

Fehlerkorrigierende Codes mit Expandergraphen

Daniel Hoske

Seminar Expandergraphen

18. Juli 2011

- Modell: Sende Element aus endlicher Menge M über einen gestörten Kanal, der Binärwörter der Länge n übertragen kann ($2^n \geq |M|$)
- Vereinfachung: Im Kanal kann eine Maximalzahl an Bitfehlern auftreten
- Lösung: Bestimme injektive Kodierungsabbildung $\varphi : M \rightarrow \mathbb{F}_2^n$ und eine dazu linksinverse Dekodierungsabbildung $\psi : \mathbb{F}_2^n \rightarrow M$, so dass ψ jedes gestörte $\varphi(x)$ auf $x \in M$ abbildet. Diese Funktionen sollen effizient berechenbar sein.

- 1 Gute Codes
- 2 Güteschranken
- 3 LDPC-Codes mit Expandergraphen

Gliederung

1 Gute Codes

2 Güteschranken

3 LDPC-Codes mit Expandergraphen

Codes

Definition 1

Eine Teilmenge $C \subseteq \mathbb{F}_2^n$ heißt **Code**.

Bemerkung 2

- 1 Es gibt $\binom{2^n}{|C|}$ verschiedene Codes. Im Allgemeinen werden also exponentiell viele Bits in n zu ihrer Darstellung benötigt.
- 2 Im Folgenden sei $d(x, y) := |\{i \in \{1, \dots, n\} : x_i \neq y_i\}| = |x - y|_1$ die **Hammingdistanz**.
- 3 Natürliche Dekodierung eines Wortes $y \in \mathbb{F}_2^n$: Wähle ein Codewort $x \in C$ mit $d(x, y) = \min\{d(z, y) : z \in C\}$.

Güte von Codes

Definition 3

Die Zahl $\text{dist}(C) := \min\{d(x, y) : x, y \in C, x \neq y\}$ heißt **Distanz** von C .
Durch Normalisierung $\delta(C) := \text{dist}(C)/n$ erhält man die **normalisierte Distanz**.

Die **Rate** von C ist $\text{rate}(C) := (\log_2 |C|)/n$.

Bemerkung 4

- 1 Beide Gütemaße sollen möglichst groß sein.
- 2 Mit einem Code von Distanz d können maximal $\lfloor \frac{d-1}{2} \rfloor$ Bitfehler korrigiert und weniger als d Bitfehler erkannt werden.

Gute Codes

Definition 5

Eine Familie $(C_n)_{n \in \mathbb{N}}$ von Codes mit $C_n \subseteq \{0, 1\}^n$ ist **asymptotisch gut**, falls es Konstanten $r > 0$ und $\delta > 0$ gibt, so dass $\text{dist}(C_n) > \delta n$ und $\text{rate}(C_n) > r$ gilt. Sie heißt **effizient**, falls die Kodierung und die Dekodierung in polynomialer Zeit in n möglich sind.

Linear Codes (1)

Definition 6

Ein Untervektorraum C von \mathbb{F}_2^n heißt ein **linearer Code**.

Bemerkung 7

- 1 Ein linearer Unterraum C der Dimension k kann durch $C = \text{bild } G = \text{kern } H$ für ein $G \in \mathbb{F}_2^{n \times k}$, $H \in \mathbb{F}_2^{(n-k) \times n}$ dargestellt werden. Die Matrix G heißt **Generatormatrix** und H ist die **Prüfmatrix**.
- 2 In einem linearen Code ist die Distanz die minimale Anzahl der Einsen eines Nicht-Nullvektors und deshalb die minimale Anzahl linear abhängiger Spalten der Prüfmatrix.

Linear Codes (2)

Bemerkung 8

- 1 Kodierung von $x \in \mathbb{F}_2^k$: Berechne Gx in $\mathcal{O}(n^2)$.
- 2 Dekodierung von $y \in \mathbb{F}_2^n$: \mathcal{NP} -hart.
- 3 Ist $y \in \mathbb{F}_2^n$ ein Codewort? Prüfe $Hy = 0$ in $\mathcal{O}(n^2)$.

