Boolean Circuit Size

Alexander S. Kulikov
Steklov Mathematical Institute at St. Petersburg

June 1, 2019, ECCO

Computing Boolean Functions

Computing (or representing) a Boolean function

$$f(x_1, x_2, x_3)\colon \{0,1\}^3 \to \{0,1\}$$

Computing Boolean Functions

Computing (or representing) a Boolean function

$$f(x_1, x_2, x_3)\colon \{0,1\}^3 \to \{0,1\}$$

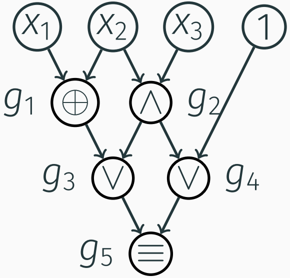
$$\begin{aligned}
g_1 &= x_1 \oplus x_2 \\
g_2 &= x_2 \wedge x_3 \\
g_3 &= g_1 \vee g_2 \\
g_4 &= g_2 \vee 1 \\
g_5 &= g_3 \equiv g_4
\end{aligned}$$

Computing Boolean Functions

Computing (or representing) a Boolean function

$$f(x_1, x_2, x_3)\colon \{0,1\}^3 \to \{0,1\}$$

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



Fundamental Question

Given a Boolean function $f\colon \{0,1\}^n \to \{0,1\}$, what is the minimum number of gates needed to compute f?

Fundamental Question

Given a Boolean function $f\colon \{0,1\}^n \to \{0,1\}$, what is the minimum number of gates needed to compute f?

Does there exist an infinite sequence of functions $f_1, f_2, \ldots$ such that f_n has n inputs, $\bigcup_{i=1}^{\infty} f^{-1}(1) \in \mathrm{NP}$, and f_n requires $\mathsf{superpoly}(n)$ gates? (This would mean that $\mathrm{P} \neq \mathrm{NP}$.)

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].

Outline

Upper Bounds: known upper bounds for some basic functions, using SAT-solvers for circuit synthesis.

Lower Bounds: overview of known lower bounds and approaches for proving them.

1. Upper Bounds

Computing the Sum Function

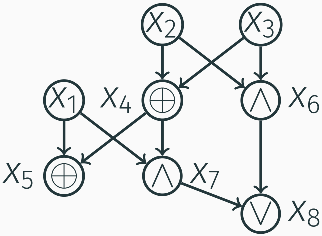
Let SUM_n be a Boolean function with n inputs and $\lceil \log_2(n+1) \rceil$ outputs that computes the binary representation of the sum of n input bits

Computing the Sum Function

Let SUM_n be a Boolean function with n inputs and $\lceil \log_2(n+1) \rceil$ outputs that computes the binary representation of the sum of n input bits

Computing $\mathsf{SUM}_3(x_1, x_2, x_3)$:

$$x_4 = x_2 \oplus x_3$$
$$x_5 = x_1 \oplus x_4$$
$$x_6 = x_2 \wedge x_3$$
$$x_7 = x_1 \wedge x_4$$
$$x_8 = x_6 \vee x_7$$



Is There a Smaller Circuit?

- It can be verified using SAT-solvers that there is no smaller circuit
- Roughly, one translates a statement “there exists a circuit with four gates computing a function with the given truth table” to CNF-SAT and then uses SAT-solvers to show that the resulting formula is unsatisfiable

State of the Art

- Modern SAT-solvers are able to find circuits of size around 10–12
- Proving that there is no circuit of size 12 is already a difficult task to the state-of-the-art SAT-solvers
- Implementations:
    - `github.com/alexanderskulikov/circuit-synthesis`
    - `www-cs-faculty.stanford.edu/~knuth/programs.html`

Why should we care about $n \leq 7$?

Practice: We are interested in much larger values of n — say, $n = 1024$ (also, in practice, we should take into account other parameters of a circuit like its depth, area, etc)

Why should we care about $n \leq 7$?

