The Minimum Circuit Size Problem is hard for Sum of Squares

Kilian Risse

KTH Royal Institute of Technology,
Stockholm, Sweden

July 5 2022,
ICMS, Edinburgh

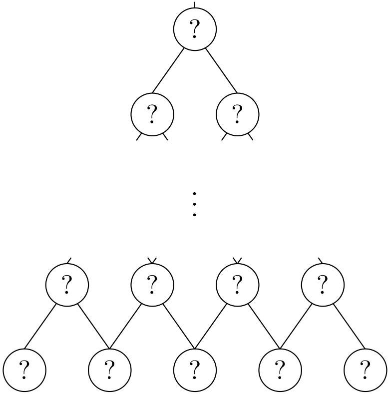
Joint work with Per Austrin

The Minimum Circuit Size Problem (MCSP)

$$f = \boxed{1|0|0|0|1|1|1|0|0|1|1|0|1 \quad \cdots \quad 0|1|1|0|1|1|0|0|1|0|1|0|0|0|1|1|0|1|0|0|0|1|1|0|0|1|0|1}$$

The Minimum Circuit Size Problem (MCSP)

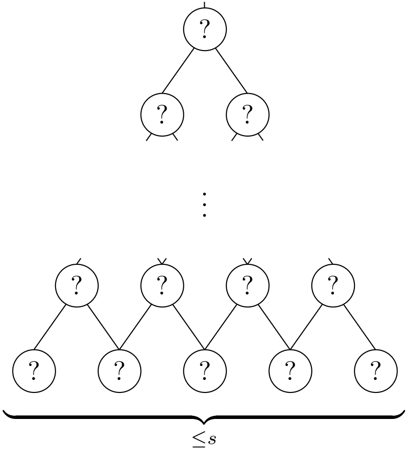
$f = \boxed{1|0|0|0|1|1|1|0|0|1|1|0|1 \ \cdots \ 0|1|1|0|1|1|0|0|1|0|1|0|0|0|1|1|0|1|0|0|0|1|1|0|0|1|0|1}$



$? \in \{\wedge, \vee, \neg\}$

The Minimum Circuit Size Problem (MCSP)

$$f = \boxed{1|0|0|0|1|1|1|0|0|1|1|0|1\ \cdots\ 0|1|1|0|1|1|0|0|1|0|1|0|0|0|1|1|0|1|0|0|0|1|1|0|0|1|0|1}$$



$$? \in \{\wedge, \vee, \neg\}$$

The Minimum Circuit Size Problem (MCSP)

- $\mathrm{MCSP}(f, s)$: is there a circuit of size $\leq s$ computing the given a truthtable $f \in \{0,1\}^{2^n}$?

The Minimum Circuit Size Problem (MCSP)

- $\mathrm{MCSP}(f, s)$: is there a circuit of size $\leq s$ computing the given a truthtable $f \in \{0,1\}^{2^n}$?
- $\mathrm{MCSP}(f, s) \in$ NP: have time to check whether given circuit computes f

The Minimum Circuit Size Problem (MCSP)

- $\mathrm{MCSP}(f, s)$: is there a circuit of size $\leq s$ computing the given a truthtable $f \in \{0,1\}^{2^n}$?
- $\mathrm{MCSP}(f, s) \in$ NP: have time to check whether given circuit computes f
- ... is $\mathrm{MCSP}(f, s)$ NP-hard?

The Minimum Circuit Size Problem (MCSP)

- $\mathrm{MCSP}(f, s)$: is there a circuit of size $\leq s$ computing the given a truthtable $f \in \{0,1\}^{2^n}$?
- $\mathrm{MCSP}(f, s) \in$ NP: have time to check whether given circuit computes f
- . . . is $\mathrm{MCSP}(f, s)$ NP-hard? We do not know!

