Proposition 6: $\mathcal{C}_u$ is a constant-composition code with parameters of (1).

To prove the optimality of the constant-composition codes $\mathcal{C}_u$, we need to introduce one bound on constant-composition codes. Let $A_q(n, d, [w_0, w_1, \ldots, w_{q-1}])$ denote the maximum size of an $(n, M, d, [w_0, w_1, \ldots, w_{q-1}]; q)$ constant-composition code. Luo, Fu, Vinck, and Chen [3] developed the following bound for constant-composition codes.

Lemma 7: If $nd - n^2 + (w_0^2 + w_1^2 + \cdots + w_{q-1}^2) > 0$, then

$$A_q(n, d, [w_0, w_1, \ldots, w_{q-1}]) \leq \frac{nd}{nd - n^2 + \left(w_0^2 + w_1^2 + \cdots + w_{q-1}^2\right)}.$$

Proposition 8: The codes $\mathcal{C}_u$ are optimal with respect to the Luo–Fu–Vinck–Chen bound of Lemma 7.

Proof: It is straightforward to check that the condition of Lemma 7 is met, and the Luo–Fu–Vinck–Chen bound of Lemma 7 is achieved. □

IV. Concluding Remarks

In this correspondence, we constructed a family of optimal ternary constant-composition codes from a class of newly discovered perfect nonlinear functions. It would be interesting to find out if optimal constant-composition codes can be obtained directly from certain known classes of linear or nonlinear codes.

Acknowledgment

The authors wish to thank the referees for their comments and suggestions that much improved the presentation of this correspondence.

References

[1] M. Svanström, "Constructions of ternary constant-composition codes," *IEEE Trans. Inf. Theory*, vol. 46, no. 7, pp. 2644–2647, Nov. 2000.

[2] M. Svanström, P. R. J. Östergaard, and G. T. Bogdanova, "Bounds and constructions for ternary constant-composition codes," *IEEE Trans. Inf. Theory*, vol. 48, no. 1, pp. 101–111, Jan. 2002.

[3] Y. Luo, F.-W. Fu, A. J. H. Vinck, and W. Chen, "On constant composition codes over Z_q," *IEEE Trans. Inf. Theory*, vol. 49, no. 11, pp. 3010–3016, Nov. 2003.

[4] C. Carlet and C. Ding, "Highly nonlinear mappings," *J. Complexity*, vol. 20, no. 2, pp. 205–244, 2004.

[5] R. S. Coulter and R. W. Matthews, "Planar functions and planes of Lenz-Barlotti class II," *Des., Codes Cryptogr.*, vol. 10, pp. 167–184, 1997.

[6] C. Ding and J. Yuan, "A new family of skew Hadamard difference sets," *J. Comb. Theory A*, to be published.

[7] R. Lidl and H. Niederreiter, *Finite Fields*. Cambridge, U.K.: Cambridge Univ. Press, 1997.

Combinatorial Constructions of Optimal Constant-Composition Codes

Cunsheng Ding, *Senior Member, IEEE,* and Jianxing Yin

***Abstract*—Constant-composition codes (CCCs) are a special class of constant-weight codes. They include permutation codes as a subclass. In this correspondence, a link between CCCs and generalized double resolvable packing designs is developed, and used to construct several infinite series of optimal CCCs.**

***Index Terms*—Constant-composition codes (CCCs), constant-weight codes, generalized double resolvable packing designs.**

I. Introduction

We use the standard notations for codes as follows. Let Z_q denote the set $\{0, 1, \ldots, q-1\}$ (alphabet), and Z_q^n be the set of all n-tuples (*words*) over Z_q, where q is a positive integer. An $(n, M, d, w)_q$ *constant-weight code* (CWC) is a code $C \subset Z_q^n$ with size M and minimum Hamming distance d such that the Hamming weight of each codeword is w. An $(n, M, d, [w_0, w_1, \ldots, w_{q-1}])_q$ *constant-composition code* (CCC) is a code $C \subset Z_q^n$ with size M and minimum Hamming distance d such that in every codeword the element i appears exactly w_i times for every $i \in Z_q$. An $(n, M, d, [w_0, w_1, \ldots, w_{q-1}])_q$ CCC is called a *permutation code* if $n = q$ and $w_i = 1$ for all i. Hence, permutation codes are a special class of CWCs. Clearly, CCCs are a subclass of CWCs. A code is said to be *equidistant* if any two of its distinct codewords have the same Hamming distance.

