On the other hand, if we define $\tilde{D}(i)$ to be

$$\tilde{D}(i) = \{l \in \Lambda^c \mid c-1+i-l \in \Lambda^c, i < l < c-1\}$$

then

$$D(c-1+i-g) = \begin{cases} \tilde{D}(i) \cup \{c-1, i\}, & \text{if } i \in \Lambda^c \\ \tilde{D}(i), & \text{otherwise.} \end{cases} \quad (3)$$

So, from (2) and (3)

$$i \text{ is a nongap} \iff \nu_{c-1+i-g} = c + i - 2g + \#\tilde{D}(i).$$

This gives an inductive procedure to decide whether i belongs to Λ decreasingly from $i = c-2$ to $i = 2$. □

Remark 8.2: From the proof of Theorem 8.1 we see that a semigroup can be determined by $k = \max\{i \mid \nu_i = \nu_{i+1}\}$ and the values ν_i for $i \in \{c-g+1, \ldots, 2c-g-3\}$.

Acknowledgment

The author would like to thank Michael E. O'Sullivan, Ruud Pellikaan, and Pedro A. García-Sánchez for many helpful discussions. She would like to thank also the referees for their careful reading and for many interesting remarks.

References

[1] V. Barucci, D. E. Dobbs, and M. Fontana, "Maximality properties in numerical semigroups and applications to one-dimensional analytically irreducible local domains," *Mem. Amer. Math. Soc.*, vol. 125, no. 598, p. x+78, 1997.
[2] M. Bras-Amorós, "Improvements to evaluation codes and new characterizations of Arf semigroups," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2003.
[3] A. Campillo and J. I. Farrán, "Computing Weierstrass semigroups and the Feng-Rao distance from singular plane models," *Finite Fields Appl.*, vol. 6, no. 1, pp. 71–92, 2000.
[4] A. Campillo, J. I. Farrán, and C. Munuera, "On the parameters of algebraic-geometry codes related to Arf semigroups," *IEEE Trans. Inform. Theory*, vol. 46, pp. 2634–2638, Nov. 2000.
[5] H. M. Farkas and I. Kra, *Riemann Surfaces (Graduate Texts in Mathematics)*, 2nd ed. New York: Springer-Verlag, 1992, vol. 71.
[6] G. L. Feng and T. R. N. Rao, "A simple approach for construction of algebraic-geometric codes from affine plane curves," *IEEE Trans. Inform. Theory*, vol. 40, pp. 1003–1012, July 1994.
[7] ——, "Improved geometric Goppa codes. I. Basic theory," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1678–1693, Nov. 1995.
[8] A. Garcia and H. Stichtenoth, "On the asymptotic behavior of some towers of function fields over finite fields," *J. Number Theory*, vol. 61, no. 2, pp. 248–273, 1996.
[9] P. A. García-Sánchez and J. C. Rosales, "Numerical semigroups generated by intervals," *Pacific J. Math.*, vol. 191, no. 1, pp. 75–83, 1999.
[10] O. Geil, "On codes from norm-trace curves," *Finite Fields Their Applic.*, vol. 9, no. 3, pp. 351–371, 2003.
[11] D. M. Goldschmidt, *Algebraic Functions and Projective Curves (Graduate Texts in Mathematics)*. New York: Springer-Verlag, 2003, vol. 215.
[12] T. Høholdt, J. H. van Lint, and R. Pellikaan, *Algebraic Geometry Codes*. Amsterdam, The Netherlands: North-Holland, 1998, pp. 871–961.
[13] C. Kirfel and R. Pellikaan, "The minimum distance of codes in an array coming from telescopic semigroups," *IEEE Trans. Inform. Theory*, pt. 1, vol. 41, pp. 1720–1732, Nov. 1995.
[14] R. Pellikaan, H. Stichtenoth, and F. Torres, "Weierstrass semigroups in an asymptotically good tower of function fields," *Finite Fields Appl.*, vol. 4, no. 4, pp. 381–392, 1998.
[15] R. Pellikaan and F. Torres, "On Weierstrass semigroups and the redundancy of improved geometric goppa codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 2512–2519, Nov. 1999.
[16] O. Pretzel, *Codes and Algebraic Curves*. New York: Clarendon/Oxford Univ. Press, 1998.
[17] J. C. Rosales and M. B. Branco, "Irreducible numerical semigroups," *Pacific J. Math.*, vol. 209, no. 1, pp. 131–143, 2003.
[18] J. C. Rosales, P. A. García-Sánchez, J. I. García-García, and M. B. Branco, "Arf numerical semigroups," *J. Algebra*, to be published.
[19] H. Stichtenoth, "A note on Hermitian codes over GF (q^2)," *IEEE Trans. Inform. Theory*, pt. 2, vol. 34, pp. 1345–1348, Sept. 1988.
[20] ——, *Algebraic Function Fields and Codes*. Berlin, Germany: Springer-Verlag, 1993.
[21] K.-O. Stöhr and J. F. Voloch, "Weierstrass points and curves over finite fields," *Proc. London Math. Soc. (3)*, vol. 52, no. 1, pp. 1–19, 1986.

