Non-reducible descriptions for conditional Kolmogorov complexity

Andrej Muchnik* Alexander Shen† Mikhail Ustinov‡
Nikolai Vereshchagin§ Michael Vyugin¶

Abstract

Assume that a program p on input a outputs b. We are looking for a shorter program q having the same property ($q(a) = b$). In addition, we want q to be simple conditional to p (this means that the conditional Kolmogorov complexity $K(q|p)$ is negligible). In the present paper, we prove that sometimes there is no such program q, even in the case when the complexity of p is much bigger than $K(b|a)$. We give three different constructions that use the game approach, probabilistic arguments and algebraic arguments, respectively.

1 Definitions and statements

Let a and b be binary strings. Consider programs p such that $p(a) = b$ (the program p on input a outputs b). What is the minimal length of such a program? If the programming language is chosen appropriately, this length is close to $K(b|a)$, the conditional Kolmogorov complexity of b given a. We will ignore additive terms of order $O(\log n)$ where n is the maximum length of the strings involved. With this precision all the versions of Kolmogorov complexity (the plain one, the prefix one etc.) coincide. For the definition of Kolmogorov complexity $K(b)$ and $K(b|a)$ we refer to the textbook [2].

*Institute of New Technologies; e-mail: muchnik@lpcs.math.msu.su. The work was supported by RFBR grants 04-01-00427, 06-01-00122a.

†The work was supported by CNRS (LIF, Marseille, France; Poncelet laboratory, Moscow), STINT foundation, Uppsala university (Sweden), Royal Holloway College (UK), RFBR (grants 02-01-22001, 03-01-00475, 06-01-00122a) and Scientific schools supporting council (grant NSh-358.2003.1); e-mail: shen@mccme.ru, alexander.shen@lif.univ-mrs.fr.

‡Moscow State University, e-mail: mihail@ustinov.mccme.ru. The work was supported in part by the RFBR grants 02-01-22001, 03-01-00475, 06-01-00122a, NSh-358.2003.1.

§Moscow State University, e-mail: ver@mccme.ru. The work was supported in part by the RFBR grants 02-01-22001, 03-01-00475, 06-01-00122a, NSh-358.2003.1.

¶Moscow State University, e-mail: misha@vyugin.mccme.ru, misha@cs.rhul.ac.uk. The work was supported in part by the RFBR grants 02-01-22001, 03-01-00475, 06-01-00122a, NSh-358.2003.1.

To avoid references to a specific programming language we will consider "descriptions" instead of programs. A string p is called a conditional *description* of a string b given a if $K(b|a,p)$ is negligible. Here $K(b|a,p)$ stands for the conditional complexity of b given the pair $\langle a,p\rangle$. We will specify what is considered as "negligible" in each case.

For given a and b consider all strings p such that $K(b|a,p)\approx 0$. One can easily verify that the length of any such p is at least $K(b|a)$. This bound is tight. Both assertions are true with $O(\log n)$ precision; the same precision is required in the equality $K(b|a,p)\approx 0$.

We say that a description q is a *simplification* of a description p if $K(q|p)\approx 0$ with logarithmic precision. The relation $K(q|p)<\varepsilon$ is not transitive for a fixed ε: $K(q|p)<\varepsilon$ and $K(r|q)<\varepsilon$ imply only that $K(r|p)<2\varepsilon+O(\log n)$. However, this relation resembles a pre-ordering on strings and we are interested in the structure of the set of all conditional descriptions (for given a,b) with respect to this "pre-ordering".

The string b itself is a conditional description of b given a. Muchnik [1] has shown that, among all descriptions of b relative to a, there exists a description of minimal length ($\approx K(b|a)$) that is at the same time a simplification of b. We will prove that this is not true in the general case (for arbitrary description p instead of b): for some a,b there is a description p of complexity much larger than $K(b|a)$ that has no simplifications of length close to $K(b|a)$.

The exact statement is as follows:

Theorem 1. *There is a function $\varepsilon=\varepsilon(k,n)$ of order $O(\log(k+n))$ such that for all k,n there are strings a,b,p of lengths $n,2n,k$, respectively, having the following properties:*

(a) $K(b|a,p)\leqslant\varepsilon$ (*"the string p is a conditional description of b given a"*);

(b) $K(p|a)\geqslant k-\varepsilon$ (*"... that has complexity close to its length k even with condition a"*);

(c) *there is no string q such that $K(q)\leqslant k-n-\varepsilon$, $K(q|p)\leqslant n-\varepsilon$ and $K(b|a,q)\leqslant n-\varepsilon$* (*"$p$ has no simplifications of complexity $k-n$"*).

To be specific, in this theorem we have (quite arbitrary) chosen some relation between lengths of strings a and b. The statement is interesting when $k\gg 2n$ (e.g., if $k=4n$); it says that we have a description p that has high complexity k (even if a is known, so p is a "random" string independent of a), but there is no simplification of p that has complexity less than $k-n$ even if $k-n$ is much larger than the lower bound $K(b|a)$ which does not exceed $2n$ (the length of b). Note that the word "negligible" is understood in a rather strict way when we guarantee it in (a), but quite liberal for the adversary in (c) (the bounds for $K(q|p)$ and $K(b|a,q)$ are $n-\varepsilon$ which is much more than $O(\log n)$.

