Department of Mathematical Sciences, Clemson University

http://www.ces.clemson.edu/ keyj/

Permutation decoding for binary self-dual codes from the graph Q_n where n is even.

J. D. Key

keyj@ces.clemson.edu

Abstract

For $n \geq 2$, the graph with vertices the 2^n vectors of $\mathbb{F}_2^n$ and two vertices adjacent if their coordinates differ in precisely one place, is called the n-cube, denoted by Q_n. We examine the binary code obtained from the row span of an adjacency matrix for Q_n over the field $\mathbb{F}_2$, and show that when n is even it is a self-dual $[2^n, 2^{n-1}, n]_2$ code. For $n \geq 6$ and even we obtain 2- and 3-PD-sets of size $n2^n$ for permutation decoding.

Joint work with Pani Seneviratne. [5]

April 27, 2007

Binary codes of cubic graphs

For $n \geq 2$ let Q_n denote the n-cube (see [10]) and $\mathcal{D}_n$ the symmetric 1-design obtained by defining the 2^n vertices (i.e. vectors in $\mathbb{F}_2^n$) to be the points $\mathcal{P}$, and a block $\bar{v}$ for every point (vector) v by

$$\bar{v} = \{w \mid w \in \mathcal{P} \text{ and } w \text{ adjacent to } v \text{ in } Q_n\}.$$

Then $\mathcal{D}_n$ is a 1-$(2^n, n, n)$ symmetric design with the property that two distinct blocks meet in zero or two points and similarly any two distinct points are together on zero or two blocks.

We will use the following notation:

for $r \in \mathbb{Z}$ and $0 \leq r \leq 2^n - 1$, if

$$r = \sum_{i=1}^{n} r_i 2^{i-1}$$

is the binary representation of r, let

$$\mathbf{r} = (r_1, \ldots, r_n)$$

be the corresponding vector in $\mathbb{F}_2^n$, i.e. point in $\mathcal{P}$.

The **complement** of $v \in \mathcal{P}$ will be denoted by v_c. Thus

$$v_c(i) = 1 + v(i)$$

for $1 \leq i \leq n$, where $v(i)$ denotes the i^{th} coordinate entry of v.

Similarly, for $\alpha \in \mathbb{F}_2$, $\alpha_c = \alpha + 1$. Clearly $v_c = v + \mathbf{2^n} - \mathbf{1}$.

The binary code C_n of the design $\mathcal{D}_n$ is the same as the row span over $\mathbb{F}_2$ of an adjacency matrix for Q_n, and for n even and $n \geq 4$, it is a $[2^n, 2^{n-1}, n]_2$ self-dual code.

Before showing this, we show why the case for n odd is not of interest.

Proposition 1 *For n odd, the binary code C_n of $\mathcal{D}_n$ is the full space $\mathbb{F}^{2^n}$.*

Proof: For n odd, it can be verified directly that

$$v^{(x_1,\ldots,x_n)} = v^{\overline{(x_1,\ldots,(x_n)_c)}} + \sum_{i=1}^{n-1} v^{\overline{(x_1,\ldots,(x_i)_c,\ldots,x_{n-1},x_n)}}$$

for all choices of $x = (x_1, \ldots, x_n)$. Thus C_n contains all the vectors of weight 1 and is the full space. ■

Notation: for $X \subseteq \mathcal{P}$, v^X is the **incidence vector** of X.

The **automorphism group** of the design and of the code contains (properly, for $n \geq 4$) the automorphism group

$$TS_n = T \rtimes S_n$$

of the graph (see [10]), where T is the translation group of order 2^n and S_n is the symmetric group acting on the n coordinate positions of the points $v \in \mathcal{P}$.

