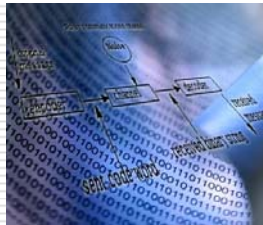


## Kapitel 14: Polynomevaluationscodes



Lineare und zyklische  
Codes

Copyright M. Gross, ETH Zürich  
2005, 2006

1

## Ziele des Kapitels

ETH

- Polynomevaluationscodes

Lineare und  
zyklische Codes

Informationstheorie  
Copyright M. Gross, ETH Zürich 2005, 2006

2

## Polynomevaluationscodes ETH

### Codierung:

Fasse  $K$  Informationssymbole über  $GF(q)$  als  
Koeffizienten eines Polynoms vom Grad  $K - 1$  auf

Codewort erhält man durch Auswertung des  
Polynoms an  $N$  fixen und bekannten Stellen  
 $x_1, \dots, x_N$

Damit dies möglich ist, muss  $q \geq N$  erfüllt sein

Lineare und  
zyklische Codes

Informationstheorie  
Copyright M. Gross, ETH Zürich 2005, 2006

3

## Polynomevaluationscodes ETH

### Beispiel:

- Auf Polynomevaluation  
basierender linearer  
[5, 2]-Code  $C$
- Körper  $GF(5)$
- Auswertungsstellen  
 $x_i := i - 1 \ (i \in \{1, \dots, 5\})$

Informations-  
vektor

Assoziiertes  
Polynom

Codewort

$a_0 \parallel a_1$	$a(x)$	$a(0) \parallel a(1) \parallel a(2) \parallel a(3) \parallel a(4)$
00	0	00000
01	$x$	01234
02	$2x$	02413
03	$3x$	03142
04	$4x$	04321
10	1	11111
11	$x+1$	12340
12	$2x+1$	13024
13	$3x+1$	14203
14	$4x+1$	10432
20	2	22222
21	$x+2$	23401
22	$2x+2$	24130
23	$3x+2$	20314
24	$4x+2$	21043
30	3	33333
31	$x+3$	34012
32	$2x+3$	30241
33	$3x+3$	31420
34	$4x+3$	32104
40	4	44444
41	$x+4$	40123
42	$2x+4$	41302
43	$3x+4$	42031
44	$4x+4$	43210

Lineare und  
zyklische Codes

Informationstheorie  
Copyright M. Gross, ETH Zürich 2005, 2006

4

## Polynomevaluationscodes ETH

### Beispiel (Fortsetzung):

- Dazugehörige Generatormatrix

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

- Systematische Generatormatrix

$$\tilde{G} = \begin{bmatrix} 1 & 0 & 4 & 3 & 2 \\ 0 & 1 & 2 & 3 & 4 \end{bmatrix}$$

- Parity-Check Matrix

$$H = \begin{bmatrix} 1 & 3 & 1 & 0 & 0 \\ 2 & 2 & 0 & 1 & 0 \\ 3 & 1 & 0 & 0 & 1 \end{bmatrix}$$

$a_0 \parallel a_1$	$a(x)$	$a(0) \parallel a(1) \parallel a(2) \parallel a(3) \parallel a(4)$
00	0	00000
01	$x$	01234
02	$2x$	02413
03	$3x$	03142
04	$4x$	04321
10	1	11111
11	$x+1$	12340
12	$2x+1$	13024
13	$3x+1$	14203
14	$4x+1$	10432
20	2	22222
21	$x+2$	23401
22	$2x+2$	24130
23	$3x+2$	20314
24	$4x+2$	21043
30	3	33333
31	$x+3$	34012
32	$2x+3$	30241
33	$3x+3$	31420
34	$4x+3$	32104
40	4	44444
41	$x+4$	40123
42	$2x+4$	41302
43	$3x+4$	42031
44	$4x+4$	43210

Lineare und  
zyklische Codes

Informationstheorie  
Copyright M. Gross, ETH Zürich 2005, 2006

5

## Polynomevaluationscodes ETH

- Singleton Bound:** Die Minimaldistanz eines linearen  $[N, K]$ -Codes über  $GF(q)$  ist höchstens  $N - K + 1$

