ТРУДЫ МАТЕМАТИЧЕСКОГО ИНСТИТУТА ИМ. В.А. СТЕКЛОВА, 2011, т. 274, с. 210–221

УДК 510.5

Колмогоровская сложность и криптография[1]

©2011 г. Ан. А. Мучник

Поступило в марте 2011 г.

С точки зрения колмогоровской сложности рассматриваются задачи о построении сообщений, которые содержат разное количество информации о заданном объекте в зависимости от того, какой дополнительной информацией располагает получатель. Предположим, что получатель знает слово a и мы хотим сообщить получателю информацию о некотором слове b, причем таким образом, чтобы наше сообщение само по себе (без a) не позволяло восстановить b. Оказывается, что это возможно (если слова a и b не слишком просты). Далее рассматриваются более сложные родственные вопросы: что будет, если "противник" знает некоторую информацию c? насколько длинным должно быть сообщение? Мы уточняем эти вопросы, указываем условия, при которых сообщение может иметь полиномиальную длину, и показываем, что они существенны.

1. НЕИНФОРМАТИВНОЕ УСЛОВНОЕ ОПИСАНИЕ

В этом разделе мы для данных слов a и b (при некоторых ограничениях) построим слово f, которое позволяет получить b из a, но само по себе (без a) не содержит информации относительно b, а также рассмотрим некоторые обобщения этой задачи.

Равномерная и неравномерная сложность. Начнем с некоторых общих замечаний, мотивирующих постановку задачи с точки зрения колмогоровской сложности условного описания. Пусть X — некоторое множество (двоичных) слов, а y — слово. Тогда можно определить $\mathrm{KS}(X \to y)$ как минимальную длину программы, которая дает y на любом входе x из X. (Как обычно, мы фиксируем некоторый оптимальный способ записи программ; можно также вместо минимальной длины говорить о минимальной сложности.) Очевидно, что

$$\mathrm{KS}(X \to y) \geq \max_{x \in X} \mathrm{KS}(y|x)$$

(если программа p годится для всех $x \in X$, то она годится для любого из них), но обратное верно не всегда и левая часть может быть существенно больше правой. Можно сказать, что "равномерная" сложность задачи $X \to y$ (левая часть) может быть существенно больше "неравномерной".

Чтобы убедиться в этом, возьмем в качестве y несжимаемое слово длины n, а в качестве X возьмем множество всех слов x, для которых $\mathrm{KS}(y|x) < n/2$. Тогда правая часть по построению не превосходит $n/2$. Покажем, что левая не меньше $n - O(\log n)$. В самом деле, пусть p — некоторая программа, которая дает y на любом входе x, для которого $\mathrm{KS}(y|x) < n/2$. Среди таких входов есть слова сложности $n/2 + O(\log n)$, и вместе с p их достаточно для получения y, поэтому $\mathrm{KS}(y|p) \leq n/2 + O(\log n)$. Значит, существует слово e длины $O(\log n)$, для которого $\mathrm{KS}(y|\langle p, e\rangle) < n/2$. По предположению $p(\langle p, e\rangle) = y$ и потому сложность p не меньше $n - O(\log n)$.

Замечание. Множество X можно сделать конечным, ограничившись, скажем, словами длины не более $2n$.

[1] Результаты этой работы были доложены Ан.А. Мучником (1958–2007) на Колмогоровском семинаре кафедры математической логики и теории алгоритмов МГУ (заседания 11 марта и 8 апреля 2003 г.), но не были тогда опубликованы; их формулировки составили содержание доклада Ан.А. Мучника и А.Л. Семёнова на семинаре в Dagstuhl (Seminar 03181, 27.04.2003–03.05.2003). Текст подготовили А. Чернов и А. Шень в 2008–2009 гг.

Сложность задачи $(a \to b) \to b$**.** Построенный пример показывает, что равномерная и неравномерная сложности могут сильно отличаться. В следующем примере это не так, но доказательство их совпадения требует дополнительных усилий.

Пусть a, b — двоичные слова. Определим $(a \to b)$ как множество всех программ, которые на входе a дают b. Известно [2], что

$$\mathrm{KS}((a \to b) \to b) = \min\{\mathrm{KS}(a), \mathrm{KS}(b)\} + O(\log N)$$

для любых слов a, b длины не более N. Оказывается, что это утверждение можно усилить, заменив равномерную сложность на неравномерную.

Теорема 1. *Для любых слов a и b длины не больше N найдется программа f, переводящая a в b, для которой*

$$\mathrm{KS}(b|f) = \min\{\mathrm{KS}(a), \mathrm{KS}(b)\} + O(\log N).$$

Доказательство. В одну сторону ($\leq$) неравенство очевидно для любой программы f, переводящей a в b. В самом деле, имея такую программу и любое из слов a и b, можно восстановить b.

Докажем, что для некоторой функции f верно и обратное неравенство. Пусть m — максимальная из сложностей $\mathrm{KS}(b|f)$ для всех функций, переводящих a в b. (При этом мы ограничиваемся конечными функциями, определенными на множестве всех слов длины не более N и принимающими значения в том же множестве, так что они являются конечными объектами и условная сложность естественно определяется. Заметим также, что с логарифмической точностью нет разницы между функциями и их программами.) Нам надо показать, что сложность хотя бы одного из слов a и b не превосходит $m + O(\log N)$.

Рассмотрим множество S пар $\langle a', b'\rangle$ слов длины не больше N, для которых выполнено такое свойство: $\mathrm{KS}(b'|f) \leq m$ *для всякой функции f, определенной на всех словах длины не более N и принимающей значения в том же множестве, для которой* $f(a') = b'$. По построению пара $\langle a, b\rangle$ входит в S.

Множество S можно перечислять, зная N и m. В ходе этого перечисления будем браковать пары, у которых абсцисса или ордината встречается не в первый раз (среди незабракованных); от S останется некоторое подмножество $\widetilde{S}$, которое является графиком некоторого взаимно однозначного соответствия. Пара $\langle a, b\rangle$ уже не обязана принадлежать $\widetilde{S}$, но в $\widetilde{S}$ есть либо пара с абсциссой a, либо пара с ординатой b (иначе мы бы не выбросили $\langle a, b\rangle$).

Поэтому достаточно показать, что $\widetilde{S}$ содержит не более $O(2^m)$ элементов (тогда порядковый номер указанной пары в перечислении множества $\widetilde{S}$ содержит m битов и позволяет восстановить либо a, либо b).