In the preliminary version of this paper [3] we gave a more natural (but weaker) version of this statement and three different proofs of it (using games, probabilistic arguments and explicit algebraic construction). The current version includes improvements made by two of us (M.U. and A.M.); to avoid repetitions now we give the game proof of Theorem 1 (Section 2), a probabilistic proof of a stronger statement (Theorem 2 below) and a combinatorial proof of a constructive version of Theorem 1 (Theorem 3 below).

Before formulating these improved statements, let us note that Theorem 1 is only interesting if k is bigger than $2n$. If k is close to $2n$ (or is less) then the statement of Theorem 1

becomes trivial. Indeed, if $k \leqslant 2n + O(\log n)$, let a be the empty string and let p and b be the same string of length $2n$ and complexity $k + O(\log n)$. If some q satisfies (c), then we get

$$K(b) = K(b|a) \leqslant K(q) + K(b|a, q) + O(\log n) \leqslant k - 2\varepsilon + O(\log n).$$

Since $k \leqslant 2n + O(\log n)$, if ε is big enough, this inequality contradicts the choice of b having complexity $k + O(\log n)$.

Theorem 1 asserts only that *there exists* a pair of strings $\langle a, b\rangle$ having a non-reducible description of b given a. Surprisingly, it turns out that *for all* $\langle a, b\rangle$ and k, except for trivial cases, there exists a non-reducible description p of b relative to a of complexity k. Here are the trivial cases:

(1) $K(a) \approx 0$; in this case the string b is a simplification of every description of b given a.

(2) $K(b|a) \approx 0$; in this case the empty string is a simplification of every description.

(3) k is much less than $K(b|a)$; in this case there is no conditional description p of b relative to a of complexity about k.

The exact statement is as follows:

Theorem 2. *There is a function $\varepsilon(k, n)$ of order $O(\log(k+n))$ such that for all k, n and all strings a, b such that*

$$K(a) > n + \varepsilon, \quad K(b|a) > 2n + \varepsilon, \quad k > K(b|a) + \varepsilon$$

there is a string p of length k having the properties (a), (b) *and* (c) *from Theorem 1.*

Note that Theorem 2 implies Theorem 1. Indeed, let ε in Theorem 1 be three times bigger than provided by Theorem 2. Assume that n, k are given. If $k < 2n + 2\varepsilon$ (where ε is the function from Theorem 2) then a, b can be constructed as in the remark above, without using Theorem 2. Otherwise let $n' = n - 2\varepsilon$ and let a and b be independent random strings of lengths n and $2n$, respectively. Then a, b, k, n' satisfy the conditions of Theorem 2 and the string p given by Theorem 2 together with a, b satisfies Theorem 1 (with 3ε in place of ε).

The proof of Theorem 2 is given in Section 3; it uses probabilistic arguments. Finally, in Section 4 we give a combinatorial proof of the following "constructive" version of Theorem 1.

Theorem 3. *Consider a finite field F of cardinality 2^n, a random point $a \in F$ and independent random linear function $p(x) = p_1 x + p_2$ from F to F. Let $b = p(a)$. Then $p = \langle p_1, p_2\rangle$ is a description of b relative to a of complexity about $2n$ that cannot be simplified: for all $i \leqslant n/4$ there is no string q such that $K(q) \leqslant 2n - 3i - \varepsilon$, $K(q|p) \leqslant i - \varepsilon$ and $K(b|a, q) \leqslant i - \varepsilon$. Here $\varepsilon = O(\log n)$.*

The independence requirement means that the triple $\langle a, p_1, p_2\rangle$ has complexity $3n + O(1)$. This theorem shows that for $3i$-decrease in the complexity of the description we have to pay i bits in the complexity of $K(q|p)$ ot $K(b|a, q)$, so no significant simplification of possible if these complexities remain negligible.

The authors are grateful to all participants of Kolmogorov seminar of the Department of Mathematics (Mathematical Logic and Theory of Algorithms Division) at Moscow University.

2 Game approach

Consider the following game we play against an adversary.

Let P, Q, A and B be finite sets (as we see later, they correspond to strings p, q, a, b respectively). On our moves we construct a partial function $\Xi\colon P \times A \to B$. At the start of the game the function Ξ is empty, and on each move we may define the value of Ξ at one point (once defined values cannot be changed later). Or we may skip the move, that is, we may leave Ξ unchanged.

The adversary on his moves constructs multi-valued functions $\Phi\colon P \to Q$ and $\Psi\colon Q \times A \to B$. That is, the values of Φ are subsets of Q, and the values of Ψ are subsets of B. Initially Φ and Ψ are empty (all their values are empty). At each move the adversary may add one new value to Φ (adding a new element to $\Phi(p)$ for some p) or Ψ (adding a new element to $\Psi(q, a)$ for some q, a). The existing elements cannot be removed. The adversary also may skip the move.

The adversary must obey the following rules: the function Φ takes on every argument at most φ values (i.e., $\#\Phi(p) \leqslant \varphi$ for any $p \in P$) and the function Ψ takes on every argument at most ψ values ($\#\Psi(q, a) \leqslant \psi$ for any q, a).

