[6] G. K. Huth and C. L. Weber, "Minimum weight convolutional codewords of finite length," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 243–246, Mar. 1976.
[7] I. L. Traiger and A. Gill, "On an asymptotic optimization problem in finite directed weighted graphs," *Inform. Contr.*, vol. 13, pp. 527–533, Mar. 1968.
[8] R. Jordan, V. Pavlouchkov, and V. V. Zyablov, "Maximum slope convolutional codes," *IEEE Trans. Inform. Theory*, submitted for publication.
[9] F. Hemmati and D. J. Costello, Jr., "Asymptotically catastrophic convolutional codes," *IEEE Trans. Inform. Theory*, vol. IT-26, pp. 298–304, May 1980.
[10] M. F. Hole and K. J. Hole, "Tight bounds on the minimum average weight per branch for rate $(N-1)/N$ convolutional codes," *IEEE Trans. Inform. Theory*, vol. 43, pp. 1301–1305, July 1997.
[11] K. J. Hole, "A note on asymptotically catastrophic convolutional codes of rate $(n-1/n)$," *IEEE Trans. Commun.*, vol. 45, pp. 1014–1016, Sept. 1997.
[12] R. Jordan, J. Freudenberger, V. Pavlouchkov, M. Bossert, and V. V. Zyablov, "Optimum slope convolutional codes," in *Proc. IEEE Int. Symp. Information Theory*, Sorrento, Italy, June 25–30, 2000, p. 95.
[13] G. Solomon and H. C. A. van Tilborg, "A connection between block and convolutional codes," *SIAM J. Appl. Math.*, vol. 37, pp. 358–369, 1979.
[14] I. E. Bocharova, R. Johannesson, B. D. Kudryashov, and P. Ståhl, "Tailbiting codes: Bounds and search results," *IEEE Trans. Inform. Theory*, vol. 48, pp. 137–148, Jan. 2002.
[15] M. Handlery, S. Höst, R. Johannesson, and V. V. Zyablov, "A distance measure tailored to tailbiting codes," *Probl. Inform. Transm. (Probl. Pered. Inform.)*, submitted for publication.
[16] A. E. Brouwer and T. Verhoeff, "An updated table of minimum-distance bounds for binary linear codes," *IEEE Trans. Inform. Theory*, vol. 39, pp. 662–677, Mar. 1993. [Online] Available : http://www.win.tue.nl/~aeb/voorlincod.html.
[17] S. Litsyn, E. M. Rains, and N. J. A. Sloane. Table of nonlinear binary codes. [Online]. Available: http://www.research.att.com/~njas/codes/And/index.html.
[18] E. R. Berlekamp, *Algebraic Coding Theory*, revised ed. Laguna Hills, CA: Aegean Park, 1984.
[19] S. W. Golomb, *Shift Register Sequences*, revised ed. Laguna Hills, CA: Aegean Park, 1982.
[20] W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes*, 2nd ed. Cambridge/MA, London/ U.K.: MIT Press, 1972.
[21] T. A. Gulliver and V. K. Bhargava, "Some best rate $1/p$ and rate $(p-1)/p$ systematic quasi-cyclic codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 552–555, May 1991.
[22] P. Heijnen, H. van Tilborg, T. Verhoeff, and S. Weijs, "Some new binary, quasi-cyclic codes," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1994–1996, Sept. 1998.
[23] Z. Chen, "New results on binary quasi-cyclic codes," in *Proc. IEEE Int. Symp. Information Theory*, Sorrento, Italy, June 25–30, 2000, p. 197, [Online]. Available: http://www.tek.hcr.se/~chen/research/codes..
[24] M. Karlin, "Decoding of circulant codes," *IEEE Trans. Inform. Theory*, vol. IT-16, pp. 797–802, Nov. 1970.
[25] P. Heijnen and H. van Tilborg, "The decoding of binary quasi-cyclic codes," in *Communication and Coding*, M. Darnell and B. Honary, Eds. London, U.K.: Research Studies/Wiley, 1998, pp. 146–159.
[26] J. H. Ma and J. K. Wolf, "On tail biting convolutional codes," *IEEE Trans. Commun.*, vol. COM-34, pp. 104–111, Feb. 1986.
[27] A. R. Calderbank, G. D. Forney, Jr., and A. Vardy, "Minimal tail-biting trellises: The golay code and more," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1435–1455, July 1999.

On Binary 1-Perfect Additive Codes: Some Structural Properties

Kevin T. Phelps and Josep Rifà, *Member, IEEE*

***Abstract*—The rank and kernel of 1-perfect additive codes is determined. Additive codes could be seen as translation-invariant propelinear codes and, in this correspondence, a characterization of propelinear codes as codes having a regular subgroup of the full group of isometries of the code is established. A characterization of the automorphism group of a 1-perfect additive code is given and also the cardinality of this group is computed. Finally, an efficiently computable characterization of the Steiner triple systems associated with a 1-perfect binary additive code is also established.**

***Index Terms*—Additive codes, automorphism group, kernel, 1-perfect codes, rank.**

I. Introduction

The *(Hamming) weight* $W(v)$ of a vector $v \in \mathbb{Z}_2^n$ is the number of nonzero coordinates of v. We define the *(Hamming) distance* between two vectors $v,\ u \in \mathbb{Z}_2^n$ as $d(v,\ u) = W(v+u)$.

A *(binary) code* of length n is a subset of $\mathbb{Z}_2^n$. If this subset is a linear subspace, then the code is *linear*. If C is a code, then its elements are called *codewords*.

A *perfect single error-correcting code* C of length $n \geq 3$ is a subset of $\mathbb{Z}_2^n$ such that all the vectors in $\mathbb{Z}_2^n$ are within distance 1 from a codeword and the distance between two codewords is at least 3. A perfect single error-correcting code is said to be a 1-*perfect code*. For any $n = 2^t - 1\ (t > 1)$, there exists exactly one 1-perfect linear code of length n, up to isomorphism, which is the well-known *Hamming code*.

Define $C^{\perp}$ as the dual of the span of C and the kernel of code C as $K = \{a \in C | a + C = C\}$.

The Gray map between $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4$ transforms $(0,\ 0)$ into 0, $(1,\ 0)$ into 1, $(1,\ 1)$ into 2, and $(0,\ 1)$ into 3, so using this map we can see the elements in $\mathbb{Z}_2^n$ as elements in $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta}$, where $n = \alpha + 2\beta$. Throughout this correspondence, we will distinguish between $\mathbb{Z}_2^n$, n copies of $\mathbb{Z}_2$, which gives us the elementary Abelian group and $\mathbb{F}^n$, which is also n copies of $\mathbb{Z}_2$ but with the Abelian structure given by $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta}$, where $n = \alpha + 2\beta$ and using the Gray map to convert the elements in $\mathbb{Z}_4$ to elements in $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Additive codes (see [5]) can be seen as a generalization of the classical linear codes over a field. In the binary case, they are Abelian subgroups of $\mathbb{F}^n = \mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta}\ (n = \alpha + 2\beta)$. It is well known (see [3]) that any 1-perfect binary additive code is equivalent to a 1-perfect translation invariant propelinear code, so throughout this correspondence we will use both concepts interchangeably.

