

# Goppa Codes

In diesem Abschnitt beschreibt  $F/\mathbb{F}_q$  einen Funktionenkörper vom Geschlecht  $g$  mit exaktem Konstantenkörper  $\mathbb{F}_q$ .

## Definition

Seien  $P_1, \dots, P_n$  Stellen vom Grad eins und  $A = \sum_{i=1}^n P_i$ . Sei  $G$  ein weiterer Divisor mit  $\text{supp}(G) \cap \text{supp}(A) = \emptyset$ . Der Goppa-Code zu  $A$  und  $G$  (mittels Auswertung) ist

$$C(A, G) = \{(x(P_1), \dots, x(P_n)) \mid x \in \mathcal{L}(G)\}.$$

**1 Satz.** *Der Goppa-Code  $C(A, G)$  ist ein  $(n, k, d)_q$ -Code mit*

$$\begin{aligned} n &= \deg(A), \\ k &= \dim(G) - \dim(G - A), \\ d &= \deg(A) - \deg(G) + c_G, \end{aligned}$$

wobei  $c_G = \min\{\deg(C) \mid C \geq 0 \text{ und } C \sim G - B \text{ für ein } 0 \leq B \leq A\}$ .

*Beweis.* Die Aussage  $n = \deg(A)$  ist klar. Weiter ist  $\text{ev} : \mathcal{L}(G) \rightarrow C(A, G)$ ,  $x \mapsto (x(P_1), \dots, x(P_n))$  ein Epimorphismus mit Kern  $\mathcal{L}(G - A)$ . Also folgt  $C(A, G) \cong \mathcal{L}(G)/\mathcal{L}(G - A)$  und daraus  $k = \dim(G) - \dim(G - A)$ .

Für  $x \in \mathcal{L}(G) \setminus \{0\}$  sei  $0 \leq B \leq A$  definiert als Summe der Stellen  $P_i$  mit  $x(P_i) = 0$  und  $C \geq 0$  definiert als  $C = (x) + G - B$ . Dann gilt  $C \sim G - B$  und  $C$  kommt in der Minimumsbildung vor. Umgekehrt seien  $C$  und  $B$  aus der Minimumsbildung. Wähle  $x \in F^\times$  mit  $(x) = C - G + B$ . Dann gilt  $x \in \mathcal{L}(G) \setminus \{0\}$ . Wir sehen, daß die Abbildungen  $(x) \mapsto (B, C)$  und  $(B, C) \mapsto (x)$  zueinander invers sind. Nun gilt  $w(\text{ev}(x)) = \deg(A) - \deg(B) = \deg(A) - \deg(G) + \deg(C)$  und die Minimumsbildungen über  $x \in L(G)$  auf der linken und  $C$  mit den obigen Bedingungen auf der rechten Seite liefern dasselbe Ergebnis  $d$ .  $\square$

**2 Korollar.** Für  $\deg(G - A) < 0$  gilt

$$\begin{aligned} k &= \dim(G), \\ d &\geq n - k + 1 - g. \end{aligned}$$

Für  $\deg(G - A) \geq 2g - 1$  gilt  $k = n$ .

*Beweis.* Folgt aus dem Satz von Riemann Roch, siehe Matzat Skript Korollar 11.4.  $\square$

Goppa-Codes mit  $\deg(G - A) < 0$  erfüllen nach der Singleton-Schranke also

$$n + 1 - g \leq d + k \leq n + 1.$$

## Vergleich mit Reed-Solomon Codes

In diesem Abschnitt sei  $F = \mathbb{F}_q(t)$ . Wir zeigen, daß die Klasse der Goppa-Codes  $C(A, G)$  mit  $\deg(A) \leq q$  gleich der Klasse der Reed-Solomon Codes  $RS_k(a, b)$  ist.

Für  $z \in F$  mit  $F = \mathbb{F}_q(z)$ ,  $u \in F^\times$  und  $k \leq 0$  definieren wir

$$V_{z,u,k} = \sum_{i=0}^{k-1} \mathbb{F}_q z^i u.$$

Dies ist ein  $\mathbb{F}_q$ -Untervektorraum von  $F$  mit  $\dim(V_{z,u,k}) = k$ .

**3 Lemma.** Sei  $z \in F$  mit  $F = \mathbb{F}_q(z)$ .

Für jedes  $D \in \text{Div}(F/\mathbb{F}_q)$  gibt es ein bis skalare Vielfache eindeutig bestimmtes  $u \in F^\times$  und ein eindeutig bestimmtes  $k \geq 0$  mit  $\mathcal{L}(D) = V_{z,u,k}$ .