Players' moves alternate. Obviously, each player can make only finite number of non-trivial moves (moves that change the functions). Thus after a certain move all the three functions remain unchanged. The result of the game is defined as follows: we win if there exist $p \in P$, $a \in A$ and $b \in B$ such that $\Xi(p, a) = b$ and p, a, b are not "covered" by the adversary: the latter means that there is no $q \in \Phi(p)$ such that $b \in \Psi(q, a)$.

So the game is determined by the sets A, B, P and Q (actually, only their cardinalities matter) and the parameters φ and ψ. We represent the function Ξ as a table with $\#P$ rows and $\#A$ columns. The cells of this table initially are empty; they are filled by elements of B (each cell may contain at most one element).

The adversary fills the table for function Ψ. It has $\#Q$ rows of the same length $\#A$ as in our table. Each cell may contain up to ψ elements of B. The adversary also constructs the function Φ. It is convenient to represent this function by arrows going from row p of our table to all rows of adversary's table that belong to $\Phi(p)$. The out-degree is bounded by φ. We win if our table has a non-covered cell. A cell $\langle p, a\rangle$ is *covered* if its row is connected by an arrow to a row of adversary's table that has in the same column the same element of B (and, may be, some other elements). See Fig. 1.

The proof is based on the following simple observation:

Lemma 1. *If $\varphi \cdot \psi < \#B$ and $\varphi \cdot \#P + \psi \cdot \#A \cdot \#Q < \#A \cdot \#P$ then we have a winning strategy in the game.*

Proof. The first inequality guarantees that if Ξ is not yet defined on a pair $\langle p, a\rangle$ then we can choose a value $b = \Xi(p, a)$ so that the cell $\langle p, a\rangle$ is not covered (at the current step). Indeed, for each of at most φ values $q \in \Phi(a)$ there exist at most ψ values $b \in \Psi(q, a)$, so there exists b that is different from all those values.

Choosing b in this way (assuming that there are empty slots in Ξ-table), we guarantee that after each our move there exists a non-covered cell $\langle p, a\rangle$. Our move is non-trivial only

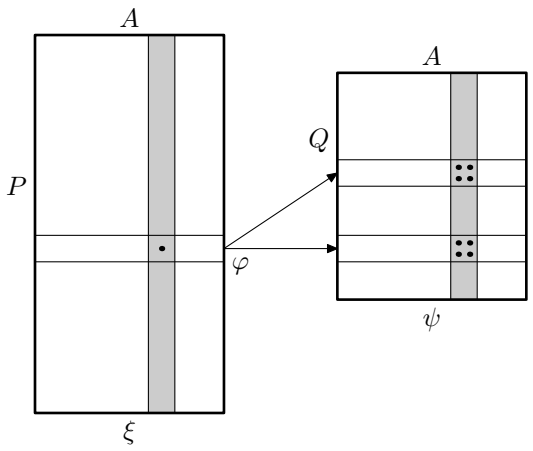

Figure 1: Cells of our table Ξ and adversary's table Ψ are filled with elements of B; each row of Ξ has at most φ outgoing edges, each cell of Ψ contains at most ψ elements.

when the previous adversary's move is non-trivial. The second inequality guarantees that the number of cells in Ξ-table is greater than the number of adversary's non-trivial moves (so the empty slots do exist). Indeed, for each of $\#P$ arguments the value of Φ may be changed at most φ times and for each of $\#A \cdot \#Q$ pairs $\langle q, a\rangle$ the value of Ψ may be changed at most ψ times.

Hence after every adversary's non-trivial move we can find an empty cell in Ξ-table and enter a value in it so that the cell becomes non-covered. The lemma is proved. □

Now we prove Theorem 1 using Lemma 1. Let A, B be the set of all strings of lengths $n, 2n$, respectively. Let P be the set of all strings of length k and let Q be the set of all strings of length less than $k - n$.

Let us fix the adversary's strategy now. Assume that the adversary includes in $\Phi(p)$ (one by one) all $q \in Q$ such that $K(q|p) < n - 2$, and includes in $\Psi(q, a)$ all the strings $b \in B$ such that $K(b|a, q) < n - 2$. One can do this effectively given n, as the function K is upper semi-computable (that is, the set $\{\langle x, y, l\rangle \mid K(x|y) < l\}$ is recursively enumerable). This strategy does not violate the rules provided $\varphi = \psi = 2^{n-2}$.

Let us verify that the conditions of Lemma 1 are satisfied:

$$\varphi \cdot \psi = 2^{n-4} < 2^n = \#B,$$

and

$$\varphi \cdot \#P + \psi \cdot \#A \cdot \#Q = 2^{n-2+k} + 2^{(n-2)+n+(k-n)} = 2^{n-1+k} < \#A \cdot \#P.$$

Therefore, by Lemma 1, we have a winning strategy in the game.

The winning strategy is computable given n, k. Applying it against the adversary's strategy described above we obtain a function Ξ that is computable given n, k (as the adversary's moves are computable, so are ours). To be precise we should write Ξ_{nk} indicating the dependence on n, k; complexity of algorithm that computes Ξ_{nk} is $O(\log(n + k))$ since Ξ_{nk} is

determined by n, k. Since our strategy is a winning one, there exists a cell $\langle p, a\rangle$ that is not covered after all non-trivial moves are performed. (It depends on n, k in a non-computable way, as we do not know which of the adversary's moves is the last non-trivial one.)

