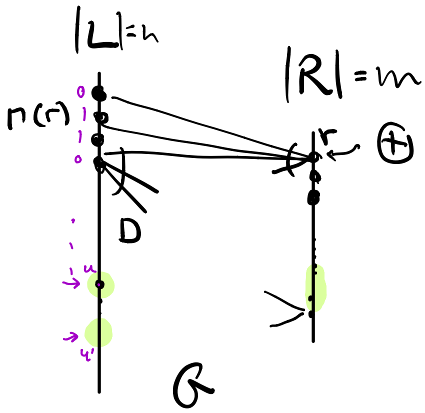
Lecture 14 — codes from expanders

$E : \{0,1\}^k \longrightarrow \{0,1\}^n$

$\forall \; x \neq y \in \{0,1\}^k$ $\quad E(x)$ is far from $E(y)$

$\text{dist}\,(E(x), E(y)) \geq \Delta \cdot n$

$E(\{0,1\}^k) =: C$



$C(G) = \left\{ x \in \{0,1\}^n \;\middle|\; \forall r \in R \;\; \sum_{i \in \Gamma(r)} x(i) = 0 \bmod 2 \right\}$

$\dim C \geq n - m$

$\alpha = D \cdot (1 - \varepsilon)$

Definition 1 *A $(n, m, D, \gamma, \alpha)$ bipartite expander is a D-left-regular bipartite graph $G(L \cup R, E)$ where $|L| = n$ and $|R| = m$ such that $\forall S \subseteq L$ with $|S| \leq \gamma n$, $N(S) \geq \alpha|S|$.*

Theorem 2 *$\forall \epsilon > 0, m \leq n$, $\exists \gamma > 0$ and $D \geq 1$ such that a $(n, m, D, \gamma, D(1-\epsilon))$ expander exists. Additionally, $D = \Theta(\frac{\log(n/m)}{\epsilon})$ and $\gamma n = \Theta(\frac{\epsilon m}{D})$.*

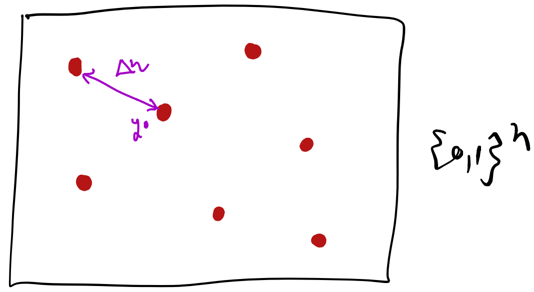
Lemma 3 *Let G be a $(n, m, D, \gamma, D(1-\epsilon))$ expander graph with $\epsilon < 1/2$. For any $S \subseteq L_G$ such that $|S| \leq \gamma n$, $U(S) \geq D(1-2\epsilon)|S|$.*

where $\quad U(S) = \{ u \in R \mid u$ has exactly one nbr in $S \}$

Theorem 4 *Let G be a $(n, m, D, \gamma, D(1-\epsilon))$ expander. Then $\Delta(C(G)) \geq 2\gamma(1-\epsilon)n$.*

(exercise)

Decoding: Given $y \in \{0,1\}^n$, find $z \in C$ closest to y.
s.t. $\text{dist}(y, C) \le \gamma \cdot (1-2\varepsilon) n$



C

Lemma 5 *If the number of errors is at most than γn (and at least 1), then there exists a node in L_G which is adjacent to more than $D/2$ unsatisfied checks. (This assumes that $\epsilon < 1/4$.)*

Every unique nbr is an unsat constraint.
There are $\underline{D(1-2\varepsilon)} \cdot |S|$ unique nbrs S = set of errors $|S| \le \gamma n$.

