

The Complexity of Depth-Two Information Networks

D. Yu. Cherukhin

Moscow State University, Faculty of Mechanics and Mathematics,
 Leninskie Gory, Moscow, 119991 Russia

Received September 05, 2007

Abstract—The lower bound $\Omega(n \log_2 n)$ for the complexity of an arbitrary depth-two information network with n inputs and n outputs is proved providing the inputs are independent, the outputs are independent, and the total information of any input and any output is n times less than the entropy of any input or output. A similar estimate for Boolean depth-two circuits of functional elements is obtained as a corollary.

DOI: 10.3103/S0027132209010045

We prove the lower bound $\Omega(n \log_2 n)$ for the complexity of an arbitrary depth-two information network with n inputs and n outputs providing the inputs are independent, the outputs are independent, and the total information of any input and any output is n times less than the entropy of any input or output. A similar estimate for Boolean circuits of functional elements (CFE, see [1]) with depth 2 is obtained as a corollary.

Let us formalize information properties which we suppose to use to prove a lower bound for the complexity. An *information space* (IS) is defined as a collection $\mathcal{S} = (M, \circ, |\cdot|)$, where M is a set of objects referred to as *messages*; $\circ: M^2 \rightarrow M$ denotes the *union* operation for messages; and $|\cdot|: M \rightarrow \mathbb{R}$ is the *messages norm* functional (by norm we understand the amount of information), such that for any $x, y, z \in M$ the following axioms are valid:

- (I) $x \circ x = x$; (II) $x \circ y = y \circ x$; (III) $(x \circ y) \circ z = x \circ (y \circ z)$;
- (IV) $\exists \Lambda \in M (|\Lambda| = 0 \ \& \ \forall t \in M \ \Lambda \circ t = t)$;
- (V) $|x \circ y| + |x \circ z| \geq |x \circ y \circ z| + |x|$ (strong subadditivity).

Let $\mathcal{S} = (M, \circ, |\cdot|)$ be an IS, $x, y, z, u \in M$. Assume $|x|_u = |x \circ u| - |u|$. Then the collection $\mathcal{S}_u = (M, \circ, |\cdot|_u)$ is also an IS (it suffices to verify Axiom (V): $|x \circ y|_u + |x \circ z|_u = |x \circ y \circ u| + |x \circ z \circ u| - 2|u| \geq |x \circ y \circ z \circ u| + |x \circ u| - 2|u| = |x \circ y \circ z|_u + |x|_u$). Introduce the following notations: $I(x, y) = |x| + |y| - |x \circ y|$; $x \subseteq y \iff |x \circ y| = |y|$. If some function (or relation) ϕ is defined in terms of an IS, then by ϕ_u we denote the same function with respect to the norm $|\cdot|_u$. For example, $x \subseteq_u y \iff |x \circ y|_u = |y|_u$.

Assertion 1. For any messages x, y, z the following relations are valid:

- (a) $(|x|_y)_z = |x|_{y \circ z}$; (b) $|x| = I(x, y) + |x|_y$; (c) $I(x, y \circ z) = I_z(x, y) + I(x, z)$;
- (d) $|x| \geq 0$; (e) $|x \circ y| \geq |x|$; (f) $I(x, y) \geq 0$;
- (g) $I(x, y \circ z) \geq I_z(x, y)$; (h) $I(x, y \circ z) \geq I(x, y)$.

If $x \subseteq y$, then the following relations hold:

- (i) $I(x, y) = |x|$; (j) $x \subseteq y \circ z$; (k) $x \subseteq_z y$.

If $I(x, y) = 0$, then (l) $I(x \circ y, z) \geq I(x, z) + I(y, z)$.

Proof. Statements (a)–(c), and (i) follow directly from the definitions, statements (d)–(f) follow from Axiom (V): in the first case we assume $y = z$, $x = \Lambda$, in the second case we assume $y = z$, and in the third case $x = \Lambda$; statements (g) and (h) follow from (c) and (f).

