

# Сложностная интерпретация задачи о вилочной сети<sup>1</sup>

А.Е.Ромашенко

Институт проблем передачи информации, Российской академии наук, Москва, Россия  
e-mail: anromash@mccme.ru

Поступила в редакцию 27.12.2004

**Аннотация**— Для многих утверждений классической (шенноновской) теории информации известны аналоги в теории колмогоровской сложности. В первой части данной статьи даётся краткий обзор результатов, показывающих параллелизм между свойствами энтропии Шенна и колмогоровской сложностью. Во второй части доказывается новый результат, демонстрирующий данный параллелизм: для колмогоровской сложности оказывается верен аналог теоремы Вольфа о характеристиках пропускной способности вилочной сети.

## 1. ВВЕДЕНИЕ

В [1] А. Н. Колмогоров ввёл понятие *алгоритмической сложности*. Алгоритмической сложностью двоичного слова (т.е. конечной последовательности нулей и единиц) называется длина кратчайшей программы, которая печатает данное слово; сложностью слова  $x$  относительно слова  $y$  называется длина кратчайшей программы, которая печатает  $x$ , получив на вход  $y$ . Определённая таким образом сложность зависит от способа программирования. Однако можно выбрать *оптимальный* способ программирования, который обеспечивает минимальную возможную (с точностью до ограниченного аддитивного члена) сложность всех слов, см. [1, 2]. Колмогоров отмечал, что алгоритмическая сложность является уточнением меры информации, введённой К. Шенном — шенноновской энтропии. При этом формальные определения энтропии Шенна и алгоритмической сложности (часто называемой колмогоровской сложностью) совершенно различны: первое относится к теории вероятностей и даёт численную характеристику распределения случайной функции, а второе использует методы теории рекурсивных функций и описывает количество информации, заключённой в двоичном слове. Однако оба подхода формализуют близкие интуитивные идеи о том, что такое *информация*, содержащаяся в некотором объекте.

Неудивительно, что многие свойства колмогоровской сложности и шенноновской энтропии оказываются аналогичны. Далее мы рассмотрим несколько примеров параллелизма формальных свойств энтропии Шенна и колмогоровской сложности. Во второй части статьи мы докажем новый результат, демонстрирующий указанный параллелизм. А именно, мы докажем колмогоровский аналог теоремы Вольфа [5] о характеристиках достижимых скоростей передачи информации в вилочной сети.

## 2. ПАРАЛЛЕЛИЗМ МЕЖДУ КЛАССИЧЕСКОЙ И АЛГОРИТМИЧЕСКОЙ ТЕОРИЯМИ ИНФОРМАЦИИ

### 2.1. Линейные информационные неравенства

Начнём с наиболее простого примера. И для энтропии Шенна, и для колмогоровской сложности некоторые важные свойства выражаются линейными неравенствами. Одно из таких свойств — субаддитивность. Для шенноновской энтропии оно выражается неравенством

$$H(\alpha_1, \alpha_2) \leq H(\alpha_1) + H(\alpha_2),$$

<sup>1</sup> Работа выполнена при поддержке Фонда содействия отечественной науке и гранта РФФИ № 03-01-00475.

которое верно для любого совместного распределения<sup>1</sup>  $(\alpha_1, \alpha_2)$ . Аналогичное неравенство верно и для колмогоровской сложности:

$$K(a_1, a_2) \leq K(a_1) + K(a_2) + O(\log(K(a_1) + K(a_2))),$$

где  $a_1$  и  $a_2$  – двоичные слова. Отметим, что в последнем неравенстве нельзя устраниТЬ добавочный член  $O(\log(K(a_1) + K(a_2)))$ .

