

Expander Graphs and Their Applications (XIV)

Yijia Chen
Shanghai Jiaotong University

Review of the Previous Lecture

Preprocessing

Definition

Let $d_0 \in \mathbb{N}$ be the constant from the previous first lemma for the existence of expanders. Let $G = \langle (V, E), \Sigma, \mathcal{C} \rangle$ be a constraint graph. The constraint graph $\text{prep}_1(G) := \langle (V', E'), \Sigma, \mathcal{C}' \rangle$ is defined as follows.

1. For each $v \in V$ let $[v] := \{(v, e) \mid e \in E \text{ is incident to } v\}$, and set $V' := \bigcup_{v \in V} [v]$.
2. For each $v \in V$ let X_v be a d_0 -regular graph on vertex set $[v]$ and edge expansion at least h_0 . Let $E_1 := \bigcup_{v \in V} E(X_v)$ and set

$$E_2 := \left\{ \begin{array}{l} \text{an edge between } (v, e) \text{ and } (v', e) \\ \mid \\ \text{an edge } e \in E \text{ between } v \text{ and } v' \end{array} \right\}$$

Finally let $E' := E_1 \cup E_2$.

3. The constraints are $\mathcal{C}' := \{c(e')\}_{e' \in E'}$ with
 - If $e' \in E_1$ then $c(e') := \{(a, a) \mid a \in \Sigma\}$.
 - If $e' \in E_2$ has end vertices (v, e) and (v', e) then $c(e') := c(e) \in \mathcal{C}$.

prep₁ (cont'd)

Lemma

Let $G = \langle (V, E), \Sigma, \mathcal{C} \rangle$ be a constraint graph and $G' = \langle (V', E'), \Sigma, \mathcal{C}' \rangle := \text{prep}_1(G)$. Then G' is a $d := (d_0 + 1)$ -regular constraint graph such that $|V'| \leq 2|E|$ and

$$c \cdot \text{unsat}(G) \leq \text{unsat}(G') \leq \text{unsat}(G)$$

for some constant $c > 0$.

Moreover, for every assignment $\sigma' : V' \rightarrow \Sigma$ let $\sigma : V \rightarrow \Sigma$ be defined according to the plurality value, i.e., $\sigma(v) := a$ such that

$$\Pr_{(v,e) \in [V]} [\sigma'(v, e) = a] \geq \Pr_{(v,e) \in [V]} [\sigma'(v, e) = a'] \text{ for all } a' \in \Sigma.$$

Then

$$c \cdot \text{unsat}_\sigma(G) \leq \text{unsat}_{\sigma'}(G').$$

Definition

Let $d'_0, \lambda_0 \in \mathbb{N}$ be the constants from the previous second lemma for the existence of expanders.

Let $G = \langle (V, E), \Sigma, \mathcal{C} \rangle$ be a constraint graph. The constraint graph $\text{prep}_2(G) := \langle (V, E'), \Sigma, \mathcal{C}' \rangle$ is defined as follows.

1. The vertices remain the same.
2. Let X be a d'_0 -regular graph on vertex set V and edge set E_1 with $\lambda(X) \leq \lambda_0 < d'_0$. Let $E_2 := \{\text{a new selfloop on } v \mid v \in V\}$ and finally let $E' := E \cup E_1 \cup E_2$.
3. The constraints are $\mathcal{C}' := \{c(e')\}_{e' \in E'}$ with
 - If $e' \in E$ then $c(e')$ remains the same.
 - If $e' \in E_1 \cup E_2$, then $c(e') := \{(a, b) \mid a, b \in \Sigma\}$.

Lemma

Let G be a d -regular constraint graph G and $G' := \text{prep}_2(G)$. Then G' has the following properties.

