Codierungstheorie

Reinhold Hübl

Woche 8 - Winter 2022

Polynome

Ist $f(X) \in \mathbb{F}_q[X]$ ein Polynom, so können wir für die Unbekannte X ein Element $b \in \mathbb{F}_q$ einsetzen und erhalten ein Element $f(b) \in \mathbb{F}_q$.

Beispiel

Ist $f(X) = 3 + 2X + 4X^4 \in \mathbb{F}_7[X]$, so ist

$$f(2) = 3 + 2 \cdot 2 + 4 \cdot 2^4 = 3 + 4 + 1 = 1$$

Beispiel

Ist $\mathbb{F}_4$ der Körper mit 4 Elementen und definierender Relation $\alpha^2 = \alpha + 1$, und ist $f(X) = 1 + \alpha \cdot X^2 + (\alpha + 1) \cdot X^3 \in \mathbb{F}_4[X]$, so ist

$$f(\alpha) = 1 + \alpha \cdot \alpha^2 + (\alpha + 1) \cdot \alpha^3 = \alpha + 1$$

Definition

Ein $b \in \mathbb{F}_q$ heißt **Nullstelle** von $f(X) \in \mathbb{F}_q[X]$, wenn $f(b) = 0$.

Nullstellen

Übung

Bestimmen Sie alle Nullstellen des Polynoms $f(X) = X^6 + 6 \in \mathbb{F}_7[X]$.

Nullstellen

Ist $f(X) \in \mathbb{F}_q[X]$ ein Polynom vom Grad k, und ist $b \in \mathbb{F}_q$ eine Nullstelle von $f(X)$, so geht die Polynomdivision von $f(X)$ durch $X - b$ in $\mathbb{F}_q[X]$ ohne Rest auf.
Genauer gilt sogar

$$f(X) = g(X) \cdot (X - b)$$

wobei $g(X)$ ein Polynom vom Grad $k - 1$ ist.

Beispiel

Wir betrachten $\mathbb{F}_4$ mit der Relation $\alpha^2 = \alpha + 1$. Dann ist α eine Nullstelle von $f(X) = X^3 + 1$ und

$$X^3 + 1 = (X^2 + \alpha X + (\alpha + 1)) \cdot (X + \alpha)$$

Polynome

Wir betrachten nun einen endlichen Körper $\mathbb{F}_q$ mit q Elementen und setzen

$$\mathscr{L}(k-1) = \{f(X) \in \mathbb{F}_q[X] \mid \deg(f) \leq k-1\} \subset \mathbb{F}_q[X]$$

betrachten also die Menge aller Polynome $f(X)$ vom Grad $\deg(f) \leq k-1$.

Bemerkung

Die Menge $\mathscr{L}(k-1)$ (mit Additon und Skalarmultiplikation von Poylnomen) ist ein $\mathbb{F}_q$–Vektorraum der Dimension k.
Die Elemente

$$f_0(X) = 1,\ f_1(X) = X,\ f_2(X) = X^2, \ldots, f_{k-1}(X) = X^{k-1}$$

bilden eine Basis von $\mathscr{L}(k-1)$.

Auswertung

Wir betrachten n (paarweise verschiedene) Punkte $b_1, \ldots, b_n \in \mathbb{F}_q$, setzen $\mathscr{B} = \{b_1, \ldots, b_n\}$ und definieren die **Auswertungsabbildung**

$$\mathrm{Ev}_{\mathscr{B}} : \mathscr{L}(k-1) \longrightarrow \mathbb{F}_q^n$$

mit $\mathrm{Ev}_{\mathscr{B}}(f) = (f(b_1), \ldots, f(b_n))$.

Regel

Die Abbildung $\mathrm{Ev}_{\mathscr{B}}$ ist linear. Ist außerdem $k \leq n$, so ist sie auch injektiv und $C = \mathrm{Im}\,(\mathrm{Ev}_{\mathscr{B}}) \subseteq \mathbb{F}_q^n$ ist ein k–dimensionaler Untervektorraum.

Wir nehmen nun immer an, dass $k < n$.

duale Reed–Solomon–Codes

Wir nehmen nun immer an, dass $k < n$.

