

УДК 519.174

О ПРАВИЛЕ СЛОЖЕНИЯ ЭНТРОПИЙ ДЛЯ НЕДООПРЕДЕЛЁННЫХ ДАННЫХ *)

Л. А. Шоломов

Аннотация. Введены основные информационные характеристики недоопределённых данных и установлено, что для недоопределённых данных общего вида правило сложения энтропий $H(X) + H(Y|X) = H(XY)$ классической теории информации заменяется более сложным соотношением. Найден вид этого соотношения и получены необходимые и достаточные условия, при которых оно совпадает с обычным правилом сложения энтропий.

Ключевые слова: недоопределённые данные, информационные характеристики, энтропия, условная энтропия, доопределение, лучшее доопределение, правило сложения энтропий.

Введение

Под *недоопределёнными данными* понимаются последовательности недоопределённых (в другой терминологии — недетерминированных [9], нечётких [6]) символов. Каждому такому символу соответствует некоторое множество основных (полностью определённых) символов, одним из которых он может быть заменён (доопределён). С недоопределёнными данными имеют дело во многих разделах информатики.

Систематическое изучение информационных свойств недоопределённых данных начато в [4] в связи с задачей синтеза схем для систем недоопределённых булевых функций. В [5] рассмотрена задача сжатия недоопределённых данных, в постановке которой требуется, чтобы по коду недоопределённой последовательности можно было восстановить какое-либо её доопределение (но не саму последовательность). Для случая, когда последовательности порождаются вероятностным источником X , вырабатывающим недоопределённые символы независимо, доказана теорема кодирования, обобщающая соответствующий результат для полностью определённых источников. Роль энтропии в этой теореме играет

*) Исследование выполнено при финансовой поддержке Отделения нанотехнологий и информационных технологий РАН по программе «Информационные технологии и методы анализа сложных систем» (проект 1–1 «Теория и методы эффективного использования недоопределённых данных»).

функция $\mathcal{H}(X)$, введённая в [1, с. 92] из эвристических соображений в качестве меры неопределённости задач с несколькими ответами. Она задаётся неявно как минимум некоторого выражения. В [5] исследованы свойства этой энтропии и установлено, что они являются модификациями соответствующих свойств энтропии Шеннона.

Кодирование недоопределённых источников тесно связано с комбинаторной задачей построения доопределяющих множеств для классов последовательностей с заданным частотным составом недоопределённых символов. Эта задача может быть сформулирована также в терминах построения протыкающих множеств для систем комбинаторных кубоидов [9, 11]. Дополнительный интерес к задачам протыкания возник в связи с их ролью в проблеме дерандомизации алгоритмов [10] (подробнее в обзоре [7]).

Настоящая статья посвящена условной энтропии $\mathcal{H}(Y|X)$ недоопределённых данных. Введя её, можно обычным образом задать для недоопределённых данных меру информации $\mathcal{I}(X; Y) = \mathcal{H}(Y) - \mathcal{H}(Y|X)$ в X относительно Y . Существенную роль в классической теории информации играет правило сложения энтропий $H(X) + H(Y|X) = H(XY)$. Некоторый вариант этого правила включён Шенноном в число свойств, аксиоматически задающих энтропию, и во многом определил вид энтропийной функции. При введении условной энтропии $\mathcal{H}(Y|X)$ для недоопределённых данных этому свойству будет уделено особое внимание.

Из результатов [6] следует, что если источник X полностью определён, то условная энтропия $\mathcal{H}(Y|X)$, введённая по обычной схеме, удовлетворяет правилу сложения энтропий и согласована с колмогоровской интерпретацией [3] условной энтропии в терминах относительной сложности. Случай всюду определённого X будем считать базовым, и для недоопределённого источника X общего вида в качестве $\mathcal{H}(Y|X)$ будет принято значение $\mathcal{H}(Y|\hat{X})$ при некотором специальном выборе для X доопределения \hat{X} .

Вначале изучаем правило сложения энтропий при произвольно заданном доопределении \dot{X} . Наряду с $\mathcal{H}(Y|\dot{X})$ вводятся величины $\mathcal{H}_{\dot{X}}(X)$ и $\mathcal{H}_{\dot{X}}(XY)$, характеризующие энтропию источника X и произведения XY при доопределении \dot{X} источника X . Показано, что правило сложения энтропий при заданном доопределении приобретает вид

$$\mathcal{H}_{\dot{X}}(X) + \mathcal{H}(Y|\dot{X}) = \mathcal{H}_{\dot{X}}(XY).$$

Все величины, входящие в это равенство, заданы неявно как минимумы достаточно сложных выражений, и это создает определённые трудности при его доказательстве.

Далее рассмотрен вопрос о выборе доопределения \hat{X} , используемого для вычисления условной энтропии $\mathcal{H}(Y|X)$. Доопределение \hat{X} , на котором достигается энтропия, т.е. такое, что $\mathcal{H}_{\hat{X}}(X) = \mathcal{H}(X)$, названо *лучшим*. В работе показано, что если допустить вычисление $\mathcal{H}(X)$ и $\mathcal{H}(Y|X)$ на основе разных доопределений, появится возможность занижения суммы $\mathcal{H}(X) + \mathcal{H}(Y|X)$ за счёт манипулирования доопределениями. В связи с этим предлагается взять $\mathcal{H}(Y|X) = \mathcal{H}(Y|\hat{X})$, где \hat{X} — лучшее доопределение. Возникающее при этом правило сложения энтропий названо *обобщённым*. В заключение найдены необходимые и достаточные условия, при которых обобщённое правило сложения энтропий совпадает с обычным.

Краткое изложение некоторых результатов статьи имеется в [8].

1. Энтропия недоопределённых данных

Задан алфавит $A_0 = \{a_0, a_1, \dots, a_{m-1}\}$ *основных символов*. Пусть $M = \{0, 1, \dots, m-1\}$ и каждому непустому $T \subseteq M$ сопоставлен символ a_T . Положим $A = \{a_T, T \subseteq M\}$. Будем называть символы a_T *недоопределёнными* и *доопределением* символа a_T считать всякий основной символ a_i , $i \in T$. Символ a_M , доопределимый любым основным символом, назовём *неопределённым* и обозначим через $*$.

Будем рассматривать *недоопределённые источники* X , порождающие символы $a_T \in A$ независимо с вероятностями $p(a_T) \geq 0$. Пусть $P = (p(a_T), T \subseteq M)$. Если $p(a_T) = 0$ для всех $a_T \notin A_0$, то источник будем называть *полностью определённым*. Задав набор $Q = (q_i, i \in M)$, $q_i \geq 0$, $\sum_i q_i = 1$, введём функцию*

$$\mathcal{H}(P, Q) = - \sum_T p(a_T) \log \sum_{i \in T} q_i. \quad (1)$$

Энтропией источника X назовём величину

$$\mathcal{H}(X) = \mathcal{H}(P) = \min_Q \mathcal{H}(P, Q). \quad (2)$$

Она играет для недоопределённых источников роль энтропии Шеннона и в случае полностью определённых источников совпадает с ней [5].

Если набор Q минимизирует правую часть (1), будем говорить, что на нём достигается энтропия. Имеет место следующий факт [5].

*Всюду логарифмы предполагаются двоичными.

Утверждение 1. Энтропия $\mathcal{H}(P)$ достигается на наборе \hat{Q} тогда и только тогда, когда при каждом $i \in M$ выполнено

$$\sum_{T: i \in T} \frac{p(a_T)}{\sum_{j \in T} \hat{q}_j} \leq 1, \quad (3)$$

где строгое неравенство может иметь место лишь при тех i , для которых $\hat{q}_i = 0$.

Поскольку нарушение равенства возможно лишь в случае $\hat{q}_i = 0$, домножив обе части на \hat{q}_i , получим равенство

$$\sum_{T: i \in T} \frac{p(a_T) \hat{q}_i}{\sum_{j \in T} \hat{q}_j} = \hat{q}_i. \quad (4)$$

Численный алгоритм нахождения набора \hat{Q} , основанный на этом соотношении, описан в добавлении к [5].

Следующий факт уточняет заключительную часть утверждения 1.

Утверждение 2. Если \hat{Q} — набор, на котором достигается энтропия, и при некотором i неравенство (3) для него является строгим, то при этом i во всех Q , на которых достигается энтропия, $q_i = 0$.