The Minimum Circuit Size Problem (MCSP)

- $\mathrm{MCSP}(f, s)$: is there a circuit of size $\leq s$ computing the given a truthtable $f \in \{0,1\}^{2^n}$?
- $\mathrm{MCSP}(f, s) \in$ NP: have time to check whether given circuit computes f
- ... is $\mathrm{MCSP}(f, s)$ NP-hard? We do not know!
- NP-hardness of $\mathrm{MCSP}(f, s)$ would imply breakthrough circuit lower bounds

The Minimum Circuit Size Problem (MCSP)

- $\mathrm{MCSP}(f, s)$: is there a circuit of size $\leq s$ computing the given a truthtable $f \in \{0,1\}^{2^n}$?
- $\mathrm{MCSP}(f, s) \in$ NP: have time to check whether given circuit computes f
- ... is $\mathrm{MCSP}(f, s)$ NP-hard? We do not know!
- NP-hardness of $\mathrm{MCSP}(f, s)$ would imply breakthrough circuit lower bounds

Goal: show that classes of efficient algorithms do not solve $\mathrm{MCSP}(f, s)$.

MCSP in Proof Complexity

- Formalize $\mathrm{MCSP}(f, s)$ as a CNF-formula over $O(2^n \cdot s)$ variables

MCSP in Proof Complexity

- Formalize $\mathrm{MCSP}(f, s)$ as a CNF-formula over $O(2^n \cdot s)$ variables
- The $\mathrm{MCSP}(f, s)$ formula is central to proof complexity:

MCSP in Proof Complexity

- Formalize $\mathrm{MCSP}(f, s)$ as a CNF-formula over $O(2^n \cdot s)$ variables
- The $\mathrm{MCSP}(f, s)$ formula is central to proof complexity:
  - lower bounds on $\mathrm{MCSP}(\mathsf{SAT}, n^c)$ essentially imply that NP $\not\subseteq$ P/poly requires long proofs

MCSP in Proof Complexity

- Formalize $\mathrm{MCSP}(f,s)$ as a CNF-formula over $O(2^n \cdot s)$ variables
- The $\mathrm{MCSP}(f,s)$ formula is central to proof complexity:
  - lower bounds on $\mathrm{MCSP}(\text{SAT}, n^c)$ essentially imply that NP $\not\subseteq$ P/poly requires long proofs
  - one of few formulas conjectured hard for strong proof systems such as extended Frege

MCSP in Proof Complexity

- Formalize $\mathrm{MCSP}(f, s)$ as a CNF-formula over $O(2^n \cdot s)$ variables
- The $\mathrm{MCSP}(f, s)$ formula is central to proof complexity:
  - lower bounds on $\mathrm{MCSP}(\mathsf{SAT}, n^c)$ essentially imply that NP $\not\subseteq$ P/poly requires long proofs
  - one of few formulas conjectured hard for strong proof systems such as extended Frege
- Only have lower bounds for weak proof systems:

MCSP in Proof Complexity

- Formalize $\mathrm{MCSP}(f, s)$ as a CNF-formula over $O(2^n \cdot s)$ variables

- The $\mathrm{MCSP}(f, s)$ formula is central to proof complexity:
  - lower bounds on $\mathrm{MCSP}(\mathsf{SAT}, n^c)$ essentially imply that NP $\not\subseteq$ P/poly requires long proofs
  - one of few formulas conjectured hard for strong proof systems such as extended Frege

- Only have lower bounds for weak proof systems:
  - Polynomial Calculus (over any field) [Raz98]

MCSP in Proof Complexity

- Formalize $\mathrm{MCSP}(f, s)$ as a CNF-formula over $O(2^n \cdot s)$ variables
- The $\mathrm{MCSP}(f, s)$ formula is central to proof complexity:
  - lower bounds on $\mathrm{MCSP}(\mathsf{SAT}, n^c)$ essentially imply that NP $\not\subseteq$ P/poly requires long proofs
  - one of few formulas conjectured hard for strong proof systems such as extended Frege
- Only have lower bounds for weak proof systems:
  - Polynomial Calculus (over any field) [Raz98]
  - Resolution [RWY02, PR04, Raz04a, Raz04b]

