Per Austrin

Detta är föreläsningsanteckningar från Jakob Nordströms föreläsning om Expandergrafer, torsdag 24 mars 2005.

1 Introduktion

På en intuitiv nivå är en expandergraf en ”gles men spretig” graf, en graf med relativt få kanter men relativt korta stigar mellan varje par av hörn. Expandergrafer har väldigt många tillämpningsområden. Några av dessa är:

Nätverksdesign Om man är intresserad av att konstruera robusta nätverk, där det finns stigar mellan varje par av noder även om vissa noder försvinner, är expandergrafer lämpliga.

Slumpreduktion av algoritmer Mer om detta i Douglas anteckningar från en av Johans föreläsningar.

Felrättande koder Mer om detta i avsnitt 4.

Icke-approximation Expandergrafer är bl.a. användbara för att visa att det finns en konstant $\delta > 0$ så att överbestämda linjära ekvationssystem över de rationella talen med m ekvationer inte kan approximeras inom m^δ (där måttet är antalet satisfierade ekvationer).

Kryptografi

Beviskomplexitet

2 Notation och definitioner

Så länge inte annat uttryckligen sägs kommer G i dessa anteckningar att beteckna en d-reguljär oriktad graf $G = (V, E)$ med hörnmängd resp. kantmängd $V = V(G), E = E(G)$, där vi även tillåter multipla kanter och öglor (loopar). För en mängd S betecknar $\overline{S} = V(G) \setminus S$ komplementet av S i $V(G)$. Såvida inget annat sägs kommer vi att reservera n för $n = |V(G)|$.

För två (inte nödvändigtvis disjunkta) mängder S, T betecknar vi mängden kanter mellan S och T som

$$E(S,T) = \{\, (u,v) \in E(G) \mid u \in S, v \in T \,\}\,. \tag{1}$$

Definition 1. *Kantranden* av S är kanterna som leder ut från S, d.v.s.

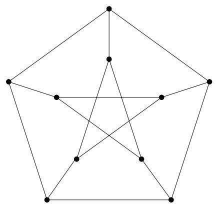
$$\partial S = E(S, \overline{S}). \tag{2}$$

Definition 2. G har *kantexpansion* (δ, ϵ) om

$$\min_{|S| \le \delta n} |\partial S|/|S| \ge \epsilon \tag{3}$$

Med kantexpansionen $h(G)$ för G åsyftar vi maximalt möjligt ϵ för $\delta = 1/2$, d.v.s.

$$h(G) = \min_{|S| \le n/2} |\partial S|/|S|, \tag{4}$$



Figur 1: Petersengrafen

Exempel 1. Den kompletta $(n-1)$-reguljära grafen K_n har kantexpansion $h(K_n) = \lceil n/2 \rceil$.

Exempel 2. Den 3-reguljära *Petersengrafen* (se figur 1) har kantexpansion $h = 1$.

Exempel 3. Den m-reguljära booleska hyperkuben C_m på $n = 2^m$ hörn har också kantexpansion $h(C_m) = 1$.

Exempel 4. Om G inte är sammanhängande gäller $h(G) = 0$.

Det vi är ute efter (expandergrafer), är grafer med hög kantexpansion, men med så få kanter (d.v.s. lågt värde på d) som möjligt.

Definition 3. En *familj av expandergrafer* är en familj $\{G_i\}_{i \in \mathbb{N}}$ av grafer sådan att det finns d och $\epsilon > 0$ sådana att

1. G_i är d-reguljär för alla i.
2. $|V(G_i)| = n_i$ för $n_{i-1} < n_i \leq n_{i-1}^2$, säg.
3. $h(G_i) \geq \epsilon$ för alla i

Observera att vi förvisso i exempel 1 och 3 hade oändliga familjer av grafer med stor kantexpansion, men att gradtalet d inte var konstant.

Definition 4. En familj expandergrafer är *explicit* om varje G_i kan konstrueras i tid polynomiell i n_i (av en deterministisk Turingmaskin).

Definition 5. En familj expandergrafer är *jätteexplicit* (eng. ”very explicit”) om vi i polylogaritmisk tid (med en deterministisk Turingmaskin) i n_i kan beräkna den j:te ($1 \leq j \leq d$) grannen till en godtycklig nod $v \in V(G_i)$.

