Recent developments in permutation decoding

J. D. Key
Department of Mathematical Sciences
Clemson University
Clemson SC 29634
U.S.A.

February 2, 2006

Abstract

Recent advances in technology have produced a requirement for new implementations of good error-correcting codes. Such applications of codes also require efficient encoding and decoding methods.

The method of permutation decoding was first developed by Jessie MacWilliams in the early 60's and can be used when a linear code has a sufficiently large automorphism group to ensure the existence of a set of automorphisms, called a PD-set, that has some specific properties.

This paper will give a brief survey of permutation decoding and some recent results in the search for PD-sets.

1 Introduction

Permutation decoding was first developed by MacWilliams [Mac64]. It involves finding a set of automorphisms of a linear code, called a PD-set, that acts in a certain way with respect to a known information set for the code. If such a set can be found, then a simple algorithm using this set can be followed to correct the maximum number of errors of which the code is capable. The method is described fully in MacWilliams and Sloane [MS83, Chapter 15] and also in Huffman [Huf98, Section 8], where a survey of results up to the time of writing that chapter is given. We will describe the method and the algorithm in Section 3.

We will give here a brief, but complete, description of permutation decoding, and discuss some recent results. In particular we will look at codes defined by designs or graphs, where the automorphism group is known and large enough to allow permutation decoding or partial permutation decoding to be used.

In the sections to follow we first give some background material on designs, codes and graphs in Section 2. Section 3 describes permutation decoding and the notions of PD-sets and s-PD-sets. The remaining sections outline some of the known results for PD-sets.

2 Background and terminology

Terminology for codes and designs will be as in Assmus and Key [AK92]. An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{I}$ is a t-(v, k, λ) design, if $|\mathcal{P}| = v$, every block $B \in \mathcal{B}$ is incident with precisely k points, and every t distinct points are together incident with precisely λ blocks.

The code of the design $\mathcal{D}$ over the finite field F is the space spanned by the incidence vectors of the blocks over F. If the point set of $\mathcal{D}$ is $\mathcal{P}$ and the block set is $\mathcal{B}$, and if $\mathcal{Q}$ is any subset of $\mathcal{P}$, then we will denote the incidence vector of $\mathcal{Q}$ by $v^{\mathcal{Q}}$. Thus the code of the design over F is $C = \langle v^B \mid B \in \mathcal{B} \rangle$, and is a subspace of $F^{\mathcal{P}}$, the full vector space of functions from $\mathcal{P}$ to F.

All the codes here will be **linear codes**, i.e. subspaces of the ambient vector space. If a code C over a field of order q is of length n, dimension k, and minimum weight d, then we write $[n, k, d]_q$ to show this information. A **generator matrix** for the code is a $k \times n$ matrix made up of a basis for C. The **dual** code $C^\perp$ is the orthogonal under the standard inner product, i.e. $C^\perp = \{v \in F^n | (v, c) = 0 \text{ for all } c \in C\}$. A **check matrix** for C is a generator matrix for $C^\perp$; the **syndrome** of a vector $y \in F^n$ is Hy^T. A code C is **self-orthogonal** if $C \subseteq C^\perp$ and is **self-dual** if $C = C^\perp$. If c is a codeword then the **support** of c is the set of non-zero coordinate positions of c. A **constant word** in the code is a codeword, all of whose coordinate entries are either 0 or 1. The all-one vector will be denoted by $\boldsymbol{\jmath}$, and is the constant vector of weight the length of the code. Two linear codes of the same length and over the same field are **equivalent** if each can be obtained from the other by permuting the coordinate positions and multiplying each coordinate position by a non-zero field element. They are **isomorphic** if they can be obtained from one another by permuting the coordinate positions. Any code is isomorphic to a code with generator matrix in so-called **standard form**, i.e. the form $[I_k \mid A]$; a check matrix then is given by $[-A^T \mid I_{n-k}]$. The first k coordinates are the **information symbols** and the last $n - k$ coordinates are the **check symbols**. An **automorphism** of a code C is any permutation of the coordinate positions that maps codewords to codewords.

Terminology for **graphs** is also standard: the graphs, $\Gamma = (V, E)$ with vertex set V and edge set E, are undirected and the **valency** of a vertex is the number of edges containing the vertex. A graph is **regular** if all the vertices have the same valency; a regular graph is **strongly regular** of type (n, k, λ, μ) if it has n vertices, valency k, and if any two adjacent vertices are together adjacent to λ vertices, while any two non-adjacent vertices are together adjacent to μ vertices. The **line graph** of a graph $\Gamma = (V, E)$ is the graph $\Gamma^t = (E, V)$ where e and f are adjacent in Γ^t if e and f share a vertex in Γ. The code associated with a graph over a field $\mathbb{F}_p$ will be the row span over $\mathbb{F}_p$ of an adjacency matrix for the graph.

