Facetten der Codierungstheorie

Axel Kohnert, Alfred Wassermann

Aachen SPP 1489 Februar 2011

http://codes.uni-bayreuth.de

Universität Bayreuth

axel.kohnert@uni-bayreuth.de

UNIVERSITÄT BAYREUTH

Facetten

- Kombinatorische Optimierung
- Geometrie
- Kryptographie

Suche nach Codes mit Minimialdistanz d

- Suche nach $[n, k, \geq d]_q$ -Code =

Suche nach Codes mit Minimialdistanz d

- Suche nach $[n, k, \geq d]_q$ -Code =
- Suche nach Generatormatrix G

Suche nach Codes mit Minimialdistanz d

- Suche nach $[n, k, \geq d]_q$ -Code =
- Suche nach Generatormatrix G
- G hat Minimumdistanz $\geq d$ $\Longleftrightarrow$

Suche nach Codes mit Minimialdistanz d

- Suche nach $[n, k, \geq d]_q$ -Code =
- Suche nach Generatormatrix G
- G hat Minimumdistanz $\geq d \iff$
- Hamming-Gewicht jeder der $q^k - 1$ möglichen Nichtnull-Linearkombination (=$v\Gamma$) der Zeilen $\geq d$ ist $\iff$

Suche nach Codes mit Minimialdistanz d

- Suche nach $[n, k, \geq d]_q$ -Code =
- Suche nach Generatormatrix G
- G hat Minimumdistanz $\geq d \iff$
- Hamming-Gewicht jeder der $q^k - 1$ möglichen Nichtnull-Linearkombination (=$v\Gamma$) der Zeilen $\geq d$ ist $\iff$
- Anzahl der Nullen jeweils $\leq (n - d)$ ist.

Suche nach Generatormatrix mit Minimialdistanz d

- Insgesamt $q^k - 1$ mögliche Spalten γ einer Generatormatrix G.

Suche nach Generatormatrix mit Minimialdistanz d

- Insgesamt $q^k - 1$ mögliche Spalten γ einer Generatormatrix G.
- Der Beitrag der Spalte γ zum Codewort vG (des Informationswort v) ist gerade $\langle v, \gamma \rangle$.

Suche nach Generatormatrix mit Minimialdistanz d

- Insgesamt $q^k - 1$ mögliche Spalten γ einer Generatormatrix G.
- Der Beitrag der Spalte γ zum Codewort vG (des Informationswort v) ist gerade $\langle v, \gamma \rangle$.

Konstruiere den gesuchten Code als Lösung eines Diophantischen Gleichungssystem.

Diophantischen Gleichungssystem

- kontrolliere, dass $\langle v, \gamma \rangle$ nicht zu oft Null wird.

Diophantischen Gleichungssystem

- kontrolliere, dass $\langle v, \gamma \rangle$ nicht zu oft Null wird.
- Definiere die Matrix $M = M(q,k)$ als die $\left(q^k - 1\right) \times \left(q^k - 1\right) -$ Matrix (Zeilen = Informationswort v, Spalten =γ) durch

$$M_{v,\gamma} := \begin{cases} 1 & \text{falls } \langle v, \gamma \rangle = 0 \\ 0 & \text{sonst} \end{cases}$$

Es ex ein $[n, k, \geq d]_q$ -Code

$\Longleftrightarrow$

es existiert eine Lösung $x \in \mathbb{N}^{q^k - 1}$ von

$$Mx^T \leq \begin{pmatrix} n-d \\ n-d \\ \vdots \\ n-d \\ n-d \end{pmatrix}$$

mit der Nebenbedingung $\sum x_i = n$

Inzidenzgeometrie

- Wegen der Bilinearität von $\langle v, \gamma \rangle$ genügt es die $\frac{q^k-1}{q-1}$ möglichen Zeilen und Spalten zu betrachten, deren erste Eintrag $\neq 0$ auf 1 normiert ist.

Inzidenzgeometrie

- Wegen der Bilinearität von $\langle v, \gamma \rangle$ genügt es die $\frac{q^k-1}{q-1}$ möglichen Zeilen und Spalten zu betrachten, deren erste Eintrag $\neq 0$ auf 1 normiert ist.
- Neue Interpretation für $M(q,k)$:

Inzidenzgeometrie

- Wegen der Bilinearität von $\langle v, \gamma \rangle$ genügt es die $\frac{q^k-1}{q-1}$ möglichen Zeilen und Spalten zu betrachten, deren erste Eintrag $\neq 0$ auf 1 normiert ist.
- Neue Interpretation für $M(q,k)$:
- Spalten werden durch die Punkte γ der projektiven Geometrie $PG(k-1,q)$ gelabelt.

