Übungen zur Vorlesung Diskrete Strukturen

Abt. Reine Mathematik SS 06 – Blatt 1

Abgabetermin: Di., 02.05.2006 um 14:15 Uhr vor Beginn der Vorlesung

---

1. Beweisen Sie: Ist $n \in \mathbb{N}$ mit $n > 4$ keine Primzahl, so gilt $(n-1)! \equiv 0 \mod n$.

2. Berechnen Sie den größten gemeinsamen Teiler und das kleinste gemeinsame Vielfache d von folgenden Zahlen a , b und bestimmen Sie ganze Zahlen α , β mit $d = \alpha \cdot a + \beta \cdot b$.

   (a) $a = 252$, $b = 462$

   (b) $a = 3640$, $b = 7091$

3. Es seien a, m, s, t natürliche Zahlen.

   (a) Die Zahl $a^{st} - 1$ hat die Faktoren $a^t - 1$ und $\sum_{j=0}^{s-1} a^{jt}$.

   (b) Ist eine Zahl $a^m - 1$, $m > 1$, eine Primzahl, so ist m eine Primzahl und es gilt $a = 2$.

   Die Zahlen $M_p := 2^p - 1$, p Primzahl, heißen *Mersennesche Zahlen.*

4. Berechnen Sie das Inverse von 137 modulo 5003 .

Übungen zur Vorlesung Diskrete Strukturen

Abt. Reine Mathematik SS 06 – Blatt 2

Abgabetermin: Di., 09.05.2006 um 14:15 Uhr vor Beginn der Vorlesung

---

1. Berechnen Sie die folgenden Ausdrücke falls sie existieren:
   (a) $\overline{2}^3 \cdot \overline{7}^{-1} + \overline{1000}$ in $\mathbb{Z}/25 \cdot \mathbb{Z}$
   (b) $\overline{5}^{-1} \cdot \overline{10}$ in $\mathbb{Z}/1000001 \cdot \mathbb{Z}$
   (c) $\overline{1111}^{-1}$ in $\mathbb{Z}/13 \cdot \mathbb{Z}$
   (d) A^{-1} von $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ in $M(2 \times 2, \mathbb{Z})$ bzw. in $M(2 \times 2, \mathbb{Z}/9\mathbb{Z})$

2. Lösen Sie das folgende lineare Gleichungssystem über $\mathbb{Z}/\mathbb{Z} \cdot 13$.

$$\begin{pmatrix} 1 & 2 & 1 \\ 1 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}$$

3. Bestimmen Sie die kleinste Zahl $x \in \mathbb{N}$, welche die folgenden Kongruenzen erfüllt

$$x \equiv 20 \mod 23 \ , \ x \equiv 19 \mod 37 \ .$$

4. Zeigen Sie, dass jede Zahl $n \in \mathbb{N}$ mit $n \neq 0$ eine *Binärdarstellung*

$$n = \sum_{i=0}^{l-1} b_i 2^i \text{ mit } b_i \in \{0, 1\} \text{ und } b_{l-1} \neq 0$$

   besitzt.
   (a) Berechnen Sie die Binärdarstellung für $n = 1003257$ und mit Satz 1.2.11 die Potenz

$$17^n \mod 5003 \ .$$

   (b) Berechnen Sie mit Satz 1.3.6 die Potenz $17^n \mod 5003$.

Übungen zur Vorlesung Diskrete Strukturen

Abt. Reine Mathematik SS 06 – Blatt 3

Abgabetermin: Di., 16.05.2006 um 14:15 Uhr vor Beginn der Vorlesung

---

1. Betrachten Sie den Ring der ganzen *Gaußschen Zahlen* $\mathbb{Z}[\imath] = \mathbb{Z} \oplus \mathbb{Z} \cdot \imath \subseteq \mathbb{C}$.
   Zeigen Sie:
   (a) Mit der Funktion $\delta(x) := |x|^2 = x\,\overline{x}$ für $x \in \mathbb{Z}[\imath]$ ist $\mathbb{Z}[\imath]$ ein euklidischer Ring.
   (Hinweis: Sie können den Beweis geometrisch führen; veranschaulichen Sie sich die ganzen Gaußschen Zahlen als Punkte eines Gitters in der komplexen Ebene.)
   (b) 2 und 5 sind nicht irreduzibel in $\mathbb{Z}[\imath]$.
   (c) Ein $x \in \mathbb{Z}[\imath]$ ist genau dann eine Einheit von $\mathbb{Z}[\imath]$, wenn $\delta(x) = 1$ gilt.
   (d) Bestimmen Sie die Einheiten von $\mathbb{Z}[\imath]$.
   (e) 3 ist Primelement in $\mathbb{Z}[\imath]$.

