Generalizations of the Gate Elimination Method

Alexander S. Kulikov
Magnus Find, Alexander Golovnev, Edward A. Hirsch

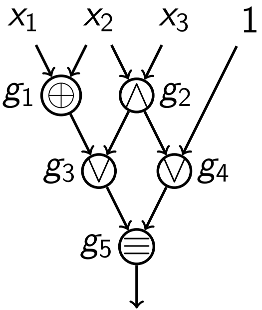
Steklov Institute of Mathematics at St. Petersburg
Russian Academy of Sciences

Connections Between Algorithm Design and Complexity Theory
October 1, 2015

Boolean Circuits

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

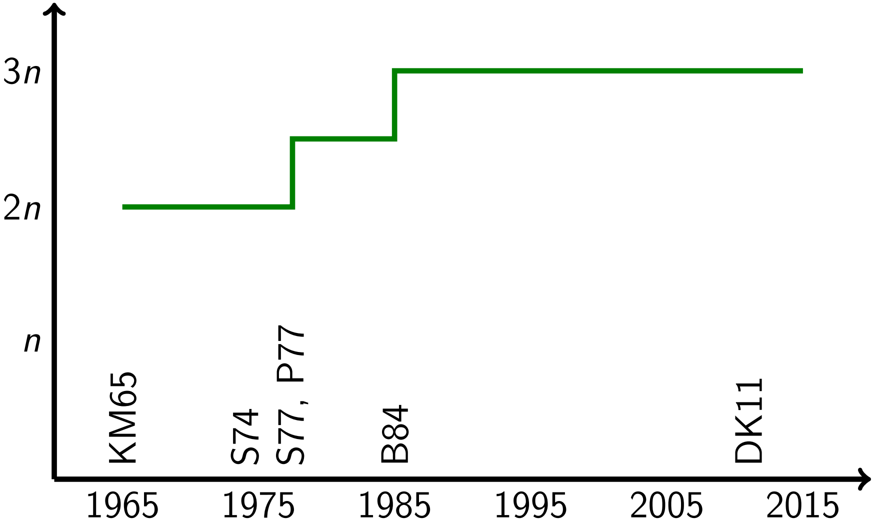
$$
\begin{aligned}
g_1 &= x_1 \oplus x_2 \\
g_2 &= x_2 \wedge x_3 \\
g_3 &= g_1 \vee g_2 \\
g_4 &= g_2 \vee 1 \\
g_5 &= g_3 \equiv g4
\end{aligned}
$$



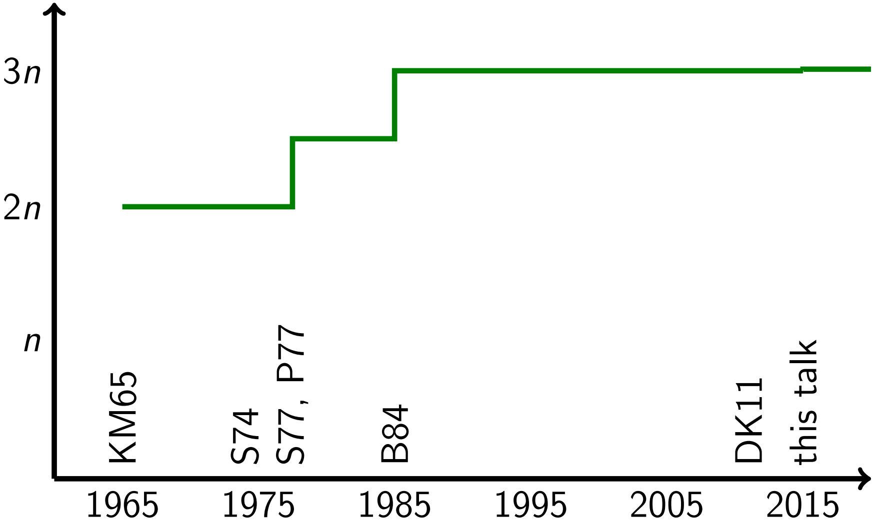
Known Lower Bounds

$2n$	$f(x) = \sum_{i<j} x_i x_j$	[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, K 2011]
$3.011n$	affine dispersers	[this talk]
$3.11n$	quadratic dispersers (non-explicit)	[this talk]

