РОССИЙСКАЯ АКАДЕМИЯ НАУК
ОРДЕНА ЛЕНИНА ИНСТИТУТ ПРИКЛАДНОЙ МАТЕМАТИКИ
ИМЕНИ М.В. КЕЛДЫША

Н.Л. Брошкова, С.В. Попов

СВОЙСТВА ЛОГИЧЕСКОЙ ЭНТРОПИИ

Москва, 2005г.

УДК 004.62

Брошкова Н.Л., Попов С.В. Свойства логической энтропии. Препринт Института прикладной математики им. М.В. Келдыша РАН. Москва, 2005г.

Исследуются свойства логической энтропии, служащей мерой сложности информационных моделей. Демонстрируется отличие логической энтропии от энтропии Теории информации. Доказывается ряд соотношений, позволяющих оценивать энтропию информационных моделей в зависимости от энтропии предметных областей.

Broshkova N.L., Popov S.V. Properties of logic entropy. Preprint of the Keldysh Institute of Applied Mathematics of RAS. Moscow, 2005.

There are researched the characteristic of logical entropy, described the measure of complicity information models. It is demonstrated difference of logical entropy from entropy of the Theories of information. It is proved correlation between entropy of the information model and entropy of the application domain.

Введение. Содержательное обоснование меры неопределенности информационных моделей было введено в [1]. В [2] приводится формальное определение логической энтропии, и обсуждаются некоторые ее свойства и их содержательные интерпретации. В этой работе продолжено исследование логической энтропии, как меры сложности информационных моделей.

1. О логической энтропии. Сформулируем и докажем ряд свойств логической энтропии.

Очевидна следующая теорема.

***Теорема* 1.** *Если для функции* $f(\boldsymbol{y}, \boldsymbol{z})$ *доли* $p_y(i)$ *классов* $\boldsymbol{y}$*-эквивалентности равны, то энтропия* H_y *равна логарифму от числа классов эквивалентности* (*или, что аналогично, от величины* $\boldsymbol{y}$*-сечения*).

Поэтому, *если имеются только два класса с одинаковыми долями, то энтропия равна* 1; *если один класс, то энтропия равна* 0.

Основные свойства энтропии формулируются следующим образом.

***Теорема* 2.** *При фиксированном числе всех путей бинарной программы из истока в* $\boldsymbol{y}$*-сечение, которое имеет* k *узлов, энтропия* H_y *максимальна, когда все доли* $p_y(i)$ *одинаковы и равны* k^{-1}.

Доказательство этого свойства вытекает из того, что математическое ожидание $\mathbf{M}[\log |t_y(i)|]$ минимально при равных значениях $p_y(i)$.

***Теорема* 3.** *Если* $H_y = k$, *то число узлов* $\boldsymbol{y}$*-сечения бинарной программы не менее* 2^k.

Доказательство. Пусть в $\boldsymbol{y}$-сечении бинарной программы имеется $h = 2^n < 2^k$ узлов. При фиксированном числе путей из истока в $\boldsymbol{y}$-сечение энтропия H_y максимальна при равных долях $p_y(i)$. Поэтому энтропия H_y не превосходит величины $-\sum_{i=1,h} h^{-1} \log h^{-1} = \log h < k$. Противоречие.

Теорема доказана.

Следствие. *Чтобы функция* $f(\boldsymbol{y}, \boldsymbol{z})$ *обладала энтропией* $H_y = k$, *число переменных* $\boldsymbol{y}$ *должно быть не менее* k.

***Пример* 1.** Пусть $\boldsymbol{y}$-сечение бинарной программы для функции $f(\boldsymbol{y}, \boldsymbol{z})$ имеет k узлов, а для функции $g(\boldsymbol{y}, \boldsymbol{z})$ – h узлов. Верхняя граница энтропии $H^f_{\boldsymbol{y}}$ равна $log\ k$, а $H^g_{\boldsymbol{y}}$ - $log\ h$. Эти значения достигаются в случае, когда $p_{\boldsymbol{y}}(i) = k^{-1}$ для функции f и $p_{\boldsymbol{y}}(i) = h^{-1}$ для g. Потому функция, обладающая большим $\boldsymbol{y}$-сечением, имеет большую верхнюю границу энтропии. Это согласуется с содержательной интерпретацией логической энтропии как меры неопределенности вычислительного процесса. Действительно, чем больше сечение бинарной программы, тем больше неопределенность того, какой вычислитель осуществит вычисление при заданных входных значениях.

Пусть разложения функции $f(\boldsymbol{y}, \boldsymbol{z})$ по переменным $\boldsymbol{y}$ выглядят следующим образом: $\vee_{i=1,k}\ [\boldsymbol{y}^{\sigma^i}]\ f(\boldsymbol{\sigma}^i_1, \boldsymbol{z})$, а по переменным $\boldsymbol{z}$ так $\vee_{j=1,h}\ [\boldsymbol{z}^{\lambda^j}]\ f(\boldsymbol{y}, \boldsymbol{\lambda}^j_1)$, где в квадратных скобках приведены дизъюнкты, определяемые одним классом эквивалентности, и $\boldsymbol{\sigma}^i = \{\boldsymbol{\sigma}_1^i, \boldsymbol{\sigma}_2^i, \ldots, \boldsymbol{\sigma}_m^i\}$, $\boldsymbol{\lambda}^j = \{\boldsymbol{\lambda}_1^j, \boldsymbol{\lambda}_2^j, \ldots, \boldsymbol{\lambda}_n^j\}$, $i = 1, 2, \ldots, k$, $j = 1, 2, \ldots, h$.

Разложение по переменным $\boldsymbol{yz}$ выглядит так:

$$f(\boldsymbol{y}, \boldsymbol{z}) = \vee_{i=1,k\ j=1,h}\ [\boldsymbol{y}^{\sigma^i}\boldsymbol{z}^{\lambda^j}]\ f(\boldsymbol{\sigma}^i_1, \boldsymbol{\lambda}^j_1) = \vee_{i=1,k\ j=1,h}\ [\boldsymbol{y}^{\sigma^i}\boldsymbol{z}^{\lambda^j}]\ f_{ij}.$$

Здесь квадратными скобками $[\boldsymbol{y}^{\sigma^i}\boldsymbol{z}^{\lambda^j}]$ обозначена конъюнкция дизъюнктов, соответствующих i-му $\boldsymbol{y}$-классу и j-му $\boldsymbol{z}$-классу, f_{ij} получена из f подстановкой $\boldsymbol{y}$-набора $\boldsymbol{\sigma}^i_1$ и $\boldsymbol{z}$-набора $\boldsymbol{\lambda}^j_1$. Если f представляет всюду определенную вычислимую функцию, то среди f_{ij}, $i = 1, 2, \ldots, k$, $j = 1,2, .., h$ нет тождественно нулевых функций.

Справедлива следующая

***Теорема* 4.** *Если логическая функция $f(\boldsymbol{y}, \boldsymbol{z})$ представляет всюду определенную вычислимую функцию, то верно неравенство*

$$H_{\boldsymbol{yz}} \le H_{\boldsymbol{y}} + H_{\boldsymbol{z}}.$$

Доказательство. Обозначим $p_y(i)$ долю $\boldsymbol{y}$-наборов из i-го класса $\boldsymbol{y}$-эквивалентности, $p_z(j)$ – долю $\boldsymbol{z}$-наборов из j-го класса $\boldsymbol{z}$-эквивалентности, $p(i, j)$ – долю $\boldsymbol{yz}$-наборов, $\boldsymbol{y}$-компоненты которых принадлежат i-му классу $\boldsymbol{y}$-эквивалентности, а $\boldsymbol{z}$-компоненты - j-му классу $\boldsymbol{z}$-эквивалентности. Так как f представляет всюду определенную функцию, то для всех пар (i, j) справедливы равенства $p(i, j) = p_y(i)\, p_z(j)$ и $\sum_{(i,\, j)} p(i, j) = 1$, где суммирование ведется по всем $i = 1, 2, \ldots, k$, и $j = 1, 2, \ldots, h$.

Пусть $\boldsymbol{yz}$-сечение бинарной программы содержит m узлов и к множеству $\boldsymbol{yz}$-наборов из q-го $\boldsymbol{yz}$-класса A_q, $q = 1, 2, \ldots, m$, относятся $\boldsymbol{yz}$-наборы, характеризующиеся определенными значениями пар (i, j). Тогда $p_{yz}(q)$ есть доля $\boldsymbol{yz}$-наборов, определяемых q-м $\boldsymbol{yz}$-классом, и эта доля вычисляется как сумма

$$p_{yz}(q) = \textstyle\sum_{(i,\, j)\in A_q} p(i, j).$$

Из равенства $p(i, j) = p_y(i)\, p_z(j)$ вытекает, что:

$$-\textstyle\sum_{i,\, j} p(i, j) \log p(i, j) = -\sum_{i,\, j} p_y(i)\, p_z(j) \log p_y(i) - \sum_{i,\, j} p_y(i)\, p_z(j) \log p_z(j) =$$

$$= -\textstyle\sum_{i} p_y(i) \log p_y(i) - \sum_{j} p_z(j) \log p_z(j) = H_y + H_z.$$

Рассмотрим условную случайную величину $x|A_q$, которая принимает значения (i, j) из класса A_q с вероятностью $P[x = (i, j)|(i, j) \in A_q]$. По формуле условной вероятности имеем $P[x = (i, j)|(i, j) \in A_q] = P[x = (i, j)]/P[(i, j)\in A_q] = p(i, j)/p_{yz}(q)$. Энтропия этой случайной равна

$$-\textstyle\sum_{(i,\, j)|(i,\, j)\in A_q} p(i, j)/\, p_{yz}(q) \log p(i, j)/\, p_{yz}(q).$$

Так как энтропия любой случайной величины не отрицательная, то

$$-\textstyle\sum_{(i,\, j)|(i,\, j)\in A_q} p(i, j)/\, p_{yz}(q) \log p(i,j)/\, p_{yz}(q) \geq 0.$$

В силу того, что $p_{yz}(q) > 0$ последнее неравенство можно переписать так:

$$-\textstyle\sum_{(i,\, j)|(i,\, j)\in A_q} p(i, j) \log p(i, j)/\, p_{yz}(q) \geq 0.$$

Откуда вытекают соотношения:

$$-\textstyle\sum_{(i,\, j)|(i,\, j)\in A_q} p(i, j) \log p(i, j) \geq -\sum_{(i,\, j)|(i,\, j)\in A_q} p(i, j) \log p_{yz}(q) = -\, p_{yz}(q) \log p_{yz}(q)$$

Суммируя обе части неравенства по всем классам $\boldsymbol{yz}$-эквивалентности, получаем, что

$$-\sum_{(i,\, j)} p(i, j) \log p(i, j) \geq -\sum_q p_{\boldsymbol{yz}}(q) \log p_{\boldsymbol{yz}}(q).$$

То есть $H_{\boldsymbol{yz}} \leq H_{\boldsymbol{y}} + H_{\boldsymbol{z}}$.

Теорема доказана.

Докажем теперь утверждение, анонсированное в [2]. Оно касается соотношения между суммой $H_1 + H_2$ неопределенностей, характеризующих состояние уже спроектированной информационной системы и неопределенности H_0 предметной области. В терминах бинарной программы и логической энтропии это выглядит следующим образом.

Пусть для логической функции $f(\boldsymbol{y}, \boldsymbol{z})$ переменные $\boldsymbol{y}$ определяют логическую энтропию $H_{\boldsymbol{y}} = -\sum_{i=1,k} p_{\boldsymbol{y}}(i) \log p_{\boldsymbol{y}}(i)$, и H_0 есть двоичный логарифм от мощности множества T ее единичных означиваний. Введем для $\boldsymbol{y}$-сечения бинарной программы новую величину H_2, которую назовем *остаточной* энтропией: $H_2 = \sum_{i=1,k} p_{\boldsymbol{y}}(i) \log T_i$, где T_i есть мощность множества единичных означиваний функции, соответствующей i-му узлу $\boldsymbol{y}$-сечения.