В самом деле, множество $\widetilde{S}$ можно расширить до графика некоторой функции g. Если $\langle a', b'\rangle \in \widetilde{S}$, то $g(a') = b'$ и потому $\mathrm{KS}(b'|g) \leq m$ по построению ($\widetilde{S}$ является подмножеством S). Значит, в $\widetilde{S}$ имеется не более $O(2^m)$ различных b', а по построению их столько же, сколько пар в $\widetilde{S}$. $\square$

Криптографическая интерпретация. Утверждение предыдущего пункта имеет следующую интерпретацию. Мы хотим передать информацию о слове b некоторому человеку, уже знающему слово a, послав ему некоторое сообщение f. (Вместе с a это сообщение позволит легко восстановить слово b.) При этом мы хотим, чтобы для непосвященных, т.е. людей, не знающих слова a, сообщение f несло минимально возможную информацию о b, т.е. чтобы сложность $\mathrm{KS}(b|f)$ была максимально возможной. Как мы уже видели, эта сложность не может быть больше $\mathrm{KS}(b)$ и не может быть больше $\mathrm{KS}(a)$ (поскольку вместе с a сообщение f позволяет легко восстановить b). Теорема 1 показывает, что эта граница ($\min\{\mathrm{KS}(a), \mathrm{KS}(b)\}$) действительно достигается.

Можно рассмотреть релятивизованный вариант этой задачи, когда непосвященный знает некоторое третье слово c. Наше рассуждение (соответственно релятивизованное) позволяет найти функцию f, переводящую a в b, для которой

$$\mathrm{KS}(b|f,c) \approx \min\{\mathrm{KS}(a|c), \mathrm{KS}(b|c)\};$$

эта функция содержит минимально возможную информацию о b (с точки зрения знающих c). Формально говоря, верно следующее утверждение (и его доказательство повторяет доказательство теоремы 1).

Теорема 2. *Пусть a, b, c — слова длины не более N. Тогда найдется слово f, для которого*

(1) $\mathrm{KS}(b|a,f) = O(\log N)$;

(2) $\mathrm{KS}(b|c,f) = \min\{\mathrm{KS}(a|c), \mathrm{KS}(b|c)\} + O(\log N)$.

Условие (1) говорит, что сообщение f для посвященных (знающих слово a) содержит всю необходимую информацию о b, а условие (2) говорит, что для непосвященных (знающих только c) оно содержит минимально возможную информацию о b.

Замечание. С первого взгляда может показаться, что для доказательства теоремы 1 достаточно в качестве f взять кратчайшее описание b при известном a — дескать тогда в нем не будет "лишней информации". Но это не так: если a и b — независимые случайные слова длины n, то b является таким кратчайшим описанием, но не годится в качестве f (поскольку $\mathrm{KS}(b)$ и $\mathrm{KS}(a)$ близки к n, а $\mathrm{KS}(b|b)$ близко к нулю). В этом примере можно взять в качестве f побитовую сумму $a \oplus b$ слов a и b по модулю 2 — она позволяет знающему a восстановить b, но $\mathrm{KS}(b|f) \approx n$.

Воспользовавшись теоремой о простом условном описании [1], можно аналогичным способом доказать утверждение теоремы 1. Согласно теореме о простом условном описании существует слово b', которое является минимальным описанием b при известном a, простым относительно b. Это означает, что $\mathrm{KS}(b'|b) = O(\log N)$, $\mathrm{KS}(b|a,b') = O(\log N)$ и длина b' равна $\mathrm{KS}(b|a) + O(\log N)$. Рассмотрим также слово a', которое является минимальным описанием a при известном b, простым относительно a, и уравняем его по длине с b' (отрезав лишние биты или добавив нули в зависимости от того, у какого из слов a и b больше сложность), получится a''. Теперь можно взять в качестве f слово $a'' \oplus b'$.

Зная f и a, мы можем получить a' и затем a'' без дополнительной информации (точнее, с логарифмической дополнительной информацией), после чего можно получить b' и затем b. Несложно проверить также, что $\mathrm{KS}(b|f) = \min\{\mathrm{KS}(a), \mathrm{KS}(b)\}$ с логарифмической точностью.

В самом деле, с логарифмической точностью

$$\begin{aligned}\mathrm{KS}(b|f) = \mathrm{KS}(b,f|f) = \mathrm{KS}(b,b',f|f) = \mathrm{KS}(b,a''|f) \geq \\ \geq \mathrm{KS}(b,a'') - \mathrm{KS}(f) \geq \mathrm{KS}(b,a'') - |f| = \mathrm{KS}(b,a'') - \mathrm{KS}(b|a).\end{aligned}$$

Слова a' и b независимы (имеют логарифмическую взаимную информацию), поэтому слово a'' (которое получается из a' с логарифмической сложностью) также независимо с b. Поэтому нижнюю оценку можно продолжить как $\mathrm{KS}(b) - \mathrm{KS}(b|a) + \mathrm{KS}(a'')$, что равно $\min\{\mathrm{KS}(a), \mathrm{KS}(b)\}$ (конец альтернативного доказательства теоремы 1).

Преимущество этого рассуждения в том, что слово f получается полиномиальной (от N) длины и даже минимально возможной длины $\mathrm{KS}(b|a)$. (В другом доказательстве слово f было функцией с экспоненциально большой областью определения.) Другими словами, мы доказали такое утверждение.

Теорема 3. *Для любых двух слов a и b длины не более N найдется слово f длины* $\mathrm{KS}(b|a)$, *для которого*

$$\mathrm{KS}(b|f,a) = O(\log N)$$

и

$$\mathrm{KS}(b|f) = \min\{\mathrm{KS}(a), \mathrm{KS}(b)\} + O(\log N).$$

С другой стороны, недостаток этого рассуждения в том, что оно не обобщается (по крайней мере непосредственно) на случай дополнительной информации c (т.е. не позволяет доказать теорему 2). Пусть опять a и b — случайные независимые слова одинаковой длины $2n$, а a_1, a_2 (b_1, b_2) — первая и вторая половины слова a (соответственно b). Пусть слово c состоит из двух половин $a_1 \oplus a_2 \oplus b_1$ и $a_2 \oplus b_1 \oplus b_2$. Тогда $\mathrm{KS}(a|c) = \mathrm{KS}(a,c|c) = \mathrm{KS}(a,b|c) = 2n$, $\mathrm{KS}(b|c) = 2n$, но $\mathrm{KS}(b|c, a \oplus b) = 0$.

