Codierungstheorie
Decodierung eines Reed–Solomon Codes

Reinhold Hübl

Woche 9 - Winter 2022

DHBW
Duale Hochschule
Baden-Württemberg
Mannheim

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.

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

$$[a, X^0] = 2, \quad [a, X^1] = 7, \quad [a, X^2] = 10, \quad [a, X^3] = 3$$

Damit hat das Gleichungssystem die Gestalt

$$\begin{array}{rcrcrcl} 2 \cdot Y_0 & + & 7 \cdot Y_1 & + & 10 \cdot Y_2 & = & 0 \\ 7 \cdot Y_0 & + & 10 \cdot Y_1 & + & 3 \cdot Y_2 & = & 0 \end{array}$$

Dieses Gleichungssystem hat die nichttriviale Lösung $l = (5,5,1)$, und wir erhalten das fehlerlokalisierende Polynom

$$L(X) = 5 + 5 \cdot X + X^2$$

Decodierung

Sind bei der Übertragung von a höchstens t Fehler aufgetreten, und ist $L(X)$ das fehlerlokalisierende Polynom von a, so setze

$$N(L) = \{i \in \{1, \ldots, n\} \mid L(b_i) = 0\}$$

Regel (Fehlerstellenbestimmung)

Ist i eine fehlerhafte Stelle von a (dh. ist $e_i \neq 0$), so gilt: $i \in N(L)$. Die möglichen Fehlerstellen von a sind also in $N(L)$ enthalten.

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 $b = (3,1,2,1,9,8)$ ist $L(X) = 5 + 5 \cdot X + X^2$ und

$$\begin{array}{lllll} L(b_1) & = & L(0) & = & 5 \\ L(b_3) & = & L(2) & = & 8 \\ L(b_5) & = & L(4) & = & 8 \end{array} \qquad \begin{array}{lllll} L(b_2) & = & L(1) & = & 0 \\ L(b_4) & = & L(3) & = & 7 \\ L(b_6) & = & L(5) & = & 0 \end{array}$$

Mögliche Fehlerstellen sind also die Stellen $i_1 = 2$ und $i_2 = 6$.

Decodierung

Regel (Fehlerkorrektur)

Sind bei der Übertragung von a höchstens t Fehler aufgetreten und sind $i_1, \ldots, i_\tau$ die potentiellen Fehlerstellen von a und $e_{i_1}, \ldots, e_{i_\tau}$ die Fehlerterme, so setze

$$e_i = \begin{cases} e_{i_k} & \text{falls } i = i_k \text{ für ein } k \\ 0 & \text{sonst} \end{cases}$$

und $e = (e_1, \ldots, e_n)$.
Dann ist

$$c = a - e$$

das zu a gehörige Codewort.

Decodierung

Regel (Fehlerkorrektur)

Sind bei der Übertragung von a höchstens t Fehler aufgetreten und sind $i_1, \ldots, i_\tau$ *die potentiellen Fehlerstellen von a und* $e_{i_1}, \ldots, e_{i_\tau}$ *die Fehlerterme, so setze*

$$e_i = \begin{cases} e_{i_k} & \text{falls } i = i_k \text{ für ein } k \\ 0 & \text{sonst} \end{cases}$$

und $e = (e_1, \ldots, e_n)$.
Dann ist

$$c = a - e$$

das zu a gehörige Codewort.

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 $b = (3,1,2,1,9,8)$ mit den Fehlertermen $e_2 = 9$ und $e_6 = 4$ ist

$$e = (0,9,0,0,0,4)$$

Damit ist

$$\begin{aligned} c &= b - e \\ &= (3,1,2,1,9,8) - (0,9,0,0,0,4) \\ &= (3,3,2,1,9,4) \end{aligned}$$

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 $b = (3,1,2,1,9,8)$ mit den Fehlertermen $e_2 = 9$ und $e_6 = 4$ ist

$$e = (0,9,0,0,0,4)$$

Damit ist

$$\begin{aligned} c &= b - e \\ &= (3,1,2,1,9,8) - (0,9,0,0,0,4) \\ &= (3,3,2,1,9,4) \end{aligned}$$

Die Nachricht dazu ist $m = (9,4)$.

