Prüfmatrizen von Goppa Codes

mit $\frac{G(z) - G(\alpha_i)}{G(\alpha_i)(z-\alpha_i)}$: $\quad G(z) = G_s z^s + G_{s-1} z^{s-1} + \dots + G_0$

$$\left(G_s z^s + G_{s-1} z^{s-1} + G_{s-2} z^{s-2} + \dots + G_0 - G(\alpha_i)\right) : (z-\alpha_i) = G_s z^{s-1} + (G_{s-1} + G_s\alpha_i) z^{s-2} + (G_{s-2} + G_{s-1}\alpha_i + G_s\alpha_i^2) z^{s-3} + \dots$$

$$\frac{G_s z^s + (-G_s\alpha_i) z^{s-1}}{(G_{s-1} + G_s\alpha_i) z^{s-1} + G_{s-2} z^{s-2} + \dots + G_0 - G(\alpha_i)}$$

$$\frac{(G_{s-1} + G_s\alpha_i) z^{s-1} - (G_{s-1}\alpha_i + G_s\alpha_i^2) z^{s-2}}{(G_{s-2} + G_{s-1}\alpha_i + G_s\alpha_i^2) z^{s-2}}$$

$$\Rightarrow \quad H = \begin{pmatrix} \frac{G_s}{G(\alpha_0)} & \frac{G_s}{G(\alpha_1)} & \dots & \frac{G_s}{G(\alpha_{n-1})} \\ \frac{G_{s-1} + G_s\alpha_0}{G(\alpha_0)} & \dots & & \frac{G_{s-1} + G_s\alpha_{n-1}}{G(\alpha_{n-1})} \\ \vdots & \vdots & & \vdots \\ \frac{G_1 + G_2\alpha_0 + \dots G_s\alpha_0^{s-1}}{G(\alpha_0)} & \dots & & \frac{G_1 + G_2\alpha_{n-1} + \dots G_s\alpha_{n-1}^{s-1}}{G(\alpha_{n-1})} \end{pmatrix}$$

$$\Rightarrow \quad H = \begin{pmatrix} G_s & 0 & 0 & \cdots \\ G_{s-1} & G_s & 0 & 0 \cdots \\ G_{s-2} & G_{s-1} & G_s & 0 \cdots \\ \vdots & & & G_s \cdots \\ G_1 & G_2 & \cdots & G_s \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{G(\alpha_0)} & \frac{1}{G(\alpha_1)} & \frac{1}{G(\alpha_2)} & \cdots & \frac{1}{G(\alpha_{n-1})} \\ \frac{\alpha_0}{G(\alpha_0)} & \frac{\alpha_1}{G(\alpha_1)} & \frac{\alpha_2}{G(\alpha_2)} & \cdots & \frac{\alpha_{n-1}}{G(\alpha_{n-1})} \\ \frac{\alpha_0^2}{G(\alpha_0)} & \frac{\alpha_1^2}{G(\alpha_1)} & \frac{\alpha_2^2}{G(\alpha_2)} & \cdots & \frac{\alpha_{n-1}^2}{G(\alpha_{n-2})} \\ \vdots & \vdots & \vdots & & \vdots \\ \frac{\alpha_0^{s-1}}{G(\alpha_0)} & \frac{\alpha_1^{s-1}}{G(\alpha_1)} & \frac{\alpha_2^{s-1}}{G(\alpha_2)} & & \frac{\alpha_{n-1}^{s-1}}{G(\alpha_{n-1})} \end{pmatrix}$$

$\det(\;) \neq 0$

äquivalente Prüfmatrix

am "einfachsten" zu benutzen

H'

$$H' = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha_0 & \alpha_1 & \alpha_2 & & \alpha_{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ \alpha_0^{s-1} & \alpha_1^{s-1} & \alpha_2^{s-1} & & \alpha_{n-1}^{s-1} \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{G(\alpha_0)} & & & \underline{0} \\ & \frac{1}{G(\alpha_1)} & & \\ & & \ddots & \\ \underline{0} & & & \frac{1}{G(\alpha_{n-1})} \end{pmatrix}$$

↑

vergl. Prüfmatrix von BCH und RS-Codes.

Systematische Codierung von Goppa Codes

Beispiel: $G(z) = z^2+z+1$, $GF(2^3)$

$G(z)$ hat keine Nullstellen in $GF(2^3)$ $\Rightarrow$ $L = GF(2^3)$

$\Rightarrow$ $[8, 2, 5]$ binärer Goppa Code

i	0	1	2	3	4	5	6	7
α_i	0	1	α	α^2	α^3	α^4	α^5	α^6
$G(\alpha_i)$	1	1	α^5	α^3	α^5	α^6	α^6	α^3