- ▶ G' is $(d + d'_0 + 1)$ -regular, has a selfloop on every vertex, and $\lambda(G') \leq d + \lambda_0 + 1 < \text{deg}(G')$.
- ▶ For every $\sigma : V \rightarrow \Sigma$,

$$\frac{d}{d + d'_0 + 1} \cdot \text{unsat}_\sigma(G) \leq \text{unsat}_\sigma(G') \leq \text{unsat}_\sigma(G).$$

Preprocessing Lemma

Lemma

There exist constants $0 < \lambda < \bar{d}$ and $\beta_1 > 0$ such that any constraint graph G can be transferred into a constraint graph $G' := \text{prep}(G)$ such that

- ▶ G' is \bar{d} -regular with selfloops and $\lambda(G') \leq \lambda < \bar{d}$.
- ▶ G' has the same alphabet as G and $\text{size}(G') = O(\text{size}(G))$.
- ▶ $\beta_1 \cdot \text{unsat}(G) \leq \text{unsat}(G') \leq \text{unsat}(G)$.

Amplification Lemma

Graph Powering

Fix some $d \in \mathbb{N}$.

Let $G = \langle (V, E), \Sigma, \mathcal{C} \rangle$ be a constraint graph with (V, E) being d -regular, and $t \in \mathbb{N}$.

Recall, a sequence (u_0, u_1, \dots, u_t) is a t -step walk in G if there is an edge between u_{i-1} and u_i for all $i \in [t]$.

Then we will define the following t -th power of G

$$\underline{G^t} := \langle (V, E^t), \Sigma^{d^{\lceil t/2 \rceil}}, \mathcal{C}^t \rangle$$

$$G^t := \langle (V, E^t), \Sigma^{d^{\lceil t/2 \rceil}}, \mathcal{C}^t \rangle$$

1. The vertices of G^t are the same as G . The number of edges in E^t between u and v is the number of t -step walks from u to v in G .
2. The alphabet of G^t is $\Sigma^{d^{\lceil t/2 \rceil}}$: Let

$$\Gamma(u) := \{u' \in V \mid u = u_0, u_1, \dots, u_{\lceil t/2 \rceil} = u' \text{ is a walk in } G\}.$$

Then $|\Gamma(u)| \leq d^{\lceil t/2 \rceil}$ and *by choosing some canonical order*, a value $a \in \Sigma^{d^{\lceil t/2 \rceil}}$ can be interpreted as an assignment $a : \Gamma(u) \rightarrow \Sigma$. One might think of this value as describing u 's opinion of its neighbor's values.

3. The constraint $C(e)$ associated with an edge $e \in E^t$ with end vertices u and v contains those pairs $a, b \in \Sigma^{d^{\lceil t/2 \rceil}}$ if: There is an assignment $\sigma : \Gamma(u) \cup \Gamma(v) \rightarrow \Sigma$ that satisfies every constraint $c(e) \in \mathcal{C}$ where $e \in E \cap (\Gamma(u) \times \Gamma(v))$, and such that

$$\text{for all } u' \in \Gamma(u) \text{ and } v' \in \Gamma(v), \quad \sigma(u') = a_{u'} \text{ and } \sigma(v') = b_{v'}$$

where $a_{u'}$ is the value a assigns u' , and $b_{v'}$ the value b assigns to v' .

Amplification Lemma

Lemma

Let $0 < \lambda < d$ and $|\Sigma|$ be constants.

Amplification Lemma

Lemma

Let $0 < \lambda < d$ and $|\Sigma|$ be constants. Then there exists a constant $\beta_2 = \beta_2(\lambda, d, |\Sigma|) > 0$ such that for every $t \in \mathbb{N}$ and for every d -regular constraint graph G with a selfloop on each vertex and $\lambda(G) \leq \lambda$,

$$\text{unsat}(G^t) \geq \beta_2 \cdot \sqrt{t} \cdot \min\left(\text{unsat}(G), \frac{1}{t}\right).$$

Amplification Lemma (stronger version)

Amplification Lemma (stronger version)

Lemma

Let $0 < \lambda < d$ and $|\Sigma|$ be constants.

Amplification Lemma (stronger version)

Lemma

Let $0 < \lambda < d$ and $|\Sigma|$ be constants. Then there exists a constant $\beta_2 = \beta_2(\lambda, d, |\Sigma|) > 0$ such that for every $t \in \mathbb{N}$ and for every d -regular constraint graph G with a selfloop on each vertex and $\lambda(G) \leq \lambda$, the following hold.

