

Т. ЛАУСМАА

## ОБ АЛГЕБРАИЧЕСКИХ ОСНОВАХ ПОНЯТИЯ ЭНТРОПИИ

(Представил Н. Алумяэ)

Говоря об энтропии, выраженной формулой Шеннона, обычно молчаливо предполагают ее статистическую природу. Поэтому не удивительно, что в большинстве работ, посвященных изучению энтропии, ее обоснование всегда пытались искать в рамках теории вероятностей. Но для этого можно использовать и чисто алгебраический подход с привлечением понятия полуоценки для решеток. Отказ от вероятностной трактовки энтропии связан с изучением информационных свойств объектов, которые не имеют статистического характера.

В настоящей статье мы продолжаем алгебраическое обоснование понятия энтропии, начатое У. Накамурой [1], используя в качестве алгебраической интерпретации информации понятие разбиения в духе Дж. Хартманиса и Р. Е. Стирнза [2]. Наш подход к определению энтропии базируется на понятии полуоценки для решеток разбиений, который логически независим от вероятностного и алгоритмического подходов. Показывается, что если функция с вещественной областью значений, определенная на разбиениях из конечных решеток разбиений, является нижней полуоценкой для каждой из этих решеток и удовлетворяет некоторым естественным условиям, возникающим при алгебраической интерпретации информации, то она выражается через формулу Шеннона для энтропии линейно.

Разбиение произвольного конечного множества  $X = \{x_1, x_2, \dots, x_m\}$  на блоки  $B_i^{(1)}, B_i^{(2)}, \dots, B_i^{(\alpha)}, \dots, B_i^{(m_i)}$  обозначим через  $\pi_i(X)$ . В частности,  $0_X$  — нулевое разбиение, а  $1_X$  — единичное. Для любого подмножества  $X' \subset X$  определим его вес  $q(X')$  как отношение  $q_X(X') = \frac{\|X'\|}{\|X\|}$  (обычно индекс у  $q$  опускается). Разбиение,

состоящее из  $n$  равновесных блоков, будем называть однородным разбиением ранга  $n$ . Разбиения  $\pi_i(X')$  и  $\pi_j(X'')$  будем называть эквивалентными (обозначение  $\pi_i(X') \equiv \pi_j(X'')$ ), если только существует биекция  $\varphi: \pi_i \rightarrow \pi_j$  такая, что для любого  $B_i^{(\alpha)} \in \pi_i$  имеет место  $q(B_i^{(\alpha)}) = q(\varphi(B_i^{(\alpha)}))$ . Сужением разбиения  $\pi_i(X)$  на  $X' \subset X$  будем называть разбиение  $\pi_i(X') = \{B_i^{(\alpha)} \cap X' \mid B_i^{(\alpha)} \in \pi_i \wedge B_i^{(\alpha)} \cap X' \neq \emptyset\}$ , а его расширением на  $Y \supset X$  — разбиение  $\pi_i(Y) = \{\pi_i(X) \cup \{Y \setminus X\}\}$ . Для любых разбиений  $\pi_i(X)$  и  $\pi_j(X)$  примем, что  $\pi_i \cdot \pi_j = \{B_i^{(\alpha)} \cap B_j^{(\beta)} \mid B_i^{(\alpha)} \in \pi_i \wedge B_j^{(\beta)} \in \pi_j\}$  и  $\pi_i + \pi_j = \prod_{\text{Df}} \{\pi_k(X) \mid \pi_k \geq \pi_i, \pi_j\}$ , где  $\pi_i \leq \pi_j \Leftrightarrow \pi_i \cdot \pi_j = \pi_i$ . Относительно операций умножения и сложения всевозможные разбиения на  $X$  образуют полумодулярную решетку [3], которую будем обозначать через  $\mathfrak{Q}(X)$ . Определим для каждого разбиения  $\pi_i \in \mathfrak{Q}(X)$  энтропию

$$H(\pi_i) = - \sum_{\text{Df}}^{m_i} q(B_i^{(\alpha)}) \ln q(B_i^{(\alpha)}).$$

Функции энтропии присущи следующие свойства [4]:

- а) неотрицательность: для любого  $\pi_i(X)$  всегда  $H(\pi_i) \geq 0$ ;
- б) инвариантность: если  $\pi_i(X') \equiv \pi_j(X'')$ , то  $H(\pi_i) = H(\pi_j)$ ;
- в) рекурсивность: для любых  $\pi_i(X)$  и  $\pi_j(X)$  верно

$$H(\pi_i \cdot \pi_j) = H(\pi_i) + \sum_{\alpha=1}^{m_i} q(B_i^{(\alpha)}) H(\overline{\pi_j}(B_i^{(\alpha)})).$$

Пусть  $R^+$  — множество положительных вещественных чисел. Функцию  $F: \mathfrak{L}(X) \rightarrow R^+$  будем называть нижней полуоценкой  $\mathfrak{L}(X)$ , если только она удовлетворяет при любых  $\pi_i, \pi_j \in \mathfrak{L}(X)$  двум условиям:

- а)  $F(\pi_i) + F(\pi_j) \geq F(\pi_i \cdot \pi_j) + F(\pi_i + \pi_j)$ ;
- б)  $\pi_i \leq \pi_j \Rightarrow F(\pi_i) \geq F(\pi_j)$ .

