*Constructions of 1-perfect partitions on the n-cube $(\mathbb{Z}/2)^n$

J. Borges, C. Fernandez, J. Rifa & M. Villanueva

Departament d'Informàtica
Universitat Autònoma de Barcelona
08193 Bellaterra, Spain

Abstract

We will study 1-perfect partitions, some of their constructions and the algebraic structures related to them. We will see the ways of constructing 1-perfect partitions on the n-cube $(\mathbb{Z}/2)^n$ by using a generalized Slov'eva-Phelps' switching technique. For each 1-perfect distance-preserving partition we can define an associated operation such that $\mathbb{F}^n$ becomes distance-compatible quasigroup. We relate the quasigroups associated to isomorphic or equivalent distance-preserving 1-perfect partitions.

Keywords: Perfect partitions, switching, distance-preserving, distance-compatible quasigroup.

Introduction

Let $\mathbb{F}^n$ be a vector space of dimension n over $\mathbb{Z}/2$. The Hamming distance between vectors $x, y \in \mathbb{F}^n$, denoted by $d(x, y)$, is the number of coordinates in which x and y differ. The Hamming weight of a vector $x \in \mathbb{F}^n$, denoted by $wt(x)$, is the number of its nonzero coordinates. The support of a vector $x = (x_1, x_2, \cdots, x_n) \in \mathbb{F}^n$, denoted by $Supp(x)$, is the subset of $\{1, 2, \cdots, n\}$ given by $\{j | x_j \neq 0\}$.

A *binary 1-perfect code* C of length n is a subset of $\mathbb{F}^n$, such that every $x \in \mathbb{F}^n$ is within distance 1 from exactly one codeword of C. If we consider distance $r \neq 1$ instead of 1, we have trivial codes, repetition codes, the binary Golay code or equivalents codes to these ones; so we will henceforth use the word "perfect" to refer specifically to 1-perfect codes.

The length n of a perfect code is $n = 2^m - 1$ for some $m \geq 3$. The linear perfect codes exist $\forall m \geq 3$ and are unique up to isomorphism (they are the well-known Hamming codes).

*This work has been partially supported by spanish CICYT grant TIC2000-0739-C04-01.

A *1-perfect partition* is a partition of the space $\mathbb{F}^n$ into $n+1$ perfect codes $C_0, C_1, \dots, C_n$. We can assume the zero vector is in C_0 and the vectors having a one in the *ith* coordinate and zeroes elsewhere, e_i, are in C_i, $\forall i \in \{1, \dots, n\}$. Given a perfect code C of length $n = 2^m - 1$ we know that there always exists $n+1$ translates of C, $C+e_0,\ C+e_1, \dots,\ C+e_n$, that form a 1-perfect partition of $\mathbb{F}^n$, we will call this the trivial partition.

Two partitions $C_0, C_1, \dots, C_n$ and $D_0, D_1, \dots, D_n$ are *isomorphic* if there exists a permutation π of the coordinates which maps the vectors of each class into the vectors of a class in the second partition, that is $\forall j \in \{1, \dots, n\}$ $D_j = \pi(C_i)$ for some $i \in \{1, \dots, n\}$. Two partitions $C_0, C_1, \dots, C_n$ and $D_0, D_1, \dots, D_n$ are *equivalent* if there exists a permutation π of the coordinates and a translation τ such that for all classes D_j there exists a class C_i such that $D_j = \pi(C_i) + \tau$.

1 Construction of 1-perfect partitions with the switching technique

Many interesting problems concerning perfect codes remain unsolved. For example, Etzion and Vardy [1] compiled a list of ten open problems. The last of them is the following:

> **Space partitions:** Given a perfect code C of length $n = 2^m - 1$ we know that there always exist $n + 1$ translates of C, say $C_0, C_1, \dots, C_n$ with $C_0 = C$, that form a partition of $\mathbb{F}^n$. Under which conditions is there another, different, partition of $\mathbb{F}^n$ into perfect codes $D_0, D_1, \dots, D_n$ with $D_0 = C$? Can such partitions be classified for a given perfect code?

Rifà and Vardy [2] provide a complete answer to the first question. They show that it is always possible to construct more than one different perfect partition from a given perfect code.