2. Finden Sie den größten gemeinsamen Teiler von $11 + 7\imath$ und $18 - \imath$ in $\mathbb{Z}[\imath]$.

3. (a) Beweisen Sie, dass die Polynome $f = X^2 + X + 1$ und $g = X^3 + X^2 + 1$ irreduzibel in $\mathbb{F}_2[X]$ sind.
   (b) Beweisen Sie, dass die Restklassenringe $\mathbb{F}_2[X]/(f)$ und $\mathbb{F}_2[X]/(g)$ Körper sind.
   (c) Fertigen Sie Verknüpfungstabellen an für $+$ und $\cdot$ in $\mathbb{F}_2[X]/(g)$.
   (d) Finden Sie eine Nullstelle von $T^3 + T + 1$ in dem Körper $\mathbb{F}_2[X]/(g)$.

4. (a) Es seien p eine Primzahl und $f \in \mathbb{Z}[X]$. Weiterhin sei $x \in \mathbb{Z}/p\mathbb{Z}$ eine Nullstelle von $f \mod p$ mit $f(x) \equiv 0 \mod p$ und $f'(x) \not\equiv 0 \mod p$.
   Beweisen Sie: Für alle $k \in \mathbb{N}$ existiert genau ein $x_k \in \mathbb{Z}/p^k\mathbb{Z}$ mit

   $$f(x_k) \equiv 0 \mod p^k \text{ und } x_k \equiv x \mod p.$$

   Hinweis: Konstruieren Sie x_{k+1} aus x_k mit dem *Newtonverfahren*:

   $$x_{k+1} = x_k + a \cdot p^k,\ f(x_{k+1}) = f(x_k) + a \cdot p^k \cdot f'(x_k) \mod p^{k+1}.$$

   (b) Bestimmen Sie Lösungen der Kongruenzen
   $x^3 \equiv 5 \mod 13^{64}$, $x^3 \equiv 7 \mod 10^{1000}$.

Übungen zur Vorlesung Diskrete Strukturen

Abt. Reine Mathematik SS 06 – Blatt 4

Abgabetermin: Di., 23.05.2006 um 14:15 Uhr vor Beginn der Vorlesung

---

1. Man schreibe eine Funktion `cyclen`, welche als Parameter die natürlichen Zahlen `x0, N, a` $\in \mathbb{N}$ hat und als Ausgabe die Periodenlänge der rekursiv definierten Folge

$$x_0 := \mathtt{x0} \mod \mathtt{N}, \quad \mathtt{x_{i+1}} := (\mathtt{x_i^2} + \mathtt{a}) \mod \mathtt{N}.$$

   Man bestimme nun die Periodenlänge für $\mathtt{a} = 2$, $\mathtt{N} = 68111$ und die Startwerte $\mathtt{x0} = 975, 976, 977, 978$.

2. Man erstelle eine Tabelle zur Laufzeit des Pollardschen Rho-Verfahren für die Auffindung des kleinsten Primfaktors p von $N = p \cdot q \cdot r$ mit Hilfe der ARIBAS- Funktion `poll_rho(N, Anz)`. Hierbei gilt $p \approx 10^k$ für $k = 7, \cdots, 14$ und $q, r \approx 10^{15}$ und man wählt $\mathtt{Anz} \approx \sqrt{\mathtt{p}}$. Zum Stoppen der Zeit gibt es die ARIBAS-Funktion `timer()`.

3. Es sei p eine ungerade Primzahl, $a \in \mathbb{Z}/p\mathbb{Z}$ und $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ definiert durch

$$f(x) = x^2 \mod p.$$

   Ein Zyklus von f der Länge $n \in \mathbb{N}$ ist eine Folge $x_0, x_1, \ldots, x_{n-1}$ in $\mathbb{Z}/p\mathbb{Z}$ mit $f(x_i) = x_{i+1}$ für $0 < i < n-1$ und $f(x_{n-1}) = x_0$ und $x_i \neq x_j$ für $i \neq j$.

   (a) Man bestimme die Anzahl der Zyklen der Länge 1 bzw. 2 von f.
   Hinweis: Es gilt $(X^2 + b)^2 + b - X = (X^2 + X + b + 1)(X^2 - X + b)$.

   (b) Man beweise, daß ein Zyklus höchstens die Länge $(p-3)/2$ haben kann.

   (c) Es sei p eine Primzahl

   (d) Es sei nun p von der Gestalt $p = 2q + 1$ mit einer Primzahl q. Dann heißt q eine *Sophie-Germain-Primzahl*. Man beweise empirisch:

   Ist 2 eine Primitivwurzel modulo q, so gibt es einen Zyklus C mit der Länge $(p-3)/2$. Für jedes x mit $x \neq 0, \pm 1$ liegt x oder $f(x)$ auf C.