Amplification Lemma (stronger version)

Lemma

Let $0 < \lambda < d$ and $|\Sigma|$ be constants. Then there exists a constant $\beta_2 = \beta_2(\lambda, d, |\Sigma|) > 0$ such that for every $t \in \mathbb{N}$ and for every d -regular constraint graph G with a selfloop on each vertex and $\lambda(G) \leq \lambda$, the following hold.

For every $\vec{\sigma} : V \rightarrow \Sigma^{d^{\lceil t/2 \rceil}}$ let $\sigma : V \rightarrow \Sigma$ be defined according to “popular opinion” by setting, for each $v \in V$, $\sigma(v) := a$ such that

$$\Pr[\text{a random } \lceil t/2 \rceil\text{-step walk from } v \text{ reaches a vertex } w \text{ with } \vec{\sigma}(w)_v = a],$$

where $\vec{\sigma}(w)_v \in \Sigma$ denotes the restriction of $\vec{\sigma}(w)$ to v , is maximized over all $a \in \Sigma$.

Amplification Lemma (stronger version)

Lemma

Let $0 < \lambda < d$ and $|\Sigma|$ be constants. Then there exists a constant $\beta_2 = \beta_2(\lambda, d, |\Sigma|) > 0$ such that for every $t \in \mathbb{N}$ and for every d -regular constraint graph G with a selfloop on each vertex and $\lambda(G) \leq \lambda$, the following hold.

For every $\vec{\sigma} : V \rightarrow \Sigma^{d^{\lceil t/2 \rceil}}$ let $\sigma : V \rightarrow \Sigma$ be defined according to “popular opinion” by setting, for each $v \in V$, $\sigma(v) := a$ such that

$$\Pr[\text{a random } \lceil t/2 \rceil\text{-step walk from } v \text{ reaches a vertex } w \text{ with } \vec{\sigma}(w)_v = a],$$

where $\vec{\sigma}(w)_v \in \Sigma$ denotes the restriction of $\vec{\sigma}(w)$ to v , is maximized over all $a \in \Sigma$.

Then

$$\text{unsat}_{\vec{\sigma}}(G^t) \geq \beta_2 \cdot \sqrt{t} \cdot \min\left(\text{unsat}_{\sigma}(G), \frac{1}{t}\right).$$

Proof of the Amplification Lemma

Proof of the Amplification Lemma

Let $\vec{\sigma} : V \rightarrow \Sigma^{d^{\lceil t/2 \rceil}}$ be an assignment for G^t .

Proof of the Amplification Lemma

Let $\vec{\sigma} : V \rightarrow \Sigma^{d^{\lceil t/2 \rceil}}$ be an assignment for G^t . Define the assignment $\sigma : V \rightarrow \Sigma$ as before, i.e., according to “popular opinion.”

Proof of the Amplification Lemma

Let $\vec{\sigma} : V \rightarrow \Sigma^{d^{\lceil t/2 \rceil}}$ be an assignment for G^t . Define the assignment $\sigma : V \rightarrow \Sigma$ as before, i.e., according to “popular opinion.”

For every $v \in V$, let X_v be a random variable such that for every $a \in \Sigma$

$$\Pr[X_v = a] = \Pr \left[\text{a random } \lceil t/2 \rceil\text{-step walk from } v \right. \\ \left. \text{reaches a vertex } w \text{ with } \vec{\sigma}(w)_v = a \right].$$

Proof of the Amplification Lemma

Let $\vec{\sigma} : V \rightarrow \Sigma^{d^{\lceil t/2 \rceil}}$ be an assignment for G^t . Define the assignment $\sigma : V \rightarrow \Sigma$ as before, i.e., according to “popular opinion.”

