SIAM J. DISCRETE MATH.
Vol. 12, No. 1, pp. 35–47


# WELL-ORDERED STEINER TRIPLE SYSTEMS AND 1-PERFECT PARTITIONS OF THE $N$-CUBE*

JOSEP RIFÀ†

**Abstract.** Binary 1-perfect codes which give rise to partitions of the $n$-cube are presented. The 1-perfect partitions are characterized as homomorphic images of simple algebraic structures on $\boldsymbol{F}^n$ and are constructed starting from a particular case of a structure defined in $\boldsymbol{F}^n$.

A special property (so-called *well-ordering*) of $STS(n)$ is given in such a way that for this kind of STS it is possible to define the algebraic structure we need in $\boldsymbol{F}^n$ and to construct 1-perfect partitions of the $n$-cube.

These 1-perfect partitions give us a kind of 1-perfect code for which it is easy to do the coding and decoding. Furthermore, there exists a syndrome which allows us to perform error correction. We present systematic codes of length $n = 15$ and we give examples of how to do the coding, decoding, and error correction.

**Key words.** 1-perfect binary codes, 1-perfect partitions, Steiner triple systems, Sloops, distance-compatible action

**AMS subject classifications.** 94B25, 05B30, 68R05

**PII.** S0895480197330722

## 1. Introduction.

Let $\boldsymbol{F}$ be the binary finite field $GF(2)$ and consider the $n$-cube $\boldsymbol{F}^n$.

A binary code $C$ of length $n$ is a subset of $\boldsymbol{F}^n$. If this subset is a linear subspace of $\boldsymbol{F}^n$, then $C$ will be a linear code. In any case we will call the vectors in $C$ codewords.

The concept of Hamming distance between two vectors $v, w \in \boldsymbol{F}^n$ is defined as the number of coordinates in which they differ. A binary code is a 1-perfect code if all the vectors in $\boldsymbol{F}^n$ are either in $C$ or at distance one from exactly one codeword of $C$.

A binary 1-perfect code has length $n = 2^m - 1$, and the linear 1-perfect codes are unique up to isomorphism (see [4]). The characterization of binary nonlinear 1-perfect codes is not complete. Nonlinear 1-perfect codes were first constructed by Vasil'ev, and other constructions have been presented subsequently by Mollard, Phelps, Solov'eva, Bauer, and more recently by Etzion and Vardy (the reader can see a review of all these constructions in [2]).

Two 1-perfect codes are isomorphic if there exists a permutation of the coordinates such that the codewords in the first code are converted to the codewords in the second code.

Two 1-perfect codes are equivalent if there exists a translation such that the codewords in the first code are converted to the codewords in the second code or isomorphic to them (see [7]).

In this paper a construction of 1-perfect partitions of $\boldsymbol{F}^n$ is proposed, that is, partitions of the $n$-cube in 1-perfect codes. The construction is based on Theorems 3.1 and 3.2, which we present in section 3. In particular, within the various possibilities offered by these theorems, we have opted to use the Steiner loop (Sloop) structure associated with the well-ordered Steiner triple system (STS).

*Received by the editors December 1, 1997; accepted for publication March 10, 1998; published electronically January 29, 1999. This research was partially supported by Spanish grant TEL97-0663.
http://www.siam.org/journals/sidma/12-1/33072.html

†Department of Computer Sciences, Universitat Autònoma de Barcelona, 08193 Bellaterra, Spain (jrifa@ccd.uab.es).

In section 2, we present several general characteristics of quasi groups, Sloops, STSs, and 1-perfect codes.

In section 3 (the main section), we look at Theorems 3.1 and 3.2, which allow the algebraic construction of 1-perfect partitions and, therefore, of 1-perfect codes. Using these theorems and the Sloop structure given by possible STSs, we see in Theorem 3.5 that, for a specific type of STS, we can ensure the construction of 1-perfect partitions of the $n$-cube.

In section 4, we analyze the well-ordered STSs, and in section 5 we see an example of how to handle coding, decoding, and error correction using the 1-perfect codes constructed.

Finally, we present our conclusions in section 6, along with possibilities for future research on this topic.

**2. Sloops, STSs, and 1-perfect codes.**

DEFINITION 2.1. *Let $A, F$ be two sets. We say that $A$ acts on $F$ by means of $\cdot$ if there exists a map*

$$\begin{array}{ccc} F \times A & \longrightarrow & F, \\ (f, a) & \longrightarrow & f \cdot a. \end{array}$$

DEFINITION 2.2. *Assume $A$ acts on $F$ by means of $\cdot$ and also on $G$ by means of $*$. An $A$-homomorphism $h : F \longrightarrow G$ is a map compatible with the action of $A$ on $F$ and on $G$, that is, a map such that for all $a \in A$, $f \in F$ it holds that $f \cdot a = h(f) * a$.*

We are interested in algebraic structures defined on the $n$-cube $\boldsymbol{F}^n$, and also in the Hamming distance defined between vectors in $\boldsymbol{F}^n$.

Let $\boldsymbol{A}_n$ be the set $\{e_0, e_1, \ldots, e_n\}$, where $e_0 \in F^n$ is the zero vector and $e_i$ $(i = 1, 2, \ldots, n)$ are the basis vectors in $\boldsymbol{F}^n$ having a one in the $i$th coordinate and zeroes elsewhere.

DEFINITION 2.3. *A distance-compatible (Hamming distance) action of the set $\boldsymbol{A}_n$ on $\boldsymbol{F}^n$ is a map*

$$\begin{array}{ccc} \boldsymbol{F}^n \times \boldsymbol{A}_n & \rightarrow & \boldsymbol{F}^n, \\ (v, e_i) & \rightarrow & v \cdot e_i, \end{array}$$

*such that*

- *for all $v \in \boldsymbol{F}^n$ there is a permutation $\pi_v$ of $n$ coordinates such that $v \cdot e_i = v + e_{\pi_v(i)}$;*
- *for all $e_i \in \boldsymbol{A}_n$ the induced map $v \rightarrow v \cdot e_i$ is one-to-one.*

For instance, the translation $(v, e_i) \rightarrow v + e_i$ is a distance-compatible action of $\boldsymbol{A}_n$ on the $n$-cube.