Für jedes  $u \in F^\times$  und  $k \geq 0$  gibt es ein eindeutig bestimmtes  $D \in \text{Div}(F/\mathbb{F}_q)$  mit  $\mathcal{L}(D) = V_{z,u,k}$ .

*Beweis.* Übung.  $\square$

**4 Satz.** Jeder Goppa-Code  $C(A, G)$  mit  $\deg(A) \leq q$  ist gleich einem Reed-Solomon Code  $RS_k(a, b)$  und umgekehrt.

*Beweis.* Sei  $C = C(A, G)$  mit  $\deg(A) \leq q$ . Es gibt eine Stelle  $P$  von  $F/\mathbb{F}_q$  mit  $P \not\leq A$ . Sei  $z \in F^\times$  mit  $(z)_\infty = P$  und folglich  $F = \mathbb{F}_q(z)$ . Sei  $k = \dim(C)$  und  $u \in F^\times$  mit  $\mathcal{L}(G) = V_{z,u,k}$ . Sei  $a = (z(P_1), \dots, z(P_n))$  und  $b = (u(P_1), \dots, u(P_n))$ . Da  $F = \mathbb{F}_q(z)$  gilt  $z(P_i) \neq z(P_j)$  für  $P_i \neq P_j$ , also sind die Koordinaten von  $a$  paarweise verschieden. Außerdem gilt  $u(P_j) \neq 0$

für alle  $j$ , da sonst  $u \in \mathcal{L}(D - P_j)$  und  $\mathcal{L}(D - P_j) = V_{z,u,k} = \mathcal{L}(D)$  folgen würde. Aufgrund der Form von  $V_{z,u,k}$  ergibt sich  $C = RS_k(a, b)$ .

Sei  $C = RS_k(a, b)$ , wobei in der Definition von  $RS_k(a, b)$  Polynome  $f \in \mathbb{F}_q[t]$  mit  $\deg(f) \leq k - 1$  ausgewertet werden. Seien  $P_j = (t - a_j)_0$  und  $A = \sum_{i=1}^n P_j$ . Sei  $u \in \mathbb{F}_q[t]$  ein Interpolationspolynom mit  $u(a_j) = b_j$ . Sei  $G$  der Divisor mit  $\mathcal{L}(G) = V_{t,u,k}$ . Dann gilt  $(t^i u)(P_j) = a_j^i u(a_j) = a_j^i b_j$  und daraus ergibt sich  $C = C(A, G)$ .  $\square$

## Dualer Code

Die Klasse der Goppa-Codes is abgeschlossen unter Dualisierung. Dies wird zum Beispiel für den Dekodierungsalgorithmus benötigt.

**5 Satz.** *Es gibt einen von  $A$  und  $G$  abhängigen kanonischen Divisor  $W$  mit*

$$C(A, G)^\perp = C(A, G^*)$$

für  $G^* = W + A - G$ .

*Beweis.* Der Beweis verwendet Differentiale und den Residuensatz.  $\square$

Wir schreiben die Parameter von  $C(A, G^*)$  in Abhängigkeit von  $A$  und  $G$  auf:

**6 Satz.** *Der Goppa-Code  $C(A, G^*)$  ist ein  $(n^*, k^*, d^*)_q$ -Code mit*

$$\begin{aligned} n^* &= \deg(A), \\ k^* &= i(G - A) - i(G), \\ d^* &= \deg(G) - (2g - 2) + c_G^*, \end{aligned}$$

wobei  $c_G^* = \min\{\deg(C) \mid C \geq 0 \text{ und } C \sim W - G + \tilde{B} \text{ für ein } 0 \leq \tilde{B} \leq A\}$ .