Справедлива

***Лемма* 5**. *Пусть $a = b + c$. Тогда верно неравенство*

$$1+(1/2)(\log b + \log c) \leq \log a.$$

Доказательство. Пусть $b \leq c$, и $b = c - x$ для некоторого не отрицательного x. Искомое неравенство следует из неравенства $1+(\log (c - x) + \log c) \leq 2 \log (2c - x)$, которое вытекает из $\log 2(c - x) c \leq \log (2c - x)^2$. Последнее неравенство следует из легко проверяемого неравенства $2(c - x)c \leq (2c - x)^2$.

Лемма доказана.

Справедлива

***Теорема* 6**. *Для логической функции $f(\boldsymbol{y}, \boldsymbol{z})$ имеет место неравенство*

$$H_{\boldsymbol{y}} + H_2 \leq H_0.$$

Доказательство проведем индукцией по h - мощности множества переменных $\boldsymbol{y}$.

<u>*Базис индукции*</u>, когда $h = 0$, элементарен, так как в этом случае $H_{\boldsymbol{y}} = 0$ и $H_{\boldsymbol{2}} = H_0$.

<u>*Индукционный переход*</u>. Пусть для $\boldsymbol{y}$-сечения, когда множество $\boldsymbol{y}$ содержит h переменных, теорема верна, и мы продолжаем построение бинарной программы для $f(\boldsymbol{y}, \boldsymbol{z})$, означивая новую переменную z. Допустим, что в $\boldsymbol{y}z$-сечении имеется в точности m узлов и T_j есть мощность множества единичных означиваний функции, приписанной его j-му узлу.

Допустим вначале, что такое продолжение не приводит к склейке узлов в $\boldsymbol{y}z$-сечении. В этом случае для каждого узла j $\boldsymbol{y}z$-сечения доля $p_{yz}(j)$ путей, ведущих из истока в этот узел, равна либо $(1/2)p_y(i)$ либо $p_y(i)$ для определенного узла i $\boldsymbol{y}$-сечения. Это следует из определения бинарной программы.

Но тогда сумма

$$\sum_{j=1,m} p_{yz}(j)(- \log p_{yz}(j) + \log T_j)$$

представима в виде двух сумм:

$$\sum{}^1 p_{yz}(j)(- \log p_{yz}(j) + \log T_j) \text{ и } \sum{}^2 p_{yz}(j)(- \log p_{yz}(j) + \log T_j).$$

Здесь первое суммирование осуществляется по тем узлам $\boldsymbol{y}z$-сечения, для которых доли путей, ведущих в эти узлы, представляют собой половину от долей путей, ведущих в соответствующие узлы $\boldsymbol{y}$-сечения. Второе - по тем узлам, для которых доли путей, ведущих в них, совпадают с долями путей, ведущих в соответствующие узлы $\boldsymbol{y}$-сечения. Это позволяет перейти к суммированию по узлам $\boldsymbol{y}$-сечения.

В результате первая сумма выглядит так:

$$\sum_i p_y(i) - \log (p_y(i)/2) + ½\, p_y(i) \log T_{j1} + ½\, p_y(i) \log T_{j2}$$

Здесь j_1 и j_2 это те узлы $\boldsymbol{y}z$-сечения, которые образованы из одного i-го узла $\boldsymbol{y}$-сечения. Преобразуя эту сумму, получаем

$$\sum_i p_y(i)\, (- \log p_y(i) + 1 + ½(\log T_{j1} + \log T_{j2})).$$

По Лемме 5, $1 + ½(log\ T_{j_1} + log\ T_{j_2}) \le log\ T_i$, где T_i есть мощность множества единичных означиваний функции, приписанной i-узлу $\boldsymbol{y}$-сечения. Следовательно, эта сумма не превосходит величины

$$\sum\nolimits_i^{\,1} p_y(i)\ (-\ log\ p_y(i) + log\ T_i),$$

где суммирование ведется по тем же узлам.

В силу того, что во второй сумме каждому узлу $\boldsymbol{y}z$-сечения соответствует в точности один узел $\boldsymbol{y}$-сечения, сумму

$$\sum\nolimits^{2}\ p_{yz}(j)(-\ log\ p_{yz}(j) + log\ T_j)$$

можно представить так:

$$\sum\nolimits_i^{\,2} p_y(i)(-\ log\ p_y(i) + log\ T_i).$$

Здесь суммирование ведется по соответствующим узлам $\boldsymbol{y}$-сечения, для каждого узла $\boldsymbol{y}z$-сечения указывается в точности один соответствующий узел $\boldsymbol{y}$-сечения.

Складывая $\sum\nolimits_i^{\,1} p_y(i)\ (-\ log\ p_y(i) + log\ T_i) + \sum\nolimits_i^{\,2} p_y(i)(-\ log\ p_y(i) + log\ T_i)$, получим, что суммирование ведется по всем узлам $\boldsymbol{y}$-сечения. Следовательно, эта сумма не превосходит величины H_0. В частном случае теорема доказана.

Приведем теперь доказательство для общего случая.

Пусть при переходе к $\boldsymbol{y}z$-сечению два различных узла i_1 и i_2 $\boldsymbol{y}$-сечения порождают эквивалентные функции. В результате можно считать, что в $\boldsymbol{y}z$-сечении склеились два узла j_1 и j_2, которые в итоге превратились в один узел j. Тогда соответствующая доля выглядит так: $p_{yz}(j) = p_{yz}(j_1) + p_{yz}(j_2)$. Мощности множеств единичных означиваний функций, соответствующих трем узлам j, j_1 и j_2, совпадают и пусть равны T_j.

Легко проверить неравенство

$$(p_{yz}(j_1)+p_{yz}(j_2))(-\log(p_{yz}(j_1)+p_{yz}(j_1))+\log T_j) \le$$
$$p_{yz}(j_1)(-log p_{yz}(j_1)+log T_j)+p_{yz}(j_2))(-log(p_{yz}(j_2)+log T_j).$$

Следовательно, склейка узлов $\boldsymbol{y}z$-сечения не приводит к увеличению левой части искомого неравенства.

Теорема доказана.

В итоге на промежуточном этапе построения информационной модели наши знания, по сравнению с исходными, увеличились на величину

$$H_0 - (H_y + H_2).$$

Введем следующее обозначение для логической функции $f(\boldsymbol{y}, \boldsymbol{z})$.

При построении бинарной программы увеличение множества означиваемых переменных не всегда приводит к увеличению энтропии. Чтобы это показать, приведем следующие рассуждения.

Пусть $q(i, j)$ – доля $\boldsymbol{yz}$-наборов, таких, что одновременно их $\boldsymbol{y}$-наборы принадлежат i-му классу $\boldsymbol{y}$-эквивалентности, а сами они принадлежат j-му классу $\boldsymbol{yz}$-эквивалентности. В терминах бинарной программы $q(i, j)$ есть доля путей, проходящих из истока в j-й узел $\boldsymbol{yz}$-сечения, одновременно проходя через i-й узел $\boldsymbol{y}$-сечения. Справедливы равенства:

$$p_y(i) = \sum_{j=1,h} q(i, j), \ \ p_{\boldsymbol{yz}}(j) = \sum_{i=1,k} q(i, j).$$

Энтропия H_y функции $f(\boldsymbol{y}, \boldsymbol{z})$ равна

$$-\sum_{i=1,k} p_y(i) \log p_y(i) = -\sum_{i=1,k} (\sum_{j=1,h} q(i, j)) \log p_y(i) = -\sum_{i=1,k} (\sum_{j=1,h} q(i, j) \log p_y(i)) =$$

$$= -\sum_{i=1,k} \sum_{j=1,h} q(i, j) \log p_y(i) = -\sum_{i=1,k \ j=1,h} q(i, j) \log p_y(i).$$

Выразим энтропию $H_{\boldsymbol{yz}}$.

$$-\sum_{j=1,h} p_{\boldsymbol{yz}}(j) \log p_{\boldsymbol{yz}}(j) = -\sum_{j=1,h} (\sum_{i=1,k} q(i, j)) \log p_{\boldsymbol{yz}}(j) = -\sum_{j=1,h} (\sum_{i=1,k} q(i, j) \log p_{\boldsymbol{yz}}(j)) =$$

$$= -\sum_{i=1,k} \sum_{j=1,h} q(i, j) \log p_{\boldsymbol{yz}}(j) = -\sum_{i=1,k \ j=1,h} q(i, j) \log p_{\boldsymbol{yz}}(j).$$

Разность $H_{\boldsymbol{yz}} - H_y$ равна

$$\sum_{i=1,k \ j=1,h} q(i, j) \log p_y(i) - \sum_{i=1,k \ j=1,h} q(i, j) \log p_{\boldsymbol{yz}}(j) =$$

$$= \sum_{i=1,k \ j=1,h} q(i, j) (\log p_y(i) - \log p_{\boldsymbol{yz}}(j)) = \sum_{i=1,k \ j=1,h} q(i, j) \log (p_y(i) / p_{\boldsymbol{yz}}(j)).$$

Величину $\log (p_y(i)/p_{\boldsymbol{yz}}(j))$ можно рассматривать как случайную с распределением $q(i, j)$. Тогда разность $H_{\boldsymbol{yz}} - H_y$. есть ее среднее значение. Если она больше нуля, то эффективное ***yz***-сечение больше эффективного ***y***-сечения. Так как ширина эффективного сечения определяет сложность представления исходной функции через ее подфункции, то положительная разность обозначает, что функция выражается сложнее через переменные ***yz***, чем от ***y***.

2. Не зависимые переменные. В теории информации доказывается, что если *система состоит из независимых подсистем, то ее энтропия представляет собой сумму энтропий ее подсистем*. Аналогичным свойством обладает логическая энтропия: если логическая функция зависит от независимых аргументов, то суммарная энтропия этих аргументов равна сумме энтропий каждого из них.

Чтобы уточнить понятия независимости переменных логической функции, введем ряд определений и докажем несколько утверждений.

Будем говорить, что у функции $f(\boldsymbol{y}, \boldsymbol{z})$ переменные ***z*** *не зависят от переменных* ***y***, если в разложении $f(\boldsymbol{y}, \boldsymbol{z}) = \vee_{i=1,k\ j=1,h} [\boldsymbol{y}^{\sigma^i} \boldsymbol{z}^{\lambda^j}]$ каждая функция $f_{ij} = u_i \wedge v_j$, $i = 1, 2, \ldots, k$, $j = 1, 2, \ldots, h$. В терминах матрицы M_f (см. рис.1) независимость переменных ***z*** от ***y*** обозначает, что для каждого ее столбца (каждой строки) зафиксирована одна функция u_i (v_j), входящая в конъюнкцию на пересечении этой строки (столбца) со всеми другими столбцами (строками).

$\boldsymbol{z}$ / $\boldsymbol{y}$	λ^1	λ^2	λ^3	…
σ^1	$u_1 \wedge v_1$	$u_1 \wedge v_2$	$u_1 \wedge v_3$	…
σ^2	$u_2 \wedge v_1$	$u_2 \wedge v_2$	$u_2 \wedge v_3$	…
σ^3	$u_3 \wedge v_1$	$u_3 \wedge v_2$	$u_3 \wedge v_3$	…
…	…	…	…	…

Рис. 1

Просто доказывается

***Лемма* 7.** *Если функция* $f(\boldsymbol{y}, \boldsymbol{z}) = f_1(\boldsymbol{y}) \wedge f_2(\boldsymbol{z})$, *где* $f_1(\boldsymbol{y})$ *не содержит переменных* $\boldsymbol{z}$, *а* $f_2(\boldsymbol{z})$ - *переменных* $\boldsymbol{y}$, *то переменные* $\boldsymbol{z}$ *не зависят от* $\boldsymbol{y}$, *и наоборот, переменные* $\boldsymbol{y}$ *не зависят от* $\boldsymbol{z}$.

