

Probabilistically Checkable Proofs

Lecture 16

Probability (and techniques)

Algorithms (models and applications)

Random Walks

Stationary Distribution

Perron-Frobenius Theorem

Pagerank

Lecture 18

Probability (and techniques)

Algorithms (models and applications)

Hitting times

Cover times

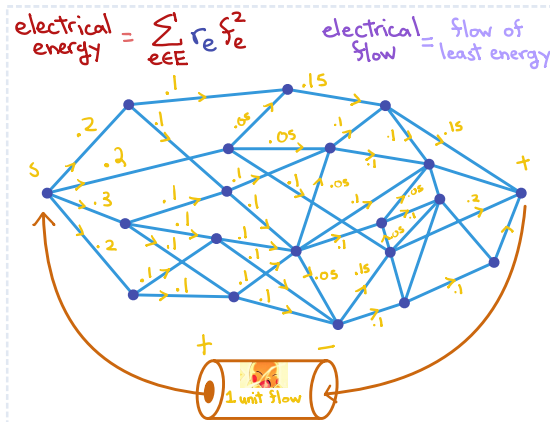
Electrical networks

Connectivity
in $O(\log n)$ space

random walk terminology:

Hitting time $H(s, t)$ = expected # steps until a random walk from s reaches t

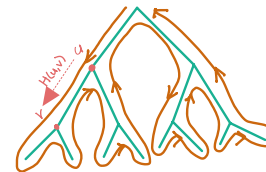
Cover time $C(s)$ = expected # steps until a random walk from s visits every vertex



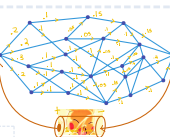
Lemma $H(u, v) + H(v, u) = 2m \cdot (\text{energy of unit flow } (u, v))$

Theorem $C(s) \leq 2mn$

proof Six traversal of spanning tree



$$\begin{aligned} \text{total time} &= \sum_{u, v \in V} H(u, v) + H(v, u) \\ &= 2m \sum_{u, v \in V} (\text{energy of unit flow } (u, v)) \leq 2m(n-1) \end{aligned}$$



electrical energy = $\sum_{e \in E} r_e f_e^2$
electrical flow = least energy

des $B: \mathbb{R}^E \rightarrow \mathbb{R}^V$ by
(BS) $_v$ = net flow at v
 $d_v = \begin{cases} -1 & \text{if } v = s \\ 1 & \text{if } v = t \\ 0 & \text{otherwise} \end{cases}$

min $\frac{1}{2} \sum_{e \in E} r_e f_e^2$ s.t. $BS = d$
(electrical energy) (is a typical)

effective resistance of d = optimum value/energy

Ohm's law: $f = R^{-1} B^T p$
for electric flow by electric potentials p

$L = BR^{-1}B^T \in \mathbb{R}^{V \times V}$
(effective resist. of d) $\leq \langle d, L^{-1}d \rangle$

Lecture 19

Probability (and techniques)

Algorithms (models and applications)

Spectral theorem
for symmetric maps

Spectral analysis of
random walks

Lecture 20

Probability
(and techniques)

Algorithms
(models and applications)

Conductance

Cheeger's inequality

Conductance-based
mixing time

Fiedler's algorithm
for low-conductance
cuts

Lecture 21

Probability
(and techniques)

Algorithms
(models and applications)

Expanders

Zigzag product

tensors

Deterministic

Connectivity in

$O(\log n)$ space

Lecture 22

Probability
(and techniques)

classes RP and BPP

tensors of graphs

Algorithms
(models and applications)

More efficient
amplification

Efficient construction
of exponentially
large expanders

A language L is in...

no error

P if there is a (det.) polytime algo to decide if $x \in L$
(polynomial time)

one-sided
error

RP if there's a random. polytime algo that, on input x :
(randomized polynomial time)

- if $x \in L$, decides $x \in L$ w/ constant prob.
- if $x \notin L$, always decides $x \notin L$

two-sided
error

BPP if there's a random. polytime algo that, on input x :
(bounded error probabilistic polynomial time)

- if $x \in L$, decides $x \in L$ w/ prob $\geq 2/3$
- if $x \notin L$, decides $x \notin L$ w/ prob. $\geq 2/3$

Amplification

RP if there's a random. polytime algo that, on input x :
(randomized polynomial time)

- if $x \in L$, decides $x \in L$ w/ constant prob.
- if $x \notin L$, always decides $x \notin L$

let LERP

$\Rightarrow$ algo w/ False-negative error prob. (say) $1/2$
using (say) m random bits

how to reduce error prob. to δ ?

1. run algo $O(\log(1/\delta))$ times
2. Output disjunction (or) of all trials

total # of random bits?

$$O(m \log(1/\delta))$$

Better?

RP if there's a random. polytime algo that, on input x :
(randomized polynomial time)

- if $x \in L$, decides $x \in L$ w/ constant prob.
- if $x \notin L$, always decides $x \notin L$

BPP if there's a random. polytime algo that, on input x :
(bounded error probabilistic polynomial time)

- if $x \in L$, decides $x \in L$ w/ prob. $\geq 2/3$
- if $x \notin L$, decides $x \notin L$ w/ prob. $\geq 2/3$

Theorem

Given RP/BPP algo, one can get error prob δ w/

- $O(\log(1/\delta))$ -factor increase in running time
- $O(\log(1/\delta))$ additional random bits

ideas?

Lecture 23/24

Probability
(and techniques)

Algorithms
(models and applications)

Probabilistically
checkable proofs

A language L is in...

P
(polytime) if there is a det. polytime decision algo

NP
(nondeterministic polytime) if there is a polytime "verifier" that takes as input $x \in \{0,1\}^n$ and $y \in \{0,1\}^{\text{poly}(n)}$ and:

- if $x \in L$, answers " $x \in L$ " for some y
- if $x \notin L$, answers " $x \notin L$ " for all y

PCP(r, q): (nonadaptive) probabilistically checkable proof
w/ r random bits and q queries

Oracle model: query i th bit of proof y

Verifier:

Given $x \in \{0, 1\}^n$ and oracle access to $y \in \{0, 1\}^{\text{poly}(n)}$:

1. select $O(q)$ queries based on x , $O(r)$ random bits
2. make $O(q)$ queries to oracle
3. accept or reject x
 - if $x \in L$, always accept x
 - if $x \notin L$, accept x w/ prob. $\leq 1/2$

PCP theorem [90's]

$$NP = PCP(\underbrace{O(\log n)}_{\text{random bits}}, \underbrace{O(1)}_{\text{queries}})$$

leads to:

Theorem. [Håstad 1997]

$\forall \epsilon > 0$, $(7/8 + \epsilon)$ -APX for 3SAT is NP-Hard

A language L is in...

P _(polytime) if there is a det. polytime decision algo

NP _(nondeterministic polytime) if there is a polytime "verifier" that takes as input $x \in \{0,1\}^n$ and $y \in \{0,1\}^{\text{poly}(n)}$ and:

- if $x \in L$, answers " $x \in L$ " for some y
- if $x \notin L$, answers " $x \notin L$ " for all y

PCP(r, q): (nonadaptive) probabilistically checkable proof w/ r random bits and q queries

Oracle model: query i th bit of proof y

Verifier:

Given $x \in \{0,1\}^n$ and oracle access to $y \in \{0,1\}^{\text{poly}(n)}$:

1. select $O(q)$ queries based on x , $O(r)$ random bits
2. make $O(q)$ queries to oracle
3. accept or reject x
 - if $x \in L$, always accept x
 - if $x \notin L$, accept x w/ prob. $\leq 1/2$

Lemma:

$$\text{PCP}(\underbrace{O(\log n)}_{\text{random bits}}, \underbrace{O(1)}_{\text{queries}}) \subseteq \text{NP}$$

why?

A language L is in...

P _(polytime) is there is a det. polytime decision algo

NP _(nondeterministic polytime) is there is a polytime "verifier" that takes as input $x \in \{0,1\}^n$ and $y \in \{0,1\}^{\text{poly}(n)}$ and:

- if $x \in L$, answers " $x \in L$ " for some y
- if $x \notin L$, answers " $x \notin L$ " for all y

$\text{PCP}(r,q)$: (nonadaptive) probabilistically checkable proof w/ r random bits and q queries

Oracle model: query i th bit of proof y

Verifier:

Given $x \in \{0,1\}^n$ and oracle access to $y \in \{0,1\}^{\text{poly}(n)}$:

1. select $O(q)$ queries based on x , $O(r)$ random bits
2. make $O(q)$ queries to oracle
3. accept or reject x
 - if $x \in L$, always accept x
 - if $x \notin L$, accept x w/ prob. $\leq 1/2$