After this result, Rifà and Vardy reformulate the initial problem to ask about not only different partitions of space into perfect codes, but about non-isomorphic and non-equivalent partitions. They prove that it is always possible to construct more than one different and non-equivalent perfect partition from a given perfect code.

We will generalize the problem by starting not only from trivial partitions, but from any partition $C * e_0,\ C * e_1, \dots,\ C * e_n$, where $C * e_0 = C$ and for all $x \in C$, $x * e_i$ is the only vector in class $C * e_i$ at distance one apart from x [3] (if $x * e_i = x + e_i$, we have the trivial partition). The problem is now the following:

> **Space partitions:** Given a perfect code C of length $n = 2^m - 1$ and a 1-perfect partition (not necessary the trivial one) of $\mathbb{F}^n$, $C_0, C_1, \dots, C_n$ with $C_0 = C$. Under which conditions is there another, different partition of $\mathbb{F}^n$ into perfect codes $D_0, D_1, \dots, D_n$ with $D_0 = C$? Can such partitions be classified for a given perfect code?

From a given partition we will show that with some restrictions we can construct another, different partition of $\mathbb{F}^n$. To show that, we will generalize the Solov'eva-Phelps' switching technique [4]-[5] to construct two new perfect codes. First of all we take two classes C and $C * e_i$ of the partition and define a graph (V, E) in C by $V = C$

$$(x,y) \in E \Leftrightarrow \begin{cases} d(x,y) = 3 \\ d(x, y * e_i) = 2 \text{ or } d(y, x * e_i) = 2 \end{cases}$$

Let $S \subset C$ be a connected component in the above graph, and let $S' \subset C * e_i$, be the subset in $C * e_i$ defined by $S' = \{x * e_i, \quad \forall x \in S\}$. If we switch S and S', we define classes $D = (C \backslash S) \cup S'$ and $H = D * e_i$.

Lemma 1 *If C is a perfect code, $D = (C \backslash S) \cup S'$ and H are perfect codes.*

Proof: By construction, it is enough to prove that the minimum distance in D is 3.

In D, there are elements that belong to C or to S', and in these sets we know that the minimum distance is 3, because C and $C * e_i \supseteq S'$ are perfect codes.

Let $y \in C \backslash S$. We suppose that $d(y, z) \leq 2$ for some $z = x * e_i \in S'$, where $x \in S \subset C$, that is the only element in $C * e_i$ that $d(x, z) = 1$. If $d(y, z) = 0$, $y = x * e_i$ but then $y \notin C$. If $d(y, z) = 1$, then $d(x, y) \leq 2$ because $d(z, x) = 1$ but this is not possible because $x, y \in C$. So, $d(y, z) = 2$, and then $d(x, y) = 3$. In this case, there is an edge between x and y, so $y \in S$ but $y \in C \backslash S$.

By the same way, we can prove H is a perfect code. ∎

Let $\mathcal{A}$ the partition $C, \; C * e_1, \ldots, \; C * e_n$ and $\mathcal{B}$ the partition $D, \; C * e_1, \ldots, \; C * e_{i-1}, \; D * e_i, \; C * e_{i+1}, \ldots, \; C * e_n$.

Proposition 2 *If the graph (V, E) has more than one connected component for some $i \in \{1, \ldots, n\}$, the partitions $\mathcal{A}$ and $\mathcal{B}$ are different.*

Proof: The partitions $\mathcal{A}$ and $\mathcal{B}$ are different because the new classes D and H are different from C and $C * e_i$. ∎

It is not always possible to obtain a different partition with this construction. The problem is that there exist partitions of $\mathbb{F}^n$ such that $\forall i \in \{1, \ldots, n\}$ the graph has only one connected component. For example, for $\mathbb{F}^7$, the following partition [6]:

$C =$ [1, 8, 26, 31, 44, 45, 51, 54, 75, 78, 84, 85, 98, 103, 121, 128]
$C * e_1 =$ [2, 11, 23, 30, 37, 48, 52, 57, 72, 77, 81, 92, 99, 106, 118, 127]
$C * e_2 =$ [3, 16, 18, 29, 38, 41, 55, 60, 69, 74, 88, 91, 100, 111, 113, 126]
$C * e_3 =$ [5, 12, 24, 25, 35, 46, 50, 63, 66, 79, 83, 94, 104, 105, 117, 124]
$C * e_4 =$ [6, 9, 19, 32, 36, 47, 53, 58, 71, 76, 82, 93, 97, 110, 120, 123]
$C * e_5 =$ [7, 14, 17, 28, 34, 43, 56, 61, 68, 73, 86, 95, 101, 112, 115, 122]
$C * e_6 =$ [10, 15, 20, 21, 33, 40, 59, 62, 67, 70, 89, 96, 108, 109, 114, 119]
$C * e_7 =$ [4, 13, 22, 27, 39, 42, 49, 64, 65, 80, 87, 90, 102, 107, 116, 125]

where the binary vectors are represented in base 10 begining with 1, that is, the $(0,0,0,0,0,0,0)$ is 1, $(1,0,0,0,0,0,0)$ is 2, ...

2 Distance-preserving, 1-perfect partitions on the n-cube $(\mathbb{Z}/2)^n$

Definition 3 *Given a 1-perfect partition $C_0, C_1, \ldots, C_n$. For every $v \in \mathbb{F}^n$ we can define a permutation π_v on the coordinate set $\{1, 2, \ldots, n\}$, in the following way:*

$\pi_v(e_i) = e_j$, where $v + e_j$ is the only element in coset C_k at distance 1 from v and C_k is the coset where there is the element $e_s + e_i$, and e_s is the leader in the coset of v.

Proposition 4 *π_v is a permutation on the coordinate set $\{1, 2, \ldots, n\}$ and $\pi_0 = Id$.*

Proof: Suppose $\pi_v(e_i) = \pi_v(e_j)$. If e_s is the leader in the coset of vector v, the former assumption means that $e_s + e_i$ and $e_s + e_j$ are in the same coset and this is only possible if $i = j$, so π_v is a permutation on the coordinate set $\{1, 2, \ldots, n\}$.

Now assume $\pi_0(e_i) = e_j$. This means that e_j is in the coset of e_i and this is only possible if $e_i = e_j$. ∎

Definition 5 *Given a 1-perfect partition we can define the associated* **π-operation** *on $\mathbb{F}^n$ as:*

$$v * w = v + \pi_v(w) \tag{1}$$

Definition 6 *A 1-perfect partition, C, C_1, C_2, $\ldots$, C_n, is* **k-distance-preserving** *if for any $v, w \in \mathbb{F}^n$ and any vector $s \in \mathbb{F}^n$ of weight k, we have $d(v, w) = d(v * s, w * s)$.*

Remark that the elements $v * s$ i $w * s$ does not have necessarily to be in the same class. In the affirmative case the partition would become a uniform partition and the classes would be propelinear codes [7].

Definition 7 *We will say that a 1-perfect partition C, C_1, C_2, $\ldots$, C_n, is* **distance-preserving**, *if it is k-distance preserving, for all k.*

Proposition 8 *Let C, C_1, C_2, $\ldots$, C_n, be a distance-preserving, 1-perfect partition. For all $v \in \mathbb{F}^n$, the permutation π_v is an involution and the order of v is 2 or 4.*

Proof: Notice that if $e_i \in Supp(v)$ and $\pi_v(e_i) = e_j \neq e_i$, then $e_j \notin Supp(v)$ because, if it no were in this way $d(v, 0) = d(v * e_i, 0 * e_i) = \mathrm{wt}(v + \pi_v(e_i) + e_i) = \mathrm{wt}(v) - 2$.

Also notice if $e_i \notin Supp(v)$ and $\pi_v(e_i) = e_j \neq e_i$, then $e_j \in Supp(v)$.

If $e_i \neq e_j = \pi_v(e_i)$ and $e_j \neq e_k = \pi_v(e_j)$, we will see that $d(v, 0) = d(v * (e_i + e_j), 0 * (e_i + e_j)) = \mathrm{wt}(v + e_i + e_j + e_j + e_k) \neq \mathrm{wt}(v)$, because e_i and e_k are two both either in the support of v or out of it. ∎

Definition 9 *A binary operation $*$ on $\mathbb{F}^n$ is distance-compatible if $\forall v, w \in \mathbb{F}^n$ and $\forall i \in \{1, \ldots, n\}$*

(i) $d(v * e_i, v) = 1$

(ii) $0 * v = v$

(iii) $v * e_i = w * e_i \Leftrightarrow v = w$

Proposition 10 *Given a 1-perfect partition, the associated π-operation on $\mathbb{F}^n$ is distance-compatible.*

Proof: The first and second part is trivial because we have the π-operation defined in (1).

