УДК 519.714

О СЛОЖНОСТИ ИНФОРМАЦИОННЫХ СЕТЕЙ

Д. Ю. Черухин

В работе рассмотрена аксиоматическая теория, описывающая количественные соотношения, возникающие при передаче и преобразовании информации. Получена нижняя оценка сложности сети, осуществляющей равномерное смешивание информации из нескольких независимых источников. Показано применение данного результата к теории сложности булевых функций.

Информационным пространством (*ИП*) назовём набор $\mathcal{S} = (M, \circ, |\cdot|)$, где M — множество объектов, называемых *сообщениями*, $\circ\colon M^2 \to M$ — операция *объединения* сообщений, $|\cdot|\colon M \to \mathbb{R}$ — функционал *нормы* сообщения, если для любых $x, y, z \in M$ выполнены следующие аксиомы:

I.	$x \circ x = x$	(идемпотентность)
II.	$x \circ y = y \circ x$	(коммутативность)
III.	$(x \circ y) \circ z = x \circ (y \circ z)$	(ассоциативность)
IV.	$\exists \Lambda\ (|\Lambda| = 0 \,\&\, \forall t\ \Lambda \circ t = t)$	(пустое сообщение)
V.	$|x \circ y| + |x \circ z| \geqslant |x \circ y \circ z| + |x|$	(сильная субаддитивность)

Неформально, под сообщением мы понимаем нечто общее, присущее некоторым текстам, содержащим одну и ту же информацию; норма сообщения есть количество информации в нём. Возможно изменить аксиомы так, чтобы сообщение интерпретировалось как конкретный текст или же, напротив, как нечто общее, присущее всем текстам, содержащим одну и ту же информацию, однако мы выбрали средний путь из соображений удобства работы в данной формальной системе.

Отметим близость теории ИП с такими известными структурами, как субмодулярные решётки и матроиды. Также отметим её связь с классической теорией информации Шеннона [1] (см. тж. [2, 3]). А именно, сообщениям соответствуют случайные величины, объединение сообщений соответствует совместному распределению случайных величин, а норма — энтропии.

Приведём три примера ИП.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

1. Пусть $(\Omega, \mathcal{A}, \mu)$ — измеримое пространство. Тогда $(\mathcal{A}, \cup, \mu)$ — ИП, где $\cup$ — операция объединения множеств.

2. Пусть L — линейное пространство над некоторым полем, M — множество его конечномерных подпространств, $+$ — операция суммы подпространств, $\dim$ — функционал размерности. Тогда $(M, +, \dim)$ — ИП.

3. Пусть $P_2(n) = \{f \mid f\colon \{0,1\}^n \to \{0,1\}\}$ — множество булевых функций n переменных, $M = \{S \mid S \subseteq P_2(n)\}$. Для любого $S \in M$ введём отношение эквивалентности ρ_S на множестве $\{0,1\}^n$:

$$\tilde{x}\ \rho_S\ \tilde{y} \iff \forall f \in S\ f(\tilde{x}) = f(\tilde{y}).$$

Пусть $K_1, \ldots, K_s$ — все классы эквивалентности отношения ρ_S. Положим

$$|S| = \sum_{i=1}^{s} p_i \log_2 \frac{1}{p_i}, \quad \text{где } p_i = \frac{|K_i|}{2^n},\ i = 1, \ldots, s. \tag{1}$$

Тогда $(M, \cup, |\cdot|)$ — ИП.

Доказательства аксиом ИП во всех трёх примерах достаточно очевидны, за исключением аксиомы V в примере 3 (т. е. сильной субаддитивности энтропии Шеннона). Доказательство последней приведено в заключительной части данной статьи.

Сейчас мы введём в ИП несколько понятий и выведем следствия из аксиом. В средней части статьи мы рассмотрим информационные сети и докажем для них нижнюю оценку сложности. В конце статьи, после доказательства аксиомы V для примера 3, мы рассмотрим приложение теории ИП к сложности булевых функций, основанное на примере 3. В частности, доказанную нижнюю оценку сложности сетей мы перенесём на класс булевых схем из функциональных элементов (СФЭ, [4]).

Далее будем считать, что имеется некоторое ИП $(M, \circ, |\cdot|)$. Укажем на два свойства ИП, следующие непосредственно из аксиом.

Утверждение 1. *$\forall x, y \in M$:*
а) $|x| \geqslant 0$ (неотрицательность);
б) $|x \circ y| \geqslant |x|$ (монотонность);
в) $|x| + |y| \geqslant |x \circ y|$ (субаддитивность).

Для доказательства п. б) нужно в аксиоме V положить $z = y$, а для доказательства п. в) — положить $x = \Lambda$. П. а) следует из б), если положить $x = \Lambda$.

Пусть $u \in M$. Введём *фактор-норму* $|\cdot|_u\colon M \to \mathbb{R}$, соответствующую условной энтропии в классической теории информации:

$$|x|_u = |x \circ u| - |u|$$

и рассмотрим её свойства.

Утверждение 2. *$\forall x, y, z, u \in M$:*
а) $|x| = |x|_\Lambda$; *б)* $(|x|_y)_z = |x|_{y\circ z}$; *в)* $|x|_y \geqslant |x|_{y\circ z}$;
г) $|x\circ y|_u + |x\circ z|_u \geqslant |x\circ y\circ z|_u + |z|_u$.

Доказательство. а) $|x|_\Lambda = |x\circ\Lambda| - |\Lambda| = |x|$;
б) $(|x|_y)_z = |x\circ z|_y - |z|_y = |x\circ z\circ y| - |y| - (|z\circ y| - |y|) = |x\circ y\circ z| - |y\circ z| = |x|_{y\circ z}$;
в) $|x\circ y| + |y\circ z| \geqslant |x\circ y\circ z| + |y| \Longrightarrow |x|_y = |x\circ y| - |y| \geqslant |x\circ y\circ z| - |y\circ z| = |x|_{y\circ z}$;
г) $|x\circ y|_u + |x\circ z|_u = |x\circ y\circ u| + |x\circ z\circ u| - 2|u| \geqslant |x\circ y\circ z\circ u| + |x\circ u| - 2|u| = |x\circ y\circ z|_u + |x|_u$. □

В силу утв. 2 г) фактор-норма удовлетворяет аксиоме V, а значит, набор $(M, \circ, |\cdot|_u)$ является ИП, которое мы назовём *фактор-ИП*. В дальнейшем, если в ИП введена некоторая функция (или отношение), выражаемая через норму, то нижний индекс u (где $u \in M$) у знака этой функции означает, что она берётся относительно фактор-нормы $|\cdot|_u$. Например, если $\varphi(x, u) = |x| - |x|_u$, то $\varphi_z(x, u) = |x|_z - |x|_{u\circ z}$.

Введём в ИП отношение вложения:

$$x \subseteq y \iff |x\circ y| = |y|.$$

Вложение $x \subseteq y$ означает, что x не добавляет к y никакой существенно новой информации. Также можно сказать, что сообщение x получено в результате преобразования сообщения y (возможно, с потерей информации).