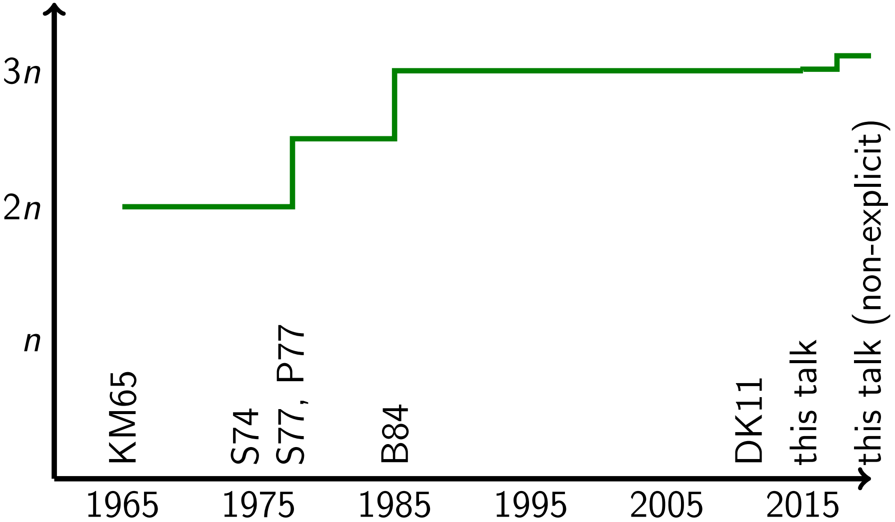
History



History


3n
2n
n
KM65
S74
S77, P77
B84
DK11
this talk
1965
1975
1985
1995
2005
2015

History


3n
2n
n
KM65
S74
S77, P77
B84
DK11
this talk
this talk (non-explicit)
1965
1975
1985
1995
2005
2015

Method: Gate Elimination

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

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

Outline

1. $3n - o(n)$ Lower Bound for Affine Dispersers
2. $3.01n$ Lower Bound for Affine Dispersers
3. (Conditional) $3.1n$ Lower Bound for "Quadratic" Dispersers

Function: Affine Dispersers

- A function $f \in \{0,1\}^n \to \{0,1\}$ 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 sublinear dimension $d = o(n)$ (e.g., [Ben-Sasson, Kopparty 2010]).

$3n - o(n)$ Lower Bound

Theorem 1 [DK11]

For a circuit C computing an A.D. for dimension d:

$$s(C) + i(C) \geq 4(n - d)\,,$$

where $i(C) = \#\text{inputs}$ and $s(C) = \#\text{gates}$.

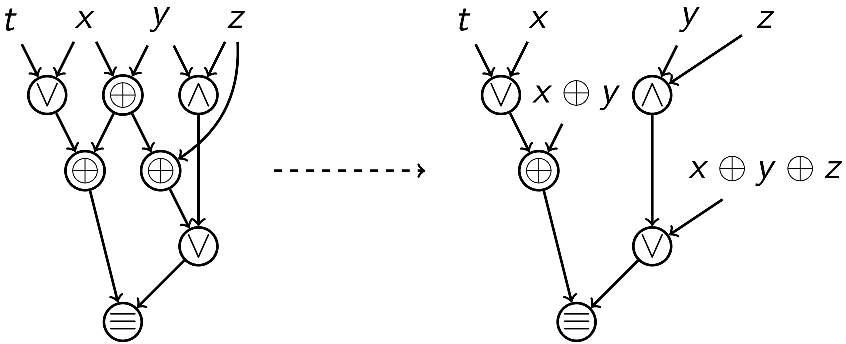
Corollary

$C(f) \geq 3n - o(n)$ for an A.D. for $d = o(n)$.

Observation

The bound is tight: $C(IP) = n - 1$ and IP is an A.D. for $d = n/2 + 1$.

XOR-layered Circuits



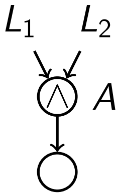
$n = 4$ inputs
$s = 7$ gates

$n = 6$ inputs
$s = 5$ gates

Proof

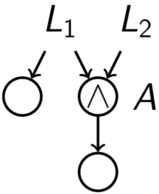
- Need to show that $s(C) + i(C) \geq 4(n - d)$.
- For this, make $n - d$ affine restrictions each time reducing $s + i$ by at least 4.
- Convert C to XOR-layered and take a top-gate A:

Case 1



$L_1 \leftarrow 0$:
$\Delta s = 2$
$\Delta i = 2$

Case 2



$L_1 \leftarrow 0$:
$\Delta s = 3$
$\Delta i = 1$

Outline

$3.01n$ Lower Bound

Theorem 2 [FGHK15]

