



Ekspandery - teoria i zastosowania

Filip Piękniewski

Wydział Matematyki i Informatyki
UMK

Prezentacja dostępna na
<http://www.mat.uni.torun.pl/~philip/ekspandery.pdf>

18 listopada 2007



1

Wstęp

- Ekspandery nieformalnie
- Źródła zamieszania - reprezentacja grafu
- Wycieczka w stronę Laplasjanu kombinatorycznego
- Oznaczenia
- Ekspansja wierzchołkowa, krawędziowa

2

Widma

- Pewne własności widma grafu
- Ekspansja spektralna i jej własności
- Lemat o mieszanii
- Oszacowanie Alona-Boppana

3

Zastosowania

- Grafy magiczne
- Od ekspanderów do superkoncentratorów
- Kody poprawiające błędy
- Derandomizacja
- Sieci sortujące

4

Konstrukcje ekspanderów

- Konstrukcje klasyczne
- Iloczyn zygzakowy (zig-zag product)



Ekspandery nieformalnie

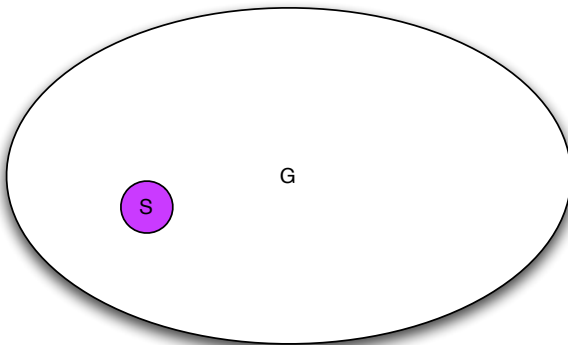
- Graf relatywnie rzadki
- W którym każdy "mały" podzbiór wierzchołków posiada "duże" otoczenie
- Jeśli dla każdego zbioru wierzchołków S mniejszego od $\frac{|V|}{2}$ da się oszacować rozmiar jego otoczenia za pomocą $\alpha|S|$ dla pewnej stałej α , mamy do czynienia z ekspanderem (w sensie ekspansji wierzchołkowej)
- W rzeczywistości chcielibyśmy mieć całą rosnącą rodzinę grafów, o stałym stopniu i wspólnie ograniczonym z dołu parametrem ekspansji
- Dopiero "duże" instancje takich grafów zaczynają być ciekawe! (są rzadkie - stały stopień, i nadal ekspandują)



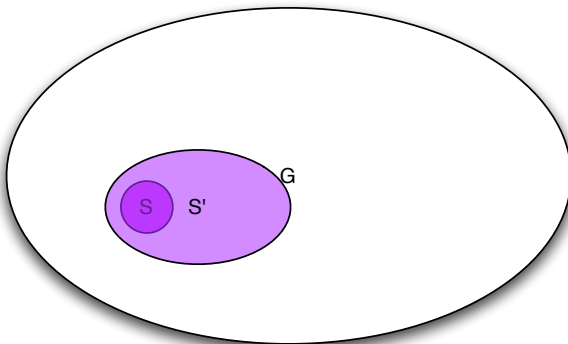
Skutki i intuicje

Intuicyjnie bycie "dobrym" ekspanderem pociąga za sobą ciekawe skutki:

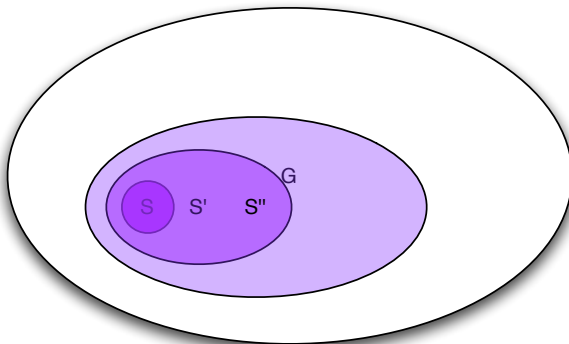
- Startując z dowolnie małego zbioru, po n krokach BFS otrzymujemy wykładniczo duży graf
- Oznacza to, że każde drzewo BFS ma logarytmiczną głębokość
- Patrząc na graf jak na łańcuch Markowa, startując z dowolnego rozkładu na G , bardzo szybko dochodzimy do rozkładu stacjonarnego na G



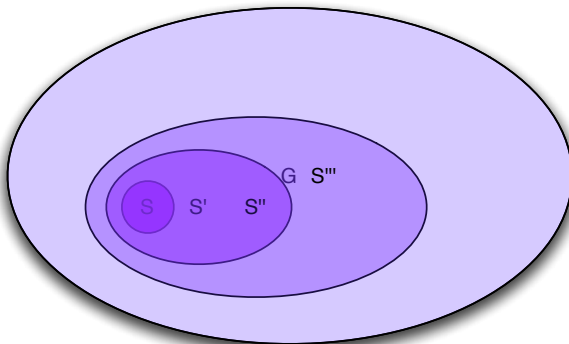
Rysunek: Schematyczne przedstawienie idei ekspansji



Rysunek: Schematyczne przedstawienie idei ekspansji



Rysunek: Schematyczne przedstawienie idei ekspansji



Rysunek: Schematyczne przedstawienie idei ekspansji

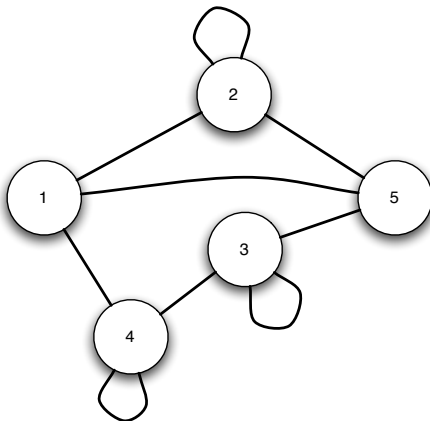


Bałagan reprezentacyjny

Istotnym problemem w tej teorii jest fakt, iż graf może być różnie reprezentowany za pomocą macierzy. W każdej reprezentacji niektóre z prezentowanych twierdzeń formułują się łatwo a niektóre nie.

Możliwe reprezentacje to:

- Macierz sąsiedztwa
- Znormalizowana macierz sąsiedztwa
- Laplasjan kombinatoryczny
- Znormalizowany laplasjan kombinatoryczny



Rysunek: Nieskierowany graf 3-regularny z pętlami



Macierz sąsiedztwa:

$$\begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \end{bmatrix}$$

Wartości własne: 3, 1.618, 0.618, -0.618, -1.618



Znormalizowana macierz sąsiedztwa:

$$\begin{bmatrix} 0 & 1/3 & 0 & 1/3 & 1/3 \\ 1/3 & 1/3 & 0 & 0 & 1/3 \\ 0 & 0 & 1/3 & 1/3 & 1/3 \\ 1/3 & 0 & 1/3 & 1/3 & 0 \\ 1/3 & 1/3 & 1/3 & 0 & 0 \end{bmatrix}$$

Wartości własne: 1, 0.5393, 0.2060, -0.2060, -0.5393



Laplasjan kombinatoryczny:

$$\begin{bmatrix} 3 & -1 & 0 & -1 & -1 \\ -1 & 2 & 0 & 0 & -1 \\ 0 & 0 & 2 & -1 & -1 \\ -1 & 0 & -1 & 2 & 0 \\ -1 & -1 & -1 & 0 & 3 \end{bmatrix}$$

Wartości własne: 4.618, 3.618, 2.382, 1.382, 0



Znormalizowany laplasjan kombinatoryczny:

$$\begin{bmatrix} 1 & -1/3 & 0 & -1/3 & -1/3 \\ -1/3 & 2/3 & 0 & 0 & -1/3 \\ 0 & 0 & 2/3 & -1/3 & -1/3 \\ -1/3 & 0 & -1/3 & 2/3 & 0 \\ -1/3 & -1/3 & -1/3 & 0 & 1 \end{bmatrix}$$

Wartości własne: 1.5393, 1.2060, 0.794, 0.4607, 0



Dlaczego właściwie Laplasjan?

- W "normalnych" okolicznościach Laplasjan jest operatorem przypisującym danej funkcji pole dywergencji jej gradientu.
- $\Delta = \nabla^2$, lub $\Delta = \sum \frac{\partial^2}{\partial x_i^2}$
- Co to ma wspólnego z grafami?



Dlaczego właściwie Laplasjan?

- Niech $G = (V, E)$ będzie grafem
- Załóżmy, że mamy pewną funkcję $f : V \rightarrow \mathbb{R}$ przyjmującą pewną wartość w każdym wierzchołku grafu
- Jak zdefiniować gradient f ? Intuicyjnie powinien być to operator przypisujący każdej krawędzi w grafie przyrost f
- Niech $M \in M_{|V| \times |E|}$ będzie macierzą incydencji, indeksowaną wierzchołkami i krawędziami, $M(v, e)$ równe jest 1 lub -1 (nadaje to skierowanie krawędziom)
- Odwzorowanie $f \rightarrow M^t f$ przypisuje każdej krawędzi przyrost f na jej końcach. $(M^t f)_e = f_u - f_v$ gdy $e = (u, v)$.
- Operator M^t nazwiemy gradientem na grafie G .



