Codierungstheorie (Sommersemester 2014)

Irene Bouw, Michel Börner

Blatt: 09
Punkte: 10

Abgabe zu zweit vor der Vorlesung am Di., **24.06.14** um 10:15 Uhr im Raum E 20.

Aufgabe 20 (Zyklische RS-Codes)

Wir betrachten den zyklischen $RS^{8,2}(\beta)$-Code $\mathcal{C}$ mit $\beta = \gamma$ über $\mathbb{F}_9 := \mathbb{F}_3[x]/(x^2 + x - 1)$, wobei $\gamma \in \mathbb{F}_9$ ein Element mit $\min_{\mathbb{F}_3}(\gamma) = x^2 + x - 1$ ist.

a) Über $\mathbb{F}_3$ zerfällt das Polynom $x^9 - x$ in folgende irreduzible Faktoren (dies muss nicht gezeigt werden):

$$x^9 - x = x(x+1)(x-1)(x^2+1)(x^2+x-1)(x^2-x-1). \qquad (*)$$

Zeige mit $(*)$, dass $\mathrm{ord}(\gamma) = 8$.

b) Wende Algorithmus 3.5.1 auf das Wort $r = (\gamma+1, -\gamma-1, 0, 0, -\gamma+1, \gamma, \gamma-1, -1)$ an. Berechne insbesondere $S(x)$, $\Lambda(x)$ und $R(x)$ sowie das gesendete Codewort c.

Kontrolle: Als Syndrompolynom ergibt sich $S(x) = (-\gamma-1)x^5 - \gamma x^4 + (\gamma+1)x^3 + \gamma x^2 + (-\gamma-1)x - \gamma$, der einzige Fehlerwert ist γ.

Tipp: Verwende Maple und die Befehle auf der Rückseite. Mache dir zunächst klar, was die Befehle genau tun. Es wird diesmal keine von Hand gerechnete Lösung erwartet, der Maple-Code reicht.

Sei nun $f := x - a \in \mathbb{F}_q[x]$ mit einem Parameter $a \in \mathbb{F}_q$ und $S(x), \Lambda(x), R(x)$ aus b) gegeben.

c) Zeige, dass das Paar $(\tilde{\Lambda}, \tilde{R}) := (\Lambda \cdot f, R \cdot f)$ ebenfalls die Gleichung $\tilde{\Lambda} \cdot S \equiv \tilde{R} \pmod{x^6}$ löst.

d) Liefert der Algorithmus mit dem Paar $(\tilde{\Lambda}, \tilde{R})$ aus c) noch die korrekten Fehlerwerte, wenn der Parameter a

i) eine Nullstelle von Λ,
ii) eine Potenz von β, aber keine Nullstelle von Λ,
iii) keine Potenz von β ist?

Begründe jeweils deine Behauptungen.

(1+2,5+0,5+3 = **7 P**)

Aufgabe 21 (Zyklische Codes)

Prüfe jeweils, ob folgende Codes zyklisch sind.

a) Der Code über $\mathbb{F}_2$ gegeben durch die Erzeugermatrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

b) Der RS-Code mit Auswertungsvektor $a = (0, 1, 2, \ldots, p-1)$, d.h. das Bild der Abbildung

$$\varphi : P_k \to \mathbb{F}_q^n, \qquad f \mapsto (f(a_i))_{i=0}^{p-1}.$$

Hinweis: Zeige, dass $\sigma : x^i \mapsto (x+1)^i$ ein Automorphismus auf P_k ist. (1+2 = **3 P**)

Bitte wenden!

Endliche Körper in Maple

Wie man Maple startet, wurde auf Blatt 5 erklärt.

Für Aufgabe 20 b):

Element γ definieren:

```
> p:=x^2+x+2;
> alias(gamma = RootOf(p));
```

Einige der Dinge, die man in Aufgabe 20b) tun muss:

```
> for k from 0 to 8 do
> evala(gamma^k) mod 3;
> end do;
```

```
> r:=gamma+1+(-gamma-1)*x+...;
> for k ...
> evala(eval(r,x=gamma^k)) mod 3;
> end do;
```

```
> s:=0;
> for ...
> s:=s+x^(6-k)*(evala(eval(r,x=gamma^k)) mod 3);
> end do;
```

Immer nützlich:

```
> quo(f,g,x);
> rem(f,g,x);
```

Tipp: Maple vereinfacht sehr wenig. Wiederholtes anwenden von evala() und mod 3 liefert bessere Ergebnisse:

```
> evala(evala(expand(rem(x^6,s,x)))mod 3)mod 3;
```