Expander graphs – Constructions, Connections and Applications

Avi Wigderson
IAS

'00 Reingold, Vadhan, W.
'01 Alon, Lubotzky, W.
'01 Capalbo, Reingold, Vadhan, W.
'02 Meshulam, W.
'04 Rozenman, Shalev, W.
'05 Reingold
'06 Hoory, Linial, W. "Expander graphs and applications" Bulletin of the AMS.

Expanding Graphs - Properties

- Combinatorial: no small cuts, high connectivity
- Probabilistic: rapid convergence of random walk
- Algebraic: small second eigenvalue

Theorem. [C,T,AM,A,JS] All properties are equivalent!

Expanders - Definition

Undirected, regular (multi)graphs.

Definition: The 2nd eigenvalue of a d-regular G

$\lambda(G) = \max \{ \| (A_G/d)\, v \| : \|v\|=1 , v \perp 1 \}$

$\lambda(G) \in [0,1]$

Definition: $\{G_i\}$ is an expander family if $\lambda(G_i) \leq \alpha < 1$

Theorem [P] Most 3-regular graphs are expanders.

Challenge: Explicit (small degree) expanders!

G is $[n,d]$-graph: n vertices, d-regular

G is $[n,d,\alpha]$-graph: $\lambda(G) \leq \alpha$.

Applications of Expanders

In CS

- Derandomization
- Circuit Complexity
- Error Correcting Codes
- Communication Networks
- Approximate Counting
- Computational Information
- Data Structures
- …

Applications of Expanders

In Pure Math

- Topology – expanding manifolds [B]

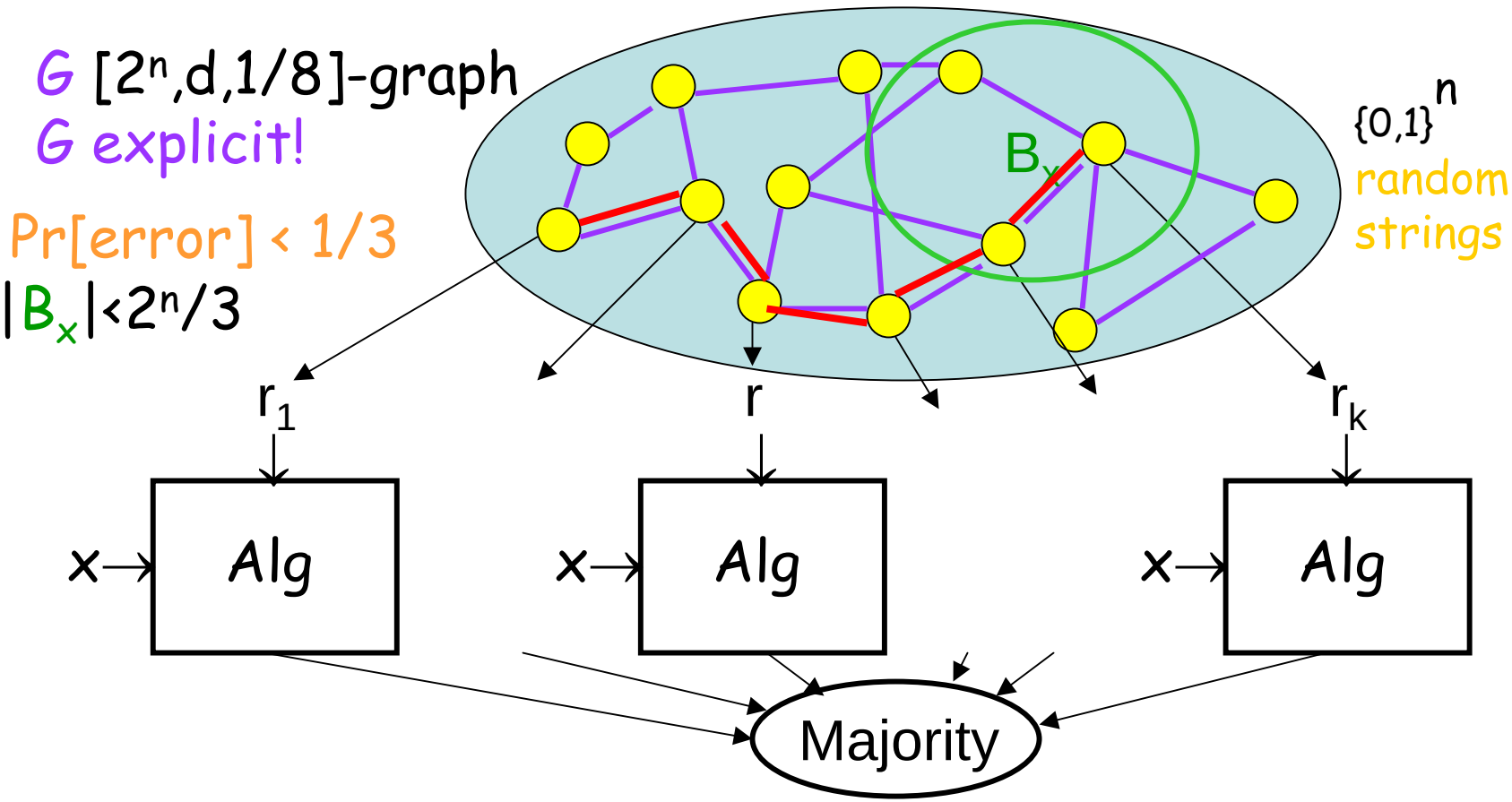
  - Baum-Connes Conjecture [G]
- Group Theory – generating random gp elements [Ba,LP]
- Measure Theory – Ruziewicz Problem [D,LPS],