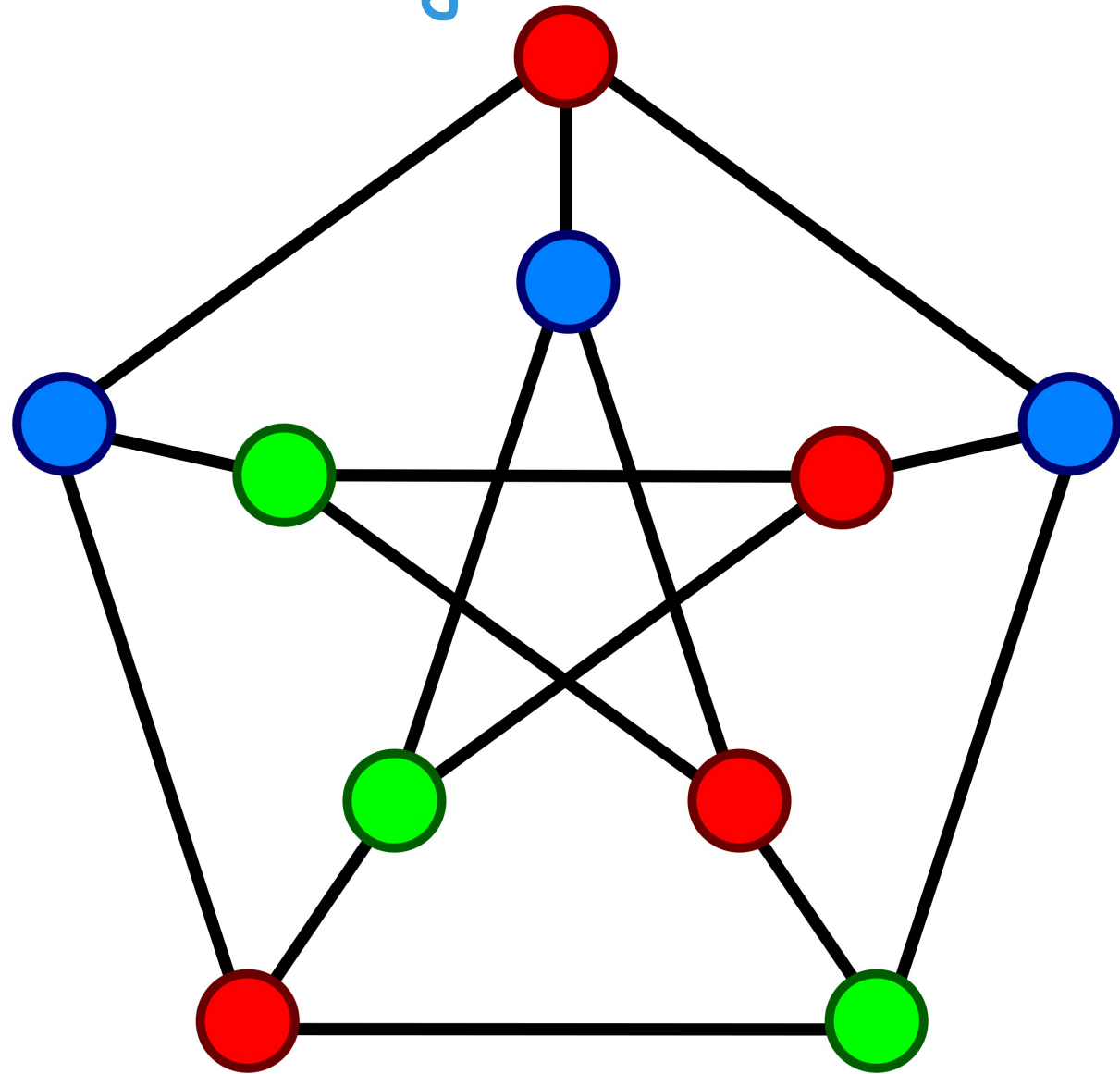
PCP theorem $\text{NP} = \text{PCP}(\underbrace{O(1)}_{\text{random bits}}, \underbrace{O(\log n)}_{\text{queries}})$

Theorem. [Håstad 1997]

$\forall \epsilon > 0$, $(7/8 + \epsilon)$ -APX for 3SAT is NP-Hard

3-colorability

can vertices of G be colored in 3 colors s.t.
there are no monochromatic edges?



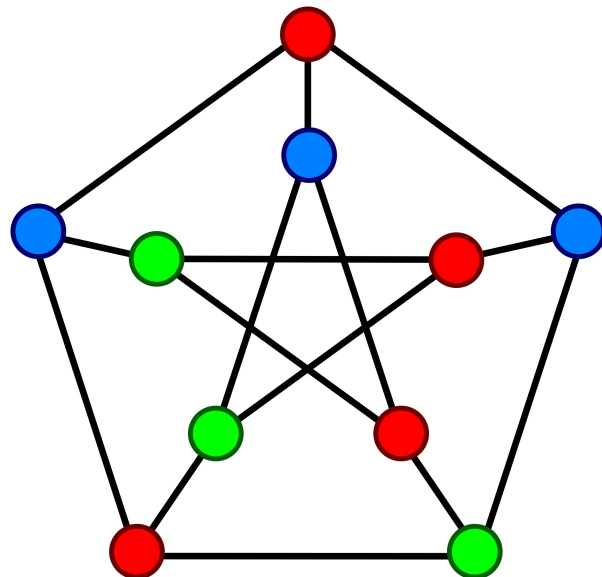
q-ary constraint satisfaction problems

- n variables V • finite alphabet A • m clauses
- a clause consists of q variables $v_1, \dots, v_q \in V$ and "satisfying" set $S \subseteq A^q$
- $\pi: V \rightarrow A$ satisfies clause if $(\pi(v_1), \dots, \pi(v_q)) \in S$

$V = \text{vertices}$

$A = \{\text{red, blue, green}\}$

clauses = edges



q-ary constraint satisfaction problems

- n variables V
- finite alphabet A
- m clauses
- a clause consists of q variables $v_1, \dots, v_k \in V$ and "satisfying" set $S \subseteq A^q$
- $\pi: V \rightarrow A$ satisfies clause if $(\pi(v_1), \dots, \pi(v_k)) \in S$

given CSP P , let

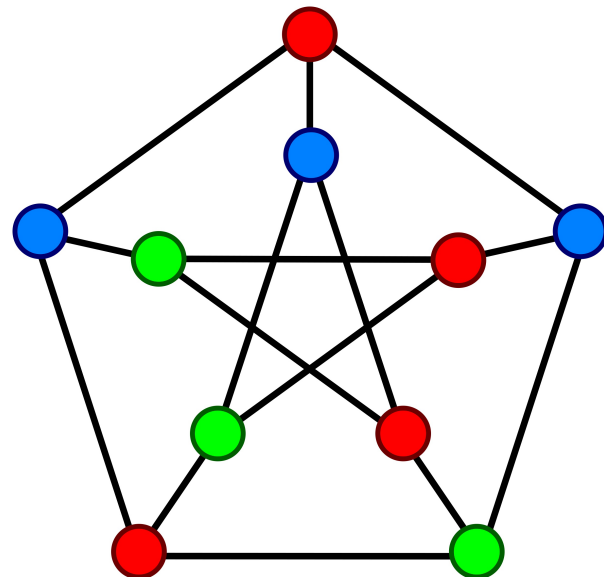
$\text{UNSAT}(P) = \text{min fraction of unsatisfied clauses}$

(e.g., $\text{UNSAT}(P) = 0$ means P satisfiable)

$V = \text{vertices}$

$A = \{\text{red, blue, green}\}$

clauses = edges



q-ary constraint satisfaction problems

- n variables V
- finite alphabet A
- m clauses
- a clause consists of q variables $v_1, \dots, v_k \in V$ and "satisfying" set $S \subseteq A^q$

$\pi: V \rightarrow A$ satisfies clause if $(\pi(v_1), \dots, \pi(v_k)) \in S$

Theorem:

there are integers $q > 1$, $|A| > 1$ s.t.

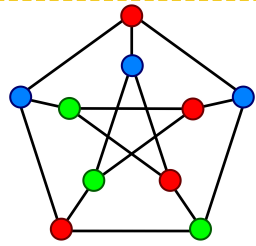
given q-ary CSP P over alphabet A ,
it is NP-Hard to decide whether:

- all clauses can be satisfied ($\text{UNSAT}(P) = 0$)
- $\leq \frac{1}{2}$ of clauses can be satisfied ($\text{UNSAT}(P) \geq \frac{1}{2}$)

$V = \text{vertices}$

$A = \{\text{red, blue, green}\}$

clauses = edges



PCP theorem

$$NP = PCP(\underbrace{O(\log n)}_{\text{random bits}}, \underbrace{O(1)}_{\text{queries}})$$

Theorem:

there are integers $q > 1$, $|A| > 1$ s.t.
given q -ary CSP over alphabet A ,
it is NP-Hard to decide whether:

- all clauses can be satisfied
- $\leq \frac{1}{2}$ of clauses can be satisfied

equivalent
(exercise)



Graph CSP

2-ary CSP

variables = vertices

clause over $u, v \in V \approx$ edge between u and v

q -ary constraint satisfaction problems

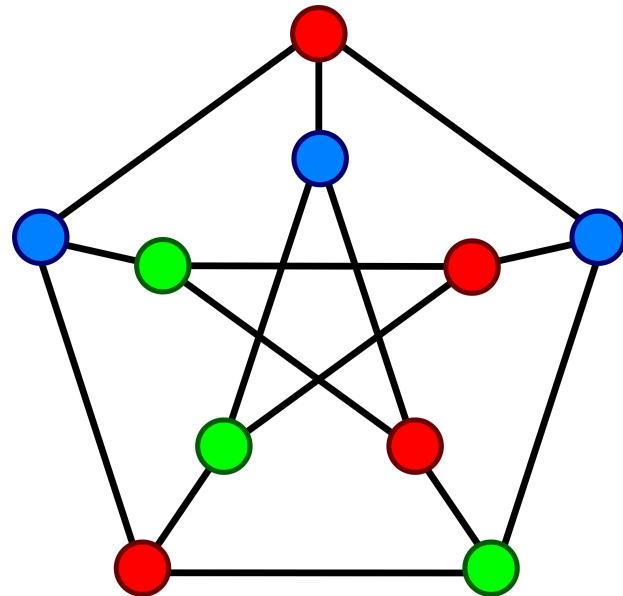
- n variables V
- finite alphabet A
- m clauses
- a clause consists of q variables $v_1, \dots, v_q \in V$ and "satisfying" set $S \subseteq A^q$

$\pi: V \rightarrow A$ satisfies clause if $(\pi(v_1), \dots, \pi(v_q)) \in S$

$V = \text{vertices}$

$A = \{\text{red, blue, green}\}$

clauses = edges



there are integers $q > 1$, $|A| > 1$ s.t.
given q -ary CSP P over alphabet A ,
it is NP-Hard to decide whether:

- $\text{UNSAT}(P) = 0$
- $\text{UNSAT}(P) \geq \frac{1}{2}$

q -ary constraint satisfaction problems

- n variables V
- finite alphabet A
- m clauses
- a clause consists of q variables $v_1, \dots, v_q \in V$
and "satisfying" set $S \subseteq A^q$

$\pi: V \rightarrow A$ satisfies clause if $(\pi(v_1), \dots, \pi(v_q)) \in S$

Graph CSP 2-ary CSP

variables = vertices

clause over $u, v \in V$

$\approx$ edge between u, v

given graph-CSP G , it is NP-Hard to distinguish:

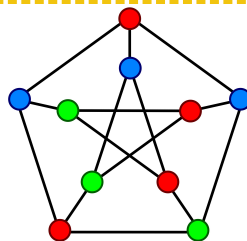
- $\text{UNSAT}(G) = 0$
- $\text{UNSAT}(G) \geq \frac{1}{m}$

Goal: amplify  to a constant

V = vertices

$A = \{\text{red, blue, green}\}$

clauses = edges



given graph-CSP G , it is NP-Hard

to distinguish:

- $UNSAT(G) = 0$
- $UNSAT(G) \geq \frac{1}{m}$

Goal: amplify $\nearrow$ to a constant

q -ary constraint satisfaction problems

- n variables V
- finite alphabet A
- m clauses
- a clause consists of q variables $v_1, \dots, v_k \in V$ and "satisfying" set $S \subseteq A^q$

$\pi: V \rightarrow A$ satisfies clause if $(\pi(v_1), \dots, \pi(v_k)) \in S$

Graph CSP 2-ary CSP
Variables = vertices
clause over $u, v \in V$
 $\approx$ edge between u, v

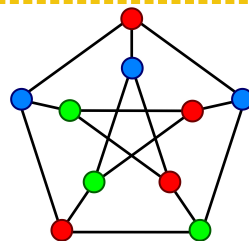
Three transformations:

1. "Expander-ification" make G a constant degree expander
2. Powering raises $UNSAT(G)$ but also increases $|A|$
3. Alphabet reduction

V = vertices

$A = \{\text{red, blue, green}\}$

clauses = edges



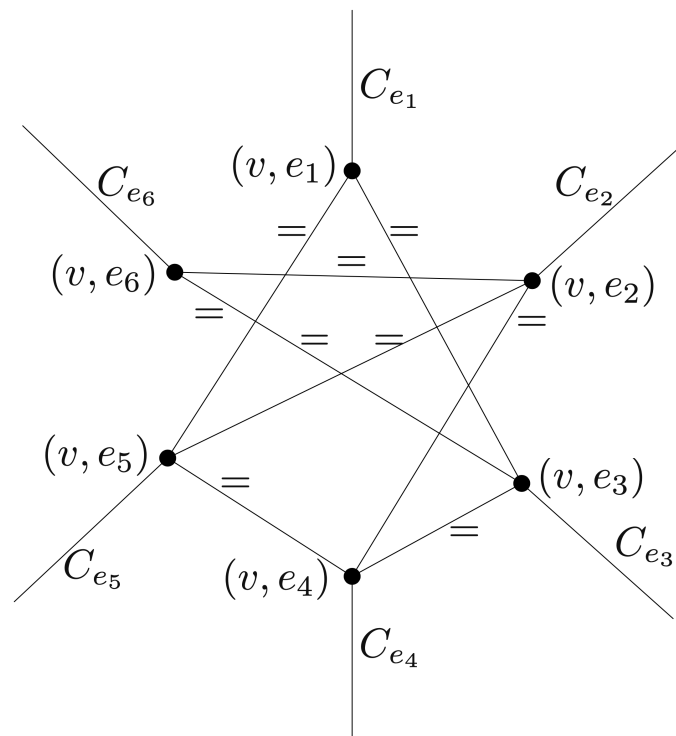
1. "Expander-ification" make G a constant degree expander

idea: replace each $v \in V$ w/ $O(1)$ -degree expander

1. for each edge $e = \{u, v\}$, make new vertices (u, e) and (v, e)

2. for each edge $e = (u, v)$, make edge $((u, e), (v, e))$ w/ same constraint

3. for each vertex v , add $O(1)$ -degree expander over $\{(v, e) : v \in e\}$. each of these edges get "equality constraint"



claim let $G = (V, E)$ be old graph, $G' = (V', E')$ be new graph.

(a) $|E'| \leq O(|E|)$ (b) G' is $O(1)$ -regular

(c) $\text{UNSAT}(G) \geq \text{UNSAT}(G') \geq \Omega(\text{UNSAT}(G))$

(exercise)

given graph-CSP G , it is NP-Hard

to distinguish:

- $UNSAT(G) = 0$
- $UNSAT(G) \geq \frac{1}{m}$

Goal: amplify $\nearrow$ to a constant

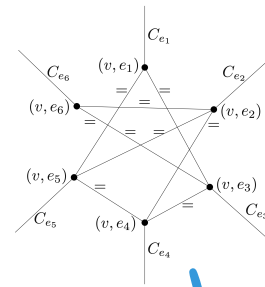
Three transformations:

1. "Expander-ification" make G a constant degree expander
2. Powering raises $UNSAT(G)$ but also increases $|A|$
3. Alphabet reduction

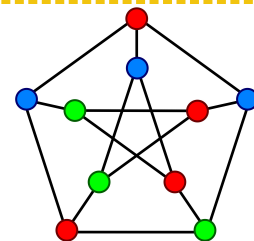
q -ary constraint satisfaction problems

- n variables V
- finite alphabet A
- m clauses
- a clause consists of q variables $v_1, \dots, v_k \in V$ and "satisfying" set $S \subseteq A^q$
- $\pi: V \rightarrow A$ satisfies clause if $(\pi(v_1), \dots, \pi(v_k)) \in S$

Graph CSP 2-ary CSP
Variables = vertices
clause over $u, v \in V$
 $\approx$ edge between u, v



V = vertices
 $A = \{\text{red, blue, green}\}$
clauses = edges



thought experiment: let $t \in \mathbb{N}$

given graph-CSP $G=(V,E)$

for $e_1, \dots, e_t \in E$, let $C_{e_1, \dots, e_t} = C_{e_1} \wedge C_{e_2} \wedge \dots \wedge C_{e_t}$
(constraint for e_1)

let $P = \{C_{e_1, \dots, e_t} : e_1, \dots, e_t\}$

$$\text{UNSAT}(P) = 1 - (1 - \text{unsat}(G))^t \approx t \text{ unsat}(G)$$

$$|P| = m^t$$

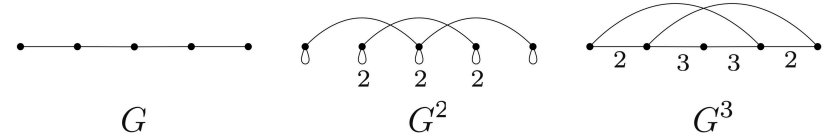
is P a graph CSP?

how to do something similar but graphically?

2. Powering raises $\text{UNSAT}(G)$ but also increases $|A|$

Idea: one constraint for each t -step walk

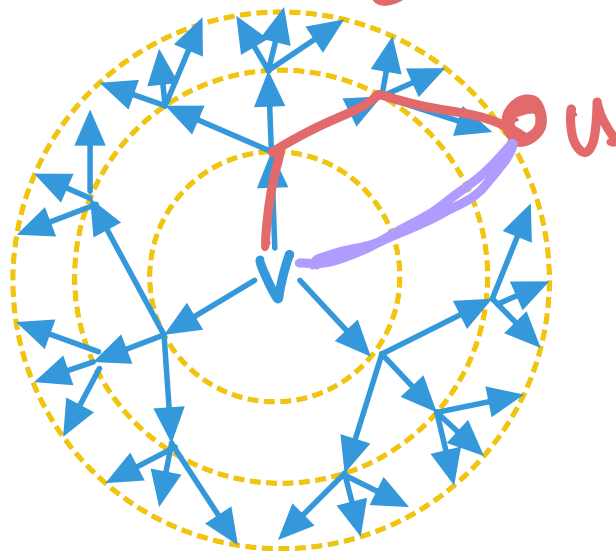
let $G^t = (V, E_t) = t$ th graph power



for $v \in V$, let $N_t(v) = \{u \text{ within } t \text{ steps of } v\}$

$$|N_t(v)| \leq D \text{ where } D = \sum_{i=1}^t d^i = (1+d)^t$$

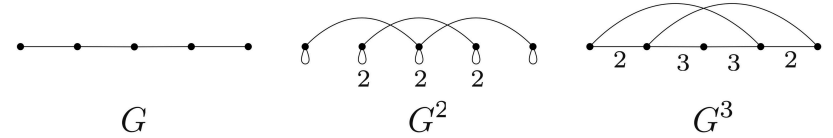
alphabet is A^D . for $\bar{\pi}: V \rightarrow A^D$, interpret $\bar{\pi}(v) \in A^D$
as an assignment $\bar{\pi}_v: N_t(v) \rightarrow A$



2. Powering raises $\text{UNSAT}(G)$ but also increases $|A|$

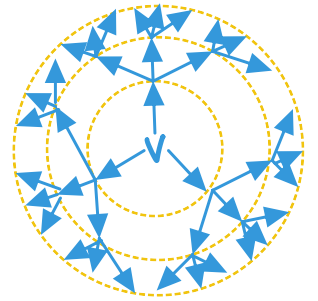
Idea: one constraint for each t -step walk

let $G^t = (V, E_t) = t$ th graph power



for $v \in V$, let $N_t(v) = \{u \text{ within } t \text{ steps of } v\}$

$$|N_t(v)| \leq D \text{ where } D = \sum_{i=1}^t d^i = (1+d)^t$$



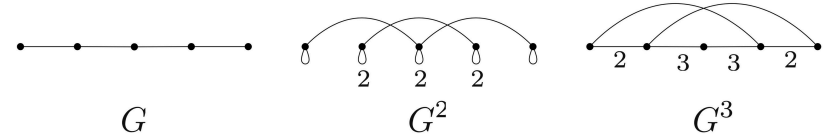
alphabet is A^D . for $\bar{\pi}: V \rightarrow A^D$, interpret $\bar{\pi}(v) \in A^D$
as an assignment $\bar{\pi}_v: N_t(v) \rightarrow A$

for each walk $W = (v_0 \xrightarrow{e_1} v_1 \xrightarrow{e_2} \dots \xrightarrow{e_t} v_t)$, edge $e_W = \{v_0, v_t\}$
in G_t is satisfied iff

2. Powering raises $\text{UNSAT}(G)$ but also increases $|A|$

Idea: one constraint for each t -step walk

let $G^t = (V, E_t) = t$ th graph power



for $v \in V$, let $N_t(v) = \{u \text{ within } t \text{ steps of } v\}$

$$|N_t(v)| \leq D \text{ where } D = \sum_{i=1}^t d^i = (1+d)^t$$

alphabet is A^D . for $\bar{\pi}: V \rightarrow A^D$, interpret $\bar{\pi}(v) \in A^D$
as an assignment $\bar{\pi}_v: N_t(v) \rightarrow A$

for each walk $W = (v_0 \xrightarrow{e_1} v_1 \xrightarrow{e_2} \dots \xrightarrow{e_t} v_t)$, edge $e_W = \{v_0, v_t\}$
in G_t is satisfied iff

