Pseudorandom Objects and Generators

Journées ALEA 2012
Lecture 1: Pseudorandom objects: examples and constructions

David Xiao
LIAFA
CNRS, Université Paris 7
Plan

• Today: examples of pseudorandom objects
  • Expander graphs
  • Error-correcting codes
• Tomorrow: applications of pseudorandom objects to computer science
Why Pseudorandom Objects?

- Because random objects are interesting!
- Can show random objects have many interesting properties
- "Probabilistic method": show existence of object satisfying some property
- Define probability distribution \( D \)
- Show \( \Pr_x \leftarrow D \{x \text{ does not satisfy property}\} \ll 1 \)
- First used systematically in work of Erdös
- For example, proves existence of good expander graphs and good error-correcting codes
Pseudorandom objects

- Great, random objects have nice properties
- **But**: usually need *explicit* constructions
  - Will see applications of expanders tomorrow
- **Explicit**: give algorithm for constructing size $n$ object in time $\text{poly}(n)$
Expander Graphs
Expander graphs

- Expander graphs: highly connected and sparse graphs, e.g. $|E| = O(|V|)$
- Useful: algorithms, network design, coding theory, graph theory, topology, geometry, group theory, number theory...
- Many equivalent definitions

- Def: for all sets $S \subseteq V$, where $|S| \leq |V|/2$ it holds that $|N(S)| \geq (3/2) |S|$
- Thm [Pinsker'73]: random graphs are expander graphs

Proof of bipartite case...
Expander graphs

- Expander graphs: highly connected and sparse graphs, e.g. $|E| = O(|V|)$
- Useful: algorithms, network design, coding theory, graph theory, topology, geometry, group theory, number theory...
- Many equivalent definitions

Random walk converges quickly to uniform
Defining Expanders

- Want family of \((n, D, \lambda)\) graphs with \(n \to \infty\), \(D\) constant, \(\lambda\) constant in \([0, 1]\)

- Suppose \(G\) is \((n, D, \lambda)\) expander, then:
  - \(G\) has vertex expansion [Alon-Milman’85, Tanner’84]:
    - For all \(S \subseteq V\), \(|S| \leq |V|/2\), it holds that
      \(|N(S)| \geq 2/(\lambda^2 + 1) |S|\)

Spectral expander: \(G\) is \((n, D, \lambda)\)-expander if:
- \(G\) is \(D\)-regular, \(|V| = n\)
- Let \(M = \text{adjacency matrix of } G\)
  - \(M_{ij} = 1/D\) if \((i, j) \in G\), 0 else
  - Eigenvalues of \(M\) in \([-1, 1]\)
  - Max eigenvalue = 1
  - \(\lambda \geq \) all other eigenvalues of \(M\) in absolute value
Defining Expanders

Suppose $G$ is $(n, D, \lambda)$ expander, then:

- **Expander Chernoff bound** [Gillman’93]:
  For any $S \subseteq V$, small $|S| \leq |V|/3$
  $\Pr[ \text{majority of random walk of length } t \text{ lies in } S ] < 2^{-(1-\lambda)t}$

**Spectral expander:** $G$ is $(n, D, \lambda)$-expander if:
- $G$ is $D$-regular, $|V| = n$
- Let $M = \text{adjacency matrix of } G$
  - $M_{ij} = 1/D$ if $(i, j) \in G$, $0$ else
  - Eigenvalues of $M$ in $[-1, 1]$
  - Max eigenvalue = 1
  - $\lambda \geq$ all other eigenvalues of $M$ in absolute value
Defining Expanders

- Suppose $G$ is $(n, D, \lambda)$ expander, then:
  - **Expander mixing lemma** [Alon-Chung’88]:
    For all $S, T \subseteq V$, \[ |E(S, T)| - |S||T| \frac{D}{n} \leq \lambda D \sqrt{|S||T|} \]

Spectral expander: $G$ is $(n, D, \lambda)$-expander if:
- $G$ is $D$-regular, $|V| = n$
- Let $M =$ adjacency matrix of $G$
  - $M_{ij} = 1/D$ if $(i, j) \in G$, $0$ else
  - Eigenvalues of $M$ in $[-1, 1]$
  - Max eigenvalue $= 1$
- $\lambda \geq$ all other eigenvalues of $M$ in absolute value

- Proof...
Defining Expanders

- Building expander graphs?
- \( V = \left( \mathbb{Z} / N \mathbb{Z} \right)^2 \)  
  E: \((x, y)\) connected to:  
  \((x, y + 2x), (x, y + 2x + 1), (x, y - 2x), (x, y - 2x - 1)\)  
  \((x + 2y, y), (x + 2y + 1, y), (x - 2y, y), (x - 2y - 1, y)\)

- Theorem [Gabber-Galil’81]: above is \((N^2, 8, 0.89)\)-expander

- Theorem [Lubotzky-Philips-Sarnak’88, Margulis’88]: constructions of “Ramanujan graphs” where \( \lambda = (2/D)\sqrt{(D-1)} \) (optimal [Alon’86])

- Theorem [Reingold-Vadhan-Wigderson’01]: combinatorial constructions of expander graphs

Spectral expander: \( G \) is \((n, D, \lambda)\)-expander if:
- \( G \) is \( D \)-regular, \( |V| = n \)
- Let \( M = \) adjacency matrix of \( G \)
  - \( M_{ij} = 1/D \) if \((i, j) \in G\), \( 0 \) else
  - Eigenvalues of \( M \) in \([-1, 1]\)
  - Max eigenvalue = 1
  - \( \lambda \geq \) all other eigenvalues of \( M \) in absolute value
Error correcting codes
Error correcting codes

• Alice and Bob communicate over noisy channel
• Encode messages to handle errors
• \([n, k, d]\) code:
  • Codeword length \(n\): bits transmitted across channel
  • Message length \(k\): bits before encoding
  • Distance \(d = 2 \times \) (maximum # of errors tolerated)
• Given \(n\), maximize \(k\) and \(d\)

Not very good code
A geometric view

- Code: subset of \( \{0,1\}^n \), codeword length \( n \)
- Message length \( k = \log(\# \text{ codewords}) \)
- Distance \( d \) = minimal distance between any two codewords
- Linear code: code forms subspace of \( \{0,1\}^n \cong \mathrm{GF}(2)^n \)
  - Suffices to define basis of subspace \( v_1 \ldots v_k \)
Theorem [G’52]: for all $n$ and $\varepsilon$, random code is a $[n, \varepsilon^2 n, n(1/2-\varepsilon)]$ code

Theorem [V’57]: for all $n$ and $\varepsilon$, random linear code is a $[n, \varepsilon^2 n, n(1/2-\varepsilon)]$ linear code

No known explicit codes with such good parameters

Theorem [Alon-Goldreich-Håstad-Peralta’92]: for all $\varepsilon$ and infinitely many $n$, can construct explicitly $[n, 2\varepsilon \sqrt{n}, n(1/2-\varepsilon)]$ linear code
Summary

- Pseudorandom objects: non-random objects that have some properties of random objects:
  - Expander graphs: connectivity
  - Error-correcting codes: large distance
- Common tools:
  - Extremal combinatorics
  - Linear Algebra
  - Group theory, representation theory
  - Finite fields, polynomials over finite fields
- Open questions: better constructions
  - Combinatorial construction of optimal expanders?
  - Binary linear codes matching Gilbert-Varshamov bound?
- Tomorrow: applications to computer science
Fin