Combinatorial Structure of binary 1-perfect additive codes[§]

K.T. Phelps [¶], J. Rifà[‖]

21/11/01

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 paper, 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 automorphisms 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 an 1-perfect binary additive code is also established.

keywords: 1-perfect codes, kernel, rank, additive codes, automorphism group.

1 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*.

[§]Research partially supported by Spanish CICYT Grant TIC2000-0739-c04-01 and also supported by Catalan DURSI grant PIV2000-10

[¶]Discrete & Statistical Sciences, Auburn University, Auburn, Al 36849-5307. USA. This research was done while visiting the Mathematical Research Center (CRM) in Barcelona in September-December 2001. phelpkt@dms.auburn.edu

[‖]Computer Sciences, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain. josep.rifa@uab.es

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 one 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 $n = \alpha + 2\beta$. In all this paper 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 in all this paper we will use both concepts interchangeably.

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

The paper is organized as follows, in Section 2 we give some basic properties about the automorphism in a binary code. In Section 3 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 4 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 5 we compute the kernel and rank for all the binary 1-perfect additive codes and, finally, in Section 6 we characterize in an efficiently computable way the Steiner Triple System associated with a binary 1-perfect additive code.

2 Preliminaries

Let C be a binary code of length n and 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 2.1 *If $\phi(y) = x + \pi(y)$ is an isometry of C then π is an automorphism of $C^{\perp}$.*

Proof: For any permutation π, and code C, $\dim < \pi(C) >= \dim < C >$ and $\pi(C)^{\perp} = \pi(C^{\perp})$. Given any isometry $x + \pi()$, we have $x \in C$ since $0 \in C$ and $\pi(C) = C + x \subseteq < C >$ and the statement follows. ∎

Lemma 2.2 *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 2.3 *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 $\phi_x = x + \pi_x() \in Iso(C)$. 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 2.4 *Let K be the kernel of a binary code C then* $\mathrm{Aut}(C) \subset \mathrm{Aut}(K)$.

Proof: Let $\pi \in \mathrm{Aut}(C)$ so $\pi \in Iso(C)$. Hence, by lemma 2.2, $\pi \in \mathrm{Aut}(K)$. ∎

3 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:

1. for all $x, y \in C$, $x+\pi_x(y) \in C$ (or equivalently $\forall\, x \in C, \phi() = x+\pi_x() \in Iso(C)$).

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 $\pi_{\mathbf{0}}$ 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 [7]). 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 3.1 *Let $(C, \star) \subset \mathbb{Z}_2^n$ be a group. C is a propelinear code if and only if the group $Iso(C)$ contains a regular subgroup acting transitively on C.*

Proof: Assume C is a propelinear code and take $\phi_x : C \longrightarrow C$ defined by $\phi_x(v) = x \star v = x + \pi_x(v)$. We have $\phi_x\phi_y(z) = \phi_x(y + \pi_y(z)) = x + \pi_x(y + \pi_y(z)) = x \star y + \pi_x\pi_y(z) = x \star y + \pi_{x\star y}(z) = \phi_{x\star y}(z)$.

Also $d(\phi_x(v), \phi_x(w)) = d(x + \pi_x(v), x + \pi_x(w)) = W(\pi_x(v) + \pi_x(w)) = W(\pi_x(v + w)) = W(v + w) = d(v, w)$.

Hence, $G = \{\phi_x | \, x \in C\} < Iso(C)$, 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 $\phi_x(v) = x+\pi_x(v) = x+\pi_w\pi_{v^{-1}}(v) = x + \pi_w(v^{-1}) = w + \pi_w(v^{-1}) + \pi_w(v^{-1}) = w$.

Conversely, assume $Iso(C)$ 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 $\pi_x\pi_y = \pi_{x\star y}$. ∎

Proposition 3.2 *Let C 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 the above proposition 3.1, C is a propelinear code if and only if the group $Iso(C)$ contains a regular subgroup.

Let $\Gamma(C)$ the minimum distance graph associated to C, that is, the graph whose vertices are the codewords and the edges joints vertices at distance three. For a binary code, always $Iso(C) \subset \mathrm{Aut}(\Gamma(C))$, but when C is a binary 1-perfect code, from [1], $Iso(C) = \mathrm{Aut}(\Gamma(C))$, 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, using an old result from [8], this happens if and only if $\Gamma(C)$ is the Cayley graph of C acting on the set of the weight three codewords. ∎

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

Corollary 3.3 *Let C 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 three 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 3.4 *A_{Id} is a normal subgroup and each A_π is a coset $A_\pi = A_{Id} + x$, where $\pi_x = \pi$.*

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

Clearly ϕ is an epijective group homomorphism and $Ker(\phi) = A_{Id}$.

