CS 598: Spectral Graph Theory. Lecture 14

Cayley Graphs

Alexandra Kolla

Today

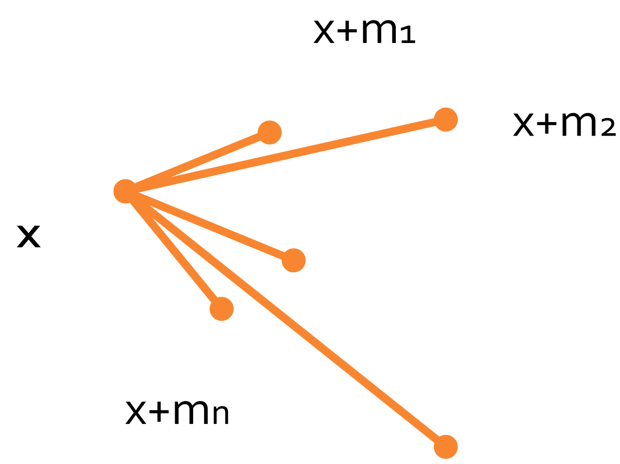
- Graphs from linear codes
- Groups
- Cayley graphs
- Eigenvectors and Eigenvalues of Cayley graphs of abelian groups

Graphs from Linear Codes

- Consider linear code over {0,1} from m bits to n bits (rate m/n)
- View the encoding as m-by-n matrix M, and codewords as the vectors bM, $b \in \{0,1\}^m$
- Let d be min distance
- We use code to construct n-regular graph on 2^m vertices with $\lambda_2 = 2d$
- Generalization of Hypercube ($M=I_m$)

Graphs from Linear Codes

- V= $\{0,1\}^m$,
- $E = \{x, x + m_j, x \in V, m_j \ column \ of \ M\}$
- x,y neighbors if x+y is a column of M (degree n)



Evectors and Evalues

- For each $b \in \{0,1\}^m$, define the function $v_b: V \rightarrow R$,

$$v_b(x) = (-1)^{b^T x}$$

Think of b as being an index for Fourier coefficient

Evectors and Evalues

Theorem: For each $b \in \{0,1\}^m$, v_b is an adjacency matrix evector with evalue

n-2|bM|

- Asymptotically good code gives good expander graph but of logarithmic degree.

- (Last week) For every δ, exists codes of length n, rate r, relative min distance δn
- Those provide graphs on $2^m = 2^{rn}$ vertices, of degree n, and second evalue 2δn. With some work we can show that max evalue is also bounded (unlikely that there are codewords of large hamming weight).

Groups

- Graphs constructed from groups are called Cayley graphs.
- Group is defined by set of elements, Γ and a binary operation $\circ$
- For elements g,h in Γ $g \circ h$ is also an element of Γ.

Groups

- (Γ , ∘) form a group if
  - Γ contains a special element called the identity (id) such that g∘id=id∘g=g for all g∈ Γ
  - For every element g ∈ Γ , there is another element g^{-1}∈ Γ such that $g^{-1} \circ g = g \circ g^{-1} = id$
  - For every three elements f,g,h ∈ Γ $f \circ (g \circ h) = (f \circ g) \circ h$
  - Group is abelian if for every g,h ∈Γ, *if*
    $g \circ h = h \circ g$

Groups: Examples You Already Know

1. (Integers , +)
2. (Z/n=Integers mod n, addition mod n)
3. (Z/p-0=Integers mod prime without zero, multiplication)
4. ($\{0,1\}^k$, componentwise addition mod 2) ; every element is its own inverse
5. For some k>0, (set of non-singular k-by-k matrices over integers, addition)
6. For some k>0, (set of non-singular k-by-k matrices over integers, multiplication)

Today: groups 2 and 4 : finite, abelian!

Cayley Graphs

- Cayley graph is defined by
  - a group $(\Gamma, \circ)$
  - a set of generators $S \subseteq \Gamma$ that is closed under inverse. That is, for every $g \in \Gamma$, $g^{-1} \in \Gamma$

The vertex set of Cayley graph is Γ and the edges are the pairs

$$\{(g,h): h = g \circ s, some\ s \in S\} = \{(g, g \circ s): s \in S\}$$

E.g. Ring graph on n vertices if $(\Gamma, \circ) = (Z/n, +)$

And S=(-1,+1) (-1 =n-1 mod n)

Evectors and Evalues of Cayley Graphs of Abelian Groups

- We can find orthogonal set of eigenvectors without knowing S. Eigenvectors only depend on group
- Will consider adjacency matrix but doesn’t really matter since Cayley graphs are regular.
- Next we re-prove the evectors of the “generalized” ring graph =(Z/n,+) and any set S of generators
- Get logn degree expanders from random set of logn generators