Practice: We are interested in much larger values of n — say, $n = 1024$ (also, in practice, we should take into account other parameters of a circuit like its depth, area, etc)

Theory: We are interested in upper bounds w.r.t. all n rather than some $n = O(1)$

First Reason: Guaranteed Improvement

For some families of functions $\{f_n\}_{n=0}^{\infty}$, proving an upper bound on $\mathsf{gates}(f_n)$ for $n = O(1)$ automatically translates into an upper bound on $\mathsf{gates}(f_n)$ for all n

This is usually because a circuit for f_n can be constructed naturally from constant size blocks

Examples

$$\mathrm{gates}(\mathrm{SUM}_3) \leq 5 \Rightarrow \mathrm{gates}(\mathrm{SUM}_n) \leq 5n$$

Examples

$$\text{gates}(\text{SUM}_3) \leq 5 \Rightarrow \text{gates}(\text{SUM}_n) \leq 5n$$

$$\text{gates}(\text{SUM}_7) \leq 19 \Rightarrow \text{gates}(\text{SUM}_n) \leq 4.75n$$

Examples

$\text{gates}(\text{SUM}_3) \leq 5 \Rightarrow \text{gates}(\text{SUM}_n) \leq 5n$

$\text{gates}(\text{SUM}_7) \leq 19 \Rightarrow \text{gates}(\text{SUM}_n) \leq 4.75n$

Record: $\text{gates}(\text{SUM}_n) \leq 4.5n$

Second Reason: Potential Improvement

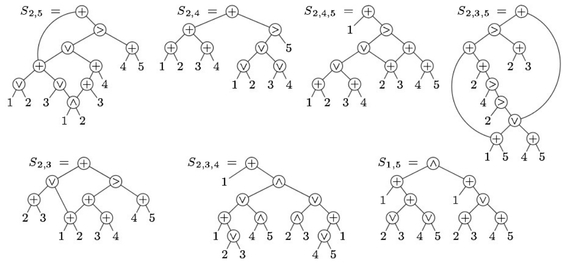
For some families of functions $\{f_n\}_{n=0}^{\infty}$, knowing good upper bounds on $\mathsf{gates}(f_n)$ for small values of n may help us to improve known upper bounds for all n

Encyclopedia of Minimum Circuits

"Our knowledge of Boolean circuit complexity is quite poor. [...] One good reason why we don't know much about the true power of circuits is that we don't have many examples of minimum circuits. We don't know, for example, what an optimal circuit for 3×3 Boolean matrix multiplication looks like. It is possible that we could make progress in understanding circuits by cataloging the smallest circuits we know for basic functions, on small input sizes (such as $n = 1, \ldots, 10$)."

Ryan Williams, Applying Practice to Theory

Small Circuits



"Some of them are astonishingly beautiful; some of them are beautifully simple; and others are simply astonishing."

Donald E. Knuth
The Art of Computer Programming, Volume 4

Open Problems

- The state-of-the-art SAT-solvers are not able to answer the following questions. Can other solvers help?
  - $\text{gates}([x_1 + \cdots + x_6 \equiv 1 \bmod 3]) < 13$?
  - $\text{gates}(\text{SUM}_7) \leq 17$? $\text{gates}(\text{SUM}_{15}) \leq 49$?

Open Problems

- The state-of-the-art SAT-solvers are not able to answer the following questions. Can other solvers help?
    - gates($[x_1 + \cdots + x_6 \equiv 1 \bmod 3]$) < 13?
    - gates(SUM_7) ≤ 17? gates(SUM_{15}) ≤ 49?
- Other approaches? E.g., local search, ILP, branch-and-bound, gradient descent

