On the Characterization of Linear Uniquely Decodable Codes

G. Cohen, J. Rifà, J. Tena, G. Zémor*

October 1998

Abstract

A Uniquely Decodable (UD) Code is a code such that any vector of the ambient space has a unique closest codeword. In this paper we begin a study of the structure of UD codes and identify perfect subcodes. In particular we determine all linear UD codes of covering radius ≤ 2.

1 Introduction

We call *n-cube* or *hypercube* of dimension n the graph whose vertices are all the binary vectors of length n, two vertices being adjacent if their Hamming distance is one. If a subgraph Γ of the n-cube $\mathbb{F}^n$ is isomorphic to the r-subcube $\mathbb{F}^r$ we will say that Γ *is* an r-subcube ($r \leq n$). Clearly an r- subcube of $\mathbb{F}^n$ is obtained by taking all vectors that have some fixed values in $n-r$ fixed coordinate positions.

A *Perfect Dominating Set* (PDS) S of a graph Γ is a set of vertices of Γ such that every vertex of Γ is either in S or adjacent to *exactly* one vertex of S. Removing "exactly" yields a Dominating Set (DS). The latter appears in quite a variety of contexts : in Game theory, a DS is a kernel, and its existence implies a winning strategy for one of the two players (namely, force the opponent into the kernel, see [2]). In this setting a PDS gives a unique winning strategy.

*G.Cohen and G.Zémor are with ENST, Dept Inf. and Res., J.Rifà is with the Computer Science Department in the Autonomous University of Barcelona and J.Tena is with the Mathematics Department in the University of Valladolid. This work has been partially supported by Spanish grant TEL97-0663 and the French-Spanish Integrated Action HF97-047

In computer architecture a common model of parallel processor network is a d- regular graph (e.g. a cube). In case of edge or vertex failure, one tries to reconfigurate the surviving network into an induced regular graph too. Then a PDS is in a sense optimal, as shown by the following result essentially due to Weichsel ([11]).

Proposition 1 *If Γ is a d- regular graph, then Δ is a $(d-1)$-regular induced subgraph of Γ if and only if $V(\Gamma) - V(\Delta)$ is a PDS of Γ.*

Proof: A vertex $v \in V(\Delta)$ is adjacent to exactly $d-1$ vertices of Δ if and only if it is adjacent to exactly one vertex in $V(\Gamma) - V(\Delta)$. ∎

Examples: Let Γ be the n-cube $\mathbb{F}^n$.

1. The set Γ is a -trivial- PDS
2. Any hypercube S of dimension $n-1$ is a PDS. Since S fixes a coordinate with value 0 or 1, any remaining vector is at distance one from exactly one vector of S.
3. If $n = 2^m - 1$ for some positive integer m, then a perfect 1–error correcting code is a PDS, whose connected components are 0-cubes, i.e. isolated points.

In [11] it is proved that all the connected components of a PDS in $\mathbb{F}^n$ are subcubes, and that if r is the dimension of a component, then $n - r \equiv 1$ or $3 \pmod 6$. A PDS is *uniform* if all the components have the same dimension. Furthermore, if all the components fix the same set of coordinate positions, we say that the PDS is *parallel*. In [7], uniform and non parallel PDS's can be found. Weichsel conjectured that all PDS are uniform. This was proved for $n \leq 8$, however disproved for $n = 13$ in [10].

If S is a parallel PDS in the n-cube, then there exists a perfect single-error-correcting code in $\mathbb{F}^{n-r}$ i.e. an independent PDS, where r is the common dimension of the components in S (see [4]).

The goal of this paper is to initialize a study of a natural generalization of PDS : we shall require that every vertex not in S has a unique closest element in S. In the case of the Hamming cube and its q-ary extension, S will be called a uniquely decodable (UD) code, and denoted by C. More formally,

Definition 2 *A subset $C \subseteq \mathbb{F}^n$ is a* uniquely decodable (UD) code *if $\forall \mathbf{v} \in \mathbb{F}^n \;\; \exists! \mathbf{c} \in C$ such that $d(\mathbf{v}, C) = d(\mathbf{v}, \mathbf{c})$.*

Denoting by $\rho = max\{d(\mathbf{v}, C) \mid \mathbf{v} \in \mathbb{F}_2^n\}$ the *covering radius* of C, (see [5]), we see that a PDS is a UD code with $\rho = 1$.

