Otokar Grošek

Энтропия на алгебраических структурах

Mathematica Slovaca, Vol. 29 (1979), No. 4, 411--424

Persistent URL: http://dml.cz/dmlcz/136221

Math. Slovaca 29, 1979, No. 4, 411—424

ЭНТРОПИЯ НА АЛГЕБРАИЧЕСКИХ СТРУКТУРАХ

ОТОКАР ГРОШЕК

Методы, применимые в сегодня уже «классической» теории информации были в первую очередь естественным образом продолжены в работах Колмогорова и Синая. (Обзор дан например в книгах [1], [11].) Позже была опубликована статья трех американских математиков [7], где была введена топологическая энтропия. Риечан в статье [10] изучал некоторые общие свойства топологической энтропии и энтропии Колмогорова–Синая. Ввел общую схему, частичным случаем которой являются эти энтропии.

В настоящей работе исходим из этой общей схемы. При этом стоят в центре внимания алгебраические аспекты, которым не было до сих пор посвящено надлежащее внимание.

1. Введение

Напомним некоторые основные алгебраические понятия и свойства.

Частично упорядоченное множество S называется верхней полуструктурой, если каждое двухэлементное подмножество $\{a, b\}$ множества S имеет объединение в S; в этом случае $a \leqq b$ эквивалентно равенству $a \vee b = b$ ([3], стр. 44).

В верхней полуструктуре справедливо: Если $x \leqq y$ и $u \leqq v$, то $x \vee u \leqq y \vee v$.

Пусть S_1, S_2 – две верхние полуструктуры, а f – гомоморфизм, $f\colon S_1 \to S_2$. Тогда не трудно показать, что f сохраняет упорядочение. Справедливо следующее утверждение: Если $x \leqq y$, т.е. $y = x \vee y$, тогда $f(y) = f(x \vee y) = f(x) \vee f(y)$. Значит, $f(x) \leqq f(y)$, что и требовалось доказать.

Полуструктура S называется полугруппой Кронекера, если выполняется: $x \vee y = 0$ для всех $x \neq y$.

Буквой Z будем обозначать множество целых чисел, а кардинальное число множества M будем обозначать через $|M|$.

Определение 1. *Пусть S – верхняя полуструктура и T – эндоморфизм на S. Энтропия – это функция $H\colon S \to \langle 0, \infty)$ обладающая следующими свойствами:*

а) *Если* $x \leqq y$, *то* $H(x) \leqq H(y)$;

б) $H(Tx) \leqq H(x)$;

в) $H(x \vee Tx \vee \ldots \vee T^n x) \leqq H(x \vee Tx \vee \ldots \vee T^j x) + H(T^{j+1}x \vee \ldots \vee T^n x)$

для всех $x \in S$, $n > 0$ *и* j, $0 \leqq j \leqq n-1$.

Примечание 1. Ясно, что энтропия H зависит от S и T и для произвольных S и T всегда существует по крайней мере одна энтропия, а именно: $H = \text{const}$.

Примечание 2. Свойство в) из определения 1 слабее чем, свойство

в′) $H(x \vee y) \leqq H(x) + H(y)$,

потому что из в) не вытекает в′). Чтобы показать это, достаточно положить $S = \{x, y, x \vee y\}$, пусть T – тождественный автоморфизм и выполняется $H(x) = 2$, $H(y) = 3$, $H(x \vee y) = 6$. Тогда H – энтропия, но $H(x \vee y) > H(x) + H(y)$.

В дальнейшем положим $H(x \vee Tx \vee \ldots \vee T^{n-1}x) = H_n(x)$.

Определение 2. *Упорядоченая пара* (S, T) *называется базисом энтропии* H, *если* S – *верхняя полуструктура,* T – *эндоморфизм, определеный на* S, *а* H – *энтропия.*

Определение 3. *Пусть* (S, T) – *базис энтропии* H. L – *энтропией (=предельной энтропией) элемента* $x \in S$ *называется функция* h, *определенная равенством:*

$$h(x) = \lim_{n \to \infty} n^{-1} H_n(x)$$

для всех $x \in S$.

Примечание 3. Доказательство существования предела смотри, например, в [7], [10].

Лемма 1.

$$h(x) = h\left(\bigvee_{j=0}^{k} T^j x\right)$$

для всех натуральных чисел k.

Доказательство. Согласно определению 3 можно писать:

$$h(x) = \lim_{n \to \infty} (n+k-1)^{-1} H_{n+k-1}(x) = \lim_{n \to \infty} (n+k-1)^{-1} \cdot$$

$$\cdot H[(x \vee Tx \vee \ldots \vee T^k x) \vee T(x \vee Tx \vee \ldots \vee T^k x) \vee \ldots \vee T^{n-1}(x \vee Tx \vee \ldots \vee T^k x)].$$

Это равенство верно ввиду того, что все элементы S – идемпотенты и T – эндоморфизм. Если положим $u = x \vee Tx \vee \ldots \vee T^k x$, получим

$$h(x) = \lim_{n \to \infty} (n+k-1)^{-1} H_n(u) = \lim_{n \to \infty} n(n+k-1)^{-1} \cdot \lim_{n \to \infty} n^{-1} H_n(u) = h(u).$$

Теорема 1. *L – энтропия является энтропией в смысле определения 1.*

Доказательство. 1) Если мы применим последовательно изотонность эндоморфизма T, Получим для $x \leqq y$ отношение

$$\bigvee_{i=0}^{n-1} T^i x \leqq \bigvee_{i=0}^{n-1} T^i y.$$

Теперь достаточно применить монотонность энтропии H и определение 3.

