Generalizations of the Gate Elimination Method

Alexander Golovnev
New York University

Joint work with:

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

New York University
March 22, 2016

Gate Elimination

Dispersers

Lower Bounds for Affine Dispersers

Lower Bound for Quadratic Dispersers

Open Problems

Outline

Gate Elimination

Dispersers

Lower Bounds for Affine Dispersers

Lower Bound for Quadratic Dispersers

Open Problems

Boolean Circuits

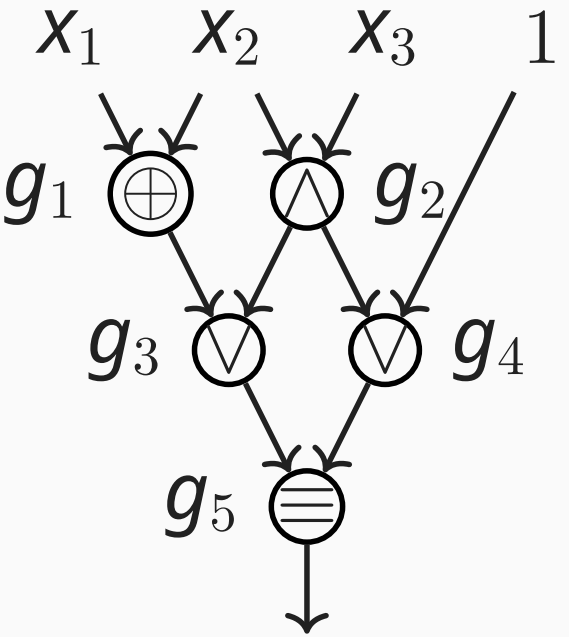
Inputs:
$x_1, \ldots, x_n, 0, 1$

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

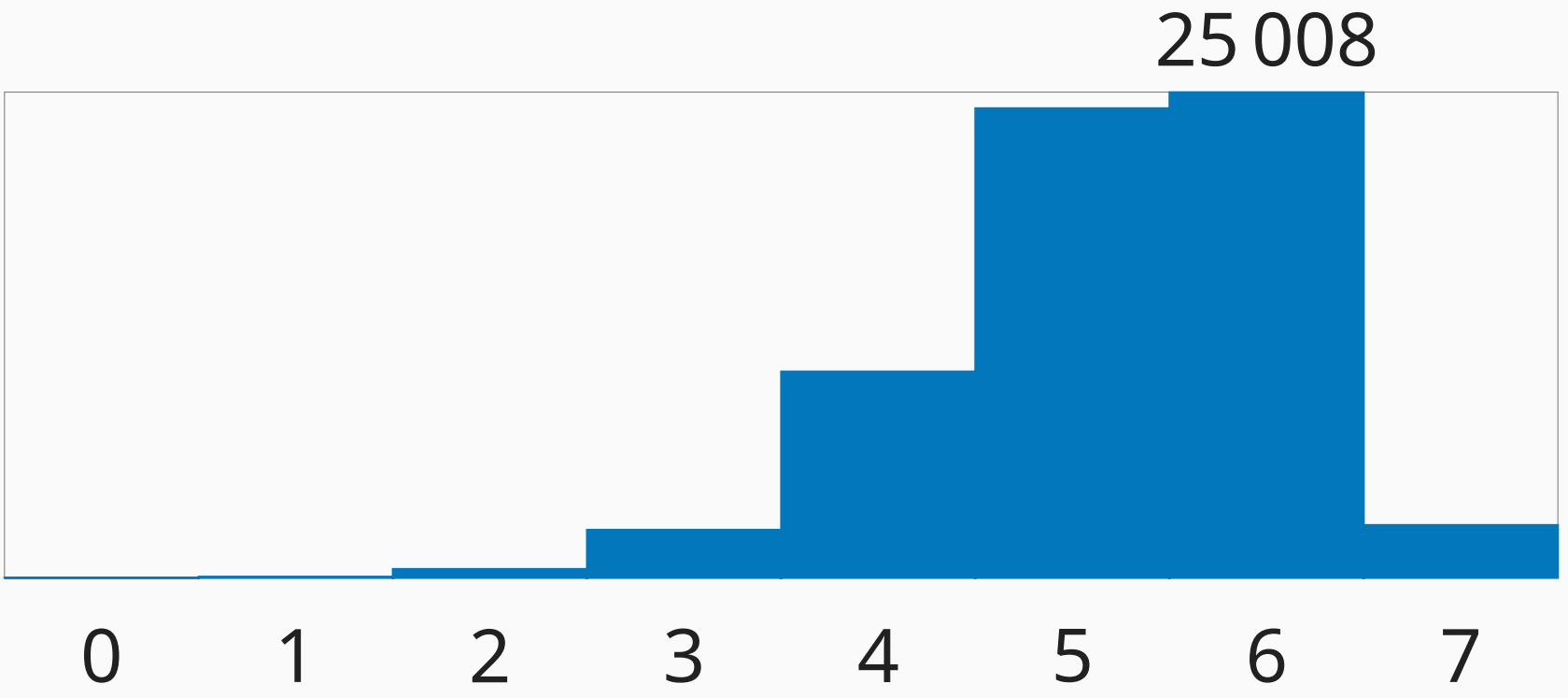
Lower Bound

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

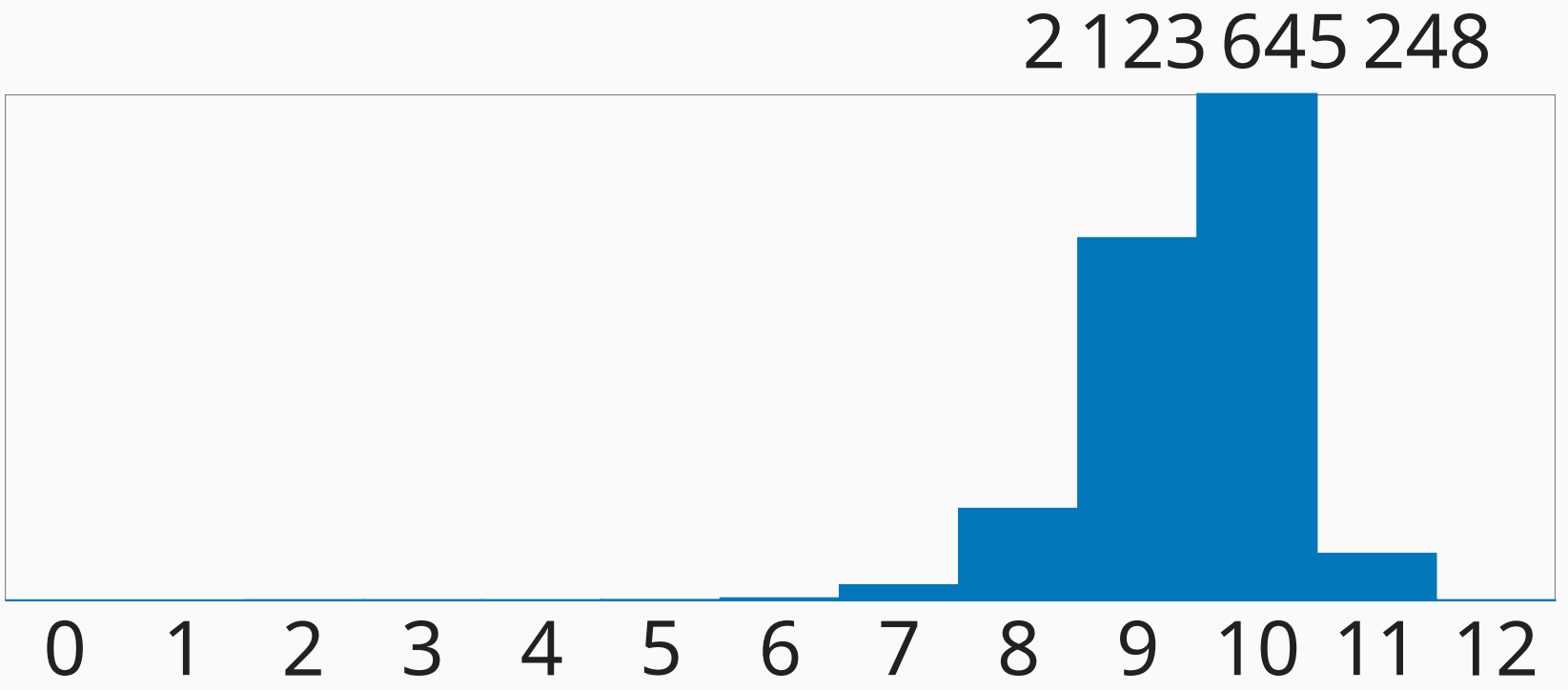
Upper Bound

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

Distribution: $n = 4$



Distribution: $n = 5$



Explicit Lower Bounds

Previous

$2n$	$f(x) = \sum_{i<j} x_i x_j$	[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, Kulikov 2011]

Explicit Lower Bounds

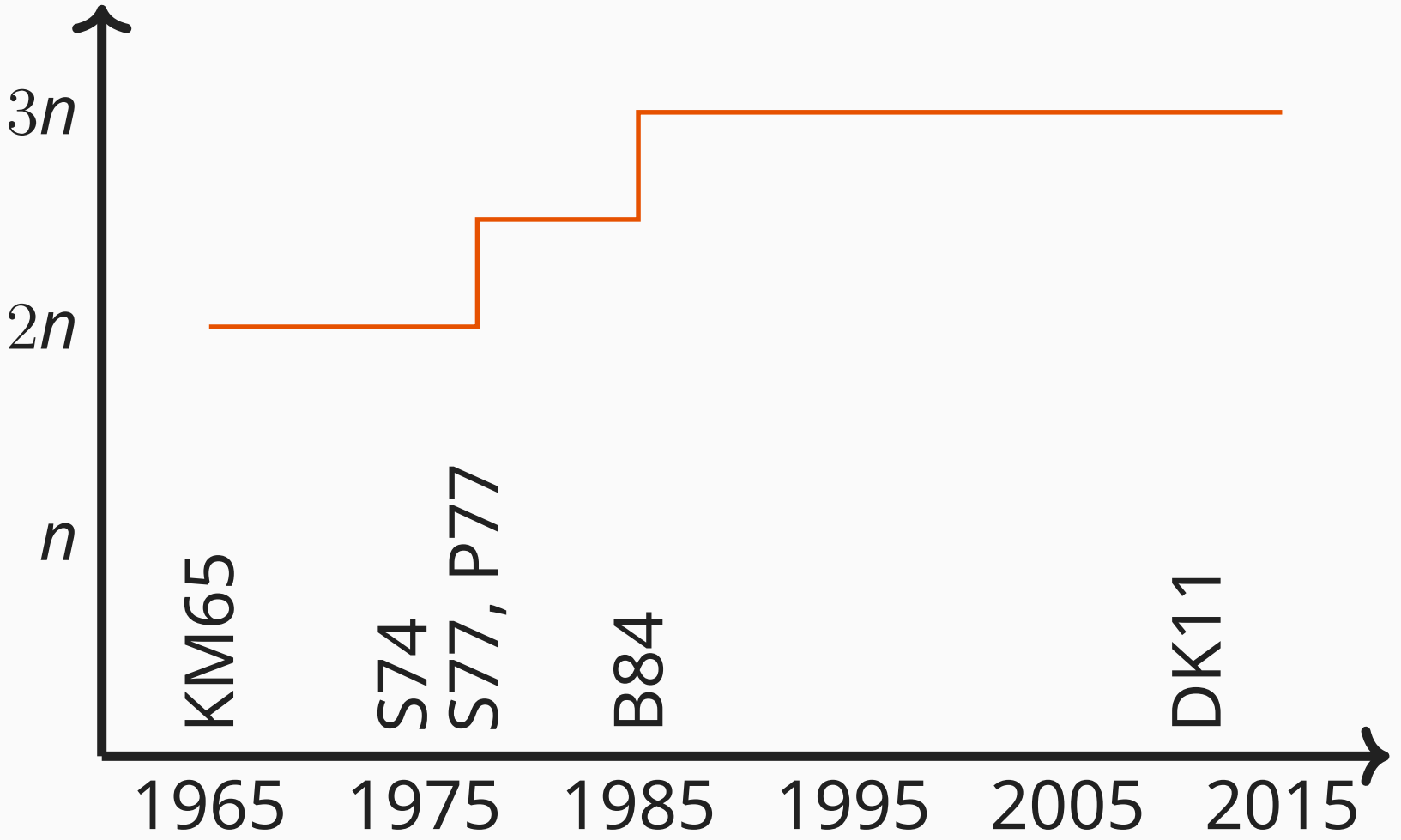
Previous

$2n$	$f(x) = \sum_{i<j} x_i x_j$	[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, Kulikov 2011]

