Structural Complexity of Rational Interactive Proofs

Daniil Musatov[1,2] and Georgii Potapov[1]

[1]Moscow Institute of Physics and Technology
[2]Caucasus Mathematical Center at Adyghe State University

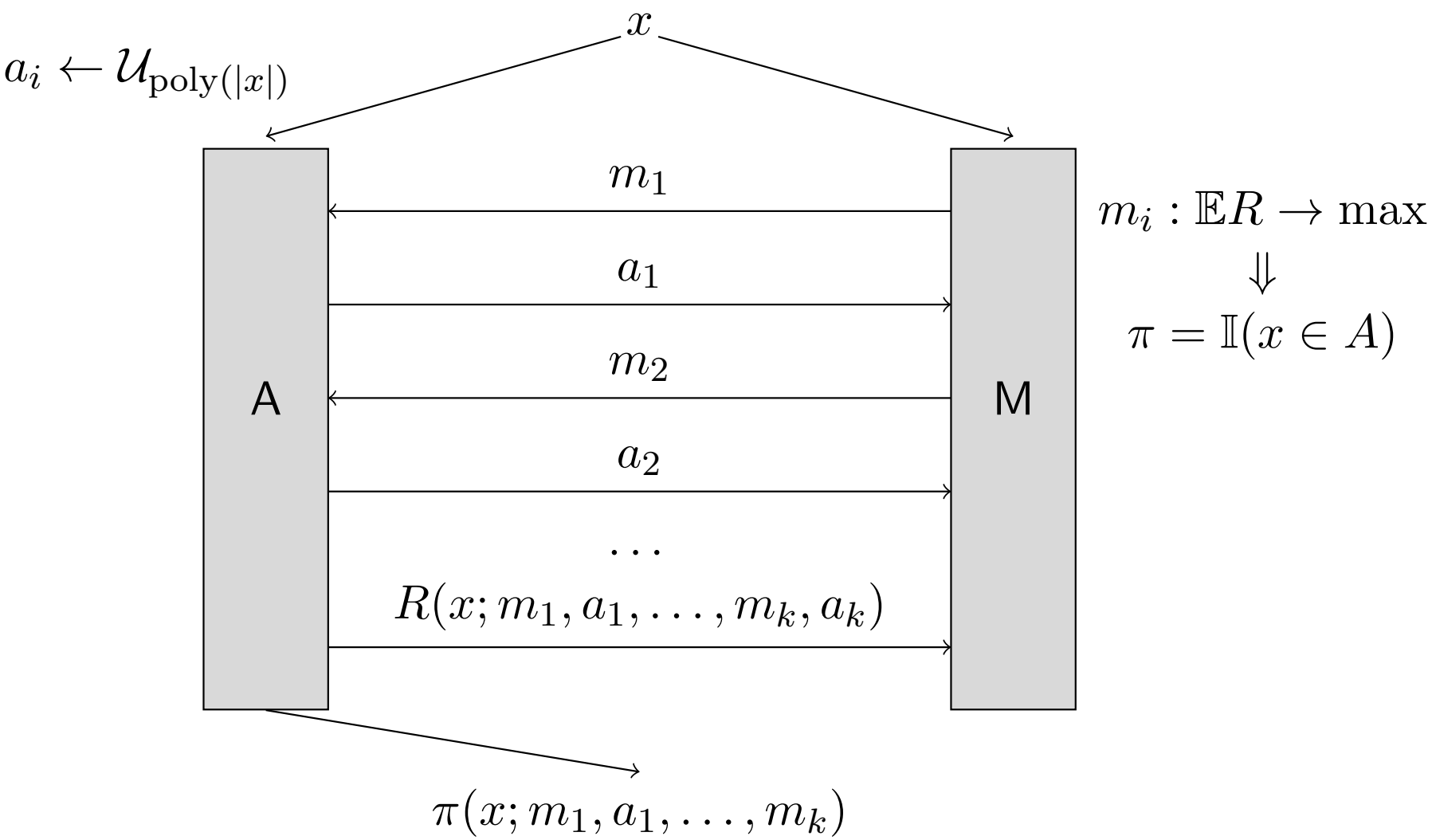
Computability in Europe 2023
July 25th, Batumi, Georgia

Introduction

In 2012, P. D. Azar and S. Micali introduced a new model of interactive proofs, called "Rational Interactive Proofs". In this model the prover is neither honest nor malicious, but rational in terms of maximizing his expected reward.