*Beweis.* Die Aussage für  $n^*$  ist klar. Weiter gilt  $k^* = \dim(G^*) - \dim(G^* - A) = \dim(W + A - G) - \dim(W + A - G - A) = i(G - A) - i(G)$  und  $d^* = \deg(A) - \deg(G^*) + c_{G^*} = \deg(A) - \deg(W + A - G) + c_{G^*} = \deg(G) - (2g - 2) + c_{G^*}$ . Es bleibt  $c_{G^*} = c_G^*$  zu zeigen. Sei  $C \geq 0$  und  $B, \tilde{B} \geq 0$  mit  $A = B + \tilde{B}$ . Dann gelten die Äquivalenzen:

$$C \sim G^* - B \Leftrightarrow C \sim W + A - G - B \Leftrightarrow C \sim W + \tilde{B} - G.$$

Also sind die  $C$  in den Minimumsbildungen für  $c_{G^*}$  und  $c_G^*$  die gleichen und es ergibt sich  $c_{G^*} = c_G^*$ .  $\square$

## Dekodierung

Da es hier um Algorithmen geht, sind zuerst ein paar Worte über das Rechnen in Funktionenkörpern erforderlich. Wir gehen davon aus, daß folgende Berechnungen durchgeführt werden können.

1. Berechnung von  $g$ .
2. Berechnung aller Stellen vom Grad  $d$ .
3. Berechnung von  $v_P(f)$  und  $f(P)$ .
4. Berechnung einer Basis von  $\mathcal{L}(D)$ .
5. Lineare Algebra über  $\mathbb{F}_q$  in  $F$ .

Für diese Berechnungen existieren effiziente Algorithmen, deren Laufzeit polynomiell in der Länge der Eingabe ist. Dies gilt nicht für 2., da dort ca.  $q^d$  Stellen berechnet werden müssen. Die Laufzeit für 2. ist polynomiell in  $g$  und  $q^d$ .

Zum Vergleich hat die Syndromdekodierung eines  $(n, k, d)_q$ -Codes eine Laufzeit von ca.  $q^k$ , also eine in der Länge der Eingabe exponentielle Laufzeit. Das Hauptziel ist daher, ein Dekodierverfahren für Goppa-Codes anzugeben, welches polynomiell in der Länge der Eingabe ist.

Die Idee besteht wie bei den Dekodierverfahren für Reed-Solomon Codes darin, das kombinatorische Problem der Bestimmung der Fehlerpositionen algebraisch zu lösen. Kennen wir die Fehlerpositionen, so können wir den Fehlervektor mittels linearer Algebra wie bei den Reed-Solomon Codes bestimmen (siehe Matzat, Beweis von Bemerkung 3.20). In beiden Schritten müssen wir jedoch annehmen, daß die Anzahl der Fehlerpositionen jeweils durch eine eigene geeignete Schranke nach oben beschränkt sind. Die Schranke beim ersten Schritt ist durch  $e = \lfloor (d-1)/2 \rfloor$  gegeben. Die Schranke beim zweiten Schritt ist durch  $d-1$  gegeben. Beide Schranken können so auch für Reed-Solomon Codes verwendet werden (d.h. es müssen nicht etwa noch kleinere Schranken verwendet werden).

Wir verwenden das folgende Setting. Wir betrachten (wie im Skript von Matzat) den Code  $C = C(A, G^*)$  mit den Parametern  $(n, k^*, d^*)$ . Das Element  $x \in C$  ist das gesendete Element, das Element  $y \in \mathbb{F}_q^n$  das empfangene Wort. Der Fehlervektor ist  $e = y - x$ . Wir nennen  $i$  Fehlerindex und  $P_i$  Fehlerstelle, wenn  $e_i \neq 0$  gilt. Wir gehen zunächst von  $w(e) \leq \lfloor (d^* - 1)/2 \rfloor$  aus.

Die Algebraisierung besteht nun im Prinzip darin, einen geeigneten Divisor  $H$  zu finden, so daß die Dekodierung anhand von  $y$  ein  $u \in \mathcal{L}(H)$  bestimmen kann, dessen Nullstellen gerade die Fehlerstellen beinhalten. Dann kann

man  $u(P_i) = 0$  für alle  $i$  testen und so die Fehlerindizes herausfinden. Das Element  $u$  heißt Fehlerortungsfunktion. Allgemeiner kann man  $H$  und  $u$  auch so wählen, daß man anstelle von  $u(P_i) = 0$  die Bedingung  $v_{P_i}(u) > -v_{P_i}(H)$  überprüft. Diese Bedingung benennen wir wie folgt. Für einen Divisor  $D$  und  $f \in \mathcal{L}(D)$  sagen wir, daß  $P_i$  eine Nullstelle von  $f$  bezüglich  $D$  ist, wenn  $f \in \mathcal{L}(D - P_i)$  gilt.