For every $v \in V$, let X_v be a random variable such that for every $a \in \Sigma$

$$\Pr[X_v = a] = \Pr[\text{a random } \lceil t/2 \rceil\text{-step walk from } v \\ \text{reaches a vertex } w \text{ with } \vec{\sigma}(w)_v = a].$$

Then for every $a \in \Sigma$,

$$\Pr[X_v = \sigma(v)] \geq \Pr[X_v = a].$$

Proof of the Amplification Lemma

Let $\vec{\sigma} : V \rightarrow \Sigma^{d^{\lceil t/2 \rceil}}$ be an assignment for G^t . Define the assignment $\sigma : V \rightarrow \Sigma$ as before, i.e., according to “popular opinion.”

For every $v \in V$, let X_v be a random variable such that for every $a \in \Sigma$

$$\Pr[X_v = a] = \Pr[\text{a random } \lceil t/2 \rceil\text{-step walk from } v \\ \text{reaches a vertex } w \text{ with } \vec{\sigma}(w)_v = a].$$

Then for every $a \in \Sigma$,

$$\Pr[X_v = \sigma(v)] \geq \Pr[X_v = a].$$

Hence,

$$\Pr[X_v = \sigma(v)] \geq \frac{1}{|\Sigma|}.$$

Proof of the Amplification Lemma (cont'd)

Proof of the Amplification Lemma (cont'd)

Let

$$F := \begin{cases} \{e \in E \mid \sigma \text{ violates } e\} & \text{if } \text{unsat}_\sigma(G) < 1/t \\ \text{an arbitrary subset of the above } \{\dots\} & \\ \text{with } |F| = \lfloor |E|/t \rfloor & \text{otherwise.} \end{cases}$$

Proof of the Amplification Lemma (cont'd)

Let

$$F := \begin{cases} \{e \in E \mid \sigma \text{ violates } e\} & \text{if } \text{unsat}_\sigma(G) < 1/t \\ \text{an arbitrary subset of the above } \{\dots\} & \\ \text{with } |F| = \lfloor |E|/t \rfloor & \text{otherwise.} \end{cases}$$

Then

$$\Omega\left(\frac{|F|}{|E|}\right) = \min\left(\text{unsat}_\sigma(G), \frac{1}{t}\right)$$

Proof of the Amplification Lemma (cont'd)

Let

$$F := \begin{cases} \{e \in E \mid \sigma \text{ violates } e\} & \text{if } \text{unsat}_\sigma(G) < 1/t \\ \text{an arbitrary subset of the above } \{\dots\} & \\ \text{with } |F| = \lfloor |E|/t \rfloor & \text{otherwise.} \end{cases}$$

Then

$$\Omega\left(\frac{|F|}{|E|}\right) = \min\left(\text{unsat}_\sigma(G), \frac{1}{t}\right)$$

From now on, we fix $\vec{\sigma}$, σ , and F .

Proof of the Amplification Lemma (cont'd)

Proof of the Amplification Lemma (cont'd)

Let $\mathbf{E} := E(G^t) = E^t$.

Proof of the Amplification Lemma (cont'd)

Let $\mathbf{E} := E(G^t) = E^t$. Recall there is a one-to-one correspondence between every edge $\mathbf{e} \in \mathbf{E}$ and every walk of length t in G .

Proof of the Amplification Lemma (cont'd)

Let $\mathbf{E} := E(G^t) = E^t$. Recall there is a one-to-one correspondence between every edge $\mathbf{e} \in \mathbf{E}$ and every walk of length t in G .

With some abuse of notation we write $\mathbf{e} = (v_0, v_1, \dots, v_t)$ where $(v_{i-1}, v_i) \in E$ for all $i \in [t]$.

Proof of the Amplification Lemma (cont'd)

Let $\mathbf{E} := E(G^t) = E^t$. Recall there is a one-to-one correspondence between every edge $\mathbf{e} \in \mathbf{E}$ and every walk of length t in G .

With some abuse of notation we write $\mathbf{e} = (v_0, v_1, \dots, v_t)$ where $(v_{i-1}, v_i) \in E$ for all $i \in [t]$.

Definition

A walk $\mathbf{e} = (v_0, v_1, \dots, v_t)$ is hit by its i -th edge if

Proof of the Amplification Lemma (cont'd)

Let $\mathbf{E} := E(G^t) = E^t$. Recall there is a one-to-one correspondence between every edge $\mathbf{e} \in \mathbf{E}$ and every walk of length t in G .