В следующем разделе мы дадим комбинаторное доказательство существования короткого сообщения f, которое содержит всю информацию о b для знающих a, но не для знающих только c.

2. КОМБИНАТОРНОЕ ПОСТРОЕНИЕ ОПИСАНИЯ МИНИМАЛЬНОЙ СЛОЖНОСТИ

Сейчас мы докажем, что если слово a содержит достаточно много информации (точнее говоря, если $\mathrm{KS}(a|c) \geq \mathrm{KS}(b|c) + \mathrm{KS}(b|a) + O(\log N)$), то существует сообщение f, которое обладает указанными в теореме 2 свойствами и имеет сложность $\mathrm{KS}(b|a) + O(\log N)$. Для этого мы используем следующую комбинаторную лемму. (Через $\mathbb{B}^k$ мы обозначаем множество всех k-битовых слов.)

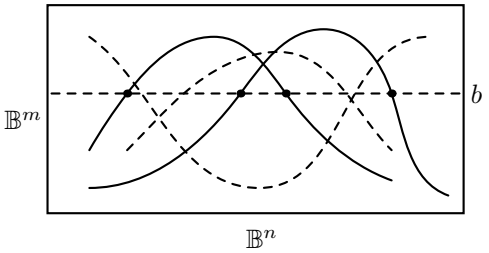
Комбинаторная лемма. *Для любых натуральных m и $n \geq m$ существует семейство $\mathcal{F}$ функций вида $\mathbb{B}^n \to \mathbb{B}^m$, состоящее из $2^m\,\mathrm{poly}(n)$ функций и обладающее таким свойством: для любого слова $b \in \mathbb{B}^m$ и для любого подмножества $\mathcal{F}'$, содержащего не менее половины всех функций из $\mathcal{F}$, множество точек с второй координатой b, не покрытых графиками функций из $\mathcal{F}'$, содержит не более $O(2^m)$ точек.*

Формально свойство семейства $\mathcal{F}$, о котором идет речь в лемме (рисунок), можно записать так:

$$\forall b\, \forall \mathcal{F}' \subset \mathcal{F} \left[|\mathcal{F}'| \geq \frac{1}{2}|\mathcal{F}| \;\Rightarrow\; \left|\left\{a \in \mathbb{B}^n \mid f(a) \neq b \text{ для всех } f \in \mathcal{F}'\right\}\right| = O(2^m) \right].$$

(Заметим также, что условие $n \geq m$ излишне: при $n < m$ утверждение леммы выполнено очевидным образом, поскольку количество всех a есть $O(2^m)$.)

Идея применения леммы: функции, не несущие информации о b, составляют в любом простом семействе большинство и потому среди них найдется функция, переводящая a в b, если



Часть функций (до 50%) из $\mathcal{F}$ выброшены; тем не менее графики оставшихся покрывают любую горизонталь, не считая $O(2^m)$ точек

только a не принадлежит малому множеству исключений (что будет противоречить предположению об a, так как эти исключения имеют малую сложность).

Доказательство леммы. Используя вероятностный метод, возьмем случайное семейство из 2^t случайных функций $\varphi_1, \ldots, \varphi_{2^t}$. (Все эти функции независимы и равномерно распределены в множестве всех функций $\mathbb{B}^n \to \mathbb{B}^m$; точное значение параметра t мы выберем позже.) Оценим вероятность того, что этот набор не обладает требуемым свойством. Это означает, что найдутся

- $b \in \mathbb{B}^m$;
- множество $S \subset \mathbb{B}^n$ из $s \cdot 2^m$ элементов (константу s мы выберем позже);
- множество $I \subset \{1, 2, \ldots, 2^t\}$, содержащее половину всех индексов,

для которых

$$\varphi_i(a) \neq b \qquad \text{для любого } a \in S \text{ и для любого } i \in I. \tag{$*$}$$

Оценим вероятность этого события. Количество различных b есть 2^m, количество различных I не превосходит 2^{2^t}, а количество различных S не превосходит $(2^n)^{s\cdot 2^m}$. При фиксированных b, S и I вероятность выполнения условия $(*)$ есть

$$\left(1 - \frac{1}{2^m}\right)^{2^{t-1}s\cdot 2^m}$$

(каждая из 2^{t-1} функций с номером в I в каждой точке $a \in S$ не попадает в b с вероятностью $1 - 1/2^m$). Всего для вероятности получаем верхнюю оценку

$$2^m \cdot 2^{2^t} \cdot 2^{ns\cdot 2^m}\left(1 - \frac{1}{2^m}\right)^{2^{t-1}s\cdot 2^m},$$

и надо показать, что при правильно выбранных значениях параметров это выражение меньше единицы. Учитывая, что $(1 - 1/2^m)^{2^m} \approx 1/e$ (с гораздо большей точностью, чем нужно нам), можно переписать это как

$$2^{m+2^t} \cdot 2^{ns\cdot 2^m}(1/e)^{s\cdot 2^{t-1}}.$$

Основную роль играют члены, которые содержат 2^t и 2^m в показателе степени (поскольку $2^t, 2^m \gg m, n, s$). Нам нужно, чтобы малый последний сомножитель перевесил два остальных. Разобьем последний сомножитель на две части $(1/e)^{s\cdot 2^{t-2}}$ и сравним эти части с первым и вторым сомножителем. Нам нужно, чтобы

$$2^{m+2^t}(1/e)^{s\cdot 2^{t-2}} < 1 \qquad \text{и} \qquad 2^{ns\cdot 2^m}(1/e)^{s\cdot 2^{t-2}} < 1.$$

Первое неравенство будет выполнено, если взять константу s достаточно большой. Выполнения второго неравенства (в котором степени можно сократить на s) легко добиться, положив $2^t = 2^m \operatorname{poly}(n)$. $\square$

Основной результат. Теперь мы можем дать точную формулировку и доказательство основного результата.

Теорема 4. *Найдется такая константа C, что для любых слов a, b, с длины не более N, для которых*

$$\mathrm{KS}(a|c) \geq \mathrm{KS}(b|c) + \mathrm{KS}(b|a) + C\log N,$$

существует слово f длины не более $\mathrm{KS}(b|a) + C\log N$, для которого $\mathrm{KS}(b|a, f) \leq C\log N$ и $\mathrm{KS}(b|c, f) \geq \mathrm{KS}(b|c) - C\log N$.