2. Lower Bounds

Explicit Lower Bounds

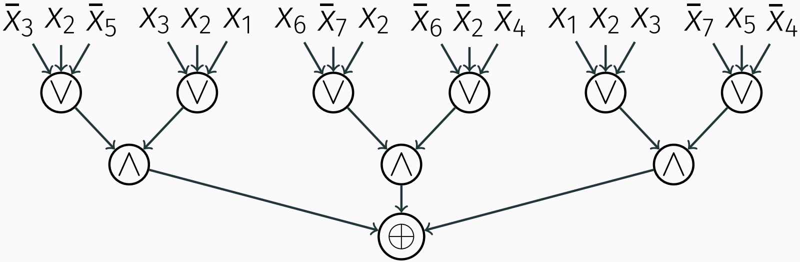
The lower bound $\Omega(2^n/n)$ by Shannon is non-constructive: it does not give an explicit function (i.e., a function from NP) with superpolynomial circuit size.

Explicit Lower Bounds

The lower bound $\Omega(2^n/n)$ by Shannon is non-constructive: it does not give an explicit function (i.e., a function from NP) with superpolynomial circuit size.

What can we prove for explicit functions? What about restricted circuit classes?

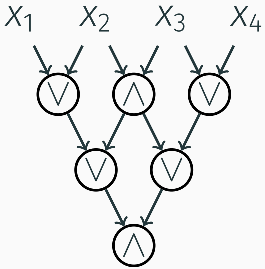
Restricted classes: constant depth circuits



- depth: constant, fan-in: unbounded
- exponential lower bounds: switching lemma [A83, FSS84, Y85, H86, R95], approximating polynomials [RS87]

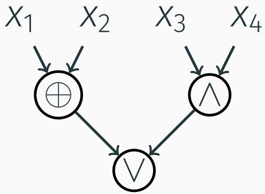
Restricted classes: monotone circuits

- fanin: 2
  fanout: unbounded
  operations: $\{\wedge, \vee\}$
- exponential lower bounds: method of approximations [R85, A85, AB87]



Restricted classes: formulas

- fanin: 2, fanout: 1
- n^2, n^3 lower bounds: random restrictions, universal functions, formal complexity measures [S61, N66, K71, A85, IN93, PZ93, H98]



Explicit Lower Bounds

Restricted classes

lower bounds:
n^3, $2^{n^{1/8}}$, $2^{n-o(n)}$

many beautiful techniques are known

Explicit Lower Bounds

Restricted classes

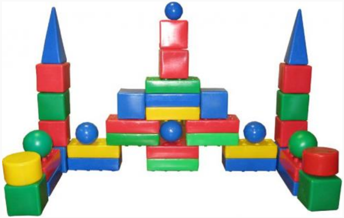
lower bounds:
n^3, $2^{n^{1/8}}$, $2^{n-o(n)}$

many beautiful techniques are known

General circuits

lower bounds:
$2n$, $2.5n$, $3n$

just one simple technique is known



Explicit Lower Bounds for General Circuits

Previous

$2n$	$f(x) = \bigoplus_{i<j} x_i x_j$	[KM 1965]
$2n$	$f(x) = [\sum x_i \geq 2]$	[S 1974]
$2.5n$	$f(x, a, b) = x_a \oplus x_b$	[P 1977]
$2.5n$	symmetric	[S 1977]
$3n$	$f(x, a, b, c) = x_a x_b \oplus x_c$	[B 1984]
$3n$	affine dispersers	[DK 2011]