Dlaczego właściwie Laplasjan?

- Niech teraz g będzie funkcją $g : E \rightarrow \mathbb{R}$
- Jak określić dywergencję g ?
- Zauważmy, że operator $g \rightarrow Mg$ przypisuje każdemu wierzchołkowi v grafu wartość
$$Mg_v = \sum_{e \text{ wchodzi do } v} g(e) - \sum_{e \text{ opuszcza } v} g(e)$$
- Operator M nazwiemy dywergencją w grafie
- Zauważmy, że operator $f \rightarrow MM^t f$ odpowiada dokładnie intuicjom dotyczącym Laplasjanu.
- Macierz $L = MM^t$ nazywamy Laplasjanem kombinatorycznym grafu. Nietrudno sprawdzić, że $L = D - A$, gdzie D jest macierzą diagonalną zawierającą stopnie wierzchołków oraz A jest macierzą sąsiedztwa.



Twierdzenie Kirchhoffa o drzewach rozpinających

Twierdzenie

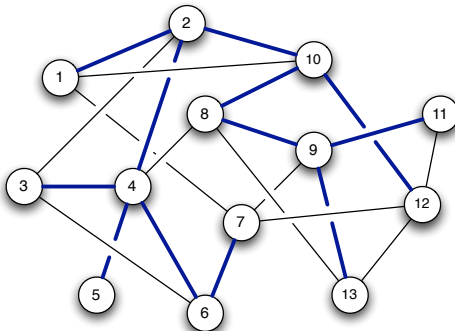
^aNiech G będzie grafem a L jego Laplasjanem kombinatorycznym. Wtedy każdy minor główny L równa się liczbie drzew rozpinających w G .

^aZnane jako tree-matrix theorem

DOWÓD. Niech $M \in M_{|V| \times |E|}$ oznacza macierz incydencji dla grafu G zdefiniowaną jak poprzednio. Wtedy:

$$L = MM^t$$

Można to sprawdzić, rozpisując iloczyn skalarne dla par indeksów i, j :



Rysunek: Przykład grafu oraz drzewa rozpinającego.



DOWÓD.

- Jeśli $i = j$ dostajemy 1 na każdej krawędzi incydentnej z i -tym wierzchołkiem, zatem

$$(MM^t)_{i,i} = D_{i,i}$$

- Jeśli $i \neq j$ dostaniemy 0 gdy nie ma krawędzi z i do j lub -1 gdy taka krawędź istnieje, zatem

$$(MM^t)_{i,j} = -A_{i,j}$$

Oznaczmy przez M_0 macierz M z usuniętym pewnym wierszem (dla ustalenia uwagi może być pierwszy wiersz). Wtedy

$$L_0 = M_0 M_0^t$$



DOWÓD. Ze wzoru Cauchyego-Bineta mamy:

$$\begin{aligned}\det(L_0) &= \det(M_0 M_0^t) = \sum_{X \subset E, |X|=n-1} \det(M_X M_X^t) = \\ &= \sum_{X \subset E, |X|=n-1} (\det(M_X))^2\end{aligned}$$

Gdzie L_0 to macierz L z usuniętym pierwszym wierszem i kolumną, zaś M_X to macierz M ograniczona do kolumn odpowiadających krawędziom ze zbioru X .



DOWÓD. Zauważmy następujący fakt:

$$\det(M_X) = \begin{cases} 0 & \text{jeśli } X \text{ zawiera cykl,} \\ 1 & \text{jeśli } X \text{ nie zawiera cyklu.} \end{cases}$$

Drzewo rozpinające to dokładnie podgraf acykliczny zawierający $n - 1$ krawędzi, zatem sumy na poprzednim slajdzie zliczają drzewa rozpinające w grafie G . ■



Przykład

Zauważmy, że cykl rzeczywiście implikuje liniową zależność kolumn macierzy M :

$$\left[\begin{array}{ccc|c} 1 & 0 & 1 & \\ -1 & 1 & 0 & * \\ 0 & -1 & -1 & \\ & 0 & & * \end{array} \right]$$

Wystarczy dodać kolumnę 1 do 2 i otrzymujemy kolumnę 3.



Jeśli nie będzie zaznaczone inaczej, w tej prezentacji domyślne są:

- Nieskierowany d -regularny graf G o zbiorze wierzchołków V i krawędzi E
- Reprezentacja grafu jako zwykłej macierzy sąsiedztwa, wartości własne liczone z takiej macierzy
- Dla zbioru $S \subset V$ przez ∂S oznaczamy zbiór krawędzi których jeden kraniec leży w S a drugi w $V \setminus S$
- Analogicznie przez $\Gamma(S)$ oznaczamy zbiór wierzchołków z $V \setminus S$ posiadających sąsiada z S .
- Zbiór $\{\lambda_1, \lambda_2, \dots, \lambda_n\}$ wartości własnych macierzy sąsiedztwa będziemy nazywać widmem grafu, przyjmiemy przy tym konwencję sortowania $d = \lambda_1 \geq \lambda_2 \geq \lambda_3 \geq \dots \geq \lambda_n$



Dla grafu d -regularnego G parametrem ekspansji (krawędziowej)¹ nazywamy:

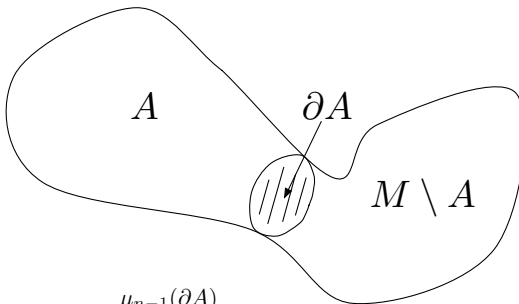
$$h(G) = \min_{S \subset V, 1 \leq |S| \leq \frac{|V|}{2}} \frac{|\partial S|}{|S|}$$

Warto zauważyć tutaj związek ze stałą Cheegera dla zwartych n -wymiarowych rozmaitości riemanowskich postaci:

$$h(M) = \inf_A \frac{\mu_{n-1}(\partial A)}{\min(\mu_n(A), \mu_n(M \setminus A))}$$

Nieformalnie rzecz ujmując jedna i druga funkcja mierzy "wąskie gardło" grafu lub rozmaitości.

¹W tej mierze również istnieje pewne zamieszanie, niektórzy autorzy używają sformułowania *vertex expansion* w stosunku do tej wielkości



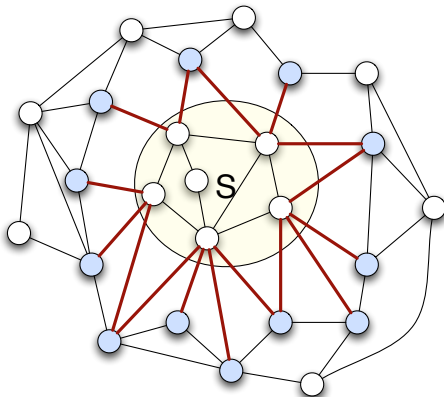
$$h(M) = \inf_A \frac{\mu_{n-1}(\partial A)}{\min(\mu_n(A), \mu_n(M \setminus A))}$$

Rysunek: Intuicje związane ze stałą Cheegera w przypadku rozmaitości Riemannowskich



Dla d -regularnego grafu G i stałej α parametrem α -ekspansji wierzchołkowej nazywamy

$$g_{\alpha}(G) = \min_{S \subset V, 1 \leq |S| \leq \alpha|V|} \frac{|\Gamma(S)|}{|S|}$$



Rysunek: Przykład podzbioru w grafie planarnym, $|\partial S| = 16$, $|\Gamma(S)| = 12$



Twierdzenie

Dla grafu d -regularnego G , mamy: $\lambda_1 = d$ oraz wektor posiadający wszystkie współrzędne równe jest wektorem własnym.

DOWÓD. Rozważmy maksymalną wartość własną λ_i oraz jej wektor własny v . Dla pewnego i mamy $|v_i| = \max_j |v_j|$. Wtedy $\lambda \leq d$ gdyż z nierówności trójkąta i maksymalności v_i mamy:

$$|\lambda||v_i| = \left| \sum_j a_{ij} v_j \right| \leq |v_i| \sum_j |a_{i,j}| = d|v_i|$$

W szczególności, równość zachodzi gdy:

- 1 $\forall_j a_{ij} \neq 0 \Rightarrow v_j = v_i$
- 2 $\forall_j a_{ij} \neq 0 \Rightarrow v_j = -v_i$



Twierdzenie

Graf d -regularny G jest spójny gdy największa wartość własna λ jego macierzy sąsiedztwa ma krotność algebraiczną 1.