Утверждение 3. *$\forall x, y, z \in M$:*
а) $x \subseteq x\circ y$; *б)* $\Lambda \subseteq x$; *в)* $x \subseteq x$;
г) $x \subseteq y \,\&\, y \subseteq z \Longrightarrow x \subseteq z$;
д) $x \subseteq z \,\&\, y \subseteq z \Longrightarrow x\circ y \subseteq z$;
е) $x \subseteq y \Longrightarrow x\circ z \subseteq y\circ z$;
ж) $x \subseteq y \Longrightarrow x \subseteq_z y$.

Доказательство. П. а) следует из $|x\circ x\circ y| = |x\circ y|$; пп. б), в) следуют из а) и равенства $x\circ\Lambda = x$.

г) Имеем $|x\circ y| = |y|$ и $|y\circ z| = |z|$. Покажем, что $|x\circ y\circ z| \leqslant |y\circ z|$. Действительно, в силу аксиомы V,

$$|y\circ z| - |x\circ y\circ z| \geqslant |y| - |x\circ y| = 0.$$

Тогда

$$|z| \leqslant |x\circ z| \leqslant |x\circ y\circ z| \leqslant |y\circ z| = |z|, \tag{2}$$

следовательно, в (2) все неравенства можно заменить на равенства, а значит, $|x\circ z| = |z|$, т. е. $x \subseteq z$.

д) $|x \circ z| = |z| \,\&\, |y \circ z| = |z| \Longrightarrow 2|z| = |x \circ z| + |y \circ z| \geqslant |x \circ y \circ z| + |z| \Longrightarrow |x \circ y \circ z| = |z| \Longrightarrow x \circ y \subseteq z$;

е) $x \subseteq y \subseteq y \circ z \,\&\, z \subseteq y \circ z \Longrightarrow x \circ z \subseteq y \circ z$;

ж) $x \subseteq y \Longrightarrow x \circ z \subseteq y \circ z \Longrightarrow |x \circ y \circ z| = |y \circ z| \Longrightarrow |x \circ y|_z = |x \circ y \circ z| - |z| = |y \circ z| - |z| = |y|_z \Longrightarrow x \subseteq_z y$. □

В силу утв. 3, отношение вложения является предпорядком (пп. в, г) с наименьшим элементом (п. б) и в этом предпорядке операция $\circ$ вычисляет точную верхнюю грань двух элементов (пп. а, д).

Скажем, что сообщения $x_1, \ldots, x_n$ *независимы* (*в совокупности*), если

$$|x_1 \circ \ldots \circ x_n| = |x_1| + \ldots + |x_n|.$$

Независимость сообщений x и y будем обозначать в виде $x \perp y$.

Утверждение 4. *Пусть сообщения $x_1, \ldots, x_n$ независимы, $\{x_1, \ldots, x_n\} = X_1 \sqcup \ldots \sqcup X_k$ и $\hat{X}_i$ — объединение всех сообщений из множества X_i. Тогда сообщения $\hat{X}_1, \ldots, \hat{X}_{k-1}$ независимы.*

Доказательство. Используя субаддитивность, получим

$$\begin{aligned} |\hat{X}_1 \circ \ldots \circ \hat{X}_{k-1}| + |\hat{X}_k| \geqslant |\hat{X}_1 \circ \ldots \circ \hat{X}_k| = |x_1 \circ \ldots \circ x_n| = \\ = |x_1| + \ldots + |x_n| \geqslant |\hat{X}_1| + \ldots + |\hat{X}_k| \geqslant |\hat{X}_1 \circ \ldots \circ \hat{X}_{k-1}| + |\hat{X}_k|. \end{aligned} \tag{3}$$

В (3) все неравенства можно заменить равенствами, поэтому $|\hat{X}_1 \circ \ldots \circ \hat{X}_{k-1}| = |\hat{X}_1| + \ldots + |\hat{X}_{k-1}|$. □

Введём меру зависимости сообщений — аналог классической общей информации:

$$I(x, y) = |x| + |y| - |x \circ y|,$$

и её обобщение на случай трёх сообщений:

$$I(x, y, z) = |x| + |y| + |z| - |x \circ y| - |x \circ z| - |y \circ z| + |x \circ y \circ z|.$$

Заметим, что

$$I_z(x, y) = |x \circ z| + |y \circ z| - |x \circ y \circ z| - |z|,$$

а значит,

$$I(x, y, z) = I(x, y) - I_z(x, y).$$

Утверждение 5. *$\forall x, y, z \in M$:*
а) $0 \leqslant I(x,y) \leqslant |x|$; *б)* $I(x,y) = 0 \iff x \perp y$; *в)* $I(x,y) = |x| \iff x \subseteq y$;
г) $I(x \circ y, z) = I(x,z) + I_x(y,z)$;
д) $I(x \circ y, z) \geqslant I(x,z)$; *е)* $I(x \circ y, z) \geqslant I_x(y,z)$;
ж) $x \subseteq y \Longrightarrow I(x,z) \leqslant I(y,z)$;
з) $x \perp y \Longrightarrow I(x,y,z) \leqslant 0$;
и) $x \perp y \Longrightarrow I(x \circ y, z) \geqslant I(x,z) + I(y,z)$;
к) $x \perp y \circ z \Longrightarrow x \perp_z y$.

Доказательство. П. а) следует из субаддитивности и монотонности, пп. б), в) — непосредственно из определения;

г) $I(x,z) + I_x(y,z) = |x| + |z| - |x \circ z| + |x \circ y| + |x \circ z| - |x \circ y \circ z| - |x| = |z| + |x \circ y| - |x \circ y \circ z| = I(x \circ y, z)$; пп. д), е) следуют из г) и неотрицательности функции I (п. а);

ж) $x \subseteq y \subseteq y \circ z \Longrightarrow |x \circ y| = |y| \,\&\, |x \circ y \circ z| = |y \circ z| \Longrightarrow I(y,z) = I(x \circ y, z) \geqslant I(x,z)$;

з) $x \perp y \Longrightarrow I(x,y,z) = I(x,y) - I_z(x,y) = -I_z(x,y) \leqslant 0$;

и) $x \perp y \Longrightarrow I(x \circ y, z) = I(x,z) + I_x(y,z) = I(x,z) + I(y,z) - (I(y,z) - I_x(y,z)) = I(x,z) + I(y,z) - I(x,y,z) \geqslant I(x,z) + I(y,z)$;

к) $x \perp y \circ z \Longrightarrow 0 = I(x, y \circ z) \geqslant I_z(x,y) \Longrightarrow I_z(x,y) = 0 \Longrightarrow x \perp_z y$. $\square$

Следующее утверждение является ключевым при доказательстве нижней оценки сложности.