Explicit Lower Bounds for General Circuits

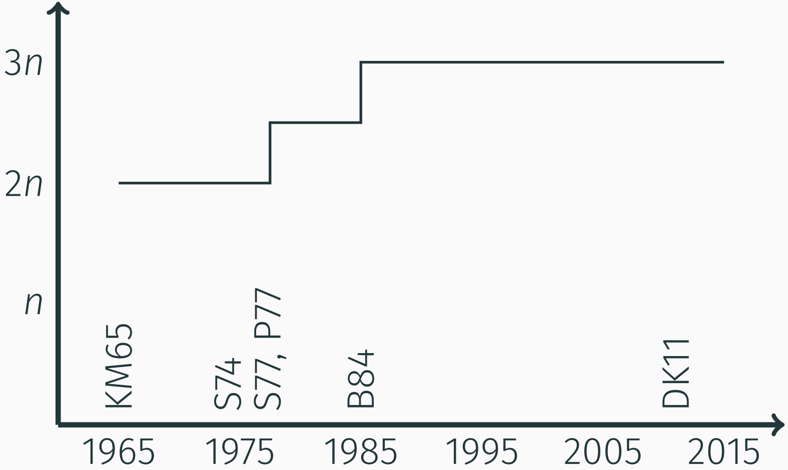
Previous

$2n$	$f(x) = \bigoplus_{i<j} x_i x_j$	[KM 1965]
$2n$	$f(x) = [\sum x_i \geq 2]$	[S 1974]
$2.5n$	$f(x, a, b) = x_a \oplus x_b$	[P 1977]
$2.5n$	symmetric	[S 1977]
$3n$	$f(x, a, b, c) = x_a x_b \oplus x_c$	[B 1984]
$3n$	affine dispersers	[DK 2011]

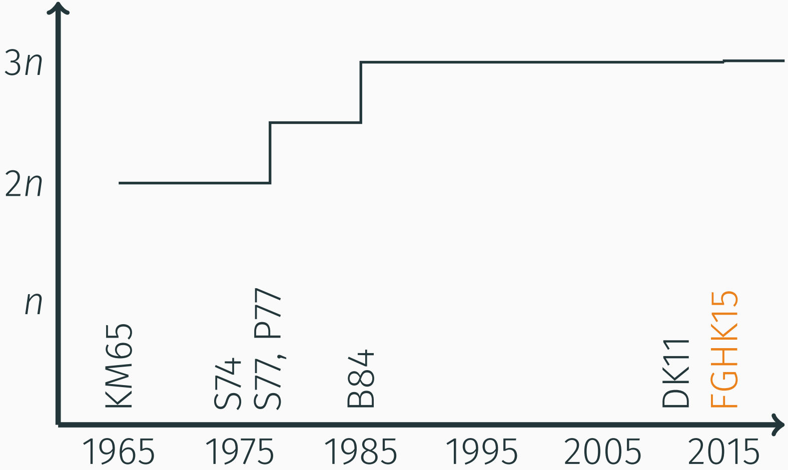
New

$(3 + 1/86)n$	affine dispersers	[FGHK 2015]

Explicit Lower Bounds: Pictorially



Explicit Lower Bounds: Pictorially



Quote

“This may seem quite depressing. It is.”

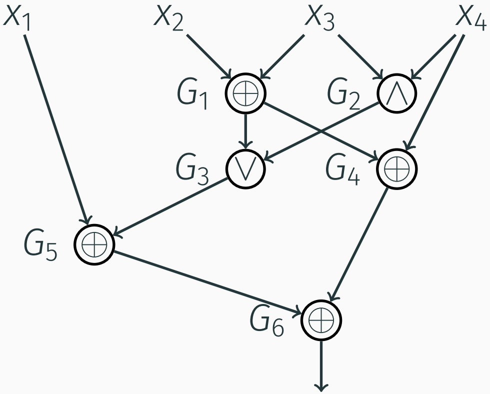
Saxena, Seshadhri, 2010. From Sylvester–Gallai Configurations to Rank Bounds: Improved Blackbox Identity Test for Depth-3 Circuits

Gate Elimination Method

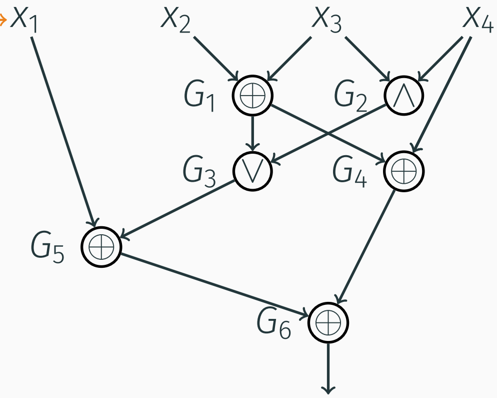
To prove, say, a $3n$ lower bound for all functions f from a certain class $\mathcal{F}$:

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

Gate Elimination: Example

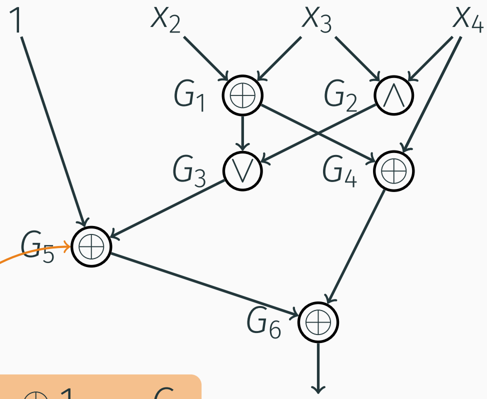


Gate Elimination: Example



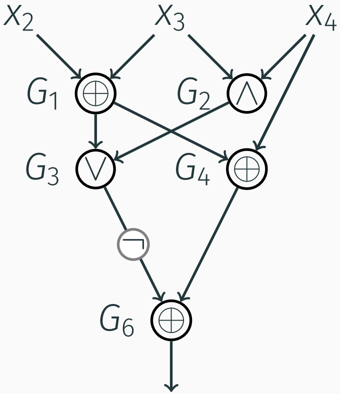
assign $x_1 = 1$

Gate Elimination: Example

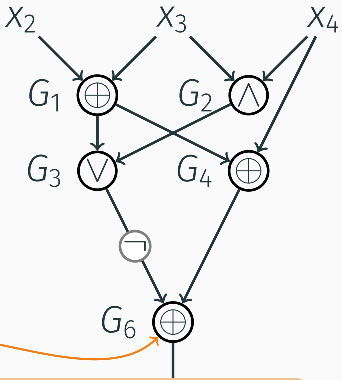


G_5 now computes $G_3 \oplus 1 = \neg G_3$

Gate Elimination: Example

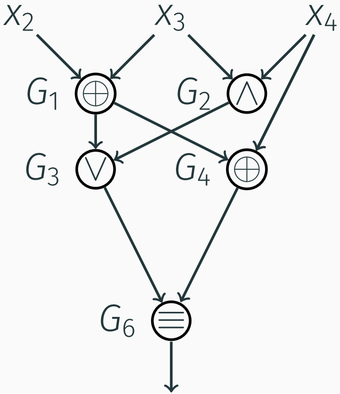


Gate Elimination: Example

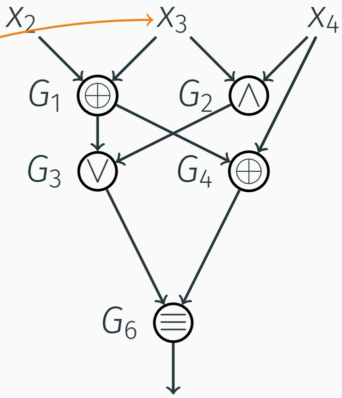


now we can change the binary function assigned to G_6

Gate Elimination: Example

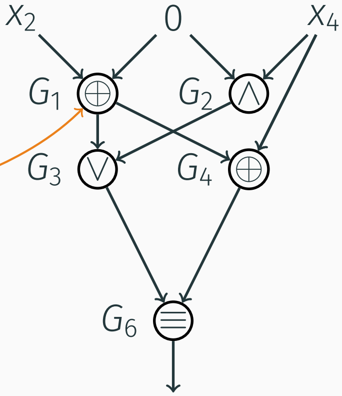


Gate Elimination: Example



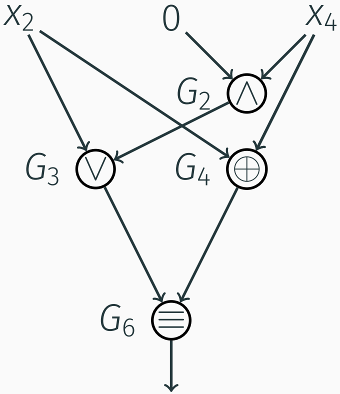
now assign $x_3 = 0$

Gate Elimination: Example

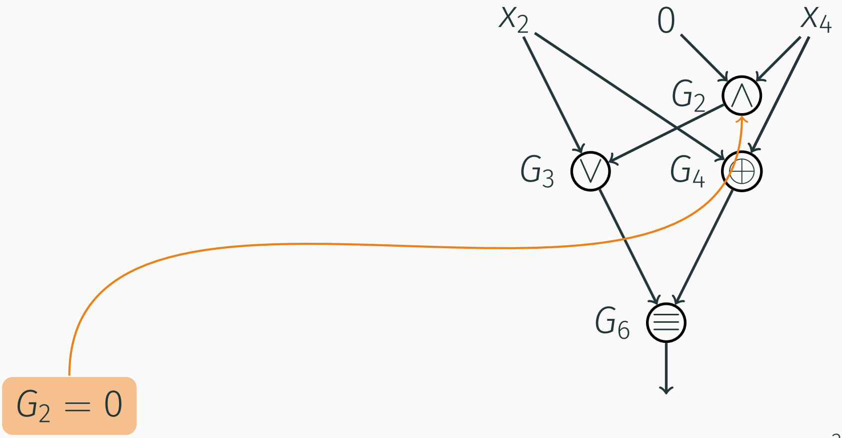


G_1 then is equal to x_2

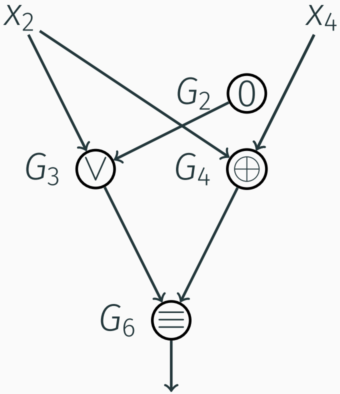