Rational interactive proofs provide a model for delegated computations and cloud computing, but they also introduce new classes that are interesting from the structural complexity point of view.

Definition (informal)



Definition (formal)

Definition

- Let Σ be a finite alphabet (e.g. $\Sigma = \{0, 1\}$). A protocol of a rational interactive proof with k rounds is defined by two polynomial time computable functions $R : \Sigma^* \to [0, 1]$, $\pi : \Sigma^* \to \{0, 1\}$. Let $x \in \Sigma^*$ be an instance of a problem.
- We use symbols $a_1, \ldots, a_k$ for Verifier's (Arthur's) messages and symbols $m_1, \ldots, m_k$ for Prover's (Merlin's) messages.
- Arthur's messages are chosen uniformly and independently from the sets of strings of length polynomial in $|x|$ *(although many of our results still hold for the model with private randomness)*.
- We say that the word x is accepted by the protocol if $\pi(x; m_1, a_1, \ldots, a_{k-1}, m_k) = 1$.
- We say that the value $R(x; m_1, a_1, \ldots, m_k, a_k)$ is the reward computed for the transcript $\mathcal{T} = (x; m_1, a_1, \ldots, m_k, a_k)$.

Rational Merlin and rational proofs

Definition

When talking about the protocol defined by functions R and π, we say that Merlin is rational, if $m_1, \ldots, m_k$ satisfy the following condition:

$$m_{i+1} \in \operatorname{Argmax}_m \mathbb{E}_{a_{i+1}} \max_{m_{i+2}} \ldots \max_{m_k} \mathbb{E}_{a_k} R(x; m_1, \ldots, a_i, m, a_{i+1}, \ldots, m_k, a_k),$$

in other words, in each round, Merlin chooses his message in a way that maximizes the expected reward.

Definition

We say that a rational interactive protocol recognizes set A, if for any x and any Merlin's rational behaviour, it holds that

$$x \in A \iff \pi(x; m_1, a_1, \ldots, a_{k-1}, m_k) = 1.$$

Finally, definitions of $\mathbf{DRMA}[k]$ and $\mathbf{FRMA}[k]$

Definition

Class $\mathbf{DRMA}[k]$ is the class of all languages recognised by some k-round rational interactive protocol.

Definition

Functional class $\mathbf{FRMA}[k]$ is defined in a similar manner with decision predicate π replaced by an arbitrary polynomial time computable function φ. A rational interactive protocol computes f if, for any Merlin's rational behavior, it holds that $\varphi(\mathcal{T}) = f(x)$.

Example of a $\mathbf{DRMA}[1]$-protocol

Reminder

Class $\mathbf{PP}$ is the class of all languages L for which there exists a polynomial p and a polynomial time computable predicate V such that

$$L = \left\{ x \in \Sigma^* \;\middle|\; V(x, y) = 1 \text{ for at least half of all } y \in \{0,1\}^{p(|x|)} \right\}.$$

For a language $L \in \mathbf{PP}$, consider the following protocol:

- $\pi(x; m) = m$ for Merlin's message $m \in \{0, 1\}$,
- $R(x; m, a) = \mathbb{I}\{m = V(x, a)\}$.

It is easy to see that the rational Merlin will "bet" on the actual majority among the values of $V(x, \cdot)$.