We use $A_q(n, d, [w_0, w_1, \ldots, w_{q-1}])$ to denote the maximum size of an $(n, M, d, [w_0, w_1, \ldots, w_{q-1}])_q$ CCC. Recently, the following bound for CCCs was developed [18].

Lemma 1: If $nd - n^2 + (w_0^2 + w_1^2 + \cdots + w_{q-1}^2) > 0$, then

$$A_q(n, d, [w_0, w_1, \ldots, w_{q-1}]) \leq \frac{nd}{nd - n^2 + \left(w_0^2 + w_1^2 + \cdots + w_{q-1}^2\right)}.$$

The study of permutation codes goes back to at least 1965 [21]. In the 1970s, Blake [2]–[4], Deza and Vanstone [11], and Frankel and Deza [14] investigated permutation codes. Recently, advances on permutation codes have been made by Chu, Colbourn, and Dukes [7], Colbourn, Kløve, and Ling [10], Ding, Fu, Kløve, and Wei [12], and Fu and Kløve [15]. Nonbinary CCCs were studied already in the 1960s. Both algebraic and combinatorial constructions have been presented. For further information, the reader is referred to Bogdanova and Kapralov [6], Colbourn, Kløve, and Ling [10], Chu, Colbourn, and Dukes [8], [9], Ding, and Yin [13], Luo, Fu, Vink, and Chen [18], Semakov and Zinoviev [19], Semakov, Zinoviev, and Zaitsev [20], Svanström [23], Svanström, Östergård, and Bogdanova [24], and Zinoviev [25].

In this correspondence, we consider optimal CCCs meeting the upper bound of Lemma 1. In Section II, a link between CCCs and

Manuscript received January 14, 2005; revised June 25, 2005. This work was supported by the Research Grants Council of the Hong Kong Special Administration Region, Project HKUST6124/05E, and the Natural Science Foundation of China, Project NSFC 10371086.

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

J. Yin is with the Department of Mathematics, Suzhou University, Suzhou, 215006, China; (e-mail: jxyin@suda.edu.cn).

Communicated by C. Carlet, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2005.855612

generalized double resolvable packing designs is discussed. Combinatorial constructions of several infinite series of optimal CCCs are presented in Section III.

II. The Link Between CCCs and Generalized Double Packing Designs

Suppose that there exists a set X of v points and that from these a collection $\mathcal{A}$ of subsets, or *blocks*, is drawn. The ordered pair $(X, \mathcal{A})$ is called a *design* of order v. In design theory there are normally a number of additional rules imposed when the blocks are selected [1]. A design $(X, \mathcal{A})$ is referred to as a *packing design*, or a *packing* for short, of index λ if every pair of distinct points of X occurs in at most λ blocks in $\mathcal{A}$. Throughout this correspondence, we call such packing an $(n, \lambda; v)$-packing when every point of X appears in precisely n blocks. Here, there are no restrictions on the block sizes in an $(n, \lambda; v)$-packing and a block is allowed to have size 1. In the extreme case, where every pair of distinct points of the packing occurs in exactly its λ blocks, the packing is commonly termed a *pairwise balanced design* (PBD), and we write an $(n, \lambda; v)$-PBD instead of an $(n, \lambda; v)$-packing. Note that a PBD having blocks of the same size is known as a *balanced incomplete block design* (BIBD).

For an arbitrary design $(X, \mathcal{A})$, an *α-parallel class* is a set of blocks in $\mathcal{A}$ such that each point of X occurs in precisely its α blocks. It is simply called a *parallel class* whenever $\alpha = 1$. A *resolution* of a design is a partition of $\mathcal{A}$ into certain classes. A design is said to be *resolvable* if it admits at least one resolution so that each resolution class forms a parallel class. For more information on resolvable designs, the reader is referred to [16].