Справедлива

***Лемма* 8.** *Если у функции* $f(\boldsymbol{y}, \boldsymbol{z})$ *переменные* $\boldsymbol{z}$ *не зависят от* $\boldsymbol{y}$, *то она представима в виде конъюнкции* $f_1(\boldsymbol{y}) \wedge f_2(\boldsymbol{z})$, *где* $f_1(\boldsymbol{y})$ *не содержит переменных* $\boldsymbol{z}$, *а* $f_2(\boldsymbol{z})$ - *переменных* $\boldsymbol{y}$.

Доказательство. Представим функцию $f(\boldsymbol{y}, \boldsymbol{z})$ в таком виде:

$$\vee_{i=1,k\ j=1,h} [\boldsymbol{y}^{\sigma^i} \boldsymbol{z}^{\lambda^j}]\, f_{ij}.$$

В силу независимости переменных $\boldsymbol{z}$ от $\boldsymbol{y}$ получаем равенства:

$$f(\boldsymbol{y}, \boldsymbol{z}) = \vee_{i=1,k} [\boldsymbol{y}^{\sigma^i}] \wedge (\vee_{j=1,h} [\boldsymbol{z}^{\lambda^j}]\, (u_i \wedge v_j)) =$$

$$= \vee_{i=1,k} [\boldsymbol{y}^{\sigma^i}] \wedge u_i \wedge (\vee_{j=1,h} [\boldsymbol{z}^{\lambda^j}]\, v_j) = \vee_{i=1,k} [\boldsymbol{y}^{\sigma^i}] \wedge u_i \wedge f_2(\boldsymbol{z}) =$$

$$= f_2(\boldsymbol{z}) \wedge (\vee_{i=1,k} [\boldsymbol{y}^{\sigma^i}] \wedge u_i) = f_1(\boldsymbol{y}) \wedge f_2(\boldsymbol{z})$$

Лемма доказана.

Следствие. *Если у функции* $f(\boldsymbol{y}, \boldsymbol{z})$ *переменные* $\boldsymbol{z}$ *не зависят от* $\boldsymbol{y}$, *то переменные* $\boldsymbol{y}$ *также не зависят от* $\boldsymbol{z}$.

Основываясь на этом, будем говорить просто о *независимых* переменных.

С другой стороны, верна

***Теорема* 9.** *Если у функции* $f(\boldsymbol{y}, \boldsymbol{z})$ *переменные* $\boldsymbol{y}$, $\boldsymbol{z}$ *не зависимы, то ее нельзя представить в виде дизъюнкции* $g(\boldsymbol{y}) \vee h(\boldsymbol{z})$, *где* $g(\boldsymbol{y})$ *не содержит переменных* $\boldsymbol{z}$, *и* $h(\boldsymbol{z})$ - *переменных* $\boldsymbol{y}$.

Доказательство. Так как переменные $\boldsymbol{y}$ и $\boldsymbol{z}$ не зависимы, то функция $f(\boldsymbol{y}, \boldsymbol{z})$ определяет матрицу M_f, как на рис. 1. Функция $f(\boldsymbol{y}, \boldsymbol{z})$ не тождественная константа. Поэтому все функции в клетках матрицы M_f попарно не эквивалентны. Пусть $f(\boldsymbol{y}, \boldsymbol{z}) = g(\boldsymbol{y}) \vee h(\boldsymbol{z})$, и $g(\boldsymbol{y})$ не содержит переменных $\boldsymbol{z}$, а $h(\boldsymbol{z})$ - переменных $\boldsymbol{y}$. Допустим, что функция $g(\boldsymbol{y})$ истинна при некотором означивании $\boldsymbol{\sigma}_y$ ее переменных. Но тогда все $\boldsymbol{yz}$–наборы вида $\boldsymbol{\sigma}_y\boldsymbol{\sigma}_z$, где $\boldsymbol{\sigma}_z$ все возможные $\boldsymbol{z}$–наборы, принадлежат одному классу эквивалентности. Это обозначает, что в матрице M_f все функции в строке, характеризующейся одним $\boldsymbol{y}$–набором $\boldsymbol{\sigma}_y$, эквивалентны. Противоречие с условием о независимости переменных $\boldsymbol{y}$ и $\boldsymbol{z}$.

Теорема доказана.

Отметим, что если функция $f(\boldsymbol{y}, \boldsymbol{z})$ представлена в к.н.ф., то независимые переменные $\boldsymbol{y}$, $\boldsymbol{z}$ могут принадлежать одному дизъюнкту, но таких дизъюнктов должно быть, по меньшей мере, два.

***Теорема* 10.** *Если у функции* $f(\boldsymbol{y}, \boldsymbol{z})$ *переменные* $\boldsymbol{y}$ и $\boldsymbol{z}$ *не зависимы, то* $H_{\boldsymbol{yz}} = H_{\boldsymbol{y}} + H_{\boldsymbol{z}}$.

Доказательство. Величина $p_{\boldsymbol{yz}|\boldsymbol{y}}(j \mid i)$ одинакова для каждого фиксированного i и всех узлов j, достижимых из i. Более того, $p_{\boldsymbol{yz}|\boldsymbol{y}}(j \mid i) = p_{\boldsymbol{z}}(j')$, $j, j' = 1, 2, \ldots, k$ при определенном соответствии узлов j и j' $\boldsymbol{yz}$-сечения и $\boldsymbol{z}$-сечения. Но тогда $p_{\boldsymbol{yz}}(j) = p_{\boldsymbol{z}}(j')\, p_{\boldsymbol{y}}(i)$. Следовательно,

$$H_{\boldsymbol{yz}} = \sum_j p_{\boldsymbol{yz}}(j) \log p_{\boldsymbol{yz}}(j) = \sum_{j,i} p_{\boldsymbol{y}}(i)\, p_{\boldsymbol{z}}(j') \log p_{\boldsymbol{y}}(i)\, p_{\boldsymbol{z}}(j') = H_{\boldsymbol{y}} + H_{\boldsymbol{z}}.$$

Теорема доказана.

Содержательная трактовка аддитивности энтропии достаточно понятна. Если два множества аргументов независимы, то они не влияют друг на друга, так как разложение по одному множеству аргументов никак не сказывается на наших знаниях о разложении по другому. Понятно, что в общем случае аддитивность энтропии места не имеет, так как не каждая пара (i, j) индексов матрицы M_f определяет в точности один класс $\boldsymbol{yz}$-эквивалентности.

3. Условная энтропия. В этом разделе введем определение и рассмотрим свойства условной энтропии, которая определяется так же, как это делается в Теории информации.

Напомним обозначения, введенные при определении логической энтропии для функции $f(\boldsymbol{y}, \boldsymbol{z})$:

$p_{yz|y}(j \mid i)$ есть доля путей, ведущих из i-го узла $\boldsymbol{y}$-сечения в j-й узел $\boldsymbol{yz}$-сечения среди всех путей из i-го узла $\boldsymbol{y}$-сечения в $\boldsymbol{yz}$-сечение;

$p_y(i)$ – доля путей из истока в i-й узел $\boldsymbol{y}$-сечения среди всех путей из истока в $\boldsymbol{y}$-сечение;

$p_z(i)$ - доля путей из истока в i-й узел $\boldsymbol{z}$-сечения среди всех путей из истока в $\boldsymbol{z}$-сечение;

$p_{yz}(i)$ –доля путей из истока в i-й узел $\boldsymbol{yz}$-сечения среди всех путей из истока в $\boldsymbol{yz}$-сечение.

Пусть $p_{yz}(i, j) = p_{yz|y}(j \mid i)\, p_y(i)$. Это есть доля путей, проходящих из истока через i-й узел $\boldsymbol{y}$-сечения, которые ведут в j-й узел $\boldsymbol{yz}$-сечения.

Из этого определения следует равенство $p_y(i) = \sum_j p_{yz}(i, j)$.

Аналогично вводятся соответствующие обозначения, когда рассматривается не бинарная программа, а означивания переменных.

Рассмотрим следующую задачу.

Пусть для функции $f(\boldsymbol{y}, \boldsymbol{z})$ необходимо установить класс $\boldsymbol{yz}$-эквивалентности, которому принадлежит некоторый $\boldsymbol{yz}$-набор. Если не пользоваться никакой дополнительной информацией, то неопределенность этого события вычисляется как энтропия аргументов $\boldsymbol{yz}$. Допустим, теперь известно, каким $\boldsymbol{y}$-классом порождается этот $\boldsymbol{yz}$-набор. Поэтому при известном $\boldsymbol{y}$-классе доли порождаемых им $\boldsymbol{yz}$-классов отличаются от долей $\boldsymbol{yz}$-классов всей функции. Эти доли могут рассматриваться как условные доли $p(\boldsymbol{yz}|\boldsymbol{y})$ $\boldsymbol{yz}$-классов, когда известно, каким $\boldsymbol{y}$-классом они определяются. Эти рассуждения приводят к понятию условной энтропии:

$$H_{yz|\xi(y)=i} = - \Sigma_j\, p_{yz|y}(j \mid i)\, log\, p_{yz|y}(j \mid i) \text{ и}$$

$$H_{yz|y} = - \Sigma_{i,j}\, p_y(i)\, p_{yz|y}(j \mid i)\, log\, p_{yz|y}(j \mid i) = - \Sigma_{i,j}\, p_{yz}(i, j)\, log\, p_{yz|y}(j \mid i).$$

Условная энтропия обладает такими свойствами.

***Теорема* 11.** $H_{yz|y} \le H_{\boldsymbol{z}}$.

Доказательство. Пусть i-ый класс $\boldsymbol{y}$-эквивалентности порождает h классов $\boldsymbol{yz}$-эквивалентности, которые занумеруем 1, 2, …, h. Очевидно, что h не больше числа H классов $\boldsymbol{z}$-эквивалентности. В терминах матрицы M_f в ее i-ой строке одному классу $\boldsymbol{yz}$-эквивалентности соответствует несколько клеток, в то время как одному классу $\boldsymbol{z}$-эквивалентности соответствует в точности одна клетка. Но тогда энтропия $H_{\boldsymbol{yz}|\xi(y) = i}$ меньше, чем энтропия $H_{\boldsymbol{z}}$, так как для некоторых классов $j = 1, 2, \ldots, h$ доли $p_{\boldsymbol{yz}|\boldsymbol{y}}(j \mid i)$ представляют собой суммарные доли нескольких классов $\boldsymbol{z}$-эквивалентности.

Теорема доказана.

***Теорема* 12.** *Если аргументы* $\boldsymbol{y}$ *и* $\boldsymbol{z}$ *независимы, то* $H_{\boldsymbol{yz}|\boldsymbol{y}} = H_{\boldsymbol{z}}$.

Доказательство. При независимых аргументах $\boldsymbol{y}$ и $\boldsymbol{z}$ верны следующие равенства $p_{\boldsymbol{yz}|\boldsymbol{y}}(1|\, i) = p_{\boldsymbol{yz}|\boldsymbol{y}}(2|\, i) = \ldots = p_{\boldsymbol{yz}|\boldsymbol{y}}(h|\, i)$, $i = 1, 2, \ldots, k$, так как доли путей в $\boldsymbol{yz}$-сечение, проходящие через фиксированный i-ый узел $\boldsymbol{y}$-сечения, не зависят от i. Поэтому $p_{\boldsymbol{yz}|\boldsymbol{y}}(j|\, i) = p_{\boldsymbol{z}}(j')$ при определенном соответствии между узлами $\boldsymbol{yz}$-сечения и $\boldsymbol{z}$-сечения. В этом случае

$$H_{\boldsymbol{yz}|\xi(y) = i} = - \Sigma_j\, p_{\boldsymbol{yz}|\boldsymbol{y}}(j \mid i) \log p_{\boldsymbol{yz}|\boldsymbol{y}}(j \mid i) = H_{\boldsymbol{z}} \text{ и } H_{\boldsymbol{yz}|\boldsymbol{y}} = \Sigma_i\, p_{\boldsymbol{y}}(i)\, H_{\boldsymbol{z}} = H_{\boldsymbol{z}}.$$

Теорема доказана.