Утверждение 6. *Если $x_0, x_1, x_2, u_1, u_2 \in M$, $u_1 \subseteq x_0 \circ x_1$ и $u_2 \subseteq x_1 \circ x_2$, то*

$$I(x_0, u_1) + I_{u_1}(x_0 \circ x_2, u_2) \geqslant |u_1 \circ u_2| - |x_1|.$$

Доказательство. Используя утв. 5 (а, в, г, е) и утв. 3 (а, ж), получим

$$\begin{gathered}
|x_1| \geqslant I(x_1, x_0 \circ x_2 \circ u_1 \circ u_2) = I(x_1, x_0 \circ u_1) + I_{x_0 \circ u_1}(x_1, x_2 \circ u_2) \geqslant \\
\geqslant I_{x_0}(x_1, u_1) + I_{x_0 \circ x_2 \circ u_1}(x_1, u_2) = \\
= I(x_0 \circ x_1, u_1) - I(x_0, u_1) + I_{u_1}(x_0 \circ x_1 \circ x_2, u_2) - I_{u_1}(x_0 \circ x_2, u_2) = \\
= |u_1| - I(x_0, u_1) + |u_2|_{u_1} - I_{u_1}(x_0 \circ x_2, u_2) = |u_1 \circ u_2| - I(x_0, u_1) - I_{u_1}(x_0 \circ x_2, u_2),
\end{gathered}$$

откуда и следует требуемое. $\square$

Теперь перейдём к рассмотрению сетей. Назовём (n,m)-*сетью* набор $\mathcal{N} = (G, V_-, V_+)$, в котором G — конечный ориентированный граф без ориентированных циклов с множеством вершин V и множеством рёбер E, $V_- \in V^n$ —

набор *входов* сети, $V_+ \in V^m$ — набор её *выходов*, причём все входы различны, входная степень каждого входа равна 0, а входная степень любой вершины, отличной от входов, равна 2 (входная степень вершины — число рёбер, входящих в эту вершину). Отметим, что выходы могут совпадать друг с другом и совпадать со входами.

Предпосылкой для именно такого определения сети явилось основное (в данной статье) приложение теории информационных сетей, связанное со сложностью СФЭ; в данном случае имеются в виде СФЭ в базисе из всех двуместных булевых функций. Вершины, отличные от входов, назовём *элементами*. *Сложностью* сети назовём число элементов в ней. Будем считать, что нам дана некоторая (n, m)-сеть. Множество её входов обозначим через X, множество выходов — через Y, сложность — через L.

Скажем, что вершина v *предшествует* вершине v', если существует ориентированный путь из v в v'. Скажем, что вершина v *непосредственно* предшествует вершине v', если из v в v' ведёт ребро. В силу отсутствия ориентированных циклов элементы можно занумеровать числами $1, \ldots, L$ так, что номер элемента больше номеров всех предшествующих ему элементов; каждому входу припишем номер 0. Такую нумерацию назовём *монотонной*.

Утверждение 7. *Если в монотонной нумерации номер элемента v равен i, то элементу v предшествуют не более, чем $(i+1)$ входов.*

Доказательство. Пусть G' — подграф графа G, порождённый множеством вершин, предшествующих элементу v, V' и E' — множества вершин и рёбер графа G', X' — множество входов, предшествующих вершине v.

Подсчитаем число $|E'|$ двумя способами. С одной стороны, в каждую вершину из множества $V' \backslash X'$ входят ровно два ребра графа G', поэтому $|E'| = 2|V' \backslash X'|$. С другой стороны, из каждой вершины графа G', кроме v, выходит хотя бы одно ребро графа G' (ребро, по которому проходит путь, ведущий в вершину v), поэтому $|E'| \geqslant |V'| - 1$. Наконец, номер вершины v не меньше числа элементов в G', т. е. $|V' \backslash X'|$. Поэтому

$$|X'| - 1 = |V'| - 1 - |V' \backslash X'| \leqslant |E'| - |V' \backslash X'| = |V' \backslash X'| \leqslant i,$$

откуда и следует требуемое. □

Назовём (n, m)-*информационной* сетью ((n, m)-*ИС*) набор $\hat{\mathcal{N}} = (\mathcal{N}, \mathcal{S}, \hat{\cdot})$, в котором $\mathcal{N}$ является (n, m)-сетью, $\mathcal{S} = (M, \circ, |\cdot|)$ — ИП и $\hat{\cdot}\colon V \to M$ — функция, сопоставляющая каждой вершине v сети $\mathcal{N}$ сообщение $\hat{v}$ из ИП $\mathcal{S}$, если выполнены условия:

i) $\forall v \in V \ |\hat{v}| \leqslant 1$;

ii) если v непосредственно предшествует вершинам v_1 и v_2, то $\hat{v} \subseteq \hat{v}_1 \circ \hat{v}_2$.

ИС можно интерпретировать следующим образом: по рёбрам передаётся информация. В каждом элементе объединяется пришедшая в него информация и в результате её преобразования получается новая информация (в количестве, не превосходящем 1), которая рассылается по всем исходящим рёбрам.

Отметим, что ИС можно определить несколько иначе, ограничив не количество информации, исходящей из вершины, а количество информации, передаваемой по ребру, и разрешив ориентированные циклы. В таком случае получится объект, аналогичный транспортной сети (точнее, потоку в сети) [5]. Более того, в последнем случае транспортная сеть является частным случаем ИС, а именно, такой ИС, в которой используется ИП $(\mathbb{R}_+^d, +, \sum\limits_{i=1}^{d} x_i)$, где d — число передаваемых продуктов, и выполнено правило Кирхгофа (которое на языке ИП означает обратимость преобразования информации). Данное нами определение продиктовано приложением к сложности СФЭ.

Для любого множества вершин $B = \{v_1, \dots , v_k\} \subseteq V$ обозначим

$$\hat{B} = \hat{v}_1 \circ \ldots \circ \hat{v}_k.$$

Пусть $A, B, C \subseteq V$. Скажем, что множество вершин B *разделяет* множества A и C, если любой ориентированный путь, пересекающийся с множеством A и множеством C, пересекается также с B. Скажем, что множество A [вершина v] *опирается* на множество B, если B разделяет множества X и A [$\{v\}$].

Утверждение 8. *Если вершина v опирается на множество B, то $\hat{v} \subseteq \hat{B}$.*

Доказательство. Рассмотрим монотонную нумерацию вершин и проведём индукцию по номеру вершины v. Базис индукции: $v \in B$ (сюда включается случай, когда v — вход). Тогда в силу утв. 3 а) $\hat{v} \subseteq \hat{B}$.

Индуктивный переход: $v \notin B$. Пусть v непосредственно предшествует вершинам v_1 и v_2. Последние опираются на множество B и по предположению индукции, $\hat{v}_1 \subseteq \hat{B}$ и $\hat{v}_2 \subseteq \hat{B}$. Тогда в силу условия ii) и утв. 3 (г, д) $\hat{v} \subseteq \hat{v}_1 \circ \hat{v}_2 \subseteq \hat{B} \Longrightarrow \hat{v} \subseteq \hat{B}$. $\square$

Следствие 1. *а) если множество A опирается на множество B, то $\hat{A} \subseteq \hat{B}$;*

б) $\hat{Y} \subseteq \hat{X}$.

Рассмотрим частный случай ИС, для которого мы получим нижнюю оценку сложности. Назовём (n, n)-ИС *равномерной* (n-*РИС*), если выполнены также следующие условия:

iii) $|\hat{X}| = |\hat{Y}| = n$;
iv) $\forall x \in X \ \forall y \in Y \ I(\hat{x}, \hat{y}) = \frac{1}{n}$.
Далее будем считать, что нам дана некоторая n-РИС.