Известны и другие, более сложные линейные неравенства для энтропии и для колмогоровской сложности (см. [9, 13, 14]). При этом, как показано в [9], параллелизм между сложностными и энтропийными неравенствами является общим правилом. Сформулируем данное утверждение более точно. Для этого дадим общее определение *информационного неравенства*. Будем говорить, что набор коэффициентов  $\{\lambda_W\}$  задаёт неравенство для энтропии Шеннона, если для любого распределения  $n$ -ки случайных функций  $(\alpha_1, \dots, \alpha_n)$  выполнено

$$\sum \lambda_{i_1, \dots, i_k} H(\alpha_{i_1}, \dots, \alpha_{i_k}) \geq 0, \quad (1)$$

где суммирование берётся по всем непустым подмножествам  $\{i_1, \dots, i_k\} \subset \{1, \dots, n\}$ . Аналогично, говорят, что набор коэффициентов  $\{\lambda_W\}$  задаёт неравенство для колмогоровской сложности, если для любого набора слов  $(x_1, \dots, x_n)$  выполнено

$$\sum \lambda_{i_1, \dots, i_k} K(x_{i_1}, \dots, x_{i_k}) + C \log(|x_1| + \dots + |x_n|) + C \geq 0, \quad (2)$$

где сумма также берётся по всем непустым подмножествам  $\{i_1, \dots, i_k\} \subset \{1, \dots, n\}$ ; константа  $C$  в неравенстве зависит только от набора коэффициентов и от выбора оптимального способа программирования (но не от слов  $x_1, \dots, x_n$ ).

**Теорема 1** ([9]). *Для любого набора коэффициентов  $\{\lambda_W\}$  неравенство (1) выполнено для энтропии Шеннона тогда и только тогда, когда неравенство (2) с теми же коэффициентами выполнено для колмогоровской сложности.*

В настоящее время не известно никакого простого описания класса всех информационных неравенств. Более того, не удается доказать или опровергнуть некоторые конкретные информационные неравенства для четвёрок случайных величин (и, соответственно, для четвёрок слов) [11].

## 2.2. Теорема Вольфа–Слепяна

Другой важный пример параллелизма между шенноновской и колмогоровской теориями – это теорема Вольфа–Слепяна и её алгоритмический аналог. Результат Вольфа и Слепяна обобщает классическую теорему Шеннона о передачи информации в канале без шума. Она показывает, как вспомогательный источник информации  $\beta$  может быть использован для кодирования основного источника  $\alpha$ :

**Теорема 2** ([4]). *Пусть  $(\alpha^i, \beta^i)$ ,  $i = 1, 2, \dots$ , – независимые одинаково распределённые пары случайных величин на  $A \times B$ . Тогда для любого  $\varepsilon > 0$  существуют отображения*

$$\begin{aligned} f^n : A^n &\rightarrow \{0, 1\}^{l(n)}, \\ g^n : \{0, 1\}^{l(n)} \times B^n &\rightarrow A^n \end{aligned}$$

такие, что

$$\text{Prob}[(\alpha^1, \dots, \alpha^n) = g^n(f^n(\alpha^1, \dots, \alpha^n), (\beta^1, \dots, \beta^n))] > 1 - \varepsilon,$$

причём  $\lim_{n \rightarrow \infty} (l(n)/H(\alpha|\beta)) = 1$ .

---

<sup>1</sup> Здесь и далее мы рассматриваем распределения вероятностей только на конечных множествах.

Интуитивный смысл Теоремы 2 прост: требуется закодировать и передать наиболее экономным способом результат  $n$  независимых испытаний случайной величины  $\alpha$ . Для кодирования используется функция  $f^n : A^n \rightarrow \{0, 1\}^{l(n)}$ . При декодировании допускается вероятность ошибки не более  $\varepsilon$ . Из теоремы Шеннона известно, что длину посылаемого сообщения  $l(n)$  можно сделать равной  $nH(\alpha) + o(n)$ . Однако в данном случае при декодировании (которое производится с помощью функции  $g^n$ ) имеется дополнительная информация – значение случайной величины  $\beta$ . Это позволяет сократить длину кодовых слов до  $H(\alpha|\beta)n + o(n)$ . Нетривиальной теореме Вольфа–Слепяна делает то, что значения  $\beta$  известно лишь при декодировании, но не при кодировании (формально это значит, что  $(\beta^1, \dots, \beta^n)$  является аргументом  $g^n$ , но не  $f^n$ ).

Для колмогоровской сложности аналог данного результата был доказан Ан. А. Мучником:

**Теорема 3 ([10]).** Для любых слов  $a, b$  найдётся такое слово  $a'$ , что

1.  $K(a'|a) = O(\log n)$ ,
2.  $K(a|a', b) = O(\log n)$ ,
3.  $|a'| = K(a|b)$ ,

где  $n = K(a) + K(b)$ .