Note that this defines a notion akin to "discrete convexity": any point has a unique projection on S.

In a UD code, Voronoi regions and decoding regions coincide, namely with the following sets

$$V(\mathbf{c}) = \{\mathbf{x} \in \mathbb{F}^n : \mathrm{d}(\mathbf{x}, \mathbf{c}) = \mathrm{d}(\mathbf{x}, \mathrm{C})\}.$$

Thus a UD code yields a tiling of $\mathbb{F}^n$ by tiles $V(0)$ centered at codewords (see [6] for more on tilings).

The notion of a UD codes appears for the first time in the book of van Lint (see [9]) and, although a natural combinatorial object, has seemingly not attracted attention ever since.

Notice that perfect codes are particular instances of UD codes. A general natural construction of new UD codes from old ones goes as follows : Suppose S and S' are UD codes in Γ and Γ' respectively, then the Cartesian product $S \times S'$ is a UD code in $\Gamma \times \Gamma'$. In the linear case, the Cartesian product is equivalent to the direct sum.

Surprisingly enough, finding other linear UD codes seems a difficult open problem.

The paper is organised as follows : in Section 2 we investigate the structure of general binary linear UD code and identify perfect subcodes. In Section 3 we apply those results to solve the existence problem for UD codes in the case when the covering radius $\rho \leq 2$. Finally, nonlinear and nonbinary versions of Section 2 are envisaged.

2 The perfect subcodes of a linear UD code

Let C be a UD code with minimal distance d. First observe that d must be odd : otherwise, some vectors would be at distance $d/2$ from at least two codewords. For the rest of this section we suppose C is binary and linear. First we deal with the case when $d = 1$. We have the following easy proposition.

Proposition 3 *If the direct sum $C = C' \oplus C''$ is a UD code, then C' and C'' are UD.*

Proof: Suppose C' and C'' are of lengths n' and n''. Let $\mathbf{v}'$ be any vector in $\mathbb{F}^{n'}$. Append a string of n'' zeros to form a vector $\mathbf{v}$ of $\mathbb{F}^n$. Let $\mathbf{c}$ be the

unique codeword of C closest to $\mathbf{v}$. Discard the n'' last coordinates of $\mathbf{c}$ to obtain the unique codeword of C' closest to $\mathbf{v}'$. Therefore C' is UD. ∎

Let C'' be the maximal complete $[r, r, 1]$ subcode of C. Then C clearly decomposes into a direct sum $C = C' \oplus C''$. The above proposition implies that C' is a UD code with minimum distance ≥ 3. The study of linear UD codes reduces therefore to the study of linear UD codes with minimum distance $d \geq 3$.

Remark : in the terminology of the introduction, a linear UD code is uniform and parallel.

Suppose now $d \geq 3$. Consider the set $\mathcal{V}$ of all minimum weight codewords of C. Let $2e + 1$ be their common weight. Denote by $supp(\mathbf{v})$ the support of a vector $\mathbf{v} \in \mathbb{F}^n$. For a subset L of $\mathbb{F}^n$, we shall denote by $supp(L)$ the union of the supports of the vectors of L.

Definition 4 *Call two vectors* $\mathbf{v}$ *and* $\mathbf{w}$ *of* $\mathcal{V}$ adjacent, $\mathbf{v}$ — $\mathbf{w}$ *for short, if*

$$|supp(\mathbf{v}) \cap supp(\mathbf{w})| = e.$$

The above adjacency condition defines a graph on the vertex set $\mathcal{V}$. The object of this section is to prove :

Proposition 5 *Let* $\mathcal{M}$ *be a connected component of* $\mathcal{V}$ *and consider the vector space* D *generated by the vectors in* $\mathcal{M}$. D *is a perfect linear code.*

We shall prove proposition 5 by invoking the following theorem, ([1] Theorem 3, pag. 376).

Theorem 6 *Let* D *be a linear code over* $GF(q)$ *of length* n *and minimum weight* $d = 2e + 1$, *and let* $\mathcal{D}$ *be the holding pattern of the code vectors of weight* d. *Then* D *is perfect if and only if* $\mathcal{D}$ *is a* t*-design on the set* S *of coordinate places of type* $(q-1)^e; (e+1) - d - n$.

In the binary case the t*-design is of type* $1; (e+1) - d - n$.

Therefore, we only need to prove that the codewords of $\mathcal{M}$ make up the blocks of an $(e+1)$-design. We shall achieve this through some intermediate lemmas.