ДОКАЗАТЕЛЬСТВО. Положим* $\hat{\alpha}_T = \sum_{i \in T} \hat{q}_i$. Пусть Q' — произвольный набор, на котором достигается энтропия, и $\alpha'_T = \sum_{i \in T} q'_i$. Покажем, что $\alpha'_T = \hat{\alpha}_T$ при всех T . Допустим, что $\alpha'_{T_0} \neq \hat{\alpha}_{T_0}$. Для произвольного μ , $0 < \mu < 1$, в силу выпуклости вверх логарифма (и положительности $p(a_T)$) справедливо неравенство

$$-p(a_T) \log(\mu \hat{\alpha}_T + (1 - \mu) \alpha'_T) \leq -\mu p(a_T) \log \hat{\alpha}_T - (1 - \mu) p(a_T) \log \alpha'_T,$$

которое при $T = T_0$ является строгим. Просуммировав по T с учётом $\mathcal{H}(P, \hat{Q}) = \mathcal{H}(P, Q') = \mathcal{H}(P)$, получаем

$$\mathcal{H}(P, \mu \hat{Q} + (1 - \mu) Q') < \mu \mathcal{H}(P, \hat{Q}) + (1 - \mu) \mathcal{H}(P, Q') = \mathcal{H}(P),$$

что противоречит определению $\mathcal{H}(P)$.

Из доказанного следует, что при каждом i левая часть (3) для всех наборов Q' , на которых достигается энтропия, принимает одинаковое значение $\sum_{T: i \in T} p(a_T) / \hat{\alpha}_T$, и если для некоторого i она меньше 1, то при

*Здесь и дальше рассматриваются только такие T , для которых $p(a_T) > 0$.

этом i она меньше 1 для всех Q' и по утверждению 1 для них $q'_i = 0$. Утверждение 2 доказано.

Обозначим через \mathcal{T} систему множеств, состоящую из всех таких T , для которых $p(a_T) > 0$, и множества M . Положим $\chi_{i,T}$ равным 1 при $i \in T$ и равным 0 при $i \notin T$. Образует матрицу $\chi = \|\chi_{i,T}\|$, $T \in \mathcal{T}$, $i \in M$, с t столбцами и $|\mathcal{T}|$ строками, столбцы которой обозначим через χ_i , $i \in M$. Скажем, что столбец χ_i *мажорирует* χ_j , если $\chi_{i,T} \geq \chi_{j,T}$, $T \in \mathcal{T}$, и *строго мажорирует*, если какое-либо из этих неравенств является строгим. Обозначим через χ' матрицу, полученную из χ удалением всех строго мажорируемых столбцов.

Утверждение 3. Если столбцы матрицы χ' линейно независимы, то энтропия $\mathcal{H}(P)$ достигается на единственном наборе Q .

ДОКАЗАТЕЛЬСТВО. При доказательстве предыдущего утверждения установлено, что точки Q , на которых достигается энтропия, удовлетворяют при некоторых α_T системе

$$\sum_i \chi_{i,T} q_i = \alpha_T, \quad T \in \mathcal{T}, \quad (5)$$

(уравнение при $T = M$ с $\alpha_M = 1$ добавлено, чтобы обеспечить равенство $\sum_i q_i = 1$). Поскольку на неотрицательных решениях этой системы функция $\mathcal{H}(P, Q)$ принимает одинаковые значения, множество этих решений задаёт все наборы, на которых достигается энтропия.

Если столбец χ_i строго мажорирует χ_j , то в точке Q минимума функции $\mathcal{H}(P, Q)$ соотношение (3) для i содержит дополнительные положительные члены в сравнении с соотношением (3) для j , а потому

$$\sum_T \frac{\chi_{j,T} p(a_T)}{\sum_t \chi_{t,T} q_t} < \sum_T \frac{\chi_{i,T} p(a_T)}{\sum_t \chi_{t,T} q_t} \leq 1,$$

и по утверждению 1 $q_j = 0$. Подставив в (5) значения $q_j = 0$ для строго мажорируемых столбцов, получим систему уравнений с матрицей χ' , из которой в силу независимости столбцов однозначно находятся остальные компоненты точки Q . Утверждение 3 доказано.

Замечание. Поскольку длина столбцов χ_i может достигать до 2^m , а их число в матрице χ' не превосходит m , «типичным» следует считать случай, когда столбцы этой матрицы линейно независимы. Это обеспечивает единственность набора Q , на котором достигается энтропия $\mathcal{H}(P)$.

2. Правило сложения энтропий при заданном доопределении

Под *доопределением источника* X будем понимать полностью определённый источник \dot{X} , который строится по X применением операции *доопределения* (для различения символов a_i источников X и \dot{X} символ a_i в \dot{X} будем обозначать через \dot{a}_i). Операция доопределения задаётся набором переходных вероятностей $p(\dot{a}_i|a_T)$, $T \subseteq M$, $i \in M$, где $p(\dot{a}_i|a_T) = 0$ для $i \notin T$. В применении к X она даёт источник \dot{X} такой, что $X\dot{X}$ имеет совместное распределение $p(a_T, \dot{a}_i) = p(a_T)p(\dot{a}_i|a_T)$, и, следовательно, $p(\dot{a}_i) = \sum_T p(a_T)p(\dot{a}_i|a_T)$. Далее считаем, что $p(\dot{a}_i) > 0$, ибо символы \dot{a}_i с $p(\dot{a}_i) = 0$ не участвуют в доопределении и их можно исключить.

Величину взаимной информации [2]

$$I(X; \dot{X}) = \sum_{T,i} p(a_T)p(\dot{a}_i|a_T) \log \frac{p(\dot{a}_i|a_T)}{p(\dot{a}_i)} \quad (6)$$

будем называть *энтропией источника X при доопределении \dot{X}* и обозначать через $\mathcal{H}_{\dot{X}}(X)$.

Замечание. Этот термин объясняется следующей сложностной интерпретацией. Рассмотрим класс «достаточно длинных» последовательностей в алфавите A , содержащих символы a_T с частотами $p(a_T)$. Пусть требуется закодировать эти последовательности так, чтобы по коду последовательности восстанавливалось какое-либо её доопределение, в котором символы a_T замещены символами \dot{a}_i , $i \in T$, с частотой $p(\dot{a}_i|a_T)$. Можно доказать, что величина $I(X; \dot{X})$ указывает наилучшую характеристику (среднюю длину кода на символ последовательности) такого кодирования.

Пусть произведение XY недоопределённых источников с алфавитами $A = \{a_T, T \subseteq M\}$ и $B = \{b_U, U \subseteq L\}$, $L = \{0, 1, \dots, l-1\}$, задано совместным распределением $p(a_T, b_U)$, $T \subseteq M$, $U \subseteq L$.

Будем считать вначале, что X полностью определён. В этом случае условную энтропию введём обычным равенством [2]:

$$\mathcal{H}(Y|X) = \sum_i p(a_i) \mathcal{H}(Y|a_i). \quad (7)$$

Входящие в него величины $\mathcal{H}(Y|a_i)$ находятся подобно (1), (2) с заменой в (1) вероятностей условными вероятностями $p(b_U|a_i) = \frac{p(a_i, b_U)}{p(a_i)}$, где $p(a_i) = \sum_U p(a_i, b_U)$. При $p(a_i) = 0$ значения $\mathcal{H}(Y|a_i)$ и условных вероятностей $p(b_U|a_i)$ несущественны и их можно не вычислять.

Из результатов [6] следует, что введённая так условная энтропия (для полностью определённого X) удовлетворяет правилу сложения энтропий $\mathcal{H}(X) + \mathcal{H}(Y|X) = \mathcal{H}(XY)$ и согласована с колмогоровской интерпретацией [3] условной энтропии как относительной сложности (подробнее в [6]).

Пусть теперь источник X в произведении XY не является полностью определённым. Применим к нему операцию доопределения при некоторых переходных вероятностях $p(\dot{a}_i|a_T)$. Получим полностью определённый источник \dot{X} . Считаем, что доопределение источника X в XY производится независимо от Y : вероятности троек (a_T, b_U, \dot{a}_i) в $XY\dot{X}$ равны

$$p(a_T, b_U, \dot{a}_i) = p(a_T, b_U)p(\dot{a}_i|a_T). \quad (8)$$

В результате возникает произведение $\dot{X}Y$ с совместным распределением $p(\dot{a}_i, b_U) = \sum_T p(a_T, b_U)p(\dot{a}_i|a_T)$. По $\dot{X}Y$ можно подобно (7) вычислить условную энтропию $\mathcal{H}(Y|\dot{X})$ при доопределении \dot{X} .