Утверждение 9. *Пусть* $X' \subseteq X$, $Y' \subseteq Y$, $|X'| = k$, $|Y'| = l$. *Тогда*
а) $|\hat{X}'| = k$, $|\hat{Y}'| = l$;
б) $I(\hat{X}', \hat{Y}') = \frac{kl}{n}$;
в) если $Z \subseteq Y$, $Z \cap Y' = \varnothing$, *то* $I_{\hat{Z}}(\hat{X}', \hat{Y}') = \frac{kl}{n}$.

Доказательство. Обозначим $X'' = X \backslash X'$, $Y'' = Y \backslash Y'$.

а) В силу условия i) и субаддитивности $|\hat{X}'| \leqslant k$ и $|\hat{X}''| \leqslant n - k$, поэтому

$$n = |\hat{X}| = |\hat{X}' \circ \hat{X}''| \leqslant |\hat{X}'| + |\hat{X}''| \leqslant k + (n-k) = n,$$

а значит, неравенства можно заменить равенствами и $|\hat{X}'| = k$. Аналогично, $|\hat{Y}'| = l$.

б) Пусть $X = \{x_1, \ldots, x_k\}$, $Y' = \{y_1, \ldots, y_l\}$. Из п. а) следует, что сообщения, соответствующие входам [выходам] независимы. Тогда, в силу утв. 5 и)

$$I(\hat{X}', \hat{Y}') = I(\hat{x}_1 \circ \ldots \circ \hat{x}_k,\ \hat{y}_1 \circ \ldots \circ \hat{y}_l) \geqslant \sum_{i,j} I(\hat{x}_i, \hat{y}_j) = \frac{kl}{n}.$$

Аналогично,

$$I(\hat{X}'', \hat{Y}') \geqslant \frac{(n-k)l}{n}, \quad I(\hat{X}, \hat{Y}'') \geqslant \frac{n(n-l)}{n}.$$

Далее, так как $\hat{Y} \subseteq \hat{X}$, то $I(\hat{X}, \hat{Y}) = |\hat{Y}| = n$. Поэтому, в силу утв. 5 и)

$$n = I(\hat{X}, \hat{Y}) = I(\hat{X}' \circ \hat{X}'',\ \hat{Y}' \circ \hat{Y}'') \geqslant$$
$$\geqslant I(\hat{X}', \hat{Y}') + I(\hat{X}'', \hat{Y}') + I(\hat{X}, \hat{Y}'') \geqslant \frac{kl}{n} + \frac{(n-k)l}{n} + (n-l) = n,$$

откуда, заменив неравенства равенствами, получим требуемое.

в) Пусть $|Z| = m$. Из утв. 5 г) и п. б) следует

$$I_{\hat{Z}}(\hat{X}', \hat{Y}') = I(\hat{X}',\ \hat{Y}' \circ \hat{Z}) - I(\hat{X}', \hat{Z}) = \frac{k(l+m)}{n} - \frac{km}{n} = \frac{kl}{n}. \qquad \square$$

Лемма 1. *Если $X' \subseteq X$, $Y' \subseteq Y$, $|X'| = k$, $|Y'| = l$ и множество $B \subseteq V$ разделяет множества X' и Y', то*

$$|B| \geqslant \frac{kl}{n}.$$

Доказательство. Пусть $X'' = X \backslash X'$. Покажем, что множество Y' опирается на множество $B \cup X''$. Действительно, рассмотрим произвольный ориентированный путь, ведущий из входа $x \in X$ в выход $y \in Y'$. Если $x \in X'$, то этот путь пересекается с множеством B, в если $x \in X''$ — то с множеством X''; в любом случае он пересекается с множеством $B \cup X''$. Тогда $\hat{Y}' \subseteq \hat{B} \circ \hat{X}''$. Из утв. 2 в), утв. 5 (а, в, г) и утв. 9 следует

$$|B| \geqslant |\hat{B}| \geqslant |\hat{B}|_{\hat{X}''} \geqslant I_{\hat{X}''}(\hat{B}, \hat{Y}') = I(\hat{B} \circ \hat{X}'', \hat{Y}') - I(\hat{X}'', \hat{Y}') = \\ = |\hat{Y}'| - I(\hat{X}'', \hat{Y}') = l - \frac{(n-k)l}{n} = \frac{kl}{n}. \square$$

Следствие 2. *а) Каждый вход предшествует каждому выходу;*
б) $L \geqslant 2n - 2$.

Действительно, если данный вход не предшествует данному выходу, то они разделяются пустым множеством, что противоречит лемме 1 (вообще, вследствие леммы 1 и теоремы Дилуорса, найдутся $\lceil \frac{kl}{n} \rceil$ непересекающихся путей, начинающихся в множестве X' и оканчивающихся в Y'). В силу утв. 7, номер каждого выхода не меньше, чем $n-1$ (иначе выход опирался бы на множество входов, не содержащее некоторого входа). Поскольку все выходы различны (это следует из условий i и iii), то максимальный из номеров выходов не меньше, чем $(n-1)+n-1$, а значит, $L \geqslant 2n-2$. Далее мы покажем, что $L \geqslant 2{,}5n - O(1)$.

Будем считать, что $n \geqslant 2$, тогда никакой выход не совпадает со входом. Введём вспомогательный неориентированный граф Γ. Вершинами графа Γ являются те вершины графа G, которые непосредственно предшествуют хотя бы одному выходу сети. Рёбра графа Γ соответствуют выходам сети; ребро, соответствующее выходу $y \in Y$, соединяет вершины, непосредственно предшествующее выходу y (если такая вершина одна, то ребро является петлёй). Пусть V_Γ и E_Γ — множества вершин и рёбер графа Γ.

Утверждение 10. *В любом подграфе графа Γ число рёбер не больше числа вершин.*

Действительно, если Γ' — подграф графа Γ с множеством вершин V' и множеством рёбер E', Y' — множество выходов сети, соответствующих рёбрам из

E', то множество Y' опирается на множество V', а значит, $|E'| = |Y'| = |\hat{Y}'| \leqslant |\hat{V}'| \leqslant |V'|$.

Заметим, что если Γ' — компонента связности графа Γ, то

$$|E'| \leqslant |V'| \leqslant |E'| + 1$$

(правое неравенство следует из связности компоненты), а значит, либо $|V'| = |E'|$, либо $|V'| = |E'| + 1$. Во втором случае компонента является деревом, а в первом — деревом с одним дополнительным ребром. В этом случае граф Γ' представляет из себя множество корневых деревьев, корни которых объединены в цикл (другими словами, цикл, из которого "растут" деревья). Такую компоненту и все её вершины назовём *критическими*.

Для каждой вершины v обозначим через Y_v множество выходов сети, предшествующих вершине v (не исключено, что выход сети используется для вычисления другого выхода). Через X_v обозначим множество тех входов x, для которых множества $\{x\}$ и $\{v\}$ не разделяются множеством Y_v. Тогда v опирается на множество $X_v \cup Y_v$, следовательно, $\hat{v} \subseteq \hat{X}_v \circ \hat{Y}_v$.