MCSP in Proof Complexity

- Formalize $\mathrm{MCSP}(f, s)$ as a CNF-formula over $O(2^n \cdot s)$ variables
- The $\mathrm{MCSP}(f, s)$ formula is central to proof complexity:
  - lower bounds on $\mathrm{MCSP}(\mathsf{SAT}, n^c)$ essentially imply that NP $\not\subseteq$ P/poly requires long proofs
  - one of few formulas conjectured hard for strong proof systems such as extended Frege
- Only have lower bounds for weak proof systems:
  - Polynomial Calculus (over any field) [Raz98]
  - Resolution [RWY02, PR04, Raz04a, Raz04b]
  - Res($\varepsilon \log s$) [Raz15]

MCSP in Proof Complexity

- Formalize $\mathrm{MCSP}(f, s)$ as a CNF-formula over $O(2^n \cdot s)$ variables
- The $\mathrm{MCSP}(f, s)$ formula is central to proof complexity:
  - lower bounds on $\mathrm{MCSP}(\mathsf{SAT}, n^c)$ essentially imply that NP $\not\subseteq$ P/poly requires long proofs
  - one of few formulas conjectured hard for strong proof systems such as extended Frege
- Only have lower bounds for weak proof systems:
  - Polynomial Calculus (over any field) [Raz98]
  - Resolution [RWY02, PR04, Raz04a, Raz04b]
  - Res($\varepsilon \log s$) [Raz15]

Open Problem ([Raz22])

Prove that SoS requires degree $s^{\Omega(1)}$ to refute $\mathrm{MCSP}(f, s)$.

Sum of Squares

- Let $\mathcal{P} = \{p_1 = 0, \ldots, p_m = 0\}$ be a system of polynomial equations
- An SoS certificate of unsatisfiability of $\mathcal{P}$ are polys $\pi = (t_1, \ldots, t_a; s_1, \ldots s_b)$ such that

$$\sum_{i=1}^{a} t_i \cdot p_i + \sum_{j=1}^{b} s_j^2 = -1$$

Sum of Squares

- Let $\mathcal{P} = \{p_1 = 0, \ldots, p_m = 0\}$ be a system of polynomial equations
- An SoS certificate of unsatisfiability of $\mathcal{P}$ are polys $\pi = (t_1, \ldots, t_a; s_1, \ldots s_b)$ such that

$$\sum_{i=1}^{a} t_i \cdot p_i + \sum_{j=1}^{b} s_j^2 = -1$$

- The SoS degree of refuting $\mathcal{P}$ is the min degree of any SoS refutation

Sum of Squares

- Let $\mathcal{P} = \{p_1 = 0, \ldots, p_m = 0\}$ be a system of polynomial equations
- An SoS certificate of unsatisfiability of $\mathcal{P}$ are polys $\pi = (t_1, \ldots, t_a; s_1, \ldots s_b)$ such that

$$\sum_{i=1}^{a} t_i \cdot p_i + \sum_{j=1}^{b} s_j^2 = -1$$

- The SoS degree of refuting $\mathcal{P}$ is the min degree of any SoS refutation
- The SoS size of refuting $\mathcal{P}$ is the min number of monomials in any SoS refutation

Results

Results

Theorem

For all Boolean functions $f : \{0,1\}^n \to \{0,1\}$ *and* $s \geq n^{d(\varepsilon)}$*, it holds that SoS requires degree* $\Omega_\varepsilon(s^{1-\varepsilon})$ *to refute* $\mathrm{MCSP}(f, s)$*.*

Results

Theorem

For all Boolean functions $f : \{0,1\}^n \to \{0,1\}$ and $s \geq n^{d(\varepsilon)}$, it holds that SoS requires degree $\Omega_\varepsilon(s^{1-\varepsilon})$ to refute $\mathrm{MCSP}(f, s)$.

