Seminar Expandergraphen

Verlustfreie Leiter und verlustfreie Expandergraphen

Neil JAMI

8. Juli 2011

Motivation: Es gibt viele Anwendungen, die (N, D)-Graphen benötigen, in denen Knotenmengen der Größe ϵN möglichst große Knotenexpansion γD haben.

Bemerkung 1. *Kahale [Kah95]* hat eine Untere Schranke von $\frac{1}{2}D$ für die Knotenexpansion kleiner Knotenmengen linerarer Größe in (N, D)-Graphen gezeigt.

Bemerkung 2. *Kahale* zeigt jedoch auch, dass es einen Ramanujan Graphen gibt, also einen Graphen mit maximaler spektraler Lücke, mit Knotenexpansion kleiner als $\frac{1}{2}D$.

Offenes Problem: Erzeugung einer Familie von (N, D)-Graphen, in den Menge von Knoten der Größe ϵN eine Knoten Expansion von γD mit $\gamma > \frac{1}{2}$.

Ziel: Mit Hilfe einer Erweiterung des Zigzag Produkts werden hier bipartite Graphen erzeugt, sogenannte verlustfreie Expandergraphen, deren Knotenexpansion für kleine Mengen von Knoten groß ist. Anstatt der spektralen Lücke wird die Entropie betrachtet.

Definition 1. Verlustfreie Expandergraphen : Sei $G = (V_L, V_R; E)$ ein bipartiter Graph mit $|V_L| = N$ linken Knoten und $|V_R| = M \leq N$ rechten Knoten, und Grad D für jeden Knoten $v \in V_L$.

G ist ein (K_{max}, ϵ)-**verlustfreier Expandergraph** wenn jede Menge von $K < K_{max}$ linken Knoten mindestens $(1 - \epsilon) \cdot D \cdot K$ Nachbarn hat.

Bemerkung 3. Die **Entropie** einer Wahrscheinlichkeitsverteilung $p \in \mathbb{R}^N$ zeigt wieviel Zufall sie enthält. Hier wird die Min-Entropie $H_\infty(p) = -\log_2(\|p\|_\infty)$ benutzt.

Dabei ist $\|p\| = -\log_2(\max_{1 \leq i \leq N} p_i)$.

Beobachtung 1. Sei G ein bipartiter Graph mit $N = 2^n$ linken Knoten und $M = 2^m$ rechten Knoten, wobei jeder linke Knoten $D = 2^d$ Nachbarn hat. Außerdem seien feste Indizes der linken und rechten Knoten sowie der Kanten pro linkem Knoten gegeben. Dann ist G äquivalent zu solch einer Funktion E:

$$E : \{0,1\}^n \times \{0,1\}^d \longrightarrow \{0,1\}^m$$

Definition 2. Eine k-**Quelle** ist eine Wahrscheinlichkeitsverteilung X mit $H_\infty(X) \geq k$.

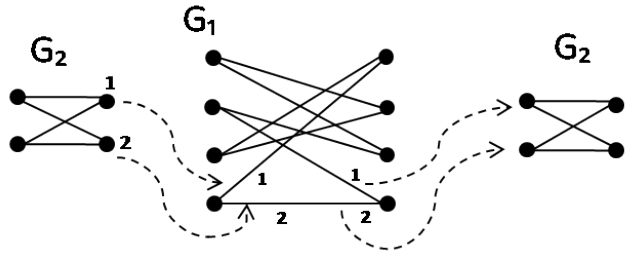
Der l_1 Abstand zwischen zwei Wahrscheinlichkeitsverteilungen $X \in \mathbb{R}^N$ und $Y \in \mathbb{R}^N$ ist so definiert: $\|X - Y\|_1 = \sum_{1 \leq i \leq N} |X_i - Y_i|$. Eine Wahrscheinlichkeitsverteilung Y ist eine (k, ϵ)-Quelle, wenn eine k-Quelle X ϵ-**nah** von ihr ist: $\|X - Y\|_1 < \epsilon$.

Definition 3. Leiter : Sei $E : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ eine Funktion. E ist ein (k_{max}, a, ϵ)-Leiter wenn für jede $k < k_{max}$ und jede k-Quelle X auf $\{0,1\}^n$ die Verteilung $E(X, U_d)$ eine $(k + a, \epsilon)$-Quelle ist.

Ein (k_{max}, ϵ)-**verlustfreier Leiter** ist ein (k_{max}, d, ϵ)-Leiter. Solch ein Leiter verliert keine Entropie in einer zufälligen Bewegung.

Beobachtung 2. Ein verlustfreier Leiter ist auch ein verlustfreier Expandergraph.

Beispiel 1. *Zigzag Produkt für bipartite Graphen:*



Definition 4. Eine Funktion E ist ein (a, ϵ)**-extrahierender Leiter** wenn sie ein $(m-a, a, \epsilon)$ Leiter ist. In diesem Leiter erhöht sich die Entropie jeder (k, ϵ)-Quelle um a, falls $k \leq m-a$. (Ansonsten ist die übrige Entropie verloren.)

