Basic Research in Computer Science

BRICS RS-94-2 A. E. Andreev: Complexity of Nondeterministic Functions

Complexity of Nondeterministic Functions

Alexander E. Andreev

BRICS Report Series **RS-94-2**

ISSN 0909-0878 **February 1994**

See back inner page for a list of recent publications in the BRICS Report Series. Copies may be obtained by contacting:

**BRICS
Department of Computer Science
University of Aarhus
Ny Munkegade, building 540
DK - 8000 Aarhus C
Denmark**

**Telephone: +45 8942 3360
Telefax: +45 8942 3255
Internet: BRICS@brics.dk**

BRICS publications are in general accessible through WWW and anonymous FTP:

`http://www.brics.dk/`
`ftp ftp.brics.dk (cd pub/BRICS)`

Complexity of Nondeterministic Functions

Alexander E. Andreev*

Department of Mechanics and Mathematics
Moscow State University, Moscow, 119899, Russia
E-mail: andreev@matis.math.msu.su

Abstract

The complexity of a nondeterministic function is the minimum possible complexity of its determinisation. The entropy of a nondeterministic function, F, is minus the logarithm of the ratio between the number of determinisations of F and the number of all deterministic functions.

We obtain an upper bound on the complexity of a nondeterministic function with restricted entropy for the worst case.

These bounds have strong applications in the problem of algorithm derandomization. A lot of randomized algorithms can be converted to deterministic ones if we have an effective hitting set with certain parameters (a set is hitting for a set system if it has a nonempty intersection with any set from the system).

Linial, Luby, Saks and Zuckerman (1993) constructed the best effective hitting set for the system of k-value, n-dimensional rectangles. The set size is polynomial in $k(\log n)/\epsilon$.

Our bounds of nondeterministic functions complexity offer a possibility to construct an effective hitting set for this system with almost linear size in $k(\log n)/\epsilon$.

*Research finished while visiting the Computer Science Department of Aarhus University. The visit was funded by BRICS, Centre of the Danish National Research Foundation.
The research was supported by the ESPRIT II BRA Programme of the EC under contract #7141 (ALCOM II), by Grant N 93-011-16005 of the Russian Fund for Fundamental Researches, and by Grant N 93-1-60-15 of the Russian Ministry of Science and Education.

Contents

1 Introduction

1.1 Computation and complexity of nondeterministic functions

Let $\mathcal{A}$ and $\mathcal{B}$ be finite sets. By $\mathrm{Hom}(\mathcal{A},\mathcal{B})$ we denote the system of all functions (mappings) from the set $\mathcal{A}$ into the set $\mathcal{B}$. By $\mathcal{B}^*$ we denote the system of all nonempty subsets of the set $\mathcal{B}$. We suppose, that there is no difference between element b of the set $\mathcal{B}$ and element $\{b\}$ of the set $\mathcal{B}^*$. In that way $\mathcal{B} \subseteq \mathcal{B}^*$. We define

$$\mathrm{HOM}(\mathcal{A},\mathcal{B}) \;=\; \mathrm{Hom}(\mathcal{A},\mathcal{B}^*) \;.$$

We say that functions from the set $\mathrm{HOM}(\mathcal{A},\mathcal{B})$ are nondeterministic functions from $\mathcal{A}$ into $\mathcal{B}$. It is easy to see, that

$$\mathrm{Hom}(\mathcal{A},\mathcal{B}) \;\subseteq\; \mathrm{HOM}(\mathcal{A},\mathcal{B}) \;.$$

Now we define some relations between the functions from $\mathrm{HOM}(\mathcal{A},\mathcal{B})$. For

$$\mathbf{f} \;\in\; \mathrm{Hom}(\mathcal{A},\mathcal{B}) \;, \qquad \mathbf{F} \;\in\; \mathrm{HOM}(\mathcal{A},\mathcal{B}) \;,$$

we let

$$\mathbf{f} \in \mathbf{F} \qquad \Longleftrightarrow \qquad \forall a \in \mathcal{A} \;:\; \mathbf{f}(a) \in \mathbf{F}(a) \;.$$

For

$$\mathbf{F},\mathbf{G} \;\in \mathrm{HOM}(\mathcal{A},\mathcal{B}) \;,$$

we let

$$\mathbf{F} \subseteq \mathbf{G} \qquad \Longleftrightarrow \qquad \forall a \in \mathcal{A} \;:\; \mathbf{F}(a) \subseteq \mathbf{G}(a) \;.$$

For any function $\mathbf{F}$ from $\mathrm{HOM}(\mathcal{A},\mathcal{B})$ we introduce the following notations:

- $\mathbf{P}(\mathbf{F})$ – the relative volume:

$$\mathbf{P}(\mathbf{F}) \;=\; \prod_{a\in\mathcal{A}} \frac{\mid \mathbf{F}(a) \mid}{\mid \mathcal{B} \mid} \;;$$

- $\mathbf{H}(\mathbf{F})$ – the entropy of $\mathbf{F}$:

$$\mathbf{H}(\mathbf{F}) \;=\; -\log \mathbf{P}(\mathbf{F}) \;.$$

- $\mathcal{M}(\mathbf{F})$ – the domain of $\mathbf{F}$:

$$\mathcal{M}(\mathbf{F}) \ = \ \{a \mid \ a \in \mathcal{A} \ , \ \mathbf{F}(a) \neq \mathcal{B}\} \ .$$

It is easy to see, that

$$\mathbf{H}(\mathbf{F}) \ = \ \sum_{a \in \mathcal{A}} \log \frac{\mid \mathcal{B} \mid}{\mid \mathbf{F}(a) \mid} \ = \ \sum_{a \in \mathcal{M}(\mathbf{F})} \log \frac{\mid \mathcal{B} \mid}{\mid \mathbf{F}(a) \mid} \ .$$

If ϕ is some bijection from $\mathrm{Hom}(\mathcal{A}_1, \mathcal{A}_2)$, then we can define the mapping Φ such that

$$\Phi \ : \ \mathrm{HOM}(\mathcal{A}_2, \mathcal{B}) \ \longrightarrow \ \mathrm{HOM}(\mathcal{A}_1, \mathcal{B}) \ ,$$

$$\Phi(\mathbf{F}) \ = \ \phi \circ \mathbf{F} \ , \qquad \text{where} \qquad \forall a \in \mathcal{A}_1 \ : \ (\phi \circ \mathbf{F})(a) = \mathbf{F}(\phi(a)) \ .$$

It is easy to check, that for any $\mathbf{F}$, $\mathbf{G}$ from $\mathrm{HOM}(\mathcal{A}_2, \mathcal{B})$ we have

$$\mathbf{P}(\Phi(\mathbf{F})) \ = \ \mathbf{P}(\mathbf{F}) \ , \qquad \mathbf{H}(\Phi(\mathbf{F})) \ = \ \mathbf{H}(\mathbf{F}) \ ,$$

$$\phi(\mathcal{M}(\Phi(\mathbf{F})) \ = \ \mathcal{M}(\mathbf{F}) \ ,$$

$$\forall \mathbf{f} \in \mathrm{Hom}(\mathcal{A}_2, \mathcal{B}) \ : \ \mathbf{f} \in \mathbf{F} \iff \Phi(\mathbf{f}) \in \Phi(\mathbf{F}) \ ,$$

$$\mathbf{F} \subseteq \mathbf{G} \iff \Phi(\mathbf{F}) \subseteq \Phi(\mathbf{G}) \ .$$

We will investigate the complexity of nondeterministic functions from $\mathrm{HOM}(\mathcal{A}, \mathcal{B})$. We suppose, that in this case some coding algorithm for the sets $\mathcal{A}$ and $\mathcal{B}$ is fixed. We can suppose that

$$\mathcal{A} \subseteq \{0,1\}^r \ , \qquad r \ = \ \lceil \log \mid \mathcal{A} \mid \rceil \ ,$$

$$\mathcal{B} \subseteq \{0,1\}^k \ , \qquad k \ = \ \lceil \log \mid \mathcal{B} \mid \rceil \ .$$

Let $\mathbf{S}(x_1, x_2, ..., x_r)$ be a circuit with k outputs. By $\mathbf{S}(\mathbf{a})$ we denote the output sequence from $\{0,1\}^k$ on the input sequence $\mathbf{a}$ from $\{0,1\}^r$.

The circuit $\mathbf{S}$ compute nondeterministic function $\mathbf{F}$ from $\mathrm{HOM}(\mathcal{A}, \mathcal{B})$, if

$$\forall \mathbf{a} \in \mathcal{A} \ : \qquad \mathbf{S}(\mathbf{a}) \in \mathbf{F}(\mathbf{a}) \ .$$

The complexity of the nondeterministic function $\mathbf{F}$ is minimal possible complexity of the circuits computing it. We denote the complexity of the function $\mathbf{F}$ by $\mathbf{L}(\mathbf{F})$.

In this paper we consider circuits built from elements with two inputs. We use circuit size as the complexity of circuits.

If $\mathcal{R}$ is a subsystem of $\mathrm{HOM}(\mathcal{A},\mathcal{B})$, then we define the Shannon function of $\mathcal{R}$ by:

$$\mathbf{L}(\mathcal{R}) \;=\; \max_{\mathbf{F}\in\mathcal{R}} \mathbf{L}(\mathbf{F}) \;.$$

We will try to obtain bounds for the values

$$\mathbf{L}(\mathrm{HOM}_\epsilon(\mathcal{A},\mathcal{B})) \qquad \text{and} \qquad \mathbf{L}(\mathrm{HOM}^m(\mathcal{A},\mathcal{B})) \;,$$

where

$$\mathrm{HOM}_\epsilon(\mathcal{A},\mathcal{B}) \;=\; \{\mathbf{F} \mid \; \mathbf{F}\in\mathrm{HOM}(\mathcal{A},\mathcal{B}) \;,\; \mathbf{P}(\mathbf{F})\geq\epsilon\} \qquad \text{and}$$

$$\mathrm{HOM}^m(\mathcal{A},\mathcal{B}) \;=\; \{\mathbf{F} \mid \; \mathbf{F}\in\mathrm{HOM}(\mathcal{A},\mathcal{B}) \;,\; \mathbf{H}(\mathbf{F})\leq m\} \;.$$

It is easy to see, that for $\epsilon = 2^{-m}$ we have

$$\mathrm{HOM}^m(\mathcal{A},\mathcal{B}) \;=\; \mathrm{HOM}_\epsilon(\mathcal{A},\mathcal{B}) \;.$$

1.2 Previous and new results

This work is a natural development of the line of almost optimal circuit design. Shannon (1949) has put the problem and has obtained the first results in this direction. He defined the function $\mathbf{L}(n)$, the worst case complexity of n-variable boolean function, and has proved that

$$c_1\frac{2^n}{n} \;\leq\; \mathbf{L}(n) \;\leq\; c_2\frac{2^n}{n} \;,$$

for some positive constants c_1 and c_2.

Lupanov(1956) has obtained that the asymptotic behavior of Shannon function is

$$\mathbf{L}(n) \;\sim\; \frac{2^n}{n} \;.$$

The research that followed has concentrated on the analysis of different classes of boolean functions, for example monotone function. Jablonsky(1957), Ugolnikov(1976), Pippenger(1978), Andreev(1988) has obtained interesting results in this area. Lupanov(1965) has developed local coding principle for this problem. Andreev(1985) has created stronger and more general method.

Nechiporuk(1965) has considered partial boolean functions. This is degenerate case of nondeterministic functions, i.e. the system $\mathrm{HOM}(\{0,1\}^n,\{0,1\})$. He has obtained the asymptotic for the Shannon function

$$\mathbf{L}(\mathrm{HOM}^m(\{0,1\}^n,\{0,1\})) \;\sim\; \frac{m}{\log m} \;.$$

in the case where the entropy m and the number 2^n are not very much different. Sholomov(1969) had proved this asymptotic behavior for more general case.

Pippenger(1977) has considered the classes of partial functions with fixed part of units in case of Nechiporuk(1965) restrictions for the domain size.

