Kolmogorov entropy in the framework of general theory of algorithms

An. A. Muchnik S. E. Posicelsky

Авторы очень благодарны Московскому Институту Новых Технологий, который поддержал их работу в нынешнее нелегкое для российской науки время. Мы признательны руководителям (А. Семенов, А. Шень, Н. Верещагин) и участникам Колмогоровского семинара Московского Государственного Университета, с которыми авторы всегда могли обсуждать данную научную тему. B. Durand оказал важную помощь, пригласив первого автора для завершения работы в (название лаборатории). Перевод текста на английский язык любезно согласился выполнить А. Шень. Спасибо всем, кто способствовал нам в этом деле.

Предисловие

В 1960-е годы в работах А. Колмогорова и Р. Соломонова появилось важное математическое понятие — энтропия конечного объекта. Существенным приложением этого понятия является матетматическое уточнение представлений о случайности (относительно того или иного распределения вероятностей). В настоящем тексте мы не рассматриваем ни вероятностных распределений, ни других структур на конечных объектах (таких, как функция спаривания). Нас интересует чисто алгоритмическая характеризация функции энтропии. Заметим, что после первого определения этой функции было дано еще несколько близких по духу определений. Их систематизация приведена в [**?**, **?**]. Кроме специально отмеченных случаев наши рассуждения будут одинаково относиться ко всем определениям энтропии. Для полноты и независимости изложения мы рассказываем и о новых, и об известных результатах.

Функция энтропии отображает конструктивный универсум (например, множество двоичных слов) во множество натуральных чисел. Эта функция (обозначается через $K(\cdot)$) перечислима сверху, то есть перечислим ее надграфик $M = \{(x, n) \mid K(x) < n\}$. Изучая множество M, мы пришли к алгоритмическим свойствам, которые интересны сами по себе.

В части I исследуются эти свойства. Они, в частности, используются

для построения такого "естественного" класса Π перечислимых неразрешимых множеств, что $\Pi \neq \emptyset$ и $\forall \delta \in \Pi$ (δ — неполное по Тьюрингу множество). Е. Пост надеялся доказать существование "промежуточных" перечислимых множеств, именно найдя подходящий класс Π. Однако, оказалось, что классы простых, гиперпростых, гипергиперпростых и даже максимальных множеств содержат полныые по Тьюрингу множества. В работах А. Мучника и Р??. Фридберга построение промежуточных множеств пошло по другому пути (метод приоритета). *Неформальная* проблема Поста ξ — найти естественный класс Π_ξ долго оставалась открытой. Первый претендент на искомый класс был построен А. Дегтяревым и С. Марченковым (в 1973 году Дегтярев доказал непустоту класса [**?**], в 1976 году Марченков доказал, что в нем нет полных множеств [**?**]). В 1985 году М.Арсланов построил еще один класс [**?**]. И в том, и в другом примере особенно сложны доказательства непустоты класса. Построенный нами класс Π обладает еще одним свойством: он содержит представителей во *всех* степенях неразрешимости, в которых есть неразрешимые неполные перечислимые множества.

Мы будем анализировать поведение множеств относительно нескольких типов алгоритмических сводимостей. Из многих сводимостей (которые рассматривались в теории алгоритмов) мы выбрали семь. Во-первых, это m-сводимось, роль которой для вычислимости аналогична роли гомоморфизма в алгебре. Говорим, что $A \leq_m B$, если множество A является прообразом множества B относительно вычислимой всюду определенной функции. Кроме того, нас будут интересовать те шесть сводимостей, которые транзитивны и булево-замкнуты (то есть $A \leq B \wedge B \leq C \Rightarrow A \leq C$, $A \leq C \wedge B \leq C \Rightarrow A \cup B \leq C$, $A \leq B \Rightarrow \bar{A} \leq B$). А именно, мы рассматриваем сводимость по Тьюрингу (T-сводимость), слаботабличную сводимость (W-сводимость), табличную сводимость (tt-сводимость) и их ограниченные варианты (bT, bW, btt). Сводимость по Тьюрингу осуществляется алгоритмом с оракулом без каких-либо ограничений. Для слаботабличной сводимости ограничение состоит в том, что алгоритм обращается к оракулу один раз (задавая сразу несколько вопросов). Для табличной сводимости ограничение состоит в том, что алгоритм дает какой-нибудь выход даже если ответы оракула не совпадают с характеристической функцией того множества, к которому мы сводим. Ограниченные варианты сводимостей предполагают, что число вопросов к оракулу ограничено константой, не зависящей от входа алгоритма.

