

Колмогоровская сложность и криптография

Ан. А. Мучник*

Аннотация

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.

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

Начнём 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 $KS(X \rightarrow y)$ как минимальную длину программы, которая даёт 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

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

(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 $X \rightarrow y$ (левая часть) может быть существенно больше «неравномерной».

Чтобы убедиться в этом, возьмём в качестве y несжимаемое слово длины n , а в качестве X возьмём множество всех слов x , для которых $KS(y|x) < n/2$. 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 даёт y на любом входе x , для которого $KS(y|x) < n/2$. Среди таких входов есть слова сложности $n/2 + O(\log n)$, и вместе с

*В статье излагается часть результатов Ан. А. Мучника (1958–2007), рассказанных им 11 марта и 8 апреля 2003 года на колмогоровском семинаре кафедры математической логики и теории алгоритмов механико-математического факультета МГУ; формулировки этих результатов 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 годах.

p их достаточно для получения y , поэтому $KS(y|p) \leq n/2 + O(\log n)$. Значит, существует слово e длины $O(\log n)$, для которого $KS(y|\langle p, e \rangle) < n/2$. 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 $2n$.

Сложность задачи $(a \rightarrow b) \rightarrow b$

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 $(a \rightarrow b)$ как множество всех программ, которые на входе a дают b . Известно [2], что

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

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 найдётся программа f , переводящая a в b , для которой

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

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 $KS(b|f)$ для всех функций, переводящих a в b . (При этом мы ограничиваемся конечными функциями, определёнными на множестве всех слов длины не более N со значениями 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: $KS(b'|f) \leq m$ для всякой функции f , определённой 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 \tilde{S} , которое является графиком некоторого взаимно однозначного соответствия. Пара $\langle a, b \rangle$ уже не обязана принадлежать \tilde{S} , но в \tilde{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 \tilde{S} содержит не более $O(2^m)$ элементов (тогда порядковый номер указанной пары в перечислении множества \tilde{S} содержит m битов и позволяет восстановить либо a , либо b).

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

Криптографическая интерпретация

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

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

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

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 найдётся слово f , для которого:

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

Условие (1) говорит, что сообщение f для посвящённых (знающих слово a) содержит всю необходимую информацию о b , а условие (2) говорит, что для непосвящённых (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 нём 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 $KS(b)$ и $KS(a)$ близки к n , а $KS(b|b)$ 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 $KS(b|f) \approx n$.

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 $KS(b'|b) = O(\log N)$, $KS(b|a, b') = O(\log N)$ и длина b' равна $KS(b|a) + O(\log N)$. 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 $KS(b|f) = \min\{KS(a), KS(b)\}$ с логарифмической точностью.

В самом деле, с логарифмической точностью

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

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 $KS(b) - KS(b|a) + KS(a'')$, что равно $\min\{KS(a), KS(b)\}$. (Конец альтернативного доказательства теоремы 1).

Преимущество этого рассуждения в том, что слово f получается полиномиальной (от N) длины и даже минимально возможной длины $KS(b|a)$. (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 найдётся слово f длины $KS(b|a)$, для которого*

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

и

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

С другой стороны, недостаток этого рассуждения в том, что оно не обобщается (по крайней мере непосредственно) на случай дополнительной информации c (то есть 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 $KS(a|c) = KS(a, c|c) = KS(a, b|c) = 2n$, $KS(b|c) = 2n$, но $KS(b|c, a \oplus b) = 0$.

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 $KS(a|c) \geq KS(b|c) + KS(b|a) + O(\log N)$), то существует сообщение f , которое обладает указанными в теореме 2 свойствами и имеет сложность $KS(b|a) + O(\log N)$. Для этого мы используем следующую комбинаторную лемму.

Комбинаторная лемма

Лемма. Для любых натуральных m и $n \geq m$ существует семейство \mathcal{F} функций вида $\mathbb{B}^n \rightarrow \mathbb{B}^m$, состоящее из $2^m \text{poly}(n)$ 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 со второй координатой b , не покрытых графиками функций из \mathcal{F}' , содержит не более $O(2^m)$ точек.

Формально свойство семейства \mathcal{F} , о котором идёт речь в лемме, можно записать так:

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

(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 найдётся функция, переводящая a в b , если только a не принадлежит малому множеству исключений (что будет противоречить предположению об a , так как эти исключения имеют малую сложность).

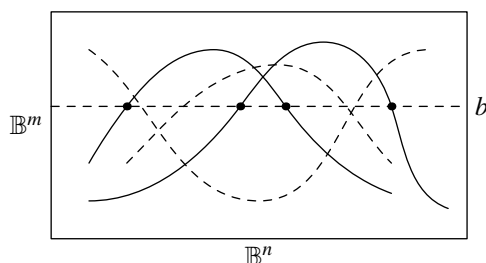


Рис. 1. Часть функций (до 50%) из \mathcal{F} выброшены; тем не менее графики оставшихся покрывают любую горизонталь, не считая $O(2^m)$ точек.

