Weighted Gate Elimination

Alexander Golovnev
New York University

Alexander S. Kulikov
Steklov Institute of Mathematics

ITCS 2016

Gate Elimination

Lower Bounds for Affine Dispersers

Lower Bound for Quadratic Dispersers

Open Problems

Outline

Gate Elimination

Lower Bounds for Affine Dispersers

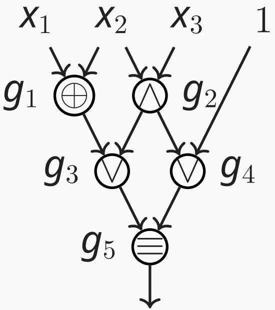
Lower Bound for Quadratic Dispersers

Open Problems

Boolean Circuits

Inputs:
$x_1, \ldots, x_n, 0, 1$
Gates:
binary functions
Fan-out:
unbounded
Depth:
unbounded

$$
\begin{aligned}
g_1 &= x_1 \oplus x_2 \\
g_2 &= x_2 \wedge x_3 \\
g_3 &= g_1 \vee g_2 \\
g_4 &= g_2 \vee 1 \\
g_5 &= g_3 \equiv g4
\end{aligned}
$$



Exponential Bounds

Lower Bound

Counting shows that almost all functions of n variables have circuit size $\Omega(2^n/n)$ [Shannon 1949].

Upper Bound

Any function can be computed by circuits of size $(1+o(1))2^n/n$ [Lupanov 1958].

Explicit Lower Bounds

Previous

$2n$	$f(x) = \bigoplus_{i<j} x_i x_j$	[Kloss, Malyshev 1965]
$2n$	$f(x) = [\sum x_i \equiv_3 0]$	[Schnorr 1974]
$2.5n$	$f(x, a, b) = x_a \oplus x_b$	[Paul 1977]
$2.5n$	symmetric	[Stockmeyer 1977]
$3n$	$f(x, a, b, c) = x_a x_b \oplus x_c$	[Blum 1984]
$3n$	affine dispersers	[Demenkov, Kulikov 2011]
$3.011n$	affine dispersers	[FGHK 2015]

Explicit Lower Bounds

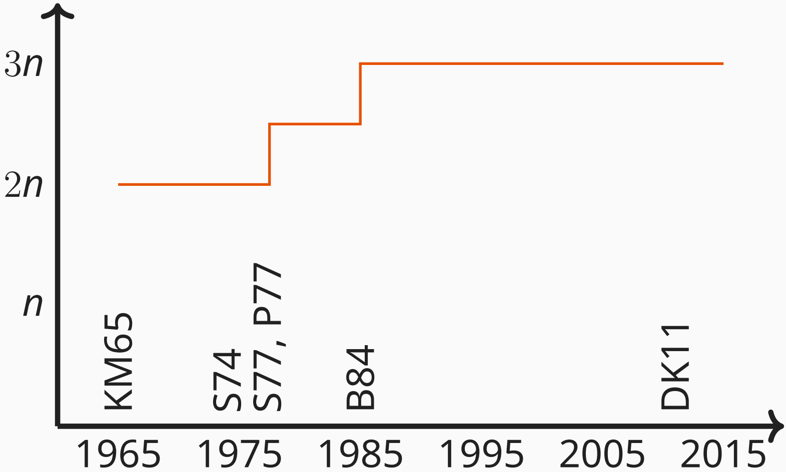
Previous

$2n$	$f(x) = \bigoplus_{i<j} x_i x_j$	[Kloss, Malyshev 1965]
$2n$	$f(x) = [\sum x_i \equiv_3 0]$	[Schnorr 1974]
$2.5n$	$f(x, a, b) = x_a \oplus x_b$	[Paul 1977]
$2.5n$	symmetric	[Stockmeyer 1977]
$3n$	$f(x, a, b, c) = x_a x_b \oplus x_c$	[Blum 1984]
$3n$	affine dispersers	[Demenkov, Kulikov 2011]
$3.011n$	affine dispersers	[FGHK 2015]

