PPP-Completeness and Extremal Combinatorics

Romain Bourneuf
Joint work with Lukáš Folwarczný, Pavel Hubáček,
Alon Rosen and Nikolaj I. Schwartzbach

CoA 2023

Total search problems

Total search problems

Definition (Total search problem, TFNP)

- A search problem is *total* if all instances have a solution.

Total search problems

Definition (Total search problem, TFNP)

- A search problem is *total* if all instances have a solution.
- TFNP is the class of total search problems for which we can check in polytime if an answer is indeed a solution.

Total search problems

Definition (Total search problem, TFNP)

- A search problem is *total* if all instances have a solution.
- TFNP is the class of total search problems for which we can check in polytime if an answer is indeed a solution.

Example: Factoring

Input: Integer $n \geq 2$.
Solution : A prime factor of n.

Total search problems

Definition (Total search problem, TFNP)

- A search problem is *total* if all instances have a solution.
- TFNP is the class of total search problems for which we can check in polytime if an answer is indeed a solution.

Example: Factoring

Input: Integer $n \geq 2$.
Solution : A prime factor of n.

Many interesting problems in cryptography lie in TFNP.

Subclasses of TFNP

Subclasses of TFNP

TFNP subclasses are defined based on the mathematical argument used to prove the totality of a problem.

Subclasses of TFNP

TFNP subclasses are defined based on the mathematical argument used to prove the totality of a problem.

Classical Theorem (Weak Pigeonhole Principle)

If $f : [2n] \to [n]$ then there exist $x \neq y \in [2n]$ s.t. $f(x) = f(y)$.

Subclasses of TFNP

TFNP subclasses are defined based on the mathematical argument used to prove the totality of a problem.

Classical Theorem (Weak Pigeonhole Principle)

If $f : [2n] \to [n]$ then there exist $x \neq y \in [2n]$ s.t. $f(x) = f(y)$.

Definition (WeakPigeon [Jeřábek '15])

Input: Poly-sized circuit $H : \{0,1\}^n \to \{0,1\}^{n-1}$.
Solution : $x \neq y \in \{0,1\}^n$ s.t. $H(x) = H(y)$.

Subclasses of TFNP

TFNP subclasses are defined based on the mathematical argument used to prove the totality of a problem.

Classical Theorem (Weak Pigeonhole Principle)

If $f : [2n] \to [n]$ then there exist $x \neq y \in [2n]$ s.t. $f(x) = f(y)$.

Definition (WeakPigeon [Jeřábek '15])

Input: Poly-sized circuit $H : \{0,1\}^n \to \{0,1\}^{n-1}$.
Solution : $x \neq y \in \{0,1\}^n$ s.t. $H(x) = H(y)$.

PWPP is the class whose complete problem is WeakPigeon.

Subclasses of TFNP

TFNP subclasses are defined based on the mathematical argument used to prove the totality of a problem.

Classical Theorem (Weak Pigeonhole Principle)

If $f : [2n] \to [n]$ then there exist $x \neq y \in [2n]$ s.t. $f(x) = f(y)$.

Definition (WeakPigeon [Jeřábek '15])

Input: Poly-sized circuit $H : \{0,1\}^n \to \{0,1\}^{n-1}$.
Solution : $x \neq y \in \{0,1\}^n$ s.t. $H(x) = H(y)$.

PWPP is the class whose complete problem is WeakPigeon.

- Characterize PWPP: new complete problems from extremal combinatorics.

PWPP and Extremal Combinatorics

Definition (Extremal Combinatorics)

If the size of some object is large enough then some structure must appear.

PWPP and Extremal Combinatorics

Definition (Extremal Combinatorics)

If the size of some object is large enough then some structure must appear.

Classical Theorem (Ramsey's Theorem)

If G is a graph on 2^{2n} vertices, then G has a clique or an independent set of size n.

PWPP and Extremal Combinatorics

Definition (Extremal Combinatorics)

If the size of some object is large enough then some structure must appear.

Classical Theorem (Ramsey's Theorem)

If G is a graph on 2^{2n} vertices, then G has a clique or an independent set of size n.

Definition (Ramsey [Krajiček '05])

Input: Poly-sized circuit $C : \{0,1\}^{2n} \times \{0,1\}^{2n} \to \{0,1\}$.

Solution :
- $x, y \in \{0,1\}^{2n}$ such that $C(x,y) \neq C(y,x)$.
- $x_1, \dots, x_n$ that form a clique or an independent set.

Ramsey is PWPP-hard

Theorem [Komargodski, Naor, Yogev '19]

Ramsey is PWPP-hard.

Ramsey is PWPP-hard

Theorem [Komargodski, Naor, Yogev '19]

Ramsey is PWPP-hard.

Input: $H : \{0,1\}^{2n} \to \{0,1\}^{n/8}$, want to find a collision.

Ramsey is PWPP-hard

Theorem [Komargodski, Naor, Yogev '19]

Ramsey is PWPP-hard.