В данном случае слово  $a'$  играет роль *кода*, который позволяет легко восстановить  $a$  при известном  $b$ . При этом сам код  $a'$  просто вычисляется по слову  $a$ . Как это обычно бывает в теории колмогоровской сложности, формализуя условие *относительной просты*, мы требуем, чтобы соответствующие относительные колмогоровский сложности имели величину  $O(\log n)$ .

Иногда Теорему 3 формулируют следующим образом: среди кратчайших (точнее, *близких* по длине к кратчайшей) программ, переводящих  $b$  в  $a$ , можно выбрать такую, которая проста относительно  $a$ .

Нетрудно проверить, что Теорему 2 нельзя усилить, сделав отношение  $\frac{l(n)}{H(\alpha|\beta)}$  меньше единицы. Аналогично, в Теореме 3 при выполнении условий 1) и 2) с необходимостью выполнено  $|a'| \geq K(a|b) - O(\log n)$ . Таким образом, достигнуты асимптотически оптимальные результаты.

Доказательство Теоремы 2 и Теоремы 3 состоит в построении своего рода ‘контрольных сумм’, легко вычислимых по значениям первого источника информации, и позволяющих восстановить его значение, если в качестве дополнительной информации задан второй источник. Но при этом техника, используемая в доказательствах Вольфа–Слепяна и Мучника, совершенно различна.

### 2.3. Передача информации в вилочной сети

Интересное обобщение Теоремы 2 – теорема о кодировании вилочной сети. Сначала дадим определение:

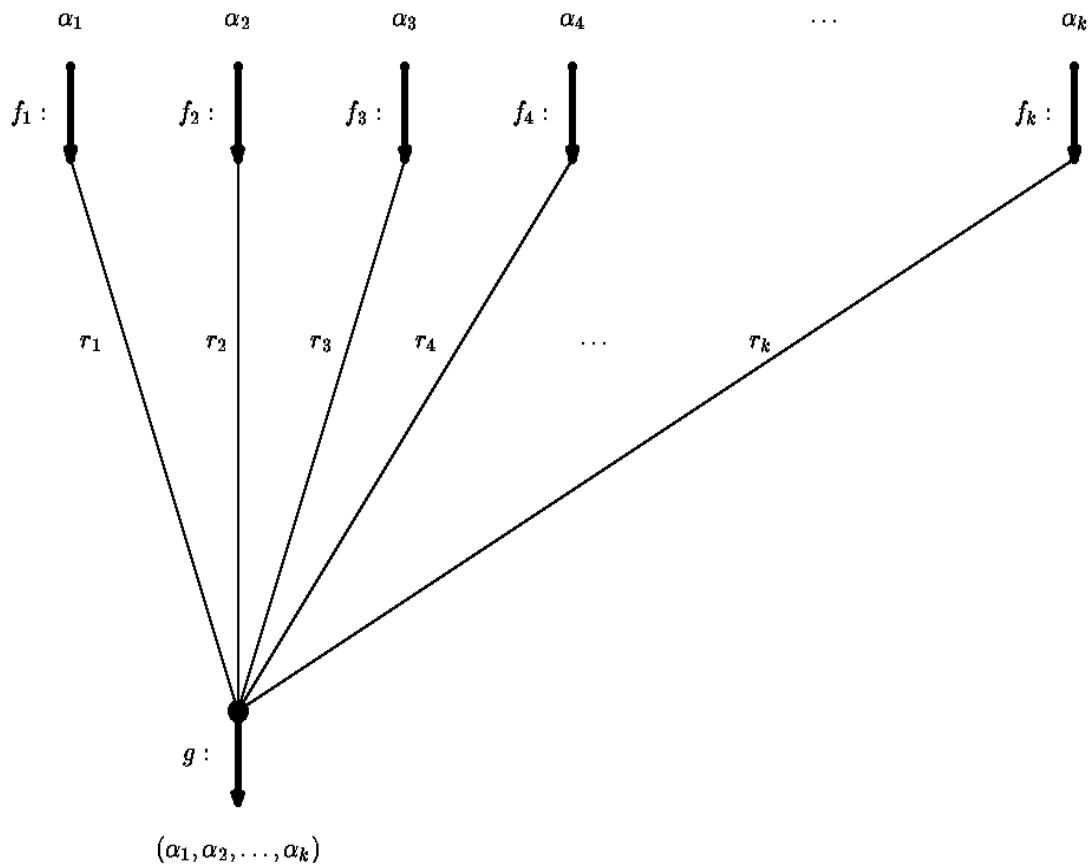
**Определение 1.** Пусть задано распределение вероятностей  $(\alpha_1, \dots, \alpha_k)$  на  $A_1 \times \dots \times A_k$ . Обозначим  $(\alpha_1^i, \dots, \alpha_k^i)$  ( $i = 1, 2, \dots$ ) последовательность независимых  $k$ -мерных случайных величин, каждая из которых имеет такое же распределение, как  $(\alpha_1, \dots, \alpha_k)$ . Набор из  $k$  чисел  $(r_1, \dots, r_k)$  называется  $\varepsilon$ -достижимым набором скоростей для вилочной сети с источниками  $\alpha_1, \dots, \alpha_k$ , если для любого  $\delta > 0$  и достаточно больших  $n$  существуют функции  $f_1^n, \dots, f_k^n, g^n$ ,