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 $b = (3,1,2,1,9,8)$ mit den Fehlertermen $e_2 = 9$ und $e_6 = 4$ ist

$$e = (0,9,0,0,0,4)$$

Damit ist

$$\begin{aligned} c &= b - e \\ &= (3,1,2,1,9,8) - (0,9,0,0,0,4) \\ &= (3,3,2,1,9,4) \end{aligned}$$

Die Nachricht dazu ist $m = (9,4)$.

Decodierungsalgortihmus

Ist C ein $[n,k]_q$–Reed–Solomon–Code zu $b_1,\ldots,b_n$, und ist $t=\lfloor\frac{n-k}{2}\rfloor$, so decodiere eines Wortes a mit höchstens t Fehlern wie folgt:

1. Für $r=0,\ldots,n-k-1$ bestimme Syndrome $s_r=[a,X^r]=\sum_{i=1}^{n} a_i\cdot b_i^r$.
   Fall $[a,X^r]=0$ für alle r, $\longrightarrow$ STOPP, a ist ein Codewort.
2. Bestimme eine nichttriviale Lösung $l=(l_0,\ldots,l_t)$ des Gleichungssystems für das fehlerlokalisierende Polynoms und setze $L(X)=l_0+l_1\cdot X+\cdots+l_t\cdot X^t$.
3. Bestimme $N(L)=\{i\in\{1,\ldots,n\}\mid L(b_i)=0\}=\{i_1,\ldots,i_\tau\}$.
   Falls $N(L)=\emptyset$, $\longrightarrow$ STOPP, a ist nicht korrigierbar.
4. Bestimme die Lösung $e_1,\ldots,e_\tau$ des Gleichungssystems für die Fehlerterme.
   Falls Gleichungssystem nicht lösbar, $\longrightarrow$ STOPP, a ist nicht korrigierbar.
5. Korrigiere den Fehler.

Decodierung

Übung

Wir betrachten den Körper $\mathbb{F}_8$, gegeben durch $\alpha^3 = \alpha + 1$.
Codiert wird mit dem $[6, 2]_8$–Reed–Solomon–Code C zu den Punkten

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

Decodierung

Übung

Der Code C hat Paritätsprüfmatrix

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

Empfangen wird $a = (\alpha^2+\alpha, \alpha+1, \alpha^2+1, \alpha^2+\alpha, \alpha^2, \alpha+1)$.
Bestimmen Sie die Syndrome

$$[a, X^r] = \sum_{i=1}^{6} a_i \cdot b_i^r$$

für $r = 0, \ldots, 3$.

Decodierung

Übung

Das Wort $a = (\alpha^2 + \alpha, \alpha + 1, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2, \alpha + 1)$ hat die Syndrome

$$[a, X^0] = 1, \quad [a, X^1] = \alpha + 1, \quad [a, X^2] = 1, \quad [a, X^3] = 1$$

Bestimmen Sie das fehlerlokalisierende Polynom, indem Sie eine nichttriviale Lösung des folgenden Gleichungssystems finden:

$$\begin{array}{rcrcrcl} [a, X^0] \cdot Y_0 & + & [a, X^1] \cdot Y_1 & + & [a, X^2] \cdot Y_2 & = & 0 \\ [a, X^1] \cdot Y_0 & + & [a, X^2] \cdot Y_1 & + & [a, X^3] \cdot Y_2 & = & 0 \end{array}$$

Decodierung

Übung

Das Wort $a = (\alpha^2 + \alpha, \alpha + 1, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2, \alpha + 1)$ hat das fehlerlokalisierende Polynom

$$L(X) = \alpha^6 + \alpha^6 \cdot X + X^2$$

Bestimmen Sie die potentiellen Fehlerstellen von a. Es ist

$$b_1 = \alpha, \quad b_2 = \alpha^2, \quad b_3 = \alpha^3, \quad b_4 = \alpha^4, \quad b_5 = \alpha^5, \quad b_6 = \alpha^6$$