Ein (k_{max}, a, ϵ)**-buffer Leiter** ist ein Paar von Funktionen $< E, C >$: $\{0,1\}^n \times \{0,1\}^d \longrightarrow \{0,1\}^m \times \{0,1\}^b$ so dass E ein (a, ϵ)-extrahierender Leiter ist, und $< E, C >$ einen (k_{max}, ϵ)-verlustfreien Leiter bildet. Somit wird die übrigene Entropie aus E in C gespeichert.

Ein (k_{max}, a, ϵ)**-permutation Leiter** ist ein Paar von Funktionen $< E, C >$: $\{0,1\}^n \times \{0,1\}^d \longrightarrow \{0,1\}^m \times \{0,1\}^{n+d-m}$, wobei E ein (a, ϵ)-extrahierender Leiter ist, und $< E, C >$ eine Permutation ist.

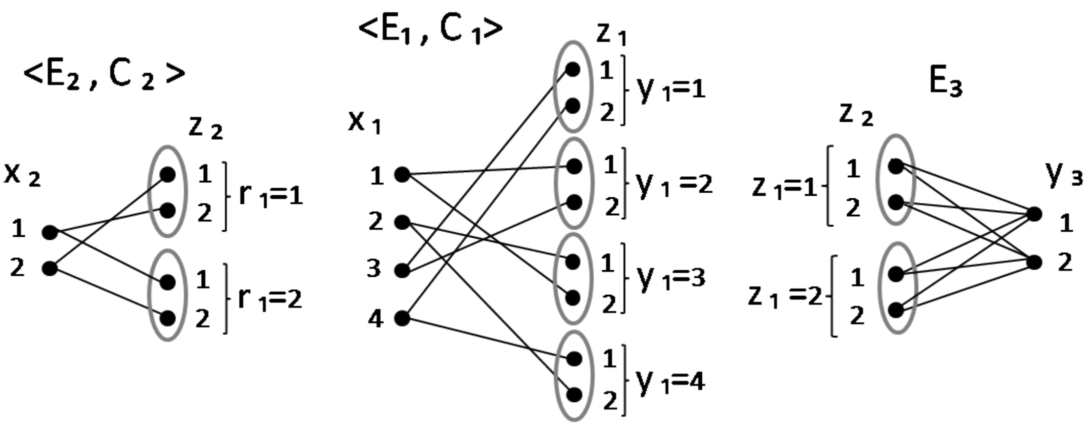
Definition 5. Das **Zigzag Produkt für Leiter** ist eine Funktion $E : \{0,1\}^{n_1+n_2} \times \{0,1\}^{d_2+d_3} \longrightarrow \{0,1\}^{m_1+m_3}$, definiert mit Hilfe von den folgenden Funktionen:

- $\langle E_2, C_2 \rangle : \{0,1\}^{n_2} \times \{0,1\}^{d_2} \longrightarrow \{0,1\}^{d_1} \times \{0,1\}^{b_1}$: ein buffer-Leiter.
- $\langle E_1, C_1 \rangle : \{0,1\}^{n_1} \times \{0,1\}^{d_1} \longrightarrow \{0,1\}^{m_1} \times \{0,1\}^{b_1}$: ein permutation-Leiter.
- $E_3 : \quad \{0,1\}^{b_2+b_1} \times \{0,1\}^{d_3} \longrightarrow \{0,1\}^{m_3}$: ein verlustfreier-Leiter.

Dann wird die Abbildung $(y_1 : y_3) = E(x_1 : x_2, r_2 : r_3)$ durch die folgenden Schritte berechnet:

1. $(r_1, z_2) := \langle E_2, C_2 \rangle (x_2, r_2)$
2. $(y_1, z_1) := \langle E_1, C_1 \rangle (x_1, r_1)$
3. $y_3 := E_3(z_1 : z_2, r_3)$

Beispiel 2. Zigzag Produkt für Leiter:



Satz 1. Sei $a = 1000 \log(1/\epsilon)$ und $d = 2a$. Die folgenden Funktionen erzeugen mittels einem Zigzag Produkt mit Leiter einen $(n - 30a, 4\epsilon)$-verlustfreien Leiter:

- $\langle E_2, C_2 \rangle : \{0,1\}^{20a} \times \{0,1\}^a \longrightarrow \{0,1\}^{14a} \times \{0,1\}^{21a}$: $(14a, 0, \epsilon)$-Buffer Leiter.
- $\langle E_1, C_1 \rangle : \{0,1\}^{n-20a} \times \{0,1\}^{14a} \rightarrow \{0,1\}^{n-20a} \times \{0,1\}^{14a}$:($n$-$30a$, $6a$, ϵ)-Permutationsleiter.
- $E_3 : \qquad \{0,1\}^{14a+21a} \times \{0,1\}^a \longrightarrow \{0,1\}^{17a}$: $(15a, \epsilon)$-verlustfreier Leiter.