$GF(2^3)$

i	α^i	α^2	α	1
0	1	0	0	1
1	α	0	1	0
2	α^2	1	0	0
3	α^3	0	1	1
4	α^4	1	1	0
5	α^5	1	1	1
6	α^6	1	0	1
7	α^7	0	0	1

$$H = \begin{pmatrix} \frac{1}{G(\alpha_0)} & \frac{1}{G(\alpha_1)} & \frac{1}{G(\alpha_2)} & \frac{1}{G(\alpha_3)} & \cdots & \frac{1}{G(\alpha_7)} \\ \frac{\alpha_0}{G(\alpha_0)} & \frac{\alpha_1}{G(\alpha_1)} & \cdots & \cdots & & \frac{\alpha_7}{G(\alpha_7)} \end{pmatrix}$$

$$\Rightarrow H = \begin{pmatrix} 1 & 1 & \alpha^2 & \alpha^4 & \alpha^2 & \alpha & \alpha & \alpha^4 \\ 0 & 1 & \alpha^3 & \alpha^6 & \alpha^5 & \alpha^5 & \alpha^6 & \alpha^3 \end{pmatrix}$$

Als Binärmatrix:

$$H = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Matrix in Form $H_{sys} = (P^T \mid I_{n-k})$ bringen

$$\begin{matrix}1\\2\\3\\4\\5\\6\end{matrix}\begin{pmatrix}0&0&1&0&1&1&1&0\\0&0&0&1&0&1&1&1\\1&1&0&0&0&0&0&0\\0&0&0&1&1&1&1&0\\0&1&0&1&0&0&1&0\\0&1&1&1&1&1&1&1\end{pmatrix}$$

← 1. + 2. Zeile

← 5. + 6. Zeile

$$\begin{matrix}1\\2\\3\\4\\5\\6\end{matrix}\begin{pmatrix}0&0&1&0&1&1&1&0\\0&1&1&0&1&0&0&0\\1&1&0&0&0&0&0&0\\0&1&0&0&1&1&0&0\\0&1&0&1&0&0&1&0\\0&0&1&0&1&1&0&1\end{pmatrix}$$

← 2. + 6. Zeile

← 4. + 5. Zeile

← 5. + 6. Zeile

$$\begin{matrix}1\\2\\3\\4\\5\\6\end{matrix}\begin{pmatrix}0&1&1&1&1&1&0&0\\0&1&1&0&1&0&0&0\\1&1&0&0&0&0&0&0\\0&1&0&0&1&1&0&0\\0&1&0&1&0&0&0&0\\0&1&1&0&0&0&0&1\end{pmatrix}$$

← 1. + 5. Zeile

← 4. + 6. Zeile

$$\begin{matrix}1\\2\\3\\4\\5\\6\end{matrix}\begin{pmatrix}0&0&1&1&0&0&0&0\\0&1&1&0&1&0&0&0\\1&1&0&0&0&0&0&0\\0&0&1&0&0&1&0&0\\0&1&0&1&0&0&1&0\\0&1&1&0&0&0&0&1\end{pmatrix}$$

← 1. + 4. Zeile

← 2. + 4. Zeile

$$\begin{pmatrix}1&1&0&0&0&0&0&0\\0&0&1&1&0&0&0&0\\0&1&1&0&1&0&0&0\\0&0&1&0&0&1&0&0\\0&1&1&0&0&0&1&0\\0&1&1&0&0&0&0&1\end{pmatrix}$$

← 3. Zeile
← 1. "
← 2. "
← 1. + 5. Zeile

Vertausche 1. und 3. Spalte ⇒ α_0 und α_2 vertauschen

$$\Rightarrow \quad H_{sys} = \begin{pmatrix} 0&1&1&0&0&0&0 \\ 1&0&0&1&0&0&0 \\ 1&1&0&0&1&0&0 \\ 1&0&0&0&0&1&0 \\ 1&1&0&0&0&0&1 \end{pmatrix} = (\underline{P}^T \vdots \underline{I}_6)$$

$$G_{sys} = \begin{pmatrix} 1&0 & \vdots & 0&1&1&1&1&1 \\ 0&1 & \vdots & 1&0&1&0&1&1 \end{pmatrix} \Rightarrow \begin{aligned} \underline{c}_0 &= 0\,0\,0\,0\,0\,0\,0\,0 \\ \underline{c}_1 &= 1\,0\,0\,1\,1\,1\,1\,1 \\ \underline{c}_2 &= 0\,1\,1\,0\,1\,0\,1\,1 \\ \underline{c}_3 &= 1\,1\,1\,1\,0\,1\,0\,0 \end{aligned}$$

i	0	1	2	3	4	5	6	7
α_i	α	1	0	α^2	α^3	α^4	α^5	α^6

Mit dem Tausch von α_0 und α_2 ist der

Goppa Code systematisch.

H. A.: Decodieren Sie $\underline{r} = (1\,1\,0\,1\,1\,0\,1\,1)$

zum nächsten Codewort (mit Decodierverfahren).