Andreev(1989) has proved the best result, namely

$$\mathbf{L}\left(\mathrm{HOM}^m(\{0,1\}^n,\{0,1\})\right) \ \sim \ \frac{m}{\log m} \ + \ O(n) \ ,$$

(no restrictions for domain size).

In this paper we consider the problem for the general case of nondeterministic functions. We prove that

$$\mathbf{L}\left(\mathrm{HOM}^m(\mathcal{A},\mathcal{U})\right) \ \sim \ \frac{m}{\log m} \ + \ O(n) \ .$$

for the sufficiently general case, when

$$\log |\, \mathcal{U} \,| = \ o(\log m) \ .$$

This result has very strong applications in the area of algorithms derandomization. We discuss this connection in the next subsection.

1.3 Derandomization problem and nondeterministic functions complexity

One of the main problems of complexity theory is the derandomization problem, i.e. effective conversion of randomized algorithms to deterministic.

For this problem there are two main approaches. The first is effective computation of the number of units of boolean circuits. Luby and Velicovic (1991), Karpinsky and Luby (1993) have developed this approach.

The second way is effective construction of pseudorandom generators. Nisan(1990), Even, Goldreich and Luby (1992) have constructed some restricted pseudorandom generators.

Sipser (1986), Chor and Goldreich (1989), Linial, Luby, Saks and Zuckerman (1993) have investigated the problem of hitting sets, i.e. weak variant of pseudorandom generator.

A lot of randomized algorithms can be converted to deterministic ones, if we have an effective hitting set with certain parameters. This fact makes actual the problem of its construction.

The set $\mathcal{Q}$ is hitting set for the set system $\mathcal{R}$ if $\mathcal{Q} \cap \mathcal{Z} \neq \emptyset$ for any set $\mathcal{Z}$ from $\mathcal{R}$.

Up to now there is no nontrivial results for general cases of all derandomization approaches. The hitting set problem has strong connection with complexity bounds for nondeterministic functions and below we discuss only this derandomization approach.

The main goal of this problematic is to construct effective hitting set for the system of sets with restricted complexity of its characteristic functions. As we have said earlier, there are no nontrivial results about such hitting set. This fact explains actuality of considerations of simpler set systems.

By $\mathcal{E}_\kappa$ we denote the set $\{0, 1, \ldots, \kappa - 1\}$. For the sequence $\mathbf{A} = (\mathcal{A}_1, \mathcal{A}_2, ..., \mathcal{A}_n)$ from $(\mathcal{E}_\kappa^*)^n$ we define the corresponding rectangle

$$\mathcal{N}_{\mathbf{A}} \ = \ \mathcal{A}_1 \times \mathcal{A}_2 \times ... \times \mathcal{A}_n \ .$$

By $\mathbf{P}(\mathcal{N}_{\mathbf{A}})$ we denote the rectangle volume:

$$\mathbf{P}(\mathcal{N}_{\mathbf{A}}) \ = \ \prod_{i=1}^{n} \frac{\mid \mathcal{A}_i \mid}{\mid \mathcal{E}_\kappa \mid} \ = \ \prod_{i=1}^{n} \frac{\mid \mathcal{A}_i \mid}{\kappa} \ .$$

Let

$$\mathcal{I}_\kappa(n, \epsilon) \ = \ \{\mathcal{N}_{\mathbf{A}} \mid \ \mathbf{A} \in (\mathcal{E}_\kappa^*)^n \ , \ \mathbf{P}(\mathcal{N}_{\mathbf{A}}) \geq \epsilon\} \ .$$

Nechiporuk (1965) has obtained the first result about hitting sets for the system $\mathcal{I}_2(n, \epsilon)$, in connection with his research of partial boolean functions complexity. He had proposed deterministic algorithm with the working time $2^{O(n)}$. This algorithm constructs for the system $\mathcal{I}_2(n, \epsilon)$ hitting set with cardinality $O(n/\epsilon)$.

Sipser(1986) has proposed for this problem an algorithm which uses $O(n)$ random bits. Chor and Goldreich(1989) have created an algorithm which uses $2n$ random bits.

The best result for the considered problem is obtained by Linial, Luby, Saks and Zuckerman (1993). They have proposed deterministic algorithm of a hitting set construction for the system $\mathcal{I}_\kappa(n, \epsilon)$. The set cardinality and the algorithm working time are polynomial in $\kappa(\log n)/\epsilon$.

Let $\mid \mathcal{A} \mid = n$ and ϕ is bijection from $\mathrm{Hom}\,(\mathcal{A}\,, \{1, 2, ..., n\})$.We define the following mappings

$$\Phi \ : \ (\mathcal{E}_\kappa)^n \qquad \longrightarrow \qquad \mathrm{Hom}(\mathcal{A}, \mathcal{E}_\kappa) \ ,$$

$$\Phi^* \ : \ \mathcal{I}_\kappa(n) \qquad \longrightarrow \qquad \mathrm{HOM}(\mathcal{A}, \mathcal{E}_\kappa) \ ,$$

by the conditions

$$\mathbf{d} = (d_1, d_2, ..., d_n) \qquad \Rightarrow \qquad \Phi\,(\mathbf{d})\,(x) \ = \ d_{\phi(x)} \ , \qquad x \in \mathcal{A} \ ,$$

$$\mathbf{D} = (\mathcal{D}_1, \mathcal{D}_2, ..., \mathcal{D}_n) \qquad \Rightarrow \qquad \Phi^*\,(\mathcal{N}_\mathbf{D})\,(x) \ = \ \mathcal{D}_{\phi(x)} \ , \qquad x \in \mathcal{A} \ .$$

It is not difficult to check the following facts:

- Φ and Φ^* are bijections;
- $\mathbf{d} \in \mathcal{N}_\mathbf{D} \qquad \Longleftrightarrow \qquad \Phi(\mathbf{d}) \in \Phi^*(\mathcal{N}_\mathbf{D})$;
- $\mathcal{N}_\mathbf{D} \subseteq \mathcal{N}_\mathbf{C} \qquad \Longleftrightarrow \qquad \Phi^*(\mathcal{N}_\mathbf{D}) \subseteq \Phi^*(\mathcal{N}_\mathbf{C})$;
- $\mathbf{P}(\mathcal{N}_\mathbf{D}) \ = \ \mathbf{P}(\Phi^*(\mathcal{N}_\mathbf{D}))$.

In that way the mapping pair (Φ, Φ^*) is a natural isomorphism between the systems

$$((\mathcal{E}_\kappa)^n, \mathcal{I}_\kappa(n), \in, \subseteq, \mathbf{P}) \qquad \text{and} \qquad (\mathrm{Hom}(\mathcal{A}, \mathcal{E}_\kappa), \mathrm{HOM}(\mathcal{A}, \mathcal{E}_\kappa), \in, \subseteq, \mathbf{P}) \ .$$

It is easy to check, that

$$\mathrm{HOM}_\epsilon(\mathcal{A}, \mathcal{E}_\kappa) \ = \ \Phi^*\,(\mathcal{I}_\kappa(n, \epsilon)) \ .$$

In new terms the definition of the hitting set is the following:
a set $\mathcal{Q} \subseteq \mathrm{Hom}(\mathcal{A}, \mathcal{B})$ is hitting for the system $\mathcal{R} \subseteq \mathrm{HOM}(\mathcal{A}, \mathcal{B})$, if

$$\forall \mathbf{F} \in \mathcal{R} \ \exists \mathbf{f} \in \mathcal{Q} \ : \ \mathbf{f} \in \mathbf{F} \ .$$

By $\lambda(\mathcal{R})$ we denote the minimal possible element number in the hitting sets for the system $\mathcal{R}$.

By $\mathrm{Hom}_l^{\mathrm{compl}}(\mathcal{A}, \mathcal{U})$ we denote the set of all functions from $\mathrm{Hom}(\mathcal{A}, \mathcal{U})$ with the complexity at most l. If

$$l \ \geq \ \mathbf{L}(\mathrm{HOM}_\epsilon(\mathcal{A}, \mathcal{E}_\kappa)) \ ,$$

then the set $\mathrm{Hom}_l^{\mathrm{compl}}(\mathcal{A}, \mathcal{E}_\kappa)$ is the hitting set for the system $\mathrm{HOM}_\epsilon(\mathcal{A}, \mathcal{E}_\kappa)$.

For boolean case this fact was remarked independently in Krichevsky(1994) and Andreev(1994).

The size of the set $\mathrm{Hom}_l^{\mathrm{compl}}(\mathcal{A},\mathcal{U})$ is at most the number of circuits with complexity l. Consequently the upper bound for Shannon function $\mathbf{L}(\mathrm{HOM}_\epsilon(\mathcal{A},\mathcal{E}_\kappa))$ follows the bound of the hitting set size.

The construction of this hitting set includes consideration of all circuits with complexity l with conversion on each step of a circuit to the sequence of its values.

Our bounds of nondeterministic functions complexity offer a possibility to construct the small hitting set for the system $\mathcal{I}(n,\epsilon)$. Its size is almost linear of $(\log n)/\epsilon$ in the case

$$\log \kappa \;=\; o\left(\log\log \frac{1}{\epsilon}\right) \;.$$

We must remark, that trivial lower bound for the hitting set size is $1/\epsilon$.

In that way we obtain in significant case more strong result then Linial, Luby, Saks and Zuckerman (1993).

2 Complexity bounds for the worst case

2.1 Lower and preliminary upper bounds

Lemma 1 *If*

$$|\,\mathcal{A}\,| \geq 2 \;, \qquad |\,\mathcal{U}\,| \geq 2 \;,$$

then

$$\mathbf{L}\,(\mathrm{HOM}^m(\mathcal{A},\mathcal{U})) \;\leq\; 8\; m\,|\,\mathcal{U}\,|\log|\,\mathcal{U}\,| \;,$$

and for any function $\mathbf{F}$ *from* $\mathrm{HOM}(\mathcal{A},\mathcal{U})$ *it is true*

$$\mathbf{L}(\mathbf{F}) \;\leq\; O(1)\,|\,\mathcal{M}(\mathbf{F})\,|\,\log|\,\mathcal{U}\,| \;\;.$$

Proof. We suppose, that

$$\mathcal{A} \;\subseteq\; \{0,1\}^r \;, \qquad r = \lceil \log|\,\mathcal{A}\,| \rceil \;.$$

Let $\mathbf{F}$ be some function from $\mathrm{HOM}^m(\mathcal{A},\mathcal{U})$. We will prove by $|\,\mathcal{M}(\mathbf{F})\,|$-induction that

$$\mathcal{M}(\mathbf{F}) \neq \emptyset \qquad \Longrightarrow \qquad \mathbf{L}(\mathbf{F}) \;\leq\; (4\,|\,\mathcal{M}(\mathbf{F})\,| - 3)\;(\log|\,\mathcal{U}\,| + 1) \;.$$

If $\mid \mathcal{M}(\mathbf{F}) \mid = 1$, then evidently there exist constant function $\mathbf{c}$ from $\mathrm{Hom}(\mathcal{A},\mathcal{U})$ such that $\mathbf{c} \in \mathbf{F}$, consequently

$$\mathbf{L}(\mathbf{F}) \ \leq \ \mathbf{L}(\mathbf{c}) \ \leq \ \lceil \log \mid \mathcal{U} \mid \rceil \ \leq \ (\log \mid \mathcal{U} \mid +1) \ .$$

We suppose that $x_1, x_2, ..., x_r$ is the sequence of input variables. Let

$$\mathcal{A}_{i,\alpha} \ = \ \{0,1\}^{i-1} \times \{\alpha\} \times \{0,1\}^{r-i} \ .$$

Suppose that $\mid \mathcal{M}(\mathbf{F}) \mid \geq 2$, then there exist variable x_i such that

$$\mathcal{M}(\mathbf{F}) \cap \mathcal{A}_{i,0} \neq \emptyset \ , \qquad \mathcal{M}(\mathbf{F}) \cap \mathcal{A}_{i,1} \neq \emptyset \ .$$