Exempel 5. Låt $G_i = (V_i, E_i)$ med $V_i = \mathbb{Z}_i \times \mathbb{Z}_i$. Från $[x, y] \in V_i$ drar vi kanter till $[x + y, y]$, $[x - y, y]$, $[x, y + x]$, $[x, y - x]$. Detta är en jättexplicit familj av $d = 4$-reguljära expandergrafer.

Exempel 6. För p primtal, låt $G_p = (V_p, E_p)$ med $V_p = \mathbb{Z}_p^*$. Från $x \in V_p$ drar vi kanter till $x \boxplus 1$, $x \boxminus 1$ och x^{-1}, där operationerna $\boxplus$ och $\boxminus$ är addition och subtraktion i $\mathbb{Z}_{p-1}$ (representerat av talen 1 till $p - 1$) och x^{-1} är inversion. Detta är en jättexplicit familj av $d = 3$-reguljära expandergrafer.

Det är inte jättelätt att inse att dessa exempel faktiskt är expandergrafer.

2.1 Andra mått på expansion

Det sätt på vilket vi hittills definierat ”expansion” för en graf är på intet vis kanoniskt; det finns även andra rimliga sätt. Ett sådant är *hörnexpansionen*. Vi säger att G har hörnexpansion (δ, ϵ) om

$$\min_{|S| \leq \delta |V(G)|} |N(S)|/|S| \geq \epsilon, \tag{5}$$

där $N(S) = \{\, u \mid \text{finns kant från } u \text{ till något hörn i } S \,\}$ är grannarna till S. En viktiga skillnad mot kantexpansionen är att vi i $N(S)$ även inkluderar hörn vi kan nå med hjälp av kanter som går inom S. Detta har som följd att alla d-reguljära grafer har hörnexpansion $\epsilon \geq 1$ för alla δ. En graf med god hörnexpansion har också bra kantexpansion:

Påstående 1. *Om G (d-reguljär) har hörnexpansion $(\delta, 1 + \epsilon)$ så har den kantexpansion (δ, ϵ).*

Bevis. Om $|N(S)| \geq (1 + \epsilon)|S|$ måste S ha kanter till åtminstone $\epsilon|S|$ hörn utanför S, d.v.s. $E(S, \overline{S}) \geq \epsilon|S|$. □

En något svagare koppling från kantexpansion till hörnexpansion ges av:

Påstående 2. *Om G (d-reguljär) har kantexpansion (δ, ϵ), så har G hörnexpansion*

$$\left(\frac{\delta}{2 + \epsilon/d}, 1 + \epsilon/d \right).$$

Bevis. Antag motsatsen, att det finns en mängd $S \subseteq V(G)$ sådan att $|S| \leq \delta/(2+\epsilon/d)|V|$ och $|N(S)| < (1+\epsilon/d)|S|$. Låt $T = S \cup N(S)$ (notera $|S| \leq |T| \leq \delta|V|$. Alla kanter mellan T och $\overline{T}$ måste komma från $N(S)$. Det finns totalt $d \cdot |N(S)| < (d+\epsilon)|S|$ kanter med något hörn i $|N(S)|$, men $d \cdot |S|$ av dem måste ha andra hörnet i S, varför vi får att

$$|E(T, \overline{T})| < (d + \epsilon)|S| - d|S| = \epsilon|S|, \tag{6}$$

med andra ord

$$\frac{E(T, \overline{T})}{|T|} < \epsilon, \tag{7}$$

vilket motsäger att G är en (δ, ϵ)-kantexpander. □

En trevlig användning av hörnexpansion är att visa att en graf har låg diameter (d.v.s. längsta kortaste avstånd mellan två hörn i grafen): om G har hörnexpansion (δ, ϵ) så är det enkelt att visa att diametern av G är högst

$$\frac{2 \log n + \log \delta + \log(1 - \delta)}{\log \epsilon}. \tag{8}$$

Det finns naturligtvis även fler sätt att definiera expansion på, man kan t.ex. tänka sig att definiera hörnexpansionen som minumum av $|N(S) \setminus S|/|S|$ (d.v.s. hur många ”nya” hörn vi kommer till) istället. De flesta (alla?) ”rimliga” sätt att definiera expansion på hänger mer eller mindre ihop (som illustreras av påståendena 1 och 2 ovan), det gäller bara att man tänker sig för lite och är på det klara med vilken definition man använder.

