Vol.2010-AL-128 No.5
2010/1/26

Verification Procedures of Assisted Proofs by One-Way Finite Automata

(Abstract)

Tomoyuki Yamakami[†1]

A computational verification procedure of a "proof" given by a mighty prover has been discussed for decades using various mathematical models of interactive computation. We shall study in this work a situation in which a mighty prover presents a proof, either correct or erroneous, for its verification by a weak verifier, who runs a one-way finite (state) automaton. A more general interactive model has been studied in the literature[2),5)].

Now, we examine a special case where proofs are assisted by "advice," which is provided to the verifier, depending only on input size. The notion of such advice was first discussed in computational complexity theory[3)]. This notion was further applied to finite automata[1),6)–10)]. Loosely speaking, a proof w is said to be *assisted* by a piece of advice s if the verifier receives a string of the form $\left[\begin{smallmatrix} w \\ s \end{smallmatrix}\right]$, which is given for the verification of its correctness. One such proof-verification model is "nondeterminism." Using this model, we introduce a language family 1NRFA consisting of all languages A for which there exist a one-way reversible automaton (or $1rfa$) M and a proof alphabet Γ satisfying $A = \{x \mid \exists y \in \Gamma^n (M \text{ accepts } \left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right])\}$. By adding a piece of advice, we introduce a new advised family 1NRFA/n.

Another well-known proof-verification model is "Merlin-Arthur proof systems." We say that a language L over an alphabet Σ has an advised Merlin-Arthur proof system if there exist a one-way finite automaton (called Arthur) such that, for every input and any proof given by the prover (called Merlin), Arthur accepts the input with a help of advice if he can verify that the proof is correct; on the contrary, he rejects the input if he discovers that the proof is actually false.

†1 Department of Information Science, University of Fukui

Here, we consider three types of Merlins. The first type of Merlin deterministically chooses a string as a "proof" and sends it to Arthur, who runs a one-way quantum finite automaton (or 1qfa). Next, in a randomized Merlin model, Merlin chooses a probability distribution $D_x : \Gamma^n \to [0,1]$, generates a string y with probability $D_x(y)$, and sends it to Arthur. The error probability is calculated according to the probability distribution D_x as well as the 1qfa's internal measurement. Finally, we consider the model in which Merlin applies any quantum operation and gives Arthur a "quantum proof," which is a pure quantum state.

To make our notations readable, we use the prefix "MA" to indicate the deterministic Merlin model, "RMA" for the randomized Merlin model, and "QMA" for the quantum Merlin model. Using these notations, we define the following language families: MA($1qfa$)/n, RMA($1qfa$)/n, and QMA($1qfa$)/n.

In this work, we shall study the power and limitations of the aforementioned language families.

References

1) C. Damm and M. Holzer. Automata that take advice. In *Proc. MFCS 1995*, LNCS Vol.969, pp.149–152, Springer, 1995.
2) C. Dwork and L. Stockmeyer. Finite state verifier I: the power of interaction. *J. ACM* 39 (1992) 800–828.
3) R. M. Karp and R. Lipton. Turing machines that take advice. *LEnseignement Mathématique*. 2nd series, 28 (1982) 191–209.
4) H. Nishimura and T. Yamakami. Polynomial-time quantum computation with advice. *Inf. Process. Lett.* 90 (2004) 195–204.
5) H. Nishimura and T. Yamakami. An application of quantum finite automata to interactive proof systems. *J. Comput. Syst. Sci.* 75 (2009) 255-269.
6) K. Tadaki, T. Yamakami, and J. Lin. Theory of one tape linear time Turing machines. *Theor. Comput. Sci.* 411 (2010) 22–43.
7) T. Yamakami. Swapping lemmas for regular and context-free languages. Manuscript, 2008. See arXiv:0808.4122.
8) T. Yamakami. Immunity and pseudorandomness of context-free languages. Manuscript, 2009. See arXiv:0902.0261.
9) T. Yamakami. The roles of advice to one-tape linear-time Turing machines and finite automata. In *Proc. ISAAC 2009*, LNCS Vol.5878, pp.933–942, Springer, 2009.
10) T. Yamakami. One-way quantum finite automata with advice. Manuscript, 2009.