We define functions $\mathbf{F}_0$ and $\mathbf{F}_1$ from $\mathrm{HOM}(\mathcal{A},\mathcal{U})$ by the following way

$$\mathbf{F}_\alpha(b) \ = \ \begin{cases} \mathbf{F}(b) & \textbf{if } b \in \mathcal{A}_{i,\alpha} \\ \mathcal{U} & \textbf{otherwise} \end{cases} \ , \qquad \alpha \in \{0,1\} \ .$$

It is easy to see, that

$$\mathcal{M}(\mathbf{F}) \ = \ \mathcal{M}(\mathbf{F}_0) \cup \mathcal{M}(\mathbf{F}) \ , \qquad \mathbf{H}(\mathbf{F}) \ = \ \mathbf{H}(\mathbf{F}_0) + \mathbf{H}(\mathbf{F}_1) \ .$$

Let $\mathbf{w}$ be the selector function from $\mathrm{Hom}(\{0,1\} \times \mathcal{U} \times \mathcal{U}, \mathcal{U})$, i.e.

$$\mathbf{w}(a,u_1,u_2) \ = \ \begin{cases} u_1 & \textbf{if } a = 1 \\ u_2 & \textbf{if } a = 0 \end{cases} \ .$$

It is easy to see, that

$$\mathbf{L}(\mathbf{w}) \ \leq \ 3\lceil \log \mid \mathcal{U} \mid \rceil \ \leq \ 3(\log \mid \mathcal{U} \mid +1) \ .$$

If $f_1 \in \mathbf{F}_1$ and $\mathbf{f}_0 \in \mathbf{F}_0$, then

$$\mathbf{w}(x_i, f_1, f_0) \ \in \ \mathbf{F} \ .$$

Consequently

$$\mathbf{L}(\mathbf{F}) \ \leq \ \mathbf{L}(\mathbf{F}_1) + \mathbf{L}(\mathbf{F}_0) + \mathbf{L}(\mathbf{w}) \ .$$

For $\mathbf{F}_1$ and $\mathbf{F}_0$ the induction hypothesis is true, and we have

$$\mathbf{L}(\mathbf{F}) \ \leq \ ((4 \mid \mathcal{M}(\mathbf{F}_1) \mid -3)(\log \mid \mathcal{U} \mid +1)) \ +$$

$$+ \ ((4 \mid \mathcal{M}(\mathbf{F}_0) \mid -3)(\log \mid \mathcal{U} \mid +1)) \ + \ 3(\log \mid \mathcal{U} \mid +1) \ =$$

$$= \ (4 \mid \mathcal{M}(\mathbf{F}) \mid -3)(\log \mid \mathcal{U} \mid +1) \ .$$

If $\emptyset \neq \mathcal{V} \subseteq \mathcal{U}$ and $\mathcal{V} \neq \mathcal{U}$ then

$$\log \frac{\mid \mathcal{U} \mid}{\mid \mathcal{V} \mid} \ \geq \ \log \frac{\mid \mathcal{U} \mid}{\mid \mathcal{U} \mid -1} \ \geq \ \frac{1}{\mid \mathcal{U} \mid} \ .$$

Consequently

$$\mathbf{H}(\mathbf{F}) \ \geq \ \sum_{a \in \mathcal{M}(\mathbf{F})} \log \frac{\mid \mathcal{U} \mid}{\mid \mathbf{F}(a) \mid} \ \geq \ \sum_{a \in \mathcal{M}(\mathbf{F})} \frac{1}{\mid \mathcal{U} \mid} \ = \mid \mathcal{M}(\mathbf{F}) \mid \frac{1}{\mid \mathcal{U} \mid} \ ,$$

and we have

$$\mid \mathcal{M}(\mathbf{F}) \mid \leq \mid \mathcal{U} \mid \mathbf{H}(\mathbf{F}) \ ,$$

$$\mathbf{L}(\mathbf{F}) \ \leq \ (4 \mid \mathcal{U} \mid \mathbf{H}(\mathbf{F}) - 3)(\log \mid \mathcal{U} \mid +1) \ \leq \ 8 \mid \mathcal{U} \mid \mathbf{H}(\mathbf{F})(\log \mid \mathcal{U} \mid \ .$$

□

2.2 Nonconstructive upper bound for hitting set size

By $\Theta(x)$ we denote any nonnegative function such that

$$x \to \infty \qquad \Longrightarrow \qquad \Theta(x) = o(1) \ .$$

By $\mathrm{HOM}_{\epsilon,\phi}(\mathcal{A},\mathcal{U})$ we denote the following set

$$\{\mathbf{F} \mid \ \mathbf{F} \in \mathrm{HOM}_{\epsilon}(\mathcal{A},\mathcal{U}) \ , \ \forall a \in \mathcal{A} \ : \mathbf{F}(a) \mid = \mid \mathcal{U} \mid -\phi(a)\} \ ,$$

and by $\mathrm{Hom}_{\Sigma,l}(\mathcal{A},\mathcal{E}_k)$ the following

$$\{\phi \mid \ \phi \in \mathrm{Hom}(\mathcal{A},\mathcal{E}_k) \ , \ \sum_{a \in \mathcal{A}} \phi(a) \leq l\} \ .$$

Lemma 2 *If*

$$\mid \mathcal{A} \mid \geq 2 \ , \qquad \mid \mathcal{U} \mid \geq 2 \ ,$$

then

$$\log \mid \mathrm{HOM}_{\epsilon}(\mathcal{A},\mathcal{U}) \mid \leq \ (\log \mid \mathcal{A} \mid + \log \mid \mathcal{U} \mid +3) \mid \mathcal{U} \mid \log \frac{1}{\epsilon} \ .$$

Proof. We let

$$\mid \mathcal{A} \mid = n \ , \qquad \mid \mathcal{U} \mid = k \ ,$$

$$\phi \in \mathrm{Hom}(\mathcal{A},\mathcal{E}_k) \ , \qquad \mathbf{F} \in \mathrm{HOM}_{\epsilon,\phi}(\mathcal{A},\mathcal{U}) \ .$$

We have

$$\epsilon \ \leq \ \mathbf{P}(\mathbf{F}) \ = \ \prod_{a\in\mathcal{A}} \frac{\mid \mathbf{F}(a) \mid}{k} \ = \ \prod_{a\in\mathcal{A}} \left(1 - \frac{\phi(a)}{k}\right) \ \leq$$

$$\leq \ \prod_{a\in\mathcal{A}} \exp\left(-\frac{\phi(a)}{k}\right) \ = \ \exp\left(-\frac{1}{k}\sum_{a\in\mathcal{A}} \phi(a)\right) \ .$$

Consequently

$$\frac{1}{\epsilon} \ \geq \ \exp\left(\frac{1}{k}\sum_{a\in\mathcal{A}} \phi(a)\right) \ ,$$

$$\sum_{a\in\mathcal{A}} \phi(a) \ \leq \ k \ln\frac{1}{\epsilon} \ .$$

In that way we have

$$\phi \in \mathrm{Hom}_{\Sigma,l}(\mathcal{A},\mathcal{E}_k) \ , \qquad \text{where} \ \ l = \left\lfloor k \ln\frac{1}{\epsilon} \right\rfloor \ ,$$

and then

$$\mathrm{HOM}_{\epsilon}(\mathcal{A},\mathcal{U}) \ \subseteq \bigcup_{\phi \in \mathrm{Hom}_{\Sigma,l}(\mathcal{A},\mathcal{E}_k)} \mathrm{HOM}_{\epsilon,\phi}(\mathcal{A},\mathcal{U}) \ . \qquad (1)$$

It is easy to check, that

$$\log \mid \mathrm{HOM}_{\epsilon,\phi}(\mathcal{A},\mathcal{U}) \mid \ = \ \log\left(\prod_{a\in\mathcal{A}} \left(\begin{array}{c} k \\ \phi(a) \end{array} \right)\right) \ \leq$$

$$\leq \ \log\left(\prod_{a\in\mathcal{A}} k^{\phi(a)}\right) \ = \ (\log k)\sum_{a\in\mathcal{A}} \phi(a) \ \leq$$

$$\leq \ (\log k) l \ = \ \log\left(k^l\right) \ .$$

By (1) for $l \geq 1$ we have

$$\mid \mathrm{HOM}_{\epsilon}(\mathcal{A},\mathcal{U}) \mid \leq \ k^l \mid \mathrm{Hom}_{\Sigma,l}(\mathcal{A},\mathcal{E}_k) \mid \leq$$

$$\leq \ k^l \left(\begin{array}{c} n+l \\ n \end{array} \right) \ = \ k^l \left(\begin{array}{c} n+l \\ l \end{array} \right) \ \leq$$

$$\leq \ k^l \left(\frac{4(n+l)}{l}\right)^l \ \leq \ k^l (8n)^l \ .$$

In the case $l = 0$ this bound is true also.

□

Lemma 3 *If*

$$| \mathcal{A} | \geq 2 \ , \qquad | \mathcal{U} | \geq 2 \ ,$$

then

$$\lambda \left(\mathrm{HOM}_\epsilon (\mathcal{A}, \mathcal{U}) \right) \ \leq \ \left(\frac{1}{\epsilon} \right)^{1+\Theta(1/\epsilon)} | \mathcal{U} |^{1+\Theta(|\mathcal{U}|)} \log | \mathcal{A} | \ .$$

Proof. For any function $\mathbf{F}$ from $\mathrm{HOM}_\epsilon (\mathcal{A}, \mathcal{U})$ we have

$$\frac{| \{ \mathbf{f} \mid \ \mathbf{f} \in \mathrm{Hom}(\mathcal{A}, \mathcal{U}) \ , \ \mathbf{f} \in \mathbf{F} \} |}{| \mathrm{Hom}(\mathcal{A}, \mathcal{U}) |} \ = \ \mathbf{P}(\mathbf{F}) \ \geq \ \epsilon \ .$$

Consequently, by the Nechiporuk (1965) way, we can construct by r steps the set $\mathcal{Q}_r$ such that

$$\mathcal{Q}_r \subseteq \mathrm{Hom}(\mathcal{A}, \mathcal{U}) \ , \qquad | \mathcal{Q}_r | = r \ ,$$

$$| \{ \mathbf{F} \mid \ \mathbf{F} \in \mathrm{HOM}_\epsilon (\mathcal{A}, \mathcal{U}) \ , \ \mathcal{N}_{\mathbf{F}} \cap \mathcal{Q}_r = \emptyset \} | \leq$$
$$(1 - \epsilon)^r \ | \mathrm{HOM}_\epsilon (\mathcal{A}, \mathcal{U}) | \leq \ e^{-\epsilon \, r} \ | \mathrm{HOM}_\epsilon (\mathcal{A}, \mathcal{U}) | \ ,$$

where

$$\mathcal{N}_{\mathbf{F}} \ = \ \{ \mathbf{f} \mid \ \mathbf{f} \in \mathrm{Hom}(\mathcal{A}, \mathcal{U}) \ , \ \mathbf{f} \in \mathbf{F} \} \ .$$

We let

$$r \ = \ \left\lceil \frac{1}{\epsilon} \ \ln | \mathrm{HOM}_\epsilon (\mathcal{A}, \mathcal{U}) | \right\rceil \ ,$$

and obtain

$$| \{ \mathbf{F} \mid \ \mathbf{F} \in \mathrm{HOM}_\epsilon (\mathcal{A}, \mathcal{U}) \ , \ \mathcal{N}_{\mathbf{F}} \cap \mathcal{Q}_r = \emptyset \} | < \ 1 \ .$$

Consequently for any function $\mathbf{F}$ from $\mathrm{HOM}_\epsilon (\mathcal{A}, \mathcal{U})$ we have

$$\mathcal{N}_{\mathbf{F}} \cap \mathcal{Q}_r \ \neq \ \emptyset \ .$$

By Lemma 2 we obtain

$$r \ \leq \ \frac{1}{\epsilon} \ \ln | \mathrm{HOM}_\epsilon (\mathcal{A}, \mathcal{U}) | + 1 \ \leq$$

$$\leq \ \frac{1}{\epsilon} \left(\ln | \mathcal{A} | + \ln | \mathcal{U} | + 3 \right) \ | \mathcal{U} | \ \ln \frac{1}{\epsilon} \ + \ 1 \ \leq$$

$$\leq \ \left(\frac{1}{\epsilon} \right)^{1+\Theta(1/\epsilon)} | \mathcal{U} |^{1+\Theta(|\mathcal{U}|)} \log | \mathcal{A} | \ .$$