Decodierung

Übung

Bestimmen Sie für das Wort $a = (\alpha^2 + \alpha, \alpha + 1, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2, \alpha + 1)$ mit den potentiellen Fehlerstellen 1 und 5 die Fehlerterme, indem Sie das folgende Gleichungssystem lösen:

$$\begin{array}{rcrcl} E_1 & + & E_5 & = & 1 \\ \alpha \cdot E_1 & + & \alpha^5 \cdot E_5 & = & \alpha^3 \\ \alpha^2 \cdot E_1 & + & \alpha^3 \cdot E_5 & = & 1 \\ \alpha^3 \cdot E_1 & + & \alpha \cdot E_5 & = & 1 \end{array}$$

Decodierung

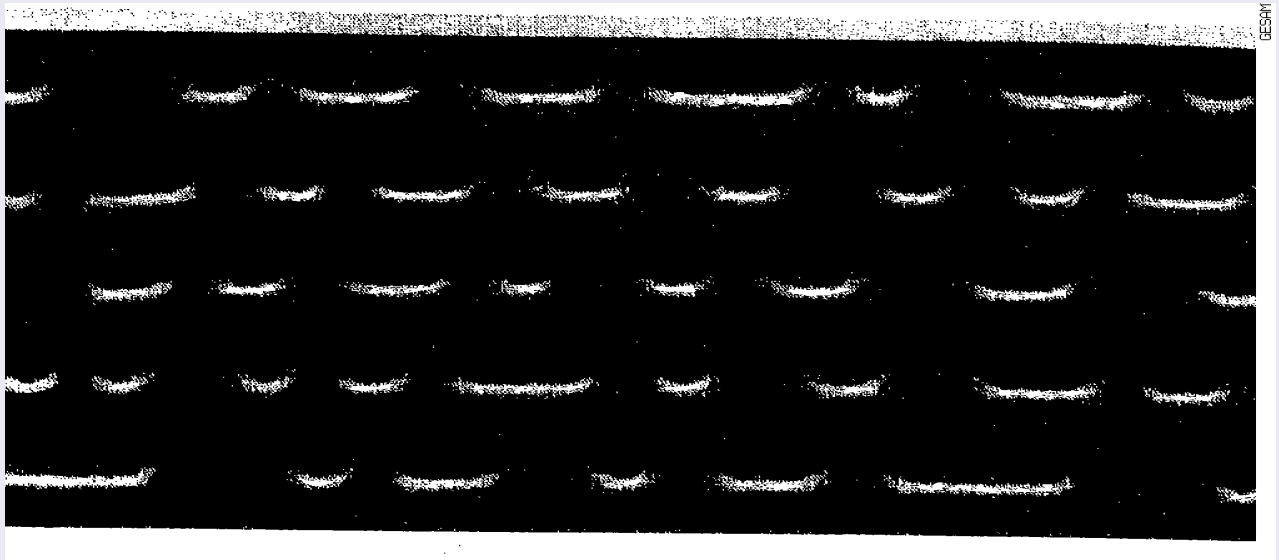
Übung

Korrigieren Sie das Wort $a = (\alpha^2 + \alpha, \alpha + 1, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2, \alpha + 1)$ mit den Fehlertermen $e_1 = \alpha + 1$ und $e_5 = \alpha$.

Decodierung am Beispiel der CD

Beispiel

Erste Anwendungen der Codierungstheorie im großen Umfang: die CD.



Die Datenspur auf einer CD haben eine Breite von 1.6 μm. Eine Einkerbung (ein *Pit*) ist dabei 0.12 μm tief, 0.6 μm breit und mindestens 0.9 μm lang (maximal 3.3 μm). Der Bereich zwischen zwei pits (das sogenannte *land*) hat ebenfalls eine Länge zwischen 0.9 μm und 3.3 μm. Fehler treten schon durch kleinste Kratzer und Verunreinigungen auf.

