

RAMANUJAN GRAPHEN IN DER KOMMUNIKATION

ALEXANDER SALLE

1. GRUNDLEGENDE DEFINITIONEN

Definition 1. Sei $G = (V, E)$ ein nicht-leerer Graph.

- Der *Grad* einer Ecke v ist d_v , die Anzahl aller abgehenden Kanten.
- Eine Ecke vom Grad 0 heißt *isoliert*.
- Hat jede Ecke von G den gleichen Grad, so heißt G *k-regulär*.

Definition 2. Sind je zwei Ecken $v \in G$ benachbart (adjazent), so heißt G *vollständig*. Die *Menge der Nachbarn* einer Ecke v bezeichnet man mit $N(v)$. Sei $U \subset V(G)$. Dann ist $N(U)$ die Menge der Nachbarn aller $u \in U$.

Definition 3. Ein Graph heißt *zusammenhängend*, wenn es zwischen je zwei seiner Ecken einen Weg gibt (d.h., wenn alle Ecken über Wege mit einander verbunden sind).

Definition 4. Für eine Teilmenge $S \subset V(G)$ ist

$$vol(S) := \sum_{x \in S} d_x$$

Die *Ecken-Grenze* $\delta(S)$ ist definiert als

$$\delta(S) := N(S) - S = \{x \in V \setminus S \mid x \sim y \in S\}$$

Bemerkung. $\delta(S)$ ist die Menge der Ecken, die direkt an S liegen, d.h. durch eine Kante mit einem Punkt $s \in S$ verbunden sind.

Definition 5. Für $S \subset V(G)$ ist das *Komplement* notiert mit $\bar{S} = V(G) - S$

2. EXPANDER-GRAPHEN

Erinnerung. Aus vorherigen Vorträgen ist bekannt:

- Falls $\Delta f = \lambda f$ und $f \neq 0$, dann heißt λ *Eigenwert* von Δ und f *Eigenvektor* (Eigenfunktion).
- Da Δ symmetrisch und linear in einem euklidischen Vektorraum V ist, existiert eine Orthonormalbasis aus Eigenvektoren.
- Außerdem gibt es $\dim(V)$ Eigenwerte, diese sind alle reell ($\lambda_0 = 0$ ist immer Eigenwert).
- Man ordnet die Eigenwerte der Größe nach:

$$\lambda_0 \leq \lambda_1 \leq \dots \leq \lambda_{n-1} \quad n = \dim(V)$$

Dies nennt man das *Spektrum von G* .

Definition 6. Sei $G = (V, E)$ ein k -regulärer Graph auf n Ecken. Man nennt G einen (n, k, c) -*Expander*, falls für jede Teilmenge $S \subseteq V(G)$ gilt:

$$|\delta(S)| \geq c \left(1 - \frac{|S|}{n}\right) |S|$$

c heißt *Expander-Koeffizient*.

Bemerkung. Man kann auch alternativ den Expansions-Faktors definieren, und gelangt so zu einer etwas veränderten Ansicht der Expander.

Definition 7. Der *Expansions-Faktor* c' ist definiert als

$$c' = \sup_{S \subseteq V(G)} \frac{|\delta(S)|}{\left(\frac{|S| \cdot |\bar{S}|}{n}\right)}$$

Bemerkung. Der Expansions-Faktor hängt mit der Cheeger-Konstante zusammen, genauer mit

$$g_G = \inf_S \frac{\text{vol}(\delta(S))}{\min(\text{vol}(S), \text{vol}(\bar{S}))}$$

Aus diesem Zusammenhang formuliert man für $|\delta(S)|$ Kriterien, ob ein bestimmter Graph ein Expander ist. Dazu betrachtet man das Spektrum von G .