Lemma 7 *Let* $\mathbf{v}, \mathbf{w} \in \mathcal{M}$, *with* $P = supp(\mathbf{v}) \cap supp(\mathbf{w})$, *and suppose that* $|P| = e$, *i.e.* $\mathbf{v}$ — $\mathbf{w}$. *Let* $p \in P$ *and let* $a \in supp(\mathbf{v}) \setminus P$, $b \in supp(\mathbf{w}) \setminus P$,

Then there exists a codeword $\mathbf{x} \in \mathcal{M}$, *such that*

1. $\mathbf{x}$ — $\mathbf{v}$ *and* $\mathbf{x}$ — $\mathbf{w}$

2. $supp(\mathbf{x}) \supset P \setminus \{p\} \cup \{a, b\}$.

Proof: Let $A = P \cup \{a, b\}$. The set A has size $|A| = e+2$ and, identified with its characteristic vector, is such that $d(A, \mathbf{v}) = e + 1$, and $d(A, \mathbf{w}) = e + 1$. Therefore, since code C is UD, there exists a codeword $\mathbf{y}$ at distance at most e from A. Since the weight of $\mathbf{y}$ is at least $d = 2e+1$, $\mathbf{y}$ must contain A and we have $w(\mathbf{y}) = 2e+1$ or $w(\mathbf{y}) = 2e+2$. But because $P \cup \{a\} \subset supp(\mathbf{v}) \cap supp(\mathbf{y})$ we must actually have $w(\mathbf{y}) = 2e + 2$.

Consider now $A \setminus \{p\}$. We have $|A \setminus \{p\}| = e + 1$, so that $A \setminus \{p\}$ is at distance $e + 1$ from both $\mathbf{y}$ and the 0 codeword. Therefore, again because C is UD, there must exist a codeword $\mathbf{x}$ at distance at most e from $A \setminus \{p\}$. Codeword $\mathbf{x}$ must therefore be of minimum weight and satisfies the conclusion of the lemma. ∎

Lemma 8 *Let* $\mathbf{v}$ *and* $\mathbf{w}$ *be two codewords of* $\mathcal{M}$ *such that* $\mathbf{v}$ — $\mathbf{w}$. *Let* $A \subset supp(\mathbf{v})$ *be such that* $|A| = e$ *and let* $b \in supp(\mathbf{w})$. *Then there exists a codeword* $\mathbf{u}$ *of* $\mathcal{M}$ *whose support contains* $A \cup \{b\}$.

Proof: Let $P = supp(\mathbf{v}) \cap supp(\mathbf{w})$. If $b \in supp(\mathbf{v})$ or if $A = P$, there is nothing to prove : $\mathbf{u} = \mathbf{v}$ or $\mathbf{u} = \mathbf{w}$. Otherwise, apply Lemma 7 to obtain a vector $\mathbf{w}'$ such that $\mathbf{v}$ and $\mathbf{w}'$ satisfy the hypothesis of the lemma with $|A \cap supp(\mathbf{w}')| > |A \cap supp(\mathbf{w})|$. Reapply Lemma 7 as many times as necessary. ∎

Lemma 9 *Let* $\mathbf{v}, \mathbf{w} \in \mathcal{M}$. *Let* $A \subset supp(\mathbf{v})$ *be such that* $|A| = e$ *and let* $b \in supp(\mathbf{w})$. *Then there exists a codeword in* $\mathcal{M}$ *containing* $A \cup \{b\}$.

Proof: Since $\mathbf{v}, \mathbf{w} \in \mathcal{M}$ there is a chain $\mathbf{v} = \mathbf{v}_1, \ldots, \mathbf{v}_s = \mathbf{w}$ of length s between $\mathbf{v}$ and $\mathbf{w}$. Proceed by induction on s. If $s = 1$ then Lemma 8 gives the result. Otherwise, apply Lemma 8 to $\mathbf{v}_{s-1}$ and $\mathbf{v}_s$, b, and the set $supp(\mathbf{v}_{s-2}) \cap supp(\mathbf{v}_{s-1})$ instead of A. We obtain a codeword $\mathbf{u}$ such that $b \in supp(\mathbf{u})$ and $\mathbf{u}$ — $\mathbf{v}_{n-2}$. ∎

Let M be the union of supports of the codewords in $\mathcal{M}$. We now prove our claim that $(M, \mathcal{M})$ is a $(e + 1)$-design ; or equivalently that any set of $e + 1$ elements of M is contained in a the support of a vector of $\mathcal{M}$. To do this, we prove by induction on k that any subset $K \subset M$ of k elements, $k \leq e + 1$, is contained in a codeword of $\mathcal{M}$.