4. Sei $f : M \to M$ eine Selbstabbildung einer endlichen Menge M. Der zugeordnete gerichtete Graph Γ_f besteht aus den Eckpunkten $x \in M$ und den gerichteten Kanten, die von x nach $f(x)$ führen.
   Man betrachte das Beispiel $M = \mathbb{Z}/N\mathbb{Z}$ und $f(x) = (x^2 + a) \bmod N$.

   (a) Sei N eine ungerade Primzahl. Man beweise:

      i. In jeden Punkt des Graphen münden höchstens zwei verschiedene Kanten.

      ii. Es gibt genau $\frac{N-1}{2}$ verschiedene Punkte des Graphen, in die keine Kante mündet.

      iii. Es gibt einen Punkt, in den genau eine Kante mündet.

   (b) Man zeichne für $a = 2$ und $N = 7, 15, 39$ jeweils den zugehörigen Graphen Γ_f in der Ebene.

Übungen zur Vorlesung Diskrete Strukturen

Abt. Reine Mathematik SS 06 – Blatt 5

Abgabetermin: Di., 30.05.2006 um 14:15 Uhr vor Beginn der Vorlesung

---

1. Ist $f(T) = f_0 + f_1T^1 + \ldots + f_nT^n \in k[T]$ ein Polynom über einem Körper k, so definiert man die formale Ableitung durch $f'(T) := f_1 + 2f_2T^1 + \ldots + nf_nT^{n-1} \in k[T]$. Beweisen Sie folgende Rechenregeln:

   (a) $(f+g)' = f' + g'$

   (b) $(f \cdot g)' = f \cdot g' + f' \cdot g$

   (c) $(f^m)' = m \cdot f^{m-1} \cdot f'$

   (d) Ist $f(T) = f_1(T)^{e_1} \cdot f_2(T)^{e_2} \cdot \ldots \cdot f_m(T)^{e_m}$ die Zerlegung von f in Primpotenzfaktoren, so gilt
   $$\frac{f(T)}{\mathrm{ggT}(f(T), f'(T))} = f_1(T) \cdot \ldots \cdot f_m(T)$$

   (e) Zeigen Sie: $f(T)$ ist genau dann quadratfrei, wenn $f(T)$ und seine formale Ableitung relativ prim sind.

2. Zerlegen Sie das Polynom $T^{16} - T \in \mathbb{F}_2[T]$ in irreduzible normierte Polynome.

3. Betrachten Sie das Polynom
   $$\Phi(T) := T^6 + T^3 + 1 \in \mathbb{F}_2[T] \ .$$
   Zeigen Sie, dass Φ irreduzibel ist. Betrachten Sie nun den Körper
   $$\mathbb{F}_{64} := \mathbb{F}_2[T]/(\Phi) \text{ und } \alpha := \overline{T} \in \mathbb{F}_{64} \ .$$
   Berechnen Sie nun:

   (a) $(1+\alpha)^{-1} \in \mathbb{F}_{64}$

   (b) $\mathrm{Tr}_{\mathbb{F}_2}^{\mathbb{F}_{64}}(1+\alpha) \in \mathbb{F}_2$

   (c) $\mathrm{N}_{\mathbb{F}_2}^{\mathbb{F}_{64}}(1+\alpha) \in \mathbb{F}_2$

4. Betrachten Sie das Polynom
   $$\Psi(T) := T^3 + T^2 + 1 \in \mathbb{F}_2[T] \ .$$
   Zeigen Sie, dass Ψ irreduzibel ist. Betrachten Sie nun den Körper
   $$\mathbb{F}_8 := \mathbb{F}_2[T]/(\Psi) \ .$$
   Sei nun $\alpha \in \mathbb{F}_{64}$ wie in Aufgabe 3.

   (a) Man kann $\mathbb{F}_8$ als Teilkörper von $\mathbb{F}_{64}$ auffassen. Wie?

   (b) Berechnen Sie $\mathrm{Tr}_{\mathbb{F}_8}^{\mathbb{F}_{64}}(1+\alpha) \in \mathbb{F}_8$.

   (c) Berechnen Sie $\mathrm{N}_{\mathbb{F}_8}^{\mathbb{F}_{64}}(1+\alpha) \in \mathbb{F}_8$.

