Permutation decoding for codes from designs, finite geometries and graphs

J. D. Key

Abstract

The method of permutation decoding was first developed by 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 specifed properties.

These talks will describe some recent developments in finding PD-sets for codes defined through the row-span over finite fields of incidence matrices of designs or graphs, or adjacency matrices of regular graphs, since these codes have many properties that can be deduced from the combinatorial properties of the designs or graphs, and often have a great deal of symmetry and large automorphism groups.

EXTENDED ABSTRACT

Permutation decoding, first developed by MacWilliams [Mac64], involves finding a set of automorphisms of a code called a PD-set. The method is described fully in MacWilliams and Sloane [MS83, Chapter 16, p. 513] and Huffman [Huf98, Section 8]. In [KMM05] and [KV05] the definition of PD-sets was extended to that of s-PD-sets for s-error-correction:

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 can be 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 can be moved by at least one member of $\mathcal{S}$ into $\mathcal{C}$.*

The algorithm for permutation decoding is as follows: if C is an $[n, k, d]_q$ code that can correct t errors, with check matrix H in standard form, then the generator matrix $G = [I_k|A]$ and $H = [A^T|I_{n-k}]$, for some A, with the first k coordinate positions corresponding to the information symbols. Any vector v of length k is encoded as vG. Suppose x is sent and y is received and at most t errors occur. Let $\mathcal{S} = \{g_1, \ldots, g_s\}$ be the PD-set. Compute the syndromes $H(yg_i)^T$ for $i = 1, \ldots, s$ until an i is found such that the weight of this vector is t or less. Compute the codeword c that has the same information symbols as yg_i and decode y as cg_i^{-1}.

The algorithm requires the generator matrix to be in standard form and thus an information set needs to be known. The property of having a PD-set will not, in general, be invariant under isomorphism of codes, i.e. it depends on the choice of information set. Notice also that the algorithm uses some ordering of the PD-set; ordering the PD-set according to nested s-PD-sets can reduce the time complexity of the decoding.

Furthermore, there is a bound on the minimum size of $\mathcal{S}$ (see [Gor82],[Sch64], or [Huf98]):

Result 1 *If $\mathcal{S}$ is a PD-set for a t-error-correcting $[n,k,d]_q$ code C, and $r = n-k$, then $|\mathcal{S}| \geq \left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \left\lceil \cdots \left\lceil \frac{n-t+1}{r-t+1} \right\rceil \cdots \right\rceil \right\rceil \right\rceil$.*

This result can be adapted to s-PD-sets for $s \leq t$ by replacing t by s in the formula.

Here the codes considered will be classes that arise from the row span over a finite field of an adjacency matrix or an incidence matrix of a graph, or an incidence matrix of a design or finite geometry. PD-Sets or s-PD-sets have been found for some classes of graphs and geometries, including

- triangular graphs;
- lattice and rectangular lattice graphs;;
- line graphs of complete multipartite graphs;
- graphs on triples (uniform subset graphs);
- Hamming graphs;
- Paley graphs;
- finite affine and projective planes;
- other finite geometry designs;
- first-order and second-order Reed-Muller codes.

A nested sequence of s-PD-sets for $0 \leq s \leq t$ will reduce the time complexity of the decoding.

References

[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.

[KMM05] J. D. Key, T. P. McDonough, and V. C. Mavron. Partial permutation decoding for codes from finite planes. *European J. Combin.*, 26:665–682, 2005.

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

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

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

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