$$\begin{aligned} f_j^n : (A_j)^n &\rightarrow \{0, 1\}^{l_j(n)}, \\ g^n : \{0, 1\}^{l_1(n)+\dots+l_k(n)} &\rightarrow A_1 \times \dots \times A_k \end{aligned}$$

такие, что  $l_j(n) \leq (r_j + \delta)n$ , и

$$\text{Prob}[g^n(f_1^n(\bar{\alpha}_1), \dots, f_k^n(\bar{\alpha}_k)) = (\bar{\alpha}_1, \dots, \bar{\alpha}_k)] > 1 - \varepsilon,$$

где  $\bar{\alpha}_j$  обозначает  $n$ -ку  $(\alpha_j^1, \dots, \alpha_j^n)$ .

Рис. 1. Виличная сеть с  $k$  источниками

Данное определение соответствует передаче информации в сети, изображённой на Рис.1. Имеется  $k$  коррелированных источников информации, которые заданы распределением  $\alpha_1, \dots, \alpha_k$ . Каждый источник независимо от других кодируется с помощью блокового кода  $f_j^n$ . На один кодируемый символ  $\alpha_j$  в среднем приходится около  $r_j$  передаваемых битов. Получатель с помощью декодера  $g^n$  восстанавливает значения всех  $k$  источников информации с вероятностью ошибки меньше  $\varepsilon$ .

Множество наборов  $\varepsilon$ -достижимых скоростей имеет простое описание в терминах энтропий случайных величин  $\alpha_j$ :

**Теорема 4 ([5]).** Для любого распределения вероятностей  $(\alpha_1, \dots, \alpha_k)$  и любого  $\varepsilon > 0$  набор чисел  $(r_1, \dots, r_k)$  является  $\varepsilon$ -достижимым набором скоростей для виличной сети с данными  $k$  источниками, если и только если для всякого непустого  $W \subset \{1, \dots, k\}$  выполнено неравенство

$$\sum_{j \in W} r_j \geq H(\alpha_W | \alpha_{\neg W}),$$

где  $\alpha_W$  – набор случайных величин, составленный из  $\alpha_j$  для всех  $j \in W$ , а  $\alpha_{\neg W}$  – набора случайных величин, составленный из  $\alpha_j$  для  $j \notin W$ .

*Комментарий к обозначениям:* Здесь мы впервые использовали обозначение  $\alpha_W$  для набора индексов  $W$ . Оно позволяет сократить весьма громоздкую запись. На пример, если  $W = \{1, 2, 5\}$ , то  $\alpha_W$  обозначает тройку  $(\alpha_1, \alpha_2, \alpha_5)$ . Если  $W = \emptyset$ , будем считать  $\alpha_W$  константой (случайной функцией с энтропией ноль). В частности, если  $W = \{1, \dots, k\}$  и  $\neg W = \emptyset$ , то  $H(\alpha_W | \alpha_{\neg W}) = H(\alpha_W)$ .