An *isometry* of a binary code is a distance preserving 1–1 mapping $\phi\colon\ C \rightarrow C$. An isometry ϕ of $\mathbb{Z}_2^n$ can always be represented by a translation plus a coordinate permutation, i.e., $\phi(y) = x + \pi(y)$. The isometries of a code form a group, $\mathrm{Iso}\,(C)$, which has sometimes been called the automorphism group of the code. In this correspondence, will

Manuscript received November 26, 2001; revised May 10, 2002. This work was supported in part by Spanish CICYT under Grants TIC00-0232-P4-02, TIC2000-0739-c04-01 and by Catalan DURSI under Grants 2001SGR 00219 and PIV2000-10.

K. T. Phelps is with the Department of Discrete and Statistical Sciences, Auburn University, Auburn, AL 36849-5307 USA (e-mail: phelpkt@dms.auburn.edu).

J. Rifà is with the Computer Sciences Department, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain (e-mail: josep.rifa@uab.es).

Communicated by P. Solé, Associate Editor for Coding Theory.

Publisher Item Identifier 10.1109/TIT.2002.801474.

refer to the group of coordinate permutations $\pi\colon C \to C$ as $\mathrm{Aut}\,(C)$, the automorphism group of the code.

The correspondence is organized as follows. In Section II, we give some basic properties about the automorphism in a binary code. In Section III, we give two characterizations of propelinear codes by using the automorphism group of the code and also by using the minimum-distance graph associated to it. In Section IV, we introduce the automorphism group $\mathrm{Aut}_P(C)$ of a 1-perfect additive code taking into account the automorphisms which are also group morphisms for the propelinear operation and we compute both the cardinality of $\mathrm{Aut}_P(C)$ and of $\mathrm{Aut}\,(C)$. In Section V, we compute the kernel and rank for all the binary 1-perfect additive codes and, finally, in Section VI, we characterize in an efficiently computable way the Steiner triple system associated with a binary 1-perfect additive code.

II. Preliminaries

Let C be a binary, not necessarily linear code of length n. We will assume that the vector with all the coordinates zeros is in C. Let $\mathcal{S}_n$ denote the symmetric group of permutations of the set $\{1, 2, \ldots, n\}$. Let $\pi \in \mathcal{S}_n$. Then for any vector $v = (v_1, \ldots, v_n) \in \mathbb{Z}_2^n$, we write $\pi(v)$ to denote the vector $(v_{\pi^{-1}(1)}, \ldots, v_{\pi^{-1}(n)})$.

Lemma II.1: If $\phi(y) = x + \pi(y)$ is an isometry of C then π is an automorphism of $C^\perp$.

Proof: Given any isometry $\phi(\,) = x + \pi(\,)$, we have $x \in C$ since $\mathbf{0} \in C$ and for all $v \in C$ and $w \in C^\perp$ we have

$$0 = \phi(v) \cdot w = x \cdot w + \pi(v) \cdot w = 0 + v \cdot \pi(w)$$

so $\pi^{-1}(w) \in C^\perp$ and $\pi - 1$ is an automorphism of $C^\perp$. Since $\mathrm{Aut}\,(C^\perp)$ is a group, it follows that $\pi \in \mathrm{Aut}\,(C^\perp)$ as well. □

Lemma II.2: If $\phi(y) = x + \pi(y)$ is an isometry of C then π is an automorphism of K, the kernel of C.

Proof: Let $A \subseteq C$ be any linear subcode of C. Following [2], if C is the union of cosets of A then $A \subseteq K$, the kernel of C. Since

$$x + \pi(C) = \bigcup_y \pi(K) + \pi(y) + x = C$$

we have $\pi(K) \subseteq K$ and the result follows. □

These two lemmas are helpful but we should remark that the converse of these lemmas are not true in general.

Lemma II.3: Let K be the kernel of a binary code C and assume for all $x \in C$ there exists a coordinate permutation π_x such that $\phi_x(\,) = x + \pi_x(\,) \in \mathrm{Iso}\,(C)$. We have $K = \{a \in C | \pi_a \in \mathrm{Aut}\,(C)\}$.

Proof: Let $a \in K$ and let $c \in C$. Now $a + C = C$ and $\phi_a(a) = a + \pi_a(c) \in C$, so $\pi_a(c) \in a + C = C$ and $\pi_a \in \mathrm{Aut}\,(C)$.

Reciprocally, if $\pi_a \in \mathrm{Aut}\,(C)$ then $\pi_a(C) = C$. We know $\phi_a(C) = C$, so $a + \pi_a(C) = C$ and $a + C = C$. Hence $a \in K$. □

Lemma II.4: Let K be the kernel of a binary code C then $\mathrm{Aut}\,(C) \subseteq \mathrm{Aut}\,(K)$.

Proof: Let $\pi \in \mathrm{Aut}\,(C)$ so $\pi \in \mathrm{Iso}\,(C)$. Hence, by Lemma II.2, $\pi \in \mathrm{Aut}\,(K)$. □

III. Propelinear Codes

A code C of length n is said to be *propelinear* if for any codeword $x \in C$ there exists $\pi_x \in \mathcal{S}_n$ satisfying the following conditions:

1) for all $x, y \in C$, $x + \pi_x(y) \in C$ (or, equivalently, $\forall x \in C$, $\phi(\,) = x + \pi_x(\,) \in \mathrm{Iso}\,(C)$);
2) $\pi_x \circ \pi_y = \pi_z \quad \forall y \in C$, where $z = x + \pi_x(y)$.

For all $x \in C$ and for all $y \in \mathbb{Z}_2^n$, denote by $*$ the binary operation such that $x * y = x + \pi_x(y)$. Then, $(C, *)$ is a group, which is not Abelian in general. The vector $\mathbf{0}$ is always a codeword and π_0 is the identity permutation. Hence, $\mathbf{0}$ is the identity element in C and $x^{-1} = \pi_x^{-1}(x)$, for all $x \in C$ (see [8]). Note that $\Pi = \{\pi_x \mid x \in C\}$ is a subgroup of $\mathcal{S}_n$ with the usual composition of permutations as the multiplication.

Clearly, the propelinear code class is more general than the linear code class.

Proposition III.1: Let $(C, \star) \subset \mathbb{Z}_2^n$ be a group. C is a propelinear code if and only if the group $\mathrm{Iso}\,(C)$ contains a regular subgroup acting transitively on C.