For the third part, assume $v * e_i = w * e_i$, now $v + w = \pi_v(e_i) + \pi_w(e_i)$, so either $v = w$ or $d(v, w) = 2$. We can write vectors v and w as $v = c * e_j$ and $w = c' * e_l$, where $c, c' \in C$.

But $v * e_i$ and $w * e_i$ are in the same class (in fact, both elements are equals), so $e_i + e_j$ i $e_i + e_l$ are in the same class too and $e_j = e_l$. This means that v and w are in the same class (the class where the element e_j belongs) and, so, $d(v, w) = 0$ and $v = w$. ∎

Proposition 11 *Given a distance-preserving, 1-perfect partition, the associated π-operation defines a distance-compatible quasigroup, of exponent 2 or 4, in $\mathbb{F}^n$.*

Proof: First we will prove that $\mathbb{F}^n$ has a quasigroup structure with the π-operation. For this we only need to show that $s * v = s * w \Rightarrow v = w$ and $v * s = w * s \Rightarrow v = w$.

1: $s * v = s * w \Rightarrow s + \pi_s(v) = s + \pi_s(w) \Rightarrow \pi_s(v) = \pi_s(w) \Rightarrow v = w$

2: Suppose that $v * s = w * s$ and then, as the partition is distance-preserving, $d(v, w) = d(v * s, w * s)$, so $v = w$.

Now, from Proposition 8, the order of all the elements in $\mathbb{F}^n$ is 2 or 4. ∎

Remark 12 *We will say π-quasigroup a distance-compatible quasigroup.*

All the previous propositions leads us to consider π-group or π-quasigroup operations (abelians or not) of exponent 2 or 4, defined in a set from which C be a subset.

One important thing to be proved is that isomorphic π-quasigroups give rise to isomorphic (or equivalent) distance-preserving partitions and vice versa.

In this way the classification of all the possible 1-perfect, distance-preserving, partitions is replaced by the classification of all the π-quasigroup structures of exponent 2 or 4.

Let $\Omega = \{C_0, \ldots, C_n\}$ and $\Omega' = \{C'_0, \ldots, C'_n\}$ be two binary distance-preserving 1-perfect partitions of length n. For any vector v, let π_v be the associated permutation induced by Ω and let λ_v be the associated permutation induced by Ω'.

For any pair of vectors $v, w \in \mathbb{F}^n$, we define the operations $*$ and $\perp$ such that:

$$\begin{aligned} v * w &= v + \pi_v(w) \\ v \perp w &= v + \lambda_v(w) \end{aligned}$$

Now, we consider the two loop (quasigroup with identity element) structures on the n-cube, $(\mathbb{F}^n, *)$ and $(\mathbb{F}^n, \perp)$.

Lemma 13 *If Ω and Ω' are isomorphic, then*

$$\lambda_v = \sigma \circ \pi_{\sigma^{-1}(v)} \circ \sigma^{-1} \quad \forall v \in \mathbb{F}^n$$

where σ is the coordinate permutation such that $\sigma(\Omega) = \Omega'$.

Proof: Without loss of generality, we may assume that $\sigma(C_i) = C'_i$, for all $i = 0, \ldots, n$. Now, for any vector $v \in C'_i$, we have that if

$$v \perp e_j = v + \lambda_v(e_j) = u$$

then u must be in the class C'_k which contains $\sigma(e_i) + e_j$. Hence

$$\sigma^{-1}(v) + \sigma^{-1}(\lambda_v(\sigma(e_\ell))) = \sigma^{-1}(u) \tag{2}$$

where $\ell = \sigma^{-1}(e_j)$, $\sigma^{-1}(v) \in C_i$, $\sigma^{-1}(u) \in C_k$ and $d(\sigma^{-1}(v), \sigma^{-1}(u)) = 1$. Also, we have that the class C_k contains $e_i + e_\ell$. Thus, it is clear that

$$\sigma^{-1}(v) * e_\ell = \sigma^{-1}(u) \Longrightarrow \sigma^{-1}(v) + \pi_{\sigma^{-1}(v)}(e_\ell) = \sigma^{-1}(u) \tag{3}$$