Gate Elimination: Example



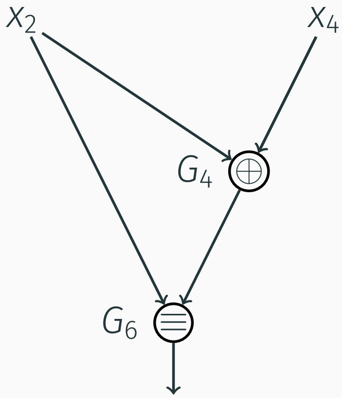
Gate Elimination: Example



Gate Elimination: Example



Gate Elimination: Example



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.

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 $n-d$ affine restrictions (i.e., restrictions of the form $x_2 \oplus x_3 \oplus x_9 = 0$).

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 $n - d$ affine restrictions (i.e., restrictions 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]).

Lower Bound

Theorem (DK11)

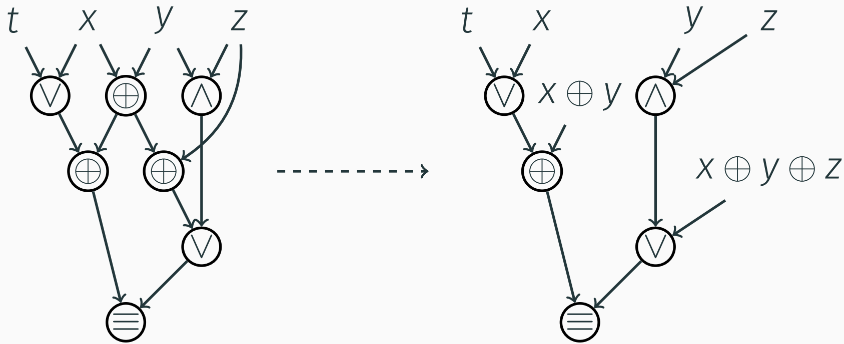
If $f\colon \{0,1\}^n \to \{0,1\}$ *is an affine disperser for dimension* $d = o(n)$*, then*

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

Proof Idea

Make $n - o(n)$ substitutions each time eliminating at least three gates.

