On the Quantum Automatability of Propositional Proof Systems

Noel Arteche, [1] Gaia Carenini [2] Matthew Gray [3]

[1]Lund University [2]École Normale Supérieure - PSL [3]University of Oxford

Abstract

We prove the first hardness results against efficient proof search by quantum algorithms. We show that under standard lattice-based cryptographic assumptions, no quantum algorithm can weakly automate $\mathbf{TC}^0$-Frege. This extends the line of results of Krajíček and Pudlák (*Information and Computation*, 1998), Bonet, Pitassi and Raz (*FOCS*, 1997), and Bonet, Domingo, Gavalda, Maciel and Pitassi (*Computational Complexity*, 2004), who showed that Extended Frege, $\mathbf{TC}^0$-Frege and $\mathbf{AC}^0$-Frege, respectively, cannot be weakly automated by classical algorithms if either the RSA cryptosystem or the Diffie-Hellman key exchange protocol are secure. To the best of our knowledge, this is the first interaction between quantum computation and propositional proof search.

Automatability ~ (Efficient) Proof Search

How Hard is to Find Proofs?

$$\text{CNF Formula } \mathcal{F} \to \underbrace{\text{Deterministic Algorithm } \mathcal{A}}_{\text{time?}} \to \text{Proof } \mathcal{P} : \begin{cases} \text{satisfying assignment}, & \text{if } \mathcal{F} \in \text{SAT} \\ \text{refutation}, & \text{if } \mathcal{F} \in \text{UNSAT} \end{cases}$$

- Running time at least $|\mathcal{F}| + |\mathcal{P}|$;
- Focus on UNSAT
  - if $\mathcal{F}$ has refutation of poly-size, $\exists$ algorithm that finds a refutation in poly-time?
  - Or anything better than trivial 2^n?
- Problem is in $\mathbf{NP}$, so any "impossibility" results are at least under $\mathbf{P} \neq \mathbf{NP}$.

(Frege) Proof Systems

Proof system $\mathcal{S}$ is a proof-verification algorithm, such that:

$$(\mathcal{F}, \mathcal{P}) \to \underbrace{\text{Verification by } \mathcal{S}}_{\text{poly-time}} \to (\mathcal{F}, \mathcal{P}) \text{ accepted} \iff \mathcal{P} \text{ is a proof of } \mathcal{F}$$

- $\mathcal{F}$ has a $\mathcal{S}$-proof $\iff$ $\mathcal{F} \in$ Taut.

Frege system, $Fr(K, R)$, is a proof system, where:

- K: finite functionally complete set of Boolean connectives;
- R: finite set of rules of the form: $$\frac{B_1, \dots, B_n}{B}$$

where $B_1, \dots, B_n, B$ are formulas built on a set of variables using $K-$connectives.

Frege proofs are sequences of formulas derived sequentially by using $R-$rules.

$\mathbf{TC}^0-$Frege is the subsystem of Frege where each rule can be "computed" by $\mathbf{TC}^0$ circuits.

How Hard is to Find Proofs in Proof System $\mathcal{S}$?

Proof system $\mathcal{S}$ is automatable in time $f(N)$ if $\exists$ algorithm:

$$\text{UNSAT CNF Formula } \mathcal{F} \to \underbrace{\text{Deterministic Algorithm } \mathcal{A}}_{\text{time } f(s)} \to \text{Refutation in Proof System } \mathcal{S}$$

where s is the size of the smallest refutation of $\mathcal{F}$ in proof system $\mathcal{S}$.

- Best running time we can hope for $|\mathcal{F}| + s$;
- Here we are asking for time poly($|\mathcal{F}| + s$).

$\mathcal{S}, \mathcal{S}'$: proof systems.

$$\mathcal{S}' \text{ simulates (in time } t) \ \mathcal{S} \iff \begin{cases} \mathcal{S}' \text{ and } \mathcal{S} \text{ verify the same formulas} \\ \mathcal{S} - \text{proofs can be converted in } \mathcal{S}' - \text{proof (in time } t) \end{cases}$$

Proof system $\mathcal{S}$ is weakly automatable if $\exists$ proof system $\mathcal{S}'$ (simulating $\mathcal{S}$) which is automatable.

