Basis-transitive Gruppen vom Rang 3

Uncovering durch Tripel

Theorem:
Sei $\Omega = \mathbb{Z}_{2m}$ und U={(i-1,i,i+m): $i \in \mathbb{Z}_{2m}$}.
Dann ist U ein (2m,3,m-1)-Uncovering bzgl. der Addition (mod 2m).

Beispiel 1:
Sei m=5. Dann ist U={(i-1,i,i+5): $i \in \mathbb{Z}_{10}$} ein (10,3,4)-Uncovering.

[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]

Lemma:
Sei Ω={1,...,v}, v gerade und U ein (v,k,t)-Uncovering. Konstruiere eine Teilmenge W von U, in dem man die Koblöcke aus U enfernt, die v enthalten.
Dann ist W ein (v-1,k,t-1)-Uncovering (von $\bar{\Omega} = \Omega \setminus \{v\}$.)

Korollar:
Sei U ein (2m,3,m-1)-Uncovering wie im Theorem beschrieben. Erhalte die Teilmenge W von U, durch Entfernen aller Tripel, die den Punkt 2m enthalten. Dann ist W ein (2m-1,3,m-2)-Uncovering. (W hat 2m-3 Elemente.)

Beispiel 2:
Konstruiere W durch Streichen der Koblöcke aus Beisipel 1, welche die 10 enthalten. Dann ist W ein (9,3,3)-Uncovering der Größe 7:

Beispiel 1:

[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]~~

(9,3,3)-Uncovering W:

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

Einige Eigenschaften von endlichen Körpern:

Bemerkung:

1) Sei F_q der endliche Körper mit q Elementen, wobei q Primzahlpotenz ist. Dann ist $F_{q^n}: F_q$ Körpererweiterung vom Grad n.
2) Sei $\bar{F}_q := F_q \setminus \{0\}$, dann ist $\bar{F}_q$ bzgl. der Multiplikation eine zyklische Gruppe der Ordnung q-1

Definition 1:
Sei E:K Körpererweiterung. Sei $\alpha \in E\,(hier\ F_{q^n})$. Dann heißen $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}$ die (algebraischen) Konjugierten von $\alpha\ über\ K\,(hier\ F_q)$.

Definition 2:
Sei $\alpha \in E$, dann ist die Spur von α wie folgt definiert:

$$Tr_{E:K}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \ldots + \alpha^{q^{n-1}}$$

Satz:
Sei $f(x) = x^n + a_{n-1} \cdot x^{n-1} + \ldots + a_1 \cdot x + a_0$ das Minimalpolynom von α über K. Dann gilt:
$Tr_{E:K}(\alpha) = -a_{n-1}$

Definition 3:
Eine Basis der Form $B = \{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}\}$ heißt normale Basis von E:K.
α heißt dann freies Element.

Lemma:
Sei $\alpha \in E$ ein freies Element. Dann gilt: $Tr_E: K(\alpha) \neq 0$.

Theorem:
Für jede Primzahlpotenz q und n>1, existiert eine primitive normale Basis von $F_{q^n}: F_q$.

Korollar:
Für jede Primzahlpotenz q und n>1, existiert ein Element $\alpha \in F_{q^n}$ mit $Tr_{F_{q^n}: F_q}$.

Quelle: R. F. Bailey, *Permutation Groups, Error-Correcting Codes and Uncoverings*, Queen Mary, University of London, 02.11.2005