Лемма 2. *Пусть v, w — вершины графа Γ. Тогда*
а) если v и w соединены ребром в Γ, то

$$|X_v \cup X_w| = n;$$

б) если v и w соединены в графе Γ цепью, содержащей хотя бы одно ребро, и w не предшествует ни одному выходу из Y_v, то

$$|X_v| + |X_v \cup X_w| \geqslant n;$$

в) если v входит в цикл графа Γ, то

$$|X_v| \geqslant \frac{n}{2};$$

г) если v — критическая вершина, не входящая в цикл графа Γ, то

$$|X_v| = n.$$

Доказательство. а) Пусть v и w соединены ребром, соответствующим выходу y. Тогда $\hat{y} \subseteq \hat{v} \circ \hat{w} \subseteq \hat{X}_v \circ \hat{Y}_v \circ \hat{X}_w \circ \hat{Y}_w$. Заметим, что $y \notin Y_v \cup Y_w$, так как в противном случае в сети был бы ориентированный цикл. Поэтому $\hat{y} \perp \hat{Y}_v \circ \hat{Y}_w$. Используя утв. 5 (б, в, г) и утв. 9 (а, в), получим

$$1 = |\hat{y}| = I(\hat{y}, \hat{X}_v \circ \hat{Y}_v \circ \hat{X}_w \circ \hat{Y}_w) = \\ = I(\hat{y}, \hat{Y}_v \circ \hat{Y}_w) + I_{\hat{Y}_v \circ \hat{Y}_w}(\hat{y}, \hat{X}_v \circ \hat{X}_w) = 0 + \frac{1 \cdot |X_v \cup X_w|}{n}.$$

б) Рассмотрим цепь, соединяющую вершины v и w. Пусть она последовательно проходит через вершины $v = v_0, \dots , v_k = w$ и рёбра, соответствующие выходам $y_1, \dots , y_k$. Если $k = 1$, то п. б) следует из п. а). Пусть $k \geqslant 2$.

Обозначим $x_0 = \hat{v}_0$, $x_1 = \hat{v}_1 \circ \ldots \circ \hat{v}_{k-1}$, $x_2 = \hat{v}_k$, $u_1 = \hat{y}_1$, $u_2 = \hat{y}_k$, $Y' = \{y_2, \dots , y_{k-1}\}$. Рассмотрим фактор-ИП с нормой $|\cdot|_{\hat{Y}'}$. Имеем $u_1 = \hat{y}_1 \subseteq \hat{v}_0 \circ \hat{v}_1 \subseteq x_0 \circ x_1$, следовательно (в силу утв. 3 ж) $u_1 \subseteq_{\hat{Y}'} x_0 \circ x_1$. Аналогично, $u_2 \subseteq_{\hat{Y}'} x_1 \circ x_2$. Применив утв. 6, получим

$$I_{\hat{Y}'}(x_0, u_1) + I_{\hat{Y}' \circ u_1}(x_0 \circ x_2, u_2) \geqslant |u_1 \circ u_2|_{\hat{Y}'} - |x_1|_{\hat{Y}'}. \tag{4}$$

Заметим, что

$$|u_1 \circ u_2|_{\hat{Y}'} = |\hat{y}_1 \circ \ldots \circ \hat{y}_k| - |\hat{y}_2 \circ \ldots \circ \hat{y}_{k-1}| = 2. \tag{5}$$

Далее, так как множество Y' опирается на множество $\{v_1, \dots , v_{k-1}\}$, то $\hat{Y}' \subseteq \hat{v}_1 \circ \ldots \circ \hat{v}_{k-1} = x_1$, следовательно

$$|x_1|_{\hat{Y}'} = |x_1 \circ \hat{Y}'| - |\hat{Y}'| = |x_1| - |\hat{Y}'| \leqslant (k-1) - (k-2) = 1. \tag{6}$$

Из (5) и (6) следует, что правая часть в (4) не меньше единицы.

Преобразуя (4), используя вложения $x_0 = \hat{v} \subseteq \hat{X}_v \circ \hat{Y}_v$, $x_2 = \hat{w} \subseteq \hat{X}_w \circ \hat{Y}_w$ и утверждения 5, 9, получим цепочку соотношений:

$$1 \leqslant I_{\hat{Y}'}(\hat{X}_v \circ \hat{Y}_v, \hat{y}_1) + I_{\hat{Y}' \circ \hat{y}_1}(\hat{X}_v \circ \hat{Y}_v \circ \hat{X}_w \circ \hat{Y}_w, \hat{y}_k) = \\ = I_{\hat{Y}'}(\hat{Y}_v, \hat{y}_1) + I_{\hat{Y}' \circ \hat{Y}_v}(\hat{X}_v, \hat{y}_1) + I_{\hat{Y}' \circ \hat{y}_1}(\hat{Y}_v \circ \hat{Y}_w, \hat{y}_k) + \\ + I_{\hat{Y}' \circ \hat{y}_1 \circ \hat{Y}_v \circ \hat{Y}_w}(\hat{X}_v \circ \hat{X}_w, \hat{y}_k) = 0 + \frac{|X_v| \cdot 1}{n} + 0 + \frac{|X_v \cup X_w| \cdot 1}{n}. \tag{7}$$

К обоснованию выкладки (7) заметим, что в силу отсутствия ориентированных циклов, $y_1 \notin Y_v$ и $y_k \notin Y_w$. Кроме того, $y_k \notin Y_v$, иначе мы бы получили противоречие с условием п. б) (а именно, вершина w предшествовала бы выходу $y_k \in Y_v$). Заметим также, что $y_1 \notin Y'$ и $y_k \notin Y' \cup \{y_1\}$, так как

$Y' = \{y_2, \ldots, y_{k-1}\}$ и все выходы $y_1, \ldots, y_k$ различны. Итак, $\hat{y}_1 \perp \hat{Y}' \circ \hat{Y}_v$ и $\hat{y}_k \perp \hat{Y}' \circ \hat{y}_1 \circ \hat{Y}_v \circ \hat{Y}_w$, благодаря чему на последнем шаге в (5) мы можем первое и третье слагаемое заменить нулями (в силу утв. 5 и), а ко второму и четвёртому применить утв. 9 в). Из (7) следует требуемое.

П. в) следует из п. б), если положить $v = w$ и в качестве цепи взять цикл, содержащий вершину v; вершина v не предшествует ни одному выходу из Y_v в силу отсутствия ориентированных циклов.

г) Пусть Γ' — подграф графа Γ, состоящий из цикла, входящего в ту же компоненту связности, что и v, и цепи, соединяющей этот цикл с вершиной v (такая цепь единственна). Обозначим через y выход, соответствующий ребру графа Γ', инцидентному вершине v, через Y' — множество выходов, соответствующих остальным рёбрам графа Γ'; через V' обозначим множество вершин графа Γ', за исключением вершины v.