Proof: Assume C is a propelinear code and take $\phi_x\colon C \longrightarrow C$ defined by $\phi_x(v) = x \star v = x + \pi_x(v)$. We have

$$\begin{aligned}\phi_x\phi_y(z) &= \phi_x(y + \pi_y(z)) = x + \pi_x(y + \pi_y(z)) \\ &= x \star y + \pi_x\pi_y(z) = x \star y + \pi_{x\star y}(z) = \phi_{x\star y}(z).\end{aligned}$$

Also

$$\begin{aligned}d(\phi_x(v), \phi_x(w)) &= d(x + \pi_x(v), x + \pi_x(w)) \\ &= W(\pi_x(v) + \pi_x(w)) = W(\pi_x(v + w)) \\ &= W(v + w) = d(v, w).\end{aligned}$$

Hence, $G = \{\phi_x | x \in C\} < \mathrm{Iso}\,(C)$, and $|G| = |C|$. Given $v, w \in C$, it is easy to find $x \in C$ such that $\phi_x(v) = w$, so G acts transitively on C. In fact, given $v, w \in C$ take $x = w * v^{-1}$. Now

$$\begin{aligned}\phi_x(v) &= x + \pi_x(v) = x + \pi_w\pi_{v^{-1}}(v) = x + \pi_w(v^{-1}) \\ &= w + \pi_w(v^{-1}) + \pi_w(v^{-1}) = w.\end{aligned}$$

Conversely, assume $\mathrm{Iso}\,(C)$ contains a regular subgroup G acting transitively on C then $|C| = |G|$.

For all $\phi \in G$ call $\phi_x = \phi$, where $x = \phi(\mathbf{0})$. Now $\phi_x \longrightarrow x$ is a bijection $G \longrightarrow C$ due to the fact that G acts transitively on C and is regular.

For $x \in C$, define $\pi_x(v) = x + \phi_x(v)$. It is easy to see that π_x is a coordinate permutation because ϕ_x is an isometry on C. For $x \in C$ define $x \star v = x + \pi_x(v) = \phi_x(v)$. With this operation, we claim that C has a propelinear structure.

Clearly, $\phi_x(v) \in C$ if and only if $v \in C$ so we just need to prove that $\pi_x\pi_y = \pi_{x\star y}$. G acts transitively on C, so $\phi_x\phi_y = \phi_{x\star y}$ if and only if they have the same values on $\mathbf{0} \in C$.

First, $\phi_x\phi_y(\mathbf{0}) = \phi_x(y) = x \star y$ and, also, $\phi_{x\star y}(\mathbf{0}) = x \star y$.

Moreover, $\phi_{x\star y}(z) = x \star y + \pi_{x\star y}(z)$ and, also

$$\phi_x\phi_y(z) = \phi_x(y + \pi_y(z)) = x + \pi_x(y) + \pi_x\pi_y(z) = x \star y + \pi_x\pi_y(z)$$

hence $\pi_x\pi_y = \pi_{x\star y}$. □

The next proposition characterizes propelinear codes looking at the structure of minimum distance graph associated to a given code C.

To make the correspondence self-contained, we will introduce the graph of minimum distances associated to a given binary 1-perfect code C such that $(C, \star) \subset \mathbb{Z}_2^n$ is a group. This graph $\Gamma(C)$ has as vertices the elements in C and two vertices are connected by an edge if they are at distance 3. Also recall that a group acting transitively on a set is said to act regularly if only the identity fixes any point (see [6, p. 8]).

Let H be the set of weight 3 codewords in C and observe that $H = H^{-1} = \{s^{-1} | s \in H\}$, so we can define the Cayley graph $\Gamma_{C,H} = \Gamma((C, \star); H)$ as the graph with vertices the elements of $(C, \star)$ and edges from $g \in (C, \star)$ to $g \star s \in (C, \star)$, for all $s \in H$.

Lemma III.2 (See [9]): Given a graph $\Gamma(C)$, a necessary and sufficient condition for the existence of a group $(C, \star)$ and a subset H of $(C, \star)$, such that $\Gamma(C) \cong \Gamma_{C,H}$, is that $\mathrm{Aut}\,(\Gamma(C))$ contains a regular subgroup. In that case, $(C, \star)$ is this regular subgroup.

Proposition III.3: Let C be a binary 1-perfect code, such that $(C, \star) \subset \mathbb{Z}_2^n$ is a group. C is a propelinear code if and only if the minimum distance graph of C is a Cayley graph.

Proof: From Proposition III.1, C is a propelinear code if and only if the group $\mathrm{Iso}\,(C)$ contains a regular subgroup.

Let $\Gamma(C)$ be the minimum-distance graph associated to C. For a binary code, always $\mathrm{Iso}\,(C) \subset \mathrm{Aut}\,(\Gamma(C))$, but when C is a binary 1-perfect code it is well known (see [1]) that $\mathrm{Iso}\,(C) = \mathrm{Aut}\,(\Gamma(C))$, so we can conclude that C is a propelinear code if and only if the group $\mathrm{Aut}\,(\Gamma(C))$ contains a regular subgroup. But now, from Lemma III.2, this happens if and only if $\Gamma(C)$ is the Cayley graph of C acting on the set H of the weight 3 codewords. □

In a more specific way we can write this last proposition in this other form.

Corollary III.4: Let C be a binary 1-perfect code, such that $(C, \star) \subset \mathbb{Z}_2^n$ is a group. C is a propelinear code if and only if for all $a, b \in C$ such that $d(a, b) = 3$, then there exists a vector $v \in C$ of weight 3 such that $b = a \star v$.

Again we assume that C is a propelinear code.

Let A_π be the set $\{a \in C | \pi_a = \pi\}$. Let $Id(x) = x$ denotes the identity permutation.

Proposition III.5: A_{Id} is a normal subgroup and each A_π is a coset $A_\pi = A_{Id} + x$, where $\pi_x = \pi$.

Proof: Define ϕ: $C \longrightarrow \Pi$ as $\phi(x) = \pi_x$.

Clearly, ϕ is an epijective group homomorphism and $\mathrm{Ker}(\phi) = A_{Id}$. Also, every A_π is a coset $A_\pi = A_{Id} \star x$, but $A_{Id} \star x = A_{Id} + x$. □

Proposition III.6: $C^\perp$ is a subgroup in K and C.