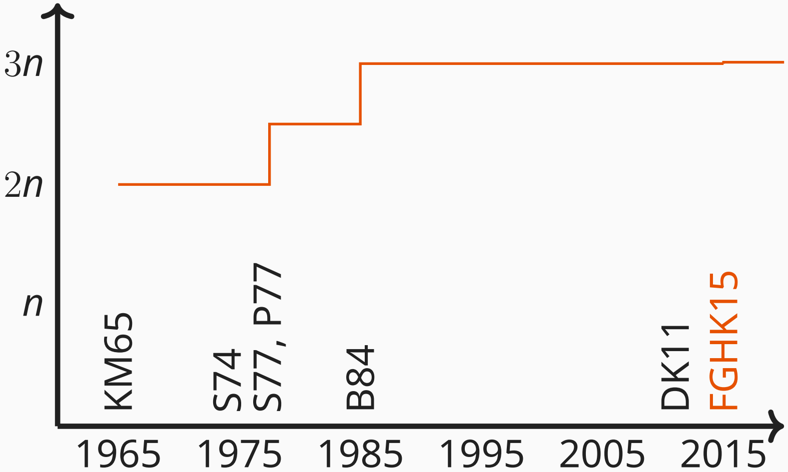
New

$3.11n$	quadratic dispersers (non-explicit)	[G, Kulikov 2015]

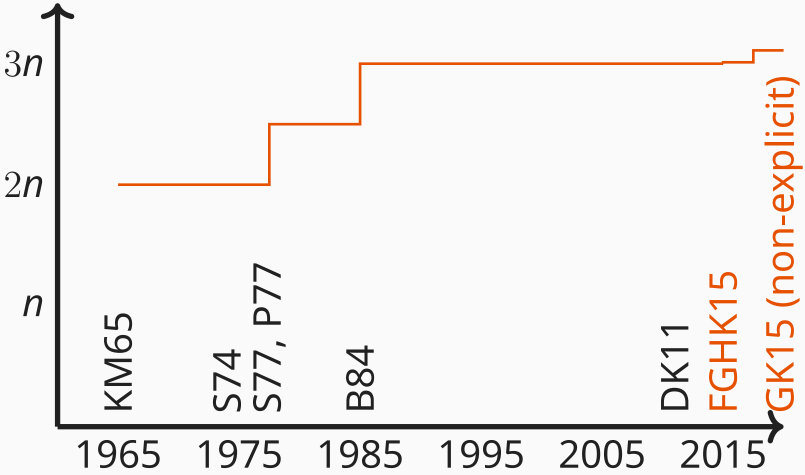
Explicit Lower Bounds: Pictorially



Explicit Lower Bounds: Pictorially



Explicit Lower Bounds: Pictorially

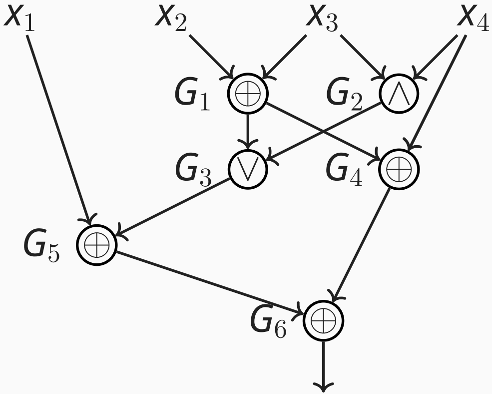


Gate Elimination Method

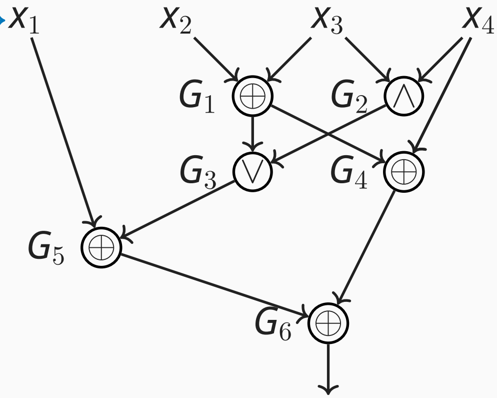
To prove, say, a $3n$ lower bound for all functions f from a certain class $\mathcal{C}$:

- show that for any circuit computing f, one can find a substitution eliminating at least 3 gates;
- show that the resulting subfunction still belongs to $\mathcal{C}$;
- proceed by induction.