Das Kryptosystem von McEliece

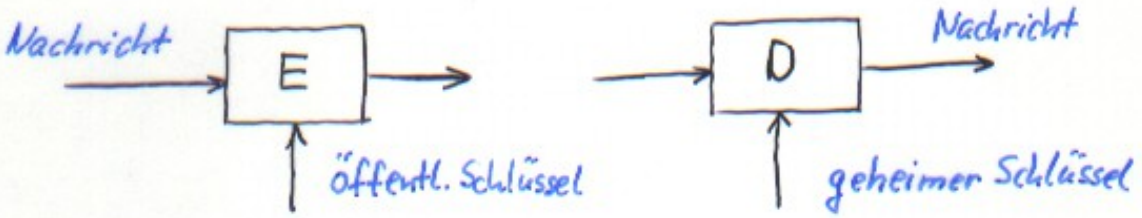
- Basierend auf Goppa Codes
- sogenanntes Asymmetrisches Verschlüsselungs-verfahren oder Öffentliches Verschl. verfahren (engl. Public-key-System) ← PKS

Asymmetrische Verschlüsselungsverfahren basieren auf sog. Einwegfunktionen, das sind Funktionen, die sich leicht in eine Richtung berechnen lassen aber nur sehr schwer "rückwärts".

Anschauliches Beispiel:

Telefonbuch Zu gegebenem Namen und Adresse läßt sich die Telefonnummer leicht finden. Mit vorgegebener Telefonnummer läßt sich Name und Adresse aus dem Telefonbuch nur mit großem Aufwand finden.

Public-Key-Systeme sind Einwegfunktionen mit Hintertür. Der Schlüssel für die Hintertür bleibt geheim.



E: Encryption

D: Decryption

Vorteile von PKS: Der öffentliche Schlüssel kann in ein "Telefonbuch" eingetragen werden. → Trust Center

Es entfällt ein aufwendiger Schlüsselaustausch.

Es können weitere Funktionen wie z.B. digitale Unterschriften kreiert werden.

PKS basieren auf als "schwierig angesehenen mathematischen" Problemen.

Bewiesen ist nichts!

Die wichtigsten Probleme sind:

Das Faktorisierungsproblem (→ RSA Verfahren)
→ von großen ganzen Zahlen

Das diskrete Logarithmusproblem
(→ Diffie-Hellman; ElGamal Verfahren)

Das Rucksackproblem

McEliece System: Benutzt einen linearen fehlerkorrigierenden Code mit schnellem Decodierverfahren.
Dieser Code wird als allgemeiner linearer Code "verschleiert". Decodierverfahren für allgemeine lineare Codes sind sehr aufwendig.

Es wird ein $[n, k, d = 2t+1]$ binärer Goppa Code zufällig ausgewählt. → Durch Wahl eines irreduziblen Goppapolynoms vom Grad t über $GF(2^m)$ ($\rightarrow n = 2^m$.)

Es gibt $\approx \frac{2^{t \cdot m}}{t}$ irreduzible Polynome über $GF(2^m)$ vom Grad t.

Generatormatrix: $\underline{G}$ ← $k \times n$ Matrix; bleibt geheim

Zufällige $k \times k$ Matrix: $\underline{S}$ ← nichtsinguläre Matrix; bleibt geheim

$n \times n$ Permutationsmatrix: $\underline{P}$ ← bleibt geheim

Öffentlicher Schlüssel: $\underline{G'} = \underline{S} \cdot \underline{G} \cdot \underline{P}$ und t

Nachricht: Vektor $\underline{m}$ der Länge k. (← Binärvektor)

Verschlüsselung: $\underline{v} = \underline{m} \cdot \underline{G'} + \underline{e}$

$\underline{v}$: n Bit Chiffretext; $\underline{e}$: Fehlervektor mit Gewicht $\leq t$

Entschlüsselung: $\underline{v} \cdot \underline{P}^{-1} = \underline{m} \cdot (\underline{S} \cdot \underline{G} \cdot \underline{P}) \cdot \underline{P}^{-1} + \underline{e} \cdot \underline{P}^{-1}$

$\underline{v} \cdot \underline{P}^{-1} = (\underline{m} \cdot \underline{S}) \cdot \underline{G} + \underline{e} \cdot \underline{P}^{-1}$

$\underline{e} \cdot \underline{P}^{-1}$ hat ebenfalls Gewicht $\leq t$.

Die Decodierung von $\underline{v} \cdot \underline{P}^{-1}$ liefert $\underline{m} \cdot \underline{S}$

$\Rightarrow \underline{m}$.

"Optimierter" Parametersatz für $n = 1024$

$n = 1024$ ← $GF(2^{10})$

$k \geq 614$ $(= n - m \cdot t)$

$d = 83 = 2 \cdot 41 + 1$ mit $t = 41$

Mit diesem Parametersatz bietet das McEliece Verfahren einen Schutz mit einer Größenordnung von $O(2^{72})$ gegen Angriffe. (→ siehe Li, Deng, Wang, Tr. II, Vol 40, 1, pp. 271-273)

Heutzutage: Länge verdoppeln oder vervierfachen

Grundlage für den besten bekannten Angriff:

Wähle k Bits aus den n Bits von y aus.