**7 Lemma.** *Besitzt  $f_1 \in \mathcal{L}(D_1)$  eine Nullstelle  $P_i$  bezüglich  $D_1$  und ist  $f_2 \in \mathcal{L}(D_2)$  so besitzt  $f_1 f_2 \in \mathcal{L}(D_1 + D_2)$  die Nullstelle  $P_i$  bezüglich  $D_1 + D_2$ . Besitzt umgekehrt  $f_1 f_2$  eine Nullstelle  $P_j$  bezüglich  $D_1 + D_2$  und ist  $P_j$  keine Nullstelle von  $f_2$  bezüglich  $D_2$ , so ist  $P_j$  eine Nullstelle von  $f_1$  bezüglich  $D_1$ .*

*Beweis.* Die erste Aussage ist klar. Die zweite sieht man wie folgt: Es gilt

$$\begin{aligned} v_{P_j}(f_1 f_2) &= v_{P_j}(f_1) + v_{P_j}(f_2) = -v_{P_j}(D_1) + v_{P_j}(f_2) \\ &\geq -v_{P_j}(D_1 + D_2 - P_j) = -v_{P_j}(D_1) - v_{P_j}(D_2 - P_j). \end{aligned}$$

Daraus ergibt sich  $v_{P_j}(f_2) \geq -v_{P_j}(D_2 - P_j)$  wie gewünscht.  $\square$

Für  $P_j \notin \text{supp}(D)$  ist  $P_j$  eine Nullstelle von  $f$  bezüglich  $D$  genau dann, wenn  $P_j$  eine Nullstelle von  $f$  ist. Es ist auch möglich, Nullstellen bezüglich Divisoren mit Vielfachheiten zu betrachten.

Wir definieren eine Bilinearform, genannt Syndrom, durch

$$[\cdot, \cdot] : \mathbb{F}_q^n \times \mathcal{L}(G) \rightarrow \mathbb{F}_q, \quad (x, z) \mapsto \sum_{i=1}^n x_i z(P_i).$$

Wir definieren weitere Bilinearformen durch

$$[\cdot, \cdot]_v : \mathbb{F}_q^n \times \mathcal{L}(H) \rightarrow \mathbb{F}_q, \quad (x, u) \mapsto [x, uv]$$

für  $v \in \mathcal{L}(G - H)$ .

Das Dekodierverfahren führt dann die folgenden Schritte aus:

1. Berechne

$$\begin{aligned} V_y &= \bigcap_{v \in \mathcal{L}(G-H)} \ker([y, \cdot]_v) \\ &= \{u \in \mathcal{L}(H) \mid [y, u]_v = 0 \text{ für alle } v \in \mathcal{L}(G - H)\}. \end{aligned}$$

2. Wähle  $u \in V_y \setminus \{0\}$  und berechne

$$I'_y = \{i \mid P_i \text{ ist Nullstelle von } u \text{ bezüglich } H\}.$$

3. Berechne eine Lösung  $(e_i)_{i \in I'_y} \in \mathbb{F}_q^{\#I'_y}$  des Gleichungssystems

$$\sum_{i \in I'_y} e_i z(P_i) = [y, z] \text{ für alle } z \in \mathcal{L}(G).$$

4. Setze  $e = e_i$  für  $i \in I'_y$  und  $e_i = 0$  für  $1 \leq i \leq n$ ,  $i \notin I'_y$ . Ausgabe der Dekodierung  $x = y - e$ .

Wir bemerken, daß in Schritt 1 und Schritt 3 die  $v$  und  $z$  wegen der Linearität nur über eine Basis von  $\mathcal{L}(G - H)$  beziehungsweise von  $\mathcal{L}(G)$  laufen müssen.

Wir beweisen im folgenden die Korrektheit des Dekodierverfahrens unter geeigneten Voraussetzungen.

Wir stellen zuerst fest: Wegen  $C(A, G^*)^\perp = C(A, G)$  gilt  $[c, z] = 0$  für alle  $c \in C(A, G^*)$  und  $z \in \mathcal{L}(G)$ . Wegen  $y - e = x \in C(A, G^*)$  folgt daher

$$[y, z] = [e, z]$$

für alle  $z \in \mathcal{L}(G)$ . Wir können also die unbekannte Information  $[e, z]$  mittels  $[y, z]$  für alle  $z \in \mathcal{L}(G)$  berechnen.