- (a) $\bar{\pi}_{v_0}: N_t(v_0) \rightarrow A$ satisfies $e_1, \dots, e_t$ (c) $\bar{\pi}_{v_0}$ and $\bar{\pi}_{v_t}$ agree
(b) $\bar{\pi}_{v_t}: N_t(v_t) \rightarrow A$ satisfies $e_1, \dots, e_t$ on $N_t(v_0) \cap N_t(v_t)$

$N_+(v) = \{u \text{ within } t \text{ steps of } v\}$ $|N_+(v)| \leq D$ where $D = \sum_{i=1}^t d^i = (1+d)^t$

alphabet is A^D . for $\bar{\pi}: V \rightarrow A^D$, interpret $\bar{\pi}(v) \in A^D$
as an assignment $\bar{\pi}_v: N_+(v) \rightarrow A$

for each walk $W = (v_0 \xrightarrow{e_1} v_1 \xrightarrow{e_2} \dots \xrightarrow{e_t} v_t)$, edge $e_W = \{v_0, v_t\}$
in G_+ is satisfied iff

- | | |
|---|---|
| (a) $\bar{\pi}_{v_0}: N_+(v_0) \rightarrow A$ satisfies $e_1, \dots, e_t$ | (c) $\bar{\pi}_{v_0}$ and $\bar{\pi}_{v_t}$ agree |
| (b) $\bar{\pi}_{v_t}: N_+(v_t) \rightarrow A$ satisfies $e_1, \dots, e_t$ | on $N_+(v_0) \cap N_+(v_t)$ |
-



claim:

$$\text{UNSAT}(G^+) \geq$$

$$\Omega(\sqrt{t}) \min\{\text{UNSAT}(G), \frac{1}{t}\}$$

$N_t(v) = \{u \text{ within } t \text{ steps of } v\}$ $|N_t(v)| \leq D$ w/ $D = \sum_{i=1}^t d^i = (1+d)^t$
alphabet is A^D . For $\bar{\pi}: V \rightarrow A^D$, interpret $\bar{\pi}(v) \in A^D$
as an assignment $\bar{\pi}_v: N_t(v) \rightarrow A$

for walk $W = (v_0 \xrightarrow{e_1} v_1 \xrightarrow{e_2} \dots \xrightarrow{e_t} v_t)$, edge $e_W = \{v_0, v_t\}$
in G_+ is satisfied iff

- | | |
|---|---|
| (a) $\bar{\pi}_{v_0}: N_t(v_0) \rightarrow A$ satisfies $e_1, \dots, e_t$ | (c) $\bar{\pi}_{v_0}$ and $\bar{\pi}_{v_t}$ agree |
| (b) $\bar{\pi}_{v_t}: N_t(v_t) \rightarrow A$ satisfies $e_1, \dots, e_t$ | on $N_t(v_0) \cap N_t(v_t)$ |

t suff. large constant $\Rightarrow$

either $\text{UNSAT}(G) = \Omega(1)$ or $\text{UNSAT}(G^+) \geq 2\text{UNSAT}(G)$

how to set up a proof?

let $\bar{\pi}: V \rightarrow A^D$ be optimal for G^+
 define $\pi: V \rightarrow A$ as follows.

$N_+(v) = \{u \text{ within } t \text{ steps of } v\}$ $|N_+(v)| \leq D$
w/ $D = (1+d)^t$
 alphabet is A^D . for $\bar{\pi}: V \rightarrow A^D$,
 interpret $\bar{\pi}(v) \in A^D$ as $\bar{\pi}_v: N_+(v) \rightarrow A$
 for each walk $W = (v_0 \xrightarrow{e_1} v_1 \xrightarrow{e_2} \dots \xrightarrow{e_t} v_t)$,
 edge $e_W = \{v_0, v_t\}$ is satisfied iff
 (a) $\bar{\pi}_{v_0}: N_+(v_0) \rightarrow A$ satisfies $e_1, \dots, e_t$
 (b) $\bar{\pi}_{v_t}: N_+(v_t) \rightarrow A$ satisfies $e_1, \dots, e_t$
 (c) $\bar{\pi}_{v_0}$ and $\bar{\pi}_{v_t}$ agree on $N_+(v_0) \cap N_+(v_t)$

claim: $\text{UNSAT}(G^+) \geq$
 $\Omega(\sqrt{t}) \min\{\text{UNSAT}(G), \frac{1}{t}\}$

Some high-level ideas:

suppose π satisfies C_e w/ $e = \{u, v\}$

$N_+(v) = \{u \text{ within } t \text{ steps of } v\}$ $|N_+(v)| \leq D$
w/ $D = (1+d)^t$
alphabet is A^D . For $\bar{\pi}: V \rightarrow A^D$,
interpret $\bar{\pi}(v) \in A^D$ as $\bar{\pi}_v: N_+(v) \rightarrow A$

for each walk $W = (v_0 \xrightarrow{e_1} v_1 \xrightarrow{e_2} \dots \xrightarrow{e_t} v_t)$,
edge $e_W = \{v_0, v_t\}$ is satisfied iff

(a) $\bar{\pi}_{v_0}: N_+(v_0) \rightarrow A$ satisfies $e_1, \dots, e_t$

(b) $\bar{\pi}_{v_t}: N_+(v_t) \rightarrow A$ satisfies $e_1, \dots, e_t$

(c) $\bar{\pi}_{v_0}$ and $\bar{\pi}_{v_t}$ agree on $N_+(v_0) \cap N_+(v_t)$

claim: $\text{UNSAT}(G^+) \geq$
 $\Omega(\sqrt{t}) \min\{\text{UNSAT}(G), \frac{1}{t}\}$

$\bar{\pi}: V \rightarrow A^D$ optimal for G^+

$\pi(v) \stackrel{\text{def}}{=} \text{most likely } \bar{\pi}(v_{t/2}, v)$

w/ $(v_0 = v, v_1, \dots, v_{t/2})$ is $(\frac{1}{2})$ -step lazy rand. walk

$$\Pr[\pi(v) = \bar{\pi}(v_{t/2}, v)] \geq \Omega(1)$$

let $\bar{\pi}: V \rightarrow A^D$ be optimal for G^+

define $\pi: V \rightarrow A$ as follows.

- for each $v \in V$, let $(v_0 = v, v_1, \dots, v_{t/2})$ be $(\frac{t}{2})$ -step lazy random walk (RW)



$\bar{\pi}(v_{t/2}, v) \in A$ is a random letter

define $\pi(v)$ as most likely to be $\bar{\pi}(v_{t/2}, v)$

$N_t(v) = \{u \text{ within } t \text{ steps of } v\}$ $|N_t(v)| \leq D$
w/ $D = (1+d)^t$
alphabet is A^D . for $\bar{\pi}: V \rightarrow A^D$,
interpret $\bar{\pi}(v) \in A^D$ as $\bar{\pi}_v: N_t(v) \rightarrow A$
for each walk $W = (v_0 \xrightarrow{e_1} v_1 \xrightarrow{e_2} \dots \xrightarrow{e_t} v_t)$,
edge $e_W = \{v_0, v_t\}$ is satisfied iff
(a) $\bar{\pi}_{v_0}: N_t(v_0) \rightarrow A$ satisfies $e_1, \dots, e_t$
(b) $\bar{\pi}_{v_t}: N_t(v_t) \rightarrow A$ satisfies $e_1, \dots, e_t$
(c) $\bar{\pi}_{v_0}$ and $\bar{\pi}_{v_t}$ agree on $N_t(v_0) \cap N_t(v_t)$

claim: $\text{UNSAT}(G^+) \geq \Omega(\sqrt{t}) \min \{ \text{UNSAT}(G), \frac{1}{t} \}$

claim:

$$\text{UNSAT}(\bar{\pi} | G^+) \geq \Omega(\sqrt{t}) \min \{ \text{UNSAT}(\pi | G), \frac{1}{t} \}$$

first we need 2 lemmas

let $I = \{i: |i - t/2| \leq \sqrt{t/2}\}$

let $v_0 = v, v_1, v_2, \dots$ lazy RW from v

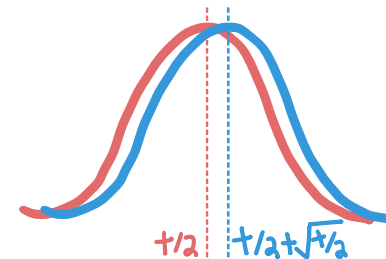
Lemma for all $i \in I$,

$$P[\pi(v) = \bar{\pi}(v_i, v)] \geq \Omega(1)$$

$N_t(v) = \{u \text{ within } t \text{ steps of } v\}$ $|N_t(v)| \leq D$
w/ $D = (1+d)^t$
alphabet is A^D . for $\bar{\pi}: V \rightarrow A^D$,
interpret $\bar{\pi}(v) \in A^D$ as $\bar{\pi}_v: N_t(v) \rightarrow A$
for each walk $W = (v_0 \xrightarrow{e_1} v_1 \xrightarrow{e_2} \dots \xrightarrow{e_t} v_t)$,
edge $e_W = \{v_0, v_t\}$ is satisfied iff
(a) $\bar{\pi}_{v_0}: N_t(v_0) \rightarrow A$ satisfies $e_1, \dots, e_t$
(b) $\bar{\pi}_{v_t}: N_t(v_t) \rightarrow A$ satisfies $e_1, \dots, e_t$
(c) $\bar{\pi}_{v_0}$ and $\bar{\pi}_{v_t}$ agree on $N_t(v_0) \cap N_t(v_t)$

claim: $\text{UNSAT}(G^t) \geq \Omega(\sqrt{t}) \min\{\text{UNSAT}(G), \frac{1}{t}\}$