The following proposition shows us three properties of distance-compatible actions of $\boldsymbol{A}_n$ on $\boldsymbol{F}^n$ that we will give without proof, because they proceed directly from the definition.

PROPOSITION 2.4.

1. *For all $v \in \boldsymbol{F}^n$ we have $v \cdot e_i = v \cdot e_j$ if and only if $i = j$.*
2. *For all $e_i$, $d(v \cdot e_i, v) = 1$.*
3. *The set $\{a \cdot e_i | i = 1..n\}$ is the set of all the vectors in $\boldsymbol{F}^n$ at distance one from a given $a \in \boldsymbol{F}^n$.*

One of the simplest algebraic structures is that of a quasi group, which we will use in this paper. Readers interested in quasi groups and related structures can find more information in [6].

DEFINITION 2.5. *Let $A$ be a finite set. An algebraic structure of a quasi group consists of $A$ and a binary operation on $A$ defined by the function*

$$* : A \times A \longrightarrow A$$

*such that $x * y = x * z$ and $y * x = z * x$ only if $y = z$ for all $x$, $y$, $z \in A$.*

DEFINITION 2.6. *A quasi group $(A, *)$ is called a Sloop if*

- *there exists $0 \in A$ such that $0 * a = a * 0 = a$ for all $a \in A$;*
- *the operation is totally symmetric, that is, any relation $a * b = c$ implies any other relation obtained by permuting $a$, $b$, and $c$.*

DEFINITION 2.7. *A Steiner triple system $STS(n)$ is a pair $(A, B)$, where $A$ is a finite set of $n$ elements and $B$ is a collection of 3-subsets of $A$, which we will call blocks, such that every two different elements $x, y \in A$ are contained in exactly one block of $B$.*

- It is easy to see that starting from a Sloop $A$, we can define an STS on the set $A^* = A - \{0\}$ by taking a set of blocks $B = \{(x, y, x * y) \mid \forall\, x, y \in A^*,\ x \neq y\}$.
- Conversely, starting from an $STS(n) = (A^*, B)$, we can define a Sloop on the set $A = A^* \cup \{0\} = \{0, 1, 2, \ldots, n\}$ by

$$\begin{array}{ccc} A \times A & \longrightarrow & A, \\ (a, b) & \longrightarrow & a * b, \end{array}$$

$$\begin{cases} \text{if } a \neq b & \text{then} & a * b = c, \quad \text{where } (a, b, c) \in B, \\ \text{if } a = b & \text{then} & a * b = 0, \\ \text{if } a = 0 & \text{then} & a * b = b, \\ \text{if } b = 0 & \text{then} & a * b = a \end{cases}$$

- Two STSs $(A, B)$ and $(A', B')$ are isomorphic if $A = A'$ and there exists a permutation of the elements in $A$ such that the triples in $B$ are converted to the triples in $B'$.
  If $\|A^*\| = 15$, there are 80 nonisomorphic triples (see [9]).
  If $\|A^*\| = 31$, there are $\approx 10^{200}$ nonisomorphic triples (see [5]).

Starting from a 1-perfect binary code $C \in \boldsymbol{F}^n$ (not necessarily linear but such that $0 \in C$), we can construct an STS by taking the supports of the codewords of weight three. Take $A^* = \{1, 2, \ldots, n\}$ as the set of coordinates, and the set of blocks as $B = \{(i, j, k)\}$, where $(i, j, k)$ are the support of any codeword in $C$ of weight three. We denote this set by $STS_0$.

Let $C$ be a 1-perfect binary code. Let $v \in C$ be a codeword in $C$. The set of all $w \in C$ at distance three from $v$ is an $STS_v$ taking as the set of blocks $B$ the support of all the vectors $v + w$ $(\forall\, w \in C \mid d(w, v) = 3)$.

Starting from a 1-perfect code $C$ we can obtain different STSs, for instance $STS_0$, $STS_v$, etc.

An STS can be obtained from a 1-perfect code or not. In the case that the STS comes from a 1-perfect code, it can be unique or not and, moreover, if there is more than one 1-perfect code which gives the same STS, they do not need to be isomorphic nor equivalent.

Phelps (see [7]) constructs several 1-perfect codes in a combinatorial way which lead to 23 of 80 nonisomorphic STSs of length 15 (these STSs are called "perfect"). Levan (see [3]) adds 8 codes to the previous list.

In this paper we prove that starting from a well-ordered STS it is possible to construct a partition of $\boldsymbol{F}^n$ in 1-perfect codes such that the given STS is the support of the minimum-weight codewords. It will remain the same problem when the given STS is not well ordered.

**3. 1-perfect partitions.** In this paper, we are interested in 1-perfect codes which give rise to partitions of $\boldsymbol{F}^n$ in 1-perfect codes, rather than in 1-perfect codes alone.

We already know that, given any 1-perfect code $C$ of length $n$, we can always find a partition of $\boldsymbol{F}^n$ generated by this code. For example, the trivial partition $\{C_i \,|\, C_i = C + e_i;\, \forall\, i = 1, \ldots, n\}$, where $e_i$ are the different vectors of $\boldsymbol{F}^n$ of weight 1 and $e_0 = (0, 0, \ldots, 0)$, is a partition of $\boldsymbol{F}^n$ on 1-perfect codes, that is, a 1-perfect partition. The above partition is only natural when $C$ is a linear code, that is, in those cases where $C + C = C$.

In other 1-perfect codes, another type of partition would be more natural. For example, in propelinear codes (see [8]), it would be more natural to use the partition on $\boldsymbol{F}^n$ given by $\{C_i \,|\, C_i = C * e_i;\, \forall\, i = 1, \ldots, n\}$ since, for these codes, $C * C = C$.

Generally, for 1-perfect codes, there does not exist an operation on $\boldsymbol{F}^n$ allowing a natural partition. There is a gap in the literature on this aspect and this paper attemps to analyze it.

We begin by assuming that we have $\boldsymbol{F}^n$ partitioned into classes, each of which is a 1-perfect code. In every class other than the class $C$, which includes the vector 0, we can take a vector of weight 1 as a representative and, therefore, we can consider the partition as given by $\boldsymbol{A}_n = \{e_0, e_1, e_2, \ldots, e_n\}$.