Продолжением доопределения \dot{X} на XY называется полностью определённый источник $\dot{X}Y'$, построенный по $XY\dot{X}$ применением некоторого набора переходных вероятностей $p(b'_j|a_T, b_U, \dot{a}_i)$, $p(b'_j|a_T, b_U, \dot{a}_i) = 0$ для $j \notin U$, и порождающий пары (\dot{a}_i, b'_j) с вероятностями

$$p(\dot{a}_i, b'_j) = \sum_{T,U} p(a_T, b_U, \dot{a}_i)p(b'_j|a_T, b_U, \dot{a}_i).$$

Подчёркнём разницу между доопределением источника $\dot{X}Y$ и продолжением доопределения \dot{X} на XY . Доопределение строится по $\dot{X}Y$ и не использует исходную информацию о X , а при построении продолжения она может быть использована в полной мере.

Величину

$$\mathcal{H}_{\dot{X}}(XY) = \min_{\dot{X}Y'} I(XY; \dot{X}Y'), \quad (9)$$

где минимум берётся по всем продолжениям доопределения \dot{X} на XY , назовём *энтропией произведения XY при заданном доопределении \dot{X}* .

Теорема 1. *Имеет место следующее правило сложения энтропий при доопределении \dot{X} :*

$$\mathcal{H}_{\dot{X}}(X) + \mathcal{H}(Y|\dot{X}) = \mathcal{H}_{\dot{X}}(XY).$$

Доказательство этой теоремы содержится в последующих разделах.

3. Формулировка оптимизационной задачи

Пусть $\dot{X}Y'$ — продолжение доопределения \dot{X} на XY . Выражение для взаимной информации

$$I(XY; \dot{X}Y') = \sum_{T,U,i,j} p(a_T, b_U, \dot{a}_i, b'_j) \log \frac{p(a_T, b_U, \dot{a}_i, b'_j)}{p(a_T, b_U) \sum_{T',U'} p(a_{T'}, b_{U'}, \dot{a}_i, b'_j)} \quad (10)$$

с учётом (8) представим в форме

$$\begin{aligned} I(XY; \dot{X}Y') &= \sum_{T,U,i,j} p(a_T, b_U, \dot{a}_i) p(b'_j | a_T, b_U, \dot{a}_i) \\ &\quad \times \log \frac{p(a_T, b_U) p(\dot{a}_i | a_T) p(b'_j | a_T, b_U, \dot{a}_i)}{p(a_T, b_U) \sum_{T',U'} p(a_{T'}, b_{U'}, \dot{a}_i) p(b'_j | a_{T'}, b_{U'}, \dot{a}_i)} \end{aligned} \quad (11)$$

и преобразуем к виду

$$I(XY; \dot{X}Y') = \Sigma_1 + \Sigma_2, \quad (12)$$

где*

$$\begin{aligned} \Sigma_1 &= \sum_{T,U,i,j} p(a_T, b_U, \dot{a}_i) p(b'_j | a_T, b_U, \dot{a}_i) \log \frac{p(\dot{a}_i | a_T)}{p(\dot{a}_i)}, \\ \Sigma_2 &= \sum_{T,U,i,j} p(a_T, b_U, \dot{a}_i) p(b'_j | a_T, b_U, \dot{a}_i) \\ &\quad \times \left(\log p(b'_j | a_T, b_U, \dot{a}_i) - \log \left(\sum_{T',U'} \frac{p(a_{T'}, b_{U'}, \dot{a}_i)}{p(\dot{a}_i)} p(b'_j | a_{T'}, b_{U'}, \dot{a}_i) \right) \right). \end{aligned}$$

Лемма 1. $\Sigma_1 = \mathcal{H}_{\dot{X}}(X)$.

ДОКАЗАТЕЛЬСТВО. Представим Σ_1 в виде

$$\Sigma_1 = \sum_{T,i} \log \frac{p(\dot{a}_i | a_T)}{p(\dot{a}_i)} \sum_U p(a_T, b_U, \dot{a}_i) \sum_j p(b'_j | a_T, b_U, \dot{a}_i).$$

С учётом соотношений $\sum_j p(b'_j | a_T, b_U, \dot{a}_i) = 1$ и $\sum_U p(a_T, b_U, \dot{a}_i) = p(a_T, \dot{a}_i)$ это выражение приводится к виду, эквивалентному (6). Лемма 1 доказана.

Будем рассматривать Σ_2 как функцию от набора переходных вероятностей $P = (p(b'_j | a_T, b_U, \dot{a}_i), T \subseteq M, U \subseteq L, i \in T, j \in U)$.

*Напомним, что $p(\dot{a}_i) > 0$.

Лемма 2. Функция $\Sigma_2(P)$ выпукла вниз.

Доказательство. Воспользуемся тем, что информация $I(XY; \dot{X}Y')$ выпукла вниз по набору переходных вероятностей $p(\dot{a}_i, b'_j | a_T, b_U)$ [2]. В силу равенства

$$p(\dot{a}_i, b'_j | a_T, b_U) = p(\dot{a}_i | a_T) p(b'_j | a_T, b_U, \dot{a}_i),$$

вытекающего из (8), она выпукла вниз и по набору переходных вероятностей $p(b'_j | a_T, b_U, \dot{a}_i)$. Так как Σ_2 отличается от $I(XY; \dot{X}Y')$ постоянным слагаемым Σ_1 , то Σ_2 также выпукла вниз по этому набору. Лемма 2 доказана.

В результате доказательство теоремы 1 свелось к задаче минимизации по набору переходных вероятностей P выпуклой вниз функции $\Sigma_2(P)$ и установлению того, что этот минимум совпадает с $\mathcal{H}(Y|\dot{X})$.

4. Условия минимальности

Положим $D_m = \{(p_1, \dots, p_m) \mid p_1, \dots, p_m \geq 0, p_1 + \dots + p_m = 1\}$.

Лемма 3. Пусть $F(P) = F(p_{11}, \dots, p_{1m_1}, \dots, p_{k1}, \dots, p_{km_k})$ — выпуклая вниз функция на $D = D_{m_1} \times \dots \times D_{m_k}$. Тогда если в некоторой точке \hat{P} существуют и непрерывны все частные производные $\frac{\partial F}{\partial p_{ij}}$ и при некоторых λ_i , $1 \leq i \leq m_i$, они удовлетворяют условиям

$$\frac{\partial F(\hat{P})}{\partial p_{ij}} \leq \lambda_i, \quad 1 \leq j \leq m_i, \quad (13)$$

где строгие неравенства могут иметь место лишь при тех j , для которых $p_{ij} = 0$, то \hat{P} — точка минимума функции F на D .

Эта лемма обобщает достаточное условие теоремы 4.4.1 из [2] на случай, когда функция зависит от нескольких наборов вероятностей. Её доказательство аналогично доказательству из [2] и мы его опускаем.*

С учётом леммы 2 переформулируем результат леммы 3 применительно к функции $\Sigma_2(P)$.

Лемма 4. Если для набора $\hat{P} = (\hat{p}(b'_j | a_T, b_U, \dot{a}_i), T \subseteq M, U \subseteq L, i \in T, j \in U)$ существуют такие $\lambda_{T,U,i}$, что для всех $T, U, i \in T, j \in U$ выполнено

$$\frac{\partial \Sigma_2(\hat{P})}{\partial p(b'_j | a_T, b_U, \dot{a}_i)} \geq \lambda_{T,U,i},$$

*Утверждение леммы может быть подобно теореме 4.4.1 из [2] сформулировано в виде необходимого и достаточного условий. Мы ограничились достаточностью, поскольку необходимость не понадобится.

где строгие неравенства могут иметь место лишь при тех T, U, i, j , для которых $\hat{p}(b'_j|a_T, b_U, \dot{a}_i) = 0$, то \hat{P} — точка минимума функции $\Sigma_2(P)$.