DOWÓD. Załóżmy, że graf jest niespójny. Niech $X \subsetneq V$ oraz $Y = V \setminus X$. Dla dowolnego $S \subset V$ niech χ_S oznacza jego wektor charakterystyczny ($\chi_{Si} = 1 \iff v_i \in S$). Wtedy $x = \chi_X$ oraz $y = \chi_Y$ są wektorami własnymi λ .

$$(Ax)_i = \sum_j a_{ij}x_j = \sum_{j \in X} a_{ij}x_j = \begin{cases} d & , i \in X \\ 0 & , i \notin X \end{cases}$$

z czego automatycznie wynika $Ax = dx$. Analogicznie postępujemy z y .



DOWÓD. Teraz założmy, że $\lambda = d$ występuje z krotnością > 1 .
Wtedy istnieje pewien wektor x (niejednostajny) dla λ . Niech
 $X = \{i | x_i = \max_j x_j\}$. Ponieważ jest to wektor własny dla wartości
własnej równej d , z poprzedniego twierdzenia wiadomo, że dla
każdego $i \in X$ oraz $a_{ij} \neq 0$ zachodzi $x_i = x_j$. Zatem $a_{ij} = 0$ dla
każdego $i \in X, j \in V \setminus X$, zatem X nie jest połączony z $V \setminus X$.





Twierdzenie

Dla dowolnego grafu G liczba jego spójnych składowych jest równa krotności algebraicznej wartości własnej $\lambda = 0$ laplasjanu kombinatorycznego G .



Twierdzenie

Graf d -regularny G jest dwudzielny wtedy i tylko wtedy gdy posiada wartość własną równą $\lambda_i = -d$

DOWÓD. Rozważmy graf $G^2 = (V, E^2)$, którym istnieje krawędź między wierzchołkiem u i v jeśli w oryginalnym grafie G istniała ścieżka długości 2 między u i v . Łatwo zauważyć, że macierz sąsiedztwa dla G^2 jest równa dokładnie A^2 , gdzie A jest macierzą sąsiedztwa grafu G . Ponieważ graf G był dwudzielny, więc G^2 jest niespójny, zatem największa wartość własna macierzy A^2 musi mieć krotność 2. Zauważmy, że

$$\lambda_{A^2} = \lambda_A^2$$

zatem

$$\max \lambda_{A^2} = \max \lambda_A^2$$



DOWÓD. Mamy

$$\max \lambda_{A^2} = \max \lambda_A^2 = d^2$$

Jest krotności dwa, zaś w oryginalnym grafie $\lambda = d$ miała krotność jeden. Zatem w grafie G musiała istnieć wartość własna $\lambda_i = -d$, skąd

$$\lambda_i^2 = (-d)^2 = d^2$$





Niech $d = \lambda_1 \geq \lambda_2 \geq \lambda_3 \geq \dots \geq \lambda_n$ będą wartościami własnymi grafu. Liczbę $d - \lambda_2$ nazywamy separacją spektralną grafu. Separacja spektralna ma pewien niezwykle ciekawy związek z parametrem ekspansji odkryty w wersji ciągłej przez Cheegera i Busera, a dla przypadku dyskretnego przez Dodziuka [Dodziuk(1984)] i niezależnie przez Alona i Milmana [Alon and Milman(1985), Alon(1986)]. Wyraża się on następująco:

Twierdzenie

Niech G będzie d -regularnym grafem z widmem $d = \lambda_1 \geq \lambda_2 \geq \lambda_3 \geq \dots \geq \lambda_n$. Wtedy:

$$\frac{d - \lambda_2}{2} \leq h(G) \leq \sqrt{2d(d - \lambda_2)} \quad (1)$$



Lemat o mieszaniu dla ekspanderów

Lemat

Niech G będzie d -regularnym grafem z n wierzchołkami i $\lambda = \lambda(G) = \max(|\lambda_2|, |\lambda_n|)$. Wtedy dla każdych $S, T \subseteq V$

$$\left| |E(S, T)| - \frac{d|S||T|}{n} \right| \leq \lambda \sqrt{|S||T|} \quad (2)$$

Zauważmy co mówi ten lemat: lewa strona wyznacza różnicę między ilością krawędzi $|E(S, T)|$ w grafie ze zbioru S do T , a średnią ilością takich krawędzi w d -regularnym grafie losowym $\frac{d|S||T|}{n}$. Oznacza to, że jeśli λ jest niewielkie, graf ma duży "rozrzut" (discrepancy) krawędzi, i w tym sensie wygląda podobnie do losowego.



Lemat odwrotny do lematu o mieszaniu

Lemat

Niech G będzie d -regularnym grafem i załóżmy, że dla każdych dwóch rozłącznych zbiorów wierzchołków i pewnego ρ

$$\left| |E(S, T)| - \frac{d|S||T|}{n} \right| \leq \rho \sqrt{|S||T|} \quad (3)$$

Wtedy $\lambda \leq \mathcal{O}(\rho(1 + \log(d/\rho)))$. Ograniczenie jest ścisłe.



Twierdzenie

(Alona-Boppana). Dla każdego d -regularnego grafu G o n wierzchołkach zachodzi:

$$\lambda \geq 2\sqrt{d-1} - o_n(1) \quad (4)$$

Czynnik $o_n(1)$ zbiega do zera dla ustalonego d i $n \rightarrow \infty$.



W tej części prezentacji:

- Pokażemy istnienie grafów *magicznych*
- Wykorzystamy grafy magiczne do konstrukcji superkoncentratorów o $\mathcal{O}(n)$ krawędziach
- Dalej wykorzystamy grafy magiczne do konstrukcji optymalnych kodów korygujących błędy
- Pokażemy, że odpowiednie zastosowanie ekspanderów pozwala zmniejszyć zapotrzebowanie na bity losowe dla algorytmów *RP* bez straty na prawdopodobieństwie
- Dowiemy się o sieci sortującej AKS o logarytmicznej głębokości



Definicja

Niech $G = (L, R, E)$ będzie grafem dwudzielnym. Mówimy, że G jest grafem (n, m, d) -magicznym jeśli $|L| = n$, $|R| = m$ i każdy lewy wierzchołek ma d sąsiadów oraz zachodzą związki:

- (i) $|\Gamma(S)| \geq \frac{5d}{8}|S|$ dla każdego $S \subset L$, $|S| \leq \frac{n}{10d}$
- (ii) $|\Gamma(S)| \geq |S|$ dla każdego $S \subset L$, $\frac{n}{10d} < |S| \leq \frac{n}{2}$



Twierdzenie

Istnieje stała n_0 taka, że dla każdego $d \geq 32$ i $n \geq n_0$, $m \geq 3n/4$ istnieje (n, m, d) -magiczny graf.

DOWÓD. Niech G będzie losowym grafem dwudzielnym z n wierzchołkami po lewej i m wierzchołkami po prawej, przy czym każdy wierzchołek z lewej ma d sąsiadów. G z dużym prawdopodobieństwem jest magiczny.

Udowodnimy najpierw, że własność (i) zachodzi z dużym prawdopodobieństwem. Niech $S \subset L$ ma moc $s = |S| \leq \frac{n}{10d}$ i niech $T \subset R$ ma moc $t = |T| < \frac{5ds}{8}$. Niech $X_{S,T}$ będzie zmienną losową przyjmującą 1 gdy wszystkie krawędzie z S idą do T (0 w p.p). Jeśli $\sum X_{S,T} = 0$ gdy suma przebiega wszystkie wybory S i T jak wyżej, wtedy własność (i) zachodzi.