THEOREM 3.1. *Given a 1-perfect partition $\boldsymbol{A}_n$ on $\boldsymbol{F}^n$ it is possible to define a distance-compatible action of $\boldsymbol{A}_n$ on $\boldsymbol{F}^n$, such that the given partition can be considered as a quasi group which is an $\boldsymbol{A}_n$-homomorphic image of $\boldsymbol{F}^n$.*

*Proof.* In essence, we assume a 1-perfect partition $\boldsymbol{A}_n$ and define an operation on $\boldsymbol{A}_n$ as follows:

$$e_i * e_j = e_k, \tag{3.1}$$

where $e_k$ represents the class containing the vector $e_i + e_j$. $\boldsymbol{A}_n$ has a quasi group structure with this operation, where $e_0$ is the zero element. In fact $\boldsymbol{A}_n$ has a Sloop structure.

This operation is not the only one which could be defined on $\boldsymbol{A}_n$.

Assuming that $\boldsymbol{A}_n$ has a quasi-group structure, it is important to observe whether $\boldsymbol{A}_n$ can be considered as an $\boldsymbol{A}_n$-homomorphic image of $\boldsymbol{F}^n$. For this purpose, we must have defined an operation on $\boldsymbol{F}^n$ or at least an operation between elements of $\boldsymbol{F}^n$ and $\boldsymbol{A}_n$ ($\boldsymbol{A}_n$ could be considered a subset of $\boldsymbol{F}^n$).

Given any element $c \in C$, we define $c \cdot e_i$ as the only element of class $e_i$ at distance one from $c$.

Given any element $v \in \boldsymbol{F}^n$, since $C$ is a 1-perfect code, we can always write it uniquely as $v = c \cdot e_i$, where $c \in C$. We now define an operation $\boldsymbol{F}^n \times \boldsymbol{A}_n \longrightarrow \boldsymbol{F}^n$ such that $v \cdot e_j = w$ is the only vector of the class $e_k \in \boldsymbol{A}_n$ at distance one from $v$, where $e_i * e_j = e_k$.

This operation $\boldsymbol{F}^n \times \boldsymbol{A}_n$ meets the conditions of Definition 2.3, so we have a distance-compatible action of $\boldsymbol{A}_n$ on $\boldsymbol{F}^n$.

Now we can define

$$\phi : \boldsymbol{F}^n \longrightarrow \boldsymbol{A}_n$$

such that $\phi(v) = e_i$ if and only if $v$ is in class $e_i$.

If $\phi(v \cdot e_j) = e_k$, then $e_i * e_j = e_k$, where $\phi(v) = e_i$. Hence $\phi(v) * \phi(e_j) = e_k$ and $\phi(v \cdot e_j) = \phi(v) * \phi(e_j)$, so $\phi$ is an $\boldsymbol{A}_n$-homomorphism, which is the identity map on $\boldsymbol{A}_n$. ∎

Now the inverse: let us assume that we have defined a distance-compatible action of $\boldsymbol{A}_n$ on $\boldsymbol{F}^n$ and also that we have defined a quasi-group structure with a zero element on $\boldsymbol{A}_n$.

With these conditions, we will consider the following theorem.

THEOREM 3.2. *Let us assume there is an $\boldsymbol{A}_n$-homomorphism $\phi : \boldsymbol{F}^n \longrightarrow \boldsymbol{A}_n$ which is the identity map on $\boldsymbol{A}_n$.*

*Then, for all $e_i \in \boldsymbol{A}_n$, the sets $H = \phi^{-1}(e_i) \subset \boldsymbol{F}^n$ are 1-perfect codes.*

*Proof.* First, we will see that the minimum distance of $H$ is 3.

Suppose $d(a,b) = 1$, where $a, b \in H$. For some index $j$, $a \cdot e_j = b$, since all $a \cdot e_j$ are different and we obtain the elements of $\boldsymbol{F}^n$ at distance one from $a$. Hence, $\phi(b) = \phi(a \cdot e_j) = \phi(a) * \phi(e_j) = \phi(a) * e_j$, but $\phi(a) = \phi(b)$, so $e_0 = e_j$, which contradicts the initial assumption.

Let us now assume $d(a,b) = 2$, where $a, b \in H$. There will be $e_i \neq e_j$ such that $a \cdot e_i = b \cdot e_j$. Hence $\phi(a \cdot e_i) = \phi(b \cdot e_j)$ and, since $\phi(a) = \phi(b)$, then $\phi(e_i) = \phi(e_j)$ and, therefore, $e_i = e_j$, which is impossible.

Finally, we will see that, given any element $v \in \boldsymbol{F}^n$, then either $v \in H$, or there is a unique element $w \in H$ such that $d(v,w) = 1$.

In essence, let us assume that $v \notin H$ and $\phi(H) = e_k$. Then for any index $i$, $\phi(v) = e_i$. Since $\forall\, j \in \boldsymbol{A}_n$, $j \neq 0$, the elements $e_i * e_j \in \boldsymbol{A}_n$ are all different, there will be a certain value for which $e_i * e_j = e_k$. Hence $\phi(v \cdot e_j) = \phi(v) * e_j = e_k$ and $w = v \cdot e_j \in H$. Moreover, $d(v,w) = 1$.

Suppose now that there is a $w' \in H$, $w' \neq w$ at distance 1 from $v$. This means that, for a certain $s$, we have $w' = v \cdot e_s$ and $\phi(w') = e_k$. Therefore, $e_i * e_s = e_k = e_i * e_j$ and $e_s = e_j$, contrary to what we assumed. □

According to this theorem, our interest lies, therefore, in defining distance-compatible actions of $\boldsymbol{A}_n$ on $\boldsymbol{F}^n$ for which $\boldsymbol{A}_n$ is a homomorphic image.

One way to do so is the following.

Fix an order in the set $\boldsymbol{A}_n - \{e_0\}$; for instance $e_1 < e_2 < e_3 \cdots < e_n$.

For $x \in \boldsymbol{F}^n$, $x = (x_1, x_2, \ldots, x_n)$ define the ordered support of $x$ as $s_x = e_{a_1} < e_{a_2} < \cdots < e_{a_r}$, where $e_{a_i} \in s_x$ if and only if $x_{a_i} = 1$.