Wenn die k Bits ohne Fehler sind

folgt m durch z.B. Gaußsche Elimination.

Verbesserte Angriffe beziehen Fehler mit ein.
(→ Lee, Brickell)

Hauptnachteil von McEliece Verfahren: Schlüssellänge

H.A.: Bestimmen Sie den Speicherplatz, der nötig ist um den öffentlichen und den geheimen Schlüssel eines Nutzers zu speichern.

Anzahl der irreduziblen Polynome über GF(q)

Zunächst $q = 2$: Sei $f(x)$ ein irreduzibles Polynom über GF(2) mit Grad $f(x) = m$

Sei A_k die Anzahl der binären Polynome vom Grad k, die Potenzen von $f(x)$ sind

$$\Rightarrow A_k = \begin{cases} 1 & \text{für } m \mid k \\ 0 & m \nmid k \end{cases}$$

$f^0(x) = 1$

Generatorpolynom: $A(z) = 1 + z^m + z^{2m} + z^{3m} + \dots$

$$\Rightarrow A(z) = \frac{1}{1 - z^m}$$

Entsprechendes Generatorpolynom für irreduzibles Polynom $g(x)$ vom Grad n:

$$B(z) = \frac{1}{1 - z^n}$$

Sei C_k die Anzahl der binären Polynome vom Grad k deren einzige Faktoren $f(x)$ und $g(x)$ sind.

$\Rightarrow$ Wenn $g(x)^{e_1}$ den Grad i hat muß $f(x)^{e_2}$ den Grad $k-i$ haben, d.h.

$$C_k = \sum B_i A_{k-i}$$

dies entspricht Polynommultiplikation.

$$\Rightarrow C(z) = A(z) \cdot B(z) = \frac{1}{1 - z^m} \cdot \frac{1}{1 - z^n}$$

$$\Rightarrow \sum_{k=0}^{\infty} \underbrace{2^k}_{\text{es gibt } 2^k \text{ binäre Polynome vom Grad } k.} z^k = \prod_{m=1}^{\infty} \left(\frac{1}{1-z^m}\right)^{I_m}$$

I_m : Anzahl der irreduziblen binären Polynome vom Grad m.

geom. Reihe

$$\Rightarrow \frac{1}{1-2z} = \prod_{m=1}^{\infty} \left(\frac{1}{1-z^m}\right)^{I_m}$$

Bei $q \neq 2$ $\Rightarrow$ Beschränkung auf monische irred. Polynome (höchster Koeffizient = 1).

$$\Rightarrow \frac{1}{1-qz} = \prod_{m=1}^{\infty} \left(\frac{1}{1-z^m}\right)^{I_m}$$

$$\Rightarrow \log(1-qz) = \sum I_m \log(1-z^m)$$

$$\Rightarrow \frac{-q}{1-qz} = \sum \frac{-m I_m \cdot z^{m-1}}{1-z^m}$$

$$\frac{qz}{1-qz} = \sum_{m=1}^{\infty} \frac{m I_m z^m}{1-z^m}$$

$$\Rightarrow \sum_{k=1}^{\infty} (qz)^k = \sum_{m=1}^{\infty} m I_m \sum_{\substack{k \\ m|k}} z^k = \sum_{k=1}^{\infty} \sum_{\substack{m \\ m|k}} m I_m z^k$$

$$\boxed{q^k = \sum_{\substack{m \\ m|k}} m I_m}$$

$k = 1$: $\quad q = \sum_{\substack{m \\ m|k}} m I_m = I_1 \Rightarrow \underline{I_1 = q}$

Da gilt $I_m \geq 0 \Rightarrow k I_k \leq q^k - q \Rightarrow \underline{I_k \leq \frac{q^k - q}{k}}$

Für k = Primzahl gilt Gleichheitszeichen: $I_p = \frac{q^p - q}{p}$

$\Rightarrow I_2 > 0 \,, I_3 > 0$

Weiter gilt: $q^k = \sum_{\substack{m \\ m|k}} m I_m \leq k I_k + \sum_{i=0}^{k/2} q^i < k I_k + q^{\frac{k}{2}+1}$

$$\Rightarrow \boxed{I_k > \frac{q^k - q^{\frac{k}{2}+1}}{k} = \frac{q^k}{k}\left(1 - q^{-\frac{k}{2}+1}\right)}$$

$\Rightarrow \quad I_k > 0 \quad$ für $k \geq 2$

$\Rightarrow$ Für jedes k gibt es mindestens ein irreduzibles Polynom.

$\Rightarrow$ Existenz eines endlichen Körpers mit p^m Elementen.

