4.5 Uncoverings-by-bases für GL(3,q)

Thema: Konstruktion eines Uncovering-by-bases (UBB) für $GL(3,q)$, operierend auf $\mathbb{F}_q^3 \backslash \{0\}$.

Wir übertragen das Problem in den Erweiterungskörper $\mathbb{F}_{q^3}$, da Vektorräume über $\mathbb{F}_q$ isomorph sind. Daher können wir uns die Ergebnisse über endliche Körper aus dem letzten Abschnitt zunutze machen. Wir bekommen also eine Menge von Basen für $\mathbb{F}_{q^3}$ und erhalten mittels eines Isomorphismus Basen für $\mathbb{F}_q^3$.
Um die Uncoverings zu UBBs zu machen, betrachten wir die Fälle q gerade und q ungerade gesondert.

q ungerade

Dann ist $m := q^3 - 1$ gerade. Wenn α ein primitives Element von $\mathbb{F}_{q^3}$ ist, dann sind alle Elemente von $\mathbb{F}_{q^3}$, die ungleich 0 sind, Potenzen von α, also $1, \alpha, \alpha^2, ..., \alpha^{2m-1}$. Es gilt $(\alpha^m)^2 = \alpha^{2m} = 1$, also $\alpha^m = -1$.
Wir nehmen die "zyklische Tripel"-Konstruktion eines Uncoverings aus 4.2.1 und versuchen, diese mittels einer Bijektion ψ in ein UBB umzuwandeln:

$$\psi : \mathbb{Z}_{2m} \to \mathbb{F}_{q^3}^* = \mathbb{F}_{q^3} \backslash \{0\}$$

$$i \mapsto \alpha^i$$

Das funktioniert nicht, da jedes Tupel nun die Form $\{\alpha^{i-1}, \alpha^i, \alpha^{i+m}\}$ hat. Dies ist eine Basis, genau dann wenn $\{1, \alpha, \alpha^{m-1}\}$ eine Basis ist. Da aber $\alpha^m = -1$ ist, ist $\alpha^{m+1} = -\alpha$ und $\{1, \alpha, -\alpha\}$ ist keine Basis.

Also brauchen wir eine andere Bijektion:

$$\varphi : \mathbb{Z}_{2m} \to \mathbb{F}_{q^3}^*$$

mit

i	0	1	2 ...	$m-1$	m	$m+1$ ...	$2m-3$	$2m-2$	$2m-1$
$\varphi(i)$	1	α	α^2 ...	α^{m-1}	α^{m+2}	α^{m+3} ...	α^{2m-1}	α^m	α^{m+1}

Theorem 4.5.1

Sei q ungerade. Dann ist $\{\varphi(i-1), \varphi(i), \varphi(i+m)\}$, mit $i \in \mathbb{Z}_{2m}$, ein UBB für $GL(3,q)$, operierend auf $\mathbb{F}_{q^3}$.

Wir wollten aber ein UBB für $GL(3,q)$, operierend auf $\mathbb{F}_q^3$. Für jedes q brauchen wir also einen Isomorphismus zwischen $\mathbb{F}_{q^3}$ und $\mathbb{F}_q^3$. Das kleinste Beispiel hierfür ist immer noch groß: $GL(3,3)$, operierend auf den 26 Nicht-Null-Vektoren von $\mathbb{F}_3^3$.

Beispiel 4.5.2

Um den Isomorphismus zwischen dem Vektorraum $\mathbb{F}_3^3$ und dem Erweiterungskörper $\mathbb{F}_{27}$ zu bestimmen, müssen wir das Minimalpolynom des primitiven Elements α kennen. Nach Lidl und Niederreiter ist das Polynom x^3+2x^2+1 irreduzibel und hat ein primitives Element als Nullstelle. Da die Spur dieses Elements ungleich Null ist, genügt es unseren Anforderungen. Sei dieses Polynom also das Minimalpolynom von α. Also gilt:

$$\begin{aligned} & 0 &&= \alpha^3 + 2\alpha^2 + 1 \\ \Leftrightarrow\ & \alpha^3 &&= -2\alpha^2 - 1 \\ \Leftrightarrow\ & \alpha^3 &&= \alpha^2 - 1 \end{aligned}$$

Mittels dieser Gleichung können wir jede Potenz von α als Linearkombination von $1, \alpha, \alpha^2$ schreiben und die Koeffiziententripel als Elemente des Vektorraums:

1	001
α	010
α^2	010
$\alpha^3 = \alpha^2 + 2$	102
$\alpha^4 = \alpha^2 + 2\alpha + 2$	122
$\alpha^5 = 2\alpha + 2$	022
$\alpha^6 = 2\alpha^2 + 2\alpha$	220
$\alpha^7 = \alpha^2 + 1$	101
$\alpha^8 = \alpha^2 + \alpha + 2$	122
$\alpha^9 = 2\alpha^2 + 2\alpha + 2$	222
$\alpha^{10} = \alpha^2 + 2\alpha + 1$	121
$\alpha^{11} = \alpha + 2$	012
$\alpha^{12} = \alpha^2 + 2\alpha$	120
$\alpha^{13} = 2$	002
$\alpha^{14} = 2\alpha$	020
$\alpha^{15} = 2\alpha^2$	200
$\alpha^{16} = 2\alpha^2 + 1$	201
$\alpha^{17} = 2\alpha^2 + \alpha + 1$	211
$\alpha^{18} = \alpha + 1$	011
$\alpha^{19} = \alpha^2 + \alpha$	110
$\alpha^{20} = 2\alpha^2 + 2$	202
$\alpha^{21} = 2\alpha^2 + 2\alpha + 1$	211
$\alpha^{22} = \alpha^2 + \alpha + 1$	111
$\alpha^{23} = 2\alpha^2 + \alpha + 2$	212
$\alpha^{24} = 2\alpha + 1$	021
$\alpha^{25} = 2\alpha^2 + \alpha$	210

Basis für $\mathbb{F}_{27}$	Basis für $\mathbb{F}_3^3$
$1, \alpha, \alpha^{16}$	011,010,201
$\alpha, \alpha^2, \alpha^{17}$	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
$\alpha^{16}, \alpha^{17}, \alpha^2$	201,211,010
$\alpha^{17}, \alpha^{18}, \alpha^3$	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

q gerade

Sei nun q gerade und $2^s := q$. Da die Anzahl der Elemente von $\mathbb{F}^*_{2^{3s}}$ jetzt ungerade ist, nutzen wir die induzierte Konstruktion eines Uncoverings aus 4.2.4. Dazu führen wir das zusätzliche Element ∞ ein, konstruieren ein Uncovering von $S = \mathbb{F}^*_{2^{3s}} \cup \{\infty\}$ und entfernen dann die Tripel, die ∞ enthalten.

Wir haben $S = \{1, \alpha, \alpha^2, \ldots, \alpha^{2^{3s}-2}, \infty\}$, also $|S| = 2^{3s} =: 2m$. Konstruiere eine Bijektion:

$$\begin{aligned} \chi: \quad & \mathbb{Z}_{2m} \to S & \\ & i \mapsto \alpha^i & 0 \le i \le 2m-2 \\ & i \mapsto \infty & i = 2m-1 \end{aligned}$$

Theorem 4.5.3

Sei q gerade. Dann ist $\{\chi(i-1), \chi(i), \chi(i+m)\}, i \in \mathbb{Z}_{2m}$, ausgenommen die Tupel, die ∞ enthalten, ein UBB für $GL(3,q)$, operierend auf $\mathbb{F}_{q^3}$.

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