Given an $STS(n)$ we can define in $\boldsymbol{A}_n = \{e_0, e_1, \ldots, e_n\}$ the Sloop structure as we stated in Definition 2.7. Hence, if $B$ is the set of blocks of the given STS we have

$$\left\{\begin{array}{llll} \text{if } e_i \neq e_j, & \text{then} & e_i * e_j = e_k, & \text{where } (e_i, e_j, e_k) \in B, \\ \text{if } e_i = e_j, & \text{then} & e_i * e_j = 0, & \\ \text{if } e_i = e_0, & \text{then} & e_i * e_j = e_j, & \\ \text{if } e_j = e_0, & \text{then} & e_i * e_j = e_i. & \end{array}\right. \tag{3.2}$$

For $x \in \boldsymbol{F}^n$ define the value $\phi(x)$ of $x$ in the following way:

$$\begin{array}{ccc} \boldsymbol{F}^n & \xrightarrow{\phi} & \boldsymbol{A}_n, \\ x & \longrightarrow & \phi(x) = ((\cdots((e_{a_1} * e_{a_2}) * e_{a_3}) * e_{a_4} * \cdots) * e_{a_r}), \end{array} \tag{3.3}$$

where $s_x = e_{a_1} < e_{a_2} < \cdots < e_{a_r}$.

Given $c_1, c_2, \ldots, c_r$, we will write $[c_1 c_2 \cdots c_r] \in \boldsymbol{A}_n$ to represent the result of the chain of operations $((\cdots((c_1 * c_2) * c_3) * c_4 * \cdots) * c_r)$.

Given $a, x, y \in \boldsymbol{A}_n$, the equation $(a * x) * y = (a * \bar{y}) * x$ always has a unique solution that can be calculated as

$$\bar{y} = [axyxa]. \tag{3.4}$$

For some STS the condition $\bar{y} = y$ is always true, for example, when we consider the first STS of the 80 possible STSs of length 15 (we will consider the list of 80 STSs to be ordered normally, as, for example, in [1]).

DEFINITION 3.3. *We will say that an STS is a well-ordered STS if it is possible to order the elements in $\boldsymbol{A}_n$ such that $\forall\, a, x, y \in \boldsymbol{A}_n$ we have $x < y$ if and only if $x < \bar{y}$, where $\bar{y} = [axyxa]$.*

LEMMA 3.4. *Let $(A^*, B)$ be a well-ordered STS and let $\boldsymbol{A}_n$ be the Sloop defined in* (3.2).

*Then there is a distance-compatible action of $\boldsymbol{A}_n$ on $\boldsymbol{F}^n$ such that the value map $\phi : \boldsymbol{F}^n \longrightarrow \boldsymbol{A}_n$ defined in* (3.3) *is an $\boldsymbol{A}_n$-homomorphism.*

*Proof.* Let $x = (x_1, x_2, \ldots, x_n) \in \boldsymbol{F}^n$, and let $s_x = e_{a_1} < e_{a_2} \cdots < e_{a_r}$ be the ordered support of $x$.

Then $\phi(x) * e_i = [e_{a_1} e_{a_2} \cdots e_{a_r} e_i] = [e_{a_1} e_{a_2} \cdots e_{a_{r-1}} e_{i'} e_{a_r}] = [e_{a_1} e_{a_2} \cdots e_{a_{r-2}} e_{i''} e_{a_{r-1}} e_{a_r}] = \ldots$, where $e_i < e_{a_r}$ if and only if $e_{i'} < e_{a_r}$ and $e_{i'} < e_{a_{r-1}}$ if and only if $e_{i''} < e_{a_{r-2}}$.

The same argument brings us finally to an index $j$ such that $\phi(x) * e_i = [e_{a_1} \cdots e_{a_{s-1}} e_j e_{a_s} \cdots e_{a_r}]$, where $e_{a_{s-1}} \le e_j < e_{a_s}$.

Now we define $\pi_x(e_i) = e_j$. $\pi_x$ is a permutation of $\{e_i \,|\, i = 1..n\}$ that allows us to define, for all $x \in \boldsymbol{F}^n$,

$$x \cdot e_i = x + e_j = x + \pi_x(e_i)$$

so that $\boldsymbol{A}_n$ acts on $\boldsymbol{F}^n$ and this is a distance-compatible action.

Furthermore, with the given definition, $\phi(x) * \phi(e_i) = \phi(x + e_j) = \phi(x \cdot e_i)$, so $\phi$ is an $\boldsymbol{A}_n$-homomorphism. □

As a consequence of Theorem 3.2 and Lemma 3.4, we can establish the following theorem which proves that the well-ordered property of STSs is of interest because it allows us to start from an $STS(n)$ and efficiently determine when there is a 1-perfect partition associated with it.

THEOREM 3.5. *Let $(A^*, B)$ be a well-ordered $STS(n)$ and let $\boldsymbol{A}_n$ be the Sloop defined in* (3.2).

*Then there is a distance-compatible action of $\boldsymbol{A}_n$ on $\boldsymbol{F}^n$ such that the value map $\phi : \boldsymbol{F}^n \longrightarrow \boldsymbol{A}_n$ gives us a partition of $\boldsymbol{F}^n$ into 1-perfect codes $H = \phi^{-1}(e_i)$ for all $e_i \in \boldsymbol{A}_n$.*

Starting from a well-ordered STS not only can we assure that $\boldsymbol{A}_n$ acts in a distance-compatible way on $\boldsymbol{F}^n$ but we can extend the action to all the elements in $\boldsymbol{F}^n$ as we can see in the following proposition.

PROPOSITION 3.6. *Let $(A^*, B)$ be a well-ordered STS and let $\boldsymbol{A}_n$ be the Sloop defined in* (3.2).