  F-spaces [KR]
- Number Theory – Thin Sets [AIKPS],

  - Sieve method [BGS]

  - Dist of integer points on spheres [V]
- Graph Theory - …

Deterministic amplification



Thm [Chernoff] $r_1 r_2 \ldots r_k$ independent (kn random bits)

Thm [AKS] $r_1 r_2 \ldots r_k$ random path (n+ O(k) random bits)

then Pr[error] = $\Pr[|\{r_1 r_2 \ldots r_k\} \cap B_x\}| > k/2] < \exp(-k)$

Algebraic explicit constructions [M,GG,AM,LPS,L,...N,K]

Many such constructions are Cayley graphs.

A a finite group, S a set of generators.

Def. $C(A,S)$ has vertices A and edges (a, as) for all $a \in A$, $s \in S \cup S^{-1}$.

$A = SL_2(p)$: group 2 x 2 matrices of *det* 1 *over* Z_p.

$S = \{ M_1 , M_2 \}$: $M_1 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $M_2 = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$

Theorem. [L] $C(A,S)$ is an expander family.

Proof: "The mother group approach":

Appeals to a property of $SL_2(Z)$ proved by Selberg

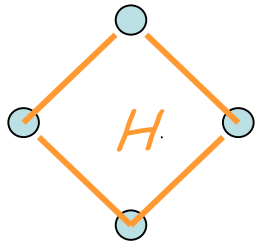
Algebraic Constructions (cont.)

Very explicit
-- computing neighbourhoods in logspace

Gives optimal results G_n family of $[n,d]$-graphs
-- **Theorem.** [AB] $d\lambda(G_n) \geq 2\sqrt{(d-1)}$
--**Theorem.** [LPS,M] Explicit $d\lambda(G_n) \leq 2\sqrt{(d-1)}$
(Ramanujan graphs)

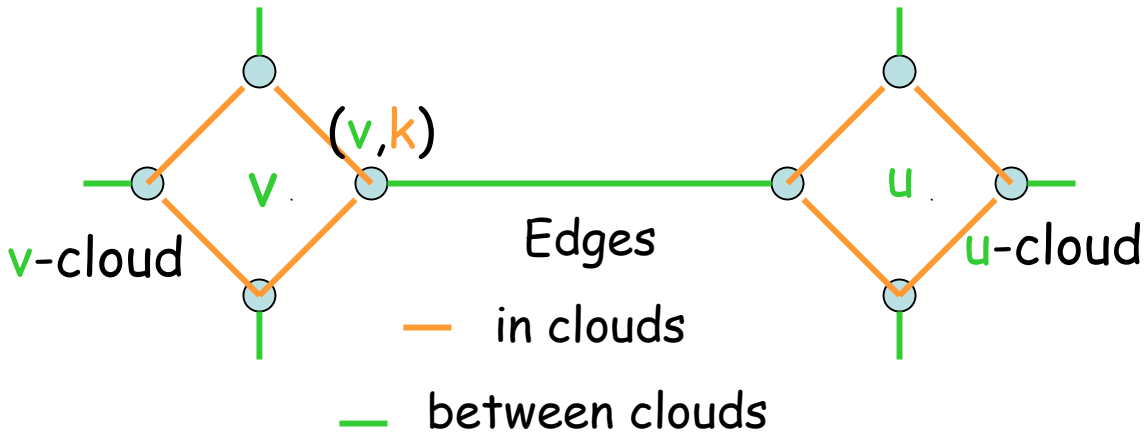
Hot off the press:
-- **Theorem** [KN] $SL_n(q)$ is expanding (q fixed!)
-- **Theorem** [K] Symmetric group S_n is expanding.
-- **Theorem** [L] All finite simple groups expand.
-- **Theorem** [H,BG] $SL_2(p)$ expands with most generators.