XOR-layered Circuits



$\text{inputs}(C) = 4$

$\text{gates}(C) = 7$

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

$\text{gates}(C') = 5$

$$\text{inputs}(C) + \text{gates}(C) \geq \text{inputs}(C') + \text{gates}(C').$$

$3n - o(n)$ Lower Bound

Lemma

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

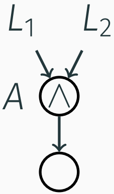
$$\mathrm{inputs}(C) + \mathrm{gates}(C) \geq 4(n - d)\,.$$

Corollary

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

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

Case 1

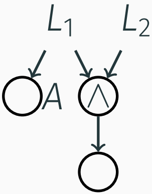


$L_1 \leftarrow 0$:

$\Delta\,\mathsf{gates} = 2$

$\Delta\,\mathsf{inputs} = 2$

Case 2



$L_1 \leftarrow 0$:

$\Delta\,\mathsf{gates} = 3$

$\Delta\,\mathsf{inputs} = 1$

3. Open Problems

New Methods

- It is very unlikely that the gate elimination method will lead to non-linear or, say, $10n$ lower bounds: it tries to argue about a circuit by looking at its top part.
- "Global" properties of circuits?
- Mass production effect?

Affine Dispersers

Do there exist affine dispersers of linear circuit size?

$2n$	$f(x) = \bigoplus_{i<j} x_i x_j$	[KM 1965]
$2n$	$f(x) = [\sum x_i \geq 2]$	[S 1974]
$2.5n$	$f(x, a, b) = x_a \oplus x_b$	[P 1977]
$2.5n$	symmetric	[S 1977]
$3n$	$f(x, a, b, c) = x_a x_b \oplus x_c$	[B 1984]
$3n$	affine dispersers	[DK 2011]

Affine Dispersers

Do there exist affine dispersers of linear circuit size?

$2n$	$f(x) = \bigoplus_{i<j} x_i x_j$	$2.5n$
$2n$	$f(x) = [\sum x_i \geq 2]$	$2.5n$
$2.5n$	$f(x, a, b) = x_a \oplus x_b$	4n
$2.5n$	symmetric	$2.5n$
$3n$	$f(x, a, b, c) = x_a x_b \oplus x_c$	$6n$
$3n$	affine dispersers	$O(n^3)$

Annoying Gaps for Symmetric Functions

- $2.5n \leq C(x_1 + x_2 + \cdots + x_n) \leq 4.5n$
- $2n \leq C(AND, OR, XOR) \leq 2.5n$
- $2.5n \leq C(x_1 + x_2 + \cdots + x_n \equiv_3 0) \leq 3n$
- $2n \leq C(x_1 + x_2 + \cdots + x_n \geq 3) \leq 3n$

Summary of Open Problems

- New approaches (heuristics) for circuit synthesis
- New approaches for circuit lower bounds
- Affine dispersers of linear circuit size?
- Annoying gaps:
    - $2.5n \leq C(x_1 + x_2 + \cdots + x_n) \leq 4.5n$
    - $2n \leq C(AND, OR, XOR) \leq 2.5n$
    - $2.5n \leq C(x_1 + x_2 + \cdots + x_n \equiv_3 0) \leq 3n$
    - $2n \leq C(x_1 + x_2 + \cdots + x_n \geq 3) \leq 3n$

Thank you for your attention!