Лемма 5. Если для набора $\hat{P} = (\hat{p}(b'_j|a_T, b_U, \dot{a}_i), T \subseteq M, U \subseteq L, i \in T, j \in U)$ существуют такие $\lambda_{T,U,i}$, что для всех $T, U, i \in T, j \in U$ выполнено

$$\frac{p(\dot{a}_i)\hat{p}(b'_j|a_T, b_U, \dot{a}_i)}{\sum_{T',U'} p(a_{T'}, b_{U'}, \dot{a}_i)\hat{p}(b'_j|a_{T'}, b_{U'}, \dot{a}_i)} \geq \lambda_{T,U,i}, \quad (14)$$

где строгие неравенства могут иметь место лишь при тех T, U, i, j , для которых $\hat{p}(b'_j|a_T, b_U, \dot{a}_i) = 0$, то \hat{P} — точка минимума функции $\Sigma_2(P)$.

ДОКАЗАТЕЛЬСТВО. Введём функцию $\psi(x) = x \log x$ и представим Σ_2 в виде

$$\begin{aligned} \Sigma_2 = & \sum_{T,U,i,j} p(a_T, b_U, \dot{a}_i) \psi(p(b'_j|a_T, b_U, \dot{a}_i)) \\ & - \sum_i p(\dot{a}_i) \sum_j \psi\left(\sum_{T,U} \frac{p(a_T, b_U, \dot{a}_i)}{p(\dot{a}_i)} p(b'_j|a_T, b_U, \dot{a}_i)\right). \end{aligned}$$

С учётом равенства

$$\frac{\partial}{\partial x_v} \psi\left(\sum_u c_u x_u\right) = c_v \log\left(\sum_u c_u x_u\right) + c_v \log e$$

найдем частные производные

$$\begin{aligned} \frac{\partial \Sigma_2}{\partial p(b'_j|a_T, b_U, \dot{a}_i)} = & p(a_T, b_U, \dot{a}_i) \log p(b'_j|a_T, b_U, \dot{a}_i) + p(a_T, b_U, \dot{a}_i) \log e \\ & - p(a_T, b_U, \dot{a}_i) \log\left(\sum_{T',U'} \frac{p(a_{T'}, b_{U'}, \dot{a}_i)}{p(\dot{a}_i)} p(b'_j|a_{T'}, b_{U'}, \dot{a}_i)\right) \\ & - p(a_T, b_U, \dot{a}_i) \log e. \end{aligned}$$

Это выражение приводится к виду

$$\frac{\partial \Sigma_2}{\partial p(b'_j|a_T, b_U, \dot{a}_i)} = p(a_T, b_U, \dot{a}_i) \log\left(\frac{p(\dot{a}_i)p(b'_j|a_T, b_U, \dot{a}_i)}{\sum_{T',U'} p(a_{T'}, b_{U'}, \dot{a}_i)p(b'_j|a_{T'}, b_{U'}, \dot{a}_i)}\right).$$

Отсюда и из (14) заключаем, что к Σ_2 применима лемма 4, если в ней в качестве $\lambda_{T,U,i}$ взять $p(a_T, b_U, \dot{a}_i) \log \lambda_{T,U,i}$, где $\lambda_{T,U,i}$ из (14). По лемме 4 точка \hat{P} минимизирует функцию $\Sigma_2(P)$. Лемма 5 доказана.

5. Завершение доказательства теоремы 1

Обозначим через $Q^{(i)} = (q_j^{(i)}, j \in L)$, $i \in M$, набор, на котором достигается энтропия $\mathcal{H}(Y|\dot{a}_i)$. Применительно к нему утверждение 1 приобретает вид:

$$\sum_{U: j \in U} \frac{p(b_U|\dot{a}_i)}{\sum_{u \in U} q_u^{(i)}} \leq 1, \quad j \in L, \quad (15)$$

где строгое неравенство может иметь место лишь при тех j , для которых $q_j^{(i)} = 0$. Аналогом равенства (4) для $Q^{(i)}$ является

$$\sum_{U: j \in U} \frac{p(b_U|\dot{a}_i)q_j^{(i)}}{\sum_{u \in U} q_u^{(i)}} = q_j^{(i)}. \quad (16)$$

Положим для $j \in U$

$$\hat{p}(b'_j|a_T, b_U, \dot{a}_i) = \frac{q_j^{(i)}}{\sum_{u \in U} q_u^{(i)}}, \quad (17)$$

$$\hat{P} = (\hat{p}(b'_j|a_T, b_U, \dot{a}_i), T \subseteq M, U \subseteq L, i \in T, j \in U).$$

Лемма 6. Минимум функции $\Sigma_2(P)$ достигается на наборе \hat{P} .

ДОКАЗАТЕЛЬСТВО. Убедимся, что точка \hat{P} удовлетворяет условиям леммы 5. Обозначим через Σ' сумму в знаменателе (14). Так как при $j \notin U'$ имеет место $p(b'_j|a_{T'}, b_{U'}, \dot{a}_i) = 0$, суммирование по U' в ней можно заменить суммированием по тем U' , которые содержат j . Вычислим Σ' при значениях (17):

$$\Sigma' = q_j^{(i)} \sum_{U': j \in U'} \frac{1}{\sum_{u \in U'} q_u^{(i)}} \sum_{T'} p(a_{T'}, b_{U'}, \dot{a}_i) = q_j^{(i)} p(\dot{a}_i) \sum_{U': j \in U'} \frac{p(b_{U'}|\dot{a}_i)}{\sum_{u \in U'} q_u^{(i)}}.$$

С учётом этого левая часть в (14) принимает значение*

$$\frac{p(\dot{a})q_j^{(i)}}{\sum_{u \in U'} q_u^{(i)} \cdot \Sigma'} = \left(\sum_{u \in U} q_u^{(i)} \sum_{U': j \in U'} \frac{p(b_{U'}|\dot{a}_i)}{\sum_{u \in U'} q_u^{(i)}} \right)^{-1},$$

*Для $q_j^{(i)} = 0$ сокращение на $q_j^{(i)}$ произведено путём предельного перехода при $q_j^{(i)} \rightarrow 0 + 0$.

которое в силу (15) не меньше $(\sum_{u \in U} q_u^{(i)})^{-1}$. Строгое неравенство может иметь место лишь при $q_j^{(i)} = 0$, но в этом случае $p(b'_j | a_T, b_U, \dot{a}_i) = 0$. Тем самым условия леммы 5 выполнены при $\lambda_{T,U,i} = (\sum_{u \in U} q_u^{(i)})^{-1}$ и \hat{P} является точкой минимума функции $\Sigma_2(P)$. Лемма 6 доказана.

Лемма 7. $\min_P \Sigma_2(P) = \mathcal{H}(Y|\dot{X})$.

ДОКАЗАТЕЛЬСТВО. Введя обозначение

$$z_{T,U,i,j} = \frac{p(\dot{a}_i) \hat{p}(b'_j | a_T, b_U, \dot{a}_i)}{\sum_{T',U'} p(a_{T'}, b_{U'}, \dot{a}_i) \hat{p}(b'_j | a_{T'}, b_{U'}, \dot{a}_i)}, \quad (18)$$

представим Σ_2 в виде

$$\Sigma_2 = \sum_{T,U,i,j} p(a_T, b_U, \dot{a}_i) p(b'_j | a_T, b_U, \dot{a}_i) \log z_{T,U,i,j}.$$

Отсюда и из (17) имеем

$$\Sigma_2(\hat{P}) = \sum_{T,U,i} p(a_T, b_U, \dot{a}_i) \sum_{j \in U} \frac{q_j^{(i)}}{\sum_{u \in U} q_u^{(i)}} \log z_{T,U,i,j}(\hat{P}). \quad (19)$$

Величина $z_{T,U,i,j}(\hat{P})$ совпадает с левой частью (14) и, как было установлено при доказательстве леммы 6, в случае $q_j^{(i)} > 0$ она равна $(\sum_{u \in U} q_u^{(i)})^{-1}$.