The result is clearly true for $k = 1$ by definition of $\mathcal{M}$. Suppose it proved for $k < e+1$, and let $K \subset M$ with $|K| = k$. Let $b \in M \setminus K$. By the induction hypothesis, there exists a codeword $\mathbf{v} \in \mathcal{M}$ such that $K \subset supp(\mathbf{v})$. Let

$\mathbf{w} \in \mathcal{M}$ be such that $b \in supp(\mathbf{w})$. Choose any $A \subset M$ such that $|A| = e$, $K \subset A \subset supp(\mathbf{v})$ and apply Lemma 9 to $\mathbf{v}, \mathbf{w}, A, b$: this proves the result for $k+1$, and completes the proof of proposition 5.

Corollary 10 *Let D_1 and D_2 be two different perfect subcodes of C generated by two connected components $\mathcal{M}_1$ and $\mathcal{M}_2$. Then $|supp(D_1) \cap supp(D_2)| < e$.*

Proof: Otherwise take $A \subset supp(D_1) \cap supp(D_2)$ with $|A| = e$. Since $\mathcal{M}_1$ and $\mathcal{M}_2$ are designs, there exist two codewords $\mathbf{v}$ and $\mathbf{w}$ of $\mathcal{M}_1$ and $\mathcal{M}_2$ respectively whose supports both contain A. But then $\mathbf{v}$ and $\mathbf{w}$ are adjacent, so they cannot be in different connected components. ∎

As mentioned in the introduction, PDS are UD codes with covering radius $\rho = 1$. A natural step, therefore, towards classifying all UD codes is to study the case $\rho = 2$. This is the object of the next section.

3 Linear UD codes of covering radius 2

In this section we prove :

Theorem 11 *A linear UD code with covering radius 2 and minimum distance $d \geq 3$ is either the trivial $[5, 1, 5]$ repetition code or the product of two Hamming codes.*

We start with two simple propositions.

Proposition 12 *Let D be a perfect subcode of a UD code C, with $d(D) = 2e+1$. Then $d(C \setminus D, D)$ is an odd integer, say $2f+1$.*

In particular, if D contains all minimum weight codewords of C, then $f > e$.

Proof: Note first that even though $C \setminus D$ is not linear, $d(C \setminus D, D) = w(C \setminus D)$ still holds by linearity of C and D. Let $\mathbf{x}$ be a minimum weight codeword in $C \setminus D$, and assume that $w(\mathbf{x}) = 2i$. Choose a vertex $\mathbf{y}$ equidistant from 0 and $\mathbf{x}$. By the UD property, $\mathbf{y}$ is at distance at most $i-1$ from some $\mathbf{c} \in C$. Now both $d(\mathbf{c}, 0) \leq 2i-1$ and $d(\mathbf{c}, \mathbf{x}) \leq 2i-1$ hold by the triangle inequality; thus $\mathbf{c}$ may belong neither to $C \setminus D$ nor to D, a contradiction. ∎

Proposition 13 *Every $\mathbf{x}$ of minimum weight in $C \setminus D$ satisfies*

$$|\mathbf{x} \cap supp(D)| \leq e.$$

Proof: Suppose such an $\mathbf{x}$ intersects $supp(D)$ in at least $e+1$ positions. Set $S = \mathbf{x} \cap supp(D)$ and choose $E \subset S, |E| = e+1$. Then $|\mathbf{x} \setminus supp(D)| \leq 2f - e$. By the design property, there is a -unique- codeword $c' \in D$ of weight $2e+1$ covering E. Now $w(\mathbf{x} + \mathbf{c}') \leq 2f$ and $\mathbf{x} + \mathbf{c}' \in C \setminus D$, a contradiction. ∎

Remark : With the previous notation, $f \leq \rho(C)$.
Indeed, a vector $\mathbf{v}$ of weight f such that $supp(\mathbf{v}) \cap supp(D) = \emptyset$ is at distance f from C.