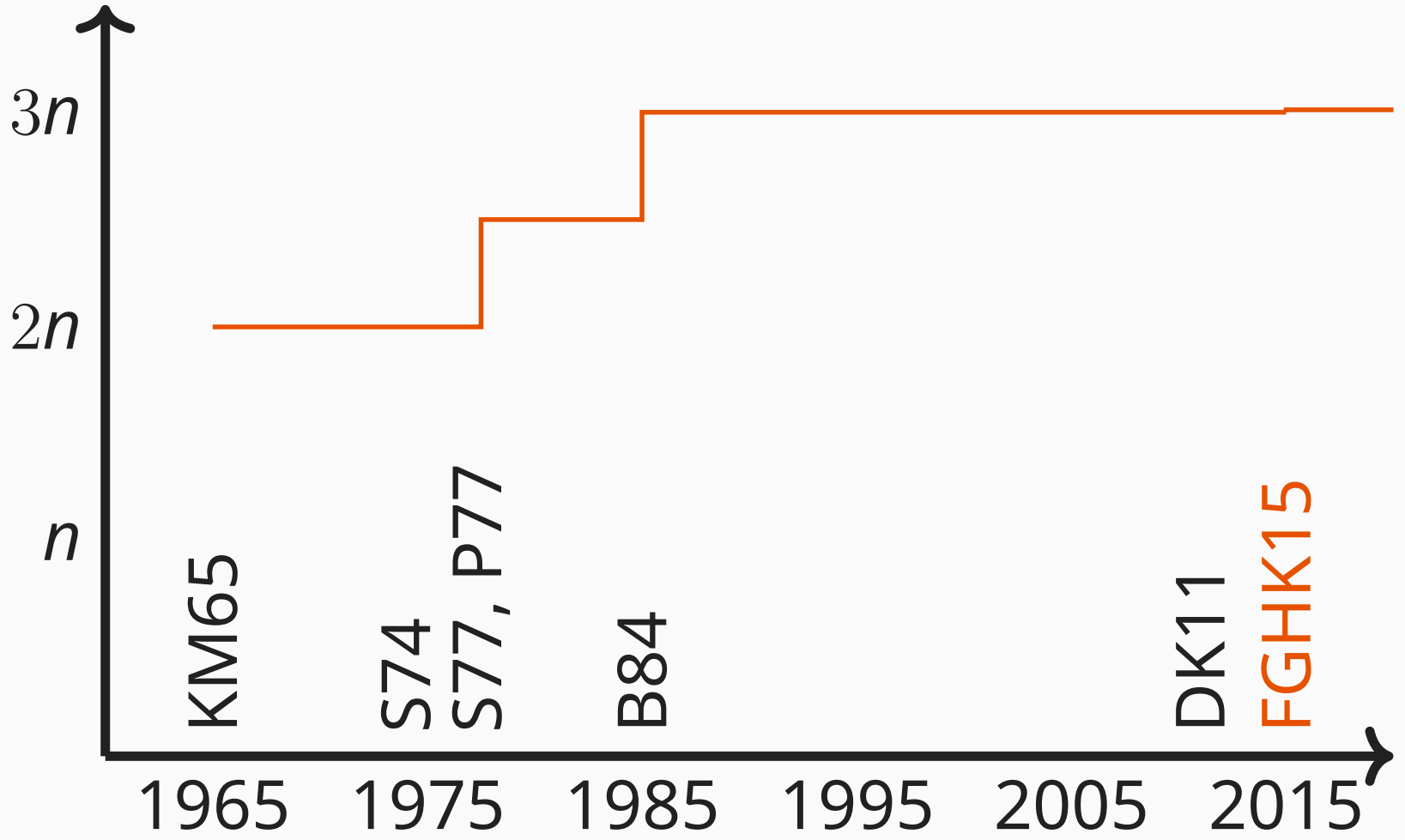
New

$3.011n$	affine dispersers	[FGHK 2015]
$3.11n$	quadratic dispersers (non-explicit)	[G, Kulikov 2015]

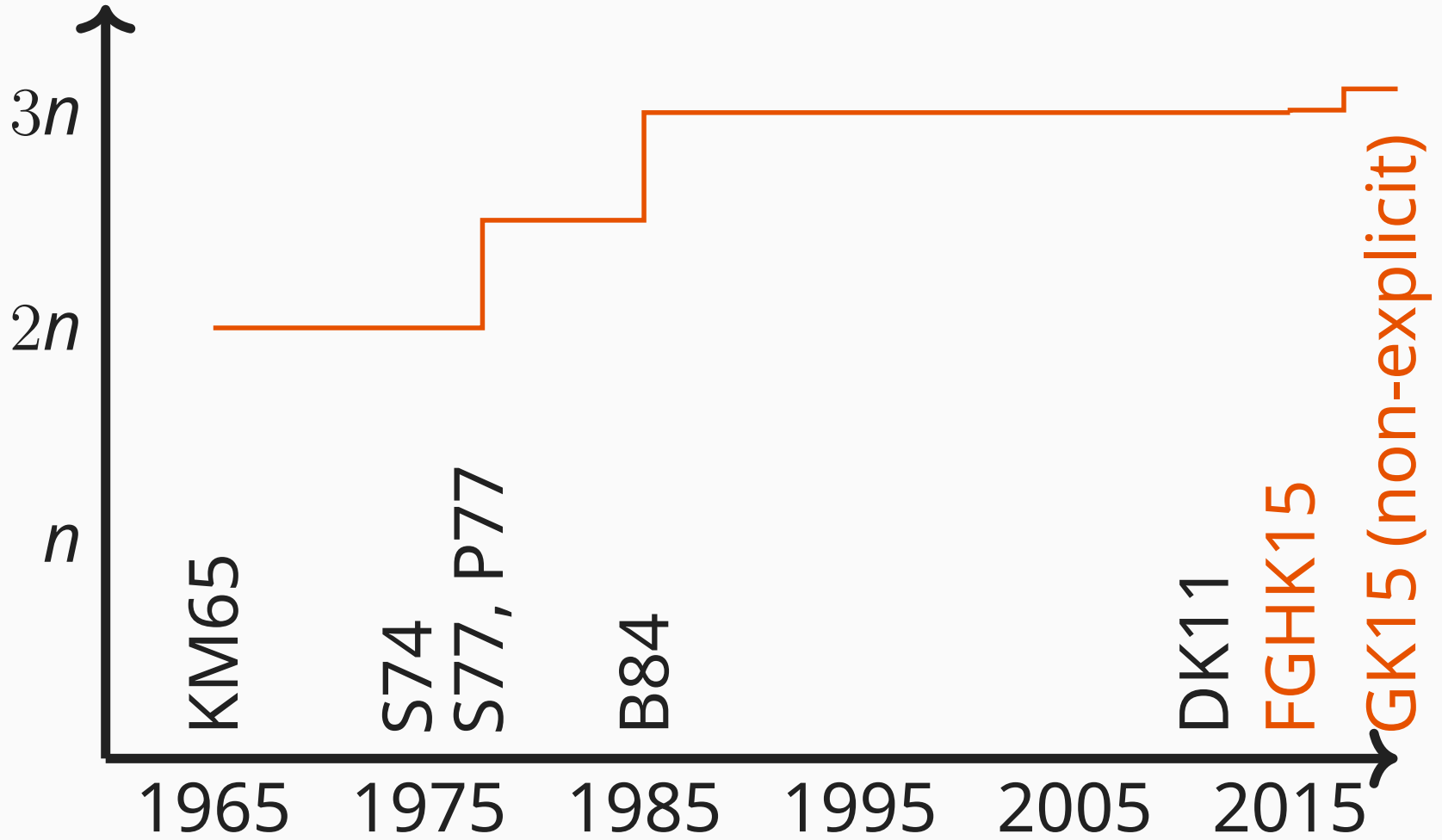
Explicit Lower Bounds: Pictorially



Explicit Lower Bounds: Pictorially



Explicit Lower Bounds: Pictorially

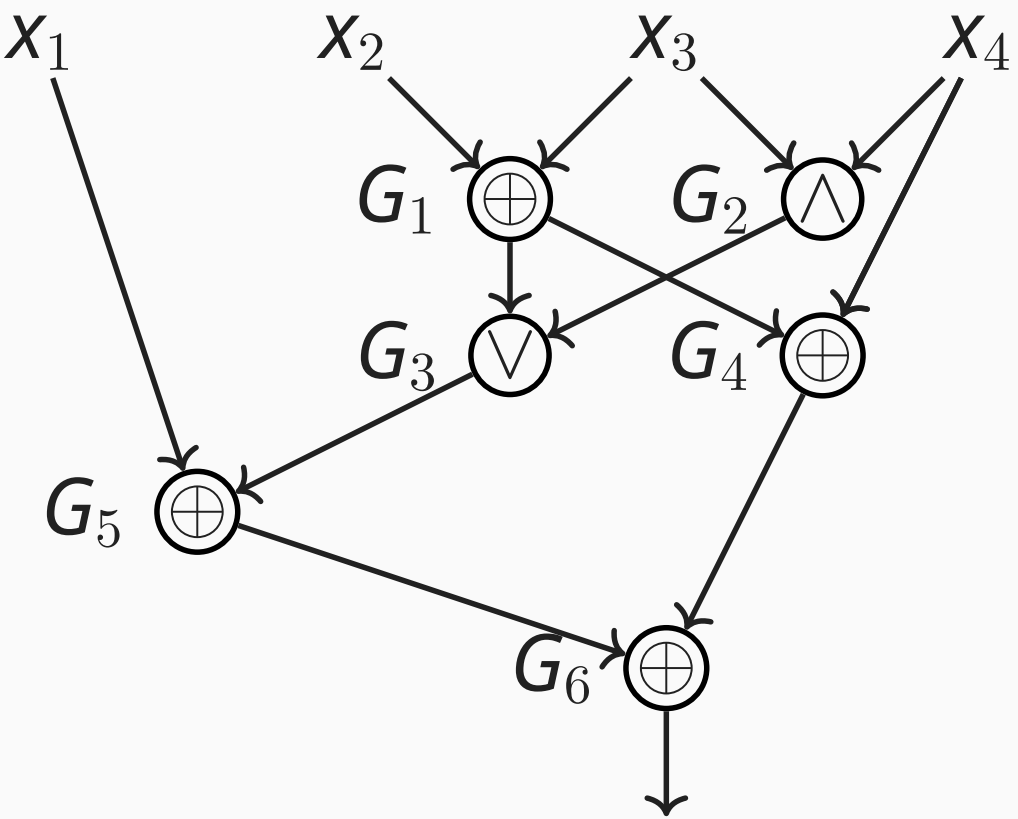


Gate Elimination Method

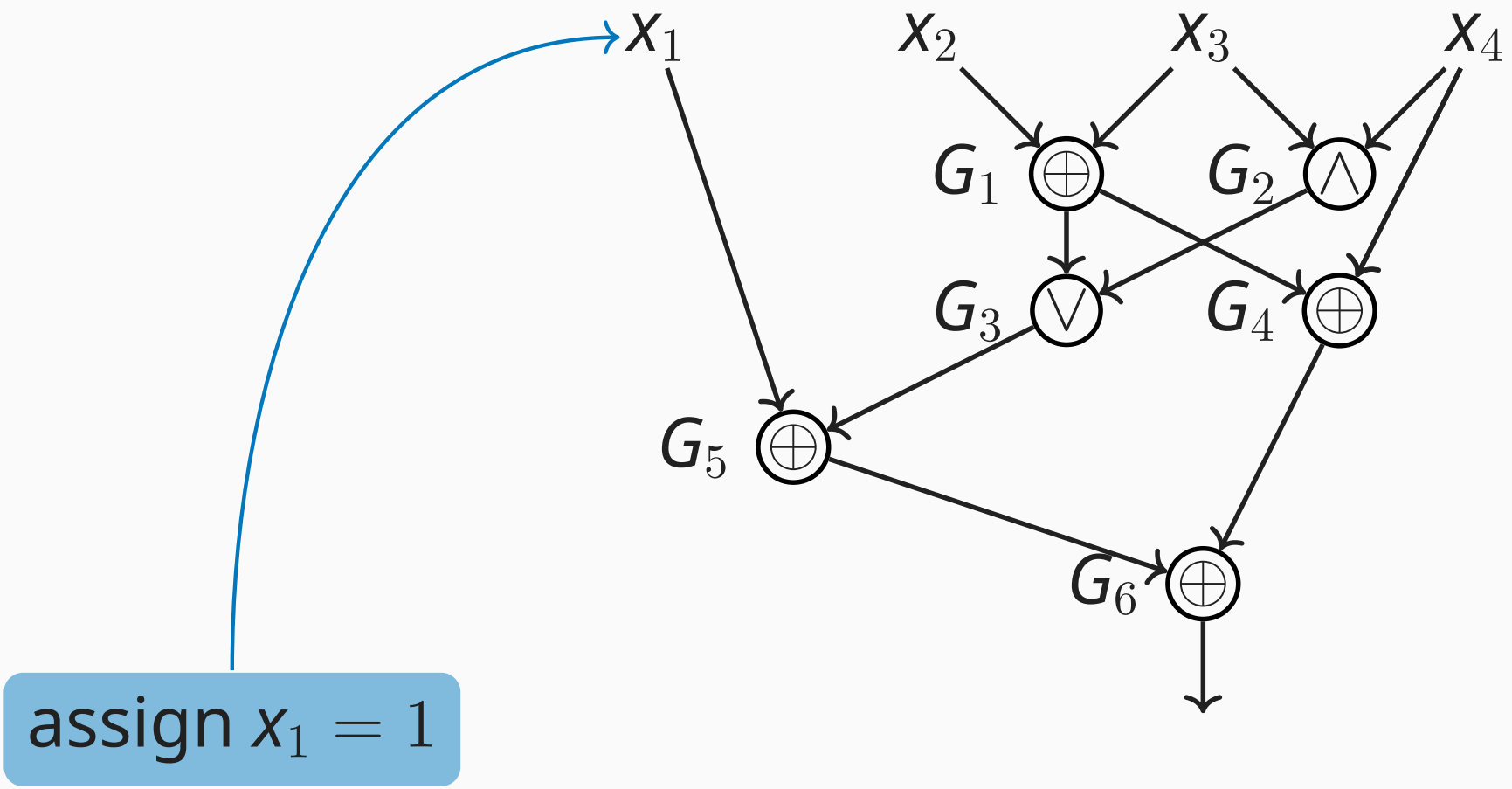
To prove, say, a $3n$ lower bound for all functions f from a certain class $\mathcal{C}$:

- 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.