Permutation Arrays for Powerline Communication and Mutually Orthogonal Latin Squares

Charles J. Colbourn, Torleiv Kløve, *Fellow, IEEE*, and Alan C. H. Ling

***Abstract*—We develop a connection between permutation arrays that are used in powerline communication and well-studied combinatorial objects, mutually orthogonal latin squares (MOLS). From this connection, many new results on permutation arrays can be obtained.**

***Index Terms*—Doubly resolvable design, mutually orthogonal latin squares (MOLS), permutation array, permutation code, powerline communications.**

I. Introduction and Definitions

We consider permutations of the elements of some fixed set R with n elements. Let S_n denote the set of all $n!$ permutations. 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 subset is at least d. Some constructions for permutation arrays are given in [2], [7], [10]. We develop here a correspondence between these arrays and certain combinatorial objects. From this link, many constructions in [7], [10] are obtained.

Permutation arrays are of recent interest because of their application to data transmission over power lines (see, for example, [8], [9], [12]). Permutation arrays have also been applied in the design of block ciphers [5], and some of the constructions described here are outlined there in that setting. In the powerline application, the main idea is to vary the voltage by a small amount and use this variation to transmit signals. There are three main forms of noise which may affect the transmission:

- permanent narrow-band noise, which affects some frequency over a long period (e.g., noise from electrical equipment);
- impulse noise of short duration, which affects many frequencies; and
- white Gaussian noise (background noise).

In many traditional data transmission media (e.g., telephone lines and satellite communication) white Gaussian noise is the dominating

Manuscript received December 4, 2002; revised November 11, 2003. This work was supported by ARO under Grant DAAD19-01-1-0406 and by the Norwegian Research Council.
C. J. Colbourn is with the Department of Computer Science and Engineering, Arizona State University, Tempe, AZ 85287 USA (e-mail: colbourn@asu.edu).
T. Kløve is with the Department of Informatics, University of Bergen, HIB, N-5020 Bergen, Norway (e-mail: Torleiv.Klove@ii.uib.no).
A. C. H. Ling is with the Department of Computer Science, University of Vermont, Burlington, VT 05405 USA (e-mail: aling@emba.uvm.edu).
Communicated by K. Abdel-Ghaffar, Associate Editor for Coding Theory.
Digital Object Identifier 10.1109/TIT.2004.828150

kind of error affecting the system, but in this application the other two kinds of error are more important. In [8], [9], permutation arrays are used to correct errors for this type of transmission. The problem reduces to finding, for a given n and d, the maximum number of codewords in an (n, d) permutation array.

II. Equivalent Objects

We represent an (n, d) PA of size v on the elements of S_n as a $v \times n$ array

- each row is a permutation of the symbols of a set S of size n, and
- any two rows disagree in at least d columns.

The second condition is equivalent to requiring that any two distinct rows agree in at most $n-d$ columns; we write $\lambda = n - d$. Such a permutation array is then denoted by $\mathrm{B}(n, \lambda; v)$. For example, a $\mathrm{B}(4, 1; 6)$ is shown next

1	2	3	4
1	3	4	2
2	3	1	4
3	4	1	2
4	1	3	2
4	2	1	3

Let X be a set of cardinality v. A generalized Room square packing (GRSP) of *size* n and *index* λ defined on X is an $n \times n$ array F having the following properties:

- every cell of F contains a subset (possibly empty) of X;
- each symbol of X occurs once in each row and once in each column of F; and
- any two distinct symbols of X occur together in at most λ cells of F.

Denote such a GRSP by $\mathrm{T}(n, \lambda; v)$.