Definition

Der Untervektorraum $C = \mathrm{Im}\left(\mathrm{Ev}_{\mathscr{B}}\right) \subseteq \mathbb{F}_q^n$ heißt **dualer $[n,k]_q$–Reed–Solomon–Code** zu $\mathscr{B}$.

Regel

Ist C der duale $[n,k]_q$–Reed–Solomon–Code zu $\mathscr{B}$, so ist $d(C) = n - k + 1$. Der Code C ist also ein MDS–Code

duale Reed–Solomon–Codes

Betrachten wir die Basis $f_0(X) = 1, f_1(X) = X, \ldots, f_{k-1}(X) = X^{k-1}$ von $\mathscr{L}(k-1)$, so ist $\mathrm{Ev}_{\mathscr{B}}(f_0(X)), \ldots, \mathrm{Ev}_{\mathscr{B}}(f_{k-1}(X))$ eine Basis von C.

Dabei gilt

$$\mathrm{Ev}_{\mathscr{B}}(f_l(X)) = (b_1^l, b_2^l, \ldots, b_n^l)$$

Daraus erhalten wir eine Erzeugermatrix von C als

$$G = \begin{pmatrix} 1 & 1 & \ldots & 1 & 1 \\ b_1 & b_2 & \ldots & b_{n-1} & b_n \\ \vdots & & \ddots & & \vdots \\ b_1^{k-1} & b_2^{k-1} & \ldots & b_{n-1}^{k-1} & b_n^{k-1} \end{pmatrix}$$

duale Reed–Solomon–Codes

Beispiel

Der duale $[6,4]_{11}$–Reed–Solomon–Code zu $\mathscr{B} = \{0,1,2,3,4,5\}$ hat die Erzeugermatrix

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 4 & 9 & 5 & 3 \\ 0 & 1 & 8 & 5 & 9 & 4 \end{pmatrix}$$

und Paritätsprüfmatrix

$$H = \begin{pmatrix} 1 & 7 & 6 & 7 & 1 & 0 \\ 4 & 7 & 9 & 1 & 0 & 1 \end{pmatrix}$$

duale Reed–Solomon–Codes

Übung

Wir betrachten den Körper $\mathbb{F}_8$, gegeben durch $\alpha^3 = \alpha + 1$. Bestimmen Sie die Erzeugermatrix des dualen $[6, 4]_8$–Reed–Solomon–Codes zu

$$\mathscr{B} = \{\alpha, \alpha^2, \alpha + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1, \alpha^2 + 1\}$$

Reed–Solomon–Codes

Definition

Der $[n,k]_q$–Reed–Solomon–Code C zu $\mathscr{B} = \{b_1, \ldots, b_n\} \subseteq \mathbb{F}_q$ ist der duale Code zum dualen $[n, n-k]_q$–Reed–Solomon–Code $C^\perp$ zu $\mathscr{B}$.

Regel

Für einen $[n,k]_q$–Reed–Solomon–Code C gilt

$$d(C) = n - k + 1$$

Reed–Solomon–Codes sind also MDS–Codes

Reed–Solomon–Codes

Regel

Der $[n,k]_q$–Reed–Solomon–Code C zu $\mathscr{B} = \{b_1, \ldots, b_n\}$ hat Paritätsprüfmatrix

$$H = \begin{pmatrix} 1 & 1 & \ldots & 1 & 1 \\ b_1 & b_2 & \ldots & b_{n-1} & b_n \\ \vdots & & \ddots & & \vdots \\ b_1^{n-k-1} & b_2^{n-k-1} & \ldots & b_{n-1}^{n-k-1} & b_n^{n-k-1} \end{pmatrix}$$

Die Erzeugermatrix kann nicht allgemein angegeben werden.