For each $w \in \mathcal{P}$, write $T(w)$ for the automorphism of C_n defined by the translation on $\mathbb{F}_2^n$ given by

$$T(w) : v \mapsto v + w$$

for each $v \in \mathbb{F}_2^n$. The identity map will be denoted by $\iota = T(0)$. Then

$$T = \{T(w) \mid w \in \mathcal{P}\}.$$

Lemma 2 *The group TS_n acts imprimitively on the points of the design $\mathcal{D}_n$ for $n \geq 4$ with $\{v, v_c\}$, for each $v \in \mathbb{F}_2^n$, a block of imprimitivity.*

Proof: We need only show that for $g \in TS_n$, and any $v \in \mathbb{F}_2^n$, $v_c g = (vg)_c$, which will make the set $\{v, v_c\}$ a block of imprimitivity.

Clearly TS_n is transitive on points. For $g \in S_n$ the assertion is clear. If g is the translation $T(u)$, where $T(u) : v \mapsto v + u$, then $v_c g = v_c T(u) = v + \mathbf{2^n} - \mathbf{1} + u = vT(u) + \mathbf{2^n} - \mathbf{1} = (vg)_c$. Thus for any $g \in TS_n$ and any $v \in \mathbb{F}_2^n$, $v_c g = (vg)_c$. ■

For each i such that $1 \leq i < n$ let $t_i = (i, n) \in S_n$, i.e. the automorphism of C_n defined by the transposition of the coordinate positions. For $n \geq 4$ let

$$\begin{aligned} P_n &= \{t_i \mid 1 \leq i \leq n-1\} \cup \{\iota\} && (1) \\ T_n &= T P_n. && (2) \end{aligned}$$

Since the translation group T is normalized by S_n, elements of the form $T(w)t_iT(u)$ are all in T_n, i.e. $\sigma^{-1}T(u)\sigma = T(u\sigma)$, so that for transpositions t, $tT(u) = T(ut)t$.

Proposition 3 *For n even, $n \geq 4$, C_n is a $[2^n, 2^{n-1}, n]_2$ self-dual code with*

$$\mathcal{I} = [\mathbf{0}, \mathbf{1}, \ldots, \mathbf{2^{n-1} - 3}, \mathbf{2^n - 2}, \mathbf{2^n - 1}]$$

as an information set.

Proof: Using the natural ordering for the points and blocks, the incidence matrix for Q_n has the form

$$B_n = \begin{pmatrix} B_{n-2} & I_{2^{n-2}} & I_{2^{n-2}} & 0 \\ I_{2^{n-2}} & B_{n-2} & 0 & I_{2^{n-2}} \\ I_{2^{n-2}} & 0 & B_{n-2} & I_{2^{n-2}} \\ 0 & I_{2^{n-2}} & I_{2^{n-2}} & B_{n-2} \end{pmatrix} \tag{3}$$

where B_{n-2} is the incidence matrix of the graph Q_{n-2}. It is easy to prove that the matrix has rank 2^{n-1} and it can be shown by induction that the minimum weight is n. That the code is self-dual follows from the earlier observation that blocks meet in 0, 2 or n points.

To show that $\mathcal{I}$ is an information set, let B_n^* be the first 2^{n-1} rows of B_n. Clearly B_n^* has rank 2^{n-1} and generates the same code as B_n.

We want to switch the column indexed by $\mathbf{2^{n-1}-2}$ with that indexed by $\mathbf{2^n-2}$, and the column indexed by $\mathbf{2^{n-1}-1}$ with that indexed by $\mathbf{2^n-1}$.

Notice that $\mathbf{2^{n-1}-2} \in \overline{\mathbf{2^{n-1}-1}}$, so the 2×2 submatrix of B_n^* from the $(2^{n-1}-2)^{th}$ and $(2^{n-1}-1)^{th}$ rows and columns has the form $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, while the corresponding 2×2 submatrix from the same rows but the last two columns is just I_2. Thus the column interchanges described will give the information set $\mathcal{I}$. ■

