On bounded depth proofs for Tseitin formulas on the grid; revisited

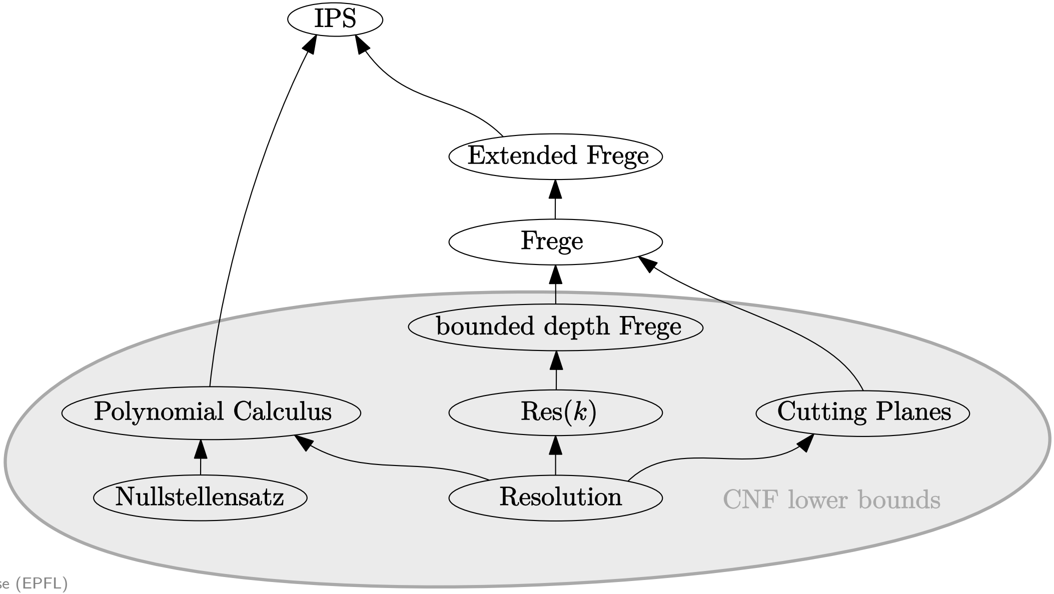
Kilian Risse

EPFL

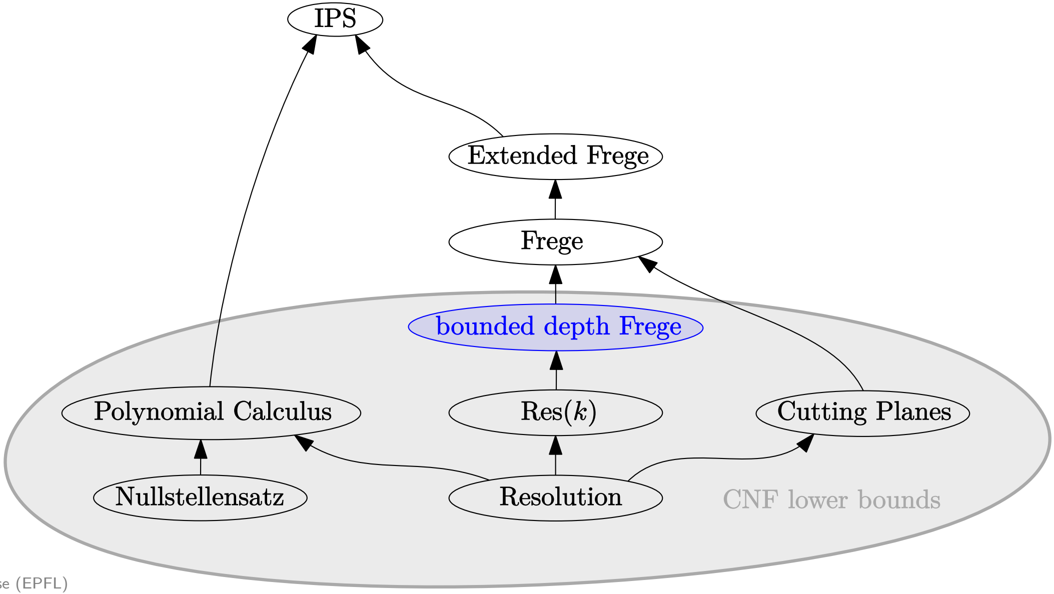
April 2023
Simons Institute

Joint work with Johan Håstad

Some Proof Systems



Some Proof Systems

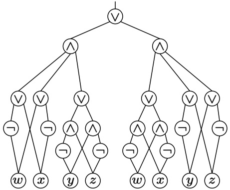


Frege Proof System

- Frege Refutation π of a CNF F_n on n variables is a sequence of lines $\ell_1, \ldots, \ell_N$ where

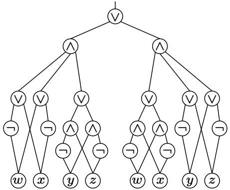
Frege Proof System

- Frege Refutation π of a CNF F_n on n variables is a sequence of lines $\ell_1, \ldots, \ell_N$ where
  - each line ℓ_i is a Boolean formula over the basis $\{\lor, \neg\}$,



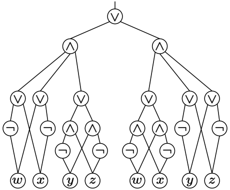
Frege Proof System

- Frege Refutation π of a CNF F_n on n variables is a sequence of lines $\ell_1, \ldots, \ell_N$ where
  - each line ℓ_i is a Boolean formula over the basis $\{\vee, \neg\}$ ($\wedge := \neg \vee \neg$),



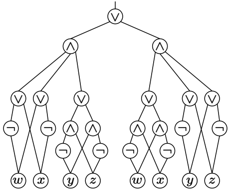
Frege Proof System

- Frege Refutation π of a CNF F_n on n variables is a sequence of lines $\ell_1, \ldots, \ell_N$ where
  - each line ℓ_i is a Boolean formula over the basis $\{\vee, \neg\}$ $(\wedge := \neg \vee \neg)$,
  - each line ℓ_i is either



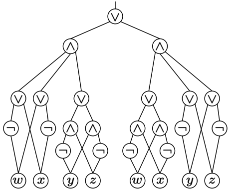
Frege Proof System

- Frege Refutation π of a CNF F_n on n variables is a sequence of lines $\ell_1, \ldots, \ell_N$ where
  - each line ℓ_i is a Boolean formula over the basis $\{\vee, \neg\}$ ($\wedge := \neg \vee \neg$),
  - each line ℓ_i is either
    - a clause $C \in F_n$, or



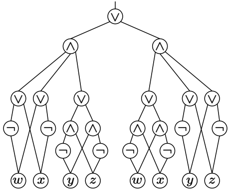
Frege Proof System

- Frege Refutation π of a CNF F_n on n variables is a sequence of lines $\ell_1, \ldots, \ell_N$ where
  - each line ℓ_i is a Boolean formula over the basis $\{\vee, \neg\}$ ($\wedge := \neg \vee \neg$),
  - each line ℓ_i is either
    - a clause $C \in F_n$, or
    - derived from previous lines by a derivation rule



Frege Proof System

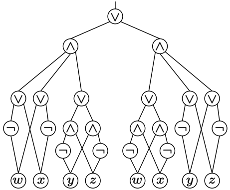
- Frege Refutation π of a CNF F_n on n variables is a sequence of lines $\ell_1, \ldots, \ell_N$ where
  - each line ℓ_i is a Boolean formula over the basis $\{\vee, \neg\}$ $(\wedge := \neg \vee \neg)$,
  - each line ℓ_i is either
    - a clause $C \in F_n$, or
    - derived from previous lines by a derivation rule



$$\frac{}{p \vee \neg p} \qquad \frac{p}{p \vee q} \qquad \frac{p \vee p}{p} \qquad \frac{p \vee (q \vee r)}{(p \vee q) \vee r} \qquad \frac{q \vee p \qquad \neg p \vee r}{q \vee r}$$

Frege Proof System

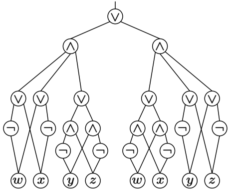
- Frege Refutation π of a CNF F_n on n variables is a sequence of lines $\ell_1, \ldots, \ell_N$ where
  - each line ℓ_i is a Boolean formula over the basis $\{\vee, \neg\}$ $(\wedge := \neg \vee \neg)$,
  - each line ℓ_i is either
    - a clause $C \in F_n$, or
    - derived from previous lines by a derivation rule



$$\frac{}{p \vee \neg p} \qquad \frac{p}{p \vee q} \qquad \frac{p \vee p}{p} \qquad \frac{p \vee (q \vee r)}{(p \vee q) \vee r} \qquad \frac{q \vee p \qquad \neg p \vee r}{q \vee r}$$

Frege Proof System

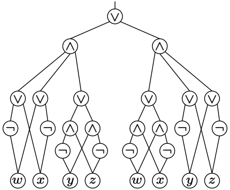
- Frege Refutation π of a CNF F_n on n variables is a sequence of lines $\ell_1, \ldots, \ell_N$ where
  - each line ℓ_i is a Boolean formula over the basis $\{\vee, \neg\}$ $(\wedge := \neg \vee \neg)$,
  - each line ℓ_i is either
    - a clause $C \in F_n$, or
    - derived from previous lines by a derivation rule
  - $\ell_N = \bot$ is constant false



$$\frac{}{p \vee \neg p} \qquad \frac{p}{p \vee q} \qquad \frac{p \vee p}{p} \qquad \frac{p \vee (q \vee r)}{(p \vee q) \vee r} \qquad \frac{q \vee p \qquad \neg p \vee r}{q \vee r}$$

Frege Proof System

- Frege Refutation π of a CNF F_n on n variables is a sequence of lines $\ell_1, \dots, \ell_N$ where
  - each line ℓ_i is a Boolean formula over the basis $\{\vee, \neg\}$ $(\wedge := \neg \vee \neg)$,
  - each line ℓ_i is either
    - a clause $C \in F_n$, or
    - derived from previous lines by a derivation rule
  - $\ell_N = \bot$ is constant false

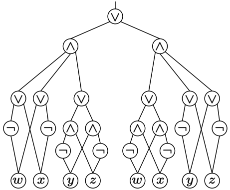


- Length of π is N, the line-size is $\max_i \mathrm{Size}(\ell_i)$, the size is $\sum_i \mathrm{Size}(\ell_i)$ and the depth is $\max_i \mathrm{Depth}(\ell_i)$

$$\frac{}{p \vee \neg p} \qquad \frac{p}{p \vee q} \qquad \frac{p \vee p}{p} \qquad \frac{p \vee (q \vee r)}{(p \vee q) \vee r} \qquad \frac{q \vee p \qquad \neg p \vee r}{q \vee r}$$

Frege Proof System

- Frege Refutation π of a CNF F_n on n variables is a sequence of lines $\ell_1, \ldots, \ell_N$ where
  - each line ℓ_i is a Boolean formula over the basis $\{\vee, \neg\}$ $(\wedge := \neg \vee \neg)$,
  - each line ℓ_i is either
    - a clause $C \in F_n$, or
    - derived from previous lines by a derivation rule
  - $\ell_N = \bot$ is constant false



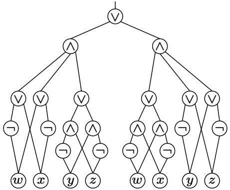
- Length of π is N, the line-size is $\max_i \mathrm{Size}(\ell_i)$, the size is $\sum_i \mathrm{Size}(\ell_i)$ and the depth is $\max_i \mathrm{Depth}(\ell_i)$

Ultimate Goal

Prove a super-polynomial length lower bound in n on Frege refutations for a CNF F_n.