**Пример 1.** Применим Теорему 4 для  $k = 2$ : пара  $(r_1, r_2)$  является  $\varepsilon$ -достижимым набором скоростей для  $(\alpha_1, \alpha_2)$ , если и только если

$$\begin{aligned} r_1 &\geq H(\alpha_1|\alpha_2), \\ r_2 &\geq H(\alpha_2|\alpha_1), \\ r_1 + r_2 &\geq H(\alpha_1, \alpha_2). \end{aligned}$$

Доказательство Теоремы 4 опирается на теорему Вольфа–Слепяна (см. обсуждение в [7]).

Далее мы сформулируем и докажем аналог Теоремы 4 для колмогоровской сложности. В шенноновском случае мы указали необходимые и достаточные условия для возможности передать случайные величины  $\alpha_1, \dots, \alpha_k$  в вилочной сети со скоростями  $r_1, \dots, r_k$ . В алгоритмическом аналоге этой задачи мы укажем критерий для следующего свойства колмогоровских сложностей слов  $a_1, \dots, a_n$ :

Для заданных слова  $a_1, \dots, a_k$  и набора чисел  $r_1, \dots, r_k$  существуют слова  $a'_1, \dots, a'_k$ , такие что

- 1)  $|a'_j| \leq r_j, j = 1, \dots, k,$
  - 2)  $K(a'_j|a_j) \leq C_0 \log n, j = 1, \dots, k,$
  - 3)  $K(a_1, \dots, a_k|a'_1, \dots, a'_k) < C_0 \log n,$
- $n = |a_1| + \dots + |a_k|$ .
- (\*)

**Теорема 5** (Основная теорема).

**(Необходимость:)** Для всякого целого  $k > 0$  и  $C_0 > 0$  существует такая константа  $C_1$ , что для любых слов  $a_1, \dots, a_k$  и чисел  $r_1, \dots, r_k$  для выполнения свойства (\*) необходимо, чтобы для любого непустого  $W \subset \{1, \dots, k\}$  выполнялось неравенство

$$\sum_{j \in W} r_j \geq K(a_W|a_{\neg W}) - C_1 \log n.$$

**(Достаточность:)** Для любого целого  $k > 0$  и любого  $C_2 > 0$  существует такое число  $C_0$ , что для любых слов  $a_1, \dots, a_k$  и чисел  $r_1, \dots, r_k$  для выполнения свойства (\*) достаточно, чтобы для любого непустого  $W \subset \{1, \dots, k\}$  выполнялось неравенство

$$\sum_{j \in W} r_j \geq K(a_W|a_{\neg W}) + C_2 \log n.$$

Здесь  $a_W$  – кортеж слов, составленный из  $a_j$  для всех  $j \in W$ , а  $a_{\neg W}$  – кортеж слов, составленный из  $a_j$  для  $j \notin W$ ,  $n = |a_1| + \dots + |a_k|$ .

Мы используем обозначение  $a_W$  аналогичное введённому выше обозначению для случайных величин. Для пустого  $W$  будем считать  $a_W$  пустым словом. В частности, если  $W = \{1, \dots, k\}$  и  $\neg W = \emptyset$ , то  $K(a_W|a_{\neg W})$  с точностью до ограниченного слагаемого совпадает с  $K(a_W)$ .

**Пример 2.** При  $k = 2$  теорема даёт необходимые и достаточные условия вида

$$\begin{aligned} r_1 &\geq K(a_1|a_2) + O(\log n), \\ r_2 &\geq K(a_2|a_1) + O(\log n), \\ r_1 + r_2 &\geq K(a_1, a_2) + O(\log n). \end{aligned}$$

Для  $n = 2, 3$  данная теорема была доказана в [12]. Полное доказательство Теоремы 5 является основным результатом данной статьи. Предлагаемое доказательство опирается на алгоритмический аналог теоремы Вольфа–Слепяна.

Обычное доказательство Теоремы 4 (см. [7]) нельзя перевести на язык колмогоровской сложности, механически заменив Теорему 2 на её алгоритмический аналог (Теорему 3). Дело в том, что доказательство, предложенное в [7], существенно использует принцип *разделения времени*. Для колмогоровской сложности данный приём не работает. Поэтому для доказательства основной теоремы нам потребуется утверждение более сильное, чем Теорема 3:

**Теорема 6 ([10]).** Для любого целого  $k > 0$  существует  $C = C(k)$  со следующим свойством. Пусть даны слова  $x_0, x_1, \dots, x_k$ ,  $n = |x_1| + \dots + |x_k|$ , и число  $r < |x_0|$ . Тогда найдётся слово  $y$  такое, что

1.  $|y| = r$ ,
2.  $K(y|x_0) \leq C \log n$ ,

а также  $K(y|x_j) \geq \min\{K(x_0|x_j), r\} - C \log n$  для любого  $j = 1, \dots, k$ .

