Boolean function complexity and two-dimensional cover problems

Igor Carboni Oliveira

Joint work with Bruno Cavalar

1. Matrices and intersections

The number of intersections

▷ Given a **boolean matrix**

$$A = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix},$$

Q. How many **intersections** are needed to construct A from **row** and **column** matrices (using **unions** and **intersections**)?

The base matrices

- ▷ **Row** matrices $R_1, \ldots, R_4$.

$$R_3 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

- ▷ **Column** matrices $C_1, \ldots, C_4$.

$$C_2 = \begin{bmatrix} 0 & \mathbf{1} & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 \end{bmatrix}$$

Constructing A from $R_1, \ldots, R_4, C_1, \ldots, C_4$

$$\boldsymbol{A} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix} =$$

$$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \cup \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \cup \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \cup \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix}.$$

(We view each boolean matrix as a subset of $\Gamma \stackrel{\text{def}}{=} [4] \times [4]$.)

Claim. Each remaining matrix constructed with 1 intersection.

Constructing A from $R_1, \ldots, R_4, C_1, \ldots, C_4$

Claim. Each remaining matrix constructed with 1 intersection:

$$\boldsymbol{A'} \stackrel{\text{def}}{=} \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \mathbf{1} & 0 & \mathbf{1} & \mathbf{1} \end{bmatrix} = \begin{bmatrix} \mathbf{1} & 0 & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & 0 & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & 0 & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & 0 & \mathbf{1} & \mathbf{1} \end{bmatrix} \cap \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \end{bmatrix},$$

In other words, $\boldsymbol{A'} = (\boldsymbol{C_1} \cup \boldsymbol{C_3} \cup \boldsymbol{C_4}) \cap \boldsymbol{R_4}$.

Constructing A from $R_1, \ldots, R_4, C_1, \ldots, C_4$

Claim. Each remaining matrix constructed with 1 intersection:

$$\boldsymbol{A'} \stackrel{\text{def}}{=} \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \mathbf{1} & 0 & \mathbf{1} & \mathbf{1} \end{bmatrix} = \begin{bmatrix} \mathbf{1} & 0 & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & 0 & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & 0 & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & 0 & \mathbf{1} & \mathbf{1} \end{bmatrix} \cap \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \end{bmatrix},$$

In other words, $\boldsymbol{A'} = (\boldsymbol{C_1} \cup \boldsymbol{C_3} \cup \boldsymbol{C_4}) \cap \boldsymbol{R_4}$.

$$\Longrightarrow \quad \boldsymbol{A} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$ constructed with ≤ 4 **intersections**.

Notation

▷ For $A \subseteq [N] \times [N]$ and $\mathcal{G}_N = \{R_1, \ldots, R_N, C_1, \ldots, C_N\}$,

$\boldsymbol{D_\cap(A \,|\, \mathcal{G}_N)}$ is the number of $\cap$ needed to construct A from $\mathcal{G}_N$.

▷ The previous construction establishes more generally that:

Claim. For every boolean matrix $A \subseteq [N] \times [N]$,

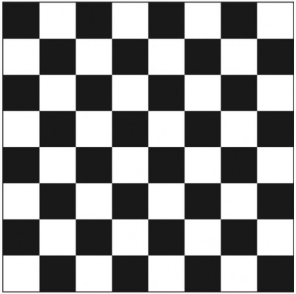
$$D_\cap(A \,|\, \mathcal{G}_N) \leq N.$$

▷ **Interested in matrices that require several intersections.**

A simple example

- Consider the $N \times N$ "parity" matrices P_N,

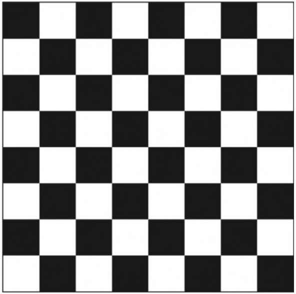
$$(i, j) \in P_N \iff i + j \equiv 0 \pmod 2$$



A simple example

▷ Consider the $N \times N$ "parity" matrices P_N,

$$(i, j) \in P_N \iff i + j \equiv 0 \pmod 2$$



$$D_\cap(P_N \,|\, \mathcal{G}_N) \;=\; O(1)$$

Another example

Consider the $N \times N$ symmetric matrices

$$\overline{I_N} \stackrel{\text{def}}{=} \begin{bmatrix} 0 & & \vec{1} \\ & \ddots & \\ \vec{1} & & 0 \end{bmatrix}.$$

Another example

Consider the $N \times N$ symmetric matrices

$$\overline{I_N} \stackrel{\text{def}}{=} \begin{bmatrix} 0 & & \vec{1} \\ & \ddots & \\ \vec{1} & & 0 \end{bmatrix}.$$

Exercise. If N is a power of 2 then $D_\cap(\overline{I_N} \mid \mathcal{G}_N) = \log N$.