Beweis, daß fast alle irreduziblen Goppa Codes asymptotisch gut sind

Goppa Codes, bei denen das Goppa Polynom $G(z)$ irreduzibel über $GF(q^m)$ ist, nennt man irreduzible Goppa Codes. ($\Rightarrow L = GF(q^m)$, $n = q^m$)

Sei $G(z)$ ein über $GF(q^m)$ irreduzibles Polynom vom Grad s. Es gibt I_s derartige Polynome

mit $$I_s \geq \frac{(q^m)^s}{s} \cdot \left(1 - (q^m)^{-\frac{s}{2}+1}\right)$$

Ein Vektor $\underline{k}$ gehört dem Goppa Code mit Goppa-Polynom $G_t(z)$ an, wenn gilt: $\sum \frac{k_i}{z-\beta_i} \equiv 0 \bmod G_t$

Wenn das Hamming Gewicht von $\underline{k}$ gleich d ist, dann kann $\sum \frac{k_i}{z-\beta_i}$ als Quotient von zwei Polynomen geschrieben werden mit Grad{Zählerpolynom} $\leq d-1$.
Da die G_t irreduzibel sind gibt es maximal

$\left\lfloor \frac{d-1}{s} \right\rfloor$ Goppa Codes in denen $\underline{k}$ Codewort ist.

Solange gilt

$$\sum_{d=1}^{D} \underbrace{\left\lfloor \frac{d-1}{s} \right\rfloor}_{\text{je Auswahl gibt es maximal } \left\lfloor \frac{d-1}{s} \right\rfloor \text{ Goppa Codes}} \underbrace{(q-1)^d \binom{q^m}{d}}_{\text{Auswahl gemäß "Gilbert-Varshamov"}} < \frac{q^{ms}}{s} \left(1 - q^{-\frac{ms}{2}+m}\right)$$

ist die Anzahl der "schlechten" Goppa Codes

kleiner als die Gesamtzahl der Goppa Codes

$\Rightarrow$ Es gibt Goppa Codes mit Mindestdistanz $\geq D$.

Setze $s = (1-R)\, q^m / m \qquad \left(R = \frac{k}{n},\ n = q^m\right)$

Rechte Seite

$$\Rightarrow \frac{q^{m\cdot(1-R)\,q^n/m}}{s} \left(1 - q^{m(1-R)\,q^n/2m + m}\right)$$

$$= \frac{q^{(1-R)n}}{s} \left(1 - q^{(1-R)\frac{n}{2} + m}\right)$$

mit $S = q^{\log S} = q^{\log \frac{(1-R)n}{m}}$ $\quad S = (1-R)q^m/m$

$\Rightarrow$

$$= q^{(1-R)n - \log\frac{(1-R)n}{m}} \left(1 - q^{(1-R)\frac{n}{2} + m}\right)$$

Für große n: $\rightarrow q^{(1-R)n}$

↑

Identisch zur Gilbert Schranke

$$\sum_{d=0}^{D} (q-1)^d \binom{n}{d} < q^{(1-R)n}$$

Satz: Fast alle Goppa Codes sind asymptotisch nur unwesentlich schlechter als die Gilbert-Varshamov Schranke.

Das heißt, fast alle irreduziblen Goppa Codes sind asymptotisch gut.

Codes für andere Metriken

Die Hamming Metrik unterscheidet nur an wievielen Stellen zwei Vektoren sich unterscheiden.

z.B. $c_1 = (0, 1, 2, 3, 4, 5, 6)$

$c_2 = (0, a, 0, 0, 0, 0, 0)$

Hamming Distanz: $0+1+1+1+1+1+1 = 6$

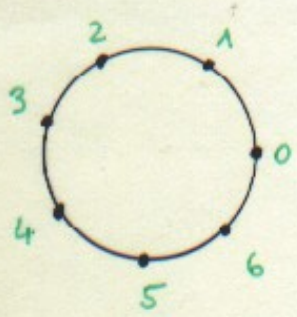
Bei vielen Anwendungen, z.B. in der Nachrichtentechnik, spielt es eine Rolle wie "groß" die einzelnen Fehler sind. Meist sind Fehler, die zu Nachbarsymbolen führen wahrscheinlicher. Wenn man diese Ineffizienzen verbessern will, kann man statt der Hamming-Distanz andere besser geeignete Distanzen nehmen.

z.B. Euklidsche Distanz oft beste Lösung aber in der Codierungstheorie schlecht algebraisch verwertbar.

Codes für die Lee-Metrik

Die Lee Metrik ist nach der Hamming Metrik die populärste algebraisch handhabbare Metrik.

Bei der Lee Distanz wird der kürzeste Abstand zwischen Punkten auf einem Kreis gezählt.



Distanz zwischen 0 und 1 → 1
0 2 → 2
0 3 → 3
0 4 → 3
0 5 → 2
0 6 → 1

$\underline{c}_1 = (0, 1, 2, 3, 4, 5, 6)$

$\underline{c}_2 = (0, 0, 0, 0, 0, 0, 0)$

Lee Distanz: $0+1+2+3+3+2+1 = 12$

Berlekamps negazyklische Codes

→ können eine bestimmte Anzahl von Fehlern in der Lee Metrik korrigieren.

→ Beschränkung auf Codes über $GF(p)$, p Primzahl.