2) Докажем, что для всех $x \in S$ выполняется $h(x) = h(Tx)$. Из свойств функции H вытекает, что $H_{n+1}(x) \leqq H(x) + H_n(Tx)$, т.е. $h(x) \leqq h(Tx)$. С другой стороны, из монотонности H вытекает, что $H_n(Tx) \leqq H_{n+1}(x)$, т.е. $h(Tx) \leqq h(x)$. Следовательно, $h(x) = h(Tx)$.

3) Свойство в) из определения 1 просто и вытекает из леммы 1.

Следовательно, базис энтропии H является тоже базисом соответствующей L – энтропии. L – энтропия h, это специальный выбор энтропии, принадлежащей базису (S, T). Кроме того, L – энтропия, принадлежащая к данной L – энтропии, является функцией тождественно равной нулю, что непосредственно вытекает из леммы 1.

Примечание 4. Если полуструктура S имеет нуль, конечное число элементов или если T – тождественное отображение, то $h(x) = 0$ для всех $x \in S$.

Ввиду примечания 1 возможно к базису (S, T) энтропии H определить еще одну энтропию.

Определение 4. *Энтропия эндоморфизма T при определенном базисе (S, T) – это число (может быть тоже ∞)*

$$h\overset{*}{T} = \sup_{x \in S} h(x).$$

Примечание 5. Если (S, T) – базис энтропии H, то для $k > 0$ (S, T^k) уже не должна быть базисом энтропии H и наоборот, как показывают следующие примеры.

Пример 1. Пусть S и H имеют то самое значение, как в примечании 2: $S = \{x, y, x \vee y\}$, $H(x) = 2$, $H(y) = 3$ и $H(x \vee y) = 6$. Определим эндоморфизм T равенствами: $Tx = y$, $Ty = x$ и $T(x \vee y) = x \vee y$. Тогда (S, T^2) – базис энтропии H, но (S, T) не является базисом ввиду того, что

$$6 = H(x \vee Tx) > H(x) + H(Tx) = 5.$$

Пример 2. В этом примере быдет (S, T) базисом энтропии H, в то время как (S, T^2) не будет. Пусть S – свободная полуструктура над множеством $X = \{x_i ; i \in Z\}$. Пусть T – сдвиг, т.е. если $u = x_i \vee x_j \vee \ldots \vee x_k$, то $Tu = x_{i+1} \vee x_{j+1} \vee \vee \ldots \vee x_{k+1}$, а функция H определена следующим образом: $H(u) = 2{,}5$ для

$$u \in G = \{x_i \vee x_{i+2};\ i \in Z\} \text{ и } H(u) = \|u\| \text{ для } u \in S - G,$$

где $\|u\|$ – длина слова $u \in S$. Покажем, что (S, T) – базис энтропии H.

Функция H, очевидно, сохраняет упорядочение, так как $u \leqq v$ влечет за собой $\|u\| \leqq \|v\|$.

Так как сдвиг сохраняет «расстояния» между индексами, то $H(Tu) = H(u)$ для всех $u \in S$.

Остается показать, что H полуаддитивная функция относительно операции „$\vee$“. 1) Если $v \notin G$, то

$$\bigvee_{i=0}^{n} T^i v \notin G$$

для произвольного n. Кроме того, $\|u \vee v\| \leqq \|u\| + \|v\|$ и, следовательно, (используя $H(Tu) = H(u)$) $H_n(v) \leqq H_j(v) + H_{n-j}(v)$ для $1 \leqq j \leqq n$.

2) Если $v \in G$, то $H_n(v) = n + 2$ для $n > 1$ и

$$H_n(v) \leqq \begin{cases} H_1(v) + H_1(v) = 5 & \text{для } n = 2; \\ H_1(v) + H_{n-1}(v) = 2{,}5 + n + 2 & \text{для } n > 2; \\ H_j(x) + H_{n-j}(v) = j + 2 + n - j + 2 & \text{для } 1 < j < n - 1. \end{cases}$$

Следовательно, (S, T) – базис энтропии H, но (S, T^2) не является базисом для H. Дело в том, что $H(x_i \vee T^2 x_i) = 2{,}5 > H(x_i) + H(T^2 x_i) = 2$. Так как отображение T «линейно» увеличивает индексы, то выполняется

$$h(u) = \lim_{n \to \infty} n^{-1} H_n(x_i) = 1 = h\{T\}.$$

(Доказательство этого равенства смотри в примере 6.)