		0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
		0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
		0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
		0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
[0,0,0,0]	0		1	1		1				1							
[1,0,0,0]	1	1			1		1				1						
[0,1,0,0]	2	1			1			1				1					
[1,1,0,0]	3		1	1					1				1				
[0,0,1,0]	4	1					1	1						1			
[1,0,1,0]	5		1			1			1						1		
[0,1,1,0]	6			1		1			1							1	
[1,1,1,0]	7				1		1	1									1
[0,0,0,1]	8	1									1	1		1			
[1,0,0,1]	9		1							1			1		1		
[0,1,0,1]	10			1						1			1			1	
[1,1,0,1]	11				1						1	1					1
[0,0,1,1]	12					1				1					1	1	
[1,0,1,1]	13						1				1			1			1
[0,1,1,1]	14							1				1		1			1
[1,1,1,1]	15								1				1		1	1	

Figure 1: Adjacency matrix for Q_4

If $\mathcal{I}$ is as in the proposition, the corresponding check set is $\mathcal{C}$. We will write

$$\begin{aligned} \mathcal{I}_1 &= [\mathbf{0}, \mathbf{1}, \ldots, \mathbf{2^{n-1}} - \mathbf{3}] && (4) \\ \mathcal{C}_1 &= [\mathbf{2^{n-1}}, \mathbf{2^{n-1}} + \mathbf{1}, \ldots, \mathbf{2^{n}} - \mathbf{3}] && (5) \\ \mathcal{I}_2 &= [\mathbf{2^{n}} - \mathbf{2}, \mathbf{2^{n}} - \mathbf{1}] && (6) \\ \mathcal{C}_2 &= [\mathbf{2^{n-1}} - \mathbf{2}, \mathbf{2^{n-1}} - \mathbf{1}] && (7) \end{aligned}$$

and

$$\begin{aligned} a = \mathbf{2^{n}} - \mathbf{2} = (0, 1, \ldots, 1, 1) \quad &, \quad b = \mathbf{2^{n}} - \mathbf{1} = (1, 1, \ldots, 1, 1) && (8) \\ A = \mathbf{2^{n-1}} - \mathbf{2} = (0, 1, \ldots, 1, 0) \quad &, \quad B = \mathbf{2^{n-1}} - \mathbf{1} = (1, 1, \ldots, 1, 0) && (9) \end{aligned}$$

Notice that the points a and b are placed in $\mathcal{I}$ in order to have points and their complements in $\mathcal{I}$ since under any automorphism $g \in TS_n$ of the design, if $vg = w$ then $v_c g = w_c$, by Lemma 2. Thus we have $a_c = \mathbf{1}$ and $b_c = \mathbf{0}$, $A_c = \mathbf{1} + \mathbf{2^{n-1}}$, $B_c = \mathbf{2^{n-1}}$, and $v + v_c = b$ for any vector $v \in \mathcal{P}$.

		$\mathcal{I}_1$						$\mathcal{I}_2$		$\mathcal{C}_1$						$\mathcal{C}_2$	
		0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
		0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
		0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
		0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0
		0	1	2	3	4	5	a	b	8	9	10	11	12	13	A	B
		0	1	2	3	4	5	14	15	8	9	10	11	12	13	6	7
[0,0,0,0]	0		1	1		1				1							
[1,0,0,0]	1	1			1		1				1						
[0,1,0,0]	2	1			1			1				1					
[1,1,0,0]	3		1	1					1				1				
[0,0,1,0]	4	1					1	1						1			
[1,0,1,0]	5		1			1			1						1		
[0,1,1,0]	6			1		1		1									1
[1,1,1,0]	7				1		1		1							1	

Figure 2: Generator matrix for the $[16, 8, 4]_2$ self-dual code from Q_4

Permutation decoding

Permutation decoding was first developed by Jessie MacWilliams [7] following also Prange [9]. It can be used when a code has sufficiently many automorphisms to ensure the existence of a set of automorphisms called a PD-set. See MacWilliams and Sloane [8, Chapter 16, p. 513] and Huffman [3, Section 8].