Prove (j) and (k): $|x \circ y| + |y \circ z| \geq |y| + |x \circ y \circ z| \iff 0 = |x \circ y| - |y| \geq |x \circ y \circ z| - |y \circ z| \iff |y \circ z| \geq |x \circ y \circ z|$; on the other hand (e) implies $|y \circ z| \leq |x \circ y \circ z|$. Thus, we have $|y \circ z| = |x \circ y \circ z| \iff x \subseteq y \circ z$. At the same time, $|y \circ z| = |x \circ y \circ z| \iff |y|_z = |x \circ y|_z \iff x \subseteq_z y$.

Prove (l) using (c) and (h): $I(x \circ y, z) = I(x, z) + I_x(y, z) = I(x, z) + I(y, x \circ z) - I(y, x) = I(x, z) + I(y, x \circ z) \geq I(x, z) + I(y, z)$. \square

By (n, m) -*network* (or just by a *network*) we call a finite oriented graph without oriented cycles where n inputs and m outputs are chosen and none of inputs is an end of an edge. By x_1, \dots, x_n we denote inputs of the network and by y_1, \dots, y_m we denote its outputs. We also assume $X = \{x_1, \dots, x_n\}$, $Y = \{y_1, \dots, y_m\}$. The complexity of a network is the number of its edges and its depth is the maximal length of an oriented path in this network. A network is said to be two-tier if the length of any its oriented path joining an input

with an output is equal to 2. Any depth-two network can be reduced to a two-tier network by an evident transformation, which enlarges the complexity at most by a constant factor; therefore, we restrict ourselves to consideration of two-tier networks.

We say that an (n, n) -network is *uniform informational* (an n -UIN) if any its vertex v is endowed with a message \hat{v} from some fixed IS and the following properties are valid:

- i) if v_1, \dots, v_s are all the vertices with outgoing edges incoming into v , then $\hat{v} \subseteq \hat{v}_1 \circ \dots \circ \hat{v}_s$;
- ii) $\forall v |\hat{v}| \leq 1$; iii) $|\hat{y}_1 \circ \dots \circ \hat{y}_n| = n, \forall i, j I(x_i, y_j) = \frac{1}{n}$.

Let S be a network with a vertex set W , and $V \subseteq W, U \subseteq W$. By $S \setminus V$ we denote the network obtained from S by elimination of all vertices from V (V may contain inputs and outputs). We say that a set V *relies* on a set U if any oriented path going from an input to some vertex from V contains at least one vertex from U . If a network is n -UIN and $V = \{v_1, \dots, v_s\}$, then assume $\hat{V} = \hat{v}_1 \circ \dots \circ \hat{v}_s$. It is not difficult to show that if V relies on U , then $\hat{V} \subseteq \hat{U}$.

Assertion 2. *Let S be an n -UIN, $X_1 \subseteq X, Y_1 \subseteq Y$. Then the equalities*

$$(a) |\hat{X}_1| = |X_1|; \quad (b) |\hat{Y}_1| = |Y_1|; \quad (c) I(\hat{X}_1, \hat{Y}_1) = \frac{1}{n} |X_1| |Y_1| \tag{2}$$

are valid.

Proof. Assume $X_2 = X \setminus X_1, Y_2 = Y \setminus Y_1$. Notice that the set Y relies on X and hence $\hat{Y} \subseteq \hat{X}$.

(b) We have

$$n = |\hat{Y}| = |\hat{Y}_1 \circ \hat{Y}_2| \leq |\hat{Y}_1| + |\hat{Y}_2| \leq |Y_1| + |Y_2| \leq |Y_1| + |Y_2| = n. \tag{3}$$

Since the right-hand side and the left-hand side of (3) are equal to each other, then all inequalities can be replaced by equalities and hence $|\hat{Y}_1| = |Y_1|$.

(a) Due to the inclusion $\hat{Y} \subseteq \hat{X}$, we have $n = |\hat{Y}| \leq |\hat{X}| \leq n$ and hence $|\hat{X}| = n$. Then Item (a) can be proved similarly to Item (b).