Поскольку при $q_j^{(i)} = 0$ значения $z_{T,U,i,j}(\hat{P})$ несущественны, это выражение может быть подставлено в (19) при всех i и j . После такой подстановки приведём (19) к виду

$$\Sigma_2(\hat{P}) = \sum_i \sum_U \log \frac{1}{\sum_{u \in U} q_u^{(i)}} \sum_T p(a_T, b_U, \dot{a}_i) \sum_{j \in U} \frac{q_j^{(i)}}{\sum_{u \in U} q_u^{(i)}}.$$

Преобразуем это выражение с учётом того, что последняя сумма в нём обращается в 1, а $\sum_T p(a_T, b_U, \dot{a}_i) = p(b_U, \dot{a}_i) = p(\dot{a}_i) p(b_U | \dot{a}_i)$:

$$\Sigma_2(\hat{P}) = \sum_i p(\dot{a}_i) \sum_U p(b_U | \dot{a}_i) \log \frac{1}{\sum_{u \in U} q_u^{(i)}}.$$

Поскольку энтропия $\mathcal{H}(Y|\dot{a}_i)$ достигается в точке $Q^{(i)}$, получаем

$$\Sigma_2(\hat{P}) = \sum_i p(\dot{a}_i) \mathcal{H}(Y|\dot{a}_i) = \mathcal{H}(Y|\dot{X}),$$

и остаётся сослаться на лемму 6. Лемма 7 доказана.

Утверждение теоремы следует из (12) и лемм 1, 6, 7.

Замечание. Из того, что условные вероятности (17) не зависят от X , следует, что $\dot{X}Y'$, на котором достигается $\mathcal{H}_{\dot{X}}(XY)$, может быть получено доопределением произведения $\dot{X}Y$.

6. Обобщённое правило сложения энтропий

В [4] (см. также [5]) доказано утверждение, которое может быть переформулировано в введённых выше терминах следующим образом.

Утверждение 4. *Справедливо равенство*

$$\min_{\dot{X}} \mathcal{H}_{\dot{X}}(X) = \mathcal{H}(X),$$

где минимум берётся по всем доопределениям \dot{X} источника X .

Всякое доопределение \hat{X} , для которого

$$\mathcal{H}_{\hat{X}}(X) = \mathcal{H}(X), \tag{20}$$

будем называть *лучшим*.

Замечание. Такое название объясняется следующей интерпретацией в терминах сжатия. Пусть недоопределённый источник X имеет единственное лучшее доопределение \hat{X} (эта ситуация типична — см. дальше). Рассмотрим такое кодирование достаточно длинных последовательностей \mathbf{x} в алфавите A , содержащих символы a_T с частотами $p(a_T)$, при котором по коду последовательности восстанавливается какое-либо её доопределение. Можно доказать, что если средняя длина кода асимптотически минимальна и $\hat{\mathbf{x}}$ — доопределение последовательности \mathbf{x} при этом кодировании, то для почти всех последовательностей \mathbf{x} частота появления пар символов (a_T, \hat{a}_i) в паре $(\mathbf{x}, \hat{\mathbf{x}})$ асимптотически равна вероятности $p(a_T, \hat{a}_i)$ в произведении $X\hat{X}$.

Следующее утверждение указывает переходные вероятности, приводящие к лучшему доопределению.

Лемма 8. Доопределение \hat{X} является лучшим тогда и только тогда, когда оно задаётся переходными вероятностями

$$p(\hat{a}_i|a_T) = \frac{\hat{q}_i}{\sum_{j \in T} \hat{q}_j}, \quad i \in T, \quad (21)$$

где $\hat{Q} = (\hat{q}_i, i \in M)$ — один из наборов (любой), на которых достигается $\mathcal{H}(X)$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим произвольное доопределение \dot{X} . Положим $P_{\dot{X}} = (p(\dot{a}_j), j \in M)$ и $J^+ = \{j \mid p(\dot{a}_j) > 0\}$. При заданном T введём для $i \in T \cap J^+$ величины

$$\alpha_i^{(T)} = \frac{p(\dot{a}_i)}{\sum_{j \in T} p(\dot{a}_j)}, \quad x_i^{(T)} = \frac{p(\dot{a}_i|a_T)}{p(\dot{a}_i)}. \quad (22)$$

Поскольку $\sum_{i \in T \cap J^+} p(\dot{a}_i) = \sum_{i \in T} p(\dot{a}_i)$, то $\sum_{i \in T \cap J^+} \alpha_i^{(T)} = 1$. Воспользуемся для выпуклой вниз функции $f(x) = x \log x$ неравенством Иенсена:

$$\sum_{i \in T \cap J^+} \alpha_i^{(T)} f(x_i^{(T)}) \geq f\left(\sum_{i \in T \cap J^+} \alpha_i^{(T)} x_i^{(T)}\right). \quad (23)$$

Учитывая, что

$$\sum_{i \in T \cap J^+} p(\dot{a}_i|a_T) = \sum_{i \in T} p(\dot{a}_i|a_T) = 1,$$

находим

$$\sum_{i \in T \cap J^+} \alpha_i^{(T)} x_i^{(T)} = \sum_{i \in T \cap J^+} \frac{p(\dot{a}_i|a_T)}{\sum_{j \in T} p(\dot{a}_j)} = \frac{1}{\sum_{j \in T} p(\dot{a}_j)}.$$

Подстановка этого значения в (23) даёт неравенство

$$\sum_{i \in T \cap J^+} \frac{p(\dot{a}_i|a_T)}{\sum_{j \in T} p(\dot{a}_j)} \log \frac{p(\dot{a}_i|a_T)}{p(\dot{a}_i)} \geq \frac{1}{\sum_{j \in T} p(\dot{a}_j)} \log \frac{1}{\sum_{j \in T} p(\dot{a}_j)}.$$

Принимая во внимание, что $p(\dot{a}_i|a_T) = 0$ для $i \notin J^+$, заменим в этом неравенстве суммирование по $i \in T \cap J^+$ суммированием по $i \in T$. После этого, домножив обе части на $p(a_T) \sum_{j \in T} p(\dot{a}_j)$ и просуммировав по T , получим

$$\mathcal{H}_{\dot{X}}(X) = I(X; \dot{X}) \geq \mathcal{H}(P, P_{\dot{X}}) \geq \mathcal{H}(X).$$

Отсюда видно, что равенство (20) возможно, лишь если на наборе $P_{\hat{X}}$ достигается энтропия $\mathcal{H}(X)$. Пусть \hat{Q} — произвольная точка минимума функции $\mathcal{H}(P, Q)$, $J^+ = \{j \mid \hat{q}_j > 0\}$ и доопределение \hat{X} таково, что $P_{\hat{X}} = \hat{Q}$. В этом случае равенство (20) имеет место тогда и только тогда, когда при каждом T неравенство (23) обращается в равенство. Поскольку для $i \in T \cap J^+$ все $\alpha_i^{(T)}$ строго положительны, условием равенства является совпадение всех $x_i^{(T)}$, $i \in T \cap J^+$. Обозначив их величину через γ_T , получаем $p(\hat{a}_i|a_T) = \gamma_T \hat{q}_i$. Это равенство справедливо для всех $i \in T$, ибо при $i \notin J^+$ обе части обращаются в 0. Отсюда и из $\sum_{j \in T} p(\hat{a}_j|a_T) = 1$ находим $\gamma_T = \frac{1}{\sum_{j \in T} \hat{q}_j}$, что приводит к (21). Чтобы можно было назначить $p(\hat{a}_i|a_T)$ указанным образом, необходимо выполнение равенств $\sum_T p(a_T)p(\hat{a}_i|a_T) = p(\hat{a}_i)$, $i \in M$. Их справедливость следует из того, что при условиях (21) они совпадают с (4). Лемма 8 доказана.

Замечание. Из доказательства вытекают следующие факты, которые понадобятся в дальнейшем.

- (а) Если лучшее доопределение задаётся посредством (21), то $p(\hat{a}_i) = \hat{q}_i$, $i \in M$.
- (б) Имеется единственное лучшее доопределение с $p(\hat{a}_i) = \hat{q}_i$, $i \in M$, и оно задаётся переходными вероятностями (21).
- (в) Если \hat{X} — лучшее доопределение, то на наборе $P_{\hat{X}} = (p(\hat{a}_i), i \in M)$ достигается энтропия $\mathcal{H}(X)$.

Недоопределённый источник назовём *категоричным*, если он имеет единственное лучшее доопределение.

Следствие 1. *Источник категоричен тогда и только тогда, когда его энтропия достигается в единственной точке.*

В «типичном» (невыврожденном) случае это условие выполнено (замечание к утверждению 3).