Input: $H : \{0,1\}^{2n} \to \{0,1\}^{n/8}$, want to find a collision.
Let G be a graph on $2^{n/8}$ vertices that has no clique or independent set of size n.

Ramsey is PWPP-hard

Theorem [Komargodski, Naor, Yogev '19]

Ramsey is PWPP-hard.

Input: $H : \{0,1\}^{2n} \to \{0,1\}^{n/8}$, want to find a collision.
Let G be a graph on $2^{n/8}$ vertices that has no clique or independent set of size n.
We consider the graph G' on vertex set $\{0,1\}^{2n}$ with an edge xy if and only if there is an edge $H(x)H(y)$ in G.

Ramsey is PWPP-hard

Theorem [Komargodski, Naor, Yogev '19]

Ramsey is PWPP-hard.

Input: $H : \{0,1\}^{2n} \to \{0,1\}^{n/8}$, want to find a collision.
Let G be a graph on $2^{n/8}$ vertices that has no clique or independent set of size n.
We consider the graph G' on vertex set $\{0,1\}^{2n}$ with an edge xy if and only if there is an edge $H(x)H(y)$ in G.
If we have a clique or independent set of size n in G', two of its vertices must form a collision.

Sperner Antichain Problem

Classical Theorem (Sperner, 1928)

If we have $> \binom{2n}{n}$ subsets of $[2n]$, then one of them is contained in another.

Sperner Antichain Problem

Classical Theorem (Sperner, 1928)

If we have $> \binom{2n}{n}$ subsets of $[2n]$, then one of them is contained in another.

Definition (Weak Sperner Antichain Problem)

Input: Poly-sized circuit $C : \{0,1\}^{\alpha+1} \to \{0,1\}^{2n}$, with $\alpha = \log \binom{2n}{n}$.
Solution: $x \neq y \in \{0,1\}^{\alpha+1}$, s.t. $C(x) \subseteq C(y)$.

Sperner Antichain Problem

Classical Theorem (Sperner, 1928)

If we have $> \binom{2n}{n}$ subsets of $[2n]$, then one of them is contained in another.

Definition (Weak Sperner Antichain Problem)

Input: Poly-sized circuit $C : \{0,1\}^{\alpha+1} \to \{0,1\}^{2n}$, with $\alpha = \log \binom{2n}{n}$.
Solution: $x \neq y \in \{0,1\}^{\alpha+1}$, s.t. $C(x) \subseteq C(y)$.

Theorem

Weak Sperner Antichain is PWPP-complete.

Proof sketch

Hardness: Variant of the graph-hash product.

Proof sketch

Hardness: Variant of the graph-hash product.
Take a large antichain and “blow it up”.

Proof sketch

Hardness: Variant of the graph-hash product.
Take a large antichain and "blow it up".

Inclusion: Let $N = \binom{2n}{n}$.

Proof sketch

Hardness: Variant of the graph-hash product.
Take a large antichain and "blow it up".

Inclusion: Let $N = \binom{2n}{n}$.
We have a "list" of $2N$ sets $S_1, \ldots, S_{2N}$.

Proof sketch

Hardness: Variant of the graph-hash product.
Take a large antichain and "blow it up".

Inclusion: Let $N = \binom{2n}{n}$.
We have a "list" of $2N$ sets $S_1, \ldots, S_{2N}$.
By Dilworth, partition $(2^{[2n]}, \subseteq)$ into N chains $C_1, \ldots, C_N$.

Proof sketch

Hardness: Variant of the graph-hash product.
Take a large antichain and "blow it up".

Inclusion: Let $N = \binom{2n}{n}$.
We have a "list" of $2N$ sets $S_1, \ldots, S_{2N}$.
By Dilworth, partition $(2^{[2n]}, \subseteq)$ into N chains $C_1, \ldots, C_N$.
Consider the circuit H which maps i to the unique j such that $S_i \in C_j$.

Proof sketch

Hardness: Variant of the graph-hash product.
Take a large antichain and "blow it up".

Inclusion: Let $N = \binom{2n}{n}$.
We have a "list" of $2N$ sets $S_1, \ldots, S_{2N}$.
By Dilworth, partition $(2^{[2n]}, \subseteq)$ into N chains $C_1, \ldots, C_N$.
Consider the circuit H which maps i to the unique j such that $S_i \in C_j$.
Collisions in H correspond to sets in the same chain.

From PWPP to PPP

Classical Theorem (Weak Pigeonhole Principle)

If $f : [2n] \to [n]$, $\exists x \neq y, f(x) = f(y)$.

From PWPP to PPP

Classical Theorem (Weak Pigeonhole Principle)

If $f : [2n] \to [n]$, $\exists x \neq y, f(x) = f(y)$.

Classical Theorem (Strong Pigeonhole Principle)

If $f : [n] \to [n]$, either $\exists x \neq y, f(x) = f(y)$, or f is a permutation.

From PWPP to PPP

Classical Theorem (Weak Pigeonhole Principle)

If $f : [2n] \to [n]$, $\exists x \neq y, f(x) = f(y)$.