Из леммы 1 [5] вытекает, что энтропия представляет собой нижнюю полуоценку для  $\mathfrak{L}(X)$ .

Примем, что  $\pi_i(X)$  квазинеzáвисимо относительно  $\pi_j(X)$  (обозначение  $\pi_i \perp \pi_j$ ), если только для любых  $B \in \pi_i + \pi_j$  и  $B_j^{(\alpha)} \in \pi_j$  при  $B_j^{(\alpha)} \subset B$  справедливо  $\overline{\pi_i}(B) \equiv \overline{\pi_i}(B_j^{(\alpha)})$ . Из определения квазинеzáвисимости непосредственно следует ее рефлексивность (т. е.  $(\forall \pi_i)(\pi_i \perp \pi_i)$ ).

**Теорема 1.** В любой решетке  $\mathfrak{L}(X)$  следующие условия равносильны:

- 1)  $\pi_i \perp \pi_j$ ;
- 2)  $\pi_j \perp \pi_i$ ;
- 3)  $H(\pi_i) + H(\pi_j) = H(\pi_i \cdot \pi_j) + H(\pi_i + \pi_j)$ ;
- 4) для любых  $B \in \pi_i + \pi_j$ ,  $B_i^{(\alpha)} \in \pi_i$  и  $B_j^{(\beta)} \in \pi_j$  при  $B_i^{(\alpha)}, B_j^{(\beta)} \subset B$  справедливо  $q_B(B_i^{(\alpha)} \cap B_j^{(\beta)}) = q_B(B_i^{(\alpha)}) q_B(B_j^{(\beta)})$ .

**Доказательство.** 1)  $\Leftrightarrow$  2)  $\Leftrightarrow$  3). Теорема 2 из [5].

3)  $\Rightarrow$  4). В силу свойства рекурсивности энтропии получаем

$$\begin{aligned} & H(\pi_i) + H(\pi_j) - H(\pi_i \cdot \pi_j) - H(\pi_i + \pi_j) = 0 \Rightarrow \\ & \Rightarrow H(\pi_i + \pi_j) + \sum_{B^{(\alpha)} \in \pi_i + \pi_j} q(B^{(\alpha)}) H(\overline{\pi_i}(B^{(\alpha)})) + \\ & + H(\pi_i + \pi_j) + \sum_{B^{(\beta)} \in \pi_i + \pi_j} q(B^{(\beta)}) H(\overline{\pi_j}(B^{(\beta)})) - H(\pi_i + \pi_j) - \\ & - \sum_{B^{(\gamma)} \in \pi_i + \pi_j} q(B^{(\gamma)}) H(\overline{\pi_i \cdot \pi_j}(B^{(\gamma)})) - H(\pi_i + \pi_j) = 0 \Rightarrow \\ & \Rightarrow \sum_{B^{(\alpha)} \in \pi_i + \pi_j} q(B^{(\alpha)}) [H(\overline{\pi_i}(B^{(\alpha)})) + H(\overline{\pi_j}(B^{(\alpha)})) - H(\overline{\pi_i \cdot \pi_j}(B^{(\alpha)}))] = 0 \Rightarrow \\ & \Rightarrow (\forall B^{(\alpha)} \in \pi_i + \pi_j) (H(\overline{\pi_i}(B^{(\alpha)})) + H(\overline{\pi_j}(B^{(\alpha)})) - H(\overline{\pi_i \cdot \pi_j}(B^{(\alpha)})) = 0). \end{aligned}$$

Пусть теперь  $B \in \pi_i + \pi_j$ . Тогда  $H(\overline{\pi_i}(B)) + H(\overline{\pi_j}(B)) - H(\overline{\pi_i \cdot \pi_j}(B)) = 0$ . Отсюда по теореме 1.2 из [6] выводим, что для любых  $B_i^{(\alpha)}, B_j^{(\beta)} \in B$  справедливо  $q_B(B_i^{(\alpha)} \cap B_j^{(\beta)}) = q_B(B_i^{(\alpha)}) q_B(B_j^{(\beta)})$ .

4)  $\Rightarrow$  1). Пусть для любых  $B_i^{(\alpha)} \in \pi_i$  и  $B_j^{(\beta)} \in \pi_j$  при  $B_i^{(\alpha)}, B_j^{(\beta)} \subset B \in \pi_i + \pi_j$  справедливо  $q_B(B_i^{(\alpha)} \cap B_j^{(\beta)}) = q_B(B_i^{(\alpha)}) q_B(B_j^{(\beta)})$ . Тогда, как легко проверить, отображение  $\varphi: (B_i^{(\alpha)} \cap B_j^{(\beta)}) \rightarrow B_i^{(\alpha)}$  устанавливает эквивалентность  $\overline{\pi_i}(B_j^{(\beta)}) \equiv \overline{\pi_i}(B)$ , откуда непосредственно следует  $\pi_i \perp \pi_j$ .