Inzidenzgeometrie

- Wegen der Bilinearität von $\langle v, \gamma \rangle$ genügt es die $\frac{q^k-1}{q-1}$ möglichen Zeilen und Spalten zu betrachten, deren erste Eintrag $\neq 0$ auf 1 normiert ist.
- Neue Interpretation für $M(q,k)$:
- Spalten werden durch die Punkte γ der projektiven Geometrie $PG(k-1,q)$ gelabelt.
- Zeilen ebenso durch die Punkte v.

Inzidenzgeometrie

- Wegen der Bilinearität von $\langle v, \gamma \rangle$ genügt es die $\frac{q^k-1}{q-1}$ möglichen Zeilen und Spalten zu betrachten, deren erste Eintrag $\neq 0$ auf 1 normiert ist.
- Neue Interpretation für $M(q,k)$:
- Spalten werden durch die Punkte γ der projektiven Geometrie $PG(k-1,q)$ gelabelt.
- Zeilen ebenso durch die Punkte v.
- Eintrag $M_{v,\gamma}$ ist $1 \iff$ Punkt $\gamma \in v^{\perp}$.

Inzidenzgeometrie

- M ist die Inzidenzmatrix zwischen Punkten und Hyperebenen in $PG(k-1,q)$.

Inzidenzgeometrie

- M ist die Inzidenzmatrix zwischen Punkten und Hyperebenen in $PG(k-1,q)$.
- $0/1$-Lösungen sind Punktmengen in $PG(k-1,q)$.

Inzidenzgeometrie

- M ist die Inzidenzmatrix zwischen Punkten und Hyperebenen in $PG(k-1,q)$.
- $0/1$-Lösungen sind Punktmengen in $PG(k-1,q)$.
- Es ex ein projektiver $[n,k,\geq d]_q$ -Code
  $\Longleftrightarrow$
  es gibt n Punkte in $PG(k-1,q)$ mit der Eigenschaft: jede Hyperebene enthält maximal $n-d$ dieser Punkte.

Inzidenzgeometrie

- M ist die Inzidenzmatrix zwischen Punkten und Hyperebenen in $PG(k-1,q)$.
- $0/1$-Lösungen sind Punktmengen in $PG(k-1,q)$.
- Es ex ein projektiver $[n,k,\geq d]_q$ -Code
  $\Longleftrightarrow$
  es gibt n Punkte in $PG(k-1,q)$ mit der Eigenschaft: jede Hyperebene enthält maximal $n-d$ dieser Punkte.
- Arc-Problem in $PG(k-1,q)$

Inzidenzgeometrie

- Normalform der Generatormatrix liefert dann Normalform der Punktmenge.

Inzidenzgeometrie

- Normalform der Generatormatrix liefert dann Normalform der Punktmenge.
- Die Berücksichtigung von Körperautomorphismen liefert, dass die komplete Automorphismengruppe $P\Gamma L(k-1,q)$ von $PG(k-1,q)$ betrachtet wird.

Inzidenzgeometrie

- Normalform der Generatormatrix liefert dann Normalform der Punktmenge.
- Die Berücksichtigung von Körperautomorphismen liefert, dass die komplette Automorphismengruppe $P\Gamma L(k-1,q)$ von $PG(k-1,q)$ betrachtet wird.
- Hilft bei Klassifizierungsfragen.

Inzidenzgeometrie

- Normalform der Generatormatrix liefert dann Normalform der Punktmenge.
- Die Berücksichtigung von Körperautomorphismen liefert, dass die komplete Automorphismengruppe $P\Gamma L(k-1,q)$ von $PG(k-1,q)$ betrachtet wird.
- Hilft bei Klassifizierungsfragen.
- nützliches Zusammenspiel:

  Geometrie $\leftrightarrow$ Codierungstheorie

Hjelmslev Geometrie

- statt endlicher Körper: Ring $\mathbb{Z}_4 := \mathbb{Z}/4\mathbb{Z}$.

Hjelmslev Geometrie

- statt endlicher Körper: Ring $\mathbb{Z}_4 := \mathbb{Z}/4\mathbb{Z}$.
- Die projektive Geometrie der freien Untermoduln von $\mathbb{Z}_4^k$ wird mit $PHG(k-1, \mathbb{Z}_4)$ bezeichnet.

Hjelmslev Geometrie

- statt endlicher Körper: Ring $\mathbb{Z}_4 := \mathbb{Z}/4\mathbb{Z}$.
- Die projektive Geometrie der freien Untermoduln von $\mathbb{Z}_4^k$ wird mit $PHG(k-1, \mathbb{Z}_4)$ bezeichnet.
- Beispiel einer endlichen projektiven Hjelmslev Geometrie.

Hjelmslev Geometrie

- statt endlicher Körper: Ring $\mathbb{Z}_4 := \mathbb{Z}/4\mathbb{Z}$.
- Die projektive Geometrie der freien Untermoduln von $\mathbb{Z}_4^k$ wird mit $PHG(k-1, \mathbb{Z}_4)$ bezeichnet.
- Beispiel einer endlichen projektiven Hjelmslev Geometrie.
- Allgemeiner funktioniert dies für Kettenringe, d.h. Ringe deren Idealverband eine Kette bildet.

