ETH Zürich, D-INFK
HS 2016, 28. November 2016

Prof. Ueli Maurer
Daniel Tschudi

Diskrete Mathematik

Lösung 11

11.1 Der Ring $F[x]_{m(x)}$

a) Die Elemente von $\mathrm{GF}(3)[x]_{x^2+2x}$ sind Polynome über $\mathrm{GF}(3)$ mit Grad höchstens 1 (Def. 5.35). Davon gibt es insgesamt 9 Stück. Durch Ausprobieren ermitteln wir die Nullteiler x (mit $x+2$), $x+2$ (mit x), $2x$ (mit $2x+1$) und $2x+1$ (mit $2x$).

b) Es ist

$$\mathrm{GF}(3)[x]_{x^2+2} = \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}.$$

Nach Lemma 5.36 ist

$$\mathrm{GF}(3)[x]^*_{x^2+2} = \{a(x) \in \mathrm{GF}(3)[x]_{x^2+2} \mid \mathrm{ggT}(a(x), x^2+2) = 1\}.$$

Da jedes $a(x) \in \mathrm{GF}(3)[x]_{x^2+2}$ Grad höchstens 1 hat, kann es lediglich zu $a(x) = c \cdot b(x)$ mit $c \in \mathrm{GF}(3)$ und $b(x) \in \mathrm{GF}(3)[x]$ von Grad 1 zerlegt werden (denn $\deg(pq) = \deg(p) + \deg(q)$ in $\mathrm{GF}(3)[x]$). Also sind die einzigen Teiler von $a(x)$ die konstanten Polynome und die konstanten Vielfachen von $a(x)$.

Als $\mathrm{ggT}(a(x), x^2+2)$ kommen also nur die monischen Polynome 1 und $x + a_1^{-1}a_0$ in Frage. Dabei gilt $\mathrm{ggT}(a(x), x^2+2) = x + a_1^{-1}a_0 \neq 1$ genau dann, wenn $a(x)$ und x^2+2 einen gemeinsamen Teiler von Grad 1 (also ein konstantes Vielfaches von $a(x)$) haben, also $a(x)$ ein linearer Teiler von x^2+2 ist. Um alle linearen Teiler von x^2+2 zu finden, reicht es, alle monischen linearen Polynome (x, $x+1$ und $x+2$) als Teiler von x^2+2 zu testen. Durch Ausprobieren sieht man, dass $x+1$ und $x+2$ (und somit auch ihre Vielfachen $2x+2$ und $2x+1$) x^2+2 teilen. Es gilt also $GF(3)[x]^*_{x^2+2} = \{1, 2, x, 2x\}$.

Alternativ kann man für jedes $a(x) \in \mathrm{GF}(3)[x]_{x^2+2}$ den Wert von $\mathrm{ggT}(a(x), x^2+2)$ berechnen und dann diejenigen Polynome auswählen, bei denen er gleich 1 ist.

c) Wir wählen das Element $x \in \mathrm{GF}(3)[x]^*_{x^2+2}$ berechnen das Inverse mit Hilfe eines Gleichungssystems. Dazu bemerken wir, dass das Inverse wiederum ein Polynom von Grad ≤ 1, also setzen wir an

$$x \cdot (ax + b) \equiv_{x^2+2} 1,$$

was äquivalent ist zu

$$x \cdot (ax + b) = t(x)(x^2 + 2) + 1$$

als eine Gleichung über $\mathrm{GF}(3)$ mit Polynom $t(x) \in \mathrm{GF}(3)[x]$. Auf der linken Seite der Gleichung haben wir ein Polynom von Grad ≤ 2, somit muss t ein konstantes Polynom sein, d.h. $t \in \mathrm{GF}(3)$ und wir erhalten

$$x \cdot (ax + b) = t(x^2 + 2) + 1$$

als eine Gleichung über $\mathrm{GF}(3)$. Diese können wir dann per Koeffizientenvergleich in ein Gleichungssystem umwandeln:

$$\begin{aligned} a &= t, \\ b &= 0, \\ 0 &= 2t + 1. \end{aligned}$$

Nun ist also $2t = 2$, also $b = 0$ und $a = t = 1$, also ist $x^{-1} = x$ oder anders gesagt $x^2 \equiv_{x^2+2} -2 \equiv_3 1$.

d) Das Polynom $a(x) = a_0 + a_1 x + \ldots + a_d x^d \in F[x]_{x^n}$ ist genau dann invertierbar, wenn $\mathrm{ggT}(a(x), x^n) = 1$ ist, was genau dann der Fall ist, wenn $a_0 \neq 0$ gilt. Dies sehen wir wie folgt:
$a_0 \neq 0$ ist notwendig, denn ist $a_0 = 0$, so ist x ein gemeinsamer Teiler von $a(x)$ und x^n und somit gilt $\mathrm{ggT}(a(x), x^n) \neq 1$. Da die einzigen Teiler von x^n (bis auf konstante Vielfache) $1, x, \ldots x^n$ sind, ist $a_0 \neq 0$ auch hinreichend, denn dann ist $a(x)$ nicht durch x und auch durch keine Potenz von x teilbar. Aus $a_0 \neq 0$ folgt also $\mathrm{ggT}(a(x), x^n) = 1$.