**Theorem:** Die Minimaldistanz eines linearen Codes mit Parity-Check-Matrix  $H$  ist gleich der minimalen Anzahl von Spalten in  $H$ , die linear abhängig sind

Beweisidee: jede Menge von  $N - K + 1$  Spaltenvektoren der  $((N - K) \times N)$ -Parity-Check-Matrix eines  $[N, K]$ -Codes ist linear abhängig

- Codes basierend auf **Polynomevaluation** erreichen diese obere Schranke für  $q \geq N$

Lineare und  
zyklische Codes

Informationstheorie  
Copyright M. Gross, ETH Zürich 2005, 2006

6

## Polynomevaluationscodes **ETH**

- ❑ **Polynomeigenschaft:** Jedes Polynom vom Grad  $d$  lässt sich eindeutig aus den Polynomwerten an beliebigen  $d + 1$  Stützstellen interpolieren  
-> (z.B. durch Lagrange-Interpolation)
- ❑ Das Polynom vom Grad  $K - 1$  und damit der Informationsvektor kann folglich aus beliebigen  $K$  Stellen des Codewortes eindeutig rekonstruiert werden
- ❑ Zwei verschiedene Codewörter können also höchstens in  $K - 1$  Positionen übereinstimmen, und die Minimaldistanz ist also mindestens  $d_{\min} = N - (K - 1) = N - K + 1$

## Polynomevaluationscodes **ETH**

- ❑ Ein Polynomevaluationscode besitzt also immer maximale Minimaldistanz
- ❑ Effiziente Decodierung nach Algorithmus von Welch und Berlekamp (1983)

## Polynomevaluationscodes **ETH**

- ❑ „Codes basierend auf **Polynomevaluation** erreichen diese obere Schranke für  $q \geq N^r$ “
- ❑ Zur Konstruktion eines Codes mit grosser Minimaldistanz setzt die Konstruktion einen grossen Körper voraus
- ❑ Erweiterung auf  $GF(2)$  durch Gleichsetzen von einem  $[n, k]$ -Code über  $GF(2^r)$  mit einem binären  $[rn, rk]$ -Code
- ❑ Für jedes  $r > 0$ ,  $N \leq r2^r$  und  $K \leq N - r$  gibt es einen linearen binären  $[N, K]$ -Code mit Minimaldistanz mindestens  $n - k + 1$ , wobei  $n = \text{floor}(N/r)$  und  $k = \text{ceil}(K/r)$

## Polynomevaluationscodes **ETH**

- ❑ Für jedes  $r > 0$ ,  $N \leq r2^r$  und  $K \leq N - r$  gibt es einen linearen binären  $[N, K]$ -Code mit Minimaldistanz mindestens  $n - k + 1$ , wobei  $n = \text{floor}(N/r)$  und  $k = \text{ceil}(K/r)$
- ❑ **Beispiel: Mindestens erreichbare Minimaldistanz für linearen binären [1000,537]-Code**
  - kleinstes ganzzahlige  $r$  mit  $N \leq r2^r$  ist 8
  - erreichbare Minimaldistanz:  
 $\text{floor}(N/r) - \text{ceil}(K/r) + 1 =$   
 $\text{floor}(1000/8) - \text{ceil}(537/8) + 1 =$   
 $125 - 68 + 1 = 58$

## Weitere Informationen **ETH**

- ❑ Weitere Verfahren im Skript.
- ❑ Nicht prüfungsrelevant:
  - Codes basierend auf Polynommultiplikation
  - Reed-Solomon Codes
  - Fehlerbündel, Interleaving
  - CD-Codierung

## Letzte Uebung **ETH**

- ❑ Nur Vorbesprechung
- ❑ Gut vorbereiten!
- ❑ Bei späteren Fragen:
  - Forum
  - E-Mail
  - Persönlich nach Voranmeldung: bei Keiser, Wicke, Cotting
- ❑ -> Ueberblick