(c) The inclusion $\hat{Y} \subseteq \hat{X}$ implies $I(\hat{X}, \hat{Y}) = |\hat{X}| + |\hat{Y}| - |\hat{X} \circ \hat{Y}| = |\hat{Y}| = n$. Due to (a), for any nonintersecting $X', X'' \subseteq X$ the relation $I(\hat{X}', \hat{X}'') = 0$ holds; due to (b), a similar statement is valid for the set Y . Using Assertion 1 (l), we get

$$n = I(\hat{X}, \hat{Y}) \geq I(\hat{X}_1, \hat{Y}_1) + I(\hat{X}_2, \hat{Y}_1) + I(\hat{X}, \hat{Y}_2) \geq \sum_{i,j} I(\hat{x}_i, \hat{y}_j) = n. \tag{4}$$

Replacing all inequalities in (4) by equalities, we obtain what was required. \square

If S is an (n, m) -network, then by $M^S = (m_{ij}^S)$ we denote the Boolean $(n \times m)$ matrix such that $m_{ij}^S = 1$ if and only if there exists an oriented path from x_i to y_j . Let $M = (m_{ij})$ be a Boolean $(n \times m)$ matrix. A pair $(i, j) \subseteq \{1, \dots, n\} \times \{1, \dots, m\}$ is called a *lower zero* of the matrix M if for any i' from the set $\{1, \dots, i\}$ and for any j' from the set $\{1, \dots, j\}$ the equality $m_{i'j'} = 0$ is valid. Introduce the following notations: $N(M)$ denotes the number of lower zeros of the matrix M ; $N^*(M) = \max_{M'} N(M')$, where the maximum is taken over all matrices M' obtained from M by some permutation of its rows and columns.

Lemma 1. *Let S be an n -UIN and Z be a subset of its vertex set. Then $N^*(M^{S \setminus Z}) \leq n|Z|$.*

Proof. Due to symmetry, we can assume that inputs and outputs are enumerated so that $N^*(M^{S \setminus Z}) = N(M^{S \setminus Z})$. Let $i \in \{1, \dots, n\}$. Assume $X'_i = \{x_j \mid m_{ji}^{S \setminus Z} = 1\}$, $\theta_i = \hat{X}'_i \circ \hat{y}_i$, $X_i = X'_1 \cup \dots \cup X'_i$, $Y_i = \{y_1, \dots, y_i\}$. The set $\{y_i\}$ relies (in the network S) on the set $X'_i \cup Z$. Therefore, $\hat{y}_i \subseteq \hat{X}'_i \circ \hat{Z}$. Then, due to Assertion 1 (j) and (k), we have $\hat{y}_i \subseteq_{\hat{Y}_{i-1}} \hat{X}'_i \circ \hat{Z}$ and hence (due to Assertion 1 (i))

$$I_{\hat{Y}_{i-1}}(\hat{X}'_i \circ \hat{Z}, \hat{y}_i) = |\hat{y}_i|_{\hat{Y}_{i-1}}. \tag{5}$$

We have

$$\begin{aligned} |Z| &\geq |\hat{Z}| \stackrel{(1)(b)}{=} I(\hat{Z}, \theta_1) + |\hat{Z}|_{\theta_1} = I(\hat{Z}, \theta_1) + I_{\theta_1}(\hat{Z}, \theta_2) + |\hat{Z}|_{\theta_1 \circ \theta_2} \\ &\dots = \sum_{i=1}^n I_{\hat{X}_{i-1} \circ \hat{Y}_{i-1}}(\hat{Z}, \theta_i) + |\hat{Z}|_{\hat{X}_n \circ \hat{Y}_n} \stackrel{(1)(d)}{\geq} \sum_{i=1}^n I_{\hat{X}_{i-1} \circ \hat{Y}_{i-1}}(\hat{Z}, \theta_i) \\ &\stackrel{(1)(g)}{\geq} \sum_{i=1}^n I_{\hat{X}_i \circ \hat{Y}_{i-1}}(\hat{Z}, \hat{y}_i) \stackrel{(1)(c)}{=} \sum_i \left(I_{\hat{Y}_{i-1}}(\hat{X}'_i \circ \hat{Z}, \hat{y}_i) - I_{\hat{Y}_{i-1}}(\hat{X}'_i, \hat{y}_i) \right) \stackrel{(5)}{=} \sum_i \left(|\hat{y}_i|_{\hat{Y}_{i-1}} - I_{\hat{Y}_{i-1}}(\hat{X}'_i, \hat{y}_i) \right) \end{aligned}$$