□

2.3 Main decomposition methods

Let

$$\mathcal{C} = \{0,1\}^r \ , \qquad \mathcal{A} = \{0,1\}^p \ , \qquad \mathcal{B} = \{0,1\}^s \ ,$$
$$r = p + s \ , \qquad p \geq 1 \ , \qquad s \geq 1 \ . \tag{2}$$

Let ϕ be some bijection from $\mathrm{Hom}(\mathcal{A} \times \mathcal{B}, \mathcal{C})$ and ϕ^{-1} is inverse mapping from $\mathrm{Hom}(\mathcal{C}, \mathcal{A} \times \mathcal{B})$. Let

$$\psi_1 \in \mathrm{Hom}(\mathcal{C}, \mathcal{A}) \ , \qquad \psi_2 \in \mathrm{Hom}(\mathcal{C}, \mathcal{B}) \ ,$$

and for all c from $\mathcal{C}$

$$\phi^{-1}(c) \ = \ (\psi_1(c), \psi_2(c)) \ . \tag{3}$$

If

$$\mathbf{F} \in \mathrm{HOM}(\mathcal{C},\mathcal{U}) \ , \qquad \mathbf{D} \in \mathrm{HOM}(\mathcal{C}, \{0,1\}) \ ,$$
$$\mathbf{G} \in \mathrm{HOM}(\mathcal{A} \times \mathcal{B},\mathcal{U}) \ , \qquad \mathbf{Q} \in \mathrm{HOM}(\mathcal{A}, \{0,1\}) \ ,$$

then by $\mathbf{F} \mid_{\mathbf{Q}=\alpha}$ we denote function from $\mathrm{HOM}(\mathcal{A} \times \mathcal{B},\mathcal{U})$ such that

$$\mathbf{G} \mid_{\mathbf{Q}=\alpha}(a,b) \ = \ \begin{cases} \mathbf{G}(a,b) & \textbf{if } \mathbf{Q}(a) = \alpha \\ \mathcal{U} & \textbf{otherwise} \end{cases} \ .$$

and by $\mathbf{F} \mid_{\mathbf{D}=\alpha}$ we denote function from $\mathrm{HOM}(\mathcal{C},\mathcal{U})$ such that

$$\mathbf{F} \mid_{\mathbf{D}=\alpha}(c) \ = \ \begin{cases} \mathbf{F}(c) & \textbf{if } \mathbf{D}(c) = \alpha \\ \mathcal{U} & \textbf{otherwise} \end{cases} \ .$$

Let $\mathbf{w}$ be the selector function from $\mathrm{Hom}(\{0,1\} \times \mathcal{U} \times \mathcal{U},\mathcal{U})$ i.e.

$$\mathbf{w}(a,u_1,u_2) \ = \ \begin{cases} u_1 & \textbf{if } a = 1 \\ u_2 & \textbf{if } a = 0 \end{cases} \ .$$

Lemma 4 *If for functions*

$$\mathbf{F} \in \mathrm{HOM}(\mathcal{C},\mathcal{U}) \ , \qquad \mathbf{Q} \in \mathrm{HOM}(\mathcal{A}, \{0,1\}) \ ,$$

it is true, that

$$\mathbf{Q}(a) = \{0,1\} \qquad \Longrightarrow \qquad \forall b \in \mathcal{B} \ : \ (\phi \circ \mathbf{F})(a,b) = \mathcal{U} \ ,$$

then we have, that $\mathbf{L}(\mathbf{F})$ *is at most*

$$\mathbf{L}\left((\phi \circ \mathbf{F}) \mid_{\mathbf{Q}=1}\right) \ + \ \mathbf{L}\left(\mathbf{F} \mid_{(\psi_1 \circ \mathbf{Q})=0}\right) \ + \ \mathbf{L}(\mathbf{Q}) \ + \ \mathbf{L}(\phi^{-1}) \ + \ \mathbf{L}(\mathbf{w}) \ .$$

Proof. Let $\mathbf{g}_1$ be some function from $\mathrm{Hom}(\mathcal{A}\times\mathcal{B},\mathcal{U})$ and $\mathbf{f}_0$ some function from $\mathrm{Hom}(\mathcal{C},\mathcal{U})$, such that

$$\mathbf{g}_1 \in (\phi\circ\mathbf{F})\mid_{\mathbf{Q}=1}\ , \qquad \mathbf{f}_0 \in \mathbf{F}\mid_{(\psi_1\circ\mathbf{Q})=0}\ , \tag{4}$$

and $\mathbf{q}$ function from $\mathrm{Hom}(\mathcal{A},\{0,1\})$ such that $\mathbf{q}\in\mathbf{Q}$. We will check, that for any c from $\mathcal{C}$ the following condition is true

$$\mathbf{w}\left(\mathbf{q}(\psi_1(c)),\ \mathbf{g}_1(\phi^{-1}(c)),\ \mathbf{f}_0(c)\right)\ \in\ \mathbf{F}(c)\ . \tag{5}$$

Let

$$a=\psi_1(c)\ , \qquad b=\psi_2(c)\ ,$$

If $\mathbf{Q}(a)=0$ then we have

$$(\psi_1\circ\mathbf{Q})(c)\ =\ \mathbf{Q}(\psi_1(c))\ =\ \mathbf{Q}(a)\ =\ 0\ ,$$

consequently

$$\mathbf{F}\mid_{(\psi_1\circ\mathbf{Q})=0}(c)\ =\ \mathbf{F}(c) \qquad \text{and} \qquad \mathbf{f}_0(c)\in\mathbf{F}(c)\ .$$

In this case we have

$$\mathbf{w}\left(\mathbf{q}(\psi_1(c)),\ \mathbf{g}_1(\phi^{-1}(c)),\ \mathbf{f}_0(c)\right)\ =$$

$$=\ \mathbf{w}\left(0,\ \mathbf{g}_1(\phi^{-1}(c)),\ \mathbf{f}_0(c)\right)\ =\ \mathbf{f}_0(c)\in\mathbf{F}(c)\ .$$

Consequently (5) is true.

Our condition is equivalent to the following

$$\mathbf{w}\left(\mathbf{q}(a),\ \mathbf{g}_1(a,b),\ \mathbf{f}_0(c)\right)\ \in\ (\phi\circ\mathbf{F})(a,b)\ , \tag{6}$$

because

$$\mathbf{F}(c)\ =\ \left(\phi^{-1}\circ\phi\circ\mathbf{F}\right)(c)\ =\ (\phi\circ\mathbf{F})\left(\phi^{-1}(c)\right)\ =\ (\phi\circ\mathbf{F})(a,b)\ .$$

If $\mathbf{Q}(a)=\{0,1\}$, then $(\phi\circ\mathbf{F})(a,b)=\mathcal{U}$ and (6) is true in any case. If $\mathbf{Q}(a)=1$, then

$$(\phi\circ\mathbf{F})\mid_{\mathbf{Q}=1}(a,b)\ =\ (\phi\circ\mathbf{F})(a,b)$$

and consequently, by (4), we have

$$\mathbf{g}_1(a,b)\ \in\ (\phi\circ\mathbf{F})(a,b)\ .$$

In this case we have also, that

$$\mathbf{w}\,(\mathbf{q}(a),\ \mathbf{g}_1(a,b),\ \mathbf{f}_0(c))\ =\ \mathbf{w}\,(1,\ \mathbf{g}_1(a,b),\ \mathbf{f}_0(c))\ =\ \mathbf{g}_1(a,b)\ ,$$

consequently (6) is true.

In that way we can compute the function $\mathbf{F}$ by the circuits from the figure 1. This fact implies necessary bounds for the complexity of the function $\mathbf{F}$.

□

For $\mathbf{G}$ from $\mathrm{HOM}(\mathcal{A}\times\mathcal{B},\mathcal{U})$ we let

$$\mathbf{G}_a \in \mathrm{HOM}(\mathcal{A},\mathcal{U})\ ,\qquad \forall b\in\mathcal{B}\ :\ \mathbf{G}_a(b)=\mathbf{G}(a,b)\ .$$

We define also two other functions:

$$\mathbf{Q}_{\mathbf{F},\phi,\mathcal{A}}\ \in\ \mathrm{HOM}(\mathcal{A},\{0,1\})\ ,\qquad \mathbf{C}_{\mathbf{F},\phi,\mathcal{A}}\ \in\ \mathrm{HOM}(\mathcal{A},\mathcal{U})\ ,$$

by the following way

$$\mathbf{Q}_{\mathbf{F},\phi,\mathcal{A}}(a)\ =\ \begin{cases} \{0,1\} & \textbf{if}\ \ \mathcal{M}((\phi\circ\mathbf{F})_a)=\emptyset \\ 1 & \textbf{if}\ \ \mid\mathcal{M}((\phi\circ\mathbf{F})_a)\mid=1 \\ 0 & \textbf{if}\ \ \mid\mathcal{M}((\phi\circ\mathbf{F})_a)\mid\geq 2 \end{cases}\ ,$$

$$\mathbf{C}_{\mathbf{F},\phi,\mathcal{A}}(a)\ =\ \bigcap_{b\in\mathcal{B}}(\phi\circ\mathbf{F})\mid_{\mathbf{Q}=1}(a,b)\ ,\qquad \text{where}\qquad \mathbf{Q}=\mathbf{Q}_{\mathbf{F},\phi,\mathcal{A}}\ .$$

We must check, that definition of the function $\mathbf{C}_{\mathbf{F},\phi,\mathcal{A}}$ is correct, i.e. for any a from $\mathcal{A}$ we have

$$\bigcap_{b\in\mathcal{B}}(\phi\circ\mathbf{F})\mid_{\mathbf{Q}=1}(a,b)\ \neq\ \emptyset\ .$$

If $\mathbf{Q}(a)\neq 1$, then we have

$$\forall b\in\mathcal{B}\ :\ (\phi\circ\mathbf{F})\mid_{\mathbf{Q}=1}(a,b)\ =\ \mathcal{U}\ ,$$

and consequently

$$\bigcap_{b\in\mathcal{B}}(\phi\circ\mathbf{F})\mid_{\mathbf{Q}=1}(a,b)\ =\ \mathcal{U}\ .$$

If $\mathbf{Q}(a)=1$, then

$$\mid\mathcal{M}((\phi\circ\mathbf{F})_a)\mid=\ 1\qquad\text{and}\qquad \forall b\in\mathcal{B}\ :\ (\phi\circ\mathbf{F})\mid_{\mathbf{Q}=1}(a,b)=(\phi\circ\mathbf{F})(a,b)\ .$$

Consequently in this case there exist element b_a from $\mathcal{B}$ such that

$$(\phi \circ \mathbf{F})(a, b_a) \neq \mathcal{U} \ , \qquad \forall b \in \mathcal{B} \ , \ b \neq b_a \ : \ (\phi \circ \mathbf{F})(a, b) = \mathcal{U} \ ,$$

and we have

$$\bigcap_{b \in \mathcal{B}} (\phi \circ \mathbf{F}) \mid_{\mathbf{Q}=1}(a, b) \ = \ \mathbf{G}(a, b_a) \ .$$

Lemma 5 *It is true, that* $\mathbf{L}(\mathbf{F})$ *at most*

$$\mathbf{L}\left(\mathbf{C}_{\mathbf{F},\phi,\mathcal{A}}\right) \ + \ \mathbf{L}\left(\mathbf{F} \mid_{\psi_1 \circ \mathbf{Q}_{\mathbf{F},\phi,\mathcal{A}}=0}\right) \ + \ \mathbf{L}\left(\mathbf{Q}_{\mathbf{F},\phi,\mathcal{A}}\right) \ + \ \mathbf{L}(\psi_1) \ + \ \mathbf{L}(\mathbf{w}) \ .$$

Proof. Let $\mathbf{c}$ be a function from $\mathrm{Hom}(\mathcal{A},\mathcal{U})$, such that $\mathbf{c} \in \mathbf{C}_{\mathbf{F},\phi,\mathcal{A}}$, then for any a from $\mathcal{A}$ and for any b from $\mathcal{B}$ we have

$$\mathbf{c}(a) \ \in \ (\phi \circ \mathbf{F}) \mid_{\mathbf{Q}=1}(a, b) \ , \tag{7}$$

(we suppose, that $\mathbf{Q} = \mathbf{Q}_{\mathbf{F},\phi,\mathcal{A}}$) because

$$\mathbf{c}(a) \ \in \ \mathbf{C}_{\mathbf{F},\phi,\mathcal{A}}(a) \ = \ \bigcap_{q \in \mathcal{B}} (\phi \circ \mathbf{F}) \mid_{\mathbf{Q}=1}(a, q) \ \subseteq \ (\phi \circ \mathbf{F}) \mid_{\mathbf{Q}=1}(a, b) \ .$$

Let

$$\mathbf{f}_0 \in \mathbf{F} \mid_{\psi_1 \circ \mathbf{Q}=0} \qquad \mathbf{g}_1 \in (\phi \circ \mathbf{F}) \mid_{\mathbf{Q}=1} \ , \qquad \mathbf{q} \in \mathbf{Q} \ ,$$

then function $\mathbf{F}$ may be to compute by the circuit on Figure 1. In the correspondence with (7) we can suppose that

$$\forall a \in \mathcal{A} \ \forall b \in \mathcal{B} \ : \ \ \mathbf{g}_1(a, b) = \mathbf{c}(a) \ .$$

In this case our circuit transforms into the circuit on the Figure 2 and we have necessary bound for the complexity of $\mathbf{F}$.