Энтропия $\mathcal{H}(X)$ совпадает с минимумом по \dot{X} энтропии $\mathcal{H}_{\dot{X}}(X)$. Представляется естественным и условную энтропию $\mathcal{H}(Y|X)$ определить как минимум по \dot{X} условной энтропии $\mathcal{H}(Y|\dot{X})$. Однако это приводит к нежелательным эффектам, связанным с тем, что эти минимумы могут достигаться на разных доопределениях.

Рассмотрим пример. Пусть в произведении XU источников с алфавитами $\{0, 1, *\}$ и $\{0, 1\}$, где $*$ означает неопределённый символ (доопределимый до 0 и 1), пары (0, 0) и (*, 1) порождаются с ненулевыми вероятностями, а вероятности остальных пар равны 0. Лучшее доопределение \hat{X} соответствует замене в X всех символов $*$ символом 0. Для

него $\mathcal{H}_{\hat{X}}(X) = \mathcal{H}(X) = 0$ и $\mathcal{H}(Y|\hat{X}) = \mathcal{H}(Y)$. При замене в X всех * символом 1 придём к источнику X' , совпадающему с Y . В этом случае $\mathcal{H}_{X'}(X) = \mathcal{H}(Y)$ и $\mathcal{H}(Y|X') = 0$. Если в качестве $\mathcal{H}(Y|X)$ взять минимальное значение, то сумма $\mathcal{H}(X) + \mathcal{H}(Y|X)$ в правиле сложения энтропий даст 0. Занижение суммы здесь произошло за счёт использования в слагаемых разных доопределений. Подобный эффект проявляется и в более сложных ситуациях и служит доводом в пользу того, чтобы при введении $\mathcal{H}(Y|X)$ использовать то же доопределение, что и в $\mathcal{H}(X)$, т. е. лучшее. (Отметим, что если так поступить в данном примере, то правило сложения энтропий будет выполнено.)

В соответствии со сказанным будем в качестве основного рассматривать случай, когда источник X категоричен, и полагать по определению

$$\mathcal{H}(Y|X) = \mathcal{H}(Y|\hat{X}), \quad (24)$$

где \hat{X} — лучшее доопределение. Случай некатегоричного X обсудим позже.

Величину $\mathcal{H}_{\hat{X}}(XY)$ энтропии произведения XY при лучшем доопределении \hat{X} источника X обозначим через $\hat{\mathcal{H}}(XY)$. Из теоремы 1 при $\hat{X} = \hat{X}$ вытекает следующая

Теорема 2. Для категоричного источника X справедливо равенство

$$\mathcal{H}(X) + \mathcal{H}(Y|X) = \hat{\mathcal{H}}(XY). \quad (25)$$

Соотношение (25) будем называть *обобщённым правилом сложения энтропий*.

Замечание. Из замечания, завершающего разд. 5, следует, что произведение $\hat{X}Y'$, на котором достигается $\hat{\mathcal{H}}(XY)$, может быть найдено последовательным построением лучших доопределений — вначале для источника X , затем для $\hat{X}Y$.

В общем случае, когда источник X может иметь неединственное лучшее доопределение, вместо (24) естественно положить

$$\mathcal{H}(Y|X) = \min_{\hat{X}} \mathcal{H}(Y|\hat{X}),$$

где минимум берётся по всем лучшим доопределениям. Использование минимума здесь допустимо, поскольку множество лучших доопределений задаётся системой уравнений (5) и леммой 8, а потому является компактом.

Согласно утверждению 2 если при заданном i для некоторого набора, на котором достигается энтропия, неравенство (3) является строгим, то оно является строгим для всех \hat{Q} , на которых достигается энтропия, и $\hat{q}_i = 0$. Соответствующий символ a_i не участвует ни в каком лучшем доопределении. Исключив такие i из M , получим множество M' . При $i \in M'$ лучшие доопределения удовлетворяют равенствам

$$\sum_{T: i \in T} \frac{p(a_T)}{\sum_{j \in T} \hat{q}_j} = 1. \quad (26)$$

В силу замечания (а) к лемме 8 $p(\hat{a}_i) = \hat{q}_i$ и потому

$$\mathcal{H}(Y|\hat{X}) = \sum_{i \in M'} \hat{q}_i \mathcal{H}(Y|\hat{a}_i). \quad (27)$$

Утверждение 5. Величины $\mathcal{H}(Y|\hat{a}_i)$ в (27) не зависят от выбора лучшего доопределения \hat{X} .

ДОКАЗАТЕЛЬСТВО. Согласно лемме 8 произведению $\hat{X}Y$ соответствует совместное распределение

$$p(\hat{a}_i, b_U) = \sum_T p(a_T, b_U) p(\hat{a}_i | a_T) = \sum_{T: i \in T} \frac{p(a_T, b_U) \hat{q}_i}{\sum_{t \in T} \hat{q}_t}.$$

Если $\hat{q}_i \neq 0$, то

$$p(b_U | \hat{a}_i) = \frac{p(\hat{a}_i, b_U)}{\hat{q}_i} = \sum_{T: i \in T} \frac{p(a_T, b_U)}{\sum_{t \in T} \hat{q}_t}. \quad (28)$$

В случае $\hat{q}_i = 0$ величины $p(b_U | \hat{a}_i)$ несущественны, и их задаём тем же выражением. Корректность такого задания следует из (26):

$$\sum_U p(b_U | \hat{a}_i) = \sum_{T: i \in T} \frac{\sum_U p(a_T, b_U)}{\sum_{t \in T} \hat{q}_t} = \sum_{T: i \in T} \frac{p(a_T)}{\sum_{t \in T} \hat{q}_t} = 1.$$

При доказательстве леммы 2 установлено, что величины $\sum_{t \in T} \hat{q}_t$ не зависят от выбора лучшего доопределения \hat{X} , поэтому от него не зависят условные вероятности (28) и определяемая ими энтропия $\mathcal{H}(Y|\hat{a}_i)$. Утверждение 5 доказано.

Поскольку значения $h_i = \mathcal{H}(Y|\hat{a}_i)$, $i \in M'$, и ограничения (5) не зависят от выбора лучшего доопределения \hat{X} , для вычисления $\mathcal{H}(Y|X)$ можно вначале, используя произвольное лучшее доопределение, найти величины h_i и ограничения (5), а затем решить задачу линейного программирования $\sum_{i \in M'} \hat{q}_i h_i \rightarrow \min$ при этих ограничениях на \hat{Q} .

Величину

$$\hat{\mathcal{H}}(XY) = \min_{\hat{X}, \hat{X}Y'} I(XY; \hat{X}Y'),$$

где минимум берётся по всем продолжениям $\hat{X}Y'$ всех лучших доопределений \hat{X} , назовём *энтропией произведения XY при лучшем доопределении источника X* . Обобщённое правило сложения энтропий распространяется на общий случай в том же виде (25). Для его доказательства достаточно применить теорему 1 к лучшим доопределениям и взять минимум от обеих частей равенства.

7. Критерий выполнимости обычного правила сложения энтропий

В данном разделе рассмотрены условия, при которых обобщённое правило сложения энтропий превращается в обычное правило

$$\mathcal{H}(X) + \mathcal{H}(Y|X) = \mathcal{H}(XY). \quad (29)$$

Источник X будем считать категоричным. Тогда энтропия $\mathcal{H}(X)$ достигается на единственном наборе $\hat{Q} = (\hat{q}_i, i \in M)$, лучшее доопределение \hat{X} задаётся переходными вероятностями (21) и для него $p(\hat{a}_i) = \hat{q}_i$ (замечание (а) к лемме 8). Положим $M' = \{i \mid \hat{q}_i > 0\}$. Для $i \in M'$ обозначим через $Q^{(i)} = (q_j^{(i)}, j \in L)$ некоторый набор, на котором достигается энтропия $\mathcal{H}(Y|\hat{a}_i)$ из (27).