2.2 Lite linjär algebra

Ett viktigt verktyg för att arbeta med expandergrafer är linjär algebra, och i synnerhet grundläggande spektralteori. Vi fräschar upp de grundläggande definitionerna. Låt A och B vara reella $n \times n$-matriser.

Definition 6. Om det finns $\mu \in \mathbb{R}$ och en nollskild vektor v sådan att $Av = \mu v$ kallas μ ett *egenvärde* till A och v är en motsvarande *egenvektor*.

Definition 7. Det *karaktäristiska polynomet* till A är den formella determinanten

$$c_A(x) = \det(xI - A) \tag{9}$$

Egenvärdena till A är precis rötterna till $c_A(x)$.

Definition 8. *Egenrummet* E_μ för egenvärdet μ består av alla egenvektorer v till egenvärdet μ, samt nollvektorn $v = 0$.

Det är enkelt att verifiera att egenrummet E_μ är ett delrum till $\mathbb{R}^n$. Om A är symmetrisk gäller dessutom följande trevliga egenskaper:

- alla rötter till $c_A(x)$ (och därmed alla egenvärden) är reella.
- egenvektorer svarande mot olika egenvärden är linjärt obereonde.
- dimensionen för egenrummet E_μ är multipliciteten för egenvärdet μ.

Definition 9. A och B är *similära* om det finns en inverterbar matris P sådan att $B = P^{-1}AP$.

Definition 10. A är *diagonaliserbar* om den är similär med någon diagonalmatris.

Definition 11. A är *ortogonal* om $A^{-1} = A^T$.

Definition 12. A är *ortogonalt diagonaliserbar* om det finns en ortogonal matris P sådan att $P^{-1}AP$ är en diagonalmatris.

Similära matriser har samma uppsättning egenvärden. Notera att en diagonalmatris har sina egenvärden på diagonalen.

Sats (Reella spektralsatsen)**.** *Låt A vara en reell $n \times n$-matris. Följande villkor är ekvivalenta:*

- *A har en ortonormal mängd egenvektorer (som är en bas för $\mathbb{R}^n$).*
- *A är ortogonalt diagonaliserbar.*
- *A är symmetrisk.*

3 Grannmatriser och egenvärden

Grannmatrisen $A(G)$ för G är en $n \times n$-matris där elementet a_{ij} på rad i kolumn j är antalet kanter mellan i och j. Notera att grannmatrisen är symmetrisk och att den för en d-reguljär graf har varje rad- och kolumnsumma lika med d. Låt $\mu_1 \geq \mu_2 \geq \ldots \geq \mu_n$ vara egenvärdena till $A(G)$. Vi kallar dessa G:s spektrum.

Påstående 3. $\mu_1 = d$.

Bevis. Observera att 1-vektorn är en egenvektor till $A = A(G)$ med motsvarande egenvärde d. Det räcker alltså att visa att alla egenvärden har absolutbelopp begränsat av d. Låt v vara någon egenvektor till A med egenvärde μ. Låt v_i vara den koordinat i v som har högst belopp. Vi har att den i:te koordinaten i $A \cdot v$ uppfyller

$$|\mu v_i| = |(A \cdot v)_i| = \left| \sum_j a_{ij} v_j \right| \leq |v_i| \cdot \sum_j |a_{ij}| = d|v_i| \tag{10}$$

så $|\mu| \leq d$, som önskat. □

Påstående 4. *Multipliciteten för egenvärdet d i $A(G)$ är antalet sammanhängande komponenter i G.*

Bevis. Tag en egenvektor v med motsvarande egenvärde $\mu = d$. Antag utan inskränkning att v har något positivt element (titta på $-v$ annars). Låt $r = \max v_i$, och låt $I = \{\, i \mid v_i = r \,\}$.

För $i \in I$ gäller

$$d \cdot v_i = (A \cdot v)_i = \sum_{j=1}^{n} a_{ij} v_j \leq \sum_{j=1}^{n} a_{ij} r = d \cdot r = d \cdot v_i \tag{11}$$

Sålunda måste likhet gälla i olikheten, m.a.o. måste vi ha $v_j = r$ för alla j så att $a_{ij} \neq 0$. Detta ger att alla kanter från i även har sin andra ändpunkt i I, varför I består av en eller flera sammanhängande komponenter av G.