Frege Proof System

- Frege Refutation π of a CNF F_n on n variables is a sequence of lines $\ell_1, \ldots, \ell_N$ where
  - each line ℓ_i is a Boolean formula over the basis $\{\vee, \neg\}$ ($\wedge := \neg \vee \neg$),
  - each line ℓ_i is either
    - a clause $C \in F_n$, or
    - derived from previous lines by a derivation rule
  - $\ell_N = \bot$ is constant false



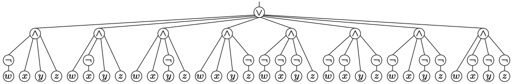
- Length of π is N, the line-size is $\max_i \mathrm{Size}(\ell_i)$, the size is $\sum_i \mathrm{Size}(\ell_i)$ and the depth is $\max_i \mathrm{Depth}(\ell_i)$
- d-bounded depth Frege consists of all Frege refutations of depth $\leq d$

Ultimate Goal

Prove a super-polynomial length lower bound in n on Frege refutations for a CNF F_n.

Frege Proof System

- Frege Refutation π of a CNF F_n on n variables is a sequence of lines $\ell_1, \ldots, \ell_N$ where
  - each line ℓ_i is a Boolean formula over the basis $\{\vee, \neg\}$ $(\wedge := \neg \vee \neg)$,
  - each line ℓ_i is either
    - a clause $C \in F_n$, or
    - derived from previous lines by a derivation rule
  - $\ell_N = \bot$ is constant false



- Length of π is N, the line-size is $\max_i \mathrm{Size}(\ell_i)$, the size is $\sum_i \mathrm{Size}(\ell_i)$ and the depth is $\max_i \mathrm{Depth}(\ell_i)$

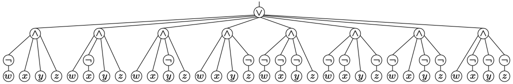
- d-bounded depth Frege consists of all Frege refutations of depth $\leq d$

Ultimate Goal

Prove a super-polynomial length lower bound in n on Frege refutations for a CNF F_n.

Frege Proof System

- Frege Refutation π of a CNF F_n on n variables is a sequence of lines $\ell_1, \ldots, \ell_N$ where
  - each line ℓ_i is a Boolean formula over the basis $\{\vee, \neg\}$ $(\wedge := \neg \vee \neg)$,
  - each line ℓ_i is either
    - a clause $C \in F_n$, or
    - derived from previous lines by a derivation rule
  - $\ell_N = \bot$ is constant false



- Length of π is N, the line-size is $\max_i \mathrm{Size}(\ell_i)$, the size is $\sum_i \mathrm{Size}(\ell_i)$ and the depth is $\max_i \mathrm{Depth}(\ell_i)$

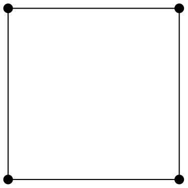
- d-bounded depth Frege consists of all Frege refutations of depth $\leq d$

Ultimate Goal

Prove a super-polynomial length lower bound in n on Frege refutations for a CNF F_n.

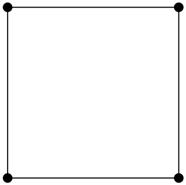
Tseitin Formula

- The CNF Tseitin(G) is defined over a connected graph G



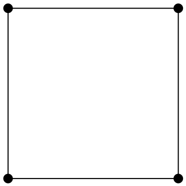
Tseitin Formula

- The CNF Tseitin(G) is defined over a connected graph G
- Boolean variable x_e associated with each edge $e \in E(G)$



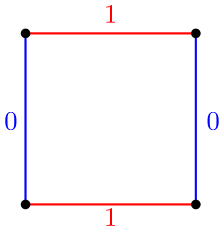
Tseitin Formula

- The CNF Tseitin(G) is defined over a connected graph G
- Boolean variable x_e associated with each edge $e \in E(G)$
- Each vertex claims that an odd number of incident edges are set to 1



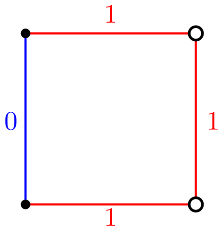
Tseitin Formula

- The CNF Tseitin(G) is defined over a connected graph G
- Boolean variable x_e associated with each edge $e \in E(G)$
- Each vertex claims that an odd number of incident edges are set to 1



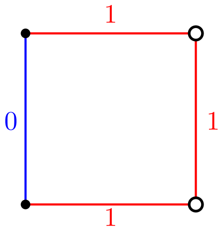
Tseitin Formula

- The CNF Tseitin(G) is defined over a connected graph G
- Boolean variable x_e associated with each edge $e \in E(G)$
- Each vertex claims that an odd number of incident edges are set to 1



Tseitin Formula

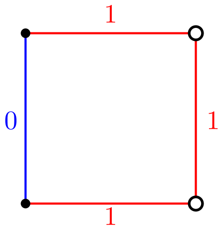
- The CNF Tseitin(G) is defined over a connected graph G
- Boolean variable x_e associated with each edge $e \in E(G)$
- Each vertex claims that an odd number of incident edges are set to 1



- Tseitin(G) is satisfiable iff $|V(G)|$ even

Tseitin Formula

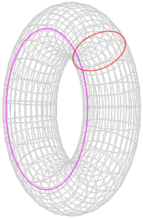
- The CNF Tseitin(G) is defined over a connected graph G
- Boolean variable x_e associated with each edge $e \in E(G)$
- Each vertex claims that an odd number of incident edges are set to 1



- Tseitin(G) is satisfiable iff $|V(G)|$ even
- We consider the two dimensional $n \times n$ torus T_n^2

Tseitin Formula

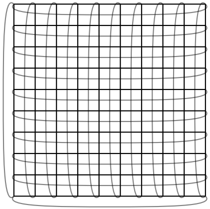
- The CNF Tseitin(G) is defined over a connected graph G
- Boolean variable x_e associated with each edge $e \in E(G)$
- Each vertex claims that an odd number of incident edges are set to 1



- Tseitin(G) is satisfiable iff $|V(G)|$ even
- We consider the two dimensional $n \times n$ torus T_n^2

Tseitin Formula

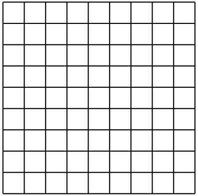
- The CNF Tseitin(G) is defined over a connected graph G
- Boolean variable x_e associated with each edge $e \in E(G)$
- Each vertex claims that an odd number of incident edges are set to 1



- Tseitin(G) is satisfiable iff $|V(G)|$ even
- We consider the two dimensional $n \times n$ torus T_n^2

Tseitin Formula

- The CNF Tseitin(G) is defined over a connected graph G
- Boolean variable x_e associated with each edge $e \in E(G)$
- Each vertex claims that an odd number of incident edges are set to 1



- Tseitin(G) is satisfiable iff $|V(G)|$ even
- We consider the two dimensional $n \times n$ torus T_n^2

Pigeonhole Principle

- The CNF PHP(n) claims that $n+1$ pigeons fit into n holes

Pigeonhole Principle

- The CNF PHP(n) claims that $n + 1$ pigeons fit into n holes
- Boolean variable x_{ph} associated with each pigeon p and hole h

Pigeonhole Principle

- The CNF PHP(n) claims that $n+1$ pigeons fit into n holes
- Boolean variable x_{ph} associated with each pigeon p and hole h
- Pigeon p claims that it flies into at least one hole

$$\bigvee_{h \in [n]} x_{ph}$$

Pigeonhole Principle

- The CNF PHP(n) claims that $n+1$ pigeons fit into n holes
- Boolean variable x_{ph} associated with each pigeon p and hole h
- Pigeon p claims that it flies into at least one hole

$$\bigvee_{h \in [n]} x_{ph}$$

- Each hole h occupied by at most 1 pigeon

$$\bar{x}_{ph} \vee \bar{x}_{p'h} \quad \forall p \neq p'$$

History

Super-poly d-bounded depth Frege lower bound for...

Pigeonhole Principle

Tseitin Formula

- Aitaj [Ait94] $d = \omega(1)$

History

Super-poly d-bounded depth Frege lower bound for...

Pigeonhole Principle

- Aitaj [Ait94] $d = \omega(1)$
- Bellantoni et al [BPU92] $d = \Omega(\log^* n)$

Tseitin Formula

History

Super-poly d-bounded depth Frege lower bound for...

Pigeonhole Principle

Tseitin Formula

- Aitaj [Ait94] $d = \omega(1)$
- Bellantoni et al [BPU92] $d = \Omega(\log^* n)$
- Kraijeck et al, Pitassi et al [KPW95, PBI93] $d = \Omega(\log \log n)$

History

Super-poly d-bounded depth Frege lower bound for...

Pigeonhole Principle

Tseitin Formula

- Aitaj [Ait94] $d = \omega(1)$
- Bellantoni et al [BPU92] $d = \Omega(\log^* n)$
- Kraijeck et al, Pitassi et al [KPW95, PBI93] $d = \Omega(\log \log n)$
- Håstad [Hås23] $d = \Omega(\log n / \log \log n)$

History

Super-poly d-bounded depth Frege lower bound for...

Pigeonhole Principle

- Aitaj [Ait94] $d = \omega(1)$
- Bellantoni et al [BPU92] $d = \Omega(\log^* n)$
- Kraijeck et al, Pitassi et al [KPW95, PBI93] $d = \Omega(\log \log n)$
- Håstad [Hås23] $d = \Omega(\log n / \log \log n)$

Tseitin Formula

- Ben-Sasson [Ben02], Urquhart and Fu [UF96] $d = \Omega(\log \log n)$

History

Super-poly d-bounded depth Frege lower bound for...

Pigeonhole Principle

- Aitaj [Ait94] $d = \omega(1)$
- Bellantoni et al [BPU92] $d = \Omega(\log^* n)$
- Kraijeck et al, Pitassi et al [KPW95, PBI93] $d = \Omega(\log \log n)$
- Håstad [Hås23] $d = \Omega(\log n / \log \log n)$

Tseitin Formula

- Ben-Sasson [Ben02], Urquhart and Fu [UF96] $d = \Omega(\log \log n)$
- Pitassi et al [PRST16] $d = \Omega(\sqrt{\log n})$

History

Super-poly d-bounded depth Frege lower bound for...

Pigeonhole Principle

- Aitaj [Ait94] $d = \omega(1)$
- Bellantoni et al [BPU92] $d = \Omega(\log^* n)$
- Kraijeck et al, Pitassi et al [KPW95, PBI93] $d = \Omega(\log \log n)$
- Håstad [Hås23] $d = \Omega(\log n / \log \log n)$

Tseitin Formula

- Ben-Sasson [Ben02], Urquhart and Fu [UF96] $d = \Omega(\log \log n)$
- Pitassi et al [PRST16] $d = \Omega(\sqrt{\log n})$
- Håstad [Hås17] $d = \Omega(\log n / \log \log n)$

Frege and Tseitin

Long line of work [UF96, B02, PRST16, Hås17] ultimately culminated in the following

Theorem ([Hås17])

Any Frege refutation of Tseitin(T_n^2) *of depth* d *requires proofs of size* $\exp(\Omega(n^{1/58d}))$.

Frege and Tseitin

Long line of work [UF96, B02, PRST16, Hås17] ultimately culminated in the following

Theorem ([Hås17])

Any Frege refutation of Tseitin(T_n^2) *of depth* d *requires proofs of size* $\exp(\Omega(n^{1/58d}))$.

Significant improvement on dependence on d gives superpoly Frege lower bound

Frege and Tseitin

Long line of work [UF96, B02, PRST16, Hås17] ultimately culminated in the following

Theorem ([Hås17])

Any Frege refutation of Tseitin(T_n^2) *of depth* d *requires proofs of size* $\exp(\Omega(n^{1/58d}))$.

Significant improvement on dependence on d gives superpoly Frege lower bound

. . . all done!