Примечание 6. Если бы мы рассматривали в примере 2 вместо множества G множество $G_k = \{x_i \vee x_{i+k};\ i \in Z\}$, то (S, T) – базис, а (S, T^k) не является базисом энтропии.

Теорема 2. *Пусть k – натуральное число и пусть (S, T) и (S, T^k) – базисы энтропии H. Тогда справедливо равенство: $h\{T^k\} = k \cdot h\{T\}$.*

Доказательство смотри, например в [7], [10].

Пример 3. Если в примере 2 «выгладим» функцию H, т.е. определим $H'(u) = \|u\|$ для всех $u \in S$, то (S, T) и (S, T^k) будут базисами энтропии H' и, следовательно, $h\{T^k\} = k \cdot h\{T\}$, $h\{T\} = 1$.

2. Теоремы для вычисления энтропии эндоморфизма

В энтропии Колмогорова–Синая существуют специальные разбиения, которые достаточно применить, чтобы вычислить соответствующую энтропию метрического автоморфизма. Следуя эту идею, Риечан определил в [10]

некоторое подмножество Q полуструктуры S. (Определение 5.) В теореме 3 покажем, что Q – полугруппа Кронекера. В определении 6 определим некоторое подмножество полуструктуры S, которое можно использовать для вычисления энтропии эндоморфизма.

Определение 5. *Пусть (S, T) – базис некоторой энтропии и $Q \subset S$. Будем говорить, что Q – характеристическое множество для базиса (S, T), если выполнены следующие условия:*

i) Если $0 \in S$, то $0 \in Q$;

ii) Для всякого $x \in S$, $x \neq 0$, существует $y \in Q$, $y \neq 0$, и число k так, что

$$\bigvee_{i=0}^{k} T^i y \geqq x;$$

iii) Q – это наименьшее подмножество S со свойствами i) соотв. ii) в том смысле, что не существует $Q' \subsetneqq Q$ со свойствами i) и ii).

Теорема 3. *Пусть Q – характеристическое множество для базиса (S, T). Тогда выполнено одно из следующих условий:*

а) $Q = \{y\}$, т.е. Q имеет только один элемент;

б) Q содержит 0 и Q – полугруппа Кронекера.

Доказательство. Предположим, что Q – характеристическое множество для (S, T), и пусть $y_1 \neq y_2$; $y_1, y_2 \in Q$. Тогда y_1 и y_2 несравнимые элементы. Действительно, если $y_1 < y_2$, то y_1 можно исключить и, следовательно, Q не удовлетворяет условию iii) определения 5. Это противоречит предположению теоремы.

Рассмотрим элемент $x = y_1 \vee y_2 \in S$. Покажем, что $x = 0$. Если бы $x \neq 0$, то существовало бы такое $y^* \in Q$, $y^* \neq 0$, что

$$\bigvee_{i=0}^{k} T^i y^* \geqq y_1 \vee y_2 \geqq y_1,$$

(соотв. $\geqq y_2$). Очевидно, элемент y^* не сравним ни с y_1, ни с y_2. Следовательно, из этих неравенств мы получаем:

$$T\left(\bigvee_{i=0}^{k} T^i y^*\right) = Ty_1, \quad \bigvee_{i+1}^{k+1} T^i y \geqq Ty_1,$$

$$y^* \vee \bigvee_{i+1}^{k+1} T^i y^* = \bigvee_{i=0}^{k+1} T^i y^* \geqq Ty_1.$$

Значит,

$$\bigvee_{i=0}^{k+1} T^i y^* \geqq Ty_1, \quad \bigvee_{i=0}^{k+2} T^i y^* = T^2 y_1, \ldots, \quad \bigvee_{i=0}^{k+m} T^i y^* = T^m y_1.$$

Если мы теперь перемножим левые и правые стороны последних неравенств, то мы получим:

$$\bigvee_{i=0}^{k+m} T^i y^* \geqq \bigvee_{i=0}^{m} T^i y_1 \tag{1}$$

для всех $m = 1, 2, \ldots$ Так как $y^* \in Q$, $y^* \neq 0$, то Q не является минимальным, а это противоречие.

Значение характеристического множества в следующем:

Теорема 4. *Пусть Q – характеристическое множество для (S, T). Тогда*

$$h^{\ddagger} = \max_{y \in Q} h(y).$$

Доказательство. Рассмотрим два случая (ввиду теоремы 3). Если $0 \in Q$, то ввиду примечания 4 $h(x) = 0$ для всех $x \in S$. Следовательно, $h^{\ddagger} = 0$. Если $0 \notin Q$, то $Q = \{y\}$. Согласно лемме 1

$$h(y) = h\left(\bigvee_{i=0}^{k} T^i y\right)$$

и по определению 5 для всех $x \in S$ существует k так, что

$$x \leqq \bigvee_{i=0}^{k} T^i y.$$

Следовательно,

$$h(x) \leqq h\left(\bigvee_{i=0}^{k} T^i y\right) = h(y), \quad h^{\ddagger} = \sup_{x \in S} h(x) = h(y).$$

Примечание 7. Пусть $\mathscr{S}$ – система всех подполуструктур полуструктуры S. Определим отображение τ: $Q \to \mathscr{S}$ следующим образом:

а) Если $y \in Q$, $y \neq 0$, то

$$\tau(y) = \left\{x; \bigvee_{i=0}^{k} T^i y \geqq x, \ x \in S\right\};$$

б) Если $0 \in S$, то $\tau(0) = \{0\}$.