11.2 Körper

a) Das neutrale Element der Operation $\oplus$ ist $(0, 0)$. Weiter gilt $(1, 0) \otimes (0, 1) = (0, 0)$. Somit hat $F \times F$ Nullteiler. Da aber ein Körper keine Nullteiler hat, kann $F \times F$ kein Köper sein.

b) Wir bemerken, dass 0 keine Lösung der Gleichung $x^{q-1} - 1 = 0$ ist. Wir zeigen, dass jedes Element in $F^* = F - \{0\}$ die Gleichung $x^{q-1} - 1 = 0$ löst. Sei also $a \in F$ mit $a \neq 0$. Dann ist $\langle a \rangle$ eine Untergruppe von F^* der Ordnung $\mathrm{ord}(a)$, also gilt nach Lagrange $\mathrm{ord}(a) | (q - 1)$. Somit existiert ein $k \in \mathbb{Z}$, so dass $(q - 1) = k \cdot \mathrm{ord}(a)$ und damit ist

$$a^{q-1} = a^{k \cdot \mathrm{ord}(a)} = \left(a^{\mathrm{ord}(a)}\right)^k = 1^k = 1,$$

woraus die Behauptung folgt.

11.3 Endliche Körper

a) Da 9 keine Primzahl ist, ist $\mathbb{Z}_9$ *kein* Körper. Der gesuchte Körper K muss also ein Erweiterungskörper sein. Da $9 = 3^2$ eine Primzahlpotenz muss K ein Erweiterungskörper von $\mathrm{GF}(3) = \{0, 1, 2\}$ sein (vgl. Beispiel 5.64 oder Theorem 5.39). *(1 Punkt)*
Mit anderen Worten gilt $K = \mathrm{GF}(3)[x]_{m(x)}$ für ein ein irreduzibles Polynom $m(x)$ in $\mathrm{GF}(3)[x]$ von Grad 2. *(1 Punkt)*
Um K zu konstruieren muss also ein solches $m(x)$ gefunden werden. Mit Durchprobieren finden wir als Kandidaten $m(x) = x^2 + 1$. *(1 Punkt)*
Einsetzen von $0, 1, 2$ zeigt, dass $m(x)$ keine Nullstelle in $\mathrm{GF}(3)$ hat und somit irreduzibel ist (Korollar 5.30). *(1 Punkt)*
Damit ist $K = \mathrm{GF}(3)[x]_{m(x)}$ ein endlicher Körper mit 9 Elementen. *(1 Punkt)*
Die Elemente von F sind also $\{0, 1, 2, x, 2x, x + 1, x + 2, 2x + 1, 2x + 2\}$ (Definition 5.35). *(1 Punkt)*

b) Sei K der Körper aus Aufgabe a). Es gilt $K^* = \mathrm{GF}(3)[x]^*_{x^2+1} = \{1, 2, x, 2x, x+1, x+2, 2x+1, 2x+2\}$. *(1 Punkt)*

Die multiplikative Gruppe K^* und somit auch ein Generator G hat somit Ordnung 8. *(1 Punkt)*

Nach Lagrange gilt für ein $a \in K^*$, dass $\mathrm{ord}(a) \mid 8$. *(1 Punkt)*

Um zu zeigen, dass ein Element $g \in K^*$ ein Generator ist, genügt es also zu zeigen, dass $g^4 \neq 1$. gilt. *(1 Punkt)*

Durch Ausprobieren sehen wir, dass zum Beispiel $g := x + 1$ diese Eigenschaft hat: *(1 Punkt)*

$$(x+1)^4 = (2x+1).$$

c) Es gilt $\mathrm{GF}(2)[x]_{x^2+x+1} = \{0, 1, x, x+1\}$. Wir testen alle vier Elemente, ob sie eine Nullstelle von $p(y)$ sind. Wir verwenden dabei unter anderem, dass in dem betrachteten Körper $x^2 = x + 1$ und $1 + 1 = x + x = 0$ gilt.

$$\begin{aligned}
p(0) &= x \cdot 0^2 + 0 + x + 1 = x + 1 && \neq 0 \\
p(1) &= x \cdot 1^2 + 1 + x + 1 && = 0 \\
p(x) &= x \cdot x^2 + x + x + 1 = x(x+1) + 1 = x^2 + x + 1 && = 0 \\
p(x+1) &= x \cdot (x+1)^2 + (x+1) + x + 1 = x \cdot (x^2 + 1) = x^2 = x + 1 && \neq 0
\end{aligned}$$

(jeweils 0.5 Punkte)