Låt G bestå av k sammanhängande komponenter $G_1, \ldots, G_k$ av storlek $|V(G_i)| = n_i$. Genom en lämplig numrering av noderna i G kan $A(G)$ skrivas som

$$A = \begin{pmatrix} A_1 & 0 & \ldots & 0 \\ 0 & A_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & A_k \end{pmatrix}, \tag{12}$$

där $A_i = A(G_i)$ är $n_i \times n_i$-grannmatrisen till G_i. I varje A_i har egenvärdet d multiplicitet ett, eftersom den enda uppsättningen sammanhängande komponenter som kan väljas är G_i självt och alla egenvektorer med egenvärde d därmed måste vara multipler av 1-vektorn . Men det karaktäristiska polynomet till A kan skrivas som

$$\det(xI_n - A) = \prod_{i=1}^{k} \det(xI_{n_i} - A_i). \tag{13}$$

Så multipliciteten för egenvärdet d i A är summan av multipliciteterna för d i de olika komponenterna, d.v.s. precis antalet komponenter. □

Påstående 5. *Multipliciteten för egenvärdet $-d$ i $A(G)$ är antalet sammanhängande bipartita komponenter i G.*

Bevis. Antag att $\mu_n = -d$, och tag en motsvarande egenvektor v. I samma anda som det föregående beviset, låt $r = \max |v_i|$, och definiera mängderna $I_L = \{ i \mid v_i = r \}$ och $I_R = \{ i \mid v_i = -r \}$. För $i \in I_L$ har vi

$$-dv_i = (A \cdot v)_i = \sum_{j=1}^{n} a_{ij} v_j \geq \sum_{j=1}^{n} a_{ij} \cdot (-r) = -d \cdot r = -d \cdot v_i \tag{14}$$

På samma sätt som förut måste vi ha likhet i olikheten, och vi inser att alla utgående kanter från i måste ha sin ändpunkt i I_R. På samma sätt inses att utgående kanter från noder i I_R har sin ändpunkt i I_L. Alltså utgör $I_L \cup I_R$ en eller flera bipartita sammanhängande komponenter till G. Resten av beviset är analogt med slutklämmen i föregående bevis. □

Definition 13. *Spektralgapet* för G är $\mu_1 - \mu_2 = d - \mu_2$.

Vi kommer också att vara intresserade av absolutbeloppen av egenvärdena till $A(G)$, och kommer att beteckna dessa som $\lambda_1, \lambda_2, \ldots, \lambda_n$ i fallande storleksordning. Vi har alltså $\lambda_1 = |\mu_1| = d$, $\lambda_2 = \max(|\mu_2|, |\mu_n|)$, och så vidare.

Sats 1. *För en d-reguljär graf G gäller*

$$\frac{d - \mu_2}{2} \leq h(G) \leq \sqrt{2d(d - \mu_2)}, \tag{15}$$

där μ_2 är det näst största egenvärdet till $A(G)$.

Bevis av denna sats (eller liknande) kommer levereras i senare anteckningar av Douglas från en av Johans föreläsningar. Intuitivt säger satsen att grafer där andra egenvärdet är litet har bra expansionsegenskaper.

En annan koppling mellan den näst största egenvärdet och egenskapen att "se slumpvis ut" ges av följande lemma, som säger att ju mindre det näst största egenvärdet är, desto närmare kommer antalet kanter mellan två godtyckliga mängder att vara det förväntade antalet kanter mellan dessa två mängder i en slumpgraf.

Lemma 1. *För alla $S, T \subseteq V(G)$ gäller*

$$\left| |E(S,T)| - \frac{d|S||T|}{n} \right| \leq \lambda_2 \sqrt{|S||T|} \tag{16}$$

Bevis. Låt $A = A(G)$. Vi kan skriva $|E(S,T)|$ som

$$|E(S,T)| = \chi_S^\top A \chi_T, \tag{17}$$

där χ_U är den karaktäristiska vektorn för delmängden U (d.v.s. element i i χ_U är 1 om $i \in U$ och 0 annars). Eftersom A är symmetrisk finns en ortonormal bas $v_1, v_2, \ldots, v_n$ av egenvektorer, där v_i är en egenvektor till μ_i, och se till att välja basen så att $v_1 = (1/\sqrt{n}, 1/\sqrt{n}, \ldots, 1/\sqrt{n})$. Skriv

$$\begin{aligned} \chi_S &= \sum_{i=1}^{n} a_i v_i \\ \chi_T &= \sum_{i=1}^{n} b_i v_i \end{aligned}$$