Это отображение индуцирует на S топологию. Этой топологии посвящена работа [2].

Определение 6. *Пусть G – подмножество коммутативной полугруппы S. Множество G называется почти идеалом в S, если выполнено следующее условие: Для всякого $s \in S$ существует $g \in G$, что $sg \in G$.*

Примечание 8. В дальнейшем S обозначает верхнюю полуструктуру. Почти идеалом будет посвящена работа [9].

Теорема 5. *Пусть (S, T) – базис некоторой энтропии H и G – почти идеал в верхней полуструктуре S. Тогда*

$$h\ddagger = \sup_{g \in G} h(g).$$

Доказательство. Имеет место:

$$\sup_{g \in G} h(g) \leqq \sup_{x \in S} h(x) = h\ddagger.$$

С другой стороны, для всякого $x \in S$ существует $g' \in G$, что $x \vee g' = g \in G$. Следовательно, $h(g) = h(x \vee g') \geqq h(x)$,

$$\sup_{g \in G} h(g) \geqq \sup_{x \in S} h(x) = h\ddagger,$$

что и требовалось показать.

Следствие 1. *Пусть $\{x_i\}_{i=1}^{\infty}$ – последовательность элементов S и пусть для всякого $u \in S$ существует n так, что $x_n \geqq u$. Тогда*

$$h\ddagger = \lim_{n \to \infty} h(x_n).$$

Доказательство. Достаточно положить $G = \{x_i;\ i = 1, 2, \ldots\}$.

Следствие 2. *Пусть $Q = \{y\}$ и*

$$G = \left\{ \bigvee_{i=0}^{k} T^i y;\ k = 0, 1, 2, \ldots \right\}.$$

Тогда

$$\lim_{k \to \infty} h\left(\bigvee_{i=0}^{k} T^i y \right) = \lim_{k \to \infty} h(y) = h(y) = h\ddagger.$$

Последовательность из следствия 1 в работе [7] называется "refining".

В примере 2, очевидно, не существует характеристическое множество для базиса энтропии. Никакое одноэлементное подмножество не удовлетворяет условиям i)–iii) из определения 5 и, кроме того, $0 \notin S$.

В примере 1 для базиса (S, T^2) выполняется $S = Q$.

В следующем тривиальном примере Q будет одноэлементным множеством.

Пример 4. Пусть S – полуструктура натуральных чисел с операцией $a \vee b = \max\{a, b\}$, отображение T определим равенством $Ta = a + 1$ и пусть энтропия $H = \text{const}$.

Так как $\bigvee_{i=0}^{k} T^i a = a + k$, то $Q = \{q\}$, где q – любой элемент полуструктуры S.

3. Изоморфизм базисов энтропии

В этом параграфе объясним, при каких условиях два базиса энтропии изоморфны. Кроме того, покажем, что энтропия отображения, вообще гово-

ря, не является полным инвариантом для базиса энтропии в следующем смысле: Если (S, T_1) и (S, T_2) – два базиса энтропии H и, кроме того, $h^*_{T_1} = h^*_{T_2}$, то они не должны быть изоморфны (Определение 7.).

Определение 7. *Пусть (S_1, T_1), (S_2, T_2) – два базиса некоторых энтропий H, соотв. H'. Говорят, что (S_1, T_1) можно погрузить в (S_2, T_2), если существует гомоморфизм f: $S_1 \to S_2$ так, что для всякого $x \in S_1$ выполняется:*

а) $f(T_1 x) = T_2 f(x)$;

б) $H'(f(x)) = H(x)$.

Если f – изоморфизм, говорят что базисы изоморфны.

Теорема 6. *Пусть (S_1, T_1) можно погрузить в (S_2, T_2). Тогда выполняется:*

а) $h(x) = h'(f(x))$;

б) $h^*_{T_1} \leqq h^*_{T_2}$;

б) Если f – изоморфизм, то $h^*_{T_1} = h^*_{T_2}$.

Доказательство этой теоремы является следствием определения 7. (Смотри тоже [10].)

Теорема 7. *Пусть f – изоморфизм базисов (S_1, T_1) и (S_2, T_2). Кроме того, пусть Q_1 – характеристическое множество для (S_1, T_1). Тогда $f(Q_1) = Q_2$ – характеристическое множество для (S_2, T_2).*

Доказательство. Требуется доказать во-первых, что Q_2 удовлетворяет свойствам i) и ii) определения 5. Выберем $q \in Q_1$ и $x \in \tau(q)$ (Смотри прим. 7.). Из неравенства

$$\bigvee_{i=0}^{k} T_1^i q \geqq x$$

вытекает:

$$f\left(\bigvee_{i=0}^{k} T_1^i q\right) = \bigvee_{i=0}^{k} T_2^i f(q) \geqq f(x).$$

Теперь докажем, что множество Q_2 удовлетворяет свойству iii). Приведем доказательство от противного. Пусть множество $Q_2' = f(Q_1) - \{f(q)\}$ удовлетворяет условиям i) и ii) характеристического множества. Согласно первой части доказательства множество $f^{-1}(Q_2')$ удовлетворяет первым двум свойствам характеристического множества. Кроме того, $q \notin f^{-1}(Q_2')$ и $Q_1 \supset \supset f^{-1}(Q_2')$, а это противоречит минимальности множества Q_1.