Essentially tight: there is a degree $O(s)$ SoS refutation.

Results

Theorem

For all Boolean functions $f : \{0,1\}^n \to \{0,1\}$ *and* $s \geq n^{d(\varepsilon)}$*, it holds that SoS requires degree* $\Omega_\varepsilon(s^{1-\varepsilon})$ *to refute* $\mathrm{MCSP}(f, s)$*.*

Essentially tight: there is a degree $O(s)$ SoS refutation.

Theorem

Let f *be a Boolean function that has a circuit of size* $s \geq n^{d(\varepsilon)}$ *computing* f *on all but* t *inputs. Then SoS requires size* $\exp\left(\Omega_\varepsilon(s^{2-\varepsilon}/t)\right)$ *to refute* $\mathrm{MCSP}(f, s)$*.*

Results

Theorem

For all Boolean functions $f : \{0,1\}^n \to \{0,1\}$ *and* $s \geq n^{d(\varepsilon)}$*, it holds that SoS requires degree* $\Omega_\varepsilon(s^{1-\varepsilon})$ *to refute* $\mathrm{MCSP}(f, s)$*.*

Essentially tight: there is a degree $O(s)$ SoS refutation.

Theorem

Let f *be a Boolean function that has a circuit of size* $s \geq n^{d(\varepsilon)}$ *computing* f *on all but* t *inputs. Then SoS requires size* $\exp\left(\Omega_\varepsilon(s^{2-\varepsilon}/t)\right)$ *to refute* $\mathrm{MCSP}(f, s)$*.*

For example, we may set $s = 2^{n^{0.99}}$ and $t = s^{1.5}$, then SoS requires size $2^{\Omega(2^{n^{0.99}})}$.

Results

Theorem

For all Boolean functions $f : \{0,1\}^n \to \{0,1\}$ and $s \geq n^{d(\varepsilon)}$, it holds that SoS requires degree $\Omega_\varepsilon(s^{1-\varepsilon})$ to refute $\mathrm{MCSP}(f, s)$.

Essentially tight: there is a degree $O(s)$ SoS refutation.

Theorem

Let f be a Boolean function that has a circuit of size $s \geq n^{d(\varepsilon)}$ computing f on all but t inputs. Then SoS requires size $\exp\left(\Omega_\varepsilon(s^{2-\varepsilon}/t)\right)$ to refute $\mathrm{MCSP}(f, s)$.

For example, we may set $s = 2^{n^{0.99}}$ and $t = s^{1.5}$, then SoS requires size $2^{\Omega(2^{n^{0.99}})}$.

Similar results in the monotone setting for monotone slice functions.

Proof Ideas

Encoding $\mathrm{MCSP}(f, s)$

- There exists circuit C s.t. for all inputs $\alpha \in \{0,1\}^x$ it holds that $C(\alpha) = f(\alpha)$

Encoding $\mathrm{MCSP}(f, s)$

- There exists circuit C s.t. for all inputs $\alpha \in \{0,1\}^x$ it holds that $C(\alpha) = f(\alpha)$
- $\mathrm{MCSP}(f, s) = \mathrm{Circuit}_s(y) \quad \wedge \quad \left(\bigwedge_{\alpha \in \{0,1\}^n} C_y(\alpha) = f(\alpha) \right)$

Encoding $\mathrm{MCSP}(f, s)$

- There exists circuit C s.t. for all inputs $\alpha \in \{0,1\}^x$ it holds that $C(\alpha) = f(\alpha)$
- $\mathrm{MCSP}(f, s) = \mathrm{Circuit}_s(y) \quad \wedge \quad \left(\bigwedge_{\alpha \in \{0,1\}^n} C_y(\alpha) = f(\alpha)\right)$
  - $\mathrm{Circuit}_s(\beta)$ is sat iff $\beta \in \{0,1\}^y$ encodes a valid circuit of size s