Let $b = \Xi(p, a)$ be the element in the "winning" cell of our table. Then $K(b|a, p) = O(\log(n + k))$. As the cell (p, a) is not covered, there is no string q of *length* less than $k - n$ such that $K(q|p) < n - 2$ and $K(b|a, q) < n - 2$. This is weaker than required: we want the statement to be true for all q of *complexity* less than $k - n - \varepsilon$ (and not the length less than $k - n$) . However it is easy to fix this. Replacing q by its shortest description we increase $K(b|a, q)$ and $K(q|p)$ by $O(\log(n + k))$ and this increase can be compensated by the choice of ε. It remains to fix only one problem: we want the complexity of p given a to be at least $k - \varepsilon$ and the rules of the game do not provide any guarantee for this.

Let us change the game allowing the adversary at any step to remove (="mark as unusable") any cell of the table of Ξ; in every column, the total number of removed cells should not exceed $\#P/2$, so at least half of cells remain intact. In the winning rule we require that the cell $\langle p, a\rangle$ has not been removed by the adversary. For the modified game the statement of Lemma 1 is changed as follows: in the right hand side of the inequality $\varphi \cdot \#P + \psi \cdot \#A \cdot \#Q < \#A \cdot \#P$ the term $\#A \cdot \#P$ is replaced by $\#A \cdot \#P/2$. The modified lemma is still true: Indeed, if we cannot perform any move then we have used all the non-removed cells, thus we have done $\#A \cdot \#P/2$ moves. And the conditions of the modified lemma are still fulfilled.

Other changes are as follows: the adversary removes all the cells $\langle p, a\rangle$ such that $K(p|a) < k-1$. It is clear that, in every column, at most half cells are removed. After this modification we know that for the winning cell $\langle p, a\rangle$ the complexity of p given a is at least $k - 1$, and the theorem is proved.

3 Probabilistic approach

Assume that finite sets A, B, P, Q are fixed. (They will play the same role as before.) Consider functions $\Xi\colon P \times A \to B$ and multi-valued functions $\Phi\colon P \to Q$, $\Theta\colon A \to P$ and $\Psi\colon Q \times A \to B$ having at most φ, θ and ψ values, respectively, for each argument. Call a pair $\langle a, b\rangle \in A \times B$ *covered* (for given Ξ, Φ, Θ, Ψ) if for all $p \in P \setminus \Theta(a)$ such that $\Xi(p, a) = b$ there is $q \in \Phi(p)$ such that $b \in \Psi(q, a)$. Let $B(a)$ denote the set of all $b \in B$ such that the pair $\langle a, b\rangle$ is covered.

Fix two natural parameters $\alpha \ll \#A$ and $\beta \ll \#B$ and call a function Ξ a *winning* function (cf. the game described above) if for all multi-valued Φ, Θ and Ψ satisfying given bounds on the number of values, it holds

$$\#\{a \in A \mid \#B(a) \geqslant \beta\} < \alpha.$$

If a function Ξ is winning, we can put its values in the table ignoring the adversary's moves and be sure that we win and, moreover, there will be many winning pairs $\langle a, b\rangle$: for almost all $a \in A$ for almost all $b \in B$ the pair $\langle a, b\rangle$ will be not covered.

Using probabilistic arguments, we will show the following

Lemma 2. *Let $s = (\beta - \varphi\psi)/\#B$. If*

$$2^{\#A}(2^{\#B}(1-s)^{\#P-\theta})^{\alpha} \cdot (\#Q)^{\varphi\cdot\#P} \cdot (\#P)^{\theta\cdot\#A} \cdot (\#B)^{\psi\cdot\#Q\cdot\#A} < 1$$

then there is a winning function.

Let us prove now Theorem 2 assuming the lemma. Given a, b, n, k satisfying the conditions of the theorem (for ε to be chosen later) let A, B be the sets of strings of length $K(a), K(b|a)$ respectively. Let δ be a function of $K(a)$, k of order $O(\log(K(a)+k))$ to be chosen later. Let P be the set of strings of length k and Q the set of strings of length less than $k - n - 3\delta$. Fix the functions Φ, Θ, Ψ as follows:

$$\Phi(p) = \{q \mid K(q|p) < n\}, \quad \Theta(a') = \{p \mid K(p|a') < k - 3\delta\}, \quad \Psi(q, a') = \{b \mid K(b|q, a') < n\}.$$

They satisfy the requirements for the number of values provided $\varphi = \psi = 2^n$ and $\theta = 2^{k-3\delta}$.

Let $\alpha = 2^{K(a)-\delta}$, $\beta = 2^{K(b|a)-\delta}$ and verify that if ε is much greater than δ then the chosen parameters satisfy the conditions of Lemma 2.