Утверждение 1 *Используя соображения компактности, tt-сводящий алгоритм можно эффективно переделать в алгоритм, удовлетворяющий (одновременно) ограничениям для tt и для w.*

Аналогично, btt-сводящий алгоритм можно эффективно переделать в алгоритм, удовлетворяющий (одновременно) ограничениям для btt и для bw. При этом, если исходный алгоритм задавал не более с вопросов ора-

кулу, то новый алгоритм задает не более 2^c вопросов оракулу.

В дальнейшем, говоря о tt (btt)-сводящих алгоритмах, мы будем подразумевать, что они удовлетворяют также ограничению w (bw). Очевидно, что транзитивность и булева-замкнутость для всех шести сводимостей выполнены эффективно.

Из результатов части I отметим усиление теоремы Поста о btt-неполноте простых множеств. Доказывается, что простые множества даже bT-неполны.

Для чтения части II требуется знакомство с определениями условной и безусловной энтропии (простой и префиксной). Сначала изучается условная энтропия. Это перечислимая сверху функция $K(\cdot|\cdot)$. Про соответствующее перечислимое множество $M = \{(x, y, n) \mid K(x|y) < n\}$ доказывается, что оно является m-полным. Так как все m-полные перечислимые множества вычислимо изоморфны (по теореме ??????), то характеризация условной энтропии завершена. Сложнее оказывается ситуация с безусловной энтропией. Ее надграфик не является bT-полным. С другой стороны, надграфик энтропии является w-полным. Остается вопрос о tt-полноте. М.Куммер доказал, что надграфик простой энтропии является tt-полным. Здесь мы должны вспомнить, что для каждого типа энтропии по настоящему определяется не одна функция энтропии, но счетное семейство функций. Разность любых двух функций из этого семейства ограничена. В предыдущем изложении все результаты относились в равной степени ко всем представителям семейства функций энтропии. Неожиданно получается, что существует функция префиксной энтропии, надграфик которой является tt-полным; и существует функция префиксной энтропии, надграфик которой не является tt-полным.

В части II доказывается интересное следствие[1]:

$$\forall d \exists x, y \ (KS(x) + d < KS(y) \wedge KP(y) + d < KP(x)).$$

Таким образом, "с точностью до логарифма" простая и префиксная энтропии ведут себя одинаково, а "с большей точностью" уже по-разному.

Часть I

В 1956 году А. Мучник ввел следующее понятие [**?**].

Определение I.1 *Перечислимое множество A называется r-отделимым, если для любого перечислимого множества B, не пересекающегося с A, существует разрешимое множество C, которое отделяет A от B (то есть $A \subset C$ и $B \cap C = \emptyset$).*

KS обозначает простую энтропию, а KP обозначает префиксную энтропию. Как известно, $KS(z) - O(1) < KP(z) < KS(z) + O(\log(KS(z)))$.

К классу r-отделимых множеств, очевидно, относятся разрешимые множества и простые множества. М. Куммер и Ф. Стефан доказали, что перечислимые частотно разрешимые множества являются r-отделимыми [**?**]. Надграфик функции энтропии тоже является r-отделимым. Интересно, что весьма богатый класс частотно разрешимых множеств не содержит, однако, надграфика энтропии (теорема М. Куммера [**?**]). С другой стороны, m-полные перечислимые множества не являются r-отделимыми (это следует из того, что m-полные перечислимые множества вычислимо изоморфные универсальному перечислимому множеству, и из существования алгоритмически неотделимой пары перечислимых множеств).

В общей теории алгоритмов многие определения могут эффективизироваться, причем, по-разному.

Определение I.2 *r-отделимое множество A называется эффективно r-отделимым, если существует следующий алгоритм γ. Для всякого перечислимого множества B, не пересекающегося с A, алгоритм γ определен на тексте каждой программы β, перечисляющей множество Bю При этом $\gamma(\beta)$ является текстом программы разрешения множества C, отделяющего A от B. (Программа, разрешающая множество, выдает 1 на элементах этого множества и выдает 0 на остальных элементах).*

Понятно, что разрешимые множества эффективно r-отделимы.

Теорема I.1 *Эффективно r-отделимые множества разрешимы.*

Доказательство. Здесь и в последующем нам придется строить перечислимые множества, используя в построении текст программы перечисления множества, которое мы строим. Для устранения порочного круга следует строить множество по тексту программы перечисления другого множества. А затем достигнуть совпадения этих двух множеств с помощью теоремы С. Клини о неподвижной точке. То же соображение относится к построению вычислимых функций (частично определенных).

