Upper semilattice of binary strings with the relation "x is simple conditional to y"

Andrei Muchnik
Institute of New Technologies
10 Nizhnyaya Radischewskaya,
Moscow, Russia 109004

Andrei Romashchenko
Dept. of Mathematical Logic and Theory of Algorithms
Moscow State University
Vorobjewy Gory, Moscow, Russia 119899
an@romash.mccme.ru

Alexander Shen*
Institute of Problems
of Information Transmission
shen@mccme.ru

Nikolai Vereshchagin†
Dept. of Mathematical Logic and Theory of Algorithms
Moscow State University
Vorobjewy Gory, Moscow, Russia 119899
ver@mech.math.msu.su

Abstract

In this paper we construct a structure R that is a "finite version" of the semilattice of Turing degrees. Its elements are strings (technically, sequences of strings) and $x \leq y$ means that $K(x|y) =$ (conditional Kolmogorov complexity of x relative to y) is small.

We construct two elements in R that do not have greatest lower bound. We give a series of examples that show how natural algebraic constructions give two elements that have lower bound 0 (minimal element) but significant mutual information. (A first example of that kind was constructed by Gács–Körner [4] using completely different technique.)

We define a notion of "complexity profile" of the pair of elements of R and give (exact) upper and lower bounds for it in a particular case.

1. Introduction

Let α and β be two infinite binary sequences. We say that α is Turing reducible to β if there exists a Turing machine M that produces α on its output tape when β is provided on input tape. Turing reducibility is reflexive and transitive, so we get a preorder on the set of all infinite binary sequences (this preorder is usually denoted by $\leq_T$). The equivalence classes $((x \sim y) \Leftrightarrow (x \leq_T y) \wedge (y \leq_T x))$ form an upper semilattice whose elements are called Turing degrees. This semilattice is well studied in recursion theory (see, e.g., [6])

*The work was supported by Volkswagen Foundation while visiting Bonn University

†The work was partially done while visiting the University of Amsterdam and DIMACS center

Now let us replace infinite sequences α and β by finite binary strings a and b. Of course, for any a and b there exists a Turing machine M that produces a from b. So to get a non-trivial relation we have to put some restrictions on M. It is natural to require that M is simple (its program is short compared to x and y). Here the notion of Kolmogorov complexity comes into play. By definition, the conditional Kolmogorov complexity $K(a|b)$ is the length of the shortest program that produces a having b as an input. Now we can define the relation $a \leq_c b$ as $K(a|b) \leq c$ (here a and b are binary strings, c is a number).

If c is a constant, this relation does not have good properties (for example, it is not transitive). This relation also depends on a specific programming language used in the definition of Kolmogorov complexity. To overcome this difficulties, we use the standard trick and consider the asymptotic behavior of the complexity for sequences of strings.

Let $\boldsymbol{x} = x_1, x_2, \ldots$ be a sequence of binary strings. We call it *regular* if length of x_i is polynomially bounded, i.e., if $|x_i| \leq ci^k$ for some c, k and for all i. Let R denote the set of all regular sequences. We say that regular sequence $\boldsymbol{x}$ is *simple* conditional to a regular sequence $\boldsymbol{y}$ if

$$K(x_i|y_i) = O(\log i)$$

and write $\boldsymbol{x} \leq \boldsymbol{y}$. The $\leq$-relation is a preorder defined on R. The relation $(x \leq y) \wedge (y \leq x)$ is an equivalence relation. Equivalence classes form a partially ordered set which (for the same reasons as in the case of Turing degrees) is an upper semilattice (any two elements have a least upper bound).

We prove (section 2) that this set is not a lower semilattice: there are two elements that do not have greatest lower bound. Note that the set of Turing degrees is also not a lower semilattice (see, e.g., [6]), but our proof goes in a completely different way.

The semilattice R is useful for analyzing the notion of common information. This notion was introduced by Gács and Körner [4] in the context of Shannon information theory. They also described a similar notion in the algorithmic theory but do not give a precise definition. We give such a definition in terms of the semilattice R (section 3).

The main result of [4] is an example of two objects whose "common information" is far less than their "mutual information"; Gács and Körner provide such an example in context of Shannon information theory and mention that it could be reformulated for algorithmic information theory. This example was analyzed in [1] where an alternative proof for some special case of Gács–Körner example was provided.

A completely different example of two strings whose common information is much less than their mutual information was given in [2]; for details see [3].

In this paper we develop a third approach to the construction of such pairs of strings. It is based on the geometry of finite fields. Several examples of this type are given in Section 4.

The amount of common information does not determine completely how much the strings a and b have in common. What reflects this better is the "complexity profile of a and b", defined as the set of triples (u, v, w) such that $K(c) \leq u$, $K(a|c) \leq v$, and $K(b|c) \leq w$ for some string c. We use the method of [3] to find exact upper and lower bounds for complexity profile (Section 5). (Technically we have to speak not about strings a and b but about sequences of strings $a_0, a_1, \ldots$ and $b_0, b_1, \ldots$ such that complexity of a_i and b_i is proportional to i; see Section 5 for details.)

2. The upper semi-lattice $\boldsymbol{R}$

Let us recall the definition of conditional Kolmogorov complexity. Let U be a computable function of two arguments; arguments and values are binary strings. (Informally, U is an interpreter of some programming language, the first argument is a program and the second one is program's input.) Let us define $K_U(x|y)$ as $\min\{|p| : U(p, y) = x\}$; here $|p|$ stands for the length of p. There exists an optimal U such that $K_U \leq K_V + O(1)$ for any other computable function V. We fix some optimal U and call $K_U(x|y)$ the *conditional complexity* of x when y is known.

The *unconditional* Kolmogorov complexity can be defined as $K(x|\Lambda)$ where Λ is an empty string. It turns out (see, e.g., [5]) that conditional complexity can be expressed in terms of unconditional complexity. Indeed, let us fix some computable bijection $p, q \mapsto \langle p, q\rangle$ between pairs of strings and strings. Then

$$K(\langle p, q\rangle) = K(p) + K(q|p) + O(\log(|p| + |q|))$$

A sequence $\boldsymbol{x} = x_1, x_2, \ldots$ of binary strings is called *regular* if there exist constants c and k such that $|x_i| \leq ci^k$ for all i. The set of all regular sequences is denoted by R. We define a preorder on R saying that $\boldsymbol{x} = x_1, x_2 \ldots$ precedes $\boldsymbol{y} = y_1, y_2, \ldots$ if there exists a constant c such that $K(x_i|y_i) \leq c \log i$ for all i. (Let us agree that $\log x$ means $\log_2(x + 2)$ so $\log x$ is positive for all $x \geq 0$ and we do not need to consider the case $i = 1$ separately.)