$$\begin{aligned}
&\stackrel{(1)(c)}{=} \sum_i \left(|\hat{Y}_i| - |\hat{Y}_{i-1}| - (I(\hat{X}_i, \hat{Y}_i) - I(\hat{X}_i, \hat{Y}_{i-1})) \right) \stackrel{(2)}{=} \sum_i \left(i - (i-1) - \frac{1}{n} |X_i| (i - (i-1)) \right) \\
&= \frac{1}{n} \sum_i (n - |X_i|) = \frac{1}{n} \sum_i |(X \setminus X'_1) \cap \dots \cap (X \setminus X'_i)|. \tag{6}
\end{aligned}$$

It remains to note that the set $(X \setminus X'_1) \cap \dots \cap (X \setminus X'_i)$ contains all x_j such that the pair (j, i) is a lower zero of the matrix $M^{S \setminus Z}$. Therefore, proceeding with (6), we obtain $|Z| \geq \frac{1}{n} N(M^{S \setminus Z}) = \frac{1}{n} N^*(M^{S \setminus Z})$. \square

Lemma 2. *Let S be a two-tier (n, n) -network whose each input and each output is incident to at most r edges. Let k be the number of zeros in the matrix M^S . Then*

$$N^*(M^S) \geq \frac{k}{C_{2r}^r}.$$

Proof. Let $V = \{v_1, \dots, v_t\}$ be the vertex set of the middle layer of the network S (i.e., the vertices which are neither input, nor output). By V_i ($i = 1, \dots, n$) we denote the set of vertices from V adjacent to x_i ; by W_j ($j = 1, \dots, n$) we denote the set of vertices from V adjacent to y_j . Then $|V_i| \leq r$, $|W_j| \leq r$. Notice that $m_{ij}^S = 0$ if and only if $V_i \cap W_j = \emptyset$.

Consider an arbitrary permutation $\tau \in S_t$. Assume $X_i^\tau = \max\{\tau(l) \mid v_l \in V_i\}$, $Y_j^\tau = \min\{\tau(l) \mid v_l \in W_j\}$. There exist permutations $\sigma, \pi \in S_n$ such that

$$X_{\sigma(1)}^\tau \leq \dots \leq X_{\sigma(n)}^\tau \quad \text{and} \quad Y_{\pi(1)}^\tau \geq \dots \geq Y_{\pi(n)}^\tau. \tag{7}$$

Consider the matrix $M' = (m'_{ij})$, where $m'_{ij} = m_{\sigma(i)\pi(j)}^S$, which is obtained from M^S by permutation of rows and columns. If the relation $X_{\sigma(i)}^\tau < Y_{\pi(j)}^\tau$ holds for some i, j , then by (7) the relation $X_{\sigma(i')}^\tau < Y_{\pi(j')}^\tau$ is valid for any $i' \leq i$, $j' \leq j$. Then $V_{\sigma(i')} \cap W_{\pi(j')} = \emptyset$ and so $m'_{i'j'} = 0$. Thus, if $X_{\sigma(i)}^\tau < Y_{\pi(j)}^\tau$, then (i, j) is a lower zero of the matrix M' and hence

$$N^*(M^S) \geq N(M') \geq |\{(i, j) \mid X_{\sigma(i)}^\tau < Y_{\pi(j)}^\tau\}| = |\{(i, j) \mid X_i^\tau < Y_j^\tau\}|. \tag{8}$$

Consider an arbitrary pair (i, j) such that $m_{ij}^S = 0$ and estimate the quota of permutations τ which $X_i^\tau < Y_j^\tau$ for. Let $|V_i| = p$, $|W_j| = q$. If we fix the set of places where the vertices from $V_i \cup W_j$ are located, then the condition $X_i^\tau < Y_j^\tau$ is fulfilled by permutations τ such that first p places are taken by the vertices from V_i and the last q places are occupied by the vertices from W_j . Hence, the quota required is equal to $\frac{1}{C_{p+q}^p} \geq \frac{1}{C_{2r}^r}$.