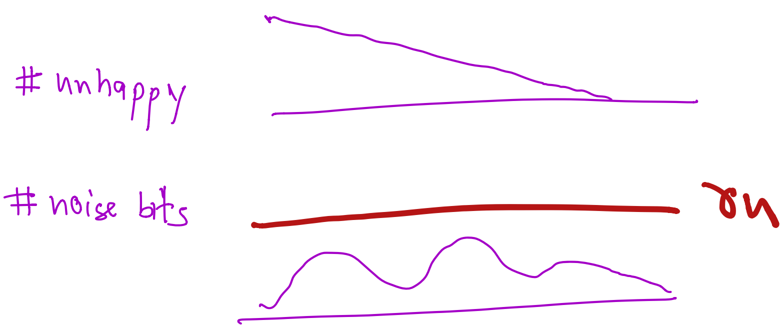
On avg vertices in S have $\geq D/2$ unique nbrs
$\exists s \in S$ w this property.

Lemma 6 *If we start with a received word having less than $\gamma(1-2\epsilon)n$ errors then we can never reach a word with γn errors in any interim step of the algorithm.*

$< (1-2\varepsilon)\gamma n \cdot D$ is an upper bound on #unhappy

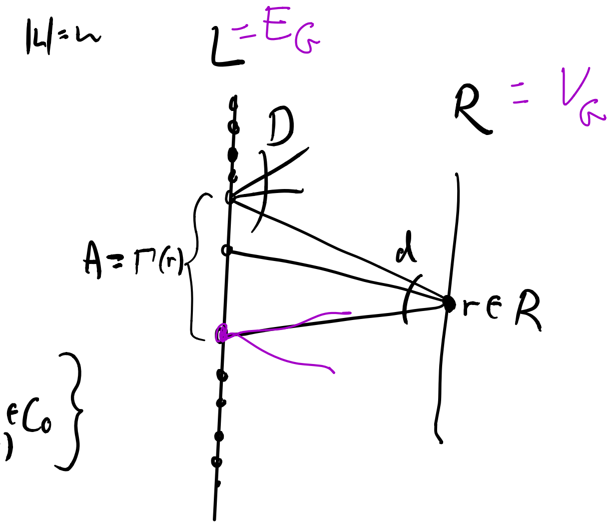
if S was of size γn (S = set of bits that are in error)
S would have $\geq \gamma n \cdot (1-2\varepsilon) \cdot D$ unique nbrs (all are unhappy)

S has $|S| \cdot (1-2\varepsilon) D$ unique nbrs
$|S| \le \gamma n$



Tanner Codes

Fix $C_0 \subseteq \{0,1\}^d$



$$C(G,C_0) = \left\{ w \in \{0,1\}^L \;\middle|\; \forall r \in R \;\; w|_{\Gamma(r)} \in C_0 \right\}$$

$w : L \to \{0,1\}$

$w|_A : A \to \{0,1\}$ $\quad w|_A \in \{0,1\}^A$

Start with d-regular G, create b'p. E_G vs V_G

$D=2 \qquad d=d$

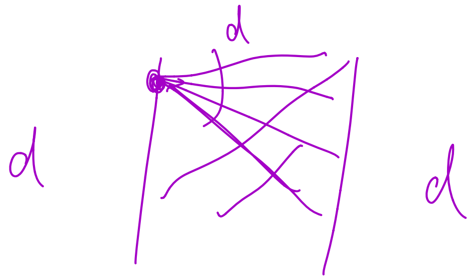
instead, define $C(G,C_0)$ differently.

Let $G=(V,E)$ be d-reg graph. Let $C_0 \subset \{0,1\}^d$

Def $T[G,C_0] = \left\{ x \in \{0,1\}^E \;\middle|\; \forall v \in V \;\; x|_{E(v)} \in C_0 \right\}$

Assume G has $\lambda = \max(|\lambda_2|, |\lambda_n|)$

Theorem 15 *Let $C_0 \subset \mathbb{F}_2^d$ have distance $\geq \delta_0 d$. Then the relative distance of $T(H, C_0)$ is $\geq \delta_0(\delta_0 - \frac{\lambda}{d})$*



C_0 d bit

$C_0^{\otimes 2}$ d^2 bit code

$(\delta_0)^2$