Таким образом, в случае независимых аргументов $\boldsymbol{y}$ и $\boldsymbol{z}$ условная энтропия $H_{\boldsymbol{zy}|\boldsymbol{y}}$ совпадает с безусловной $H_{\boldsymbol{z}}$. Поэтому знание о порождении набора определенным $\boldsymbol{y}$-классом не влияет на наши знания о принадлежности $\boldsymbol{yz}$-набора тому или иному $\boldsymbol{yz}$-классу.

Справедлива

***Лемма* 13**. *Если* r_i, q_i , $i = 1, 2, \ldots, n$, *– дискретные распределения случайных величин, то справедливо неравенство*

$$\Sigma_{i = 1, n}\, r_i \log (r_i / q_i) \geq 0.$$

Докажем следующее утверждение.

***Теорема* 14**. $H_{\boldsymbol{yz}|\boldsymbol{y}} \leq H_{\boldsymbol{yz}}$.

Доказательство. Искомое неравенство преобразуется в следующее

$$- \Sigma_{i,j}\, p_{yz}(i, j) \log p_{yz|y}(j \mid i) \le - \Sigma_j\, p_{yz}(j) \log p_{yz}(j).$$

Для его доказательством воспользуемся неравенством из Леммы 11, положив $r_j = p_{yz|y}(j \mid i)$, $q_j = p_{yz}(j)$. Тогда неравенство из Леммы 11 превращается в такое:

$$\Sigma_{j = 1, n}\, p_{yz|y}(j \mid i) \log (p_{yz|y}(j \mid i) / p_{yz}(j)) \ge 0.$$

Преобразуя, получаем

$$\Sigma_{j = 1, n}\, p_{yz|y}(j \mid i) \log p_{yz|y}(j \mid i) \ge \Sigma_{j = 1, n}\, p_{yz|y}(j \mid i) \log\ p_{yz}(j)).$$

Так как неравенство справедливо для каждого i, то умножая на $p_y(i)$ и суммируя по i, получаем неравенство

$$\Sigma_{j,i}\, p_{yz|y}(j \mid i)\ p_y(i) \log p_{yz|y}(j \mid i) \ge \Sigma_{j,i}\, p_{yz|y}(j \mid i)\, p_y(i) \log\ p_{yz}(j)).$$

Используя равенство $p_{yz}(i, j) = p_{yz|y}(j \mid i)\, p_y(i)$, преобразуем левую часть неравенства в $\Sigma_{j,i}\, p_{yz}(i, j) \log p_{yz|y}(j \mid i)$. Используя равенство $\Sigma_i\, p_{yz|y}(j \mid i)\, p_y(i) = p_{yz}(j)$, правую часть неравенства преобразуем в $\Sigma_j\, p_{yz}(j) \log\ p_{yz}(j))$. Из этого следует искомое неравенство.

Теорема доказана.

Пример* 2.** Верхняя граница энтропии $H_{yz|\xi(y) = i}$ достижима и равна $\log k$, если $p_{yz|y}(j \mid i) = k^{-1}$ при всех значениях j. Поэтому, если сравнивать верхние границы частной энтропии при одинаковых значениях долей $p_{yz|y}(j \mid i)$, то она тем больше, чем больше число узлов ***yz-сечения достижимо из i-го узла ***y***-сечения. Это согласуется с содержательным представлением о неопределенности вычислительного процесса, представляемого бинарной программой. Действительно, число возможных продолжений вычисления из i-го узла ***y***-сечения будет больше при большем числе достижимых вычислителей (т.е. узлов ***yz***-сечения) из i-го узла ***y***-сечения.

***Пример* 3.** Из того, что математическое ожидание случайной величины увеличивается при увеличении ее значений и при одинаковом распределении следует, что условная энтропия $H_{yz|y}$ возрастает при возрастании частных условных энтропий $H_{yz|\xi(y) = i}$. Это согласуется с содержательным представлением о неопределенности вычислительного процесса. Действительно, если число достижимых узлов $\boldsymbol{yz}$-сечения из каждого узла $\boldsymbol{y}$-сечения увеличивается, то при прочих равных условиях возрастает и усредненное значение

$$\Sigma_i\, p_y(i)\, H_{yz|\xi(y)=i}.$$

***Теорема* 15.** *Верно неравенство* $H_{yz} \le H_y + H_{yz|y}$.

Доказательство. Используя равенство $p_{yz}(i, j) = p_{yz|y}(j \mid i)\, p_y(i)$, получаем

$$H_{yz|y} = -\,\Sigma_{i,j}\, p_{yz}(i, j) \log\, p_{yz}(i, j) / p_y(i) = .$$

$$-\,\Sigma_{i,j}\, p_{yz}(i, j) \log\, p_{yz}(i, j) + \Sigma_{i,j}\, p_{yz}(i, j) \log\, p_y(i).$$

Так как $p_y(i) = \sum_j p_{yz}(i, j)$, то получаем

$$H_{yz|y} = -\,\Sigma_{i,j}\, p_{yz}(i, j) \log\, p_{yz}(i, j) + \Sigma_i\, p_y(i) \log\, p_y(i) =$$

$$-\,\Sigma_{i,j}\, p_{yz}(i, j) \log\, p_{yz}(i, j) - H_y.$$

Так как $\Sigma_i\, p_{yz}(i, j) = \Sigma_i\, p_{yz|y}(j \mid i)\, p_y(i) = p_{yz}(j)$, то $-\Sigma_i\, p_{yz}(i, j) \log p_{yz}(i, j) \ge -\, p_{yz}(j) \log p_{yz}(j)$. Поэтому верно такое соотношение

$$-\,\Sigma_{i,j}\, p_{yz}(i, j) \log p_{yz}(i, j) \ge -\,\Sigma_j\, p_{yz}(j) \log p_{yz}(j) = H_{yz}$$

Отсюда получаем искомое неравенство

$$H_{yz|y} \ge H_{yz} - H_y.$$

Теорема доказана.

4. Зависимые переменные. Следующим исследуемым классом функций будут так называемые функции *с сильной зависимостью* между переменными. Введем такое определение.

Назовем $f(\boldsymbol{y}, \boldsymbol{z})$ функцией *с сильной зависимостью между переменными* $\boldsymbol{y}$ и $\boldsymbol{z}$ (обозначим $\boldsymbol{y} \leftrightarrow \boldsymbol{z}$), если в матрице M_f не константные функции встречаются в точности по одной в каждой строке и в каждом столбце. Из этого вытекает, что для функции $f(\boldsymbol{y}, \boldsymbol{z})$ совпадают мощности фактор-множеств, определяемых $\boldsymbol{y}$-эквивалентностью, $\boldsymbol{z}$-эквивалентностью и $\boldsymbol{yz}$-эквивалентностью. Кроме того, для каждого $\boldsymbol{yz}$-класса, для которого результирующая функция не константа, его $\boldsymbol{y}$-проекции однозначно определяют соответствующие $\boldsymbol{z}$-проекции. В терминах матрицы M_f имеем, что все пары (i, j), где i – фиксированный номер столбца и j пробегает по всем номерам строк, определяют единственный класс $\boldsymbol{yz}$-эквивалентности. Аналогично, если зафиксировать номер строки этой матрицы, то все ее столбцы также определяют единственный класс эквивалентности. Из этих рассуждений видно, что матрица M_f квадратная.

Содержательно сильная зависимость трактуется, как взаимно-однозначная зависимость в следующем смысле. Каждый класс $\boldsymbol{y}$-эквивалентности соответствует в точности одному классу $\boldsymbol{z}$-эквивалентности и наоборот. Следовательно, каждый класс $\boldsymbol{y}$-эквивалентности единственным образом определяет вычислитель, который перечисляет $\boldsymbol{z}$-наборы лишь из одного класса $\boldsymbol{z}$-эквивалентности. Очевидно, что верно и обратное.

Если $f(\boldsymbol{y}, \boldsymbol{z})$ есть функция с сильной зависимостью между переменными $\boldsymbol{y}$ и $\boldsymbol{z}$, то ее разложение по переменным $\boldsymbol{yz}$ имеет вид $\vee_{i=1,k\ j=1,h}\ [\boldsymbol{y}^{\sigma^i}\boldsymbol{z}^{\lambda^j}]\ f_{ij}$, $k = h$ и существует взаимно однозначное отображение φ:$\{1, 2, ..., k\} \to \{1, 2, ..., h\}$ такое, что для всякого $i \in \{1, 2, ..., k\}$ не константа лишь функция $f_{i\varphi(i)}$. Разложив функцию $f(\boldsymbol{y}, \boldsymbol{z})$ по переменным $\boldsymbol{y}$, получим $\vee_{i=1,k}\ [\boldsymbol{y}^{\sigma^i}]\ f(\sigma_1^{\ i}, \boldsymbol{z})$. В этом случае означивающие наборы для функции $f(\sigma_1^{\ i}, \boldsymbol{z})$ обладают таким свойством: лишь наборы, порожденные $\boldsymbol{z}$-классом с номером $\varphi(i)$ не превращают $f(\sigma_1^{\ i}, \boldsymbol{z})$ в константу. Аналогично, разложив функцию $f(\boldsymbol{y}, \boldsymbol{z})$ по переменным $\boldsymbol{z}$, получим $\vee_{i=1,h}\ [\boldsymbol{z}^{\lambda^j}]\ f(\boldsymbol{y}, \lambda_1^{\ j})$. И имеет место аналогичный факт: лишь наборы, порожденные $\boldsymbol{y}$-классом с номером $\varphi^{-1}(j)$ не превращают $f(\boldsymbol{y}, \lambda_1^{\ j})$ в константу.

Следовательно, функция $f(\boldsymbol{y}, \boldsymbol{z})$ представима в виде $\vee_{i=1,k}\ [\boldsymbol{y}^{\sigma^i}\boldsymbol{z}^{\ \lambda\varphi(j)}]\ f_{i\varphi(j)}$ или $\vee_{\ j=1,h}\ [\boldsymbol{y}^{\sigma\varphi^{-1}(j)}\boldsymbol{z}^{\lambda^j}]\ f_{\varphi^{-1}(j)j}$.

Очевидна такая теорема.

***Теорема* 16.** *Если $f(\boldsymbol{y}, \boldsymbol{z})$ есть функция с сильной зависимостью $\boldsymbol{y} \leftrightarrow \boldsymbol{z}$, то* $H_{\boldsymbol{yz}|\boldsymbol{y}} = 0$.

Доказательство. Если $p_{\boldsymbol{yz}}(i, j)$ есть доля путей из истока в $\boldsymbol{yz}$-сечение, одновременно проходящие через i-й узел $\boldsymbol{y}$-сечения и j-й узел $\boldsymbol{yz}$-сечения, то

$p_{yz}(i, \varphi(i)) = p_y(i)$, а для остальных значений j $p_{yz}(i, j) = 0$. Отсюда следует, что $p_{yz|y}(\varphi(i) \mid i) = 1$ и $p_{yz|y}(j \mid i) = 0$ для остальных значений j. Теперь $H_{yz|y} = - \Sigma_{i,j}$ $p_y(i)\, p_{yz|y}(j \mid i) \log p_{yz|y}(j \mid i) = 0$.

Следствие. Для функции $f(\boldsymbol{y}, \boldsymbol{z})$ *с сильной зависимостью* $\boldsymbol{y} \leftrightarrow \boldsymbol{z}$, $H_{yz} = H_y$.

Можно несколько перефразировать отношение сильной зависимости следующим образом. Говорим, что два множества $\boldsymbol{y}$ и $\boldsymbol{z}$ переменных логической функции $f(\boldsymbol{y}, \boldsymbol{z})$ *обладают одинаковым распределением,* если,

во-первых, существует взаимно-однозначное соответствие фактор-множеств, определяемых этими множествами переменных и,

во-вторых, доли наборов, порождаемых соответствующими классами, совпадают.