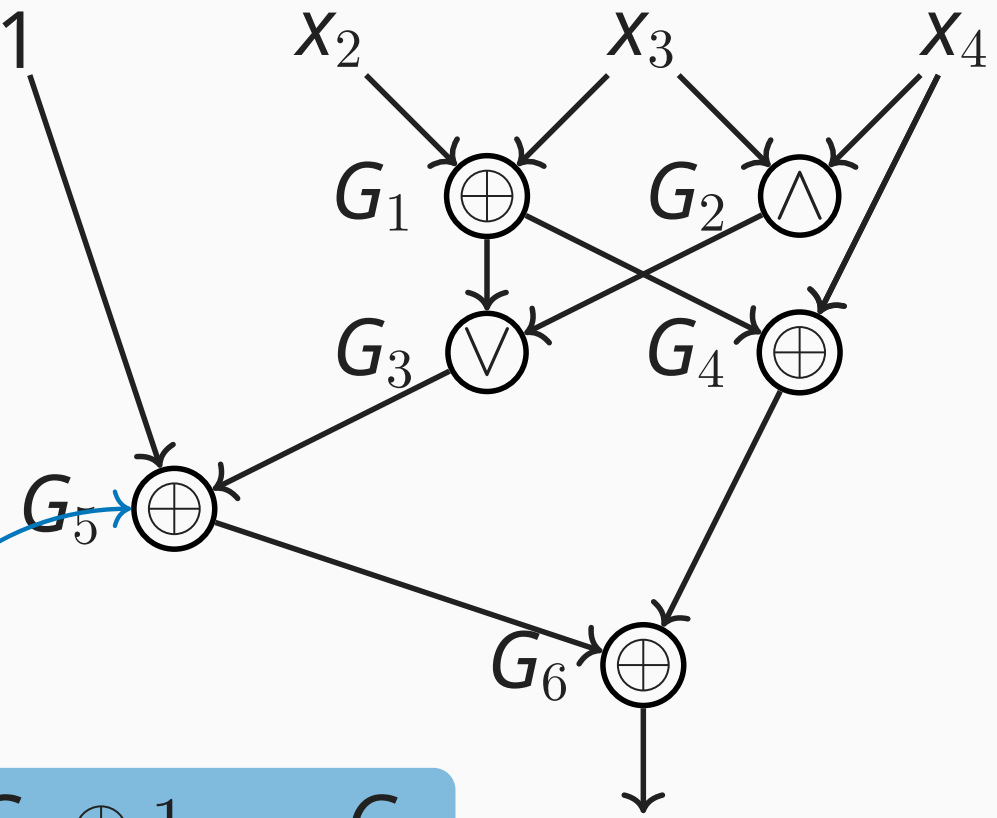
Gate Elimination: Example



Gate Elimination: Example

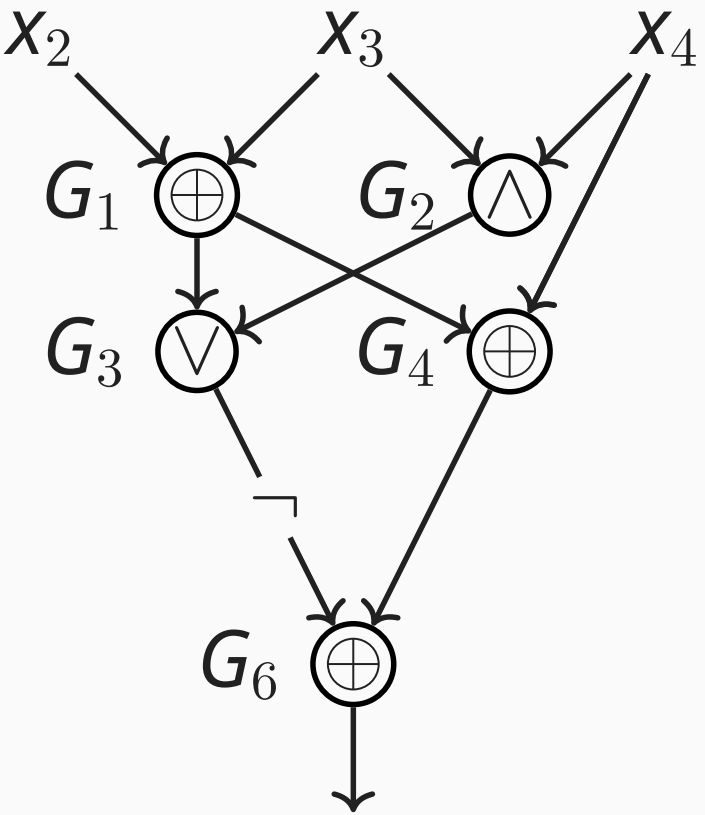


Gate Elimination: Example

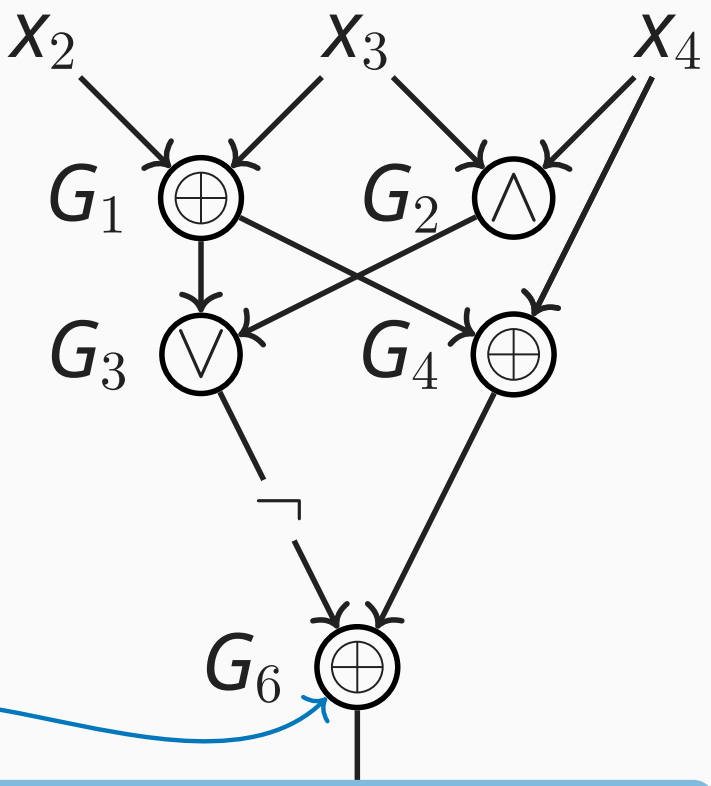


G_5 now computes $G_3 \oplus 1 = \neg G_3$

Gate Elimination: Example

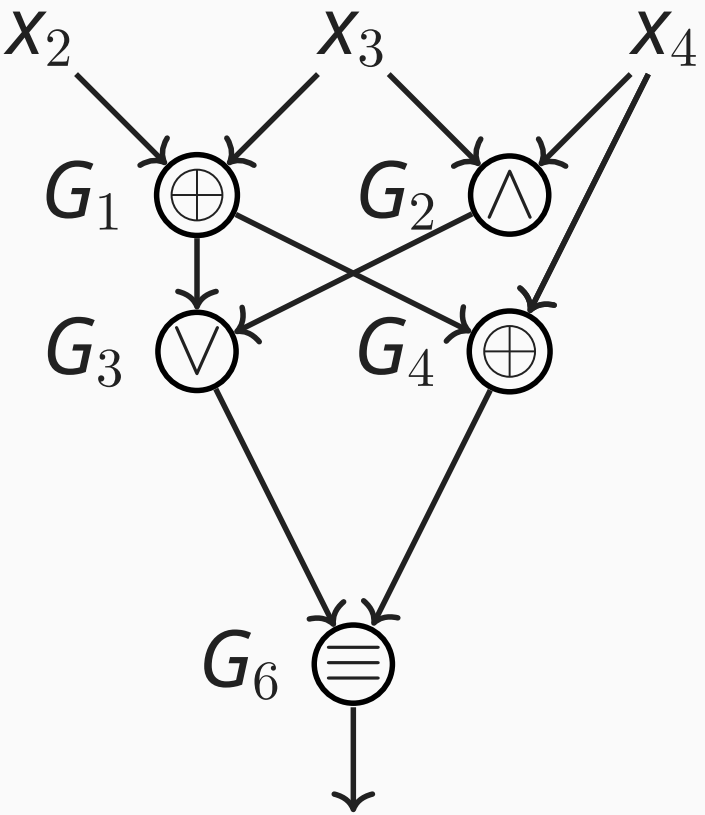


Gate Elimination: Example

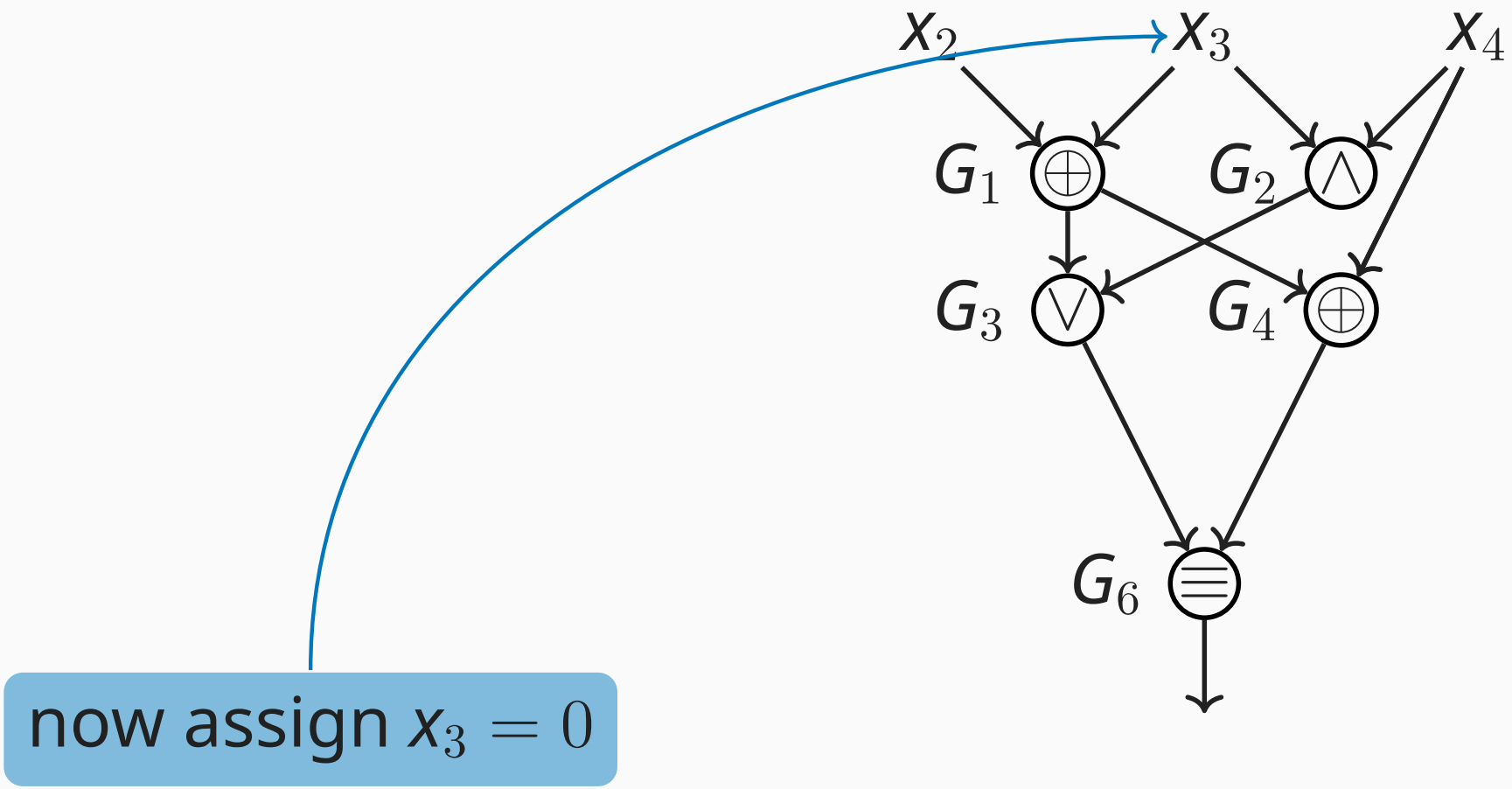


now we can change the binary function assigned to G_6

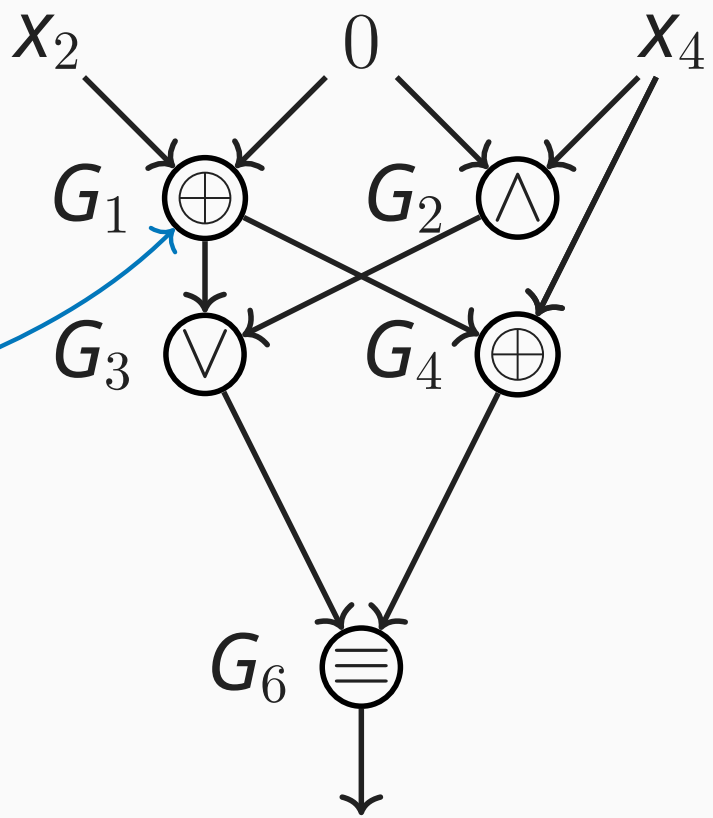
Gate Elimination: Example



Gate Elimination: Example

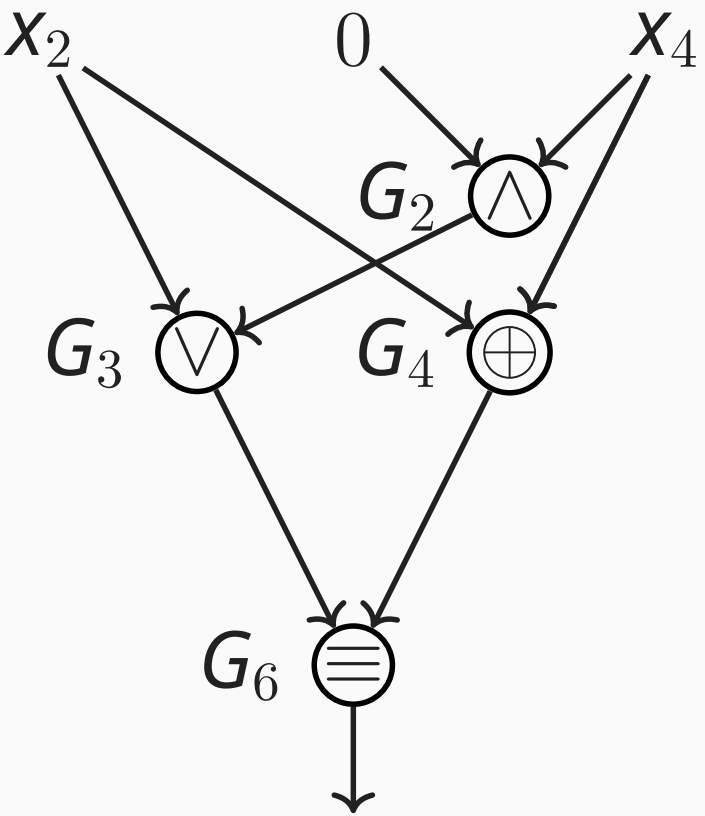


Gate Elimination: Example

