Fehlerkorrigierende Codes mit Expandergraphen

Daniel Hoske, 18. Juli 2011, im Seminar Expandergraphen

1 Gute Codes

Definition 1. Eine Teilmenge $C \subseteq \mathbb{F}_2^n$ heißt **Code**.

Bemerkung 2.

2. Im Folgenden sei $d(x,y) := |\{i \in \{1,\dots,n\} : x_i \neq y_i\}|$ die **Hammingdistanz**.
3. Natürliche Dekodierung von y: Wähle ein $x \in C$ mit $d(x,y) = \min\{d(z,y) : z \in C\}$.

Definition 3. Die Zahl $\operatorname{dist}(C) := \min\{d(x,y) : x,y \in C, x \neq y\}$ heißt **Distanz** von C. Durch Normalisierung $\delta(C) := \operatorname{dist}(C)/n$ erhält man die **normalisierte Distanz**.
Die **Rate** von C ist $\operatorname{rate}(C) := (\log_2 |C|)/n$.

Bemerkung 4.

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

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 $\operatorname{dist}(C_n) > \delta n$ und $\operatorname{rate}(C_n) > r$ gilt. Sie heißt **effizient**, falls die Kodierung und die Dekodierung in polynomialer Zeit in n möglich sind.

Definition 6. Ein Untervektorraum C von $\mathbb{F}_2^n$ heißt ein **linearer Code**.

Bemerkung 7.

- Ein linearer Unterraum C der Dimension k kann durch $C = \operatorname{bild} G = \operatorname{kern} H$ 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**.
- 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.

Bemerkung 8.

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

2 Güteschranken

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 $\delta \in [0,1]$.

Satz 9 (Gilbert-Varshamov). Für jedes n gibt es einen (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 $r \geq 1 - H(\delta)$

Satz 11 (Kugelpackung). Jeder Code C der Länge n und der Distanz d erfüllt die Ungleichung $|C| \leq 2^n / v(\lfloor (d-1)/2 \rfloor)$.

Satz 12 (Kugelpackung asymptotisch). Für große n hat jeder Code C der Länge n mit relativer Distanz δ eine Rate $r \leq 1 - H(\delta/2)$.

3 LDPC-Codes mit Expandergraphen

Definition 13. Sei $A \in \mathbb{F}_2^{m \times n} = (a_{ij})$ eine Matrix. Der bipartite Graph $G(A) = (V, E)$ mit $V = V_L + V_R$, $V_L := \{c_1, \ldots, c_n\}$, $V_R := \{r_1, \ldots, r_m\}$ und $\{r_i, c_j\} \in E \Leftrightarrow a_{ij} = 1$ für $i \in \{1, \ldots, m\}, j \in \{1, \ldots, n\}$ 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 $C(G) := \operatorname{kern} A(G)$ ist der Code, der $A(G)$ als Prüfmatrix hat.

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.

Satz 16 (Sipser-Spielman). Sei G ein k-links-regulärer bipartiter Graph. Falls $L(G,d) > k/2$ ist, dann gilt $\operatorname{dist}(C(G)) > d$.

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 $i \in \{1, \ldots, n\}$ 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.

Satz 19 (Hauptsatz des Vortrags). Es gibt eine explizit konstruierbare Familie verlustfreier Expandergraphen, deren zugehörige Codefamilie asymptotisch gut und effizient ist.