Frege and Tseitin, Continued

... Pitassi, Ramakrishnan and Tan: what if we also restrict the size of each line?

Frege and Tseitin, Continued

…Pitassi, Ramakrishnan and Tan: what if we also restrict the size of each line?

Theorem ([PRT21])

Any Frege refutation of Tseitin(T_n^2) *of depth* d *and line-size* M *is of length* $\exp(n/2^{O(d\sqrt{\log M})})$.

Frege and Tseitin, Continued

…Pitassi, Ramakrishnan and Tan: what if we also restrict the size of each line?

Theorem ([PRT21])

Any Frege refutation of Tseitin(T_n^2) *of depth* d *and line-size* M *is of length* $\exp(n/2^{O(d\sqrt{\log M})})$.

For $M = \text{poly}(n)$ this lower bound is $\exp(n^{1-o(1)})$ up to $d = o(\sqrt{\log n})$, whereas Håstad's lower bound is of the form $\exp(n^{o(1)})$.

Frege and Tseitin, Continued

...Pitassi, Ramakrishnan and Tan: what if we also restrict the size of each line?

Theorem ([PRT21])

Any Frege refutation of Tseitin(T_n^2) *of depth* d *and line-size* M *is of length* $\exp(n/2^{O(d\sqrt{\log M})})$.

For $M = \text{poly}(n)$ this lower bound is $\exp(n^{1-o(1)})$ up to $d = o(\sqrt{\log n})$, whereas Håstad's lower bound is of the form $\exp(n^{o(1)})$.

Conjecture ([PRT21])

Any Frege refutation of Tseitin(T_n^2) *of depth* d *and line-size* M *is of length* $\exp(n/\log^{d-1} M)$.

Our Results

Our Results

Main Theorem

Frege refutations of $\mathsf{Tseitin}(T_n^2)$ *of depth* d *and line-size* M *are of length* $\exp\big(n/\log^{O(d)} M\big)$.

Our Results

Main Theorem

Frege refutations of Tseitin(T_n^2) *of depth* d *and line-size* M *are of length* $\exp(n/\log^{O(d)} M)$.

For $M \leq \cancel{\text{poly}(n)}\ n^{\text{polylog}(n)}$ and $d = o(\cancel{\sqrt{\log n}}\ \frac{\log n}{\log \log n})$ this gives $\exp(n^{1-o(1)})$ lower bounds.

Our Results

Main Theorem

Frege refutations of Tseitin(T_n^2) *of depth* d *and line-size* M *are of length* $\exp(n/\log^{O(d)} M)$.

For $M \leq$ ~~$\text{poly}(n)$~~ $n^{\text{polylog}(n)}$ and $d = o($~~$\sqrt{\log n}$~~ $\frac{\log n}{\log\log n})$ this gives $\exp(n^{1-o(1)})$ lower bounds.

Theorem

Any Frege refutation of Tseitin(T_n^2) *of depth* d *requires proofs of size* $\exp(\tilde{\Omega}(n^{1/(d-1)}))$.

improves over the previous $\exp(\Omega(n^{1/58d}))$ lower bound

Proof Ideas: Size Lower Bound

Proof Outline: Bounded Depth Circuit Lower Bounds

Given a small circuit C of depth d computing parity on n bits

Proof Outline: Bounded Depth Circuit Lower Bounds

Given a small circuit C of depth d computing parity on n bits

- Hit C with a random restriction ρ, keeping each variable independently with prob p

Proof Outline: Bounded Depth Circuit Lower Bounds

Given a small circuit C of depth d computing parity on n bits

- Hit C with a random restriction ρ, keeping each variable independently with prob p
- Argue that the circuit depth shrinks by 1

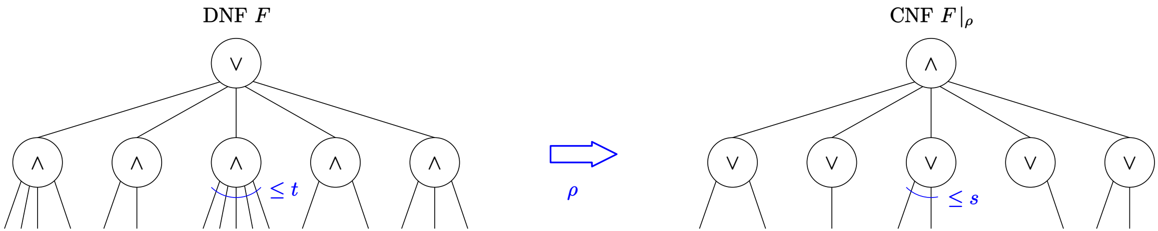
Proof Outline: Bounded Depth Circuit Lower Bounds

Given a small circuit C of depth d computing parity on n bits

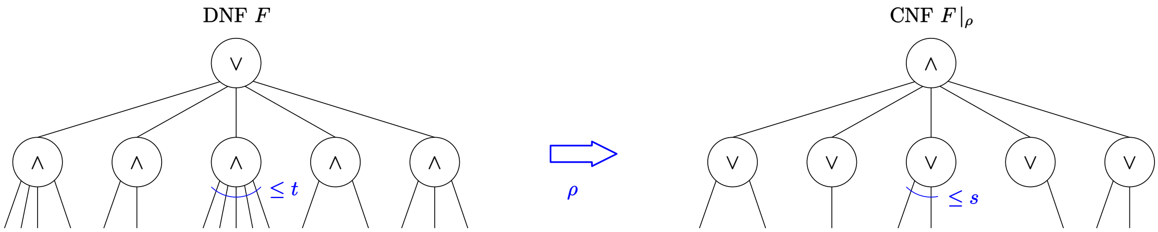
- Hit C with a random restriction ρ, keeping each variable independently with prob p
- Argue that the circuit depth shrinks by 1

Prove a Switching Lemma!

Switching Lemma

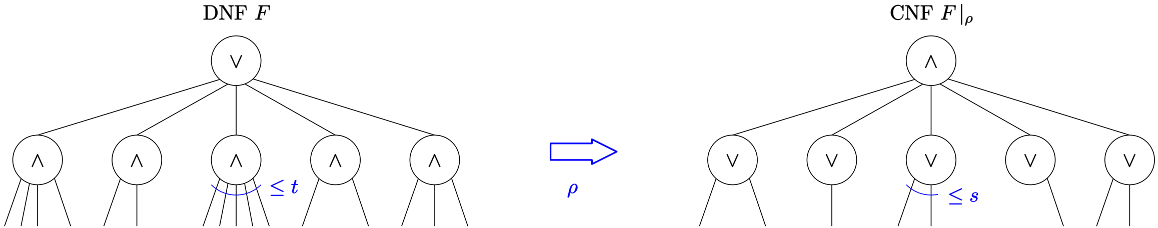


Switching Lemma



except with probability $\mathrm{Fail}(p, t, s, n)$.

Switching Lemma

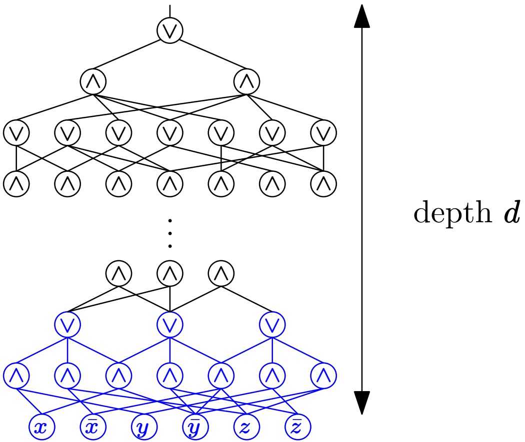


except with probability $\mathrm{Fail}(p, t, s, n)$.

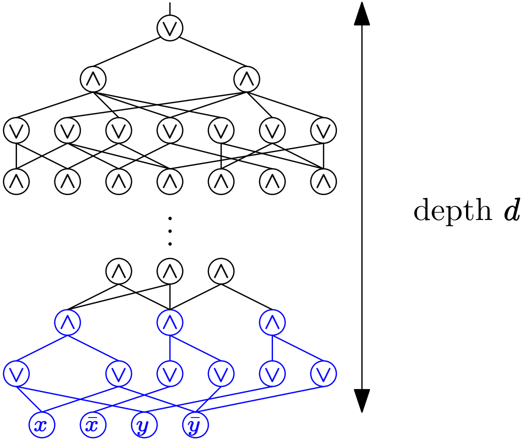
Classic result [Hås86]:

$$\mathrm{Fail}(p, t, s, n) \leq (5pt)^s$$

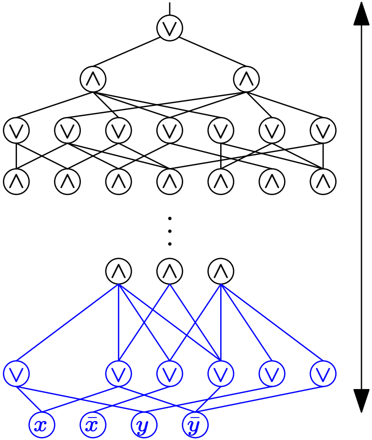
Applying the Switching Lemma



Applying the Switching Lemma



Applying the Switching Lemma



depth $d-1$

How to apply this Machinery to a Frege Proof?

Proof Outline: Bounded Depth Frege Lower Bounds

- Hit the Frege refutation $\pi = (\ell_1, \ldots, \ell_N)$ with a restriction ρ

Proof Outline: Bounded Depth Frege Lower Bounds

- Hit the Frege refutation $\pi = (\ell_1, \ldots, \ell_N)$ with a restriction ρ
- Depth of every line ℓ_i shrinks by 1

Proof Outline: Bounded Depth Frege Lower Bounds

- Hit the Frege refutation $\pi = (\ell_1, \ldots, \ell_N)$ with a restriction ρ
- Depth of every line ℓ_i shrinks by 1
- Reduce the Tseitin(T_n^2) formula to Tseitin(T_m^2), where $m < n$

Proof Outline: Bounded Depth Frege Lower Bounds

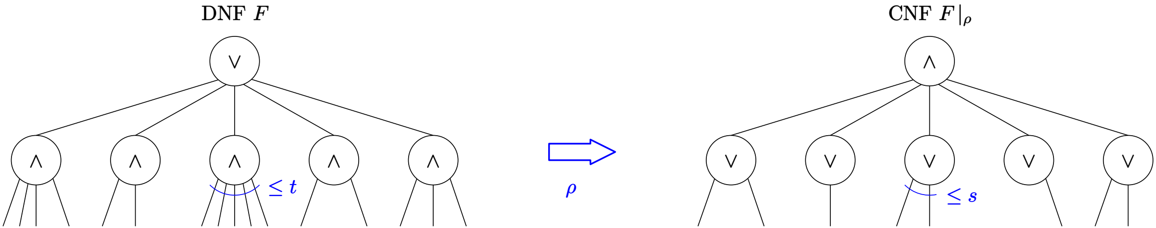
- Hit the Frege refutation $\pi = (\ell_1, \ldots, \ell_N)$ with a restriction ρ
- Depth of every line ℓ_i shrinks by 1
- Reduce the Tseitin(T_n^2) formula to Tseitin(T_m^2), where $m < n$
- Requires carefully crafted restriction ρ

Proof Outline: Bounded Depth Frege Lower Bounds

- Hit the Frege refutation $\pi = (\ell_1, \ldots, \ell_N)$ with a restriction ρ
- Depth of every line ℓ_i shrinks by 1
- Reduce the Tseitin(T_n^2) formula to Tseitin(T_m^2), where $m < n$
- Requires carefully crafted restriction ρ

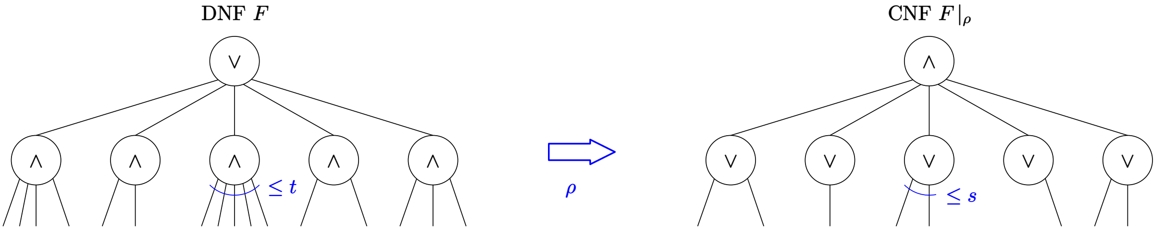
Prove a Switching Lemma!