Условие теоремы означает, что имеющееся в распоряжении получателя слово a содержит достаточно информации, отсутствующей у "противника" (знающего слово c); заключение говорит, что слово f позволяет восстановить b по a и имеет (среди таких слов) минимально возможную длину, а также не упрощает восстановление b по c. (Во всех выражениях $O(\log N)$ использована одна и та же константа C, но, поскольку с ростом C утверждение становится слабее, это не принципиально.)

Доказательство теоремы 4. Применим теорему об условном кодировании [1] и найдем слово b' длины $\mathrm{KS}(b|a)$, для которого сложности $\mathrm{KS}(b|b',a)$ и $\mathrm{KS}(b'|b)$ равны $O(\log N)$. Применим комбинаторную лемму и построим семейство отображений $\mathbb{B}^n \to \mathbb{B}^m$ с указанными в ней свойствами, взяв m равным длине b', т.е. $\mathrm{KS}(b|a)$, а n равным длине a. Без ограничения общности можно считать, что семейство $\mathcal{F}$ является простым, т.е. имеющим сложность $O(\log N)$, поскольку при данных m и n семейство функций с нужными свойствами можно искать перебором.

Большинство функций в этом семействе (как и в любом другом простом семействе) не сильно упрощают задание b при известном c (имеют малое значение разности $\mathrm{KS}(b|c) - \mathrm{KS}(b|c,f)$). В самом деле, с точностью $O(\log N)$ это можно переписать как $\mathrm{KS}(f|c) - \mathrm{KS}(f|b,c)$ (по теореме о сложности пары и условной сложности), среднее значение обоих членов есть логарифм числа элементов семейства (в данном случае $m + O(\log N)$), поэтому среднее значение разности есть $O(\log N)$ и остается воспользоваться неравенством Чебышева.

Оставив в семействе $\mathcal{F}'$ только функции из этого большинства, мы (по лемме) покроем их графиками пары вида $\langle a', b'\rangle$ при всех a' длины n, кроме $O(2^m)$ "плохих" a', и нам надо убедиться, что a не попало в число плохих. Для этого достаточно показать, что

$$\mathrm{KS}(a'|c) < \mathrm{KS}(b|c) + \mathrm{KS}(b|a) + O(\log N)$$

для всех плохих a'. В самом деле, зная b и c, а также $\mathrm{KS}(b|c)$ (последнее число содержит $O(\log N)$ битов, и с логарифмической точностью им можно пренебречь), можно перечислять все функции f, не попавшие в семейство $\mathcal{F}'$ (упрощающие задание b при известном c), а потому и точки, не покрытые графиками функций из семейства $\mathcal{F}'$. (Напомним, что b' можно также восстановить по b с логарифмической сложностью.) Этих точек по лемме не более $O(2^m)$, поэтому их сложность при известных b, c не более $m + O(\log N)$. Получаем

$$\mathrm{KS}(a'|b,c) \le \mathrm{KS}(b|a) + O(\log N)$$

для всех плохих a', и потому

$$\mathrm{KS}(a'|c) \le \mathrm{KS}(a'|b,c) + \mathrm{KS}(b|c) + O(\log N) \le \mathrm{KS}(b|a) + \mathrm{KS}(b|c) + O(\log N),$$

что и требовалось. □

3. ОТРИЦАТЕЛЬНЫЙ РЕЗУЛЬТАТ И ВОПРОСЫ

Условие на сложности в теореме 4 может показаться искусственным. Скажем, если слова a, b, c попарно независимы, мы требуем, чтобы сложность слова a была вдвое больше сложности слова b, и это выглядит странно (почему агент должен изначально иметь вдвое больше информации, чем мы хотим передать? Может быть, условия $\mathrm{KS}(a) > \mathrm{KS}(b)$ было бы достаточно?).

В этом разделе мы покажем, что неравенство в условии теоремы 4 на самом деле существенно: если этого не требовать, то может оказаться, что все слова f, для которых выполнено утверждение теоремы 2, имеют очень большую длину. Точное утверждение (см. ниже теорему 5) и его доказательство довольно длинные, и мы начнем с более простого рассуждения,

которое, правда, дает пример с очень большой сложностью слова c. Затем мы покажем, как можно уменьшить сложность слова c.

Будем строить три слова a, b, c, обладающие такими свойствами: любая не очень длинная (скажем, полиномиальная от сложностей слов или даже субэкспоненциальная) программа f, получающая b из a, значительно упрощает получение b из c. В этом примере слова a и b будут иметь сложность примерно $1.3n$ и n соответственно, а их взаимная информация будет близка к нулю. (Коэффициент 1.3 выбран достаточно произвольно; важно, что он больше 1 и меньше 2.) Сложность b при известном c будет равна примерно n, так что добавление c в качестве условия не уменьшает сложность b. А вот добавление (к условию c) любой программы f, получающей b из a, существенно уменьшает условную сложность b: вместо $\mathrm{KS}(b|c) \approx n$ получается $\mathrm{KS}(b|f,c) \approx 0.3n$.

Основная идея конструкции такова: слово c само будет функцией, переводящей a в b (но при этом без a слово c не содержит никакой информации о b). Пусть нам дана некоторая программа f, которая также переводит a в b. Как она помогает задать b при известном c? Мы знаем, что и c, и f переводят a в b, поэтому a является одним из решений уравнения $c(x) = f(x)$. Эти решения можно перечислять, зная c и f (программа f может быть определена не всюду, но это не мешает). Если решений мало, то можно задать a (а тем самым и b), указав его порядковый номер в перечислении таких решений. Этого достаточно при известных c и f, и это может требовать меньше битов, чем $\mathrm{KS}(b)$ (которое равно $\mathrm{KS}(b|c)$; как мы говорили, само по себе c не содержит информации о b).

Покажем, что с большой вероятностью такой пример получится, если случайно выбрать пару слов $\langle a, b\rangle$ соответствующих длин ($1.3n$ и n), а в качестве c выбрать случайную функцию (с аргументами и значениями соответствующих длин), график которой проходит через $\langle a, b\rangle$. (То же самое распределение вероятностей получится, если сначала выбрать случайную функцию, а потом на ее графике выбрать случайную точку.)