Пусть A — эффективно r-отделимое множество и $/gamma$ — алгоритм, обеспечивающий эту эффективность. Для каждого построим множество B_n, перечисляемое программой β_n. Если γ определено на β_n, будем применять программу $\gamma(\beta_n)$ к числу n. Если выход программы $\gamma(\beta_n)$ на входе n будет, то $\beta_n = \{n\}$. Если выход программы $\gamma(\beta_n)$ на входе n не определен или не равен 1, то $\beta_n = \emptyset$.

Утверждается, что $n \notin A \leftrightarrow [\gamma(\beta_n)](n) = 0$, и поэтому дополнение до A перечислимо.

Докажем " $\rightarrow$". Если $n \notin A$, то B_n во всех случаях не пересекается с A. Поэтому алгоритм γ определен на входе β_n, и программа $\gamma(\beta_n)$ определена на всех входах. Если $[\gamma(\beta_n)](n) = 1$, то $B_n = \{n\}$. Это противоречит тому, что $\gamma(\beta_n) = 0$.

Докажем " $\leftarrow$". Если $[\gamma(\beta_n)](n) = 0$, то $B_n = \emptyset$. Из определения алгоритма γ следует, что $A \subset \{x \mid [\gamma(\beta_n)](x)\}$. Получается $n \notin A$. $\square$

Более продуктивной оказалась следующая ослабленная эффективизация r-отделимости.

Определение I.3 *r-отделимое множество A называется упругим (resilient), если существует следующий алгоритм γ. Для всякого веречислимого множества B, не пересекающегося с A, алгоритм γ определен на тексте каждой программы β, перечисляющей множество B. При этом $\gamma(\beta)$ является текстом программы перечисления разрешимого множества C, отделяющего A от B.*

Упругость отличается от эффективной r-отделимости только одним: хотя отделяющее множество C остается разрешимым, по перечислению для B находится только перечисление (а не разрешение) для C.

К классу упругих множеств, очевидно, относятся разрешимые множества и сильно эффективные простые множества[2]. В следующей части статьи будет доказано, что надграфик функции энтропии является упругим.

Достоинством классов r-отделимых и упругих множеств можно назвать то, что они образуют решетки (так же, как классы разрешимых, перечислимых, частично разрешимых множеств).

Теорема I.2 *Класс r-отделимых множеств замкнут относительно объединения и пересечения.*

Класс упругих множеств эффективно замкнут относительно объединения и пересечения.

Эффективность второго утверждения означает, что по алгоритмам, обеспечивающим упругость множеств A_1 и A_2, эффективно строятся алгоритмы, обеспечивающие упругость $A_1 \cup A_2$ и $A_1 \cap A_2$.

Доказательство. Фактически, одно и то же рассуждение годится для обоих утверждений теоремы. Пусть A_1 и A_2 — r-отделимые (или, соответственно, упругие множества).

Докажем r-отделимость (упругость) $A_1 \cup A_2$. Пусть B — перечислимое множество, не пересекающееся с $A_1 \cup A_2$. Тогда B отделимо от A_1 и B отделимо от A_2. Найдем разрешимые множества C_1 и C_2 (заданные своими перечислениями), для которых $A_1 \subset C_1$, $A_2 \subset C_2$, $B \cap C_1 = \emptyset$, $B \cap C_2 = \emptyset$. Множества $A_1 \cup A_2$ и B отделимы с помощью разрешимого множества $C_1 \cup C_2$ (перечисление которого нам известно).

Докажем r-отделимостть (упругость) $A_1 \cap A_2$. Пусть B — перечислимое множество, не пересекающееся с $A_1 \cap A_2$. Так как $A_1 \cap (A_2 \cap B) = \emptyset$,

---

Перечислимое множество A называется сильно эффективно простым, если по каждой программе, перечисляющей какое-нибудь множество B, не пересекающееся с A,??

то A_1отделимо от перечислимого множества $A_2 \cap B$. Найдем разрешимое множество C (заданное своим перечислением), для которого $A_1 \subset C$ и $(A_2 \cap (B \cap C)) = \emptyset$. Так как $A_2 \cap (B \cap C) = \emptyset$, то A_2 отделимо от перечислимого множества $B \cap C$ (перечисление которого нам известно). Найдем разрешимое множество D (заданное своим перечислением), для которого $A_2 \subset D$ и $(B \cap C) \cap D = \emptyset$. То есть разрешимое множество $C \cap D$ отделяет $A_1 \cap A_2$ от B (при этом перечисление $C \cap D$ нам известно). □

Очевидно, что класс r-отделимых (упругих) множеств замкнут (эффективно) относительно цилиндрификации. Это дает замкнутость (эффективную) относительно разных операций. Например, прямое произведение можно рассмотреть как пересечение двух циллиндров.