Из теоремы 1 вытекает, что отношение квазинезависимости является симметричным (т. е.  $(\forall \pi_i, \pi_j) (\pi_i \top \pi_j \Rightarrow \pi_j \top \pi_i)$ ). Итак, квазинезависимость представляет собой отношение толерантности (т. е. является рефлексивной и симметричной).

**Теорема 2.** *Отношение квазинезависимости  $\top$  обладает следующими свойствами:*

- а)  $(\forall \pi_i(X), \pi_j(X)) ((\forall B \in \pi_i + \pi_j) (\overline{\pi_i}(B) \leq \overline{\pi_j}(B) \vee \overline{\pi_i}(B) \geq \overline{\pi_j}(B)) \Rightarrow \pi_i \top \pi_j)$ ;
- б)  $\pi_i \top \pi_j \wedge \pi_k \geq \pi_i \Rightarrow \pi_i \top \pi_j \cdot \pi_k \wedge \pi_k \cdot (\pi_i + \pi_j) = \pi_i + \pi_j \cdot \pi_k$ ;
- в)  $\pi_{A1} \geq \pi_A \wedge \pi_{B1} \geq \pi_B \wedge \pi_A \top \pi_B \Rightarrow \pi_{A1} \cdot \pi_{B1} \top \pi_A \cdot \pi_B \wedge \wedge \pi_{A1} \cdot \pi_B + \pi_A \cdot \pi_{B1} = \pi_{A1} \cdot \pi_{B1} \cdot (\pi_A + \pi_B)$ ;
- г)  $\pi_i(X) \top \pi_j(X) \Rightarrow (\forall Z \supset X) (\underline{\pi_i}(Z) \top \underline{\pi_j}(Z))$ .

**Доказательство.** Свойства а) и г) следуют непосредственно из определения, а свойство б) — из леммы 2 и теоремы 3 [5]. Осталось доказать в). Действительно, так как  $\pi_{B1} \geq \pi_B \wedge \pi_A \top \pi_B \Rightarrow \pi_B \top \pi_A \cdot \pi_{B1}$  и  $\pi_{A1} \geq \pi_A \Rightarrow \pi_{A1} \geq \pi_A \cdot \pi_{B1}$ , то в силу свойства б) верно  $\pi_{A1} \cdot \pi_{B1} \top \pi_A \cdot \pi_{B1}$ . Далее получаем, что  $\pi_B \top \pi_A \cdot \pi_{B1} \wedge \pi_{A1} \geq \pi_A \cdot \pi_{B1} \Rightarrow \pi_{A1} \cdot (\pi_B + \pi_A \cdot \pi_{B1}) = \pi_{A1} \cdot \pi_B + \pi_A \cdot \pi_{B1}$ . С другой стороны,  $\pi_A \top \pi_B \wedge \pi_{B1} \geq \pi_B \Rightarrow (\pi_B + \pi_A \cdot \pi_{B1}) = \pi_{B1} \cdot (\pi_A + \pi_B) \Rightarrow \pi_{A1} \cdot (\pi_B + \pi_A \cdot \pi_{B1}) = \pi_{A1} \cdot \pi_{B1} \cdot (\pi_A + \pi_B)$ . Итак,  $\pi_{A1} \cdot \pi_{B1} + \pi_A \cdot \pi_{B1} = \pi_{A1} \cdot \pi_{B1} \cdot (\pi_A + \pi_B)$ .

При  $\pi_i(X) + \pi_j(X) = 1_X$  разбиения  $\pi_i$  и  $\pi_j$  будем называть ортогональными. Квазинезависимые и ортогональные разбиения  $\pi_i$  и  $\pi_j$  будем называть независимыми (обозначение  $\pi_i \top \pi_j$ ). Легко видеть, что отношение независимости  $\top$  антирефлексивно и симметрично. Можно показать, что отношение  $\pi_i(X) \top \pi_j(X)$  эквивалентно двум условиям:

- а)  $H(\pi_i) + H(\pi_j) = H(\pi_i \cdot \pi_j)$ ;
- б) для любых  $B_i^{(\alpha)} \in \pi_i$  и  $B_j^{(\beta)} \in \pi_j$  верно  $q(B_i^{(\alpha)} \cap B_j^{(\beta)}) = q(B_i^{(\alpha)})q(B_j^{(\beta)})$ .

Систему разбиений  $P(X) = \{\pi_1(X), \pi_2(X), \dots, \pi_w(X)\}$  будем называть независимой (квазинезависимой), если только для произвольных дизъюнктивных подсистем  $P', P'' \subset P$  (т. е.  $P' \cap P'' = \emptyset$ ) верно  $m(P') \top m(P'') \equiv m(P' \cdot P'')$ , где  $m(P^{(i)}) \stackrel{\text{Df}}{=} \prod_{\pi_h \in P^{(i)}} \pi_h$ .

