Expander graphs – a ubiquitous pseudorandom structure
(applications & constructions)

Avi Wigderson
IAS, Princeton

Monograph: [Hoory, Linial, W. 2006]
"Expander graphs and applications"
Bulletin of the AMS.
Tutorial: [W'10]
www.math.ias.edu/~avi

Applications

in Math & CS

Applications of Expanders

In CS

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

Applications of Expanders

In Pure Math

- Topology – expanding manifolds [Brooks]

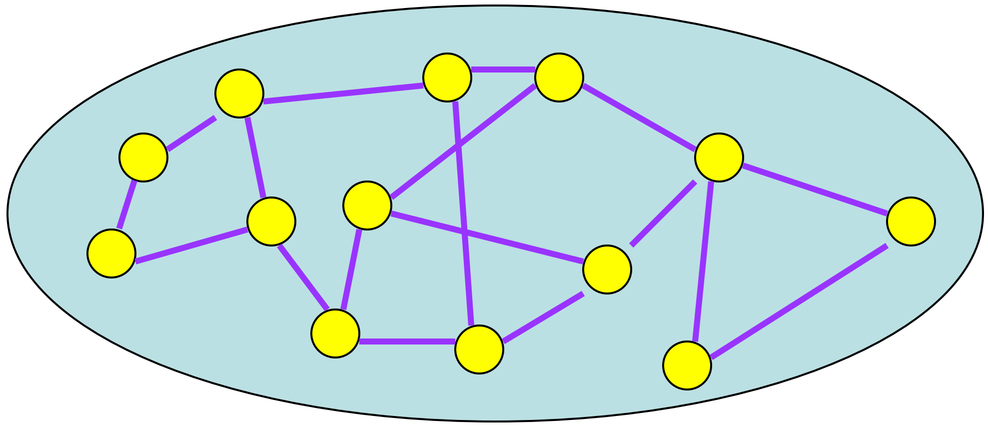
  - Baum-Connes Conjecture [Gromov]
- Group Theory – generating random group elements [Babai,Lubotzky-Pak]
- Measure Theory – Ruziewicz Problem [Drinfeld, Lubotzky-Phillips-Sarnak], *F*-spaces [Kalton-Rogers]
- Number Theory Thin Sets [Ajtai-Iwaniec-Komlos-Pintz-Szemeredi] -Sieve method [Bourgain-Gamburd-Sarnak]

  - Distribution of integer points on spheres [Venkatesh]
- Graph Theory - …

Expander graphs:

Definition and basic properties

Expanding Graphs - Properties



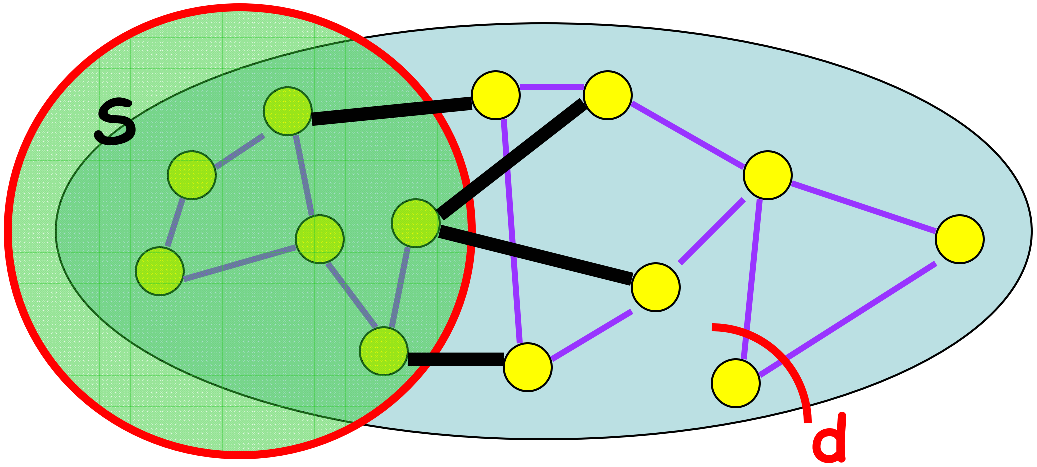
- Combinatorial/Goemetric

- Probabilistic

- Algebraic

Theorem. [Cheeger, Buser, Tanner, Alon-Milman, Alon, Jerrum-Sinclair,…]: All properties are equivalent!

Expanding Graphs - Properties



$G(V,E)$

V vertices, E edges

$|V|=n$ (∞)

d-regular (d fixed)

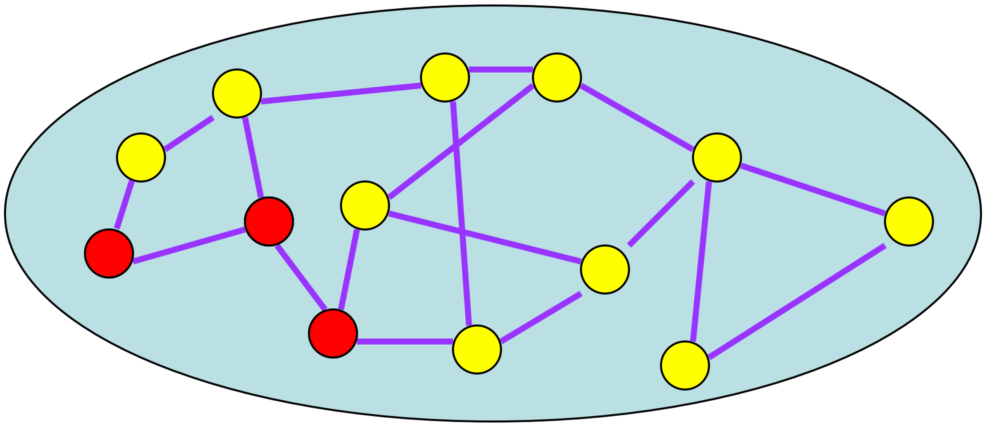
$\forall S\ |S| < n/2$

$|E(S,S^c)| > \alpha |S| d$ (what we expect in a random graph)