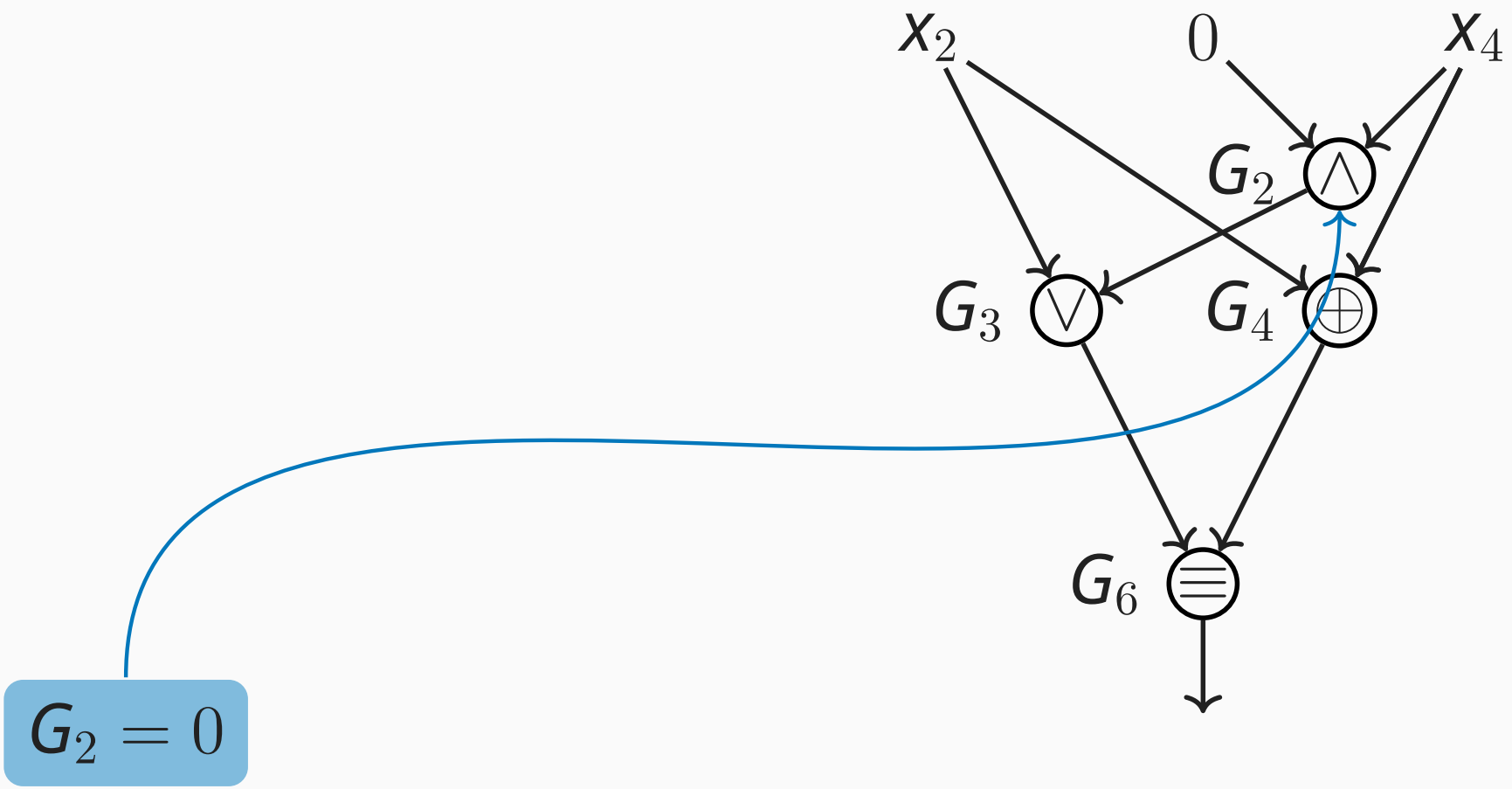


G_1 then is equal to x_2

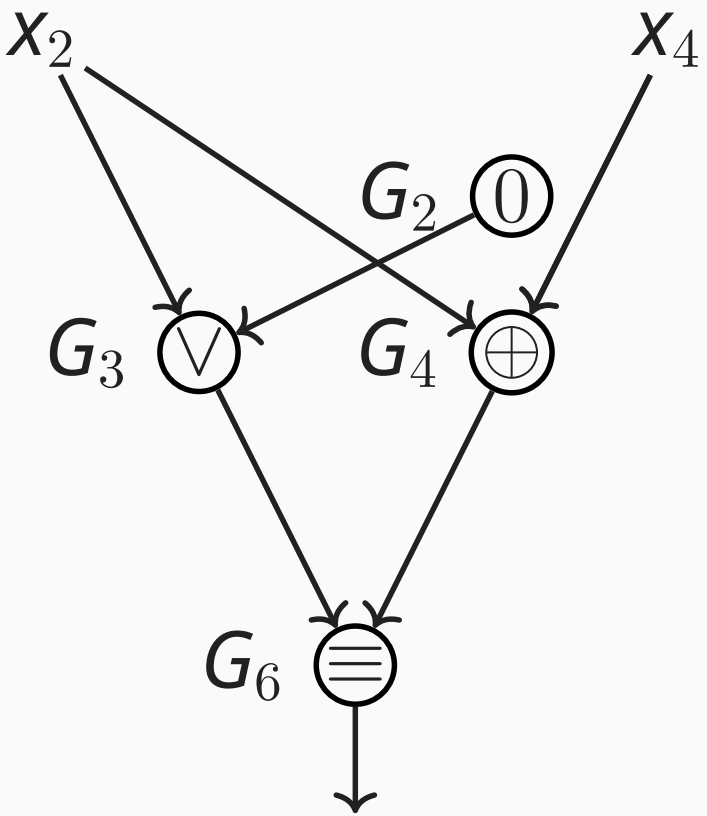
Gate Elimination: Example



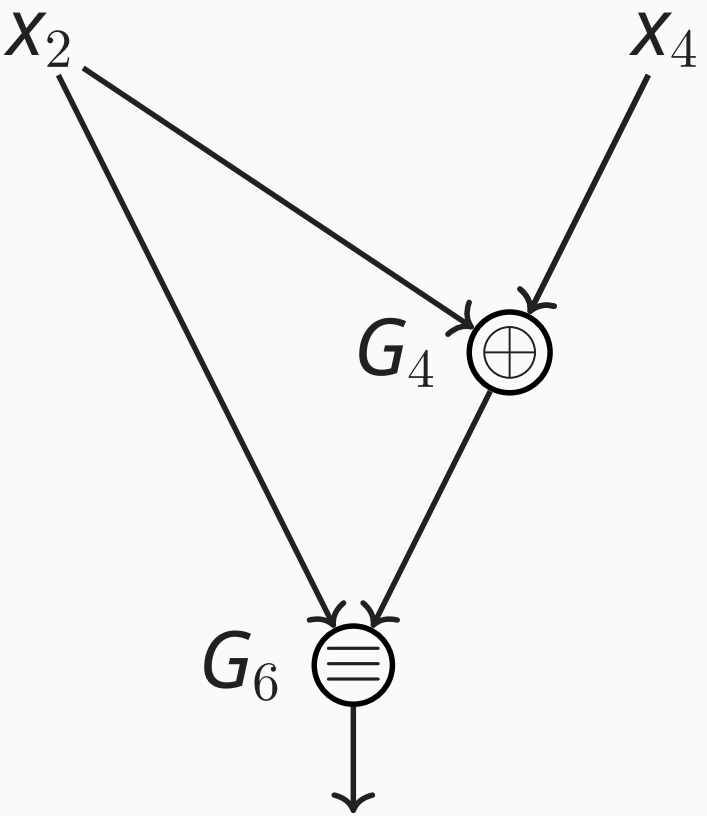
Gate Elimination: Example



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

Dispersers

Lower Bounds for Affine Dispersers

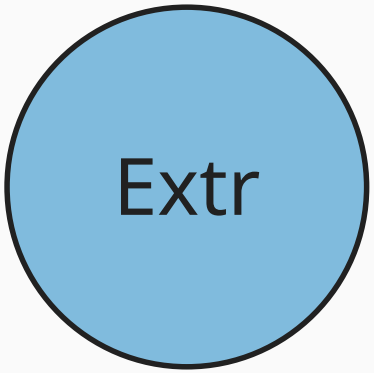
Lower Bound for Quadratic Dispersers

Open Problems

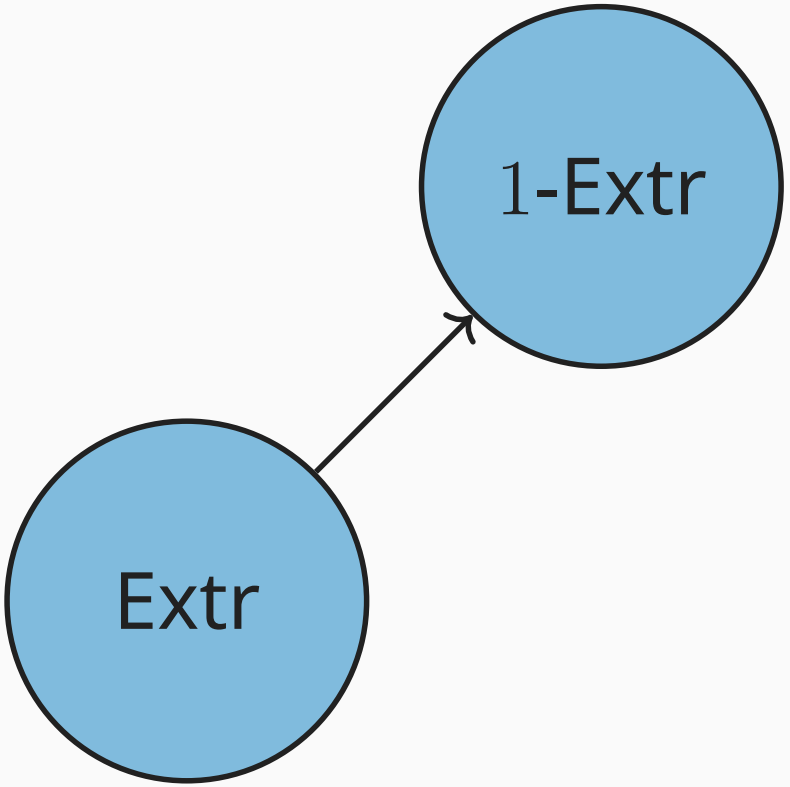
Randomness

- TCS requires randomness
- One general source is not enough
- Several sources
- One source with structure
- Extractors: output is close to uniform
- Dispersers: output has large support