DOWÓD. Prawdopodobieństwo zdarzenia $X_{S,T}$ wynosi $(t/m)^{sd}$.
Korzystając z nierówności $\binom{n}{k} \leq (ne/k)^k$ dostajemy:

$$\begin{aligned} Pr[\sum_{S,T} X_{S,T} > 0] &\leq \sum_{S,T} Pr[X_{S,T} = 1] = \sum_{S,T} (t/m)^{sd} \\ &\leq \sum_{s=1}^{n/10d} \binom{n}{s} \binom{m}{5ds/8} \left(\frac{5ds}{8m}\right)^{sd} \\ &\leq \sum_{s=1}^{n/10d} \left(\frac{ne}{s}\right)^s \left(\frac{8me}{5ds}\right)^{5ds/8} \left(\frac{5ds}{8m}\right)^{sd} < 1/10 \end{aligned}$$

Ostatnia nierówność zachodzi, ponieważ s -ty wyraz jest ograniczony przez 20^{-s}



DOWÓD. Podobnie szacujemy prawdopodobieństwo złamania własności (ii). Dla każdego $S \subset L$ o rozmiarze $\frac{n}{10d} < s = |S| \leq \frac{n}{2}$ i $T \subset R$, $t = |T| < |S|$ niech $Y_{S,T}$ będzie zmienną losową przyjmującą wartość 1 gdy wszystkie krawędzie z S idą do T (0 w p.p.). Tak jak w poprzednim przypadku chcemy aby prawdopodobieństwo zdarzenia $\sum_{S,T} Y_{S,T} = 0$ było niewielkie:

$$\begin{aligned} Pr\left[\sum_{S,T} Y_{S,T} > 0\right] &\leq \sum_{S,T} Pr[Y_{S,T} = 1] = \sum_{S,T} (t/n)^{sd} \leq \\ &\leq \sum_{s=n/10d}^{n/2} \binom{n}{s} \binom{m}{s} (s/m)^{sd} \leq \sum_{s=1}^{n/2} \left[\frac{ne}{s} \frac{me}{s} \left(\frac{s}{m}\right)^d \right]^s < 1/10 \end{aligned}$$

Ostatnia nierówność zachodzi, gdyż s -ty wyraz jest ograniczony przez 10^{-s} . Zatem większość grafów jest magiczna. ■

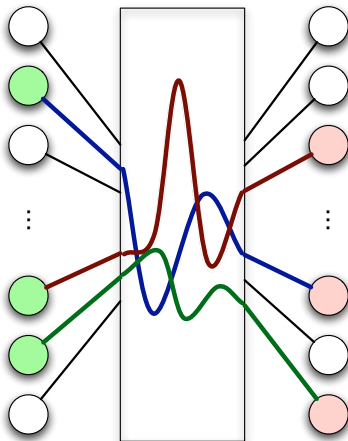


Superkoncentratory

Definicja

Graf G nazywamy superkoncentratorem jeśli

- *G jest "rzadki"*
- *Posiada wyszczególnione dwa rozłączne, n -elementowe zbiory wierzchołków wejść IN i wyjść OUT*
- *Dla dowolnego $k \leq n$ i każdych $S \subseteq IN$ i $T \subseteq OUT$, $|S| = |T| = k$, istnieje zbiór rozłącznych ścieżek z S do T .*



Rysunek: Schemat superkoncentratora

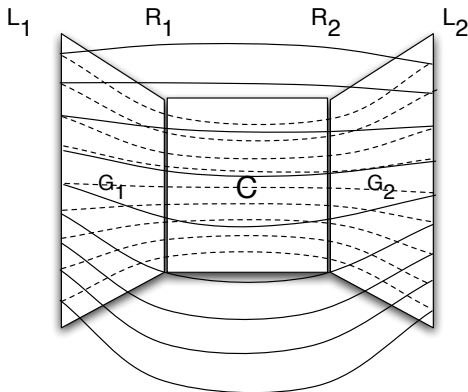


Oczywiście graf pełny jest superkoncentratorem, jednak ma mnóstwo krawędzi. Przez długi czas otwarte było pytanie czy istnieją superkoncentratory o liniowej liczbie krawędzi? Odpowiedź na to pytanie jest twierdząca, a do konstrukcji takich grafów trzeba wykorzystać grafy magiczne będące specyficznymi ekspanderami.



Konstrukcja superkoncentratora o $\mathcal{O}(n)$ krawędziach

Niech G będzie $(n, 3n/4, d)$ -magicznym grafem, wtedy $|\Gamma(S)| \geq |S|$ dla każdego $S \subset L$, $|S| \leq \frac{2}{n}$. Na podstawie twierdzenia Halla istnieje skojarzenie doskonałe z S do $\Gamma(S)$. Zbudujemy superkoncentrator C' z n wierzchołkami po każdej stronie rekursywnie. Dla n poniżej pewnej stałej n_0 wystarczy wziąć pełen graf dwudzielny, (jest superkoncentratorem z n^2 krawędzi). Dla $n \geq n_0$ konstruujemy superkoncentrator używając dwóch kopii grafu magicznego $G_1 = (L_1, R_1, E_1)$ oraz $G_2 = (L_2, R_2, E_2)$, gdzie $|L_i| = n$, $|R_i| = 3n/4$. Następnie łączymy wyjścia G_1 z wyjściami G_2 za pomocą superkoncentratora C o $\mathcal{O}(n)$ krawędziach. Ponieważ C ma $3n/4$ wejść i wyjść, więc na mocy założenia indukcyjnego istnieje. Na koniec łączymy pojedynczą krawędzią wierzchołki z L_1 i L_2 .



Rysunek: Konstrukcja superkoncentratora C'



Twierdzenie

Graf skonstruowany tak jak powyżej jest superkoncentratorem z $\mathcal{O}(n)$ krawędziach.

DOWÓD. (poprawność) Niech S i T , $|S| = |T| = k$ będą wejściem i wyjściem. Jeśli $k \leq \frac{n}{2}$, wtedy $|\Gamma_{G_1}(S)| \geq |S|$ oraz $|\Gamma_{G_2}(T)| \geq |T|$ (z magiczności). Istnieje zatem skojarzenie doskonałe pomiędzy S a $S' \subset \Gamma_{G_1}(S)$ w G_1 i T a $T' \subset \Gamma_{G_2}(T)$ w G_2 . Ponieważ C jest superkoncentratorem, zbiory S' i T' mogą być połączone ścieżkami rozłącznymi.

Jeśli $k > \frac{n}{2}$, wtedy istnieje przynajmniej $k - n/2$ par wierzchołków połączonych bezpośrednimi krawędziami z S do T . Dla pozostałych par stosujemy rozumowanie jak powyżej.



DOWÓD. Potrzeba jeszcze oszacować liczbę krawędzi $e(n)$ w grafie C' . Dostajemy następujące równanie rekurencyjne:

$$e(n) \leq \begin{cases} 2nd + n + e(3n/4) & \text{dla } n > n_0, \\ n^2 & \text{dla } n \leq n_0. \end{cases}$$

Rozwiązanie tej rekursji implikuje $e(n) \leq Kn$ gdzie stała K zależy jedynie od n_0 i d . Otrzymaliśmy zatem superkoncentrator o $\mathcal{O}(n)$ krawędziach. ■



Tworzenie superkoncentratorów z minimalną stałą K stało się popularnym "sportem". Obecny rekord opisany jest w pracy [Alon and Capalbo(2003)]. Podana tam została konstrukcja superkoncentratora o gęstości $K = 44$ z wykorzystaniem rodziny grafów Ramanujana (optymalnych ekspanderów spektralnych).



Kody poprawiające błędy (ECC - Error Correcting Codes)

- Załóżmy, że następuje komunikacja cyfrowa przez kanał w którym mogą się pojawić zakłócenia
- Niech maksymalna proporcja zakłóconych bitów wynosi ρ , jak wysłać k -bitową wiadomość tak aby dotarła bezbłędnie?
- Z pomocą przychodzą pomysły Claude Shannona:
 - Niech $C \subset \{0, 1\}^n$ będzie słownikiem, oraz $|C| = 2^k$
 - Kodujemy każdą k -bitową wiadomość jako element $c \in C$, otrzymujemy n -bitowe kodowanie
 - Dla słowa s które przeszło przez kanał komunikacyjny znajdujemy najbliższe w sensie odległości Hamminga słowo $s' \in C$
 - Dekodujemy s' z nadzieją otrzymania oryginalnej wiadomości
 - Jeśli odległość między każdymi dwoma słowami w słowniku jest większa niż $2\rho n$ mamy gwarancję odzyskania dobrej wiadomości



Jak tworzyć kody?

- Pytanie o komunikację sprowadza się zatem do znalezienia dobrego słownika
- Przez parametr efektywności słownika określamy

$$R = \frac{\log |C|}{n}$$

- Średnicą kodu nazywamy

$$\delta = \frac{\min_{c_1 \neq c_2 \in C} d_H(c_1, c_2)}{n}$$



Definicja

Problem efektywnego kodowania: czy jest możliwe zaprojektowanie rodziny słowników $\{C_k\}_{k=1}^{\infty}$ taką, że $|C_k| = 2^k$, średnica każdego słownika jest większa od pewnej stałej $\delta_0 > 0$ oraz parametr efektywności kodu większy od pewnej stałej $R_0 > 0$.

Jak zobaczymy za chwilę, problem ten można rozwiązać za pomocą ekspanderów...



Skonstruujemy kodowanie $C \subset \{0, 1\}^n$ z parametrem efektywności przynajmniej $1/4$ i średnicą przynajmniej $1/10d$. Wykorzystamy do tego po raz kolejny grafy magiczne.

Twierdzenie

Niech G będzie grafem magicznym z n lewych wierzchołków i $3n/4$ prawych wierzchołków. Dla każdego podzbioru $\emptyset \neq S \subset L$, $|S| \leq \frac{n}{10d}$ istnieje wierzchołek $u \in R$ posiadający dokładnie jednego sąsiada z S czyli $|\Gamma(u) \cap S| = 1$.