Codierung am Beispiel der CD

Beispiel

Anforderungen, die bei der Entwicklung der Codierung der CD berücksichtigt werden mussten:

- Vereinzelt (aber regelmäßig) auftretende Lesefehler müssen korrigiert werden können (*sporadic error correction*).
- Selten auftretende Kratzer bis zu einer Breite von 0.2 mm müssen fehlerfrei korrigiert werden können (*burst error correction*).
- (Selten auftretende Kratzer bis zu einer Breite von 0.7 mm müssen näherungsweise korrigiert werden können.)

Decodierung am Beispiel der CD

Beispiel

Die Technik, die bei der Nachrichtencodierung auf einer CD benutzt wird, ist die der **cross interleaved Reed–Solomon**–Codes (CIRS–Codes). Das Alphabet, über dem gearbeitet wird, ist dabei $\mathbb{A} = \mathbb{F}_{2^8} = \mathbb{F}_{256}$, der Raum der Bytes.
Für den CD–Spieler benutzt man dabei zwei solche Codes, einen $[28, 24]$–Reed–Solomon Code C_1 der Zuverlässigkeit 5 und ein $[32, 28]$–Reed–Solomon Code C_2, ebenfalls mit Zuverlässigkeit 5. Diese beiden Codes werden nicht einfach hintereinandergeschaltet sondern in geeigneter Weise miteinander (zur Tiefe 28) verflochten (**interleaving**).

Codierung am Beispiel der CD

Beispiel

Der Körper $\mathbb{F}_{256}$ wird durch die Relation $\alpha^8 = \alpha^4 + \alpha^3 + \alpha^2 + 1$ definiert. Der $[28, 24]$–Reed–Solomon Code C_1 wird gebildet bezüglich der Punkte $\alpha^{27}, \alpha^{26}, \ldots, \alpha^2, \alpha, 1$, hat also die Paritätsprüfmatrix

$$H = \begin{pmatrix} 1 & 1 & \ldots & 1 & 1 & 1 \\ \alpha^{27} & \alpha^{26} & \ldots & \alpha^2 & \alpha & 1 \\ \alpha^{54} & \alpha^{52} & \ldots & \alpha^4 & \alpha^2 & 1 \\ \alpha^{81} & \alpha^{78} & \ldots & \alpha^6 & \alpha^3 & 1 \end{pmatrix}$$

Dieser Code C_1 hat die Zuverlässigkeit $d = 5$ und die Fehlerkorrekturschranke $t = 2$.

Codierung am Beispiel der CD

Beispiel

Der $[32, 28]$–Reed–Solomon Code C_2 wird gebildet bezüglich der Punkte $\alpha^{31}, \alpha^{30}, \ldots, \alpha^2, \alpha, 1$, hat also die Paritätsprüfmatrix

$$H = \begin{pmatrix} 1 & 1 & \ldots & 1 & 1 & 1 \\ \alpha^{31} & \alpha^{30} & \ldots & \alpha^2 & \alpha & 1 \\ \alpha^{62} & \alpha^{60} & \ldots & \alpha^4 & \alpha^2 & 1 \\ \alpha^{93} & \alpha^{90} & \ldots & \alpha^6 & \alpha^3 & 1 \end{pmatrix}$$

Dieser Code C_2 hat ebenfalls die Zuverlässigkeit $d = 5$ und die Fehlerkorrekturschranke $t = 2$.

Prinzip der Interleaving

Beispiel

Benutze Code C_1 um 28 Nachrichtenwörter $m_1, \ldots, m_{28} \in \mathbb{F}_{256}^{24}$ zu Codewörtern $c_1, \ldots, c_{28}$ zu codieren. Schreibe

$$c_i = (c_{i,1}, \ldots c_{i,28})$$

und schreibe diese c_i als die Zeilen einer 28×28–Matrix,

$$A = \begin{pmatrix} c_{1,1} & c_{1,2} & \ldots & c_{1,27} & c_{1,28} \\ c_{2,1} & c_{2,2} & \ldots & c_{2,27} & c_{2,28} \\ \vdots & & \ddots & & \vdots \\ c_{28,1} & c_{28,2} & \ldots & c_{28,27} & c_{28,28} \end{pmatrix}$$

