数理解析研究所講究録
1093 巻 1999 年 173-175

ゼロ知識証明の定式化について

一橋大学情報処理センター 奈古屋 広昭 (Hiroaki Nagoya) *

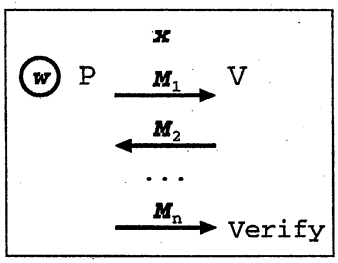
キーワード: ゼロ知識証明, Kolmogorov Complexity

1 はじめに

ゼロ知識証明の定式化には通信系列の識別不能性を示す必要があり、通常シミュレータを用いて証明するが、これを具体的なプロトコルにあてはめた場合に、そのプロトコルの直観的なイメージと証明の間にギャップがあるように思われる。そこで直観的な解釈により近い形で「ゼロ知識証明」を定式化できないかを考えてみてもよいであろう。本稿ではひとつの案として資源制約型の Kolmogorov Complexity を用いての定式化を試みてみた。

2 モデル

Prover P が秘密の情報 w を知っていることを Verifier V が n ラウンドの対話により検証するというモデルを考える (下図参照)。



ここで P, V は共に多項式時間計算の計算能力を持つ確率的チューリングマシン、x は P,V が共有する情報、$M_1 \ldots M_n$ は P と V の間の通信系列とする。このとき $M_1 \ldots M_n$ は確率変数となる。

3 Kolmogorov Complexity

x,y をビット列、U を 2 入力の (自然な) 万能チューリングマシンとする。このときに

$$K^t(x|y) = \min_p\{|p| \mid t(|x|) \text{ ステップ以内で } U(p,y) = x \text{ となる}\}$$

*nagoya@cc.hit-u.ac.jp

で x の (時間) 資源制約型 Kolmogorov Complexity $K^t(x|y)$ を定義する。ここで t は計算時間についての制約関数である。

4 定式化

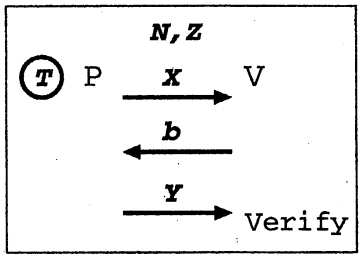
通信前に V が秘密情報 w について持っている知識は $K^t(w|x)$、通信後に V が秘密情報 w について持っている知識は $K^t(w|x, M_1, \ldots, M_n)$ であると考えられる。そこで高確率で前者と後者の差が小さい、たとえば

$$\Pr\left\{K^t(w|x) - K^t(w|x, M_1 \ldots M_n) < k \log |w|\right\} > 1 - 1/|w|^k$$

であるとき「ゼロ知識」であると考えることにする[1]。

5 具体例

次のような mod N での Z の平方根を知っているかどうかについての「ゼロ知識」証明プロトコルを考える。



1. P: R をランダムに選び $X \equiv R^2 \bmod N$ を V へ送る
2. V: $b \in \{0, 1\}$ をランダムに選び P へ送る
3. P: $Y \equiv T^b R \bmod N$ を V へ送る
4. V: $X \equiv Z^b Y^2 \bmod N$ かどうかチェック

このとき P と V の通信により V が得た T についての情報は $K^t(T|N, Z) - K^t(T|N, Z, X, b, Y)$ と考えられる。

一般的に $|u|$ と $|v|$ を固定したときに $2^{|u|}(1 - 1/2^c d)$ コ以上の u に対して

$$\Pr_v\left\{K^t(u|v) > |u| - c\right\} > 1 - d$$

となることが数え上げによって示せる。そこで T, N, Z を ℓ ビットの整数として、計算すると $1 - 2/\ell^k$ 以上の割合の T に対して

$$\Pr_{R,b}\left\{K^t(T|N, Z) - K^t(T|N, Z, X, b, Y) < 3 \log \ell\right\} > 1 - 1/\ell^k$$

[1]確率は P, V のランダムビットについて測る

であることがわかる[2]。したがってこのプロトコルは大部分のTに対して前節の「ゼロ知識」性を満たしていることになる。

6 まとめ

時間資源制約型の Kolmogorov Complexity を使って「ゼロ知識」性についての定式化を試み具体例をひとつ示した。

スタンダードなゼロ知識性との関係やきちんとした数学的な定式化がないと説得力に欠けるので、これを今後の課題としたい。

参考文献

[1] M. Bellare, M. Jakobsson and M. Yung, *Round-Optimal Zero-Knowledge Arguments Based on Any One-Way Function*, LNCS 1233, 1997.

[2] G.Brassard, D.Chaum and C.Crepeau, *Minimum Disclosure Proofs of Knowledge*, J. Computer and System Sciences, Vol. 37, 1988, pp. 156 - 189

[3] M. Li and P. Vitanyi, *Introduction to Kolmogorov Complexity and Its Applications*, Springer-Verlag, 1997

[4] L. Longpre and O. Watanabe, *On Symmetry of Information and Polynomial Time Invertibility*, Infomation and Computation, Vol 121, No.1, 1995

[5] 岡本龍明・太田和夫 共編, 暗号・ゼロ知識証明・数論, 共立出版, 1995

[2]正確には$< R, b >$が一様ランダムに分布しても$< X, b, Y >$は一様にはならないのでその分の補正が必要になる