Proof: For $c \in C$ and $a, b \in C^\perp$, we know (see [7]) that $a, b \in C^\perp \subset K$

$$\begin{aligned}(a \star b^{-1}) \cdot c &= (a + \pi_a(b^{-1})) \cdot c = (a + \pi_a \pi_b^{-1}(b)) \cdot c \\ &= (\pi_a \pi_b^{-1}(b)) \cdot c = 0\end{aligned}$$

since $\pi_a, \pi_b \in \mathrm{Aut}\,(C)$. □

If we have a 1-perfect code of length $n = 2^t - 1$ and rank $r_C = n - t + s$ then in [7] it is proved that the kernel has dimension at least 2^{t-s} for $s > 1$. From [4] and [12] and also by using the arguments in [7] it is possible to say more; the dual code $C^\perp$ induces a partition of the coordinates into one set of $2^s - 1$ coordinates which correspond to the coordinates that are zero in every codeword in $C^\perp$, and $2^{t-s} - 1$ disjoint sets of coordinates of size 2^s which are always equal in $C^\perp$. If $a_0, a_1, \ldots, a_m$ are the codewords having these sets as their support, then they are always in the kernel of C. In addition, we have the following proposition.

Proposition III.7 [7], [12]: Let C be a propelinear code, so for $x \in C$, $\pi_x(a_0) = a_0$, and $\pi_x(a_i) = a_j$ for $i \neq 0$. Moreover, the dual code $C^\perp$ determines a lattice of 1-perfect subcodes (and sub-STS (Steiner triple system)) in C that is equivalent to the lattice of 1-perfect subcodes in the Hamming code of length $m = 2^{t-s} - 1$.

IV. 1-Perfect Binary Additive Codes: The Automorphism Group $\mathrm{Aut}_P(C)$ and $\mathrm{Aut}\,(C)$

A 1-perfect additive code C of type $(\alpha = 2^r - 1, \beta = 2^{t-1} - 2^{r-1})$ can be seen as an Abelian subgroup $(C, \star) \subset \mathbb{F}^n$. The operation $\star$ is the usual addition in $\mathbb{Z}_2$ and $\mathbb{Z}_4$. In [3], it is proved that $(C, \star)$ is also the kernel of a groups homomorphism

$$\vartheta: \mathbb{F}^n \longrightarrow G$$

where G is the group $\mathbb{Z}_2^{2r-t} \times \mathbb{Z}_4^{t-r}$.

The homomorphism ϑ will have a 1-perfect additive code, as its kernel only when $\vartheta(e_i) = \vartheta(e_j)$ if and only if $e_i = e_j$ and $\vartheta(e_i \star e_j) = 0$ if and only if $e_i \star e_j = 0$, where $e_i, e_j \in \mathbb{F}^n$ are two different unit vectors of length n. Notice that $e_i \star e_i$ could be nonzero because e_i could be the unit element in some $\mathbb{Z}_4$.

If $C = \mathrm{Ker}\,(\vartheta)$, these properties mean that in each coset in $\mathbb{F}^n/C$ there is one and only one binary vector of length n and weight 1.

In the quoted paper [3], the 1-perfect additive codes were studied and classified. For each value r and t such that $2 \leq r \leq t \leq 2r$ there is exactly one 1-perfect additive code of type $(\alpha = 2^r - 1, \beta = 2^{t-1} - 2^{r-1})$. The unicity means that if ϑ' is another homomorphism of $\mathbb{F}^n$ onto G such that $C' = \mathrm{Ker}\,(\vartheta')$ then there exists a permutation $\tau \in \mathcal{S}_n$ such that $\tau(C) = C'$ and $\vartheta' = \vartheta\tau$.

This kind of automorphism of C, like the previous τ, is not only a permutation in $\mathcal{S}_n$, and so a linear mapping on $\mathbb{Z}_2^n$, but also a propelinear mapping, that is a homomorphism on $\mathbb{F}^n$. This leads to the consideration of $\mathrm{Aut}_P(C)$, the automorphism group of C made up of the permutations on $\mathcal{S}_n$ that fix the code C and that are also group homomorphisms on F^n.

Example: In length 15 there are three nonisomorphic 1-perfect additive codes. They exist for $(r = 2, t = 4)$, $(r = 3, t = 4)$ and $(r = 4, t = 4)$.

For the case $(r = 3, t = 4)$, we can see the additive code as the kernel of a group homomorphism ϑ: $\mathbb{F}^{15} \longrightarrow \mathbb{Z}_2^2 \times \mathbb{Z}_4$ which, moreover, for all pairs of different unit vectors $e_i, e_j \in \mathbb{F}^{15}$ satisfies $\vartheta(e_i \star e_j) = 0$ if and only if $e_i \star e_j = 0$.

Hence, the kernel of the homomorphism given by the matrix H is the additive code C of type $(\alpha = 7, \beta = 4)$. The first α coordinates are the binary ones and the last 2β, taken in pairs, are those which correspond to the $\mathbb{Z}_4$ part

$$H = \left(\begin{array}{ccccccc|cccccccc} 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 2 & 2 & 0 & 2 & 0 & 2 & 0 & 1 & 3 & 1 & 3 & 1 & 3 & 1 & 3 \end{array}\right).$$

Proposition IV.1: The automorphism group $\mathrm{Aut}_P(C)$ of a binary 1-perfect additive code coincides with the automorphism group of the group $G = \mathbb{Z}_2^{2r-t} \times \mathbb{Z}_4^{t-r}$.

Proof:

$$\begin{array}{ccc} \mathbb{F}^n & \xrightarrow{\vartheta} & G \\ \tau \downarrow & & \downarrow \phi \\ \mathbb{F}^n & \xrightarrow{\vartheta} & G \end{array}$$

Let C be the kernel of ϑ: $\mathbb{F}^n \longrightarrow G$ and let $\tau \in \mathrm{Aut}_P(C)$, then τ is a permutation $\tau \in \mathcal{S}_n$, which is also a homomorphism of $\mathbb{F}^n$, such that $\tau(C) = C$. This means that τ acts on the quotient group $\mathbb{F}^n/C \equiv G$ and, so, $\phi = \vartheta\tau\vartheta^{-1}$ is well defined and also is an automorphism of G. On the other hand, if ϕ is an automorphism of G, then we could take $\phi\vartheta$ which defines a quotient group $\mathbb{F}^n/C$ and, so, a partition in $\mathbb{F}^n$. For each unit vector e_i, representative in a coset, take $\tau(e_i)$ such that $\phi\vartheta(e_i) = \vartheta\tau(e_i)$. Hence τ is a coordinate permutation $\tau \in \mathcal{S}_n$ which fixes code C. We can extend τ to all $\mathbb{F}^n$ and $\tau \in \mathrm{Aut}_P(C)$. □

This last proposition allows us to compute the cardinality of the automorphism group of an additive code. For instance, in the linear case we have for the Hamming code H_t of length $n = 2^t - 1$

$$\begin{aligned}|\mathrm{Aut}\,(H_t)| &= \prod_{i=0}^{t-1}((2^t - 1) - (2^i - 1)) \\ &= 2^{\binom{t}{2}} \prod_{i=0}^{t-1}(2^{t-i} - 1).\end{aligned}$$

