

Stability of Kolmogorov type properties under
relativization.
(extended abstract)

An.Muchnik, Comp. center of RAS, Dep. of Cybernetics
email:muchnik@lpcs.math.msu.su

A.Romashchenko, IITP (Moscow) and LIP (Lyon)
email:anromash@mccme.ru

30 January 2006, Dagstuhl

Abstract

Let us have a tuple of strings x_1, \dots, x_n , and some oracle O . Assume that there is no information in O about x_i 's, i.e., $I(x_1, \dots, x_n; O) \approx 0$. Can any 'informational' properties of x_1, \dots, x_n essentially change under relativization conditional to the oracle O ? We discuss a formalization of this question and show that some special cases of these general conjecture hold.

We are talking about 'informational' properties of finite binary strings, i.e., about properties that can be expressed in terms of Kolmogorov complexity. We use the following notations for the *complexity profile*:

Notations 1. $\vec{C}(x_1, \dots, x_n) = (C(x_1), C(x_2), \dots, C(x_1, x_2), \dots)$

A very general form of algorithmic-informational property:

$$\forall y_1 \exists y_2 \forall y_3 \dots \vec{C}(x_1, \dots, x_n, y_1, \dots, y_m) \in A$$

where A is some set.

The relativized version of the same notations:

Notations 2.

$$\vec{C}(x_1, \dots, x_n|O) = (C(x_1|O), C(x_2|O), \dots, C(x_1, x_2|O), \dots),$$

where O is an oracle.

We want to compare the non-relativized properties of a tuple of strings x_1, \dots, x_n and relativized properties of the same tuple conditional to an oracle O .

Before relativization:

$$\forall y_1 \exists y_2 \forall y_3 \dots \vec{K}(x_1, \dots, x_n, y_1, \dots, y_m) \in A$$

After relativization:

$$\forall y_1 \exists y_2 \forall y_3 \dots \vec{K}(x_1, \dots, x_n, y_1, \dots, y_m | O) \in A'$$

It is natural to assume that the properties do not change essentially under relativization if there is no information about x_i 's in the oracle O .

Conjecture 1 (Main). *Kolmogorov complexity properties of a tuple $\bar{x} = \langle x_1, \dots, x_n \rangle$ does not change essentially under relativization with respect to an oracle O (i.e., $A \approx A'$) if and only if the mutual information $I(O : \bar{x}) = K(\bar{x}) - K(\bar{x}|O)$ is small.*

We cannot prove this conjecture in the most general case; further we consider some special cases of this statement.

A simple case: formulae without quantifiers

Theorem 1. *(trivial) Assume for some $\bar{x} = (x_1, \dots, x_n)$ and z*

$$I(\bar{x} : z) \leq \delta.$$

Then the distance between the profiles $\vec{K}(\bar{x})$ and $\vec{K}(\bar{x}|z)$ is at most $\delta + \mathcal{O}(\log K(\bar{x}, z))$.

More involved case: \exists -formulae with parameters

Theorem 2. *Assume for some \bar{x}, z*

$$I(\bar{x} : z) \leq \delta.$$

Then for any $\bar{y} = (y_1, \dots, y_m)$ there exists a $\bar{y}' = (y'_1, \dots, y'_m)$ such that the distance between the profiles $\vec{K}(\bar{x}, \bar{y})$ and $\vec{K}(\bar{x}, \bar{y}'|z)$ is at most $\delta + \mathcal{O}(\log K(\bar{x}, \bar{y}, z))$.

Conversation of theorem 2:

Conjecture 2. Assume for some $\bar{x} = (x_1, \dots, x_n)$ and z

$$I(\bar{x} : z) \leq \delta.$$

Then for any $\bar{y} = (y_1, \dots, y_m)$ there exists a $\bar{y}' = (y'_1, \dots, y'_m)$ such that the distance between $\vec{K}(\bar{x}, \bar{y}|z)$ and $\vec{C}(\bar{x}, \bar{y}')$ is at most $\delta + \mathcal{O}(\log C(\bar{x}, \bar{y}, z))$.

We cannot prove even Conjecture 2 for all strings x_i . But we can show this conjecture holds for an important class of tuples.

Definition 1. A string x is called (α, β) -stochastic if there exists a set $A \ni x$ such that

- $C(A) \leq \alpha$,
- $C(x|A) \geq \log |A| - \beta$

The class of (α, β) -stochastic tuples is defined similarly for any length of a tuple. We call $(\mathcal{O}(\log N), \mathcal{O}(\log N))$ -stochastic tuples just *stochastic*.

Theorem 3. Conjecture 2 holds for stochastic \bar{x} .

Further we formulate results concerning another interesting special case of the Main conjecture.

We say, that for some x_1, x_2 we can extract α bits of the mutual information between x_1 and x_2 with precision δ , if there exists y such that

$$C(y|x_i) \leq \delta$$

for $i = 1, 2$, and

$$C(y) \geq \alpha - \delta$$

It is easy to check that for any precision δ we cannot extract more than $I(x_1; x_2) + \delta + \mathcal{O}(\log C(x_1, x_2))$ bit of the mutual information. The nontrivial fact is that for some pairs of strings only a negligible part of the mutual information can be extracted (Gács–Körner 1973). In other words, the property of extractability of the mutual information cannot be determined by the complexity profile $\vec{C}(x_1, x_2)$.

Theorem 4. For any $C > 0$ there exists a D as follows. Assume for some x_1, x_2, O

$$I(x_1, x_2 : O) \leq C \log N,$$

and all $I(x_1; x_2)$ bits of the mutual information between x_1 and x_2 can be extracted with precision $C \log N$, given O as an oracle.

Then the mutual information between x_1 and x_2 can be extracted without relativization, with precision $D \log N$.

Thus, if in an oracle there is no information about a given pair of strings, then relativization conditional to this oracle cannot change the property of *extractability of the whole mutual information*. A natural question: does a similar statement hold for *extracting some part of the mutual information* between x_1 and x_2 ? We cannot prove this statement for logarithmic precision, but showed it holds for a more rough precision $o(N)$.

Theorem 5. *For any $f(N)$, $f(N) = o(N)$ there exists $g(N)$, $g(N) = o(N)$ as follows. Assume that for some x_1, x_2, O ,*

$$I(x_1, x_2 : O) \leq f(N),$$

(where $N = C(x_1, x_2, O)$), and α bits of the mutual information between x_1 and x_2 can be extracted given an oracle O , with precision $f(N)$.

Then α bits of the mutual information between x_1 and x_2 can be extracted without an oracle, with precision $g(N)$.

References

- [1] *Li M. and Vitányi P.*. An introduction to Kolmogorov complexity and its applications. // Second edition, Springer-Verlag, New York, 1997.
- [2] *Gács P., Körner J.* Common information is far less than mutual information. // Problems of Control and Information Theory, V. 2. 1973. P. 49-62.
- [3] *Ahlswede R., Körner J.* On common information and related characteristics of correlated information sources. // Presented at the 7th Prague Conf. on Inf. Th., Stat. Dec. Fct's and Rand. See also <http://www.mathematik.uni-bielefeld.de/ahlswede/pub/ahlswede/source.ps>
- [4] *Muchnik An.A.* On common information. // Theoretical Computer Science. V. 207. 1998. P. 319-328.
- [5] *Romashchenko A.* Extracting the Mutual Information for a Triple of Binary Strings. // Proc. 18th Annual IEEE Conference on Computational Complexity. 2003. P. 209-220.