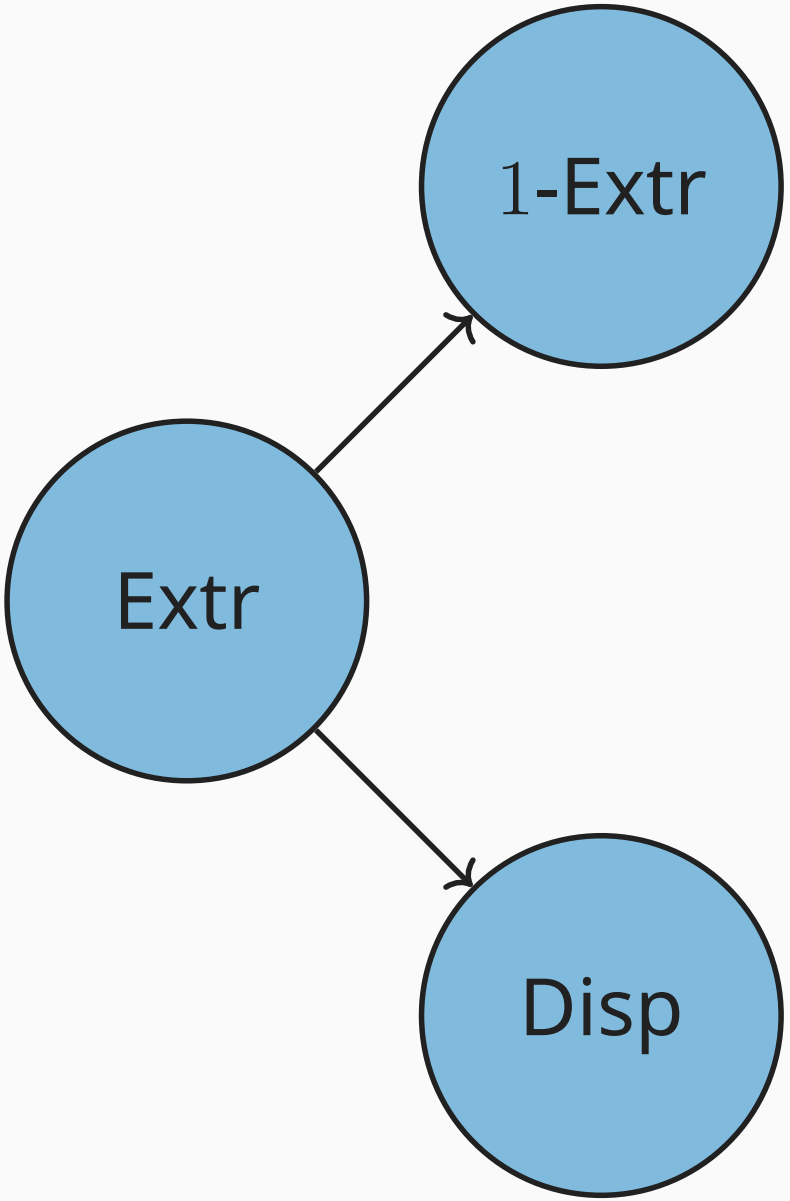
Extractors & Dispersers



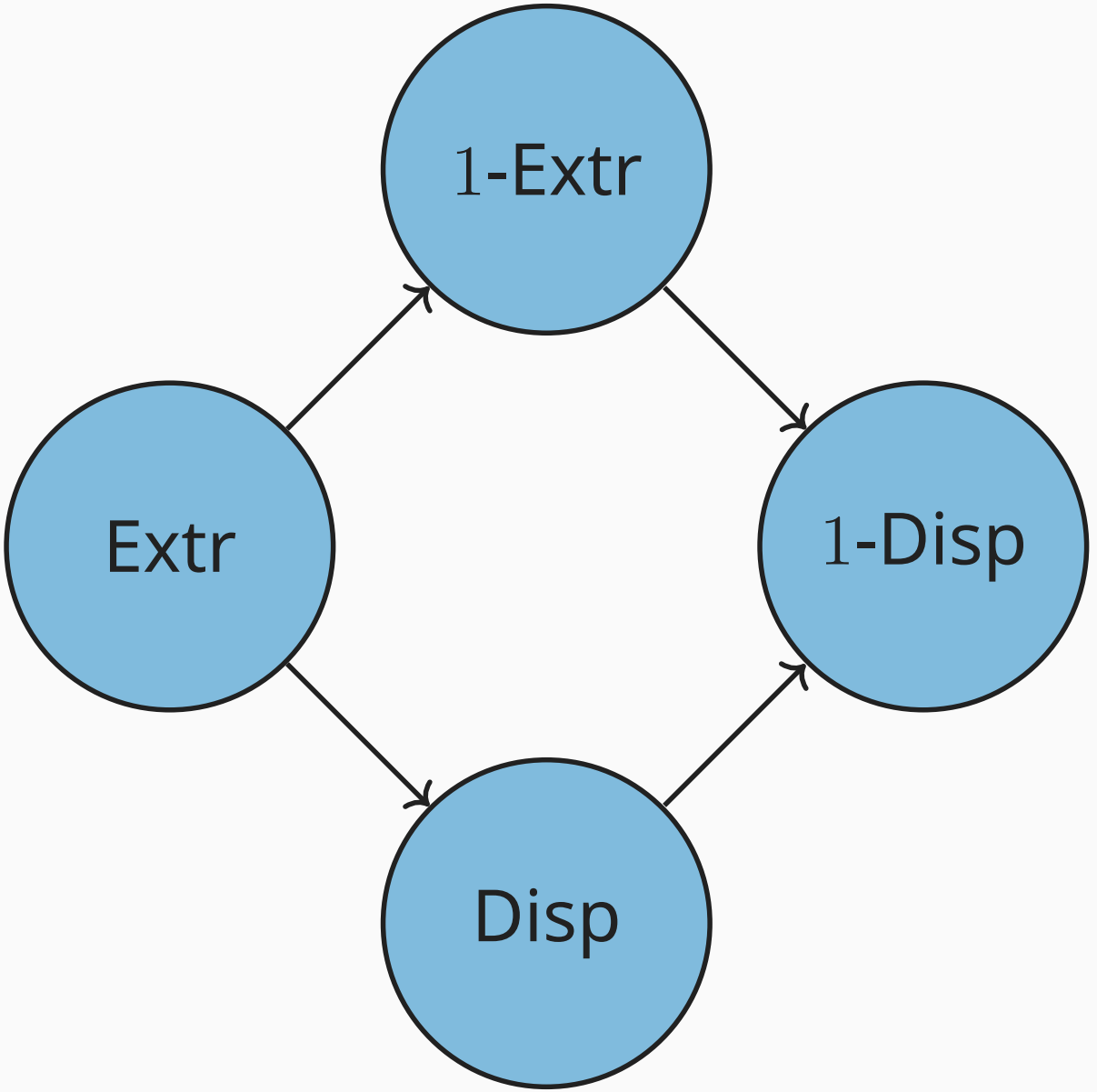
Extractors & Dispersers



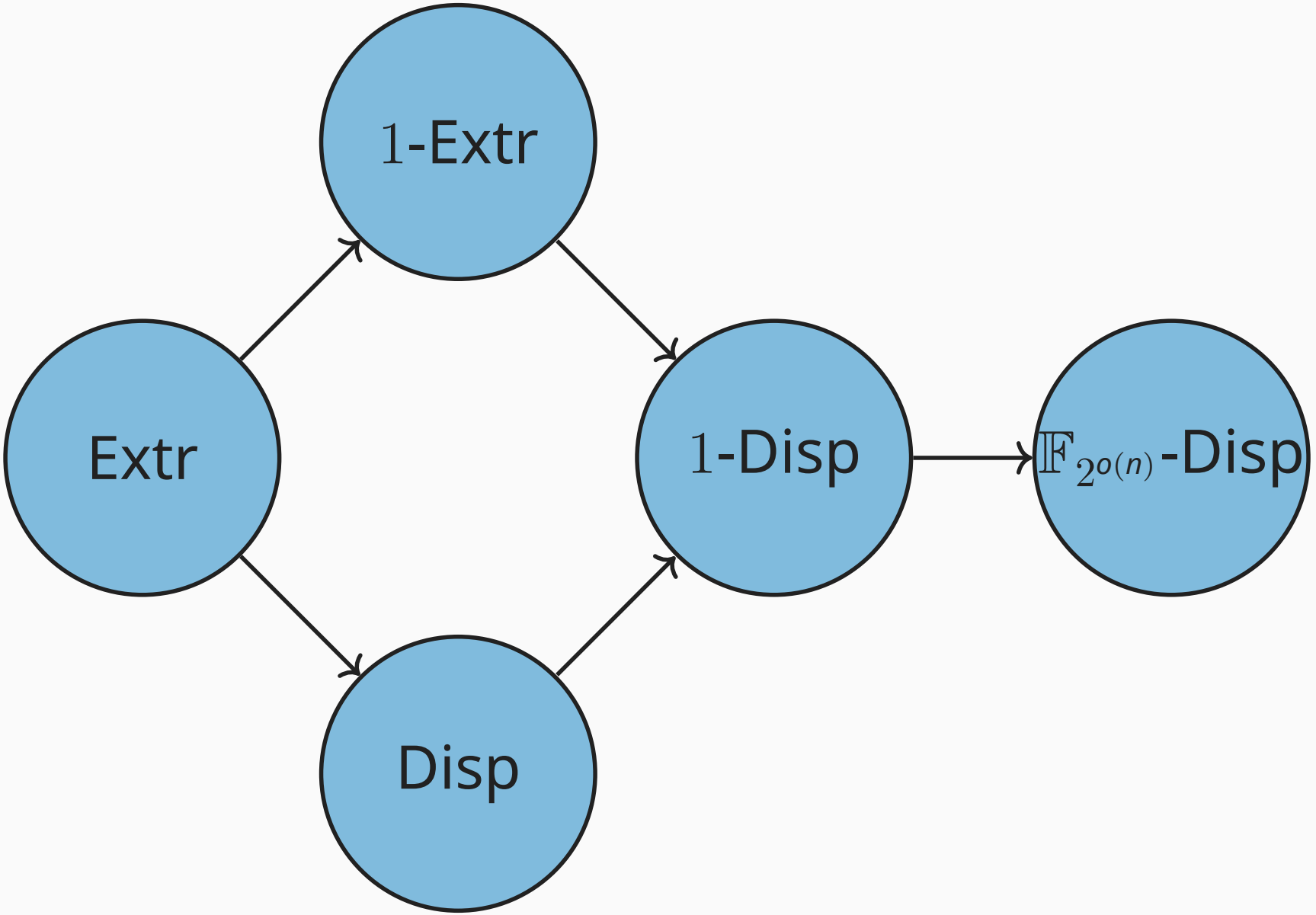
Extractors & Dispersers



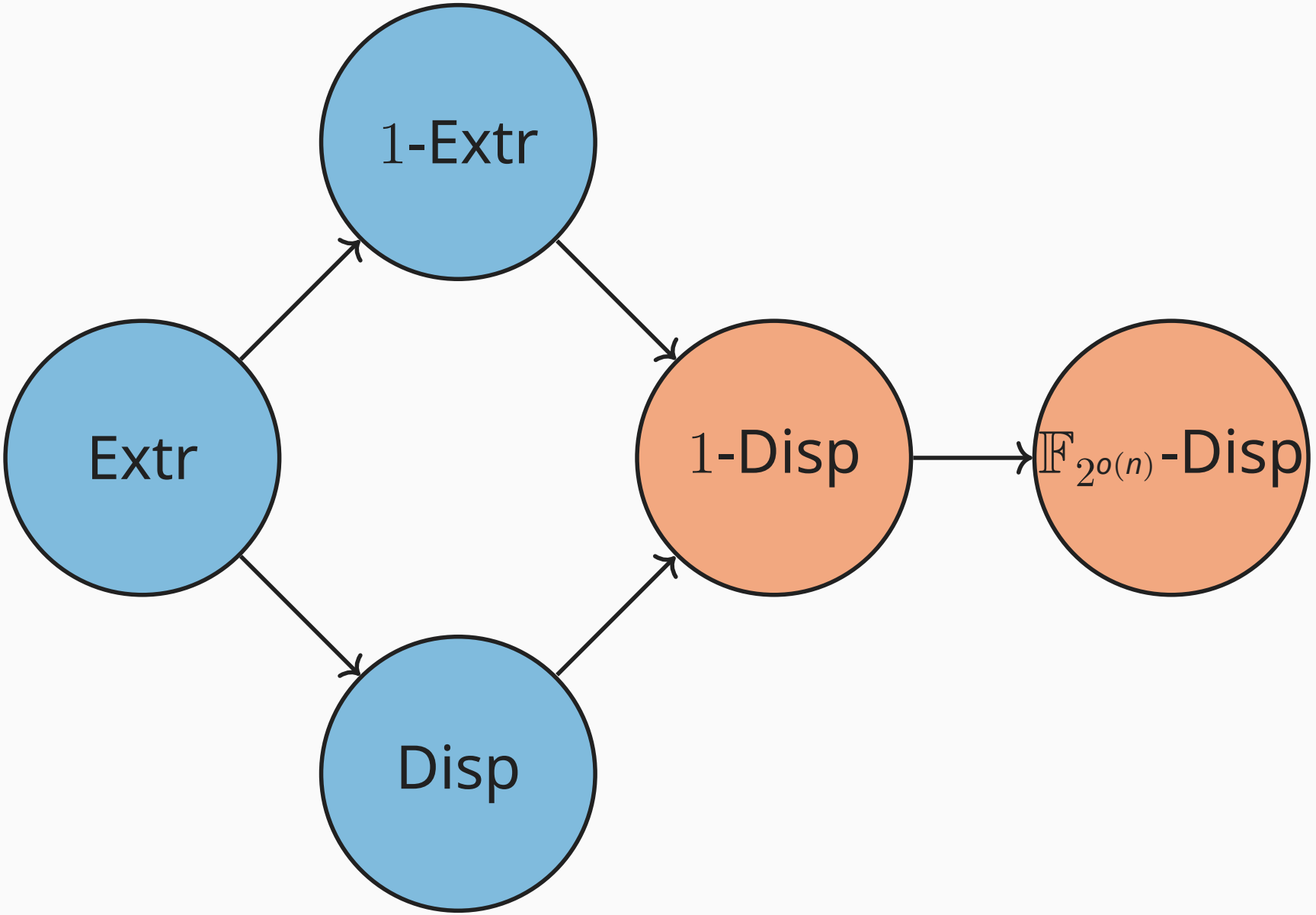
Extractors & Dispersers



Extractors & Dispersers



Extractors & Dispersers



DEPTH-3 CIRCUITS

Dispersers

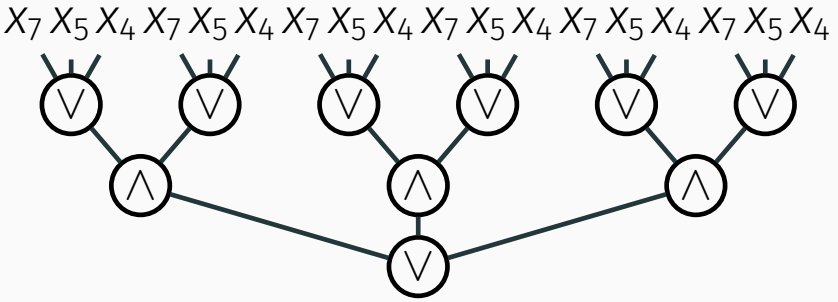
$f\colon \{0,1\}^n \to \{0,1\}$ is a disperser if $f|_S \not\equiv \text{const}$,
$\forall S = \{x \in \{0,1\}^n : p_1(x) = \ldots = p_k(x) = 0\}$.

DEPTH-3 CIRCUITS

Dispersers

$f\colon \{0,1\}^n \to \{0,1\}$ is a disperser if $f|_S \not\equiv \text{const}$,
$\forall S = \{x \in \{0,1\}^n : p_1(x) = \ldots = p_k(x) = 0\}$.

- Bit-fixing Disperser
  - $p_i(x) = x_j \oplus c_j$
  - parity
  - $\Sigma_3(f) \geq 2^{\Omega(\sqrt{n})}$ [Hås89]



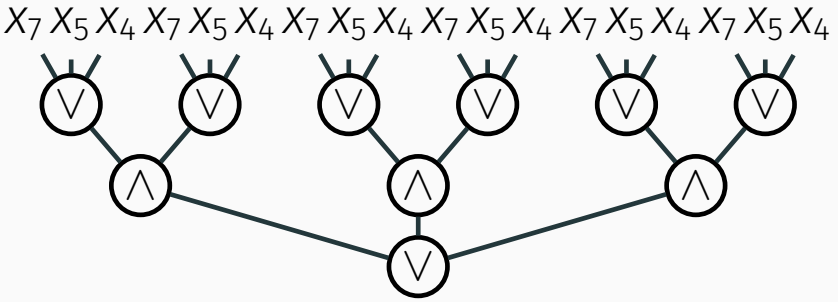
depth: 3, bottom fan-in: unbounded

DEPTH-3 CIRCUITS

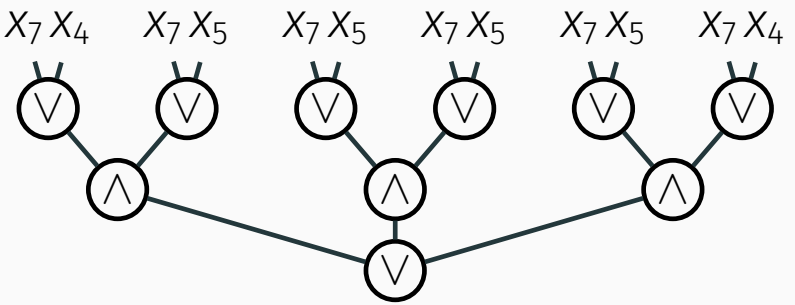
Dispersers

$f\colon \{0,1\}^n \to \{0,1\}$ is a disperser if $f|_S \not\equiv \text{const}$,
$\forall S = \{x \in \{0,1\}^n : p_1(x) = \ldots = p_k(x) = 0\}$.

- Bit-fixing Disperser
  - $p_i(x) = x_j \oplus c_j$
  - parity
  - $\Sigma_3(f) \geq 2^{\Omega(\sqrt{n})}$ [Hås89]
- Projections Disperser
  - $p_i(x) = x_j \oplus x_k \oplus c_j$
  - BCH codes [PSZ97]
  - $\Sigma_3^2(f) \geq 2^{n-o(n)}$ [PSZ97]



depth: 3, bottom fan-in: unbounded



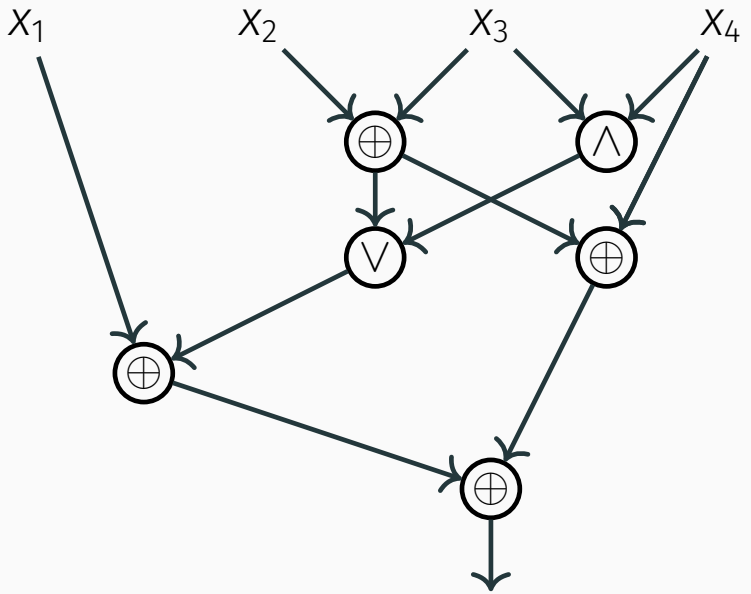
depth: 3, bottom fan-in: 2