The random boolean matrix

Claim. If $\boldsymbol{R} \subseteq_{1/2} [N] \times [N]$ is a random boolean matrix, then

$$D_\cap(\boldsymbol{R} \,|\, \mathcal{G}_N) = \Omega(N) \quad \text{with probability} \to 1.$$

The random boolean matrix

Claim. If $\boldsymbol{R} \subseteq_{1/2} [N] \times [N]$ is a random boolean matrix, then

$$D_{\cap}(\boldsymbol{R} \,|\, \mathcal{G}_N) = \Omega(N) \text{ with probability } \to 1.$$

- $\triangleright$ Showing a lower bound of $\Omega(N/\log N)$ is not difficult.
- $\triangleright$ Tight bound uses a result of Uri Zwick (1996).

Summary and Main Problem

- $\triangleright$ Every matrix A satisfies $D_\cap(A \,|\, \mathcal{G}_N) \leq N$.
- $\triangleright$ A uniformly random matrix $\boldsymbol{R}$ satisfies $D_\cap(\boldsymbol{R} \,|\, \mathcal{G}_N) = \Omega(N)$.
- $\triangleright$ The symmetric matrices $\overline{I_N}$ satisfy $D_\cap(\overline{I_N} \,|\, \mathcal{G}_N) = \log N$.

Summary and Main Problem

▷ Every matrix A satisfies $D_\cap(A \mid \mathcal{G}_N) \le N$.

▷ A uniformly random matrix $\boldsymbol{R}$ satisfies $D_\cap(\boldsymbol{R} \mid \mathcal{G}_N) = \Omega(N)$.

▷ The symmetric matrices $\overline{I_N}$ satisfy $D_\cap(\overline{I_N} \mid \mathcal{G}_N) = \log N$.

Problem. Show that some "**explicit**" sequence E_N satisfies

$$D_\cap(E_N \mid \mathcal{G}_N) \ge 10 \log N.$$

2. The connection to computation

– Based on the following work:

Pavel Pudlák, Vojtech Rödl, and Petr Savický.
Graph complexity.
Acta Inf., 25(5):515–535, 1988.

Matrices, intersections, and computation

▷ Constructing such matrices has implications for Theoretical Computer Science.

Proposition. If there is an “explicit” sequence E_N such that

$$D_{\cap}(E_N \,|\, \mathcal{G}_N) \geq (\log N)^{\omega(1)},$$

then P $\neq$ NP.

Matrices, intersections, and computation

▷ Constructing such matrices has implications for Theoretical Computer Science.

Proposition. If there is an “explicit” sequence E_N such that

$$D_\cap(E_N \mid \mathcal{G}_N) \geq (\log N)^{\omega(1)},$$

then P $\neq$ NP.

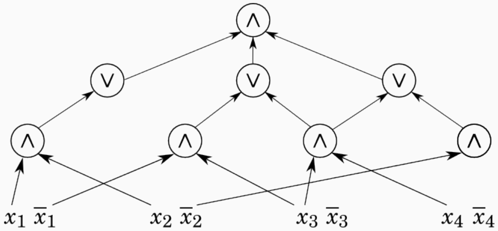
▷ Give me instead a sequence with $D_\cap(E_N \mid \mathcal{G}_N) \geq C \cdot \log N$.

▷ $C \geq 10$ would establish a **new result** in complexity theory.

Sketch of the proof (1/4)

$D_\cap(E_N \mid \mathcal{G}_N) \geq (\log N)^{\omega(1)} \implies$ "Complexity Lower Bounds"

▷ Any computation can be simulated by **boolean circuits.**



▷ A circuit computes a boolean function $g\colon \{0,1\}^n \to \{0,1\}$.

▷ Enough to prove **circuit size lower bound** for explicit $f\colon \{0,1\}^n \to \{0,1\}$ obtained from matrix E_N.