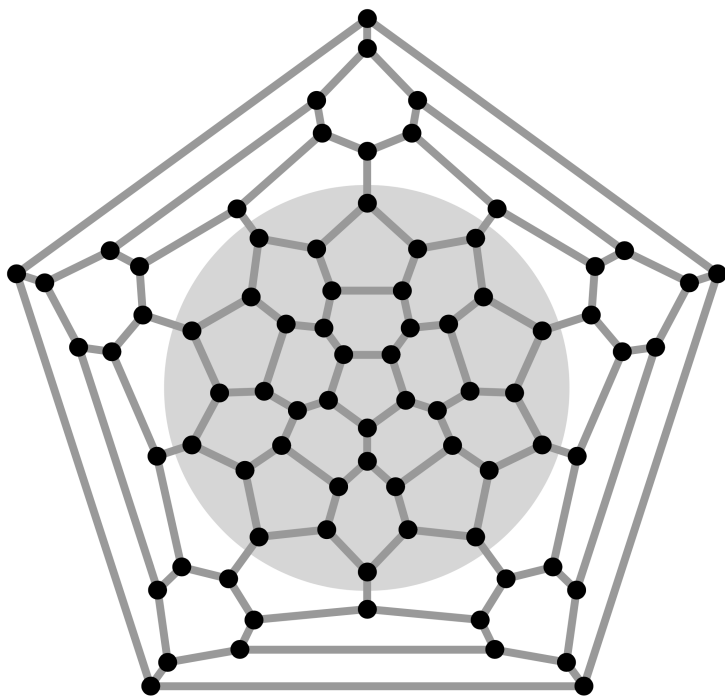
$\bar{\pi}: V \rightarrow A^D$ optimal for G^t
 $\pi(v) \stackrel{\text{def}}{=} \text{most likely } \bar{\pi}(v_{t/2}, v)$
w/ $(v_0 = v, v_1, \dots, v_{t/2})$ is $(\frac{1}{2})$ -step lazy rand. walk
 $P[\pi(v) = \bar{\pi}(v_{t/2}, v)] \geq \Omega(1)$



Lemma let $F \subseteq E$, $\mu = |F|/|E|$

let $v_0, v_1, v_2, \dots$ be RW where v_0 is a random endpoint of a random edge in F . Then

$$\Pr[(v_i, v_{i+1}) \in F] \leq \mu + (1-\gamma)^i$$



$N_+(v) = \{u \text{ within } t \text{ steps of } v\}$ $\frac{|N_+(v)| \leq D}{w/D = (1+d)^t}$
 alphabet is A^D . for $\bar{\pi}: V \rightarrow A^D$,
 interpret $\bar{\pi}(v) \in A^D$ as $\bar{\pi}_v: N_+(v) \rightarrow A$

for each walk $W = (v_0 \xrightarrow{e_1} v_1 \xrightarrow{e_2} \dots \xrightarrow{e_t} v_t)$,
 edge $e_W = \{v_0, v_t\}$ is satisfied iff

- (a) $\bar{\pi}_{v_0}: N_+(v_0) \rightarrow A$ satisfies $e_1, \dots, e_t$
- (b) $\bar{\pi}_{v_t}: N_+(v_t) \rightarrow A$ satisfies $e_1, \dots, e_t$
- (c) $\bar{\pi}_{v_0}$ and $\bar{\pi}_{v_t}$ agree on $N_+(v_0) \cap N_+(v_t)$

claim: $\text{UNSAT}(G^+) \geq \Omega(\sqrt{t}) \min\{\text{UNSAT}(G), \frac{1}{t}\}$

$\bar{\pi}: V \rightarrow A^D$ optimal for G^+
 $\pi(v) \stackrel{\text{def}}{=} \text{most likely } \bar{\pi}(v_{t/2}, v)$

w/ $v_0 = v, v_1, v_2, \dots$ lazy RW from v

let $I = \{i: |i - t/2| \leq \sqrt{t/2}\}$

Lemma for all $i \in I$,

$$\Pr[\pi(v) = \bar{\pi}(v_i, v)] \geq \Omega(1)$$

$$\text{UNSAT}(\bar{\pi} | G^+) \geq$$

$$\Omega(\sqrt{F}) \min \{ \text{UNSAT}(\pi | G), \frac{1}{4} \}$$

$F =$ edges failed by π , $\mu = |F|/|E|$
 $= \text{UNSAT}(\pi | G)$

assume $\mu \leq 1/4$ (else drop edges from F)

$N_+(v) = \{u \text{ within } t \text{ steps of } v\}$ $|N_+(v)| \leq D$
w/ $D = (1+d)^t$
 alphabet is A^D . For $\bar{\pi}: V \rightarrow A^D$,

interpret $\bar{\pi}(v) \in A^D$ as $\bar{\pi}_v: N_+(v) \rightarrow A$

for each walk $W = (v_0 \xrightarrow{e_1} v_1 \xrightarrow{e_2} \dots \xrightarrow{e_t} v_t)$,

edge $e_W = \{v_0, v_t\}$ is satisfied iff

(a) $\bar{\pi}_{v_0}: N_+(v_0) \rightarrow A$ satisfies $e_1, \dots, e_t$

(b) $\bar{\pi}_{v_t}: N_+(v_t) \rightarrow A$ satisfies $e_1, \dots, e_t$

(c) $\bar{\pi}_{v_0}$ and $\bar{\pi}_{v_t}$ agree on $N_+(v_0) \cap N_+(v_t)$

claim: $\text{UNSAT}(G^+) \geq$

$$\Omega(\sqrt{F}) \min \{ \text{UNSAT}(G), \frac{1}{4} \}$$

$\bar{\pi}: V \rightarrow A^D$ optimal for G^+

$\pi(v) \stackrel{\text{def}}{=} \text{most likely } \bar{\pi}(v_{t/2}, v)$

w/ $v_0 = v, v_1, v_2, \dots$ lazy RW from v

let $I = \{i: |i - t/2| \leq \sqrt{t/2}\}$

Lemma for all $i \in I$,

$$P[\pi(v) = \bar{\pi}(v_i, v)] \geq \Omega(1)$$

Lemma let $F \subseteq E$, $\mu = |F|/|E|$

let $v_0, v_1, v_2, \dots$ be RW where v_0 is a random endpoint of a random edge in F . Then

$$Pr[(v_i, v_{i+1}) \in F] \leq \mu + (1-\delta)^i$$

$w = (v_0, \sim, v_t) = \text{unif. random } t\text{-step lazy RW}$



let $e_i = (v_{i-1}, v_i) = \text{ith edge/step on walk}$

for $i \in I$, R.V. $X_i \in \{0, 1\}$ w/ $X_i = 1$ if:

(a) $\pi(v_{i-1}) = \bar{\pi}_{v_0}(v_{i-1})$ & $\pi(v_i) = \bar{\pi}_{v_t}(v_i)$

(b) π fails constraint C_{e_i} (i.e., $e_i \in F$)

let $X = \sum_{i \in I} X_i$. then $\text{UNSAT}(G^t) \geq P[X > 0]$

next: analyze $P[X > 0]$

$N_t(v) = \{u \text{ within } t \text{ steps of } v\}$ $|N_t(v)| \leq D$
w/ $D = (1+d)^t$
alphabet is A^D . for $\bar{\pi}: V \rightarrow A^D$,
interpret $\bar{\pi}(v) \in A^D$ as $\bar{\pi}_v: N_t(v) \rightarrow A$

for each walk $W = (v_0 \xrightarrow{e_1} v_1 \xrightarrow{e_2} \dots \xrightarrow{e_t} v_t)$,

edge $e_W = \{v_0, v_t\}$ is satisfied iff

(a) $\bar{\pi}_{v_0}: N_t(v_0) \rightarrow A$ satisfies $e_1, \dots, e_t$

(b) $\bar{\pi}_{v_t}: N_t(v_t) \rightarrow A$ satisfies $e_1, \dots, e_t$

(c) $\bar{\pi}_{v_0}$ and $\bar{\pi}_{v_t}$ agree on $N_t(v_0) \cap N_t(v_t)$

claim: $\text{UNSAT}(G^t) \geq$

$\Omega(\sqrt{t}) \min\{\text{UNSAT}(G), \frac{1}{t}\}$

$\bar{\pi}: V \rightarrow A^D$ optimal for G^t

$\pi(v) \stackrel{\text{def}}{=} \text{most likely } \bar{\pi}(v_{t/2}, v)$

w/ $v_0 = v, v_1, v_2, \dots$ lazy RW from v

let $I = \{i: |i - t/2| \leq \sqrt{t/2}\}$

Lemma for all $i \in I$,

$P[\pi(v) = \bar{\pi}(v_i, v)] \geq \Omega(1)$

Lemma let $F \subseteq E$, $\mu = |F|/|E|$

let $v_0, v_1, v_2, \dots$ be RW where v_0 is a random endpoint of a random edge in F . Then

$P_r[(v_i, v_{i+1}) \in F] \leq \mu + (1-\gamma)^i$

$F = \text{edges failed by } \pi$,

$\mu = |F|/|E| = \text{UNSAT}(\pi|G)$, $\mu \leq 1/4$

$$\text{UNSAT}(G^+) \geq P[X > 0]$$

$$\text{claim: } E[X_i] \geq \Omega(\mu) \quad \forall i \in I$$

alternative way to sample w

① sample $e_i = (v_{i-1}, v_i)$ unif. random

② take lazy RW's $\begin{cases} v_{i-1}, \rightsquigarrow, v_0 \\ v_i, \rightsquigarrow, v_t \end{cases}$



$$P[X_i = 1]$$

$$= \mu P[\bar{\pi}(v_0, v_{i-1}) = \pi(v_i)] P[\bar{\pi}(v_t, v_i) = \pi(v_i)]$$

$$= \Omega(\mu)$$

$$\text{UNSAT}(\bar{\pi}|G^+) \geq \Omega(\sqrt{t}) \min\{\text{UNSAT}(\pi|G), \frac{1}{t}\}$$

$\bar{\pi}: V \rightarrow A^D$ optimal for G^+
 $\pi(v) \stackrel{\text{def}}{=} \text{most likely } \bar{\pi}(v_{t/2}, v)$

w/ $v_0 = v, v_1, v_2, \rightsquigarrow$ lazy RW from v

let $I = \{i: |i - t/2| \leq \sqrt{t/2}\}$

Lemma for all $i \in I$

$$P[\pi(v) = \bar{\pi}(v_i, v)] \geq \Omega(1)$$

Lemma let $F \subseteq E$, $\mu = |F|/|E|$

let $v_0, v_1, v_2, \rightsquigarrow$ be RW where v_0 is a random endpoint of a random edge in F . Then

$$Pr[(v_i, v_{i+1}) \in F] \leq \mu + (1-\delta)^i$$

F = edges failed by π ,

$$\mu = |F|/|E| = \text{UNSAT}(\pi|G), \mu \leq 1/4$$

$w = (v_0, \rightsquigarrow, v_t)$ = unif. random t -step lazy RW

let $e_i = (v_{i-1}, v_i)$ = i th edge/step on walk

for $i \in I$, R.V. $X_i \in \{0, 1\}$ w/ $X_i = 1$ is:

(a) $\pi(v_{i-1}) = \bar{\pi}_{v_0}(v_{i-1})$ & $\pi(v_i) = \bar{\pi}_{v_t}(v_i)$

(b) π fails constraint C_{e_i}

let $X = \sum_{i \in I} X_i$. then $\text{UNSAT}(G^+) \geq P[X > 0]$

$$\text{UNSAT}(G^+) \geq P[X > 0]$$

$$\checkmark E[X_i] \geq \Omega(\mu) \quad \forall i \in I$$

$$\text{claim: } E[X^2] \leq O(\sqrt{t})\mu$$

$$\text{claim: for } i \neq j, E[X_i X_j] \leq \mu(\mu + (1-\delta)^{j-i-1})$$

$$\text{let } Y_i = \begin{cases} 1 & \text{if } e_i \in F \\ 0 & \text{otherwise} \end{cases}$$

$$E[X_i X_j] \leq E[Y_i Y_j] \\ = E[Y_i] E[Y_j | Y_i = 1]$$

μ $\nearrow$

$\mu + (1-\delta)^{j-i-1}$ $\nwarrow$

$$\text{UNSAT}(\bar{\pi} | G^+) \geq \Omega(\sqrt{t}) \min \{ \text{UNSAT}(\pi | G), \frac{1}{t} \}$$

$\bar{\pi}: V \rightarrow A^D$ optimal for G^+

$\pi(v) \stackrel{\text{def}}{=} \text{most likely } \bar{\pi}(v_{t/2}, v)$

w/ $v_0 = v, v_1, v_2, \dots$ lazy RW from v

let $I = \{i: |i - t/2| \leq \sqrt{t/2}\}$

Lemma for all $i \in I$

$$P[\pi(v) = \bar{\pi}(v_i, v)] \geq \Omega(1)$$

Lemma let $F \subseteq E$, $\mu = |F|/|E|$

let $v_0, v_1, v_2, \dots$ be RW where v_0 is a random endpoint of a random edge in F . Then

$$Pr[(v_i, v_{i+1}) \in F] \leq \mu + (1-\delta)^i$$

F = edges failed by π ,

$$\mu = |F|/|E| = \text{UNSAT}(\pi | G), \mu \leq 1/t$$

$w = (v_0, \dots, v_t) = \text{unif. random } t\text{-step lazy RW}$

let $e_i = (v_{i-1}, v_i) = i\text{th edge/step on walk}$

for $i \in I$, R.V. $X_i \in \{0, 1\}$ w/ $X_i = 1$ is:

(a) $\pi(v_{i-1}) = \bar{\pi}_{v_0}(v_{i-1})$ & $\pi(v_i) = \bar{\pi}_{v_t}(v_i)$

(b) π fails constraint C_{e_i}

let $X = \sum_{i \in I} X_i$. then $\text{UNSAT}(G^+) \geq P[X > 0]$

$$\text{UNSAT}(G^\dagger) \geq P[X > 0]$$

$$\checkmark E[X_i] \geq \Omega(\mu) \quad \forall i \in I$$

$$\text{claim: } E[X^2] \leq O(\sqrt{F}) \mu$$

$$\checkmark \text{ for } i \neq j, E[X_i X_j] \leq \mu(\mu + (1-\delta)^{j-i-1})$$

$$E[X^2] = \sum_{i \in I} E[X_i] + \sum_{\substack{i, j \in I \\ i \neq j}} E[X_i X_j]$$

$$\leq \mu |I| + 2\mu^2 |I|^2 + 2\mu \sum_{\substack{i, j \in I \\ i \neq j}} (1-\delta)^{j-i-1}$$

$$\leq O(\mu |I| + \mu^2 |I|^2)$$

$$= O(\sqrt{F}) \mu$$

$$\leq O(|I|)$$

$$\text{UNSAT}(\bar{\pi} | G^\dagger) \geq \Omega(\sqrt{F}) \min \{ \text{UNSAT}(\pi | G), \frac{1}{t} \}$$

$\bar{\pi}: V \rightarrow A^D$ optimal for $G^\dagger$
 $\pi(v) \stackrel{\text{def}}{=} \text{most likely } \bar{\pi}(v_{t/2}, v)$

w/ $v_0 = v, v_1, v_2, \dots$ lazy RW from v

let $I = \{i: |i - t/2| \leq \sqrt{t/2}\}$

Lemma for all $i \in I$,

$$P[\pi(v) = \bar{\pi}(v_i, v)] \geq \Omega(1)$$

Lemma let $F \subseteq E$, $\mu = |F|/|E|$

let $v_0, v_1, v_2, \dots$ be RW where v_0 is a random endpoint of a random edge in F . Then

$$Pr[(v_i, v_{i+1}) \in F] \leq \mu + (1-\delta)^i$$

$F =$ edges failed by π ,

$$\mu = |F|/|E| = \text{UNSAT}(\pi | G), \mu \leq 1/t$$

$w = (v_0, \dots, v_t) =$ unif. random t -step lazy RW

let $e_i = (v_{i-1}, v_i) =$ i th edge/step on walk

for $i \in I$, R.V. $X_i \in \{0, 1\}$ w/ $X_i = 1$ is:

(a) $\pi(v_{i-1}) = \bar{\pi}_{v_0}(v_{i-1})$ & $\pi(v_i) = \bar{\pi}_{v_t}(v_i)$

(b) π fails constraint C_{e_i}

let $X = \sum_{i \in I} X_i$. then $\text{UNSAT}(G^\dagger) \geq P[X > 0]$

$$\text{UNSAT}(G^+) \geq P[X > 0]$$

$$\checkmark E[X_i] \geq \Omega(\mu) \quad \forall i \in I$$

$$\checkmark E[X^2] \leq O(\sqrt{t})\mu$$

$$E[X] = \sum_{i \in I} E[X_i] \geq \Omega(\sqrt{t})\mu$$

$$E[X^2] = E[X^2 | X > 0] P[X > 0]$$

$$\text{UNSAT}(\bar{\pi} | G^+) \geq \Omega(\sqrt{t}) \min \{ \text{UNSAT}(\pi | G), \frac{1}{t} \}$$

$\bar{\pi}: V \rightarrow A^D$ optimal for G^+
 $\pi(v) \stackrel{\text{def}}{=} \text{most likely } \bar{\pi}(v_{t/2}, v)$

w/ $v_0 = v, v_1, v_2, \dots$ lazy RW from v

let $I = \{i: |i - t/2| \leq \sqrt{t/2}\}$

Lemma for all $i \in I$,

$$P[\pi(v) = \bar{\pi}(v_i, v)] \geq \Omega(1)$$

Lemma let $F \subseteq E$, $\mu = |F|/|E|$

let $v_0, v_1, v_2, \dots$ be RW where v_0 is a random endpoint of a random edge in F . Then

$$P_r[(v_i, v_{i+1}) \in F] \leq \mu + (1-\delta)^i$$

$F =$ edges failed by π ,

$$\mu = |F|/|E| = \text{UNSAT}(\pi | G), \mu \leq 1/4$$

$w = (v_0, \dots, v_t) =$ unif. random t -step lazy RW

let $e_i = (v_{i-1}, v_i) =$ i th edge/step on walk

for $i \in I$, R.V. $X_i \in \{0, 1\}$ w/ $X_i = 1$ is:

(a) $\pi(v_{i-1}) = \bar{\pi}_{v_0}(v_{i-1})$ & $\pi(v_i) = \bar{\pi}_{v_t}(v_i)$

(b) π fails constraint C_{e_i}

let $X = \sum_{i \in I} X_i$. then $\text{UNSAT}(G^+) \geq P[X > 0]$

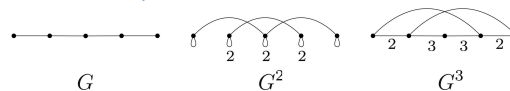
Jensen's inequality: for convex ζ ,

$$\zeta(E[X]) \leq E[\zeta(X)]$$

2. Powering raises $\text{UNSAT}(G)$ but also increases $|A|$

Idea: one constraint for each t -step walk

let $G^t = (V, E_t) = t$ th graph power



for $v \in V$, let $N_t(v) = \{u \text{ within } t \text{ steps of } v\}$

$$|N_t(v)| \leq D \text{ where } D = \sum_{i=1}^t d^i = (1+d)^t$$

alphabet is A^D . for $\bar{\pi}: V \rightarrow A^D$, interpret $\bar{\pi}(v) \in A^D$
as an assignment $\bar{\pi}_v: N_t(v) \rightarrow A$

for each walk $W = (v_0 \xrightarrow{e_1} v_1 \xrightarrow{e_2} \dots \xrightarrow{e_t} v_t)$, edge $e_W = \{v_0, v_t\}$
in G_t is satisfied iff

- (a) $\bar{\pi}_{v_0}: N_t(v_0) \rightarrow A$ satisfies $e_1, \dots, e_t$
- (b) $\bar{\pi}_{v_t}: N_t(v_t) \rightarrow A$ satisfies $e_1, \dots, e_t$
- (c) $\bar{\pi}_{v_0}$ and $\bar{\pi}_{v_t}$ agree on $N_t(v_0) \cap N_t(v_t)$

claim: $\text{UNSAT}(G^t) \geq \Omega(\sqrt{t}) \min\{\text{UNSAT}(G), \frac{1}{t}\}$

given graph-CSP G , it is NP-Hard

to distinguish:

- $UNSAT(G) = 0$
- $UNSAT(G) \geq \frac{1}{m}$

Goal: amplify $\nearrow$ to a constant

q -ary constraint satisfaction problems

- n variables V
- finite alphabet A
- m clauses
- a clause consists of q variables $v_1, \dots, v_k \in V$ and "satisfying" set $S \subseteq A^q$

$\pi: V \rightarrow A$ satisfies clause if $(\pi(v_1), \dots, \pi(v_k)) \in S$

Graph CSP 2-ary CSP
Variables = vertices
clause over $u, v \in V$
 $\approx$ edge between u, v

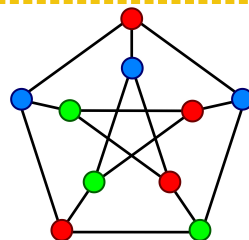
Three transformations:

- ✓ 1. "Expander-ification" make G a constant degree expander
- ✓ 2. Powering raises $UNSAT(G)$ but also increases $|A|$
3. Alphabet reduction