Summing relation (8) over all τ , we finally get

$$N^*(M^S) \geq \frac{1}{t!} |\{(i, j, \tau) \mid X_i^\tau < Y_j^\tau\}| \geq \frac{1}{t!} \sum_{i,j: m_{ij}=0} |\{\tau \mid X_i^\tau < Y_j^\tau\}| \geq \frac{1}{t!} k \frac{t!}{C_{2r}^r} = \frac{k}{C_{2r}^r}. \quad \square$$

Theorem. *The complexity of a two-tier n -UIN is at least of order $n \log_2 n$.*

Proof. Let S be a two-tier n -UIN of the minimal complexity being equal to L . Assume $r = \lceil \frac{2L}{n} \rceil$. By X_1 we denote the set of all inputs adjacent to more than r vertices, by Y_1 we denote the set of outputs adjacent to more than r vertices, and let Z be the set of vertices from the middle layer adjacent to more than $\frac{n}{4r}$ outputs. Let $S' = S \setminus (X_1 \cup Y_1 \cup Z)$, $X_2 = X \setminus X_1$, $Y_2 = Y \setminus Y_1$. The edges of a two-tier network which are incident to distinct inputs and outputs are distinct themselves, therefore, $L \geq (r+1)(|X_1| + |Y_1|) > \frac{2L}{n}(|X_1| + |Y_1|)$. Similarly, $L \geq \frac{n}{4r}|Z|$. Thus,

$$|X_1| \leq \frac{n}{2}, \quad |Y_1| \leq \frac{n}{2}, \quad |Z| \leq L \frac{4r}{n} \leq 2r(r+1). \tag{9}$$

Let k be the number of zeros in the matrix $M^{S'}$. Each input of the network S' is adjacent to at most r vertices from the middle layer (of the network S') each of which in its turn is adjacent to at most $\frac{n}{4r}$ outputs. Thus, from each input of the network S' one can get to at most $r \frac{n}{4r} = \frac{n}{4}$ outputs through an oriented path. Hence, the number of units in the matrix $M^{S'}$ does not exceed $|X_2| \frac{n}{4}$. Then, taking into account (9), we have

$$k \geq |X_2| |Y_2| - |X_2| \frac{n}{4} = |X_2| \left(|Y_2| - \frac{n}{4} \right) \geq \frac{n}{2} \left(\frac{n}{2} - \frac{n}{4} \right) = \frac{n^2}{8}. \tag{10}$$

Combining Lemmas 1 and 2, relations (9) and (10), and taking into account that the matrix $M^{S'}$ is a submatrix of the matrix $M^{S \setminus Z}$, we obtain

$$\frac{n^2}{8C_{2r}^r} \leq \frac{k}{C_{2r}^r} \leq N^*(M^{S'}) \leq N^*(M^{S \setminus Z}) \leq n|Z| \leq 2nr(r+1).$$

Thus, $n \leq 16C_{2r}^r r(r+1) \leq 4^{r(1+o(1))}$. Substituting the definition of r , we obtain the estimate required. \square

In conclusion we demonstrate how to apply the theorem to obtain a similar lower estimate for the complexity of CFE of depth 2 in the basis consisting of all Boolean functions. Let $P_2(n) = \{f \mid f: \{0,1\}^n \rightarrow \{0,1\}\}$. Consider an IS $\mathcal{S}_n = (M_n, \circ, |\cdot|)$, where M_n is the set of subsets of the set $P_2(n)$, \circ is the set union operation, and the norm $|\cdot|$ is defined as follows. Let $\mathcal{F} \in M$ and K_1, \dots, K_s be all maximal subsets in $\{0,1\}^n$ such that any function $f \in \mathcal{F}$ is constant on each of them. Then we assume

$$|\mathcal{F}| = \sum_{i=1}^s p_i \log_2 \frac{1}{p_i}, \quad \text{where } p_i = \frac{|K_i|}{2^n}. \tag{11}$$

It is not difficult to see that Axioms (I)–(IV) are valid. Explain why Axiom (V) holds. In fact, we consider functions from $P_2(n)$ as random variables whose simple events set is $\{0,1\}^n$. A set of such functions corresponds to the joint distribution of random variables, and the norm (11) is the Shannon entropy [2] of the joint distribution (note that the entropy of a joint distribution does not depend on the order of random variables in the collection, therefore, one can consider the set of variables instead of their collection). Then Axiom (V) follows from the strong subadditivity property of the Shannon entropy, which is well known.