Lemma 2.1. Sei $G = (V, E)$ und $S \subseteq V(G)$. Die Ecken-Grenze $\delta(S)$ erfüllt die Ungleichung:

$$\begin{aligned} \frac{\text{vol}(\delta(S))}{\text{vol}(S)} &\geq \frac{\lambda(2 - \lambda) \frac{\text{vol}(\bar{S})}{\text{vol}(G)}}{1 - \lambda(2 - \lambda) \frac{\text{vol}(\bar{S})}{\text{vol}(G)}} \\ &\geq \lambda(2 - \lambda) \frac{\text{vol}(\bar{S})}{\text{vol}(G)} \end{aligned}$$

mit $\lambda = \frac{2\lambda_1}{\lambda_{n-1} + \lambda_1}$, d.h. G ist ein $(n, k, \lambda(2 - \lambda))$ -Expander.

Beweis. Wir verwenden folgendes Hilfslemma aus dem Vortrag Eigenvalues (evtl.):

Lemma 2.2. Für alle $S \subseteq V(G)$ ist

$$\frac{\text{vol}(\delta(S))}{\text{vol}(S)} \geq \frac{1 - (1 - \lambda)^2}{(1 - \lambda)^2 \cdot \frac{\text{vol}(S)}{\text{vol}(G)}}$$

mit λ wie oben.

Damit ist

$$\begin{aligned}
\frac{\text{vol}(\delta(S))}{\text{vol}(S)} &\geq \frac{1 - (1 - \lambda)^2}{(1 - \lambda)^2 \cdot \frac{\text{vol}(S)}{\text{vol}(\bar{S})}} = \frac{1 - (1 - 2\lambda + \lambda^2)}{\frac{(1 - \lambda)^2 \cdot \text{vol}(\bar{S}) + \text{vol}(S)}{\text{vol}(S)}} \\
&= \frac{(2\lambda - \lambda^2) \text{vol}(\bar{S})}{(1 - \lambda)^2 \cdot \text{vol}(\bar{S}) + \text{vol}(S)} \\
&= \frac{\lambda(2 - \lambda) \frac{\text{vol}(\bar{S})}{\text{vol}(G)}}{1 - \lambda(2 - \lambda) \cdot \frac{\text{vol}(\bar{S})}{\text{vol}(G)}}
\end{aligned}$$

Wenn wir nun zeigen, dass der Nenner kleiner 1 ist, dann ist die Behauptung gezeigt. Dies ist aber der Fall, da

$$\begin{aligned}
1 - \lambda(2 - \lambda) \cdot \frac{\text{vol}(\bar{S})}{\text{vol}(G)} &\geq 1 - \lambda(2 - \lambda) \cdot 1 \\
&= 1 - \left(\frac{2\lambda_1}{\lambda_{n-1} + \lambda_1} \cdot \frac{2\lambda_{n-1}}{\lambda_{n-1} + \lambda_1} \right) \\
&= \frac{(\lambda_{n-1} - \lambda_1)^2}{(\lambda_{n-1} + \lambda_1)^2} \geq 1,
\end{aligned}$$

denn nach Voraussetzung ist $\lambda_{n-1} \geq \lambda_1 > 0$ und somit folgt die Behauptung. $\square$

3. EXPLIZITE KONSTRUKTIONEN

Definition 8. Die *explizite Konstruktion* eines Graphen auf n Ecken ist ein Algorithmus, der nach m Schritten abbricht, wobei m polynomial in n ist.

Definition 9. Sei p ungerade Primzahl, sei $a \in \mathbb{Z}$ mit $(a, p) = 1$. Dann ist das *Legendre-Symbol*:

$$\left(\frac{a}{p} \right) = \begin{cases} +1 & a \text{ quadratischer Rest modulo } p \\ -1 & a \text{ kein quadratischer Rest modulo } p \end{cases}$$

Konstruktion 1. Wir konstruieren den *Paley-Graph* P_p mit p prim und $p \equiv 1 \pmod{4}$. Die Eckenmenge $V = \{0, 1, 2, \dots, p-1\}$. Für die Kanten gilt $i \sim j \Leftrightarrow i - j \neq 0$ und $\left(\frac{i-j}{p} \right) = 1$.