The O-term guarantees that the definition does not change if we replace the optimal function U used in the definition of Kolmogorov complexity by another optimal function. Moreover, since we use $O(\log i)$ (and not $O(1)$), the definition remains the same if we replace conditional Kolmogorov complexity defined as above by prefix complexity (see [5] for the definition). Indeed, these complexities differ only by $O(\log n)$ for strings of length n. Since elements of R are regular, this difference is absorbed by $O(\log i)$-term.

Two elements $\boldsymbol{x}$ and $\boldsymbol{y}$ are *equivalent* if $\boldsymbol{x} \leq \boldsymbol{y}$ and $\boldsymbol{y} \leq \boldsymbol{x}$. The equivalence classes form a partially ordered set. We denote this set by $\boldsymbol{R}$.

Proposition 1 *The set $\boldsymbol{R}$ is an upper semilattice: any two elements have a least upper bound.*

Proof. By definition, $\boldsymbol{z} \in \boldsymbol{R}$ is a least upper bound of $\boldsymbol{x}, \boldsymbol{y} \in \boldsymbol{R}$ if

- $\boldsymbol{z}$ is an upper bound for $\boldsymbol{x}$ and $\boldsymbol{y}$, i.e., $\boldsymbol{x} \leq \boldsymbol{z}$ and $\boldsymbol{y} \leq \boldsymbol{z}$;
- $\boldsymbol{z} \leq \boldsymbol{u}$ for any other upper bound $\boldsymbol{u}$ of $\boldsymbol{x}$ and $\boldsymbol{y}$.

Let $\boldsymbol{x} = x_1, x_2, \ldots$ and $\boldsymbol{y} = y_1, y_2, \ldots$ be any two elements of $\boldsymbol{R}$. Consider the sequence $\boldsymbol{z} = z_1, z_2, \ldots$ where $z_i = \langle x_i, y_i\rangle$. (Here $p, q \mapsto \langle p, q\rangle$ denotes a computable bijection between pairs of strings and strings.) It is easy to see that $\boldsymbol{z}$ is a least upper bound for $\boldsymbol{x}$ and $\boldsymbol{y}$. $\square$

Theorem 2 *The set $\boldsymbol{R}$ is not a lower semilattice: there exist two elements $\boldsymbol{x}$ and $\boldsymbol{y}$ that do not have a greatest lower bound.*

Proof. To prove the theorem we have to construct two sequences $\boldsymbol{x}$ and $\boldsymbol{y}$ that have no greatest lower bound. Assume some n is fixed; let us explain how n-th terms of $\boldsymbol{x}$ and $\boldsymbol{y}$ are constructed. Consider $2n$ binary strings of length n denoted by

$$b_1^0, b_2^0, \ldots, b_n^0, b_1^1, b_2^1, \ldots, b_n^1,$$

and one more string of length n denoted by

$$\varepsilon = \varepsilon_1 \ldots \varepsilon_n$$

(ε_i are individual bits). We want all these strings to be random and independent in the following sense: its concatenation is a string of length $2n^2 + n$ which is incompressible (its Kolmogorov complexity is equal to its length up to $O(1)$ additive term). Such strings do exist, see [5]. Now consider two strings

$$x = b_1^0 b_2^0 \dots b_n^0 b_1^1 b_2^1 \dots b_n^1$$

and

$$y = b_1^{\varepsilon_1} b_2^{\varepsilon_2} \dots b_n^{\varepsilon_n}$$

Strings x and y are n-th terms of the sequences $\boldsymbol{x}$ and $\boldsymbol{y}$.

Let us mention that the pair $\langle x, y\rangle$ contains the same information as the concatenation string of length $2n^2 + n$ mentioned above, so the complexity of the pair $\langle x, y\rangle$ is $2n^2 + n + O(1)$.

In the sequel we use the following terminology. Strings b_i^e (for $e = 0, 1$ and $i = 1, \dots, n$) are called *blocks*. We have $2n$ blocks; each block has length n. All the blocks $b_i^{\varepsilon_i}$ that are included in y are called *selected* blocks; all other blocks $b_i^{1-\varepsilon_i}$ are called *omitted* blocks. Our constructions starts with n pairs of blocks and a string ε that says which block is selected in each pair. The string x is a concatenation of all $2n$ blocks; the string y is a concatenation of n selected blocks.

Now the proof goes as follows. Each selected block is simple relative to both x and y since it is a substring of both x and y and position and length information could be encoded by $O(\log n)$ bits. (When we say that a string u is *simple* relative to a string v we mean that $K(u|v) = O(\log n)$.)

Therefore, if z is the greatest lower bound of x and y, any selected block is simple relative to z. On the other hand, any omitted block could not be simple relative to z. Indeed, assume that some omitted block b is simple relative to z. Then b is simple relative to y since z is simple relative to y by assumption. Then to restore x from y it is enough to specify the string ε and $n \Leftrightarrow 1$ omitted blocks different from b, i.e., n^2 bits, and the complexity of pair $\langle x, y\rangle$ is at most $2n^2 + O(\log n)$ (n^2 bits in y and n^2 bits to specify x when y in known). This contradiction shows that no omitted block is simple relative to z.

Now let us show that y is simple relative to x. Indeed, to find y when x is known we need only to distinguish between omitted and selected blocks in each pair of blocks. We may assume that z is known since it is simple relative to x. Then we may enumerate all the objects that have small complexity relative to z until we find n blocks (we have the list of all blocks since we know x). These n blocks will be (as shown above) exactly the selected blocks, and we are done. So y is simple relative to x. But this is impossible, because in this case the pair $\langle x, y\rangle$ will have complexity at most $2n^2 + O(\log n)$ (instead of $2n^2 + n$).

In the argument above we were quite vague about O-notation, so let us repeat the same argument more formally. The construction described above is performed for each n; to indicate the dependence on n let us write $x(n)$ instead of x, $b_i^0(n)$ instead of b_i^0, etc. Assume that $\boldsymbol{z} = z(0), z(1), \dots$ is a common lower bound of $\boldsymbol{x}$ and $\boldsymbol{y}$. The first step in the proof is the following

Lemma 1 *There exists some constant c such that*

$$K(b|z(n)) \le c \log n$$

for any n and for any block b that was selected at n-th step of the construction. (*There were n selected blocks at n-th step; each of them has length n.*)

Indeed, consider all the blocks b that were selected at n-th step; let $b(n)$ be one of them for which the complexity $K(b|z(n))$ is maximal. The sequence $\boldsymbol{b} = b(1), b(2), \dots$ belongs to R. It is easy to see that $\boldsymbol{b} \le \boldsymbol{x}$ and that $\boldsymbol{b} \le \boldsymbol{y}$, because $b(n)$ is a substring of both $x(n)$ and $y(n)$. Therefore, $\boldsymbol{b} \le \boldsymbol{z}$, since z is the greatest lower bound of $\boldsymbol{x}$ and $\boldsymbol{y}$. By definition,

$$K(b(n)|z(n)) \le c \log n$$

for some constant c; the same inequality is valid for all other selected blocks b since $b(n)$ has maximal complexity (relative to $z(n)$) among them. Lemma 1 is proved.