Resolvable designs have played an important role in coding theory. In 1968, Semakov and Zinoviev [19] showed that there is a one-to-one correspondence between resolvable BIBDs and certain equidistance CWCs. A generalization of this result was made by Bogdanova *et al.* [5], which can be applied to the broader class of resolvable PBDs. A combinatorial interpretation for permutation codes was given by Deza and Vanstone [11] in 1978. This idea was recently further developed by Colbourn *et al.* [10]. The designs they employed are "*double resolvable packings*," which are widely used in design theory (see, for example, Hartman and Phelps [17]). A design is termed *double resolvable* if it admits two resolutions into parallel classes in which any two parallel classes from the two distinct resolutions intersect in at most one block. To extend their idea to constructing CCCs, we define the notion of *generalized double resolvable designs* in the following.

Consider a design $(X, \mathcal{A})$. Suppose that it admits two resolutions. The first is a partition of $\mathcal{A}$ into u classes: An α_0-parallel class, ..., an α_{u-1}-parallel class in turn, which we call an $[\alpha_0, \alpha_1, \ldots, \alpha_{u-1}]$-resolution. The second is a $[\beta_0, \beta_1, \ldots, \beta_{w-1}]$-resolution whose w resolution classes constitute a β_0-parallel class, ..., a β_{w-1}-parallel class in turn. If each α_i-parallel class $(0 \le i \le u-1)$ intersects every β_j-parallel class $(0 \le j \le w-1)$ in at most one block, then we say that this design is $([\alpha_0, \alpha_1, \ldots, \alpha_{u-1}], [\beta_0, \beta_1, \ldots, \beta_{w-1}])$-*double resolvable*.

We now consider a $([1, 1, \ldots, 1], [\lambda_0, \lambda_1, \ldots, \lambda_{q-1}])$-double resolvable $(n, \lambda; v)$-packing, $(X, \mathcal{A})$. As every point appears in precisely n blocks of the packing, there must be exactly n parallel classes in the $[1, 1, \ldots, 1]$-resolution, and $n = \sum_{j=0}^{q-1} \lambda_j$. So, we are always able to arrange the blocks of such a packing into a $q \times n$ array $\mathcal{R}$ in such a way that:

1) the rows of $\mathcal{R}$ are labeled $0, 1, \ldots, q-1$ corresponding to the λ_i-parallel classes of its $[\lambda_0, \lambda_1, \ldots, \lambda_{q-1}]$-resolution;
2) the columns of $\mathcal{R}$ are labeled by $1, 2, \ldots, n$ corresponding to the n parallel classes of its $[1, 1, \ldots, 1]$-resolution;
3) the intersection of row i and column j is occupied by the common block of the λ_i-parallel class and the jth parallel class, or empty if the λ_i-parallel class and the jth parallel class do not share any common block.

Employing generalized double resolvable packings, we have the following combinatorial characterization of CCCs, which is a generalization of related results in [5], [10], [11], [19].

Theorem 2: A $([1, 1, \ldots, 1], [\lambda_0, \lambda_1, \ldots, \lambda_{q-1}])$-double resolvable $(n, \lambda; v)$-packing exists if and only if an $(n, M, d, [w_0, w_1, \ldots, w_{q-1}])_q$ CCC exists, where

$$M = v, n = \sum_{j=0}^{q-1} \lambda_j, d = n - \lambda$$

and $\lambda_j = w_j$ for $0 \le j \le q-1$.

Proof: Let $(X, \mathcal{A})$ be a $([1, 1, \ldots, 1], [\lambda_0, \lambda_1, \ldots, \lambda_{q-1}])$-double resolvable $(n, \lambda; v)$-packing. Without loss of generality, we may take its point set to be Z_v. The blocks of $\mathcal{A}$ are arranged as a $q \times n$ array $\mathcal{R}$, as indicated above. We then form a $v \times n$ array C over Z_q from $\mathcal{R}$ in such a way that its (i, j) entry $(i \in Z_v, 1 \le j \le n)$ is $u \in Z_q$ if and only if the point i appears in the block at the intersection of row u and column j of $\mathcal{R}$. Now, since any pair of distinct points of Z_v occurs in at most λ blocks of the packing, any two rows agree in at most λ positions, or equivalently, any two rows disagree in at least $n - \lambda$ positions. In addition, since the blocks in each row i of $\mathcal{R}$ constitute a λ_i-parallel class of the packing, the symbol $i \in Z_q$ appears in every row of C precisely w_i $(=\lambda_i)$ times. Finally, since the blocks in each column of $\mathcal{R}$ constitute a parallel class of the packing, any cell of C is occupied by a unique element of Z_q. Therefore, C represents an $(n, M, d, [w_0, w_1, \ldots, w_{q-1}])_q$ CCC.