DOWÓD. Rozważmy $e(S, \Gamma(S))$. Oczywiście

$e(S, \Gamma(S)) = d|S| = ds$. Z drugiej strony skoro $|\Gamma(S)| \geq \frac{5ds}{8}$, średnia liczba sąsiadów z S w $\Gamma(S)$ wynosi $8/5 < 2$. Ale każdy wierzchołek z $\Gamma(S)$ ma przynajmniej jednego sąsiada w S . Istnieje zatem przynajmniej jeden (a w rzeczywistości wiele) wierzchołków w $\Gamma(S)$ posiadających dokładnie jednego sąsiada w S . ■



Definicja

Niech $G = (R, L, E)$ będzie grafem magicznym reprezentowanym przez macierz A ze zbiorem wierszy R i kolumn L , przy czym $a_{i,j}$ jest równe 1 lub 0, zależnie czy i -ty wierzchołek w R jest sąsiadem j -tego wierzchołka w L . Kod C definiujemy jako prawe jądro macierzy A , czyli $C = \{x \in \{0, 1\}^n \mid Ax = 0\}$, przy czym operacje wykonujemy nad ciałem $\mathbb{Z}_2$. C jest podprzestrzenią liniową o wymiarze przynajmniej $n/4$, stąd $|C| \geq 2^{n/4}$, co daje żądane ograniczenie na parametr efektywności.



Twierdzenie

Kod zdefiniowany powyżej ma średnicę $\geq 1/10d$

DOWÓD. Ponieważ C jest podprzestrzenią liniową, zatem najmniejsza odległość między jej wektorami jest równa najmniejszej wadze niezerowego wektora (słowa kodowego). Niech $x \neq 0$ będzie n bitowym wektorem z nośnikiem $S = j \in L, x_j = 1$. Jeśli $|S| \leq \frac{n}{10d}$, wtedy istnieje pewne i takie, że $|\Gamma(i) \cap S| = 1$. Wynika z tego, że i -ta współrzędna Ax jest jeden, co stoi w sprzeczności z faktem, iż x należy do jądra przekształcenia A . Wynika z tego, że minimalna znormalizowana odległość Hamminga kodu C wynosi przynajmniej $1/10d$. ■



Prezentowane podejście to specjalny przypadek LDPC (Low Density Parity Check). Pomysł ten był zaproponowany przez Gallagera [Gallager(1963)], następnie rozwijana przez Bassalygo, Pinsker i Margulisa [Pinsker(1973), Margulis(1973), Bassalygo and Pinsker(1973)]. Przez 20 lat dziedzina ta była uśpiona, by powrócić w latach 90-tych. Dzisiaj uważa się, że LDPC dają najlepsze parametry kodów jednocześnie przy dobrej efektywności implementacyjnej. Przegląd tej dziedziny można znaleźć w [Richardson and Urbanke(2004)].



Derandomizacja algorytmów RP

Definicja

Język $L \subset \{0,1\}^*$ należy do klasy RP, jeśli istnieje wielomianowy algorytm A , pobierający na wejściu pewną liczbę bitów losowych (ilość bitów zależy również wielomianowo od rozmiaru problemu), taki że:

- Jeśli $x \in L$, wtedy A akceptuje x z prawdopodobieństwem przynajmniej^a $1/16$:

$$\Pr[A(x, \text{Rand}(\text{Poly}(|x|))) = 1] \geq 1/16$$

- Jeśli $x \notin L$, A zawsze odrzuca x

^aWybór jest dowolny, ale $1/16$ będzie wygodna dla obliczeń. Standardowo w definicjach RP jest $1/2$



Zauważmy, że po k niezależnych próbach prawdopodobieństwo pomyłki zanika wykładniczo:

$$\Pr[A(x, \text{Rand}(\text{Poly}(|x|))) = 0 \wedge \dots \wedge A(x, \text{Rand}^n(\text{Poly}(|x|))) = 0] \leq 16^{-n}$$

- Przykładem algorytmu probabilistycznego jest algorytm Rabina-Millera na testowanie pierwszości liczb naturalnych, chociaż wiadomo, że problem ten należy do klasy P.
- Podstawowym cennym surowcem zużywanym przez algorytmy RP są bity losowe
- Być może zabrzmi to dziwnie, ale zebranie sensownego zbioru bitów losowych nie jest łatwym zadaniem
- Ekspandery pozwalają zachować ograniczenia na prawdopodobieństwo, przy znacznym ograniczeniu używanych bitów losowych



Zaczniemy od pewnej prostej obserwacji związanej z magicznymi grafami. Niech $G = (L, R, E)$ będzie (n, n, d) magicznym grafem z $n = 2^k$, gdzie k jest długością słowa wejściowego i dla uproszczenia ilością zużywanych bitów losowych. Niech B oznacza zbiór złych ciągów bitów losowych dla których algorytm A akceptuje x nawet jeśli $x \notin L$. Wiemy, że $|B| \leq n/16$. Dla każdej liczby naturalnej d zbudujemy algorytm, który uruchomi algorytm A d razy i osiągnie prawdopodobieństwo błędu $\epsilon \leq \frac{1}{10d}$ przy użyciu tylko jednej "paczki" bitów losowych.



- Wybierz losowy ciąg k bitów, wybierz odpowiadający mu wierzchołek v w L
- Niech $\{r_1, r_2, \dots, r_d\} = \Gamma(v) \subset R$ będzie zbiorem sąsiadów v w R .
- Akceptuj słowo x jeśli wszystkie wywołania $A(x, r_1), \dots, A(x, r_d)$ zaakceptowały



Twierdzenie

Algorytm powyżej ma prawdopodobieństwo błędu mniejsze niż $\frac{1}{10d}$

DOWÓD. Algorytm popełnia błąd gdy $x \notin L$ i $r_1, r_2, \dots, r_d \in B$, czyli $\Gamma(v) \subset B$. Niech S będzie zbiorem wierzchołków w L które spełniają ten warunek (zatem gdy $v \in S$ algorytm się myli). Oczywiście $\Gamma(S) \subset B$, jednak musi zachodzić $|S| \leq \frac{n}{10d}$ bo inaczej dostaniemy sprzeczność:

$$|B| \geq |\Gamma(S)| > \frac{5d}{8} \frac{n}{10d} \geq n/16$$

To górne ograniczenie na rozmiar S oznacza, że algorytm myli się z prawdopodobieństwem najwyżej $\frac{1}{10d}$. Zauważmy, że polepszenie błędu uzyskaliśmy bez wykorzystania dodatkowych bitów losowych!





Optymalna redukcja błędu z wykorzystaniem ekspanderów spektralnych

Pokażemy teraz, że można dokonać optymalnej redukcji błędu (zanik wykładniczy) przy wykorzystaniu logarytmicznie małej ilości bitów losowych.

W tym celu przypomnijmy:

$$\lambda = \lambda(G) = \max(|\lambda_2|, |\lambda_n|)$$

Oraz oznaczmy $\alpha = \lambda/d$.



Jeśli graf G jest ekspanderem spektralnym z parametrem $\alpha = \lambda/d$,
lemat o mieszaniu formułuje się następująco:

$$\left| |E(S, T)| - \frac{d|S||T|}{n} \right| \leq \alpha d \sqrt{|S||T|} \leq \alpha dn$$

Co można przepisać:

$$\left| \frac{|E(S, T)|}{dn} - \frac{|S||T|}{n^2} \right| \leq \alpha$$



Rozważmy teraz dwa eksperymenty losowe polegające na wybieraniu par (i, j) wierzchołków w G . Za sukces będziemy uznawać zdarzenie, że $i \in S$ oraz $j \in T$. W pierwszym eksperymencie wybieramy losowo obydwa wierzchołki z rozkładu jednostajnego na V . Prawdopodobieństwo sukcesu w tym przypadku wynosi $|S||T|/n^2$. W drugim eksperymencie losowo wybieramy $i \in V$ a następnie j jednostajnie wśród sąsiadów i . Prawdopodobieństwo sukcesu w tym wypadku wynosi $|E(S, T)|/dn$. Lemat o mieszaniu dla ekspanderów orzeka, że pomimo różnej natury próbkowań, prawdopodobieństwa sukcesu w obydwu przypadkach różnią się jedynie o niewielki parametr α .