Теорема 3. *Если источник X категоричен, то правило сложения энтропий (29) имеет место тогда и только тогда, когда выполнены условия:*

(а) *на наборе $\tilde{Q} = (\tilde{q}_{ij} = \hat{q}_i q_j^{(i)}, i \in M, j \in L)$, достигается энтропия $\mathcal{H}(XY)$,*

(б) *для всех T и U таких, что $p(a_T, b_U) > 0$, сумма $\sum_{u \in U} q_u^{(i)}$ одинакова для всех $i \in T \cap M'$.*

Доказательство. НЕОБХОДИМОСТЬ. Пусть выполнено правило сложения энтропий. В соответствии с равенствами (8), (17) и леммой 6 ве-

личина $I(XY; \hat{X}Y')$ в (10) принимает минимальное значение при

$$p(a_T, b_U, \hat{a}_i, b'_j) = p(a_T, b_U) p(\hat{a}_i | a_T) \frac{q_j^{(i)}}{\sum_{u \in U} q_u^{(i)}}. \quad (30)$$

Отсюда и из того, что минимум совпадает с $\mathcal{H}(XY)$, в силу замечания (в) к лемме 8 вытекает, что $\mathcal{H}(XY)$ достигается на наборе вероятностей

$$\begin{aligned} p(\hat{a}_i, b'_j) &= \sum_{T \ni i, U \ni j} p(a_T, b_U, \hat{a}_i, b'_j) \\ &= \sum_{U \ni j} \frac{q_j^{(i)}}{\sum_{u \in U} q_u^{(i)}} \sum_{T \ni i} p(a_T, b_U) p(\hat{a}_i | a_T) = \sum_{U \ni j} \frac{p(\hat{a}_i, b_U) q_j^{(i)}}{\sum_{u \in U} q_u^{(i)}}. \end{aligned}$$

Считая вначале $\hat{q}_i > 0$ и учитывая, что $\hat{q}_i = p(\hat{a}_i)$, преобразуем это выражение с использованием (16). Имеем

$$p(\hat{a}_i, b'_j) = \hat{q}_i \sum_{U \ni j} \frac{p(b_U | \hat{a}_i) q_j^{(i)}}{\sum_{u \in U} q_u^{(i)}} = \hat{q}_i q_j^{(i)} = \tilde{q}_{ij}.$$

Если $\hat{q}_i = p(\hat{a}_i) = 0$, то $p(\hat{a}_i, b'_j) = 0$ и равенство $p(\hat{a}_i, b'_j) = \hat{q}_i q_j^{(i)}$ выполнено тривиальным образом. Необходимость п. (а) доказана.

Равенство (30) с учётом леммы 8 приобретает вид

$$p(a_T, b_U, \hat{a}_i, b'_j) = \frac{p(a_T, b_U) \hat{q}_i q_j^{(i)}}{\sum_{t \in T} \hat{q}_t \sum_{u \in U} q_u^{(i)}}.$$

Из замечания (б) к лемме 8 следует, что для значений $p(\hat{a}_i, b'_j) = \hat{q}_i q_j^{(i)}$ минимум величины $I(XY; \hat{X}Y')$ достигается лишь при

$$p(a_T, b_U, \hat{a}_i, b'_j) = \frac{p(a_T, b_U) \hat{q}_i q_j^{(i)}}{\sum_{t \in T, u \in U} \hat{q}_t q_u^{(t)}}.$$

Отсюда

$$\frac{p(a_T, b_U) \hat{q}_i q_j^{(i)}}{\sum_{t \in T} \hat{q}_t \sum_{u \in U} q_u^{(i)}} = \frac{p(a_T, b_U) \hat{q}_i q_j^{(i)}}{\sum_{t \in T, u \in U} \hat{q}_t q_u^{(t)}}. \quad (31)$$

Пусть $p(a_T, b_U) > 0$ и $\hat{q}_i > 0$. Из (21) следует, что $p(\hat{a}_i|a_T) > 0$, а потому $p(\hat{a}_i, b_U) \geq p(a_T, b_U)p(\hat{a}_i|a_T) > 0$ и $p(b_U|\hat{a}_i) > 0$. Отсюда и из (15) заключаем, что $\sum_{u \in U} q_u^{(i)} > 0$ и, следовательно, найдётся $j \in U$, для которого $q_j^{(i)} > 0$. Рассмотрим (31) при этом значении j . Осуществив сокращения и учитывая, что $\sum_{t \in T} \hat{q}_t \geq \hat{q}_i > 0$, из него находим

$$\sum_{u \in U} q_u^{(i)} = \frac{\sum_{t \in T, u \in U} \hat{q}_t q_u^{(t)}}{\sum_{t \in T} \hat{q}_t}.$$

Выражение в правой части не зависит от i . Необходимость доказана.

Достаточность. Пусть выполнены условия (а) и (б) теоремы.

Обозначим через $z'_{T,U,i,j}$ выражение под знаком логарифма в представлении (11) при $\dot{X} = \hat{X}$. Будем считать вначале, что $p(a_T, b_U) > 0$, $p(\hat{a}_i) = \hat{q}_i > 0$ и $q_j^{(i)} > 0$. Используя обозначение (18) и лемму 8, запишем $z'_{T,U,i,j}$ в виде $z'_{T,U,i,j} = \frac{p(\hat{a}_i|a_T)z_{T,U,i,j}}{p(\hat{a}_i)} = \frac{z_{T,U,i,j}}{\sum_{t \in T} \hat{q}_t}$. Все дальнейшие выкладки относятся к точке (17) минимума выражения (11). В доказательстве леммы 7 было установлено, что $z'_{T,U,i,j} = \left(\sum_{u \in U} q_u^{(i)}\right)^{-1}$ при

$q_j^{(i)} > 0$. Подставляя это значение в предшествующее равенство, получаем $z'_{T,U,i,j} = \frac{1}{\sum_{t \in T} \hat{q}_t \sum_{u \in U} q_u^{(i)}}$. Преобразуем это выражение, используя условия

(б) и (а) теоремы. Имеем

$$z'_{T,U,i,j} = \frac{1}{\sum_{t \in T} \hat{q}_t \sum_{u \in U} q_u^{(t)}} = \frac{1}{\sum_{t \in T, u \in U} \hat{q}_t q_u^{(t)}} = \frac{1}{\sum_{t \in T, u \in U} \tilde{q}_{tu}}.$$

Поскольку слагаемые выражения (11), соответствующие нулевым значениям хотя бы одной из величин $p(a_T, b_U)$, \hat{q}_i и $q_j^{(i)}$, обращаются в 0 независимо от значений $z'_{T,U,i,j}$, полученные выражения могут быть подставлены в (11) при всех T, U, i и j . Это даёт

$$\begin{aligned} I(XY; \hat{X}Y') &= \sum_{T,U,i,j} p(a_T, b_U, \hat{a}_i) p(b'_j|a_T, b_U, \hat{a}_i) \log z'_{T,U,i,j} \\ &= - \sum_{T,U} \log \left(\sum_{t \in T, u \in U} \tilde{q}_{tu} \right) \sum_{i \in T} p(a_T, b_U, \hat{a}_i) \sum_{j \in U} p(b'_j|a_T, b_U, \hat{a}_i). \end{aligned}$$

Принимая во внимание равенства

$$\sum_{j \in U} p(b'_j|a_T, b_U, \hat{a}_i) = 1, \quad \sum_{i \in T} p(a_T, b_U, \hat{a}_i) = p(a_T, b_U)$$

и условие (а) теоремы, отсюда получаем

$$I(XY; \hat{X}Y') = - \sum_{T,U} p(a_T, b_U) \log \left(\sum_{t \in T, u \in U} \tilde{q}_{tu} \right) = \mathcal{H}(XY).$$

Теорема 3 доказана.

Проиллюстрируем применение теоремы 3 примерами. Будем говорить, что символ $a_T \in A$ конкретней символа $b_U \in B$, если $a_T \in A_0$ либо $b_U = *$, и что источник X конкретней источника Y , если $p(a_T, b_U) > 0$, лишь если a_T конкретней b_U .

Утверждение 6. Если источник X конкретней Y , то справедливо правило сложения энтропий (29).

ДОКАЗАТЕЛЬСТВО. Проверим выполнение условий (а) и (б) теоремы 3.