**Теорема 3.** *Если для совокупности всех разбиений  $\pi_i(X)$  на всевозможных конечных множествах  $X$  существует функция с вещественной областью значений  $G(\pi_i)$ , инвариантная относительно отношения эквивалентности (т. е.  $\pi_i(X') \equiv \pi_j(X'') \Rightarrow G(\pi_i) = G(\pi_j)$ ), представляющая собой нижнюю полуоценку для каждой решетки  $\mathfrak{L}(X)$  и удовлетворяющая при любых  $\pi_i, \pi_j \in \mathfrak{L}(X)$  условию  $\pi_i \top \pi_j \Rightarrow G(\pi_i) + G(\pi_j) = G(\pi_i \cdot \pi_j) + G(\pi_i + \pi_j)$ , то  $G(\pi_i) = aH(\pi_i) + b$ , где  $a$  и  $b$  — некоторые положительные константы.*

Для доказательства теоремы 3 нам понадобится ряд лемм, при формулировке которых будем заменять функцию  $G$  функцией  $F$ , определяя ее для каждого  $\pi_i(X)$  через  $F(\pi_i(X)) \stackrel{\text{Df}}{=} G(\pi_i(X)) - G(1_X)$ .

**Лемма 1.** *Если  $\pi_i(X)$  и  $\pi_j(X)$  — однородные разбиения ранга  $s^n$  и  $s$  соответственно, то  $F(\pi_i) = nF(\pi_j)$ .*

**Доказательство.** Разбиение  $\pi_i$  в силу его однородности можно представить в виде произведения разбиений из независимой системы  $P_j(X) = \{\pi_j^{(1)}, \pi_j^{(2)}, \dots, \pi_j^{(n)}\}$  (т. е.  $\pi_i = m(P_j)$ ), где для любых  $\pi_j^{(\alpha)}$ ,

$\pi_j^{(\beta)} \in P_j$  верно  $\pi_j^{(\alpha)} \equiv \pi_j^{(\beta)} \equiv \pi_j$ . Поэтому, по определению независимости,  $F(\pi_i) = F(m(P_j)) = \sum_{\alpha=1}^n F(\pi_j^{(\alpha)}) = nF(\pi_j)$ .

Лемма 2. Пусть  $\pi_i(X)$  и  $\pi_j(X)$  — однородные разбиения ранга  $n$  и  $n+1$  соответственно. Тогда верно неравенство  $F(\pi_j) \geq F(\pi_i)$ .

Доказательство. Определим разбиения  $\pi_{i1}(Y)$  и  $\pi_{j1}(Y)$  так, чтобы  $\pi_{i1}(Y) \equiv \pi_i(X)$ ,  $\pi_{j1}(Y) \equiv \pi_j(X)$ ,  $\|Y\| = n^2(n+1)$  и

$$\|B_{i1}^{(\alpha)} \cap B_{j1}^{(\beta)}\|_{\text{Df}} = \begin{cases} n & \text{при } \beta=1; \\ 1 & \text{при } \beta=\alpha+1; \\ n+1 & \text{в остальных случаях.} \end{cases}$$

Такое определение корректно, ибо, как легко проверить, для любых  $B_{i1}^{(\alpha)} \in \pi_{i1}$  и  $B_{j1}^{(\beta)} \in \pi_{j1}$  справедливо  $\|B_{i1}^{(\alpha)}\| = \sum_{\gamma=1}^{m_{j1}} \|B_{i1}^{(\alpha)} \cap B_{j1}^{(\gamma)}\| = n(n+1)$

и  $\|B_{j1}^{(\beta)}\| = \sum_{\delta=1}^{m_{i1}} \|B_{i1}^{(\delta)} \cap B_{j1}^{(\beta)}\| = n^2$ . Определим теперь однородное разбиение  $\pi_0(Y)$  ранга  $n^2$ , принимая, что  $\pi_0(Y) \stackrel{\text{Df}}{=} \{B_0^{(\alpha\beta)} \mid \alpha = 1, \dots, n; \beta = 2, \dots, n+1\}$ , где  $B_0^{(\alpha\beta)} \stackrel{\text{Df}}{=} B_{i1}^{(\alpha)} \cap B_{j1}^{(\beta)}$  при  $\beta \neq \alpha+1$  и  $B_0^{(\alpha(\alpha+1))} \stackrel{\text{Df}}{=} B_{i1}^{(\alpha)} \cap (B_{j1}^{(\alpha+1)} \cup B_{j1}^{(\alpha)})$ .

Из определения ясно, что  $\pi_0 \geq \pi_{i1} \cdot \pi_{j1}$ . Поэтому, учитывая лемму 1, получаем  $F(\pi_{i1}) + F(\pi_{j1}) \geq F(\pi_{i1} \cdot \pi_{j1}) + F(\pi_{i1} + \pi_{j1}) \geq F(\pi_0) \Rightarrow F(\pi_i) + F(\pi_j) \geq 2F(\pi_i) \Rightarrow F(\pi_j) \geq F(\pi_i)$ .