As $K(b|a) > 2n + \varepsilon \gg 2n + \delta$, we have $s = (2^{K(b|a)-\delta} - 2^{2n})2^{-K(b|a)} > 2^{-\delta-1}$. Therefore

$$1 - s \leqslant 1 - 2^{-\delta-1} \leqslant e^{-2^{-\delta-1}} < 2^{-2^{-\delta-1}}.$$

As $\#P = 2^k \gg 2^{k-3\delta} = \theta$, we have $\#P - \theta > \#P/2$, thus, it is enough to show that

$$2^{\#A}(2^{\#B}2^{-2^{-\delta-1}\cdot\#P/2})^{\alpha} \cdot (\#Q)^{\varphi\cdot\#P} \cdot (\#P)^{\theta\cdot\#A} \cdot (\#B)^{\psi\cdot\#Q\cdot\#A} < 1$$

Let us focus on the exponents in this inequality. The inequality is true if all the positive exponents are much less than the negative exponent:

$$\begin{aligned}
\#A = 2^{K(a)} &\ll 2^{-\delta-1} \cdot \#P \cdot \alpha/2 = 2^{-\delta-2+k+(K(a)-\delta)},\\
\#B \cdot \alpha = 2^{K(b|a)+K(a)-\delta} &\ll 2^{-2\delta-2+k+K(a)},\\
\varphi \cdot \#P = 2^{n+k} &\ll 2^{-2\delta-2+k+K(a)},\\
\theta \cdot \#A = 2^{k-3\delta+K(a)} &\ll 2^{-2\delta-2+k+K(a)},\\
\psi \cdot \#Q \cdot \#A = 2^{n+(k-n-3\delta)+K(a)} &\ll 2^{-2\delta-2+k+K(a)}.
\end{aligned}$$

The first condition is true, as $k > \varepsilon \gg \delta$. The second one is true, as $k > K(b|a) + \varepsilon$. The third one is true, as $K(a) \geqslant n + \varepsilon$. The remaining two inequalities are obviously true provided δ is large enough. Note that the difference between the negative exponent and all the positive ones is at least $\delta - O(1)$. If $\delta = O(\log(k + K(a))$ is chosen appropriately the difference is large enough to compensate the difference in bases: $2^{\delta} \gg \#Q, \#P, \#B$.

By Lemma 2 there is a winning function. We need a winning function Ξ of Kolmogorov complexity of order $O(\log(K(a)+k)$, that is, the Kolmogorov complexity $K(\Xi)$ of the graph of Ξ should be $O(\log(K(a)+k))$. To prove that there is a winning function Ξ such that $K(\Xi) = O(\log(K(a) + k))$ we can use the following (very general) argument: By a very long (but

finite) exhaustive search we can check whether a given function is winning or not (checking all Θ, Φ and Ψ). Thus we can probe all the functions Ξ in some natural order until we find the first winning one. To run this algorithm we need only to know $n, k, K(a), K(b|a)$. As all these numbers are less than $K(a) + k$, the first winning function has Kolmogorov complexity $O(\log(K(a) + k))$.

As Ξ beats the chosen Φ, Θ, Ψ we have

$$\#\{a' \in A \mid \#B(a') \geqslant 2^{K(b|a)-\delta}\} < 2^{K(a)-\delta}.$$

Let us see what means that a pair $\langle a', b'\rangle$ is not covered for chosen Φ, Θ, Ψ. This means that

> *there is p of length k and complexity at least $k - 3\delta$ such that $\Xi(p, a') = b'$ and there is no q of length less than $k-n-3\delta$ such that $K(q|p) < n$ and $K(b|q, a') < n$.*

Note that $b' = \Xi(p, a')$ implies $K(b'|p, a') = O(\log(K(a) + k))$.

Now we will show that the pair $\langle$the shortest program for a, the shortest program for b given $a\rangle$ is not covered hence satisfies the quoted statement. Indeed, covered pairs can be enumerated given $k, n, K(a), K(b|a)$. This implies that all a' with $\#B(a') > 2^{K(a)-\delta}$ can be enumerated too. As Ξ is winning, the number of such a' is less than $2^{K(a)-\delta}$ hence every such a' has complexity at most $K(a) - \delta + O(\log(K(a) + k)) < K(a) - \delta/2$, provided δ is large enough. For remaining a' we have $B(a') < 2^{K(b|a)-\delta}$, hence for all $b' \in B(a')$ it holds

$$K(b'|a') < K(b|a) - \delta + O(\log(K(a) + k)) < K(b|a) - \delta/2.$$

If a' is the shortest program for a and b' is the shortest program for b given a and δ is large enough then $K(a') > K(a) - \delta/2$ and $K(b'|a') > K(b|a) - \delta/2$ hence the pair $\langle a', b'\rangle$ is not covered. That is, the statement quoted above is true for $\langle a', b'\rangle$. If we replace now a', b' by a, b, respectively, we change all the complexities involved by at most $O(\log(K(a) + k))$. In this way we obtain almost the statement in the conclusion of Theorem 2. The only problem left is that in the quoted statement q ranges over strings of *length* less than $n-k-3\delta$ and not of *complexity* less than $n-k-\varepsilon$, as in Theorem 2. This is fixed as in the proof of Theorem 1: changing q to its shortest program increases $K(b|a, q)$ and $K(q|p)$ by $O(\log(K(a) + k))$. It remains to prove Lemma 2.

Proof of Lemma 2. It is clear that without loss of generality we may assume that the functions Φ, Θ and Ψ always take maximum allowed number of values (if Ξ wins in this case, it wins always).