*Then we can extend the action of $\boldsymbol{A}_n \subset \boldsymbol{F}^n$ on $\boldsymbol{F}^n$ to an action of $\boldsymbol{F}^n$ on $\boldsymbol{F}^n$.*

*Proof.* Given $x, y \in \boldsymbol{F}^n$ with ordered supports $s_x = e_{a_1} < e_{a_2} \cdots < e_{a_r}$ and $s_y = e_{b_1} < e_{b_2} < \cdots < e_{b_s}$, respectively, we define $x \cdot y$ by using Lemma 3.4:

$$x \cdot y = (\cdots((x \cdot e_{b_1}) \cdot e_{b_2}) \cdots) \cdot e_{b_s}.$$

It is now easy to see that the previous operation is well defined, that is, $x \cdot y$ has a unique value, so we have an action of $\boldsymbol{F}^n$ on $\boldsymbol{F}^n$. □

*Remark.* Proposition 3.6 shows us that the well-ordered condition is stronger than needed to assure the construction of 1-perfect partitions starting from an STS (see Theorem 3.2). We will see in the following section that in the specific case $n = 15$ we can construct 1-perfect partitions starting in 16 $STS(15)$s, but this result does

not close the problem of finding all possible STSs which allow the construction of 1-perfect partitions.

A problem we leave open is the construction of distance-compatible actions of $\boldsymbol{A}_n \subset \boldsymbol{F}^n$ on $\boldsymbol{F}^n$ that cannot be extended to actions of $\boldsymbol{F}^n$ on $\boldsymbol{F}^n$.

**4. Well-ordered STSs.** We will now consider the STSs which have the well-ordered property.

In general, if the equality $(a * x) * y = (a * y) * x$ does not hold, we can calculate $\bar{y} = [axyxa]$ (see (3.4)) such that $(a*x)*y = (a*\bar{y})*x$ and, if the STS is well ordered, we obtain an element $\bar{y}$ that has the same order relationship with $x$ that $y$ has with $x$.

Whenever we vary $a \in \boldsymbol{A}_n$ in (3.4), we obtain $n$ elements, not necessarily different, that are greater than $x$ if $y > x$, or less than $x$ if $y < x$. For all $x \neq y$, we will use $q_{xy}$ to designate the set of different elements obtained:

$$q_{xy} = \{\bar{y} \in \boldsymbol{A}_n | \bar{y} = [axyxa] | a \in \boldsymbol{A}_n\}$$

The vector $(q_1, q_2, \ldots, q_n)$, where $q_i$ is the quantity of pairs $(x, y)$ for which $|q_{xy}| = i$, will be denoted the characteristic vector of the $STS(n)$ and, when $n = 15$, it is a complete invariant for STSs which allows us to distinguish completely nonisomorphic $STS(15)$s.

In the appendix, we have listed the 80 vectors which characterize the nonisomorphic $STS(15)$s. We have suppressed the coordinates $q_8, q_9, q_{10}, q_{11}, q_{12}, q_{13}, q_{14}, q_{15}$ in each vector since their value is always zero. Moreover, we have added to each vector a coordinate $q_{16}$ which allows us to decide which $STS(15)$s are well ordered, as we will see in Proposition 4.1.

There are other invariants which make it possible to distinguish between nonisomorphic $STS(15)$s, for example the *cycle structure* (see [5]), the *train* (see [5]), and the *fragments* (see [3]). We will use the invariant we propose, since it allows us to link the STS structure with the construction of perfect codes, as we will see later on.

All of the elements in $q_{xy}$'s have the same order relationship with $x$ that $y$ has with $x$.

Let us assume that for certain $y, y', y'' \in \boldsymbol{A}_n^*$ we have some elements $\alpha, \beta, \gamma \in A^*$ such that

$$\begin{aligned} &\alpha, \beta \in q_{\gamma y}, \\ &\alpha, \gamma \in q_{\beta y'}, \\ &\gamma, \beta \in q_{\alpha y''}. \end{aligned} \tag{4.1}$$

We will use $q_{16}$ to denote the quantity of triples $\alpha, \beta, \gamma$ that satisfy (4.1).

PROPOSITION 4.1. *The component $q_{16}$ in the characteristic vector of a well-ordered $STS(n)$ is zero (see the appendix to see the values of the $q_{16}$ for all the $STS$s of length 15).*

*Proof.* In essence, if $q_{16} \neq 0$, then there is a $\alpha, \beta, \gamma$ triple that fulfills (4.1). Nevertheless, this is absurd since, if $\alpha > \beta > \gamma$, the second equation fails; if $\alpha > \gamma > \beta$, the first equation fails, etc. For any assumption, one of the three equations in (4.1) always fails. □

Proposition 4.1 limits the number of $STS(15)$s for which it is possible to define a well-ordering that allows to obtain perfect codes. In particular, there are 16 $STS(15)$s that can be well ordered and, therefore, produce 1-perfect codes: $1 - 10$ and $13 - 18$. If, for each class of nonisomorphic $STS(15)$s, we choose as representative the one

TABLE 4.1
*Well-ordered STSs for $n = 15$.*

| STS | Ordering |
|---|---|
| 1 | 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15 |
| 2 | 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15 |
| 3 | 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15 |
| 4 | 1,2,3,4,5,6,7,8,11,9,10,12,15,13,14 |
| 5 | 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15 |
| 6 | 1,2,3,4,5,6,7,8,11,9,10,12,14,13,15 |
| 7 | 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15 |
| 8 | 1,2,3,4,5,6,7,8,11,13,14,9,10,12,15 |
| 9 | 1,2,3,4,5,6,7,8,14,9,15,10,12,11,13 |
| 10 | 1,2,3,4,5,6,7,8,14,10,12,9,15,11,13 |
| 13 | 1,2,3,4,5,6,7,8,11,13,14,9,10,12,15 |
| 14 | 1,2,3,4,5,6,7,8,11,13,14,9,10,12,15 |
| 15 | 1,2,3,4,5,6,7,8,11,12,15,9,10,13,14 |
| 16 | 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15 |
| 17 | 1,2,3,4,5,6,7,8,11,13,14,9,10,12,15 |
| 18 | 1,2,3,4,5,6,7,8,12,9,13,10,14,11,15 |

given in [1], an example of well-ordering (although not the only one), calculated computationally, associated with each of these $STS(15)$s, is the one listed in Table 4.1.