Sämtliche Nullstellen von $p(y)$ sind also 1 und x. *(1 Punkt)*

11.4 Lineare Codes

Sei $\langle \mathbb{F}; +, -, 0, \cdot, 1 \rangle$ der endliche Körper aus der Aufgabenstellung. Dann können wir auf $\mathbb{F}^n$ die komponentenweise Addition $\oplus$ und die komponentenweise Subtraktion $\ominus$ definieren:

$$\begin{aligned}
&\oplus : \mathbb{F}^n \times \mathbb{F}^n \longrightarrow \mathbb{F}^n \\
&\quad \big((a_0, \ldots, a_{n-1}), (b_0, \ldots, b_{n-1})\big) \longmapsto \big(a_0 + b_0, \ldots, a_{n-1} + b_{n-1}\big), \\
&\ominus : \mathbb{F}^n \times \mathbb{F}^n \longrightarrow \mathbb{F}^n \\
&\quad \big((a_0, \ldots, a_{n-1}), (b_0, \ldots, b_{n-1})\big) \longmapsto \big(a_0 + (-b_0), \ldots, a_{n-1} + (-b_{n-1})\big).
\end{aligned}$$

Die Hammingdistanz d_H und das Hamminggewicht w_H sind nun definiert als:

$$\begin{aligned}
&d_H : \mathbb{F}^n \times \mathbb{F}^n \longrightarrow \{0, 1, \ldots, n\} \\
&\quad \big((a_0, \ldots, a_{n-1}), (b_0, \ldots, b_{n-1})\big) \longmapsto |\{i \in \{0, \ldots, n-1\} \mid a_i \neq b_i\}|, \\
&w_H : \mathbb{F}^n \longrightarrow \{0, 1, \ldots, n\} \\
&\quad (a_0, \ldots, a_{n-1}) \longmapsto |\{i \in \{0, \ldots, n-1\} \mid a_i \neq 0\}|.
\end{aligned}$$

Um die Aufgabe zu lösen, zeigen wir zuerst folgende Gleichung:

$$\forall a, b \in \mathbb{F}^n \;\; d_H(a, b) = w_H(a \ominus b). \tag{1}$$

Aufgrund der Definitionen von d_H und w_H haben wir $\forall a \in \mathbb{F}^n\ w_H(a) = d_H(a, 0^n)$. Weiter gilt, dass $\forall a_i, b_i \in \mathbb{F}\ \ a_i = b_i \iff a_i + (-b_i) = 0$. Damit erhalten wir

$$\forall a, b \in \mathbb{F}^n\ \ d_H(a, b) = d_H(a \ominus b, 0^n) = w_H(a \ominus b).$$

Der Code $C \subseteq \mathbb{F}^n$ ist linear, d.h. $\langle C; \oplus, \ominus, 0^n \rangle$ ist eine Gruppe. Die minimale Distanz d und das minimale Hamminggewicht w sind nun definiert als:

$$d = \min_{\substack{a,b \in C \\ a \neq b}} d_H(a, b) \qquad\qquad w = \min_{\substack{a \in C \\ a \neq 0^n}} w_H(a)$$

Damit gibt es also $a, b \in C$ mit $a \neq b$ so dass

$$d = d_H(a, b) \overset{(1)}{=} w_H(a \ominus b) \geq w,$$

wobei die Ungleichung aus $a \ominus b \neq 0^n$ folgt ($a \neq b$). Umgekehrt sei $a \in C - \{0^n\}$ ein Codewort mit minimalem Gewicht. Es gilt $a = a \ominus 0^n$, da $-0 = 0$. Somit folgt

$$w = w_H(a) = w_H(a \ominus 0^n) \overset{(1)}{=} d_H(a, 0^n) \overset{a \neq 0^n}{\geq} d$$

und somit $d = w$.

11.5 Beweissysteme

Es gilt $\tau\big((a, b, c)\big) = 1 \quad :\Leftrightarrow \quad \exists x, y \in \mathbb{N}\ a = g^x \wedge b = g^y \wedge c = g^{xy}$ (vgl. Kapitel 4.6 im Skript). Seien $(a, b, c) \in \mathcal{S}$ und $p \in \mathcal{P}$. Wir definieren ϕ wie folgt:

$$\phi\big((a, b, c), p\big) = 1 \quad :\Leftrightarrow \quad a = g^p\ \wedge\ c = b^p \tag{2}$$

Diese Funktion kann effizient berechnet werden. Wir müssen nun zeigen, dass Π vollständig und korrekt ist.

Vollständigkeit: Sei $(a, b, c) \in \mathcal{S}$ mit $\tau\big((a, b, c)\big) = 1$. Dann gibt es $x, y \in \mathbb{Z}$ mit $a = g^x$, $b = g^y$ und $c = g^{xy}$. Damit gilt auch $c = b^x$. Also ist x ein Beweis für (a, b, c), d.h. $\phi\big((a, b, c), x\big) = 1$.

Korrektheit: Sei $(a, b, c) \in \mathcal{S}$ mit $\tau\big((a, b, c)\big) = 0$. Dann gilt für alle $x, y \in \mathbb{Z}$ mit $a = g^x$ und $b = g^y$, dass $c \neq g^{xy}$. Somit gibt es kein x mit $a = g^x$ und $b^x = c$. Daher gibt es für (a, b, c) keinen Beweis $p \in \mathcal{P}$ mit $\phi\big((a, b, c), p\big) = 1$.

Peggy kann also Vic von ihrer Behauptung überzeugen, indem sie ihm den diskreten Logarithmus von a oder b nennt.