Gate Elimination: Example

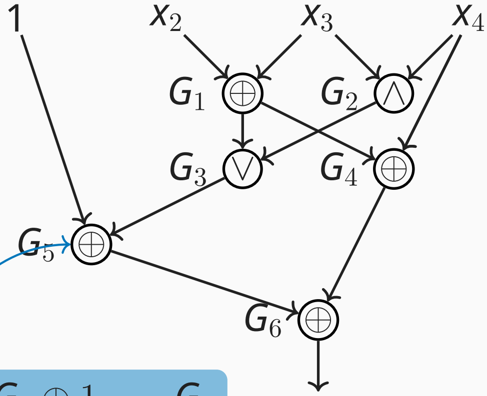


Gate Elimination: Example



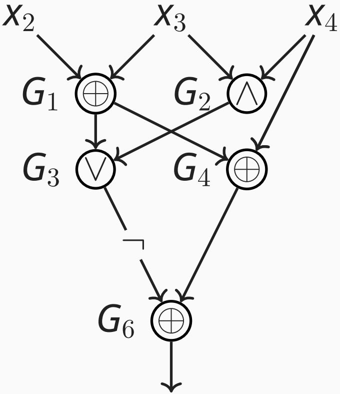
assign $x_1 = 1$

Gate Elimination: Example

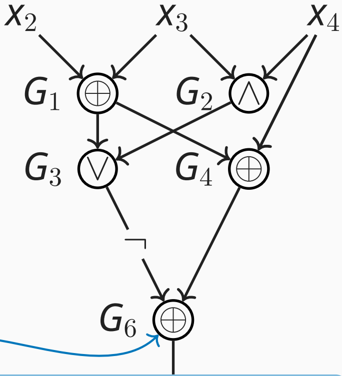


G_5 now computes $G_3 \oplus 1 = \neg G_3$

Gate Elimination: Example

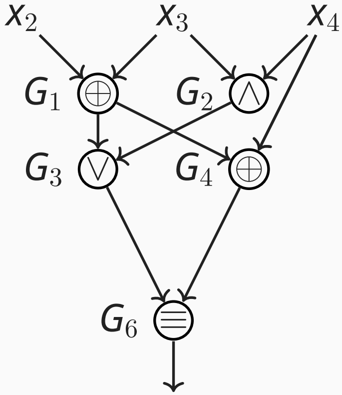


Gate Elimination: Example

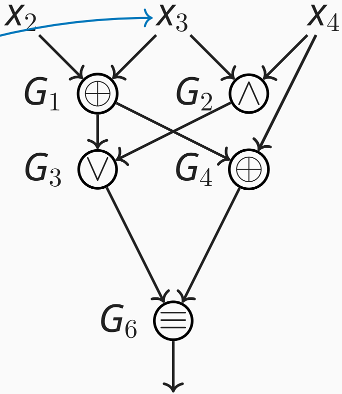


now we can change the binary function assigned to G_6

Gate Elimination: Example

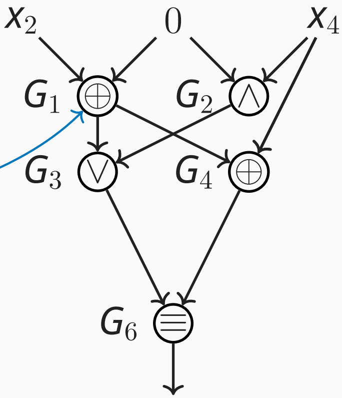


Gate Elimination: Example



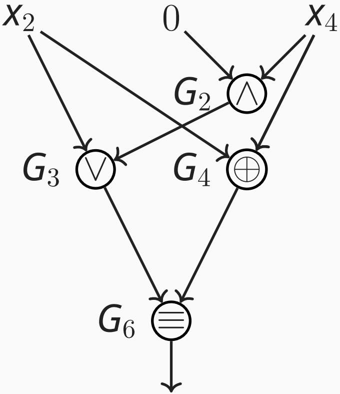
now assign $x_3 = 0$

Gate Elimination: Example

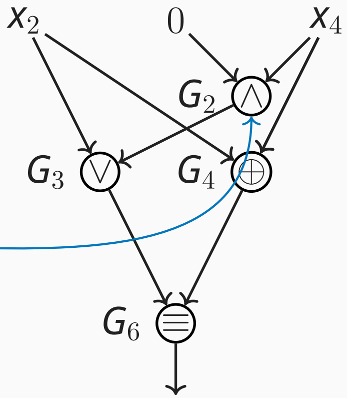


G_1 then is equal to x_2

Gate Elimination: Example

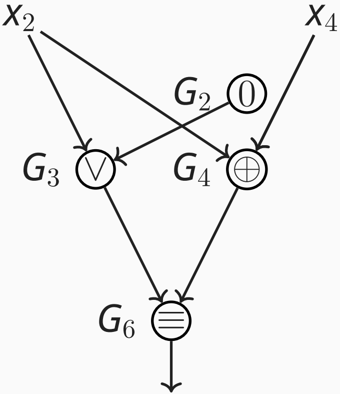


Gate Elimination: Example

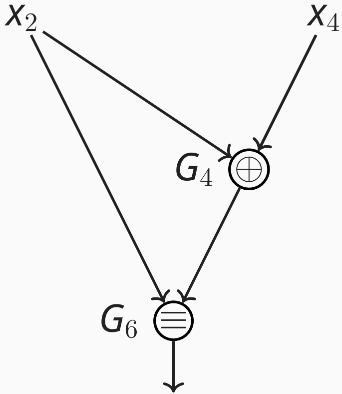


$G_2 = 0$

Gate Elimination: Example



Gate Elimination: Example



Binary Functions

There are 16 Boolean functions.