In the specific case $n = 15$, we have studied the codes constructed using the well-ordering given in Table 4.1 and calculated $r_e$ and $r_n$, respectively the outer rank and dimension of the kernel:

$$r_e = \min\{k | k = \dim(E),\ C \subset E,\ E \text{ is a vector space}\},$$

$$r_n = \dim(E), \text{ where } E = \{x \in C | x + C \subset C\}.$$

The results obtained, for the representatives we have chosen from each family, are as follows:

| STS | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $r_n$ | 11 | 9 | 8 | 7 | 8 | 6 | 8 | 7 | 6 | 6 | 6 | 6 | 6 | 8 | 6 | 6 |
| $r_e$ | 11 | 12 | 13 | 13 | 13 | 13 | 13 | 14 | 14 | 14 | 14 | 14 | 14 | 14 | 14 | 14 |

For a given STS, by considering other well-orderings, we can obtain 1-perfect codes that are neither isomorphic nor equivalent amongst themselves. Thus, for each STS we obtain a family of 1-perfect codes.

For a given code $C$, if we consider $C + v$, where $v \in C$, we obtain another code equivalent to the first one that does not have to have the same $STS(n)$ associated with it, or, in other words, the $STS_v$s associated with each of the codewords $v \in C$ do not necessarily have to match (if they match, the code is known as *homogeneous*).

In general, each of these $STS(n)$s, together with a well-ordering, will result in a partition, taking as classes $C_i = \{x | x \in \boldsymbol{F}^n, \text{ where } \phi(x) = e_i\}$, where all the classes are 1-perfect codes (what we have called a 1-perfect partition).

**5. Error-correcting, coding, and decoding.** With the codes obtained, error-correcting is very easy. In essence, the codewords are characterized by having a constant value (the value map is defined in (3.3)). Therefore, when we receive a word, we can calculate its value and use it as a syndrome to correct errors.

Let us assume a code $C$ defined using a well-ordered STS, which consists of all the vectors with value $e_i$, $C = \{v \in \boldsymbol{F}^n \mid \phi(v) = e_i\}$.

TABLE 5.1
*Redundant bits for code* 17.

| $\phi$ | $x_{10}=0$ | $x_{10}=1$ |
|---|---|---|
| 0 | 0000 | 0111 |
| 1 | 1001 | 1110 |
| 2 | 1010 | 1101 |
| 3 | 1111 | 1000 |
| 4 | 1100 | 1011 |
| 5 | 0110 | 0001 |
| 6 | 0011 | 0100 |
| 7 | 0101 | 0010 |
| 8 | 1011 | 1100 |
| 9 | 0100 | 0011 |
| 10 | 0111 | 0000 |
| 11 | 1101 | 1010 |
| 12 | 0010 | 0101 |
| 13 | 1110 | 1001 |
| 14 | 1000 | 1111 |
| 15 | 0001 | 0110 |

Given any vector $v \in \boldsymbol{F}^n$, we can compute its syndrome $\phi(v)$ and we will have $\phi(v) = e_i$ if and only if $v \in C$.

If $v \notin C$, we have $\phi(v) = e_k$, where $e_k \neq e_i$. Let $e_j$ be such that $e_i = e_k * e_j$. Now we will calculate the only vector $w \in C$ at distance one from $v$ as $w = v \cdot e_j$, since $d(v, w) = 1$ and $\phi(w) = \phi(v \cdot e_j) = \phi(v) * e_j = e_k * e_j = e_i$ (see Theorem 3.5).

Concerning coding-decoding, we were unable to show that, for any value of $n$, the codes obtained are systematic, although in the specific case $n = 15$, Table 4.1 gives systematic codes where the 11 information coordinates are $1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 13$ and the 4 redundant coordinates are $11, 12, 14, 15$ (after the well-ordering).

We have not included the proof that the codes in Table 4.1 are systematic since it is only of interest in the particular case $n = 15$.

*Example.* We will provide an example of the above, using the code 17 defined with the order given in Table 4.1.

The STS which results in this code is formed by the following triples (see [1]):
(1, 2, 3), (1, 4, 5), (1, 6, 7), (1, 8, 9), (1, 10, 11), (1, 12, 13),
(1, 14, 15), (2, 4, 6), (2, 5, 7), (2, 8, 10), (2, 9, 11), (2, 12, 14),
(2, 13, 15), (3, 4, 7), (3, 5, 6), (3, 8, 12), (3, 9, 13), (3, 10, 14),
(3, 11, 15), (4, 8, 15), (4, 9, 14), (4, 10, 13), (4, 11, 12), (5, 8, 11),
(5, 9, 12), (5, 10, 15), (5, 13, 14), (6, 8, 14), (6, 9, 10), (6, 11, 13),
(6, 12, 15), (7, 8, 13), (7, 9, 15), (7, 10, 12), (7, 11, 14).

The codeword that we wish to construct will be $v$, of which we know the 11 coordinates $x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_{11}, x_{13}, x_{10}$. Starting with these coordinates and using the value $\phi(v)$ we can calculate the 4 redundant symbols $x_{14}, x_9, x_{12}, x_{15}$, according to the coordinate 10 in the way described in Table 5.1.

- Let us suppose the information is given by the 11 bits 010 111 001 10, which we assume are the coordinates $1, 2, 3, 4, 5, 6, 7, 8, 11, 13, 10$ of the codeword we wish to construct (we have used the order given in Table 4.1 for code 17).
- Using the operation defined in $\boldsymbol{A}_n$ (according to the Steiner triples), we calculate $\phi = [x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_{11}, x_{13}] = [e_2, e_4, e_5, e_6, e_{11}, e_{13}] = e_7$.
- According to Table 5.1, for this value of $\phi(v) = e_7$ and knowing $x_{10} = 0$,

there is a redundancy 0101 for which the codeword will be

$$v = (010\,111\,001\,101\,001)$$

(the order of the coordinates is $1, 2, 3, 4, 5, 6, 7, 8, 11, 13, 14, 9, 10, 12, 15$).