Число вершин в графе Γ' равно числу рёбер, поэтому $|Y'| = |V'|$. Кроме того, множество Y' опирается на множество V', поэтому $\hat{Y}' \subseteq \hat{V}'$. Тогда $|V'| = |Y'| = |\hat{Y}'| \leqslant |\hat{V}'| \leqslant |V'|$. Заменив неравенства равенствами, получим $|\hat{Y}'| = |\hat{V}'| = |\hat{Y}' \circ \hat{V}'|$ (последнее равенство справедливо в силу вложения $\hat{Y}' \subseteq \hat{V}'$). А значит, $\hat{V}' \subseteq \hat{Y}'$. Заметив, что $\hat{y} \subseteq \hat{v} \circ \hat{V}' \subseteq \hat{X}_v \circ \hat{Y}_v \circ \hat{Y}'$ и $\hat{y} \perp \hat{Y}_v \circ \hat{Y}'$, получим

$$1 = |\hat{y}| = I(\hat{y}, \hat{X}_v \circ \hat{Y}_v \circ \hat{Y}') = I(\hat{y}, \hat{Y}_v \circ \hat{Y}') + I_{\hat{Y}_v \circ \hat{Y}'}(\hat{y}, \hat{X}_v) = 0 + \frac{1}{n}|X_v|. \qquad \square$$

Далее будем считать, что $n \geqslant 4$. Обозначим через W множество вершин сети, состоящее из всех входов, выходов, а также элементов, имеющих номера, меньшие $n/2 - 1$ в некоторой фиксированной монотонной нумерации. Заметим, что если v — вход, то $|X_v| = 1 < n/2$, если v — выход, то $|X_v| = 0$ (так как $Y_v = \{v\}$), если v — элемент с номером, меньшим $n/2 - 1$, то в силу утв. 8 $|X_v| < n/2$. Итак, для любой вершины $v \in W$ $|X_v| < n/2$.

Лемма 3. *Пусть Γ' — компонента связности графа Γ. Тогда*

а) если Γ' — критическая компонента, то она не содержит вершин из множества W;

б) если Γ' — не критическая компонента, то она содержит не более одной вершины из множества W.

Доказательство. а) Пусть v — произвольная вершина компоненты Γ'. Если v входит в цикл, то в силу леммы 2 в) $|X_v| \geqslant n/2$, а если v не входит в цикл, то в силу леммы 2 г) $|X_v| = n$. В любом случае получаем противоречие с условием $|X_v| < n/2$, необходимым для принадлежности множеству W.

б) Предположим противное: в компоненте Γ' есть две вершины, входящие в множество W. Обозначим их через v и w, причём через w обозначим ту из них, номер которой больше (если обе они — входы, то любую из них). Тогда вершина w не предшествует вершине v, следовательно, w не предшествует выходам из множества Y_v, а значит, условие леммы 2 б) выполнено. В силу леммы 2 б)

$$|X_v| + |X_v \cup X_w| \geqslant n. \tag{8}$$

Если хотя бы одна из вершин v, w является выходом, то либо $|X_v| = 0$, либо $|X_w| = 0$, поэтому из (8) следует, что или $|X_w| \geqslant n$, или $|X_v| \geqslant n/2$. В любом случае получаем противоречие с необходимым условием $|X_v| < n/2 \,\&\, |X_w| < n/2$. Если v, w — не выходы, но хотя бы одна из них является входом, то вершина v является входом (поскольку номер вершины w не меньше номера v). Тогда $|X_v| = 1$ и из (8) следует $|X_w| \geqslant n - 2$, что при $n \geqslant 4$ противоречит условию $|X_w| < n/2$.

Осталось рассмотреть случай, когда v и w — не входы и не выходы. Пусть номер вершины w равен k. Тогда номер вершины v не больше $k - 1$. Введём новую вершину u и новые рёбра, ведущие из вершин v и w в вершину u. Перенумеруем элементы, оставив элементам с номерами $1, \dots, k$ их прежние номера, присвоив вершине u номер $k + 1$ и увеличив на 1 номера остальных элементов. Новая нумерация монотонна и $X_u = X_v \cup X_w$, поэтому в силу утв. 8, $|X_v \cup X_w| = |X_u| \leqslant (k+1)+1 = k+2$. Кроме того, $|X_v| \leqslant (k-1)+1 = k$. Тогда из (8) следует $2k + 2 \geqslant n$, т. е. $k \geqslant n/2 - 1$, что противоречит вхождению вершины w в множество W. $\square$

Теорема 1. *Если $n \geqslant 4$, то $L \geqslant 2n + \left[\frac{n-3}{2}\right]$.*

Доказательство. Заметим, что в критической компоненте связности графа Γ число вершин равно числу рёбер, а в некритической число вершин на 1 больше числа рёбер. Поэтому из леммы 3 следует, что в любой компоненте найдётся не менее k вершин, не принадлежащих множеству W, где k — число рёбер в данной компоненте. Общее число рёбер в графе Γ равно n, следовательно, найдутся n вершин графа Γ, не принадлежащие множеству W. Тогда число вершин в сети не меньше $|W| + n$, следовательно, $L \geqslant |W|$ (входы не учитываются в сложности). Множество W состоит из n входов, n выходов и элементов с номерами $1, \dots, \left[\frac{n-1}{2}\right] - 1$. Ранее мы отмечали, что выходы различны, отличны от входов и номер любого выхода не меньше $n - 1$, а значит, $L \geqslant |W| \geqslant 2n + \left[\frac{n-3}{2}\right]$. $\square$

Перейдём к приложению теории ИП к сложности булевых функций. Вначале докажем, что структура в примере 3 является ИП. Для этого достаточно проверить аксиому V. Поскольку норма системы булевых функций S определяется через вспомогательное отношение ρ_S, докажем сильную субаддитивность нормы отношения эквивалентности.

А именно, рассмотрим отношения эквивалентности на произвольном конечном множестве D (отношение мы понимаем, как подмножество в D^2). Норму отношения ρ ($|\rho|$) определим так же, как в (1) (она определяется через классы эквивалентности $K_1, \dots, K_s$). Кроме того, введём операции пересечения и объединения отношений: $\tau \circ \rho$ и $\tau * \rho$, положив $\tau \circ \rho = \tau \cap \rho$ и $\tau * \rho = <\tau \cup \rho>$, где $<\rho>$ — транзитивное замыкание отношения ρ. Заметим, что объединение систем булевых функций соответствует пересечению отношений, т. е. $\rho_{S_1 \circ S_2} = \rho_{S_1} \circ \rho_{S_2}$, поэтому аксиома V вытекает из п. г) следующей леммы.

Лемма 4. *Для любых отношений эквивалентности τ, ρ, π на множестве D:*

а) $\pi \subseteq \rho \Longrightarrow |\pi| \geqslant |\rho|$;
б) $|\tau| + |\rho| \geqslant |\tau \circ \rho|$;
в) $|\tau| + |\rho| \geqslant |\tau \circ \rho| + |\tau * \rho|$;
г) $|\tau \circ \pi| + |\rho \circ \pi| \geqslant |\tau \circ \rho \circ \pi| + |\pi|$.

