

Error-correcting Codes, Permutation Groups and Uncoverings

Robert Bailey

Queen Mary, University of London

`r.f.bailey@qmul.ac.uk`

`http://www.maths.qmul.ac.uk/~rfb/`

ALCOMA05, 6th April 2005

20th British Combinatorial Conference, 13th July 2005

PERMUTATION GROUPS AS CODES

- Let G be a permutation group acting on $\Omega = \{1, \dots, n\}$.
- We can write elements of G as ordered n -tuples of distinct symbols from Ω ,

$$\text{e.g. } 231794685 \in S_9$$

- Idea: use permutations in this form as codewords.
- Define the Hamming distance in the usual way, e.g.

$$d(15432, 25413) = 3$$

- However,

$$\begin{aligned}d_H(g, h) &= \#x \text{ where } x^g \neq x^h \\ &= n - |\text{Fix}(gh^{-1})|\end{aligned}$$

- Thus the minimum distance is

$$d = \min_{\substack{g \in G \\ g \neq 1}} \{n - |\text{Fix}(g)|\},$$

the *minimum degree* of G .

- Clearly we can correct $r = \lfloor \frac{d-1}{2} \rfloor$ errors.

A DECODING ALGORITHM

Definition

A *base* for G is a sequence of points (x_1, \dots, x_b) from Ω such that its pointwise stabiliser is the identity.

- The action of $g \in G$ on a base *uniquely determines that element*, i.e. if $(x_1, \dots, x_b)^g = (x_1, \dots, x_b)^h$, then $g = h$.
- If the error positions lie outside positions labelled by a base, we can decode successfully.
- **PROBLEM:** We can't necessarily tell in which positions the errors are.

SOLUTION:

- We need a set of bases such that any combination of r error positions is disjoint from at least one base.
- We call this an *uncovering-by-bases*.
- E.g. for a sharply k -transitive group, ANY k points form a base.
- So we need a set \mathcal{U} of k -subsets of $\{1, \dots, n\}$ such that any r -subset is *disjoint* from at least one k -set.
- These k -sets are the complements of the blocks of a *covering design*, so we call it an *uncovering*.

Example:

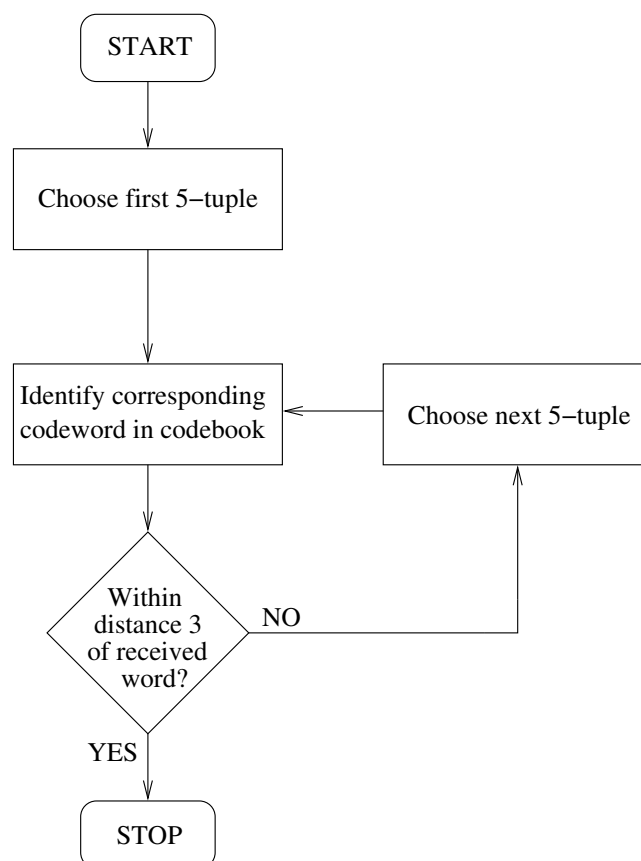
- Mathieu Group M_{12}
- Sharply 5-transitive, degree 12, order 95040
- Minimum degree 8
- Can correct $\left\lfloor \frac{8-1}{2} \right\rfloor = 3$ errors
- Need a $(12, 5, 3)$ -uncovering

Example:

1	2	3	4	5
1	2	6	11	12
1	3	7	8	9
1	4	6	7	10
1	5	8	9	11
2	4	8	9	12
2	5	7	10	11
3	4	7	11	12
3	5	6	10	12
3	6	8	9	11
6	7	8	9	10

Once we have such an uncovering, for each 5-set we determine the *unique* group element agreeing with received word in these 5 positions.