Vi får

$$A \cdot \chi_T = \sum_{i=1}^{n} b_i A v_i = \sum_{i=1}^{n} b_i \mu_i v_i, \tag{18}$$

vilket ger

$$|E(S,T)| = \chi_S^\top \cdot A \cdot \chi_T = \sum_{i=1}^{n} \sum_{j=1}^{n} a_i b_j \mu_j \cdot (v_i \cdot v_j) = \sum_{i=1}^{n} a_i b_i \mu_i, \tag{19}$$

där vi utnyttjar att $\{v_i\}_{i=1}^n$ är en ortonormal bas, d.v.s. att

$$v_i \cdot v_j = \begin{cases} 1 & \text{om } i = j \\ 0 & \text{om } i \neq j \end{cases} .$$

Vi har $a_1 = \chi_S \cdot v_1 = |S|/\sqrt{n}$, och på samma sätt $b_1 = |T|/\sqrt{n}$. Utnyttjar vi $\mu_1 = d$ får vi

$$|E(S,T)| - \frac{d|S||T|}{n} = \sum_{i=2}^{n} a_i b_i \mu_i \tag{20}$$

Tar vi absolutbelopp på detta får vi

$$\left| |E(S,T)| - \frac{d|S||T|}{n} \right| = \left| \sum_{i=2}^{n} a_i b_i \mu_i \right| \leq \lambda_2 \sum_{i=2}^{n} |a_i| \cdot |b_i|, \tag{21}$$

eftersom $|\mu_i| \leq \lambda_2$ för $i \geq 2$. Låt $a = (a_1, \ldots, a_n)$, $b = (b_1, \ldots, b_n)$. Cauchy-Swartz olikhet ger att

$$\sum_{i=2}^{n} |a_i| \cdot |b_i| \leq ||a|| \cdot ||b|| = \sqrt{|S||T|}, \tag{22}$$

och vi är klara. □

4 Tillämpning: felrättande koder

Vi erinrar oss att en felrättande kod är en mängd $C \subseteq \{0,1\}^n$.

Definition 14. Det *relativa avståndet* för en kod C är

$$\min_{x,y \in C, x \neq y} \frac{d_H(x,y)}{n}, \tag{23}$$

där $d_H(x,y)$ är Hammingavståndet.

Definition 15. *Informationskvoten* för en felrättande kod C är $\log_2 |C|/n$.

Definition 16. En kodfamilj $\{C_n\}$ är *asymptotisk bra* om alla koder har relativt avstånd och informationskvot större än någon positiv konstant.

Definition 17. En felrättande kod är *linjär* om den är ett delrum till $\{0,1\}^n$ betraktat som ett vektorrum över $\mathbb{Z}_2$.

Ett meddelande kan kodas med en linjär kod i polynomiell tid, men avkodning är generellt sett (för meddelanden som är så förstörda att vi inte längre har unik avkodning) NP-svårt. Vårt mål för stunden är att konstruera asymptotiskt bra koder där unikt avkodbara ord kan avkodas i linjär tid.

Låt $G = (V_L \cup V_R, E)$ vara en vänster-c-reguljär bipartit graf, $V_L = \{a_1, \ldots, a_n\}$, $V_R = \{b_1, \ldots, b_m\}$, $m < n$. Vi konstruerar en felrättande kod $C \subseteq \{0,1\}^n$ bestående av alla $\{x_1, \ldots, x_n\}$ sådana att

$$\sum_{\{a_i,b_j\} \in E} x_i \equiv 0 \pmod 2 \tag{24}$$

för alla $1 \leq j \leq m$. Vi får m stycken villkor på pariteten av olika c-delmängder av variablerna. Varje sådant villkor kan högst halvera mängden giltiga kodord, varför $|C| \geq 2^{n-m}$.