We extend the definition of PD-sets to s-PD-sets for s-error-correction [4] and [6]:

Definition 1 *If C is a t-error-correcting code with information set $\mathcal{I}$ and check set $\mathcal{C}$, then a PD-set for C is a set $\mathcal{S}$ of automorphisms of C which is such that every t-set of coordinate positions is moved by at least one member of $\mathcal{S}$ into the check positions $\mathcal{C}$.*

For $s \leq t$ an s-PD-set is a set $\mathcal{S}$ of automorphisms of C which is such that every s-set of coordinate positions is moved by at least one member of $\mathcal{S}$ into $\mathcal{C}$.

Specifically, if $\mathcal{I} = \{1, \ldots, k\}$ are the information positions and $\mathcal{C} = \{k+1, \ldots, n\}$ the check positions, then every s-tuple from $\{1, \ldots, n\}$ can be moved by some element of $\mathcal{S}$ into $\mathcal{C}$.

Algorithm for permutation decoding

C is a q-ary t-error-correcting $[n,k,d]_q$ code; $d = 2t+1$ or $2t+2$.

$k \times n$ generator matrix for C: $G = [I_k|A]$.
Any k-tuple v is encoded as vG. The first k columns are the information symbols, the last $n-k$ are check symbols.

$(n-k) \times n$ check matrix for C: $H = [-A^T|I_{n-k}]$.
$\mathcal{S} = \{g_1, \ldots, g_m\}$ is a PD-set for C, written in some chosen order.

Suppose x is sent and y is received and at most t errors occur:

- for $i = 1, \ldots, m$, compute yg_i and the syndrome $s_i = H(yg_i)^T$ until an i is found such that the weight of s_i is t or less;
- if $u = u_1u_2\ldots u_k$ are the information symbols of yg_i, compute the codeword $c = uG$;
- decode y as cg_i^{-1}.

Why permutation decoding works

Result 1 *Let C be an $[n,k,d]_q$ t-error-correcting code.*

Suppose H is a check matrix for C in standard form, i.e. such that I_{n-k} is in the redundancy positions.

Let $y = c + e$ be a vector, where $c \in C$ and e has weight $\leq t$.

Then the information symbols in y are correct if and only if the weight of the syndrome Hy^T of y is $\leq t$.

3-PD-sets

Theorem 4 *For n even and $n \geq 8$, let*

$$T_n = \{T(w)t_i \mid w \in \mathbb{F}_2^n, 1 \leq i \leq n\},$$

where $T(w)$ is the translation by $w \in \mathbb{F}_2^n$, $t_i = (i, n)$ for $i < n$ is a transposition in the symmetric group S_n, and t_n is the identity map.

Then T_n is a 3-PD-set of size $n2^n$ for the self-dual $[2^n, 2^{n-1}, n]_2$ code C_n from an adjacency matrix for the n-cube Q_n, with the information set

$$\mathcal{I} = [\mathbf{0}, \mathbf{1}, \ldots, \mathbf{2^{n-1} - 3}, \mathbf{2^n - 2}, \mathbf{2^n - 1}].$$

Proof: Let $\mathcal{T} = \{x, y, z\}$ be a set of three points in $\mathcal{P}$. We need to show that there is an element in T_n that maps $\mathcal{T}$ into $\mathcal{C}$.

We consider the various possibilities for the points in $\mathcal{T}$.

If $\mathcal{T} \subseteq \mathcal{C}$ then use ι.

Thus suppose at least one of the points is in $\mathcal{I}$ and, by using a translation, suppose that one of the points, say z, is $\mathbf{0}$. If $\mathcal{T} \subseteq \mathcal{I}$, then $T(\mathbf{2^{n-1}})$ will work. Now we consider the other cases.