Now, from equations 2 and 3 we have that

$$\pi_{\sigma^{-1}(v)}(e_\ell) = \sigma^{-1}(\lambda_v(\sigma(e_\ell)))$$

as this result holds for all $\ell = 0, \ldots, n$, we obtain

$$\sigma \circ \pi_{\sigma^{-1}(v)} \circ \sigma^{-1} = \lambda_v$$

∎

Theorem 14 *Let Ω and Ω' be two distance-preserving 1-perfect partitions of length n and let $(\mathbb{F}^n, *)$ and $(\mathbb{F}^n, \perp)$ be the two induced loops, respectively, as before. Then Ω and Ω' are isomorphic if and only if $(\mathbb{F}^n, *)$ and $(\mathbb{F}^n, \perp)$ are isomorphic.*

Proof: Suppose that $\Omega' = \sigma(\Omega)$. We will prove that the bijection $\sigma : \mathbb{F}^n \longrightarrow \mathbb{F}^n$ is a loop morphism:

(i) $\sigma(\mathbf{0}) = \mathbf{0}$, thus σ maps the identity element of $(\mathbb{F}^n, *)$ to the identity element of $(\mathbb{F}^n, \perp)$.

(ii) For all $x, y \in \mathbb{F}^n$, we have

$$\begin{aligned} \sigma(x * y) &= \sigma(x + \pi_x(y)) = \sigma(x) + \sigma(\pi_{\sigma^{-1}(\sigma(x))}(\sigma^{-1}(\sigma(y)))) \\ &= \sigma(x) + (\sigma \circ \pi_{\sigma^{-1}(\sigma(x))} \circ \sigma^{-1})(\sigma(y)) \end{aligned}$$

Now, using Lemma 13 we have

$$\sigma(x * y) = \sigma(x) + \lambda_{\sigma(x)}(\sigma(y)) = \sigma(x) \perp \sigma(y)$$

Conversely, assume that σ is a loop isomorphism between $(\mathbb{F}^n, *)$ and $(\mathbb{F}^n, \perp)$. Clearly we may write $\Omega = \{C_0 * e_i\}_{i=0}^n$ and $\Omega' = \{C'_0 \perp e_i\}_{i=0}^n$, where the classes C_0 and C'_0 contain the all-zero vector. Now, we have that any class $C'_0 \perp e_j \in \Omega'$ can be described as

$$\sigma(\sigma^{-1}(C'_0)) \perp \sigma(\sigma^{-1}(e_j)) = \sigma(\sigma^{-1}(C'_0) * \sigma^{-1}(e_j)) = \sigma(C_0 * e_k)$$

for some $k \in \{0, \ldots, n\}$. Hence $\Omega' = \sigma(\Omega)$. ∎

The following question is how to relate the quasigroups when the partitions are equivalent.

Definition 15 *Let $a \in \mathbb{F}^n$ then we define the application $\varphi_a(x) = x + a$ in $\mathbb{F}^n$. We can write $\varphi_a(\Omega) = \Omega'$ if $\varphi_a(C_i) = C_i'$ for $i = 0, \dots, n$.*

Lemma 16 *Let $a \in \mathbb{F}^n$. If $\varphi_a(\Omega) = \Omega'$, then*

(i) $\varphi_a(v * e_i) = (v + a) \perp d_i$.

(ii) $\pi_v(e_i) = \lambda_{v+a}(d_i)$.

where d_i is the leader in C_i' and $v \in C = C_0$.

Proof: Let $C = \{v_0, v_1, \dots, v_r\}$ then $C_i = C * e_i = \{v_0 * e_i, \dots, v_r * e_i\}$ $C_0' = \{v_0 + a, \dots, v_r + a\}$, and $C_i' = \{(v_0 + a) \perp d_i, \dots, (v_r + a) \perp d_i\}$