3 Permutation decoding

Permutation decoding involves finding a set of automorphisms of a code, called a PD-

set. The method is described fully in MacWilliams and Sloane [MS83, Chapter 15] and Huffman [Huf98, Section 8]. In [KMM05] we extended the definition of PD-sets to s-PD-sets for s-error-correction, a term that is also used in [KV05, KV].

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 $\mathcal{C}$.*

The **algorithm for permutation decoding**, once a PD-set has been found, is as follows: we have a t-error-correcting $[n,k,d]_q$ code C with check matrix H in standard form. Thus the generator matrix G for C that is used for encoding has I_k as the first k columns, and hence as the information symbols. Any k-tuple v is encoded as vG. Suppose x is sent and y is received and at most t errors occur. Let $\mathcal{S} = \{g_1, \ldots, g_m\}$ be the PD-set. Compute the syndromes $H(yg_i)^T$ for $i = 1, \ldots, m$ until an i is found such that the weight of this vector is t or less. Now look at the information symbols in yg_i, and obtain the codeword c that has these information symbols. Now decode y as cg_i^{-1}. Note that this is valid since permutations of the coordinate positions correspond to linear transformations of F^n, so that if $y = x + e$, where $x \in C$, then $yg = xg + eg$ for any $g \in S_n$, and if $g \in Aut(C)$, then $xg \in C$.

That this method does correct t errors follows from the following result (proved in [Huf98, Theorem 8.1]):

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 of y is $\leq t$.*

There is a lower bound on the size of a PD-set (and one for an s-PD-set), due to Gordon [Gor82] using a formula of Schönheim [Sch64], and also proved in [Huf98]:

Result 2 *If $\mathcal{S}$ is a PD-set for a t-error-correcting $[n,k,d]_q$code C, and $r = n - k$, then*

$$|\mathcal{S}| \geq \left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \left\lceil \cdots \left\lceil \frac{n-t+1}{r-t+1} \right\rceil \cdots \right\rceil \right\rceil \right\rceil .$$

In Gordon [Gor82] and Wolfman [Wol83] small PD-sets for the binary Golay codes were found. In Chabanne [Cha92] abelian codes, i.e. ideals in the group algebra of an abelian group, are looked at using Gröbner bases, and the ideas of permutation decoding are generalized. In general it is rather hard to find these PD-sets, and obviously they need not even exist. Also the existence may depend on the chosen information set, and thus existence of a PD-set is not invariant under equivalence of codes. Note that PD-seets need

not be sought, in general, for codes with minimum weight 3 or 4, since correcting a single error is, in fact, simply done by using syndrome decoding, because in that case multiples of the columns of the check matrix will give the possible syndromes. Thus the syndrome of the received vector need only be compared with the columns of the check matrix, by looking for a multiple.

A simple argument yields that the worst-case time complexity for the decoding algorithm using an s-PD-set of size m on a code of length n and dimension k is $\mathcal{O}(nkm)$.

A study of the complexity of the algorithm for some algebraic geometry codes is give in [Joy05].

4 Cyclic codes

In her original paper, MacWilliams [Mac64] developed a theory for finding PD-sets for cyclic codes.

An $[n, k, d]_q$ code C is cyclic if whenever $c = c_1c_2 \dots c_n \in C$ then every cyclic shift of c is in C. Thus the mapping $\tau \in S_n$ defined by

$$\tau : i \mapsto i + 1$$

for $i \in \{1, 2, \dots n\}$, is in the automorphism group of C, and $\tau^n = 1$. If a message c is sent and t errors occur, then if e is the error vector and if there is a sequence of k zeros between two of the error positions, then τ^j for some j will move the sequence of zeros into the information positions, and thus all the errors will occur in the check positions. Thus $< \tau >$ will be a PD-set for C if $k < \frac{n}{t}$.

As shown in [Mac64], if q is a number prime to the length n, then the map

$$\rho : i \mapsto qi$$

is also an automorphism of the cyclic code and in the normalizer N of $< \tau >$. MacWilliams examines cases where N contains a PD-set.

