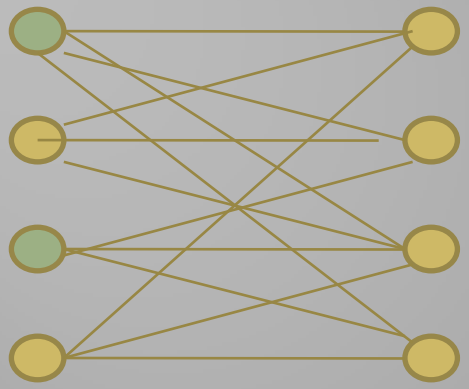
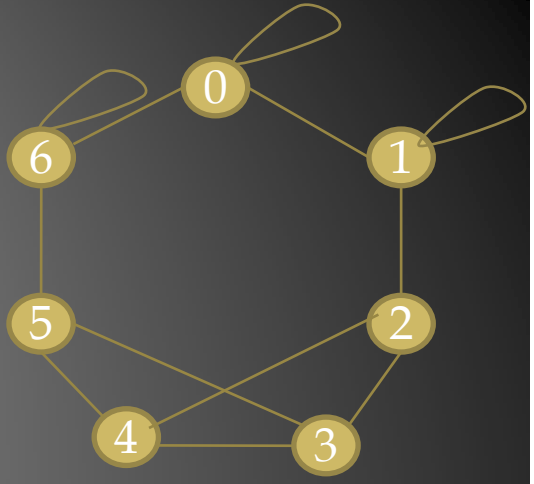




PROOF COMPLEXITY OF EXPANDER GRAPH TECHNIQUES

Antonina Kolokolova
Memorial University of Newfoundland

VNC^1 VTC^0

Barriers

- Understanding limits of proof techniques:
  - Diagonalization
  - Algebrization (limits of arithmetization technique)
  - Natural proofs

  - Power of proof techniques as provability in bounded arithmetic/proof complexity.

  - Expander graph-based techniques?

In Bounded Arithmetic:

- Independence in bounded arithmetic is related to lower bounds: e.g., Parity is not a total function in a theory for AC^0.
- If theory S^1_2 proves that a $f \in$ NP $\cap$ coNP, then f is polynomial-time computable (Buss).
- If S^1_2 proves Fermat Little Theorem, then there is a probabilistic polynomial time algorithm breaking RSA
- Natural proofs: unprovability of circuit lower bounds in such theories, assuming existence of pseudorandom number generators (Razborov).

Expander graphs

- Graphs which are both
  - sparse (usually constant degree)
  - and well connected (log length path between any two points.
- Expander graphs are pseudorandom objects.
- Random walk on an expander converges fast.

Uses of expanders

- As pseudorandom objects
  - One-way functions of Goldreich'2000
  - Cryptographic hash functions: Charles/Goren/Lauter...
  - Error-correcting codes, derandomization...
- In complexity theory
  - Reingold and Rozenman/Vadhan: USTCON in LogSpace
  - Dinur: combinatorial proof of the PCP theorem
  - Ajtai/Komlos/Szemeredi: AKS sorting networks

Existence and constructions

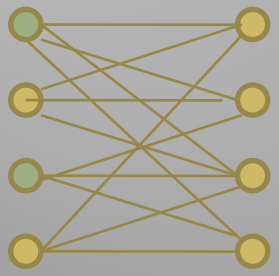
- A random graph is an expander with high probability (even 3-regular random graph)
- There are algebraic explicit constructions
- There are combinatorial constructions (with algebraic analysis).

Combinatorial definition of expanders

- Vertex Expansion: every "small enough" set of vertices has "a lot of" neighbours ($|\Gamma(S)| \geq \epsilon |S|$ for some constant ϵ).

- Edge expansion: equivalently, every set has many edges going to vertices outside the set.
  - $h(G) = \min_{\emptyset \neq U,\ |U| \leq n/2} |E(U, U^c)| / |U|$
  - (A minimum over all small sets) of an expected number of edges out of a random vertex in U going outside.