α constant

- Combinatorial: no small cuts, high connectivity
- Geometric: high isoperimetry

Expanding Graphs - Properties



$G(V,E)$

d-regular

$v_1, v_2, v_3, \dots, v_t, \dots$

v_{k+1} a random neighbor of v_k

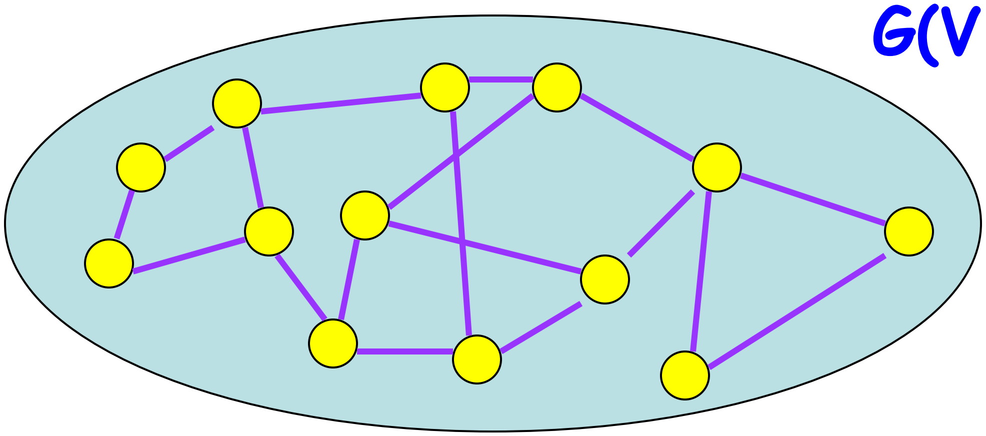
v_t converges to the uniform distribution

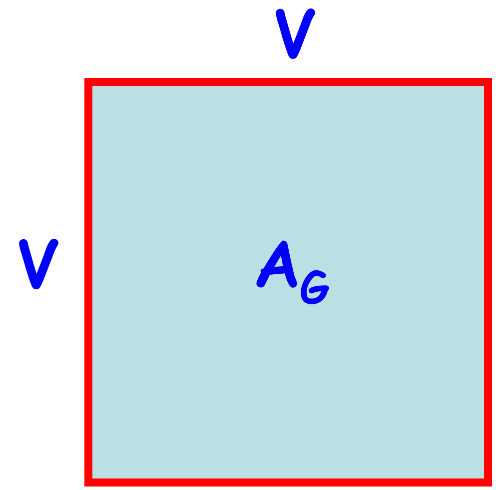
in $O(\log n)$ steps (as fast as possible)

- **Probabilistic:** rapid convergence of random walk

Expanding Graphs - Properties

$G(V,E)$





$1 = \lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n \geq -1$

$\lambda(G) = \max_{i>1} |\lambda_i| =$

$\max \{ \|A_G v\| : \|v\| = 1,\ v \perp u \}$

$\lambda(G) \leq \delta < 1$

$1 - \lambda(G)$ "spectral gap"

$$A_G(u,v) = \begin{cases} 0 & (u,v) \notin E \\ 1/d & (u,v) \in E \end{cases}$$

normalized adjacency matrix

(random walk matrix)

- **Algebraic:** small second eigenvalue

Expanders – Definition & Existence

Undirected, regular (multi)graphs.

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

G is [n,d, δ]-graph: $\lambda(G) \leq \delta$. G expander if $\delta < 1$.

Definition: An infinite family $\{G_i\}$ of [n_i,d, δ]-graphs is an expander family if for all i $\delta < 1$.

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

Challenge: Construct ***Explicit*** (small degree) expanders!

Pseudorandomness: G $[n,d,\delta]$-graph

Thm. For all $S,T \subseteq V$, $|E(S,T)| = d|S||T|/n \pm \delta dn$

edges from S to T	expectation in random graph	small error

Cor 1: Every set of size > δn contains an edge.

Chromatic number (G) > $1/\delta$

Graphs of large girth and chromatic number

Cor 2: Removing any fraction $\gamma < \delta$ of the edges leaves a connected component of $1-O(\gamma)$ of the vertices.

Networks

- Fault-tolerance
- Routing
- Distributed computing
- Sorting

Infection Processes: G $[n,d,\delta]$-graph, $\delta<1/4$

Cor 3: Every set S of size $s < \delta n/2$ contains at most $s/2$ vertices with a majority of neighbors in S

Infection process 1: Adversary infects I_0, $|I_0| \leq \delta n/4$.

$I_0=S_0, S_1, S_2, \ldots S_t, \ldots$ are defined by:

$v \in S_{t+1}$ **iff a majority of its neighbors are in** S_t.

Fact: $S_t=\varnothing$ for $t > \log n$ [**infection dies out**]

Infection process 2: Adversary picks $I_0, I_1, \ldots$, $|I_t| \leq \delta n/4$.