Switching Lemma



except with probability $\mathrm{Fail}(t, s, n, m)$.

Switching Lemma

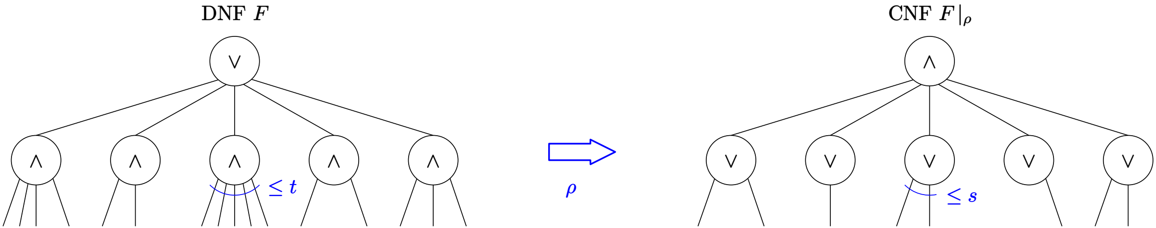


except with probability $\mathrm{Fail}(t, s, n, m)$.

Original proof [Hås17]:

$$\mathrm{Fail}(t, s, n, m) \approx \left(s^{27} t \sqrt{m/n}\right)^{\Omega(s)}$$

Switching Lemma

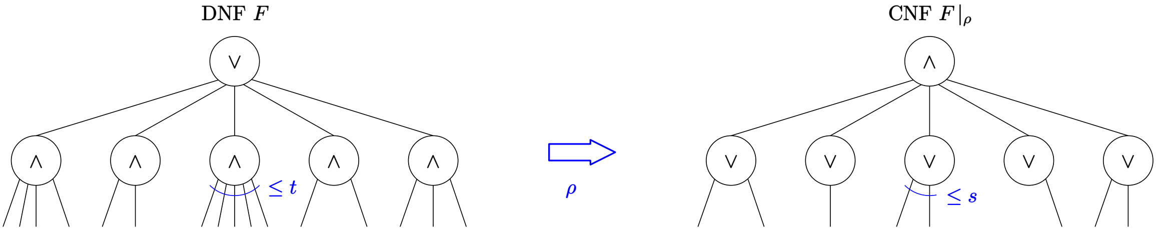


except with probability $\mathrm{Fail}(t, s, n, m)$.

Original proof [Hås17]:

$$\mathrm{Fail}(t, s, n, m) \approx \left(s^{27} t \sqrt{m/n}\right)^{\Omega(s)} \overset{!}{\ll} \frac{1}{\mathrm{Size}(\pi)}$$

Switching Lemma

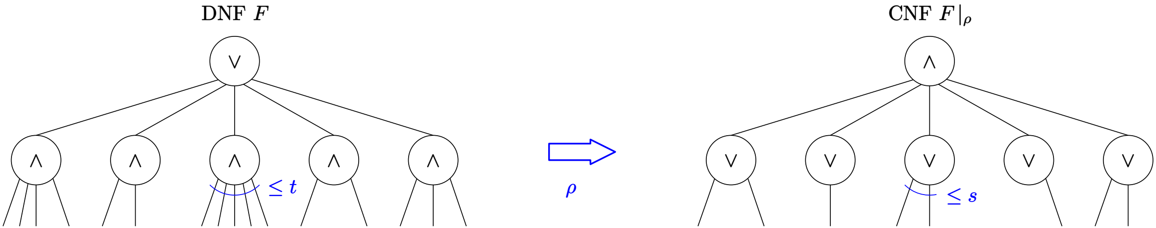


except with probability $\mathrm{Fail}(t, s, n, m)$.

Original proof [Hås17]:

$$\mathrm{Fail}(t, s, n, m) \approx \left(s^{27} t \sqrt{m/n}\right)^{\Omega(s)} \overset{!}{\ll} \frac{1}{\mathrm{Size}(\pi)}$$

Switching Lemma

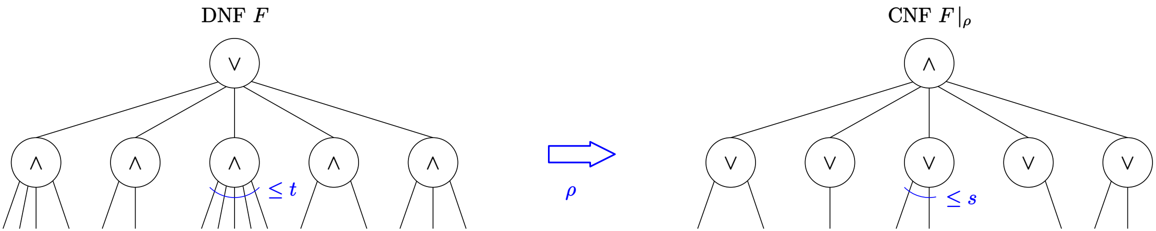


except with probability $\mathrm{Fail}(t, s, n, m)$.

Our Proof:

$$\mathrm{Fail}(t, s, n, m) \approx \left((\log n)^{27} t \sqrt{m/n}\right)^{\Omega(s)} \overset{!}{\ll} \frac{1}{\mathrm{Size}(\pi)}$$

Switching Lemma



except with probability $\mathrm{Fail}(t, s, n, m)$.

Our Proof:

$$\mathrm{Fail}(t, s, n, m) \approx \left((\log n)^{27} t \sqrt{m/n}\right)^{\Omega(s)} \overset{!}{\ll} \frac{1}{\mathrm{Size}(\pi)}$$

...skipping a few steps ...

$$\mathrm{Size}(\pi) \gtrsim \exp(n^{1/d})$$

Proof Ideas: Line-Size vs Length

From Frege Tradeoffs to Multi-Switching

Main Theorem

Frege refutations of Tseitin(T_n^2) *of depth* d *and line-size* M *are of length* $\exp(n/\log^{O(d)} M)$.

From Frege Tradeoffs to Multi-Switching

Main Theorem

Frege refutations of Tseitin(T_n^2) *of depth* d *and line-size* M *are of length* $\exp(n/\log^{O(d)} M)$.

- [PRT21] crucially proved that multi-switching can be used to obtain Frege tradeoffs

From Frege Tradeoffs to Multi-Switching

Main Theorem

Frege refutations of Tseitin(T_n^2) *of depth* d *and line-size* M *are of length* $\exp(n/\log^{O(d)} M)$.

- [PRT21] crucially proved that multi-switching can be used to obtain Frege tradeoffs
- Multi-Switching [IMP12, Hås14] originally devised to get correlation bounds for circuits

From Frege Tradeoffs to Multi-Switching

Main Theorem

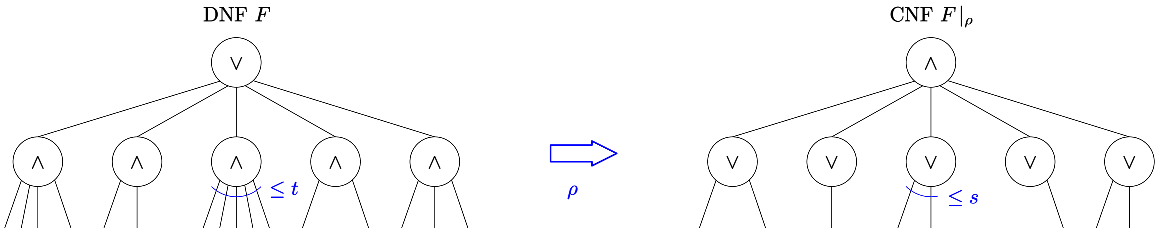
Frege refutations of $\mathrm{Tseitin}(T_n^2)$ *of depth* d *and line-size* M *are of length* $\exp(n/\log^{O(d)} M)$.

- [PRT21] crucially proved that multi-switching can be used to obtain Frege tradeoffs
- Multi-Switching [IMP12, Hås14] originally devised to get correlation bounds for circuits

Let's prove a Multi-Switching Lemma!

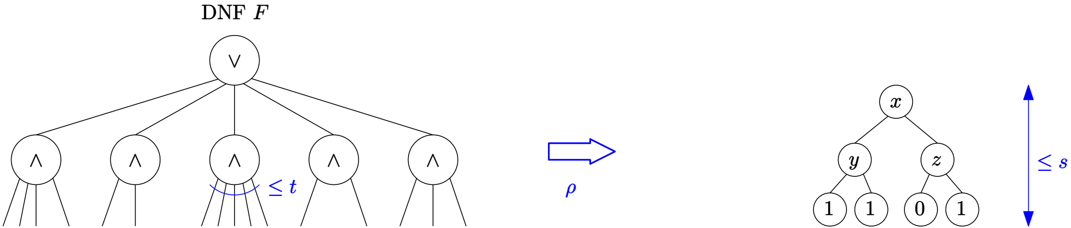
Multi-Switching Lemma

Switching lemma in fact switches into a depth $\leq s$ decision tree:



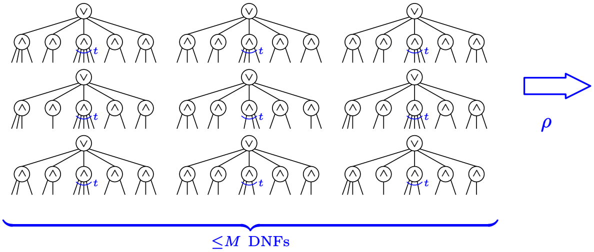
Multi-Switching Lemma

Switching lemma in fact switches into a depth $\leq s$ decision tree:



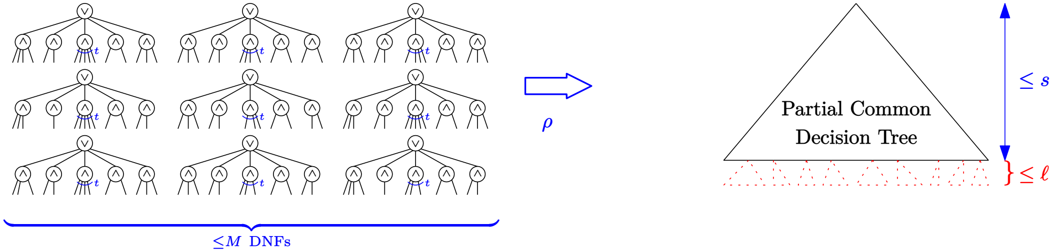
Multi-Switching Lemma

Multi-switching Lemma switches into an ℓ-partial common decision tree of depth $\leq s$:



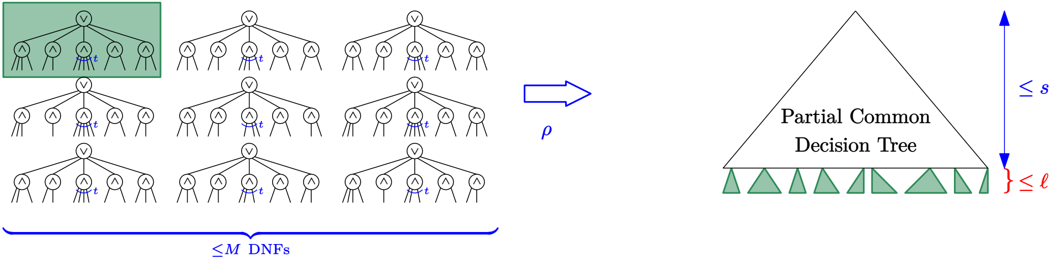
Multi-Switching Lemma

Multi-switching Lemma switches into an ℓ-partial common decision tree of depth $\leq s$:



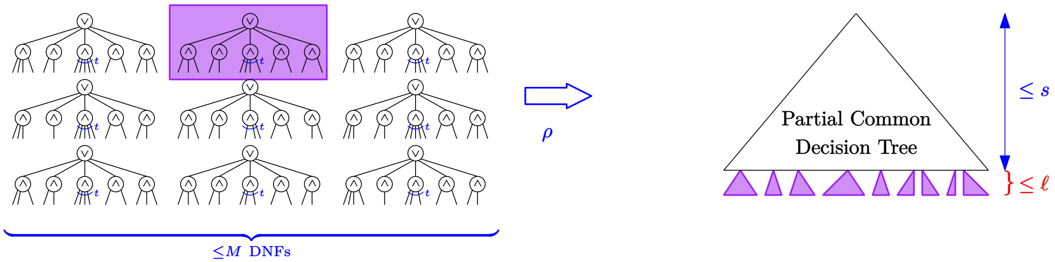
Multi-Switching Lemma

Multi-switching Lemma switches into an ℓ-partial common decision tree of depth $\leq s$:



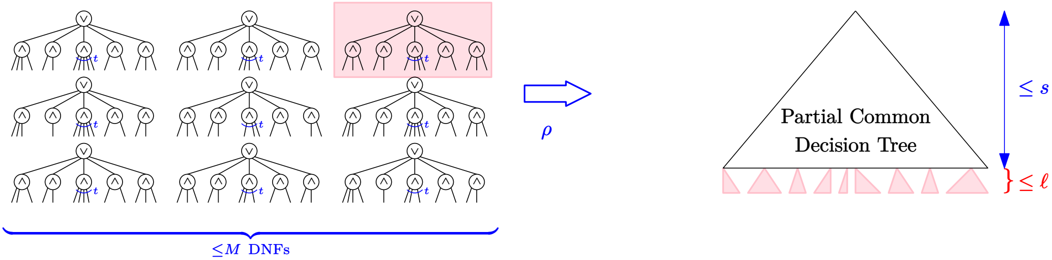
Multi-Switching Lemma

Multi-switching Lemma switches into an ℓ-partial common decision tree of depth $\leq s$:



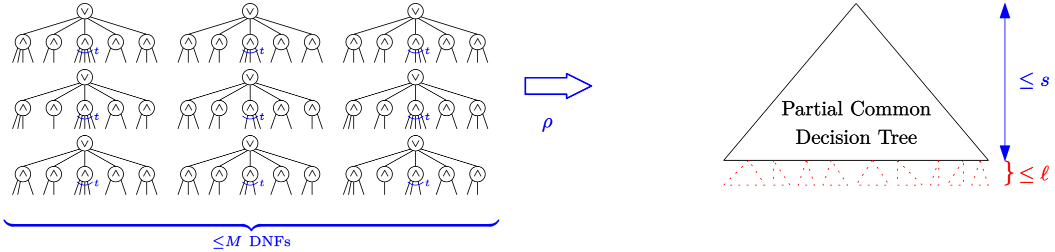
Multi-Switching Lemma

Multi-switching Lemma switches into an ℓ-partial common decision tree of depth $\leq s$:



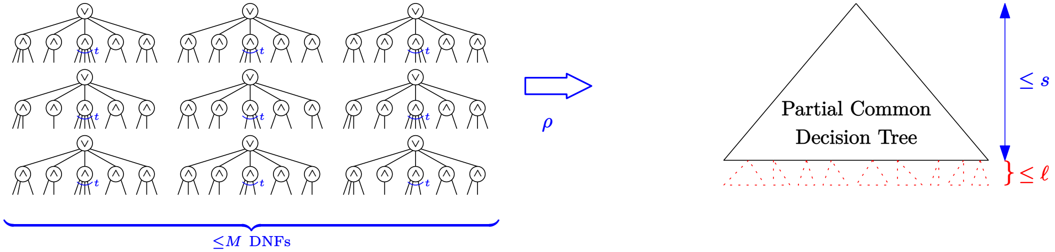
Multi-Switching Lemma

Multi-switching Lemma switches into an ℓ-partial common decision tree of depth $\leq s$:



Multi-Switching Lemma

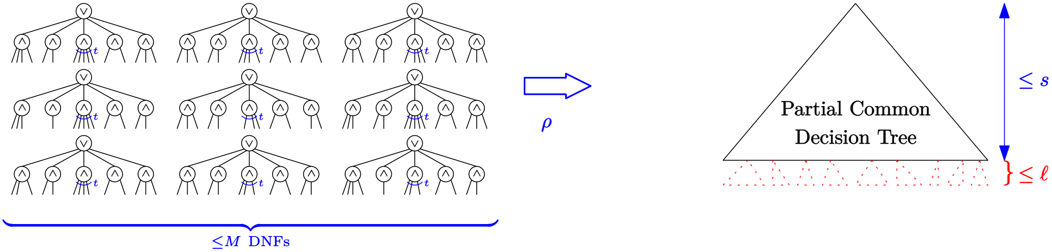
Multi-switching Lemma switches into an ℓ-partial common decision tree of depth $\leq s$:



except with probability $\mathrm{Fail}(t, s, \ell, n, m, M)$

Multi-Switching Lemma

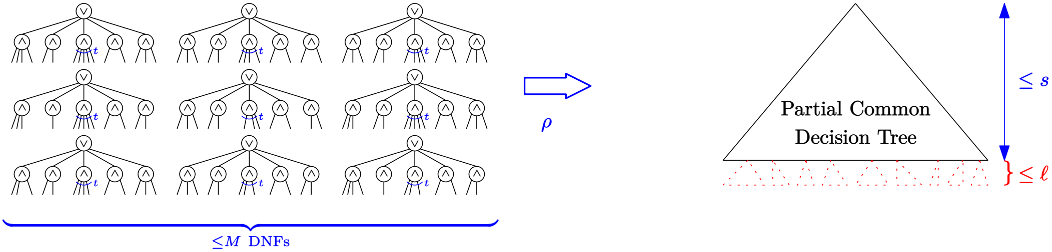
Multi-switching Lemma switches into an ℓ-partial common decision tree of depth $\leq s$:



except with probability $\mathrm{Fail}(t, s, \ell, n, m, M) \approx M^{s/\ell}(\log^{27}(n)t\sqrt{m/n})^{\Omega(s)}$

Multi-Switching Lemma

Multi-switching Lemma switches into an ℓ-partial common decision tree of depth $\leq s$:

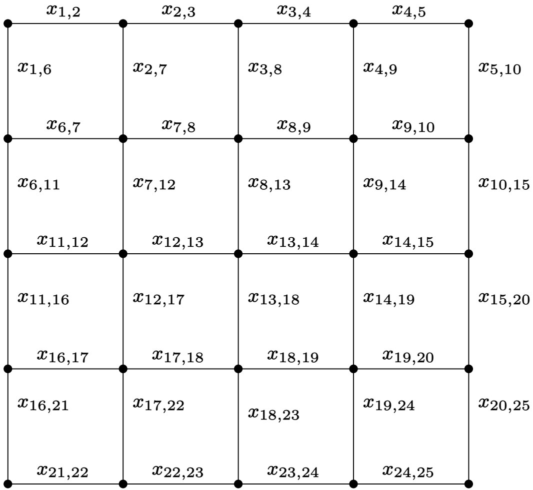


except with probability $\mathrm{Fail}(t, s, \ell, n, m, M) \approx M^{s/\ell}\left(\log^{27}(n) t \sqrt{m/n}\right)^{\Omega(s)}$

The Restriction ρ

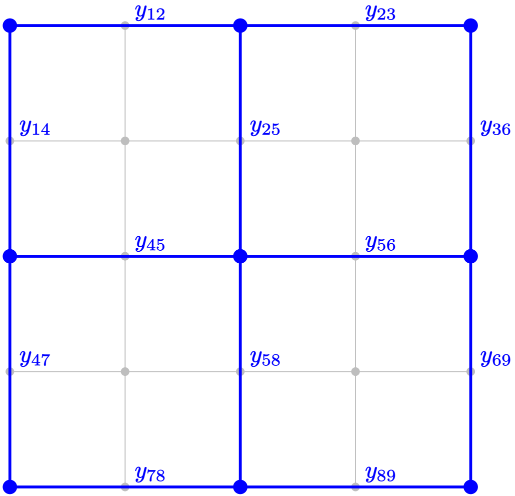
The Restriction ρ

Same restrictions as [Hås17, PRT21]



The Restriction ρ

Same restrictions as [Hås17, PRT21]

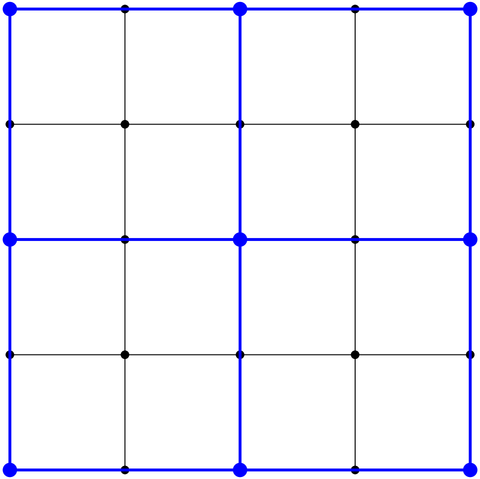


The Restriction ρ

Same restrictions as [Hås17, PRT21]

ρ is an affine restriction:

$$\rho(x) = \begin{cases} 1 & \\ 0 & \\ y & \text{a new variable} \\ \bar{y} & \text{negation of a variable.} \end{cases}$$

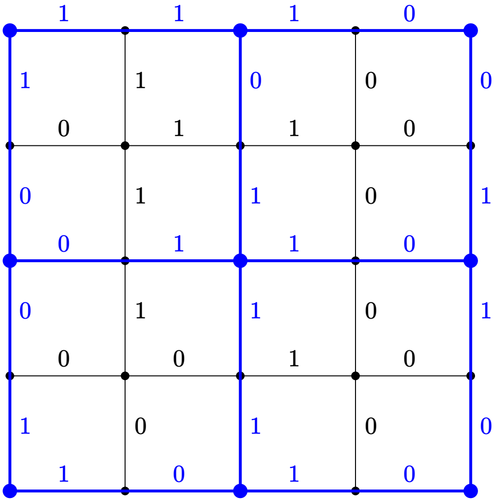


The Restriction ρ

Same restrictions as [Hås17, PRT21]

ρ is an affine restriction:

$$\rho(x) = \begin{cases} 1 & \\ 0 & \\ y & \text{a new variable} \\ \bar{y} & \text{negation of a variable.} \end{cases}$$

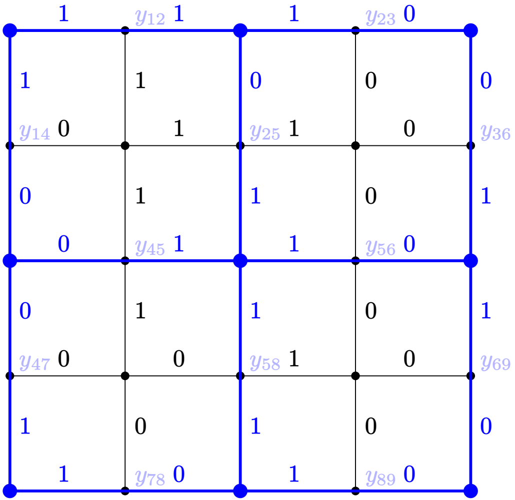


The Restriction ρ

Same restrictions as [Hås17, PRT21]