Теорема 8. *Пусть Q и Q' – два характеристических множества для базиса (S, T). Тогда $|Q| = |Q'|$.*

Доказательство. Рассмотрим два случая. 1) Пусть $Q = \{y\}$ и $|Q'| > |Q|$. Согласно теореме 3 $0 \in Q'$ (соотв. $0 \in S$), а это и противоречит предположению $Q = \{y\}$. 2) Пусть теперь $|Q'| > |Q| > 1$. Тогда существуют элементы

$y \in Q$ и $p_1, p_2 \in Q'$ так что $y \in \tau(p_1) \cap \tau(p_2)$. Согласно определению характеристического множества существуют числа k_1, k_2 так, что выполняется:

$$\bigvee_{i=0}^{k_1} T^i p_1 \geqq y, \quad \bigvee_{i=0}^{k_2} T^i y \geqq p_2.$$

Точно так же, как в доказательстве теоремы 3

$$\bigvee_{i=0}^{k_1+k_2} T^i p_1 \geqq \bigvee_{i=0}^{k_2} T^i y \geqq p_2,$$

т.е. $p_2 \in \tau(p_1)$. Последнее противоречит минимальности множества Q'.

Следствие. *Если базисы* (S_1, T_1) *и* (S_2, T_2) *изоморфны, то справедливо равенство* $|Q_1| = |Q_2|$.

Доказательство вытекает из теорем 7 и 8.

Пример 5. Пусть $S_1 = \{1, 0\}$, T – тождественное отображение и $H' = \text{const}$. Пусть, далее, (S, T) – базис энтропии $H = \text{const}$ из примера 4. Тогда можно базис (S, T) при помощи гомоморфизма $f(a) = 1$ для всех $a \in S$ погрузить в базис (S_1, T_1). Кроме того, у (S_1, T_1) существует характеристическое множество $Q_1 = S_1$, а для (S, T) характеристическое множество не существует.

Вопрос, при каких условиях из равенства $|Q_1| = |Q_2|$ вытекает изоморфизм базисов является открытым.

В примере 6 определим один специальный базис энтропии. Он будет изоморфный базису из примера 3, а это нам позволит вычислить соответствующие L-энтропии.

Пример 6. Обозначим S_1 полуструктуру всех конечных подмножеств множества Z с операцией $A \vee B = A \cup B$. Обозначим g функцию $g(a) = a - 1$, $a \in Z$ и определим $T_1 A = g^{-1}(A)$. Не трудно показать, что (S_1, T_1) – базис энтропии $\hat{H}$: $\hat{H}(A) = |A|$, $A \in S_1$. Для соответствующей L-ентропии выполняется:

$$\hat{h}(A) = \lim_{n \to \infty} n^{-1} \cdot |A \cup T_1 A \cup \ldots \cup T_1^{n-1} A| \leqq \lim_{n \to \infty} \frac{2N + n}{n} = 1,$$

где N наибольшее натуральное число по абсолютной величине, принадлежащее A. С другой стороны, для $a \in A$ справедливо $\{a\} \leqq A$ и выполняется $\hat{h}(A) \geqq \hat{h}(\{a\}) = 1$. Следовательно, для всякого $A \in S_1$ $\hat{h}(A) = 1$, $h^*_{T_1} = 1$.

Покажем, что базис (S, T) ентропии H' из примера 3 изоморфен базису (S_1, T_1) энтропии H. Определим отображение f: $S \to S_1$ следующим образом: $f(x_i) = \{i\}$, $f(u \vee x_i) = f(u) \cup f(x_i)$.

Отображение f, очевидно, изоморфизм (Сравни тоже с [3], стр. 174.), для которого справедливо утверждение: Если $u = x_{i_1} \vee x_{i_2} \vee \ldots \vee x_{i_k}$, $i_1 < i_2 < \ldots i_k$, то $f(Tu) = f(x_{i_1+1} \vee x_{i_2+1} \vee \ldots \vee x_{i_k+1}) = \{i_1 + 1, i_2 + 1, \ldots, i_k + 1\}$ и $T_1 f(u) = T_1\{i_1, i_2, \ldots, i_k\} = g^{-1}\{i_1, i_2, \ldots, i_k\} = \{i_1 + 1, i_2 + 1, \ldots, i_k + 1\}$; $\hat{H}(f(u)) = \hat{H}(\{i_1, i_2, \ldots,$

$i_k\}) = k$ и $H'(u) = \|u\| = k$. Следовательно, базисы (S_1, T_1) и (S, T) изоморфны. Ввиду теоремы 6 имеет место: $h^*_{T_1} = h^*_T = 1$.