Niech $G = (V, E)$ będzie (n, d) - ekspanderem z parametrem α oraz $B \subset V$ będzie zbiorem $|B| = \beta n$. Przeprowadzamy następujący eksperyment: wybieramy losowo element $X_0 \in V$ a następnie wykonujemy losowy spacer (random walk) kolejno $X_0, \dots, X_t$ na G . Przez (B, t) oznaczamy zdarzenie w którym wszystkie odwiedzone wierzchołki były w B , czyli $\forall_i X_i \in B$

Twierdzenie

[Ajtai et al.(1987) Ajtai, Komlos, and Szemeredi]

[Alon et al.(1995) Alon, Feige, Wigderson, and Zuckerman]

$$Pr[(B, t)] \leq (\beta + \alpha)^t$$

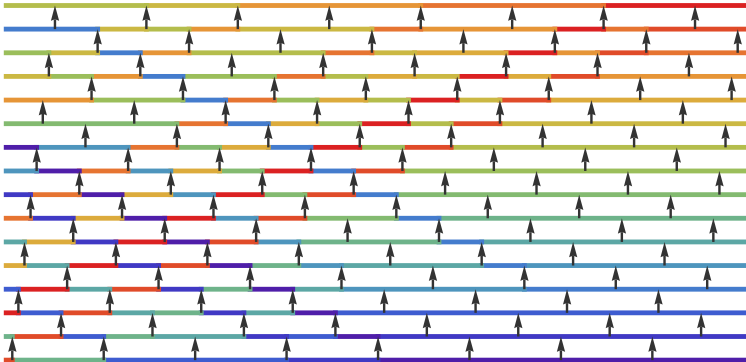


Rozważmy algorytm (przy założeniu, że A jest algorytmem probabilistycznym dla języka $L \in RP$ z prawdopodobieństwem pomyłki β , zaś $G(V, E)$, $V = \{0, 1\}^k$ ekspanderem z parametrem α):

- Wybierz losowo wierzchołek $v \in V$
- Rozpocznij losowy spacer długości t ($v_0, v_1, \dots, v_t$)
- Zaakceptuj wejście x jeśli każde uruchomienie $A(x, v_0), A(x, v_1), \dots, A(x, v_t)$ zaakceptowało x

Prawdopodobieństwo, że powyższy algorytm zawiedzie jest mniejsze niż $(\alpha + \beta)^t$. Bity losowe są konsumowane przez wybranie startowego wierzchołka na następnie na wylosowanie jedno z d sąsiadów, przy czym $d \ll 2^k$, zatem sumaryczna ilość bitów zużytych przez algorytm wynosi $k + t \log(d) = k + \mathcal{O}(t)$.

Sieci sortujące



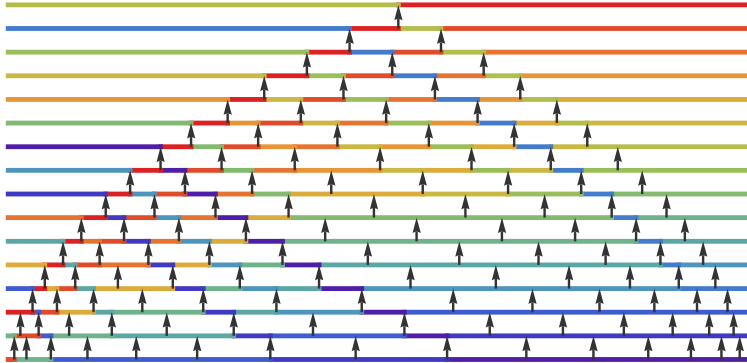
Rysunek: Najprostsza sieć sortująca oparta o transpozycje sąsiednich elementów (16 elementów, 120 porównań, głębokość 16)



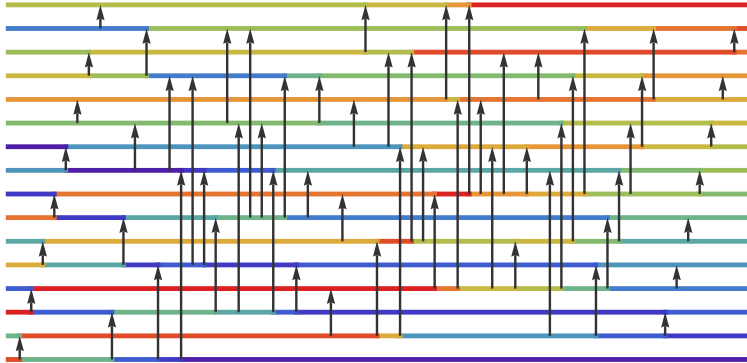
Otwarte pytania sieci sortujących to:

- Dla zadanej liczby elementów ile porównań ma sieć optymalna?
- Jaką głębokość (ilość równoległych faz) ma optymalna sieć?
- Jakiego rzędu są asymptotycznie optymalne głębokości sieci dla dowolnych n ?

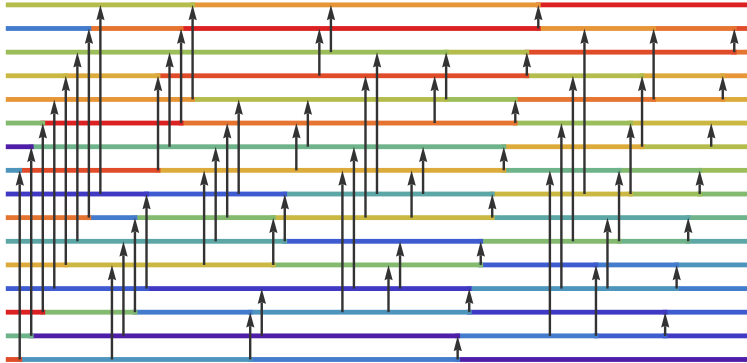
Pierwsze pytanie zawiera odpowiedź dla $n \leq 16$. Odpowiedzią na trzecie pytanie jest sieć AKS.



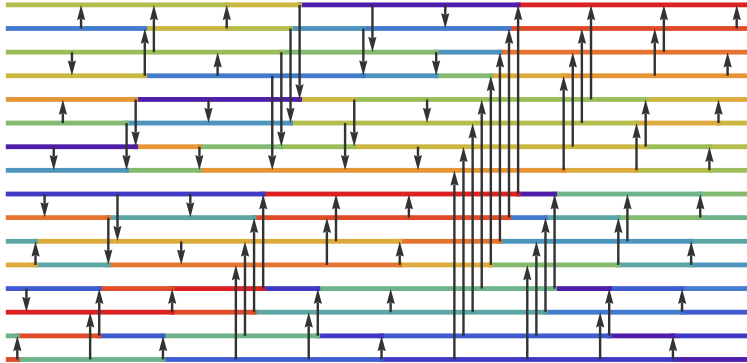
Rysunek: Sieć reprezentująca algorytm sortowania przez wstawianie (16 elementów, 120 porównań, głębokość 29)



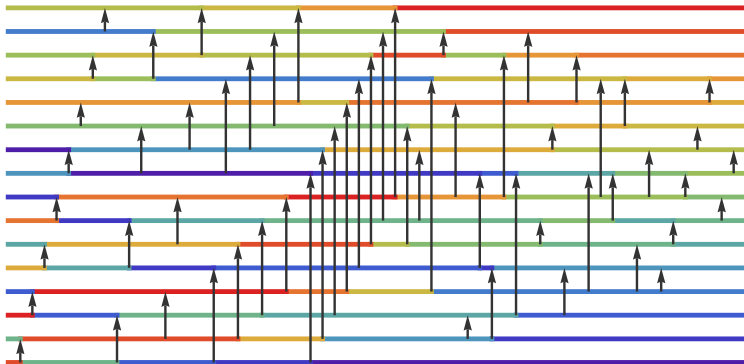
Rysunek: Kolejna sieć sortująca (16 elementów, 63 porównania, głębokość 22)



Rysunek: Sieć sortująca Batchera typu Odd-even (16 elementów, 63 porównania, głębokość 10)



Rysunek: Bitoniczna sieć sortująca Batchera (16 elementów, 80 porównań, głębokość 10)



Rysunek: Sieć sortująca optymalna dla 16 elementów (16 elementów, 60 porównań, głębokość 14)



- Wiadomo, że dolnym ograniczeniem na asymptotyczną głębokość sieci to $\mathcal{O}(\log n)$, nie było jednak wiadomo czy takie sieci dla dużych ilości elementów rzeczywiście istnieją.
- Jednak dopiero w 1983 w pracy [Ajtai et al.(1983a) Ajtai, Komlós, and Szemerédi] oraz [Ajtai et al.(1983b) Ajtai, Komlós, and Szemerédi] autorzy pokazali istnienie takiej sieci za pomocą ekspanderów
- Sama sieć jest jednak zupełnie niepraktyczna - co prawda asymptotycznie optymalna, to jednak stała ukryta w notacji $\mathcal{O}$ jest bardzo duża.



W tej części poznamy dwie konstrukcje ekspanderów, jedną klasyczną, przedstawioną w pracy Gregory'ego Margulisa w pracy [Margulis(1973)] w 1973 roku, drugą opierającą się o nową operację na grafach - iloczyn zygzakowy (zig zag product) - zaproponowany przez w pracy [Reingold et al.(2002)Reingold, Vadhan, and Wigderson].