ρ is an affine restriction:

$$\rho(x) = \begin{cases} 1 & \\ 0 & \\ y & \text{a new variable} \\ \bar{y} & \text{negation of a variable.} \end{cases}$$

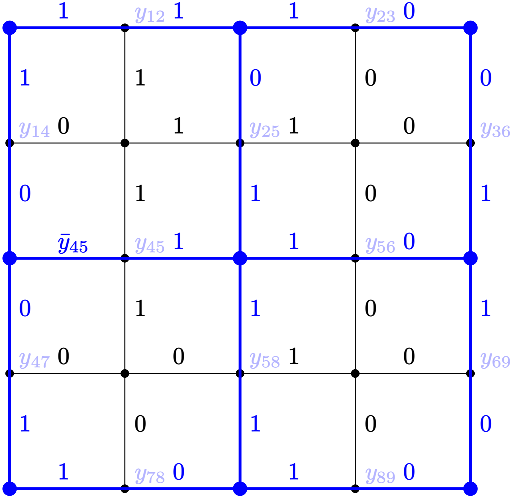


The Restriction ρ

Same restrictions as [Hås17, PRT21]

ρ is an affine restriction:

$$\rho(x) = \begin{cases} 1 & \\ 0 & \\ y & \text{a new variable} \\ \bar{y} & \text{negation of a variable.} \end{cases}$$

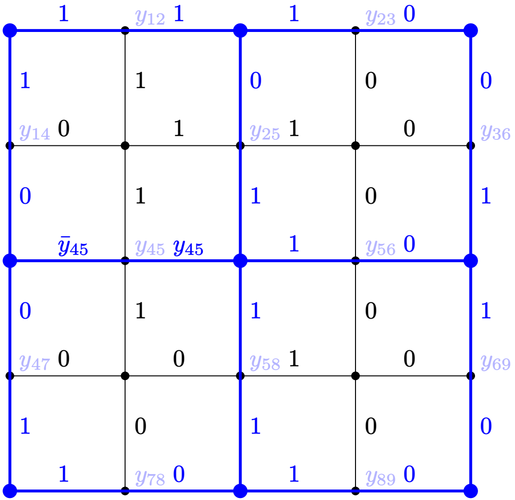


The Restriction ρ

Same restrictions as [Hås17, PRT21]

ρ is an affine restriction:

$$\rho(x) = \begin{cases} 1 & \\ 0 & \\ y & \text{a new variable} \\ \bar{y} & \text{negation of a variable.} \end{cases}$$

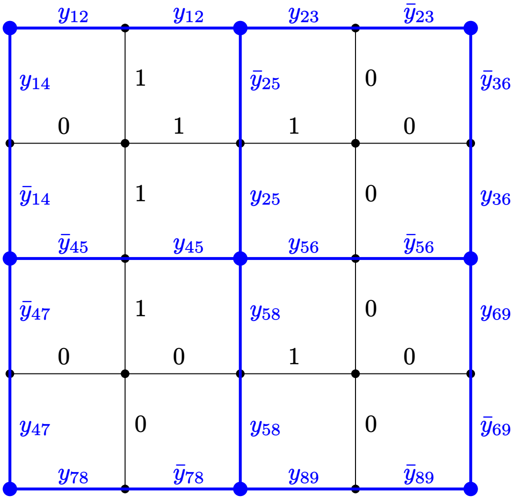


The Restriction ρ

Same restrictions as [Hås17, PRT21]

ρ is an affine restriction:

$$\rho(x) = \begin{cases} 1 & \\ 0 & \\ y & \text{a new variable} \\ \bar{y} & \text{negation of a variable.} \end{cases}$$

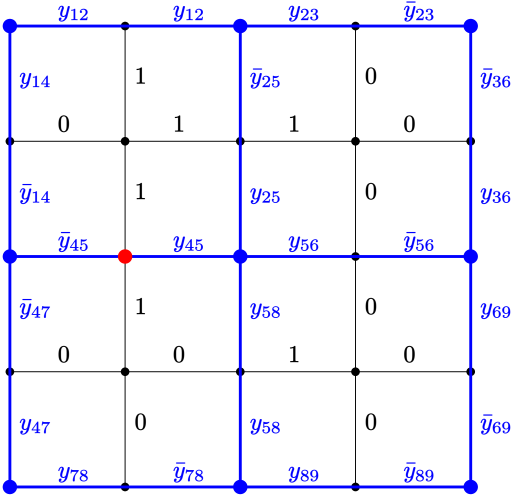


The Restriction ρ

Same restrictions as [Hås17, PRT21]

ρ is an affine restriction:

$$\rho(x) = \begin{cases} 1 & \\ 0 & \\ y & \text{a new variable} \\ \bar{y} & \text{negation of a variable.} \end{cases}$$

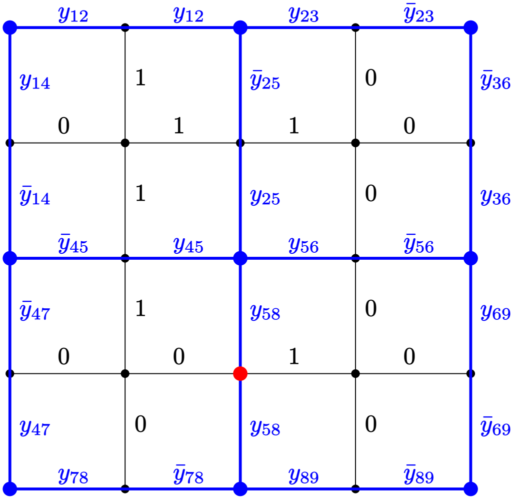


The Restriction ρ

Same restrictions as [Hås17, PRT21]

ρ is an affine restriction:

$$\rho(x) = \begin{cases} 1 & \\ 0 & \\ y & \text{a new variable} \\ \bar{y} & \text{negation of a variable.} \end{cases}$$

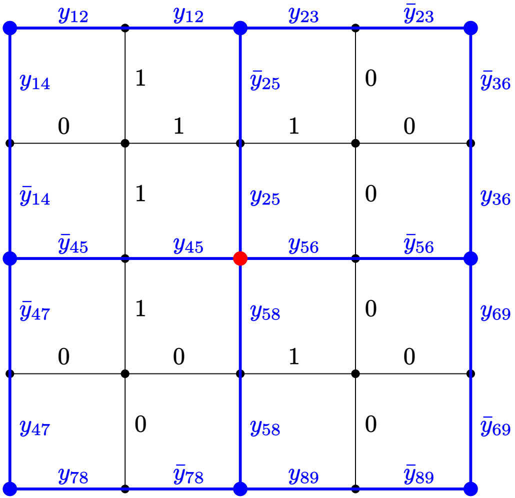


The Restriction ρ

Same restrictions as [Hås17, PRT21]

ρ is an affine restriction:

$$\rho(x) = \begin{cases} 1 & \\ 0 & \\ y & \text{a new variable} \\ \bar{y} & \text{negation of a variable.} \end{cases}$$

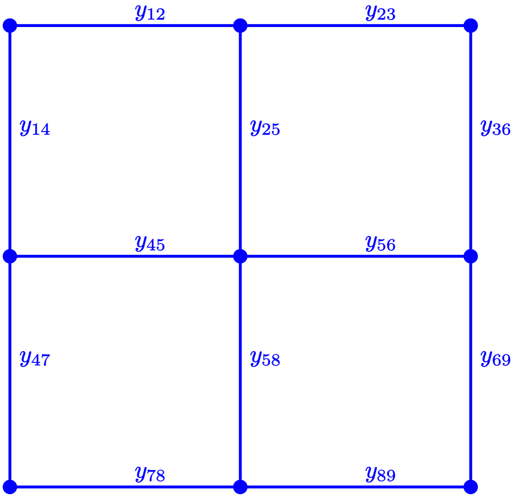


The Restriction ρ

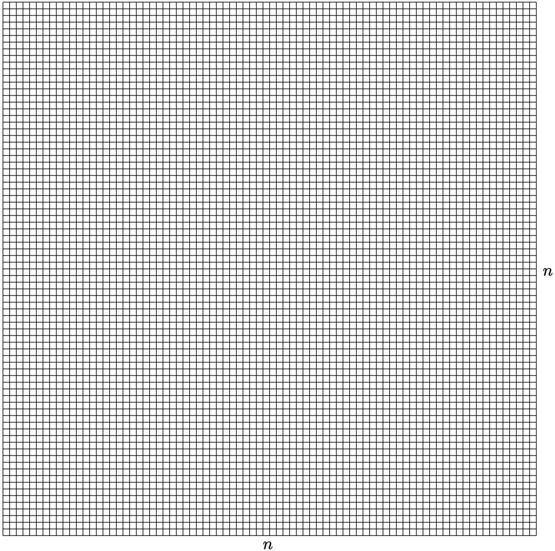
Same restrictions as [Hås17, PRT21]

ρ is an affine restriction:

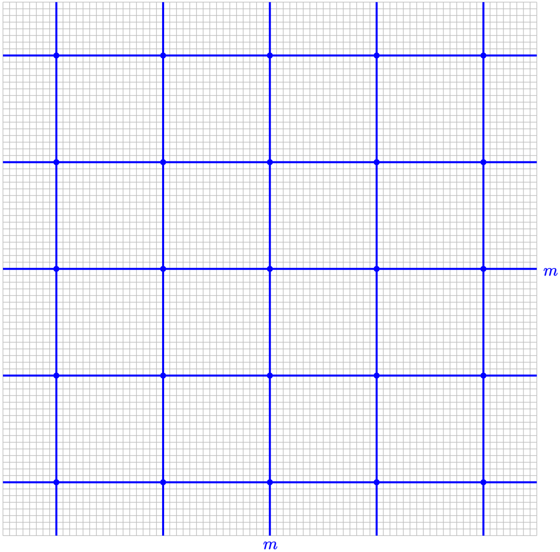
$$\rho(x) = \begin{cases} 1 & \\ 0 & \\ y & \text{a new variable} \\ \bar{y} & \text{negation of a variable.} \end{cases}$$



