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

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

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

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

Think of $b$ as being an index for Fourier coefficient
E vectors and E values

**Theorem:** For each $b \in \{0,1\}^m$, $v_b$ is an adjacency matrix eigenvector with eval $n-2|bM|$

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

- (Last week) For every $\delta$, exists codes of length $n$, rate $r$, relative min distance $\delta n$
- Those provide graphs on $2^m = 2^{rn}$ vertices, of degree $n$, and second eval $2\delta n$. With some work we can show that max eval 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, $\Gamma$ and a binary operation $\circ$.
- For elements $g, h$ in $\Gamma$, $g \circ h$ is also an element of $\Gamma$. 
Groups

- $(\Gamma, \circ)$ form a group if
  - $\Gamma$ contains a special element called the identity (id) such that $\circ g \circ \text{id} = \text{id} \circ g = g$ for all $g \in \Gamma$
  - For every element $g \in \Gamma$, there is another element $g^{-1} \in \Gamma$ such that $g^{-1} \circ g = g \circ g^{-1} = \text{id}$
  - For every three elements $f, g, h \in \Gamma$, $(f \circ g) \circ h = f \circ (g \circ h)$
  - Group is abelian if for every $g, h \in \Gamma$, $g \circ h = h \circ g$
Groups: Examples You Already Know

1. (Integers, +)
2. (Z/n=Integers mod n, addition mod n)
3. (Z/p-o=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 \(\Gamma\) and the edges are the pairs

\[
\{(g, h) : h = g \circ s, \text{some } s \in S\} = \{(g, g \circ s) : s \in S\}
\]

E.g. Ring graph on \(n\) vertices if \((\Gamma, \circ) = (\mathbb{Z}/n, +)\)
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 \((\mathbb{Z}/n,+)\) and any set \(S\) of generators.
- Get \(\log n\) degree expanders from random set of \(\log n\) generators.