If distance is ≤ 3 , then stop. Otherwise, go to next 5-set and repeat.



Example:

Suppose we transmit

$$g = 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12$$

and receive

$$w = 6\ 2\ 1\ 4\ 6\ 6\ 7\ 8\ 9\ 10\ 11\ 12$$

w has errors in positions 1, 3 and 5.

As the algorithm works through the uncovering, it outputs:

Error (repeated symbol);

Error (repeated symbol);

6 3 1 4 12 2 7 8 9 5 10 11, which is distance 6 from w and is rejected;

Error (repeated symbol);

Error (repeated symbol);

1 2 3 4 5 6 7 8 9 10 11 12, which is distance 3 from w and is accepted.

DO UNCOVERINGS-BY-BASES EXIST?

- Let G be a group acting on Ω , where $|\Omega| = n$, and suppose G has minimum degree d , so $r = \lfloor \frac{d-1}{2} \rfloor$.
- To show a UBB exists, we must show that for any r -set of error positions, there is a base disjoint from it.
- Let R be an arbitrary r -subset of Ω . Suppose for a contradiction that R meets every base for G .
- Then $\bar{R} = \Omega \setminus R$ has non-trivial pointwise stabiliser (as it does not contain a base).
- So $\exists g \in G$ which fixes \bar{R} pointwise, so g has at least $n - r$ fixed points.
- But g can have at most $n - d < n - r$ fixed points.
 $\Rightarrow \Leftarrow$
- NB. Actually *constructing* a UBB is much harder!

For which groups can we construct a UBB?

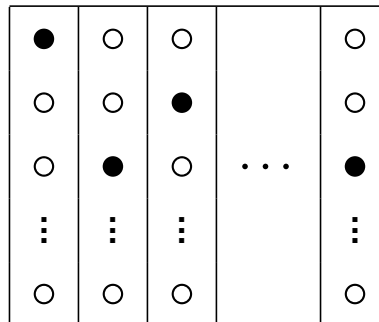
The following list of groups are all *base-transitive*, that is G acts transitively on its irredundant bases.

- *Sharply k -transitive groups*
Any k points form a base.
- $GL(n, q)$ acting on $\mathbb{F}_q^n \setminus \{0\}$
A base for the group is a basis for the vector space.
- $AGL(n, q)$ acting on \mathbb{F}_q^n
A base for the group is an affine basis for \mathbb{F}_q^n .
- $C_m \wr S_n$ acting on $\{1, \dots, m\} \times \{1, \dots, n\}$

The base-transitive groups were classified by Maund (D.Phil. thesis).

More on $C_m \wr S_n$

- A base consists of a single point from each copy of $\{1, \dots, m\}$.
- We call such a base a *transversal*.



- Here we want to correct $r = \lfloor \frac{m-1}{2} \rfloor$ errors.
- A UBB consists of $r + 1$ disjoint transversals.

A CONJECTURE

Conjecture. *For any finite permutation group G , there exists a UBB for G which is contained in a single orbit on irredundant bases.*

True for the following:

- Base-transitive groups (trivially)
- Transitive groups on ≤ 20 points (computer search)
- Primitive groups on ≤ 30 points (computer search)
- S_m acting on 2-subsets

The “single-orbit property” is preserved by taking direct products and wreath products.

Stronger conjecture: \exists UBB as above, with size bounded by a linear function in n .

S_m acting on 2-subsets

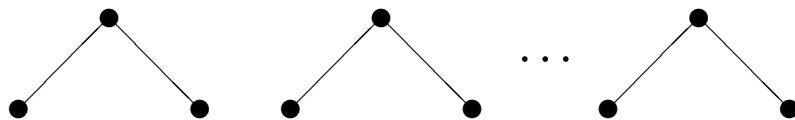
Think of these as edges of K_m .

Degree $\binom{m}{2}$.

Minimum distance $\binom{m}{2} - \binom{m-2}{2} - 1 = 2(m-2)$

\Rightarrow correction capability $r = m - 3$.

Example of an irredundant base:



Need to show that for any $m - 3$ edges, \exists base like this disjoint from them.

How?