GENERAL CIRCUITS

Dispersers

$f\colon \{0,1\}^n \to \{0,1\}$ is a disperser if $f|_S \not\equiv \text{const}$,
$\forall S = \{x \in \{0,1\}^n : p_1(x) = \ldots = p_k(x) = 0\}$.

- Affine Disperser
  - $p_i(x) = \bigoplus_{j \in J} x_j \oplus c_i$
  - constructions in **P** [BK09]
  - $C(f) \geq 3.01n$ [FGHK16]



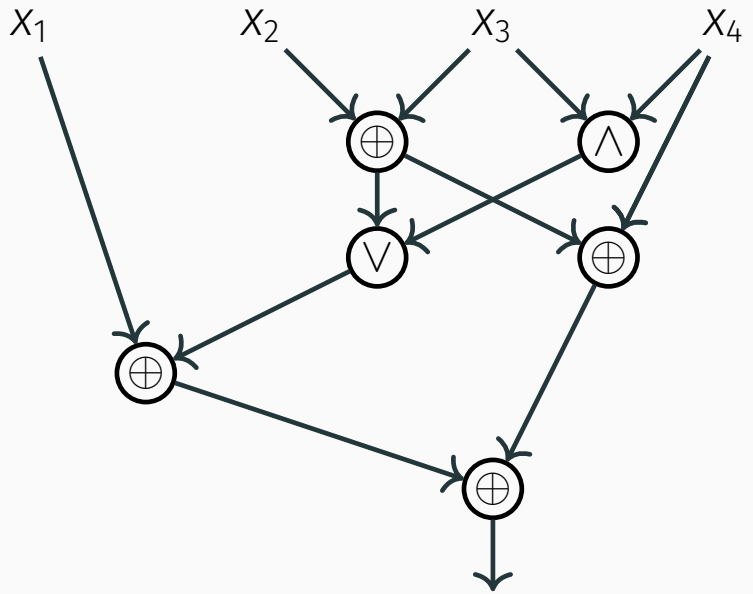
depth: unbounded, fan-in: 2

GENERAL CIRCUITS

Dispersers

$f\colon \{0,1\}^n \to \{0,1\}$ is a disperser if $f|_S \not\equiv \text{const}$,
$\forall S = \{x \in \{0,1\}^n : p_1(x) = \ldots = p_k(x) = 0\}$.

- Affine Disperser
  - $p_i(x) = \bigoplus_{j \in J} x_j \oplus c_i$
  - constructions in **P** [BK09]
  - $C(f) \geq 3.01n$ [FGHK16]
- Quadratic Disperser
  - $\deg(p_i) \leq 2$
  - over large fields [Dvi09]
  - $C(f) \geq 3.1n$ [GK16]



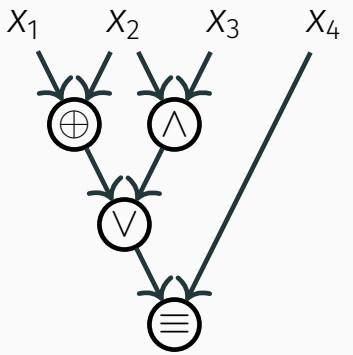
depth: unbounded, fan-in: 2

LOG-DEPTH CIRCUITS

Dispersers

$f\colon \{0,1\}^n \to \{0,1\}$ is a disperser if $f|_S \not\equiv \text{const}$,
$\forall S = \{x \in \{0,1\}^n : p_1(x) = \ldots = p_k(x) = 0\}$.

- Varieties of const deg
  - $\deg(p_i) \leq \text{const}$
  - no known constructions
  - $\omega(n)$-bound for s.-p. $\mathbf{NC}_1$



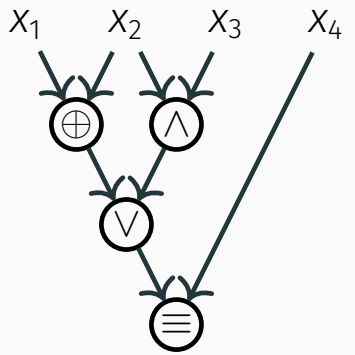
depth: $O(\log n)$, fan-in: 2
series-parallel circuit

LOG-DEPTH CIRCUITS

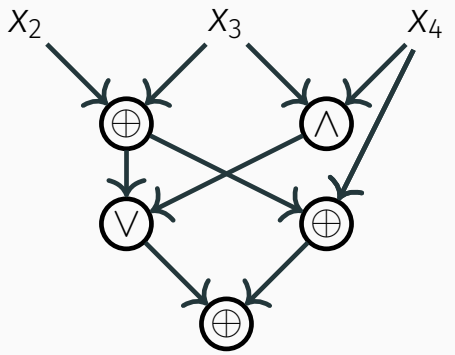
Dispersers

$f\colon \{0,1\}^n \to \{0,1\}$ is a disperser if $f|_S \not\equiv \text{const}$,
$\forall S = \{x \in \{0,1\}^n : p_1(x) = \ldots = p_k(x) = 0\}$.

