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)

$g_1 = x_1 \oplus x_2$
$g_2 = x_2 \land x_3$
$g_3 = g_1 \lor g_2$
$g_4 = g_2 \lor 1$
$g_5 = g_3 \equiv g_4$

Diagram:

```
  x1       x2       x3       1
   |       |       |        /  \
   |       |       |       g1    g2
   |       |       |       /  \
   |       |       |       g3    g4
   |       |       |       /  \
   |       |       |       g5
```

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

<table>
<thead>
<tr>
<th>$n$</th>
<th>$f(x)$</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2n$</td>
<td>$f(x) = \bigoplus_{i&lt;j} x_i x_j$</td>
<td>[Kloss, Malyshev 1965]</td>
</tr>
<tr>
<td>$2n$</td>
<td>$f(x) = [\sum x_i \equiv_3 0]$</td>
<td>[Schnorr 1974]</td>
</tr>
<tr>
<td>$2.5n$</td>
<td>$f(x, a, b) = x_a \oplus x_b$</td>
<td>[Paul 1977]</td>
</tr>
<tr>
<td>$2.5n$</td>
<td>symmetric</td>
<td>[Stockmeyer 1977]</td>
</tr>
<tr>
<td>$3n$</td>
<td>$f(x, a, b, c) = x_a x_b \oplus x_c$</td>
<td>[Blum 1984]</td>
</tr>
<tr>
<td>$3n$</td>
<td>affine dispersers</td>
<td>[Demenkov, Kulikov 2011]</td>
</tr>
<tr>
<td>$3.011n$</td>
<td>affine dispersers</td>
<td>[FGHK 2015]</td>
</tr>
</tbody>
</table>
Explicit Lower Bounds

**Previous**

<table>
<thead>
<tr>
<th>Bound</th>
<th>Function</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2n$</td>
<td>$f(x) = \bigoplus_{i&lt;j} x_i x_j$</td>
<td>[Kloss, Malyshev 1965]</td>
</tr>
<tr>
<td>$2n$</td>
<td>$f(x) = \left[ \sum x_i \equiv_3 0 \right]$</td>
<td>[Schnorr 1974]</td>
</tr>
<tr>
<td>$2.5n$</td>
<td>$f(x, a, b) = x_a \oplus x_b$</td>
<td>[Paul 1977]</td>
</tr>
<tr>
<td>$2.5n$</td>
<td>symmetric</td>
<td>[Stockmeyer 1977]</td>
</tr>
<tr>
<td>$3n$</td>
<td>$f(x, a, b, c) = x_a x_b \oplus x_c$</td>
<td>[Blum 1984]</td>
</tr>
<tr>
<td>$3n$</td>
<td>affine dispersers</td>
<td>[Demenkov, Kulikov 2011]</td>
</tr>
<tr>
<td>$3.011n$</td>
<td>affine dispersers</td>
<td>[FGHK 2015]</td>
</tr>
</tbody>
</table>

**New**

<table>
<thead>
<tr>
<th>Bound</th>
<th>Function</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>$3.11n$</td>
<td>quadratic dispersers</td>
<td>[G, Kulikov 2015]</td>
</tr>
</tbody>
</table>
Explicit Lower Bounds: Pictorially

- **1965**: KM65
- **1975**: S74, S77, P77
- **1985**: B84
- **2005**: DK11

The graph shows the progression of lower bounds from 1965 to 2015 with milestones at each year, indicating the evolution of lower bounds in computer science or a related field.
Explicit Lower Bounds: Pictorially

- KM65
- S74
- S77, P77
- B84
- GK15 (non-explicit)
- FGHK15

Explicit Lower Bounds: Pictorially

1965
KM65

1975
S74
S77, P77

1985
B84

1995

2005
DK11

2015
FGHK15
GK15 (non-explicit)
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
Theorem

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

\[
\text{size}(f) \geq 3n - o(n).
\]
A function \( f: \{0, 1\}^n \rightarrow \{0, 1\} \) is called an **affine disperser for dimension** \( d \) if it is non-constant on any affine subspace of dimension at least \( d \).

An affine disperser 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, 2012]).
XOR-layered Circuits

inputs(\(C\)) = 4
size(\(C\)) = 7

inputs(\(C'\)) = 6
size(\(C'\)) = 5

\[\text{inputs}(C') + \text{size}(C') \leq \text{inputs}(C) + \text{size}(C).\]
3n − o(n) Lower Bound

Theorem [Demenkov, Kulikov 2011]
For a circuit $C$ computing an affine disperser for dimension $d$:
$$\text{inputs}(C) + \text{size}(C) \geq 4(n - d).$$

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

**Case 1**

\[
\begin{align*}
L_1 & \leftarrow 0: \\
\Delta \text{size} & = 2 \\
\Delta \text{inp} & = 2
\end{align*}
\]

**Case 2**

\[
\begin{align*}
L_1 & \leftarrow 0: \\
\Delta \text{size} & = 3 \\
\Delta \text{inp} & = 1
\end{align*}
\]
Outline

Gate Elimination

Lower Bounds for Affine Dispersers

Lower Bound for Quadratic Dispersers

Open Problems
**Theorem**

Let $f: \{0, 1\}^n \to \{0, 1\}$ 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

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

Then

$$size(f) \geq 3.11n.$$
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 $\alpha$;
- 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

\[ xy = 0 \]

\[ xy = 1 \]

\[ S \subseteq \{0, 1\}^n \]
Toy Example

\[ x y = 0 \]
\[ x y = 1 \]

\[ S_0 = S|_{x y=0} \]
\[ S_1 = S|_{x y=1} \]
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!