$I_0=R_0, R_1, R_2, \ldots R_t, \ldots$ are defined by $R_t = S_t \cup I_t$

Fact: $|R_t| \leq \delta n/2$ for all t [**infection never spreads**]

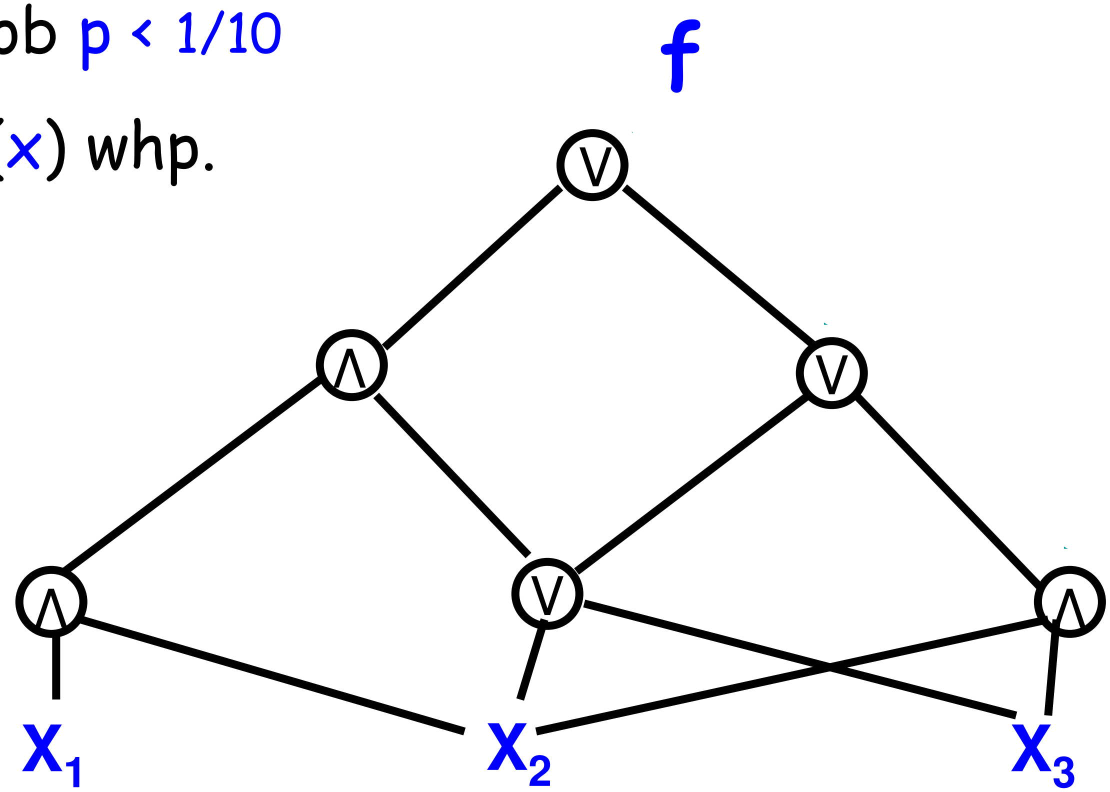
Reliable circuits from unreliable components [von Neumann]

Given, a circuit C for f of size s

Every gate fails with prob $p < 1/10$

Construct C' for $C'(x)=f(x)$ whp.

Possible? With small s'?



Reliable circuits from unreliable components
[von Neumann]