Доказательство. Для сокращения записи классы эквивалентности отношения будем называть классами отношения; символом log будем обозначать логарифм по основанию 2; будем считать, что $0 \log \frac{1}{0} = 0$ (что верно в пределе). Введём функцию $\psi(x) = x \log \frac{1}{x}$, $x \geqslant 0$.

а) Каждый класс отношения π целиком содержится в одном из классов отношения ρ. Достаточно рассмотреть случай, когда один из классов отношения ρ распадается на два, а остальные остаются прежними. Слагаемые в энтропии, относящиеся к остальным классам, совпадают, поэтому их можно не рассматривать. Итак, пусть K — класс отношения ρ, K' и K'' — классы отношения π, $K = K' \cup K''$. Обозначим $p = |K|/|D|$, $p' = |K'|/|D|$, $p'' = |K''|/|D|$. Нам нужно показать, что

$$\psi(p') + \psi(p'') \geqslant \psi(p).$$

Действительно, в силу возрастания логарифма и равенства $p = p' + p''$, имеем

$$p' \log \frac{1}{p'} + p'' \log \frac{1}{p''} \geqslant p' \log \frac{1}{p} + p'' \log \frac{1}{p} = p \log \frac{1}{p}.$$

б) Пусть $K_1, \dots, K_s$ — классы отношения τ, $L_1, \dots, L_t$ — классы отношения ρ. Тогда классами отношения $\tau \circ \rho$ будут непустые множества вида $K_i \cap L_j$. Обозначим $p_i = |K_i|/|D|$, $q_j = |L_j|/|D|$, $r_{ij} = |K_i \cap L_j|/|D|$. Тогда

$$|\tau| + |\rho| = \sum_i \psi(p_i) + \sum_j \psi(q_j) = \sum_i \Big(\sum_j r_{ij}\Big) \log \frac{1}{p_i} + \sum_j \Big(\sum_i r_{ij}\Big) \log \frac{1}{q_j} =$$

$$= \sum_{i,j} r_{ij} \Big(\log \frac{1}{p_i} + \log \frac{1}{q_j}\Big) = \sum_{i,j} r_{ij} \log \frac{1}{p_i q_j}.$$

Нам осталось показать, что

$$\sum_{i,j} r_{ij} \log \frac{1}{p_i q_j} \geqslant \sum_{i,j} r_{ij} \log \frac{1}{r_{ij}}. \tag{9}$$

Из правой части (9) вычтем левую и покажем что разность неположительна. Для этого воспользуемся неравенством Иенсена, учтя вогнутость логарифма.

$$\sum_{i,j} r_{ij} \log \frac{p_i q_j}{r_{ij}} \leqslant \log\Bigl(\sum_{i,j} r_{ij} \frac{p_i q_j}{r_{ij}}\Bigr) = \log\Bigl(\sum_i p_i \cdot \sum_j q_j\Bigr) = 0.$$

в) Пусть $K_1, \ldots, K_s$ — классы отношения $\tau * \rho$. Тогда каждый класс отношений τ, ρ и $\tau \circ \rho$ целиком вложен в один из классов $K_1, \ldots, K_s$. Пусть τ_i и ρ_i — ограничения отношений τ и ρ на класс K_i $(i = 1, \ldots, s)$. Тогда $\tau_i \circ \rho_i$ — ограничение отношения $\tau \circ \rho$ на этот класс. Обозначим через $K_i^1, \ldots, K_i^{t(i)}$ классы отношения τ_i, положим $p_i = |K_i|/|D|$, $p_i^j = |K_i^j|/|D|$, $q_i^j = |K_i^j|/|K_i|$ $(j = 1, \ldots, t(i))$. Через $|\tau_i|'$ обозначим вклад, вносимый в норму отношения τ классами $K_i^1, \ldots, K_i^{t(i)}$. В силу равенства $p_i^j = p_i q_i^j$ имеем

$$\begin{aligned} |\tau_i|' = \sum_j \psi(p_i^j) = \sum_j \psi(p_i q_i^j) = p_i \sum_j q_i^j \Bigl(\log \frac{1}{p_i} + \log \frac{1}{q_i^j}\Bigr) = \\ = p_i \log \frac{1}{p_i} \Bigl(\sum_j q_i^j\Bigr) + p_i \sum_j q_i^j \log \frac{1}{q_i^j} = \psi(p_i) + p_i |\tau_i|. \end{aligned} \tag{10}$$

Аналогично определив $|\rho_i|'$ и $|\tau_i \circ \rho_i|'$, мы получим

$$|\rho_i|' = \psi(p_i) + p_i |\rho_i|, \tag{11}$$

$$|\tau_i \circ \rho_i|' = \psi(p_i) + p_i |\tau_i \circ \rho_i|. \tag{12}$$

В силу п. б),

$$|\tau_i| + |\rho_i| \geqslant |\tau_i \circ \rho_i|, \quad i = 1, \ldots, s.$$

Отсюда и из (10)–(12) следует

$$\begin{aligned} |\tau| + |\rho| - |\tau \circ \rho| = \sum_i (|\tau_i|' + |\rho_i|' - |\tau_i \circ \rho_i|') = \\ = (1 + 1 - 1) \sum_i \psi(p_i) + p_i \sum_i (|\tau_i| + |\rho_i| - |\tau_i \circ \rho_i|) \geqslant \sum_i \psi(p_i) = |\tau * \rho|. \end{aligned}$$

г) Заметим, что

$$(\tau \circ \pi) * (\rho \circ \pi) = <(\tau \cap \pi) \cup (\rho \cap \pi)> \subseteq <\pi> = \pi,$$

поэтому, в силу п. а),

$$|(\tau \circ \pi) * (\rho \circ \pi)| \geqslant |\pi|.$$

Отсюда и из п. в) следует

$$|\tau \circ \pi| + |\rho \circ \pi| \geqslant |(\tau \circ \pi) \circ (\rho \circ \pi)| + |(\tau \circ \pi) * (\rho \circ \pi)| \geqslant |\tau \circ \rho \circ \pi| + |\pi|. \qquad \square$$

Наконец, рассмотрим приложение теории ИП к сложности булевых СФЭ. СФЭ $\mathcal{C}$ можно определить, как (n, m)-сеть $\mathcal{N}$, в которой каждому элементу v поставлена в соответствие двуместная булева функция h_v, и рёбра, входящие в элемент, упорядочены. При этом будем говорить, что СФЭ $\mathcal{C}$ *вписана* в сеть $\mathcal{N}$. Поставим в соответствие входам сети переменные $x_1, \ldots, x_n$. Тогда в каждой вершине v схемы $\mathcal{C}$ вычисляется некоторая булева функция $f_v(x_1, \ldots, x_n)$. Будем использовать ИП $\mathcal{S}_n$ из примера 3 и положим $\hat{v} = \{f_v\}$. Тем самым мы построили ИС $(\mathcal{N}, \mathcal{S}_n, \hat{\cdot})$, соответствующую данной СФЭ $\mathcal{C}$. Проверим, что условия i) и ii) из определения ИС выполнены.