Example of a $\mathbf{FRMA}[1]$-protocol

Let V be a polynomial time computable predicate like before, and let $f(x) = \mathbb{E}_r V(x, r)$. Then $f \in \mathbf{FRMA}[1]$. To see this, consider the following protocol:

- $\varphi(x; m) = m$ (here we identify a binary string m with a binary expansion of a number $0.m_1 m_2 \dots m_{|m|} \in [0, 1]$),
- $R(x; m, a) = 1 - \big(m - V(x, a)\big)^2$.

Correctness of the protocol follows from the fact that for a random variable ξ it holds that $\mathbb{E}\xi = \operatorname{argmin}_c \mathbb{E}(\xi - c)^2$.

Known upper and lower bounds on $\mathbf{DRMA}[k]$

Theorem (P. D. Azar and S. Micali, 2012)

For all k:

$$C_k\mathbf{P} \subseteq \mathbf{DRMA}[k] \subseteq C_{2k+1}\mathbf{P},$$

where $C_k\mathbf{P}$ is the k-th level of the Counting hierarchy, defined as follows: $C_0\mathbf{P} = \mathbf{P},\ C_1\mathbf{P} = \mathbf{PP},\ C_{k+1}\mathbf{P} = \mathbf{PP}^{C_k\mathbf{P}}$.

For the lower bound, the idea of the proof is that, if an execution of a protocol Π uses a result obtained in a protocol Π', then it is possible to execute both protocols consequently if the reward for Π is scaled down so much that no gain in the altered execution of Π can validate any loss in the expected reward for Π'. Different variations of this idea are widely used in many works on rational proofs.

"Decomposition" of a rational proof

S. Guo et al. (2015) have studied similar compositions of rational and classical interactive proofs for a slightly different model. In our work, we study composition and "decomposition" of two rational proofs.

Lemma

For any integer $i, j \geq 0$, for any $\mathbf{FRMA}[i+j]$-protocol Π for computing function f there exists a function $\widetilde{f}$ that:

1. *for any x maps any transcript $\mathcal{T}_i$ of the first i rounds of interacting with a rational Merlin according to protocol Π on input x to $(E_i^{\Pi}(\mathcal{T}_i), f(x))$,*
2. *maps any transcript $\mathcal{T}_i$ of i rounds (i.e. of interaction between Arthur and an arbitrary prover) to $(E_i^{\Pi}(\mathcal{T}_i), v)$ for some v,*
3. *is in $\mathbf{FRMA}[j]$.*

Bounds for oracle computations

Theorem

For all $i, j \geq 0$, the following inclusions hold:

$$\mathbf{FRMA}[i+j] \subseteq \mathbf{FRMA}[i]^{(\mathbf{FRMA}[j])[1]} \subseteq \mathbf{FRMA}[i]^{||\mathbf{DRMA}[j]},$$

$$\mathbf{DRMA}[i+j] \subseteq \mathbf{DRMA}[i]^{(\mathbf{FRMA}[j])[1]} \subseteq \mathbf{DRMA}[i]^{||\mathbf{DRMA}[j]},$$

where "$[1]$" means that only one oracle query is allowed.

Remark

For the Counting Hierarchy, we have equality: $C_i\mathbf{P}^{C_j\mathbf{P}} = C_{i+j}\mathbf{P}$.

Polynomial time computations with $\mathbf{DRMA}[k]$-oracles

Theorem

$\mathbf{P}^{\mathbf{DRMA}[k]} = \mathbf{DRMA}[k]$ *for all* k.

Applying this theorem we can immediately obtain the following result.

Corollary

$\mathbf{P}^{\mathbf{PP}} \subseteq \mathbf{DRMA}[1]$.

Note that, according to the Toda's theorem, we have $\mathbf{PH} \subseteq \mathbf{P}^{\mathbf{PP}}$, but it is not known whether or not $\mathbf{PH}$ is in $\mathbf{PP}$. This makes us believe that the class $\mathbf{DRMA}[1]$ must be wider than $\mathbf{PP}$.

"Composition" of rational proofs

Using the obtained result on $\mathbf{P}^{\mathbf{DRMA}[k]}$, we can also prove the following technical lemma.