Сейчас мы обращаемся к вопросам полноты относительно разных сводимостей. Нам потребуется следующий результат, принадлежащий А. Лахлану [**?**]. Если множество $A \cap B$ является m-полным и множество A перечислимо, то одно из множеств A или B является m-полным. Мы сформулируем и докажем некоторую эффективизацию приведенного утверждения.

Теорема I.3 (А. Лахлан) *Пусть множество U является m-полным. Существует алгоритм, который по программе перечисления множества A строит программу вычисления функции f так, что выполнено следующее: $f(U) \subset U$, $f(\bar{U}) \subset A \setminus U$ и если множество $U \cup A$ не является m-полным, то функция f всюду определена.*

Доказательство. Используя теорему о неподвижной точке, построим вспомогательную функцию $\lambda xyz \cdot g_{x,y}(z)$. По ее программе и двум элементам x, y найдем программу функции $h = \lambda z \cdot g_{x,y}(z)$. Как известно, по программе h можно эффективно найти такое v, что если $h(v)$ определено, то $v \in U \Leftrightarrow h(v) \in U$[3]. Перечисляя множества U и A, ждем пока y попает в U или v попадет в $U \cup A$. Если не случится ни того ни другого, то $\forall z\ g_{x,y}(z)$ не определено. Если первым обнаружилось $y \in U$, то $\forall z\ g_{x,y}(z) = y$. Если первым обнаружилось $v \in U \cup A$, то $\forall z\ g_{x,y}(z) = x$.

Построим функцию $\lambda x \cdot f(x)$. Получив на вход x, перебираем все значения y и ищем такое, чтобы для соответсвующего v было $g_{x,y}(v) = x$. Определяем $f(x) = v$. Докажем корректность построения. Если для некоторого x_0 значение $f(x_0)$ не определено, то множество $U \cup A$ оказывается m-полным.

Построим функцию $\lambda y \cdot p(y)$, m-сводящую множество U ко множеству $U \cup A$. Определяем $p(y)$ равным тому v, которое соответствует паре x_0, y. Если $y \in U$, то $\forall x, z\ g_{x,y}(z)$ определено. Следовательно $g_{x\ ,y}(v) = y$. Это влечет, что $v \in U \Leftrightarrow y \in U$. То есть $p(y) \in U$. Если $y \notin U$, то $v \notin U \cup A$; иначе было бы $g_{x\ ,y}(v) = x_0$ и $f(x_0) = v$. Итак, $y \in U \Leftrightarrow p(y) \in U \cup A$.

Для универсального множества U этот факт сразу следует из теоремы о неподвижной точке.

Теперь предположим, что функция f определена на x. Это значит, что $\exists y\ g_{x,y}(f(x)) = x$. Следовательно, $f(x) \in U \cup A$ и $f(x) \in U \Leftrightarrow x \in U$. Это дает искомое свойство функции f.

Проиллюстрируем доказательство тремя рисунками. □

Теорема I.4 *Никакое r-отделимое множество не является bT-полным.*

Доказательство. Пусть B — r-отделимое множество, а U — m-полное множество. Приведем к противоречию то, что $U \underset{bT}{\leq} B$. Пусть γ — алгоритм, bT-сводящий U к B с наименьшей возможной границей на число вопросов к оракулу. Если эта граница равна нулю, то множество U было бы разрешимым. Если граница равна $n+1$, мы построим новый алгоритм, который будет сводить U к B, задавая на каждом входе не более n вопросов к оракулу.

Пусть новому алгоритму дан вход x. Для каждой программы δ, перечисляющей множество D_δ, рассмотрим множество A_δ всех y, на которых алгоритм γ или не задает вопросов оракулу, или первый заданный вопрос принадлежит D_δ. Понятно, что A_δ перечислимо равномерно по δ и x.