Also every A_π is a coset $A_\pi = A_{Id} \star x$, but $A_{Id} \star x = A_{Id} + x$. ∎

Proposition 3.5 *$C^\perp$ is a subgroup in K and C.*

Proof: For $c \in C$ and $a, b \in C^\perp$, we know (see [6]) that $a, b \in C^\perp \subset K$, $(a \star b^{-1}) \cdot c = (a + \pi_a(b^{-1})) \cdot c = a + \pi_a \pi_b^{-1}(b)) \cdot c = \pi_a \pi_b^{-1}(b)) \cdot c = 0$ 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 [6] it is proved that the kernel has dimension at least 2^{t-s} for $s > 1$. From [4] and [9] and also by using the arguments in [6] 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:

Proposition 3.6 ([9],[6]) *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) in C that is equivalent to the lattice of 1-perfect subcodes in the Hamming code of length $m = 2^{t-s} - 1$.*

4 1-perfect binary additive codes. The automorphism group $\mathbf{Aut_P(C)}$ and $\mathbf{Aut(C)}$.

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 non-zero because e_i could be the unit element in some $\mathbb{Z}_4$.

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

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 $C' = Ker(\vartheta')$ 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 non-isomorphic 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 $\vartheta : \mathbb{F}^{15} \longrightarrow \mathbb{Z}_2^2 \times \mathbb{Z}_4$ which, moreover, for all couple 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, token in pairs are those which corresponds 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 4.1 *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: Let C be the kernel of $\vartheta : \mathbb{F}^n \longrightarrow G$ and let $\tau \in \mathrm{Aut}_P(C)$, then τ is a permutation $\tau \in \mathcal{S}_n$, which is also an 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. Vice versa, 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 $\tau \in \mathrm{Aut}_P(C)$. ∎

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

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 $n = 2^t - 1$:

$$|\ \mathrm{Aut}(H_t)| = \prod_{i=0}^{t-1} \left((2^t - 1) - (2^i - 1)\right) = 2^{\binom{t}{2}} \prod_{i=0}^{t-1} (2^{t-i} - 1)$$

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 $\beta = t - r$),

$$|\operatorname{Aut}_P(C)| = 2^{(\alpha+\beta)\beta}|\operatorname{Aut}(\mathbb{Z}_2^\alpha \times \mathbb{Z}_2^\beta)|$$
$$= 2^{(\alpha+\beta)\beta}2^{\binom{\alpha+\beta}{2}} \prod_{i=0}^{\alpha+\beta-1}(2^{\alpha+\beta-i}-1) = 2^{r(2t-r-1)} \prod_{i=0}^{r-1}(2^{r-i}-1)\,.$$

The usual group $\operatorname{Aut}(C)$ 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

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

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

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

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

Proposition 4.2

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

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, $\theta \cdot \vartheta(w + v) = \theta \cdot \vartheta(w \star \pi_w(v)) = \theta \cdot \vartheta(w) + \theta \cdot \vartheta(\pi_w(v)) = \theta \cdot \vartheta(w) + \theta \cdot \vartheta(v)$. ∎

We will prove in Theorem 5.8 that the kernel of $\theta \cdot \vartheta$ is the linear span $< C >$ of code C.

Now, given $\tau \in \operatorname{Aut}(C) = \operatorname{Aut}(< C >)$, we have $\tau : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2^n$ acts on the quotient $\mathbb{Z}_2^n / < C > \equiv \mathbb{Z}_2^r$. So, given an automorphism $\tau \in \operatorname{Aut}(C)$ we get an automorphism of $\mathbb{Z}_2^r$.

Vice versa, if ϕ is an automorphism of the linear space $\mathbb{Z}_2^r$ we get an automorphism in $\mathbb{Z}_2^n/ < C >$ and from this we can construct an automorphism τ in $\mathbb{Z}_2^n$ which leaves invariant code C. 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 $[e_j]$ means cosets in $\mathbb{Z}_2^n/ < C >$.

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

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

5 1-perfect binary additive codes. Kernel and Rank.