- Let us assume that a transmission error has occurred and that the vector received is $w = (010\,101\,001\,101\,001)$.
- Let us calculate the syndrome for the vector received as $\phi(w) = [e_2, e_4, e_6, e_{11}, e_{13}, e_9, e_{15}] = e_5$.
- We will correct the error made by calculating the vector $v = w \cdot e_5$ since $\phi(v) = \phi(w \cdot e_5) = e_5 * e_5 = 0$;
  $\phi(v) = \phi(w \cdot e_5) = \phi(w) * e_5 = [e_2, e_4, e_6, e_{11}, e_{13}, e_9, e_{15}] * e_5 =$
  $[e_2, e_4, e_6, e_{11}, e_{13}, e_9, e_{15}, e_5] = [e_2, e_4, e_6, e_{11}, e_{13}, e_9, e_5, e_{15}] =$
  $[e_2, e_4, e_6, e_{11}, e_{13}, e_1, e_9, e_{15}] = [e_2, e_4, e_6, e_{11}, e_5, e_{13}, e_9, e_{15}] =$
  $[e_2, e_4, e_6, e_5, e_{11}, e_{13}, e_9, e_{15}] = [e_2, e_4, e_5, e_6, e_{11}, e_{13}, e_9, e_{15}]$,
  so $v = (010111001101001)$.

*Remark.* The calculation made, $[e_{a_1} e_{a_2} \cdots e_{a_r} e_i] = [e_{a_1} e_{a_2} \cdots e_{a_{r-1}} e_{i'} e_{a_r}] = [e_{a_1} e_{a_2} \ldots e_{a_{r-2}} e_{i''} e_{a_{r-1}} e_{a_r}] = \ldots$ is as described in (3.4).

**6. Conclusions and further research.** In this paper, we have seen that a partition of the $n$-cube on 1-perfect codes is equivalent to having a quasi-group structure $\boldsymbol{A}_n = \{e_0, e_1, e_2, \ldots, e_n\}$, with zero element $e_0 = 0$, which acts in a distance-compatible way on $\boldsymbol{F}^n$ and is an $\boldsymbol{A}_n$-homomorphic image of $\boldsymbol{F}^n$.

In the specific case that $\boldsymbol{A}_n$ is considered to be the structure derived from a well-ordered STS, we have seen an effective way to construct 1-perfect partitions and, therefore, 1-perfect codes, that in the case $n = 15$ are systematic. Moreover, it is not difficult to see that according to the nomenclature of Etzion and Vardy (see [2]), these 1-perfect codes are of the noninterlaced type.

Further research in this topic should include the following:

- A consideration of quasi-group structures on $\boldsymbol{A}_n$ with more characteristics, for example, commutativity or associativity. In the extreme case, analysis should also consider the case when $\boldsymbol{A}_n$ has the commutative group structure. In this situation, the factorization theorem of commutative groups indicates what the $\boldsymbol{A}_n$ algebraic structure should be like.
- A consideration of distance-compatible actions of $\boldsymbol{A}_n$ on $\boldsymbol{F}^n$, which vary from the one given by the construction included in this paper. For instance it could be interesting to construct distance-compatible actions of $\boldsymbol{A}_n$ on $\boldsymbol{F}^n$ that could not be extended the whole $n$-cube.
- The existence of well-ordered STSs for all $n$ as well as is proved in the specific case $n = 15$.
- The codes obtained in this paper are systematic for any value of $n$ as well as in the case $n = 15$.
- Characterization of the 1-perfect partitions such that we use the partition to determine the algebraic properties of the perfect codes which make it up. For example, using uniform 1-perfect partitions, we can give the propelinear structure to all the classes of the partition (see [8]).

**Appendix.**

| STS | $q_1$ | $q_2$ | $q_3$ | $q_4$ | $q_5$ | $q_6$ | $q_7$ | $q_{16}$ |
|---|---|---|---|---|---|---|---|---|
| 1 | 225 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 129 | 96 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 113 | 24 | 24 | 64 | 0 | 0 | 0 | 0 |
| 4 | 73 | 60 | 60 | 32 | 0 | 0 | 0 | 0 |
| 5 | 73 | 108 | 12 | 32 | 0 | 0 | 0 | 0 |
| 6 | 45 | 42 | 90 | 48 | 0 | 0 | 0 | 0 |
| 7 | 57 | 36 | 36 | 96 | 0 | 0 | 0 | 0 |
| 8 | 65 | 52 | 12 | 32 | 28 | 28 | 8 | 0 |
| 9 | 41 | 32 | 48 | 52 | 34 | 18 | 0 | 0 |
| 10 | 41 | 36 | 62 | 46 | 26 | 12 | 2 | 0 |
| 11 | 25 | 6 | 50 | 62 | 62 | 12 | 8 | 64 |
| 12 | 41 | 12 | 69 | 48 | 45 | 0 | 10 | 64 |
| 13 | 57 | 20 | 28 | 72 | 48 | 0 | 0 | 0 |
| 14 | 65 | 12 | 24 | 72 | 36 | 12 | 4 | 0 |
| 15 | 37 | 30 | 50 | 40 | 32 | 36 | 0 | 0 |
| 16 | 113 | 0 | 0 | 56 | 0 | 0 | 56 | 0 |
| 17 | 57 | 12 | 12 | 64 | 24 | 48 | 8 | 0 |
| 18 | 37 | 30 | 38 | 48 | 24 | 44 | 4 | 0 |
| 19 | 21 | 14 | 42 | 64 | 36 | 36 | 12 | 64 |
| 20 | 23 | 6 | 36 | 49 | 63 | 39 | 9 | 64 |
| 21 | 25 | 0 | 15 | 81 | 69 | 21 | 14 | 91 |
| 22 | 21 | 0 | 12 | 86 | 77 | 12 | 17 | 91 |
| 23 | 23 | 6 | 47 | 42 | 57 | 34 | 16 | 122 |
| 24 | 23 | 4 | 38 | 44 | 57 | 34 | 25 | 173 |
| 25 | 33 | 4 | 21 | 45 | 58 | 51 | 13 | 167 |
| 26 | 37 | 6 | 32 | 36 | 51 | 42 | 21 | 165 |
| 27 | 21 | 2 | 29 | 37 | 64 | 57 | 15 | 183 |
| 28 | 21 | 2 | 25 | 41 | 53 | 61 | 22 | 224 |
| 29 | 29 | 6 | 18 | 54 | 42 | 54 | 22 | 178 |
| 30 | 21 | 0 | 10 | 41 | 76 | 51 | 26 | 252 |
| 31 | 23 | 8 | 56 | 38 | 50 | 34 | 16 | 96 |
| 32 | 17 | 0 | 15 | 52 | 49 | 60 | 32 | 252 |
| 33 | 17 | 0 | 11 | 33 | 56 | 61 | 47 | 297 |
| 34 | 19 | 0 | 10 | 33 | 51 | 75 | 37 | 282 |
| 35 | 25 | 0 | 0 | 30 | 48 | 72 | 50 | 313 |
| 36 | 19 | 0 | 8 | 32 | 96 | 56 | 14 | 268 |
| 37 | 19 | 0 | 0 | 24 | 72 | 36 | 74 | 322 |
| 38 | 19 | 0 | 4 | 23 | 44 | 83 | 52 | 337 |
| 39 | 19 | 0 | 6 | 39 | 64 | 73 | 24 | 290 |
| 40 | 23 | 0 | 6 | 29 | 73 | 61 | 33 | 298 |