4. Условная энтропия

Пусть S – верхняя полуструктура и $\mathscr{S}$ – система всех подполуструктур полуструктуры S. На $\mathscr{S}$ определим операцию умножения комплексов. Если G_1, соответственно G_2 – две подполуструктуры, определим упорядочение на $\mathscr{S}$: $G_1 \leqq G_2 \Leftrightarrow G_1 \vee G_2 = G_2$. Если теперь определим на $S \times \mathscr{S}$ умножение: $(x_1, G_1) \vee (x_2, G_2) = (x_1 \vee x_2, G_1 \vee G_2)$, вновь получим верхнюю полуструктуру.

Определение 8. Пусть (S, T) – базис энтропии H. Функция $\tilde{H}$, определенная на $S \times \mathscr{S}$ равенством $\tilde{H}[(x, G)] = \inf \{H(x \vee g) - H(g);\ g \in G\}$, называется условной энтропией элемента x относительно полуструктуры G.

Примечание 9. Пусть $G = \{g\}$. Тогда $\tilde{H}[(x, G)] = H(x \vee g) - H(g)$. Согласно принятому обозначению в теории информации будем в этом случае употреблять обозначение: $\tilde{H}[(x, G)] = H(x/g)$.

Примечание 10. Функция $\tilde{H}$ не является энтропией в смысле определения 1. ($\tilde{H}$ не является монотонной относительно упорядочения на $S \times \mathscr{S}$.) Все-таки понятие условной энтропии будет полезно для вычисления L-энтропии.

Ввиду теоремы 3, если Q – характеристическое множество для базиса (S, T), возможно вычислить $\tilde{H}[(x, Q)]$. Имеет место: $\tilde{H}[(x, Q)] = 0$, если $0 \in Q$; $\tilde{H}[(x, Q)] = H(x/q)$, если $Q = \{q\}$.

5. Энтропия в узком смысле слова

Если мы хотим доказать дальнейшие свойства L-энтропии (аналогичные теории информации) мы должны пользоваться более специальными свойствами функции H.

Определение 9. *Пусть S^1 – верхняя полуструктура с единицей и T – эндоморфизм, определенный на S^1. Энтропия в узком смысле слова – это функция $H: S^1 \to \langle 0, \infty)$, для которой выполнены следующие условия:*

а) $H(x \vee y) - H(y) \leqq H(x \vee z) - H(z)$ *для* $z \leqq y$;

б) $H(Tx) = H(x)$ *для всех* $x \in S^1$.

Лемма 2. *Если (S^1, T) – базис энтропии в узком смысле слова H, то функция H – ентропия в смысле определения 1.*

Доказательство. Очевидно, достаточно доказать, что H удовлетворяет условиям а) и в) из определения 1. Докажем а). Пусть $x \in S^1$ и $z \leqq y \leqq x$.

Применяя упорядочение на S^1, можно условие пункта а) определения 9 переписать так: $H(x)-H(y) \leqq H(x)-H(z)$. Следовательно, $H(z) \leqq H(y)$ для $z \leqq y$.

Докажем в). Если $z=1$, то можно условие пункта б) определения 9 переписать так: $H(x \vee y)-H(y) \leqq H(x)-H(1) \leqq H(x)$, т.е. $H(x \vee y) \leqq H(x)+H(y)$. Последнее неравенство сильнее, чем требует пункт в) определения 1.

Примечание 11. Ввиду леммы 2 – энтропия в узком смысле слова является энтропией в смысле определения 1. Следовательно, выполняются все утверждения предыдущих пунктов. В терминологии пункта 4 условие а) из определения 9 принимает вид: $H(x/y) \leqq H(x/z)$ для $z \leqq y$.

Ввиду теоремы 1 существует тоже $h(x/y) = h(x \vee y)-h(y)$ и справедлива:

Lemma 3. *Если (S^1, T) – базис энтропии в узком смысле слова H, то соответствующая L-энтропия является энтропией в узком смысле слова.*

Доказательство. Ввиду теоремы 1, $h(x)=h(Tx)$. Кроме того, $H_n(x \vee y)-H_n(y) \leqq H_n(x \vee z)-H_n(z)$, т.е. $h(x/y) \leqq h(x/z)$ для $z \leqq y$.

Теорема 9. *Пусть H – энтропия в узком смысле слова. Тогда*

$$h(x)=\lim_{n\to\infty} H\left(x \Big/ \bigvee_{i=1}^{n-1} T^i x\right).$$

Доказательство. Существование предела вытекает из условия теоремы: последовательность

$$\left\{h\left(x \Big/ \bigvee_{i=1}^{n-1} T^i x\right)\right\}_{n=2}^{\infty}$$

– невозрастающая. Непосредственным вычислением можно проверить равенство:

$$H\left(\bigvee_{i=1}^{n-1} T^i x\right)=H(x)+\sum_{j=1}^{n-1} H\left(x \Big/ \bigvee_{i=1}^{j} T^i x\right).$$

Теперь достаточно делить это равенство числом n и применить известное утверждение о пределе Чезаро для сходящихся последовательностей.