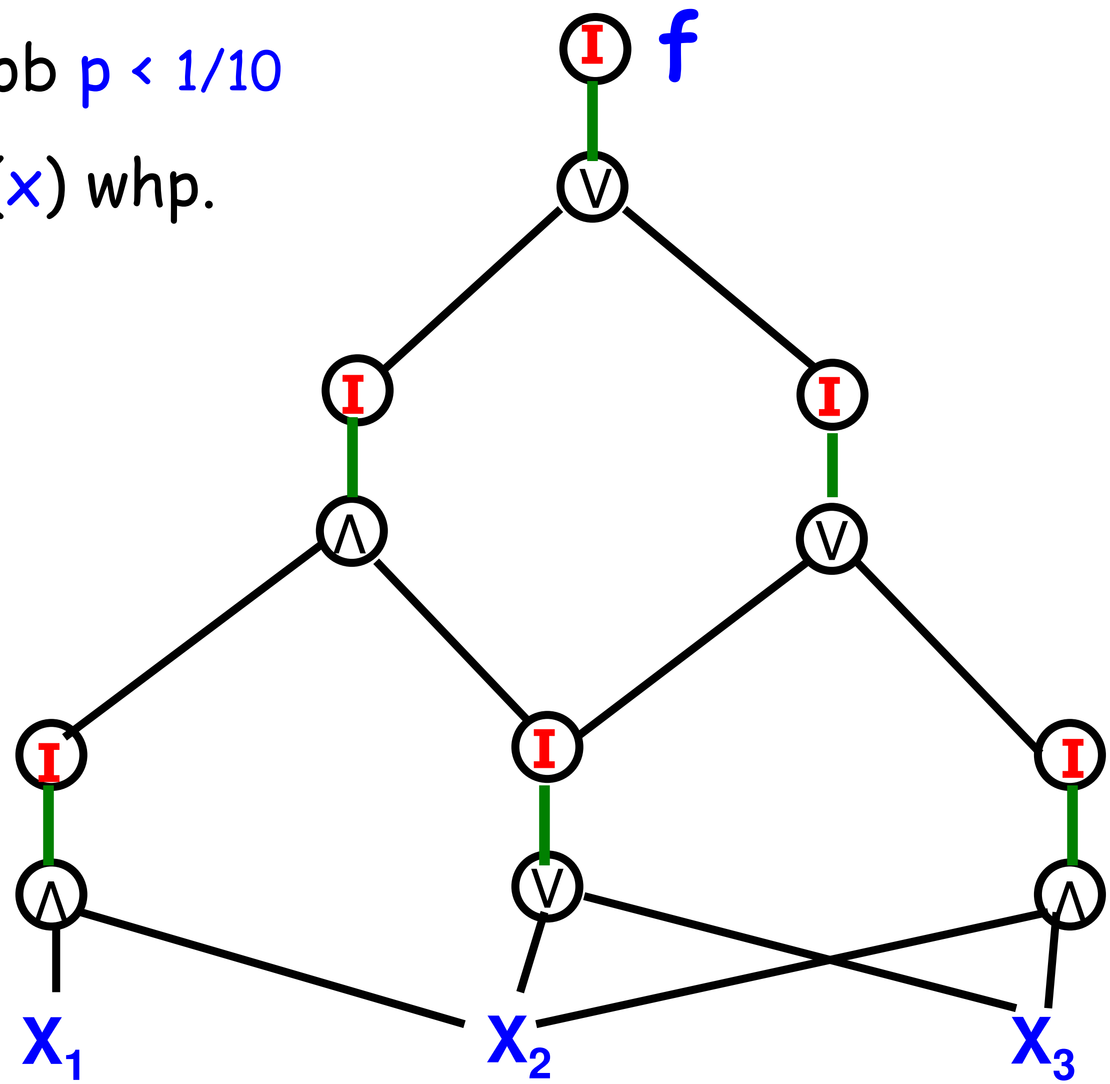
Given, a circuit C for f of size s

Every gate fails with prob $p < 1/10$

Construct C' for $C'(x)=f(x)$ whp.

Possible? With small s'?

- Add Identity gates



Reliable circuits from unreliable components
[von Neumann]

Given, a circuit C for f of size s

Every gate fails with prob $p < 1/10$

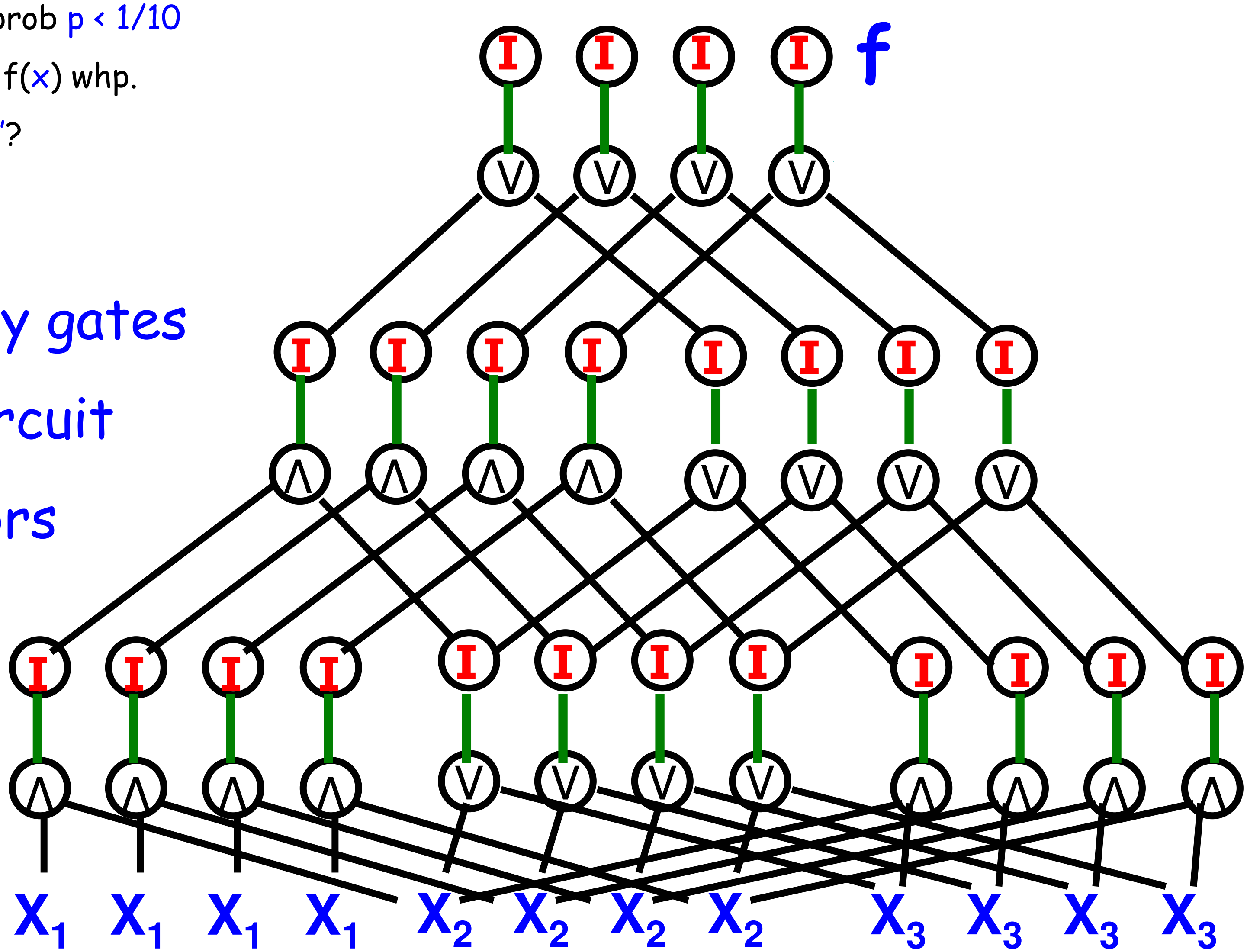
Construct C' for $C'(x)=f(x)$ whp.

Possible? With small s'?

-Add Identity gates

-Replicate circuit

-Reduce errors



Reliable circuits from unreliable components
[von Neumann, Dobrushin-Ortyukov, Pippenger]

Given, a circuit C for f of size s

Every gate fails with prob $p < 1/10$

Construct C' for $C'(x)=f(x)$ whp.