Examples of expanders

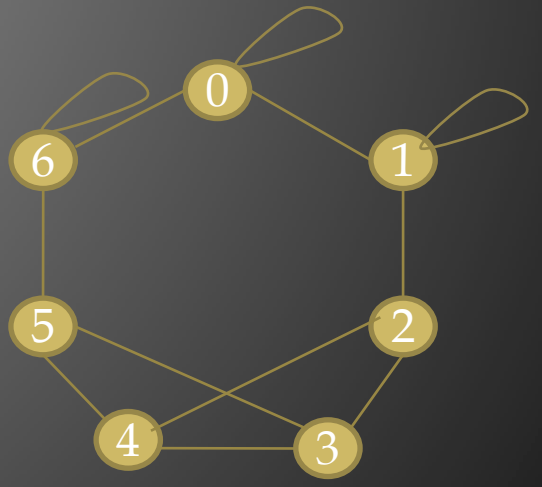


Example 1: Margulis, Gabber/Galil bipartite expanders.

(x,y) -> (x,y), (x,x+y), (x,x+y+1), (x+y,y), (x+y+1,y)

Example 2: (from Hoory/Linial/Wigderson)

G_p: for every $v \neq 0$, connect v to v-1, v+1 and v^{-1}.
For v=0, connect v to 0,1 and p-1.



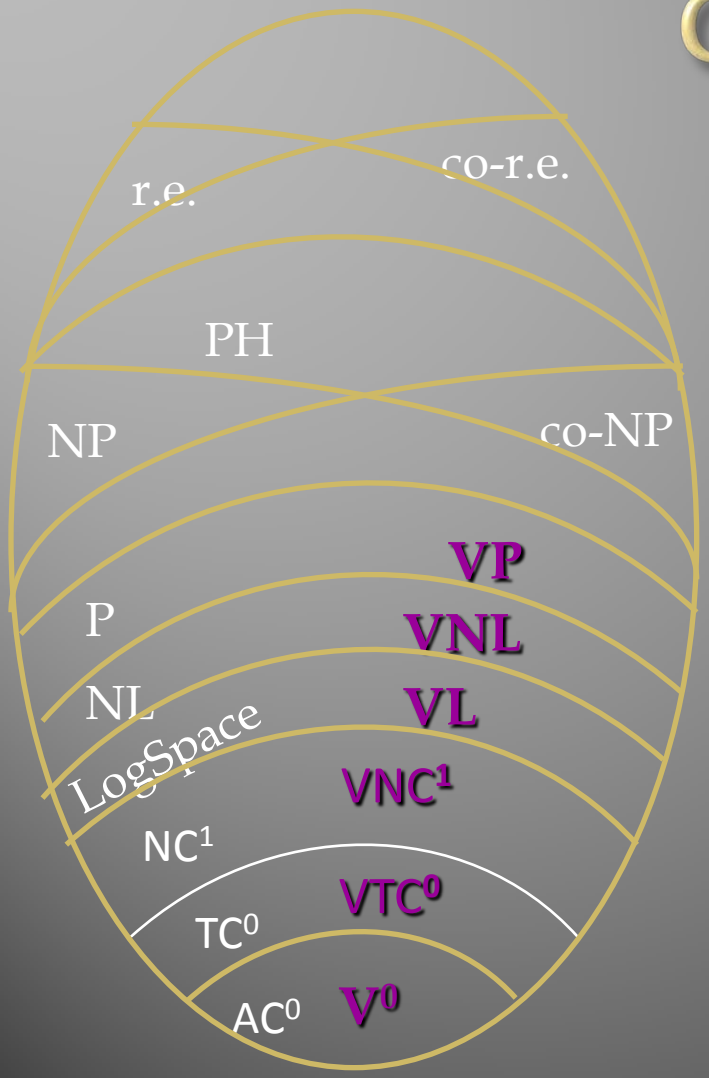
Bounded arithmetic

- Work in two-sorted setting, corresponding to inputs viewed as strings and auxiliary number inputs as string indices: formulas of the form $\phi(X,n)$.
- In formulas, all quantifiers are bounded by a polynomial in the length of the input (that is, length of string variables). $\exists Y, |Y| \leq p(|X|,n)$ ...

Bounded arithmetic vs. complexity classes

- Start with the basic axioms of Peano Arithmetic; add length induction over bounded formulas.
- This is the base theory V^0; complexity of functions it proves total is the same as data complexity of FO (it is functions of circuit class uniform AC^0).
- Now, add to V^0 axioms for totality of characteristic functions of predicates complete for corresponding complexity classes.
- Usually (for small classes) get theories proving totality of exactly the functions in that complexity class.