Gliederung

1 Gute Codes

2 Güteschranken

3 LDPC-Codes mit Expandergraphen

Notation

- Im Folgenden sei $B_r(x) := \{y \in \{0, 1\}^n : d(x, y) \leq r\}$ der abgeschlossene Ball vom Radius $r > 0$ um $x \in \mathbb{F}_2^n$.
- Es gilt $|B_r(x)| = \sum_{i=0}^r \binom{n}{i} =: v(r)$
- $H(\delta) = -\delta \log(\delta) - (1 - \delta) \log(1 - \delta)$ ist die binäre Entropiefunktion für $\delta \in [0, 1]$.

Die Gilbert-Varshamov Schranke

Satz 9 (Gilbert-Varshamov)

Für jedes n gibt es einen (sogar linearen) Code mit Distanz $\geq d$ und der Kardinalität $\geq 2^n/v(d)$.

Satz 10 (Gilbert-Varshamov asymptotisch)

Für jedes $\delta \leq 1/2$ gibt es einen linearen Code mit normalisierter Distanz $\geq \delta$ und Rate $r \geq 1 - H(\delta)$

Kugelpackungen und eine obere Schranke

Satz 11 (Kugelpackung)

Jeder Code C der Länge n und der Distanz d erfüllt $|C| \leq 2^n / v(\lfloor (d-1)/2 \rfloor)$.

Satz 12 (Kugelpackung asymptotisch)

Für große n hat jeder Code C der Länge n mit relativer Distanz δ eine Rate $r \leq 1 - H(\delta/2)$.

Graphische Darstellung

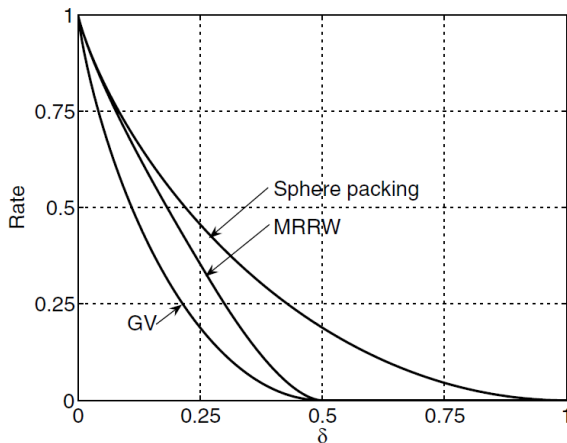


Abbildung: Asymptotische Schranken von Distanz und Rate

Gliederung

- 1 Gute Codes
- 2 Güteschranken
- 3 LDPC-Codes mit Expandergraphen**

Matrizen und Graphen

Definition 13

Sei $A \in \mathbb{F}_2^{m \times n} = (a_{ij})$ eine Matrix. Der bipartite Graph $G(A) = (V, E)$ mit $V = V_L + V_R$, $V_L := \{c_1, \dots, c_n\}$, $V_R := \{r_1, \dots, r_m\}$ und $\{r_i, c_j\} \in E \Leftrightarrow a_{ij} = 1$ für $i \in \{1, \dots, m\}$, $j \in \{1, \dots, n\}$ ist der **zu A gehörige Graph**. Falls umgekehrt G ein bipartiter Graph ist, wird die durch Umkehrung der Konstruktion (bei einer Nummerierung der Knoten) entstehende Matrix mit $A(G)$ bezeichnet und $C(G) := \ker A(G)$ ist der Code, der $A(G)$ als Prüfmatrix hat.

- Solche aus dünnen bipartiten Graphen konstruierte Codes heißen **(Low-Density Parity-Check)-Codes (LDPC-Codes)**.