- 2 constant functions: 0, 1;
- 4 degenerate functions: x, $x \oplus 1$, y, $y \oplus 1$;
- 2 xor-type functions: $x \oplus y$, $x \oplus y \oplus 1$;
- 8 and-type functions: $(x \oplus a)(y \oplus b) \oplus c$ where $a, b, c \in 0, 1$.

Outline

Gate Elimination

Lower Bounds for Affine Dispersers

Lower Bound for Quadratic Dispersers

Open Problems

$3n$ Lower Bound

Theorem

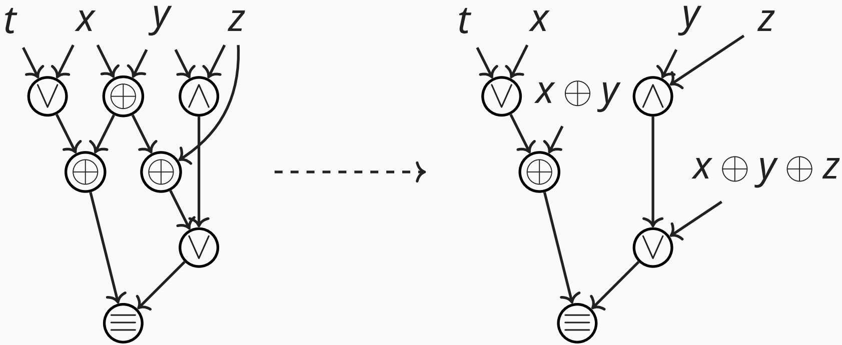
If $f\colon \{0,1\}^n \to \{0,1\}$ is an affine disperser for dimension $d = o(n)$, then

$$\mathrm{size}(f) \geq 3n - o(n).$$

Affine Dispersers

- A function $f\colon \{0,1\}^n \to \{0,1\}$ is called an affine disperser for dimension d if it is non-constant on any affine subspace of dimension at least d.
- An affine dispereser for dimension d cannot become constant after any $n - d$ linear substitutions (i.e., substitutions of the form $x_2 \oplus x_3 \oplus x_9 = 0$).
- There exist explicit constructions of affine dispersers for subliner dimension $d = o(n)$ (e.g., [Ben-Sasson, Kopparty, 2012]).

XOR-layered Circuits



$\text{inputs}(\mathcal{C}) = 4$
$\text{size}(\mathcal{C}) = 7$

$\text{inputs}(\mathcal{C}') = 6$
$\text{size}(\mathcal{C}') = 5$

$$\text{inputs}(\mathcal{C}') + \text{size}(\mathcal{C}') \leq \text{inputs}(\mathcal{C}) + \text{size}(\mathcal{C}).$$

$3n - o(n)$ Lower Bound

Theorem [Demenkov, Kulikov 2011]

For a circuit C computing an affine disperser for dimension d:

$$\mathrm{inputs}(\mathcal{C}) + \mathrm{size}(\mathcal{C}) \geq 4(n - d)\,.$$

Corollary

$\mathrm{size}(f) \geq 3n - o(n)$ for an affine disperser for $d = o(n)$.

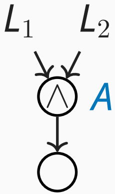
Proposition

The bound is tight: $\mathrm{size}(IP) = n - 1$ and IP is an affine disperser for dimension $d = n/2 + 1$.

Proof

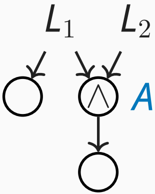
- Want to show:
$$\text{inputs}(\mathcal{C}) + \text{size}(\mathcal{C}) \geq 4(n-d).$$
- Make $n-d$ affine restrictions each time reducing $(\text{inputs} + \text{size})$ by at least 4.
- Convert $\mathcal{C}$ to XOR-layered and take a top-gate A:

Case 1



$L_1 \leftarrow 0$:
$\Delta\,\text{size} = 2$
$\Delta\,\text{inp} = 2$

Case 2



$L_1 \leftarrow 0$:
$\Delta\,\text{size} = 3$
$\Delta\,\text{inp} = 1$

Outline

Main Result

Theorem

Let $f\colon \{0,1\}^n \to \{0,1\}$ *be a function that is not constant on any set* $S \subseteq \{0,1\}^n$ *of size at least* $2^{n/100}$ *that can be defined as*

$$S = \{x\colon p_1(x) = \cdots = p_{2n}(x) = 0\},\ \deg(p_i) \leq 2.$$

Then

$$\mathrm{size}(f) \geq 3.11n\,.$$

Quadratic Dispersers

- A random function is not constant on any set S of size s that can be defined as

$$S = \{x \in \{0,1\}^n : p_1(x) = \cdots = p_{s/n^3}(x) = 0\}.$$

- We need much weaker dispersers: $(n, 2n, 2^{n/100})$-dispersers. Even in NP. Even with multiple outputs.

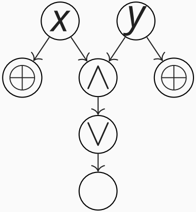
Regular Gate Elimination

- make a substitution;
- decrease S by a factor of 2;
- eliminate at least 3 gates;
- S belongs to the same class;
- repeat $n - o(n)$ times.

Weighted Gate Elimination

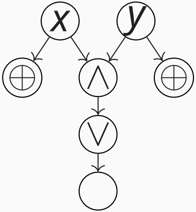
- make a restriction;
- decrease *S* by a factor of α;
- make sure to eliminate at least $3\log\alpha$ gates;
- *S* belongs to the same class;
- repeat until *S* becomes small (e.g., $2^{n/100}$).

Toy Example

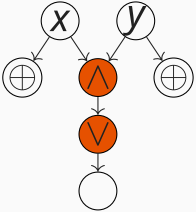


$$S \subseteq \{0, 1\}^n$$

Toy Example

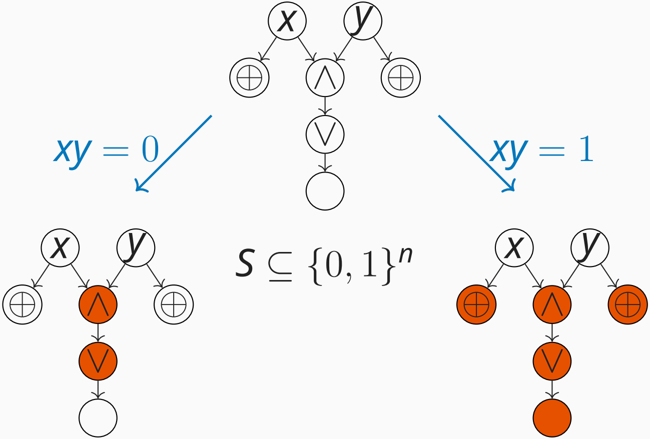


$$xy = 0$$

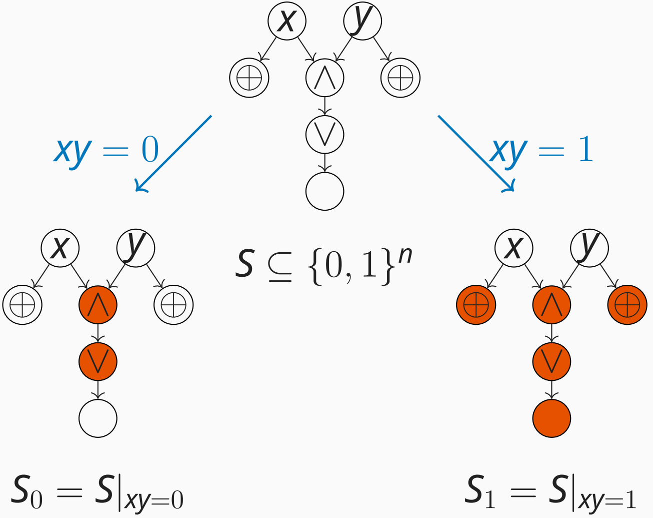


$$S \subseteq \{0,1\}^n$$

Toy Example



Toy Example



x y
$\oplus$ $\wedge$ $\oplus$
$\vee$
$xy = 0$
$xy = 1$
$S \subseteq \{0,1\}^n$
$S_0 = S|_{xy=0}$
$S_1 = S|_{xy=1}$

Outline

Gate Elimination

Lower Bounds for Affine Dispersers

Lower Bound for Quadratic Dispersers

Open Problems

Open Problems

- Quadratic dispersers in NP?

Open Problems

- Quadratic dispersers in NP?
- Lower bounds in other models?

Open Problems

- Quadratic dispersers in NP?
- Lower bounds in other models?
- Connections to algorithms for Circuit-SAT?

Thank you for your attention!