Uncoverings-by-bases for groups and matroids

Robert Bailey

Queen Mary, University of London

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

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

Workshop on Covering Arrays, 16th May 2006

COVERINGS, UNCOVERINGS AND UBBs

- An (n,m,r) *covering design* is a set $\mathcal{C}$ of m-subsets of $\{1,\ldots,n\}$ such that any r-subset of $\{1,\ldots,n\}$ is contained in at least one of the m-subsets.

- An (n,k,r)-*uncovering* is a set $\mathcal{U}$ of k-subsets of $\{1,\ldots,m\}$ such that any r-subset of $\{1,\ldots,n\}$ is *disjoint* from at least one of the k-subsets.

- A *base* for a finite permutation group G acting on a set Ω is a sequence of points $(x_1,\ldots,x_b)$ from Ω such that its pointwise stabiliser is the identity.

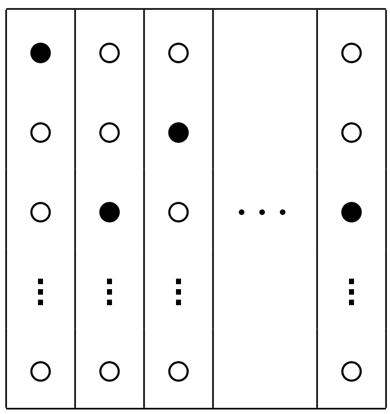
- An *uncovering-by-bases* (or UBB) for G acting on Ω is a set $\mathcal{U}$ of bases so that any r-subset of Ω is disjoint from at least one base in $\mathcal{U}$.

- Interesting case: when $r = \left\lfloor \frac{d-1}{2} \right\rfloor$, where d is the minimum degree of G.

EASY EXAMPLES

- If G is sharply k-transitive and has degree n, we have $r = \left\lfloor \frac{n-k}{2} \right\rfloor$ and any k-subset of $\{1, \ldots, n\}$ is a base. So we just need an (n, k, r)-uncovering.

- $H \wr S_n$, where H is a regular group of degree m.
  - Minimum degree is m, so $r = \left\lfloor \frac{m-1}{2} \right\rfloor$.
  - We think of Ω as an $m \times n$ rectangle. A base consists from a single point drawn from each column:

    We call this a *transversal* of Ω.
  - A UBB consists of $r + 1$ disjoint transversals.

$\mathrm{GL}(n,q)$

- A basis for the vector space $\mathbb{F}_q^n$ is a base for $\mathrm{GL}(n,q)$ acting on the non-zero vectors.

- The minimum degree is $q^n - q^{n-1}$, so $r = \left\lfloor \frac{q^n - q^{n-1} - 1}{2} \right\rfloor$.

- For $n = 2$, this is easy to deal with.

- For $n = 3$, things are more difficult!

AN UNCOVERING BY TRIPLES

- To obtain a $(2m,3,m-1)$-uncovering, think of the $2m$-set as $\mathbb{Z}_{2m}$, then take all triples of the form $\{i-1,i,i+m\}$ for $i \in \mathbb{Z}_{2m}$.

- For example, with $m=5$, we have

$\boxed{1}$	$\boxed{2}$	3	4	5	6	$\boxed{7}$	8	9	10
1	$\boxed{2}$	$\boxed{3}$	4	5	6	7	$\boxed{8}$	9	10
1	2	$\boxed{3}$	$\boxed{4}$	5	6	7	8	$\boxed{9}$	10
1	2	3	$\boxed{4}$	$\boxed{5}$	6	7	8	9	$\boxed{10}$
$\boxed{1}$	2	3	4	$\boxed{5}$	$\boxed{6}$	7	8	9	10
1	$\boxed{2}$	3	4	5	$\boxed{6}$	$\boxed{7}$	8	9	10
1	2	$\boxed{3}$	4	5	6	$\boxed{7}$	$\boxed{8}$	9	10
1	2	3	$\boxed{4}$	5	6	7	$\boxed{8}$	$\boxed{9}$	10
1	2	3	4	$\boxed{5}$	6	7	8	$\boxed{9}$	$\boxed{10}$
$\boxed{1}$	2	3	4	5	$\boxed{6}$	7	8	9	$\boxed{10}$

- We use this construction to construct a UBB for $\mathrm{GL}(3,q)$, by forcing each triple to be a basis for the vector space.

$\mathrm{GL}(3, q)$, for q odd

- We need a map from $\mathbb{Z}_{2m}$ to $\mathbb{F}_q^3$ which forces each triple to be a basis.

- Instead of the vector space, we work in the extension field $\mathbb{F}_{q^3}$.

- Suppose q is odd, so that $q^3 - 1$ is even, say $q^3 - 1 = 2m$.

- We can write the elements of $\mathbb{F}_{q^3} \setminus \{0\}$ as
$$\left\{1, \alpha, \alpha^2, \ldots, \alpha^{2m-1}\right\}$$
where α is a primitive element of $\mathbb{F}_{q^3}$.