□

2.4 Complexity of the functions with uniform entropy

By $\mathrm{HOM}_{\mathcal{A},\epsilon}(\mathcal{A} \times \mathcal{B},\mathcal{U})$ we denote the set of all functions $\mathbf{F}$ from $\mathrm{HOM}(\mathcal{A} \times \mathcal{B},\mathcal{U})$ such that

$$\forall a \in \mathcal{A} \ : \ \ \mathbf{F}_a \ \in \ \mathrm{HOM}_{\epsilon}(\mathcal{B},\mathcal{U}) \ .$$

In this subsection we suppose, that

$$\mathcal{A} = \{0,1\}^t \ , \ t \geq 1 \ , \qquad \mathcal{B} = \{0,1\}^s \ , \ s \geq 1 \ , \qquad \mid \mathcal{U} \mid \geq 2 \ , \ k = \lceil \log \mid \mathcal{U} \mid \rceil \ .$$

Lemma 6 *If* $1/2 \leq \epsilon$, *then* $\mathbf{L}\left(\mathrm{HOM}_{\mathcal{A},\epsilon}(\mathcal{A}\times\mathcal{B},\mathcal{U})\right)$ *at most*

$$\frac{|\,\mathcal{A}\,|}{\log|\,\mathcal{A}\,|}\left(1+\Theta\left(\frac{1}{\epsilon}\right)+\Theta(|\,\mathcal{A}\,|)\right)\left(\left(\log\frac{1}{\epsilon}\right)+2\log|\,\mathcal{U}\,|+2\log\log|\,\mathcal{B}\,|\right)\;+$$

$$+\;\;|\,\mathcal{B}\,|\;\;|\,\mathcal{U}\,|^{1+\Theta(|\mathcal{U}|)}\;\left(\frac{1}{\epsilon}\right)^{1+\Theta(1/\epsilon)}\;.$$

Proof. Let $\mathcal{Q}$ be some hitting set for the system $\mathrm{HOM}_{\epsilon}(\mathcal{B},\mathcal{U})$, and $\mathbf{F}$ some function from $\mathrm{HOM}_{\mathcal{A},\epsilon}(\mathcal{A}\times\mathcal{B},\mathcal{U})$. In this case

$$\forall a\in\mathcal{A}\;\exists\mathbf{q}\in\mathcal{Q}\;:\;\;\mathbf{q}\in\mathbf{F}_a\;,$$

because for any a from $\mathcal{A}$ we have

$$\mathbf{F}_a\;\in\;\mathrm{HOM}_{\epsilon}(\mathcal{B},\mathcal{U})\;.$$

Consequently there exists the function Ψ from $\mathrm{Hom}(\mathcal{A},\mathcal{Q})$ such that

$$\forall a\in\mathcal{A}\;:\;\;\Psi(a)\in\mathbf{F}_a\;.$$

Let

$$p=\lceil\log|\,\mathcal{Q}\,|\rceil\;,\qquad\mathcal{P}\;=\;\{0,1\}^p\;.$$

In this case there exist functions Ψ_1 and Ψ_2 such that

$$\Psi_1\in\mathrm{Hom}(\mathcal{A},\mathcal{P})\;,\qquad\Psi_2\in\mathrm{Hom}(\mathcal{P},\mathcal{Q})\;,\qquad\Psi=\Psi_1\circ\Psi_2\;.$$

We define a function Φ from $\mathrm{Hom}(\mathcal{P}\times\mathcal{B},\mathcal{U})$ by the following

$$\forall\alpha\in\mathcal{P}\;\forall b\in\mathcal{B}\;:\qquad\Phi(\alpha,b)\;=\;(\Psi_2(\alpha))\,(b)\;.$$

($\Psi_2(\alpha)$ is function from $\mathrm{Hom}(\mathcal{B},\mathcal{U})$.) In this case we have

$$\Phi(\Psi_1(a),b)\;=\;(\Psi_2(\Psi_1(a)))\,(b)\;=\;((\Psi_1\circ\Psi_2)(a))\,(b)\;=$$

$$=\;(\Psi(a))(b)\;\in\;\mathbf{F}_a(b)\;=\;\mathbf{F}(a,b)\;.$$

Consequently

$$\forall a\in\mathcal{A}\;,\;\forall b\in\mathcal{B}\;:\qquad\Phi(\Psi_1(a),b)\;\in\;\mathbf{F}(a,b)\;,$$

and we can compute the function $\mathbf{F}$ by the circuit on Figure 3. It is easy, that

$$\mathbf{L}(\mathbf{F})\;\leq\;\mathbf{L}(\Psi_1)+\mathbf{L}(\Phi)\;.$$

Because

$$\Psi_1 \ \in \ \mathrm{Hom}(\mathcal{A},\mathcal{P}) \ = \ \mathrm{Hom}\left(\{0,1\}^t,\{0,1\}^p\right) \ ,$$

$$\Phi \ \in \ \mathrm{Hom}(\mathcal{P}\times\mathcal{B},\mathcal{U}) \ \subseteq \ \mathrm{Hom}\left(\{0,1\}^{p+s},\{0,1\}^k\right) \ ,$$

then by Lupanov (1965) bounds we have

$$\mathbf{L}(\Psi_1) \ \leq \ \frac{2^t}{t}(1+\Theta(t))p \ \leq \ \frac{2^t}{t}(1+\Theta(t))$$

$$\left(\left(\log\frac{1}{\epsilon}\right)\left(1+\Theta\left(\frac{1}{\epsilon}\right)\right) \ + \ (\log\mid\mathcal{U}\mid)(1+\theta(\mid\mathcal{U}\mid) \ + \ \log\log\mid\mathcal{B}\mid\right) \ \leq$$

$$\frac{\mid\mathcal{A}\mid}{\log\mid\mathcal{A}\mid}\left(1+\Theta\left(\frac{1}{\epsilon}\right)+\Theta(\mid\mathcal{A}\mid)\right)\left(\log\frac{1}{\epsilon}+2\log\mid\mathcal{U}\mid+2\log\log\mid\mathcal{B}\mid\right) \ , \tag{8}$$

because, by Lemma 3,

$$p \ = \ \log\mid\mathcal{P}\mid\leq \ \left(1+\Theta\left(\frac{1}{\epsilon}\right)\right)\log\frac{1}{\epsilon}+(1+\Theta(\mid\mathcal{U}\mid))\mid\mathcal{U}\mid \ + \ \log\log\mid\mathcal{B}\mid \ .$$

By analogical way we have

$$\mathbf{L}(\Phi) \ \leq \ \frac{2^{p+s}}{p+s}(1+\Theta(p+s))k \ \leq \ O(1)\mid\mathcal{B}\mid\frac{\log\mid\mathcal{U}\mid}{\log\mid\mathcal{B}\mid+\log\mid\mathcal{Q}\mid}\mid\mathcal{Q}\mid\leq$$

$$\leq \ O(1)\mid\mathcal{B}\mid\frac{\log\mid\mathcal{U}\mid}{\log\mid\mathcal{B}\mid+\log\mid\mathcal{Q}\mid}\left(\frac{1}{\epsilon}\right)^{1+\Theta(1/\epsilon)}\mid\mathcal{U}\mid^{1+\Theta(|\mathcal{U}|)}\log\mid\mathcal{B}\mid\leq$$

$$\leq\mid\mathcal{B}\mid\left(\frac{1}{\epsilon}\right)^{1+\Theta(1/\epsilon)}\mid\mathcal{U}\mid^{1+\Theta(|\mathcal{U}|)} \ . \tag{9}$$

The sum of (8) and (9) is the necessary bound.

□

2.5 Uniform mapping classes

Let

$$\mid\mathcal{A}\mid=\mid\mathcal{B}\mid \ , \qquad \mathcal{H}\subseteq\mathrm{Hom}(\mathcal{A},\mathcal{B}) \ .$$

The set $\mathcal{H}$ of mappings is uniform class, if any mapping from $\mathcal{H}$ is a bijection and for any different a_1, a_2 from $\mathcal{A}$ and for any different b_1, b_2 from $\mathcal{B}$ we have

$$\mid\{\mathbf{J}\mid \ \mathbf{J}\in\mathcal{H} \ , \ \mathbf{J}(a_1)=b_1 \ , \ \mathbf{J}(a_2)=b_2\}\mid= \ \frac{\mid\mathcal{H}\mid}{\mid\mathcal{A}\mid(\mid\mathcal{A}\mid-1)} \ .$$

Such classes of mappings has been considered in Markovsky, Carter and Wegman (1978) and in Carter and Wegman (1979). In this subsection we obtain some new results about such function classes.

By $\mathcal{R}_+$ we denote the set of all nonnegative real numbers. If $\mathbf{J}$ is some function from $\mathrm{Hom}(\mathcal{A}, \mathcal{R}_+)$ and $\mathcal{S} \subseteq \mathcal{A}$ then we let

$$\Sigma_{\mathcal{S}} \mathbf{J} \ = \ \sum_{a \in \mathcal{S}} \mathbf{J}(a) \ ,$$

$$\Sigma^{(2)}_{\mathcal{S}} \mathbf{J} \ = \ \sum_{\substack{a, b \in \mathcal{S} \\ a \neq b}} \mathbf{J}(a) \ \mathbf{J}(b) \ .$$

Lemma 7 *If $\mathcal{H}$ is an uniform class, and*

$$\mathcal{H} \subseteq \mathrm{Hom}(\mathcal{A} \times \mathcal{B}, \mathcal{C}) \ , \qquad | \ \mathcal{A} \ | \geq 2 \ , \ | \ \mathcal{B} \ | \geq 2 \ , \tag{10}$$

then for any function $\mathbf{J}$ from $\mathrm{Hom}(\mathcal{C}, \mathcal{R}_+)$ there exists mapping ψ from $\mathcal{H}$ such that

$$\sum_{a \in \mathcal{A}} \Sigma^{(2)}_{\{a\} \times \mathcal{B}} \ \psi \circ \mathbf{J} \ \leq \ \frac{1}{| \ \mathcal{A} \ |} \ \Sigma^{(2)}_{\mathcal{C}} \ \mathbf{J} \ .$$