Ein-Fehler-Fall

Blocklänge n : → $2n$ mögliche Fehler

± 1 an jeder Stelle → $2n+1$ mögl. Syndrome
↑ CW

Kugelpackung : $M \cdot (2n+1) \leq p^n$

$= p^k$ bei linearem Code

$$\Rightarrow \quad n \leq \frac{p^{n-k}-1}{2}$$

Fehlerstellen ähnlich BCH-Fall durchnumerieren.

→ α^i im Körper $GF(p^m)$

α^i → Fehler $+1$ an Stelle i $(i = 0, 1, \ldots n-1)$

$-\alpha^i$ → Fehler -1 an Stelle i

α : primitives Element in $GF(p^m)$ $\quad \alpha^{p^m-1} = 1$

mit $n = \frac{p^m-1}{2}$ $\quad \Rightarrow \alpha^n = -1$ ↵

$$\Rightarrow \quad -\alpha^i = \alpha^{n+i}$$

1-Fehlerkorrektur

Die Prüfmatrix $\underline{H}$ mit $\underline{H} = (\alpha^0, \alpha^1, \alpha^2, \dots \alpha^{n-1})$

wobei α ein primitives Element von $GF(p^m)$ ist

und $n = \frac{p^m - 1}{2}$ erzeugt einen $[n, n-m, d_{Lee}=3]$ Code

über $GF(p)$.

Beweis: Ein Fehler mit Wert $e \in \{1, -1\}$

an der Stelle i erzeugt das Syndrom

$$S = e\alpha^i = \begin{cases} \alpha^i & \text{für } e=1 \\ \alpha^{n+i} & \text{" } e=-1. \end{cases}$$

$\Rightarrow$ Jeder Fehler erzeugt ein versch. Syndrom.

H.A.: Zeigen Sie, daß die ein-Fehler-korrigierenden Codes für die Lee Metrik perfekt sind.

Wert

α^j mit $0 \le j \le n-1$ → Fehler an Stelle j: $+1$

α^{n+j} " " → " " " j: -1

Berlekamps negazyklische Codes benutzen nur Fehlerstellenpolynom. Nullstelle bei α^j → Fehler $+1$ an Stelle j

α^{n+j} → Fehler -1

Fehlerwerte ± 2 etc.

werden durch mehrfache Nullstellen des Fehlerstellenpolynoms charakterisiert.

Beispiel für 1-Fehler korr. Code:

$p = 11$; $n = \frac{p-1}{2} = 5$; $n-k=1 \Rightarrow k=4$

$\underline{H} = (\alpha^0 \ \alpha^1 \ \alpha^2 \ \alpha^3 \ \alpha^4)$ α: prim. Element von GF(11) (z.B. $\alpha = 2$)

mit $\alpha = 2$

$\Rightarrow \underline{H} = (1, 2, 4, 8, 5)$ $\quad c(x) = i(x) \cdot (x-\alpha)$

$\Rightarrow$ [5, 4, 3] Code für die Lee Metrik über GF(11)

↑ Lee Mindestdistanz

Jeder Einzelfehler mit Wert +1 oder −1 erzeugt ein unterschiedliches Syndrom.

Negazyklische Codes

Def:

$$H = \begin{pmatrix} \alpha^0 & \alpha^1 & \alpha^2 & \cdots & \alpha^{n-1} \\ \alpha^0 & \alpha^3 & \alpha^6 & \cdots & \alpha^{(n-1)\cdot 3} \\ \alpha^0 & \alpha^5 & \alpha^{10} & \cdots & \vdots \\ \vdots & \vdots & \vdots & & \\ \alpha^0 & \alpha^{2t-1} & & & \alpha^{(n-1)(2t-1)} \end{pmatrix}$$

$\alpha^{2n} = 1$

$\alpha^n = -1$

$\Rightarrow$ Codeworte $\quad c(\alpha^i) = 0 \quad i = 1, 3, \ldots 2t-1$

$$c(x) = i(x) \cdot g(x)$$

$g(x)$ ↑ Generatorpolynom des negazyklischen Codes

Satz: Wenn die Nullstellen (des Codes) des Generatorpolynoms der Blocklänge n über $GF(p)$ die Werte $\alpha, \alpha^3, \alpha^5, \ldots \alpha^{2t-1}$ mit $2t-1 < p$ beinhalten, dann ist die Mindest Leedistanz $d_{Lee} \geq 2t+1$.

Beweis: Durch Berlekamps Decodierverfahren.

$x^{2n}-1 = (x^n+1)(x^n-1)$ $\qquad n = \frac{p^m-1}{2}$

$x^{2n}-1$ enthält alle α^i als Wurzeln (α prim. El. von $GF(p^m)$)

$\Rightarrow$ für i gerade ist α^i NS von x^n-1

$\Rightarrow$ für i ungerade ist α^i NS von x^n+1.

$\Rightarrow$ Die Codewörter eines negazyklischen Codes sind Vielfache eines Generatorpolynoms $g(x)$ welches das Polynom (x^n+1) teilt.