Лемма 3. Для произвольного однородного разбиения  $\pi_i$  верно  $F(\pi_i) = a \ln \|\pi_i\|$ , где  $a$  — некоторая положительная константа.

Доказательство. Пусть  $\pi_i$ ,  $\pi_j$  и  $\pi_k$  — однородные разбиения при  $\|\pi_i\| = s^n$ ,  $\|\pi_j\| = t^m$  и  $\|\pi_k\| = t^{m+1}$ . Обозначая функцию  $F(\pi)$  однородного разбиения  $\pi$  ранга  $r$  через  $F(r)$ , по лемме 1 получаем, что  $F(s^n) = nF(s)$ ,  $F(t^m) = mF(t)$  и  $F(t^{m+1}) = (m+1)F(t)$ . Пусть теперь  $s$ ,  $t$  и  $n$  — произвольные натуральные числа при  $t > 1$ , а натуральное число  $m$  выбрано так, чтобы имело место неравенство  $t^m \leq s^n < t^{m+1}$ . Тогда  $m \ln t \leq n \ln s < (m+1) \ln t \Rightarrow m/n \leq \ln s / \ln t < (m/n + 1/n) \Rightarrow 0 \leq \ln s / \ln t - m/n < 1/n$ . С другой стороны, в силу леммы 2 справедливо  $t^m \leq s^n < t^{m+1} \Rightarrow F(t^m) \leq F(s^n) \leq F(t^{m+1}) \Rightarrow mF(t) \leq nF(s) \leq (m+1)F(t) \Rightarrow m/n \leq F(s)/F(t) \leq (m/n + 1/n) \Rightarrow 0 \leq F(s)/F(t) - m/n \leq 1/n$ .

Итак, получаем  $|F(s)/F(t) - \ln s / \ln t| \leq 1/n$ . Так как последнее неравенство должно выполняться при сколь угодно большом  $n$ , то, очевидно,  $F(s) = a \ln s$ . Лемма доказана.

Лемма 4. Если  $\pi_{i1}(X \setminus B)$ ,  $\pi_{i2}(X \setminus B)$ ,  $\pi_{j1}(B)$  и  $\pi_{j2}(B)$  — произвольные разбиения, тогда разбиения  $\pi'_{i1}(X) \stackrel{\text{Df}}{=} \{\pi_{i1}(X \setminus B) \cup \pi_{j1}(B)\}$ ,

$\pi''_{i1}(X) \stackrel{\text{Df}}{=} \{\pi_{i1}(X \setminus B) \cup \pi_{j2}(B)\}$ ,  $\pi'_{i2}(X) \stackrel{\text{Df}}{=} \{\pi_{i2}(X \setminus B) \cup \pi_{j1}(B)\}$  и  $\pi''_{i2}(X) \stackrel{\text{Df}}{=} \{\pi_{i2}(X \setminus B) \cup \pi_{j2}(B)\}$  удовлетворяют равенству  $F(\pi'_{i1}) - F(\pi''_{i1}) = F(\pi'_{i2}) - F(\pi''_{i2})$ .

Доказательство. В силу определения  $\pi_{i1}(X) \uparrow \pi_{j1}(X)$ ,  $\pi_{i1}(X) \uparrow \pi_{j2}(X)$ ,  $\pi'_{i1}(X) = \pi_{i1}(X) \cdot \pi_{j1}(X)$  и  $\pi''_{i1}(X) = \pi_{i1}(X) \cdot \pi_{j2}(X)$ . Обозначая  $\pi_0(X) \stackrel{\text{Df}}{=} \{B, X \setminus B\}$ , имеем  $F(\pi'_{i1}) - F(\pi''_{i1}) = F(\pi_{i1}(X) \cdot \pi_{j1}(X)) - F(\pi_{i1}(X) \cdot \pi_{j2}(X)) = F(\pi_{i1}(X)) + F(\pi_{j1}(X)) - F(\pi_0(X)) - F(\pi_{i1}(X)) - F(\pi_{j2}(X)) + F(\pi_0(X)) = F(\pi_{j1}(X)) - F(\pi_{j2}(X))$ . Тот же результат

получаем и для разности  $F(\pi'_{i2}) - F(\pi''_{i2})$ . Поэтому  $F(\pi'_{i1}) - F(\pi''_{i1}) = F(\pi'_{i2}) - F(\pi''_{i2})$ .