Говоря неформально, Теорема 6 утверждает, что из слова  $x_0$  можно легко (с логарифмической сложностью) выделить  $r$  битов информации, которые являются максимально ‘случайными’ относительно любого  $x_j$ . Данный результат обобщает Теорему 3.

**Замечание 1.** Пусть даны слова  $x_0, x_1, \dots, x_k$  и число  $r$ . Предположим, что для некоторого  $j \leq k$  выполнено  $r \geq K(x_0|x_j)$ . В таком случае для слова  $y$  из Теоремы 6 выполнено  $K(x_0|y, x_j) = O(\log n)$ .

**Доказательство.** Для любых слов  $x_0, x_j, y$  верно равенство

$$K(x_0|y, x_j) = K(x_0, y|x_j) - K(y|x_j) + O(\log n). \quad (3)$$

Согласно Теореме 6, слово  $y$  имеет сложность  $O(\log n)$  относительно  $x_0$ . Следовательно, величина  $K(x_0, y|x_j)$  с точностью до логарифмического слагаемого совпадает с  $K(x_0|x_j)$ . Далее, по условию имеем  $K(y|x_j) \geq_n K(x_0|x_j)$ . Таким образом, из равенства (3) получаем  $K(x_0|y, x_j) = O(\log n)$ .

Отметим, что Теорема 3 следует из Теоремы 6 при  $k = 1$ , если положить  $x_0 = a, x_1 = b$  и  $r_1 = K(a|b)$ .

### 3. ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 5

Для краткости мы будем использовать следующие обозначения:

$$\begin{aligned} F \leq_n G &\Leftrightarrow F \leq G + O(\log n), \\ F \geq_n G &\Leftrightarrow G \leq F + O(\log n), \\ F =_n G &\Leftrightarrow F = G + O(\log n). \end{aligned}$$

Приступим к доказательству теоремы.

**Необходимость:** Пусть  $W \subset \{1, \dots, k\}$  – произвольный набор индексов,  $\neg W = \{1, \dots, k\} \setminus W$ . По условию все слова  $a_i$  имеют логарифмическую сложность относительно кортежа  $\langle a'_1, \dots, a'_k \rangle$ . Ослабляя это условие, получаем  $K(a_W|a'_W, a_{\neg W}) =_n 0$ . Следовательно, сложность кортежа  $a'_W$  не может быть меньше, чем относительная сложность  $K(a_W|a_{\neg W})$ . В то же время, сложность  $a'_W$  не превышает суммы  $r_i$  по всем  $i \in W$ , что даёт требуемое неравенство.

Более формально данное рассуждение можно записать в виде цепочки неравенств:

$$\begin{aligned} K(a_W|a_{\neg W}) &\leq_n K(a'_W) + K(a_W|a'_W, a_{\neg W}) \leq_n \\ &\leq_n K(a'_W) + K(a_W|a'_W, a'_{\neg W}) \leq_n \\ &\leq_n K(a'_W) \leq_n \sum_{j \in W} r_j. \end{aligned}$$

**Достаточность:** Будем доказывать теорему индукцией по  $k$ . При этом нам потребуется рассмотреть несколько усиленный вариант теоремы:

**Усиленное утверждение теоремы:** Для любого целого  $k$  и любого  $C_2 > 0$  существует  $C_0$  со следующим свойством. Пусть даны слова  $a_1, \dots, a_k, b$  и набор чисел  $r_1, \dots, r_k$ . Обозначим  $n = |a_1| + \dots + |a_k| + |b|$ . Для того, чтобы существовали слова  $a'_1, \dots, a'_k$  такие, что

1.  $|a'_j| \leq r_j, j = 1, \dots, k$ ,
2.  $K(a'_j | a_j) \leq C_0 \log n, j = 1, \dots, k$ ,
3.  $K(a_1, \dots, a_k | a'_1, \dots, a'_k, b) < C_0 \log n$ ,

достаточно, чтобы для любого непустого  $W \subset \{1, \dots, k\}$  выполнялось неравенство  $\sum_{j \in W} r_j \geq K(a_W | a_{\neg W}, b) + C_2 \log n$ .