- Obvious map: $i \mapsto \alpha^i$. Unfortunately, this doesn't work! (Since $\alpha^m = -1$, $\{1, \alpha, \alpha^{m+1}\} = \{1, \alpha, -\alpha\}$, which is clearly not a basis.)

Instead, we use the following trick.

- Define $\varphi_\alpha : \mathbb{Z}_{2m} \to \mathbb{F}^*_{q^3}$ by

i	0	1	2	$\cdots$	$m-1$	m	$m+1$	$\cdots$	$2m-3$	$2m-2$	$2m-1$
$\varphi_\alpha(i)$	1	α	α^2	$\cdots$	α^{m-1}	α^{m+2}	α^{m+3}	$\cdots$	α^{2m-1}	α^m	α^{m+1}

- This leaves us with several cases to check, it reduces to verifying that $\{1,\alpha,\alpha^2\}$ and $\{1,\alpha,\alpha^3\}$ are bases.

- $\{1,\alpha,\alpha^2\}$ is always a basis.

- $\{1,\alpha,\alpha^3\}$ is NOT always a basis, but by judicious choice of α, we can ensure this.

- That such an element always α exists requires non-trivial theorems from number theory (such as the *Primitive Normal Basis Theorem*).

Basis for $\mathbb{F}_{27}$	Basis for $\mathbb{F}_3^3$
$1, \alpha, \alpha^{16}$	$001, 010, 201$
$\alpha, \alpha^2, \alpha^{17}$	$010, 100, 211$
$\alpha^2, \alpha^3, \alpha^{18}$	$100, 102, 011$
$\alpha^3, \alpha^4, \alpha^{19}$	$102, 122, 110$
$\alpha^4, \alpha^5, \alpha^{20}$	$122, 022, 202$
$\alpha^5, \alpha^6, \alpha^{21}$	$022, 220, 221$
$\alpha^6, \alpha^7, \alpha^{22}$	$220, 101, 111$
$\alpha^7, \alpha^8, \alpha^{23}$	$101, 112, 212$
$\alpha^8, \alpha^9, \alpha^{24}$	$112, 222, 021$
$\alpha^9, \alpha^{10}, \alpha^{25}$	$222, 121, 210$
$\alpha^{10}, \alpha^{11}, \alpha^{13}$	$121, 012, 002$
$\alpha^{11}, \alpha^{12}, \alpha^{14}$	$012, 120, 020$
$\alpha^{12}, \alpha^{15}, 1$	$120, 200, 001$
$\alpha^{15}, \alpha^{16}, \alpha$	$200, 201, 010$
$\alpha^{16}, \alpha^{17}, \alpha^2$	$201, 211, 100$
$\alpha^{17}, \alpha^{18}, \alpha^3$	$211, 011, 102$
$\alpha^{18}, \alpha^{19}, \alpha^4$	$011, 110, 122$
$\alpha^{19}, \alpha^{20}, \alpha^5$	$110, 202, 022$
$\alpha^{20}, \alpha^{21}, \alpha^6$	$202, 221, 220$
$\alpha^{21}, \alpha^{22}, \alpha^7$	$221, 111, 101$
$\alpha^{22}, \alpha^{23}, \alpha^8$	$111, 212, 112$
$\alpha^{23}, \alpha^{24}, \alpha^9$	$212, 021, 222$
$\alpha^{24}, \alpha^{25}, \alpha^{10}$	$021, 210, 121$
$\alpha^{25}, \alpha^{13}, \alpha^{11}$	$210, 002, 012$
$\alpha^{13}, \alpha^{14}, \alpha^{12}$	$002, 020, 120$
$\alpha^{14}, 1, \alpha^{15}$	$020, 001, 200$

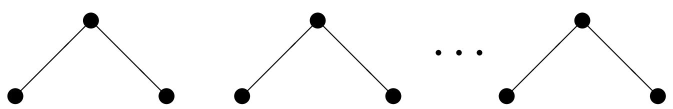
S_m ACTING ON 2-SUBSETS

- Consider $G = S_m$, acting on the 2-subsets of $\{1, \ldots, m\}$.

- Degree $\binom{m}{2}$, minimum degree $2(m-2)$, so we have $r = m - 3$.

- Think of the 2-subsets as the edges of the complete graph K_m.

- An example of a base is a spanning subgraph of the form



  We call these bases V-*graphs*.

- V-graphs can easily be embedded into Hamilton circuits.

CONSTRUCTING A UBB FOR THIS

Using Ore's Theorem, we can show that $K_m \setminus R$ is Hamiltonian (where R is an arbitrary r-set of edges). This shows us that an uncovering-by-bases formed from V-graphs always exists.