In the more general case, when C is a 1-perfect additive code of type $(2^r - 1, 2^{t-1} - 2^{r-1})$, the automorphism group $\mathrm{Aut}_P(C)$ coincides

with the automorphism group of the group $G = \mathbb{Z}_2^{2r-t} \times \mathbb{Z}_4^{t-r}$ and so (taking $\alpha = 2r - t$ and $\beta = t - r$)

$$\begin{aligned}|\mathrm{Aut}_P(C)| &= 2^{(\alpha+\beta)\beta}\left|\mathrm{Aut}\left(\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_2^{\beta}\right)\right| \\ &= 2^{(\alpha+\beta)\beta} 2^{\binom{\alpha+\beta}{2}} \prod_{i=0}^{\alpha+\beta-1} (2^{\alpha+\beta-i} - 1) \\ &= 2^{r(2t-r-1)} \prod_{i=0}^{r-1} (2^{r-i} - 1).\end{aligned}$$

The usual group $\mathrm{Aut}\,(C)$ contains the coordinate permutations which fix code C. Look at the additive propelinear codes of type $(2^r - 1,\ 2^{t-1} - 2^{r-1})$ as the kernel of the homomorphism

$$\vartheta\colon \mathbb{F}^n \longrightarrow G$$

where G is the group $\mathbb{Z}_2^{2r-t} \times \mathbb{Z}_4^{t-r}$ and $(C, \star)$ is a subgroup of $\mathbb{F}^n$.

Consider $\theta\colon \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2$ defined by $\theta(x) = x \pmod 2$ which is a group homomorphism. We can extend this mapping to $\theta\colon \mathbb{Z}_4^{t-r} \longrightarrow \mathbb{Z}_2^{t-r}$ and we can consider

$$\theta \cdot \vartheta\colon \mathbb{F}^n \longrightarrow \mathbb{Z}_2^{2r-t} \times \mathbb{Z}_4^{t-r} \longrightarrow \mathbb{Z}_2^{2r-t} \times \mathbb{Z}_2^{t-r} = \mathbb{Z}_2^r.$$

Now $\theta \cdot \vartheta$ is a group homomorphism from $\mathbb{F}^n$ to $\mathbb{Z}_2^r$.

Proposition IV.2:

$$\theta \cdot \vartheta\colon \mathbb{F}^n \longrightarrow \mathbb{Z}_2^{2r-t} \times \mathbb{Z}_4^{t-r} \longrightarrow \mathbb{Z}_2^{2r-t} \times \mathbb{Z}_2^{t-r} = \mathbb{Z}_2^r$$

is a linear mapping.

Proof: Let π be any involution involving the two coordinates in some $\mathbb{Z}_4$. Let these coordinates be e_i and e_{i+1}. Take $v \in \mathbb{F}^n$ and note that $\pi(v) = v$ or $\pi(v) = v \star e_i \star e_i$.

Then in both cases $\theta \cdot \vartheta(\pi(v)) = \theta \cdot \vartheta(v)$.

We can generalize this result by taking any permutation π_w associated to vector w. We know permutation π_w is a composition of permutations like π, so $\theta \cdot \vartheta(\pi_w(v)) = \theta \cdot \vartheta(v)$. Hence,

$$\begin{aligned}\theta \cdot \vartheta(w + v) &= \theta \cdot \vartheta(w \star \pi_w(v)) = \theta \cdot \vartheta(w) + \theta \cdot \vartheta(\pi_w(v)) \\ &= \theta \cdot \vartheta(w) + \theta \cdot \vartheta(v).\end{aligned}$$

□

We will prove in Theorem V.8 that the kernel of $\theta \cdot \vartheta$ is the linear span $\langle C\rangle$ of code C.

Now, given $\tau \in \mathrm{Aut}\,(C) = \mathrm{Aut}\,(\langle C\rangle)$, we have that $\tau\colon \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2^n$ acts on the quotient $\mathbb{Z}_2^n/\langle C\rangle \equiv \mathbb{Z}_2^r$. So, given an automorphism $\tau \in \mathrm{Aut}\,(C)$ we get an automorphism of $\mathbb{Z}_2^r$.

On the other hand, if ϕ is an automorphism of the linear space $\mathbb{Z}_2^r$ we get an automorphism in $\mathbb{Z}_2^n/\langle C\rangle$ and from this we can construct an automorphism τ in $\mathbb{Z}_2^n$ which leaves code C invariant. To do this, we need to define $\tau(e_i)$ for all the units vectors e_i in $\mathbb{Z}_2^n$. So, for each e_i define $\tau(e_i)$ as e_j, such that $\phi([e_i]) = ([e_j])$, where $[e_i]$ and $[e_j]$ are cosets in $\mathbb{Z}_2^n/\langle C\rangle$.

Each one of the 2^r cosets in $\mathbb{Z}_2^n/\langle C\rangle$ has the same number of unit vectors 2^{t-r}, except for the coset $\langle C\rangle$ which has $2^{t-r} - 1$.

After choosing $\tau(e_i)$ for all the unit vectors we can extend τ to the whole $\mathbb{Z}_2^n$ by linearity. Given two cosets $[e_i]$ and $[e_j] = \phi[e_i]$, we have $(2^{t-r})!$ different ways to choose the value of τ for the unit vectors in $[e_i]$. So, in short

$$\begin{aligned}|\mathrm{Aut}\,(C)| &= ((2^{t-r})!)^{2^r-1}((2^{t-r}-1)!)|\mathrm{Aut}\,(\mathbb{Z}_2^r)| \\ &= ((2^{t-r})!)^{2^r-1}((2^{t-r}-1)!)2^{\binom{r}{2}} \prod_{i=0}^{r-1}(2^{r-i}-1).\end{aligned}$$

V. 1-Perfect Binary Additive Codes: Kernel and Rank

Lemma V.1: Let C be a propelinear code. If C is an additive code then $A_{Id} = \{a | \pi_x(a) = a \text{ for all } x \in C\}$.

Proof: We can see the elements in A_{Id} as $a = x + y$, where $x,\ y$ are in the same coset, $x,\ y \in A_\pi$. Since for every $x \in C$ the permutation π_x has order 2, and $x \star y = y \star x$ we have for $x,\ y \in A_\pi$, $x + \pi(y) = y + \pi(x)$ or $x + y = \pi(x + y) = a \in A_{Id}$. □

Lemma V.2: Let $\sigma \in \mathcal{S}_n$ be the permutation $\sigma = (a_1 a_1') \cdots (a_\beta a_\beta')$ which is the product of all involutions involving the two coordinates in every $\mathbb{Z}_4$ code. Then $\sigma \in \mathrm{Aut}\,(C)$.