По сравнению с (\*) усиление состоит добавлении параметра  $b$ .

Для  $k = 1$  Усиленное утверждение немедленно следует из Теоремы 3. Проведём шаг индукции. Пусть даны слова  $a_1, \dots, a_k, a_{k+1}, b$ . Согласно Теореме 6 найдётся слово  $a'_{k+1}$  такое, что

1.  $|a'_{k+1}| \leq r_{k+1}$ ,
2.  $K(a'_{k+1} | a_{k+1}) \leq C \log n$ ,

а также для любого непустого  $W \subset \{1, \dots, k\}$

$$K(a'_{k+1} | a_W, b) \geq \min\{K(a_{k+1} | a_W, b), r_{k+1}\} - C \log n$$

(константа  $C$  зависит только от  $k$ ).

Далее применим предположение индукции к набору слов  $a_1, \dots, a_k$  и  $b' = \langle a'_{k+1}, b \rangle$  для набора чисел  $r_1, \dots, r_k$ . Прежде всего следует проверить, что выполнено условие Усиленного утверждения:

**Лемма 1.** Существует такое число  $C'_2 = C'_2(k, C_2)$ , что для любого непустого набора индексов  $V \subset \{1, \dots, k\}$  и соответствующего дополнения  $\neg V = \{1, \dots, k\} \setminus V$  верно неравенство

$$\sum_{j \in V} r_j \geq K(a_V | a_{\neg V}, b') + C'_2 \log n.$$

**Доказательство.** Согласно Теореме 6,  $K(a'_{k+1} | a_{\neg V}, b) \geq_n \min\{K(a_{k+1} | a_{\neg V}, b), r_{k+1}\}$ . Рассмотрим два случая.

**Случай 1.** Предположим  $r_{k+1} \geq K(a_{k+1} | a_{\neg V}, b)$ . Согласно Замечанию 1, по набору слов  $a'_{k+1}, a_{\neg V}, b$  можно с логарифмической сложностью получить  $a_{k+1}$ . Следовательно,

$$K(a_V | a_{\neg V}, b') \leq_n K(a_V | a_{\neg V}, b) \leq_n \sum_{j \in V} r_j$$

(последнее неравенство следует из условия теоремы).

**Случай 2.** Предположим  $r_{k+1} < K(a_{k+1} | a_{\neg V}, b)$ . В этом случае  $K(a'_{k+1} | a_{\neg V}, b) =_n r_{k+1}$ . Оценим сверху  $K(a_V | a_{\neg V}, b')$ :

$$\begin{aligned} K(a_V | a_{\neg V}, b') &= K(a_V | a_{\neg V}, a'_{k+1}, b) \leq_n \\ &\leq_n K(a_V, a'_{k+1} | a_{\neg V}, b) - K(a'_{k+1} | a_{\neg V}, b) \leq_n \\ &\leq_n K(a_V, a_{k+1} | a_{\neg V}, b) - r_{k+1} \leq \sum_{j \in V} r_j \end{aligned}$$

(мы воспользовались тем, что по условию теоремы  $K(a_V, a_{k+1} | a_{\neg V}, b) \leq r_{k+1} + \sum_{j \in V} r_j$ ). Лемма доказана.

Таким образом, можно воспользоваться предположением индукции. Заключаем, что существует набор слов  $a'_1, \dots, a'_k$ , для которых

1.  $|a'_j| \leq r_j, j = 1, \dots, k,$
2.  $K(a'_j | a_j) \leq C'_0 \log n, j = 1, \dots, k,$
3.  $K(a_1, \dots, a_k | a'_1, \dots, a'_k, a'_{k+1}, b) \leq C'_0 \log n$