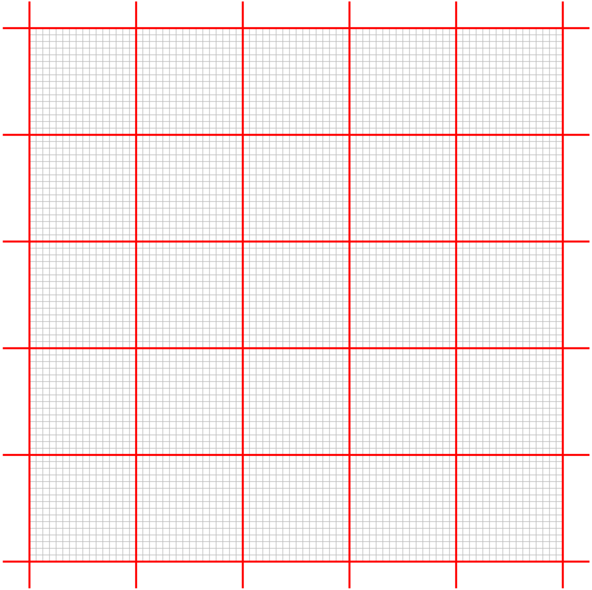
More Details about ρ



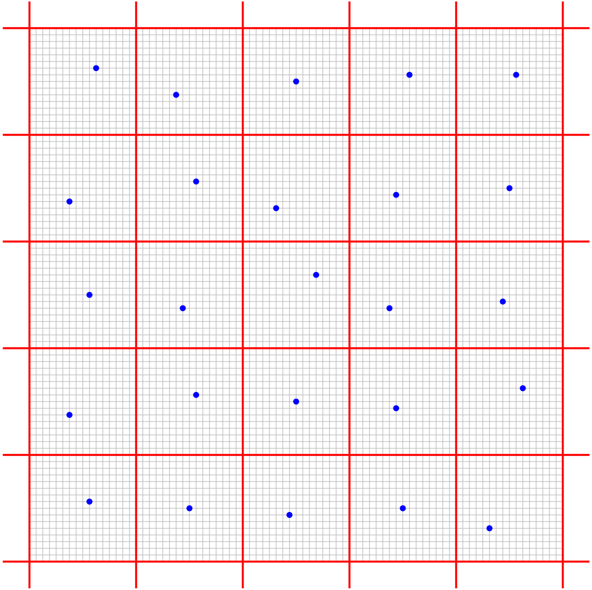
More Details about ρ



More Details about ρ

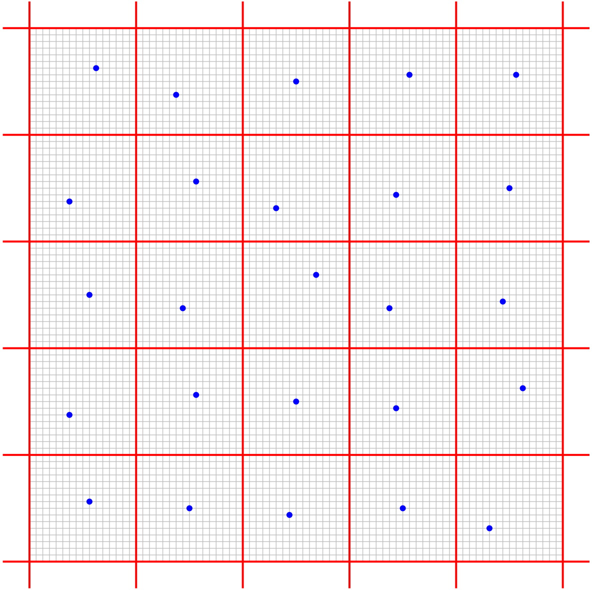


More Details about ρ

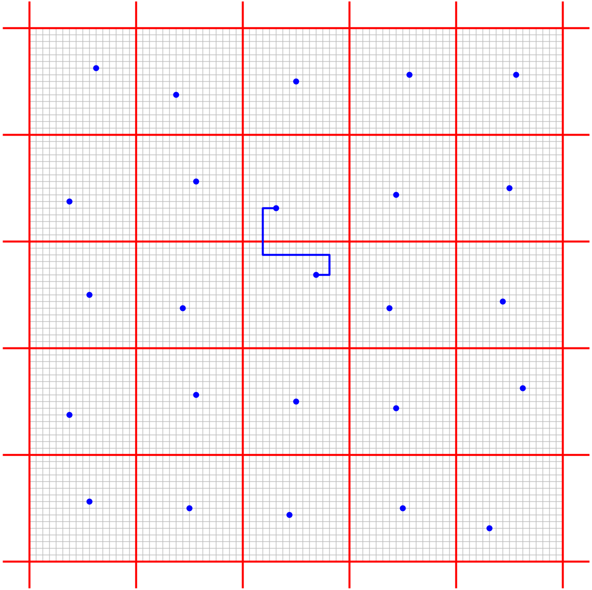


More Details about ρ

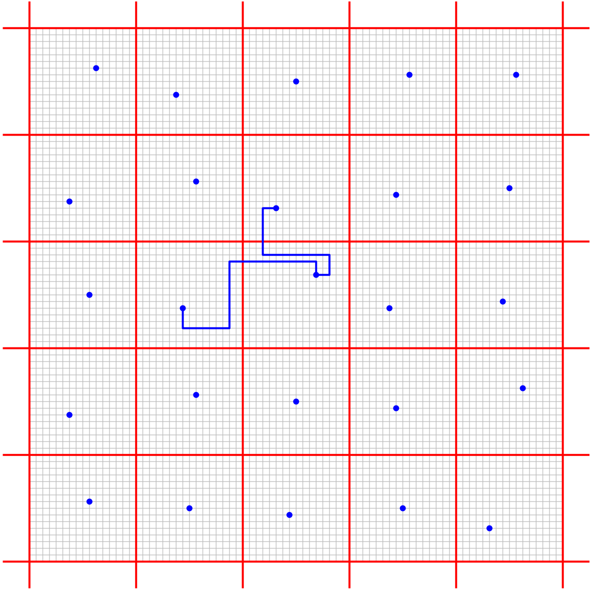
u.a.r. pick a solution to the formula
where blue nodes have even constraints