Explicit Constructions (Combinatorial)
-Zigzag Product [RVW]



G an $[n, m, \alpha]$-graph. H an $[m, d, \beta]$-graph.

Definition. $G \textcircled{z} H$ has vertices $\{(v,k) : v \in G, k \in H\}$.



Thm. [MR,RVW] $G \textcircled{z} H$ is an $[nm, d+1, f(\alpha,\beta)]$-graph, and $\alpha<1, \beta<1 \rightarrow f(\alpha,\beta)<1$.

$G \textcircled{z} H$ is an expander iff G and H are.

Combinatorial construction of expanders.

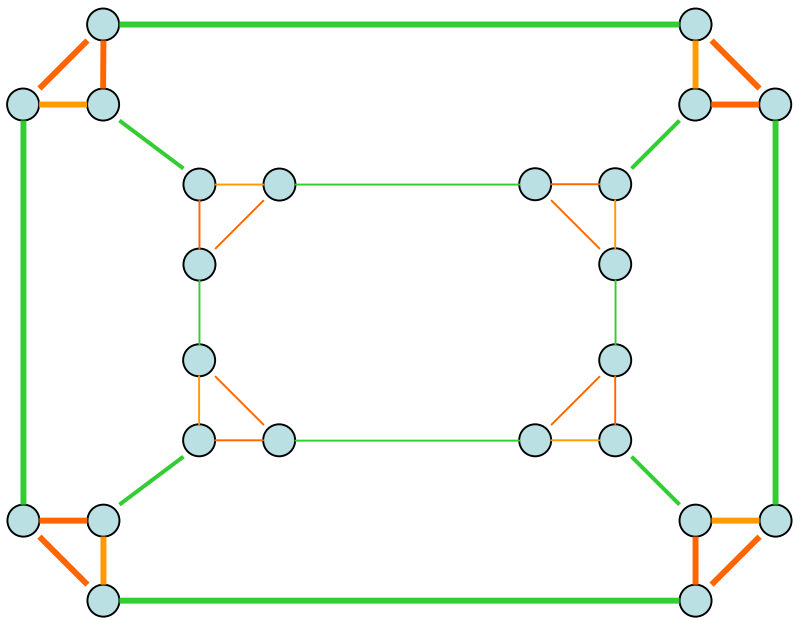
Example

$G=B_2^m$, the Boolean m-dim cube ($[2^m,m]$-graph).

$H=C_m$, the m-cycle ($[m,2]$-graph).

$G \textcircled{z} H$ is the cube-connected-cycle ($[m2^m,3]$-graph)

m=3



Iterative Construction of Expanders

A stronger product $\textcircled{z'}$:

G an $[n,m,\alpha]$-graph. H an $[m,d,\beta]$ -graph.

Theorem. [RVW] $G \textcircled{z'} H$ is an $[nm,d^2,\alpha+\beta]$-graph.

Proof: Follows simple information theoretic intuition.

The construction:

Start with a constant size H a $[d^4,d,1/4]$-graph.

- $G_1 = H^2$
- $G_{k+1} = G_k^2 \textcircled{z'} H$

Theorem. [RVW] G_k is a $[d^{4k}, d^2, \frac{1}{2}]$-graph.

Proof: G_k^2 is a $[d^{4k},d^4, \frac{1}{4}]$-graph.

H is a $[d^4, d, \frac{1}{4}]$-graph.

G_{k+1} is a $[d^{4(k+1)}, d^2, \frac{1}{2}]$-graph.