Reed–Solomon–Codes

Beispiel

Der $[6,2]_{11}$–Reed–Solomon–Code zu $\mathscr{B} = \{0,1,2,3,4,5\}$ hat die Paritätsprüfmatrix

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 4 & 9 & 5 & 3 \\ 0 & 1 & 8 & 5 & 9 & 4 \end{pmatrix}$$

und Erzeugermatrix

$$G = \begin{pmatrix} 1 & 7 & 6 & 7 & 1 & 0 \\ 4 & 7 & 9 & 1 & 0 & 1 \end{pmatrix}$$

Reed–Solomon–Codes

Übung

Wir betrachten den Körper $\mathbb{F}_{13}$ mit 13 Elementen. Bestimmen Sie die Erzeugermatrix und die Paritätsprüfmatrix des $[6, 2]_{13}$–Reed–Solomon–Codes zu

$$\mathscr{B} = \{0, 2, 4, 6, 8, 10\}$$

Reed–Solomon–Codes

Übung

Wir betrachten wieder den Körper $\mathbb{F}_8$, gegeben durch $\alpha^3 = \alpha + 1$. Bestimmen Sie die Erzeugermatrix und die Paritätsprüfmatrix des $[6, 2]_8$–Reed–Solomon–Codes zu

$$\mathscr{B} = \{\alpha, \alpha^2, \alpha + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1, \alpha^2 + 1\}$$

Codierung

Wir führen die Reed–Solomon–Codierung eine Nachricht $m = (m_1, \ldots, m_k) \in \mathbb{F}_q^k$ mit einem $[n, k]_q$–Reed–Solomon–Code C bezüglich $\mathscr{B} = \{b_1, \ldots, b_n\}$ wie folgt durch

- Füge die Nachricht als die letzten k–Stellen des Codeworts ein,

$$c_{n-k+1} = m_1, \quad c_{n-k+2} = m_2, \quad \ldots \quad , c_n = m_k$$

- Ergänze $n - k$–redundante Stellen $c_1, \ldots, c_{n-k}$ über das Gleichungssystem zur Paritätsprüfmatrix bzw. eine geeignete Erzeugermatrix.

Codierung

Beispiel

Der $[6,2]_{11}$–Reed–Solomon–Code zu $\mathscr{B} = \{0,1,2,3,4,5\}$ hat Basis

$$\begin{aligned} g_1 &= (1,7,6,7,1,0) \\ g_2 &= (4,7,9,1,0,1) \end{aligned}$$

Damit wird $m = (m_1, m_2)$ codiert zu

$$c = m_1 \cdot g_1 + m_2 \cdot g_2$$

Codierung

Beispiel

In diesem Beispiel wird als $m = (7, 3)$ codiert zu

$$\begin{aligned} C &= 7 \cdot g_1 + 3 \cdot g_2 \\ &= 7 \cdot (1, 7, 6, 7, 1, 0) + 3 \cdot (4, 7, 9, 1, 0, 1) \\ &= (7, 5, 9, 5, 7, 0) + (1, 10, 5, 3, 0, 3) \\ &= (8, 4, 3, 8, 7, 3) \end{aligned}$$

Codierung

Übung

Benutzen Sie den $[6,4]_{11}$–Reed–Solomon–Code zu $\mathscr{B} = \{0,1,2,3,4,5\}$, um das Nachrichtenwort $m = (2\,,6\,,9\,,7)$ zu codieren.

Codierung

Übung

Wir betrachten wieder den Körper $\mathbb{F}_8$, gegeben durch $\alpha^3 = \alpha + 1$.
Benutzen Sie den $[6, 2]_8$–Reed–Solomon–Codes zu

$$\mathscr{B} = \{\alpha, \alpha^2, \alpha + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1, \alpha^2 + 1\}$$

um das Nachrichtenwort $m = (\alpha + 1, \alpha^2 + \alpha + 1)$ zu codieren.
Es ist

$$G = \begin{pmatrix} \alpha^2 + 1 & \alpha^2 + \alpha + 1 & \alpha^2 + \alpha + 1 & \alpha^2 & 1 & 0 \\ \alpha & \alpha^2 & \alpha^2 + \alpha & 1 & 0 & 1 \end{pmatrix}$$

Decodierung

Ist C ein $[n,k]_q$–Reed–Solomon–Code, so gilt

$$d(C) = n + 1 - k, \quad t = \lfloor \frac{n-k}{2} \rfloor$$

und C kann bis zu t Fehler korrigieren.