Proof of Theorem 11 : Recall that $d(C)$ is odd. If it is 5, then the code is perfect, hence it is the $[5, 1, 5]$ perfect code. Thus assume that $d(C) = 3$.

¿From Corollary 10 follows that the connected components of ¿$\mathcal{V}$ generate perfect codes with disjoint supports. Hence there are at most two of them. Otherwise a vector at distance 3 from the code would be easily constructed. Furthermore, if there are exactly two Hamming codes, say D_1 and D_2, then C is their product P. For if $n = |supp(D_1)| + |supp(D_2)|$ and P is a proper subcode of C, then $d(C) \leq \rho(P) = 2$. If $n > |supp(D_1)| + |supp(D_2)|$, then $\rho(C)$ is at least 3, unless the projection of C onto the complement of the set of coordinates of P is the complete code; in the latter case, $d(C) = 1$.

Assume now there is a unique connected component $\mathcal{M}$, generating a perfect $[n_0 = 2^{m_0} - 1, n_0 - m_0, 3]$ Hamming code D. We now proceed to prove that this case may not occur.

Notice that every vector $\mathbf{v}$ of weight 2 such that $supp(\mathbf{v}) \cap D = \emptyset$ may be completed into a vector of weight 3 in n_0 ways by adding a 1 in a position of $supp(D)$. Each of these weight-three vectors is itself covered exactly once by a unique codeword of weight 5 in $C \setminus D$ (since C is UD, $\rho(C) = 2$, and $d(D, C \setminus D) = 5$). By proposition 13, such a codeword intersects $supp(D)$ in at most (hence exactly) one position. We conclude that :

Property 1 *the projection of C onto the complement of $supp(D)$ is a linear code T of length $v = n - n_0$. Its minimum distance is 4, and the set T_4 of its minimum weight codewords makes up a design of type $\lambda = n_0, t = 2, k = 4, v$.*

We will next show that the structure of T can be completely determined ; this will lead to the nonexistence of C.

Every vector at distance at most 1 from T is at distance 2 from no codeword (since $d(T) = 4$). Every vector at distance 2 from T is at distance 2 from $n_0 + 1$ codewords (for vectors of weight two, this is property 1 ; this is true of the others by linearity). In other words T is $(0, n_0 + 1)$-uniformely packed, and therefore its dual $T^{\perp}$ is a 2-weight code with weights

$$w_1 = u2^t, w_2 = (u+1)2^t \tag{1}$$

for some integers u, t (see [8]).

Furthermore, that T is $(0, n_0+1)$-uniformely packed also means that T is a perfect $(1, 1, (n_0+1)^{-1}))$ weighted perfect covering of $\mathbb{F}_2^v$ (see [5], chapter 13). This implies that the roots of the Lloyd polynomial $L(x)$, defined as

$$P_0(x) + P_1(x) + \frac{1}{n_0+1}P_2(x) = 1 + (v-2x) + (n_0+1)^{-1}(2x^2 - 2vx + \binom{v}{2}),$$

are the two nonzero weights of $T^\perp$, where P_0, P_1 and P_2 are the first three Krawtchouk polynomials. Rewriting $L(x)$ as $ax^2 + bx + c$, we get

$$\begin{aligned} a &= 2/(n_0+1), \\ b &= -2(1 + v/(n_0+1)), \\ c &= 1 + v + \binom{v}{2}/(n_0+1) = |T^\perp| = 2^r. \end{aligned}$$

The latter equality stems from the fact that c is the size of the Voronoi regions of T. Thus $w_1 w_2 = c/a$ is a power of 2, which implies that we have $u = 1$ in (1), so that we get $w_2 = 2w_1$. We therefore have :

$$\begin{aligned} 3w_1 &= w_1 + w_2 = n_0 + 1 + v \\ 2w_1^2 &= w_1 w_2 = (n_0+1)(1+v)/2 + v(v-1)/4 \end{aligned}$$

so that, eliminating w_1, we find that v must satisfy

$$v^2 + (2(n_0+1) - 9)v + 2(n_0+1)(5 - 4n_0) = 0,$$

the only positive solution of which is

$$v = 2(n_0+1).$$

We have therefore $w_1 = v/2$ and $w_2 = v$, so that $T^\perp$ is the first-order Reed-Muller code. We conclude :