Possible? With small s'?

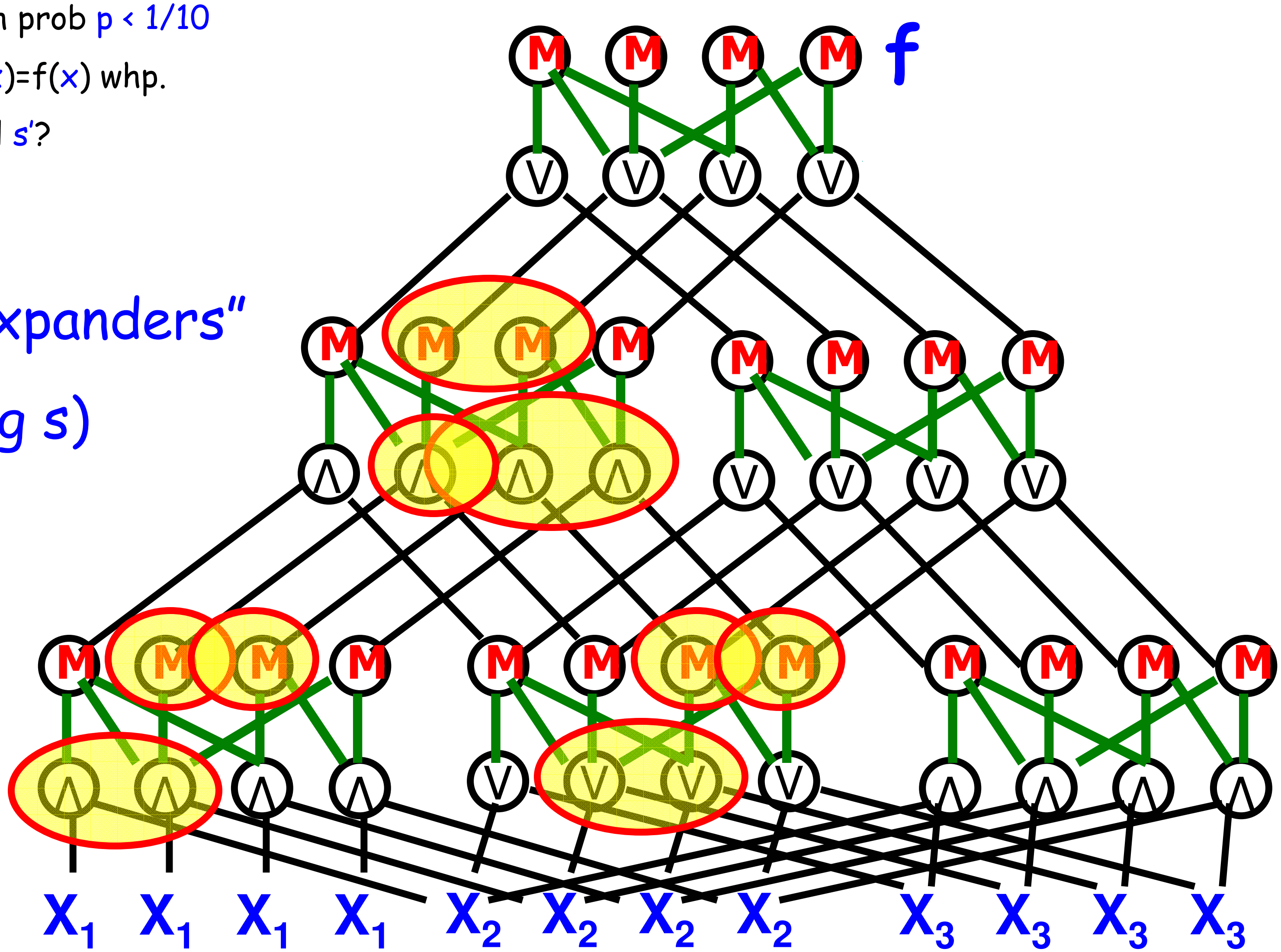
Majority "expanders"

of size $O(\log s)$

Analysis:

Infection

Process 2



Derandomization

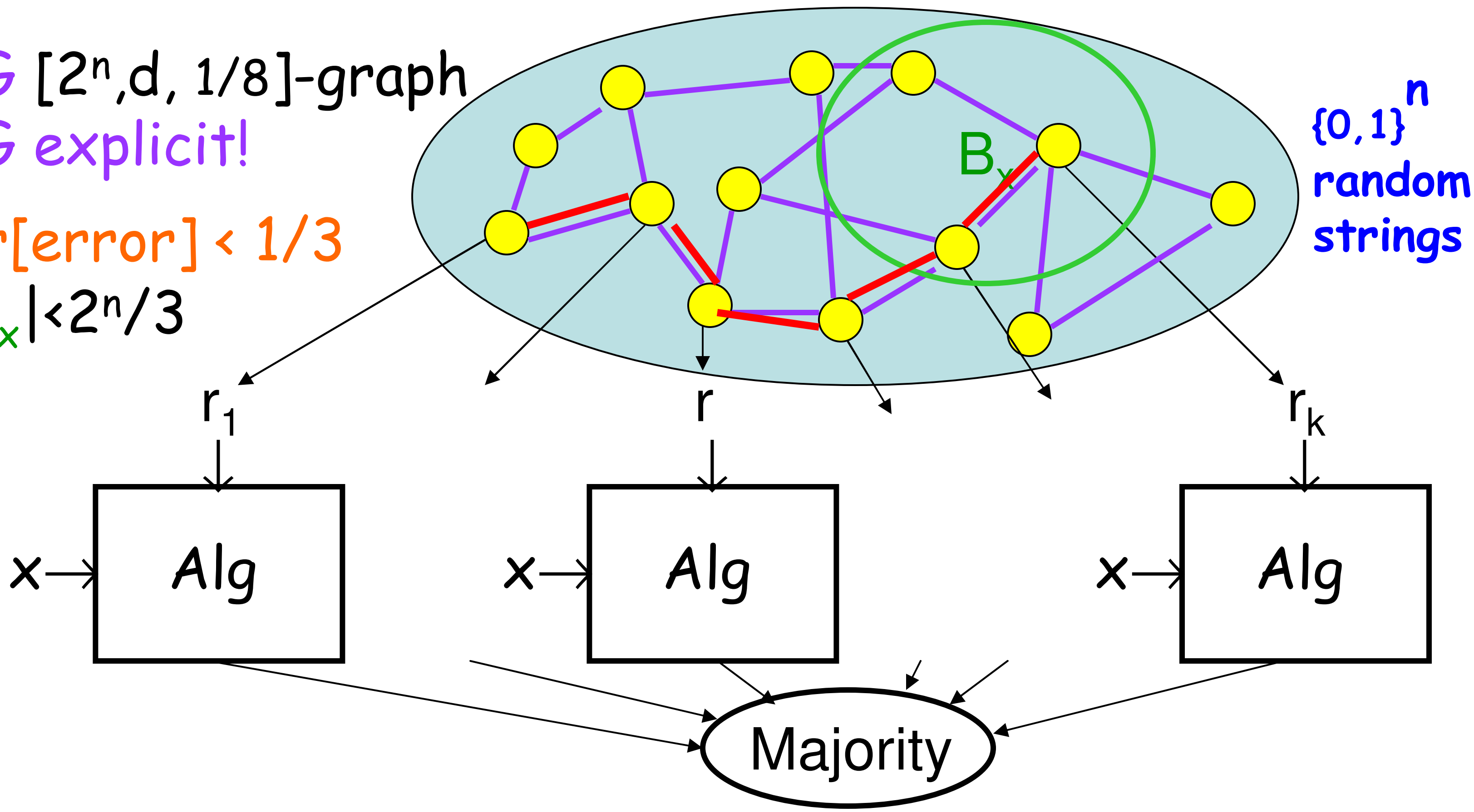
Deterministic error reduction

G $[2^n, d, 1/8]$-graph

G explicit!

Pr[error] < 1/3

$|B_x| < 2^n/3$



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)

Metric embeddings

Metric embeddings (into l_2)

Def: A metric space (X,d) embeds with distortion Δ into l_2 if $\exists\, f : X \to l_2$ such that for all x,y

$$d(x,y) \le \| f(x)-f(y) \| \le \Delta\, d(x,y)$$

Theorem: [Bourgain] Every n-point metric space has a $O(\log n)$ embedding into l_2

Theorem: [Linial-London-Rabinovich] This is tight! Let (X,d) be the distance metric of an $[n,d]$-expander G.

Proof: $\langle f,(A_G-J/n)f \rangle \le \lambda(G)\,\|f\|^2$ $\quad$ ($2ab = a^2+b^2-(a-b)^2$)

$(1-\lambda(G))E_{x,y}\,[(f(x)-f(y))^2] \le E_{x\sim y}\,[(f(x)-f(y))^2]$ **(Poincare inequality)**

$(c\log n)^2 \le$ $\quad$ All pairs $\quad$ Neighbors $\quad \le \Delta^2$

Metric embeddings (into l_2)

Def: A metric space (X,d) has a coarse embedding into l_2 if $\exists\, f : X \to l_2$ and increasing, unbounded functions $\phi,\sigma:R\to R$ such that for all x,y

$$\phi(d(x,y)) \leq \| f(x)-f(y) \|_2 \leq \sigma(d(x,y))$$

Theorem: [Gromov] There exists a finitely generated, finitely presented group, whose Cayley graph metric has no coarse embedding into l_2

Proof: Uses an infinite sequence of Cayley expanders…

Comment: Relevant to the Novikov & Baum-Connes conjectures

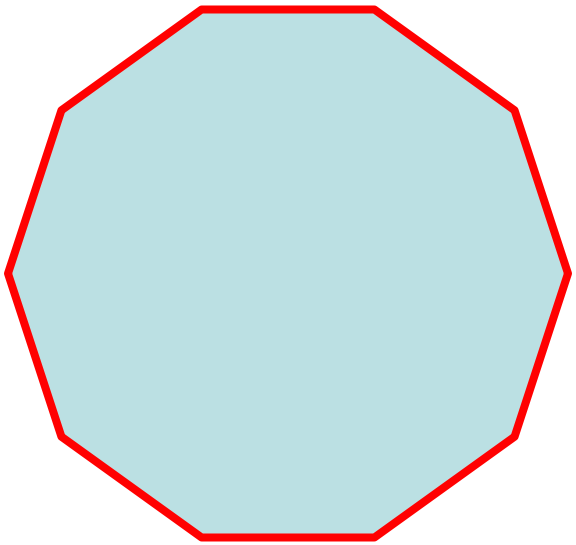
Extensions: Poincare inequalities for any uniformly convex norms ("super expander" [Lafforgue, Mendel-Naor])

Constructions

Expansion of Finite Groups

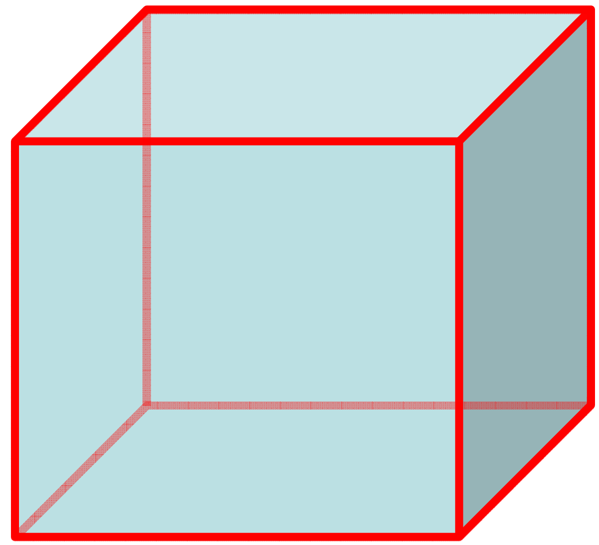
G finite group, $S \subseteq G$, symmetric. The Cayley graph

$Cay(G;S)$ has $x \quad sx$ for all $x \in G$, $s \in S$.