Consider also the IS $\mathcal{S}'_n = (M'_n, \circ', |\cdot|')$, where $M'_n = M_n^n$, $(\mathcal{F}_1, \dots, \mathcal{F}_n) \circ' (\mathcal{G}_1, \dots, \mathcal{G}_n) = (\mathcal{F}_1 \circ \mathcal{G}_1, \dots, \mathcal{F}_n \circ \mathcal{G}_n)$, and $|(\mathcal{F}_1, \dots, \mathcal{F}_n)|' = \frac{1}{n}(|\mathcal{F}_1| + \dots + |\mathcal{F}_n|)$. One can say that \mathcal{S}'_n is the direct sum of n copies of the IS \mathcal{S}_n , where the norm is n times decreased. Axioms (I)–(V) for \mathcal{S}'_n directly follow from the corresponding axioms for \mathcal{S}_n .

Each permutation $\sigma \in S_n$ corresponds to the Boolean *permutable operator* $F_\sigma: \{0,1\}^n \rightarrow \{0,1\}^n$, $F_\sigma(x_1, \dots, x_n) = (x_{\sigma(1)}, \dots, x_{\sigma(n)})$. A collection $\Sigma = (\sigma_1, \dots, \sigma_n)$ of permutations is called *orthogonal*, if the collection $(\sigma_1(i), \dots, \sigma_n(i))$ is a permutation for any i .

Let Σ be an orthogonal collection of permutations, and $F_\Sigma: \{0,1\}^{n+k} \rightarrow \{0,1\}^n$ be a Boolean operator depending on the variables $x_1, \dots, x_n, y_1, \dots, y_k$ ($k = O(n)$) such that for any permutation σ_i from the collection Σ the operator F_{σ_i} can be obtained from F_Σ by substitution of some constants for the variables y_1, \dots, y_k . Further, let S be a CFE calculating the operator F_Σ . Substituting the corresponding constants for the inputs y_1, \dots, y_k of S , we obtain a CFE S_i calculating the operator F_{σ_i} .

By S' we denote the (n, n) -network obtained from S by elimination of all vertices relying on the set $\{y_1, \dots, y_k\}$. Assign a message \hat{v} from IS \mathcal{S}'_n to each vertex v of the network S' as follows. Let f_i^v be a function of the variables x_1, \dots, x_n calculated at the vertex v of the circuit S_i . We assume $\hat{v} = (\{f_1^v\}, \dots, \{f_n^v\})$. One can verify that the network S' together with the messages \hat{v} is an n -UIN.

Corollary. *The complexity of any operator F_Σ from the class of CFE of depth 2 is at least of order $n \log_2 n$.*

Note that for the class of depth 2 circuits considered here the lower estimates of the form $\Omega(n^{3/2})$ are known [3]. Besides, the estimates $\Omega(n \log_2 n)$ (see [4]) and $\Omega(n \log_2^{3/2} n)$ (see [5]) are known for one of the operators of the form F_Σ , namely, for the cyclic shift operator.

REFERENCES

1. O. B. Lupanov, *Asymptotic Estimates for the Complexity of Control Systems*, (Moscow State Univ., Moscow, 1984) [in Russian].
2. C. Shannon, *Papers on Information Theory and Cybernetics*, (IL, Moscow, 1963) [in Russian].
3. D. Yu. Cherukhin, "The Lower Estimate of Complexity in the Class of Schemes of Depth 2 without Restrictions on a Basis," *Vestn. Mosk. Univ., Matem. Mekhan.*, No 4, 54 (2005) [Moscow Univ. Math. Bull. **60** (4), 42 (2005)].
4. P. Pudlák and P. Savický, "On Shifting Networks," *Theor. Comput. Sci.* **116**, 415 (1993).
5. P. Pudlák, V. Rödl, and J. Sgall, "Boolean Circuits, Tensor Ranks and Communication Complexity," *SIAM J. Comput.* **26** (3), 605 (1997).

Translated by A. Ivanov