Sketch of the proof (2/4)

- ▷ Let E_N require ℓ intersections when generated from $\mathcal{G}_N$.
- ▷ Write $N = 2^n$. Fix natural bijection $\varphi\colon [N] \times [N] \to \{0,1\}^{2n}$.
- ▷ Define $f\colon \{0,1\}^{2n} \to \{0,1\}$ by $f^{-1}(1) \stackrel{\text{def}}{=} \varphi(E_N) \subseteq \{0,1\}^{2n}$.

Sketch of the proof (2/4)

- ▷ Let E_N require ℓ intersections when generated from $\mathcal{G}_N$.
- ▷ Write $N = 2^n$. Fix natural bijection $\varphi\colon [N] \times [N] \to \{0,1\}^{2n}$.
- ▷ Define $f\colon \{0,1\}^{2n} \to \{0,1\}$ by $f^{-1}(1) \stackrel{\text{def}}{=} \varphi(E_N) \subseteq \{0,1\}^{2n}$.

$$\begin{bmatrix} 1 & & \vec{0} \\ & \ddots & \\ \vec{0} & & 1 \end{bmatrix}$$ becomes **Equality** function over two n-bit strings.

Sketch of the proof (2/4)

- ▷ Let E_N require ℓ intersections when generated from $\mathcal{G}_N$.
- ▷ Write $N = 2^n$. Fix natural bijection $\varphi \colon [N] \times [N] \to \{0,1\}^{2n}$.
- ▷ Define $f \colon \{0,1\}^{2n} \to \{0,1\}$ by $f^{-1}(1) \stackrel{\text{def}}{=} \varphi(E_N) \subseteq \{0,1\}^{2n}$.

$\begin{bmatrix} 1 & & \vec{0} \\ & \ddots & \\ \vec{0} & & 1 \end{bmatrix}$ becomes **Equality** function over two n-bit strings.

Lemma. If $\mathsf{SIZE}(f) \leq s$ then $D_\cap(E_N \mid \mathcal{G}_N) \leq s$.

Sketch of the proof (2/4)

- ▷ Let E_N require ℓ intersections when generated from $\mathcal{G}_N$.
- ▷ Write $N = 2^n$. Fix natural bijection $\varphi\colon [N] \times [N] \to \{0,1\}^{2n}$.
- ▷ Define $f\colon \{0,1\}^{2n} \to \{0,1\}$ by $f^{-1}(1) \stackrel{\text{def}}{=} \varphi(E_N) \subseteq \{0,1\}^{2n}$.

$\begin{bmatrix} 1 & & \vec{0} \\ & \ddots & \\ \vec{0} & & 1 \end{bmatrix}$ becomes **Equality** function over two n-bit strings.

Lemma. If $\mathsf{SIZE}(f) \leq s$ then $D_\cap(E_N \mid \mathcal{G}_N) \leq s$.

Idea: A boolean circuit C computing f generates the set $f^{-1}(1)$ starting from sets $x_1, \ldots, x_{2n}, \overline{x_1}, \ldots, \overline{x_{2n}} \subseteq \{0,1\}^{2n}$.

Sketch of the proof (3/4)

Lemma. If $\mathsf{SIZE}(f) \leq s$ then $D_\cap(E_N \,|\, \mathcal{G}_N) \leq s$.

$\triangleright$ A circuit of size s for f generates a sequence:

$x_1, \ldots, x_{2n}, \overline{x_1}, \ldots, \overline{x_{2n}}, B_1, \ldots, B_s = f^{-1}(1) \subseteq \{0,1\}^{2n}.$

Sketch of the proof (3/4)

Lemma. If $\mathsf{SIZE}(f) \leq s$ then $D_\cap(E_N \,|\, \mathcal{G}_N) \leq s$.

$\triangleright$ A circuit of size s for f generates a sequence:

$$x_1, \ldots, x_{2n}, \overline{x_1}, \ldots, \overline{x_{2n}}, B_1, \ldots, B_s = f^{-1}(1) \subseteq \{0,1\}^{2n}.$$

$\triangleright$ Get from this and bijection φ a construction of E_N from $\mathcal{G}_N$:

Example: $\varphi^{-1}(B_s) = E_N \subseteq [N] \times [N]$.

Sketch of the proof (3/4)

Lemma. If $\mathsf{SIZE}(f) \leq s$ then $D_{\cap}(E_N \,|\, \mathcal{G}_N) \leq s$.