Слова a и b будут иметь нужные сложности и малую взаимную информацию с большой вероятностью. Чуть сложнее понять, что сложность b при известном c будет близка к n. В самом деле, типичная функция c с аргументами длины $1.3n$ и значениями длины n принимает большинство своих значений примерно одинаковое число раз (около $2^{0.3n}$) и потому распределение вероятностей для второй координаты случайной точки ее графика близко к равномерному и большая часть значений будет случайна даже при известной функции c.

Пусть теперь дана некоторая программа f, переводящая a в b, причем она имеет не очень большую длину (существенно меньшую, чем то, что дает теорема 2). Сколько решений будет иметь уравнение $f(x) = c(x)$? В типичной ситуации (для данной f и случайной c) таких решений будет около $2^{0.3n}$ (в каждой точке совпадение с вероятностью 2^{-n}, а точек $2^{1.3n}$); здесь мы предполагаем, что f всюду определена, но если нет, решений будет только меньше. Существенно большее число совпадений для данной функции f и случайно выбранной c очень маловероятно, другими словами, шар соответствующего радиуса в метрике Хемминга имеет очень малую вероятность. Поскольку таких шаров не очень много, то и их объединение будет иметь малую вероятность и с большой вероятностью случайная функция c не попадет ни в один из этих шаров. Это значит, что для такой функции уравнение $c(x) = f(x)$ для любой не очень длинной программы f будет иметь лишь немного более $2^{0.3n}$ решений и потому сложности $\mathrm{KS}(a|f,c)$ и $\mathrm{KS}(b|f,c)$ будут лишь чуть больше $0.3n$, как мы и обещали.

Мы не проводим аккуратно соответствующие оценки, так как хотим доказать более сильное (и сложное) утверждение. А именно: мы хотим найти слово c сравнительно небольшой сложности (а не экспоненциальной сложности, как в изложенной конструкции); сложность слова c будет примерно на $\mathrm{KS}(b)$ больше, чем сложность программ f, для которых оно будет контрпримером. (Это не удивительно: чем больше программ f мы должны “опровергнуть”, тем большая свобода в выборе c требуется.)

Идея конструкции — выбор точки на графике случайной функции c — сохраняется, только теперь c будет выбираться не среди всех функций (с аргументами и значениями нужной длины), а среди функций некоторого семейства $\mathcal{C}$. Мы сформулируем комбинаторные свойства, которым должно удовлетворять это семейство, докажем (вероятностно), что такое семейство существует, заключим отсюда, что существует простое семейство с этими свойствами (перебор), а затем докажем, что для большинства точек a, b найдется функция c из семейства, которая удовлетворяет нужным требованиям. (Таким образом, мы докажем не просто существование тройки $\langle a, b, c\rangle$, а более сильный факт: для большинства пар $\langle a, b\rangle$ существует c.) Ограничивая размер семейства, мы тем самым ограничиваем сложность слова c.

Нужное нам комбинаторное утверждение мы сформулируем в виде леммы. Пусть даны множества A и B. Будем говорить, что некоторое семейство $\mathcal{F}$ функций вида $A \to B$ *бракует* функцию $c\colon A \to B$, если при каком-нибудь $f \in \mathcal{F}$ размер множества $\{a\colon c(a) = f(a)\}$ больше $4|A|/|B|$ (число корней более чем в 4 раза превосходит "ожидаемое"). Пусть $\mathfrak{H}$ — набор семейств функций из A в B, параметризованный элементами b (т.е. $\mathfrak{H}(b)$ при любом $b \in B$ является семейством функций вида $A \to B$). Скажем, что функция c *покрывает* пару $\langle a, b\rangle \in A \times B$ при данных $\mathcal{F}$ и $\mathfrak{H}$, если $c(a) = b$, при этом c не забраковано семейством $\mathcal{F}$ и $c \notin \mathfrak{H}(b)$.

Лемма. *Пусть A и B — непустые множества двоичных слов, причем B содержит не менее двух элементов и $|A| \geq 16|B|$. Пусть также даны числа $\varepsilon \geq 4|B|/|A|$ и $\Phi \leq 2^{|A|/4|B|}$. Тогда найдется такое семейство $\mathcal{C}$ функций вида $A \to B$ размера (мощности)*

$$\max\left\{\frac{20|B|}{\varepsilon},\ \frac{6\Phi\log_2|B|}{\varepsilon},\ 6\Phi|B|\log_2|B|\right\},$$

что для любого семейства $\mathcal{F}$ размера не более Φ и для любого набора $\mathfrak{H}$ семейств, каждое из которых имеет размер не более четверти $|\mathcal{C}|$ (т.е. $|\mathfrak{H}(b)| \leq |\mathcal{C}|/4$ при всех $b \in B$), не более ε-доли всех пар из $A \times B$ не покрыто ни одним $c \in \mathcal{C}$ при данных $\mathcal{F}$ и $\mathfrak{H}$.

Формально утверждение леммы выглядит так (мы опускаем условия на размеры $\mathcal{C}$, $\mathcal{F}$ и $\mathfrak{H}(b)$):

$$\exists\mathcal{C}\ \forall\mathcal{F},\mathfrak{H}$$
$$\left|\left\{\langle a,b\rangle\colon \forall c\left[(c(a)=b)\Rightarrow\left[(c\in\mathfrak{H}(b))\ \vee\ \left(\exists f\in\mathcal{F}\ |\{x\colon f(x)=c(x)\}|\geq\frac{4|A|}{|B|}\right)\right]\right]\right\}\right| \leq$$
$$\leq \varepsilon|A|\cdot|B|.$$

Смысл этой леммы (как она применяется) такой. Без ограничения общности можно предполагать, что семейство $\mathcal{C}$ простое (как обычно, можно взять первое в некотором естественном порядке семейство с нужными свойствами). Возьмем в качестве $\mathcal{F}$ семейство всех функций, имеющих простые программы (точнее, их продолжений, если функции частичны), а в качестве $\mathfrak{H}(b)$ семейство всех функций, простых относительно b. Для пар $\langle a, b\rangle$, не входящих в ε-долю "плохих", найдется покрывающая их функция c из семейства $\mathcal{C}$. Эта функция (точнее, ее индекс в $\mathcal{C}$) и будет нужным контрпримером (информацией у противника). Если в дополнение к c противник получает простую программу f, переводящую a в b, то задание a (а тем самым и задание b) упрощается: достаточно указать порядковый номер a в перечислении всех решений уравнения $f(x) = c(x)$. Выбранное нами $\mathfrak{H}$, кроме того, гарантирует, что c сама по себе независима с b (имеет близкую к максимальной сложность даже при известном b). Подробнее мы скажем про это дальше, а пока докажем лемму.