5 Some infinite classes of codes having PD-sets

In searching for PD-sets, suitable information sets need first to be found. Codes from some classes of graphs have large automorphism groups, so it was reasonable to consider some of these classes of graphs first. Notice that a code defined by a design or graph as outlined in Section 2 will have automorphism group at least that of the design or graph, and in some cases a larger automorphism group.

5.1 Triangular graphs

For any n, the triangular graph $T(n)$ is the line graph of the complete graph K_n, and is strongly regular. The row span over $\mathbb{F}_2$ of an adjacency matrix for $T(n)$, for $n \geq 5$, gives codes with the following parameters:

- $[\frac{n(n-1)}{2}, n-1, n-1]_2$ for n odd;
- $[\frac{n(n-1)}{2}, n-2, 2(n-1)]_2$ for n even.

The automorphism group of the graph $T(n)$ is the symmetric group S_n acting naturally on pairs. The automorphism group of the binary code of $T(n)$ is also S_n for $n \geq 5, n \neq 6$, since in the latter case the automorphism group of the code is larger. In [KMR04b, Rod03] information sets and and PD-sets were obtained, the PD-sets being of size n for n odd and $n^2 - 2n + 2$ for n even.

The computational complexity of the decoding by this method may be quite low, of the order $n^{1.5}$ if the elements of the PD-set are appropriately ordered. The codes are low density parity check (LDPC) codes.

5.2 Lattice graphs

The (square) lattice graph $L_2(n)$ is the line graph of the complete bipartite graph $K_{n,n}$, and is strongly regular. The row span over $\mathbb{F}_2$ of an adjacency matrix gives codes with parameters $[n^2, 2(n-1), 2(n-1)]_2$ for $n \geq 5$ with $S_n \wr S_2$ as automorphism group. Information sets and PD-sets of size n^2 in $S_n \times S_n$ were found in [KSc].

Similar results holds for the lattice graph $L_2(m, n)$ [KSa], i.e. the line graph of the complete bipartite graph $K_{m,n}$, where the codes are

- $[mn, m+n-2, 2m]_2$ for $m+n$ even;
- $[mn, m+n-1, m]_2$ for $m+n$ odd.

In both cases information sets and PD-sets of size mn in $S_m \times S_n$ were found.

More generally, the binary codes of the line graphs of the complete multi-partite graphs $K_{n_1,\ldots,n_m}$, where $n_i = n$ for $i = 1, \ldots m$, with automorphism group $S_{n_1} \times S_{n_2} \times \ldots \times S_{n_m}$ were considered in [KSb], and PD-sets were found for some classes, and s-PD-sets were found for all classes for some s.

5.3 Graphs on triples

We can define three regular graphs with vertex set the subsets of size three of a set of size n and adjacency according to the size of the intersection of the 3-subsets. Properties of the binary codes of these graphs were established in [KMR04a]. Again S_n in its natural action acts as an automorphism group of the codes.

If C is the binary code in the case of adjacency defined if the 3-subsets intersect in two elements, then the dual $C^\perp$ is a $[\binom{n}{3}, \binom{n-1}{2}, n-2]_2$ code and a PD-set of size n^3 was found for a particular information set in [KMRa]. Similar results hold for some of the other more interesting codes obtained in this way, but in some cases only partial decoding through s-PD-sets was possible: see [KMRb].

These graphs are particular cases of the class of uniform-subset graphs. A more general study of the binary codes of these graphs and the application of permutation decoding to the codes is being conducted by W. Fish [Fis].

6 Some infinite classes of codes only having partial PD-sets

6.1 Finite desarguesian planes

If $q = p^e$ where p is prime, the code of the desarguesian projective plane of order q has parameters $[q^2+q+1, (\frac{p(p+1)}{2})^e+1, q+1]_p$. For the affine plane the code is $[q^2, (\frac{p(p+1)}{2})^e, q]_p$. The codes are subfield subcodes of the generalized Reed-Muller codes (see [AK98]), and the automorphism groups are the semi-linear groups and doubly transitive on points.

Thus 2-PD-sets always exist. However, unlike the codes from graphs discussed in the preceding sections, it is not possible to obtain a general construction of PD-sets that will cover all members of this class of codes (i.e. for all q), since the bound of Result 2 for the size of a PD-set for error-correction using the full capability of the code is greater than the size of the group as q grows beyond a certain value: see [KMM05]. For example, in the projective desarguesian case, when q is greater than the stated value, PD-sets for full error-correction cannot exist beyond the stated values of q (computations done using Magma [BC94] and GAP [GAP]):

- $q = p$ prime and $p > 103$;
- $q = 2^e$ and $e > 12$;
- $q = 3^e$ and $e > 6$;
- $q = 5^e$ and $e > 4$;
- $q = 7^e$ and $e > 3$;
- $q = 11^e$ and $e > 2$;
- $q = 13^e$ and $e > 2$;
- $q = p^e$ for $p > 13$ and $e > 1$.