Proof: Since σ is the product of all involutions, for each $c \in C$ we have $\sigma(c) = \pi_c(c)$. Since $c + \pi_c(c) = x \in A_{Id}$, we have that $\sigma(c) = c + x \in C$. □

Lemma V.3: If C is a 1-perfect binary additive code with kernel K, then $A_\sigma \subset K$.

Proof: We know that σ is in $\mathrm{Aut}\,(C)$, so we need only proof there exists a vector $c \in C$ such that $\pi_c = \sigma$.

Note that the all-ones vector and the vectors $u = (1 \cdots 1 | 0 \cdots 0)$ and $u' = (0 \cdots 0 | 1 \cdots 1)$ are in A_{Id}. Take a vector with zeros in all the coordinates in the $\mathbb{Z}_2$ part and $(1,\ 0)$ or $(0,\ 1)$ in the projection to each $\mathbb{Z}_4$. This vector could be out of C, so let this vector be $c + e$ where $c \in C$ is the vector in C closest to it and $W(e) \leq 1$. We have that $c + \sigma(c) + u'$ is a vector in C of weight 2 unless e is zero in the $\mathbb{Z}_4$ coordinates. In this last case, we conclude that $\pi_c = \sigma$ and $c \in C$. □

Proposition V.4: If C is a nonlinear 1-perfect additive code then the dimension of A_{Id} is $2^{t-1} + 2^{r-1} - r - 1$.

Proof: The Hamming code H_r of length $2^r - 1$ and dimension $2^r - r - 1$ is contained in A_{Id}. For each involution $(a_i,\ a_i')$ in the $\mathbb{Z}_4$ coordinates there is a word of weight 3 in A_{Id} having those coordinates and a $\mathbb{Z}_2$ coordinate as its support. There are $b = 2^{t-1} - 2^{r-1}$ such triples which we denote by T_b. Thus, the dimension of A_{Id} is at least $(2^r - r - 1) + b = 2^{t-1} + 2^{r-1} - r - 1$. For any word in $(x|y) \in A_{Id}$ there is a word $(e|y) \in \langle T_b\rangle$ and hence $(x + e|0) \in H_r$. Thus, these words span A_{Id}. □

Proposition V.5: If C is a 1-perfect binary additive code with kernel K, then either $K = A_{Id} = C$ when C is linear or $K = A_{Id} \bigcup A_\sigma$ when C is not linear. In the first case, $\dim(K) = \dim(A_{Id})$ and in the second case $\dim(K) = \dim(A_{Id}) + 1$.

Proof: If C is linear then the kernel K coincides with A_{Id} and C.

If C is not linear then from the previous lemmas we know that $A_{Id} \bigcup A_\sigma \subseteq K$ and to prove the proposition we need only see that for all the elements $v \in K$ we have $\pi_v = Id$ or $\pi_v = \sigma$.

Let v be a vector in $K \backslash A_{Id}$. The permutation π_v associated to vector v is a product of involutions each of which involves the two coordinates in $\mathbb{Z}_4$ in which the projection of v is $(1,\ 0)$ or $(0,\ 1)$. In other words, π_v is the product of a subset of the involutions which make up σ. Let (bb') be an involution in σ which is not in π_v and let (aa') be an involution involved in both. Both π_v and σ are automorphisms of the code. Consider the word t of weight 3 in C whose support is $\{a,\ b,\ c\}$ and consider $\sigma(t),\ \pi_v(t) \in C$. If σ fixes coordinate c then so does π_v but then $d(t,\ \pi_v(t)) = 2$. Otherwise, $d(\sigma(t),\ \pi_v(t)) = 2$. In either case we get a contradiction. Therefore, $\pi_v = \sigma$. □

Lemma V.6: If C is a 1-perfect binary additive code of length $n > 7$, then $C^\perp \subset A_{Id}$.

Proof: Suppose $C^\perp \nsubseteq A_{Id}$, then there exists $x \in C^\perp$ such that $\pi_x = \sigma$ since $C^\perp \subset K$ and $K = A_{Id} \cup A_\sigma$. The vector $x \star x$ belongs to $C^\perp$ (see Proposition III.6) and so has a support of size $\frac{n+1}{2}$ which is in the $\mathbb{Z}_4$. Hence, vector x has $\frac{n+1}{4}$ nonzero coordinates in the $\mathbb{Z}_4$

TABLE I
PARAMTERRS, RANK, AND DIMENSION OF THE KERNEL FOR 1-PERFECT ADDITIVE CODES

t	r	type: $(2^r-1, 2^{t-1}-2^{r-1})$	$dim(K)$	r_C
2	2	$(1,1,0)$, $(3,0,0)$	3, 3	3, 3
3	2, 3	$(3,2,0)$, $(7,0,0)$	4, 4	4, 4
4	2, 3, 4	$(3,6,0)$, $(7,4,0)$, $(15,0,0)$	8, 9, 11	13, 12, 11
5	3, 4, 5	$(7,12,0)$, $(15,8,0)$, $(31,0,0)$	17, 20, 26	28, 27, 26
6	3, 4, 5, 6	$(7,28,0)$, $(15,24,0)$, $(31,16,0)$, $(63,0,0)$	33, 36, 43, 57	60, 59, 58, 57
...	...	...	...	...

part (let $x_1, x_2, \ldots x_{\frac{n+1}{4}}$ be these coordinates) and also $\frac{n+1}{4}$ nonzero coordinates in the $\mathbb{Z}_2$ part.

Fixing x_1 consider the triples v_i containing x_1 and each of the others coordinates x_i. All these triples v_i have the third coordinate in the $\mathbb{Z}_2$ part and it is not in the support of x. Now compute

$$x \star v_2 \star v_3 \star \cdots \star v_{\frac{n+1}{4}}$$

which give us the all-ones vector, except perhaps for the two coordinates in the $\mathbb{Z}_4$ the support of which contains x_1. Finally, we get a contradiction except for the cases where these two coordinates are ones. This is the case of four coordinates in the $\mathbb{Z}_4$ part or, in general, $4+8\lambda$ coordinates in the $\mathbb{Z}_4$ part, so $2(4+8\lambda) = 2^t$. This equation has solution only for $t = 3$ (which corresponds to a code of length 7). □

As a corollary of Propositions V.4 and V.5 it is easy to compute the dimension of the kernel for all the 1-perfect additive codes and we can state the following theorem.

Theorem V.7: Let C be a binary 1-perfect additive code of type $(2^r-1, 2^{t-1}-2^{r-1})$, then the kernel K of C has dimension

$$\dim(K) = \begin{cases} 2^r - r - 1, & \text{if } t = r \\ 2^{r-1} + 2^{t-1} - r, & \text{if } t \neq r. \end{cases}$$

In summary, Table I gives us the allowable parameters and dimension of the kernels for 1-perfect additive codes.