Classical Theorem (Strong Pigeonhole Principle)

If $f : [n] \to [n]$, either $\exists x \neq y, f(x) = f(y)$, or f is a permutation.

Definition (Pigeon/PPP [Papadimitriou '94])

Input : Poly-sized circuit $C : \{0,1\}^n \to \{0,1\}^n$.

Solution :
- $x \neq y \in \{0,1\}^n$, s.t. $C(x) = C(y)$.
- $x \in \{0,1\}^n$, s.t. $C(x) = 0^n$.

Strong version of Sperner

Classical Theorem (Weak Sperner Theorem)

If we have $> \binom{2n}{n}$ subsets of $[2n]$, then one of them is contained in another.

Strong version of Sperner

Classical Theorem (Weak Sperner Theorem)

If we have $> \binom{2n}{n}$ subsets of $[2n]$, then one of them is contained in another.

Classical Theorem (Strong Sperner Theorem)

If we have exactly $\binom{2n}{n}$ subsets of $[2n]$, then either one of them is contained in another, or we have all n-subsets of $[2n]$.

Strong version of Sperner

Classical Theorem (Weak Sperner Theorem)

If we have $> \binom{2n}{n}$ subsets of $[2n]$, then one of them is contained in another.

Classical Theorem (Strong Sperner Theorem)

If we have exactly $\binom{2n}{n}$ subsets of $[2n]$, then either one of them is contained in another, or we have all n-subsets of $[2n]$.

Definition (Strong Sperner Antichain Problem)

Input: Poly-sized circuit $C : \{0,1\}^\alpha \to \{0,1\}^{2n}$, with $\alpha = \log \binom{2n}{n}$.
Solution: • $x \neq y$, s.t. $C(x) \subseteq C(y)$.
• x, s.t. $C(x) = [n]$.

Strong version of Sperner

Classical Theorem (Weak Sperner Theorem)

If we have $> \binom{2n}{n}$ subsets of $[2n]$, then one of them is contained in another.

Classical Theorem (Strong Sperner Theorem)

If we have exactly $\binom{2n}{n}$ subsets of $[2n]$, then either one of them is contained in another, or we have all n-subsets of $[2n]$.

Definition (Strong Sperner Antichain Problem)

Input: Poly-sized circuit $C : \{0,1\}^\alpha \to \{0,1\}^{2n}$, with $\alpha = \log \binom{2n}{n}$.
Solution: • $x \neq y$, s.t. $C(x) \subseteq C(y)$.
• x, s.t. $C(x) = [n]$.

Theorem

The problem Strong Sperner Antichain is PPP-complete.

Other results

Classical Theorem (Weak Erdős-Ko-Rado Theorem)

If $\mathcal{F}$ is a family of pairwise intersecting n-subsets of $[kn]$ then $|\mathcal{F}| \leq \binom{kn-1}{n-1}$.

Other results

Classical Theorem (Weak Erdős-Ko-Rado Theorem)

If $\mathcal{F}$ is a family of pairwise intersecting n-subsets of $[kn]$ then $|\mathcal{F}| \leq \binom{kn-1}{n-1}$.

Theorem

The problems associated to the Erdős-Ko-Rado Theorem are respectively PWPP-complete and PPP-complete.

Other results

Classical Theorem (Weak Erdős-Ko-Rado Theorem)

If $\mathcal{F}$ is a family of pairwise intersecting n-subsets of $[kn]$ then $|\mathcal{F}| \leq \binom{kn-1}{n-1}$.

Theorem

The problems associated to the Erdős-Ko-Rado Theorem are respectively PWPP-complete and PPP-complete.

- Similar results for Cayley's theorem on trees.

Overview & Open problems

Overview:

- We characterize the classes PWPP and PPP via problems from extremal combinatorics.

Overview & Open problems

Overview:

- We characterize the classes PWPP and PPP via problems from extremal combinatorics.
- We highlight a correspondence between the strong and weak versions of several classical theorems.

Overview & Open problems

Overview:

- We characterize the classes PWPP and PPP via problems from extremal combinatorics.
- We highlight a correspondence between the strong and weak versions of several classical theorems.
- From a proof theory viewpoint, the theorems are equivalent in some sense to the pigeonhole principle.

Overview & Open problems

Overview:

- We characterize the classes PWPP and PPP via problems from extremal combinatorics.
- We highlight a correspondence between the strong and weak versions of several classical theorems.
- From a proof theory viewpoint, the theorems are equivalent in some sense to the pigeonhole principle.

Open problems:

- What about other classical theorems (Turán,...)?

Overview & Open problems

Overview:

- We characterize the classes PWPP and PPP via problems from extremal combinatorics.
- We highlight a correspondence between the strong and weak versions of several classical theorems.
- From a proof theory viewpoint, the theorems are equivalent in some sense to the pigeonhole principle.

Open problems:

- What about other classical theorems (Turán,...)?
- Do we have Ramsey $\in$ PWPP?