Codierung am Beispiel der CD

Beispiel

Die Matrix wird jetzt transponiert,

$$B = A^\top = \begin{pmatrix} c_{1,1} & c_{2,1} & \cdots & c_{27,1} & c_{28,1} \\ c_{1,2} & c_{2,2} & \cdots & c_{27,2} & c_{28,2} \\ \vdots & & \ddots & & \vdots \\ c_{1,28} & c_{2,28} & \cdots & c_{27,28} & c_{28,28} \end{pmatrix}$$

Aus den Zeilen von B werden neue Nachrichten $d_1, \ldots, d_{28}$ gebildet, wobei

$$d_j = (c_{1,j}, c_{2,j}, \ldots, c_{27,j}, c_{28,j})$$

Diese Wörter d_j werden nun mit C_2 zu neuen Codewörtern $\widetilde{c_j}$ codiert, und diese Wörter $\widetilde{c_1}, \ldots, \widetilde{c_{28}}$ werden gespeichert.

Decodierung am Beispiel der CD

Beispiel

Es soll ein Block von 28 gespeicherten Wörtern $a_1, \ldots, a_{28}$ decodiert werden. Dabei nehmen wir an, dass dieser Block durch einen Kratzer beschädigt wurde und darüberhinaus beim Auslesen vereinzelte Fehler auftreten. Zur Vereinfachung der Notation wollen wir annehmen, dass die beiden ersten Wörter a_1 und a_2 von dem Kratzer betroffen sind und dadurch zu einem großen Teil zerstört wurden. Die sporadischen Fehler erstrecken sich über die Wörter a_3 bis a_{28}.
Die sporadischen Fehler in den Wörtern a_3 bis a_{28} können durch den Code C_2 korrigiert werden. Dadurch können die Nachrichten $d_3, \ldots, d_{28}$ korrekt wieder hergestellt werden. Die Wörter a_1 und a_2 sind so stark durch Fehler betroffen, dass sie als zerstört markiert werden. Damit können d_1 und d_2 nicht (durch C_2) rekonstruiert werden.

Decodierung am Beispiel der CD

Beispiel

Die Matrix B kann teilweise rekonstruiert werden:

$$\widetilde{B} = \begin{pmatrix} — & — & \cdots & — & — \\ — & — & \cdots & — & — \\ c_{1,3} & c_{2,3} & \cdots & c_{27,3} & c_{28,3} \\ c_{1,4} & c_{2,4} & \cdots & c_{27,4} & c_{28,4} \\ \vdots & & \ddots & & \vdots \\ c_{1,28} & c_{2,28} & \cdots & c_{27,28} & c_{28,28} \end{pmatrix}$$

Die ersten beiden Zeilen können nicht rekonstruiert werden, der Rest ist allerdings korrekt.

Decodierung am Beispiel der CD

Beispiel

Zum Rückgängigmachen des Transponierens muss die Matrix wieder transponiert werden,

$$\widetilde{A} = \widetilde{B}^{\top} = \begin{pmatrix} \_ & \_ & c_{1,3} & c_{1,4} & \cdots & c_{1,27} & c_{1,28} \\ \_ & \_ & c_{2,3} & c_{2,4} & \cdots & c_{2,27} & c_{1,28} \\ \vdots & & \vdots & & \ddots & & \vdots \\ \_ & \_ & c_{28,3} & c_{28,4} & \cdots & c_{28,27} & c_{28,28} \end{pmatrix}$$

Decodierung am Beispiel der CD

Beispiel

Weiter verarbeitet werden jetzt die *Zeilen* von $\widetilde{A}$, also

$$\widetilde{c}_j = (\_, \_, c_{j,3}, c_{j,4}, \ldots, c_{j,27}, c_{j,28})$$

wobei die Stellen $c_{j,3}$ bis $c_{j,28}$ korrekte Buchstaben des ursprünglichen Codewortes c_j sind.
Da der Code C_1 zwei Fehler korrigieren kann, kann aus $\widetilde{c}_j$ das Wort c_j zurückgewonnen werden. Aus c_j schließlich kann m_j rekonstruiert werden.