**8 Proposition.** *Sei  $T_y$  die Summe der Fehlerstellen und  $t_y = \deg(T_y)$ . Es gelte  $\dim(H) \geq t_y + 1$  und  $\deg(G - H) \geq t_y + 2g - 1$ . Dann gilt*

$$V_y = \mathcal{L}(H - T_y) \neq 0.$$

*Beweis.* Wegen  $\dim(H) = \dim(H - T_y + T_y) \leq \dim(H - T_y) + \deg(T_y)$  folgt  $\dim(H - T_y) \geq \dim(H) - \deg(T_y) \geq 1$ . Dies zeigt  $\mathcal{L}(H - T_y) \neq 0$ .

Zum Beweis von  $\mathcal{L}(H - T_y) \subseteq V_y$  sei  $u \in \mathcal{L}(H - T_y)$  und  $v \in \mathcal{L}(G - H)$ . Dann gilt  $uv \in \mathcal{L}(G - T_y)$  und  $uv(P_i) = 0$  für  $P_i \leq T_y$ . Es folgt

$$[y, u]_v = [y, uv] = [e, uv] = \sum_{i=1}^n e_i uv(P_i) = 0,$$

da  $e_i = 0$  oder  $uv(P_i) = 0$  gilt.

Zum Beweis von  $V_y \subseteq \mathcal{L}(H - T_y)$  sei  $u \in V_y$ . Wegen  $\mathcal{L}(H - T_y) = \bigcap_{P_i \leq T_y} \mathcal{L}(H - P_i)$  genügt es,  $u \in \mathcal{L}(H - P_i)$  für alle  $i$  zu zeigen, also daß  $P_i$  eine Nullstelle von  $u$  bezüglich  $H$  ist. Nach Voraussetzung gilt  $\deg(G - H - T_y) \geq 2g - 1$ , also ist  $G - H - T_y + D$  für alle  $D \geq 0$  nicht speziell. Daher gibt es  $v_i \in \mathcal{L}(G - H - T_y + P_i) \setminus \mathcal{L}(G - H - T_y)$ , so daß  $v_i$  die Nullstellen  $P_j$  mit  $P_j \leq T_y$  und  $P_j \neq P_i$  bezüglich  $G - H$  besitzt und  $P_i$  keine Nullstelle von  $v_i$

bezüglich  $G - H$  ist. Dann gilt  $uv_i \in \mathcal{L}(G - T_y + P_i)$ , also  $uv_i(P_j) = 0$  für  $P_j \leq T_y$  und  $P_j \neq P_i$ . Wir erhalten

$$e_i uv_i(P_i) = \sum_{j=1}^n e_j uv_i(P_j) = [e, uv_i] = [y, uv_i] = [y, u]_{v_i} = 0,$$

wobei sie die erste Gleichung aus  $e_j = 0$  oder  $v_i(P_j) = 0$  für  $j \neq i$  ergibt und die letzte wegen  $u \in V_y$ . Da  $e_i \neq 0$  und  $P_i$  keine Nullstelle von  $v_i$  bezüglich  $G - H$ , aber eine von  $uv_i$  bezüglich  $G$  ist, ergibt sich, daß  $P_i$  eine Nullstelle von  $u$  bezüglich  $H$  sein muß. Also folgt  $u \in \mathcal{L}(H - P_i)$ .  $\square$

Unter den Voraussetzungen der Proposition ist nach Schritt 2 also eine Fehlerortungsfunktion  $u \in \mathcal{L}(H)$  berechnet, deren Nullstellen bezüglich  $H$  die Fehlerstellen beinhalten.

Wir definieren

$$t^* = \max_H \min\{\dim(H) - 1, \deg(G - H) - 2g + 1\}.$$

Der garantierte Minimalabstand von  $C(A, G^*)$  ist

$$d_G^* = \deg(G) - (2g - 2).$$

Es gilt  $d^* \geq d_G^*$ .

**9 Lemma.** *Es gilt*

$$\lfloor (d_G^* - 1 - g)/2 \rfloor \leq t^* \leq \lfloor (d_G^* - 1)/2 \rfloor.$$

*Beweis.* Zum Beweis der unteren Schranke sei  $t = \lfloor (d_G^* - 1 - g)/2 \rfloor$  und  $H = (t + g)P_1$ . Dann gilt  $\dim(H) \geq \deg(H) + 1 - g = t + 1$  und  $\deg(G - H) - 2g + 1 \geq \deg(G) - t - 3g + 1 = d_G^* - t - g - 1 \geq t$ . Es folgt  $t^* \geq t$ .