Conversely, given an $(n, M, d, [w_0, w_1, \ldots, w_{q-1}])_q$ CCC, C. We represent it as an $M \times n$ array over Z_q whose rows consist of the M codewords, and then label its rows from 0 to $v-1$. It follows that the array $\mathcal{R}$ corresponding to the $([1, 1, \ldots, 1], [\lambda_0, \lambda_1, \ldots, \lambda_{q-1}])$-double resolvable $(n, \lambda; v)$-packing over Z_v can be produced by reversing the above process. □

Setting $q = n$ and $\lambda_0 = \lambda_1 = \ldots, \lambda_{q-1} = 1$ in Theorem 2, we obtain the following corollary [10, Theorem 2.2] on permutation codes. Hence Theorem 2 about CCCs is a generalization of Theorem 2.2 on permutation codes in [10].

Corollary 3: [10] The existence of a double resolvable $(n, \lambda; v)$-packing is equivalent to that of a permutation code of length n, size v, and Hamming distance $n - \lambda$.

Theorem 2 suggests that various recursive and direct construction techniques in design theory might be utilized to yield CCCs. In the next section, we will take advantage of this fact to establish a number of combinatorial constructions of optimal CCCs.

III. The Constructions of Optimal CCCs

We now present our constructions of CCCs. Since we are mainly concerned with optimal $(n, M, d, [\lambda_0, \ldots, \lambda_{q-1}])_q$ CCCs meeting the bound in Lemma 1, the constraints that

$$nd - n^2 + (\lambda_0^2 + \lambda_1^2 + \cdots + \lambda_{q-1}^2) > 0$$

and

$$(nd - n^2 + \lambda_0^2 + \lambda_1^2 + \cdots + \lambda_{q-1}^2) \mid nd$$

are always assumed for any $(n, M, d, [\lambda_0, \ldots, \lambda_{q-1}])_q$ CCC throughout this section. By Theorem 2, there is a one-to-one correspondence between double resolvable packings and CCCs. We call a $([1, 1, \ldots, 1], [\lambda_0, \lambda_1, \ldots, \lambda_{q-1}])$-double resolvable $(n, \lambda; v)$-packing optimal if its corresponding

$$(n, M, n - \lambda, [\lambda_0, \lambda_1, \ldots, \lambda_{q-1}])_q$$

CCC is optimal, namely

$$v = M = \frac{n(n-\lambda)}{\lambda_0^2 + \lambda_1^2 + \cdots + \lambda_{q-1}^2 - \lambda n}.$$

For convenience, we adopt the following notations:

$$\begin{aligned} d &:= n - \lambda, \\ N &:= nd - n^2 + \sum_{0 \le i \le q-1} \lambda_i^2 \left(= \left[\sum_{0 \le i \le q-1} \lambda_i^2 \right] - \lambda n \right) \\ \bar{\lambda} &:= \gcd\{\lambda_i : i = 0, 1, \ldots, q-1\} \\ \bar{N} &:= N/\bar{\lambda} \\ \bar{n} &:= n/\bar{\lambda}. \end{aligned}$$

The upper bound in Lemma 1 then is $\bar{n}d/\bar{N}$ $(= \bar{n}(n-\lambda)/\bar{N})$, since both $n = \sum_{0 \le i \le q-1} \lambda_i$ and N are obviously divisible by $\bar{\lambda}$.

With the observations above, we are now able to explain the feature of optimal $(n, M, d, [\lambda_0, \lambda_1, \ldots, \lambda_{q-1}])_q$ CCCs meeting the bound of Lemma 1 in the language of designs, which is the basis of our combinatorial constructions of optimal CCCs. This is done with the following lemma whose proof is ommitted here.