(i) For $i \in \{0, \dots, n\}$, $j \in \{0, \dots, r\}$ $(v_j * e_i) + a \in C_i'$, therefore, $\exists\, v_{ij} \in C$ such that $(v_j * e_i) + a = (v_{ij} + a) \perp d_i$. We will prove that $v_{ij} = v_j$:

$$(v_j * e_i) + a = (v_{ij} + a) \perp d_i$$
$$v_j + \pi_{v_j}(e_i) + a = v_{ij} + a + \lambda_{(v_{ij}+a)}(di)$$
$$v_j + \pi_{v_j}(e_i) = v_{ij} + \lambda_{(v_{ij}+a)}(di)$$
$$\Rightarrow d(v_j + \pi_(v_j)(e_i), v_{ij}) = 1$$
$$\Rightarrow d(v_j, v_{ij}) = 0 \text{ or } 2$$

but, if $v_j \neq v_{ij}$ then $d(v_j, v_{ij}) \geq 3$, so $d(v_j, v_{ij} = 0)$ and $v_j = v_{ij}$.

Now we have $(v_j * e_i) + a = (v_j + a) \perp d_i \Rightarrow \varphi_a(v_j * e_i) = (v_j + a) \perp d_i$ for $v_j \in C$.

(ii) Let $v_j \in C$, $i \in \{1, \dots, n\}$ and let $v = v_j * e_i \in C_i$. Using the part (i) we have

$$v + a = \varphi_a(v) = \varphi_a(v_j * e_i) = (v_j + a) \perp d_i = v_j + a + \lambda_{(v_j+a)}(d_i)$$

So $v = v_j + \lambda_{(v_j+a)}(di)$. Also we know that $v = v_j * e_i = v_j + \pi_{v_j}(e_i)$. Thus, it is clear that $\pi_{v_j}(e_i) = \lambda_{(v_j+a)}(di)$.

∎

We have seen that $\pi_v(e_i) = \lambda_{v+a}(d_i)$, with $v \in C = C_0$. $0 \in C$, then $\pi_0(e_i) = \lambda_a(d_i)$ $\Rightarrow e_i = \lambda_a(d_i)$, *and* $d_i = \lambda_a^{-1}(e_i)$.

Lemma 17 *Let $a \in \mathbb{F}^n$. If $\varphi_a(\Omega) = \Omega'$, then*

$$\varphi_a(v * e_i) = (v + a) \perp d_i$$

where d_i is the leader in C_i' and $v \in \mathbb{F}^n$.

Proof: Let $v \in \mathbb{F}^n$ and e_k leader in the class of v.

$$v * e_i = u$$

where u belongs to the class containing $e_k + e_i$ and $d(v, u) = 1$.

$$\varphi_a(v * e_i) = \varphi_a(u)$$

If we proof $\pi_v(e_i) = \lambda_{v+a}(d_i)$ then:

$$v * e_i = u,$$
$$v + \pi_v(e_i) = u,$$
$$v + \lambda_{v+a}(d_i) = u,$$
$$(v + a) + \lambda_{v+a}(d_i) = u + a,$$
$$(v + a) \perp d_i = \varphi_a(u),$$
$$(v + a) \perp d_i = \varphi_a(v * e_i).$$

So, to prove the Lemma, we only have to see that $\pi_v(e_i) = \lambda_{v+a}(d_i)$ for $v \in \mathbb{F}^n$.
∎

References

[1] T. Etzion and A. Vardy. "On perfect codes and tilings: problems and solutions". SIAM J. Discrete Math., 11(2), 205-223, 1998.

[2] J. Rifà and A. Vardy. "On partitions of Space into Perfect Codes". Workshop on Coding Theory and Information Integrity. Ein Boqeq. Israel. October 1997.

[3] J. Rifà. "Well-Ordered Steiner Triple Systems and 1-perfect partitions of the n-cube". SIAM J. Discrete Math, 12(1), 35-47,1999.

[4] F.I. Solov'eva. "Perfect codes and their projections". International workshop on Algebraic and Combinatorial Coding Theory. Bulgaria. June 1992.

[5] K. Phelps and M. LeVan. "Kernels of Nonlinear Hamming Codes". Designs, Codes and Cryptography, 6, 247-257 (1995).

[6] K. T. Phelps. "An enumeration of 1-perfect binary codes of length 15". Australian journal of Combinatorics, 21, 287-298 (2000).

[7] J. Rifà, J. Pujol and J. Borges. "1-Perfect uniform and distance invariant partitions". Applicable Algebra in Engineering, Communication and Computing, 11, 297-311 (2001).