Доказательство леммы. В качестве $\mathcal{C}$ возьмем случайное семейство функций нужного размера. (Будем считать, что функции из $\mathcal{C}$ нумеруются числами от 1 до $|\mathcal{C}|$, и для каждого

номера i и каждой точки $a \in A$ мы независимо определяем значение i-й функции на a, выбирая равновероятно один из элементов B.) Докажем, что вероятность того, что $\mathcal{C}$ "неудачное", т.е. не обладает требуемым свойством, меньше 1.

Оценим вероятность при фиксированном семействе $\mathcal{F}$. Нам нужно, чтобы для любого набора семейств $\mathfrak{H}$ (с указанными в лемме ограничениями — все семейства не более четверти $\mathcal{C}$) для почти всех пар $\langle a, b\rangle$ нашлась функция из $\mathcal{C}$, проходящая через точку $\langle a, b\rangle$, не забракованная семейством $\mathcal{F}$ и не входящая в $\mathfrak{H}(b)$. Заметим, что в определении забракованной функции не участвует $\mathcal{C}$: зная $\mathcal{F}$, мы уже знаем, какие функции будут забракованы. Возможны два случая: забракованных функций много (скажем, больше четверти всех функций из $\mathcal{C}$) и забракованных функций мало (меньше четверти). Во втором случае мы можем присоединить забракованные функции ко всем семействам $\mathfrak{H}(b)$ и размер этих семейств останется небольшим (не больше половины $|\mathcal{C}|$).

Другими словами, для данного семейства $\mathcal{F}$ неудачность $\mathcal{C}$ покрывается объединением следующих двух событий:

1) $\mathcal{F}$ бракует не меньше четверти функций из $\mathcal{C}$;
2) для некоторого набора $\mathfrak{H}$, в котором все семейства $\mathfrak{H}(b)$ имеют размер не более *половины* $|\mathcal{C}|$, доля пар из $A \times B$, через которые не проходит ни одна функция $c \in \mathcal{C}$, не входящая в $\mathfrak{H}(b)$, превышает ε.

Нам нужно, чтобы сумма вероятностей этих двух событий, умноженная на количество возможностей для $\mathcal{F}$, была меньше 1. Докажем, что вероятность каждого из них меньше $1/2$, деленной на $(|B|^{|A|})^{\Phi}$ (последнее выражение — верхняя оценка на количество возможных семейств $\mathcal{F}$ размера не более Φ).

Первое событие запишем в таком виде: *существует такое подсемейство* $\mathcal{C}' \subset \mathcal{C}$ *размера* $|\mathcal{C}|/4$, *что для всех* $c \in \mathcal{C}'$ *найдутся такое подмножество* $A' \subset A$ *размера* $4|A|/|B|$ *и такая функция* $f \in \mathcal{F}$, *что* $f(a) = c(a)$ *для всех* $a \in A'$.

Количество возможных $\mathcal{C}'$ оценим сверху общим числом подсемейств в $\mathcal{C}$, т.е. $2^{|\mathcal{C}|}$. При фиксированном подсемействе (точнее, для данного множества индексов) функции с этими индексами выбираются независимо, поэтому можно оценить вероятность нежелательного события для одной из них и возвести в степень. Для оценки количества возможных подмножеств A' заметим, что число подмножеств размера r в множестве размера q, т.е. C_q^r, не превосходит $q^r/r! \le q^r/((r/3)^r) = (3q/r)^r$. Для $q = |A|$ и $r = 4|A|/|B|$ получаем, что количество возможных A' не превосходит $(3|B|/4)^{4|A|/|B|}$.

Таким образом, вероятность первого события не больше

$$2^{|\mathcal{C}|}\left(\Phi\left(\frac{3|B|}{4}\right)^{4|A|/|B|}\left(\frac{1}{|B|}\right)^{4|A|/|B|}\right)^{|\mathcal{C}|/4} = \left(2\Phi^{1/4}\left(\frac{3}{4}\right)^{|A|/|B|}\right)^{|\mathcal{C}|}.$$

После умножения на $|B|^{|A|\Phi}$ (число возможных семейств $\mathcal{F}$) она остается меньше $1/2$, поскольку по условию леммы $|B| \ge 2$, $|A| \ge 16|B|$, $\Phi \le 2^{|A|/4|B|}$ и $|\mathcal{C}| \ge 6\Phi|B|\log_2|B|$. Действительно, из последнего условия следует, что $|\mathcal{C}| \ge 12$ при $\Phi \ge 1$ (случай пустого $\mathcal{F}$ тривиален) и $|B| \ge 2$, поэтому $1+|\mathcal{C}| \le 13|\mathcal{C}|/12$ и из $1 \le |A|/16|B|$ следует, что $1+|\mathcal{C}| \le (13/192)(|A|\cdot|\mathcal{C}|/|B|)$. Из $\log_2\Phi \le |A|/4|B|$ следует, что $(|\mathcal{C}|/4)\log_2\Phi \le (1/16)(|A|\cdot|\mathcal{C}|/|B|)$. Наконец, из $|\mathcal{C}| \ge 6\Phi|B| \times$ $\times \log_2|B|$ следует, что $|A|\Phi\log_2|B| \le (1/6)(|A|\cdot|\mathcal{C}|/|B|)$. Складывая эти неравенства, замечая, что $19/64 < 1/3 < \log_2(4/3)$, и потенцируя обе части по основанию 2, после группировки сомножителей получаем требуемое неравенство.

Перейдем к второму событию (напомним, оно зависит от $\mathcal{F}$, которое мы предполагаем фиксированным): *существуют такой набор семейств* $\mathfrak{H} = \{\mathfrak{H}(b)\}_{b\in B}$, *в котором каждое семейство* $\mathfrak{H}(b)$ *имеет размер не более половины* $|\mathcal{C}|$, *и такое множество* $U \subset A \times B$ *размера*

$\varepsilon|A|\cdot|B|$, что для любой пары $\langle a,b\rangle\in U$ и для любой функции $c\in\mathcal{C}$, не принадлежащей $\mathfrak{H}(b)$, значение $c(a)$ не равно b.

Здесь нам будет удобно считать, что семейства $\mathfrak{H}(b)$ состоят не из функций, а из их индексов (чисел от 1 до $|\mathcal{C}|$). (Событие при этом останется тем же.)