Lemma 4: A $([1, 1, \ldots, 1], [\lambda_0, \lambda_1, \ldots, \lambda_{q-1}])$-double resolvable $(n, \lambda; v)$-packing is optimal if and only if it is a $([1, 1, \ldots, 1], [\lambda_0, \lambda_1, \ldots, \lambda_{q-1}])$-double resolvable $(n, \lambda; v)$-PBD which satisfies the following properties.

1) For any i $(0 \le i \le q-1)$, all blocks in its λ_i-parallel class have the same size given by $(n-\lambda)\lambda_i/N$, and hence, $(n-\lambda)\lambda_i/N$ must be an integer.
2) $\bar{N} \mid (n-\lambda)$, and hence, $v = \bar{n}(n-\lambda)/\bar{N}$ is a multiple of $\bar{n}$.

Lemma 4 tells us that for given parameters $n, d = n-\lambda$ and constant composition $[\lambda_0, \lambda_1, \ldots, \lambda_{q-1}]$ with $N \mid n(n-\lambda)$, an optimal CCC meeting the bound in Lemma 1 is equidistant (as remarked in [18]), and the distribution of values in a coordinate is (up to permutation) uniquely given by $\frac{(n-\lambda)\lambda_i}{N}$. As an immediate consequence of Lemma 4, we see that for some parameters q, n, λ, and $\lambda_i's$, even if $N | n(n-\lambda)$, an $(n, M, n-\lambda, [\lambda_0, \lambda_1, \ldots, \lambda_{q-1}])_q$ CCC cannot attain the upper bound in Lemma 1. For example, if a $(21, M, 16, [7, 7, 7])_3$ CCC exists, then its size M must be less than the upper bound $21 \cdot 16/N = 8$. Otherwise, if $M = 8$, then $d/\bar{N} = 8/3$ is an integer by Lemma 4, a contradiction. We state this in the following lemma using the notations above.

Lemma 5: If $N > 0, N | nd$, and d is not divisible by $\bar{N}$, then

$$A_q(n, d, [\lambda_0, \lambda_1, \ldots, \lambda_{q-1}]) \le \frac{nd}{N} - 1.$$

The feature of an optimal packing explored in Lemma 4 translates an optimal $(n, M, n-\lambda, [\lambda_0, \lambda_1, \ldots, \lambda_{q-1}])_q$ CCC into a $([1, 1, \ldots, 1], [\lambda_0, \lambda_1, \ldots, \lambda_{q-1}])$-double resolvable $(n, \lambda; v)$-PBD with two prescribed properties. This leads us to construct optimal CCCs by way of the difference method in design theory. To do this, we need the notion of difference families defined as follows.

Let G be an Abelian group of order v whose operation is written additively, as usual. Let $\mathcal{F} = \{D_j : 0 \le j \le t-1\}$ be a family of subsets (called *base blocks*) of G. We say that $\mathcal{F}$ is a *difference family* (DF) if any nonzero element of G occurs exactly λ times in the difference list (multiset) of $\mathcal{F}$, $\Delta\mathcal{F} = \biguplus_{0 \le j \le t-1} \Delta D_j$, where

$$\Delta D_j = \{a - b : a, b \in D_j \text{ and } a \ne b\}$$

which is the difference list (multiset) of $D_j (0 \le j \le t-1)$. Here we use the notation "$\biguplus_{i \in I} T_i$" to denote the formal sum of $|I|$ multisets $T_i (i \in I)$. It is identified with the usual union of sets $\bigcup_{i \in I} T_i$ if and only if T_i is a set for any $i \in I$. In the sequel, we call $\mathcal{F}$ a $(v, [|D_0|, |D_1|, \ldots |D_{t-1}|], \lambda)$-DF and a (v, K, λ)-DF interchangeably, where K is the set of sizes of the base blocks. The above definition is equivalent to saying that if $\mathcal{F}$ is a $(v, [|D_0|, |D_1|, \ldots |D_{t-1}|], \lambda)$-DF, then the difference function