With some abuse of notation we write $\mathbf{e} = (v_0, v_1, \dots, v_t)$ where $(v_{i-1}, v_i) \in E$ for all $i \in [t]$.

Definition

A walk $\mathbf{e} = (v_0, v_1, \dots, v_t)$ is hit by its i -th edge if

1. $(v_{i-1}, v_i) \in F$, and

Proof of the Amplification Lemma (cont'd)

Let $\mathbf{E} := E(G^t) = E^t$. Recall there is a one-to-one correspondence between every edge $\mathbf{e} \in \mathbf{E}$ and every walk of length t in G .

With some abuse of notation we write $\mathbf{e} = (v_0, v_1, \dots, v_t)$ where $(v_{i-1}, v_i) \in E$ for all $i \in [t]$.

Definition

A walk $\mathbf{e} = (v_0, v_1, \dots, v_t)$ is hit by its i -th edge if

1. $(v_{i-1}, v_i) \in F$, and
2. Both $\vec{\sigma}(v_0)_{v_{i-1}} = \sigma(v_{i-1})$ and $\vec{\sigma}(v_t)_{v_i} = \sigma(v_i)$.

Proof of the Amplification Lemma (cont'd)

Let $\mathbf{E} := E(G^t) = E^t$. Recall there is a one-to-one correspondence between every edge $\mathbf{e} \in \mathbf{E}$ and every walk of length t in G .

With some abuse of notation we write $\mathbf{e} = (v_0, v_1, \dots, v_t)$ where $(v_{i-1}, v_i) \in E$ for all $i \in [t]$.

Definition

A walk $\mathbf{e} = (v_0, v_1, \dots, v_t)$ is hit by its i -th edge if

1. $(v_{i-1}, v_i) \in F$, and
2. Both $\vec{\sigma}(v_0)_{v_{i-1}} = \sigma(v_{i-1})$ and $\vec{\sigma}(v_t)_{v_i} = \sigma(v_i)$.

Remark.

- $(v_{i-1}, v_i) \in F$ means that the edge (v_{i-1}, v_i) rejects σ .

Proof of the Amplification Lemma (cont'd)

Let $\mathbf{E} := E(G^t) = E^t$. Recall there is a one-to-one correspondence between every edge $\mathbf{e} \in \mathbf{E}$ and every walk of length t in G .

With some abuse of notation we write $\mathbf{e} = (v_0, v_1, \dots, v_t)$ where $(v_{i-1}, v_i) \in E$ for all $i \in [t]$.

Definition

A walk $\mathbf{e} = (v_0, v_1, \dots, v_t)$ is hit by its i -th edge if

1. $(v_{i-1}, v_i) \in F$, and
2. Both $\vec{\sigma}(v_0)_{v_{i-1}} = \sigma(v_{i-1})$ and $\vec{\sigma}(v_t)_{v_i} = \sigma(v_i)$.

Remark.

- $(v_{i-1}, v_i) \in F$ means that the edge (v_{i-1}, v_i) rejects σ .
- By 2, v_0 has the major opinion of v_{i-1} in G^t , (which implies that *there is a $\lfloor t/2 \rfloor$ -step walk from v_0 to v_{i-1}*). Similarly, v_t has the majority opinion of v_i .

Proof of the Amplification Lemma (cont'd)

Let $\mathbf{E} := E(G^t) = E^t$. Recall there is a one-to-one correspondence between every edge $\mathbf{e} \in \mathbf{E}$ and every walk of length t in G .

With some abuse of notation we write $\mathbf{e} = (v_0, v_1, \dots, v_t)$ where $(v_{i-1}, v_i) \in E$ for all $i \in [t]$.

Definition

A walk $\mathbf{e} = (v_0, v_1, \dots, v_t)$ is hit by its i -th edge if

1. $(v_{i-1}, v_i) \in F$, and
2. Both $\vec{\sigma}(v_0)_{v_{i-1}} = \sigma(v_{i-1})$ and $\vec{\sigma}(v_t)_{v_i} = \sigma(v_i)$.