Similar results hold for the affine and dual cases. Thus it is not possible to give a general construction of PD-sets for this whole class of codes. However, s-PD-sets that apply to the whole class can be found for some small values of $s \geq 2$: see Sections 6.2, 6.3 below.

6.2 Small 2-PD-sets in prime-order planes

It is clear that 2-PD-sets exist for any information set for the p-ary code of a desarguesian plane of order a power of p, since the group is 2-transitive. Since the smaller an s-PD-set is the more economical it will be for decoding purposes, it is desirable to find small 2-PD-sets inside the full group. In general this problem is not solved since information sets are not know in general. However, for prime order a Moorhouse [Moo91] basis can be used to find an information set, and using this, in [KMM05], the following sizes were obtained:

- 2-PD-sets of 37 elements for desarguesian affine planes of any prime order p;
- 2-PD-sets of 43 elements for desarguesian projective planes of any prime order p.

Also 3-PD-sets for the code and the dual code in the affine prime case of sizes $2p^2(p-1)$ and p^2, respectively, were found.

6.3 Affine geometry designs

Information sets for the generalized Reed-Muller codes were found in [KMMa] and using these, 2-PD sets of size $2p^3$ for $p \geq 5$ and 3-PD-sets of size $p^3(p-1)^3$ for $p \geq 7$ were found in [KMMb] for the p-ary codes from the 2-$(p^3, p, 1)$ affine geometry designs of points and lines in 3-dimensional space over $\mathbb{F}_p$, where p is a prime. The parameters of the codes are $[p^3, \frac{1}{6}p(5p^2+1), p]_p$.

6.4 Paley graphs

If n is a prime power with $n \equiv 1 \pmod 4$, the **Paley graph**,$P(n)$, has $\mathbb{F}_n$ as vertex set and two vertices x and y are adjacent if and only if $x - y$ is a non-zero square in $\mathbb{F}_n$. The row span over a field $\mathbb{F}_p$ of an adjacency matrix gives a good code (in fact, a quadratic residue code) if and only if p is a square in $\mathbb{F}_n$.

For any $\sigma \in Aut(\mathbb{F}_n)$ and $a, b \in \mathbb{F}_n$ with a a non-zero square, the group of mappings $\tau_{a,b,\sigma} : x \mapsto ax^\sigma + b$ is the automorphism group of the code, and is not in general 2-transitive on points. Using Magma [BC94], it can be verified (see [KL04, Lim05]) that for $n \geq 1697$ and prime or $n \geq 1849$ and a square, PD-sets cannot exist since the bound of Result 2 is bigger than the order of the group (using the square root bound for the minimum weight, and the actual minimum weight $q+1$ when $n = q^2$ and q is a prime power).

For the case where n is prime and $n \equiv 1 \pmod 8$, the code of $P(n)$ over $\mathbb{F}_p$ is $C = [n, \frac{n-1}{2}, d]_p$ where $d \geq \sqrt{n}$, (the square-root bound) for p any prime dividing $\frac{n-1}{4}$. In [KL04] a 2-PD-set for C of size 6, and for the dual code, a 2-PD-set of size 10, was found for all n satisfying the stated conditions. Further results for this class of codes can be found in [Lim05].

7 Conclusion

This paper does not claim to give an exhaustive survey of all the known work to date on the discovery of PD-sets and s-PD-sets. Huffman [Huf98] gives a survey up to the date of publication of his chapter in the Handbook of Coding Theory. A more complete survey of recent results will appear in [Sen]. After a somewhat sporadic interest following the intitial work of MacWilliams, interest in the subject has picked up in the last few years, due to the demand for good decoding methods, but a lot of the recent work is not yet published and available at this time only in preprint form. The website

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

contains some of the papers jointly authored by J. D. Key but still in press.

Acknowledgement

The author thanks the South African Mathematical Society for the invitation to give a plenary address at the 48^{th} annual SAMS congress at Rhodes University in November 2005, and the School of Mathematical Sciences at the University of KwaZulu-Natal in Pietermaritzburg for their hospitality.