Definition 18. En bipartit graf $G = (V_L \cup V_R, E)$ är en $(n, m, c, \delta, \epsilon)$-*bipartit expander* om $|V_L| = n$, $|V_R| = m$, G är vänster-c-reguljär och för alla $S \subseteq V_L$ med $|S| \leq \delta n$ gäller $|N(S)| > \epsilon |S|$.

Notera att vi här använder en variant av hörnexpansion anpassad för bipartita grafer.

Sats 2. *Om G är en $(n, n/2, c, \delta, 3c/4)$-bipartit expander, så är C konstruerad som ovan en kod med informationskvot $1/2$ och relativt avstånd δ. Meddelanden på avstånd $\leq \delta/2$ från C kan avkodas i linjär tid.*

Bevis. Informationskvoten torde vara uppenbar. För att visa det relativa avståndet, antag motsatsen och tag $x, y \in C$ med Hammingavstånd $d_H(x, y) < \delta n$. Låt $S = \{\, i \mid x_i \neq y_i \,\}$. Då både x och y är kodord måste

$$\sum_{\{a_i,b_j\} \in E} x_i + y_i \equiv 0 \pmod 2 \tag{25}$$

för varje $b_j \in V_R$, men $x_i + y_i \equiv 1$ om och endast om $a_i \in S$, varför vi för $b_j \in V_R$ måste ha

$$\sum_{a_i \in S, (a_i,b_j) \in E} 1 \equiv 0 \pmod 2. \tag{26}$$

För varje $b_j \in N(S)$ är summan ovan icke-tom, varför det för varje $b_j \in N(S)$ måste gå minst två kanter till noder i S. Sålunda har vi $E(S, N(S)) \geq 2N(S)$, vilket tack vare G:s expansionsegenskaper är åtminstone $3c|S|/2$. Men detta motsäger att G är vänster-c-reguljär (vi borde ha $E(S, N(S)) = c|S|$), varför vi drar slutsatsen att $x, y \in C$ med $d_H(x, y) < \delta n$ inte kan existera.

Avkodningsalgoritmen går vi inte igenom i detalj. Huvudidén är att köra följande procedur: "så länge det finns a_i med en majoritet av icke-satisfierade grannar b_j, flippa x_i". Detta klarar indata på relativt avstånd $\leq \delta/2$ från C. Att inse att det kan implementeras i linjär tid är lite pyssligare, men detta är alltså möjligt. □

Med anledning av denna sats ovan känner vi oss motiverade att leta reda på en bra bipartit expander.

Sats 3. *För $c > 4$ och lämpligt val av $\delta > 0$ är en slumpvis vald graf G en $(n, n/2, c, \delta, 3c/4)$-bipartit expander för alla tillräckligt stora n.*

Bevis. Låt G vara en slumpgraf på hörmängden $V_L \cup V_R$ där vi för varje $v \in V_L$ väljer grannmängden $N(v) \subseteq V_R$ oberoende och likformigt bland alla c-delmängder till V_R.

Låt $P(S, M) = \mathbf{Pr}_G[N(S) \subseteq M]$. Enligt definitionen av bipartit expander gäller att G inte är en bipartit expander om det existerar en delmängd $S \subseteq V_L$ sådan att $|S| \leq \delta n$ och $|N(S)| \leq \epsilon |S|$.

Använder vi unionsgränsen för sannolikheter får vi

$$\mathbf{Pr}[G \text{ inte } (n, n/2, c, \delta, \epsilon)\text{-expander}] \leq \sum_{1 \leq s \leq \delta n} \sum_{\substack{S \subseteq V_L \\ |S| = s}} \sum_{\substack{M \subseteq V_R \\ |M| = \epsilon s}} P(S, M) \tag{27}$$

Fixera $S \subseteq V_L$ och $M \subseteq V_R$ sådant att $|S| = s$ och $|M| = \epsilon s$, och notera att $\epsilon s < |V_R| = n/2$. Då har vi

$$P(S, M) = \left(\binom{\epsilon s}{c} \Big/ \binom{n/2}{c} \right)^s \leq \left(\frac{\epsilon s}{n/2} \right)^{cs}, \tag{28}$$

eftersom $\binom{m}{k} / \binom{n}{k} < (m/n)^k$ för $n > m > k$. Pluggar vi in detta i ekvation (27) och uttnyttjar $\epsilon = 3c/4$ får vi

$$\sum_{1 \leq s \leq \delta n} \binom{n}{s} \binom{n/2}{3cs/4} \left(\frac{3cs}{2n} \right)^{cs} \tag{29}$$