Consequences of the zigzag product

- Isoperimetric inequalities beating e-value bounds

  [RVW, CRVW]

- Connection with semi-direct product in groups

  [ALW]

- New expanding Cayley graphs for non-simple groups

  [MW, RSW]

- **SL=L** : How to get out of every maze deterministically

  [Reingold '05]

Semi-direct Product of groups

A, B groups. B acts on A as automorphisms.

Let a^b denote the action of b on a.

Definition. $A \times B$ has elements $\{(a,b) : a \in A, b \in B\}$.

group mult $(a',b')(a,b) = (a'a^{b'}, b'b)$

Connection: semi-direct product is a special case of zigzag

Assume $\langle T \rangle = B$, $\langle S \rangle = A$, $S = s^B$ (S is a single B-orbit)

Theorem [ALW] $C(A \times B, \{s\} \cup T) = C(A,S) \textcircled{z} C(B,T)$

Proof: By inspection $(a,b)(1,t) = (a,bt)$ (Step in a cloud)

$(a,b)(s,1) = (as^b, b)$ (Step between clouds)

Theorem [ALW] Expansion is not a group property

Theorem [MW,RSW] Iterative construction of Cayley expanders

Beating e-value expansion [WZ, RVW]

In the following a is a large constant.

Task: Construct an $[n,d]$-graph s.t. every two sets of size n/a are connected by an edge. Minimize d

Ramanujan graphs: $d=\Omega(a^2)$

Random graphs: $d=O(a \log a)$

Zig-zag graphs: [RVW] $d=O(a(\log a)^{O(1)})$

Uses zig-zag product on extractors!

Applications

Sorting in rounds, Superconcentrators,…

Lossless expanders [CRVW]

Task: Construct an $[n,d]$-graph in which every set of size at most n/a expands by a factor c. Maximize c.

Upper bound: $c \leq d$

Ramanujan graphs: [K] $c \leq d/2$

Random graphs: $c \geq (1-\varepsilon)d$ Lossless

Zig-zag graphs: [CRVW] $c \geq (1-\varepsilon)d$ Lossless

Use zig-zag product on conductors!!

Extends to unbalanced bipartite graphs.

Applications (where the factor of 2 matters):
Data structures, Network routing, Error-correcting codes

Error Correcting Codes [Shannon, Hamming]

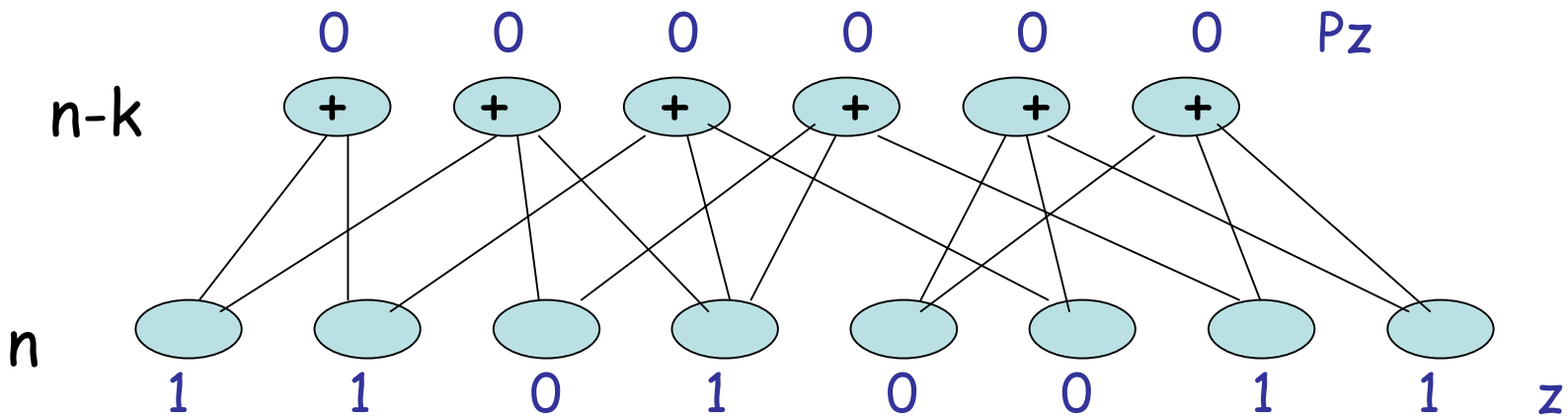
$C: \{0,1\}^k \rightarrow \{0,1\}^n$ $\quad C=\mathrm{Im}(C)$

Rate $(C) = k/n$ $\quad$ Dist $(C) = \min d(C(x),C(y))$

C good if Rate $(C) = \Omega(1)$, Dist $(C) = \Omega(n)$

Find good, explicit, efficient codes.