First fix Φ, Θ and Ψ and prove that the probability that a randomly chosen function Ξ does not beat Φ, Θ and Ψ is less than the first term $2^{\#A}(2^{\#B}(1-s)^{\#P-\theta})^{\alpha}$ in the inequality of Lemma 2 (assuming that all functions Ξ are equiprobable).

To this end upper bound the probability that $\#B(a) \geqslant \alpha$ for a fixed a. If $\#B(a) \geqslant \alpha$ then there is a set $B' \subset B$ of cardinality β such that all pairs in $\{a\} \times B'$ are covered. Fix any such B' and upper bound the probability that all pairs in $\{a\} \times B'$ are covered. If this happens then for all $p \in P \setminus \Theta(a)$, the value $\Xi(p, a)$ gets outside B' or gets into the set $\cup_{q\in\Phi(a)}\Psi(q, a)$. For fixed $p \in P$ the probability of this event is at most $(1 - \#B'/\#B) + \varphi\psi/\#B = 1 - s$,

as $\Xi(p,a)$ is chosen at random in B and the number of elements in $\cup_{q\in\Phi(a)}\Psi(q,a)$ is at most $\varphi\psi$. Since for different p the values $\Xi(p,a)$ are independent, all pairs in $\{a\}\times B'$ are covered with probability at most $(1-s)^{\#P-\Theta(a)}\leqslant(1-s)^{\#P-\theta}$. By the union bound the probability that $\#B(a)\geqslant\alpha$ is at most $2^{\#B}(1-s)^{\#P-\theta}$, where $2^{\#B}$ upper bounds the number of different B'.

Again, by union bound the probability that the number of a with $\#B(a)\geqslant\alpha$ is at least α is upperbounded by the number of $A'\subset A$ of cardinality α times the probability that $\#B(a)\geqslant\alpha$ for all $a\in A'$. The number of A' is less that $2^{\#A}$. The probability that $\#B(a)\geqslant\alpha$ for all $a\in A'$ is at most $(2^{\#B}(1-s)^{\#P-\theta})^{\alpha}$, as the values $\Xi(p,a)$ are chosen independently for different a. Multiplying these two numbers we obtain the first factor $2^{\#A}(2^{\#B}(1-s)^{\#P-\theta})^{\alpha}$ in the inequality of Lemma 1.

Is is easy to see that the other three factors are the upper bounds for the number of different functions Φ, Θ and Ψ, respectively. □

As it was mentioned above, Theorem 2 implies Theorem 1, thus we obtain a new proof of Theorem 1. What is the advantage of such, more complicated, proof? It shows that Theorem 1 can be strengthened as follows: for every oracle X there exist p,a,b satisfying conditions (a) of the theorem (unchanged, without the oracle) such that $K^X(p|a)\geqslant k-\varepsilon$ and there is no q for which both $K^X(q|p)$ and $K^X(b|a,q)$ are less than $n-\varepsilon$. Indeed, our winning function beats any adversary's strategy and its construction (and the inequality $K(b|a,p)\approx 0$) does not depend on the enemy's strategy. The same applies to Theorem 2: the items (b) and (c) in its conclusion can be relativized by any oracle X provided its condition is relativized by the same oracle; item (a) remains unrelativized. [Instead of relativizing the Kolmogorov complexity by an oracle one can add any string as the extra condition in $K(p|a)$, $K(q|p)$ and $K(b|a,q)$.]

4 Algebraic construction

Here we present the proof of Theorem 3.

Consider again the game of Section 2. Let $\Xi\colon P\times A\to B$ and let $\Phi\colon P\to Q$ and $\Psi\colon Q\times A\to B$ be multi-valued functions that have at most φ and ψ values, respectively. Call a pair $\langle p,a\rangle$ *covered* if there is $q\in\Phi(p)$ with $\Xi(p,a)=\Psi(q,a)$. Fix $\beta\in(0;1)$ and call Ξ *winning* if for all Φ,Ψ the number of covered cells is at most $\beta\cdot\#P\cdot\#A$.

The probabilistic arguments allow us to show that there exists a winning function (under certain conditions on $A,B,P,Q,\varphi,\psi,\beta$). Although we can find a winning function by an exhaustive search, this search could be very long. We would like to have a more explicit example of a winning function. We will show now that in the case $A=B=F$, $P=F^2$ (where F is a finite field) some explicit function is winning, namely $\Xi((p_1,p_2),a)=p_1+p_2a$. To this end we formulate certain conditions that guarantee that a function $\Xi\colon P\times A\to B$ is a winning one.

Consider a function $\Xi\colon P\times A\to B$. For every $p\in P$ consider the corresponding line in the table Ξ, that is, the function $\Xi_p\colon A\to B$ defined as $\Xi_p(a)=\Xi(p,a)$. We require

that the functions Ξ_p for different p (=different lines of the table Ξ) are far away from each other. This requirement seems natural: if the number of different a's where $\Xi_p(a)$ and $\Xi_r(a)$ coincide is large, then the adversary may use the same q for p and r.

Formally speaking, we give the following

Definition. A function Ξ is α-regular if for all $p \neq r$ the number of $a \in A$ such that $\Xi_p(a) = \Xi_r(a)$ is at most α (=if the Hamming distance between corresponding lines is at least $\#A - \alpha$).