$$d_{\mathcal{F}}(g) = \sum_{D \in \mathcal{F}} |(D+g) \cap D| = \lambda$$

for any nonzero element g of G. When $\mathcal{F} = \{D\}$, then one often writes D for $\mathcal{F}$ and calls it a *difference set* (DS) or a $(v, |D|, \lambda)$-DS. If the base blocks of a $(v, [|D_0|, |D_1|, \ldots |D_{t-1}|], \lambda)$-DF are mutually disjoint, then it is said to be *disjoint* and denoted by $(v, [|D_0|, |D_1|, \ldots |D_{t-1}|], \lambda)$-DDF. If the base blocks of a $(v, [|D_0|, |D_1|, \ldots |D_{t-1}|], \lambda)$-DF form a partition of G, then it is said to be *partitioned* and denoted by $(v, [|D_0|, |D_1|, \ldots |D_{t-1}|], \lambda)$-PDF.

We remark that the sizes of base blocks in a DF are often required to be greater than 1 in literature. However, block size 1 is allowed in our definition. It is clear that $\Delta D = \emptyset$ for any base block D of cardinality 1.

With the preparations above, we are now ready to describe our combinatorial construction of optimal CCCs. Based on Lemma 4, our constructions split naturally into two cases depending whether $N | (n-\lambda)$ or not. We begin with the case where $N | (n-\lambda)$. In this case, we may write $t = \frac{n-\lambda}{N}$. Then the PBD corresponding to an optimal CCC has order $v = tn$, block sizes $t\lambda_i$ $(0 \le i \le q-1)$, and index λ by Lemma 4. The following construction works for the case $N = n - \lambda$ (and hence, $t = 1$ and $n = v$).

Construction 6: If a $(v, [\lambda_0, \lambda_1, \ldots, \lambda_{q-1}], \lambda)$-PDF exists, then there is an optimal $(n, n, n-\lambda, [\lambda_0, \lambda_1, \ldots, \lambda_{q-1}])_q$ CCC meeting the bound of Lemma 1.

Proof: Suppose that $\mathcal{F} = \{D_j : 0 \le j \le q-1\}$ is the given $(v, [\lambda_0, \lambda_1, \ldots, \lambda_{q-1}]), \lambda)$-PDF over an Abelian group G. Then, as is usually done (see, for example, [1]), we get a PBD $(G, \mathcal{A})$ with block sizes λ_i $(i = 0, 1, \ldots, q-1)$, where

$$\mathcal{A} = \{D_j + g : 0 \le j \le q-1, g \in G\}$$

and $D + g = \{d_i + g : 0 \le i \le k\}$ if $D = \{d_i : 0 \le i \le k\} \in \mathcal{F}$.

It is easily seen that $\mathcal{A}_g = \{D_j + g : 0 \le j \le q-1\}$, $g \in G$, constitute a $[1, 1, \ldots, 1]$-resolution of this PBD into $n\,(=v)$ parallel classes, while $\mathcal{B}_j = \{D_j + g : g \in G\}$, $0 \le j \le q-1$, form a $[\lambda_0, \lambda_1, \ldots, \lambda_{q-1}]$-resolution. All blocks in the λ_j-parallel class have the same size λ_j for any j $(0 \le j \le q-1)$. The assertion then follows from Lemma 4. □

Without giving a proof, we state that one can apply Construction 6 and Lemma 4 to obtain optimal CCCs with the following parameters which meet the bound of Lemma 1.

1) An $(n, n, n-q, [2q-1, 2, \ldots, 2])_q$ CCC, where $n = 4q-3$ is any prime power.
2) An $(n, n, n-k+1, [k, k, \ldots, k, 1])_q$ CCC, where $q = \frac{n+k-1}{k}$, k is a positive integer, n is a prime power, and $n - 1 \equiv 0 \pmod k$.
3) An $(n, n, n - \frac{k-1}{2}, [k, k, \ldots, k, 1, 1, \ldots, 1])_q$ CCC, where k is an odd integer, n is a prime power, $n - 1 \equiv 0 \pmod{2k}$, $q = \frac{n-1}{2k} + \frac{n+1}{2}$, and the value of k occurs $\frac{n-1}{2k}$ times.
4) A $(q(q+1), q^2, q^2, [q+1, q+1, \ldots, q+1])_q$ CCC, where q is a prime power.