The State of the Play

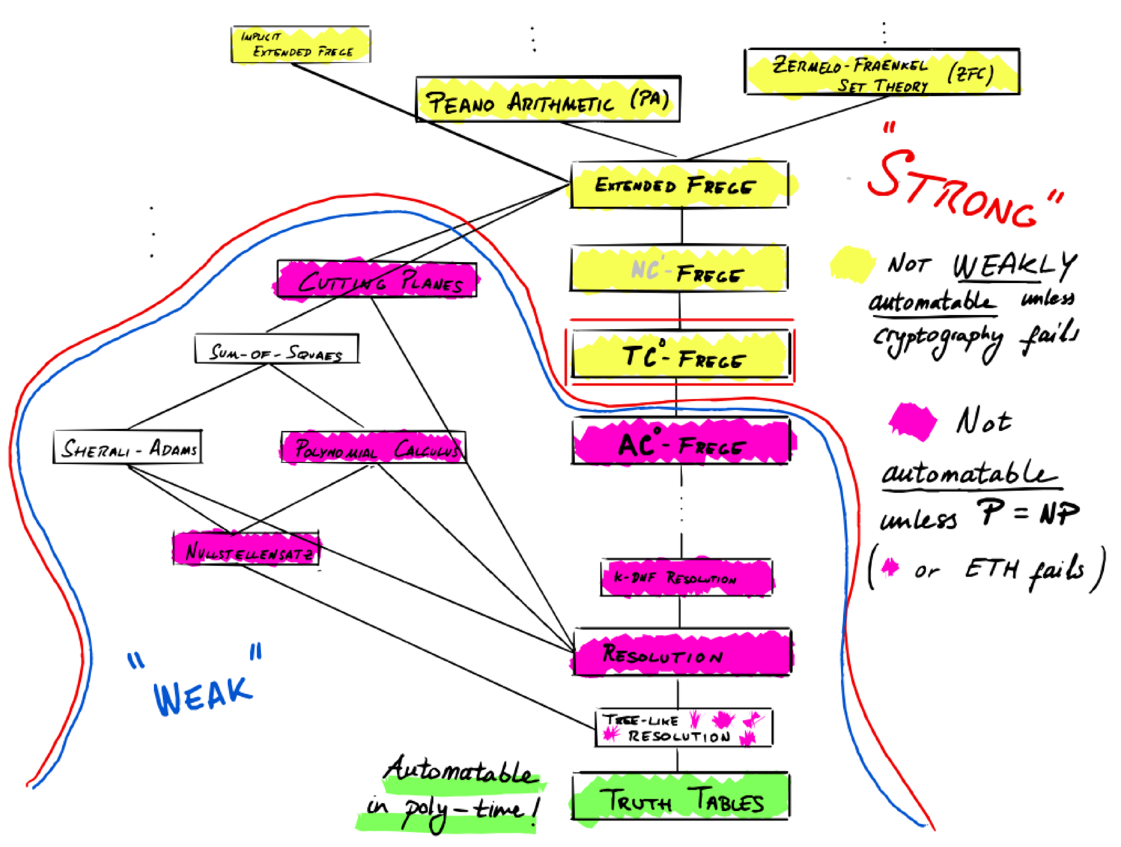

Figure 1. Overview of existing non-automatability results in classical framework.

Automatability of Strong Proof Systems

A, B : formulas. $\mathcal{S}$ has feasible interpolation property if short $\mathcal{S}-$refutation of $A(x, z) \wedge B(y, z) \to$ small circuit that given z outputs if A or B is unsat.

Impagliazzo's Observation. Weak automatability $\to$ feasible interpolation.

Theorem 1. (Krajíček and Pudlák 1998) Frege is weakly automatable $\to$ RSA cryptosystem can be broken by poly-size (classical) circuits.

Theorem 2. (Bonet, Pitassi, and Raz 1997) $\mathbf{TC}^0-$Frege is weakly automatable $\to$ Diffie-Hellman key exchange protocol can be broken by poly-size (classical) circuits. **Idea of the Proofs**

- Given "hard to invert injective function f" write a formula encoding $(f(x_0) = z) \wedge (f(x_1) = z)$;
- Since f is injective, this is an unsat formula;
- $(\mathbf{TC}^0)$-Frege has a short refutation of $(f(x_0) = z) \wedge (f(x_1) = z)$, then:

$$(\mathbf{TC}^0)\text{-Frege has feasible interpolation} \to f \text{ is not hard to invert.}$$

Our Contribution

Our Research Questions

- Which is the natural way of defining automatability in quantum setting?
- RSA is broken by quantum algorithms, can we prove non-quantum automatability under post-quantum cryptographic question?

Our Results

Quantum Automatability.

$$\text{UNSAT CNF Formula } \mathcal{F} \to \underbrace{\text{Quantum Algorithm } \mathcal{A}}_{\text{q-time } f(N)} \to \text{Refutation in Proof System } \mathcal{S}$$

Lemma. Quantum weak automatability$\to$ feasible interpolation by quantum circuits?

Main Theorem. If there exists a quantum algorithm that weakly automates $\mathbf{TC}^0$-Frege, then the Learning with Errors (LWE) problem can be solved by poly-size quantum circuits.

Outline of the Proof

We show that: Feasible Interpolation$\to$ Inverse of a (candidate) One-Way Function $\mathcal{F}$ efficiently!

Assuming the One-Wayness of $\mathcal{F}$, TC^0-Frege cannot have feasible interpolation, and by Impagliazzo's observation, we deduce that it is not automatable. There are *only* two important steps:

1. Designing a suitable $\mathcal{F}$ and an unsatisfiable split formula $\varphi_{\mathcal{F}}$;
2. Proving inside TC^0-Frege that $\varphi_{\mathcal{F}}$ is unsatisfiable .