Codes aus magischen Graphen

Definition

Sei $G = (V_L + V_R, E)$ ein bipartiter, k -regulärer Graph. Dann heißt G ein $(n, m; k)$ -magischer Graph, falls folgende Eigenschaften gelten:

- 1 $|V_L| = n, |V_R| = m$
- 2 $|\Gamma(S)| \geq \frac{5k}{8}|S|$ für $S \subseteq V_L, |S| \leq \frac{n}{10k}$
- 3 $|\Gamma(S)| \geq |S|$ für $S \subseteq V_L, \frac{n}{10k} < |S| \leq \frac{n}{2}$

Satz 14

Sei G ein $(n, (3/4)n; k)$ -magischer Graph. Dann ist $C(G)$ ein Code mit Rate $r \geq 1/4$ und Distanz $d \geq 1/(10k)$.

Erinnerung (1)

Definition (Definition 10.3)

Sei $G = (V_L + V_R, E)$ ein bipartiter Graph mit $|V_L| = l$ und $|V_R| = r$, der links (in V_L) k -regulär ist. Die **linke Knotenexpansion** $L(G, d)$ ist als $L(G, d) := \min\{|\Gamma(S)|/|S| : S \subseteq V_L, S \neq \emptyset, |S| \leq d\}$ definiert.

Der Graph G heißt ein (d, ϵ) -**verlustfreier Expander**, falls $L(G, d) \geq (1 - \epsilon)k$ gilt.

Erinnerung (2)

Satz (Theorem 10.4)

Für jedes $\epsilon > 0$ und $r \leq l$ gibt es einen expliziten links- k -regulären bipartiten Graphen mit l linken und r rechten Knoten, der ein $(\Omega(\epsilon r/k), \epsilon)$ -verlustfreier Expander ist. Dabei gilt $k \leq (l/\epsilon r)^c$ für eine feste Konstante c .

Lemma 15

Im Fall $r = \Omega(l)$ und $\epsilon := 0.01$ muss in Theorem 10.4 der Grad k auch durch eine Konstante beschränkt sein. Der Satz liefert dann eine explizite Familie von bipartiten Graphen G mit $L(G, d) > 0.99k$, $d = \Omega(l)$. Insbesondere kann r so gewählt werden, dass $\frac{l-r}{r} \geq C_1$ und $\frac{d}{l} \geq C_2$ für $C_1, C_2 > 0$ gilt.

Codes aus verlustfreien Expandern (1)

Satz 16 (Sipser-Spielman)

Sei G ein k -links-regulärer bipartiter Graph. Falls $L(G, d) > k/2$ ist, dann gilt $\text{dist}(C(G)) > d$.

Codes aus verlustfreien Expandern (2)

Bemerkung 17

Ansatz für eine naive Dekodierung mit einer Prüfmatrix A :

Ein Wort $y \in \mathbb{F}_2^n$ ist „näher“ als $x \notin C$ an C , falls $|Ay| < |Ax|$ gilt. Von x aus kann man sich also lokal verbessern, indem man ein $i \in \{1, \dots, n\}$ so sucht, dass x nach Flippen des i -ten Bits besser ist, d.h. $|A(x + e_i)| < |Ax|$.

Satz 18 (Sipser-Spielman)

Sei G ein k -links-regulärer bipartiter Graph mit n linken Knoten sowie $L(G, d) > (3/4)k$ und $y \in \mathbb{F}_2^n$ ein String, der weniger als $\lfloor (d-1)/2 \rfloor$ von einem Codewort x entfernt ist. Dann liefert die naive Dekodierung das Wort x nach einer linearen Anzahl von Schritten. Insgesamt kann also in $\mathcal{O}(kn^2)$ dekodiert werden.

Hauptsatz

Satz 19 (Hauptsatz des Vortrags)

Es gibt eine explizit konstruierbare Familie verlustfreier Expandergraphen, deren zugehörige Codefamilie asymptotisch gut und effizient ist.

Vielen Dank für Eure Aufmerksamkeit.