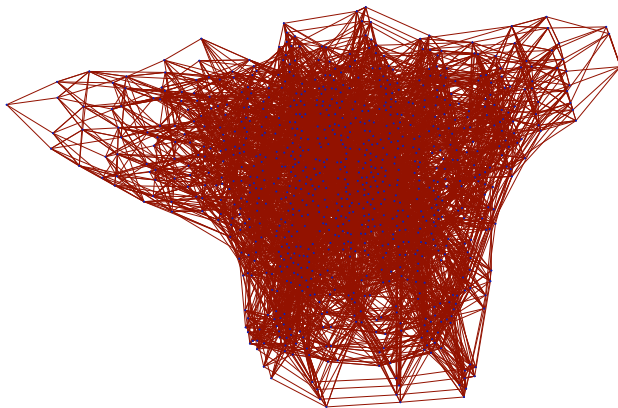
Konstrukcja Margulisa

Rozważmy rodzinę 8-regularnych grafów G_m dla każdego $m \in \mathbb{N}$. Zbiorem wierzchołków niech będzie $V_m = \mathbb{Z}_m \times \mathbb{Z}_m$. Sąsiadami wierzchołka (i, j) są odpowiednio:
 $(i + j, j)$, $(i - j, j)$, $(i, j + i)$, $(i, j - i)$, $(i + j + 1, j)$, $(i - j + 1, j)$,
 $(i, j + i + 1)$, $(i, j - i + 1)$, (wszystkie operacje brane mod m).

Twierdzenie

Rodzina grafów zdefiniowanych powyżej spełnia $\lambda(G_n) \leq 5\sqrt{2} < 8$ dla każdego n .

Zauważmy, że dowolnie duże instancje grafów G_n są relatywnie bardzo rzadkie (stopień regularności 8), a jednak zawsze mają istotną przerwę spektralną, zatem nigdy nie mają "wąskich gardeł".



Rysunek: Graf Margulisa dla $V = \mathbb{Z}_{30} \times \mathbb{Z}_{30}$ (bez pętli i krawędzi wielokrotnych)



Margulis w pracy [Margulis(1973)] dowodził, że ściśle związana z powyższymi rodzina grafów stanowi rodzinę ekspanderów, jego dowód był jednak zupełnie egzystencjalny. W 1981 Gabber i Gail w pracy [Gabber and Galil(1981)] przedstawili dolne oszacowanie na przerwę spektralną. Ich dowód wykorzystywał analizę harmoniczną. W 1987 oszacowanie zostało poprawione w pracy [Jimbo and Maruoka(1987)]. Dowód który po uproszczeniach zajmuje zaledwie kilka stron algebry liniowej jest jednak daleki od bycia prostym, zainteresowani mogą znaleźć dość przystępną wersję w [Hoory et al.(2006)Hoory, Linial, and Wigderson]



Iloczyn zygzakowy (zigzag product)

Iloczyn zygzakowy (zig-zag product), jest pewną nowatorską operacją na grafach zaproponowaną w pracy [Reingold et al.(2002)Reingold, Vadhan, and Wigderson]. Inspiracją tego produktu był zapewne produkt tensorowy, który jednak nie jest zbyt interesujący z punktu widzenia ekspanderów. Produkt zygzakowy jest dość skomplikowany na pierwszy rzut oka, do jego zrozumienia potrzebne jest pojęcie rotacji w grafie.



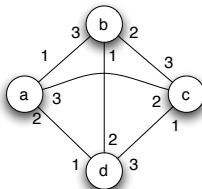
Definicja

Mapą rotacji dla d -regularnego grafu $G = (V, E)$ nazywamy przekształcenie:

$$\text{Rot}_G : V \times \{1, \dots, d\} \rightarrow V \times \{1, \dots, d\}$$

Zdefiniowane następująco: $\text{Rot}_G(i, a) = (j, b)$ dokładnie wtedy gdy j jest a -tym sąsiadem i oraz i jest b -tym sąsiadem j . Rotacja jest dobrze określona i nie zależy od wyboru konkretnego numerowania sąsiadów.

$$\text{Rot} : V \times \{1, \dots, d\} \rightarrow V \times \{1, \dots, d\}$$



Rysunek: Przykładowy graf

W powyższym przykładzie:

$$\begin{aligned} \text{Rot}(a, 1) &= (b, 3), \text{Rot}(a, 2) = (d, 1), \text{Rot}(a, 3) = (c, 2), \\ \text{Rot}(b, 3) &= (a, 1), \text{Rot}(b, 1) = (d, 2), \text{Rot}(b, 2) = (c, 3), \\ \text{Rot}(c, 3) &= (b, 2), \text{Rot}(c, 1) = (d, 3), \text{Rot}(c, 2) = (a, 3), \\ \text{Rot}(d, 3) &= (c, 1), \text{Rot}(d, 1) = (a, 2), \text{Rot}(d, 2) = (b, 1), \end{aligned}$$



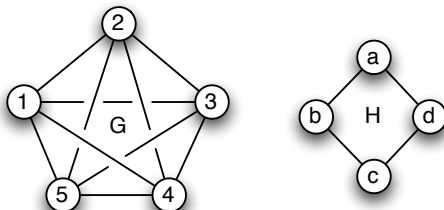
Definicja

Niech $G = (V_1, E_1)$ będzie grafem d_1 -regularnym o n wierzchołkach a $H = (V_2, E_2)$, d_2 -regularnym o d_1 wierzchołkach. Ustalmy rotację Rot_G i Rot_H . Produktem zygzakowym $\Gamma = G \circledast H$ nazywamy d_2^2 -regularny graf o nd_1 wierzchołkach ze zbiorem wierzchołków $V = V_1 \times V_2$. Krawędzie Γ zdefiniowane są przez rotację

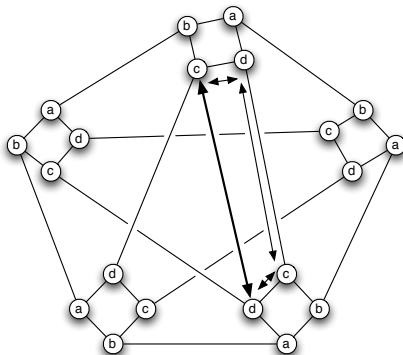
$$Rot_\Gamma : (V_1 \times V_2) \times (\{1, \dots, d_2\} \times \{1, \dots, d_2\}) \rightarrow \\ \rightarrow (V_1 \times V_2) \times (\{1, \dots, d_2\} \times \{1, \dots, d_2\})$$

określoną: $Rot_\Gamma((i, c), (k, l)) = ((j, d), (m, n))$ jeśli istnieją $p, q \in V_2$ takie, że:

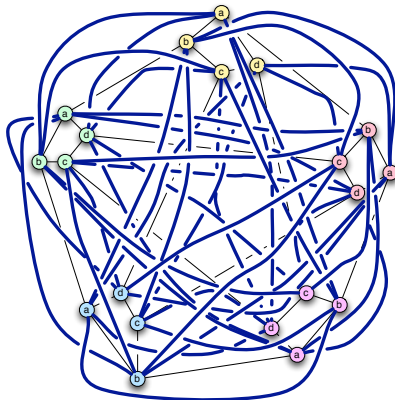
1. $Rot_H(c, k) = (p, n)$
2. $Rot_G(i, p) = (j, q)$
3. $Rot_H(q, l) = (d, m)$



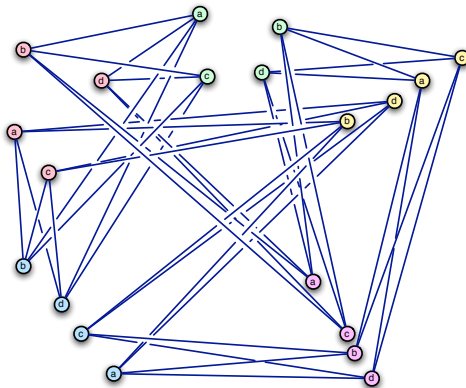
Rysunek: Produkt zig zag



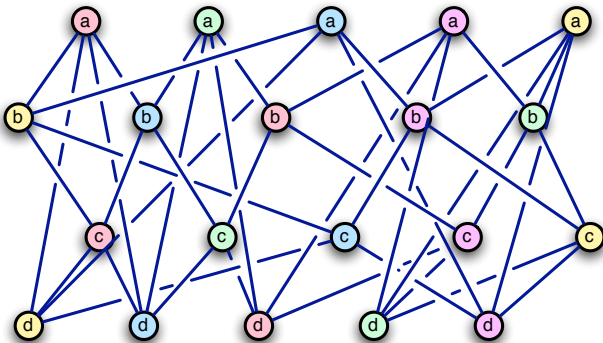
Rysunek: Schemat tworzenia produktu zygzak $G @ H$. Powstały graf pomocniczy powstaje po złożeniu dwóch map rotacji. Ścieżka w $G @ H$ istnieje, gdy istnieje trzykrawędziowa ścieżka w grafie pomocniczym której początkowy i końcowy fragment zawiera się w "małym" grafie.