Übungen zur Vorlesung Diskrete Strukturen

Abt. Reine Mathematik SS 06 – Blatt 6

Abgabetermin: Di., 6.06.2006 um 14:15 Uhr vor Beginn der Vorlesung

---

1. Es sei $K := \mathbb{F}_{q^m}$ und $F := \mathbb{F}_q$ sowie $\alpha \in K$. Zeigen Sie:
   (a) Es ist $\mathrm{Tr}_F^K(\alpha) = 0$ genau dann, wenn ein $\beta \in K$ mit $\alpha = \beta - \beta^q$ existiert.
   (b) Es ist $\mathrm{N}_F^K(\alpha) = 1$ genau dann, wenn ein $\beta \in K^\times$ mit $\alpha = \beta^{1-q}$ existiert.
2. Es sei $\mathbb{F}_{32} := \mathbb{F}_2/(T^5 + T^4 + T^2 + T + 1)$ sowie $\alpha := \overline{T}$.
   Konstruieren Sie die duale Basis zu $(\alpha^0, \alpha^1, \alpha^2, \alpha^3, \alpha^4)$ bzgl. $\mathrm{Tr}_{\mathbb{F}_2}^{\mathbb{F}_{32}}$.
3. Es sei α wie in Aufgabe 2.
   (a) Berechnen Sie die Koordinaten von $x := 1 + \alpha^3 + \alpha^4$ und $y := \alpha^2 + \alpha^3$ bzgl. der dualen Basis zu $(\alpha^0, \alpha^1, \alpha^2, \alpha^3, \alpha^4)$ bzgl. $\mathrm{Tr}_{\mathbb{F}_2}^{\mathbb{F}_{32}}$.
   (b) Berechnen Sie das Produkt $x \cdot y$ unter Benutzung von Notiz 2.3.2.
   (c) Wie sehen obige Lösungen aus, wenn man die Darstellung $\mathbb{F}_{32} := \mathbb{F}_2/(T^5+T^2+1)$ benutzt?
4. Berechnen Sie die duale Basis zu $(x_0, x_1, x_2, x_3, x_4)$ im Fall

   $$x_0 := 1 + \alpha \; ; \; x_1 := \alpha + \alpha^2 \; ; x_2 := 1 + \alpha + \alpha^2 \; ; \; x_3 := \alpha + a^3 \; ; \; x_4 := a^2 + \alpha^4 \; ,$$

   wobei α wie in Aufgabe 2 gewählt ist.

Übungen zur Vorlesung Diskrete Strukturen

Abt. Reine Mathematik SS 06 – Blatt 7

Abgabetermin: Di., 13.06.2006 um 14:15 Uhr vor Beginn der Vorlesung

---

1. Entwerfen Sie einen Schieberegister-Schaltkreis für $\mathbb{F}_{16}$, der eine Ausgangsbasis und die dazu duale Basis benutzt.

2. Entwerfen Sie einen Schieberegister-Schaltkreis für $\mathbb{F}_8$. Sie können z.B. die Darstellung

$$\mathbb{F}_8 = \mathbb{F}_2[T]/(T^3 + T^+1) \text{ und } \alpha := \overline{T}$$

   wählen und ausschließlich mit den dualen Basis zu $(\alpha^0, \alpha^1, \alpha^2)$ rechnen.

3. Schreiben Sie ein Programm, bestehend aus Booleschen Bausteinen, zur Realisierung des Schaltplans (Ende von §2.4) von $\mathbb{F}_{64}$, das eine schwach duale Basis benutzt.

4. Berechnen Sie den diskreten Logarithmus $x := \mathrm{dlog}(5003, 2, 13)$, also diejenige Zahl $x \in \{1, \ldots, 5002\}$ mit $2^x = 13$.

Übungen zur Vorlesung Diskrete Strukturen

Abt. Reine Mathematik SS 06 – Blatt 8

Abgabetermin: Di., 20.06.2006 um 14:15 Uhr vor Beginn der Vorlesung

---

1. Sei $f \in \mathbb{F}_p[T]$ ein quadratfreies Polynom und sei

$$f(T) = \prod_{1 \le i \le r} f_i(T)$$

dessen Zerlegung in irreduzible Faktoren. Seien ferner $s_i \in \mathbb{F}_p$ für $1 \le i \le r$ beliebig. Zeigen Sie, dass ein eindeutig bestimmtes Polynom $g(T) \in \mathbb{F}_p[T]$ mit $\deg(g) < \deg(f)$ existiert, für das gilt:

(i) $g(T) \equiv s_i \mod f_i$ und

(ii) $g^p(T) \equiv g(T) \mod f$.

2. Seien das Polynom f sowie die Polynome f_i wie in Aufgabe 1 gegeben. Zeigen Sie: Gilt für ein Polynom $g(T) \in \mathbb{F}_p[T]$ mit $\deg(g) < \deg(f)$ die Beziehung

$$g^p(T) \equiv g(T) \mod f,$$

so existiert für jedes i mit $1 \le i \le r$ ein $s_i \in \mathbb{F}_p$ für das gilt

$$f_i(T) \mid (g(T) - s_i).$$

Aus den Aufgaben 1 und 2 lässt sich der Berlekamp-Algorithmus zur Faktorisierung von Polynomen über endlichen Körpern ableiten. Ist beispielsweise $g(T)$ Lösung eines solchen Kongruenzsystems mit $s_1 \neq s_2$, so ist $\mathrm{ggT}(f(T), g(T) - s_1)$ durch f_1 teilbar, jedoch nicht durch f_2 . Folglich haben wir einen nicht-trivialen Teiler von f gefunden. Nach Obigem wissen wir, dass wir nicht die f_i kennen müssen, um ein geeignetes Polynom g zu finden, wir müssen lediglich die Kongruenz $g^p(T) \equiv g(T) \mod f$ lösen.