Remark.

- $(v_{i-1}, v_i) \in F$ means that the edge (v_{i-1}, v_i) rejects σ .
- By 2, v_0 has the major opinion of v_{i-1} in G^t , (which implies that *there is a $\lfloor t/2 \rfloor$ -step walk from v_0 to v_{i-1}*). Similarly, v_t has the majority opinion of v_i .

Hence, (v_0, v_t) rejects $\vec{\sigma}$ by our definition of G^t .

Proof of the Amplification Lemma (cont'd)

Proof of the Amplification Lemma (cont'd)

Let

$$I := \left\{ \frac{t}{2} - \sqrt{\frac{t}{2}} < i \leq \frac{t}{2} + \sqrt{\frac{t}{2}} \right\} \subseteq \mathbb{N}$$

be the set of “middle” indices.

Proof of the Amplification Lemma (cont'd)

Let

$$I := \left\{ \frac{t}{2} - \sqrt{\frac{t}{2}} < i \leq \frac{t}{2} + \sqrt{\frac{t}{2}} \right\} \subseteq \mathbb{N}$$

be the set of “middle” indices. For each walk \mathbf{e} , we define

$$\underline{N(\mathbf{e})} := |\{i \in I \mid \mathbf{e} \text{ is hit by its } i\text{-th edge}\}|.$$

Proof of the Amplification Lemma (cont'd)

Let

$$I := \left\{ \frac{t}{2} - \sqrt{\frac{t}{2}} < i \leq \frac{t}{2} + \sqrt{\frac{t}{2}} \right\} \subseteq \mathbb{N}$$

be the set of “middle” indices. For each walk \mathbf{e} , we define

$$N(\mathbf{e}) := |\{i \in I \mid \mathbf{e} \text{ is hit by its } i\text{-th edge}\}|.$$

$N(\mathbf{e}) > 0$ implies that \mathbf{e} rejects $\vec{\sigma}$.

Proof of the Amplification Lemma (cont'd)

Let

$$I := \left\{ \frac{t}{2} - \sqrt{\frac{t}{2}} < i \leq \frac{t}{2} + \sqrt{\frac{t}{2}} \right\} \subseteq \mathbb{N}$$

be the set of “middle” indices. For each walk \mathbf{e} , we define

$$N(\mathbf{e}) := |\{i \in I \mid \mathbf{e} \text{ is hit by its } i\text{-th edge}\}|.$$

$N(\mathbf{e}) > 0$ implies that \mathbf{e} rejects $\vec{\sigma}$.

Thus $\Pr_{\mathbf{e}}[N(\mathbf{e}) > 0] \leq \Pr_{\mathbf{e}}[\mathbf{e} \text{ rejects } \vec{\sigma}] = \text{unsat}_{\vec{\sigma}}(G^t)$.

Proof of the Amplification Lemma (cont'd)

Let

$$I := \left\{ \frac{t}{2} - \sqrt{\frac{t}{2}} < i \leq \frac{t}{2} + \sqrt{\frac{t}{2}} \right\} \subseteq \mathbb{N}$$

be the set of “middle” indices. For each walk \mathbf{e} , we define

$$N(\mathbf{e}) := |\{i \in I \mid \mathbf{e} \text{ is hit by its } i\text{-th edge}\}|.$$

$N(\mathbf{e}) > 0$ implies that \mathbf{e} rejects $\vec{\sigma}$.

Thus $\Pr_{\mathbf{e}}[N(\mathbf{e}) > 0] \leq \Pr_{\mathbf{e}}[\mathbf{e} \text{ rejects } \vec{\sigma}] = \text{unsat}_{\vec{\sigma}}(G^t)$.