$\underline{c} = (c_0, c_1, c_2, \ldots, c_{n-1}) \in \mathcal{C}$

$\Rightarrow \quad (-c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in \mathcal{C}$

als Polynomgleichung:

$\hat{c}(x) = x \cdot C(x) - c_{n-1} \cdot (x^n+1)$

$$r(x) = c(x) + e(x)$$

$$S_k = r(\alpha^k) = \underbrace{c(\alpha^k)}_{=0} + e(\alpha^k) = e(\alpha^k)$$

k ungerade

Um das wesentliche zu zeigen:

$$e(x) = \varepsilon_1 x^{\ell_1} + \varepsilon_2 x^{\ell_2}$$

$$\varepsilon_{1/2} \in \{1, -1\}$$

$$\Rightarrow S_k = \varepsilon_1 \alpha^{k\ell_1} + \varepsilon_2 \alpha^{k\ell_2}$$

$$X_1 = \alpha^{\ell_1} \qquad X_2 = \alpha^{\ell_2}$$

$$S_k = \varepsilon_1 X_1^k + \varepsilon_2 X_2^k$$

$$S_k = \varepsilon_1^k X_1^k + \varepsilon_2^k X_2^k \quad \leftarrow \varepsilon^k = \varepsilon \text{ für } k \text{ ungerade}$$

$$\Rightarrow S_k = (\varepsilon_1 X_1)^k + (\varepsilon_2 X_2)^k$$

In εX steckt Position und Vorzeichen!

Aufgabe 16

Geben Sie $\underline{H}$- und $\underline{G}$-Matrix eines $[6,4,3]$ Codes über $GF(5)$ an.

$$\underline{H} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 2 & 3 & 4 & 0 & 1 \end{pmatrix}$$

$$\underline{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 4 & 4 \\ 0 & 1 & 0 & 0 & 4 & 3 \\ 0 & 0 & 1 & 0 & 4 & 2 \\ 0 & 0 & 0 & 1 & 4 & 1 \end{pmatrix}$$

Aufgabe 17

Hamming- und Gilbert-Schranke für nichtbinäre Codes.

q statt 2: **Hamming-Schranke:**

$$M \cdot V_t \leq q^n$$

$$V_t = \sum_{i=0}^{t} \binom{n}{i} (q-1)^i$$

Vielfalt $= q-1$ (alle Werte außer 0)

Gilbert-Schranke:

$$\sum_{j=0}^{d-2} \binom{n-1}{j} (q-1)^j < q^{n-k}$$

Aufgabe 18: Bedingungen an Grad $a(z)$ und Grad $b(z)$.

Mit $G(z) = a(z)^2 + z\,b(z)^2$ und Grad $G(z) \le s$

$$\Rightarrow \text{Grad } a(z) \le \frac{s}{2}$$

$$\text{Grad } b(z) \le \frac{s-1}{2}$$

$\Rightarrow$ in ähnlicher Weise wie bei BCH, RS-Codes folgt die Lösbarkeit mit dem EEA.

Aufgabe 19: Bestimmen der $\frac{1}{z-\alpha_i}$ mod $G(z)$ für [16, 8, 5] Code

$\alpha_0 = 0$: $\frac{1}{z-0} \equiv \alpha^{12} z + \alpha^{12} \bmod G(z)$

$\alpha_1 = 1$: $\frac{1}{z-1} \equiv \alpha^{12} z$ "

$\alpha_2 = \alpha$: $\frac{1}{z-\alpha} \equiv \alpha^4 z + \alpha^8$ "

$\alpha_3 = \alpha^2$: $\frac{1}{z-\alpha^2} \equiv \alpha^3 z + \alpha^{11}$ "

$\alpha_4 = \alpha^3$: $\frac{1}{z-\alpha^3} \equiv \alpha^9 z + \alpha^8$ "

$\alpha_5 = \alpha^4$: $\frac{1}{z-\alpha^4} \equiv \alpha^4 z + \alpha^5$ "

$\alpha_6 = \alpha^5$: $\frac{1}{z-\alpha^5} \equiv \alpha z + \alpha^{11}$ "

$\alpha_7 = \alpha^6$: $\frac{1}{z-\alpha^6} \equiv \alpha^8 z + \alpha^6$ "

$\alpha_8 = \alpha^7$: $\frac{1}{z-\alpha^7} \equiv \alpha^6 z + 1$

$\alpha_9 = \alpha^8$: $\frac{1}{z-\alpha^8} \equiv \alpha^3 z + \alpha^5$

$\alpha_{10} = \alpha^9$: $\frac{1}{z-\alpha^9} \equiv \alpha^6 z + \alpha^{13}$

$\alpha_{11} = \alpha^{10}$: $\frac{1}{z-\alpha^{10}} \equiv \alpha z + \alpha^6$

$\alpha_{12} = \alpha^{11}$: $\frac{1}{z-\alpha^{11}} \equiv \alpha^2 z + \alpha^{14}$

$\alpha_{13} = \alpha^{12}$: $\frac{1}{z-\alpha^{12}} \equiv \alpha^2 z + \alpha^{13}$