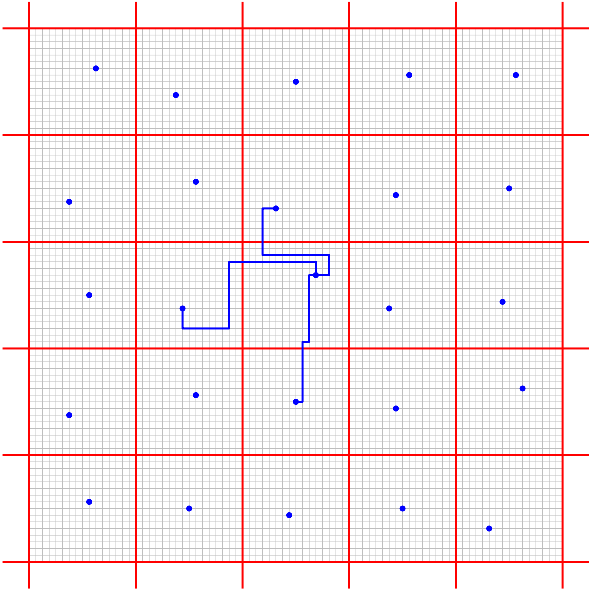
More Details about ρ



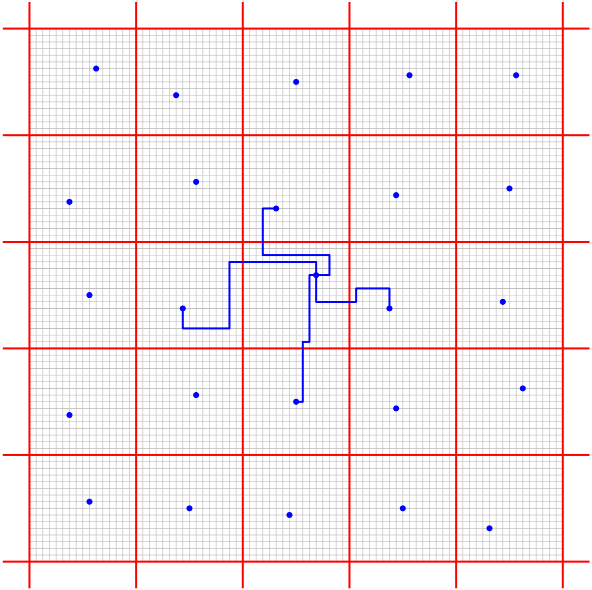
More Details about ρ



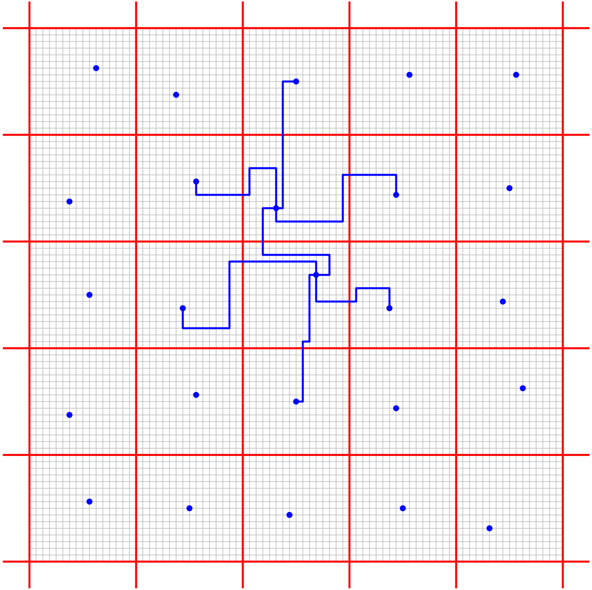
More Details about ρ



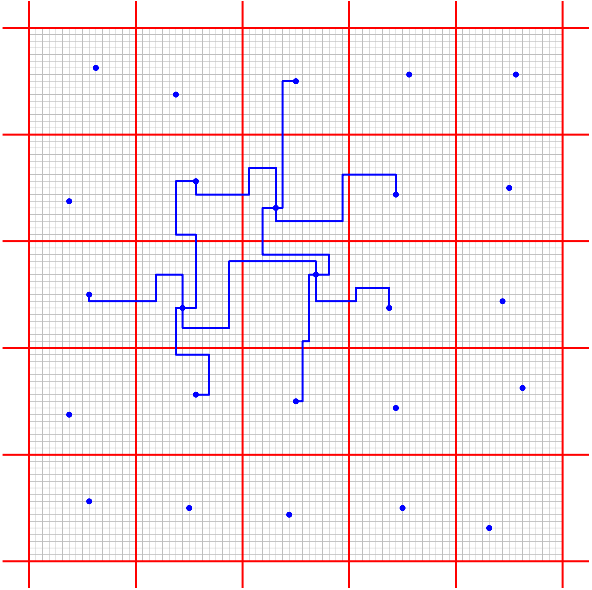
More Details about ρ



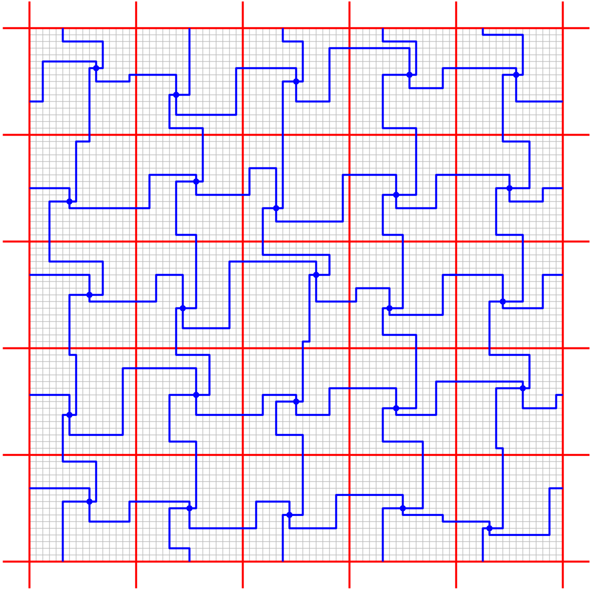
More Details about ρ



More Details about ρ

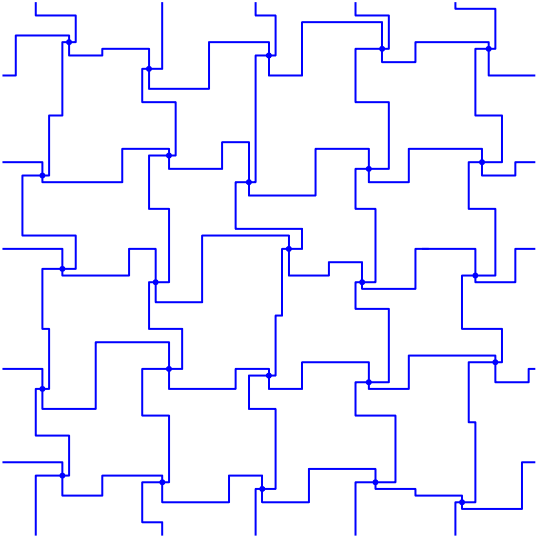


More Details about ρ



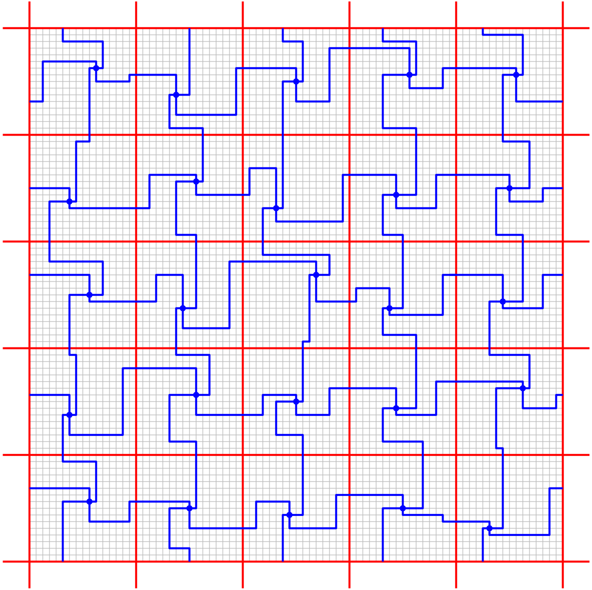
More Details about ρ

left with an $m \times m$ torus



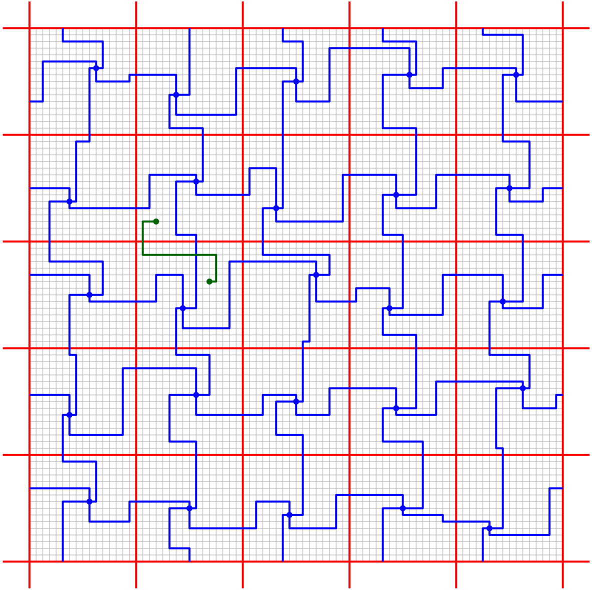
More Details about ρ

Need an intermediate restriction:



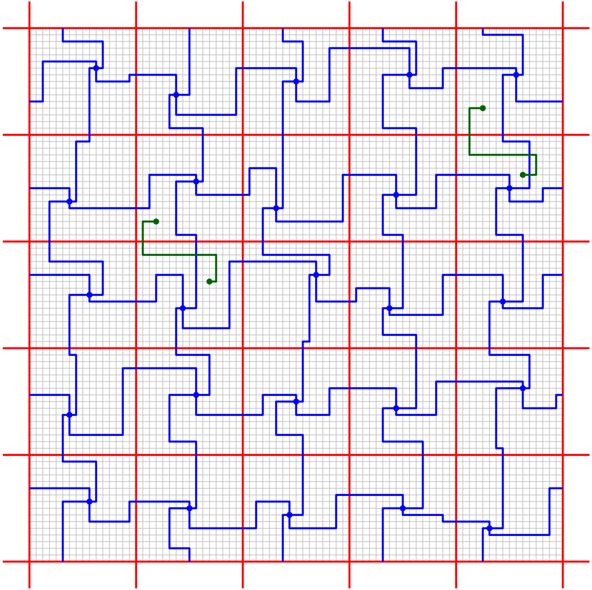
More Details about ρ

Need an intermediate restriction: pick vertices in adjacent squares & connect



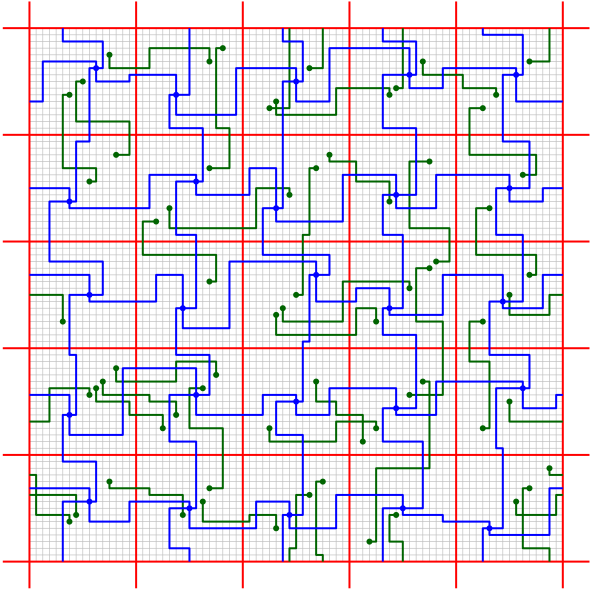
More Details about ρ

Need an intermediate restriction: pick vertices in adjacent squares & connect

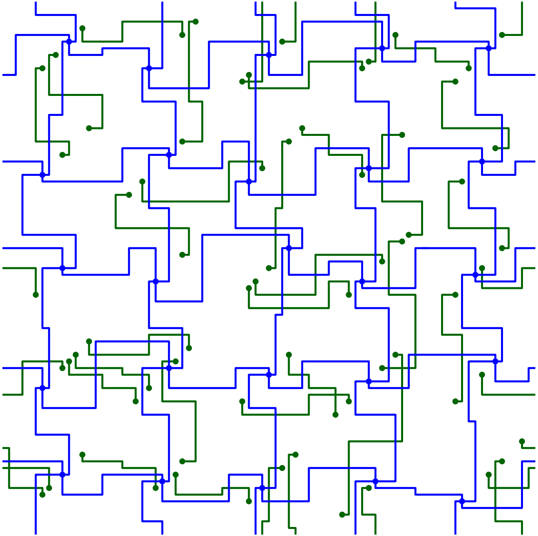


More Details about ρ

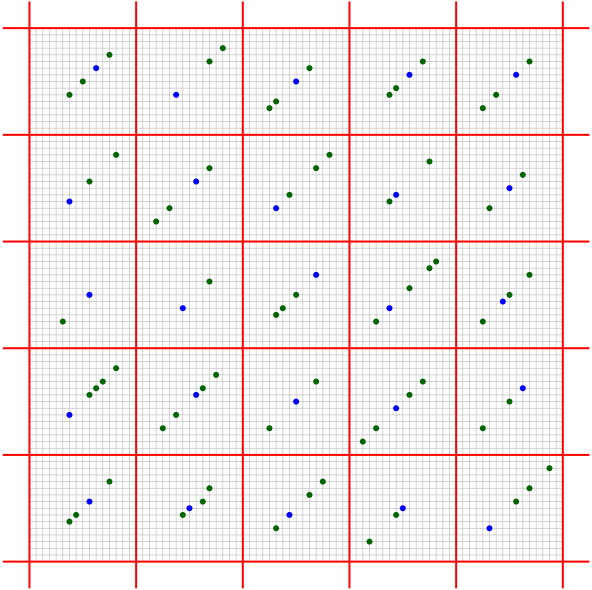
Need an intermediate restriction: pick vertices in adjacent squares & connect



More Details about ρ



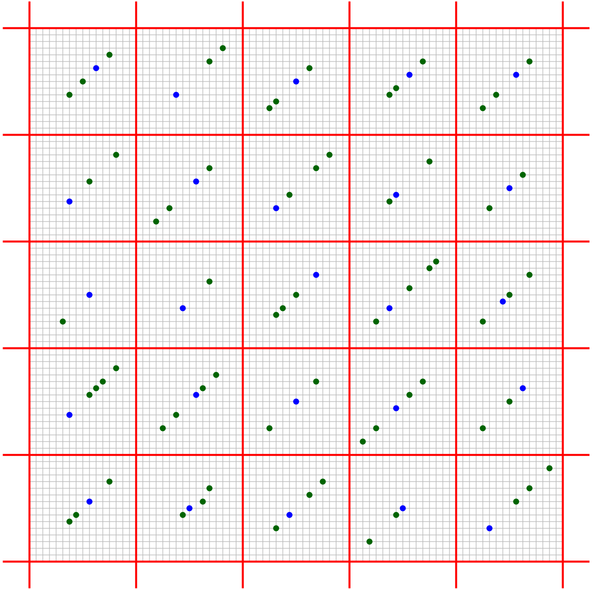
More Details about ρ



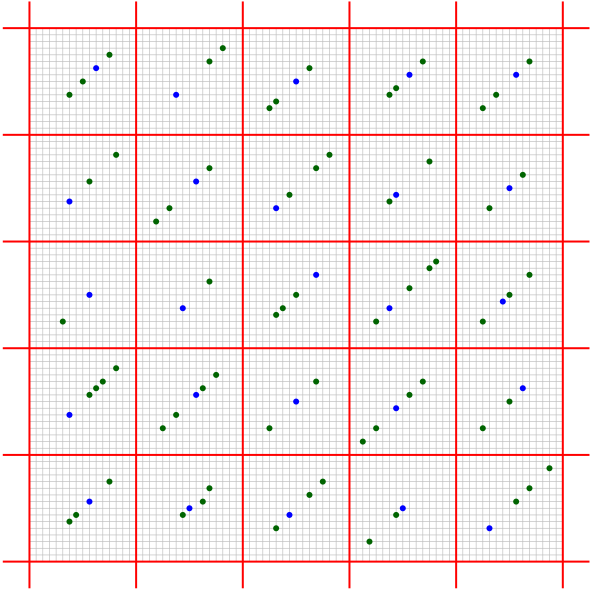
More Details about ρ

Key Difference:

#nodes with even constraint is $\log n$ instead of s per square



More Details about ρ



Limitation of this technique:

need to assign a $1 - o(1)$ fraction of vars

Conclusion

Conclusion and Open Problems

- Frege proofs of line-size M and depth d of Tseitin(T_n^2) are of length $\exp(n/\log^{O(d)} M)$
- Frege proofs of depth d of Tseitin(T_n^2) are of size $\exp(\tilde{\Omega}(n^{1/(d-1)}))$
- Open Problems:
  - Prove an $\exp(\tilde{\Omega}(n^{1/d}))$ lower bound on depth d Frege refutations for a CNF on n vars
    - Tseitin over an expander?
  - Circuits versus formulas? Can we obtain $\exp(\tilde{\Omega}(d \cdot n^{1/d}))$ lower bounds for Tseitin(T_n^2)?
  - Prove any bounded depth Frege lower bound for a (supposedly) hard formula
    - truthtable formula
    - clique
    - random CNFs

Conclusion and Open Problems

- Frege proofs of line-size M and depth d of Tseitin(T_n^2) are of length $\exp\big(n/\log^{O(d)} M\big)$
- Frege proofs of depth d of Tseitin(T_n^2) are of size $\exp\big(\tilde{\Omega}(n^{1/(d-1)})\big)$
- Open Problems:
  - Prove an $\exp\big(\tilde{\Omega}(n^{1/d})\big)$ lower bound on depth d Frege refutations for a CNF on n vars
    - Tseitin over an expander?
  - Circuits versus formulas? Can we obtain $\exp\big(\tilde{\Omega}(d \cdot n^{1/d})\big)$ lower bounds for Tseitin(T_n^2)?
  - Prove any bounded depth Frege lower bound for a (supposedly) hard formula
    - truthtable formula
    - clique
    - random CNFs

Thanks!