Следствие. $h(x)=\tilde{H}[(x, G)]$, *где G – полуструктура, образованная элементами $T^i x$, т.е. $G=[\{T^i x\};\ i=1, 2, \ldots\}]$.*

Доказательство. Справедливо:

$$\tilde{H}[(x, G)]=\inf\left\{H\left(x \Big/ \bigvee_{i=m}^{n} T^i x\right);\ m, n=1, 2, \ldots\right\}=$$

$$=\inf\left\{H\left(x \Big/ \bigvee_{i=1}^{n} T^i x\right);\ i=1, 2, \ldots\right\} \leqq H\left(x \Big/ \bigvee_{i=1}^{n} T^i x\right).$$

Следовательно,

$$\tilde{H}[(x, G)] \leqq \lim_{n\to\infty} H\left(x \Big/ \bigvee_{i=1}^{n} T^i x\right) = h(x).$$

С другой стороны, последовательность

$$\left\{h\left(x \Big/ \bigvee_{i=1}^{n} T^i x\right)\right\}_{n=1}^{\infty}$$

– невозрастающая и справедливо:

$$h(x) \leqq H\left(x \Big/ \bigvee_{i=1}^{n} T^i x\right), \qquad h(x) \leqq \tilde{H}[(x, G)].$$

Только что доказанное равенство можно применить к вычислению

$$h^{*}_{T}: \; h^{*}_{T} = \sup_{x\in S^1} \inf_{g\in G} H(x/q).$$

6. L-энтропия на некоторых специальных полуструктурах

В этом пункте покажем, что специальным выбором базиса энтропии получим разные виды энтропии, изученные в литературе, и новый пример энтропии на коммутативных полугруппах. Кроме того, приведем доказательство, что энтропия автоморфизма группы является энтропией в узком смысле слова.

А) Основным типом энтропии в узком смысле слова – это энтропия Колмогорова–Синая, которая детально исследована, например, в [1, 11].

Пусть $(\Omega, \mathcal{F}, P)$ – вероятностное пространство и T – метрический автоморфизм. Пусть α, β две конечные разбиения Ω. Если определим $\alpha \vee \beta = \{A_i \cap B_j;\ A_i \in \alpha,\ B_j \in \beta\}$, то множество этих разбиений S вместе с умножением «$\vee$» – верхняя полуструктура. Энтропия определена естественно:

$$H(\alpha) = -\sum_{A_i\in\alpha} P(A_i) \log P(A_i).$$

Б) В работе [7] авторы предупредили, что можно говорить о энтропии эндоморфизма группы.

Пусть G – коммутативная группа, A – ее конечная подгруппа, φ – эндоморфизм, определенный на G. Умножение подгрупп определено естественно: $A \vee B = M = \{ab;\ a \in A,\ b \in B\}$. Нетрудно показать (смотри например [4]), что в случае коммутативной группы M тоже является конечной группой.

Если обозначим S^1 полуструктуру конечных подгрупп группы G с умножением «$\vee$» и $TA = \varphi(A)$ для $A \in S^1$, то (S^1, T) – базис энтропии H, определенной следующим равенством: $H(A) = \log_2 |A|$.

Теорема 10. *Пусть* (S^1, T) *– базис энтропии* H, *принадлежащии абелевои группе* G. *Если* T *– автоморфизм, то соответствующая энтропия удовлетворяет условиям определения 9.*

Доказательство. Ввиду упорядочения на S^1 выполнено: $A \leqq B \Leftrightarrow A \vee B = B$. Это равносильно случаю, что $A \subset B$. Тогда для всяких $C \in S^1$ имеет место канонический изомофизм фактогрупп ([5] стр. 31): $C/C\cap A \sim C \vee A/A$ и $C/C\cap B \approx C \vee B/B$, а также справедливо:

а) $|C \vee A/A| = |C/C\cap A|$, т.е. $\dfrac{|C \vee A|}{|A|} = \dfrac{|C|}{|C\cap A|}$;

б) $|C \vee B/B| = |C/C\cap B|$ т.е. $\dfrac{|C \vee B|}{|B|} = \dfrac{|C|}{|C\cap B|}$;

Делением этих равенств получим

$$\frac{|C\cap B|}{|C\cap A|} = \frac{|C \vee A|}{|C \vee B|} \cdot \frac{|B|}{|A|}.$$

Потому что $|C\cap B| : |C\cap A| \geqq 1$, то

$$\frac{|C \vee A|}{|A|} \geqq \frac{|C \vee B|}{|B|}.$$

Следовательно, $H(C/A) = \log_2 |C \vee A| - \log_2 |A| \geqq \log_2 |C \vee B| - \log_2 |B| = H(C/B)$. Далее, $|TA| = |A|$, т.е. $H(TA) = H(A)$.

Приведем еще один новый пример вычисления энтропии автоморфизма группы.