An (n, λ)-*packing* is a pair $(X, \mathcal{B})$ where

- X is a set of v elements;
- $\mathcal{B}$ is a collection of b subsets (called *blocks*) of X such that every pair of distinct elements occurs in at most λ blocks; and
- every element occurs in precisely n blocks.

A *resolution class* is a set of disjoint blocks in $\mathcal{B}$ whose union is X. A *resolution* of an (n, λ)-packing, $(X, \mathcal{B})$, is a partition of $\mathcal{B}$ into resolution classes $\mathcal{R} = \{R_1, R_2, \ldots, R_n\}$. A packing admitting at least one resolution is *resolvable*. Two resolutions of $(X, \mathcal{B})$, say $\mathcal{R}$ and $\mathcal{S}$, are *orthogonal* if each resolution class of $\mathcal{R}$ intersects every resolution class of $\mathcal{S}$ in at most one block. An (n, λ)-packing is *doubly resolvable* if it has two orthogonal resolutions. A doubly resolvable (n, λ)-packing of order v is denoted by $\mathrm{DR}\,(n, \lambda; v)$.

The next two constructions can be found in [6], and are included here for completeness.

Theorem 2.1: There exists a $\mathrm{DR}\,(n, \lambda; v)$ if and only if there exists a $\mathrm{T}(n, \lambda; v)$.

Proof: From a $\mathrm{T}(n, \lambda; v)$, an (n, λ) packing can be constructed by taking the cells in T as blocks. Two orthogonal resolutions can be obtained by taking the rows and columns as resolution classes. Conversely, if there exists a doubly resolvable (n, λ) packing, then a $\mathrm{T}(n, \lambda; v)$ can be constructed by using the n parallel classes in the two orthogonal resolutions to index rows and columns. □

Theorem 2.2: There exists a $\mathrm{T}(n, \lambda; v)$ if and only if there exists a $\mathrm{B}(n, \lambda; v)$.

Proof: Index the rows of the $\mathrm{B}(n, \lambda; v)$ from 1 to v. We construct an $n \times n$ array as follows. The symbol k appears in the (i, j) cell of $\mathrm{T}(n, \lambda, v)$ if and only if the (k, j) entry of $\mathrm{B}(n, \lambda, v)$ is i. Every element occurs exactly once in each row since each row is a permutation and, hence, contains each element once. Every element occurs exactly once in each column because each row is a permutation and, hence, maps each element to a unique element. Two points occur together in at most λ blocks in the $n \times n$ array since any two permutations agree in at most λ positions. □

A *latin square* of *side* n is an $n \times n$ array in which each cell contains a single element from an n-set S, such that each element occurs exactly once in each row and exactly once in each column. Two latin squares L and L' of the same order are *orthogonal* if $L(a, b) = L(c, d)$ and $L'(a, b) = L'(c, d)$, implies $a = c$ and $b = d$. An equivalent definition for orthogonality is as follows: Two latin squares of side n, $L = (a_{i,j})$ (on symbol set S), and $L' = (b_{i,j})$ (on symbol set S') are *orthogonal* if every element in $S \times S'$ occurs exactly once among the n^2 pairs $(a_{i,j}, b_{i,j}), 1 \le i, j \le n$. A set of latin squares $L_1, \ldots, L_m$ is *mutually orthogonal*, or a set of *MOLS*, if for every $1 \le i < j \le m$, L_i and L_j are orthogonal.

A *transversal design* of *order* or *group size* n, *block size* k, and *index* λ, denoted $\mathrm{TD}_\lambda(k, n)$, is a triple $(V, \mathcal{G}, \mathcal{B})$, where

- V is a set of kn elements;
- $\mathcal{G}$ is a partition of V into k classes (called *groups*), each of size n;
- $\mathcal{B}$ is a collection of k-subsets of V (called *blocks*);
- every unordered pair of elements from V is either contained in exactly one group, or is contained in exactly λ blocks, but not both.

When $\lambda = 1$, one writes simply $\mathrm{TD}(k, n)$.

A $\mathrm{TD}(k, n)$ is equivalent to the existence of $k-2$ mutually orthogonal latin squares of order n, and the various generalizations of transversal designs all have reasonably natural interpretations in that formulation. An *orthogonal array* $\mathrm{OA}(k, s)$ is a $k \times s^2$ array with entries from an s-set S having the property that in any two rows, each (ordered) pair of symbols from S occurs exactly once. A $\mathrm{TD}(k, n)$ is also equivalent to an $\mathrm{OA}(k, n)$.

Now we interpret the constructions in [7].