Theorem V.8: Let $(C, \star)$ be a binary 1-perfect additive code of type $(2^r-1, 2^{t-1}-2^{r-1})$ of length $n = 2^t - 1$, where $t \geq 4$, then the rank r_C of C is

$$r_C = n - r = 2^t - r - 1.$$

.

Proof: As in Proposition IV.2, look at the additive propelinear codes of type $(2^r-1, 2^{t-1}-2^{r-1})$ as the kernel of the homomorphism ϑ: $\mathbb{F}^n \longrightarrow G$ and consider

$$\theta \cdot \vartheta \colon \mathbb{F}^n \longrightarrow \mathbb{Z}_2^{2r-t} \times \mathbb{Z}_4^{t-r} \longrightarrow \mathbb{Z}_2^{2r-t} \times \mathbb{Z}_2^{t-r} = \mathbb{Z}_2^r.$$

Let H be the linear kernel of $\theta \cdot \vartheta$. It is a linear code which contains C, so $\langle C \rangle \subset H$.

Now we are going to see that $H \subset \langle C \rangle$. For this take $v \in H$ and compute $c \cdot v$ for all $c \in C^\perp$.

If $v \in H$ then $\theta\vartheta(v) = 0$ and $\vartheta(v) = \vartheta(e_j) + \vartheta(e_j)$ for some unit vector e_j. Since $\vartheta(v) + \vartheta(e_j) + \vartheta(e_j) = 0$, we can write

$$v \star e_j \star e_j \in C.$$

Thus,

$$0 = c \cdot (v \star e_j \star e_j) = c \cdot v + c \cdot \pi_v(e_j \star e_j) = c \cdot v + c \cdot (e_j \star e_j)$$

but $C^\perp < A_{Id}$, so $c \cdot (e_j \star e_j) = 0$ and, finally, $c \cdot v = 0$.

The conclusion is that $H = \langle C \rangle$ and $r_C = \dim(H) = n - r$. □

We can sum up and give the results in Table I.

VI. BINARY ADDITIVE CODES AND STS

Let C be a binary additive code of type $(2^r-1, 2^{t-1}-2^{r-1}, 0)$, where $2 \leq r \leq t \leq 2r$. The parameters uniquely determine the code and the associated Steiner triple system to within isomorphism when $t \geq 4$. The Hamming code (of length $2^t - 1$) and its associated triple system PG $(t-1, 2)$ can be easily recognized and the code is easily generated from the triple system. We will show that, similarly, the Steiner triple system associated with a 1-perfect additive binary code can be easily recognized and can *generate* the corresponding code as well.

Proposition VI.1: Let C be a binary 1-perfect additive code of type $(2^r-1, 2^{t-1}-2^{r-1})$, of length $n = 2^t - 1$, where $t \geq 4$, then the STS(n) associated with it is unique and can be easily recognized and used to construct the code.

Proof: Let C be as in the proposition having dual code $C^\perp$ of dimension $r = t - s$. Let $S = \{i | c_i = 0 \text{ for all } c \in C^\perp\}$, and assume the $\mathbb{Z}_2$ coordinates are $R = \{1, 2, \ldots, 2^r - 1\}$. We know that $|S| = 2^s - 1$. Let σ be the fundamental involutory automorphism of the code which is a product of involutions (aa') with R as the set of fixed points. Consider the triples corresponding to the supports for the words of weight 3 in C.

- For each involution (aa'), the third point $i \in R$ of the triple containing that pair is in S. From previous arguments, we know that each of these fixed triples $t_a = \{i, a, a'\}$ are in A_{Id} and, in fact, form part of a basis for it. Since $C^\perp \subseteq A_{Id}$ we have $c \cdot (a, a') = 0$ and thus $c \cdot e_i = 0$ for all $c \in C^\perp$.
- Each point $i \in S$ which is in at least one fixed triple must be in at least 2^{r-1} such fixed triples. If $t_a = \{i, a, a'\}$ is one fixed triple then for each other $j \in R$ there is a triple $t_j = \{j, a, b\}$ but
$$t_a + t_j + \sigma(t_j) = t_b = \{i, b, b'\} \in A_0.$$
There are $2^r - 2$ points $j \in R$ generating $(2^r - 2)/2$ other fixed triples containing i.
- The remaining triples through a are contained in the $\mathbb{Z}_4$ coordinates.
If $t = \{a, u, v\}$ is such a triple and t_a, t_u, t_v are the corresponding fixed triples containing the involutions (aa'), (uu'), (vv'), respectively, then $t + \sigma(t) \in A_0$ and $t_a + t_u + t_v + t + \sigma(t)$ must be a word of weight 3 in the Hamming subcode H_r and thus each point is in exactly 2^{r-1} fixed triples and there must be $2^{t-r} - 1 = |S|$ such points. Thus, on S we have an Hamming subcode $H_s \subseteq H_r$.
- For each $i \in S$, let σ_i be the product of involutions (aa') such that $t_a = \{i, a, a'\} \in C$ and let R_i be the corresponding set of coordinates. Then for each $i \in S$ there is a 1-perfect additive subcode of length $2^{r+1} - 1$ on the coordinates $R \cup R_i$ having parameters $(2^r - 1, 2^{r-1})$.

For the converse, given an STS $(2^t - 1)$, B, we can compute its rank (and dual $B^\perp$). If the dimension of the dual is r and $2 \leq r \leq t \leq 2r$

then we can find the $2^{t-r}-1$ zero coordinates S in the dual. We can also find the subsystem R of length 2^r-1 isomorphic to PG $(r-1, 2)$. From the structure imposed by the dual, we have at most $\binom{t-s}{t-r}$ sets to consider. The rest of the coordinates can be partitioned into $2^{t-r}-1$ sets R_i of order 2^r which form sub-STS $(2^{r+1}-1)$ on the sets $R \cup R_i$. These sub-STS must all have rank $2^{r+1}-1-r$ (or codimension r, except in the case when $t=4,\ r=2$). By considering the dual of the subsystem (as a code of length $2^{r+1}-1$), we can find the unique coordinate i, that is zero in all words in this dual and hence compute the fundamental involutory automorphism σ_i of this subsystem by considering the triples through i. Each of these subsystems have a different unique point in S. This induces a mapping of the sets $R_i \to i \in S$ which must map the triples traversing these R_i onto the triples in the PG $(s-1, 2)$ subsystem on S. Finally, σ is the product of the σ_i. It is now straightforward to construct the additive code (see [3]).

We note that when $t=4,\ r=2$ then we have three STS (7) intersecting in a sub-STS (3). The STS (7) are PG $(2, 2)$ and have rank 4 (not 5) but they also have propelinear representations and fundamental involutory automorphisms which fix the sub-STS (3). One can still compute the automorphisms σ_i and σ (in several equivalent ways) and hence the code. □

ACKNOWLEDGMENT

The authors wish to thank J. Borges for useful discussions and valuable comments which have improved some proofs in this correspondence.