Это обозначает, что если $\boldsymbol{y}$-эквивалентность известна, то дополнительное знание $\boldsymbol{z}$-эквивалентности не увеличивает наших знаний о функции. Понятно, что *для функции* $f(\boldsymbol{y}, \boldsymbol{z})$ *переменные* $\boldsymbol{y}$ *и* $\boldsymbol{z}$ *обладают одинаковым распределением тогда и только тогда, когда эти множества переменных сильно зависимы*.

Будем говорить просто *о зависимости переменных* $\boldsymbol{z}$ *от переменных* $\boldsymbol{y}$ (обозначается $\boldsymbol{y} \rightarrow \boldsymbol{z}$), если в каждой строке матрицы M_f в точности одна клетка не константная функция.

Из этого определения вытекает, что *если* $f(\boldsymbol{y}, \boldsymbol{z})$ *есть функция с зависимостью* $\boldsymbol{y} \rightarrow \boldsymbol{z}$ *переменных, то для матрицы* M_f *выполняется неравенство* $h \le k$.

В этом случае между фактор-множествами, порождаемыми $\boldsymbol{y}$-эквивалентностью и $\boldsymbol{z}$-эквивалентностью, можно установить однозначное отображение $\varphi:\{1, 2, ..., k\} \rightarrow \{1, 2, ..., h\}$ такое, что для всякого $i \in \{1, 2, ..., k\}$ не тождественная константа лишь функция $f_{i\varphi(i)}$. И наоборот, для каждого значения $j \in \{1, 2, ..., h\}$ не тождественные константы лишь функции $f_{\varphi^{-1}(j),j}$.

Обратное отображение φ^{-1} не однозначно, так как одному $\boldsymbol{z}$-классу в общем случае соответствует несколько $\boldsymbol{y}$-классов.

Зависимость $\boldsymbol{y} \to \boldsymbol{z}$ трактуется как функциональная в следующем смысле: каждый класс $\boldsymbol{y}$-эквивалентности определяет в точности один класс $\boldsymbol{z}$-эквивалентности. Обратное соотношение, в общем случае, неверно – несколько классов $\boldsymbol{z}$-эквивалентности могут определяться одним классом $\boldsymbol{y}$-эквивалентности.

Пусть $f(\boldsymbol{y}, \boldsymbol{z})$ есть логическая функция с зависимостью $\boldsymbol{y} \to \boldsymbol{z}$ ее аргументов, и ее разложение по $\boldsymbol{y}$ имеет вид $f(\boldsymbol{y}, \boldsymbol{z}) = \vee_{i=1,k} [\boldsymbol{y}^{\sigma^i}]\, f(\boldsymbol{\sigma}^i{}_1, \boldsymbol{z})$. В этом случае лишь $\boldsymbol{z}$-наборы, образующие $\boldsymbol{z}$-класс с номером $\varphi(i)$ не обращают функцию $f(\boldsymbol{\sigma}^i{}_1, \boldsymbol{z})$ в константу. Разложив функцию $f(\boldsymbol{y}, \boldsymbol{z})$ по переменным $\boldsymbol{z}$, получим выражение $f(\boldsymbol{y}, \boldsymbol{z}) = \vee_{j=1,h} [\boldsymbol{z}^{\lambda^j}]\, f(\boldsymbol{y}, \boldsymbol{\lambda}^j{}_1)$. В этом случае лишь $\boldsymbol{y}$-наборы, образующие $\boldsymbol{y}$-классы с номерами $\varphi^{-1}(j)$, не обращают функцию $f(\boldsymbol{z}, \boldsymbol{\lambda}^j{}_1)$ в константу. Следовательно, $f(\boldsymbol{y}, \boldsymbol{z}) = \vee_{i=1,k} [\boldsymbol{y}^{\sigma^i}\, \boldsymbol{y}^{\lambda^{\varphi(i)}}]\, f_{i,\varphi(i)}$ и $f(\boldsymbol{y}, \boldsymbol{z}) = \vee_{j=1,h} [\boldsymbol{y}^{\sigma^{\varphi^{-1}(j)}} \boldsymbol{z}^{\lambda^j}]\, f_{\varphi^{-1}(j),j}$.

Справедлива теорема.

***Теорема* 17.** *Пусть $f(\boldsymbol{y}, \boldsymbol{z})$ есть логическая функция с зависимостью $\boldsymbol{y} \to \boldsymbol{z}$ ее аргументов. Тогда* $H_{\boldsymbol{yz}|\boldsymbol{y}} = 0$.

Доказательство. Пусть $p_{\boldsymbol{yz}}(i, j)$ есть доля путей из истока в $\boldsymbol{yz}$-сечение, одновременно проходя через i-ый узел $\boldsymbol{y}$-сечения и j-ый узел $\boldsymbol{yz}$-сечения. Отсюда следует, что $p_{\boldsymbol{yz}}(i, \varphi(i)) = p_{\boldsymbol{y}}(i)$, а для остальных значений $p_{\boldsymbol{yz}}(i, j) = 0$. Отсюда следует, что $p_{\boldsymbol{yz}|\boldsymbol{y}}(\varphi(i)|i) = 1$ и $p_{\boldsymbol{yz}|\boldsymbol{y}}(\varphi(i)|i) = 0$ для остальных значений. Но тогда $H_{\boldsymbol{yz}|\boldsymbol{y}} = \sum_{i,j} p_{\boldsymbol{y}}(i)\, p_{\boldsymbol{yz}|\boldsymbol{y}}(j|\, i) \log p_{\boldsymbol{yz}|\boldsymbol{y}}(j|\, i) = 0$.

Теорема доказана.

Следствие. *Пусть $f(\boldsymbol{y}, \boldsymbol{z})$ есть логическая функция с зависимостью $\boldsymbol{y} \to \boldsymbol{z}$ ее аргументов*. Тогда $H_{\boldsymbol{yz}} = H_{\boldsymbol{y}}$.

С другой стороны, если для функции $f(\boldsymbol{y}, \boldsymbol{z})$ имеется зависимость $\boldsymbol{y} \to \boldsymbol{z}$, но отсутствует зависимость $\boldsymbol{z} \to \boldsymbol{y}$, то $H_{\boldsymbol{zy}|\boldsymbol{z}} > 0$. Этот факт следует из того, что одному классу $\boldsymbol{z}$-эквивалентности в общем случае соответствуют несколько классов $\boldsymbol{y}$-эквивалентности. Поэтому доля путей из i-го узла $\boldsymbol{y}$-сечения в j-ый узел $\boldsymbol{yz}$-сечения при некоторых значениях i, j отлична от 1 и нуля, так как из одного i-го узла могут вести пути в несколько узлов $\boldsymbol{yz}$-сечения.

5. Свойства логической энтропии. Пусть функция $f(\boldsymbol{y}, \boldsymbol{z})$ представима в виде конъюнкции $F(\boldsymbol{y})\, G(\boldsymbol{y}, \boldsymbol{z})\, L(\boldsymbol{z})$, где функция $F(\boldsymbol{y})$ не содержит переменных $\boldsymbol{z}$, $L(\boldsymbol{z})$ - переменных $\boldsymbol{y}$ и $G(\boldsymbol{y}, \boldsymbol{z})$ содержит оба множества $\boldsymbol{y}$, $\boldsymbol{z}$ переменных. Для простоты пусть $G(\boldsymbol{y}, \boldsymbol{z})$ не содержит иных переменных, кроме $\boldsymbol{y}$, $\boldsymbol{z}$. Назовем функцию $G(\boldsymbol{y}, \boldsymbol{z})$ *сечением* функции $f(\boldsymbol{y}, \boldsymbol{z})$. Разложим функции $F(\boldsymbol{y})$, $G(\boldsymbol{y}, \boldsymbol{z})$ и $L(\boldsymbol{z})$ по переменным соответственно $\boldsymbol{y}$, $\boldsymbol{yz}$ и $\boldsymbol{z}$. Результирующее выражение выглядит так:

$$\vee_{i=1,k}\, [\boldsymbol{y}^{\sigma^i}] \wedge u_i \wedge (\vee_{i,j}\, \boldsymbol{y}^{\alpha^i} \boldsymbol{z}^{\beta^j}) \wedge (\vee_{j=1,h}\, [\boldsymbol{z}^{\lambda^j}]\, v_j).$$

В разложении функции $G(\boldsymbol{y}, \boldsymbol{z})$ фигурируют конъюнкты $\boldsymbol{y}^{\alpha^i}\boldsymbol{z}^{\beta^j}$, определенные бинарными кортежами $\boldsymbol{\alpha}^i$ и $\boldsymbol{\beta}^j$, а не дизъюнкты, определяемые классами $\boldsymbol{yz}$-эквивалентности.

Введем следующее определение.

Набор $\boldsymbol{\alpha}^i\boldsymbol{\beta}^j$ из разложения функции $G(\boldsymbol{y}, \boldsymbol{z})$ является *мостиком* между классами $\boldsymbol{\sigma}^i = \{\boldsymbol{\sigma}_1^i, \boldsymbol{\sigma}_2^i, \ldots, \boldsymbol{\sigma}_m^i\}$, $\boldsymbol{\lambda}^j = \{\boldsymbol{\lambda}_1^j, \boldsymbol{\lambda}_2^j, \ldots, \boldsymbol{\lambda}_n^j\}$ соответственно $\boldsymbol{y}$-эквивалентности и $\boldsymbol{z}$-эквивалентности для функций соответственно $F(\boldsymbol{y})$ и $L(\boldsymbol{z})$, если $\boldsymbol{\alpha}^i$ не ортогонален хотя бы одному набору из множества $\{\boldsymbol{\sigma}_1^i, \boldsymbol{\sigma}_2^i, \ldots, \boldsymbol{\sigma}_m^i\}$, а $\boldsymbol{\beta}^j$ – хотя бы одному набору из множества $\{\boldsymbol{\lambda}_1^j, \boldsymbol{\lambda}_2^j, \ldots, \boldsymbol{\lambda}_n^j\}$.

Справедлива следующая

***Теорема* 18.** *Если* $\boldsymbol{yz}$*-набор* $\boldsymbol{\alpha}^i\boldsymbol{\beta}^j$ *является мостиком между классами эквивалентности* $\boldsymbol{\sigma}^i$ *и* $\boldsymbol{\lambda}^j$, *то все наборы из* $\boldsymbol{\sigma}^i \times \boldsymbol{\lambda}^j$ *не ортогональные набору* $\boldsymbol{\alpha}^i\boldsymbol{\beta}^j$ *определяют один класс эквивалентности для функции* $f(\boldsymbol{y}, \boldsymbol{z})$.

Доказательство. Означивание функции $G(\boldsymbol{y}, \boldsymbol{z})$ $\boldsymbol{yz}$-набором $\boldsymbol{\alpha}^i\boldsymbol{\beta}^j$ превращает ее в единицу. С другой стороны, каждый $\boldsymbol{y}$-набор $\boldsymbol{\sigma}_1^i, \boldsymbol{\sigma}_2^i, \ldots, \boldsymbol{\sigma}_m^i$ превращает функцию $F(\boldsymbol{y})$ в u_i , а $\boldsymbol{z}$-набор $\boldsymbol{\lambda}_1^j, \boldsymbol{\lambda}_2^j, \ldots, \boldsymbol{\lambda}_n^j$ - функцию $L(\boldsymbol{z})$ в v_j. Отсюда вытекает, что каждый $\boldsymbol{yz}$-набор из $\boldsymbol{\sigma}^i \times \boldsymbol{\lambda}^j$ не ортогональный набору $\boldsymbol{\alpha}^i\boldsymbol{\beta}^j$ превращает конъюнкцию $F(\boldsymbol{y})\ G(\boldsymbol{y}, \boldsymbol{z})\ L(\boldsymbol{z})$ в конъюнкцию $u_i \wedge v_j$.

Теорема доказана.

С другой стороны, если $\boldsymbol{yz}$-набор $\boldsymbol{\alpha}^i\boldsymbol{\beta}^j$ не является мостиком между классами эквивалентности $\boldsymbol{\sigma}^i$ и $\boldsymbol{\lambda}^j$, то конъюнкция $u_i \wedge v_j$ не участвует в разложении функции $f(\boldsymbol{y}, \boldsymbol{z})$ по переменным $\boldsymbol{y}$ и $\boldsymbol{z}$.