3. Sei $\mathbb{F}_4$ gegeben durch $\mathbb{F}_2[T]/(T^2+T+1)$. Bestimmen Sie ein Polynom $g(T)$ mit der Eigenschaft $g^4(T) \equiv g(T) \mod (T^5 + (1+\alpha)T^3 + T^2 + \alpha)$ wobei mit α wie üblich die Restklasse von T in $\mathbb{F}_2[T]/(T^2+T+1)$ bezeichnet sei.

4. Faktorisieren Sie das Polynom $T^5 + (1+\alpha)T^3 + T^2 + \alpha \in \mathbb{F}_4[T]$ mit dem Berlekamp-Algorithmus.

Der Berlekamp-Algorithmus
Gegeben sei ein quadratfreies Polynom $f \in \mathbb{F}_p[T]$ vom Grad n. Der Algorithmus berechnet die Faktorisierung von f in irreduzible Polynome.

1. (Berechnen der Matrix Q)
   Wir berechnen zunächst für $0 \leq k < n$ die Elemente $q_{i,k} \in \mathbb{F}_p$, sodass gilt
   $$T^{pk} \equiv \sum_{0 \leq i < n} q_{i,k} T^i \mod f(T).$$

2. (Berechnen des Kerns)
   Sei $v_1, \ldots, v_r$ eine Basis von $\mathrm{Ker}\,(Q - E)$, wobei E die Einheitsmatrix bezeichne. Dann ist r die Anzahl der irreduziblen Faktoren. Ferner sei $v_1 = (1, 0, \ldots, 0)^t$. Wir setzen $E = \{A\}$, $k = 1$ und $j = 1$. (E ist die Menge der Polynome, deren Produkt f ergibt, k ist $|E|$ und j ist der Index des Vektors, den wir benutzen.)

3. (Ende?)
   Ist $k = r$, so können wir E ausgeben und den Algorithmus beenden. Ansonsten setzen wir $j = j + 1$ und es bezeichne
   $$g(T) = \sum_{0 \leq i < n} v_{j_i} T^i.$$

4. (Zerlegung)
   Für jedes Element $b \in E$ mit $\deg(b) > 1$ berechnen wir für jedes $s \in \mathbb{F}$ den größten gemeinsamen Teiler $\mathrm{ggT}(b(T), g(T) - s)$. Sei F die Menge der ggT, deren Grad größer gleich 1 ist. Nun setzen wir $E = (E \setminus \{b\}) \cup F$ und $k = k - 1 + |F|$. Ist $k = r$, so geben wir E aus und beenden den Algorithmus. Ansonsten gehen wir zu Schritt 3.

Übungen zur Vorlesung Diskrete Strukturen

Abt. Reine Mathematik SS 06 – Blatt 9

Abgabetermin: Di., 27.06.2006 um 14:15 Uhr vor Beginn der Vorlesung

---

1. Gegeben sei der Hamming-Code über $\mathbb{F}_2$ mit der Erzeugermatrix

$$G = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right)$$

   und der Kontrollmatrix

$$H = \left(\begin{array}{cccc|ccc} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right).$$

   (a) Geben Sie alle Codewörter an.

   (b) Bestimmen Sie den Minimalabstand.

   (c) Berechnen Sie alle Syndrome, die von Fehlervektoren e mit Gewicht $w(e) = 1$ induziert werden.

   (d) Bestimmen Sie die Fehlerkorrektur von $(1, 0, 1, 1, 1, 0, 1)$.

2. Betrachten Sie den Code $\mathcal{C} = \{\, c \in \mathbb{F}_2^4 \mid w(c) \equiv 0 \bmod 2 \,\}$.

   (a) Finden Sie alle Fehler, die mit der maximum-likelihood Methode eindeutig korrigiert werden können.

   (b) Bestimmen Sie die Wahrscheinlichkeit für eine fehlerhafte Übertragung über einen BSC. Ein Symbol werde hierbei mit der Wahrscheinlichkeit $p = 0.1$ gestört.

3. Betrachten Sie den Code $\mathcal{C} = \{\, (a_1, a_1, a_2, a_2, a_3, a_3) \,;\, a_i \in \mathbb{F}_2 \,\} \subset \mathbb{F}_2^6$. Berechnen Sie die Wahrscheinlichkeit für die Fehlererkennung bei Übertragung über einen BSC mit Fehlerwahrscheinlichkeit $p = 0.1$.