Die Eigenwerte von P_p sind

$$\frac{1 - \left(\sum_{x \in (\mathbb{Z}/p\mathbb{Z})^*} e^{\frac{2\pi i j x^2}{p}} \right)}{p - 1}$$

mit $j = 0, \dots, p-1$. Insbesondere sind

$$\lambda_1 = 1 - \frac{\sqrt{p}-1}{2(p-1)}$$

$$\lambda_{n-1} = 1 - \frac{\sqrt{p}+1}{2(p-1)}$$

Mit dem λ aus dem Satz bestimmt man c für die Expander-Eigenschaft.

Beispiel. Wir konstruieren den Paley-Graphen P_{13} . Dazu ordnet man zuerst die Ecken passend an. Da $\left(\frac{1}{p}\right) = 1$ gilt für n und $n-1$ (mit $n = 0, \dots, 12$) stets $n \sim n-1$. Daher ist der 'äußere Ring' geschlossen. Die Quadrate in $\mathbb{Z}/13\mathbb{Z}$ sind $\{\bar{1}, \bar{3}, \bar{4}, \bar{9}, \bar{10}, \bar{12}\}$

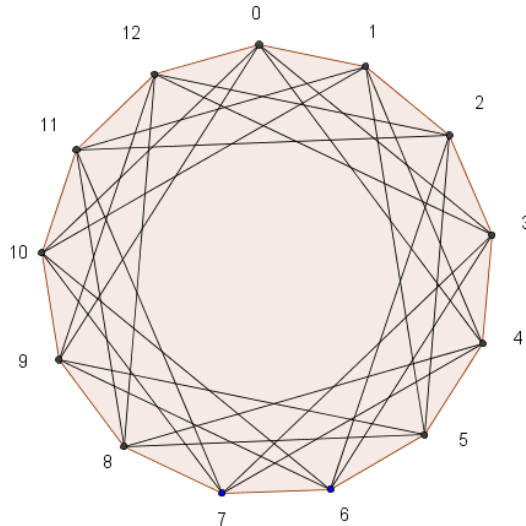


ABBILDUNG 1. Der Paley-Graph P_{13}

Definition 10. Ein Graph G heißt *bipartit*, wenn es Mengen $X, Y \subseteq V(G)$ gibt mit $X \cup Y = G$ und $X \cap Y = \emptyset$, so daß eine Endecke jeder Kante von G in X und andere Endecke in Y liegt.

Definition 11. Die *projektive Gruppe* $\text{PGL}(n, K)$ ist der Quotient

$$\text{PGL}(n, K) = \text{GL}(n, K) / \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}, \lambda \neq 0 \right\}.$$

Die *spezielle projektive Gruppe* $\text{PSL}(n, K)$ ist der Quotient

$$\text{PSL}(n, K) = \text{SL}(n, K) / \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, -\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}.$$

Konstruktion 2. *Ramanujan-Graphen* sind k -reguläre Graphen, deren Eigenwert λ_1 die folgende Ungleichung erfüllt:

$$\lambda_1 \geq 1 - \frac{2\sqrt{k-1}}{k}.$$

Sie sind von den Eigenwerten optimal für die Expander-Eigenschaft. Diese hängt (beispielsweise wie in Lemma 2.1) mit dem Spektrum des Graphen zusammen.

Definition 12. Der *Cayley-Graph* einer Gruppe G relativ zu einer Erzeugermenge S ist der Graph auf den Ecken $g \in G$ und den Kanten $\{x, y\}$, falls $x = sy$ für ein $s \in S$.

Seien p, q prim und $p, q \equiv 1 \pmod{4}$. Sei i eine ganze Zahl mit $i^2 \equiv -1 \pmod{q}$. (Diese existiert, da -1 genau dann ein Quadrat modulo q ist, wenn $q \equiv 1 \pmod{4}$.)

