Reed-Solomon-Codes

Jörg Pohle

26.11.2006

- Irving S. Reed und Gustave Solomon (MIT Lincoln Laboratory)
- „Polynomial Codes over Certain Finite Fields.“ (1960)
- Elwyn Berlekamp: Algorithmus für das kürzeste linear rückgekoppeltes Schieberegister (engl. Linear Feedback Shift Register) für eine gegebene Ausgabesequenz (1968)
- James L. Massey: Anwendung des Berlekamp-Algorithmus auf lineare Codes (1969)

Definition

BCH-Code

Sei α eine primitive n-te Einheitswurzel über GF(q). Der Code

$$C = C(\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+\delta-2})$$

heißt ein BCH-Code zum Abstand δ.

Reed-Solomon-Code

Ein BCH-Code der Länge $n = q - 1$ über GF(q) heißt Reed-Solomon-Code und hat zum Abstand δ dann das Generatorpolynom

$$g(x) = (x - \alpha^b)(x - \alpha^{b+1}) \cdots (x - \alpha^{b+\delta-2}).$$

Für $b = 1$ ist es ein Reed-Solomon-Code im engeren Sinne.

Nach der BCH-Schranke gilt: $d \geq \delta = n - k + 1.$
Gemäß der Singleton-Schranke gilt: $k \leq n - d + 1.$
Es muss also gelten: $d = \delta.$

Also erfüllt ein RS-Code die Singleton-Schranke mit Gleichheit ($k = n - d + 1$) und somit ist jeder RS-Code auch ein MDS-Code.

Satz

Jeder Reed-Solomon-Code zum Abstand $\delta = q - k$ über GF(q) ist ein zyklischer $[q - 1, k, q - k; q]$-Code, also ein MDS-Code. □

Es gilt insbesondere, dass für alle $k = 1, \ldots, q - 1$ ein zyklischer $[q - 1, k, q - k; q]$-Code existiert.

Erweiterter Code

Sei C ein Code über GF(q). Dann ist der erweiterte Code C' von C definiert als:

$$C' = \{(c_0, \ldots, c_n) : (c_0, \ldots, c_{n-1} \in C) \text{ und } c_0 + \cdots + c_n = 0\}.$$

Erweiterter Reed-Solomon-Code

Sei C ein $[q-1, k, q-k; q]$-Code im engeren Sinne (also $b = 1$) und C' der erweiterte Code.
Dann ist C' ein $[q, k, q-k+1; q]$-Code, insbesondere also auch ein MDS-Code.

Es werden zwei Codierungsmethoden „angeboten“...

...mit Generatorpolynom

$$g(x) = (x - \alpha^b)(x - \alpha^{b+1}) \cdots (x - \alpha^{b+\delta-2})$$

...über diskrete Fourier-Transformation

(das von Reed und Solomon vorgeschlagene Verfahren)
Nachricht: $m = (m_0, \ldots, m_{k-1})$
Codewort: $c_u = c = (u(1), u(\alpha), \ldots, u(\alpha^{q-2}))$,
wobei das gerade der Fouriervektor von $u(x)$ ist.
$\{c_u\}$ ist dann der $[q-1, k, q-k; q]$-RS-Code im engeren Sinne.

Majority Logic Decoding – I

Empfangen wird $y = c + e$ mit Irrtumsvektor $e = (e_0, \ldots, e_{q-2})$.
Der Empfänger kennt also

$$\begin{aligned} y_0 &= e_0 + u_0 + \cdots + u_{k-1} \\ y_1 &= e_1 + u_0 + \alpha u_1 + \cdots + \alpha^{k-1} u_{k-1} \\ &\vdots \\ y_{q-2} &= e_{q-2} + u_0 + \alpha^{q-2} u_1 + \cdots + \alpha^{(k-1)(q-2)} u_{k-1} \end{aligned}$$

und berechnet für ein beliebiges e die Lösungen der $\binom{q-1}{k}$ Teilsysteme aus je k dieser Gleichungen.

Majority Logic Decoding – II

Wir haben also Lösungen für $\binom{q-1}{k}$ Teilsysteme aus je k dieser Gleichungen.

Dann gilt:
Es sei $w(e) = w$.
Dann ergeben mindestens $\binom{q-1-w}{k}$ Teilsysteme das korrekte u, während jedes inkorrekte u höchstens $\binom{w+k-1}{k}$-mal auftritt.

Decodierung: Wir wählen dasjenige u, das am häufigsten als Lösung der Teilsysteme auftritt.
Wenn $2w(e) < d$ ist, liefert die Decodierung auch das richtige Ergebnis, weil genau dann gilt:

$$\binom{q-1-w}{k} > \binom{w+k-1}{k}$$

.

Problem: RS-Codes sind über sehr langen Alphabeten definiert.
Ausgangscode: RS-Code der Länge $q-1$ über GF(q) mit $q = p^m$.
Projizierter Code: Code über GF(p).

Projizierter Reed-Solomon-Code (für $p = 2$)

Für jeden natürliche Zahl m und jedes k mit $1 \leq k \leq 2^m - 1$ gibt es einen $[(m+1)(2^m-1), mk, d; 2]$-Code mit $d \geq 2(2^m - k)$.

Projizierter erweiterter Reed-Solomon-Code (für $p = 2$)

Für jeden natürliche Zahl m und jedes k mit $1 \leq k \leq 2^m$ gibt es einen $[(m+1)2^m, mk, d; 2]$-Code mit $d \geq 2(2^m - k + 1)$.

Beispiel 1

Ein $[15, 10, 6; 16]$-Code mit $m = 4$, $k = 10$, $d = 6$ und $q = 16$ liefert dann einen

$$[75, 40, 12; 2]\text{-Code.}$$

Problem: Dieser Code ist nicht zyklisch.

Beispiel 2

Ein $[7, 5, 3; 8]$-Code mit $m = 3$, $k = 5$, $d = 3$ und $q = 8$ liefert dann einen

$$[21, 15, 3; 2]\text{-Code.}$$

Dies ist das einzig bekannte Beispiel für einen projizierten zyklischen Code, der selbst auch wieder zyklisch ist.

Korrektur von Fehlerbündeln mit projizierten RS-Codes

Sei C ein RS-Code über GF(q) mit $q = p^m$, der t Fehler korrigieren kann. C hat demnach die Länge $n = q - 1 = p^m - 1$ und Dimension $q - 2t = p^m - 2t$.

Der projizierte Code C' über GF(p) hat die Länge $mn = m(p^m - 1)$ und Dimension $m(p^m - 2t)$. Auch C' kann nur t Fehler korrigieren.

C' kann aber darüberhinaus alle Fehlerbündel der Länge $b \leq (t-1)m + 1$ korrigieren, weil jedes solcher Fehlerbündel höchstens t aufeinanderfolgende Symbole in C verändert, die C jedoch korrigieren kann.

Danke für Eure Aufmerksamkeit.