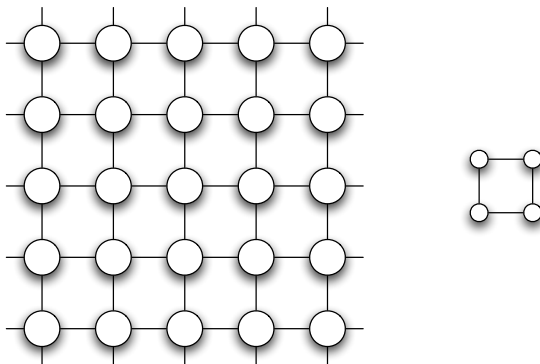
Rysunek: Graf pomocniczy po dodaniu wszystkich krawędzi z $G \boxtimes H$. W ostatecznym produkcie trzeba wymazać pomocnicze krawędzie. Dla lepszej widoczności poszczególne instancje małego grafu zostały pokolorowane.



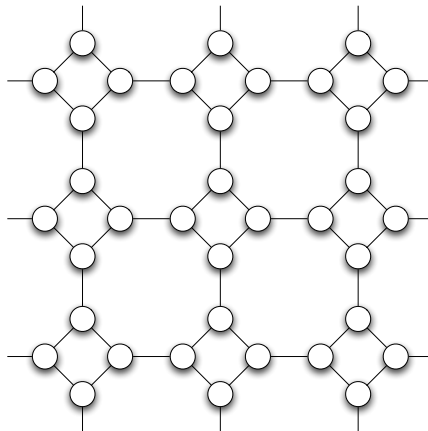
Rysunek: Ostateczny produkt zygzak $G @ H$. Dla polepszenia widoczności instancje "małego" grafu zostały lekko rozbite.



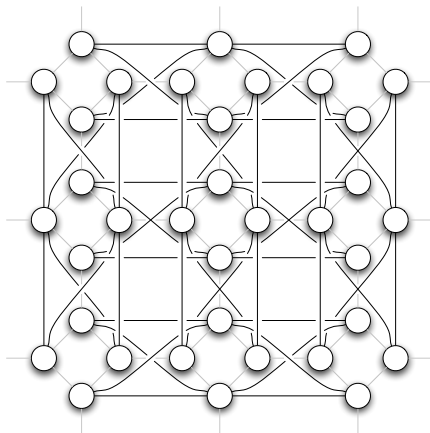
Rysunek: Alternatywne uporządkowanie dla grafu $G \boxtimes H$. Kolory reprezentują pochodzenie poszczególnych wierzchołków.



Rysunek: Kolejny przykład - grafy składowe $\mathbb{Z}^2$ oraz C_4 .



Rysunek: Graf pomocniczy produktu $\mathbb{Z}^2 @ \mathbb{Z} C_4$



Rysunek: Fragment ostatecznego produktu $\mathbb{Z}^2 \circledast C_4$



Istotą produktu zygzakowego jest fakt, że jeśli składowe są ekspanderami, wynik jest niewiele gorszym ekspanderem. Można zatem wykorzystać tą operację do iteracyjnej konstrukcji rodzin ekspanderów. Zauważmy że:

- Wynikowy graf "dziedziczy" rozmiar po pierwszej składowej produktu (zazwyczaj dużej)
- Stopień dziedziczony jest po drugiej składowej (zazwyczaj małej)
- Można zatem łatwo produkować duże grafy o małym stopniu



Twierdzenie

Niech G będzie grafem m -regularnym o n wierzchołkach i parametrze ekspansji $\alpha = \frac{\lambda}{d} = \frac{\max(|\lambda_2|, |\lambda_n|)}{d}$ zaś H d -regularnym o m wierzchołkach i parametrze ekspansji β . Wtedy $G \circledast H$ jest grafem d^2 -regularnym o nm wierzchołkach i parametrze ekspansji $\phi(\alpha, \beta)$ gdzie funkcja ϕ :

- Jeśli $\alpha < 1$ i $\beta < 1$ to $\phi(\alpha, \beta) < 1$
- $\phi(\alpha, \beta) \leq \alpha + \beta$
- $\phi(\alpha, \beta) \leq 1 - (1 - \beta^2)(1 - \alpha)/2$



M. Ajtai, J. Komlós, and E. Szemerédi.

Sorting in $c \log n$ parallel steps.

Combinatorica, 3(1):1–19, 1983a.

ISSN 0209-9683.

doi: <http://dx.doi.org/10.1007/BF02579338>.



M. Ajtai, J. Komlós, and E. Szemerédi.

An $O(n \log n)$ sorting network.

In *STOC '83: Proceedings of the fifteenth annual ACM symposium on Theory of computing*, pages 1–9, New York, NY, USA, 1983b. ACM Press.

ISBN 0-89791-099-0.

doi: <http://doi.acm.org/10.1145/800061.808726>.



M. Ajtai, J. Komlos, and E. Szemerédi.

Deterministic simulation in logspace.

In *STOC '87: Proceedings of the nineteenth annual ACM conference on Theory of computing*, pages 132–140, New York, NY, USA, 1987. ACM Press.



ISBN 0-89791-221-7.

doi: <http://doi.acm.org/10.1145/28395.28410>.



N. Alon and M. Capalbo.

Smaller explicit superconcentrators.

In *SODA '03: Proceedings of the fourteenth annual ACM-SIAM symposium on Discrete algorithms*, pages 340–346, Philadelphia, PA, USA, 2003. Society for Industrial and Applied Mathematics.

ISBN 0-89871-538-5.



N. Alon and F. R. K. Chung.

Explicit construction of linear sized tolerant networks.

Discrete Math., 72(1-3):15–19, 1988.

ISSN 0012-365X.

doi: [http://dx.doi.org/10.1016/0012-365X\(88\)90189-6](http://dx.doi.org/10.1016/0012-365X(88)90189-6).



Noga Alon.

Eigenvalues and expanders.

Combinatorica, 6(2):83–96, 1986.



Noga Alon and Vitali D. Milman.

λ_1 , isoperimetric inequalities for graphs, and superconcentrators.

Journal of Combinatorial Theory. Series B, 38(1):73–88, 1985.

ISSN 0095-8956.



Noga Alon, Uriel Feige, Avi Wigderson, and David Zuckerman.

Derandomized graph products.

Computational Complexity, 5(1):60–75, 1995.

URL citeseer.ist.psu.edu/alon96derandomized.html.



L. A. Bassalygo and M. S. Pinsker.

The complexity of an optimal non-blocking commutation scheme without reorganization.

Problemy Peredaci Informacii, 9(1):84–87, 1973.

Translated into English in Problems of Information Transmission, 9 (1974) 64-66. MR 0327387 (48:5729).



Fan R. K. Chung.



Spectral graph theory (CBMS Regional Conference Series in Mathematics, No. 92).

Cbms Regional Conference Series in Mathematics. American Mathematical Society, 1997.



J. Dodziuk.

Difference equations, isoperimetric inequality and transience of certain random walks.

Trans. Amer. Math. Soc., 284(2):787–794, 1984.



Cynthia Dwork and Prahladh Harsha.

Expanders in computer science, 2005.

URL [http:](http://ttic.uchicago.edu/~prahladh/teaching/spring05/index.html)

[//ttic.uchicago.edu/~prahladh/teaching/spring05/index.html](http://ttic.uchicago.edu/~prahladh/teaching/spring05/index.html).

Lecture notes for course at Stanford.



Ofer Gabber and Zvi Galil.

Explicit constructions of linear-sized superconcentrators.

Journal of Computer and System Sciences, 22(3):407–420, June 1981.



R. G. Gallager.

Low Density Parity-Check Codes.

MIT Press, Cambridge, MA, 1963.



Shlomo Hoory, Nathal Linial, and Avi Wigderson.

Expander graphs and their applications.

Bulletin of the American Mathematical Society, 43(4):439–561, October 2006.



Shuji Jimbo and Akira Maruoka.

Expanders obtained from affine transformations.

Combinatorica, 7(4):343–355, 1987.

ISSN 0209-9683.



Gregory A. Margulis.

Explicit constructions of expanders.

Problemy Peredači Informacii, 9(4):71–80, 1973.



Mark S. Pinsker.



On the complexity of a concentrator.

In *7th Annual Teletraffic Conference*, pages 318/1–318/4, Stockholm, 1973.



Omer Reingold, Salil Vadhan, and Avi Wigderson.

Entropy waves, the zig-zag graph product, and new constant-degree.

Ann. of Math., 155(1):157–187, 2002.

URL <http://www.citebase.org/abstract?id=oai:arXiv.org:math/0406038>.



Tom Richardson and Ruediger Urbanke.

Modern coding theory.

EPFL Lausanne, 2004.

URL <http://lthcwww.epfl.ch/mct/index.php>.



David Y. Xiao.

The evolution of expander graphs.

Master's thesis, Harvard College, Cambridge, Massachusetts, 2003.