Definition

Für ein $a = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ und $0 \leq r \leq n - k - 1$ heißt

$$[a, X^r] = \sum_{i=1}^{n} a_i \cdot b_i^r$$

das r–**te Syndrom** von a.

Regel (Syndrombestimmung)

$$a \in C \iff [a, X^r] = 0 \quad \textit{für alle } r \in \{0, \ldots, n-k-1\}$$

Decodierung

Beispiel

Der $[6,2]_{11}$–Reed–Solomon–Code zu $\mathscr{B} = \{0,1,2,3,4,5\}$ hat die Paritätsprüfmatrix

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 4 & 9 & 5 & 3 \\ 0 & 1 & 8 & 5 & 9 & 4 \end{pmatrix}$$

Für das Wort $a = (0, 7, 5, 9, 5, 7)$ gilt

$$\begin{aligned} [b, X^0] &= 0+7+5+9+5+7 &&= 0 \\ [b, X^1] &= 0+7+5\cdot 2+9\cdot 3+5\cdot 4+7\cdot 5 &&= 0 \\ [b, X^2] &= 0+7+5\cdot 4+9\cdot 9+5\cdot 5+7\cdot 3 &&= 0 \\ [b, X^3] &= 0+7+5\cdot 8+9\cdot 5+5\cdot 9+7\cdot 4 &&= 0 \end{aligned}$$

Also ist a ein Codewort (zur Nachricht $m = (5,7)$).

Decodierung

Beispiel

Für den $[6,2]_{11}$–Reed–Solomon–Code zu $b_1 = 0$, $b_2 = 1$, $b_3 = 2$, $b_4 = 3$, $b_5 = 4$ und $b_6 = 5$ und für das Wort $b = (3,1,2,1,9,8)$ gilt

$$\begin{aligned}
[a, X^0] &= 3+5+2+1+9+8 &&= 2\\
[a, X^1] &= 3\cdot 0+5\cdot 1+2\cdot 2+1\cdot 3+9\cdot 4+8\cdot 5 &&= 7\\
[a, X^2] &= 3\cdot 0+5\cdot 1+2\cdot 4+1\cdot 9+9\cdot 5+8\cdot 3 &&= 10\\
[a, X^3] &= 3\cdot 0+5\cdot 1+2\cdot 8+1\cdot 5+9\cdot 9+8\cdot 4 &&= 3
\end{aligned}$$

Also ist b auf jeden Fall kein Codewort.

Decodierung

Ist a ein fehlerhaft übertragenes Wort, so schreiben wir $a = c + e$, wobei c das eigentliche Codewort ist und e der bei der Übertragung aufgetretene Fehler.
Mit Hilfe der Syndrome bilden wir nur ein Gleichungssystem

$$\begin{array}{rcrcrcl}
[a, X^0] \cdot Y_0 & + & [a, X^1] \cdot Y_1 & + \ldots + & [a, X^t] \cdot Y_t & = & 0 \\
[a, X^1] \cdot Y_0 & + & [a, X^2] \cdot Y_1 & + \ldots + & [a, X^{t+1}] \cdot Y_t & = & 0 \\
\vdots & & & & & & \vdots \\
[a, X^{n-k-t-1}] \cdot Y_0 & + & [a, X^{n-k-t}] \cdot Y_1 & + \ldots + & [a, X^{n-k-1}] \cdot Y_t & = & 0
\end{array}$$

mit $n - k - t$ Gleichungen und $t + 1$ Unbekannten $Y_0, Y_1, \ldots, Y_t$.

Decodierung

Regel (Fehlerstellenbestimmung)

Falls a höchstens t Fehler enthält, so hat dieses Gleichungssystem immer eine nicht–triviale Lösung $l = (l_0, l_1, \ldots, l_t)$. Setzen wir

$$L(X) = l_0 + l_1 \cdot X + \cdots + l_t \cdot X^t$$

und ist $r \in \{1, \ldots, n\}$ mit $e_r \neq 0$ (ist also r ein Fehlerstelle von a), so gilt

$$L(b_r) = 0$$

Definition

Das Polynom $L(X)$ heißt **fehlerlokalisierendes Polynom** von a.