| STS | $q_1$ | $q_2$ | $q_3$ | $q_4$ | $q_5$ | $q_6$ | $q_7$ | $q_{16}$ |
|---|---|---|---|---|---|---|---|---|
| 41 | 23 | 0 | 3 | 26 | 62 | 76 | 35 | 315 |
| 42 | 17 | 0 | 0 | 17 | 71 | 79 | 41 | 368 |
| 43 | 21 | 0 | 3 | 9 | 105 | 69 | 18 | 296 |
| 44 | 17 | 0 | 4 | 19 | 65 | 77 | 43 | 354 |
| 45 | 17 | 0 | 7 | 20 | 61 | 76 | 44 | 334 |
| 46 | 17 | 0 | 0 | 14 | 53 | 88 | 53 | 373 |
| 47 | 17 | 0 | 9 | 32 | 56 | 70 | 41 | 299 |
| 48 | 17 | 0 | 5 | 23 | 69 | 73 | 38 | 317 |
| 49 | 17 | 0 | 2 | 16 | 58 | 84 | 48 | 361 |
| 50 | 17 | 0 | 2 | 26 | 62 | 88 | 30 | 300 |
| 51 | 19 | 0 | 1 | 21 | 58 | 91 | 35 | 354 |
| 52 | 17 | 0 | 2 | 25 | 59 | 83 | 39 | 344 |
| 53 | 19 | 0 | 3 | 33 | 63 | 69 | 38 | 307 |
| 54 | 19 | 0 | 6 | 34 | 63 | 68 | 35 | 311 |
| 55 | 17 | 0 | 6 | 25 | 57 | 91 | 29 | 344 |
| 56 | 17 | 0 | 4 | 23 | 64 | 79 | 38 | 333 |
| 57 | 17 | 0 | 3 | 12 | 70 | 82 | 41 | 333 |
| 58 | 17 | 0 | 5 | 40 | 75 | 56 | 32 | 259 |
| 59 | 17 | 0 | 6 | 43 | 66 | 69 | 24 | 295 |
| 60 | 17 | 0 | 0 | 21 | 57 | 81 | 49 | 364 |
| 61 | 15 | 0 | 0 | 63 | 77 | 21 | 49 | 91 |
| 62 | 15 | 0 | 9 | 26 | 44 | 90 | 41 | 328 |
| 63 | 15 | 2 | 12 | 37 | 48 | 75 | 36 | 271 |
| 64 | 15 | 0 | 3 | 24 | 53 | 66 | 64 | 337 |
| 65 | 15 | 0 | 3 | 18 | 57 | 88 | 44 | 350 |
| 66 | 15 | 0 | 0 | 15 | 52 | 93 | 50 | 374 |
| 67 | 15 | 0 | 0 | 13 | 60 | 99 | 38 | 377 |
| 68 | 15 | 0 | 2 | 18 | 68 | 80 | 42 | 359 |
| 69 | 15 | 0 | 2 | 14 | 47 | 86 | 61 | 379 |
| 70 | 15 | 0 | 7 | 28 | 53 | 88 | 34 | 338 |
| 71 | 15 | 0 | 4 | 11 | 59 | 85 | 51 | 355 |
| 72 | 15 | 0 | 1 | 17 | 60 | 87 | 45 | 360 |
| 73 | 15 | 0 | 0 | 14 | 50 | 98 | 48 | 380 |
| 74 | 15 | 0 | 16 | 32 | 40 | 98 | 24 | 289 |
| 75 | 15 | 0 | 3 | 36 | 63 | 90 | 18 | 337 |
| 76 | 15 | 0 | 15 | 25 | 85 | 45 | 40 | 330 |
| 77 | 15 | 0 | 0 | 3 | 33 | 111 | 63 | 412 |
| 78 | 15 | 0 | 4 | 26 | 62 | 98 | 20 | 340 |
| 79 | 15 | 0 | 18 | 18 | 72 | 90 | 12 | 212 |
| 80 | 15 | 0 | 0 | 0 | 0 | 90 | 120 | 455 |

**Acknowledgments.** The author wishes to thank J. Borges, K. Phelps, and J. Pujol for useful discussions and valuable comments during the preparation of this paper.

## REFERENCES


[1] C.J. Colbourn and J.H. Dinitz, *The CRC Handbook of Combinatorial Designs*, CRC Press, Boca Raton, FL, 1996.

[2] T. Etzion and A. Vardy, *Perfect binary codes: Constructions, properties and enumeration*, IEEE Trans. Inform. Theory, 40 (1994), pp. 754–763.

[3] J.M. LeVan, *Designs and Codes*, Ph.D. thesis, Auburn University, Auburn, AL, 1995.

[4] F.J. MacWilliams and N.J.A. Sloane, *Error Correcting Codes*, North–Holland, New York, 1977.

[5] R.A. Mathon, K.T. Phelps, and A. Rosa, *Small triple systems and their properties*, Ars Combin., 15 (1983), pp. 3–110.

[6] H.O. Pflugfelder, *Quasigroups and Loops. Introduction*, Helderman-Verlag, Berlin, 1990.

[7] K.T. Phelps, *A combinatorial construction of perfect codes*, SIAM J. Algebraic Discrete Meth., 4 (1983), pp. 398–403.

[8] J. Rifà and J. Pujol, *Distance invariant propelinear codes*, IEEE Trans. Inform. Theory, 43 (1997), pp. 590–598.

[9] H.S. White, F.N. Cole, and L.D. Cummings, *Complete classification of the triad systems of fifteen elements*, Mem. Mat. Acad. Sci. USA, 2nd memoir, 14 (1919), pp. 1–89.