Таким образом, число классов $\boldsymbol{yz}$-эквивалентности для функции $f(\boldsymbol{y}, \boldsymbol{z})$, определяется числом мостиков, соединяющих классы $\boldsymbol{y}$-эквивалентности для функции $F(\boldsymbol{y})$ и $\boldsymbol{z}$-эквивалентности для $L(\boldsymbol{z})$. Чем больше таких мостиков, тем ближе мощность фактор-множества $\boldsymbol{yz}$-эквивалентности к kh. Если число мостиков меньше, то число классов $\boldsymbol{yz}$-эквивалентности также уменьшается. В соответствии с этим меняется энтропия $H^f_{\boldsymbol{yz}}$ по сравнению с суммой $H^f_{\boldsymbol{y}} + H^f_{\boldsymbol{z}}$. Содержательно это значит, что увеличение числа мостиков увеличивает независимость переменных $\boldsymbol{y}$ и $\boldsymbol{z}$, уменьшение – приводит к их сильной зависимости.

Рассмотрим конъюнкцию $F(\boldsymbol{y})\ L(\boldsymbol{z})$. Ее аргументы $\boldsymbol{y}$ и $\boldsymbol{z}$ не зависимые, поэтому $H^{FL}_{yz} = H^{FL}_{y} + H^{FL}_{z}$. Так как переменные $\boldsymbol{z}$ не встречаются в $F(\boldsymbol{y})$, а переменные $\boldsymbol{y}$ – в $L(\boldsymbol{z})$, то получаем равенства $H^{FL}_{y} = H^{F}_{y}$ и $H^{FL}_{z} = H^{L}_{z}$. Отсюда $H^{FL}_{yz} = H^{F}_{y} + H^{L}_{z}$.

В общем случае для функции $F(\boldsymbol{y})\ G(\boldsymbol{y}, \boldsymbol{z})\ L(\boldsymbol{z})$ не каждая пара (i, j) определяет класс эквивалентности с той же долей, что и для функции $F(\boldsymbol{y})\ L(\boldsymbol{z})$, так как некоторые функции $u_i \wedge v_j$ не встречаются в разложении в силу того, что i-ый и j–ый классы не соединяются ни одним мостиком. Поэтому в общем случае энтропия $H^f_{\boldsymbol{yz}}$ не превосходит суммы $H^f_{\boldsymbol{y}} + H^f_{\boldsymbol{z}}$.

Справедлива следующая теорема.

***Теорема* 19.** *Пусть функция* $f(\boldsymbol{y}, \boldsymbol{z}) = F(\boldsymbol{y})\ G(\boldsymbol{y}, \boldsymbol{z})\ L(\boldsymbol{z})$ *и число переменных* $\boldsymbol{yz}$ *равно* m. *Тогда* $H^f_{\boldsymbol{yz}} \le m$.

Доказательство. Энтропия H^f_{yz} максимальная, когда доли наборов, определяемых каждым классом ***yz***-эквивалентности одинаковы. Пусть δ есть число путей бинарной программы, определяемой функцией $f(\boldsymbol{y}, \boldsymbol{z})$, проходящих из истока в один узел ***yz***-сечения. Тогда справедливо неравенство

$$H^f_{yz} \le -\sum \frac{\delta}{N} \log \frac{\delta}{N} = log\ N/\delta.$$

где N есть число всех путей из истока в ***yz***-сечение, и суммирование ведется по всем узлам ***yz***-сечения.

Число узлов ***yz***-сечения не более 2^m. Так как δ есть число путей, проходящих из истока в один узел ***yz***-сечения, то $N \le \delta\ 2^m$. Поэтому $H^f_{yz} \le m$.

Теорема доказана.

Содержательно понятно, что если сечение функции содержит небольшое число переменных, то, означив эти переменные, мы получим небольшое сечение бинарной программы и энтропия, определяемая этими переменными, не велика.

Справедлива

***Теорема* 20.** *Пусть у функции* $f(\boldsymbol{y}, \boldsymbol{z})$ *число переменных* $\boldsymbol{z}$ *равно* m. *Тогда* H_{yz} - $H_y \le m$.

Доказательство. Каждый узел ***y***-сечения бинарной программы, определяемой функцией $f(\boldsymbol{y}, \boldsymbol{z})$, соединен путями не более, чем с 2^m различными узлами ***yz***-сечении. В результате вся совокупность $N_y(i)$ путей, проходящих через i-ый узел ***y***-сечения разбивается на не более, чем 2^m не пересекающихся множеств путей, проходящих из истока в ***yz***-сечение. Энтропия H^f_{yz} будет максимальна, когда все доли путей, проходящих из истока в ***yz***-сечение, одинаковы. Поэтому для любого i-го узла ***y***-сечения имеем $N_y(i) \le 2^m N_{yz}(j)$, где $N_{yz}(j)$ – это число путей, проходящих через j-ый узел ***yz***-сечения. Но тогда $N_y(i)\ /\ N_{yz}(j) \le 2^m$. Отсюда следует утверждение теоремы.

Теорема доказана.

Исследование логической энтропии приводит к вопросу можно ли из функций с небольшой энтропией построить функцию с большой энтропией? Чтобы на него ответить докажем следующие теоремы.

***Теорема* 21**. Для логических функций $f(\boldsymbol{x}, \boldsymbol{y})$ и $g(\boldsymbol{x}, \boldsymbol{y})$ имеет место неравенство

$$H_x^{f\vee g} \geq \max\{H_x^f, H_x^g\}.$$

Доказательство. Построим для функции $f(\boldsymbol{x}, \boldsymbol{y}) \vee g(\boldsymbol{x}, \boldsymbol{y})$ бинарную программу $\pi_{f\vee g}$. Узлы ее $\boldsymbol{x}$-сечения, соответствующие не константным функциям, делятся на три типа, для которых выполняются условия соответственно: $f \neq 0, g = 0; f = 0, g \neq 0; f \neq 0, g \neq 0$.

Рассмотрим бинарную программу π_f для функции $f(\boldsymbol{x}, \boldsymbol{y})$, в которой порядок означивания переменных совпадает с порядком в $\pi_{f\vee g}$. Узлы ее $\boldsymbol{x}$-сечения, которые соответствуют не константным функциям, в программе $\pi_{f\vee g}$ разделяются на два типа, в соответствии с выполнением условий: $f \neq 0, g = 0; f \neq 0, g \neq 0$. Поэтому, каждому узлу N_i из $\boldsymbol{x}$-сечения программы π_f, для которого доля путей из истока составляет $p_x(i)$ в $\boldsymbol{x}$-сечении программы $\pi_{f\vee g}$ соответствуют два узла N_i' и N_i' в той части $\boldsymbol{x}$-сечения, для которой выполняется условие $f \neq 0, g = 0; f \neq 0, g \neq 0$.

Оставив в программе $\pi_{f\vee g}$ только пути, ведущие в эту часть $\boldsymbol{x}$-сечения, получим подграф π^1 бинарной программы $\pi_{f\vee g}$. Если обозначить для π^1 доли путей, ведущих в N_i' и N_i', соответственно p_i' и p_i'', то получим равенство $p_x(i) = p_i' + p_i''$. Отсюда вытекает неравенство $H_x^f \leq H_x^1$, где H_x^1 есть энтропия $\boldsymbol{x}$-сечения в выделенной из $\pi_{f\vee g}$ части π^1. Теперь сравним доли путей, ведущих в $\boldsymbol{x}$-сечение, в графе π^1 и всей программы $\pi_{f\vee g}$. В графе π^1 доли возрастают за счет исключения путей, ведущих в программе $\pi_{f\vee g}$ в узлы $\boldsymbol{x}$-сечения, которые удовлетворяют условию $f = 0, g \neq 0$. Но так как доли в графе π^1 возрастают по сравнению с долями аналогичных путей в $\pi_{f\vee g}$, то энтропия H_x^1 меньше, чем энтропия $H_x^{f\vee g}$. Отсюда следует неравенство $H_x^{f\vee g} > H_x^1$.

Аналогично показывается, что имеют место неравенства $H_x^g \le H_x^2 \le H_x^{f\vee g}$, где H_x^2 есть энтропия ***x***-сечения в части бинарной программы $\pi_{f\vee g}$, которая включает пути ведущие в узлы ***x***-сечения, выделяемые условиями $g \ne 0, f = 0; g \ne 0, f \ne 0$. Следовательно, имеем неравенство $H_x^{f\vee g} \ge \max\{H_x^f, H_x^g\}$.

Теорема доказана.

С другой стороны, верно утверждение.

***Теорема* 22**. Для логических функций $f(\boldsymbol{x}, \boldsymbol{y})$ и $g(\boldsymbol{x}, \boldsymbol{y})$ имеет место неравенство

$$H_x^{fg} \le \min\{H_x^f, H_x^g\}.$$

Доказательство. Построим для функции $f(\boldsymbol{x}, \boldsymbol{y})$ $g(\boldsymbol{x}, \boldsymbol{y})$ бинарную программу π_{fg}, в которой начальные отрезки всех путей из истока в сток получены означиванием переменных ***x***, и программу π_f, в которой порядок означивания переменных ***x*** совпадает с порядком в π_{fg}. Пусть пути, ведущие из истока в ***x***-сечение программы π_{fg} (π_f), образуют множество $M_{fg}(M_f)$. Легко увидеть, что $M_{fg} \subseteq M_f$. Более того, все пути из M_{fg}, ведущие в один узел ***x***-сечения, также ведут в один узел ***x***-сечения программы π_f. Назовем такие узлы соответствующими.

Отсюда следует, что число узлов ***x***-сечения программы π_{fg} не более числа узлов ***x***-сечения программы π_f, а доли путей, ведущих в один узел ***x***-сечения программы π_f не меньше долей путей, ведущих в соответствующие узлы программы π_{fg}. Отсюда следует, что $H_x^{fg} \le H_x^f$. Аналогично доказывается неравенство $H_x^{fg} \le H_x^g$. Отсюда вытекает заключение теоремы.

Теорема доказана.

Последние два утверждения согласуются с содержательными представлениями. Объединение множеств событий влечет, по меньшей мере, не уменьшение неопределенности наших знаний об этих событиях (или фактах). С другой стороны, пересечение множеств подразумевает уточнение некоторых свойств или значений и поэтому – уменьшение неопределенности. Доказать аналогичные соотношения для дополнения множеств относительно простыми средствами не удается.

6. Энтропия суперпозиции функций. В этом разделе исследуем поведение энтропии логических функций, представляющих двоичные вычислимые функции. В частности рассмотрим, как зависит энтропия суперпозиции функций от энтропий образующих ее функций. Приведем сейчас лишь общие результаты. Более конкретно этот вопрос будет исследован на примере переписывающих алгоритмов.

Пусть логические функции $f(\boldsymbol{x}, \boldsymbol{y})$ и $g(\boldsymbol{y}, \boldsymbol{z})$ представляют вычислимые функции соответственно $\boldsymbol{y} = \phi(\boldsymbol{x})$ и $\boldsymbol{z} = \psi(\boldsymbol{y})$. Суперпозиция $\boldsymbol{z} = \psi(\phi(\boldsymbol{x}))$ представима конъюнкцией $h(\boldsymbol{x}, \boldsymbol{z}) = f(\boldsymbol{x}, \boldsymbol{y})\, g(\boldsymbol{y}, \boldsymbol{z})$.

Рассмотрим $\boldsymbol{xy}$-сечение бинарной программы π_f функции f при полном множестве $N_{\boldsymbol{x}}$ означиваний переменных $\boldsymbol{x}$ одинаковой длины. Пусть оно характеризуется энтропией $H^f_{xy} = \sum_i - p_{xy}(i) \log p_{xy}(i)$. Особенность построения бинарной программы π_f состоит в том, что значения неподвижных переменных $\boldsymbol{y}$ однозначно определяются значениями аргумента $\boldsymbol{x}$. Они не меняются при увеличении длины определяющего их $\boldsymbol{x}$-набора. Каждый путь из истока в $\boldsymbol{xy}$-сечение характеризуется некоторым $\boldsymbol{x}$-набором $\sigma_x \in N_x$ и определяемым им набором σ_y значений неподвижных компонент $\boldsymbol{y}$.