Proof. If

$$a \in \mathcal{A} \ , \qquad \mathbf{b}_1, b_2 \in \mathcal{B} \ , \ b_1 \neq \mathbf{b}_2 \ ,$$

then, because $\mathcal{H}$ is uniform class, we have

$$\sum_{\phi \in \mathcal{H}} (\phi \circ \mathbf{J})(a, b_1) \cdot (\phi \circ \mathbf{J})(a, b_2) \ = \ \sum_{\phi \in \mathcal{H}} \mathbf{J}(\phi(a, b_1)) \cdot \mathbf{J}(\phi(a, b_2)) \ =$$

$$\sum_{\substack{c_1, c_2 \in \mathcal{C} \\ c_1 \neq \mathbf{c}_2}} | \ \{ \phi \mid \ \phi \in \mathcal{H} \ , \ \phi(a, b_1) = c_1 \ , \ \phi(a, b_2) = c_2 \} \ | \ \mathbf{J}(c_1) \ \mathbf{J}(c_2) \ =$$

$$= \sum_{\substack{c_1, c_2 \in \mathcal{C} \\ c_1 \neq \mathbf{c}_2}} \frac{| \ \mathcal{H} \ |}{| \ \mathcal{C} \ | \ (| \ \mathcal{C} \ |)} \ \mathbf{J}(c_1) \ \mathbf{J}(c_2) \ = \frac{| \ \mathcal{H} \ |}{| \ \mathcal{C} \ | \ (| \ \mathcal{C} \ | - 1)} \ \Sigma^{(2)}_{\mathcal{C}} \ \mathbf{J} \ .$$

Consequently

$$\sum_{\phi \in \mathcal{H}} \sum_{a \in \mathcal{A}} \Sigma^{(2)}_{\{a\} \times \mathcal{B}} \ \phi \circ \mathbf{J} \ =$$

$$= \sum_{a \in \mathcal{A}} \sum_{\substack{b_1, b_2 \in \mathcal{B} \\ b_1 \neq \mathbf{b}_2}} \sum_{\phi \in \mathcal{H}} (\phi \circ \mathbf{J})(a, b_1) \cdot (\phi \circ \mathbf{J})(a, b_2) \ =$$

$$= \sum_{a\in\mathcal{A}} \sum_{\substack{b_1,b_2\in\mathcal{B}\\ b_1\neq \mathbf{b}_2}} \frac{\mid \mathcal{H} \mid}{\mid \mathcal{C} \mid (\mid \mathcal{C} \mid -1)} \Sigma^{(2)}_{\mathcal{C}} \mathbf{J} =$$

$$= \mid \mathcal{A} \mid (\mid \mathcal{B} \mid (\mid \mathcal{B} \mid -1)) \frac{\mid \mathcal{H} \mid}{\mid \mathcal{A} \mid\mid \mathcal{B} \mid (\mid \mathcal{A} \mid\mid \mathcal{B} \mid -1)} \Sigma^{(2)}_{\mathcal{C}} \mathbf{J} =$$

$$= \frac{\mid \mathcal{H} \mid (\mid \mathcal{B} \mid -1)}{\mid \mathcal{A} \mid\mid \mathcal{B} \mid -1} \Sigma^{(2)}_{\mathcal{C}} \mathbf{J} \leq \frac{\mid \mathcal{H} \mid}{\mid \mathcal{A} \mid} \Sigma^{(2)}_{\mathcal{C}} \mathbf{J} .$$

In that way we have

$$\frac{1}{\mid \mathcal{H} \mid} \sum_{\phi\in\mathcal{H}} \left(\sum_{a\in\mathcal{A}} \Sigma^{(2)}_{\{a\}\times\mathcal{B}} \phi \circ \mathbf{J} \right) \leq \frac{1}{\mid \mathcal{A} \mid} \Sigma^{(2)}_{\mathcal{C}} \mathbf{J} .$$

Our Lemma follow from this bound.

□

Lemma 8 *If $\mathcal{H}$ is uniform class and (10), then for any function $\mathbf{J}$ from* $\mathrm{Hom}(\mathcal{A}, \mathcal{R}_+)$ *there exists mapping ψ from $\mathcal{H}$ such, that*

$$\sum_{a\in\mathcal{A}} \left(\Sigma_{\{a\}\times\mathcal{B}} \psi \circ \mathbf{J} - \frac{1}{\mid \mathcal{A} \mid} \Sigma_{\mathcal{C}} \mathbf{J} \right)^2 \leq \Sigma_{\mathcal{C}} \mathbf{J}^2 ,$$

$$\sum_{a\in\mathcal{A}(t)} \Sigma_{\{a\}\times\mathcal{B}} \psi \circ \mathbf{J} \leq \left(\frac{1}{t^2} \frac{1}{\mid \mathcal{A} \mid} \Sigma_{\mathcal{C}} \mathbf{J} + \frac{1}{t} \right) \Sigma_{\mathcal{C}} \mathbf{J}^2 ,$$

where

$$\mathcal{A}(t) = \{a \mid a\in\mathcal{A} , \Sigma_{\{a\}\times\mathcal{B}} \psi \circ \mathbf{J} \geq \frac{1}{\mid \mathcal{A} \mid} \Sigma_{\mathcal{C}} \mathbf{J} + t\} .$$

Proof. We will consider the mapping ψ, wich exists by previous Lemma. In this case we have

$$\sum_{a\in\mathcal{A}} \left(\Sigma_{\{a\}\times\mathcal{B}} \psi \circ \mathbf{J} - \frac{1}{\mid \mathcal{A} \mid} \Sigma_{\mathcal{C}} \mathbf{J} \right)^2 =$$

$$\sum_{a\in\mathcal{A}} \left(\Sigma_{\{a\}\times\mathcal{B}} (\psi \circ \mathbf{J})^2 + \Sigma^{(2)}_{\{a\}\times\mathcal{B}} \psi \circ \mathbf{J} + \frac{1}{\mid \mathcal{A} \mid^2} (\Sigma_{\mathcal{C}} \mathbf{J})^2 - \right.$$

$$\left. - 2 \left(\Sigma_{\{a\}\times\mathcal{B}} \psi \circ \mathbf{J} \right) \frac{1}{\mid \mathcal{A} \mid} \Sigma_{\mathcal{C}} \mathbf{J} \right) =$$

$$= \Sigma_{\mathcal{A}\times\mathcal{B}}\ (\psi\circ\mathbf{J})^2\ +\ \sum_{a\in\mathcal{A}}\ \Sigma^{(2)}_{\{a\}\times\mathcal{B}}\ \psi\circ\mathbf{J}\ +\frac{1}{\mid\mathcal{A}\mid}(\Sigma_{\mathcal{C}}\ \mathbf{J}\ )^2\ -$$

$$-\ 2\,(\Sigma_{\mathcal{A}\times\mathcal{B}}\ \psi\circ\mathbf{J})\,\frac{1}{\mid\mathcal{A}\mid}\ \Sigma_{\mathcal{C}}\ \mathbf{J}\ \ =$$

$$=\ \Sigma_{\mathcal{C}}\ \mathbf{J}^2\ +\sum_{a\in\mathcal{A}}\ \Sigma^{(2)}_{\{a\}\times\mathcal{B}}\ \psi\circ\mathbf{J}\ -\ \frac{1}{\mid\mathcal{A}\mid}\ (\Sigma_{\mathcal{C}}\ \mathbf{J})^2\ \le$$

$$\le\ \Sigma_{\mathcal{C}}\ \mathbf{J}^2\ +\ \frac{1}{\mid\mathcal{A}\mid}\ \Sigma^{(2)}_{\mathcal{C}}\ \mathbf{J}\ -\ \frac{1}{\mid\mathcal{A}\mid}\ (\Sigma_{\mathcal{C}}\ \mathbf{J})^2\ =$$

$$=\ \left(1-\frac{1}{\mid\mathcal{A}\mid}\right)\Sigma_{\mathcal{C}}\ \mathbf{J}^2\ \le\ \Sigma_{\mathcal{C}}\ \mathbf{J}^2\ .$$

In the following we have also the sequence of transformations.

$$\sum_{a\in\mathcal{A}(t)}\Sigma_{\{a\}\times\mathcal{B}}\ \psi\circ\mathbf{J}\ =$$

$$=\ \sum_{a\in\mathcal{A}(t)}\frac{1}{\mid\mathcal{A}\mid}\Sigma_{\mathcal{C}}\ \mathbf{J}\ +\ \sum_{a\in\mathcal{A}(t)}\left(\Sigma_{\{a\}\times\mathcal{B}}\ \psi\circ\mathbf{J}\ -\ \frac{1}{\mid\mathcal{A}\mid}\Sigma_{\mathcal{C}}\ \mathbf{J}\ \right)\ \le$$

$$\le\ \sum_{a\in\mathcal{A}(t)}\frac{\left(\Sigma_{\{a\}\times\mathcal{B}}\ \psi\circ\mathbf{J}\ -\ \frac{1}{|\mathcal{A}|}\Sigma_{\mathcal{C}}\ \mathbf{J}\ \right)^2}{t^2}\ \frac{1}{\mid\mathcal{A}\mid}\ \Sigma_{\mathcal{C}}\ \mathbf{J}\ +$$

$$+\ \sum_{a\in\mathcal{A}(t)}\frac{\left(\Sigma_{\{a\}\times\mathcal{B}}\ \psi\circ\mathbf{J}\ -\ \frac{1}{|\mathcal{A}|}\Sigma_{\mathcal{C}}\ \mathbf{J}\ \right)^2}{t}\ =$$

$$=\ \left(\frac{1}{t^2}\ \frac{1}{\mid\mathcal{A}\mid}\Sigma_{\mathcal{C}}\ \mathbf{J}\ +\frac{1}{t}\right)\sum_{a\in\mathcal{A}(t)}\left(\Sigma_{\{a\}\times\mathcal{B}}\ \psi\circ\mathbf{J}\ -\ \frac{1}{\mid\mathcal{A}\mid}\Sigma_{\mathcal{C}}\ \mathbf{J}\ \right)^2\ \le$$

$$=\ \left(\frac{1}{t^2}\ \frac{1}{\mid\mathcal{A}\mid}\Sigma_{\mathcal{C}}\ \mathbf{J}\ +\frac{1}{t}\right)\sum_{a\in\mathcal{A}}\left(\Sigma_{\{a\}\times\mathcal{B}}\ \psi\circ\mathbf{J}\ -\ \frac{1}{\mid\mathcal{A}\mid}\Sigma_{\mathcal{C}}\ \mathbf{J}\ \right)^2\ \le$$

$$=\ \left(\frac{1}{t^2}\ \frac{1}{\mid\mathcal{A}\mid}\Sigma_{\mathcal{C}}\ \mathbf{J}\ +\frac{1}{t}\right)\ \Sigma_{\mathcal{C}}\ \mathbf{J}^2\ .$$

□

Lemma 9 *If $\mathcal{H}$ is uniform class and (10), then for any function $\mathbf{J}$ from* $\mathrm{Hom}(\mathcal{A},\{0,1\})$ *there exists mapping ψ from $\mathcal{H}$ such, that*

$$\sum_{a\in\mathcal{D}}\Sigma_{\{a\}\times\mathcal{B}}\ \psi\circ\mathbf{J}\ \le\ \frac{1}{\mid\mathcal{A}\mid}\ (\Sigma_{\mathcal{C}}\ \mathbf{J})^2\ ,$$

where

$$\mathcal{D}\ =\ \left\{a\mid\ a\in\mathcal{A}\ ,\ \Sigma_{\{a\}\times\mathcal{B}}\ \psi\circ\mathbf{J}\ >\ 1\right\}\ .$$

Proof. We have

$$\Sigma^{(2)}_{\{a\}\times\mathcal{B}}\ \psi\circ\mathbf{J}\ =\ \left(\begin{array}{c}\Sigma_{\{a\}\times\mathcal{B}}\ \psi\circ\mathbf{J}\\ 2\end{array}\right)\ ,$$

$$\Sigma^{(2)}_{\mathcal{C}}\ \mathbf{J}\ =\ \left(\begin{array}{c}\Sigma_{\mathcal{C}}\ \mathbf{J}\\ 2\end{array}\right)\ \leq\ \frac{1}{2}\ (\Sigma_{\mathcal{C}}\ \mathbf{J})^2,$$

because the function $\mathbf{J}$ from $\mathrm{Hom}(\mathcal{A},\{0,1\})$. If $a\in\mathcal{D}$ we have

$$\Sigma_{\{a\}\times\mathcal{B}}\ \psi\circ\mathbf{J}\ \leq\ 2\ \Sigma^{(2)}_{\{a\}\times\mathcal{B}}\ \psi\circ\mathbf{J}\ .$$