Доказательство. Используя вероятностный метод, возьмём случайное семейство из 2^t случайных функций $\varphi_1, \dots, \varphi_{2^t}$. (Все эти функции независимы и равномерно распределены в множестве всех функций $\mathbb{B}^n \rightarrow \mathbb{B}^m$; 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 $I \subset \{1, 2, \dots, 2^t\}$, содержащее половину всех индексов,

для которых

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

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

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

(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

$$2^m \cdot 2^{2^t} \cdot 2^{ns2^m} \cdot \left(1 - \frac{1}{2^m}\right)^{2^{t-1} \cdot s2^m},$$

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

$$2^{m+2^t} \cdot 2^{ns2^m} \cdot (1/e)^{s2^{t-1}}.$$

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. Разобьём последний сомножитель на две части $(1/e)^{s2^t/4}$, и сравним эти части с первым и вторым сомножителем. Нам нужно, чтобы

$$2^{m+2^t} \cdot (1/e)^{s2^t/4} < 1$$

и

$$2^{ns2^m} \cdot (1/e)^{s2^t/4} < 1.$$

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

Основной результат

Теперь мы можем дать точную формулировку и доказательство основного результата:

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

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

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

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. Применим теорему об условном кодировании [1] и найдём слово b' длины $KS(b|a)$, для которого сложности $KS(b|b', a)$ и $KS(b'|b)$ равны $O(\log N)$. Применим комбинаторную лемму и построим семейство отображений $\mathbb{B}^n \rightarrow \mathbb{B}^m$ с указанными в ней свойствами, взяв m равным длине b' , то есть $KS(b|a)$, а n равным длине a . Без ограничения общности можно считать, что семейство \mathcal{F} является простым, то

есть 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 $KS(b|c) - KS(b|c, f)$). В самом деле, с точностью $O(\log N)$ это можно переписать как $KS(f|c) - KS(f|b, c)$ (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 остаётся воспользоваться неравенством Чебышёва.

Оставив в семействе \mathcal{F}' только функции из этого большинства, мы (по лемме) прокроем 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

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

для всех плохих a' . В самом деле, зная b и c , а также $KS(b|c)$ (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

$$KS(a'|b, c) \leq KS(b|a) + O(\log N)$$

для всех плохих a' , и потому

$$KS(a'|c) \leq KS(a'|b, c) + KS(b|c) + O(\log N) \leq KS(b|a) + KS(b|c) + O(\log N),$$

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 $KS(a) > KS(b)$ 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 начнём с более простого рассуждения, которое, правда, даёт 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 $KS(b|c) \approx n$ получается $KS(b|f, c) \approx 0,3n$.

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 может требовать меньше битов, чем $KS(b)$ (которое равно $KS(b|c)$; как мы говорили, само по себе c не содержит информации от 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 её 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 её 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 , причём она имеет не очень большую длину (существенно меньшую, чем то, что даёт 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 попадёт 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 $KS(a|f, c)$ и $KS(b|f, c)$ 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 $KS(b)$ 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 (c 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 найдётся 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 $A \rightarrow B$ *бракует* функцию $c: A \rightarrow B$, если при каком-нибудь $f \in \mathcal{F}$ размер множества $\{a: c(a) = f(a)\}$ 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 (то есть $\mathfrak{H}(b)$ при любом $b \in B$ является семейством функций вида $A \rightarrow B$). 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, причём 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 найдётся такое семейство \mathcal{C} функций вида $A \rightarrow B$ 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 $|\mathcal{C}|$ (то есть $|\mathfrak{H}(b)| \leq |\mathcal{C}|/4$ 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 $\mathfrak{H}(b)$):

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

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). Возьмём 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”, найдётся покрывающая их функция c из семейства \mathcal{C} . Эта функция (точнее, её 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 и тем самым b упрощается: достаточно указать порядковый номер a в перечислении всех решений уравнения $f(x) = c(x)$. Выбранное нами \mathfrak{H} , с другой стороны, 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. В качестве \mathcal{C} возьмём 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”, то есть 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 $1/2$, делённой 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 $c \in \mathcal{C}'$ найдётся 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} , то есть $2^{|\mathcal{C}'|}$. 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 , то есть C_q^r , не превосходит $q^r/r! \leq q^r/((r/3)^r) = (3q/r)^r$. 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 остаётся меньше $1/2$, поскольку по условию леммы $|B| \geq 2$, $|A| \geq 16|B|$, $\Phi \leq 2^{|A|/4|B|}$ и $|\mathcal{C}| \geq 6\Phi|B| \log_2 |B|$. Действительно, из последнего условия следует, что $|\mathcal{C}| \geq 12$ при $\Phi \geq 1$ (случай пустого \mathcal{F} тривиален) и $|B| \geq 2$, поэтому $1 + |\mathcal{C}| \leq 13|\mathcal{C}|/12$ и из $1 \leq |A|/16|B|$ следует, что $1 + |\mathcal{C}| \leq (13/192)(|A||\mathcal{C}|/|B|)$. Из $\log_2 \Phi \leq |A|/4|B|$ следует, что $(|\mathcal{C}|/4) \log_2 \Phi \leq (1/16)(|A||\mathcal{C}|/|B|)$. Наконец, из $|\mathcal{C}| \geq 6\Phi|B| \log_2 |B|$ следует, что $|A|\Phi \log_2 |B| \leq (1/6)(|A||\mathcal{C}|/|B|)$. 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.