**Лемма 5.** Пусть даны произвольные разбиения  $\pi_i(X)$  и  $\pi_k(X)$  при  $\overline{\pi_k(B_i^{(\alpha)})} \equiv \overline{\pi_k(B_i^{(\beta)})} \equiv \overline{\pi_k(B_i^{(\alpha)} \cup B_i^{(\beta)})}$ , где  $\alpha \neq \beta$ . Тогда для  $\pi'_i(X) \stackrel{\text{Df}}{=} \overline{\pi_i(X \setminus B_i^{(\alpha)})} \cup \overline{\pi_k(B_i^{(\alpha)})}$ ,  $\pi''_i(X) \stackrel{\text{Df}}{=} \overline{\pi_i(X \setminus B_i^{(\beta)})} \cup \overline{\pi_k(B_i^{(\beta)})}$ ,  $\pi'''_i(X) \stackrel{\text{Df}}{=} \overline{\pi_i(X \setminus (B_i^{(\alpha)} \cup B_i^{(\beta)})} \cup \overline{\pi_k(B_i^{(\alpha)} \cup B_i^{(\beta)})}$  и  $\pi_{i0}(X) \stackrel{\text{Df}}{=} \overline{\pi_i(X \setminus (B_i^{(\alpha)} \cup B_i^{(\beta)})} \cup \overline{\pi_k(B_i^{(\alpha)} \cup B_i^{(\beta)})}$  верно

$$[F(\pi'_i) - F(\pi_i)] + [F(\pi''_i) - F(\pi_i)] = F(\pi'''_i) - F(\pi_{i0}).$$

**Доказательство.** Определим еще разбиения  $\pi'_0 \stackrel{\text{Df}}{=} \{X \setminus (B_i^{(\alpha)} \cup B_i^{(\beta)})$ ,  $B_i^{(\alpha)}, B_i^{(\beta)}\}$  и  $\pi_0 \stackrel{\text{Df}}{=} \{X \setminus (B_i^{(\alpha)} \cup B_i^{(\beta)})$ ,  $B_i^{(\alpha)} \cup B_i^{(\beta)}\}$ . Нетрудно видеть, что  $\pi'''_i \uparrow \pi'_0$  и поэтому  $F(\pi'''_i) + F(\pi'_0) = F(\pi'_i \cdot \pi'_0) + F(\pi_0)$ . Ясно также, что  $\pi_{i0} \uparrow \pi'_0$ , откуда  $F(\pi_{i0}) + F(\pi'_0) = F(\pi_0) + F(\pi_i)$ . Учитывая, что  $\pi'_i \uparrow \pi''_i$ , получаем

$$\begin{aligned} [F(\pi'_i) - F(\pi_i)] + [F(\pi''_i) - F(\pi_i)] &= F(\pi'_i \cdot \pi''_i) + F(\pi_i) - F(\pi_i) - \\ - F(\pi_i) &= F(\pi'''_i) + F(\pi'_0) - F(\pi_0) - F(\pi_i) = F(\pi'''_i) + F(\pi_0) + F(\pi_i) - \\ - F(\pi_{i0}) - F(\pi_0) - F(\pi_i) &= F(\pi'''_i) - F(\pi_{i0}). \end{aligned}$$

**Лемма 6.** Пусть  $\pi_i(X)$  — однородное разбиение ранга,  $n$ , а  $\pi_j(X)$  — произвольное разбиение при  $\pi_i \uparrow \pi_j$ . Тогда для любого  $B_i^{(\alpha)} \in \pi_i$  верно  $F(\pi_j^{(\alpha)}) - F(\pi_i) = 1/n F(\pi_j)$ , где  $\pi_j^{(\alpha)}(X) \stackrel{\text{Df}}{=} \overline{\pi_i(X \setminus B_i^{(\alpha)})} \cup \overline{\pi_j(B_i^{(\alpha)})}$ .

**Доказательство.** Действительно, из лемм 4 и 5 следует, что  $\sum_{\alpha=1}^n [F(\pi_j^{(\alpha)}) - F(\pi_i)] = F(\pi_j) - F(1_X) = F(\pi_j)$ . Так как  $\pi_i \uparrow \pi_j$ , то для любых  $B_i^{(\alpha)}, B_i^{(\beta)} \in \pi_i$  верно  $\overline{\pi_j(B_i^{(\alpha)})} \equiv \overline{\pi_j(B_i^{(\beta)})}$ , а в силу  $q(B_i^{(\alpha)}) = q(B_i^{(\beta)})$  верно и  $\pi_j^{(\alpha)} \equiv \pi_j^{(\beta)}$ . Поэтому  $F(\pi_j^{(\alpha)}) = F(\pi_j^{(\beta)})$ , откуда непосредственно выводим, что  $(\forall B_i^{(\alpha)} \in \pi_i) ((F(\pi_j^{(\alpha)}) - F(\pi_i)) = 1/n F(\pi_j))$ .

**Лемма 7.** Пусть даны произвольные разбиения  $\pi_i(X)$  и  $\pi_j(B_i^{(\alpha)})$ , а  $\pi_k(X) \stackrel{\text{Df}}{=} \overline{\pi_i(X \setminus B_i^{(\alpha)})} \cup \overline{\pi_j(B_i^{(\alpha)})}$ . Тогда  $F(\pi_k) = F(\pi_i) + q_X \times \times (B_i^{(\alpha)}) F(\pi_j(B_i^{(\alpha)}))$ .