Lemma 2 *There exists some constant c such that*

$$K(b|y(n)) \ge n \Leftrightarrow c \log n$$

for any n and for any block b that was omitted at n-th step of the construction.

Proof. As we have said, the string $x(n)$ can be reconstructed from the string $y(n)$, the string $\varepsilon(n)$, some omitted block b, its number and the concatenation of all other omitted blocks. Here all the information except b has bit size $n^2 + n + (n^2 \Leftrightarrow n) + O(\log n) = 2n^2 + O(\log n)$, and this information includes $y(n)$. Therefore, the complexity of $\langle x(n), y(n)\rangle$ does not exceed $K(b|y(n)) + 2n^2 + O(\log n)$. On the other hand, the complexity of $\langle x(n), y(n)\rangle$ is $2n^2 + n + O(1)$. Comparing the two inequalities, we see that $K(b|y(n)) \ge n \Leftrightarrow O(\log n)$. Lemma 2 is proved.

Lemma 3 *There exists some constant c such that*

$$K(b|z(n)) \ge n \Leftrightarrow c \log n$$

for any n and for any block b that was omitted at n-th step of the construction.

Indeed, recall that $K(z(n)|y(n)) = O(\log n)$ by our assumption; note also that $K(b|y(n)) \le K(b|z(n)) + K(z(n)|y(n)) + O(\log n)$. Hence, $n \Leftrightarrow O(\log n) \le K(b|y(n)) \le K(b|z(n)) + K(z(n)|y(n)) + O(\log n) = K(b|z(n)) + O(\log n)$. Lemma 3 is proved.

Lemma 4

$$K(\varepsilon(n)|x(n)) = O(\log n).$$

Proof. Lemma 1 implies that for big n the value $K(b|z(n))$ is less than $n/2$ for any selected block b; Lemma 3 implies that for big n the value $K(b|z(n))$ is bigger than $n/2$ for any omitted block b. Therefore, knowing $x(n)$ and $z(n)$ we can reconstruct the list of selected blocks just enumerating the strings s such that $K(s|z(n)) < n/2$ until n blocks from $x(n)$ appear. Since $K(z(n)|x(n)) = O(\log n)$ by assumption, we need only $O(\log n)$ additional bits to reconstruct $\varepsilon(n)$ from $x(n)$. Lemma 4 is proved.

Since $y(n)$ is determined by $x(n)$ and $\varepsilon(n)$, we conclude that $K(\langle x(n), y(n)\rangle)$ is $2n^2 + O(\log n)$ but it should be $2n^2 + n + O(1)$. The contradiction shows that $\boldsymbol{x}$ and $\boldsymbol{y}$ do not have a greater lower bound. $\square$

Let us mention some other properties of the semilattice $\boldsymbol{R}$.

1. The operations "infinum" and "supremum" do not satisfy the distributive law even when they are defined. Indeed, consider sequences $\boldsymbol{a}$ and $\boldsymbol{b}$ where a_n and b_n are random independent strings of length n. Let $c_n = a_n \oplus b_n$ (bitwise addition modulo 2). Then

$$\sup(\inf(\boldsymbol{a}, \boldsymbol{b}), \boldsymbol{c}) \neq \inf(\sup(\boldsymbol{a}, \boldsymbol{c}), \sup(\boldsymbol{b}, \boldsymbol{c}),$$

since $\inf(\boldsymbol{a}, \boldsymbol{b}) = \boldsymbol{\Lambda}$ (where $\boldsymbol{\Lambda}$ is the minimal element of the semilattice), so the left-hand side is equal to $\boldsymbol{c}$ while the right-hand side is equal to $\sup(\boldsymbol{a}, \boldsymbol{b})$.

Moreover,

$$\inf(\sup(\boldsymbol{a}, \boldsymbol{b}), \boldsymbol{c}) \neq \sup(\inf(\boldsymbol{a}, \boldsymbol{c}), \inf(\boldsymbol{b}, \boldsymbol{c}),$$

since left-hand side is equal to $\boldsymbol{c}$ and right-hand side is equal to $\boldsymbol{\Lambda}$.

2. For any two elements $\boldsymbol{x}$ and $\boldsymbol{y}$ in $\boldsymbol{R}$ there exists their difference, i.e., a sequence z such that $\sup(\boldsymbol{y}, \boldsymbol{z}) = \sup(\boldsymbol{y}, \boldsymbol{x})$ and $\inf(\boldsymbol{y}, \boldsymbol{z}) = \boldsymbol{\Lambda}$. (Indeed, let z_n be a shortest program that computes x_n given y_n.)

Difference is not defined uniquely; for instance, if x_n and y_n be random independent strings of length n, both x_n and $x_n \oplus y_n$ are differences of x_n and y_n.

The semilattice $\boldsymbol{R}$ is only one of the possible refinements of the intuitive notion "x is simple relative to y". Here is another possibility. Let us fix a function $f(n) = o(n)$; assume that $\boldsymbol{x}$ and $\boldsymbol{y}$ are sequences of strings such that $|x_n| = O(n)$, $|y_n| = O(n)$. Define $\boldsymbol{x} \leq_f \boldsymbol{y}$ as $K(x_n|y_n) = O(f(n))$. One can show that this definition gives a semilattice with similar property (no greatest lower bound; however, the proof is more difficult and is omitted).

3. Common and mutual information

The semilattice R is a useful tool to analyze the amount of common information shared by two strings.

Let x and y be two strings. By *mutual* information in x and y we mean the value $I(x : y) = K(x) + K(y) \Leftrightarrow K(\langle x, y\rangle)$. (Sometimes $I(x : y)$ is defined as $K(y) \Leftrightarrow K(y|x)$, but these quantities differ only by $O(\log n)$ for strings of length at most n, see [5].)

Theorem 3 *Let $\boldsymbol{x} = x_1, x_2, \ldots$ and $\boldsymbol{y} = y_1, y_2, \ldots$ be elements of R.*

(a) *If $\boldsymbol{z} = z_1, z_2, \ldots$ is a lower bound of $\boldsymbol{x}$ and $\boldsymbol{y}$ then*

$$K(z_n) \leq I(x_n : y_n) + O(\log n). \tag{1}$$

(b) *If $\boldsymbol{z} = z_1, z_2, \ldots$ is a lower bound of $\boldsymbol{x}$ and $\boldsymbol{y}$ and*

$$K(z_n) = I(x_n : y_n) + O(\log n). \tag{2}$$

then $\boldsymbol{z}$ is the greatest lower bound of $\boldsymbol{x}$ and $\boldsymbol{y}$ in R.