Lemma 5.1 *Let C be a propelinear code. If C is an additive code then $A_{Id} = \{a \mid \pi_x(a) = a \, for \, all \, x \in C\}$.*

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 5.2 *Let $\sigma \in \mathcal{S}_n$ 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 5.3 *If C is a 1-perfect binary additive code with kernel K, then $A_\sigma \subset K$.*

Proof: We know 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 $u = (1 \ldots 1 \mid 0 \ldots 0)$ and $u' = (0 \ldots 0 \mid 1 \ldots 1)$ are in A_{Id}. Take a vector with zeroes 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 be zero in the $\mathbb{Z}_4$ coordinates. In this last case we conclude that $\pi_c = \sigma$ and $c \in C$. ∎

Proposition 5.4 *If C is a non-linear 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 $(e|y) \in < T_b >$ and thus $(x + e|0) \in H_r$. Thus these words span A_{Id}. ∎

Proposition 5.5 *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 $A_{Id} \bigcup A_\sigma \subseteq K$ 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 $K \setminus A_{Id}$. 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 $(b\, b')$ be an involution in σ which is not in π_v and let $(a\, a')$ 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 5.6 *If C is a 1-perfect binary additive of length $n > 7$, then $C^\perp \subset A_{Id}$.*

Proof: Suppose $C^\perp \not\subseteq A_{Id}$, then there exists $x \in C^\perp$ such that $\pi_x = \sigma$ since $C^\perp \subset K$ and $K = A_{Id} \cup A_\sigma$. Vector $x \star x$ belongs to $C^\perp$ (see 3.5) and so has a support of size $\frac{n+1}{2}$ which is in the $\mathbb{Z}_4$. Hence, vector x has $\frac{n+1}{4}$ non-zero coordinates in the $\mathbb{Z}_4$ part (let $x_1, x_2, \ldots x_{\frac{n+1}{4}}$ be these coordinates) and also $\frac{n+1}{4}$ non-zero coordinates in the $\mathbb{Z}_2$ part.

Fixing x_1 consider the triples v_i containing x_1 and each one 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 a 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 5.4 and 5.5 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 5.7 *Let C be a binary 1-perfect additive code of type $(2^r - 1, 2^{t-1} - 2^{r-1})$, 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 short, we have the following parameters and dimension of the kernels for 1-perfect additive codes:

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

Theorem 5.8 *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 4.2, look at the additive propelinear codes of type $(2^r-1, 2^{t-1}-2^{r-1})$ as the kernel of the homomorphism $\vartheta : \mathbb{F}^n \longrightarrow G$ and consider:

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

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

Now we are going to see that $H \subset < C >$. 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. This also means that $v \star e_j \star e_j \in C$ since $\vartheta(v) + \vartheta(e_j) + \vartheta(e_j) = 0$. 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 $H = < C >$ and $r_C = \dim(H) = n - r$. ∎

We can sum up and give this table

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
...	...	...	...	...

6 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 6.1 *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 can be 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 $(a\, a')$ with R as the set of fixed points. Consider the triples corresponding to the supports for the words of weight three 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 three in the Hamming sub-code 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 sub-code $H_s \subseteq H_r$.

- 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 an 1-perfect additive sub-code 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 a $STS(2^t - 1)$, 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 co-dimension r, except in the case when $t = 4, r = 2$). By considering the dual of the sub-system (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 sub-system by considering the triples through i. Each of these sub-systems have a different unique point in S. This induces a mapping of the sets $R_i \rightarrow i \in S$ which must map the triples traversing these R_i onto the triples in the $PG(s-1,2)$ sub-system on S. Finally, σ is the product of the σ_i. It is now straight-forward 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 paper.

References

[1] S.V. Agustinovich, *Perfect binary* $(n, 3)$ *codes: the structure of graphs of minimum distances*, Discrete Applied Maths., vol. 114 (1-3), pp.9-11, 2001.

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

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

[4] J. Doyen, X. Hubaut, M. Vandensavel, *Ranks of incidence matrices of Steiner Triple Systems*, Math.Z., vol.163, pp.251-259, 1978.

[5] P. Delsarte, V.I. Levenshtein, *Association Schemes and Coding Theory*, IEEE Trans. Inform. Theory, vol.44, pp.2477-2505, 1998.

[6] K. Phelps, M. Villanueva, *On Perfect Codes: rank and Kernel* , Designs, Codes, and Cryptography, (to appear).

[7] J. Rifà, J.M. Basart and L. Huguet, *On completely regular propelinear codes*, in *Proc. 6th International Conference, AAECC-6.*, number 357 in LNCS, pp. 341-355, Springer-Verlag, 1989.

[8] G.Sabidussi, *On a class of fixed-point-free graphs*, Proceedings of the American Mathematical Society, vol.9, Issue 5, pp.800-804, 1958.

[9] L. Teirlinck, *On projective and affine hyperplanes*, J. Combinatorial Theory, Ser. A, vol.28, pp.290-306, 1980.