V = vertices

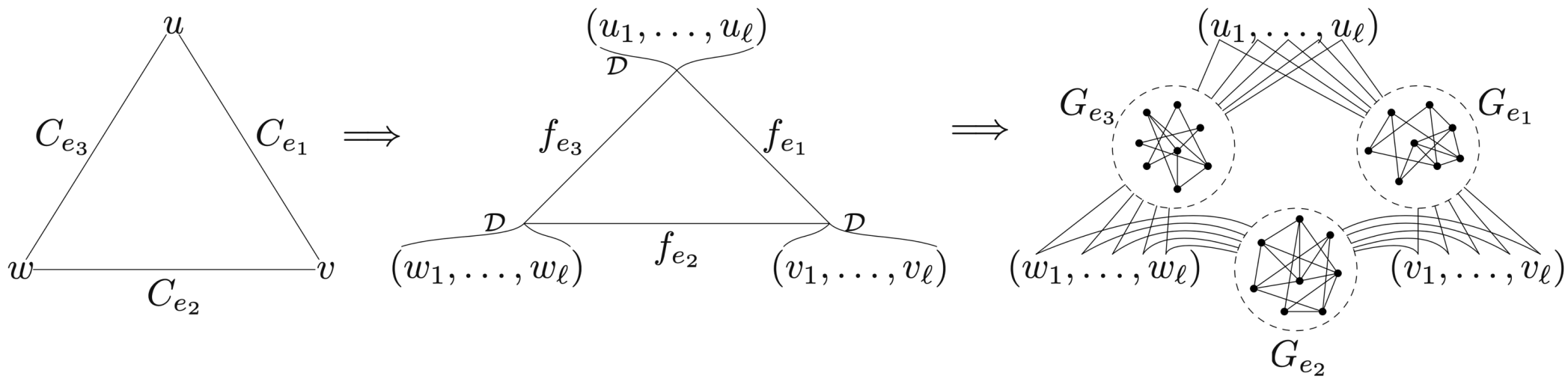
$A = \{\text{red, blue, green}\}$

clauses = edges



3. Alphabet reduction

goal: decrease alphabet size to constant



step 1: reduce to $A = \{0, 1\}$ w/ error-correcting codes

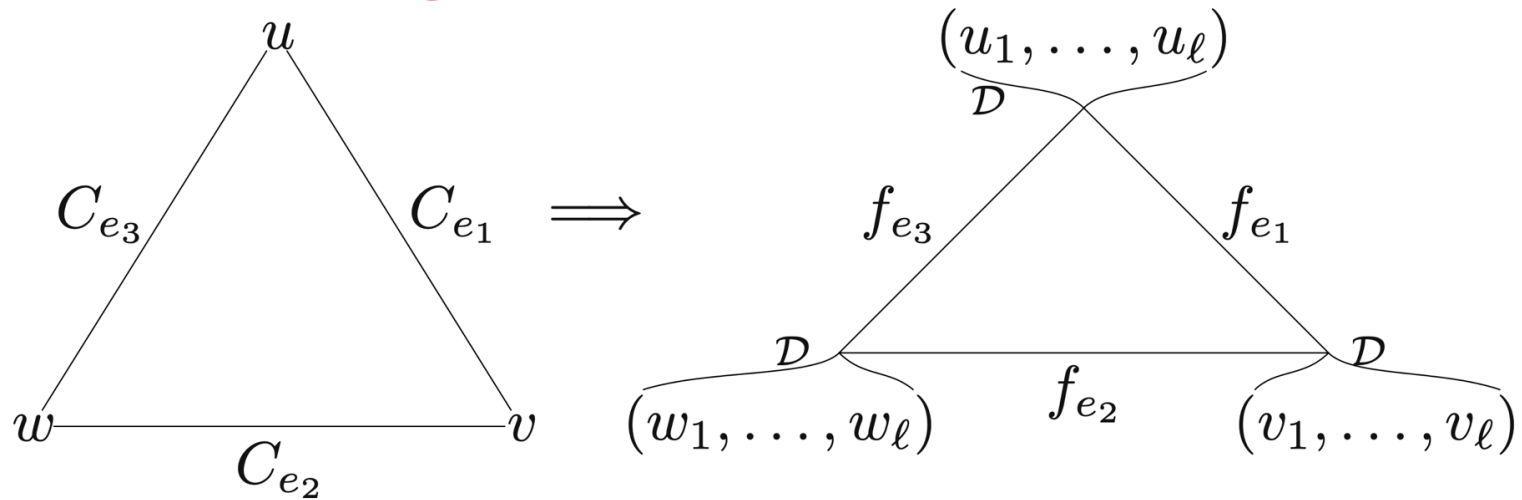
* $\uparrow$ replaces each edge w/ general constraint over $O(1)$ variables *

step 2: replace each constraint w/ graph CSP

* use techniques as black box *

step 1: reduce to $A = \{0,1\}$ w/ error-correcting codes

* $\uparrow$ replaces each edge w/ general constraint over $O(1)$ variables *



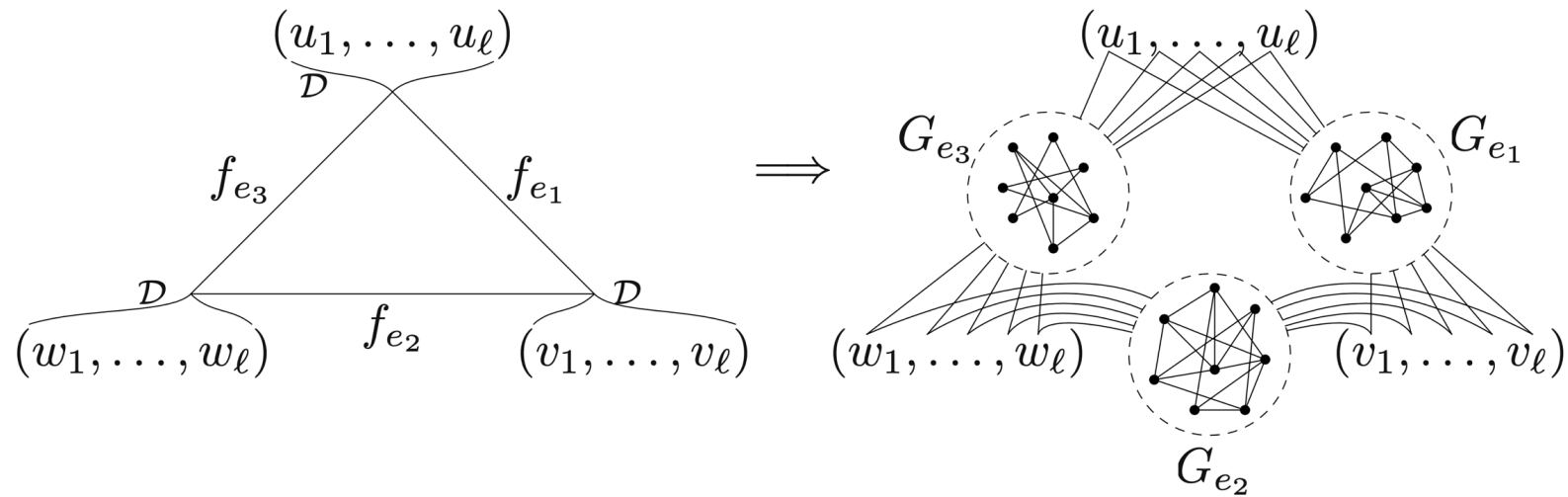
let $c: A \rightarrow \{0,1\}^\ell$ be code w/ $\ell = O(\log|A|)$ and
relative distance $\rho \in [0,1]$ ($\text{Hamming}(c(a_1), c(a_2)) \geq \rho \ell \ \forall a_1 \neq a_2$)

split each vertex u into ℓ vertices $V_u = \{v_1, \dots, v_\ell\}$

replace edge $e = \{u, v\}$ w/ formula $f_e: \{0,1\}^{V_u} \times \{0,1\}^{V_v}$ s.t.

$$f_e(x_u, x_v) = \begin{cases} 1 & \text{if } x_u = c(a_1), x_v = c(a_2), (a_1, a_2) \in C_e \\ 0 & \text{otherwise} \end{cases}$$

step 2: replace each constraint w/ graph CSP



Lemma: for $e \in E$, one can construct graph-CSP $G_e = (V_e, E_e, A_0)$ s.t.:

(a) $V_u, V_v \subseteq V_e$ (b) $|E_e|, |V_e|, |A_0| = O(1)$ and same $\forall e$

(c) completeness: if $f_e(x_u, x_v) = 1$, then one can extend (x_u, x_v) to $\sigma: V_e \rightarrow A_0$ that satisfies all of G_e

(d) soundness: if $f_e(x_u, x_v) = 0$, then $\forall$ extensions σ of (x_u, x_v) ,

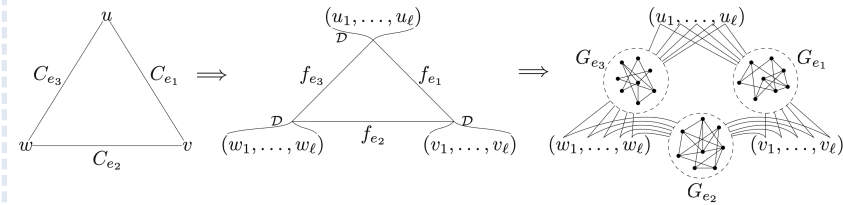
$$\text{UNSAT}(\sigma|G_e) \geq \Omega\left(\min\left\{\frac{\text{Hamming}((x_u, x_v), (y_u, y_v))}{\ell}: f(y_u, y_v) = 1\right\}\right)$$

let $\bar{G}$ = resulting graph CSP

Lemma $\text{UNSAT}(\bar{G}) \leq \text{UNSAT}(G)$

3. Alphabet reduction

goal: decrease alphabet size to constant



step 1: reduce to $A = \{0, 1\}$ w/ error-correcting codes

* $\uparrow$ replaces each edge w/ general constraint over $O(1)$ variables *

let $C: A \rightarrow \{0, 1\}^{\ell}$ be code w/ $\ell = O(\log |A|)$ and relative distance $\rho \in [0, 1]$ ($\text{Hamming}(C(a_1), C(a_2)) \geq \rho \ell \ \forall a_1 \neq a_2$)

split each vertex u into ℓ vertices $V_u = \{v_{u,1}, \dots, v_{u,\ell}\}$

replace edge $e = \{u, v\}$ w/ formula $f_e: \{0, 1\}^{V_u} \times \{0, 1\}^{V_v}$ s.t.