$Cay(C_n ; \{-1,1\})$

$\lambda(G) \approx 1-1/n^2$



$Cay(F_2^n ; \{e_1, e_2, \ldots, e_n\})$

$\lambda(G) \approx 1-1/n$

Basic Q: for which G,S is $Cay(G;S)$ expanding ?

Algebraic explicit constructions [Margulis,Gaber-Galil,Alon-Milman,Lubotzky-Philips-Sarnak,…Nikolov,Kassabov,..]

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

$S = \{ M_1 , M_2 \}$: $M_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $M_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$

Theorem. [LPS] Cay(A,S) is an expander family.

Proof: "The mother group approach":

Appeals to a property of $SL_2(Z)$ [Selberg's 3/16 thm]

Strongly explicit: Say that we need n bits to describe a matrix M in $SL_2(p)$. $|V|=\exp(n)$

Computing the 4 neighbors of M requires poly(n) time!

Algebraic Constructions (cont.)

Very explicit
-- computing neighbourhoods in logspace

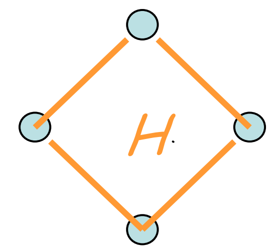
Gives optimal results G_n family of [n, d]-graphs
-- **Theorem.** **[AB]** $d\lambda(G_n) \geq 2\sqrt{(d-1)}$
--**Theorem.** **[LPS,M]** Explicit $d\lambda(G_n) \leq 2\sqrt{(d-1)}$
(Ramanujan graphs)

Recent results:
-- **Theorem** **[KLN]** All* finite simple groups expand.
-- **Theorem** **[H,BG]** $SL_2(p)$ expands with most generators.
-- **Theorem** **[BGT]** same for all Chevalley groups

Zigzag graph product

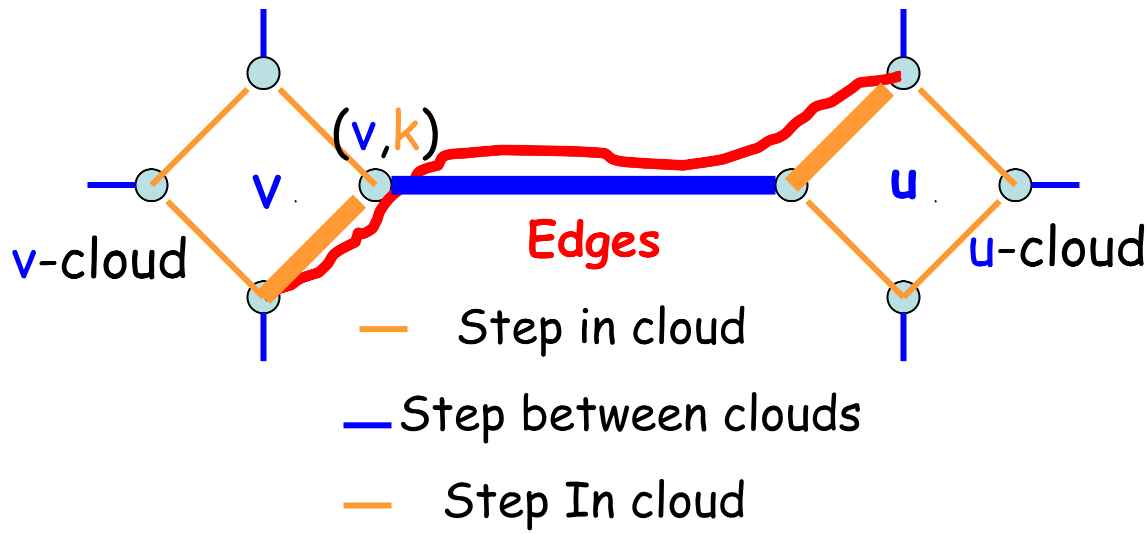
Combinatorial construction of expanders

Explicit Constructions (Combinatorial)
-Zigzag Product [Reingold-Vadhan-W]



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

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



Thm. [RVW] G ⓩ H is an $[nm, d^2, \alpha+\beta]$-graph,

G ⓩ H is an expander iff G and H are.

Combinatorial construction of expanders.

Iterative Construction of Expanders

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

Theorem. [RVW] $G Ⓩ H$ is an $[nm,d^2,\alpha+\beta]$-graph.