References

[AK92] E. F. Assmus, Jr and J. D. Key. *Designs and their Codes*. Cambridge: Cambridge University Press, 1992. Cambridge Tracts in Mathematics, Vol. 103 (Second printing with corrections, 1993).

[AK98] E. F. Assmus, Jr and J. D. Key. Polynomial codes and finite geometries. In V. S. Pless and W. C. Huffman, editors, *Handbook of Coding Theory*, pages 1269–1343. Amsterdam: Elsevier, 1998. Volume 2, Part 2, Chapter 16.

[BC94] Wieb Bosma and John Cannon. *Handbook of Magma Functions*. Department of Mathematics, University of Sydney, November 1994. http://magma.maths.usyd.edu.au/magma/.

[Cha92] Hervé Chabanne. Permutation decoding of abelian codes. *IEEE Trans. Inform. Theory*, 38:1826–1829, 1992.

[Fis] W. Fish. Private communication.

[GAP] GAP. Groups, Algorithms and Programming, Version 4. The GAP Group, Lehrstuhl D für Mathematik, RWTH Aachen, Germany and School of Mathematical and Computational Sciences, University of St. Andrews, Scotland. http://www-gap.dcs.st-and.ac.uk/ gap/.

[Gor82] D. M. Gordon. Minimal permutation sets for decoding the binary Golay codes. *IEEE Trans. Inform. Theory*, 28:541–543, 1982.

[Huf98] 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.

[Joy05] David Joyner. Conjectural permutation decoding of some AG codes. *ACM SIGSAM Bulletin*, 39, 2005. No.1, March.

[KL04] J. D. Key and J. Limbupasiriporn. Permutation decoding of codes from Paley graphs. *Congr. Numer.*, 170:143–155, 2004.

[KMMa] J. D. Key, T. P. McDonough, and V. C. Mavron. Information sets and partial permutation decoding of codes from finite geometries. *Finite Fields Appl.* (To appear).

[KMMb] J. D. Key, T. P. McDonough, and V. C. Mavron. Partial permutation decoding of codes from affine geometry designs. Submitted.

[KMM05] 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.

[KMRa] J. D. Key, J. Moori, and B. G. Rodrigues. Binary codes from graphs on triples and permutation decoding. *Ars Combin.* To appear.

[KMRb] J. D. Key, J. Moori, and B. G. Rodrigues. Partial permutation decoding of some binary codes from graphs on triples. Submitted.

[KMR04a] J. D. Key, J. Moori, and B. G. Rodrigues. Binary codes from graphs on triples. *Discrete Math.*, 282/1-3:171–182, 2004.

[KMR04b] J. D. Key, J. Moori, and B. G. Rodrigues. Permutation decoding for binary codes from triangular graphs. *European J. Combin.*, 25:113–123, 2004.

[KSa] J. D. Key and P. Seneviratne. Binary codes from rectangular lattice graphs and permutation decoding. *European J. Combin.*,To appear.

[KSb] J. D. Key and P. Seneviratne. Codes from the line graphs of complete multipartite graphs and PD-sets. Submitted.

[KSc] J. D. Key and P. Seneviratne. Permutation decoding of binary codes from lattice graphs. *Discrete Math.* (Special issue dedicated to J. Seberry), To appear.

[KV] Hans-Joachim Kroll and Rita Vincenti. Antiblocking systems and PD-sets. Preprint.

[KV05] Hans-Joachim Kroll and Rita Vincenti. PD-sets related to the codes of some classical varieties. *Discrete Math.*, 301:89–105, 2005.

[Lim05] J. Limbupasiriporn. *Partial permutation decoding for codes from designs and finite geometries*. PhD thesis, Clemson University, 2005.

[Mac64] F. J. MacWilliams. Permutation decoding of systematic codes. *Bell System Tech. J.*, 43:485–505, 1964.

[Moo91] G. Eric Moorhouse. Bruck nets, codes, and characters of loops. *Des. Codes Cryptogr.*, 1:7–29, 1991.

[MS83] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland, 1983.

[Rod03] B. G. Rodrigues. *Codes of designs and graphs from finite simple groups*. PhD thesis, University of Natal, 2003.

[Sch64] J. Schönheim. On coverings. *Pacific J. Math.*, 14:1405–1411, 1964.

[Sen] Padmapani Seneviratne. Ph.D. thesis, Clemson University, To be submitted.

[Wol83] J. Wolfmann. A permutation decoding of the (24,12,8) Golay code. *IEEE Trans. Inform. Theory*, 29:748–750, 1983.