Complexity hierarchy



- Complexity classes with some corresponding theories
- We are mainly interested in the smallest classes, ones inside polynomial time.

BA theories examples

- V^1: V^0 + comprehension for NP predicates
- VTC^0: V^0 + "exists numones(y,X)=z"
- VNC^1: V^0 + "exists evaluation of a monotone formula on a balanced binary tree of n nodes"
- VP, VNL, VL...

Intuition: a theory V-C can reason with concepts from complexity class C.

QUESTION: WHAT CAN BE PROVEN USING ONLY "C-REASONING"? E.G., WHAT CAN BE PROVEN WITH POLYNOMIAL-TIME REASONING? TC^0 REASONING? LOGSPACE REASONING?

Bounded reverse mathematics

- Program suggested by Stephen Cook as a complexity analog of reverse mathematics of Harvey Friedman (see the book by Simpson)
- Question: what is the *computational complexity* of reasoning needed to prove theorems?
- Much done in Phuong Nguyen's thesis and after.
  - Main reference a book by Cook and Nguyen
  - A lot of work in this area...

Examples

- Discrete Jordan curve theorem is provable in VTC^0 (Cook/Nguyen)
- Closure of NL under complementation is provable in VNL (Cook/K)
- A theory capturing Approximate Counting (Jerabek)

- Modulo properties of expanders, correctness of AKS sorting networks is provable in a (slightly non-uniform version of) VNC^1. (Jerabek)

- Is "USTCON in LogSpace" (equivalently, SL=L) provable with LogSpace reasoning?

Work in progress

- Find a minimal theory proving existence of the families of expanders from the proofs above.
  - Formalize Reingold and/or Rozenman/Vadhan proofs in a corresponding theory.
  - First step: simple analysis of iterative combinatorial (such as zig-zag) construction.
  - Work in progress, joint with Kabanets and Koucky
- Show existence of a family of expanders with parameters needed for Jerabek's formalization of AKS sorting networks in his theory for NC^1.

Some proof ideas

- Define the expanders using mixing time; do not bother with eigenvalues.
- Only consider small integer (rational) vectors (should be sufficient because of the connection with vertex/edge expansion)
- Formalize tools such as Cauchy/Schwartz inequality.

Two ways of proving USTCON $\in$ LogSpace

- Reingold:
  - using zig-zag construction, convert the graph into a (polynomially larger) constant-degree expander.
  - Now, any s-t path has logarithmic length.
  - Needs existence of a constant-size expander.
- Rozenman/Vadhan:
  - "Square" the graph by putting an expander on its neighbourhood instead of a clique
  - Resulting graph has same size, polynomial degree, and (with some additional work) a guaranteed s-t edge if there was an s-t path in the original graph.
  - Needs a family of expanders of growing degree.
  - Algebraic analysis.

Algebraic definition

- The first definition of expander talked about its "edge expansion": number of outgoing edges of each set.
- An algebraic definition, more closely related to mixing properties:
  - Let λ_2 be the second largest eigenvalue of (the adjacency matrix of a d-regular graph) G.
  - Then λ_2 is closely related to edge expansion: in particular, it is constant iff edge expansion is.
  - Sometimes, a notation "(n,d,λ)-graph" is used to denote a d-regular graph on n vertices with second largest eigenvalue λ.

Combinatorial construction

- Reingold/Vadhan/Wigderson: Zig-zag product construction
  - Take a power of the graph (improving connectivity)
  - "Sparsify" the graph with zig-zag operation, increasing the number of vertices, but bringing the degree back down.
  - Analysis uses bounds on λ_2.

Expander Mixing Lemma

- Let S, T be arbitrary sets of vertices of a d-regular graph, and λ_2 the second eigenvalue of its adjacency matrix. Then

- $$| E(S,T) - d|S||T|/n | \leq \lambda_2 \sqrt{|S| |T|}$$

- An almost-converse is also true.

- We can consider a graph an expander if this property holds.

Future work

- Finish "work in progress": plans for this visit!
- Formalize other proofs using expanders?
  - Any interesting corollaries for proving security of expander-based crypto constructions?
  - Independence results for expander-based techniques? Barrier results?
- Other general techniques/possible barriers?