Für die obere Schranke sei  $H$  mit  $t^* = \min\{\dim(H) - 1, \deg(G - H) - 2g + 1\}$ . Unter Beachtung von  $\dim(H) \leq \deg(H) + 1$  folgt  $2t^* \leq \dim(H) - 1 + \deg(G - H) - 2g + 1 \leq \deg(H) + \deg(G - H) - 2g + 1 \leq \deg(G) - 2g + 1 \leq d_G^* - 1$ . Also ergibt sich  $t^* \leq \lfloor (d_G^* - 1)/2 \rfloor$ .  $\square$

**10 Satz.** *Der Dekodieralgorithmus kann bis zu  $t^*$  Fehler bei entsprechender Wahl von  $H$  dekodieren.*

*Beweis.* Sei  $t \geq 0$  mit  $t \leq t^*$ . Entsprechende Wahl von  $H$  bedeutet, daß  $t \leq \min\{\dim(H) - 1, \deg(G - H) - 2g + 1\}$  gilt, also die Voraussetzungen der Proposition im Fall  $t_y \leq t$  erfüllt sind. Aufgrund der Definition von  $t^*$  gibt es stets ein passendes  $H$ .

Am Ende von Schritt 2 umfaßt  $I'_y$  dann in der Tat alle Fehlerstellen (und vielleicht noch weitere Stellen, die keine Fehlerstellen sind).

Sei  $T'_y = \sum_{i \in I'_y} P_i$ . Dann gilt  $u \in \mathcal{L}(H - T'_y)$  und  $u \neq 0$ . Es folgt  $\deg(H - T'_y) \geq 0$  und  $\#I'_y = \deg(T'_y) \leq \deg(H) \leq \deg(G) - 2g + 1 - t = d_G^* - 1 - t \leq d_G^* - 1 \leq d^* - 1$ . Also hat das Gleichungssystem in Schritt 3 eine eindeutig bestimmte Lösung.  $\square$

Das beschriebene Verfahren geht auf Skorobogatov und Vladut (1990) zurück. Ein Problem besteht in der geeigneten Wahl von  $H$ . Im allgemeinen können wir  $H$  nur so wählen, daß  $\lfloor (d_G^* - 1 - g)/2$  Fehler korrigiert werden können. Um ein besseres Korrekturverhalten zu bekommen, können wir beispielsweise versuchen, spezielle Divisoren  $H$  mit  $i(H) > 0$  zu verwenden oder  $H$  so zu wählen, daß  $G - H - T_y$  in der Proposition nicht speziell ist. Hierzu kann es erforderlich sein, daß der Funktionenkörper geeignet konstruiert werden muß.

Diese etwas unzufriedenstellende Situation wird durch das Dekodierungsverfahren von Feng und Rao (1993) behoben, mit dem man (für ungerades  $d_G^*$ ) stets bis zu  $\lfloor (d_G^* - 1)/2$  Fehler korrigieren kann. In diesem Verfahren sind die Divisoren  $G$  und  $H$  Vielfache einer festen Stelle  $P$  vom Grad eins. Mit trickreichen Überlegungen wird bewerkstelligt, daß die Syndrome  $[e, z]$  nicht nur für  $z \in \mathcal{L}(G)$ , sondern auch für  $z \in \mathcal{L}(G + \lambda P)$  und  $\lambda$  ausreichend groß ausgerechnet werden können. Das Problem bei der Berechnung der höheren Syndrome  $[e, z]$  ist, daß zwar  $[e, z] = [y, z]$  für  $z \in \mathcal{L}(G)$  gilt, dies aber für  $z \in \mathcal{L}(G + \lambda P)$  falsch ist. Mit  $G + \lambda P$  an Stelle von  $G$  gilt dann die Proposition wie gehabt und der Dekodialgorithmus läßt sich wie oben durchführen ( $[y, u]_v = 0$  muß geeignet durch  $[e, u]_v = 0$  ersetzt werden).

Ein gewisser Schönheitsmangel des Verfahrens von Feng und Rao ist, daß nicht alle Stellen vom Grad eins für die Auswertung verwendet werden können. Auch bleibt die Frage offen, ob es ein Verfahren gibt, daß bis zu  $\lfloor (d^* - 1)/2$  anstelle von  $\lfloor (d_G^* - 1)/2$  Fehler korrigieren kann.