Перейдём ко второму событию (напомним, оно зависит от \mathcal{F} , которое мы предполагаем фиксированным): *существует 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 $\varepsilon|A||B|$, 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 $c[i](a) \neq b$ (“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 $\langle i, a, b \rangle$, то есть $\varepsilon|A| \cdot |B| \cdot |\mathcal{C}|/2$. (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 $c[i](a) \neq b_1$ и $c[i](a) \neq b_2$ зависимы. Нас выручает то, что зависимость тут “в нашу пользу” — тот факт, что мы знаем, что $c[i](a) \neq b_1$, только увеличивает вероятность события $c[i](a) \neq b_2$ (знаменатель в $1/|B|$ уменьшается на единицу, аналогично и для большего количества условий). Формально говоря, можно сгруппировать события с одними и теми же a и i и воспользоваться неравенством $(1 - k/|B|) \leq (1 - 1/|B|)^k$, 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

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

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

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

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

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

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

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

$$m + n - KS^0(a, b) < \alpha \log_2 m.$$

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

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

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

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

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

при $m - n < n + O(\log N)$, то есть при $KS(a) < KS(b|c) + KS(b|a)$.

Доказательство. Пусть A — множество всех слов длины m , B — множество всех слов длины n . Возьмём $\varepsilon = 1/m^\alpha$ и $\Phi = 2^l(l + 1)$. 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 $O(\log N)$, то есть $n + l + O(\log N)$.

Возьмём в качестве $\mathfrak{H}(b)$ множество $\{c \in \mathcal{C} : KS(c|b) \leq \log_2 |\mathcal{C}| - 2\}$. 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 $KS(f) + KS(b|a, f) \leq l$. 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 ещё не помечен, помечаем его словом f и полагаем функцию с соответствующим номером равной b в точке a . Каждый раз свободный (ничем не помеченный) номер найдётся, поскольку для каждого f нужно не более $2^{l-KS(f)}$ номеров (если для некоторого f потребовалось больше, значит, для некоторого a все $2^{l-KS(f)}$ функций

определены и принимают разные значения, то есть мы перечислили уже $2^{l-KS(f)} + 1$ разных b , для которых $KS(b|a, f) \leq l - KS(f)$ — противоречие), а для всех f нужно не более $\sum_{KS(f) \leq l} 2^{l-KS(f)} = \sum_{k=0}^l \sum_{KS(f)=k} 2^{l-k} = \Phi$ номеров. После того, как все тройки с указанным свойством перечислены, оставшиеся неопределёнными значения функций доопределяются произвольно.

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

Таким образом, для любых слов a и b , у которых $m + n - KS^{\mathbf{0}'}(a, b) < \alpha \log_2 m$, найдётся такое $c \in \mathcal{C}$, что $c(a) = b$, $c \notin \mathcal{H}(b)$ 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 $KS(b|a, c) = O(\log N)$.

Из $c \notin \mathcal{H}(b)$ следует, что $KS(c|b) > \log_2 |\mathcal{C}| - 2$, то есть $KS(c) = KS(c|b) + O(\log N)$.

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

Открытые вопросы.

- 1) Можно ли в последней теореме выбрать c сложности $n + O(\log N)$ вместо $n + l + O(\log N)$?¹
- 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 $KS(f|b)$, $KS(f|a, b)$, $KS(f|a, b, c)$ для секретных f ?

Литература

- [1] Muchnik An. A. Conditional complexity and codes, *Theoretical Computer Science*, v. 271 (2002), issues 1–2, p. 97–109. [Preliminary version: Andrej Muchnik, Alexej

¹В своём докладе Ан. А. Мучник говорил, что это верно, но требует более сложного комбинаторного рассуждения (которое не было рассказано).

Semenov, Multi-conditional Descriptions and Codes in Kolmogorov Complexity, ECCC Technical Report, 2000, no. 15, January 27, 2000.]

- [2] A. Shen, N. Vereshchagin. Logical operations and Kolmogorov complexity. *Theoretical Computer Science*, 2002, v. 271, pp. 125–129.