4. Sei $\mathcal{C}$ ein binärer Code mit Erzeugermatrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \in M(4 \times 7, \mathbb{F}_2).$$

   (a) Bestimmen Sie eine maximum-likelihood Decodierungsregel zu $\mathcal{C}$, indem Sie die zugehörige Syndrom/Nebenklassenführer-Tabelle aufstellen.

   (b) Decodieren Sie hiermit die Wörter $(1, 1, 0, 1, 0, 1, 1)$, $(0, 1, 1, 0, 1, 1, 1)$ und $(0, 1, 1, 1, 0, 0, 0)$.

Übungen zur Vorlesung Diskrete Strukturen

Abt. Reine Mathematik SS 06 – Blatt 10

Abgabetermin: Di., 4.7.2006 um 14:15 Uhr vor Beginn der Vorlesung

---

1. Es sei $g := (X+1)(X^3+X^2+1) \in \mathbb{F}_2[X]$, und es sei $C_g \subset \mathbb{F}_2[X]/(X^7-1)$ der zyklische Code mit Erzeugerpolynom g .
   (a) Bestimmen Sie $h \in \mathbb{F}_2[X]$ mit $X^7 - 1 = g \cdot h$.
   (b) Bestimmen Sie eine Erzeugermatrix und eine Kontrollmatrix für C_g .
   (c) Bestimmen Sie Dimension, Informationsrate und Minimalabstand von C_g .
   (d) Bestimmen Sie zu $(1,1,0)$ ein Codewort $c = (1,1,0,c_4,c_5,c_6,c_7) \in C_g$.
   (e) Geben Sie alle möglichen Decodierungen von $u = (1,1,1,1,0,0,1)$ und $v = (1,0,1,0,1,0,1)$ an unter der Annahme, dass höchstens zwei Übertragungsfehler aufgetreten sind.

2. Es sei $g := (X^2+1)(X^2+X+2) \in \mathbb{F}_3[X]$, und es sei $C_g \subset \mathbb{F}_3[X]/(X^8-1)$ der zyklische Code mit Erzeugerpolynom g .
   (a) Bestimmen Sie $h \in \mathbb{F}_3[X]$, so daß $X^8 - 1 = g \cdot h$.
   (b) Bestimmen Sie eine Erzeugermatrix und eine Kontrollmatrix für C_g .
   (c) Bestimmen Sie Dimension, Informationsrate und Minimalabstand von C_g .
   (d) Codieren Sie das Wort $(1,0,2,1) \in \mathbb{F}_3^4$ zu einem Codewort $(1,0,2,1,c_4,c_5,c_6,c_7) \in C_g$.

3. Es sei $g := (X^2+1)(X^2+X+2)(X+1) \in \mathbb{F}_3[X]$, und es sei $C_g \subset \mathbb{F}_3[X]/(X^8-1)$ der zyklische Code mit Erzugerpolynom g .
   (a) Bestimmen Sie $h \in \mathbb{F}_3[X]$ mit $X^8 - 1 = g \cdot h$.
   (b) Bestimmen Sie eine Erzeugermatrix und eine Kontrollmatrix für C_g .
   (c) Bestimmen Sie Dimension, Informationsrate und Minimalabstand von C_g .
   (d) Codieren Sie das Wort $(1,1,2) \in \mathbb{F}_3^3$ zu einem Codewort $(1,1,2,c_3,c_4,c_5,c_6,c_7) \in C_g$.
   (e) Decodieren Sie $u := (2,1,2,0,0,0,1,1) \in \mathbb{F}_3^8$ zu einem Codewort mit minimalem Abstand zu u .

Übungen zur Vorlesung Diskrete Strukturen

Abt. Reine Mathematik SS 06 – Blatt 11

Abgabetermin: Di., 11.07.2006 um 14:15 Uhr vor Beginn der Vorlesung

---

1. Es seien $\mathcal{C}_1, \mathcal{C}_2$ zwei nicht notwendig lineare Block-Codes über $\mathbb{F}_q$ der Länge n. Dann sei $(\,\mathcal{C}_1 \mid \mathcal{C}_2\,) := \{\,(u, u+v)\,;\; u \in \mathcal{C}_1\,,\; v \in \mathcal{C}_2\,\} \subset \mathbb{F}_q^{2n}$. Man beachte, dass diese Konstruktion nicht symmetrisch in $\mathcal{C}_1, \mathcal{C}_2$ ist. Beweisen Sie:

   Es seien $\mathcal{C}_1, \mathcal{C}_2 \subset \mathbb{F}_q^n$ und $\mathcal{C} = (\,\mathcal{C}_1 \mid \mathcal{C}_2\,)$. Dann gilt:

   (i) $\mathcal{C}$ hat Blocklänge $2n$ und es gilt $\operatorname{card}(\mathcal{C}) = \operatorname{card}(\mathcal{C}_1) \cdot \operatorname{card}(\mathcal{C}_2)$

   (ii) Ist d_i die minimale Hamming-Distanz von Code-Wörtern aus $\mathcal{C}_i$, so gilt für den Minimalabstand d von $\mathcal{C}$ nun $d = \operatorname{Min}\{2d_1, d_2\}$.