Lemma 3. *Every α-regular function is winning provided*

$$4\varphi\psi^2 \cdot \#Q \leqslant \beta\#P, \qquad 4\varphi\psi\sqrt{\alpha} \leqslant \beta\sqrt{\#A}.$$

Proof. First we reduce the general case to the case $\psi = 1$. To this end we replace every line in the table Ψ by ψ lines (that contain the same elements of B as the old line, one element per cell). The height of the table, $\#Q$, becomes ψ times bigger and the function Φ has now ψ times more values (each arrow is replaced by ψ arrows). So φ is replaced by $\tilde{\varphi} = \varphi\psi$. If a function Ξ is winning in the modified game with $\tilde{Q} = \{1, \ldots, \psi\} \times Q$, $\tilde{\varphi} = \varphi\psi$ and $\tilde{\psi} = 1$ (all other parameters remain unchanged) then Ξ is winning in the original game. Indeed, every Φ, Ψ for the original game can be transformed into $\tilde{\Phi}, \tilde{\Psi}$ for the modified game: let $\tilde{\Phi}(p)$ be the set $\{\langle i, q\rangle \mid q \in \Phi(p)\}$, and let $\tilde{\Psi}(\langle j, q\rangle, a)$ be equal to the jth value of $\Psi(q, a)$, in some order. If Ξ beats $\tilde{\Phi}, \tilde{\Psi}$ then it beats also Φ, Ψ.

The conditions of the lemma translate into the inequalities

$$4\tilde{\varphi} \cdot \#\tilde{Q} \leqslant \beta\#P \quad \text{and} \quad 4\tilde{\varphi}\sqrt{\alpha} \leqslant \beta\sqrt{\#A}.$$

So we can assume that $\psi = 1$ from now on.

Let us split an φ-valued function Φ into φ single-valued functions $\Phi_1, \ldots, \Phi_\varphi$. Each Φ_i covers some cells of the table Ξ. We will estimate the fraction of elements covered by Φ_i and prove that it is less than β/φ. This implies that the fraction of covered cells is less than β.

Why any single-valued function Φ covers few cells? The reason is that $\#Q$ is much less than $\#P$, thus the same line of the table Ψ must correspond to many lines of the table Ξ. By our assumption the lines of Ξ have small intersection and hence cannot be easily covered by the same line. The formal argument use the following simple bound:

Lemma 4. *Assume that a family of k subsets of an s-element set is given such that every two subsets in this family have at most α common elements. Then the sum of cardinalities of all the subsets in the family is at most*

$$2s + 2k\sqrt{s\alpha}.$$

Remark: For small k the first term of the sum $2s + 2k\sqrt{s\alpha}$, not depending on k, is the main term; for large k the second term, linear in k, is the main term; two terms are equal for $k = \sqrt{s/\alpha}$.

Proof. Let $s_1, \ldots, s_k$ be the cardinalities of the given subsets. The inclusions-exclusions formula implies that

$$s \geqslant s_1 + s_2 + \ldots + s_k - k^2\alpha$$

(there are at most k^2 pairwise intersections, each of cardinality at most α). Therefore

$$s_1 + \ldots + s_k \leqslant s + k^2\alpha.$$

If $k \leqslant \sqrt{s/\alpha}$ then the second term ($k^2\alpha$) is bounded by s and the sum $s + k^2\alpha$ is at most $2s$. Hence the inequality of the lemma is true for all $k \leqslant \sqrt{s/\alpha}$. For $k = \sqrt{s/\alpha}$ we have also $s_1 + \ldots + s_k \leqslant 2k\sqrt{s\alpha}$, as in this case $2k\sqrt{s\alpha} = 2s$. Since the right hand side of the last inequality is linear in k, the inequality is true for all $k \geqslant \sqrt{s/\alpha}$. To demonstrate this let us delete from the sum $s_1 + \ldots + s_k$ all terms except for the $\sqrt{s/\alpha}$ largest ones. As the average of remaining terms is not smaller than the average of all terms, we are done. □

In fact this proof works only if $\sqrt{s/\alpha}$ is an integer. This is not really important since one can easily adapt the arguments below and use Lemma 2 only for integer case, but we can still prove Lemma 2 in general case using more careful bounds. Namely, $s_1 + \ldots + s_k \leqslant s + (k(k-1)/2)\alpha$, since there are at most $k(k-1)/2$ pairwise intersections. Then for $k \leqslant \lceil\sqrt{s/\alpha}\rceil$ one has

$$s + (k(k-1)/2)\alpha \leqslant s + \sqrt{s/\alpha}(\sqrt{s/\alpha} + 1)\alpha \leqslant s + \sqrt{s}(\sqrt{s} + \sqrt{\alpha}) \leqslant 2s \leqslant 2k\sqrt{s\alpha},$$

(since we may assume without loss of generality that $\alpha \leqslant s$), and the proof can be finished as before.

Let us continue the proof of Lemma 3. If k different lines of Ξ are mapped by Φ onto one line of Ψ, then the sets of covered columns in any two of these lines have at most α common elements. Hence the total number of covered cells in these k lines is at most

$$2\,\#A + 2k\sqrt{\#A\alpha}.$$

We have to sum this numbers for all $\#Q$ elements that can be values of the function Φ, that is, over all lines of table Ψ.