Рассмотрим $\boldsymbol{xy}$-сечение бинарной программы π_h функции h, для которого означивания переменных $\boldsymbol{x}$ и $\boldsymbol{y}$ совпадают с означиваниями из бинарной программы π_f. Число узлов $\boldsymbol{xy}$-сечения программы π_h совпадает с числом узлов ***xy***-сечения программы π_f и доли путей, ведущих в соответствующие узлы этих программ, также совпадают.

Продолжим построение бинарной программы π_h ниже *i*-го узла путем означивания переменных ***z***. Так как *g*(***y***, ***z***) представляет вычислимую функцию ψ, неподвижные компоненты ***z*** однозначно определяются неподвижными компонентами ***y***. Именно эти значения переменных ***z*** выберем в качестве ***z***-наборов при продолжении построения программы π_h. Если сравнить π_h с бинарной программой π_g для функции *g*(***y***, ***z***), которая получается означиванием переменных ***y*** и ***z***, как это сделано в π_h, то имеет место следующее отношение включения.

Пусть в программе π_h из истока в *i*-ый узел ***xy***-сечения ведет некоторое множество путей. Каждый из них характеризуется единственным ***x***-набором и единственным значением неподвижных компонент ***y***. Поэтому в *i*-ый узел ***xy***-сечения мы попадаем из истока по путям, характеризующимся как различными, так и совпадающими ***y***-наборами потому, что разные начальные ***x***-наборы могут определять одинаковые значения неподвижных компонент ***y***. При дальнейшем построении программы π_h ниже *i*-го узла означивания переменных ***z*** определяются неподвижными компонентами ***y***, которые фиксируются функцией *f*(***x***, ***y***). Поэтому число путей, ведущих из *i*-го узла ***xy***-сечения в ***xyz***-сечение, не превосходит числа различных ***y***-наборов, которые встречаются в путях из истока в *i*-ый узел.

Часть программы π_h, расположенная ниже *i*-го узла ***xy***-сечения, представляет собой фрагмент программы π_g, так как все пути программы π_h из истока в ***xyz***-сечение проходящие через *i*-ый узел ***xy***-сечения характеризуются множеством пар $<\sigma_y, \sigma_z>$ ***y***- и ***z***-наборов, совпадающими с метками части путей из истока в ***yz***-сечение программы π_g. Если же рассматривать все пути программы π_h из истока в ***xyz***-сечение, то они определяют все пары ***y***- и ***z***-означиваний, определяемые всеми путями программы π_g.

Нам потребуются следующие определения.

Пусть $M_{\boldsymbol{x}}$ – некоторое множество начальных ***x***-означиваний. Каждый ***x***-набор σ_x определяет единственный начальный ***y***-набор σ_y неподвижных компонент. Множество $\{(\sigma_x, \sigma_y)|\ \sigma_x \in M_{\boldsymbol{x}}\}$ разбивается функцией *f* на классы эквивалентности, пусть $K_1, K_2, \ldots, K_l$. Выделим из произвольного класса K_i все первые компоненты пар, обозначим это множество $K^i_{\boldsymbol{x}}$ и назовем ***x***-проекцией класса K_i. Из того, что *f* представляет вычислимую функцию, вытекает, что $|K^i_{\boldsymbol{x}}| = |K_i|$ и $K^i_{\boldsymbol{x}} \cap K^j_{\boldsymbol{x}} = 0$ при $i \neq j$. В этом случае говорим, что функция *f* разбивает множество $M_{\boldsymbol{x}}$ на классы $K^1_{\boldsymbol{x}}, K^2_{\boldsymbol{x}}, \ldots, K^l_{\boldsymbol{x}}$ и это разбиение порождает эквивалентность: $\sigma'_x \approx \sigma''_x$ тогда и только тогда, когда оба набора σ'_x и σ''_x принадлежат одному классу из семейства $K^1_{\boldsymbol{x}}, K^2_{\boldsymbol{x}}, \ldots, K^l_{\boldsymbol{x}}$.

В точности так же можно выделить и ***y***-проекцию $K^i_{\boldsymbol{y}}$ класса K_i. Для нее выполняется неравенство $|K^i_{\boldsymbol{y}}| \leq |\ K_i\ |$.

Пусть теперь $M_{\boldsymbol{x}} = N_{\boldsymbol{x}}$ и мы имеем совокупность *y*-проекций $K^1_{\boldsymbol{y}}, K^2_{\boldsymbol{y}}, \ldots, K^l_{\boldsymbol{y}}$. По каждому ***y***-набору $\sigma_y \in K^i_{\boldsymbol{y}}$ функция $g(\boldsymbol{y}, \boldsymbol{z})$ определяет единственный ***z***-набор σ_z значений неподвижных компонент. Множество $\{(\sigma_y,\ \sigma_z):\ \sigma_y \in K^i_{\boldsymbol{y}}\}$ таких пар функцией $g(\boldsymbol{y}, \boldsymbol{z})$ разбивается на классы эквивалентности. Таким образом, функция *h* разбивает множество $\{(\sigma_x, \sigma_y, \sigma_z)|\ \sigma_x \in N_{\boldsymbol{x}},\ \sigma_y$ - значения неподвижных компонент, определяемых по σ_x, и σ_z - значения неподвижных компонент, определяемых по $\sigma_y\}$ на классы. В свою очередь функция $f(\boldsymbol{x}, \boldsymbol{y})$ разбивает множество $\{(\sigma_x, \sigma_y)|\ \sigma_x \in N_{\boldsymbol{x}},\ \sigma_y$ - значения неподвижных компонент, определяемых по $\sigma_x\}$ на классы. И распределения этих разбиений могут существенно различаться. В силу этого отличаются энтропии $H^f_{\boldsymbol{xy}}$ и $H^h_{\boldsymbol{xyz}}$. Более конкретно значение энтропии функции *h* зависит от вида функций *f* и *g*.

Из этих рассуждений вытекают следующие утверждения.

***Лемма* 23**. *Число различных путей из **xy**-сечения в **xyz**-сечение программы π_h не превосходит числа путей из истока в **xy**-сечение.*

Доказательство. Каждый путь из истока в ***xy***-сечение определяет единственную *y*-проекцию, которая, в свою очередь, определяет единственное ***z***-означивание. Следовательно, ниже всякого узла ***xy***-сечения располагается не большее число путей, чем ведет в него из истока.

Лемма доказана.

Следовательно, все пути из истока в ***xyz***-сечение задаются путями из истока в ***xy***-сечение.

***Лемма* 24**. *Число путей из i-го узла **xy**-сечения в j-ый **xyz**-сечения программы π_h совпадает с числом путей из истока, проходящих через i-ый и j-ый узлы.*

Доказательство. Пути из *i*-го узла ***xy***-сечения в *j*-ый ***xyz***-сечения представляют собой продолжение части путей из истока в *i*-ый узел. Но тогда путей из истока, проходящих через *i*-ый узел ***xy***-сечения и *j*-ый ***xyz***-сечения? будет столько же, сколько путей из *i*-го узла в *j*-ый.

Лемма доказана.

Отсюда вытекает, что *число путей программы π_h, выходящих из i-го узла **xy**-сечения и ведущих в **xyz**-сечение, не больше числа путей из истока в i-ый узел **xy**-сечения.*

Действительно, все пути ниже *i*-го узла ***xy***-сечения определяются ***y***-проекциями, которые формируются путями из истока в *i*-ый узел.

Введем такое определение.

Пусть $p_z(j \mid i)$ есть доля путей программы π_h, ведущих из *i*-го узла ***xy***-сечения в *j*-ый узел ***xyz***-сечения среди всех путей из *i*-го узла в ***xyz***-сечение. Тогда *частной условной энтропией*, определяемой этим ***xyz***-сечением относительно *i*-го узла, называется величина $H_i^g = -\sum_j p_z(j \mid i) \log p_z(j \mid i)$. Просто *условной энтропией функции g относительно f* назовем среднее частных условных энтропий $H_{yz}^{g|f} = \sum_i p_{xy}(i) H_i^g$.

Содержательно условная энтропия $H_i^g = -\sum_j p_z(j\,|\,i)\log p_z(j\,|\,i).$ характеризует сложность функции $g\,|_{y\in K_y^i}$, где $K_{\boldsymbol{y}}^i$ есть $\boldsymbol{y}$-проекция i-го класса K_i эквивалентности, определяемой функцией $f(\boldsymbol{x}, \boldsymbol{y})$. Энтропия $H_{yz}^{g|f} = \sum_i p_{xy}(i) H_i^g$ описывает усредненную сложность функций $g\,|_{y\in K_y^i}$, когда усредняющими коэффициентами выступают доли $p_{\boldsymbol{xy}}(i)$ путей бинарной программы π_f из истока в $\boldsymbol{xy}$-сечение.

Теорема **25**. *Имеет место неравенство*: $H_{xyz}^{fg} \le H_{xy}^f + H_{yz}^{g|f}$.

(*Энтропия конъюнкции логических функций, представляющей суперпозицию двух вычислимых функций, не превосходит суммы энтропий функции f и условной энтропии функции g относительно функции f*).

Доказательство. $H_{xy}^f + \sum_i p_{xy}(i) H_i^g = -\sum_i p_{xy}(i)\log p_{xy}(i) + \sum_i p_{xy}(i) H_i^g =$

$\sum_i p_{xy}(i)(H_i^g - \log p_{xy}(i)) =$- $\sum_i p_{xy}(i)(\sum_j p_z(j\,|\,i)\log p_z(j\,|\,i) p_{xy}(i))$ =.

$\sum_{i,j} p_{xy}(i) p_z(j\,|\,i)\log p_z(j\,|\,i) p_{xy}(i)$. $p_{xy}(i) p_z(j\,|\,i) = p(i,j)$ есть доля путей бинарной программы, проходящих одновременно через i-ый узел $\boldsymbol{xy}$-сечения и j-ый узел $\boldsymbol{xyz}$-сечения. Но тогда последняя сумма равна $-\sum_{i,j} p(i,j)\log p(i,j)$.

$H_{xyz}^{fg} = -\sum_j p_{xyz}(j)\log p_{xyz}(j)$, где $p_{xyz}(j) = \sum_i p(j\,|\,i) p_{xy}(i) = \sum_i p(i,j)$. Тогда

$$H_{xyz}^{fg} = -\sum_j (\sum_i p(i,j)\log(\sum_i p(i,j))) = -\sum_{i,j} p(i,j)\log(\sum_i p(i,j)) .$$

Искомое неравенство $H_{xyz}^{fg} \le H_x^f + H_y^g$ переписывается следующим образом: $-\sum_{i,j} p(i,j)\log(\sum_i p(i,j)) \le -\sum_{i,j} p(i,j)\log p(i,j)$. Это неравенство выполняется в случае, когда

$$\sum_{i,j} p(i,j)\log(\sum_i p(i,j)) \ge \sum_{i,j} p(i,j)\log p(i,j) ,$$

что эквивалентно неравенству

$$\sum_{i,j} p(i,j)\log\left(\frac{\sum_i p(i,j)}{p(i,j)}\right) \geq 0.$$

Последнее неравенство очевидно, так как $\dfrac{\sum_i p(i,j)}{p(i,j)} \geq 1$.

***Лемма* 26**. *Если* $\{p_i\}$ *и* $\{q_i\}$, $i = 1, 2, \ldots, k$, *два множества не отрицательных чисел и* $\sum_i p_i = \sum_i q_i = 1$, *то верно неравенство*

$$\left(\frac{p_1}{q_1}\right)^{q_1}\left(\frac{p_2}{q_2}\right)^{q_2}\cdots\left(\frac{p_k}{q_k}\right)^{q_k} \leq 1$$

Доказательство вытекает из неравенства между средними арифметическим и геометрическим $a_1^{q_1}a_2^{q_2}\cdots a_k^{q_k} \leq \sum_i q_i a_i$, при условии $q_i > 0$ и $\sum_i q_i = 1$.