- Varieties of const deg
  - $\deg(p_i) \leq \text{const}$
  - no known constructions
  - $\omega(n)$-bound for s.-p. $\mathbf{NC}_1$
- Varieties of poly deg
  - $\deg(p_i) \leq n^{\varepsilon}$
  - no known constructions
  - $\omega(n)$-bound for $\mathbf{NC}_1$



depth: $O(\log n)$, fan-in: 2
series-parallel circuit



depth: $O(\log n)$, fan-in: 2

Sources

Source	Construction	Bound
bit-fixing	parity	Σ_3

Sources

Source	Construction	Bound
projections	codes	Σ_3^2
bit-fixing	parity	Σ_3

Sources

Source	Construction	Bound
affine	affine extr	B_2; Cor
projections	codes	Σ_3^2
bit-fixing	parity	Σ_3

Sources

Source	Construction	Bound
quadratic	quad disp?	B_2
affine	affine extr	B_2; Cor
projections	codes	Σ_3^2
bit-fixing	parity	Σ_3

Sources

Source	Construction	Bound
poly vars	n.k.	s.p.-NC_1
quadratic	quad disp?	B_2
affine	affine extr	B_2; Cor
projections	codes	Σ_3^2
bit-fixing	parity	Σ_3

Sources

Source	Construction	Bound
poly vars deg $= n^{\varepsilon}$	n.k.	NC_1
poly vars	n.k.	s.p.-NC_1
quadratic	quad disp?	B_2
affine	affine extr	B_2; Cor
projections	codes	Σ_3^2
bit-fixing	parity	Σ_3

Sources

Source	Construction	Bound
poly vars deg $= n^{\varepsilon}$	n.k.	NC_1
poly vars	n.k.	s.p.-NC_1
quadratic	quad disp?	B_2
affine	affine extr	B_2; Cor
projections	codes	Σ_3^2
bit-fixing	parity	Σ_3

Sources

Source	Construction	Bound
poly vars deg $= n^{\varepsilon}$	n.k.	NC_1
poly vars	n.k.	s.p.-NC_1
quadratic	quad disp?	B_2
affine	affine extr	B_2; Cor
projections	codes	Σ_3^2
bit-fixing	parity	Σ_3

Outline

Gate Elimination

Dispersers

Lower Bounds for Affine Dispersers

Lower Bound for Quadratic Dispersers

Open Problems

Main Result

Theorem

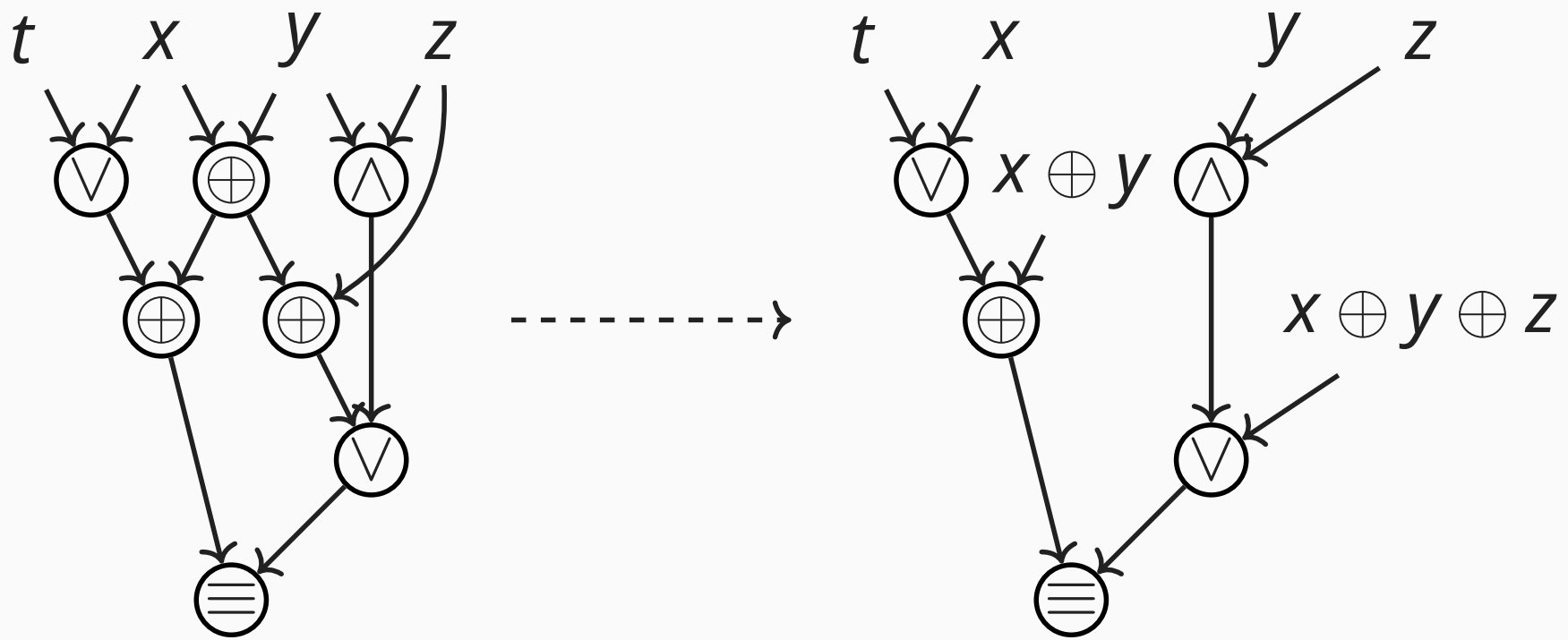
If $f\colon \{0,1\}^n \to \{0,1\}$ *is an affine disperser for dimension* $d = o(n)$*, then*

$$\mathsf{size}(f) \geq 3.011n.$$

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 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]).

XOR-layered Circuits



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

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

$$\mathsf{inputs}(\mathcal{C}) + \mathsf{size}(\mathcal{C}) \geq \mathsf{inputs}(\mathcal{C}') + \mathsf{size}(\mathcal{C}').$$

$3n - o(n)$ Lower Bound

Theorem [Demenkov, Kulikov 2011]

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

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

Corollary

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

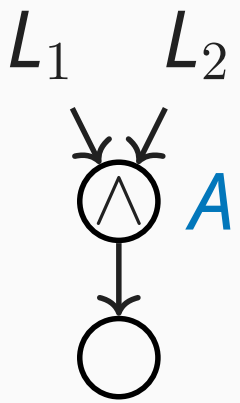
Proposition

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

Proof

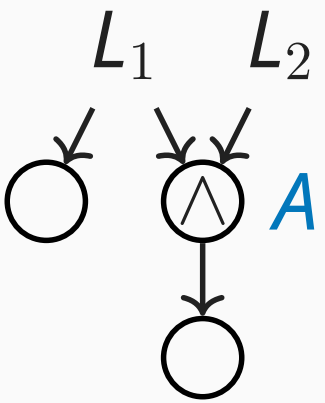
- Want to show:
$$\text{inputs}(\mathcal{C}) + \text{size}(\mathcal{C}) \geq 4(n - d).$$
- Make $n - d$ affine restrictions each time reducing $(\text{inputs} + \text{size})$ by at least 4.
- Convert $\mathcal{C}$ to XOR-layered and take a top-gate A:

Case 1



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

Case 2



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

Main Result

Theorem

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

$$\mathsf{size}(f) \geq 3.011n.$$

Main Ingredients

- Delayed linear substitutions
- Cyclic circuits
- Circuit complexity measure

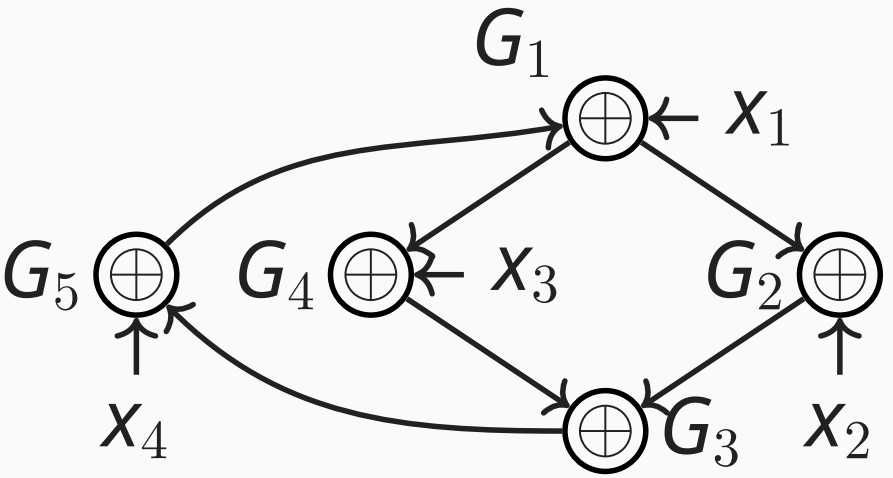
Delayed Linear Substitutions

We make substitutions of three kinds:

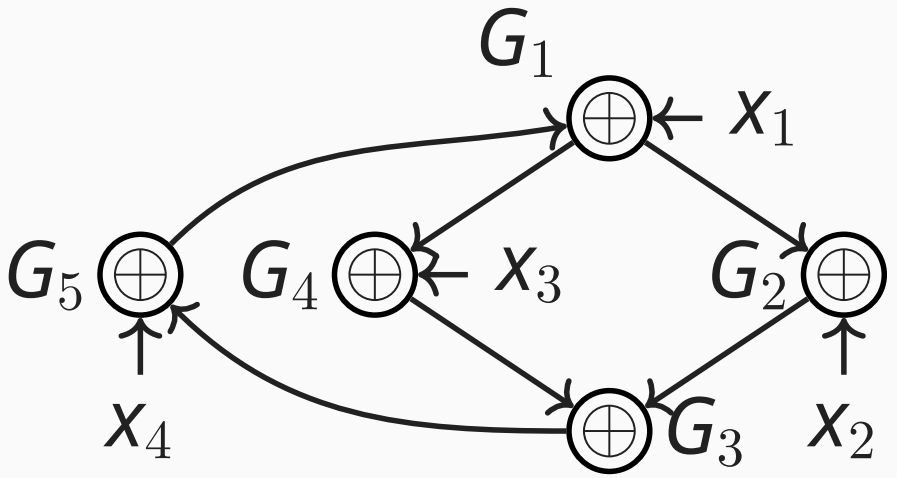
- $x_3 \leftarrow 0$
- $x_5 \leftarrow x_7 \oplus x_{10} \oplus 1$
- $x_3 \leftarrow x_4 x_7$

For each quadratic substitution of the form $x_3 \leftarrow x_4 x_7$ we later assign either x_4 or x_7 a constant making this quadratic substitution linear.