Пример 7. Пусть $G^2 = \{e, x_1, x_2, \ldots\}$ – свободная коммутативная группа с определяющим равенством $x_i^2 = e$ для $i = 1, 2, \ldots$ Пусть S^1 соответствующая полуструктура конечных подгрупп. Определим автоморфизм φ: $\varphi(e) - e$, $\varphi(x_i) = x_{i+1}$, $\varphi(x_i x_j) = x_{i+1}x_{j+1}$. Если, например, $A \in S^1$, $A = \{e, x_1\}$, то $H(A)$ $\log_2 2 = 1$ и $A \vee TA \vee \ldots \vee T^{n-1}A = \{e, x_1, x_2, \ldots, x_n, x_1, x_2, \ldots, x_1x_2x_3\ldots x_n\}$, т.е. $H_n(A) = \log_2 2^n = n$. Следовательно, $h(A) = 1$.

Вообще говоря, произвольную группу $C \in S^1$ и $C \neq \{e\}$ можно получить следующим образом $(1 < i_1 < i_2 < \ldots < i_k)$: Пусть C – группа, образованная множеством $M = \{e, x_{i_1-1}, x_{i_2-1}, \ldots, x_{i_k-1}\}$. Тогда $C = T^{i_1}A \vee T^{i_2}A \vee \ldots \vee T^{i_k}A$. Далее,

$$C \leqq \bigvee_{n=0}^{k} T^n A.$$

Согласно теореме 3 $Q = \{A\}$ – характеристическое множество для (S^1, T) и в силу теоремы 4 $h^*_T = h(A) = 1$. Из этого вытекает: $h(C) = 0$ если $C = \{e\}$ и $h(C) = 1$, если $C \neq \{e\}$ и энтропия автоморфизма группы T – $h^*_T = 1$.

Примечание 12. В случае свободной коммутативной группы $G^k = \{e, x_1, x_2, \ldots\}$ с определяющим равенством $x_i^k = e$ для $i = 1, 2, \ldots$ получим $h^*_T = \log_2 k$.

B) Энтропию эндоморфизма группы можно обобщить следующим образом:

Пусть P^1 – коммутативная полугруппа с единицей. Пусть S^1 – полуструктура всех конечных подполугрупп с единицей и с операцией умножения комплексов. Далее, пусть φ – эндоморфизм на P^1, $TA = \varphi(A)$ для $A \in S^1$ и $H(A) = \log_2 |A|$. Тогда (S^1, T) – базис энтропии H. В этом случае уже H не является, вообще говоря, энтропией в узком смысле слова, как показывает следующий пример:

Пример 8. Пусть $P^1 = \{0, 1, a_1, a_2, c_1, c_2, p\}$ верхняя полуструктура, для которой справедливо

$$1 \leqq a_1 \leqq a_2 \leqq 0, \quad 1 \leqq c_1 \leqq c_2 \leqq 0,$$
$$a_1 \leqq p \leqq c_2, \quad c_1 \leqq p \leqq a_2.$$

Если

$$A = \{0, a_2, 1\}, \quad B = \{0, a_1, a_2, 1\}, \quad C = \{0, c_1, c_2, 1\},$$

Тогда

$$C \vee A = \{0, a_2, c_2, c_1, 1\}, \quad C \vee B = P^1.$$

Следовательно,

$$A \subset B \text{ и } H(C/A) = \log_2 \frac{|C \vee A|}{|A|} = \log_2 \frac{5}{3},$$

$$H(C/B) = \log_2 \frac{|C \vee B|}{|B|} = \log_2 \frac{7}{4},$$

а это противоречит условию а) из определения 9.

ЛИТЕРАТУРА

[1] БИЛЛИНГСЛЕЙ П., Эргодическая теория и информация, Мир, Москва 1969.

[2] ГРОШЕК, О., Топология на полугруппах индуцированная эндоморфизмом, Mathematica Slovaca, 2, 1978, 217–223.

[3] КЛИФФОРД А., ПРЕСТОН Г., Алгебраическаъ теория полугрупп, Том 1., Мир, Москва 1972.

[4] КУРОШ А., Теория групп, (Изд. 3), Наука, Москва 1967.

[5] ЛЕНГ С., Алгебра, Мир, Москва 1968.

[6] РОХЛИН В., Образующие в эргодической теории, Вестник Лен. Унив. 1963, 26–32.

[7] ADLER, R. L., KONHEIM A. G., McANDREW M. H., Topological entropy, Trans. AMS., 114, 1965, 309–319.

[8] GROŠEK O., Entropia na algebraických štruktúrach, Kandidátska diz. práca, SVŠT – 1977.

[9] GROŠEK O., Entropy on quasiordered semigroups, (To appear.)

[10] RIEČAN B., Abstract entropy, Acta F.R.N. Univ. Comen. – Mat., 1974, 55–67.

[11] WALTERS P., Ergodic theory – Introductory Lectures, Lecture Notes in Math., Vol. 458, 1975.

[12] PALM G., Entropie und Erzeuger in dynamischen Verbanden, Z. Wahrschein. verw. Gebiete, 36, 1976, 27–45.

Поступило 20. 3. 1978

Katedra matematiky
Elektrotechnická fakulta SVŠT
Gottwaldovo nám. 19
884 20 Bratislava