Let C be a PA over R of size M. Represent the PA as rows of an $M \times n$ array, which we also denote by C. The following terminology is introduced in [7].

- C is r-*bounded* if no element of R appears more than r times in any column of C.
- C is r-*balanced* if each element of R appears exactly r times in each column of C.
- C is r-*separable* if it is a disjoint union of r (n, n) PAs of size n.

C is r-bounded if and only if each block in the corresponding doubly resolvable packing has block size at most r. C is r-balanced if and only if each block in the corresponding doubly resolvable packing has block size exactly equal to r.

Lemma 2.3: An $(n, n-1)$ PA C with $M = rn$ permutations is r-separable if and only if there exists r MOLS of order n.

Proof: A set of r MOLS of order n is a $\mathrm{TD}(r+2, n)$; use elements of each of two groups to define a pair of orthogonal resolutions of the $\mathrm{TD}(r, n)$ obtained by deleting the two groups. This is a $\mathrm{T}(r, 1; n)$.

In the other direction, any (n, n) PA of size n is equivalent to a latin square of order n, as follows. When we construct the $n \times n$ square A from the (n, n) PA, each cell only has one symbol because if x, $y \in A(i, j)$, then $P(x, j) = i$ and $P(y, j) = i$, but then row x and row y agree in column j. Since each cell has one entry, we use $A(i, j)$

to denote the only element in the cell. If $A(i,j) = A(i,k) = x$, then $P(x,j) = P(x,k) = i$, but then row x is not a permutation. If $A(i,j) = A(k,j) = y$, then $P(y,j) = i$ and $P(y,j) = k$ so the permutation in the PA maps one element to two symbols.

Since C is r-separable, we can obtain r latin squares in this way. Next, we establish that these r squares are orthogonal. Suppose $A_a(i_1,j_1) = A_a(i_2,j_2) = x$ and $A_b(i_1,j_1) = A_b(i_2,j_2) = y$. Then $PA(x,j_1) = i_1$, $PA(x,j_2) = i_2$, $PA(y,j_1) = i_1$, and $PA(y,j_2) = i_2$. Then, if $j_1 \neq j_2$, rows x and y agree in two positions. If $j_1 = j_2$, then it must happen that $i_1 = i_2$; otherwise, the PA is not well defined. But this is impossible. □

Now Theorem 4 in [7] can be interpreted as follows.

Lemma 2.4: If there exists a doubly resolvable packing with block size at most r on n classes on $|C|$ points, and s MOLS of order m, then there exists a doubly resolvable packing with block size at most r with nm classes on $m|C|$ points.

The proof of this is a standard inflation (see [4]), since s MOLS of order m can be viewed as a doubly resolvable $\mathrm{TD}(s,m)$. There are many known constructions for MOLS and the bounds are widely known; see [1], [3], [4], and references therein.

We state the main application of MOLS to permutation arrays.

Theorem 2.5: If there exist s MOLS of order n, then there exists an s-separable $(n, n-1)$ permutation array of size sn.

Proof: Let the symbols in the tth latin square be $(t-1)n$ to $(t-1)n + n - 1$. We construct an $n \times n$ square with the (i,j) cell containing the k symbols from the (i,j) cell in each of the k latin squares. We establish that the constructed square is a $\mathrm{T}(n,1;kn)$. Each latin square uses n symbols, so the total number of symbols is kn. Each row and each column contains each symbol exactly once since the k squares are latin. Each pair of elements occurs at most once in a cell because the k squares are mutually orthogonal. Hence, there exists a $\mathrm{T}(n,1;kn)$. By Theorem 2.2, there exists a $\mathrm{B}(n,1;kn)$. The s latin squares employed yield the s-separability. □

For many values of n, Theorem 2.5 improves upon the result of [7] (equivalently, that obtained from Lemma 2.4). For $n = 10$, we obtain size $2 \cdot 10$ rather than $1 \cdot 10$; for $n = 12$, we find $5 \cdot 12$ rather than $2 \cdot 12$, and for $n = 14$ we find $3 \cdot 14$ rather than $1 \cdot 14$. De la Torre, Colbourn, and Ling [5] use this correspondence to find a $(40, 39)$ permutation array of size $7 \cdot 40$ rather than $4 \cdot 40$. The exact number of MOLS is not known for any $n \geq 10$ which is not a prime or a power of a prime; nevertheless, Theorem 2.5 tells us the *best* result that can be obtained for separable permutation arrays. Nevertheless, it happens that the largest $(n, n-1)$ permutation array can be much larger than the largest separable one; indeed, for $n = 6$ the largest separable $(6,5)$ permutation array contains only six permutations, but Kløve [11] has shown that the largest $(6,5)$ permutation array has size 18. Thus, in the construction of permutation arrays, Theorem 2.5 provides a useful construction but may not provide the largest permutation array.