Proof. (a) Since $\boldsymbol{z} \leq \boldsymbol{x}$,

$$K(\langle x_n, z_n\rangle) = K(x_n) + K(z_n|x_n) = K(x_n) + O(\log n).$$

So

$$\begin{aligned} K(x_n) = K(\langle x_n, z_n\rangle) + O(\log n) = \\ = K(z_n) + K(x_n|z_n) + O(\log n). \end{aligned} \tag{3}$$

Similarly

$$\begin{aligned} K(y_n) = K(\langle y_n, z_n\rangle) + O(\log n) = \\ K(z_n) + K(y_n|z_n) + O(\log n). \end{aligned} \tag{4}$$

On the other hand,

$$\begin{aligned} K(\langle x_n, y_n\rangle) \leq K(z_n) + K(x_n|z_n) + \\ + K(y_n|z_n) + O(\log n). \end{aligned} \tag{5}$$

since we can reconstruct the pair $\langle x_n, y_n\rangle$ from z_n and programs that transform z_n into x_n and y_n. Combining the last three inequalities $[(3) + (4) \Leftrightarrow (5)]$, we get the statement (a).

Let us prove the part (b) now. Assume that $\boldsymbol{z}$ is a lower bound for $\boldsymbol{x}$ and $\boldsymbol{y}$ and the inequality (1) turns into equality (2). Let $\boldsymbol{z}'$ be any other lower bound for $\boldsymbol{x}$ and $\boldsymbol{y}$. Consider the sequence $\boldsymbol{z}''$ defined as $z''_n = \langle z_n, z'_n\rangle$. It is the least upper bound of $\boldsymbol{z}$ and $\boldsymbol{z}'$ (Proposition 1). Therefore $\boldsymbol{z}'' \leq \boldsymbol{x}$ and $\boldsymbol{z}'' \leq \boldsymbol{y}$. Applying (a) to $\boldsymbol{z}''$ we see that

$$K(z''_n) = K(\langle z_n, z'_n\rangle) \leq I(x_n : y_n) + O(\log n)$$

By assumption, $I(x_n : y_n) = K(z_n) + O(\log n)$, so $K(\langle z_n, z'_n\rangle) \leq K(z_n) + O(\log n)$. On the other hand, $K(\langle z_n, z'_n\rangle) = K(z_n) + K(z'_n|z_n) + O(\log n)$, therefore $K(z'_n|z_n) \leq O(\log n)$ and $\boldsymbol{z}' \leq \boldsymbol{z}$ in R. $\square$

If two sequences $\boldsymbol{x} = x_1, x_2, \ldots$ and $\boldsymbol{y} = y_1, y_2, \ldots$ have the greatest lower bound $\boldsymbol{z} = z_1, z_2, \ldots$, one may call $K(z_n)$ "the amount of common information in strings x_n and y_n". However, this is not a good definition since the good one should use only strings x_n and y_n but not the whole sequences $\boldsymbol{x}$ and $\boldsymbol{y}$.

4. Examples where common information is less than mutual information

Informally speaking, strings a and b have u-bit common information c if $K(c) = u$, $K(c|a) \approx 0$, and $K(c|b) \approx 0$. We know (Theorem 3(a)) that the amount of common information in two strings is not larger than the mutual information of this strings. A natural related question is the following one: can common information be far less than mutual information?

This question was positively answered by Gács and Körner [4]. They found out that there are pairs of strings a and b such that $I(a : b)$ is big but nevertheless any string c that is simple relative to both a and b (both $K(c|a)$ and $K(c|b)$ are small) is simple (has small $K(c)$).

Their construction uses ideas from Shannon information theory. Another construction was suggested in [2] (see [3] for details). Here we present a third way to construct examples of that kind.

Consider a finite field F_n of cardinality d close to 2^n. (Any field of size $2^{n+O(1)}$ will work, so we may use the field of cardinality 2^n or the field $\mathbb{Z}/q\mathbb{Z}$ where q is a prime number between 2^n and 2^{n+1}.) Consider three-dimensional vector space over F_n. Any non-zero vector (f_1, f_2, f_3) generates a line (by "line" we mean a line going through 0, i.e., one-dimensional subspace). Two lines generated by (f_1, f_2, f_3) and (g_1, g_2, g_3) are called orthogonal if $f_1g_1 + f_2g_2 + f_3g_3 = 0$. Now consider two random orthogonal lines a and b (i.e. pair of two orthogonal lines $\langle a, b\rangle$ which has the greatest possible complexity. We claim that $I(a : b)$ is significant but there is no string c which is simple relative to both a and b (unless c is simple).

More precisely, consider the set $O = \{\langle a, b\rangle : a \text{ and } b \text{ are orthogonal lines}\}$. This set contains $d^3 + o(d^3)$ elements (there are $d^2 + o(d^2)$ lines and each line is orthogonal to $d + o(d)$ lines). Therefore, O contains a pair $\langle a, b\rangle$ whose complexity is $\log(d^3) + O(1) = 3n + O(1)$. (We assume that elements of F_n are encoded by binary strings of length $n + O(1)$, so we can speak about complexities.) Note that $K(a) \le 2n + O(\log n)$ since there are about 2^{2n} lines; moreover, $K(b|a) \le n + O(\log n)$ since b is one of 2^n lines orthogonal to A. Recalling the inequality $K(\langle a, b\rangle) \le K(a) + K(b|a) + O(\log n)$, we conclude that $K(a) = 2n + O(\log n)$ and $K(b|a) = n + O(\log n)$. For similar reasons $K(b) = 2n + O(\log n)$ and $K(a|b) = n + O(\log n)$. Therefore, $I(a : b) = n + O(\log n)$.

Theorem 4 *Let $\langle a_n, b_n\rangle$ be a random pair of orthogonal lines in the three-dimensional space over F_n. For any sequence of strings c_n*

$$K(c_n) \le 2K(c_n|a_n) + 2K(c_n|b_n) + O(\log n)$$

assuming that c_n has polynomial (in n) length. [The constant in $O(\log n)$-notation does not depend on n.]

This theorem implies that sequences $\boldsymbol{a} = a_1, a_2, \ldots$ and $\boldsymbol{b} = b_1, b_2, \ldots$ have $\boldsymbol{\Lambda} = \Lambda, \Lambda, \ldots$ as their greatest lower bound. (Here Λ denotes an empty string.) Indeed, if $K(c_n|a_n) = O(\log n)$ and $K(c_n|b_n) = O(\log n)$ for some sequence $\boldsymbol{c} = c_1, c_2, \ldots$, then $K(c_n) = O(\log n)$ according to Theorem 4.