1. $x \in \mathcal{I}_1$, $y \in \mathcal{C}_1$

   Then there are i_x, i_y such that $2 \leq i_x, i_y \leq n-1$ such that $x(i_x) = y(i_y) = 0$. If $i_x = i_y = i$, then $\mathcal{T}t_i \subseteq \mathcal{I}$, unless $yt_i \in \{A, B\}$, so $t_iT(\mathbf{2^{n-1}})$ will work unless $yt_i \in \{A, B\}$. If $yt_i = A$, then $y(1) = y(i) = 0$, $y(j) = 1$ otherwise. If $x(1) = 0$, then $t_1T(\mathbf{2^{n-1}})$ will work. If $x(1) = 1$, then take any $j \neq 1, i, n$, and use $T(\mathbf{2^{j-1}})t_iT(\mathbf{2^{n-1}})$. If $yt_i = B$, then $y(i) = 0$ and $y(j) = 1$ otherwise. Here we can take any $j \neq 1, i, n$, and use $T(\mathbf{2^{j-1}})t_iT(\mathbf{2^{n-1}})$.

   If x and y have no common zero, then if $y = x_c$, so that $x + y = b$, we can use $T(x)T(\mathbf{2^{n-1}})$. If $x(i) = y(i) = 1$, where $1 \leq i \leq n-1$, then $t_iT(\mathbf{2^{n-1} - 1})$ can be used.

2. $x \in \mathcal{I}_1$, $y \in \mathcal{C}_2$

   Since $x \in \mathcal{I}_1$, $x(i) = 0$ for some i such that $2 \leq i \leq n-1$. If there is a j such that $j \neq i$ and $2 \leq j \leq n-1$ with $x(j) = 0$, then $T(\mathbf{2^{i-1} + 2^{n-1}})$ can be used.

   If there is no such j, then either $x(1) = x(i) = x(n) = 0$ and $x(j) = 1$ for $j \notin \{1, i, n\}$, or $x(i) = x(n) = 0$ and $x(j) = 1$ for $j \notin \{i, n\}$. In either case, take $j \neq i$, $2 \leq j \leq n-1$. Then the map $T(\mathbf{2^{j-1} + 2^{n-1}})$ can be used.

3. $x \in \mathcal{I}_2$, $y \in \mathcal{C}_1$

a) $x = a$: since $y \in \mathcal{C}_1$, there is a j such that $2 \leq j \leq n-1$ with $y(j) = 0$. If $y(i) = 1$ for $i \neq j$ and $1 \leq i \leq n$, or if $y(1) = 0$ and $y(i) = 1$ for $i \neq j$ and $2 \leq i \leq n$, then $T(A)$ will work. If there is an $i \neq j$ such that $y(i) = y(j) = 0$ where $2 \leq i, j \leq n-1$, then $t_j T(\mathbf{2^{n-1}})$ can be used.

b) $x = b$: this follows exactly as in the $x = a$ case except that in the first two cases for y use $T(B)$ instead of $T(A)$.

4. $x \in \mathcal{I}_2$, $y \in \mathcal{C}_2$

a) $x = a$, $y = A$: use $T(a)t_2T(\mathbf{2^{n-1}})$.

b) $x = a$, $y = B$: use $t_{n-1}T(B)$.

c) $x = b$, $y = A$: use $t_{n-1}T(B)$.

d) $x = b$, $y = B$: use $t_1T(\mathbf{1} + \mathbf{2^{n-1}})$.

5. $x, y \in \mathcal{C}$

a) $x, y \in \mathcal{C}_1$: if $x + y = B$ then $T(B)$ will work. Otherwise $x(i) = y(i)$ for some i such that $1 \leq i \leq n-1$. Again $T(B)$ will work unless x or y are $(0, \ldots, 0, 1)$ or $(1, 0, \ldots, 0, 1)$. If $x = (0, \ldots, 0, 1)$ then $y(i) = 0$ for some i such that $2 \leq i \leq n-1$. Then $t_iT(\mathbf{2^{n-1}})$ can be used unless $y(j) = 1$ for all $j \neq i$, or

$y(1) = y(i) = 0$ and $y(j) = 1$ for $j \neq 1, i$; in these cases $t_i T(\mathbf{2^{i-1}} + \mathbf{2^{n-1}})$ can be used. The same arguments hold if $x = (1, 0, \ldots, 0, 1)$.

b) $x \in \mathcal{C}_1$, $y \in \mathcal{C}_2$: since $x \in \mathcal{C}_1$, there is a j such that $2 \leq j \leq n-1$ with $x(j) = 0$. Then $t_j T(\mathbf{2^{j-1}} + \mathbf{2^{n-1}})$ can be used.

c) $x, y \in \mathcal{C}_2$: $T(\mathbf{2^{n-2}} + \mathbf{2^{n-1}})$ will work.