   Sind $\mathcal{C}_1, \mathcal{C}_2$ linear, und ist $\mathcal{C}_i$ ein $[n, k_i]$-Code, so gilt

   (iii) $\mathcal{C}$ ist ein $[2n, k_1+k_2]$-Code mit Minimal-Norm $d = \operatorname{Min}\{2d_1, d_2\}$.

   (iv) Ist G_i Erzeugermatrix von $\mathcal{C}_i$, so ist $\begin{pmatrix} G_1 & G_1 \\ 0 & G_2 \end{pmatrix}$ *Erzeugermatrix von* $\mathcal{C}$.

   (v) Ist q eine Potenz von 2, so ist der duale Code $\mathcal{C}^\perp$ äquivalent zu $(\mathcal{C}_1^\perp \,|\, \mathcal{C}_2^\perp)$.

2. Der binäre *Reed-Muller-Code* $\mathcal{R}(r, m)$ mit Ordnung r und Länge $n = 2^m$ ist definiert durch

   $$\mathcal{R}(-1, m) = 0$$
   $$\mathcal{R}(m, m) = \mathbb{F}_2^n\,, \qquad \text{also } \mathcal{R}(0,0) = \mathbb{F}_2^1 \text{ wegen } 1 = 2^0$$
   $$\mathcal{R}(r, m) = (\,\mathcal{R}(r, m-1) \mid \mathcal{R}(r-1, m-1)\,) \quad \text{für alle } 0 \le r < m\,.$$

   Zeigen Sie:

   (a) $\mathcal{R}(r, m)$ ist ein binärer Block-Code mit folgenden Daten

Länge	$n = 2^m$
Dimension	$k = \binom{m}{0} + \binom{m}{1} + \ldots + \binom{m}{r}$
Minimalabstand	$d = 2^{m-r}$ für $r \ge 0$.

   (b) $\mathcal{R}(r, m)^\perp$ ist äquivalent zu $\mathcal{R}(m-1-r, m)$.

3. Sei $\mathcal{C}$ der binäre zyklische $[7, 3]$-Code, der von dem Polynom $g = T^4 + T^3 + T^2 + 1 \in \mathbb{F}_2$ erzeugt wird.

   (a) Geben Sie eine Erzeugermatrix von $\mathcal{C}$ an.

   (b) Bestimmen Sie das Kontrollpolynom $h(T)$ von $\mathcal{C}$.

   (c) Berechnen Sie die Idempotente von $\mathcal{C}$.

4. (a) Konstruieren Sie einen binären BCH-Code $\mathcal{C}$ der Länge 31 mit designiertem Abstand 7. Welche Dimension lässt sich erreichen?

   (b) Zeigen Sie, dass das Polynom $g(T) = (T^4 + T + 1)(T^4 + T^3 + T^2 + T + 1)$ ein Erzeugerpolynom des $[15, 7]$-BCH-Codes ist.

Übungen zur Vorlesung Diskrete Strukturen

Abt. Reine Mathematik SS 06 – Blatt 12

Abgabetermin: Di., 18.07.2006 um 14:15 Uhr vor Beginn der Vorlesung

---

1. Sei $\mathbb{F}_8$ gegeben durch $\mathbb{F}_8 = \mathbb{F}_2[T]/(T^3+T+1)$ und bezeichne $\alpha = \bar{T}$. Ferner sei $\mathcal{C}$ der Reed-Solomon-Code über $\mathbb{F}_8$ mit Erzeugerpolynom

$$g(T) = (1+T)(\alpha+T)(\alpha^2+T)(\alpha^3+T).$$

   (a) Geben Sie eine Erzeugermatrix für $\mathcal{C}$ an.

   (b) Bestimmen Sie die Dimension und den Minimalabstand des Codes.

   (c) Liegt ein MDS-Code vor? Begründen Sie Ihre Antwort!

   (d) Bestimmen Sie ein Codewort $\underline{c} = (1, 0, \alpha^2, c_3, \ldots, c_n) \in \mathcal{C}$.

2. Konstruieren Sie einen $[4,3]$-MDS-Code über $\mathbb{F}_5$. Geben Sie dazu das Erzeugerpolynom, die Erzeugermatirx sowie das Kontrollpolynom an.

3. (a) Konstruieren Sie einen Reed-Solomon-Code mit den Parametern $[32, 28, 5]$ über $\mathbb{F}_{2^8}$.

   (b) Wie groß ist die Fehlerwahrscheinlichkeit dieses Codes, wenn bei der Übertragung über einen BSC ein Byte mit Wahrscheinlichkeit $p = 0.03$ gestört wird?