Lemma

If, for some numbers $i, j \geq 0$ and a language A there exists a $\mathbf{DRMA}[i]^{\mathbf{FRMA}[j]}$-protocol Π, such that oracle queries in it depend only on the input string and Arthur's random bits, but not on Merlin's messages, then $A \in \mathbf{DRMA}[i+j]$.

From this lemma, we can easily obtain the following theorem.

Theorem

$\mathbf{PP}^{\mathbf{DRMA}[k]} \subseteq \mathbf{DRMA}[k+1]$ *for all k.*

Other interesting corollaries

Now using the last theorem we can also obtain the following results.

Corollary

$\mathbf{PH}^{\mathbf{DRMA}[k]} \subseteq \mathbf{DRMA}[k+1]$ *for all* k.

Corollary

If $\mathbf{PP}^{\mathbf{DRMA}[k_0]} = \mathbf{DRMA}[k_0]$ *for some* k_0*, then the Counting Hierarchy collapses to* $(2k_0+1)$*-st level.*

Communication complexity

If for a language $L \subset \Sigma^*$ there exists a single round rational proof (π, R) such that for every x there is a rational Merlin's message of length $c(|x|)$ for some function c, then we say that $L \in \mathbf{DRMA}[1, c]$.
The example protocol from the beginning of our presentation shows that

$\mathbf{PP} \subseteq \mathbf{DRMA}[1, 1]$.

Thus, it is interesting to study the structure of the $\mathbf{DRMA}[1, c]$ "hierarchy".

Communication complexity of $\mathbf{PP}$

Theorem

$$\mathbf{PP} = \mathbf{DRMA}[1, O(\log n)].$$

Sketch of the proof:

1. The problem of comparing the expected rewards of any two possible messages is in $\mathbf{PP}$;
2. Due to the result by L. Fortnow and N. Reingold (1991), if L is truth-table reducible to some langueage in $\mathbf{PP}$, then the language L is itself in $\mathbf{PP}$.

What about $\oplus\mathbf{P}$?

S. Guo et al. (2014) also have studied the communication complexity of rational proofs. They have obtained a different generalisation of the fact that $\mathbf{PP} \in \mathbf{DRMA}[1,1]$ and have proven that one bit from Merlin is not enough for sublinear time Arthur to compute the parity of all bits of input, thus showing that a "scaled-down" version of a $\oplus\mathbf{P}$-problem cannot be solved with 1 bit from a rational Merlin.

Our result on communication complexity of $\mathbf{PP}$ shows that a superlogarithmic lower bound on communication complexity for problems in $\oplus\mathbf{P}$ will result in the separation of $\mathbf{PP}$ from $\oplus\mathbf{P}$.

Lower bound for $\oplus\mathbf{P}$ in a black-box model

Although we were unable to prove such a lower bound, we obtained a linear lower bound on the communication complexity of the protocols that only use a certificate verificator V from the definition of $\oplus\mathbf{P}$ as a random bit generator.

Theorem

There is no polynomial-time computable functions $R : \{0,1\}^* \to [0,1]$ *and* $\varphi : \{0,1\}^* \to \{0,1\}$ *such that for any* n *and* $0 \leq k \leq 2^n$ *the value of* $\varphi(1^n, m^*)$ *is equal to the parity of* k *where* $m^* \in \operatorname{Argmax}_m \mathbb{E}_{a,r} R(1^n, m, a, r)$, $|m^*| < \alpha n$ *for some constant* $\alpha \in (0,1)$, $a \sim \mathcal{U}_s$ *with* $s = \operatorname{poly}(n)$ *and* $r \in \{0,1\}^d$ *with* $d = \operatorname{poly}(n)$ *and bits of* r *being independently sampled from* $\operatorname{Bern}\left(\frac{k}{2^n}\right)$.

The idea is that, for fixed n, m, the reward function is a polynomial in the probability of nonuniform bits being equal to 1. If m is short, then some two of these polynomials of polynomial degree have to intersect in exponentially many points.

Thank you for your attention!