Varje term kan begränsas med hjälp av $\binom{n}{k} \leq \left(\frac{ne}{k}\right)^k$, och vi får

$$\begin{aligned}
\binom{n}{s} \binom{n/2}{3cs/4} \left(\frac{3cs}{2n} \right)^{cs} &\leq \left(\frac{ne}{s} \right)^s \left(\frac{ne/2}{3cs/4} \right)^{3cs/4} \left(\frac{3cs}{2n} \right)^{cs} \\
&= \left[\frac{ne}{s} \left(\frac{2ne}{3cs} \right)^{3c/4} \left(\frac{3cs}{2n} \right)^c \right]^s \\
&= \left[(n/s)^{1-c/4} \, e^{1+3c/4} \, (3c/2)^{c/4} \right]^s
\end{aligned} \tag{30}$$

Då $c > 4$ och $s \leq \delta n$ får vi att basen i ekvation (30) kan begränsas av

$$\begin{aligned}
(n/s)^{1-c/4} \, e^{1+3c/4} \, (3c/2)^{c/4} &\leq \delta^{c/4-1} e^{1+3c/4} \, (3c/2)^{c/4} \\
&= K = K(\delta, c) < 1,
\end{aligned} \tag{31}$$

om δ väljs tillräckligt litet. Stoppar vi in ekvationerna (30) och (31) i ekvation (29) erhåller vi till slut

$$\begin{aligned}
\mathbf{Pr}[G \text{ inte } (n, n/2, c, \delta, \epsilon)\text{-expander}] &\leq \sum_{i=1}^{\delta n} \left[(n/s)^{1-c/4} \, e^{1+3c/4} \, (3c/2)^{c/4} \right]^s \\
&\leq n^{1-c/4} e^{1+3c/4} \, (3c/2)^{c/4} \sum_{i=0}^{\infty} K^s \\
&= n^{1-c/4} \frac{e^{1+3c/4} \, (3c/2)^{c/4}}{1-K},
\end{aligned} \tag{32}$$

vilket går mot 0 då n går mot ∞.

Sålunda drar vi slutsatsen att en bipartit slumpgraf G med $n + n/2$ hörn och vänstergrad $c > 4$ nästan säkert är en $(n, n/2, c, \delta, 3c/4)$-expander när $n \to \infty$ och δ tillräckligt litet (väldigt litet). $\square$

5 Deterministisk konstruktion av bra expander

Ett problem med den bipartita expander vi konstruerade i föregående avsnitt är att vi med en viss (förvisso försumbart liten) sannolikhet kunde få en graf som inte är en expander, och att det inte finns något känt effektivt sätt att upptäcka detta. I detta avsnitt ger vi oss på att deterministiskt konstruera bra expandergrafer.

Definition 19. En d-reguljär graf G är en *Ramanujangraf* om $\lambda_2 \leq 2\sqrt{d-1}$.

Sats 4. *För alla $d > 0$, $\epsilon > 0$ gäller*

$$\mathbf{Pr}_G\left[\lambda_2 \leq 2\sqrt{d-1} + \epsilon\right] \geq 1 - n^{-\Omega(\sqrt{d})} \tag{33}$$

Å ena sidan gör denna sats oss väldigt glada; nästan alla grafer är "nästan Ramanujangrafer" (och därmed bra expandergrafer enligt sats 1). Å andra sidan är vi inte ett dugg lyckligare, då detta precis som i föregående avsnitt bara ger oss möjlighet att konstruera grafer som med väldigt hög sannolikhet har bra expansionsegenskaper.

Definition 20. Den *normaliserade grannmatrisen* för G är $\hat{A}(G)$, där $\hat{a}_{i,j}$ är antalet kanter mellan i och j delat med valensen för v_j.

För en d-reguljär graf gäller att $\hat{A}(G) = A(G)/d$, och att alla egenvärden skalats med en faktor $1/d$, eftersom alla valenser är d.

$\hat{A}$ kan ses som en övergångsmatris för en slumpvandring på G: om $p \in \mathbb{R}^n$ är en sannolikhetsfördelning så är $\hat{A} \cdot p$ fördelningen efter ett steg längs en slumpvis vald kant.