Property 2 *T must be the extended Hamming code of length $v = 2(n_0+1)$.*

We see therefore that C must admit an $(2m_0+2) \times (n_0+v)$-parity-check matrix of the form

$$\begin{bmatrix} \mathbf{H}_{n_0}^3 & \mathbf{X} \\ 0 & \mathbf{H}_v^4 \end{bmatrix}$$

where $\mathbf{H}_{n_0}^3$ is an $m_0 \times n_0$ parity-check matrix of a Hamming code, and $\mathbf{H}_v^4$ is an $(m_0+2) \times v$ parity-check matrix of an extended Hamming code. But then

$$\begin{bmatrix} \mathbf{X} \\ \mathbf{H}_v^4 \end{bmatrix}$$

must be the parity-check matrix of a code of minimal distance ≥ 6. This is not possible, because such a linear code must have redundancy at least $2m_0 + 3$ (see [3]). This concludes the proof of Theorem 11. ∎

4 Nonlinear UD codes

The problem of classifying all nonlinear UD codes seems even more daunting than in the linear case. In particular the problem generalizes that of classifying PDS, in itself a generalization of the classification of nonlinear perfect codes, already an open problem.

Nevertheless, a few results may be stated. The main purpose of this section is to provide a construction of a perfect subcode of any UD code which generalizes proposition 5. First we prove an easy generalization of a result by Weichsel [11] :

Proposition 14 *If C is a UD code then its connected components are subcubes.*

Proof: Let T be a connected component of C, R a maximal (for inclusion) subcube of T, of dimension, say, r. Without loss of generality,

$$R = \{(v_1, \ldots, v_r, 0, \ldots, 0) \ : \ v_i \in F\}.$$

Let $\mathbf{u} \in T \setminus R$, with $d(\mathbf{u}, R) = 1$; say

$$\mathbf{u} = (u_1, \ldots, u_r, 1, 0, \ldots, 0).$$

Then there is a vertex $\mathbf{w}$ not in T with $(r+1)$-st component equal to 1 (otherwise, T would contain a $(r+1)$- subcube). Consider a shortest path P going from $\mathbf{u}$ to $\mathbf{w}$ disjoint from R, (i.e. with $(r+1)$-st component equal to 1). Let $\{\mathbf{y}, \mathbf{x}\}$ be the edge where P leaves T (i.e. $\mathbf{y} \in T$ and $\mathbf{x} = (x_1, \ldots, x_r, 1, 0, \ldots, 0)$ is the first vertex on this path not in T). Then $\mathbf{x}$ is at distance 1 from two vertices in T, namely $\mathbf{y}$ and $(x_1 \ldots, x_r, 0, \ldots, 0)$ – the latter in R – contradicting the UD property. ∎

Proposition 5 can also be generalised to the nonlinear case. We first need to generalise some definitions. Let C be a UD code, not necessarily linear, of minimal distance $d = 2e + 1$. For any codeword $\mathbf{x}$ denote by $N_d(\mathbf{x})$ the *d-neighbourhood* of $\mathbf{x}$, i.e. the set of codewords of C at distance d from $\mathbf{x}$. We shall partition $N_d(\mathbf{x})$ into "connected components" that each "generate" a perfect code (in a way that will become more precise as we proceed). Denote by $supp_{\mathbf{x}}(\mathbf{v})$ the *support of* $\mathbf{v}$ *relative to* $\mathbf{x}$ or $\mathbf{x}$-support, namely $supp_{\mathbf{x}}(\mathbf{v}) = supp(\mathbf{v}+\mathbf{x})$. Define similarly $supp_{\mathbf{x}}(L)$ for $L \subset \mathbb{F}_2^n$. Two vectors $\mathbf{v}$ and $\mathbf{w}$ in $N_d(\mathbf{x})$ are defined to be $\mathbf{x}$-*adjacent* if $|supp_{\mathbf{x}}(\mathbf{v}) \cap supp_{\mathbf{x}}(\mathbf{w})| = e$.

Lemmas 7,8,9 of Section 2 do not make use of linearity and carry over to the nonlinear case, with supports being replaced by $\mathbf{x}$-supports and adjacency in $\mathcal{V}$ by $\mathbf{x}$-adjacency in $N_d(\mathbf{x})$. We have therefore :

Lemma 15 *Let $\mathcal{M}_{\mathbf{x}}$ be an $\mathbf{x}$-connected component of $N_d(\mathbf{x})$. The set*

$$\{supp_{\mathbf{x}}(\mathbf{v}) \mid \mathbf{v} \in \mathcal{M}_{\mathbf{x}}\}$$

makes up an $(e+1)$-design on the set $supp_{\mathbf{x}}(\mathcal{M}_{\mathbf{x}})$.