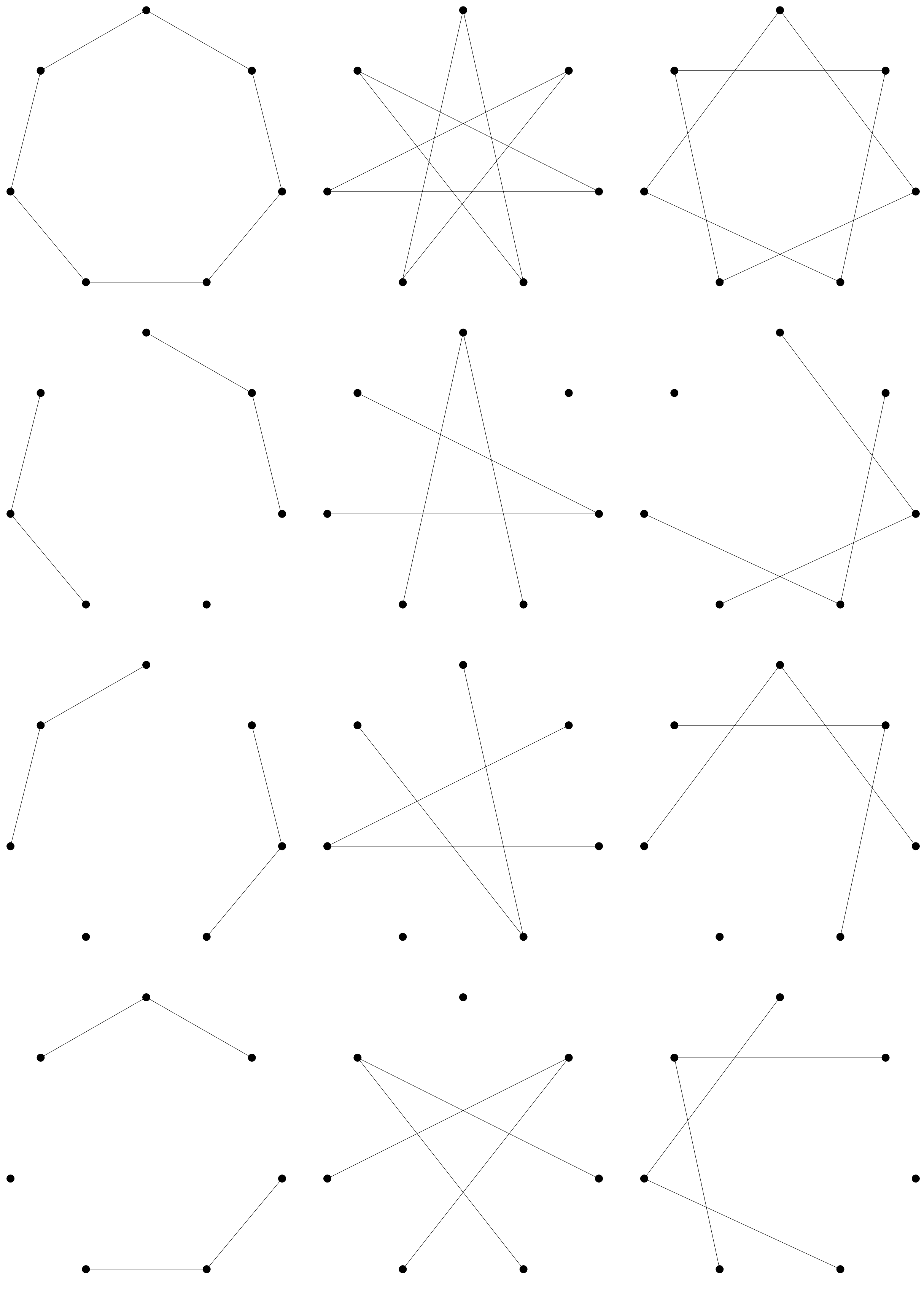
To construct one:

- Use decompositions of K_m into either (i) Hamilton cycles (if m is odd), or (ii) Hamilton cycles and a 1-factor (if m is even).

- In each Hamilton circuit obtained, obtain a number of V-graphs.

- How many we need is determined by congruence classes modulo 3, but we either need 3 or 4 to succeed.

- For example, with $m = 7$ we have the following.



UBBs FOR MATROIDS

For a particular class of groups, known as *IBIS groups*, the irredundant bases of the group are precisely the bases (i.e. maximal independent sets) of a matroid.

The definition of uncovering-by-bases holds for matroids. (For IBIS groups the two notions coincide.)

For example, with the uniform matroid $U_{m,n}$, where every m-subset of $\{1,\ldots,n\}$ is a base, a UBB is just an (n,m,r)-uncovering (for some r).

Questions:

- What is the obvious value of r to choose?
- What does the r we had before represent in terms of matroid theory?

- For an IBIS group G, the fixed point sets of G are all flats of the corresponding matroid. In fact, every maximal proper flat is a fixed point set.

- Thus r, as we had it before, can be determined from the cardinality of a maximal proper flat.

- In the group case, this parameter has a “nice” interpretation, in terms of coding theory.

- What, if anything, does it mean for matroids?