***Лемма* 27**. *Пусть* h *есть число узлов* **xyz**-*сечения, соединенных путями с* i-*м узлом* **xy**-*сечения. Тогда имеет место неравенство*

$$-\sum_j p(i,j)\log p(i,j) \leq -p_{xy}(i)\log\frac{p_{xy}(i)}{h}.$$

Доказательство. Искомое неравенство эквивалентно следующему

$$\log\frac{1}{p(i,1)^{p(i,1)}\,p(i,2)^{p(i,2)}\cdots p(i,h)^{p(i,h)}} \leq \log\frac{h^{p_{xy}(i)}}{p_{xy}(i)^{p_{xy}(i)}} \Leftrightarrow \frac{p_{xy}(i)^{p(i,1)}\,p_{xy}(i)^{p(i,2)}\cdots p_{xy}(i)^{p(i,h)}}{p(i,1)^{p(i,1)}\,p(i,2)^{p(i,2)}\cdots p(i,h)^{p(i,h)}} \leq$$

$$\frac{h^{p_{xy}(i)}}{p_{xy}(i)^{p_{xy}(i)}} \Leftrightarrow \left(\frac{\frac{1}{h}}{\frac{p(i,1)}{p_{xy}(i)}}\right)^{p(i,1)}\left(\frac{\frac{1}{h}}{\frac{p(i,2)}{p_{xy}(i)}}\right)^{p(i,2)}\cdots\left(\frac{\frac{1}{h}}{\frac{p(i,h)}{p_{xy}(i)}}\right)^{p(i,h)} \leq 1.$$

Обозначим $1/h = p_1 = p_2 = \ldots = p_h$, $p(i,1) = q_1$, $p(i,2) = q_2$, …, $p(i,h) = q_h$. Очевидно, что $\sum_i p_i = \sum_i q_i = 1$. Тогда последнее неравенство переписывается так

$$\left(\frac{p_1}{q_1}\right)^{q_1 p_{xy}(i)}\left(\frac{p_2}{q_2}\right)^{q_2 p_{xy}(i)}\cdots\left(\frac{p_h}{q_h}\right)^{q_k p_{xy}(i)} \leq 1$$

Лемма доказана.

***Теорема* 28**. *Пусть* h_i *есть число узлов* **xyz**-*сечения, в которые ведут пути из* i-*го узла* **xy**-*сечения. Тогда верно неравенство*

$$H_{yz}^{g|f} \le \sum_i p_{xy}(i)\log h_i \ .$$

Доказательство. Имеют место следующие равенства.

$$H_{xy}^{yz} = -\sum_i p_{xy}(i)p(i\,|\,j)\log p(j\,|\,i) =$$

$$-\sum_{i,j} p(i,j)\log\frac{p(i,j)}{p_{xy}(i)} = -\sum_{i,j} p(i,j)\log p(i,j) + \sum_{i,j} p(i,j)\log p_{xy}(i) =$$

$$-\sum_{i,j} p(i,j)\log p(i,j) + \sum_i p_{xy}(i)\log p_{xy}(i) = -\sum_{i,j} p(i,j)\log p_{xy}(i) - H_{xy}^f .$$

Из леммы вытекает, что

$$-\sum_{i,j} p(i,j)\log p_{xy}(i) \le \sum_i p_{xy}(i)\log\frac{p_{xy}(i)}{h_i} = H_{xy}^f + \sum_i p_{xy}(i)\log h_i \ .$$

Теорема доказана.

Таким образом, условная энтропия не превосходит среднего от логарифма мощности ***y***-проекций классов эквивалентности, задаваемых функцией *f* при полном множестве $N_{\boldsymbol{x}}$ означиваний.

Исследуем, при каких условиях энтропия суперпозиции больше энтропии образующих их функций. Для этого введем следующее определение.

Функция *g* называется *расширителем* функции *f*, если выполняется неравенство $H_{xyz}^h \ge H_{xy}^f$, где ***x***-означивания образуют полное множество $N_{\boldsymbol{x}}$ означиваний одинаковой длины, а ***y***- и ***z***-означивания определяются как при построении программы π_h.

То, что *g* является расширителем для *f*, содержательно понимается следующим образом: функция $\psi(\varphi(x))|_{x\in N_x}$ устроена сложнее, чем функция $\varphi(x)|_{x\in N_x}$. Вопрос нахождения расширителей имеет существенное значение, так как именно к нему сводится задача построения сложных вычислимых функций из простых.

Справедлива

Теорема* 29**. *Пусть для всякой пары i-го узла* ***xy*-сечения и j-го узла* ***xyz****-сечения программы* π_h*, соединенных хотя бы одним путем, выполняется соотношение*

$$\frac{p_{xy}(i)}{p_{xyz}(j)} \ge 1$$

Тогда g является расширителем f.

(Содержательно это обозначает, что доли путей, ведущих в i-ый узел ***xy***-сечения, превосходит долю путей, ведущих в j-ый узел ***xyz***-сечения. Следовательно, число путей, ведущих в i-ый узел больше числа путей, ведущих в j-ый узел.)

Доказательство.

$$H^f_{xy} < H^h_{xyz} \Leftrightarrow -\sum_i p_x(i)\log p_x(i) < -\sum_j p_{xyz}(j)\log p_{xyz}(j) \Leftrightarrow$$

$$\sum_i p_x(i)\log p_x(i) - \sum_j p_{xyz}(j)\log p_{xyz}(j) > 0 \Leftrightarrow$$

$$\sum_i p_x(i)\log p_x(i) - \sum_j (\sum_i p(j\,|\,i) p_{xy}(i))\log p_{xyz}(j) > 0 \Leftrightarrow$$

$$\sum_i p_x(i)\{\log p_x(i) - \sum_j p(j\,|\,i)\log p_{xyz}(j)\} > 0.$$

Имеет место равенство $\sum_j p(j\,|\,i) = 1$. Поэтому последнее неравенство эквивалентно

$$\sum_i p_x(i)\{\sum_j p(j\,|\,i)\log p_x(i) - \sum_j p(j\,|\,i)\log p_{xyz}(j)\} > 0 \Leftrightarrow$$

$$\sum_i p_x(i)\{\sum_j p(j\,|\,i)\log\frac{p_x(i)}{p_{xyz}(i)}\} > 0 \Leftrightarrow \sum_{i,j} p_x(i)p(j\,|\,i)\log\frac{p_x(i)}{p_{xyz}(i)} > 0 \Leftrightarrow$$

$$\sum_{i,j} p(i,j)\log\frac{p_x(i)}{p_{xyz}(i)} > 0.$$

Теорема доказана.

Литература

1. Брошкова Н.Л., Попов С.В. Логическая энтропия. Препринт ИПМ им. М.В.Келдыше РАН, 2005.
2. Брошкова Н.Л., Попов С.В. О проектировании информационных систем. Препринт ИПМ им. М.В.Келдыша РАН, 2005.

Архив

Т.25. *Пусть* $\sigma_y{}'$ *и* $\sigma_y{}''$ *суть два начальных* ***y****-набора такие, что* $\sigma_y{}' \subset \sigma_y{}''$ *и* $\sigma_y{}'$ *определяет неподвижные* ***z****-компоненты* $\sigma_z{}'$ *и* $\sigma_y{}''$*- компоненты* $\sigma_z{}''$*. Тогда выполняется включение* $\sigma_z{}' \subseteq \sigma_z{}''$.

Доказательство. Набор $\sigma_y{}'$ определяет функцию $\psi\,|\sigma_y{}'$, значения которой характеризуются неподвижными двоичными компонентами $\sigma_z{}'$, которые присутствуют в каждом ее значении, в том числе когда аргумент имеет значение, начинающееся с σ_y''. Следовательно, неподвижные компоненты функции $\psi\,|\,\sigma_y''$ включают неподвижные компоненты функции $\psi\,|\,\sigma_y'$.

Теорема доказана.

Для дальнейшего нам требуется ввести обобщение понятия логической энтропии. Напомним, что при ее определении мы рассматривали так называемые бинарные программы, характеризующиеся линейным порядком означиваемых переменных. Говоря об ***y***-сечении бинарной программы, где ***y*** = $\{y_1, y_2, \ldots, y_m\}$ есть множество логических переменных, мы имели в виду, что порождение путей бинарных программ происходит означивания этих переменных в соответствии с определенным порядком. Поэтому, если в метках дуг путей, ведущих в ***y***-сечение, рассматривать только индексы переменных, то все пути из истока в ***y***-сечение характеризуются одинаковыми последовательностями.

Значение логической энтропии зависит лишь от долей путей из истока в ***y***-сечение и при построении бинарной программы выше ***y***-сечения не учитывает собственно способа означивания переменных. Поэтому можно расширить определение логической энтропии, рассматривая не однородные программы, а программы с произвольным порядком означивания переменных в путях из истока в ***y***-сечение программы, сохраняя требование, чтобы каждый путь из истока в ***y***-сечение определял означивания всех переменных ***y***. Легко проверить, что при таком обобщении логической энтропии все полученные выше результаты остаются верными.

Наконец, ослабим последнее требование относительно означивания всех переменных ***y***, задаваемых каждым путем.

По-прежнему будем рассматривать бинарную программу и ее сечение назовем ***y***-сечением, где ***y*** = $\{y_1, y_2, \ldots, y_m\}$ есть множество логических переменных, если имеется хотя бы один путь из истока в узел этого сечения, который определяет означивания всех переменных из ***y***. Из определения бинарной программы вытекает справедливость следующего утверждения.

***Лемма* 23**. *Если i_1, i_2 суть узлы **y**-сечения и два пути, ведущие из истока в эти узлы определяют означивания соответственно* $y_{i_1}^{\sigma_1}, y_{i_2}^{\varsigma_2}, \ldots, y_{i_k}^{\sigma_k}$ *и* $y_{j_1}^{\lambda_1}, y_{j_2}^{\lambda_2}, \ldots, y_{j_m}^{\lambda_k}$ *, где $y_{i_1}, \ldots, y_{i_h}, y_{j_1}, \ldots, y_{j_m}$ переменные из **y** и $h \le m$, то при любом упорядочении первой последовательности путем перестановки ее членов она не может быть префиксом второй.*

Доказательство вытекает из определения бинарной программы и того, что оба пути начинаются в истоке.

После этого определение логической энтропии формулируется, как и прежде.

Будем характеризовать каждый путь t, ведущий в ***y***-сечение, множеством Var(t) переменных, для которых он определяет означивания. Каждый путь определяет свое множество означиваемых переменных и их означиваний. Но тогда ***y***-сечение характеризуется парой <*Max*, *Min*> соответственно наибольшим и наименьшим множествами переменных, означивания которых приводит в ***y***-сечение. Разность *Max* – *Min* назовем *интервалом*, порождаемым данным ***y***-сечением бинарной программы. Очевидно, что пара <*Max*, *Min*> зависит от конкретного способа построения бинарной программы.

Инкрементом интервала $\Delta = Max - Min$ (обозначается $in(\Delta)$) назовем число всех означиваний переменных из интервала, которые принимают участие в построении ***y***-сечения.

Рассмотрим классы так называемых локальных функций. А именно, *локальной* будем называть логическую функцию f(***y***, ***z***), если все ***y***-означивания порождают ограниченное число классов эквивалентности, определяемых лишь последними k компонентами этих означиваний.

Рассмотрим ***y***-сечение бинарной программы для локальной функции.

Имеет место

Теорема* 24**. *Пусть f*(x***, ***y***) *обобщенная функция и* $H_{\mathbf{x}}$ *– энтропия, определяемая переменными* ***x*** *, порядок означивания которых совпадает с естественным порядком переменные. Тогда определяющая окрестность для этих переменных имеет длину не менее* $H_{\mathbf{x}}$.