

Primitive Elements and Uncoverings

Robert Bailey

Queen Mary, University of London

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

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

16th Postgraduate Combinatorial Conference

21st March 2005

WHAT'S AN UNCOVERING?

- Let Ω be a set of size n .
- An (n, k, r) -*uncovering* is a set \mathcal{U} of k -subsets of Ω such that any r -subset is disjoint from at least one k -set.
- Example: $n = 12, k = 5, r = 3$

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

- Another example: $n = 10, k = 3, r = 4$

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

- This pattern can be generalised to give a $(2m, 3, m - 1)$ -uncovering.

- In general, it consists of all triples of the form

$$\{i - 1, i, i + m\}$$

with addition modulo $2m$.

BASES

- Let G be a group acting on Ω .
- A *base* for G is a sequence of points (x_1, x_2, \dots, x_b) from Ω such that its pointwise stabiliser is the identity.
- The action of an element $g \in G$ uniquely determines that element, i.e. if $(x_1, x_2, \dots, x_b)^g = (x_1, x_2, \dots, x_b)^h$, then $g = h$.
- Example: $GL(n, q)$ acting on $\mathbb{F}_q^n \setminus \{0\}$
A base for $GL(n, q)$ in this action is just a basis for the vector space \mathbb{F}_q^n .

UNCOVERINGS-BY-BASES

- An *uncovering-by-bases* for a group G acting on Ω is an uncovering of Ω with the restriction that each k -set in the uncovering is a base for G .
- Why should you care? They are useful in decoding certain error-correcting codes based on G .
- Constructing a UBB is, in general, quite hard. (Especially for linear groups like $GL(n, q)$!)
- In this talk, we'll concentrate on $GL(3, q)$ acting on \mathbb{F}_q^3 .

- Recall our “cyclic triples” uncovering.
- We’d like to use this to construct a UBB for $GL(3, q)$.
- Our construction has a nice cyclic structure to it.
- **PROBLEM:** \mathbb{F}_q^3 doesn’t.
- **SOLUTION:** Move from the vector space \mathbb{F}_q^3 into the extension field \mathbb{F}_{q^3} .

FIELD THEORY: A CRASH COURSE

- Let K be a field, and let α be a root of some irreducible polynomial $f(x) \in K[x]$ of degree n .

- Then

$$K(\alpha) = \{\lambda_0 + \lambda_1\alpha + \lambda_2\alpha^2 + \cdots + \lambda_{n-1}\alpha^{n-1} \mid \lambda_i \in K\}$$

is the *extension field* of K with *defining element* α .

- $K(\alpha)$ has a vector space structure over K of dimension n , so we say the extension has *degree* n .
- A basis for this vector space is $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ (but there are many others!).

FINITE FIELDS

- If $K = \mathbb{F}_q$, then any extension of degree n is isomorphic, so we have a unique \mathbb{F}_{q^n} .
- **FACT:** The multiplicative group $\mathbb{F}_{q^n}^*$ is a *cyclic* group of order $q^n - 1$.
- A generator for this group is called a *primitive element* of \mathbb{F}_{q^n} .
- So we can write the non-zero elements of \mathbb{F}_{q^n} as

$$\{1, \alpha, \alpha^2, \dots, \alpha^{q^n-1}\}$$

where α is a primitive element.

CONSTRUCTING A UBB

- Consider the $n = 3$ and where q is odd, so $q^3 - 1$ is even, say $q^3 - 1 = 2m$.
- We'd like to apply our "cyclic triples" construction in such a way that the image of each triple is a basis, i.e. a linearly independent set over \mathbb{F}_q .

- Try the obvious way, where $i \mapsto \alpha^i$ (for $0 \leq i \leq 2m - 1$). This gives the triple

$$\{1, \alpha, \alpha^{m+1}\},$$

and scalar multiples of it by powers of α .

- But, since $\alpha^{2m} = 1$, we have $\alpha^m = -1$, so this triple becomes

$$\{1, \alpha, -\alpha\}$$

which is clearly *not* LI.

A SILLY IDEA

- To solve this problem, we re-order the non-zero elements of \mathbb{F}_{q^3} as follows:

$$\{1, \alpha, \alpha^2, \dots, \alpha^{m-1}, \alpha^{m+2}, \alpha^{m+3}, \dots, \alpha^{2m-1}, \alpha^m, \alpha^{m+1}\}$$

- This gives triples such as $\{1, \alpha, \alpha^{m+3}\}$.
- There are various different kinds of triples, but all are either equivalent to $\{1, \alpha, \alpha^2\}$ or $\{1, \alpha, \alpha^3\}$.
- The first of these is clearly LI, as it is the standard basis. The second requires us to be judicious in our choice of primitive element.
- Note that $\{1, \alpha, \alpha^3\}$ LI $\iff \alpha$ satisfies no polynomial of the form $x^3 + ax + b = 0$ (for $a, b \in \mathbb{F}_q$).

A THEOREM FROM NUMBER THEORY

Theorem (Carlitz; Davenport; Lenstra & Schoof; Cohen & Huczynska): For any q and n , there exists a basis for \mathbb{F}_{q^n} over \mathbb{F}_q of the form

$$\{\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{n-1}}\}$$

where α is a primitive element. (Such a basis is called a *primitive normal basis*.)

- These elements are the *conjugates* of α , i.e. the complete set of roots of $m_\alpha(x)$ (the minimal polynomial of α).
- The sum of the conjugates of α , the *trace* of α , is equal to the coefficient of x^{n-1} in $m_\alpha(x)$.
- For α as above, we have $\text{Trace}(\alpha) \neq 0$. Thus the coefficient of x^{n-1} in $m_\alpha(x)$ is not zero.

- In our case, $n = 3$, so the minimum polynomial $m_\alpha(x)$ is a cubic.
- If we have a primitive normal basis, we can choose α where the coefficient of x^2 in $m_\alpha(x)$ is non-zero.
- Thus the only monic cubic satisfied by α has the form

$$x^3 + ax^2 + bx + c$$

where $a \neq 0$.

- So, in particular, α satisfies *no* polynomial of the form $x^3 + ax + b = 0$, which is what we wanted!