▷ A circuit of size s for f generates a sequence:

$$x_1, \ldots, x_{2n}, \overline{x_1}, \ldots, \overline{x_{2n}}, B_1, \ldots, B_s = f^{-1}(1) \subseteq \{0,1\}^{2n}.$$

▷ Get from this and bijection φ a construction of E_N from $\mathcal{G}_N$:

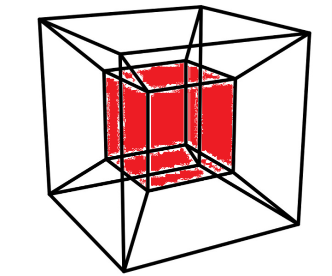
Example: $\varphi^{-1}(B_s) = E_N \subseteq [N] \times [N]$.

Crucial: Need to generate $\varphi^{-1}(x_i)$ and $\varphi^{-1}(\overline{x_j}) \subseteq [N] \times [N]$ from row and column matrices in $\mathcal{G}_N$. **Can be done without $\cap$.**

Sketch of the proof (4/4)

Crucial: Need to generate $\varphi^{-1}(x_i)$ and $\varphi^{-1}(\overline{x_j}) \subseteq [N] \times [N]$ from row and column matrices in $\mathcal{G}_N$. **Can be done without $\cap$.**

The space $\{0,1\}^4$ and its **"red"** subspace $x_4 \subseteq \{0,1\}^4$



The corresponding set in $[4] \times [4]$ via the bijection φ.

$$
\begin{array}{c} \\ 00 \\ 01 \\ 10 \\ 11 \end{array}
\begin{array}{c}
\begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\
\begin{bmatrix} 0 & \mathbf{1} & 0 & \mathbf{1} \\ 0 & \mathbf{1} & 0 & \mathbf{1} \\ 0 & \mathbf{1} & 0 & \mathbf{1} \\ 0 & \mathbf{1} & 0 & \mathbf{1} \end{bmatrix}
\end{array}
$$

3. An approach to estimate $D_{\cap}(A \,|\, \mathcal{B})$

- A is an arbitrary set contained in ambient space Γ.
- $\mathcal{B}$ is a collection of subsets of Γ.

Intersections and Cover Problems

- Would like to lower bound $\boldsymbol{D_\cap(A \mid \mathcal{B})}$.
- Can adapt "**fusion method**" (Razborov/Karchmer) to show:

$$\rho(A, \mathcal{B}) \;\leq\; \boldsymbol{D_\cap(A \mid \mathcal{B})} \;\leq\; \rho(A, \mathcal{B})^2.$$

Intersections and Cover Problems

- Would like to lower bound $\boldsymbol{D_\cap(A \mid \mathcal{B})}$.
- Can adapt "**fusion method**" (Razborov/Karchmer) to show:

$$\rho(A, \mathcal{B}) \ \leq \ \boldsymbol{D_\cap(A \mid \mathcal{B})} \ \leq \ \rho(A, \mathcal{B})^2.$$

Reduces complexity lower bounds to the analysis of "static" 2-dimensional cover problems.

Intersections and Cover Problems

- ▷ Would like to lower bound $\boldsymbol{D_\cap(A \,|\, \mathcal{B})}$.
- ▷ Can adapt "**fusion method**" (Razborov/Karchmer) to show:

$$\rho(A, \mathcal{B}) \;\le\; \boldsymbol{D_\cap(A \,|\, \mathcal{B})} \;\le\; \rho(A, \mathcal{B})^2.$$

Reduces complexity lower bounds to the analysis of "static" 2-dimensional cover problems.

- ▷ By adapting the work of Nakayama-Maruoka,

$$\rho(A, \mathcal{B}) \;=\; D_\cap^{\circlearrowright}(A \,|\, \mathcal{B}) \quad \text{(intersections in } \circlearrowright\text{-networks)}$$

Intersections and Cover Problems

- Would like to lower bound $\boldsymbol{D_\cap(A \,|\, \mathcal{B})}$.
- Can adapt "**fusion method**" (Razborov/Karchmer) to show:

$$\rho(A,\mathcal{B}) \;\leq\; \boldsymbol{D_\cap(A \,|\, \mathcal{B})} \;\leq\; \rho(A,\mathcal{B})^2.$$

Reduces complexity lower bounds to the analysis of "static" 2-dimensional cover problems.

