows directly from Theorem 4.

Corollary 1: If there exists an s-separable $(m, m-1)$ PA, then

$$B_{nm,r} \geq mB_{n,r}$$

for all n and r such that $n > r$ and $r \leq s$.

Combining Corollary 1 and Proposition 2, we get the following.

Corollary 2: If q is a prime power and $r < q$, then

$$B_{nq,r} \geq qB_{n,r}.$$

If, further, $B_{n,r} = nr$, then $B_{nq,r} = nqr$.

Remark 2: An alternative proof of Theorem 3 by induction, on the number of different prime powers in the standard factorization of n, is obtained using Proposition 4 as basis and Corollary 2 in the induction step. More general, a similar induction gives the following result.

Proposition 5: If $B_{m,r} = rm$ and $\theta(n) > r$, then $B_{nm,r} = rnm$.

Example 6: It is known that $P_{6,5} = 18$ and that there exist 3-balanced $(6, 5)$ PA, see [9]. Therefore, $B_{6,3} = 18$. An examination of [9] shows that no $(6, 5)$ PA of size 18 is 3-separable.

For $B_{n,3}$ in general, we get the following result.

Proposition 6: Let $n = 2^a 3^b m$ where $\gcd(m, 6) = 1$. If $(a, b) \notin \{(1, 0), (0, 1), (2, 1), (1, 2)\}$, then $B_{n,3} = 3n$.

Proof: For $a = b = 0$, $a = 0$ and $b \geq 2$, $a \geq 2$ and $b = 0$, or $a \geq 2$ and $b \geq 2$ this follows directly from Proposition 3.

For $a = b = 1$, $a = 1$ and $b \geq 3$, or $a \geq 3$ and $b = 1$, it follows by combining Proposition 5 and the fact that $B_{6,3} = 18$. QED

V. A Generalization

Theorem 4 can be generalized in various ways. We state without proof one immediate generalization. The proof is a simple modification of the proof of Theorem 4.

Theorem 5: If C is an r-bounded $(n, n-u)$ PA and Γ is an s-separable $(m, m-v)$ PA where $s \geq r$, then $C * \Gamma$ is an r-bounded $(mn, mn-uv)$ PA of size $m|C|$. Moreover, if C is r-balanced, then $C * \Gamma$ is r-balanced.

References

[1] I. F. Blake, G. Cohen, and M. Deza, "Coding with permutations," *Inform. Contr.*, vol. 43, pp. 1–19, 1979.

[2] C. J. Colbourn and J. H. Dinitz, *The CRC Handbook of Combinatorial Designs*. Boca Raton, FL: CRC, 1996.

[3] M. Deza and S. A. Vanstone, "Bounds on permutation arrays," *J. Statist. Planning and Inference*, vol. 2, pp. 197–209, 1978.

[4] H. C. Ferreira and A. J. H. Vinck, "Inference cancellation with permutation trellis arrays," in *Proc. IEEE Vehicular Technology Conf.*, vol. 2000, pp. 2401–2407.

[5] P. Frankl and M. Deza, "On the maximum number of permutations with given maximal and minimal distance," *J. Comb. Theory, Ser. A*, vol. 22, pp. 352–360, 1977.

[6] A. J. H. Vinck, "Coded modulation for powerline communications," *AEÜ Int.. J. Electron. and Commun.*, vol. 54, no. 1, pp. 45–49, 2000.

[7] A. J. H. Vinck and J. Häring, "Coding and modulation for power-line communications," in *Proc. Int. Symp. Power Line Communication*, Limerick, Ireland, Apr. 5–7, 2000.

[8] A. J. H. Vinck, J. Häring, and T. Wadayama, "Coded M-FSK for power-line communications," in *Proc. IEEE Int.. Symp. Information Theory*, 2000, p. 137.

[9] T. Kløve, "Classification of permutation codes of length 6 and minimum distance 5," in *Proc. Int. Symp. Information Theory and Appl.*, 2000, pp. 465–468.

[10] ——, "A combinatorial problem motivated by a data transmission application," in *Proc. Norsk Informatikkonf. (NIK)*, 2000, pp. 55–66.

[11] H. Tarnanen, "Upper bounds on permutation codes via linear programming," *Europ. J. Combin.*, vol. 20, pp. 101–114, 1999.

[12] T. Wadayama and A. J. H. Vinck, "A multilevel construction of permutation codes," *IEICE Trans. Fundamentals Electron., Commun. Comp. Sci.*, vol. 84, pp. 2518–2522, 2001.