Пусть f_δ — функция, построенная в теореме I.3 по множествам U и A_δ. Обозначим через $q(y)$ первый вопрос алгоритма γ к оракулу на входе y. Рассмотрим множество C всех элементов вида $q(f_\delta(x))$, где x фиксировано, а δ — меняется (обратим внимание, что q и f_δ — частично определенные функции). Понятно, что C перечислимо равномерно по x. Предположим, что $B \cap C = \emptyset$; тогда для некоторого ε множество D_ε является разрешимым и $B \subset D_\varepsilon$, $C \cap D_\varepsilon = \emptyset$ (за счет r-отделимости B). Множество $U \cup A_\varepsilon$ может быть bT-сведено ко множеству B, задавая не более n вопросов к оракулу на каждом входе. Действительно, если алгоритм γ не задает вопросов оракулу на входе y, то $y \in A_\varepsilon$. Если $q(y) \notin D_\varepsilon$, то $y \notin A_\varepsilon$; а принадлежность y множеству и узнается алгоритмом γ буз задавания первого ворпроса (ответ на этот вопрос известен: $q(y) \notin D_\varepsilon \ \rightarrow q(y) \notin B$). Принадлежит ли $q(y)$ множеству D_ε определяется благодаря разрешимости D_ε.

Если множество $U \cup A_\varepsilon$ не является m-полным, то по теореме I.3 $f_\varepsilon(x)$ определено и $f_\varepsilon(x) \in U \cup A_\varepsilon$, $x \in U \Leftrightarrow f_\varepsilon(x) \in U$. Если $q(f_\varepsilon(x))$ определено, то $q(f_\varepsilon(x)) \in C$, откуда $q(f_\varepsilon(x)) \notin D_\varepsilon$, откуда $f_\varepsilon(x) \notin U$, откуда $x \in U$.

Мы получаем, что выполнено одно из трех: $(B \cap C \neq 0)$ или ($f_\varepsilon(x)$ не определено, но $q(f_\varepsilon(x))$ не определено) или $(x \in U)$.

Вернемся к построению нового алгоритма. На входе x он параллельно ждет, не найдется ли такого δ, что $q(f_\delta(x) \in B$; не найдется ли такого ε, что $f_\varepsilon(x)$ определено, а $q(f_\varepsilon(x))$ не определено; не попадет ли x в перечисление U. В первом случае новый алгоритм моделирует работу γ на выходе $f_\delta(x)$, не задавая первого вопроса оракулу, поскольку ответ на него известен. Во втором случае новый алгоритм моделирует работу γ на входе $f_\varepsilon(x)$, при

этом вопросы оракулу не задаются. В третьем случае мы просто знаем, что $x \in U$. Напомним, что когда $f(x)$ определено, то $x \in U \Leftrightarrow f(x) \in U$. $\square$

Теорема I.5 *Каждое упругое множество или разрешимо, или T-полно.*

Доказательство этой теоремы будет следовать из теоремы I.6. Напомним два известных определения.

Определение I.4 (Е. Пост) *Перечислимое множество A называется творческим, если существует алгоритм γ со следующим свойством. Для всякого перечислимого множества B, не пересекающегося с A, алгоритм γ определен на тексте каждой программы β, перечисляющей множество B. При этом элемент $\gamma(\beta)$ не принадлежит ни A, ни B.*

По теореме Дж. Майхилла все творческие множества m-полны.

Определение I.5 (Дж. Деккер) *Перечислимое множество A называется полутворческим, если существует алгоритм γ со следующим свойством. Для всякого перечислимого множества B, не пересекающегося с A, алгоритм γ определен на тексте каждой программы β, перечисляющей множество B. При этом $\gamma(\beta)$ является текстом программы перечисления такого множества C, что $B \underset{\neq}{\subset} C$, $A \cap C = \emptyset$.*

Как доказал в 1957 году Дж. Шенфилд [**?**], класс полутворческих множеств строго шире класса творческих множеств. Класс слабо творческих множеств, определяемый ниже, расширяет класс творческих множеств в симметричном направлении. Проиллюстрируем это следующими рисунками.

Определение I.6 *Перечислимое множество A называется слабо творческим, если существует алгоритм γ со следующим свойством. Для всякого перечислимого множества B, не пересекающегося с A, алгоритм γ определен на тексте каждой программы β, перечисляющей множество B. При этом $\gamma(\beta)$ является текстом программы перечисления такого множества C, что $A \underset{\neq}{\subset} C$, $B \cap C = \emptyset$.*

Упругие неразрешимые множества, очевидно, являются слабо творческими.