We will prove

$$\Omega(\sqrt{t}) \cdot \frac{|F|}{|E|} \leq \Pr_{\mathbf{e}}[N(\mathbf{e}) > 0].$$

Combined with $\Omega(|F|/|E|) = \min(\text{unsat}_{\sigma}(G), 1/t)$,

$$\Omega(\sqrt{t}) \cdot \min\left(\text{unsat}_{\sigma}(G), \frac{1}{t}\right) \leq \Omega(\sqrt{t}) \cdot \frac{|F|}{|E|} \leq \Pr_{\mathbf{e}}[N(\mathbf{e}) > 0] \leq \text{unsat}_{\vec{\sigma}}(G^t).$$

Proof of the Amplification Lemma (cont'd)

Proof of the Amplification Lemma (cont'd)

To show:

$$\Omega(\sqrt{t}) \cdot \frac{|F|}{|E|} \leq \Pr_{\mathbf{e}}[N(\mathbf{e}) > 0].$$

we will prove two lemmas.

Proof of the Amplification Lemma (cont'd)

To show:

$$\Omega(\sqrt{t}) \cdot \frac{|F|}{|E|} \leq \Pr_{\mathbf{e}}[N(\mathbf{e}) > 0].$$

we will prove two lemmas.

Lemma

$$\mathbb{E}_{\mathbf{e}}[N(\mathbf{e})] \geq \Omega(\sqrt{t}) \cdot \frac{|F|}{|E|}.$$

Proof of the Amplification Lemma (cont'd)

To show:

$$\Omega(\sqrt{t}) \cdot \frac{|F|}{|E|} \leq \Pr_{\mathbf{e}}[N(\mathbf{e}) > 0].$$

we will prove two lemmas.

Lemma

$$\mathbb{E}_{\mathbf{e}}[N(\mathbf{e})] \geq \Omega(\sqrt{t}) \cdot \frac{|F|}{|E|}.$$

Lemma

$$\mathbb{E}_{\mathbf{e}}[(N(\mathbf{e}))^2] \leq O(\sqrt{t}) \cdot \frac{|F|}{|E|}.$$

Proof of $\Omega(\sqrt{t}) \cdot |F|/|E| \leq \Pr_{\mathbf{e}}[N(\mathbf{e}) > 0]$

Proof of $\Omega(\sqrt{t}) \cdot |F|/|E| \leq \Pr_{\mathbf{e}}[N(\mathbf{e}) > 0]$

From probability theory:

Lemma

For every *non-negative* random variable X which is not identically zero,

$$\Pr[X > 0] \geq \frac{\mathbb{E}^2[X]}{\mathbb{E}[X^2]}.$$

Proof of $\Omega(\sqrt{t}) \cdot |F|/|E| \leq \Pr_e[N(\mathbf{e}) > 0]$

From probability theory:

Lemma

For every *non-negative* random variable X which is not identically zero,

$$\Pr[X > 0] \geq \frac{\mathbb{E}^2[X]}{\mathbb{E}[X^2]}.$$

Proof.

$$\mathbb{E}[X] = \mathbb{E}[X \cdot \mathbf{1}_{X>0}] \leq \sqrt{\mathbb{E}[X^2]} \cdot \sqrt{\mathbb{E}[(\mathbf{1}_{X>0})^2]} = \sqrt{\mathbb{E}[X^2]} \cdot \sqrt{\Pr[X > 0]}.$$

□

Proof of $\Omega(\sqrt{t}) \cdot |F|/|E| \leq \Pr_{\mathbf{e}}[N(\mathbf{e}) > 0]$

From probability theory:

Lemma

For every *non-negative* random variable X which is not identically zero,

$$\Pr[X > 0] \geq \frac{\mathbb{E}^2[X]}{\mathbb{E}[X^2]}.$$

Proof.

$$\mathbb{E}[X] = \mathbb{E}[X \cdot \mathbf{1}_{X>0}] \leq \sqrt{\mathbb{E}[X^2]} \cdot \sqrt{\mathbb{E}[(\mathbf{1}_{X>0})^2]} = \sqrt{\mathbb{E}[X^2]} \cdot \sqrt{\Pr[X > 0]}.$$

□

Now by the previous lemmas

$$\Pr[N(\mathbf{e}) > 0] \geq \mathbb{E}^2[N(\mathbf{e})]/\mathbb{E}[(N(\mathbf{e}))^2] = \Omega(\sqrt{t}) \cdot \frac{|F|}{|E|}.$$