- By adapting the work of Nakayama-Maruoka,

$$\rho(A,\mathcal{B}) \;=\; D_\cap^{\circlearrowright}(A \,|\, \mathcal{B}) \quad \text{(intersections in } \circlearrowright\text{-\textbf{networks})}$$

- **Connections to other areas/problems + applications?**

References and Related Work

- Bruno Cavalar and Igor C. Oliveira.
  Boolean function complexity and two-dimensional cover problems.
  Preprint, 2024.
- Stasys Jukna.
  Computational complexity of graphs (book chapter).
  Advances in Network Complexity, Quantitative and Network Biology, 2013.
- Mauricio Karchmer.
  On proving lower bounds for circuit size.
  In *Structure in Complexity Theory Conference (CCC)*, pages 112–118, 1993.
- Katsutoshi Nakayama and Akira Maruoka.
  Loop circuits and their relation to Razborov's approximation model.
  Inf. Comput., 119(2):154–159, 1995.
- Pavel Pudlák, Vojtech Rödl, and Petr Savický.
  Graph complexity.
  Acta Inf., 25(5):515–535, 1988.
- Alexander A. Razborov.
  On the method of approximations.
  In *Symposium on Theory of Computing (STOC)*, pages 167–176, 1989.
- Avi Wigderson.
  The fusion method for lower bounds in circuit complexity.
  In *Combinatorics, Paul Erdos is Eighty*, pages 453–467, 1993.
- Uri Zwick.
  On the number of ANDs versus the number of ORs in monotone boolean circuits.
  Inf. Process. Lett., 59(1):29–30, 1996.

Appendix: Cover complexity (1/3)

Appendix: Definition of $\rho(A, \mathcal{B})$.

▷ Let $A^c \stackrel{\text{def}}{=} \Gamma \setminus A$, where Γ is the *ambient space*.

▷ A is *non-trivial*, i.e., both A and A^c are non-empty.

▷ $\mathcal{B}$ is a collection of subsets of Γ.

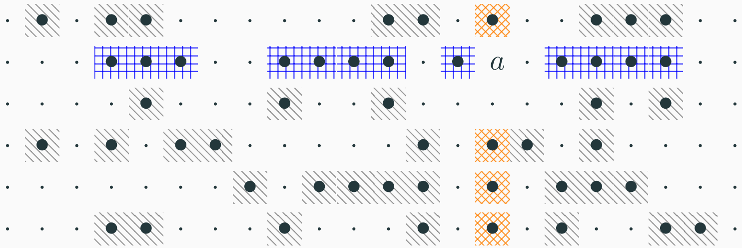
Definition (Semi-filter)
A non-empty family $\mathcal{F} \subseteq \mathcal{P}(U)$ is a *semi-filter* over U if the following hold:

- *(upward closure)* If $U_1 \in \mathcal{F}$ and $U_1 \subseteq U_2 \subseteq U$, then $U_2 \in \mathcal{F}$.
- *(non-trivial)* $\emptyset \notin \mathcal{F}$.

▷ We will always use $U \stackrel{\text{def}}{=} A^c$.

Appendix: Cover complexity (2/3)

Definition (Semi-filter above $a \in A$)
$\mathcal{F}$ is *above* an element $a \in A$ (with respect to $\mathcal{B}$) if for every $B \in \mathcal{B}$, if $a \in B$ then $B \cap A^c \in \mathcal{F}$.



Definition (Preservation of pairs of subsets)
Let $\Lambda = \{(E_1, H_1), \ldots, (E_\ell, H_\ell)\}$ be a family of pairs of subsets of A^c. $\mathcal{F}$ *preserves* a pair (E_i, H_i) if $E_i \in \mathcal{F}$ and $H_i \in \mathcal{F}$ imply $E_i \cap H_i \in \mathcal{F}$. $\mathcal{F}$ *preserves* Λ if it preserves every pair in Λ.

Appendix: Cover complexity (3/3)

Definition (Cover complexity)
$\rho(A, \mathcal{B})$ is the minimum size of a collection Λ of pairs of subsets of A^c such that there is no semi-filter $\mathcal{F}$ that preserves Λ and is above an element $a \in A$.

Theorem. The following results hold:

$$\rho(A, \mathcal{B}) \leq D_{\cap}(A \,|\, \mathcal{B}) \leq \rho(A, \mathcal{B})^2 \quad \text{and} \quad \rho(A, \mathcal{B}) = D_{\cap}^{\circlearrowright}(A \,|\, \mathcal{B})$$

Corollary: k-Clique (for $k = 3$) monotone lower bounds of Razborov extend to **number of intersections** in **monotone** $\circlearrowright$**-networks**: $\widetilde{\Theta}(n^3)$ intersections needed to detect a triangle.