Теорема I.6 *Слабо творческие множества являются T-полными.*

Доказательство. Пусть A — слабо творческое множество; γ — алгоритм, обеспечивающий то, что A — слабо творческое. Пусть U — перечислимое множество. Мы хотим узнать по x, верно ли $x \in U$.

С помощью теоремы о неподвижной точке построим вспомогательное перечислимое множество B_x. Перечисляем U. Если $x \notin U$, то $B_x = \emptyset$. Если x попало в перечисление U на шаге s, то делаем первые s шагов в перечисление A. (Часть множества E, перечисленная за s шагов, будет обозначаться E^s.) Пусть β — программа перечисления множества B_x. Пусть программа $\gamma(\beta)$ перечисляет множество C (если $\gamma(\beta)$ не определено, считаем C пустым). Во множество B_x кладется первый элемент, который попадет в перечисление C и не принадлежит A^s (если такого элемента не найдется, то $B_x = \emptyset$). Построение B_x закончено.

Алгоритм, T-сводящий U к A, работает так. Перечисляем U и параллельно выполняем следующую процедуру.

Перечисляем C. Используя оракул для A, ищем первое y, которое попадет в перечисление C и не принадлежит A. Определяем t, для которого все элементы, попавшие в перечисление C раньше y, принадлежат A^t. Если x не принадлежит U^t, отвечаем, что $x \notin U$. Описание процедуры, параллельной перечислению U, закончено.

Нам требуется доказать, что $x \notin U \Leftrightarrow$ параллельная процедура дает ответ.

Если $x \notin U$, то $B_x = \emptyset$. Тогда по определению γ имеем $A \underset{\neq}{\subset} C$. Следовательно, параллельная процедура найдет y и $x \notin U^t$.

Предположим, что параллельная процедура дала ответ, но $x \in U$. Пусть $x \in U^s$. Пусть y — элемент найденный параллельной процедурой. Тогда в B_x помещен некоторый элемент z. Причем z попало в перечисление C не позже, чем y. Рассмотрим два случая: $z = y$ и $z \neq y$.

Если $z = y$, то $B_x \cap A = \emptyset$. Следовательно, должно быть $B_x \cap C = \emptyset$, а это не так. Предположим $z \neq y$. Так как $z \notin A^s$, то $s < t$ (по построению B_x и параллельной процедуры). Так как $x \notin U^t$, то $t < s$. Противоречие. □

Упомянутые в предисловии классы T-неполных множеств, построенные Дегтяревым–Марченковым и Арслановым, являются подклассами класса полуразрешимых множеств.

Определение I.7 (С. Джонуш [?]) *Множество называется полуразрешимым, если оно вычислимо изоморфно начальному сегменту некоторого разрешимого линейного порядка.*

Утверждение 2 *Перечислимые полуразрешимые множества являются r-отделимыми.*

Доказательство. Пусть A — перечислимое полуразрешимое множество, а B — перечислимое множество, не пересекающееся с A. Будем говорить “левее-правее” про разрешимый линейный порядок, относительно которого множество A замкнуто влево. Обозначим через B' замыкание множества

B вправо. Ясно, что B' — перечислимое множество, не пересекающееся с A. Если дополнение до $A \cup B'$ пусто, то само A разрешимо. Если $x \notin A \cup B'$, то отделяющим разрешимым множеством является $\{y \mid y \text{ левее } x\}$. $\square$

Теорема I.7 *Перечислимое полуразрешимое множество является T-полным тогда и только тогда, когда оно упруго и неразрешимо.*

Доказательство. Из теоремы I.5 следует импликация "тогда" настоящей теоремы. Докажем "только тогда".

Пусть дан разрешимый линейныый порядок (про который мы будем говорить "левее-правее"). Пусть A — перечислимое множество, замкнутое влево. Пусть U — творческое множество. Пусть γ — алгоритм, T-сводящий U к A. Построим алгоритм, обеспечивающий упругость A.

Пусть дано перечисление множества B, не пересекающегося с A. Замыкание B вправо тоже не пересекается с A. Перечисление этого замыкания эффективно получается по перечислению B. Поэтому можно считать, что B замкнуто вправо. Мы хотим перечислить разрешимое множество C, которое расширяет A и не пересекается с B.

Рассмотрим множество D тех элементов, не принадлежащих U, на которых все вопросы γ к оракулу принадлежат $A \cup B$. Ясно, что можно получить перечисление D. Используя то, что U творческое, находим x, не принадлежащее $U \cup D$.