REFERENCES

[1] R. J. R. Abel, A. E. Brouwer, C. J. Colbourn, and J. H. Dinitz, "Mutually orthogonal latin squares (MOLS)," in *CRC Handbook of Combinatorial Designs*, C. J. Colbourn and J. H. Dinitz, Eds. Boca Raton, FL: CRC, 1996, pp. 111–142.

[2] W. Chu, C. J. Colbourn, and P. Dukes, "Permutation codes for powerline communication," *Des., Codes, Cryptogr.*, to be published.

[3] C. J. Colbourn and J. H. Dinitz, "Making the MOLS table," in *Computational and Constructive Design Theory*, W. D. Wallis, Ed. Norwell, MA: Kluwer Academic, 1996, pp. 67–134.

[4] ——, "Mutually orthogonal latin squares: A brief survey of constructions," *J. Statist. Plann. Infer.*, vol. 95, pp. 9–48, 2001.

[5] D. R. de la Torre, C. J. Colbourn, and A. C. H. Ling, "An application of permutation arrays to block ciphers," *Cong. Numer.*, vol. 145, pp. 5–7, 2000.

[6] M. Deza and S. A. Vanstone, "Bounds for permutation arrays," *J. Statist. Plann. Infer.*, vol. 2, pp. 197–209, 1978.

[7] C. Ding, F.-W. Fu, T. Kløve, and V. W.-K. Wei, "Constructions of permutation arrays," *IEEE Tran. Inform. Theory*, vol. 48, pp. 977–980, Apr. 2002.

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

[9] A. J. H. Vinck, "Coded modulation for powerline communications," *AEÜ Int. J. Electron. Commun.*, vol. 54, pp. 45–49, Jan. 2000.

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

[11] ——, "Classification of permutation codes of length 6 and minimum distance 5," in *Proc. Int. Symp. Information Theory and Its Applications*, Honolulu, HI, Nov. 2000, pp. 465–468.

[12] N. Pavlidou, A. J. H. Vinck, J. Yazdani, and B. Honary, "Power line communications: State of the art and future trends," *IEEE Commun. Mag.*, vol. 41, pp. 34–40, Apr. 2003.

Upper Bounds on Separating Codes

Gérard D. Cohen, *Senior Member, IEEE,* and
Hans Georg Schaathun, *Member, IEEE*

***Abstract*—The combinatorial concept of separating systems has numerous applications, such as automata theory, digital fingerprinting, group testing, and hashing. In this correspondence, we derive upper bounds on the size of codes with various separating properties.**

***Index Terms*—Error-correcting codes, hashing, separating systems, superimposed codes.**

An $(n, M, d)_q$ code is a set of M words of length n over an alphabet of q elements, at minimum distance d apart. If the code forms a linear vector space of dimension $k = \log_q M$ over $\mathsf{GF}(q)$, then we call it an $[n, k, d]_q$ code. A (t, u)-separating code, also known as a (t, u)-separating system or (t, u)-SS, is defined as follows.

Definition 1: A pair (T, U) of disjoint sets of words is called a (t, u)-configuration if $\#T = t$ and $\#U = u$. Such a configuration is separated if there is a position i, such that every word of T is different from any word of U on position i.

A code is (t, u)-separating if every (t, u)-configuration is separated.

Manuscript received June 4, 2003; revised January 5. 2004. This work was supported in part by the Aurora Programme of the Norwegian Research Council and the Ministère des Affaires Etrangères of France. The work of H. G. Schaathun was also supported by the Norwegian Research Council under Grant 146874/420. The material in this correspondence was presented in part at the International Conference on Telecommunications in French Polynesia, February 2003.

G. D. Cohen is with the Department d'Informatique et Reseaux, Ecole Nationale Superieure des Télécommunications (ENST), 7-5013 Paris, France (e-mail: cohen@infres.enst.fr).

H. G. Schaathun is with the Department of Informatics, University of Bergen, N-5020 Bergen, Norway (e-mail: georg@ii.uib.no).

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

Digital Object Identifier 10.1109/TIT.2004.828140