   (c) Wie hoch darf die Fehlerwahrscheinlichkeit eines BSC sein, damit die Fehlerwahrscheinlichkeit der Byte-Übertragung kleiner als 0.03 ist?

4. Betrachten Sie erneut den Reed-Solomon-Code mit den Parametern $[32, 28, 5]$ über $\mathbb{F}_{2^8}$. Um die Fehlerwahrscheinlichkeit bei der Übertragung über einen BSC weiter zu senken, zerlege man nun jedes zu übertagene Byte in zwei Blöcke zu je 4 Bit. Jeder dieser Blöcke werde nun mit dem $[7,4,3]$-Hamming-Code übertragen.

   (a) Bestimmen Sie die Fehlerwahrscheinlichkeit des Hamming-Codes für $p = 0.01$ und $p = 0.02$.

   (b) Wie groß darf p sein, damit die Byte-Fehlerwahrscheinlichkeit des Haming-Codes kleiner als 0.03 ist?

   (c) Berechnen Sie die Wahrscheinlichkeit für eine fehlerhafte Übertragung bei Benutzung des $[32, 28, 5]$-Reed-Solomon-Codes mit vorgeschaltetem $[7, 4, 3]$-Hamming-Code, wenn der verwendete BSC ein Zeichen mit Wahrscheinlichkeit $p = 0.01$ bzw. $p = 0.02$ verfälscht.

   (d) Geben Sie die Informationsrate an.

Übungen zur Vorlesung Diskrete Strukturen

Abt. Reine Mathematik SS 06 – Blatt 13

Abgabetermin: Di., 25.07.2006 um 14:15 Uhr vor Beginn der Vorlesung

---

1. Schreiben Sie eine Funktion, die zu gegebenen Polynomen $a_0, a_1 \in \mathbb{F}_{q^m}[T]$ mit $\deg a_0 \geq \deg a_1$ zwei Polynome $f, g \in \mathbb{F}_{q^m}[T]$ bestimmt, sodass

$$\mathrm{ggT}(a_0, a_1) = f \cdot a_0 + g \cdot a_1$$

gilt. Benutzen Sie dazu den erweiterten euklidischen Algorithmus.

2. Sei α eine primitive Einheitswurzel in $\mathbb{F}_{q^m}$ und sei $\mathcal{C}$ der Code über $\mathbb{F}_{q^m}$, der von dem Polynom $g(T) = \prod_{i=1}^{2t}(T - \alpha^i)$ erzeugt wird.

   (a) Schreiben Sie eine Funktion, die zum empfangenen Word $(R_0, \ldots, R_{n-1})$ das zugehörige Polynom $R(T) = \sum_{i=0}^{n-1} R_i T^i$ bestimmt und anschließend das Polynom

$$S(T) = \sum_{i=0}^{2t-1} R(\alpha^{i+1}) T^i$$

   zurückgibt.

   (b) Schreiben Sie eine Funktion, die zu gegebenem Polynom $S(T)$ und Parameter t die Polynome

$$\omega(T) = \sum_{i=0}^{t-1} \omega_i T^i \text{ und } \sigma(T) = \sum_{i=0}^{t} \sigma_i T^i \in \mathbb{F}_{q^m}[T]$$

   berechnet, sodass gilt

$$\omega(T) \equiv S(T)\sigma(T) \mod T^{2t}.$$

   Benutzen Sie dazu wie in der Vorlesung beschrieben den erweiterten euklidischen Algorithmus. Erweitern Sie Ihre in Aufgabe 1 erstellte Funktion entsprechend.

   (c) Implementieren Sie mit Hilfe obiger Funktionen eine Funktion, die ein empfangenes Wort $(R_0, \ldots, R_{n-1})$, welches nicht mehr als t Fehler enthält, in ein Codewort $(C_0, \ldots, C_{n-1})$ decodiert. Enthält das empfangene Wort zu viele Fehler, so soll eine Fehlermeldung ausgegeben werden.

3. Schreiben Sie eine Funktion, die einen zufälligen Fehler von vorgegebenem Gewicht t erzeugt. Die Funktion soll ein Polynom

$$E(T) = \sum_{i=0}^{q^m-2} E_i T^i \in \mathbb{F}_{q^m}[T]$$

zurückgeben, bei dem genau t Koeffizienten ungleich 0 sind.

4. Sei $\mathbb{F}_{16}$ gegeben als $\mathbb{F}_{16} = \mathbb{F}_2[T]/(T^4 + T + 1)$.

   (a) Konstruieren Sie einen primitiven BCH-Code im engeren Sinne über $\mathbb{F}_{16}$, mit dem man 3 Fehler korrigieren kann.

   (b) Testen Sie die oben implementierten Funktionen an diesem Beispiel.