(а) Учитывая, что X конкретней Y и $p(a_T, *) = p(a_T)$ для $|T| \geq 2$, запишем применительно к XY левую часть аналога неравенства (3), относящегося к паре (a_i, b_j) , в виде

$$\sum_{U: j \in U} \frac{p(a_i, b_U)}{\sum_{u \in U} q_{iu}} + \sum_{T: |T| \geq 2, i \in T} \frac{p(a_T)}{\sum_{l \in T} \sum_{u \in L} q_{lu}} = \Sigma_1 + \Sigma_2.$$

Подставляя в Σ_1 значения $q_{ij} = \hat{q}_i q_j^{(i)}$ и $p(a_i, b_U) = \hat{q}_i p(b_U | \hat{a}_i)$, получаем

$$\Sigma_1 = \sum_{U: j \in U} \frac{p(b_U | \hat{a}_i)}{\sum_{u \in U} q_u^{(i)}}.$$

Поскольку вероятность $p(\hat{a}_i, *)$ в $\hat{X}Y$ увеличилась в сравнении с $p(a_i, *)$ на $\hat{q}_i - p(a_i)$, неравенство (15) приобретает вид $\Sigma_1 + \frac{\hat{q}_i - p(a_i)}{\hat{q}_i} \leq 1$, откуда $\Sigma_1 \leq \frac{p(a_i)}{\hat{q}_i}$. Принимая во внимание, что $q_{lu} = \hat{q}_l q_u^{(l)}$ и $\sum_u q_u^{(l)} = 1$, запишем Σ_2 в виде

$$\Sigma_2 = \sum_{T: |T| \geq 2, i \in T} \frac{p_T}{\sum_{l \in T} q_l}.$$

В результате

$$\Sigma_1 + \Sigma_2 \leq \frac{p(a_i)}{\hat{q}_i} + \sum_{T: |T| \geq 2, i \in T} \frac{p(a_T)}{\sum_{t \in T} \hat{q}_t} = \sum_{T: i \in T} \frac{p(a_T)}{\sum_{t \in T} \hat{q}_t}.$$

С учётом (3) это даёт $\Sigma_1 + \Sigma_2 \leq 1$. Строгое неравенство здесь имеет место, лишь если оно возникало при использовании (15) либо (3). Но тогда $q_j^{(i)} = 0$ либо $\hat{q}_i = 0$, а потому $q_{ij} = \hat{q}_i q_j^{(i)} = 0$. Утверждение п. (а) получается применением к $\tilde{Q} = (q_{ij}, i \in M, j \in L)$ утверждения 1.

(б) Если $a_T \in A_0$, то множество T одноэлементно и условие п. (б) выполнено тривиальным образом. Если же $b_U = *$, то сумма приобретает вид $\sum_{j \in L} q_j^{(i)}$ и равна 1 при любом i . Утверждение 6 доказано.

Прямое доказательство, не использующее теорему 3, имеется в [6], но оно относится к несколько иному способу введения условной энтропии.

Условие, что X конкретней Y , определяется составом пар (a_T, b_U) , для которых $p(a_T, b_U) > 0$, и не зависит от самих вероятностей. Приведём теперь пример, когда условие выполнимости правила сложения энтропий зависит от вероятностей.

ПРИМЕР. Пусть в произведении XY источников с алфавитами $\{0, 1, *\}$ и $\{0, 1\}$, где $*$ означает неопределённый символ, ненулевыми являются вероятности $p(0, 0)$, $p(0, 1)$, $p(1, 0)$, $p(1, 1)$, $p(*, 0)$, а вероятности остальных пар равны 0. Покажем, что правило сложения энтропий здесь имеет место тогда и только тогда, когда выполнено соотношение

$$p(0, 0)p(1, 1) = p(0, 1)p(1, 0). \quad (32)$$

Источник X порождает символы с вероятностями $p(0) = p(0, 0) + p(0, 1)$, $p(1) = p(1, 0) + p(1, 1)$, $p(*) = p(*, 0)$. Лучшему доопределению \hat{X} соответствуют значения $\hat{q}_0 = \frac{p(0)}{1-p(*)}$, $\hat{q}_1 = \frac{p(1)}{1-p(*)}$, а произведению $\hat{X}Y$ — совместное распределение $p(\hat{0}, 1) = p(0, 1)$, $p(\hat{1}, 1) = p(1, 1)$, $p(\hat{0}, 0) = \hat{q}_0 - p(0, 1)$, $p(\hat{1}, 0) = \hat{q}_1 - p(1, 1)$.

Начнём с проверки условия (б), которое здесь имеет вид $q_0^{(0)} = q_0^{(1)}$. Поскольку источник $\hat{X}Y$ полностью определён, выполнено

$$q_0^{(0)} = p(0|\hat{0}) = \frac{p(\hat{0}, 0)}{\hat{q}_0}, \quad q_0^{(1)} = p(0|\hat{1}) = \frac{p(\hat{1}, 0)}{\hat{q}_1},$$

и равенство превращается в

$$p(\hat{0}, 0)\hat{q}_1 = p(\hat{1}, 0)\hat{q}_0. \quad (33)$$

С использованием приведённых выше выражений оно последовательно преобразуется к

$$(\hat{q}_0 - p(0, 1))\hat{q}_1 = (\hat{q}_1 - p(1, 1))\hat{q}_0,$$

$$p(0, 1)p(1) = p(1, 1)p(0),$$

$$p(0, 1)(p(0, 1) + p(1, 1)) = p(1, 1)(p(0, 0) + p(0, 1)),$$

$$p(0, 1)p(1, 0) = p(0, 0)p(1, 1).$$

Последнее равенство совпадает с (32).

Для проверки условия (а) воспользуемся утверждением 1. Начнём с пары $(0, 0)$. Учитывая, что $q_{00} = q_0^{(0)}\hat{q}_0 = p(\hat{0}, 0)$ и $q_{10} = q_0^{(1)}\hat{q}_1 = p(\hat{1}, 0) = \frac{p(\hat{0}, 0)\hat{q}_1}{\hat{q}_0}$ (см. (33)), преобразуем левую часть (3) применительно к источнику XU и паре $(0, 0)$:

$$\begin{aligned} \frac{p(0, 0)}{q_{00}} + \frac{p(*, 0)}{q_{00} + q_{10}} &= \frac{p(0, 0)}{p(\hat{0}, 0)} + \frac{p(*, 0)}{p(\hat{0}, 0) + \frac{p(\hat{0}, 0)\hat{q}_1}{\hat{q}_0}} \\ &= \frac{1}{p(\hat{0}, 0)}(p(0, 0) + \hat{q}_0 p(*, 0)) = \frac{p(\hat{0}, 0)}{p(\hat{0}, 0)} = 1. \end{aligned}$$

Таким образом, условие (а) для пары $(0, 0)$ выполнено. Для пары $(1, 0)$ оно проверяется аналогично, а случаи пар $(0, 1)$ и $(1, 1)$ тривиальны.

ЛИТЕРАТУРА

1. Бонгард М. М. О понятии «полезная информация» // Пробл. кибернетики. Вып. 9. — М.: Физматгиз, 1963. — С. 71–102.
2. Галлагер Р. Теория информации и надежная связь. — М.: Сов. радио, 1974. — 720 с.
3. Колмогоров А. Н. Алгоритм, информация, сложность. — М.: Знание, 1991. — 48 с.
4. Шоломов Л. А. Информационные свойства функционалов сложности для систем недоопределённых булевых функций // Пробл. кибернетики. Вып. 34. — М.: Наука, 1978. — С. 133–150.
5. Шоломов Л. А. Сжатие частично определённой информации // Нелинейная динамика и управление. Вып. 4. — М.: Физматлит, 2004. — С. 385–399.
6. Шоломов Л. А. О мере информации нечётких и частично-определённых данных // Докл. РАН. — 2006. — Т. 410, № 1. — С. 321–325.
7. Шоломов Л. А. Об эффективном построении протыкающих множеств // Вестн. ТГУ. Прил. — 2007. — № 23. — С. 68–74.
8. Шоломов Л. А. Обобщённое правило сложения энтропий для недоопределённых данных // Докл. РАН. — 2009. — Т. 427, № 1. С. 28–31.
9. Andreev A. E. Complexity of nondeterministic functions // BRICS report series RS-94-2. — February 1994. — 47 p.

10. **Andreev A. E., Clementi A. E. F., Rolim J. D. P.** Hitting sets derandomize BPP // Automata, languages and programming. 23rd Int. Colloquium (Paderborn, Germany, 1996). — Lect. Notes Comp. Sci. Vol. 1099. — Berlin: Springer-Verl., 1996. — P. 357–368.
11. **Linial L., Luby M., Saks M., Zuckerman D.** Efficient construction of a small hitting set for combinatorial rectangles in high dimension // Combinatorica. — 1997. — Vol. 17. — P. 215–234.

Шоломов Лев Абрамович,
e-mail: sholomov@isa.ru

Статья поступила
18 февраля 2010 г.
Переработанный вариант —
26 мая 2010 г.