Действительно, булева функция f_v разбивает свою область определения не больше, чем на две части (области постоянства). Энтропия (1) такого разбиения не больше, чем $\log_2 2 = 1$. Значит, $|\hat{v}| \leqslant 1$. Далее, если элемент v непосредственно предшествует вершинам v_1 и v_2, то $f_v(\tilde{x}) = h_v(f_{v_1}(\tilde{x}), f_{v_2}(\tilde{x}))$. Каждая область постоянства функции f_v есть результат объединения некоторых областей постоянства оператора (f_{v_1}, f_{v_2}). Значит, множествам $\{f_v, f_{v_1}, f_{v_2}\}$ и $\{f_{v_1}, f_{v_2}\}$ соответствует одно и то же отношение эквивалентности. Тогда $|\hat{v} \circ \hat{v}_1 \circ \hat{v}_2| = |\hat{v}_1 \circ \hat{v}_2|$, следовательно, $\hat{v} \subseteq \hat{v}_1 \circ \hat{v}_2$.

Прямой суммой ИП $(M_1, \circ_1, |\cdot|_1)$ и $(M_2, \circ_2, |\cdot|_2)$ назовём ИП $(M_1 \times M_2, \circ, |\cdot|)$, где $\circ$ выполняется покоординатно, т. е. $(x, y) \circ (z, t) = (x \circ_1 z,\ y \circ_2 t)$ и $|(x, y)| = |x|_1 + |y|_2$. Несложно проверить, что аксиомы ИП выполнены. Аксиомы останутся выполненными также в случае, если норму любого сообщения умножить на одно и то же неотрицательное число.

Каждой перестановке σ на множестве $\{1, \ldots, n\}$ соответствует перестановочный оператор F_σ: $\{0,1\}^n \to \{0,1\}^n$:

$$F_\sigma(x_1, \ldots, x_n) = (x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

Набор перестановок $(\sigma_1, \ldots, \sigma_n)$ назовём *ортогональным*, если для любого i набор $(\sigma_1(i), \ldots, \sigma_n(i))$ есть перестановка.

Пусть $(\sigma_1, \ldots, \sigma_n)$ — ортогональный набор перестановок, $\mathcal{N}$ — (n,n)-сеть, $\mathcal{C}_i$ — СФЭ, вычисляющая оператор F_{σ_i} $(i = 1, \ldots, n)$, причём $\mathcal{C}_i$ вписана в сеть $\mathcal{N}$. Схеме $\mathcal{C}_i$ соответствует ИС, которую обозначим через $\hat{\mathcal{N}}_i$. Сообщение, соответствующее вершине v в ИС $\mathcal{N}_i$, обозначим через $\hat{v}^i$. Возьмём прямую сумму n экземпляров ИП из примера 3 и в полученном пространстве норму разделим на n. Построенное в итоге ИП обозначим через $\mathcal{S}$. Каждой вершине v сети $\mathcal{N}$ поставим в соответствие сообщение $\hat{v} = (\hat{v}^1, \ldots, \hat{v}^n)$ из ИП $\mathcal{S}$. Тем самым мы построили ИС $\hat{\mathcal{N}} = (\mathcal{N}, \mathcal{S}, \hat{\cdot})$. Проверим, что она является равномерной, т. е. удовлетворяет условиям iii) и iv).

Заметим, что в ИП из примера 3 норма сообщения $\{x_{i_1}, \ldots, x_{i_k}\}$, состоящего из k различных переменных, равна k. В ИС $\hat{\mathcal{N}}_i$ $(i = 1, \ldots, n)$ как входам, так и выходам соответствуют различные переменные, поэтому норма объединения сообщений, соответствующих входам [выходам] сети $\hat{\mathcal{N}}_i$, равна n. Просуммировав по всем i и разделив на n мы получим n. Чтобы подсчитать $I(\hat{x}, \hat{y})$, где x — вход, y — выход, заметим, что ровно для одного i переменные, соответствующие (в ИС $\hat{\mathcal{N}}_i$) входу x и выходу y, совпадают. Для данного i получим $I(\hat{x}^i, \hat{x}^i) = |\hat{x}^i| = 1$. Для всех остальных i — $I(\hat{x}^i, \hat{y}^i) = 0$. Просуммировав по все i и разделив на n, получим $I(\hat{x}, \hat{y}) = 1/n$.

Для любых $i, j \in \{1, \ldots, n\}$ обозначим через $\sigma_i(j)$ число из множества $\{1, \ldots, n\}$, сравнимое с $i + j$ по модулю n. Тогда $(\sigma_1, \ldots, \sigma_n)$ — ортогональный набор перестановок. Рассмотрим оператор F^n *циклического сдвига вправо*:

$$F^n(x_1, \ldots, x_n,\, y_1, \ldots, y_r) = F_{\sigma_y}(x_1, \ldots, x_n), \text{ где } y = \sum_{i=1}^{r} y_i 2^{r-i},\ r = \lceil \log_2 n \rceil.$$

Пусть СФЭ $\mathcal{C}$ вписана в сеть $\mathcal{N}$ и вычисляет оператор F^n. Для каждого i оператор F_{σ_i} может быть получен из F^n подстановкой соответствующих констант вместо переменных $y_1, \ldots, y_r$. Поэтому, удалив из $\mathcal{N}$ все вершины, опирающиеся на множество входов $\{y_1, \ldots, y_r\}$ (и продублировав рёбра при необходимости), мы получим (n,n)-сеть $\mathcal{N}'$, в которую для каждого i можно вписать СФЭ, вычисляющую оператор F_{σ_i}.

Мы видим, что из любой СФЭ $\mathcal{C}$, вычисляющей оператор F^n, можно получить, без увеличения сложности, равномерную (n,n)-ИС. Значит, из нижней оценки сложности n-РИС следует нижняя оценка сложности оператора F^n в классе СФЭ. Обозначим через $L(F)$ сложность оператора F в классе СФЭ. Приведём следствие из теоремы 1.

Следствие 3. $L(F^n) \geqslant 2{,}5n - O(1)$.

В заключение отметим, что сложность оператора F^n в классе СФЭ нелинейна тогда и только тогда, когда нелинейна минимальная сложность сети, в которую можно вписать СФЭ для каждого из операторов F_{σ_i} [6].

Работа выполнена при финансовой поддержке РФФИ (проект 05–01–00994), программы поддержки ведущих научных школ РФ (проект НШ–1807.2003.01) и программы "Университеты России" (проект УР.04.02.528).

Список литературы

1. Шеннон К. Работы по теории информации и кибернетике. — М.: ИЛ, 1963.

2. Колмогоров А. Н. Избранные труды. Т. 3. Теория информации и теория алгоритмов. — М.: Наука, 2005.

3. Холево А. С. Введение в квантовую теорию информации. — М.: МЦНМО, 2002.

4. Лупанов О. Б. Нижние оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.

5. Ху Т. Целочисленное программирование и потоки в сетях. — М.: Мир, 1974.

6. Черухин Д. Ю. Об информационной составляющей в сложности оператора сдвига // Дискрет. анализ и исслед. операций. — 2005. — Т. 12, No 2. — с. 73–77.

мех.-мат. факультет МГУ, Воробьёвы горы, Москва, 119992, Россия
E-mail address: cherukhin@rambler.ru