Betrachte nun $\alpha = (a_0, a_1, a_2, a_3)$ und die Gleichung

$$a_0^2 + a_1^2 + a_2^2 + a_3^2 = p.$$

Es gibt genau $p+1$ Lösungen α , so dass a_0 ungerade, $a_0 > 0$ und a_j gerade für $j = 1, 2, 3$. Man assoziiert die α mit den zugeordneten Matrizen $\tilde{\alpha} \in \text{PGL}(2, \mathbb{Z}/q\mathbb{Z})$:

$$\tilde{\alpha} = \begin{pmatrix} a_0 + ia_1 & a_2 + ia_3 \\ -a_2 + ia_3 & a_0 - ia_1 \end{pmatrix}$$

Jetzt bildet man den Cayley-Graphen von $\text{PGL}(2, \mathbb{Z}/q\mathbb{Z})$ relativ zu der Menge der $\tilde{\alpha}$. Dies ist ein $p+1$ -regulärer Graph. Es gibt zwei Fälle für den Ramanujan-Graphen:

$$\left(\frac{a}{p}\right) = -1.$$

Dann ist $X^{p,q}$ gleich dem obigen Cayley-Graphen. Außerdem ist $X^{p,q}$ bipartit und zusammenhängend. Die Partition der Eckenmenge ist gegeben durch $(\text{PSL}(2, \mathbb{Z}/q\mathbb{Z}), \overline{\text{PSL}(2, \mathbb{Z}/q\mathbb{Z})})$ und die Eckenanzahl ist $n = q(q^2 - 1)$.

$$\left(\frac{a}{p}\right) = 1.$$

Dann ist $X^{p,q}$ der Cayley-Graph von $\text{PSL}(2, \mathbb{Z}/q\mathbb{Z})$. Dieser ist weder bipartit noch zusammenhängend. Die Eckenanzahl ist $n = \frac{q(q^2-1)}{2}$.

Beispiel. In Abb. 2 ist der 3-reguläre Ramanujan-Graph auf 80 Ecken dargestellt. Er hat einen Expansionsfaktor von $c' = \frac{1}{4}$.

4. ANWENDUNGEN IN DER KOMMUNIKATION

Definition 13. Ein *gerichteter Graph* ist ein Graph G , dessen Kanten jede einen Anfangs- und einen Endpunkt zugewiesen bekommt.

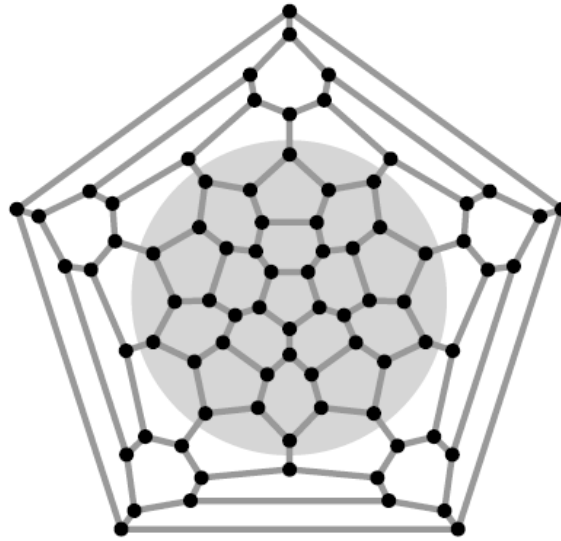


ABBILDUNG 2. Ramanujan Graph (www.ams.org)

Definition 14. Ein *non-blocking-network* ist ein gerichteter Graph G mit zwei disjunkten Teilmengen $X, Y \subseteq V(G)$, wobei X die *Eingangsmenge* und Y die *Ausgangsmenge* ist.

Definition 15. Ein *k-access Graph* hat für jede Teilmenge S von Ecken-disjunkten Pfaden zwischen Ein- und Ausgängen die Eigenschaft, einen neuen Eingang auf k schicken zu können. Dabei benutzt er keine Ecke aus S für den Weg. Ist $k \geq \frac{|Y|}{2}$, so heißt der *k-access Graph* *major-access-network*.