Graph-based codes [G,M,T,SS,S,LMSS,…]



$z \in C$ iff $Pz=0$ $\quad$ C is a linear code

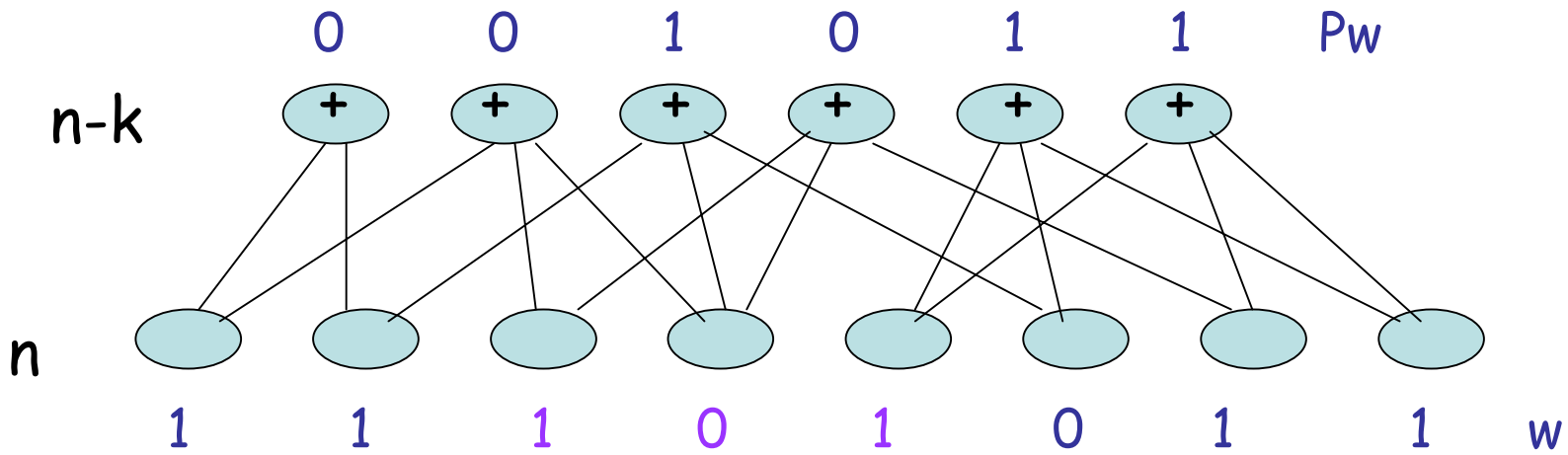
Trivial $\quad$ Rate $(C) \geq k/n$, Encoding time $= O(n^2)$

G lossless $\rightarrow$ Dist $(C) = \Omega(n)$, Decoding time $= O(n)$

Decoding

Thm [CRVW] Can explicitly construct graphs:

k=n/2, bottom deg = 10, $\forall B \subseteq [n]$, $|B| \le n/200$, $|\Gamma(B)| \ge 9|B|$