Чтобы оценить вероятность интересующего нас ("второго") события, зафиксируем $\mathcal{F}$, $\mathfrak{H}$ и U. Тогда соответствующее событие можно описать как пересечение по всем парам $\langle a,b\rangle$ и по всем $i\notin\mathfrak{H}(b)$ событий $c[i](a)\ne b$ ("функция номер i в точке a не равна b"). Оценка была бы простой, если бы эти события были независимы: тогда надо было бы возвести $1-1/|B|$ в степень, равную количеству всех троек $\langle i,a,b\rangle$, т.е. $\varepsilon|A|\cdot|B|\cdot|\mathcal{C}|/2$. (Мы умножили число пар $\langle a,b\rangle\in U$ на количество возможных i для данного b.) При разных a (а также при разных i) эти события независимы по построению, но события $c[i](a)\ne b_1$ и $c[i](a)\ne b_2$ зависимы. Нас выручает то, что зависимость тут "в нашу пользу" — тот факт, что мы знаем, что $c[i](a)\ne b_1$, только уменьшает вероятность события $c[i](a)\ne b_2$ (знаменатель в $1/|B|$ уменьшается на 1, аналогично и для большего количества условий). Формально говоря, можно сгруппировать события с одними и теми же a и i и воспользоваться неравенством $1-k/|B|\le(1-1/|B|)^k$, где k — число событий в группе.

Таким образом, мы получили верхнюю оценку для вероятности неудачи (при фиксированных $\mathcal{F}$, $\mathfrak{H}$ и U): она не превосходит

$$\left(1-\frac{1}{|B|}\right)^{\varepsilon|A|\cdot|B|\cdot|\mathcal{C}|/2}\le 2^{-\varepsilon|A|\cdot|\mathcal{C}|/2}.$$

Остается умножить эту вероятность на количество множеств U (их не больше $2^{|A|\cdot|B|}$), на количество наборов $\mathfrak{H}$ (их не больше $(2^{|\mathcal{C}|})^{|B|}$) и на количество семейств $\mathcal{F}$. В результате получим

$$2^{-\varepsilon|A|\cdot|\mathcal{C}|/2}\cdot 2^{|A|\cdot|B|}\cdot 2^{|\mathcal{C}|\cdot|B|}|B|^{|A|\Phi}.$$

Нетрудно проверить, что это меньше $1/2$ при $|B|\ge 2$, $\varepsilon\ge 4|B|/|A|$, $|\mathcal{C}|\ge 20|B|/\varepsilon$ и $|\mathcal{C}|\ge$ $\ge(6\Phi\log_2|B|)/\varepsilon$. Действительно, $1+|A|\cdot|B|\le 3|A|\cdot|B|/2$ при непустом A и $|B|\ge 2$, поэтому из $|\mathcal{C}|\ge 20|B|/\varepsilon$ следует, что $1+|A|\cdot|B|\le(3/40)\varepsilon|A|\cdot|\mathcal{C}|$. Из $\varepsilon\ge 4|B|/|A|$ следует, что $|\mathcal{C}|\cdot|B|\le(1/4)\varepsilon|A|\cdot|\mathcal{C}|$. Наконец, из $|\mathcal{C}|\ge(6\Phi\log_2|B|)/\varepsilon$ следует, что $|A|\Phi\log_2|B|\le(1/6)\varepsilon|A|\cdot|\mathcal{C}|$. Складывая эти неравенства, замечая, что $59/120<1/2$, и потенцируя обе части по основанию 2, после группировки сомножителей получаем требуемое неравенство. □

Теперь мы можем применить это комбинаторное утверждение и доказать обещанный отрицательный результат.

Пусть $\alpha>0$ — некоторая константа. Пусть m, n, l — натуральные числа, причем $n\ge 1$, $m\ge n+4$, $m-\alpha\log_2 m\ge n+2$ и $l+1+\log_2(l+1)\le 2^{m-n-2}$. Положим $N=\max\{m,l\}$.

Теорема 5. *Пусть даны слово a длины m и слово b длины n, причем*

$$m+n-\mathrm{KS}^{\mathbf{0}'}(a,b)<\alpha\log_2 m.$$

Тогда найдется слово c сложности $n+l+O(\log N)$, для которого

- $\mathrm{KS}(c|b)=\mathrm{KS}(c)+O(\log N)$;
- $\mathrm{KS}(b|a,c)=O(\log N)$;
- *для любого f, при котором $\mathrm{KS}(f)\le l-\mathrm{KS}(b|a,f)$, выполнено и $\mathrm{KS}(b|c,f)\le m-n+$ $+\mathrm{KS}(b|a,f)+O(\log N)$.*

(*Константа в $O(\cdot)$ зависит от α, но не зависит от m, n и l.*)

Объясним, каким образом эта теорема доказывает существенность условия в теореме 4. Из равенства $\mathrm{KS}(c|b) = \mathrm{KS}(c) + O(\log N)$ вытекает, что b и c независимы и $\mathrm{KS}(b|c) = \mathrm{KS}(b) = n$ (с точностью $O(\log N)$). Поскольку $\mathrm{KS}(b|a,c) = O(\log N)$, то и $\mathrm{KS}(a|c) \geq \mathrm{KS}(b|c) - \mathrm{KS}(b|a,c) = n$ (с точностью $O(\log N)$). Отметим еще, что $\mathrm{KS}(b|a) = n$ (с точностью $O(\log m)$). Таким образом, если $\mathrm{KS}(b|a,f) = O(\log N)$ для некоторого слова f длины не более l, то

$$\mathrm{KS}(b|c,f) < \min\{\mathrm{KS}(a|c), \mathrm{KS}(b|c)\} + O(\log N)$$

при $m - n < n + O(\log N)$, т.е. при $\mathrm{KS}(a) < \mathrm{KS}(b|c) + \mathrm{KS}(b|a)$.

Доказательство теоремы 5. Пусть A — множество всех слов длины m, B — множество всех слов длины n. Возьмем $\varepsilon = 1/m^\alpha$ и $\Phi = 2^{l+1}(l+1)$. Легко убедиться, что из условий на n, m, l следует, что A, B, ε и Φ удовлетворяют условиям леммы. Поэтому семейство $\mathcal{C}$ с указанными в лемме свойствами существует. Его можно эффективно найти перебором, зная A, B, ε и Φ, и поэтому сложность любого элемента $\mathcal{C}$ не превосходит логарифма числа элементов в $\mathcal{C}$ плюс $O(\log N)$, т.е. $n + l + O(\log N)$.