To identify perfect subcodes of nonlinear UD codes we need the following nonlinear version of Theorem 6 :

Proposition 16 *A code C with minimum distance d is perfect if and only if, for every $\mathbf{x} \in C$, $\mathbf{x} + N_d(\mathbf{x})$ is an $(e+1)$-design.*

Now in order to identify a perfect subcode of a UD code, we cannot simply take the linear span of some $\mathbf{x} + \mathcal{M}_{\mathbf{x}}$ as in the linear case. This is essentially where the linear case and the nonlinear case differ. Instead we proceed as follows.

Construction : let $\mathbf{x}$ be some codeword of C such that $N_d(\mathbf{x})$ is nonempty. Let $\mathcal{M}_{\mathbf{x}}$ be an $\mathbf{x}$-connected component of $N_d(\mathbf{x})$. Define the subcode D inductively by adjoining to $\mathbf{x}$ and $\mathcal{M}_{\mathbf{x}}$, for every $\mathbf{y} \in \mathcal{M}_{\mathbf{x}}$, the $\mathbf{y}$-connected component $\mathcal{M}_{\mathbf{y}}$ of $N_d(\mathbf{y})$ containing $\mathbf{x}$. Similarly, for any $\mathbf{y}$ and any element $\mathbf{z} \in \mathcal{M}_{\mathbf{y}}$, add all the codewords of the $\mathbf{z}$-connected component of $N_d(\mathbf{z})$ containing $\mathbf{y}$, and so on.

That the above construction yields a perfect subcode is not apparent. It is readily checked though, that it will follow from the following lemma.

Lemma 17 *Let $\mathcal{M}_{\mathbf{x}}$ be an $\mathbf{x}$-connected component of $N_d(\mathbf{x})$. Let $\mathbf{y} \in \mathcal{M}_{\mathbf{x}}$ and let $\mathbf{z}$ be contained in the $\mathbf{y}$-connected component $\mathcal{M}_{\mathbf{y}}$ of $N_d(\mathbf{y})$ containing $\mathbf{x}$. Then $supp_{\mathbf{x}}(\mathbf{z}) \subset supp_{\mathbf{x}}(\mathcal{M}_{\mathbf{x}})$.*

Proof: Write $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, $\mathbf{y} = (y_1, y_2, \ldots, y_n)$, $\mathbf{z} = (z_1, z_2, \ldots, z_n)$. We need to prove that $\{i | z_i \neq x_i\} \subset supp_{\mathbf{x}}(\mathcal{M}_{\mathbf{x}})$. Let i be such that $z_i \neq x_i$ and note that if $y_i \neq x_i$ then $z_i = y_i$ and there is nothing to prove. Suppose therefore that i is such that $z_i \neq x_i$ and $z_i \neq y_i$. What we need to prove is that there exists $\mathbf{u} \in \mathcal{M}_{\mathbf{x}}$ such that $u_i = z_i$.

Case 1. $\mathbf{z}$ is $\mathbf{y}$-adjacent to $\mathbf{x}$, i.e. $|I| = e$ where $I = supp_{\mathbf{y}}(\mathbf{z}) \cap supp_{\mathbf{y}}(\mathbf{x})$. Let B be the set of coordinates defined by $B = I \cup \{i\} \cup \{j\}$ where j is any coordinate in $supp_{\mathbf{y}}(\mathbf{x}) \setminus I$. Let $\mathbf{b}$ be the vector obtained from $\mathbf{y}$ by changing all the coordinates in B. We have $d(\mathbf{y}, \mathbf{b}) = e + 2$, and $d(\mathbf{b}, \mathbf{x}) = d(\mathbf{b}, \mathbf{z}) = e + 1$. Since C is UD there exists $\mathbf{u} \in C$ such that $d(\mathbf{u}, \mathbf{b}) < e + 1$. Apply the triangle inequality to obtain $d(\mathbf{x}, \mathbf{u}) \leq d$ and $d(\mathbf{y}, \mathbf{u}) \leq d + 1$. Therefore $d(\mathbf{x}, \mathbf{u}) = d$ and $d(\mathbf{y}, \mathbf{u}) = d + 1$ because $d(\mathbf{y}, \mathbf{x}) = d(\mathbf{u}, \mathbf{x}) = d$. Therefore $\mathbf{u}$ is $\mathbf{x}$-adjacent to $\mathbf{y}$ so $\mathbf{u}$ is in $\mathcal{M}_{\mathbf{x}}$, and by construction, $u_i = z_i$.