Теперь перечисляем A и параллельно моделируем (не используя оракула) работу γ на входе x. При этом предполагаем, что оракул дает положительный ответ на вопрос, если в перечисление A уже попал какой-нибудь элемент, лежащий правее этого вопроса; и отрицательный ответ в противном случае. Во время моделирования мы встретим набор ответов оракула, на которых γ дает выход. ТАким набором является набор правильных ответов (но первый встреченный набор может оказаться неправильным). Найдя такой набор ответов, берем самый левый вопрос этого набора, ответ на который отрицателен. Все, что левее этого вопроса относим ко множеству C. После конечного количества неправильных гипотез об ответах оракула мы доберемся до правильной гипотезы. Таким образом, C является конечным объединением разрешимых множеств и поэтому разрешимо. (Но мы не знаем, сколько в этом объединении членов, и поэтому не имеем программы для разрешения C.

Если гипотеза о наборе ответов оракула окажется направильной, то один из отрицательных ответов станет положительным. Тогда и самый левыый отрицательныый ответ этого набора станет положительным. Отсюда следует, что для неправильных гипотез элементы, отнесенные к C, принадлежит A.

Для правильной гипотезы самый левый вопрос, ответ на который отрицателен, не принадлежит A (иначе гипотеза не была бы правильной) и не принадлежит B (иначе x принадлежало бы D).

Итак $A \underset{\neq}{\subset} C$ и $B \cap C = \emptyset$. □

Осталось отметить,что, как известно, полуразрешимые перечислимые множества есть во всех перечислимых степенях неразрешимости.

Часть II

Теорема II.1 *Надграфик любой функции условной энтропии является m-полным множеством.*

Доказательство. Мы воспользуемся идеей из доказательства теоремы Куммера о безусловной простой энтропии.

Пусть U — перечислимое множество. Мы хотим построить алгоритм, m-сводящий ко множеству $M = \{(x, y, n) \mid K(x|y) < n\}$, где $K(x|y)$ — энтропия x при условии y. Нам понадобится вспомогательная конструкция. Натуральное число d будет свободным параметром этой конструкции.

Всякому условию y сопоставим *шкалу*. Каждая шкала имеет *планку* и 2^d *делений*, занумерованных числами $\{1, 2, ..., 2^d\}$. Во время выполнения конструкции номер деления, на котором стоит планка, не убывает. Некоторые деления *помечаются* парой натуральных чисел, у которой первая компонента совпадает с номером деления. Каждое деление помечается не более одного раза, и каждая пара помечает не более одного деления. Некоторые планки *привязывают* к делению, на котором стоят и после этого не меняют своего положения.

Фиксируем некоторый способ перечисления множеств U и M. U^t и M^t обозначают подмножества, перечисленные за t шагов. Конструкция состоит из последовательных конечных этапов. На 1-ом этапе все планки стоят на нижних делениях (с номером 1), и ни одно деление не помечено. Опишем t-ый этап.

Для всякого $v \in U^t$ все планки, стоящие на делениях, помеченных парами вида (w, v), привязываются к этим делениям. По очереди обработаем первые t шкал, планки которых не привязаны. Рассмотрим шкалу, сопоставленную условию y. Ее планка ставится на наименьшее деление x, для которого $(x, y, d) \notin M^t$. Такое x существует, поскольку $\forall y, n \ |\{x \mid (x, y, n) \in M\}| < 2^n$. Если планка сдвинулась по сравнению с предыдущим этапом, возьмем наименьшее z, для которого пара (x, z) еще не была использована в качестве метки. Пометим x-е деление y-ой шкалы парой (x, z).

Конец вспомогательной конструкции.

Предположим, что параметр d достаточно велик. Тогда покажем, что

$$\text{если планка } y\text{-ой шкалы привязана к делению } x, \text{ то } (x, y, d) \in M. \qquad (\alpha)$$

Действительно, зная y и d, запустим конструкцию с параметром d и дождемся, пока планка y-ой шкалы будет привязана. Число x — это номер

деления, к которому привязана планка. Получается $K(x|\langle y,d\rangle) < C$, где C — константа. Следовательно, $K(x|y) < C_1 \cdot \log d < d$ (C_1 — константа, d — достаточно велико).

Теперь фиксируем достаточно большое значение d. Пусть b — максимальный номер деления, которого во время выполнения вспомогательной конструкции достигают бесконечно много планок. Алгоритм, m-сводящий U к M, действует так.