ACKNOWLEDGMENT

The authors wish to thank the reviewers for their comments and suggestions that much improved this correspondence.

REFERENCES

[1] T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*. Cambridge, U.K.: Cambridge Univ. Press, 1999.

[2] I. F. Blake, "Permutation codes for discrete channels," *IEEE Trans. Inf. Theory*, vol. IT-20, no. 1, pp. 138–140, Jan. 1974.
[3] ——, "Configuration matrices of group codes," *IEEE Trans. Inf. Theory*, vol. IT-20, no. 1, pp. 95–100, Jan. 1974.
[4] ——, "Coding with permutations," *Inf. Control*, vol. 43, pp. 1–19, 1979.
[5] G. T. Bogdanova, A. E. Brouwer, S. N. Kapralov, and P. R. J. Östergård, "Error-correcting codes over an alphabet of four elements," *Des., Codes, Cryptogr.*, vol. 32, pp. 51–64, 2004.
[6] G. T. Bogdanova and S. N. Kapralov, "Enumeration of optimal ternary constant-composition codes," *Probl. Inf. Transm.*, vol. 39, no. 4, pp. 346–351, 2003.
[7] W. Chu, C. J. Colbourn, and P. Dukes, "Constructions for permutation codes in powerline communications," *Des., Codes, Cryptogr.*, vol. 32, pp. 51–64, 2004.
[8] ——, "On Constant Composition Codes," preprint.
[9] ——, "Tables for constant composition codes," *J. Comb. Math. and Comb. Comput.*, to be published.
[10] C. J. Colbourn, T. Kløve, and A. C. H. Ling, "Permutation arrays for powerline communication and mutually orthogonal Latin squares," *IEEE Trans. Inf. Theory*, vol. 50, no. 6, pp. 1289–1291, Jun. 2004.
[11] M. Deza and S. A. Vanstone, "Bounds for permutation arrays," *J. Statist. Planning and Inference*, vol. 2, pp. 197–209, 1978.
[12] C. Ding, F. W. Fu, T. Kløve, and V. W. K. Wei, "Constructions of permutation arrays," *IEEE Trans. Inf. Theory*, vol. 48, no. 4, pp. 977–980, Apr. 2002.
[13] C. Ding and J. Yin, "Algebraic constructions of constant composite codes," *IEEE Trans. Inf. Theory*, vol. 51, no. 4, pp. 1585–1589, Apr. 2005.
[14] P. Frankl and M. Deza, "On the maximum number of permutations with given maximal or minimal distance," *J. Comb. Theory A*, vol. 22, pp. 352–360, 1977.
[15] F. W. Fu and T. Kløve, "Two constructions of permutation arrays," *IEEE Trans. Inf. Theory*, vol. 50, no. 5, pp. 881–883, May 2004.
[16] S. Furino, Y. Miao, and J. Yin, *Frames and Resolvable Designs*. Boca Raton, FL: CRC, 1996.
[17] A. Hartman and K. T. Phelps, "Steiner quadruple systems," in *Contemporary Design Theory*, J. H. Dinitz and D. R. Stinson, Eds. New York: Wiley, 1992, pp. 205–240.
[18] Y. Luo, F.-W. Fu, A. J. Han Vinck, and W. Chen, "On constant composition codes over Z_q," *IEEE Trans. Inf. Theory*, vol. 49, no. 11, pp. 3010–3016, Nov. 2003.
[19] N. V. Semakov and V. A. Zinoviev, "Equidistant q-ary codes with maximal distance and resolvable balanced incomplete block designs," *Probl. Inf. Transm.*, vol. 4, no. 2, pp. 1–7, 1968.
[20] N. V. Semakov, V. A. Zinoviev, and G. V. Zaitsev, "A class of maximal equidistant codes," *Probl. Inf. Transm.*, vol. 5, no. 2, pp. 65–68, 1969.
[21] D. Slepian, "Permutation modulation," *Proc. IEEE*, vol. 53, no. 3, pp. 228–236, Mar. 1965.
[22] T. Storer, *Cyclotomy and Difference Sets*. Chicago, IL: Markhan, 1967.
[23] M. Svanström, "Construction of ternary constant-composition codes with weight three," *IEEE Trans. Inf. Theory*, vol. 46, no. Nov., pp. 2644–2647, 2000.
[24] M. Svanström, P. R. J. Östergård, and G. T. Bogdanova, "Bounds and constructions for ternary constant-composition codes," *IEEE Trans. Inf. Theory*, vol. 48, no. 1, pp. 101–111, Jan. 2002.
[25] V. A. Zinoviev, "Cascade equal-weight codes and maximal packings," *Probl. Control and Inf. Theory*, vol. 12, no. 1, pp. 3–10, 1983.
[26] R. M. Wilson, "Cyclotomy and difference families in elementary Abelian groups," *J. Number Theory*, vol. 4, pp. 17–47, 1972.