$$f_e(x_u, x_v) = \begin{cases} 1 & \text{if } x_u = C(a_1), x_v = C(a_2), (a_1, a_2) \in C_e \\ 0 & \text{otherwise} \end{cases}$$

step 2: replace each constraint w/ graph CSP

Lemma: for $e \in E$, one can construct graph-CSP $G_e = (V_e, E_e, A_0)$ s.t.:

(a) $V_u, V_v \subseteq V_e$ (b) $|E_e|, |V_e|, |A_0| = O(1)$ and same $\forall e$

(c) completeness: if $f_e(x_u, x_v) = 1$, then one can extend (x_u, x_v) to $\sigma: V_e \rightarrow A_0$ that satisfies all of G_e

(d) soundness: if $f_e(x_u, x_v) = 0$, then $\forall$ extensions σ of (x_u, x_v) ,

$$\text{UNSAT}(\sigma|G_e) \geq \Omega\left(\min\left\{\frac{\text{Hamming}((x_u, x_v), (y_u, y_v))}{\ell} : f(y_u, y_v) = 1\right\}\right)$$

let $\bar{G}=(\bar{V},\bar{E})$ = resulting graph CSP

Lemma $\text{UNSAT}(\bar{G}) \geq \Omega(\rho \text{UNSAT}(G))$

let $\bar{\pi}:\bar{V} \rightarrow A_0$ attain $\text{UNSAT}(G)$

let $\pi:V \rightarrow A$ where for $v \in V$,

$$\pi(v) = \text{decode}(\bar{\pi}(v_1), \dots, \bar{\pi}(v_\ell))$$

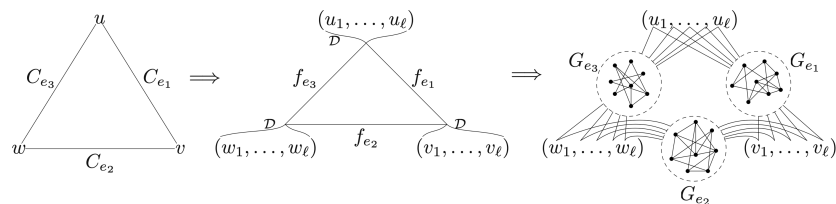
claim for $e \in E$, if π fails e ,

then $\text{UNSAT}(\bar{\pi}|G_e) \geq \Omega(\rho)$

if so, then

3. Alphabet reduction

goal: decrease alphabet size to constant



step 1: reduce to $A=\{0,1\}$ w/ error-correcting codes

* $\uparrow$ replaces each edge w/ general constraint over $O(1)$ variables *

let $C:A \rightarrow \{0,1\}^\ell$ be code w/ $\ell = O(\log |A|)$ and relative distance $\rho \in [0,1]$ ($\text{Hamming}(C(a_1), C(a_2)) \geq \rho \ell \ \forall a_1 \neq a_2$)

split each vertex u into ℓ vertices $V_u = \{v_1, \dots, v_\ell\}$

replace edge $e = \{u, v\}$ w/ formula $f_e: \{0,1\}^{V_u} \times \{0,1\}^{V_v}$ s.t.

$$f_e(x_u, x_v) = \begin{cases} 1 & \text{if } x_u = C(a_1), x_v = C(a_2), (a_1, a_2) \in C_e \\ 0 & \text{otherwise} \end{cases}$$

step 2: replace each constraint w/ graph CSP

Lemma: for $e \in E$, one can construct graph-CSP $G_e = (V_e, E_e, A_0)$ s.t.:

(a) $V_u, V_v \subseteq V_e$ (b) $|E_e|, |V_e|, |A_0| = O(1)$ and same $\forall e$

(c) completeness: if $f_e(x_u, x_v) = 1$, then one can extend (x_u, x_v) to $\sigma: V_e \rightarrow A_0$ that satisfies all of G_e

(d) soundness: if $f_e(x_u, x_v) = 0$, then $\forall$ extensions σ of (x_u, x_v) ,

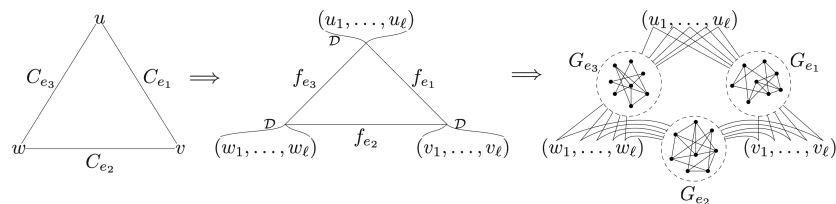
$$\text{UNSAT}(\sigma|G_e) \geq \Omega\left(\min\left\{\frac{\text{Hamming}((x_u, x_v), (y_u, y_v))}{\ell} : f(y_u, y_v) = 1\right\}\right)$$

claim for $e \in E$, if π fails e ,
then $\text{UNSAT}(\bar{\pi}|G_e) \geq \Omega(\rho)$

fix $e = \{u, v\}$.

3. Alphabet reduction

goal: decrease alphabet size to constant



step 1: reduce to $A = \{0, 1\}$ w/ error-correcting codes

* $\uparrow$ replaces each edge w/ general constraint over $O(1)$ variables *

let $C: A \rightarrow \{0, 1\}^l$ be code w/ $l = O(\log |A|)$ and
relative distance $\rho \in [0, 1]$ ($\text{Hamming}(C(a_1), C(a_2)) \geq \rho l \ \forall a_1 \neq a_2$)

split each vertex u into l vertices $V_u = \{v_{u,1}, \dots, v_{u,l}\}$

replace edge $e = \{u, v\}$ w/ formula $f_e: \{0, 1\}^{V_u} \times \{0, 1\}^{V_v}$ s.t.

$$f_e(x_u, x_v) = \begin{cases} 1 & \text{if } x_u = C(a_1), x_v = C(a_2), (a_1, a_2) \in C_e \\ 0 & \text{otherwise} \end{cases}$$

step 2: replace each constraint w/ graph CSP

Lemma: for $e \in E$, one can construct graph-CSP $G_e = (V_e, E_e, A_0)$ s.t.:

(a) $V_u, V_v \subseteq V_e$ (b) $|E_e|, |V_e|, |A_0| = O(1)$ and same $\forall e$

(c) completeness: if $f_e(x_u, x_v) = 1$, then one can extend (x_u, x_v) to $\sigma: V_e \rightarrow A_0$ that satisfies all of G_e

(d) soundness: if $f_e(x_u, x_v) = 0$, then $\forall$ extensions σ of (x_u, x_v) ,

$$\text{UNSAT}(\sigma|G_e) \geq \Omega\left(\min\left\{\frac{\text{Hamming}((x_u, x_v), (y_u, y_v))}{l} : f(y_u, y_v) = 1\right\}\right)$$

let $\bar{\pi}: \bar{V} \rightarrow A_0$ attain $\text{UNSAT}(G)$

let $\pi: V \rightarrow A$ where for $v \in V$,

$$\pi(v) = \text{decode}(\bar{\pi}(v_1), \dots, \bar{\pi}(v_l))$$

given graph-CSP G , it is NP-Hard

to distinguish:

- $UNSAT(G) = 0$
- $UNSAT(G) \geq \frac{1}{m}$

Goal: amplify $\nearrow$ to a constant

q -ary constraint satisfaction problems

- n variables V
- finite alphabet A
- m clauses
- a clause consists of q variables $v_1, \dots, v_k \in V$ and "satisfying" set $S \subseteq A^q$
- $\pi: V \rightarrow A$ satisfies clause if $(\pi(v_1), \dots, \pi(v_k)) \in S$

Graph CSP 2-ary CSP
Variables = vertices
clause over $u, v \in V$
 $\approx$ edge between u, v

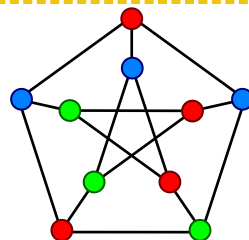
Three transformations:

- ✓ 1. "Expander-ification" make G a constant degree expander
- ✓ 2. Powering raises $UNSAT(G)$ but also increases $|A|$
- ✓ 3. Alphabet reduction

V = vertices

$A = \{\text{red, blue, green}\}$

clauses = edges

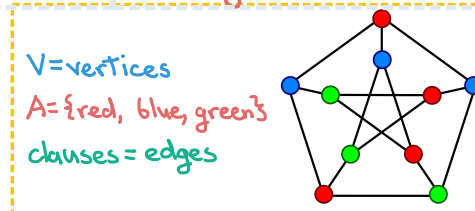


given graph-CSP G , it is NP-Hard
 to distinguish: • $UNSAT(G) = 0$ • $UNSAT(G) \geq \frac{1}{m}$
 Goal: amplify $\rightarrow$ to a constant

q -ary constraint satisfaction problems
 • n variables V • finite alphabet A • m clauses
 • a clause consists of q variables $v_1, \dots, v_k \in V$
 and "satisfying" set $S \subseteq A^q$
 $\pi: V \rightarrow A$ satisfies clause if $(\pi(v_1), \dots, \pi(v_k)) \in S$

Graph CSP 2-ary CSP
 Variables = vertices
 clause over $u, v \in V$
 $\approx$ edge between u, v

- Three transformations:
- ✓ 1. "Expander-ification" make G a constant degree expander
 - ✓ 2. Powering raises $UNSAT(G)$ but also increases $|A|$
 - ✓ 3. Alphabet reduction



Step	input	expander-ification	powering	alphabet reduction
Lemma		23.5	23.6	23.7
Degree	arbitrary $\rightarrow$	d_0	$\rightarrow d_0^t$	$\rightarrow$ arbitrary
γ	arbitrary $\rightarrow$	γ_0	$\rightarrow 1 - (1 - \gamma_0)^t$	$\rightarrow$ arbitrary
$UNSAT(G)$	$\alpha \rightarrow$	$\beta_1 \alpha$	$\rightarrow \sqrt{t} \beta_1 \beta_2 \alpha,$	$\rightarrow \sqrt{t} \beta_1 \beta_2 \beta_3 \alpha$
Alphabet	$A_0 \rightarrow$	A_0	$\rightarrow A_0^{d_0^t}$	$\rightarrow A_0$