По входу z найдем то y_z, для которого b-е деление y_z-ой шкалы помечено парой (b,z). Такое y_z есть по выбору b. Утверждается, что $z \in U \Leftrightarrow (b,y_z,d) \in M$, для всех z кроме конечного множества тех, для которых планка y_z-ой шкалы поднимается выше b. Доказательство непосредственно следует из описания вспомогательной конструкции, из (α) и из выбора (b). □

Заметим, что уже одномерное сечение $\{y \mid (b,y,d) \in M\}$ трехмерного множества M является m-полным.

Теорема II.2 *Надграфик любой функции энтропии является упругим множеством.*

Доказательство. Пусть $M = \{(x,n) \mid K(x) < n\}$ и B — перечислимое множество, не пересекающееся с M. Утверждается, что вторая компонента пар из B ограничена; причем эту границу можно эффективно найти по программе, перечисляюще B. Для данного n рассмотрим первую пару вида (x,n), попавшую в перечисление B. Если такая пара есть, то $K(x) < C \cdot \log n$, где множитель C зависит только от программы перечисления B. При больших n имеем $C \cdot \log n < n$ и, следовательно, $K(x) < n$. Последнее эквивалентно $(x,n) \in M$, что противоречит $M \cap B = \emptyset$.

Пусть d — граница, найденная в предыдущем абзаце. Тогда нам известно перечисление множества $D = M \cup \{(x,n) \mid n > d\}$. Мы знаем, что $M \subset D$ и $B \cap D = \emptyset$. Остается доказать, что D разрешимо. Действительно,

$$D = (M \cap \{(x,n) \mid n \le d\}) \cup (\{(x,n) \mid n > d\}.$$

Второй член объединения очевидно разрешим. Первый член объединения конечен для простой и префиксной энтропии. Для случаев энтропии разрешения, априорной энтропии и монотонной энтропии достаточно показать, что для любого n множество $E = \{x \mid K(x) < n\}$ разрешимо. Указанные три энтропии определяются на двоичных словах. Из их определений сразу следует, что множество E содержит вместе с каждым словом все его начала. Кроме того, всякое подмножество множества E, слова которого не продолжают друг друга имеет не более 2^n элементов. Поэтому есть не более 2^n бесконечных последовательностей, все начала которых принадлежат E. Обозначим эти последовательности $y_1,\ldots,y_i,\ldots$, а множество их начал обозначим F. Для каждого слова $z \in E \setminus F$ определим начало, называемое

стволом z. Это кратчайшее начало z, не принадлежащее F. Ясно, что все стволы принадлежат E и не продолжают друг друга. Поэтому количество стволов не превышает 2^n. Слова, имеющие один и тот же ствол, образуют запертое дерево. Ввиду компактности, это дерево конечно. Итак, множество $E \setminus F$ конечно. Каждое y_i вычислимо, так как E перечислимо и для каждого достаточно длинного w, являющегося началом y_i, ровно одна из двух последовательностей $W0$, $W1$ принадлежит E. □

Теорема II.3 *Надграфик любой функции энтропии не является bT-полным.*

Доказательство. Следствие теорем I.4 и II.2. □

Теорема II.4 (автор) *Надграфик любой функции энтропии является w-полным.*

Доказательство. Мы хотим построить алгоритм, w-сводящий перечислимое множество U ко множеству $M = \{(x, n) \mid K(x) < n\}$. Фиксируем для U и для M некоторый способ перечисления. Пусть алгоритм должен узнать, верно ли $y \in U$. Пусть d — длина двоичной записи y.

С помощью оракула найдем значение функции K на всех двоичных словах длины d^2. Поскольку эти значения заведомо не больше $\text{const} \cdot d^2$, все вопросы оракулу можно задать одновременно. Для тех слов z длины d^2, для которых $K(z) < d^2$, найдем число шагов $t(z)$, за которое пара (z, d^2) попадет в перечисление M. При этом мы предполагаем, что оракул дал правильные ответы; иначе наш алгоритм может работать бесконечно долго! Обозначим через s максимальное значение $t(z)$ (по словам z длины d^2, на которых t определено). Утверждается, что $y \in U \Leftrightarrow y$ попадает в U за первые s шагов перечисления; если d достаточно велико. Предположим, что это не так. Тогда $y \in U$. Обозначим число шагов, за которое y попадает в U, через r. Рассмотрим множество V тех слов z длины d^2, для которых пара (z, d^2) попадает в перечисление M за первые r шагов перечисления. Поскольку $|V| < 2^d$, есть слово длины d^2, не принадлежащее V. Если w — первое такое слово, то для нахождения w достаточно иметь y. □