Reed–Solomon–Codes

Der Durchbruch der Reed–Solomon–Codes kam sicherlich 1982 mit der Einführung der CD. Sie kamen und kommen jedoch auch in vielen anderen Anwendungen zum Einsatz:

- Die NASA benutzte Reed–Solomon–Codes 1977 im Voyager–Programm.
- Die QR–Codes nutzen Reed–Solomon–Codes zur Fehlerkorrektur.
- Der DAB–Standard nutzt Reed–Solomon–Codes.
- Diverse Mobilfunkstandards benutzen Reed–Solomon–Codes.

Weiterentwicklungen

Ein Nachteil von Reed–Solomon–Codes ist die Tatsache, dass die Länge der Codes durch die Anzahl der Buchstaben im Alphabet begrenzt ist.
Um längere Codes zu erzeugen, ist es möglich mit Punkten auf algebraischen Kurven über einem endlichen Körper zu arbeiten (**algebraisch–geometrische Codes**). Dadurch können über einem gegebenen Alphabet sehr viel längere Codes konstruiert werden. Anstelle von Polynomen wird in diesem Fall mit geeigneten „Funktionen“ auf den Kurven gearbeitet.
Auch für algebraische geometrische Codes gibt es Algorithmen zur Decodierung.
Algebraisch geometrische Codes sind in der Regel keine MDS–Codes, allerdings kann die Abweichung durch Charakteristika der Kurve (ihr **Geschlecht**) beschrieben werden.

Codes und Kryptographie

Für allgemeine lineare Codes ist die Fehlerkorrektur und Decodierung ein sehr hartes Problem. Im wesentlichen gibt es (nach heutigem Wissen) nichts besseres als eine vollständige Suche durch alle Codewörter, um das mit dem geringsten Abstand zu finden. Bei größeren Codes ist das naturgemäß extrem aufwendig und selbst mit Computerhilfe nicht in akzeptabler Zeit lösbar. Nur bei ausgewählten Verfahren ist es aufgrund zusätzlicher Kenntnisse möglich, die Decodierung zu beschleunigen und in akzeptabler Zeit durchzuführen.
Robert J. Eliece schlug daher schon 1978 kryptographische Protokolle vor, die auf linearen Codes basieren.

Codes und Kryptographie

Schlüsselerzeugung:

Bob erzeugt ein Schlüsselpaar wie folgt:

1. Bob wählt ein t–fehlerkorrigierendes $[n, k]_q$–Codierungsverfahren C mit bekanntem Decodierungsverfahren, das sich nicht direkt aus einer Erzeugermatrix ergibt, aus.
2. Bob bestimmt eine Erzeugermatrix G von C.
3. Bob bestimmt das Decodierungsverfahren D von C.

Der öffentliche Schlüssel von Bob ist des paar (G, t), bestehend aus der Erzeugermatrix G und der Fehlerkorrekturschranke t,

$$k_{\text{pub}} = (G, t)$$

Der private Schlüssel von Bob ist das Decodierungsverfahren D,

$$k_{\text{priv}} = D$$

Codes und Kryptographie

Verschlüsselung:

Alice verschlüsselt eine Nachricht an Bob wie folgt:

1. Alice benutzt den öffentlichen Schlüssel (G, t) und berechnet $c = m \cdot G$.
2. Alice wählt zufällig einen Fehlervektor $e \in \mathbb{F}_q^n$ mit Gewicht $w(e) \leq t$ aus.
3. Alice setzt $b = c + e$.
4. Alice schickt b über einen öffentlichen Kanal an Bob.

Codes und Kryptographie

Entschlüsselung:
Bob nutzt seinen privaten Schlüssel D, um das von Alice empfangene Chiffrat d wie folgt zu entschlüsseln:

1. Bob benutzt seinen privaten Schlüssel D, um den Fehlerterm e zu bestimmen und $c = b - e$ zurückzugewinnen.
2. Bob beseitigt die Redundanzen in c und erhält den Klartext m zurück.

Das Verfahren ist sicher, solange sich das Verschlüsselungsverfahren nicht aus der Erzeugermatrix ableiten lässt.