Proof. The proof of Theorem 4 is based on a simple combinatorial observation.

Lemma 5 *Consider a bipartite graph with k vertices $1, \ldots, k$ on the left and l vertices $1, \ldots, l$ on the right. Assume that this graph does not contain cycles of length 4. Then the following bound for the number of edges $|E|$ is valid (we assume that $k \le l$):*

- $k \le \sqrt{l} \Rightarrow |E| \le 2l$;
- $k \ge \sqrt{l} \Rightarrow |E| \le 2k\sqrt{l}$.

Indeed, for each element v on the left consider the set N_v of its neighbors on the right; let n_v be the cardinality of N_v. The intersection $N_v \cap N_w$ (for $v \ne w$) contains at most 1 element, otherwise we get a cycle of length 4. Assume that $k \le \sqrt{l}$. Consider the union of all N_v; it has at least

$$n_1 + n_2 + \ldots + n_k \Leftrightarrow \sum_{i<j} |N_i \cap N_j|$$

elements. The number of pairs $\langle i, j\rangle$ is less that $k^2 \le l$ and the union has at most l elements, therefore

$$|E| = n_1 + n_2 + \ldots + n_k < 2l$$

The first statement is proved. It implies that for $k = \sqrt{l}$ the average number of neighbors for vertices on the left is at most $2\sqrt{l}$. We use this observation to prove the second part of the lemma.

Let $k \ge \sqrt{l}$. Consider $\sqrt{l}$ vertices on the left having maximal neighborhoods and delete all other vertices on the left; this makes the average number of neighbors bigger. But we know that it does not exceed $2\sqrt{l}$. The same is true for the initial graph, therefore $|E| \le k \cdot 2\sqrt{l}$. Lemma 5 is proved.

This lemma will be applied to a bipartite graph whose vertices (both on the left and on the right) are lines; edges connect pairs of orthogonal lines. It is easy to see that this graph does not contain cycles of length 4 (if $a \perp b \perp c \perp d \perp a$ then a, c and b, d generate two orthogonal 2-dimensional subspaces in a 3-dimensional space).

Now we are ready to prove Theorem 4. As we know, $K(a) = K(b) = 2n$ and $K(\langle a, b\rangle) = 3n$ (from now we omit $O(\log n)$-terms for brevity). Let $K(c|a) = p$ and $K(c|b) = q$; we may assume that $p \le q$. We want to get an upper bound for $m = K(c)$. First, let us compute $K(a|c)$ and $K(b|c)$:

$$K(a|c) = K(\langle a, c\rangle) \Leftrightarrow K(c) =$$
$$= K(a) + K(c|a) \Leftrightarrow K(c) = 2n + p \Leftrightarrow m.$$

Similarly, $K(b|c) = 2n + q \Leftrightarrow m$. Consider the set P of all lines whose complexity relative to c does not exceed $2n + p \Leftrightarrow m$; this set contains line a and has cardinality 2^{2n+p-m} (up to a polynomial in n factor). Similarly we get a set Q that contains lines whose complexity relative to c does not exceed $2n + q \Leftrightarrow m$; this set has cardinality 2^{2n+q-m}. Consider a bipartite graph whose edges connect orthogonal lines from P and Q. This graph does not have 4-cycles, so the number of edges $|E|$ does not exceed

$$2^{2n+q-m} \quad \text{if} \quad (2n + p \Leftrightarrow m) \le \frac{2n + q \Leftrightarrow m}{2};$$
$$2^{2n+p-m} \cdot \sqrt{2^{2n+q-m}} \quad \text{if} \quad (2n + p \Leftrightarrow m) \ge \frac{2n + q \Leftrightarrow m}{2}.$$

On the other hand, the pair $\langle a, b\rangle$ represents one of the edges of that graph. If c is known, we can enumerate P, Q and E, so the pair $\langle a, b\rangle$ may be described by its number in E and $3n = K(\langle a, b\rangle) \le K(c) + \log |E|$. Therefore, the two bounds for $|E|$ imply

$$3n \le m + (2n + q \Leftrightarrow m) \Rightarrow n \le q$$

(the first one) and

$$3n \le m + (2n + p \Leftrightarrow m) + \frac{1}{2}(2n + q \Leftrightarrow m) \Rightarrow m \le 2p + q$$

(the second one). We have to prove that $m \le 2p+2q$ (recall that logarithmic terms are omitted). In the second case it is evident; in the first case one should note that $K(c) \le K(c|a) + K(a) \le p + 2n \le p + 2q \le 2p + 2q$. $\square$

Remark. The same example may be reformulated in several ways. Replacing line b by the orthogonal plane $b^\perp$, we may say that $\langle a, b\rangle$ is a random pair $\langle$line a, plane b going through $a\rangle$. We may also switch from projective plane to affine plane and say that $\langle a, b\rangle$ is a random pair $\langle$point a on the affine plane, line b that goes through $a\rangle$, etc.

There are several other examples of pairs having no common information. Here are two of them:

Theorem 5 (a) *Let $\langle a_n, b_n\rangle$ be a random pair of orthogonal lines in four-dimensional space over F_n. For any sequence of strings c_n*

$$K(c_n) \le 3K(c_n|a_n) + 3K(c_n|b_n) + O(\log n)$$

assuming that c_n has polynomial (in n) length.

(b) *The same is true if $\langle a_n, b_n\rangle$ is a random pair of intersecting affine lines (one-dimensional affine subspaces) in three-dimensional affine space over F_n.*

Here the same argument (using Lemma 5) cannot be applied directly, because now graph may have 4-cycles. However, the counting argument can be applied after an appropriate modification, because the intersection $N_v \cap N_w$ is small (only few lines are orthogonal to both lines v and w; only few affine lines intersect two given affine lines). (We omit the details.)

Let us note that in these examples some c_n still have more information about a_n and b_n than one could expect. For example, if in (b) we consider the intersection point p_n of a_n and b_n, then $K(p_n) \approx 3n$, $K(a_n|p) \approx 2n$, $K(b_n|p_n) \approx 2n$. There are some a'_n and b'_n with the same complexities ($K(a'_n) \approx 4n$, $K(b'_n) \approx 4n$, $K(\langle a'_n, b'_n\rangle) \approx 7n$) for which there is no p_n with similar properties.

Remarks. (1) Instead of intersection point we could consider two-dimensional affine subspace that contains both lines.

(2) For (a) one also can find p that contain more information about a_n and b_n than one could expect. (The way to construct such a p_n was pointed by Finkelberg and Bezrukawnikov.)

This effect (some c contains more information about a and b than one could expect) is analyzed in the next section.

5. More about common information

Let us reformulate our informal definition of common information. We say that strings x and y have u-bit common information z if $K(z) \le u$, $K(x|z) \le K(x) \Leftrightarrow u$, and $K(y|z) \le K(y) \Leftrightarrow u$. (It is easy to see that all three inequalities in fact are equalities in that case.)