для некоторого  $C'_0 = C'_0(k, C_2)$ . Иначе говоря, по набору  $(a'_1, \dots, a'_{k+1}, b)$  с логарифмической сложностью можно получить набор слов  $a_1, \dots, a_k$ . Остаётся доказать, что аналогичное утверждение верно и для  $a_{k+1}$ , то есть

$$K(a_{k+1} | a'_1, \dots, a'_k, a'_{k+1}, b) \leq C_0 \log n$$

для некоторого  $C_0 \geq C'_0$  (зависящего только от  $k$  и  $C_2$ ). Для этого достаточно установить, что  $K(a_{k+1} | a_1, \dots, a_k, a'_{k+1}, b) =_n 0$ . Но это равенство следует из условия

$$r_{k+1} \geq K(a_{k+1} | a_1, \dots, a_k, b) + C_2 \log n$$

и Замечания 1. Теорема доказана.

#### 4. ЗАКЛЮЧЕНИЕ

Мы рассмотрели несколько утверждений, демонстрирующих параллелизм свойств шенноновской энтропии и колмогоровской сложности. Краткий обзор в первой части статьи не претендует на полноту. Некоторые важные примеры данного параллелизма не были рассмотрены. В частности, не обсуждалась задача о выделении общей информации, которая изучалась как в шенноновской, так и в колмогоровской теории [3, 6, 7, 8].

В настоящее время не известно общего правила, позволяющего переводить свойства колмогоровской сложности на язык энтропии Шеннона и наоборот. Единственным результатом такого рода является Теорема 1.

Несколько известно автору статьи, остаётся открытым и вопрос о доказательстве эффективных аналогов теорем Вольфа–Слепяна и Мучника, а также теорем о кодировании для вилочной сети. Имеющиеся доказательства данных результатов (как для шенноновской, так и для колмогоровской теории) неконструктивны и не дают способов кодирования, применимых на практике.

#### СПИСОК ЛИТЕРАТУРЫ

1. Колмогоров А.Н., Три подхода к определению понятия количество информации. *Проблемы передачи информации*, 1965, том 1, № 1, стр. 3–11.
2. Звонкин А.К., Левин Л.А., Сложность конечных объектов и обоснование понятий информации и случайности с помощью теории алгоритмов. *Успехи математических наук*, 1970, том 25, № 6, стр. 85–127.
3. Gács P., Körner J., Common information is far less than mutual information. *Problems of Control and Information Theory*, vol. 2, 1973, pp. 49–62.
4. Slepian D., Wolf J.K., Noiseless coding of correlated information sources. *IEEE Transactions on Information Theory*, vol. 19, pp. 471–480.
5. Wolf J.K., Data reduction for multiple correlated sources. In: *Proc. of the Fifth Colloquium on Microwave Communication*. Budapest, 1974, pp. 287–295.
6. Ahlswede R., Körner J., On common information and related characteristics of correlated information sources. *The 7th Prague Conf. on Inf. Th., Stat. Dec. Fct's and Rand. Proc.*, included in *Information Theory* by I.Csiszár and J.Körner, NY Acad. Press, 1981.
7. Чисар И., Кёрнер Я., *Теория информации. Теоремы кодирования для дискретных систем без памяти*. М.: Мир, 1985.

8. Muchnik An.A., On common information. *Theoretical Computer Science*, vol. 207, 1998, pp. 319–328.
9. Hammer D., Romashchenko A., Shen A., Vereshchagin N., Inequalities for Shannon entropy and Kolmogorov complexity. *Journal of Computer and System Sciences*, 2000, vol. 60, pp.442–464.
10. Muchnik An.A., Semenov A.L., Multi-conditional Descriptions and codes in Kolmogorov complexity. *Electronic Colloquium on Computational Complexity (ECCC)*, 2000, vol. 7, No. 15.
11. Makarychev K., Makarychev Yu., Romashchenko A., Vereshchagin N., A New class of non Shannon type inequalities for entropies. *Communications in Information and Systems*, vol. 2, no. 2, 2002, pp. 147–166.
12. Измайлова А.А., Передача сообщений в вилочной сети с ограниченными пропускными способностями каналов. *Дипломная работа*. Москва, МГУ им. Ломоносова. 2004.
13. Hammer D., Shen A., A strange application of Kolmogorov complexity. *Theory of computing systems*, vol. 31, no. 1, 1998, pp. 1–4.
14. Yeung R.W., *A First Course in Information Theory*. Kluwer Academic / Plenum publishers, 2002.