Case 2. $\mathbf{z}$ is not $\mathbf{y}$-adjacent to $\mathbf{x}$. But then apply Lemma 15 to obtain a codeword $\mathbf{z}'$, $\mathbf{y}$-adjacent to $\mathbf{x}$, such that $\mathbf{z}'_i = \mathbf{z}_i$ and we are back to case 1. ∎

5 The q-ary case

We generalize the results of Section 2 to any finite field $\mathbb{F}_q$. Let $C \subset \mathbb{F}_q^n$ be a linear q-ary UD code, i.e. $\forall \mathbf{v} \in \mathbb{F}_q^n \ \exists! \mathbf{c} \in C$ such that $d(\mathbf{v}, \mathbf{c}) = d(\mathbf{v}, C)$.

Since the weight of a word is invariant by (nonzero) scaling we can take the vector lines of $\mathbb{F}_q^n$ (to reason projectively). So put $[\mathbf{v}] = \{\lambda \mathbf{v},\ \lambda \in \mathbb{F}_q^*\}$ and $[0]=0$.

Let now $\mathcal{V}$ be the set of all minimum weight ($= 2e+1$) vector lines of C. The first step is to properly generalize the binary adjacency relation.

Definition 18 *Call two elements* $[\mathbf{v}], [\mathbf{w}] \in \mathcal{V}$, adjacent, $\mathbf{v} \text{ — } \mathbf{w}$ *for short, if*

1. $|supp(\mathbf{v}) \cap supp(\mathbf{w})| = e$
2. *The values of these common support coordinates are the same (so that* $d(\mathbf{v}, \mathbf{w}) = 2e+1$*).*

We will call such a pair $(\mathbf{v}, \mathbf{w})$ adapted.

This adjacency condition defines a graph in $\mathcal{V}$.

Proposition 19 *Let* $\mathcal{M}$ *be a connected component of* $\mathcal{V}$ *and* $D =< \mathcal{M} >$. *Then* D *is a perfect linear code.*

The idea of the proof is to show a design property, namely to prove that for any set of $e+1$ coordinates in M=$supp(D)$ there exist $(q-1)^{e+1}$ elements in $\mathcal{M}$ with the given coordinates in their supports. The conclusion then follows by applying Theorem 6.

References

[1] E.F.Assmus, Jr. and H.F.Mattson, Jr., "Coding and Combinatorics", *SIAM Review*, **16**, n. 3, July 1974.

[2] C. Berge, *Graphes*, Gauthier-Villars, 1983.

[3] A.E. Brouwer and L.M.G.M. Tolhuizen, "A Sharpening of the Johnson Bound for Binary Linear Codes", *Designs, Codes and Cryptography*, **3**, No. 1, pp. 95-98, 1993.

[4] J. Borges and I.J. Dejter, "On Perfect Dominating Sets in Hypercubes and their Complements". *The Journal of Combinatorial Mathematics and Combinatorial Computing,* **20**, pp. 161-173, 1996.

[5] G. Cohen, I. Honkala, S. Litsyn and A. Lobstein, *Covering Codes*, North-Holland Math. Lib., **54**, 1997.

[6] G. Cohen, S. Litsyn. A. Vardy and G. Zémor, "Tilings of Binary Spaces", *SIAM J. Discrete Math.*, **9**, pp. 393-412, 1996.

[7] I.J. Dejter and P.M. Weichsel, "Twisted Perfect Dominating Subgraphs of Hypercubes", *Congressus Num.* **94**, pp. 67-78, 1994.

[8] P. Delsarte, "Weights of linear codes and strongly regular normed spaces", *Discrete Math.*, **3**, pp. 47–64, 1972.

[9] J.H. van Lint, *Introduction to Coding Theory*, Graduate Text in Mathematics, Springer-Verlag, NY. 1982.

[10] P.R.J. Östergård and W.D. Weakley, "Constructing Covering Codes with Given Automorphism", *preprint,* 1997.

[11] P.M. Weichsel, "Dominating Sets of n-Cubes", *J. Graph Theory,* **18**, pp. 479-488, 1994.