Candidate One-Way Function and Split Formula

For every matrix $A \in \mathbb{Z}_q^{m \times n}$, we define the function:

$$\mathcal{F}_A : \mathbb{Z}_q^n \times \{\varepsilon \in \mathbb{Z}_q^m : |\varepsilon| \leq C\sqrt{mn}\} \to \mathbb{Z}_q^m, \ \mathcal{F}_A(s, \varepsilon) = (As + \varepsilon) \bmod q \,.$$

Inverting $\mathcal{F}_A \to$ Inverting LWE (conjectured to be hard on average!)

Informally, our split formula is the following:

$$\varphi_{\mathcal{F}} = (\mathcal{F}_A(x) = z \wedge x(1) = 0) \wedge (\mathcal{F}_A(y) = z \wedge y(1) = 1)$$

Note that if $\mathcal{F}_A$ is injective, then $\varphi_{\mathcal{F}}$ is indeed a contradiction, and almost all $\mathcal{F}_A$s, where $A \sim \mathcal{U}(\mathbb{Z}_q^{m \times n})$, are injective. We focus on these ones.

Unsatisfiability of the Split Formula in TC^0

We define an object $\texttt{Cert}(\mathcal{F}_A)$, such that:

- $\texttt{Cert}(\mathcal{F}_A) \to \mathcal{F}_A$ injective;
- $\mathcal{F}_A$injective $\to \texttt{Cert}(\mathcal{F}_A)$ exists with high probability;
- TC^0-Frege can "use" $\texttt{Cert}(\mathcal{F}_A)$ to prove $\mathcal{F}_A$injective.

$\texttt{Cert}(\mathcal{F}_A)$ is a pair (A_L^{-1}, W) such that (i) A_L^{-1} is the left-inverse of A, and (ii) $W = \{w_1, \dots, w_n\} \subseteq \mathcal{L}^*$ linearly independent vectors:

$$\max_{i \in [n]} ||w_i|| < 1/2C\sqrt{nm}$$

.

- **$\texttt{Cert}(\mathcal{F}_A) \to \mathcal{F}_A$ injective:**
  1. $A_L^{-1} \to$ Full-rank;
  2. $A(x - y) \in \mathcal{L} \geq \lambda_1(\mathcal{L})$ since $A(x - y) \in \mathcal{L}$;
  3. $\lambda_1(\mathcal{L}) > 2C\sqrt{nm}$ by hypothesis + Transference Theorem;
  4. $\varepsilon - \varepsilon' \leq 2C\sqrt{nm}$ by hypothesis;
  5. $3 + 4 \to$ Contradiction!
- **$\mathcal{F}_A$injective $\to \texttt{Cert}(\mathcal{F}_A)$ exists with high probability:**
  1. Counting arguments;
  2. Markov inequality.

Because of its non-determinism, TC^0-Frege can guess $\texttt{Cert}(\mathcal{F}_A)$!

We only need to show that TC^0-Frege:

- can verify the correctness of $\texttt{Cert}(\mathcal{F}_A)$;
- can prove that $\texttt{Cert}(\mathcal{F}_A) \to \mathcal{F}_A$.

For this purpose, we use an extension of the formal theory of linear algebra $\texttt{LA}$.

References

[1] Albert Atserias and María Luisa Bonet.
On the automatizability of resolution and related propositional proof systems.
Information and Computation, 189(2):182–201, 2004.

[2] P. Beame and T. Pitassi.
Simplified and improved resolution lower bounds.
In *Proceedings of 37th Conference on Foundations of Computer Science*, pages 274–282, 1996.

[3] Maria Luisa Bonet, Carlos Domingo, Ricard Gavalda, Alexis Maciel, and Toniann Pitassi.
Non-automatizability of bounded-depth frege proofs.
computational complexity, 13:47–68, 2004.

[4] Maria Luisa Bonet, Toniann Pitassi, and Ran Raz.
On interpolation and automatization for frege systems.
SIAM Journal on Computing, 29(6):1939–1967, 2000.

[5] Jan Krajíček and Pavel Pudlák.
Some consequences of cryptographical conjectures for s_2^1 and ef.
Information and Computation, 140(1):82–94, 1998.

[6] Michael Soltys and Stephen Cook.
The proof complexity of linear algebra.
Annals of Pure and Applied Logic, 130(1):277–323, 2004.
Papers presented at the 2002 IEEE Symposium on Logic in Computer Science (LICS).

Acknowledgements

This work was done in part while the authors were visiting the Simons Institute for the Theory of Computing. The first author was supported by the Wallenberg AI, Autonomous Systems and Software Program (WASP) funded by the Knut and Alice Wallenberg Foundation.

 gaia.carenini@ens.psl.eu