**Доказательство.** Пусть  $m$  — натуральное число, кратное  $\|X\|$  и  $\|B_i^{(\alpha)}\|$ , а на множестве  $Z \supset X$  при  $\|Z\| = m$  определены некоторые сюръективные отображения  $\varphi_1: Z \rightarrow X$  и  $\varphi_2: Z \rightarrow B_i^{(\alpha)}$ , удовлетворяющие условиям: 1)  $\varphi_k(\varphi_k(Z)) = \varphi_k(Z)$ ; 2)  $(\forall x_i, x_j \in \varphi_k(Z)) (\|\varphi_k^{-1}(x_i)\| = \|\varphi_k^{-1}(x_j)\|)$ , где  $k=1, 2$ . Определим теперь разбиения  $\pi_{i1}(Z)$ ,  $\pi_{j1}(Z)$  и  $\pi_{k1}(Z)$  эквивалентные  $\pi_i(X)$ ,  $\pi_j(B_i^{(\alpha)})$  и  $\pi_k(X)$  соответственно, принимая, что любые  $B_{i1}^{(\beta)} \in \pi_{i1}$ ,  $B_{j1}^{(\gamma)} \in \pi_{j1}$  и  $B_{k1}^{(\delta)} \in \pi_{k1}$  выражаются через  $B_{i1}^{(\beta)} \stackrel{\text{Df}}{=} \varphi_1^{-1}(B_i^{(\beta)})$ ,  $B_{j1}^{(\gamma)} \stackrel{\text{Df}}{=} \varphi_2^{-1}(B_i^{(\gamma)})$  и  $B_{k1}^{(\delta)} \stackrel{\text{Df}}{=} \varphi_1^{-1}(B_i^{(\delta)})$ . Пусть еще  $\pi_{\alpha 0}(Z) \stackrel{\text{Df}}{=} \overline{\pi_{i1}(Z \setminus B_{i1}^{(\alpha)})} \cup \overline{\pi_{j1}(B_{i1}^{(\alpha)})}$  и  $\pi_0(Z) \stackrel{\text{Df}}{=} \{X, Z \setminus X\}$ . Тогда, согласно определению  $m$ , для  $\pi_{j1}(Z)$  всегда найдется однородное разбиение  $\pi_\alpha(Z)$  ранга  $m/\|B_i^{(\alpha)}\|$  при  $B_{i1}^{(\alpha)} \in \pi_\alpha$  такое, что  $\pi_\alpha(Z) \uparrow \pi_{j1}(Z)$ . Учитывая это, из лемм 4 и 6

Получим  $\bar{F}(\underline{\pi}_h(\bar{Z})) - F(\underline{\pi}_i(\bar{Z})) = F(\underline{\pi}_j(Z)) - F(\pi_{\alpha 0}(Z)) = F(\underline{\pi}_j(\bar{Z}) \cdot \pi_{\alpha}(Z)) - F(\pi_{\alpha}(Z)) = \|B_i^{(\alpha)}\|/mF(\pi_{j1}(Z)) = \|B_i^{(\alpha)}\|/mF(\pi_j(B_i^{(\alpha)}))$ , а из леммы 6 —

$$F(\underline{\pi}_i(Z)) - F(\pi_0(Z)) = \|X\|/mF(\pi_{i1}(Z)) = \|X\|/mF(\pi_i(X))$$

и

$$F(\underline{\pi}_h(Z)) - F(\pi_0(Z)) = \|X\|/mF(\pi_{h1}(Z)) = \|X\|/mF(\pi_h(X)).$$

Поэтому

$$\begin{aligned} F(\pi_h(X)) - F(\pi_i(X)) &= \\ &= m/\|X\| [F(\underline{\pi}_h(Z)) - F(\pi_0(Z))] - m/\|X\| [F(\underline{\pi}_i(Z)) - \\ &\quad - F(\pi_0(Z))] = m/\|X\| [F(\underline{\pi}_h(Z)) - F(\underline{\pi}_i(Z))] = \\ &= m \|B_i^{(\alpha)}\|/m \|X\| F(\pi_j(B_i^{(\alpha)})) = q_X(B_i^{(\alpha)}) F(\pi_j(B_i^{(\alpha)})), \end{aligned}$$

что и требовалось доказать.

**Лемма 8.** Для произвольных разбиений  $\pi_i(X)$  и  $\pi_j(X)$  справедливо

$$F(\pi_i \cdot \pi_j) = F(\pi_i) + \sum_{\alpha=1}^{m_i} q(B_i^{(\alpha)}) F(\overline{\pi}_j(B_i^{(\alpha)})).$$

**Доказательство.** Представим произведение  $\pi_i \cdot \pi_j$  в виде  $\pi_i \cdot \pi_j = \{\overline{\pi}_j(B_i^{(1)}) \cup \overline{\pi}_j(B_i^{(2)}) \cup \dots \cup \overline{\pi}_j(B_i^{(m_i)})\}$ . Пусть теперь  $\pi_{j\alpha}(X) \stackrel{\text{Df}}{=} \overline{\pi}_j(B_i^{(\alpha)})$ .