REFERENCES

[1] S. V. Agustinovich, "Perfect binary $(n, 3)$ codes: The structure of graphs of minimum distances," *Discr. Appl. Math.*, vol. 114, no. 1–3, pp. 9–11, 2001.

[2] H. Bauer, B. Ganter, and F. Hergert, "Algebraic techniques for nonlinear codes," *Combinatorica*, vol. 3, pp. 21–33, 1983.

[3] J. Borges and J. Rifà, "A characterization of 1-perfect additive codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1688–1697, July 1999.

[4] J. Doyen, X. Hubaut, and M. Vandensavel, "Ranks of incidence matrices of Steiner triple systems," *Math. Z.*, vol. 163, pp. 251–259, 1978.

[5] P. Delsarte and V. I. Levenshtein, "Association schemes and coding theory," *IEEE Trans. Inform. Theory*, vol. 44, pp. 2477–2505, Oct. 1998.

[6] J. D. Dixon and B. Mortimer, *Permutation Groups*. New York: Springer-Verlag, 1996.

[7] K. Phelps and M. Villanueva. On perfect codes: Rank and kernel. *Des., Codes, Cryptogr.* [Online]. Available: http://www.dms.auburn.edu/phelpkt.

[8] J. Rifà, J. M. Basart, and L. Huguet, "On completely regular propelinear codes," in *Proc. 6th Int. Conf., AAECC-6 (Lecture Notes in Computer Science)*.. Berlin, Germany: Springer-Verlag, 1989, vol. 357, pp. 341–355.

[9] G. Sabidussi, "On a class of fixed-point-free graphs," *Proc. Amer. Math. Soc.*, vol. 9, no. 5, pp. 800–804, 1958.

[10] F. I. Solov'eva, S. V. Avgustinovich, T. Honold, and H. Heise, "On the extendability for code isometries," *J. Geometry*, no. 61, pp. 3–6, 1998.

[11] F. I. Solov'eva and S. T. Topalova, "On the automorphism groups of perfect binary codes and Steiner triple systems," *Probl. Inform. Transm.*, no. 36-4, pp. 53–58, 2000.

[12] L. Teirlinck, "On projective and affine hyperplanes," *J. Combin. Theory, Ser. A*, vol. 28, pp. 290–306, 1980.

$\mathbb{Z}_{p^{k+1}}$-Linear Codes

San Ling and Jason Thomas Blackford

***Abstract*—We characterize codes over $\mathbb{Z}_p$ which are the Gray images of $(1-p^k)$-cyclic codes or cyclic codes over $\mathbb{Z}_{p^{k+1}}$ $(k \geq 1)$. A necessary and sufficient condition for the Gray image of a $\mathbb{Z}_{p^2}$-linear $(1-p)$-cyclic code to be linear is given. In many cases, this yields an explicit description of the Gray image of a linear $(1-p)$-cyclic code over $\mathbb{Z}_{p^2}$, of length relatively prime to p. Linear cyclic codes over $\mathbb{Z}_{p^2}$ whose Gray images are linear cyclic codes over $\mathbb{Z}_p$ have been characterized. Some generalizations of these results to the case of $\mathbb{Z}_{p^{k+1}}$, where $k \geq 2$, are also obtained.**

***Index Terms*—Constacyclic code, cyclic code, Gray map, linear code, quasi-cyclic code.**

I. INTRODUCTION

There has been much interest and research in codes over finite rings, especially the ring $\mathbb{Z}_4$, in recent years. Codes over $\mathbb{Z}_4$ are linked to binary codes via the Gray map. Analogs of the Gray map have also been defined for codes over other finite chain rings [3], linking these codes to codes over finite fields. It is well known that the nonlinear binary Kerdock code is the Gray image of an extended linear cyclic code over $\mathbb{Z}_4$ [4], [9].

In [11], Wolfmann showed that the Gray image of a linear negacyclic code over $\mathbb{Z}_4$ of length n is a distance-invariant, but not necessarily linear, binary cyclic code. He also showed that, for n odd, the Gray image of a linear cyclic code over $\mathbb{Z}_4$ of length n is equivalent to a (not necessarily linear) binary cyclic code. These results were later generalized to the setting of codes over $\mathbb{Z}_{2^k}$ by Tapia-Recillas *et al.* in [10]. Wolfmann also determined in a later paper [12] all linear cyclic codes over $\mathbb{Z}_4$ of odd length whose Gray images are linear binary codes and showed that they are those whose Nechaev–Gray images are linear cyclic codes.

In this correspondence, we generalize most of the results of [11], [12], and [10] to the ring $\mathbb{Z}_{p^{k+1}}$ of integers modulo p^{k+1}, where p is any prime and $k \geq 1$ is an integer.

The organization of the correspondence is as follows. In Section II, we introduce the Gray map and show that a code over $\mathbb{Z}_{p^{k+1}}$ is a $(1-p^k)$-cyclic code if and only if its Gray image is a quasi-cyclic code over $\mathbb{Z}_p$ of index p^{k-1} and of length $p^k n$. In particular, the Gray image of a linear $(1-p^k)$-cyclic code over $\mathbb{Z}_{p^{k+1}}$ is a distance-invariant quasi-cyclic code over $\mathbb{Z}_p$. In Section III, we show that the Gray image of a linear cyclic code over $\mathbb{Z}_{p^{k+1}}$ is equivalent to a (not necessarily linear) quasi-cyclic code over $\mathbb{Z}_p$. In Section IV, a necessary and sufficient condition is given for the Gray image of a linear $(1-p)$-cyclic code over $\mathbb{Z}_{p^2}$ to be linear and the Gray image of a linear $(1-p)$-cyclic code over $\mathbb{Z}_{p^2}$, of length relatively prime to p, is determined in many cases. Examples of some of the best ternary cyclic codes of length ≤ 50 obtained as the Gray images of constacyclic codes over

Manuscript received December 13, 2001; revised March 29, 2002. The work of S. Ling was supported in part by NUS-ARF under Research Grant R-146-000-029-112 and DSTA under Research Grant R-394-000-011-422. This work was performed in part while S. Ling was affiliated with the Institute for Mathematical Sciences, National University of Singapore.

S. Ling is with the Department of Mathematics, National University of Singapore, Singapore 117543, Republic of Singapore (e-mail: lings@math.nus.edu.sg).

J. T. Blackford is with the Department of Mathematical Sciences, Rensselaer Polytechnic Institute, Troy, NY 12180 USA (e-mail: blackj@rpi.edu).

Communicated by P. Solé, Associate Editor for Coding Theory.

Publisher Item Identifier 10.1109/TIT.2002.801473.