Encoding $\mathrm{MCSP}(f, s)$

- There exists circuit C s.t. for all inputs $\alpha \in \{0,1\}^x$ it holds that $C(\alpha) = f(\alpha)$
- $\mathrm{MCSP}(f, s) = \mathrm{Circuit}_s(y) \quad \wedge \quad \left(\bigwedge_{\alpha \in \{0,1\}^n} C_y(\alpha) = f(\alpha) \right)$
  - $\mathrm{Circuit}_s(\beta)$ is sat iff $\beta \in \{0,1\}^y$ encodes a valid circuit of size s

Encoding $\mathrm{MCSP}(f, s)$

- There exists circuit C s.t. for all inputs $\alpha \in \{0,1\}^x$ it holds that $C(\alpha) = f(\alpha)$
- $\mathrm{MCSP}(f, s) = \mathrm{Circuit}_s(y) \quad \wedge \quad \left(\bigwedge_{\alpha \in \{0,1\}^n} C_y(\alpha) = f(\alpha) \right)$
  - $\mathrm{Circuit}_s(\beta)$ is sat iff $\beta \in \{0,1\}^y$ encodes a valid circuit of size s
  - $C_\beta(\alpha) = f(\alpha)$ is sat iff the circuit encoded by β evaluates to $f(\alpha)$ on input α

Encoding $\mathrm{MCSP}(f, s)$

- There exists circuit C s.t. for all inputs $\alpha \in \{0,1\}^x$ it holds that $C(\alpha) = f(\alpha)$
- $\mathrm{MCSP}(f, s) = \mathrm{Circuit}_s(y) \quad \wedge \quad \left(\bigwedge_{\alpha \in \{0,1\}^n} C_y(\alpha) = f(\alpha)\right)$
  - $\mathrm{Circuit}_s(\beta)$ is sat iff $\beta \in \{0,1\}^y$ encodes a valid circuit of size s
  - $C_\beta(\alpha) = f(\alpha)$ is sat iff the circuit encoded by β evaluates to $f(\alpha)$ on input α
- Idea: restrict $\mathrm{Circuit}_s(y)$ by ρ s.t. sat assignments correspond to a "nice" set of circuits

Proof Idea

What can we base the hardness on?

Proof Idea

What can we base the hardness on?

Linear equations modulo 2.

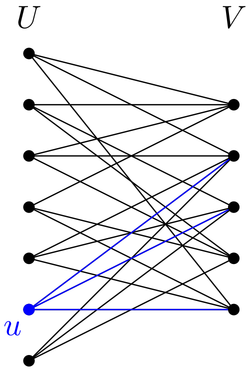
Proof Idea

What can we base the hardness on?

Linear equations modulo 2.

- Given $b \in \{0,1\}^U$, for every $u \in U$ we have the constraint

$$\bigoplus_{v \in N(u)} z_v = b_u$$



Proof Idea

What can we base the hardness on?

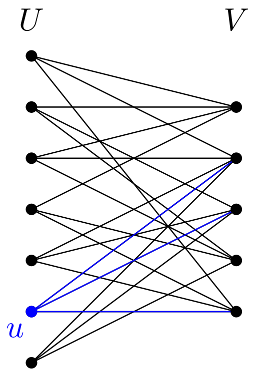
Linear equations modulo 2.

- Given $b \in \{0,1\}^U$, for every $u \in U$ we have the constraint

$$\bigoplus_{v \in N(u)} z_v = b_u$$

- Choose ρ such that for all assignments γ to $\mathrm{Circuit}_s(y)\big|_\rho$ we have

$$C_{\rho\gamma}(\alpha) = \bigoplus_{v \in N(\alpha)} \gamma_v$$



Proof Idea

What can we base the hardness on?

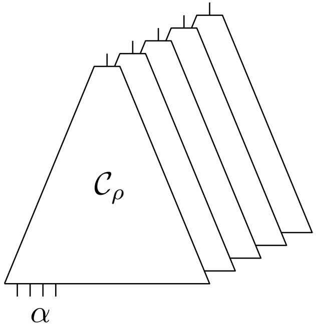
Linear equations modulo 2.

