On the Limits of Gate Elimination

Authors:

Alexander Golovnev, Edward Hirsch,
Alexander Knop, Alexander Kulikov

Institute:

St. Petersburg Department of V.A. Steklov Institute of Mathematics of the Russian Academy of Sciences

State of the art

SHANNON, 1949

Almost all functions of n variables have circuit size $\Omega(\frac{2^n}{n})$.

State of the art

SHANNON, 1949

Almost all functions of n variables have circuit size $\Omega(\frac{2^n}{n})$.

FIND, GOLOVNEV, HIRSCH, KULIKOV, 2016

There is a function $f \in \mathbf{P}$ such that $C(f) \geq 3.01n$.

Example of gate elimination

Let $\mathcal{F}_n$ be a set of functions f such that $f(x) = 1$ iff $\sum_{i=0}^{n} c_i x_i \equiv r \pmod 3$ ($c_i \in \{1, 2\}$) and $\mu(f) = \texttt{gates} + \texttt{inputs}(f)$.

Example of gate elimination

Let $\mathcal{F}_n$ be a set of functions f such that $f(x) = 1$ iff $\sum_{i=0}^{n} c_i x_i \equiv r \pmod 3$ ($c_i \in \{1, 2\}$) and $\mu(f) = \texttt{gates} + \texttt{inputs}(f)$.

INDUCTION STEP

For any function f and numbers $i, j \in [n]$

1. there is $c \in \{0, 1\}$ such that $\mu(f) - \mu(f|_{x_i \leftarrow c}) \geq 3$ or
2. for each $c \in \{0, 1\}$ holds $\mu(f) - \mu(f|_{x_i \leftarrow x_j \oplus c}) \geq 3$.

Example of gate elimination

Let $\mathcal{F}_n$ be a set of functions f such that $f(x) = 1$ iff $\sum_{i=0}^{n} c_i x_i \equiv r \pmod 3$ ($c_i \in \{1, 2\}$) and $\mu(f) = \texttt{gates} + \texttt{inputs}(f)$.

RIGIDITY

For any function $f \in \mathcal{F}_n$ and numbers $i, j \in [n]$

1. for any c holds $f|_{x_i \leftarrow c} \in \mathcal{F}_{n-1}$ or
2. there is c such that $f|_{x_i \leftarrow x_j \oplus c} \in \mathcal{F}_{n-1}$.

Example of gate elimination

Let $\mathcal{F}_n$ be a set of functions f such that $f(x) = 1$ iff $\sum\limits_{i=0}^{n} c_i x_i \equiv r \pmod 3$ ($c_i \in \{1, 2\}$) and $\mu(f) = \texttt{gates} + \texttt{inputs}(f)$.
As result we prove that for any $f \in \mathcal{F}_n$ holds $\mu(f) \geq 3n - 6$. Hence $\texttt{gates}(f) \geq 2n - 6$.

Definition of gate elimination

1. (Measure usefulness.) If $\mu(f)$ is large, then $\mathtt{gates}(f)$ is large.

Definition of gate elimination

1. (Measure usefulness.) If $\mu(f)$ is large, then $\mathtt{gates}(f)$ is large.
2. (Invariance.) For every $f \in \mathcal{F}$ and $\rho \in \mathcal{S}$, either $f|_\rho \in \mathcal{F}$ or $\mathtt{stop}(f|_\rho)$.

Definition of gate elimination

1. (Measure usefulness.) If $\mu(f)$ is large, then $\texttt{gates}(f)$ is large.
2. (Invariance.) For every $f \in \mathcal{F}$ and $\rho \in \mathcal{S}$, either $f|_\rho \in \mathcal{F}$ or $\texttt{stop}(f|_\rho)$.
3. (Induction step.) For every f with $\texttt{inputs}(f) = n$, there is a substitution $\rho \in \mathcal{S}$ such that $\mu(f|_\rho) \leq \mu(f) - \texttt{gain}(n)$. (In known proofs, $\texttt{gain}(n)$ is constant.)

Definition

COMPOSITION

For any fucntions $f\colon \{0,1\}^n \to \{0,1\}$ and $g\colon \{0,1\}^k \to \{0,1\}$ we call a function $f \diamond g$ composition of f and g if $f \diamond g\colon \{0,1\}^{nk} \to \{0,1\}$ and $f \diamond g(x_{1,1},\dots,x_{n,k}) = f(g(x_{1,1},\dots,x_{1,k}),\dots,g(x_{n,1},\dots,x_{n,k}))$

Definition

COMPOSITION

For any fucntions $f\colon \{0,1\}^n \to \{0,1\}$ and $g : \{0,1\}^k \to \{0,1\}$ we call a function $f \diamond g$ composition of f and g if $f \diamond g : \{0,1\}^{nk} \to \{0,1\}$ and $f \diamond g(x_{1,1}, \dots, x_{n,k}) = f(g(x_{1,1}, \dots, x_{1,k}), \dots, g(x_{n,1}, \dots, x_{n,k}))$

SUBADDITIVE MEASURE

We call measure μ on boolean functions subadditive if for any fucntions $f\colon \{0,1\}^n \to \{0,1\}$ and $g : \{0,1\}^k \to \{0,1\}$ holds $\mu(f) + \mu(g) \geq \mu(f \diamond g)$.

Subadditive measures

LIMITATION

If μ is a subadditive measure then there is a famyly of functions f_n and a constant $c \geq 0$ such that for any m-substitution ρ holds $\mu(f_n) - \mu(f_n|_\rho) \leq c$ and $\mathtt{gates}(f) = 2^{\Omega(n)}$.

Further directions

1. Show that many interesting functions are resistant to gate elimination.

Further directions

1. Show that many interesting functions are resistant to gate elimination.
2. Extend the result to local complexity measures or another wide class.