Below we suppose, that ψ is a function from Lemma 7. Then we have

$$\sum_{a\in\mathcal{D}}\Sigma_{\{a\}\times\mathcal{B}}\ \psi\circ\mathbf{J}\ \leq\ \sum_{a\in\mathcal{D}}2\ \Sigma^{(2)}_{\{a\}\times\mathcal{B}}\ \psi\circ\mathbf{J}\ \leq$$

$$\leq\ \sum_{a\in\mathcal{A}}2\ \Sigma^{(2)}_{\{a\}\times\mathcal{B}}\ \psi\circ\mathbf{J}\ \leq\ 2\ \frac{1}{\mid\mathcal{A}\mid}\ \Sigma^{(2)}_{\mathcal{C}}\ \mathbf{J}\ \leq\ \frac{1}{\mid\mathcal{A}\mid}\ (\Sigma_{\mathcal{C}}\ \mathbf{J})^2,$$

□

Let $\mathcal{A}$ and $\mathcal{B}$ are copies of the Galua Field $\mathbf{GF}(q)$. By $\mathcal{HL}(\mathcal{A},\mathcal{B})$ we denote the set of all ϕ from $\mathrm{Hom}(\mathcal{A},\mathcal{B})$ such that for some $x\neq 0$ and y from $\mathbf{GF}(q)$ this mapping is possible to represent in the following way

$$\phi(a)\ =\ x\cdot a\ +\ y\ .$$

It is easy to see, that

$$\mid\mathrm{Hom}(\mathcal{A},\mathcal{B})\mid\ =\ \mid\mathcal{A}\mid\ (\mid\mathcal{A}\mid -1)\ ,$$

and, how it was proved in Carter and Wegman (1979), this class is uniform. It is true, because for any different a_1, a_2 from $\mathcal{A}$ and for any different b_1, b_2 from $\mathcal{B}$ the system

$$\left\{\begin{array}{l}x\cdot a_1+y=b_1\\ x\cdot a_2+y=b_2\end{array}\right.$$

has only one solution.

2.6 Complexity of the functions with big entropy

We suppose, that conditions (2) and (3) are satisfied. Let

$$\mathbf{F}\in\mathrm{HOM}(\mathcal{C},\mathcal{U})\ ,\qquad \mathbf{G}=\phi\circ\mathbf{F}\ ,$$

and t is a real number at least 1. By $\mathcal{A}(\mathbf{F}, \phi, t)$ we denote the set of all a from $\mathcal{A}$ such that

$$\mathbf{H}(\mathbf{G}_a) \ \geq \ \frac{\mathbf{H}(\mathbf{F})}{\mid \mathcal{A} \mid} \ + \ t \ .$$

Let $\mathbf{d}_{\mathbf{F},\phi,t}$ be the characteristic function of the set $\mathcal{A}(\mathbf{F}, \phi, t)$, i.e.

$$\mathbf{d}_{\mathbf{F},\phi,t} \in \mathrm{Hom}(\mathcal{A}, \{0,1\}) \ , \qquad \mathbf{d}_{\mathbf{F},\phi,t}(a) \ = \ \begin{cases} 1 & \textbf{if } a \in \mathcal{A}(\mathbf{F}, \phi, t) \\ 0 & \textbf{otherwise} \end{cases}$$

Lemma 10 *If the following conditions are true*

$$\mathbf{H}(\mathbf{F}) \ \leq \ m \ , \qquad \mid \mathcal{C} \mid^{2/3} \ \leq \ m \leq \mid \mathcal{C} \mid \log \mid \mathcal{U} \mid \ ,$$

$$2 \ \frac{m}{\log m} \ \leq \mid \mathcal{A} \mid \leq \ 4 \ \frac{m}{\log m} \ , \qquad \frac{\log \mid \mathcal{U} \mid}{\log \mid \mathcal{C} \mid} \ \leq \ 1 \ ,$$

$$t \ = \ (\log m)^{3/4} \ (\log \mid \mathcal{U} \mid)^{1/4} \ , \tag{11}$$

then we have

$$\mathbf{L}\left((\phi \circ \mathbf{F}) \mid_{\mathbf{d}_{\mathbf{F},\phi,t}=0} \right) \ \leq \ \mid \mathcal{U} \mid^{O(1)} \ \mid \mathcal{C} \mid^{3/4+\Theta(|\mathcal{C}|)} \ +$$

$$+ \ \frac{m}{\log m} \left(1 + \Theta(\mid \mathcal{C} \mid) + O(1) \left(\frac{\log \mid \mathcal{U} \mid}{\log m} \right)^{1/4} \right) \ .$$

Proof. Let

$$\epsilon \ = \ \exp_2 \left(-\frac{m}{\mid \mathcal{A} \mid} - t \right) \ , \qquad \mathbf{G}_0 \ = \ (\phi \circ \mathbf{F}) \mid_{\mathbf{d}_{\mathbf{F},\phi,t}=0} \ .$$

In this case

$$\mathbf{G}_0 \ \in \ \mathrm{HOM}_{\mathcal{A},\epsilon}(\mathcal{A} \times \mathcal{B}, \mathcal{U}) \ .$$

Consequently we can obtain a bound for its complexity by applying Lemma 6. We have that $\mathbf{L}(\mathbf{G}_0)$ is at most

$$\frac{\mid \mathcal{A} \mid}{\log \mid \mathcal{A} \mid} \left(1 + \Theta\left(\frac{1}{\epsilon} \right) + \Theta(\mid \mathcal{A} \mid) \right) \left(\log \frac{1}{\epsilon} + 2 \log \mid \mathcal{U} \mid + 2 \log \log \mid \mathcal{B} \mid \right) \ +$$

$$+ \ \mid \mathcal{B} \mid \ \mid \mathcal{U} \mid^{1+\Theta(|\mathcal{U}|)} \left(\frac{1}{\epsilon} \right)^{1+\Theta(1/\epsilon)} \ . \tag{12}$$

By the applying (11), we obtain

$$\leq \ \frac{m}{\mid \mathcal{A} \mid} + t \ = \ \frac{m}{\mid \mathcal{A} \mid} \left(1 + t \ \frac{\mid \mathcal{A} \mid}{m} \right) \ \leq$$

$$\frac{m}{|\,\mathcal{A}\,|}\,\left(1\,+\,\log m^{3/4}\log|\,\mathcal{U}\,|^{1/4}\left(4\,\frac{m}{\log m}\right)\frac{1}{m}\right)\,=$$

$$=\,\frac{m}{|\,\mathcal{A}\,|}\,\left(1\,+\,4\,\left(\frac{\log|\,\mathcal{U}\,|}{\log m}\right)^{1/4}\right)\,.$$

In that way we have

$$\log\frac{1}{\epsilon}\,\leq\,\frac{m}{|\,\mathcal{A}\,|}\,\left(1\,+\,4\,\left(\frac{\log|\,\mathcal{U}\,|}{\log m}\right)^{1/4}\right)\,.$$

and then

$$\frac{1}{\epsilon}\,\leq\,\exp_2\left(\log m\,\left(\frac{1}{2}\,+\,2\,\left(\frac{\log|\,\mathcal{U}\,|}{\log m}\right)^{1/4}\right)\right)\qquad(13)$$

because $|\,\mathcal{A}\,|\geq\,2m/\log m$. Also by (11) we have

$$|\,\mathcal{B}\,|=\,\frac{|\,\mathcal{C}\,|}{|\,\mathcal{A}\,|}\,\leq\,|\,\mathcal{C}\,|^{1/3+\Theta(|\mathcal{C}|)}\,,$$

$$\log\log|\,\mathcal{B}\,|\leq\,\log\log|\,\mathcal{C}\,|\leq\,(1+\Theta(m))\,\log\log m\,.$$

Also it is true

$$\log m\,\leq\,(1+\Theta(m))\log|\,\mathcal{A}\,|\,\,.$$

Combining this bounds with (12) we have that $\mathbf{L}(\mathbf{G}_0)$ is at most

$$\frac{|\,\mathcal{A}\,|}{\log m}(1+\Theta(m))\cdot$$

$$\cdot\left(\frac{m}{|\,\mathcal{A}\,|}\,\left(1\,+\,4\,\left(\frac{\log|\,\mathcal{U}\,|}{\log m}\right)^{1/4}\right)\,+\,2\log|\,\mathcal{U}\,|+3\log\log m\right)\,+$$

$$+\,\,|\,\mathcal{B}\,|\,\,|\,\mathcal{U}\,|^{1+\Theta(|\mathcal{U}|)}.$$

$$\cdot\exp_2\left((\log m)\,\left(\frac{1}{2}\,+\,2\,\left(\frac{\log|\,\mathcal{U}\,|}{\log m}\right)^{1/4}\right)(1+\Theta(m))\right)\qquad(14)$$

By using of the bound

$$\frac{m}{|\,\mathcal{A}\,|}\,\geq\,\frac{1}{2}\log m\,,$$

we obtain

$$\left(\frac{m}{|\,\mathcal{A}\,|}\,\left(1\,+\,4\,\left(\frac{\log|\,\mathcal{U}\,|}{\log m}\right)^{1/4}\right)\,+\,2\log|\,\mathcal{U}\,|+3\log\log m\right)\,\leq$$

$$\leq \frac{m}{|\mathcal{A}|}\left(1 + O(1)\left(\frac{\log|\mathcal{U}|}{\log m}\right)^{1/4} + \Theta(m)\right) \qquad (15)$$

If

$$\frac{\log|\mathcal{U}|}{\log m} \leq \left(\frac{1}{32}\right)^4,$$

then, by (13), we have

$$\frac{1}{\epsilon} \leq \exp_2\left((\log m)\left(\frac{1}{2} + 2\left(\frac{\log|\mathcal{U}|}{\log m}\right)^{1/4}\right)(1+\Theta(m))\right) \leq$$

$$\leq m^{9/16+\Theta(m)}.$$

But if

$$\frac{\log|\mathcal{U}|}{\log m} > \left(\frac{1}{32}\right)^4,$$

then

$$\left(\frac{\log|\mathcal{U}|}{\log m}\right)^{1/4} \leq O(1)\left(\frac{\log|\mathcal{U}|}{\log m}\right),$$

and we obtain, that

$$\frac{1}{\epsilon} \leq \exp_2\left((\log m)\left(\frac{1}{2} + 2\left(\frac{\log|\mathcal{U}|}{\log m}\right)^{1/4}\right)(1+\Theta(m))\right) \leq$$

$$\leq m^{1/2+\Theta(m)}\,|\mathcal{U}|^{O(1)}.$$

Consequently in any case we have

$$|\mathcal{B}|\;|\mathcal{U}|^{1+\Theta(|\mathcal{U}|)}\;\exp_2\left((\log m)\left(\frac{1}{2} + 2\left(\frac{\log|\mathcal{U}|}{\log m}\right)^{1/4}\right)(1+\Theta(m))\right) \leq$$

$$\leq \frac{|\mathcal{C}|}{|\mathcal{A}|}\,m^{9/16+\Theta(m)}\,|\mathcal{U}|^{O(1)} \leq$$

$$\leq \frac{|\mathcal{C}|}{|\mathcal{A}|}\,|\mathcal{A}|^{9/16+\Theta(|\mathcal{A}|)}\,|\mathcal{U}|^{O(1)} \leq$$

$$\leq \frac{|\mathcal{C}|^{1+\Theta(|\mathcal{C}|)}}{|\mathcal{A}|^{7/16}}\,|\mathcal{U}|^{O(1)} \leq \frac{|\mathcal{C}|^{1+\Theta(|\mathcal{C}|)}}{\left(|\mathcal{C}|^{2/3}\right)^{7/16}}\,|\mathcal{U}|^{O(1)} \leq$$

$$\leq |\mathcal{C}|^{3/4+\Theta(|\mathcal{C}|)}\,|\mathcal{U}|^{O(1)}.$$

By using bounds (14) and (15), we obtain the necessary bound.