Decoding alg [SS]: while $Pw \neq 0$ flip all w_i with i in

FLIP = { i : $\Gamma(i)$ has more 1's than 0's }

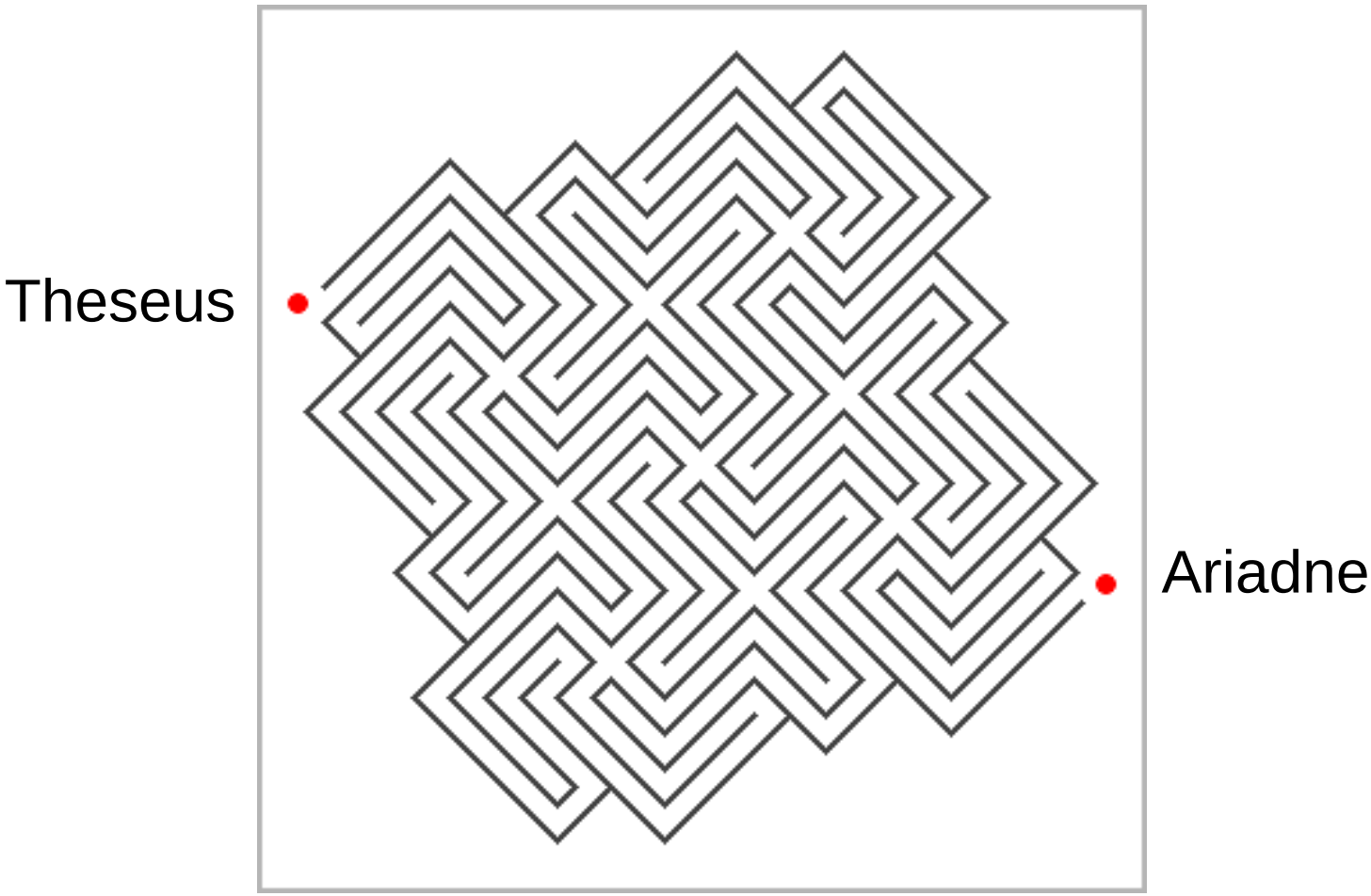
B = set of corrupted positions $|B| \le n/200$

B' = set of corrupted positions after flip

Claim [SS] : $|B'| \le |B|/2$

Proof: $|B \setminus FLIP| \le |B|/4$, $|FLIP \setminus B| \le |B|/4$

Escaping mazes deterministically, or Graph connectivity in logspace [R'05]



Crete, ~1000 BC

Expander from any connected graph [R]

A stronger product $\textcircled{z'}$:

G an $[n,m,\alpha]$-graph.

H an $[m,d,\beta]$ -graph.

Theorem. $G \textcircled{z'} H$ is an $[nm, d^2, \alpha+\beta]$-graph.

The construction:

Fix a constant size H a $[d^4,d,1/4]$-graph.

- $G_1 = H^2$
- $G_{k+1} = G_k^2 \textcircled{z'} H$

Theorem. [RVW] G_k is a $[d^{4k}, d^2, \frac{1}{2}]$-graph

Proof: G_k^2 is a $[d^{4k}, d^4, \frac{1}{4}]$-graph.

H is a $[d^4, d, \frac{1}{4}]$-graph.

G_{k+1} is a $[d^{4(k+1)}, d^2, \frac{1}{2}]$-graph.