Тогда по лемме 7 получаем, что  $\pi_i \cdot \pi_j \stackrel{\text{Df}}{=} \{\overline{\pi}_i(X \setminus B_i^{(\alpha)}) \cup \overline{\pi}_j(B_i^{(\alpha)})\}$ . Тогда по лемме 7 получаем, что

$$\sum_{\alpha=1}^{m_i} [F(\pi_{j\alpha}) - F(\pi_i)] = \sum_{\alpha=1}^{m_i} q_X(B_i^{(\alpha)}) F(\overline{\pi}_j(B_i^{(\alpha)})).$$

С другой стороны, из того, что система разбиений  $\{\pi_{j1}, \pi_{j2}, \dots, \pi_{j\alpha}, \dots, \pi_{jm_i}\}$  является квази-

независимой и  $\prod_{\alpha=1}^{m_i} \pi_{j\alpha} = \pi_i \cdot \pi_j$ , следует  $\sum_{\alpha=1}^{m_i} [F(\pi_{j\alpha}) - F(\pi_i)] =$

$$= F(\pi_i \cdot \pi_j) - F(\pi_i). \text{ Итак, } F(\pi_i \cdot \pi_j) = F(\pi_i) + \sum_{\alpha=1}^{m_i} q_X(B_i^{(\alpha)}) F(\overline{\pi}_j(B_i^{(\alpha)})).$$

Эти восемь лемм позволяют завершить

Доказательство теоремы 3. Для любого разбиения  $\pi_i(X)$

$$\text{получаем } F(\pi_i \cdot 0_X) = F(0_X) = a \ln \|X\| = F(\pi_i) + \sum_{\alpha=1}^{m_i} q(B_i^{(\alpha)}) F(\overline{0}_X(B_i^{(\alpha)})) =$$

$$= F(\pi_i) + a \sum_{\alpha=1}^{m_i} q(B_i^{(\alpha)}) \ln \|B_i^{(\alpha)}\| \Rightarrow F(\pi_i) = a \ln \|X\| - a \sum_{\alpha=1}^{m_i} q(B_i^{(\alpha)}) \ln \|B_i^{(\alpha)}\| =$$

$$= -a \sum_{\alpha=1}^{m_i} q(B_i^{(\alpha)}) \ln q(B_i^{(\alpha)}) = aH(\pi_i).$$

Пусть теперь  $Y$  — произвольное конечное множество и  $b \stackrel{\text{Df}}{=} G(1_X)$ .

Тогда из  $1_X \equiv 1_Y$  вытекает  $G(1_X) = G(1_Y) = b$ , а отсюда, в свою очередь,  $G(\pi_i(X)) = F(\pi_i(X)) + G(1_X) = aH(\pi_i) + b$ , что и требовалось доказать.

Автор выражает глубокую благодарность А. Таутсу за ценные замечания.

## ЛИТЕРАТУРА

1. Nakamura Y. Kōdai Math. Semin. Repts, 22, 443—468 (1970).
2. Hartmanis J., Stearns R. E. Algebraic Structure Theory of Sequential Machines. Prentice-Hall, Inc., Englewood Cliffs, New York, 1966.
3. Birkhoff G. Lattice Theory. Amer. Math. Soc., New York City, 1948.
4. Лаусмаа Т. Изв. АН ЭССР, Физ. Матем., 30, № 3, 226—233 (1981).
5. Лаусмаа Т. Изв. АН ЭССР, Физ. Матем., 31, № 4, 390—398 (1982).
6. Watanabe S. Knowing and Guessing. John Wiley and Sons, Inc., New York, 1969.

Институт термодинамики и электрофизики  
Академии наук Эстонской ССР

Поступила в редакцию  
21 сентября 1982

T. LAUSMAA

### ENTROOPIA ALGEBRALISEST MÄÄRANGUST

Artikkelis jätkub lõplikul hulgal määratud tükelduse kui informatsiooni algebraise interpretatsiooni omaduste vaatlus (algus vt. [2]). On näidatud, et sõltumata tõesaosuslikust käsitlusest võib Shannoni valemiga esitatud entroopia mõisteni jõuda ka tükeldusvõrel määratud alumise poolehinnangu kaudu.

T. LAUSMAA

### ON THE ALGEBRAIC FOUNDATIONS OF THE CONCEPT OF ENTROPY

As a rule, the Shannon's formula for entropy is interpreted from the probabilistic point of view. But as a fact, the formula has algebraic foundations based on the notion of semivaluation for lattices as well. The algebraic approach gives us a new independent induction of the Shannon's formula from fundamental concepts in mathematics, providing a nonprobabilistic entropy well suited for studies of the informational properties of an individual object with no statistical origin.

The basic notion of this approach is a partition on a finite set which is interpreted as in [2] for an algebraic form of the notion of information. Founded on the informational properties of partition, the notion of quasi-independence between partitions is introduced as a generalization of the well-known notion of informational independence.

The basic result of the paper can be formulated as follows. If a real-valued function on all finite partitions on finite sets is invariant relative to equivalence relation on partitions [4,5] being a meet semivaluation [1] for all finite lattices of partitions and going over to a valuation only in the case of quasi-independent partitions, the function is a linear transform of the Shannon's entropy.