Cyclic Circuits

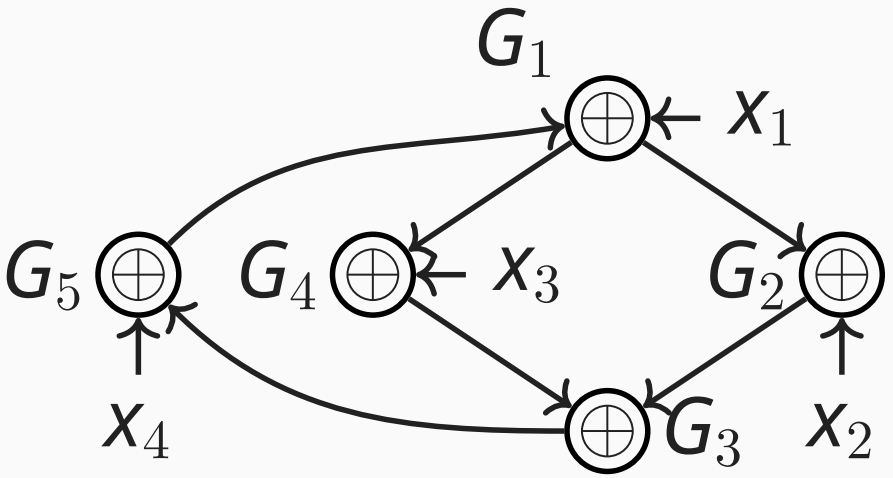


Cyclic Circuits



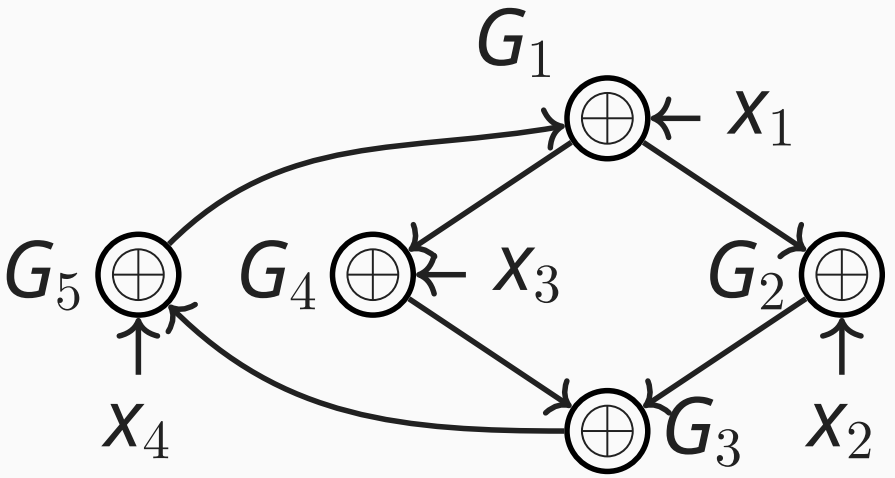
$$G_1 = x_1 \oplus G_5$$
$$G_2 = x_2 \oplus G_1$$
$$G_3 = G_2 \oplus G_4$$
$$G_4 = x_3 \oplus G_1$$
$$G_5 = x_4 \oplus G_3$$

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

$$\mu = g + \frac{65}{43} \cdot q + \frac{1}{43} \cdot b + \frac{260}{43} \cdot n \,,$$

where

- g is # of gates
- q is # of quadratic substitutions
- b is # of “bottleneck” gates in the circuit
- n is # of inputs

Outline

Gate Elimination

Dispersers

Lower Bounds for Affine Dispersers

Lower Bound for Quadratic Dispersers

Open Problems

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

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

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.

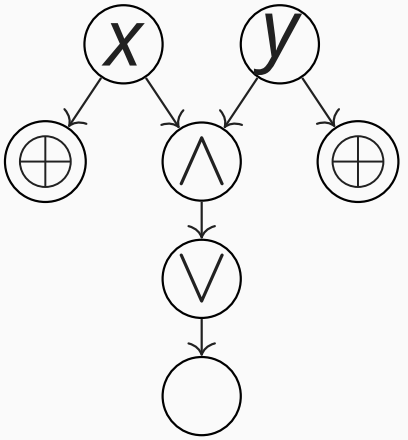
Regular Gate Elimination

- 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

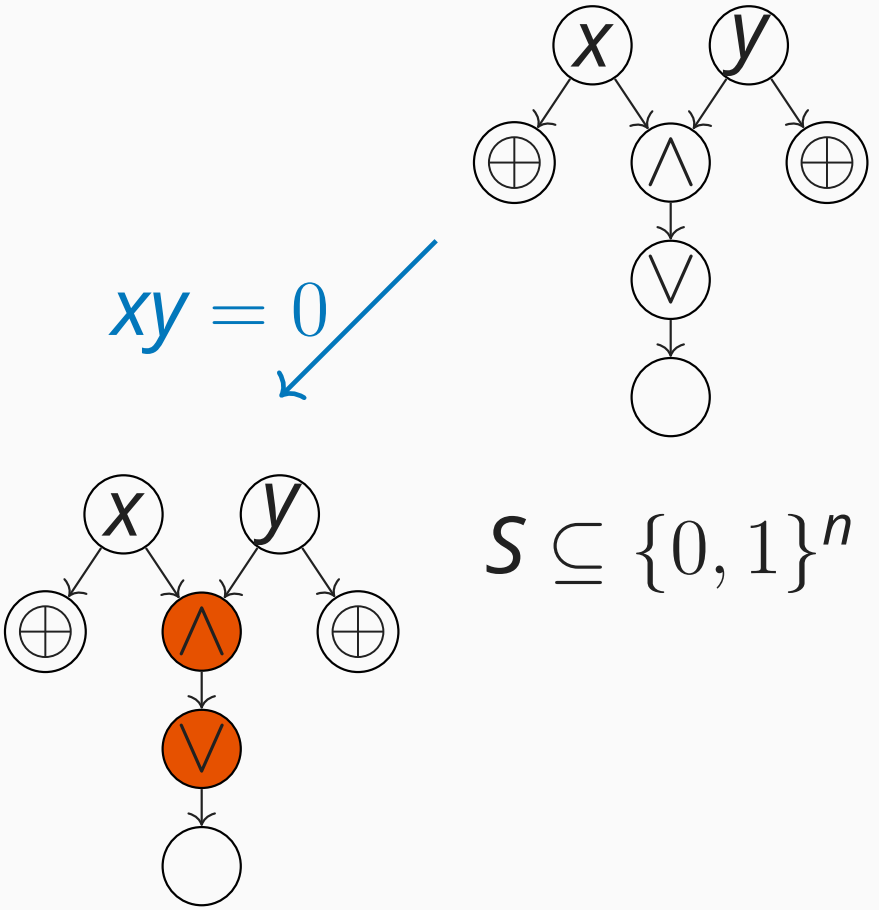
- make a restriction;
- decrease S by a factor of α.
- make sure to eliminate at least $3 \log \alpha$ gates;
- S belongs to the same class;
- repeat until S becomes small (e.g., $2^{n/100}$).

Toy Example



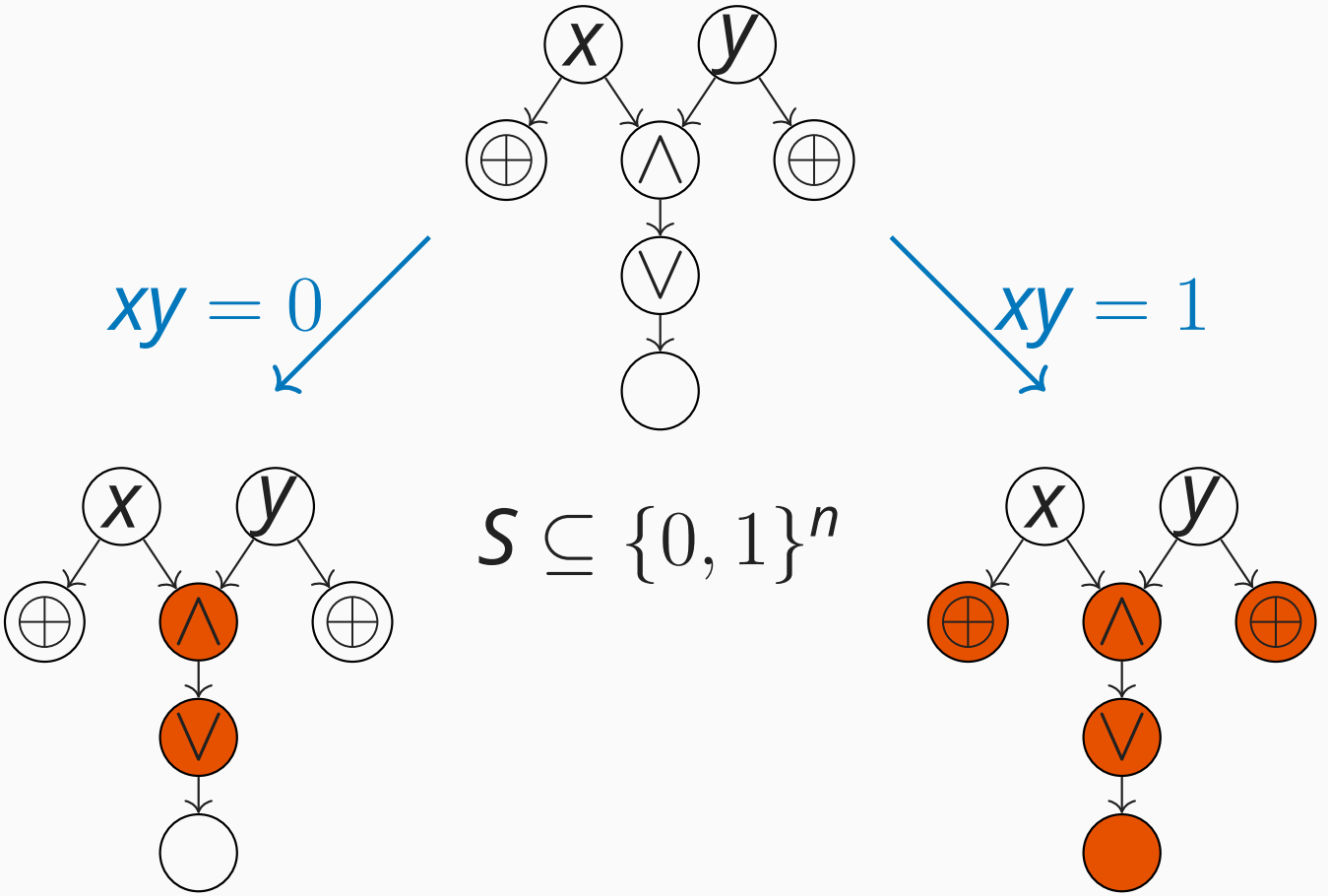
$$S \subseteq \{0,1\}^n$$

Toy Example

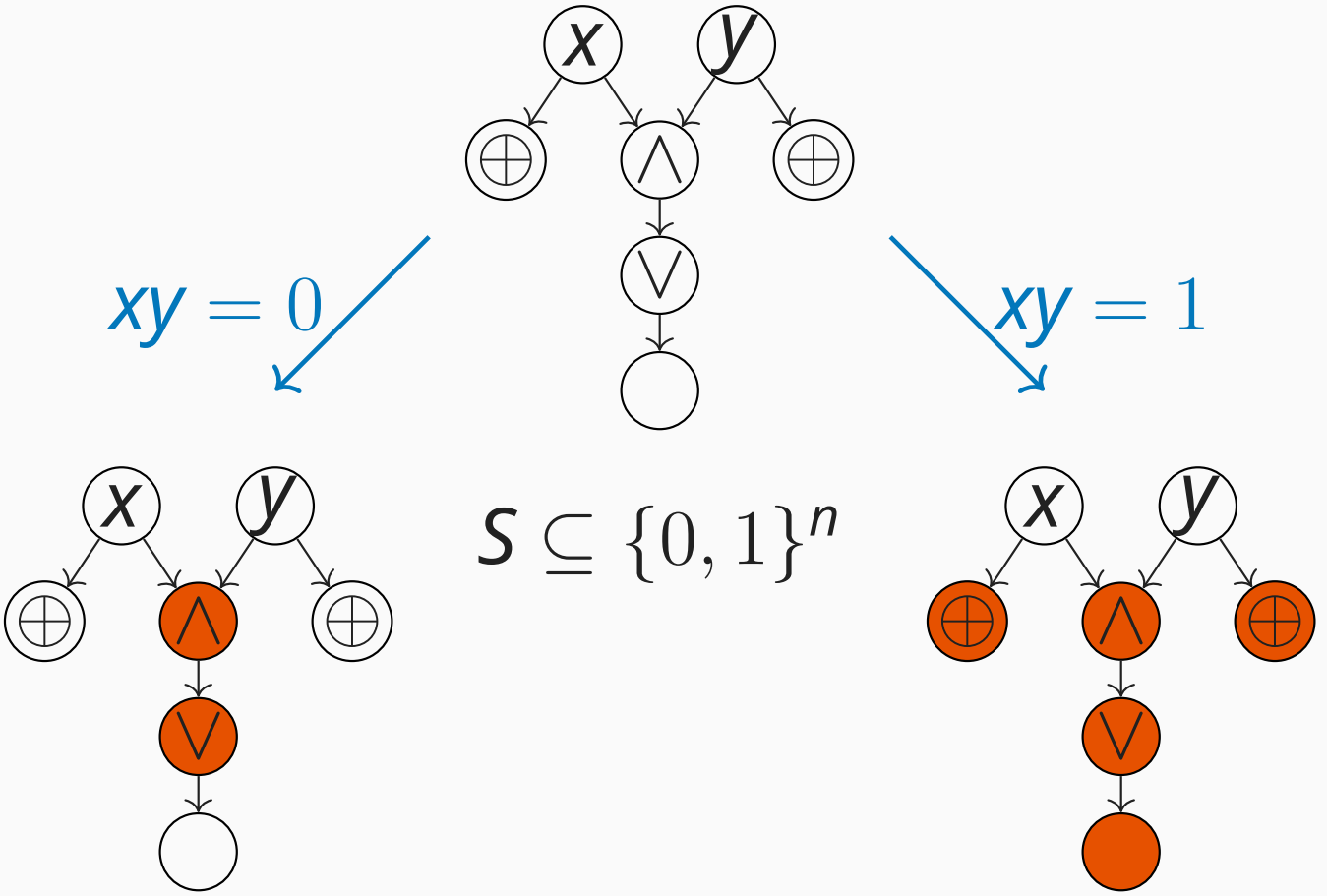


$S \subseteq \{0,1\}^n$

Toy Example



Toy Example



Outline

Gate Elimination

Dispersers

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!