A Construction of Binary Constant-Weight Codes From Algebraic Curves Over Finite Fields

Chaoping Xing and Jie Ling

***Abstract*—By employing the narrow ray class groups of algebraic curves, we give a construction of constant weight codes. This construction is a generalization of the one proposed by Xing. It turns out that this generalization gives an improvement on the lower bound of binary constant codes in the earlier work of Xing, while the latter one improves an earlier result of Graham and Sloane.**

***Index Terms*—Constant codes, curves, maps, ray class groups.**

I. Introduction

Binary constant-weight codes are of great importance due to both practical applications and theoretic interests. These codes have attracted the attention of many researchers through the last few decades. The reader may refer to [1] for a survey on this topic. Many constructions of binary constant-weight codes have been proposed. Among these constructions, only a few make use of algebraic tools. In [2], group structures are used to obtain a class of binary constant-weight codes and a lower bound on the size of binary constant-weight codes for given length, minimum distance, and weight is derived. This lower bound is improved slightly by Xing [9] using residue rings of polynomials. In this correspondence, we generalize the result of [9] from the projective line (i.e., polynomials) to arbitrary curves. It turns out that further improvements can be obtained. We illustrate our improvement using examples of curves with small genus.

In Section II, we introduce the narrow ray class group of algebraic curves and related background. The main construction is presented in Section III and some examples of using curves of small genus are used to illustrate our improvement on the bound given in [9].

II. Narrow Ray Class Group

Before proceeding to our construction in the next section, we briefly introduce narrow ray class group of algebraic curves. For the detailed result, the reader may refer to [6] and [3].

When we speak of an algebraic curve $\mathcal{X}$ over the finite field $\mathbb{F}_q$, we always mean a smooth, projective and absolutely irreducible algebraic curve defined over $\mathbb{F}_q$, simply denoted by $\mathcal{X}/\mathbb{F}_q$.

Let us fix some notations that are used for the entire paper.

- $g(\mathcal{X})$—the genus of $\mathcal{X}/\mathbb{F}_q$;
- $N(\mathcal{X})$—the number of $\mathbb{F}_q$-rational points of $\mathcal{X}/\mathbb{F}_q$;
- $\mathbb{F}_q(\mathcal{X})$—the function field of $\mathcal{X}/\mathbb{F}_q$;
- ν_P—the normalized discrete valuation with respect to a place P of $\mathbb{F}_q(\mathcal{X})$;
- $\mathrm{Cl}(\mathcal{X})$—divisor class group of degree zero of $\mathcal{X}/\mathbb{F}_q$;
- $h(\mathcal{X})$—the divisor class number, i.e., the cardinality of $\mathrm{Cl}(\mathcal{X})$.

Manuscript received March 7, 2005; revised June 19, 2005. The work was supported in part under a grant from ARF.

C. Xing is with the Department of Mathematics, National University of Singapore, 117543 Singapore, Republic of Singapore (e-mail: matxcp@nus.edu.sg).

J. Ling is with the Department of Mathematics, University of Science and Technology of China, Hefei, Anhui 230026, China (e-mail: mathlingn@ustc.edu).

Communicated by M. Sudan, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2005.855608