The question whether such z exists is a special case of a more general question: we may ask for given u, v, w whether there is a string z such that $K(z) \le u$, $K(x|z) \le v$, and $K(y|z) \le w$. The set of all triples $\langle u, v, w\rangle$ for which such a c exists could be considered as "complexity profile" of the pair x, y.

Technically speaking, we should consider sequences of strings instead of individual strings. Let $\boldsymbol{x} = x_1, x_2, \ldots$ and $\boldsymbol{y} = y_1, y_2, \ldots$ be two sequences such that $|x_n| = O(n)$ and $|y_n| = O(n)$. (Only sequences satisfying these conditions will be considered in this section.) A triple of reals (u, v, w) is called *$\boldsymbol{x}, \boldsymbol{y}$-admissible*, if there exists a sequence $\boldsymbol{z} = z_1, z_2, \ldots$ such that

$$\begin{aligned} K(z_n) &\le un + O(\log n), \\ K(x_n|z_n) &\le vn + O(\log n), \\ K(y_n|z_n) &\le wn + O(\log n). \end{aligned} \qquad (6)$$

The set of all $\boldsymbol{x}, \boldsymbol{y}$-admissible triples is denoted by $M_{\boldsymbol{x},\boldsymbol{y}}$. The larger is $M_{\boldsymbol{x},\boldsymbol{y}}$ the more information $\boldsymbol{x}$ and $\boldsymbol{y}$ share.

Here is a trivial example: assume that x_n is a random string of length n and $y_n = x_n$. Then

$$M_{\boldsymbol{x},\boldsymbol{y}} = \{(u,v,w)\colon u+v \geq 1,\ u+w \geq 1\}.$$

If x_n, y_n are random independent strings of length n, then $M_{\boldsymbol{x},\boldsymbol{y}}$ is much smaller:

$$M_{\boldsymbol{x},\boldsymbol{y}} = \{(u,v,w) \mid u+v \geq 1,\ u+w \geq 1,\ u+v+w \geq 2\}.$$

As we shall see, the values of $K(x_n)$, $K(y_n)$ and $I(x_n : y_n)$ do not determine the set $M_{\boldsymbol{x},\boldsymbol{y}}$ completely.

For simplicity we restrict ourselves to one special case: we assume that

$$\begin{aligned} K(x_n) &= 2n + O(\log n), \\ K(y_n) &= 2n + O(\log n), \\ I(x_n : y_n) &= 3n + O(\log n). \end{aligned} \tag{7}$$

Consider the following two sets of triples. The first one, called $M_{\max}$, is defined by the inequalities

$$u+v+w \geq 3,\ u+v \geq 2,\ u+w \geq 2. \tag{8}$$

The second one, called $M_{\min}$, contains all the triples from $M_{\max}$ satisfying *at least one* of the inequalities

$$u+v+w \geq 4,\ u+v \geq 3,\ u+w \geq 3. \tag{9}$$

Theorem 6 (a) *For any sequences* $\boldsymbol{x}, \boldsymbol{y}$ *satisfying* (7)

$$M_{\min} \subseteq M_{\boldsymbol{x},\boldsymbol{y}} \subseteq M_{\max}.$$

(b) *There exist sequences* $\boldsymbol{x}, \boldsymbol{y}$ *satisfying* (7) *such that* $M_{\boldsymbol{x},\boldsymbol{y}} = M_{\min}$.

(c) *There exist sequences* $\boldsymbol{x}, \boldsymbol{y}$ *satisfying* (7) *such that* $M_{\boldsymbol{x},\boldsymbol{y}} = M_{\max}$.

Proof.

(a) Using the inequalities $K(\langle x_n, y_n\rangle) \leq K(z_n) + K(x_n|z_n) + K(y_n|z_n) + O(\log n)$ and $K(x_n) \leq K(z_n) + K(x_n|z_n) + O(\log n)$ it is easy to show that for all $\mathbf{x}, \mathbf{y}$-admissible triples it holds

$$u+v+w \geq 3,\ u+v \geq 2,\ u+w \geq 2. \tag{10}$$

Thus, for every $\mathbf{x}, \mathbf{y}$ the set $M_{\boldsymbol{x},\boldsymbol{y}}$ is included in the set $M_{\max}$, defined by the inequalities (10).

Let us prove that $M_{\min} \subseteq M_{\boldsymbol{x},\boldsymbol{y}}$. Let (u,v,w) be in $M_{\min}$. Then the triple (u,v,w) satisfies the inequalities (8) and at least one of the inequalities (9). So consider three cases.

1) $u+v+w \geq 4$. If $v, w \leq 2$ let z be the concatenation of the first $(2 \Leftrightarrow v)n$ bits of x and the first $(2 \Leftrightarrow w)n$ bits of y. Since $u+v+w \geq 4$, we have $|z| = (2 \Leftrightarrow v)n + (2 \Leftrightarrow w)n \leq un$. To obtain x given z we need the remaining vn bits of x and the numbers n, vn, wn, so $K(x|z) \leq vn + O(\log n)$. Analogously, $K(y|z) \leq wn + O(\log n)$.

Otherwise, if say $v > 2$, let z consist of the first $\min\{2,u\}$ bits of y. Then $K(y|z) \leq (2 \Leftrightarrow \min\{2,u\})n + O(\log n) \leq wn + O(\log n)$, as the triple (u,v,w) satisfies (10). And $K(x|z) \leq K(x) \leq 2n + O(\log n) \leq vn + O(\log n)$.

2) $u+v \geq 3$. If $u \leq 2$ let z consist of the first un bits of y. To find x given z is suffices to know the remaining $(2 \Leftrightarrow u)n$ bits of y and the minimum program to compute x given y (having n bits). So the total number of bits needed to find x given u is $(2 \Leftrightarrow u)n + n + O(\log n) \leq vn + O(\log n)$. And $K(y|z) \leq (2 \Leftrightarrow u)n + O(\log n) \leq wn + O(\log n)$.

Otherwise (if $u > 2$) let z be the concatenation of y and the first $\min\{u \Leftrightarrow 2, 1\}n$ bits of minimum program p to compute x given y. To obtain x given z it suffices to have the remaining $n \Leftrightarrow (u \Leftrightarrow 2)n \leq vn$ bits of p.

3) $u+w \geq 3$. Similar to 2).

(b) Let $x_n = \langle p, q\rangle$, $y_n = \langle p, r\rangle$, where p, q, r are random independent strings of length n. It is easy to show that that the set of $\mathbf{x}, \mathbf{y}$-admissible triples is equal to $M_{\max}$. This fact agrees with our intuition that $\mathbf{x}$ and $\mathbf{y}$ have as much common information as possible (under restriction (7)).