The construction:

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

- $G_1 = H^2$
- $G_{k+1} = G_k^2 Ⓩ H$

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
  [Reingold-Vadhan-W, Capalbo-Reingold-Vadhan-W]
- Connection with semi-direct product in groups
  [Alon-Lubotzky-W]
- New expanding Cayley graphs for *non-simple* groups
  [Meshulam-W] : Iterated group algebras
  [Rozenman-Shalev-W] : Iterated wreath products
- **SL=L** : Escaping every maze deterministically [Reingold '05]
- Super-expanders [Mendel-Naor]
- Monotone expanders [Dvir-W]

Beating eigenvalue expansion

Lossless expanders (perfect isoperimetry)

[Capalbo-Reingold-Vadhan-W]

Task: Construct an $[n,d]$-graph in which every set S, $|S| \ll n/d$ has $> c|S|$ neighbors. Max c (vertex expansion)

Upper bound: $c \leq d$

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

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

Error Correcting Codes [Shannon, Hamming]

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

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

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

Theorem: [Shannon '48] Good codes exist (prob. method)

Challenge: Find good, explicit, efficient codes.

- Many explicit algebraic constructions: [Hamming, BCH, Reed-Solomon, Reed-muller, Goppa,…]

- Combinatorial constructions [Gallager, Tanner, Luby-Mitzenmacher-Shokrollahi-Spielman, Sipser-Spielman..]

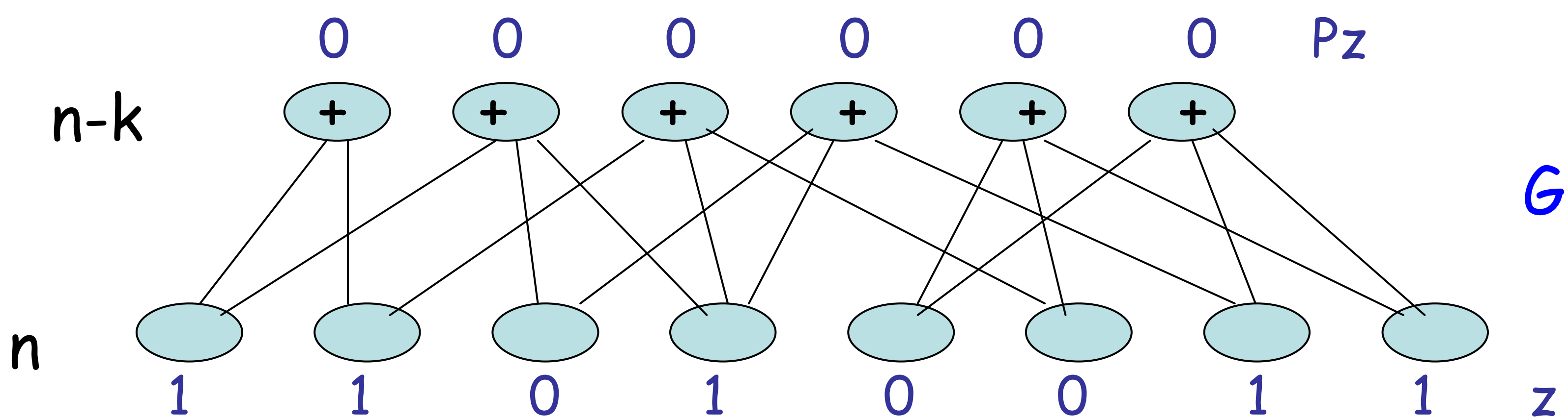
Thm: [Spielman] good, explicit, $O(n)$ encoding & decoding

Graph-based Codes [Gallager'60s]

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

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

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



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

LDPC: Low Density Parity Check   (G has constant degree)

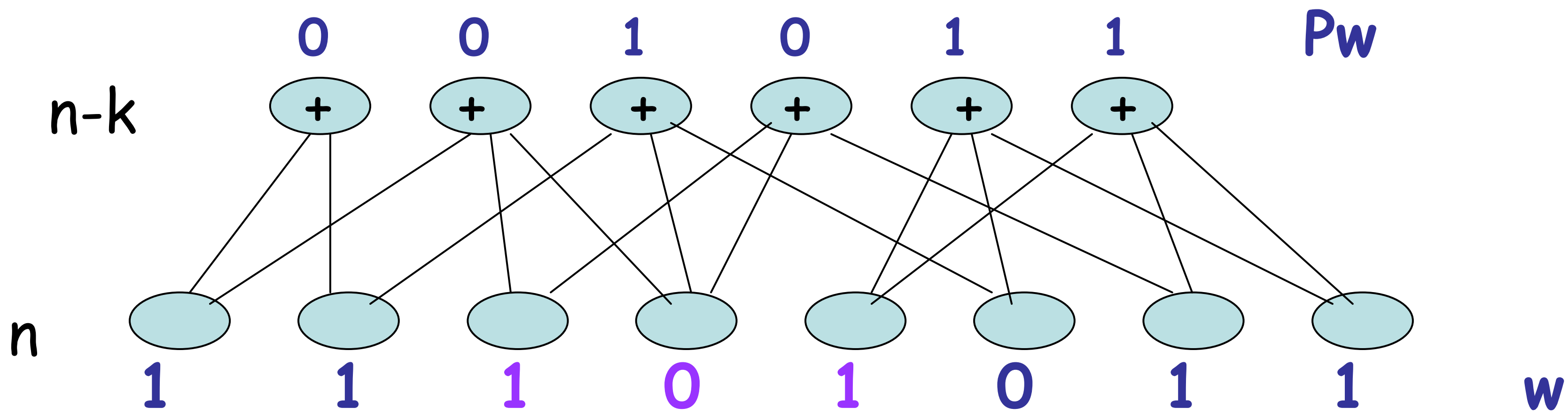
Trivial   Rate $(C) \geq k/n$, Encoding time = $O(n^2)$

G lossless $\to$ 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 algorithm [Sipser-Spielman]: while $Pw \neq 0$ flip all w_i with $i \in$ FLIP = { i : $\Gamma(i)$ has more 1's than 0's }

B = corrupted positions ($|B| \le n/200$)

B' = set of corrupted positions after flip

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

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