- Given $b \in \{0,1\}^U$, for every $u \in U$ we have the constraint

$$\bigoplus_{v \in N(u)} z_v = b_u$$

- Choose ρ such that for all assignments γ to $\mathrm{Circuit}_s(y)\big|_\rho$ we have

$$C_{\rho\gamma}(\alpha) = \bigoplus_{v \in N(\alpha)} \gamma_v$$



Proof Idea

What can we base the hardness on?

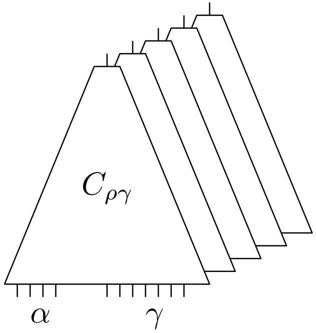
Linear equations modulo 2.

- Given $b \in \{0,1\}^U$, for every $u \in U$ we have the constraint

$$\bigoplus_{v \in N(u)} z_v = b_u$$

- Choose ρ such that for all assignments γ to $\mathrm{Circuit}_s(y)\big|_\rho$ we have

$$C_{\rho\gamma}(\alpha) = \bigoplus_{v \in N(\alpha)} \gamma_v$$



Proof Idea

What can we base the hardness on?

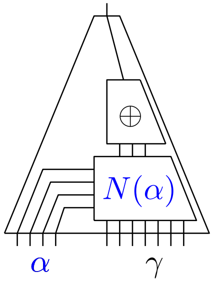
Linear equations modulo 2.

- Given $b \in \{0,1\}^U$, for every $u \in U$ we have the constraint

$$\bigoplus_{v \in N(u)} z_v = b_u$$

- Choose ρ such that for all assignments γ to $\mathrm{Circuit}_s(y)\big|_\rho$ we have

$$C_{\rho\gamma}(\alpha) = \bigoplus_{v \in N(\alpha)} \gamma_v$$



Proof Idea

What can we base the hardness on?

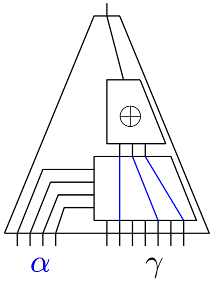
Linear equations modulo 2.

- Given $b \in \{0,1\}^U$, for every $u \in U$ we have the constraint

$$\bigoplus_{v \in N(u)} z_v = b_u$$

- Choose ρ such that for all assignments γ to $\mathrm{Circuit}_s(y)\big|_\rho$ we have

$$C_{\rho\gamma}(\alpha) = \bigoplus_{v \in N(\alpha)} \gamma_v$$



Proof Idea

What can we base the hardness on?

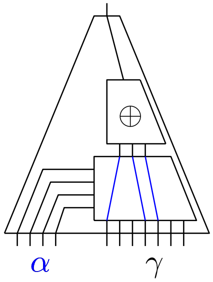
Linear equations modulo 2.

- Given $b \in \{0,1\}^U$, for every $u \in U$ we have the constraint

$$\bigoplus_{v \in N(u)} z_v = b_u$$

- Choose ρ such that for all assignments γ to $\mathrm{Circuit}_s(y)\big|_\rho$ we have

$$C_{\rho\gamma}(\alpha) = \bigoplus_{v \in N(\alpha)} \gamma_v$$



Proof Idea

What can we base the hardness on?

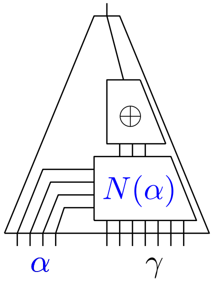
Linear equations modulo 2.