(c) This is the most interesting part of the theorem; the proof uses methods from [3].

Lemma 6 *There are* $\mathbf{x}, \mathbf{y}$ *satisfying (7) such that for any* n *there is no* $\mathbf{z}$ *satisfying the inequalities*

$$\begin{aligned} K(z_n) + K(x_n|z_n) + K(y_n|z_n) &\leq 4n \qquad (11) \\ K(z_n) + K(x_n|z_n) &\leq 3n \qquad (12) \\ K(z_n) + K(y_n|z_n) &\leq 3n. \qquad (13) \end{aligned}$$

Proof. Let us fix natural n. As usually we will omit the subscript n in x_n, y_n, etc.

Let U be the set of all strings of length $2n + C\log n$, where constant C will be chosen later. Let

$$\begin{aligned} U_1 &= \{u \in U \mid K(u) < 2n\} \\ V &= \{(x,y) \mid x,y \in U,\ K(\langle x,y\rangle) < 3n\} \\ V_1 &= \{(x,y) \mid x,y \in U, \text{ there is } c \text{ satisfying} \\ &\qquad \text{the inequalities (11), (12), and (13)}\}. \end{aligned}$$

We will show that the set $(U \times U) \setminus [(U_1 \times U_1) \cup V \cup V_1]$ is non-empty. Any pair (x,y) in this set will satisfy the following:

1) $K(x), K(y) = 2n + O(\log n)$ (as both x and y are in $U \setminus U_1$),

2) $K(\langle x,y\rangle) \geq 3n$ (as $\langle x,y\rangle \notin V$), and

3) there is no z satisfying the inequalities (11), (12), and (13) (as $\langle x,y\rangle \notin V_1$).

Thus, to prove the lemma it suffices to show that there is (x,y) in $(U \times U) \setminus [(U_1 \times U_1) \cup V \cup V_1]$ of complexity at most $3n + O(\log n)$.

The non-emptiness of $(U \times U) \setminus [(U_1 \times U_1) \cup V \cup V_1]$ is proved by counting arguments. We have $|U| = 2^{4n} n^C$,

$|U_1| < 2^{2n}$, $|V| < 2^{3n}$. To obtain an upper bound for $|V_1|$ let us count the number of pairs (x, y) for which there is z satisfying the inequality (11). For any k, l, m there are at most $2^k 2^l 2^m$ pairs x, y such that there is z with $K(z) = k$, $K(x|z) = l$, $K(y|z) = m$. And the number of triples k, l, m satisfying the inequality $k + l + m \leq 4n$ is at most $(4n+1)^3$. Therefore, $|V_1| \leq (4n+1)^3 2^{4n}$. It follows that if C is big enough, then $|U| = 2^{4n} n^C > 2^{2(2n)} + 2^{3n} + (4n+1)^3 2^{4n} \geq |U_1 \times U_1| + |V| + |V_1|$, and therefore the set $(U \times U) \setminus [(U_1 \times U_1) \cup V \cup V_2]$ is non-empty.

Let (x, y) be the lexicographically first pair in $(U \times U) \setminus [(U_1 \times U_1) \cup V \cup V_2]$.

Lemma 7 $K(\langle x, y\rangle) \leq 3n + O(\log n)$.

Proof. To identify x, y it suffices to know n and the sets U_1, V and V_1.

Let ϕ_0 be the universal conditional description method. For any $k + l \leq 3n$ let $W_{k,l}$ be the set of all (p, q) such that $|p| = k$, $|q| = l$ and both $\phi_0(p, \epsilon)$ and $G(\phi_0(p, \epsilon), q)$ are defined. To identify V_1 it suffices to know n and the sets $W_{k,l}$ for all k, l such that $k + l \leq 3n$.

Therefore, x, y can be retrieved from n and the sets U_1, V and $W_{k,l}$, $k + l \leq 3n$.

The elements of all the sets U_1, V and $W_{k,l}$ can be enumerated given n, therefore to get the lists of all these sets it suffices to know n and the number $m = |U_1| + |V| + \sum_{k+l\leq 3n} |W_{k,l}|$ (given n we enumerate elements in all these sets until m elements are enumerated). We have

$$|U_1| \leq 2^{2n},\ |V| \leq 2^{3n},\ |W_{k,l}| \leq 2^k 2^l \leq 2^{3n}.$$

Therefore

$$|U_1| + |V| + \sum_{k+l\leq 3n} |W_{k,l}| \leq (3n+3)2^{3n},$$

and

$$K(\langle x, y\rangle) \leq \log(|U_1| + |V| + \sum_{k+l\leq 3n} |W_{k,l}|) + \\ +2\log n + C \leq 3n + O(\log n).$$

□

This finishes the proof of Lemma 6. □

We claim that $M_{\boldsymbol{x},\boldsymbol{y}} = M_{\min}$ for any sequence satisfying Lemma 6. Assume for the contrary that the set $M_{\boldsymbol{x},\boldsymbol{y}} \setminus M_{\min}$ is not empty, that is there is a triple (u, v, w) satisfying the inequalities

$$u + v + w < 4,\ u + v < 3,\ u + w < 3,$$

for which there exists a sequence $\mathbf{z}$ satisfying (6). Then for n large enough we get

$$\begin{aligned} K(z_n) + K(x_n|z_n) + K(y_n|z_n) &\leq un + vn + wn + \\ &\quad +O(\log n) < 4n, \\ K(z_n) + K(x_n|z_n) &\leq un + vn + \\ &\quad +O(\log n) < 3n, \\ K(z_n) + K(y_n|z_n) &\leq un + wn + \\ &\quad +O(\log n) < 3n. \end{aligned}$$

The contradiction shows that $M_{\boldsymbol{x},\boldsymbol{y}} = M_{\min}$. □

The proof of Theorem 6(c) is non-constructive, it gives no “example” of the pair $(\mathbf{x}, \mathbf{y})$ with $M_{\min} = M_{\boldsymbol{x},\boldsymbol{y}}$. An example would be a set A_n of low complexity ($O(\log n)$) such that any random pair (x_n, y_n) in this set satisfies Theorem 6(c). We do not know whether such a proof exists.

In Section 4 we presented several examples of sequences $\boldsymbol{x}, \boldsymbol{y}$ whose common information is less than mutual information. It would be interesting to find the complexity profile for these examples. Unfortunately, we know only few things. We present here known facts about random orthogonal lines in three-dimensional space. Let $\boldsymbol{x}, \boldsymbol{y}$ be sequences mentioned in Theorem 4. Let $\widetilde{M}$ be the set $M_{\boldsymbol{x},\boldsymbol{y}}$. Let $\widehat{M}$ be the set

$$\{\langle u, v, w\rangle\colon u + v/2 + \max\{w, v/2\} \geq 3, \\ u + w/2 + \max\{v, w/2\} \geq 3\} \quad \cap \quad M_{\max}.$$

Note that both inclusions $M_{\min} \subset \widehat{M} \subset M_{\max}$ are proper (for instance, the triple $(1.5, 1, 1)$ is in $\widehat{M} \setminus M_{\min}$ and the triple $(1, 1, 1)$ is in $M_{\max} \setminus \widehat{M}$)

Theorem 7 $\widetilde{M} \subseteq \widehat{M}$.