The first terms sum up to $2\,\#A \cdot \#Q$, the second ones sum up to $2 \cdot \#P\sqrt{\#A \cdot \alpha}$. So the total number of cells covered by each Φ_i is at most

$$2\#A \cdot \#Q + 2 \cdot \#P\sqrt{\#A\alpha}.$$

Recalling that there are φ functions Φ_i we conclude that the number of covered cells is at most

$$2\varphi \cdot \#A \cdot \#Q + 2\varphi \cdot \#P\sqrt{\alpha \cdot \#A}.$$

The condition of the lemma imply that this is less than $\beta \cdot \#P \cdot \#A$. □

Assume now that n, i satisfy conditions of Theorem 3. Let $A = B$ be the field of cardinality 2^n, and let P be the set of all linear functions $(x \mapsto p_1 x + p_2)$ from A to A. A linear function is determined by 2 coefficients, thus $\#P = 2^{2n}$. We can let $\alpha = 1$, as if two linear functions coincide in 2 points then they coincide everywhere. Let $Q = \{0,1\}^{2n-3i}$ and $\varphi = \psi = 2^{i-\gamma}$, $\beta = 2^{-\gamma}$ where $\gamma = O(\log n)$ is to be specified later. Let us verify that the conditions of Lemma 3 are satisfied. We have

$$4\varphi\psi^2 \cdot \#Q = 2^{2+3(i-\gamma)+(2n-3i)} \ll 2^{2n-\gamma} = \beta \cdot \#P,$$
$$4\varphi\psi \cdot \sqrt{\alpha} = 2^{2+2(i-\gamma)} \ll 2^{n/2-\gamma} = \beta \cdot \sqrt{\#A}.$$

The last inequality is guaranteed by the condition $i \leqslant n/4$ in Theorem 3. Let

$$\Phi(p) = \{q \mid K(q|p) < i - \gamma\}, \qquad \Psi(q,a) = \{b \mid K(b|q,a) < i - \gamma\}.$$

These Φ, Ψ satisfy the requirements on the number of values. Therefore, by Lemma 3 the number of covered cells is at most $2^{3n-\gamma}$. As covered cells can be enumerated given n, the complexity of every covered cell is at most $3n - \gamma + O(\log n) < 3n$ provided γ is large enough. Thus every random cell $\langle p, a\rangle$ is not covered. This means that there is no q of length less than $2n - i$ with $K(q|p) < i - \gamma$ and $K(b|q,a) < i - \gamma$. As before, this implies that there is no q of complexity less than $2n - i$ such that $K(q|p) < i - \gamma + O(\log n)$ and $K(b|q,a) < i - \gamma + O(\log n)$. Theorem 3 is proved.

Here is another example of a non-simplifiable description, more "geometric" than that of Theorem 3. Consider the two-dimensional vector space (the plane) over the finite field of cardinality 2^n. The set A consists of all points of this plane and the set B consists of all lines on it. The set P consists also of all points of this plane. The function Ξ is defined as follows: $\Xi(p,a)$ is the line passing through a and p. This time $\alpha = 2^n$, as the line ap_1 coincides with the line ap_2 only if a lies on the line p_1p_2. Let $Q = \{0,1\}^{1.5n}$. For appropriate choice of β, φ, ψ the conditions of Lemma 3 are satisfied. And the conditional complexity of $b = \Xi(a,p)$ given a is at most $n + O(\log n)$, as there are about 2^n lines passing through any given point. Apply the winning strategy based on the function Ξ against adversary's strategy from Section 2. The covered subset of $A \times P$ is small and can be enumerated given n. This implies that all the random pairs in $A \times P$ (those whose complexity is close to $4n$) are not covered. Therefore we obtain the following result (taking into account that the line passing through a pair of random independent points is random):

> any random line b on the plane over the field of cardinality 2^n has conditional complexity $\approx n$ given every its random point a; every other random point p on that line is a description of complexity $2n$ for b (given the point a) that cannot be reduced to a description of complexity $1.5n$.

(More precisely, we should require a and p be independent random points on b, i.e., $K(a,p|b) \approx 2n$.)

The constructions of this section have the following advantage compared with proofs from Sections 2 and 3: The complexity of $K(b|a)$ remains small even if we consider time-bounded

version of Kolmogorov complexity, i.e., require that the running time of the machine finding the object from its description is bounded by a polynomial in n. And the non-reducible program exists even for complexity relativized by any oracle, as in Section 3.

References

[1] Andrej A. Muchnik, Conditional complexity and codes, *Theoretical Computer Science*, **271** (2002), p. 97–109.

[2] M. Li and P.M.B. Vitányi, *An Introduction to Kolmogorov Complexity and its Applications*, Springer-Verlag, New York, 2nd Edition, 1997.

[3] A. Muchnik, A. Shen, N. Vereshchagin, M. Vyugin. Non-reducible descriptions for conditional Kolmogorov complexity. *ECCC Report*, TR04-054, Jun 29, 2004. See also: *Theory and Applications of Models of Computation*, Lecture Notes in Computer Science, Springer Berlin/Heidelberg, 3959 (2006), p. 308–317.