Definition 21. En graf G är en $[n, d, \alpha]$-expander om

1. $n = |V(G)|$
2. G är d-reguljär
3. $\lambda_2(\hat{A}) \leq \alpha$

Kopplingen till vår ursprungliga definition av expandergrafer (definition 3) ges av sats 1: vi har $\mu_2(A) \leq \lambda_2(A) \leq \alpha d$, varför en $[n, d, \alpha]$-expander har $h(G) \geq (1-\alpha)\frac{d}{2}$.

Definition 22. *Kvadraten* av en graf G är en ny graf $G^2 = (V(G), E')$, där $u \in V$ har kanter till alla noder som kan nås i två steg i G, d.v.s.

$$E' = \{\, (u, v) \mid \exists w \text{ s.a. } (u, w), (w, v) \in E(G) \,\} \tag{34}$$

Vi har $A(G^2) = A(G)^2$, vilket ger att om G är en $[n, d, \alpha]$-expander gäller att G^2 är en $[n, d^2, \alpha^2]$-expander.

5.1 Sicksackprodukt

Som vi såg i förra avsnittet kan vi på ett enkelt sätt från en expandergraf konstruera en ny expandergraf med bättre expansionegenskaper men mycket fler kanter genom en lämplig och naturlig definition av produkten av två grafer.

Vårt mål är nu att definiera en annan (ännu lämpligare men mindre naturlig) produkt på grafer, som rätt utnyttjad också kommer att hjälpa oss förbättra expansionen av en graf, men till mindre kostnad i antal kanter.

Vi kommer att definiera *sicksackprodukten* $G \circledz H$ på grafer G och H som uppfyller

- G är $|V(H)|$-reguljär
- H är d-reguljär

Definitionen av sicksackprodukten är en smula invecklad, så vi nämner först vad man kan använda den till.

Sats (Sicksacksatsen)**.** *Låt G vara en $[n, m, \alpha]$-expander och H en $[m, d, \beta]$-expander. Då är sicksackprodukten $G \circledz H$ en $[nm, d^2, \alpha + \beta]$-expander.*

Bevis av sicksacksatsen kommer att finnas i Gustavs anteckningar från Jakobs nästa föreläsning. Sicksacksatsen hjälper oss att hitta bra expandergrafer:

Sats 5. *Låt H vara en $[d^4, d, 1/4]$-expander, och definiera*

$$\begin{aligned} G_1 &= H^2 \\ G_{i+1} &= G_i^2 \circledz H. \end{aligned}$$

Då är G_i en $[d^{4i}, d^2, 1/2]$-expander för alla $i \geq 1$.

Bevis. $G_1 = H^2$ är en $[d^4, d^2, 1/16]$-expander, och därmed även en $[d^4, d^2, 1/2]$-expander. Antag via induktion att G_i är en $[d^{4i}, d^2, 1/2]$-expander. Då är G_i^2 en $[d^{4i}, d^4, 1/4]$-expander. Antalet hörn i H är lika med valensen för G_i^2 och vi får enligt sicksacksatsen att G_{i+1} är en $[d^{4i} \cdot d^4, d^2, 1/4 + 1/4]$-expander, som önskat. □

Med detta trevliga resultat i bakhuvudet känner vi oss förhoppningsvis tillräckligt modiga för att definiera sicksackprodukten.

Definition (Sicksackprodukt)**.** Låt G vara en m-reguljär graf med $n = |V(G)|$. Ordna kanterna ut från $v \in V(G)$ som $e_v^1, e_v^2, \ldots, e_v^m$ (på något kanoniskt sätt). Låt H vara en d-reguljär graf med $V(H) = [m]$. Vi definierar sicksackprodukten $G \circledz H = (V \times [m], E')$, där

$$E' = \left\{ ([v, i], [u, j]) \mid \exists k, l \ (i, k), (l, j) \in E(H) \wedge e_v^k = e_u^l \right\} \tag{35}$$

Intuitivt ersätter vi varje nod v i G med en ”minikopia” H_v av H, och drar en kant från ett hörn i i H_v till ett hörn j i H_u om (v, u) är en kant i G och det finns k i H_v så att (i, k) är en kant i H_v och den k:te kanten från v i G är (v, u), och det finns motsvarande $l \in H_u$.