- Given $b \in \{0,1\}^U$, for every $u \in U$ we have the constraint

$$\bigoplus_{v \in N(u)} z_v = b_u$$

- Choose ρ such that for all assignments γ to $\mathrm{Circuit}_s(y)\big|_\rho$ we have

$$C_{\rho\gamma}(\alpha) = \bigoplus_{v \in N(\alpha)} \gamma_v$$



Proof Idea

What can we base the hardness on?

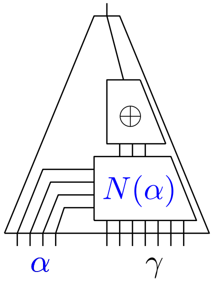
Linear equations modulo 2.

- Given $b \in \{0,1\}^U$, for every $u \in U$ we have the constraint

$$\bigoplus_{v \in N(u)} z_v = b_u$$

- Choose ρ such that for all assignments γ to $\mathrm{Circuit}_s(y)\big|_\rho$ we have

$$C_{\rho\gamma}(\alpha) = \bigoplus_{v \in N(\alpha)} \gamma_v$$



Use explicit expanders [GUV09] and known SoS lower bounds [Gri01] to obtain main theorem.

Conclusion and Open Problems

- Same ideas can be used to recover PC degree lower bounds
- Unifies and simplifies these MCSP lower bounds
- Equational CSP (e.g. k-XOR) lower bounds over expanders $\Rightarrow$ $\mathrm{MCSP}(f, s)$ lower bounds
- Some open problems:
  - Cutting Planes lower bounds for $\mathrm{MCSP}(f, s)$
  - More general size lower bounds for SoS
  - Can SoS prove anything in the monotone setting?

Conclusion and Open Problems

- Same ideas can be used to recover PC degree lower bounds
- Unifies and simplifies these MCSP lower bounds
- Equational CSP (e.g. k-XOR) lower bounds over expanders $\Rightarrow$ $\mathrm{MCSP}(f, s)$ lower bounds
- Some open problems:
  - Cutting Planes lower bounds for $\mathrm{MCSP}(f, s)$
  - More general size lower bounds for SoS
  - Can SoS prove anything in the monotone setting?

Thanks!

References I

[Gri01] Dima Grigoriev. Linear lower bound on degrees of positivstellensatz calculus proofs for the parity. *Theoretical Computer Science*, 259(1):613 – 622, 2001.

[GUV09] Venkatesan Guruswami, Christopher Umans, and Salil Vadhan. Unbalanced expanders and randomness extractors from Parvaresh–Vardy codes. *Journal of the ACM*, 56(4):20:1–20:34, July 2009. Preliminary version in *CCC '07*.

[PR04] Toniann Pitassi and Ran Raz. Regular resolution lower bounds for the weak pigeonhole principle. *Combinatorica*, 24(3):503–524, 2004. Preliminary version in *STOC '01*.

[Raz98] Alexander A. Razborov. Lower bounds for the polynomial calculus. *Computational Complexity*, 7(4):291–324, December 1998.

[Raz04a] Ran Raz. Resolution lower bounds for the weak pigeonhole principle. *Journal of the ACM*, 51(2):115–138, March 2004. Preliminary version in *STOC '02*.

[Raz04b] Alexander A. Razborov. Resolution lower bounds for perfect matching principles. *Journal of Computer and System Sciences*, 69(1):3–27, August 2004. Preliminary version in *CCC '02*.

[Raz15] Alexander A. Razborov. Pseudorandom generators hard for k-DNF resolution and polynomial calculus resolution. *Annals of Mathematics*, 181(2):415–472, March 2015.

References II

[Raz22] Alexander Razborov. Open problems. https://people.cs.uchicago.edu/~razborov/teaching/index.html, 2022. Accessed April 2022.

[RWY02] Alexander A. Razborov, Avi Wigderson, and Andrew Chi-Chih Yao. Read-once branching programs, rectangular proofs of the pigeonhole principle and the transversal calculus. *Combinatorica*, 22(4):555–574, 2002. Preliminary version in *STOC '97*.