$\alpha_{14} = \alpha^{13}$: $\frac{1}{z-\alpha^{13}} \equiv \alpha^8 z + \alpha^{14}$

$\alpha_{15} = \alpha^{14}$: $\frac{1}{z-\alpha^{14}} \equiv \alpha^9 z + \alpha^{12}$

Aufgabe 20

$\Rightarrow$ Prüfmatrix aus den $\frac{G(z)-G(\alpha_i)}{G(\alpha_i)(z-\alpha_i)}$:

$$H = \begin{pmatrix} \alpha^{12} & \alpha^{12} & \alpha^{4} & \alpha^{3} & \alpha^{9} & \alpha^{4} & \alpha & \alpha^{8} & \alpha^{6} & \alpha^{3} & \alpha^{6} & \alpha & \alpha^{2} & \alpha^{2} & \alpha^{8} & \alpha^{9} \\ \alpha^{12} & 0 & \alpha^{8} & \alpha^{11} & \alpha^{8} & \alpha^{5} & \alpha^{11} & \alpha^{6} & 1 & \alpha^{5} & \alpha^{13} & \alpha^{6} & \alpha^{14} & \alpha^{13} & \alpha^{14} & \alpha^{12} \end{pmatrix}$$

als Binärmatrix:

$$H = \left(\begin{array}{cccccccccccccccc} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ \hline 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{array}\right)$$

Aufgabe 21 Decodierung des [16, 8, 5] Goppa Codes

$\underline{r} = (0,0,0,\underset{\uparrow r_3}{1},0,\underset{\uparrow r_5}{1},0,0\ldots)$

siehe Aufgabe 19

$\Rightarrow S(z) = \frac{1}{z-\alpha_3} + \frac{1}{z-\alpha_5} = \alpha^3 z + \alpha^{11} + \alpha^4 z + \alpha^5$

$\Rightarrow S(z) = \alpha^7 z + \alpha^3 \Rightarrow T(z)$ mit $T(z)\cdot S(z) \equiv 1 \bmod z^2+z+\alpha^3$

$G(z) = 1\cdot G(z) + 0\cdot S(z)$

$S(z) = 0\cdot G(z) + 1\cdot S(z)$

$\alpha^{13} = 1\cdot G(z) + (\alpha^8 z+\alpha^5) S(z)$

$(z^2+z+\alpha^3) : (\alpha^7 z+\alpha^3) = \alpha^8 z + \alpha^5$

$z^2+\alpha^7 z$

$\alpha^7 z+\alpha^3$

$\alpha^7 z+\alpha^2$

α^{13}

$\Rightarrow 1 \equiv (\alpha^{10} z + \alpha^7)\cdot S(z) \bmod G(z)$

$T(z) = \alpha^{10} z + \alpha^7 \Rightarrow T(z) + z = \alpha^5 z + \alpha^7$

$R^2(z) = \alpha^7 + z\cdot\alpha^5 \Rightarrow R(z) = \alpha^{11} + w(z)\cdot\alpha^{10}$, $w(z) = z+\alpha^9$

$\Rightarrow \underline{R(z) = \alpha^{11} + (z+\alpha^9)\alpha^{10} = \alpha^{10} z + \alpha^{13}}$

$\Rightarrow \underbrace{\alpha^{10} z + \alpha^{13}}_{a(z)} \equiv \underbrace{1}_{b(z)}\cdot R(z) \bmod G(z)$

$\Rightarrow \underline{\sigma(z) = a(z)^2 + z\,b(z)^2 = \alpha^5 z^2 + z + \alpha^{11}}$

NS

$\alpha^2 = \alpha_3$

$\alpha^4 = \alpha_5$

$\Rightarrow \underline{e = (0,0,0,1,0,1,0,\ldots)} \Rightarrow \underline{c = 0}$

in gleicher Weise: $\underline{r} = (0,0,0,0,1,0,0,1,0,0\ldots)$

(r_4, r_7)

$$\Rightarrow S(z) = \frac{1}{z-\alpha_4} + \frac{1}{z-\alpha_7} = \alpha^9 z + \alpha^8 + \alpha^8 z + \alpha^6$$

$$\Rightarrow S(z) = \alpha^{12} z + \alpha^{14} \quad \Rightarrow \quad T(z) = \alpha^6 z + \alpha^{14}$$

$$\Rightarrow T(z) + z = \alpha^{13} z + \alpha^{14}$$

$$\Rightarrow R(z) = \alpha^{14} z + \alpha^{11}$$

$$\Rightarrow \underbrace{\alpha^{14} z + \alpha^{11}}_{a(z)} \equiv \underbrace{1}_{b(z)} \cdot R(z) \bmod G(z)$$

$$\Rightarrow G(z) = \alpha^{13} z^2 + z + \alpha^7$$

$$\Rightarrow \text{NS}: \quad \alpha_4 = \alpha^3, \quad \alpha_7 = \alpha^6$$

$$\Rightarrow \underline{c = 0}$$