G an $[n,m, 1-\varepsilon]$-graph.

H an $[m,d,1/4]$ -graph.

$[nm, d^2, 1-\varepsilon/2]$-graph.

H a $[d^{10},d,1/4]$-graph.

- $G_1 = G$
- $G_{k+1} = G_k^5 \textcircled{z} H$

Thm[R] G_1 is $[n, d^2, 1/n^3]$

➔ $G_{\log n}$ is $[n^{O(1)}, d^2, \frac{1}{2}]$

Undirected connectivity in Logspace [R05]

Algorithm

-Input $G=G_1$ an $[n,d^2]$-graph

- Compute $G_{\text{clog } n}$

-Try all paths of length clog n from vertex 1.

Correctness

- G_{i+1} is connected iff G_i is

- If G is connected than it is an $[n,d^2, 1-1/n^3\ ]$-graph

- G_1 connected → $G_{\text{clog } n}$ has diameter < clog n

-Space bound

- G_{i+1} from G_i requires constant space (squaring and zigzag are local)

- $G_{\text{clog } n}$ from G_1 requires O(log n) space

Distributed routing [Sh,PY,Up,ALM,…]

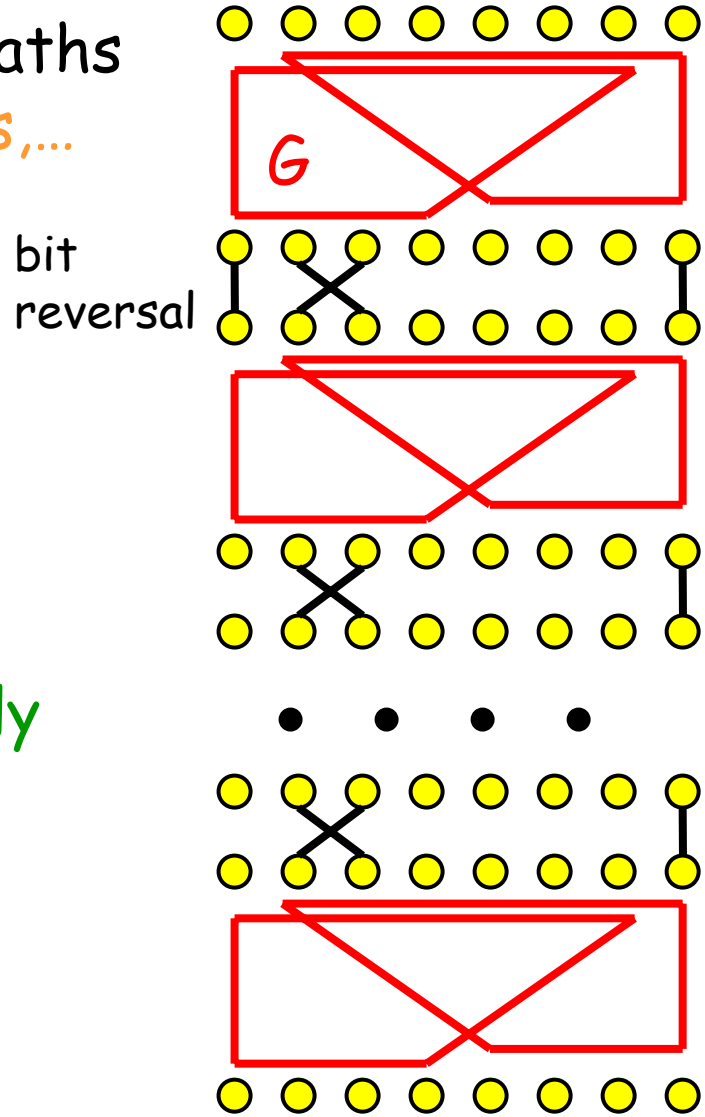
n inputs, n outputs, many disjoint paths
Permutation,Non-blocking networks,…

G 2-matching Butterfly
every path, bottlenecks

G expander multi-Butterfly
many paths, global routing

G lossless expander multi-Butterfly
many paths, local routing

Key: Greedy local alg in G
finds perfect matching



Open Questions

- Explicit undirected, const degree, lossless expanders
- Explicit dimension expanders
- Better understand expansion in groups
- Better understand and relate pseudo-random objects
  - expanders
  - extractors
  - hash functions
  - samplers
  - error correcting codes
  - Ramsey graphs