Hjelmslev Geometrie und Codierungstheorie

- Der Nordstrom-Robinson Code ist das bekannteste Beispiel eines binären nicht-linearen Codes, der besser (höhere Minimaldistanz bei gleicher Länge und Größe) ist, als es mit linearen Codes erreicht werden kann.

Hjelmslev Geometrie und Codierungstheorie

- Man erhält ihn als Bild des $\mathbb{Z}_4-$Codes mit der Generatormatrix

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 2 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 2 & 1 & 3 \\ 0 & 0 & 1 & 0 & 1 & 3 & 2 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 3 & 2 \end{array}\right)$$

unter der Gray Abbildung
$(0 \mapsto 00, 1 \mapsto 01, 2 \mapsto 11, 3 \mapsto 10)$.

Hjelmslev Geometrie und Codierungstheorie

- Man erhält ihn als Bild des $\mathbb{Z}_4-$Codes mit der Generatormatrix

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 2 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 2 & 1 & 3 \\ 0 & 0 & 1 & 0 & 1 & 3 & 2 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 3 & 2 \end{array}\right)$$

  unter der Gray Abbildung
  $(0 \mapsto 00, 1 \mapsto 01, 2 \mapsto 11, 3 \mapsto 10)$.

- Im Allgemeinen auch nicht freie Zeilen und Spalten.

Hjelmslev Geometrie und Codierungstheorie

Das Zusammenspiel von Geometrie und Codierungstheorie ist nicht mehr so direkt.

Hjelmslev Geometrie und Codierungstheorie

Das Zusammenspiel von Geometrie und Codierungstheorie ist nicht mehr so direkt.

- Geometrie: einige bekannte geometrische Konstruktionen aus $PG(k-1,q)$ funktionieren auch in $PHG(k-1,R)$ wenn R ein beliebiger Kettenring ist.

Hjelmslev Geometrie und Codierungstheorie

Das Zusammenspiel von Geometrie und Codierungstheorie ist nicht mehr so direkt.

- Geometrie: einige bekannte geometrische Konstruktionen aus $PG(k-1,q)$ funktionieren auch in $PHG(k-1,R)$ wenn R ein beliebiger Kettenring ist.
- Codierungstheorie: neben dem Hamming-Gewicht weitere Gewichte (z.B. Lee-Gewicht) wichtig. Was ist die richtige Definition der Äquivalenz?

- Sicherheit von S-Boxen

- Sicherheit von S-Boxen
- Eine boolesche Funktion $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$ heißt APN (almost perfect nonlinear) falls für alle $a \in \mathbb{F}_2^m \setminus \{0\}$ und alle $b \in \mathbb{F}_2^n$ gilt:

$$|\{x \in \mathbb{F}_2^m : f(x+a) - f(x) = b\}| \leq 2.$$

- Sicherheit von S-Boxen
- Eine boolesche Funktion $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$ heißt APN (almost perfect nonlinear) falls für alle $a \in \mathbb{F}_2^m \setminus \{0\}$ und alle $b \in \mathbb{F}_2^n$ gilt:

$$|\{x \in \mathbb{F}_2^m : f(x+a) - f(x) = b\}| \leq 2.$$

- Dies ist eine Eigenschaft, die Angriffe (differential cryptanalysis) erschwert.

- Man erhält eine Generatormatrix $\Gamma(f)$ eines linearen $[2^m, m+n]_2$-Codes indem man pro Spalte Urbild x^T und Bild $f(x)^T$ notiert.

Inzidenzgeometrie und Kryptographie

- Man erhält eine Generatormatrix $\Gamma(f)$ eines linearen $[2^m, m+n]_2$-Codes indem man pro Spalte Urbild x^T und Bild $f(x)^T$ notiert.
- APN kann als Eigenschaft des Codes zu $\Gamma(f)$ definiert werden.

Inzidenzgeometrie und Kryptographie

- Man erhält eine Generatormatrix $\Gamma(f)$ eines linearen $[2^m, m+n]_2$-Codes indem man pro Spalte Urbild x^T und Bild $f(x)^T$ notiert.
- APN kann als Eigenschaft des Codes zu $\Gamma(f)$ definiert werden.
- Verbindung zur endlichen Geometrie.

Inzidenzgeometrie und Kryptographie

- Man erhält eine Generatormatrix $\Gamma(f)$ eines linearen $[2^m, m+n]_2$-Codes indem man pro Spalte Urbild x^T und Bild $f(x)^T$ notiert.
- APN kann als Eigenschaft des Codes zu $\Gamma(f)$ definiert werden.
- Verbindung zur endlichen Geometrie.
- Normalform (bzgl CCZ-Äquivalenz) und Klassifikation von APN Funktionen.