Возьмем в качестве $\mathfrak{H}(b)$ множество $\{c \in \mathcal{C} \colon \mathrm{KS}(c|b) < \log_2|\mathcal{C}| - 2\}$. Ясно, что $|\mathfrak{H}(b)| \leq |\mathcal{C}|/4$.

Семейство функций $\mathcal{F}$ строится так. Оно будет состоять из Φ функций, пронумерованных от 1 до Φ. Мы перечисляем все тройки $\langle a,b,f\rangle$, где $a \in A$, $b \in B$ и f — слово длины l, для которого $\mathrm{KS}(f) + \mathrm{KS}(b|a,f) \leq l$. При этом некоторые номера функций имеют метки, являющиеся словами длины l. Когда появляется новая тройка $\langle a,b,f\rangle$, мы пытаемся доопределить в точке a значением b одну из функций, уже помеченных меткой f. Если все они уже определены в точке a (и не равны b), мы выбираем номер, который еще не помечен, помечаем его словом f и полагаем функцию с соответствующим номером равной b в точке a. Каждый раз свободный (ничем не помеченный) номер найдется, поскольку для каждого f нужно не более $2^{l-\mathrm{KS}(f)+1}$ номеров (если для некоторого f потребовалось больше, значит, для некоторого a все $2^{l-\mathrm{KS}(f)+1}$ функций определены и принимают разные значения, т.е. мы перечислили уже $2^{l-\mathrm{KS}(f)+1}$ разных b, для которых $\mathrm{KS}(b|a,f) \leq l - \mathrm{KS}(f)$ — противоречие), а для всех f нужно не более $\sum_{\mathrm{KS}(f)\leq l} 2^{l-\mathrm{KS}(f)+1} = \sum_{k=0}^{l} \sum_{\mathrm{KS}(f)=k} 2^{l-k+1} = \Phi$ номеров. После того как все тройки с указанным свойством перечислены, оставшиеся неопределенными значения функций доопределяются произвольно.

Рассмотрим множество пар $\langle a,b\rangle$, не покрытых $\mathcal{C}$ при выбранных $\mathcal{F}$ и $\mathfrak{H}$. Их количество не превосходит $\varepsilon \cdot 2^{m+n}$. С другой стороны, $\mathcal{F}$ и $\mathfrak{H}$ могут быть эффективно построены с оракулом $\mathbf{0}'$ и по ним эффективно строится множество непокрытых пар, поэтому для любой непокрытой пары $\mathrm{KS}^{\mathbf{0}'}(a,b) \leq m + n - \alpha \log_2 m$.

Таким образом, для любых слов a и b, у которых $m + n - \mathrm{KS}^{\mathbf{0}'}(a,b) < \alpha \log_2 m$, найдется такое $c \in \mathcal{C}$, что $c(a) = b$, $c \notin \mathfrak{H}(b)$ и для любой $f \in \mathcal{F}$ количество таких $x \in A$, что $c(x) = f(x)$, не больше 2^{m-n+2}.

Из $c(a) = b$ следует, что $\mathrm{KS}(b|a,c) = O(\log N)$.

Из $c \notin \mathfrak{H}(b)$ следует, что $\mathrm{KS}(c|b) \geq \log_2|\mathcal{C}| - 2$, т.е. $\mathrm{KS}(c) = \mathrm{KS}(c|b) + O(\log N)$.

Осталось оценить $\mathrm{KS}(b|c,f)$ для f, у которых $\mathrm{KS}(f) \leq l - \mathrm{KS}(b|a,f)$. Зная слово f, будем перечислять те функции из $\mathcal{F}$, которые помечены f. Одна из них, скажем, $\widetilde{f}$ содержит пару $\langle a,b\rangle$ (иными словами, $\widetilde{f}(a) = b$), для ее задания нужно не более $\mathrm{KS}(b|a,f) + O(\log N)$ дополнительных битов. Теперь по $\widetilde{f}$ и c можно перечислять множество таких x, что $c(x) = \widetilde{f}(x)$. (Строго говоря, при помощи $\mathrm{KS}(b|a,f) + O(\log N)$ битов мы можем задать только номер $\widetilde{f}$ в семействе $\mathcal{F}$, а не саму конечную функцию. Однако для перечисления решений уравнения $c(x) = \widetilde{f}(x)$ нам достаточно того, что мы можем перечислять пары $\langle x,y\rangle$, для которых $y = \widetilde{f}(x)$, повторяя процесс построения $\mathcal{F}$.) Это множество содержит a и состоит максимум из 2^{m-n+2} элементов, и мы можем задать a, затратив еще $m - n + 2$ битов. Итого, $\mathrm{KS}(b|c,f) \leq \mathrm{KS}(a|c,f) + O(\log N) \leq \mathrm{KS}(b|a,f) + m - n + O(\log N)$, что и требовалось. $\square$

Открытые вопросы. 1. Можно ли в последней теореме улучшить оценку, выбрав c сложности $n + O(\log N)$ вместо $n + l + O(\log N)$? (В своем докладе Ан.А. Мучник говорил, что это верно, но требует более сложного комбинаторного рассуждения, которое не было рассказано.)

2. Последняя теорема показывает, что если a не намного сложнее b, то при некотором c короткие секретные сообщения невозможны. В то же время альтернативное доказательство теоремы 1 показывает, что при пустом c короткие секретные сообщения всегда возможны. Можно ли указать какие-то классы слов c, для которых возможны и для которых невозможны короткие сообщения?

3. Что можно сказать о возможных сложностях $\mathrm{KS}(f|b)$, $\mathrm{KS}(f|a,b)$, $\mathrm{KS}(f|a,b,c)$ для секретных f?

СПИСОК ЛИТЕРАТУРЫ

1. *Muchnik An.A.* Conditional complexity and codes // Theor. Comput. Sci. 2002. V. 271, N 1–2. P. 97–109. [Предварит. версия: *Muchnik An., Semenov A.* Multi-conditional descriptions and codes in Kolmogorov complexity: ECCC Tech. Rep. N 15, Jan. 27, 2000.]
2. *Shen A., Vereshchagin N.* Logical operations and Kolmogorov complexity // Theor. Comput. Sci. 2002. V. 271, N 1–2. P. 125–129.