This completes all the cases and proves the theorem. ■

Note that this result also shows that the set T_n is a 2-PD-set for C_n for $n = 6$. However, this set T_n with this information set $\mathcal{I}$ will not give a 4-PD-set, since it is quite easy to verify that the set of four points $\{\mathbf{0}, \mathbf{2}, \mathbf{2^n} - \mathbf{2}, \mathbf{2^{n-1}} - \mathbf{1}\}$ cannot be moved by any element of T_n into the check positions.

Discussion

The automorphism group of the symmetric 1-design is much larger than that of the graph. In particular, it will contain any invertible $n \times n$ matrix over $\mathbb{F}_2$ with the property that the sum of any two of its rows has weight 2.

In fact, if $v \in \mathcal{P}$ has an even number of entries equal to 1, then the matrix A having for rows the points in $\bar{v}$, will be be an automorphism of $\mathcal{D}_n$ that also preserves the blocks of imprimitivity.

If v has an odd number of entries equal to 1, it will not be invertible.

There are also other, non-linear, automorphisms, of the design, and that also preserve these blocks of imprimitivity, as is indicated by computations with Magma [1, 2].

Magma indicates that the automorphism group of the design is the same as that of the graph Γ_2 defined on the same point set $\mathcal{P} = \mathbb{F}_2^n$ with two points (vectors) being adjacent if they differ in exactly TWO coordinate positions, i.e. if their sum has weight 2.

It is possible to arrange more interchanges so that more instances of a point and its complement in the information set occur. Thus s-PD-sets for $s > 3$ seem possible in general.

ITALIA
OCEAN AFRICA

THANKS TO

HIREN

FOR HIS FINE JOB AS

SEMINAR ORGANISER

References

[1] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system I: The user language. *J. Symb. Comp.*, 24, 3/4:235–265, 1997.

[2] J. Cannon, A. Steel, and G. White. Linear codes over finite fields. In J. Cannon and W. Bosma, editors, *Handbook of Magma Functions*, pages 3951–4023. Computational Algebra Group, Department of Mathematics, University of Sydney, 2006. V2.13, http://magma.maths.usyd.edu.au/magma.

[3] W. Cary Huffman. Codes and groups. In V. S. Pless and W. C. Huffman, editors, *Handbook of Coding Theory*, pages 1345–1440. Amsterdam: Elsevier, 1998. Volume 2, Part 2, Chapter 17.

[4] J. D. Key, T. P. McDonough, and V. C. Mavron. Partial permutation decoding of codes from finite planes. *European J. Combin.*, 26:665–682, 2005.

[5] J. D. Key and P. Seneviratne. Permutation decoding for binary self-dual codes from the graph Q_n where n is even. Advances in Coding Theory and Cryptology, T. Shaska, W. C. Huffman, D. Joyner, V. Ustimenko Series on Coding Theory

and Cryptology, 2. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ. To appear.

[6] Hans-Joachim Kroll and Rita Vincenti. PD-sets related to the codes of some classical varieties. *Discrete Math.*, 301:89–105, 2005.

[7] F. J. MacWilliams. Permutation decoding of systematic codes. *Bell System Tech. J.*, 43:485–505, 1964.

[8] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes.* Amsterdam: North-Holland, 1983.

[9] E. Prange. The use of information sets in decoding cyclic codes. *IRE Trans.*, IT-8:5–9, 1962.

[10] Gordon Royle. Colouring the cube. Preprint.