Konstruktion 3. Betrachte den Graphen $M(n)$ mit n Eingängen und $24n$ Ausgängen. $M(n)$ besteht aus zwei Kopien eines major-access-network $M(\frac{n}{2})$ und zwei Kopien des bipartiten Ramanujan-Graphen, notiert mit $R(12n, 5)$, d.h. mit $12n$ Eingängen und Grad $p + 1 = 6$. Im

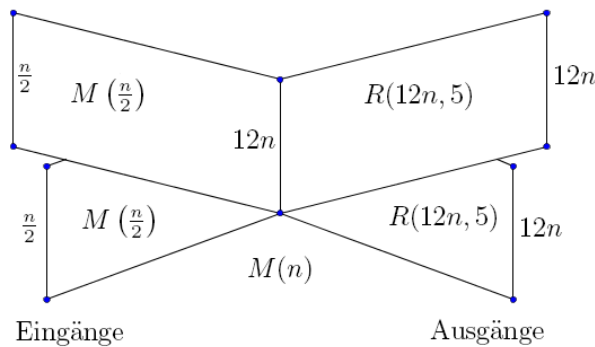


ABBILDUNG 3. Das Netzwerk $M(n)$

bipartiten $R(12n, 5)$ ist $q(q^2 - 1) \equiv 0 \pmod{24}$. Wir zeigen jetzt, dass $M(n)$, tatsächlich ein major-access-network ist.

Jeder Eingang v hat nach Konstruktion Zugang zu $6n$ der mittleren Ecken. Nun sei S die Menge der bereits 'besetzten' Ecken der mittleren Ecken, dies sind maximal n . Also bleiben noch $5n$ 'unbesetzte' Eingänge.

Lemma 4.1. *Für einen bipartiten Graphen G mit Eckenmenge $X \cup Y$ und Kanten zwischen X und Y mit $d_x = k$ für alle $x \in X$.*

Für $S' \subseteq X$ erfüllt die Nachbarschaft $N(S)$:

$$\frac{|N(S')|}{|S'|} \geq \frac{1}{\rho^2 + (1 - \rho^2) \cdot \frac{|S'|}{n}}$$

mit ρ^2 spezielle Eigenwerte der Matrix für bipartite Graphen.

Damit können wir die Nachbarschaft $N(S)$ für die oben definierte Menge S berechnen:

$$\begin{aligned} |N(S)| &\geq \frac{5n}{(1 - \lambda)^2 + \frac{5n}{12n} \cdot (1 - (1 - \lambda)^2)} \\ &= \frac{5n}{(1 - \lambda)^2 + \frac{5}{12} \cdot (1 - 1 + 2\lambda + \lambda^2)} \\ &= \frac{5n}{(1 - \lambda)^2 + \frac{5}{12} \cdot \lambda(2 - \lambda)} \end{aligned}$$

Für den Ramanujan-Graphen ist der Grad $k = p+1 = 6$ und $\lambda = 1 - \frac{\sqrt{5}}{3}$. Dies berechnet sich mit $\lambda_1 = 1 - \frac{2\sqrt{5}}{6} = 1 - \frac{\sqrt{5}}{3}$. Damit gilt

$$\frac{5n}{\frac{5}{9} + \left(1 - \frac{5}{9}\right) \cdot \frac{5}{12}} = \frac{27n}{4}.$$

Weil es zwei der $R(12n, 5)$ gibt, hat die Teilmenge S mindestens $\frac{27n}{2}$ Nachbarn bzw. Ausgänge. Da nach Voraussetzung maximal n Ausgänge besetzt sind, liegen mindestens $\frac{25n}{2}$ der Ecken nicht in S . Aber dies sind mehr als die Hälfte der $24n$ Gesamtausgänge.

Somit ist $M(n)$ ein major-access-network.

LITERATUR

- [1] F.Chung, *Spectral Graph Theory*, University of California, San Diego, La Jolla, revised 2006.
- [2] Lubotzky, Phillips, Sarnak, *Spectral Graph Theory*, in *Combinatorica* 8, Springer-Verlag, 1988.
- [3] P.Bachmann, *Niedere Zahlentheorie*, Erster Teil, Chelsea Publishing Company, Bronx, New York, 1968.
- [4] P.Sarnak, *What is an Expander?*, in *Notices of the AMS*, Volume 51 Nr. 7, <http://www.ams.org/notices/200407/what-is.pdf>, 2004.