Simulations between proof systems

Nikita Gaevoy

Saint Petersburg State University

FLoC Proof Complexity Workshop, August 1, 2022

Definitions

Definition

Let C be a class of circuits. A propositional proof system Π is C-simulated by propositional proof system Π' if and only if there exists a polynomial-time algorithm P such that for every tautology φ algorithm $P(\varphi, m)$ generates a circuit from class C that maps all Π-proofs of φ of the size m to Π'-proofs of φ.

Definitions

Definition

Let C be a class of circuits. A propositional proof system Π is C-simulated by propositional proof system Π' if and only if there exists a polynomial-time algorithm P such that for every tautology φ algorithm $P(\varphi, m)$ generates a circuit from class C that maps all Π-proofs of φ of the size m to Π'-proofs of φ.

If C is a class of all Boolean circuits, then C-simulation is equivalent to p-simulation.

Unbounded Case

Let Copy be the class of monotone NC-circuits of depth 1. In other words, the output bits of circuits from Copy could be either constants or copies of the input bits.

Theorem

Let Π be a p-optimal proof system. Then there exists a Copy*-optimal proof system Π'.*

Unbounded Case

Let Copy be the class of monotone NC-circuits of depth 1. In other words, the output bits of circuits from Copy could be either constants or copies of the input bits.

Theorem

Let Π be a p-optimal proof system. Then there exists a Copy-optimal proof system Π'.

It is important to note that it is crucial for the construction in the proof of the theorem above to allow Π' to have proofs of an arbitrary length, even the proof of lengths that can not be bound by any computable function of the size of the proven formula.

Bounded Case

Definition

An f-bounded propositional proof system is a proof system that given formula φ accepts only proofs of size at most $f(\varphi)$, where f is a polynomial-time function. An f-bounded proof system is called exactly bounded if it accepts only proofs of size exactly $f(\varphi)$.

Bounded Case

Definition

An f-bounded propositional proof system is a proof system that given formula φ accepts only proofs of size at most $f(\varphi)$, where f is a polynomial-time function. An f-bounded proof system is called exactly bounded if it accepts only proofs of size exactly $f(\varphi)$.

Lemma

If there exists an automatizable optimal proof system Π, then there exists an exactly bounded Copy*-optimal proof system Π'.*

Obtaining Bounded Proof Systems

- Any proof system could be made f-bounded just by rejecting too long proofs, if the size of the shortest proof never exceeds $f(\varphi)$.

Obtaining Bounded Proof Systems

- Any proof system could be made f-bounded just by rejecting too long proofs, if the size of the shortest proof never exceeds $f(\varphi)$.
- Any bounded proof system could be made exactly bounded by simply adding the padding to all short proofs.

Obtaining Bounded Proof Systems

- Any proof system could be made f-bounded just by rejecting too long proofs, if the size of the shortest proof never exceeds $f(\varphi)$.
- Any bounded proof system could be made exactly bounded by simply adding the padding to all short proofs.
- This operation changes the size of the shortest proof, which is important for the automatizability.

Obtaining Bounded Proof Systems

- Any proof system could be made f-bounded just by rejecting too long proofs, if the size of the shortest proof never exceeds $f(\varphi)$.
- Any bounded proof system could be made exactly bounded by simply adding the padding to all short proofs.
- This operation changes the size of the shortest proof, which is important for the automatizability.
- We can lose optimality, if the bound is too large.

Obtaining Bounded Proof Systems

- Any proof system could be made f-bounded just by rejecting too long proofs, if the size of the shortest proof never exceeds $f(\varphi)$.
- Any bounded proof system could be made exactly bounded by simply adding the padding to all short proofs.
- This operation changes the size of the shortest proof, which is important for the automatizability.
- We can lose optimality, if the bound is too large.
- This problem emerges only if NP $\neq$ coNP and it also could be avoided.

Main Results

Theorem

If there exists an exactly bounded proof system Π that is optimal under simulations with monotone circuits, then Π is automatizable.

Corollary

An automatizable p-optimal proof systems exists if and only if there exists an exactly bounded proof system that is optimal under simulations with monotone circuits.

Main Results

Theorem

If there exists an exactly bounded proof system Π that is optimal under simulations with monotone circuits, then Π is automatizable.

Corollary

An automatizable p-optimal proof systems exists if and only if there exists an exactly bounded proof system that is optimal under simulations with monotone circuits.

Theorem

If there exists an exactly bounded AC^0-optimal proof system, then it is automatizable in expected polynomial time.

Relations to p-optimality

- The most interesting case is when p-optimal propositional proof systems exist and are not automatizable.

Relations to p-optimality

- The most interesting case is when p-optimal propositional proof systems exist and are not automatizable.
- There are two possibilities for nonexistence of C-optimal exactly bounded propositional proof systems in that case.

Relations to p-optimality

- The most interesting case is when p-optimal propositional proof systems exist and are not automatizable.
- There are two possibilities for nonexistence of C-optimal exactly bounded propositional proof systems in that case.
- The first one is that p-simulation by p-optimal systems can not be expressed with circuits from the class C.

Relations to p-optimality

- The most interesting case is when p-optimal propositional proof systems exist and are not automatizable.
- There are two possibilities for nonexistence of C-optimal exactly bounded propositional proof systems in that case.
- The first one is that p-simulation by p-optimal systems can not be expressed with circuits from the class C.
- The second one is that the size of the shortest proof in any p-optimal system can not be estimated in a polynomial time up to a polynomial of this size.