The circuit complexity of an affine disperser for sublinear dimension is at least

$$\left(3 + \frac{1}{86}\right) n - o(n)\,.$$

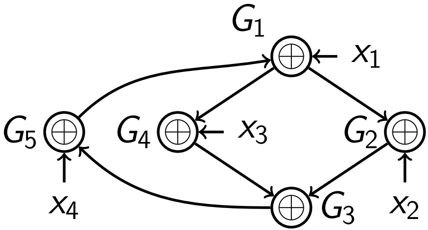
Main Ingredients of the Proof

Delayed linear substitutions: we make substitutions like $x_3 \leftarrow 0$, $x_5 \leftarrow x_7 \oplus x_{10} \oplus 1$, and $x_3 \leftarrow x_4 x_7$. For each quadratic substitution of the form $x_3 \leftarrow x_4 x_7$ we will later assign either x_4 or x_7 a constant making this quadratic substitution linear.

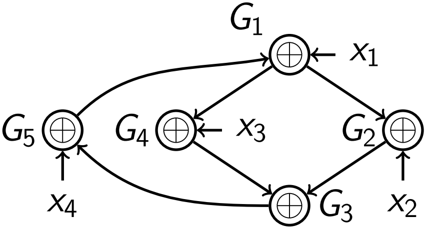
Cyclic circuits: for the induction to go through, we consider a more general model — circuits with cycles.

Circuit complexity measure: we use a carefully chosen circuit complexity measure to estimate the progress of gate elimination.

Cyclic Circuits

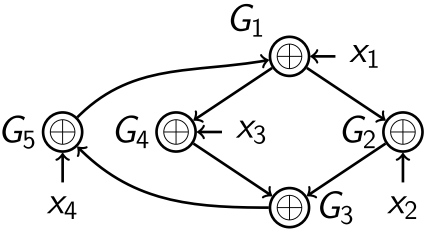


Cyclic Circuits



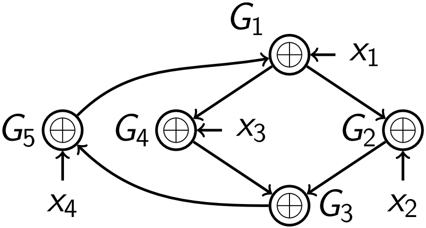
$$
\begin{aligned}
G_1 &= x_1 \oplus G_5 \\
G_2 &= x_2 \oplus G_1 \\
G_3 &= G_2 \oplus G_4 \\
G_4 &= x_3 \oplus G_1 \\
G_5 &= x_4 \oplus G_3
\end{aligned}
$$

Cyclic Circuits



$$
\begin{aligned}
G_1 &= x_1 \oplus G_5 \\
G_2 &= x_2 \oplus G_1 \\
G_3 &= G_2 \oplus G_4 \\
G_4 &= x_3 \oplus G_1 \\
G_5 &= x_4 \oplus G_3
\end{aligned}
\qquad
\begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} G_1 \\ G_2 \\ G_3 \\ G_4 \\ G_5 \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \\ 0 \\ x_3 \\ x_4 \end{bmatrix}
$$

Cyclic Circuits



$$
\begin{aligned}
G_1 &= x_1 \oplus x_2 \oplus x_3 \oplus x_4 \\
G_2 &= x_1 \oplus x_3 \oplus x_4 \\
G_3 &= x_2 \oplus x_3 \\
G_4 &= x_1 \oplus x_2 \oplus x_4 \\
G_5 &= x_2 \oplus x_3 \oplus x_4
\end{aligned}
$$

Circuit Complexity Measure

$$\mu = s + \frac{65}{43} \cdot q + \frac{1}{43} \cdot b + \frac{260}{43} \cdot i$$

where

- s is the number of gates
- q is the number of quadratic substitutions
- b is the number of “bottleneck” gates in the circuit
- i is the number of inputs

Outline

1. $3n - o(n)$ Lower Bound for Affine Dispersers
2. $3.01n$ Lower Bound for Affine Dispersers
3. (Conditional) $3.1n$ Lower Bound for "Quadratic" Dispersers

From Affine to Quadratic Dispersers

Theorem 3 [GK15]

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

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

Then

$$C(f) \geq 3.1n\,.$$

Open problem

Explicit construction of such f (even in NP, even with $o(n)$ outputs).