Proof. Consider the following bipartite graph $G = (V', V'', E)$. Let V' [V''] be the set of all lines having complexity at most $K(x|z)$ [$K(y|z)$] conditional to z. Put an edge between $\hat{x} \in V'$ and $\hat{y} \in V''$ if $\hat{x}$ is orthogonal to $\hat{y}$. As (x, y) is in E and the elements in E can be enumerated given q and z, we get

$$3n \leq K(\langle x, y\rangle) \leq \log|E| + K(z) + O(\log n).$$

If $\sqrt{|V''|} \leq |V'|$ Lemma 5 get

$$2^{3n - K(z) - O(\log n)} \leq |E| \leq 2|V'|\sqrt{|V''|},$$

and if $\sqrt{|V''|} \geq |V'|$ Lemma 5 get

$$2^{3n - K(z) - O(\log n)} \leq |E| \leq 2|V''|.$$

Thus, anyway we have

$$2^{3n} \leq 2^{K(z) + O(\log n)} \cdot 3\sqrt{|V''|}\max\{\sqrt{|V''|}, |V'|\}.$$

The number of elements in V' and V'' is at most $2^{K(x|z)+1}$ and $2^{K(y|z)+1}$, respectively, and $K(z) \le un + O(\log n)$, $K(x|z) \le vn + O(\log n)$, $K(y|z) \le wn + O(\log n)$. Therefore,

$$3n \le un + 0.5wn + \max\{0.5w, v\}n + O(\log n),$$

thus $3 \le u + 0.5w + \max\{0.5w, v\}$.

In the similar way we can prove that $3 \le u + 0.5v + \max\{0.5v, w\}$. $\square$

Theorem 7 is true for any choice of the field F_n (see Theorem 4). However, the set $\widetilde{M}$ may depend on F_n. The following theorem assumes that the field F_n has size p^2 where p is a prime number; we don't know whether it is true for other fields.

Theorem 8 *Assume that all fields F_n are of size p_n^2 where p_n are primes. Then $\widetilde{M}$ contains the triple $(1.5, 1, 1)$, and, therefore, $\widetilde{M} \ne M_{\min}$.*

Proof. Suppose that q is a square, $q = p^2$ (for all n). Then we claim that the set $M_{\boldsymbol{x},\boldsymbol{y}}$ has the point $(1.5, 1, 1)$, which is on the border of $\hat{M}$.

Let $\alpha \in F_q$ be a primitive element of F_q over F_p. Thus any element in F_q can be represented in the form $t + s\alpha$ for some $t, s \in F_p$. We can choose α in such a way that, moreover, any element in F_q can be represented in the form $t + s\alpha^2$ for some $t, s \in F_p$. Why? The multiplicative group of the field F_q is cyclic (see [7, page 184]), therefore the square of any its generator does not belong to F_p. Let us take as α any such generator. Then $\alpha^2 = e + f\alpha$, where $e, f \in F_p$ and $f \ne 0$. Thus α is a linear combination of $1, \alpha^2$ with coefficients from F_p, and we are done.

Let us find z of complexity $1.5n + O(\log n)$ such that $K(x|z) = n + O(\log n)$, $K(y|z) = n + O(\log n)$. Let (a, b, c) be the leading vector of x (defined up to a multiplicative constant). We may assume that $c \ne 0$, since the number of lines for which $c = 0$ is equal to $q + 1$, therefore the complexity of any such line is at most $\log(q + 1) + O(\log n) \le n + O(\log n)$. So let $c = 1$. By the same reason we may assume that the leading vector of the line y is $(a', 1, c')$. As y is orthogonal to x, we get $c' = \Leftrightarrow(aa' + b)$.

We have $a = z_1 + r\alpha$, $a' = z_2 + t\alpha$, where $z_1, z_2, r, t \in F_p$. Find $z_3, s \in F_p$ such that $b = \Leftrightarrow z_2 r\alpha + z_3 + s\alpha^2$. This is possible by our assumption on α. Let $z = \langle z_1, z_2, z_3 \rangle$. Obviously, $K(z) \le 3\log p + O(\log n) = 1.5n + O(\log n)$. Given z, r and s we can find x, therefore $K(x|z) \le K(r) + K(s) + O(\log n) \le 2\log p + O(\log n) \le n + O(\log n)$.

Let us prove that $K(y|z) \le n + O(\log n)$. It is easy to see that

$$\begin{aligned} c' &= \Leftrightarrow(z_1 z_2 + z_1 t\alpha + rt\alpha^2 + z_3 + s\alpha^2) = \\ &= \Leftrightarrow(z_1 z_2 + z_1 t\alpha + z_3 + (rt + s)\alpha^2). \end{aligned}$$

Therefore, given z, t and $rt + s$ we can find y. Hence $K(y|z) \le K(t) + K(rt + s) + O(\log n) \le 2\log p + O(\log n) \le n + O(\log n)$.

So, if we let for instance, $q_n = 2^{2[n/2]}$ we result with $\boldsymbol{x}, \boldsymbol{y}$ for which the set $\tilde{M}$ has the point $(1.5, 1, 1)$. And we do not know whether this is the case for (say) $q = 2^{2[n/2]+1}$. $\square$

References

[1] Daniel Hammer, Andrei Romashchenko, Alexander Shen, Nikolai Vereshchagin. "Inequalities for Shannon entropies and Kolmogorov complexities." In: *Proc. Twelfth Annual IEEE Conference on Computational Complexity*, Ulm, Germany, 13-23, June 1997.

[2] An.A. Muchnik, On the extraction of common information of two strings. *Abstracts of talks at the First World Congress of Bernoulli Society*, Moscow, Nauka, p. 453, 1986. (In Russian.)

[3] An.A. Muchnik. Common information. *Manuscript*, 1996. To appear in Theoretical Computer Science in 1998.

[4] P.Gács, J.Körner. *Common information is far less than mutual information.* Problems of Control and Information Theory, 2:149-162, 1973

[5] M.Li, P.Vitanyi. *An introduction to Kolmogorov complexity and its applications.* Second edition. Springer, 1997.

[6] Shoenfield, J.R. *Degrees of unsolvability*. North-Holland Publishing Company, 1971.

[7] S. Lang. *Algebra.* Addison-Wesley, 1965.