□

Lemma 11 *If the conditions (11) are true, then there exists a mapping ϕ from $\mathcal{HL}(\mathcal{A}\times\mathcal{B},\mathcal{C})$ such that*

$$\mathbf{H}\left((\phi\circ\mathbf{F})\mid_{\mathbf{d}_{\mathbf{F},\phi,t}=1}\right)\ \leq\ m\ \left(\frac{3}{2}\sqrt{\frac{\log\mid\mathcal{U}\mid}{\log m}}\right)\ .$$

Proof. Let $\mathbf{J}$ be the function from $\mathrm{Hom}(\mathcal{C},\mathcal{R}_+)$ such that

$$\mathbf{J}(a)\ =\ \log\frac{\mid\mathcal{U}\mid}{\mid\mathbf{F}(a)\mid}\ .$$

Then we have

$$\Sigma_{\mathcal{C}}\ \mathbf{J}\ =\ \mathbf{H}(\mathbf{F})\ \leq\ m\ ,$$
$$\Sigma_{\mathcal{C}}\ \mathbf{J}^2\ \leq\ \Sigma_{\mathcal{C}}\ (\mathbf{J}\log\mid\mathcal{U}\mid)\ \leq\ m\log\mid\mathcal{U}\mid\ .$$

By Lemma 8 there exists a mapping ϕ from $\mathcal{HL}(\mathcal{A}\times\mathcal{B},\mathcal{C})$ such that

$$\sum_{a\in\mathcal{S}(t)}\Sigma_{\{a\}\times\mathcal{B}}\ (\phi\circ\mathbf{J})\ \leq\ \left(\frac{1}{t^2}\frac{m}{\mid\mathcal{A}\mid}+\frac{1}{t}\right)m\log\mid\mathcal{U}\mid\ , \tag{16}$$

where

$$\mathcal{S}(t)\ =\ \left\{a\mid\ a\in\mathcal{A}\ ,\ \Sigma_{\{a\}\times\mathcal{B}}(\phi\circ\mathbf{J})\geq\frac{m}{\mid\mathcal{A}\mid}+t\right\}\ .$$

In the following we suppose, that

$$\mathbf{G}\ =\ \phi\circ\mathbf{F}\ ,\qquad \mathbf{G}_1\ =\ \mathbf{G}\mid_{\mathbf{d}_{\mathbf{F},\phi,t}=1}\ ,$$

We have, that

$$\mathbf{H}(\mathbf{G}_a)\ =\ \sum_{b\in\mathcal{B}}\log\frac{\mid\mathcal{U}\mid}{\mid\mathbf{G}_a(b)\mid}\ =\ \sum_{b\in\mathcal{B}}\log\frac{\mid\mathcal{U}\mid}{\mid\mathbf{G}(a,b)\mid}\ =$$

$$=\ \sum_{b\in\mathcal{B}}\log\frac{\mid\mathcal{U}\mid}{\mid\mathbf{F}(\phi(a,b))\mid}\ =\sum_{b\in\mathcal{B}}\mathbf{J}(\phi(a,b))\ =\ \Sigma_{\{a\}\times\mathcal{B}}\ (\phi\circ\mathbf{J})\ .$$

Consequently the sets $\mathcal{A}(\mathbf{F},\phi,t)$ and $\mathcal{S}(t)$ are equal and from (16) we have

$$\sum_{a\in\mathcal{A}(\mathbf{F},\phi,t)}\Sigma_{\{a\}\times\mathcal{B}}\ (\phi\circ\mathbf{J})\ \leq\ \left(\frac{1}{t^2}\frac{m}{\mid\mathcal{A}\mid}+\frac{1}{t}\right)m\log\mid\mathcal{U}\mid\ .$$

It is easy that

$$\mathbf{H}(\mathbf{G}_1)\ =\ \sum_{a\in\mathcal{A}}\mathbf{H}((\mathbf{G}_1)_a)\ =$$

$$= \sum_{a \in \mathcal{A}(\mathbf{F},\phi,t)} \mathbf{H}((\mathbf{G}_1)_a) \ + \sum_{a \in \mathcal{A} \setminus \mathcal{A}(\mathbf{F},\phi,t)} \mathbf{H}((\mathbf{G}_1)_a) \ = $$

$$= \sum_{a \in \mathcal{A}(\mathbf{F},\phi,t)} \mathbf{H}(\mathbf{G}_a) \ ,$$

because

$$(\mathbf{G}_1)_a \ = \ \begin{cases} \mathbf{G}_a & \textbf{if} \ \ a \in \mathcal{A}(\mathbf{F},\phi,t) \\ \equiv \mathcal{U} & \textbf{if} \ \ a \in \mathcal{A} \setminus \mathcal{A}(\mathbf{F},\phi,t) \end{cases} \ ,$$

and the entropy of the function $\equiv \mathcal{U}$ is equal to 0. Consequently

$$\mathbf{H}(\mathbf{G}_1) \ \le \ \left(\frac{1}{t^2} \frac{m}{\mid \mathcal{A} \mid} + \frac{1}{t} \right) m \log \mid \mathcal{U} \mid \ .$$

By (11), we have

$$\mathbf{H}(\mathbf{G}_1) \ \le \ \left(\left((\log m)^{-3/2} (\log \mid \mathcal{U} \mid)^{-1/2} \right) ((1/2) \log m) \ + \right.$$

$$\left. + \ (\log m)^{-3/4} (\log \mid \mathcal{U} \mid)^{-1/4} \right) m \log \mid \mathcal{U} \mid =$$

$$\left(\frac{1}{2} \left(\frac{\log \mid \mathcal{U} \mid}{\log m} \right)^{1/2} \ + \ \left(\frac{\log \mid \mathcal{U} \mid}{\log m} \right)^{3/4} \right) \ m \ \le \ \frac{3}{2} \left(\frac{\log \mid \mathcal{U} \mid}{\log m} \right)^{1/2} m \ .$$

□

Lemma 12 *If*

$$\mathcal{C} = \{0,1\}^n \ , \qquad \mid \mathcal{C} \mid \ge 2 \qquad , \ \mid \mathcal{U} \mid \ge 2 \ , \qquad \frac{\log \mid \mathcal{U} \mid}{\log \mid \mathcal{C} \mid} \le \frac{1}{2} \ ,$$

$$l \ = \ \frac{3}{2} \left(\frac{\log \mid \mathcal{U} \mid}{\log m} \right)^{1/2} m \ ,$$

then

$$\mathbf{L}(\mathrm{HOM}^m(\mathcal{C},\mathcal{U})) \ \le \ \frac{m}{\log m} \left(1 + \Theta(\mid \mathcal{C} \mid) + O(1) \left(\frac{\log \mid \mathcal{U} \mid}{\log \mid \mathcal{C} \mid} \right)^{1/4} \right) \ +$$

$$+ \ O(1) \mid \mathcal{C} \mid^{3/4 + \Theta(|\mathcal{C}|)} \mid \mathcal{U} \mid^{O(1)} \ + \ \mathbf{L}(\mathrm{HOM}^l(\mathcal{C},\mathcal{U})) \ .$$

Proof. If $m \le \mid \mathcal{C} \mid^{3/4}$, then our Lemma is true evidently. And in the following we suppose, that $m < \mid \mathcal{C} \mid^{3/4}$.

Let $\mathbf{F}$ be some function from $\mathrm{HOM}^m(\mathcal{C},\mathcal{U})$. We apply Lemma 4 to this function. We suppose, that $\mathbf{d} = \mathbf{d}_{\mathbf{F},\phi,t}$ and conditions (11) are true.

By Lemma 4 and Lupanov (1965) bounds we have

$$\mathbf{L}(\mathbf{F}) \ \leq \ \mathbf{L}\left((\phi \circ \mathbf{F})\mid_{\mathbf{d}=1}\right) \ + \ \mathbf{L}\left((\phi \circ \mathbf{F})\mid_{\mathbf{d}=0}\right) \ +$$

$$+ \ \frac{\mid \mathcal{A} \mid}{\log \mid \mathcal{A} \mid}(1 + \Theta(\mid \mathcal{A} \mid)) \ + \ O(1)\log^2 \mid \mathcal{C} \mid \ + O(1)\log \mid \mathcal{U} \mid \leq$$

$$\leq \ \mathbf{L}\left((\phi \circ \mathbf{F})\mid_{\mathbf{d}=1}\right) \ + \ \mathbf{L}\left((\phi \circ \mathbf{F})\mid_{\mathbf{d}=0}\right) \ +$$

$$+ \ \Theta(m)\frac{m}{\log m} \ + \ \Theta(\mid \mathcal{C} \mid)\mid \mathcal{C} \mid^{3/4} \ + \ \Theta(\mid \mathcal{U} \mid)\mid \mathcal{U} \mid \ . \qquad (17)$$

By Lemma 11 we have

$$\mathbf{H}\left((\phi \circ \mathbf{F})\mid_{\mathbf{d}=1}\right) \ \leq \ \frac{3}{2} \ m \ \left(\frac{\log \mid \mathcal{U} \mid}{\log m}\right) ,$$

consequently

$$\leq \ \mathbf{L}\left((\phi \circ \mathbf{F})\mid_{\mathbf{d}=1}\right) \ \leq \ \mathbf{L}(\mathrm{HOM}^l(\mathcal{C},\mathcal{U}) \ .$$

By combining this bound with (17) and with Lemma 10 bound for $\mathbf{L}\left((\phi \circ \mathbf{F})\mid_{\mathbf{d}=0}\right)$ we obtain necessary result.

□

Lemma 13 *If*

$$\mathcal{A} = \{0,1\}^n \ , \qquad \mid \mathcal{A} \mid \geq 2 \qquad , \ \mid \mathcal{U} \mid \geq 2 \ , \qquad \frac{\log \mid \mathcal{U} \mid}{\log \mid \mathcal{A} \mid} \leq \frac{1}{2} \ ,$$

then

$$\mathbf{L}(\mathrm{HOM}^m(\mathcal{A},\mathcal{U})) \ \leq \ \frac{m}{\log m}\left(1 + \Theta(\mid \mathcal{A} \mid) + O(1)\left(\frac{\log \mid \mathcal{U} \mid}{\log \mid \mathcal{A} \mid}\right)^{1/4}\right) \ +$$

$$+ \ O(1)\mid \mathcal{A} \mid^{3/4+\Theta(|\mathcal{A}|)} \mid \mathcal{U} \mid^{O(1)} \ .$$

Proof. Let

$$m(k) \ = \ \left(\frac{3}{2} \ \left(\frac{\log \mid \mathcal{U} \mid}{\log \mid \mathcal{A} \mid}\right)\right)^k \ m \ .$$

By Lemma 12 we have

$$\mathbf{L}(\mathrm{HOM}^{m(k)}(\mathcal{A},\mathcal{U})) \ \leq \ \frac{m(k)}{\log m(k)}\left(1 + \Theta(\mid \mathcal{A} \mid) + O(1)\left(\frac{\log \mid \mathcal{U} \mid}{\log \mid \mathcal{A} \mid}\right)^{1/4}\right) \ +$$

$$+\ O(1)|\ \mathcal{A}\ |^{3/4+\Theta(|\mathcal{A}|)}\ |\ \mathcal{U}\ |^{O(1)}\ +\ \mathbf{L}(\mathrm{HOM}^{m(k+1)}(\mathcal{A},\mathcal{U}))\ . \qquad (18)$$

By the iteration of this bound we obtain

$$\mathbf{L}(\mathrm{HOM}^{m}(\mathcal{A},\mathcal{U}))\ \le$$

$$\le\ \left(\sum_{i=1}^{k}\frac{m(k)}{\log m(k)}\right)\left(1+\Theta(|\ \mathcal{A}\ |)+O(1)\left(\frac{\log|\ \mathcal{U}\ |}{\log|\ \mathcal{A}\ |}\right)^{1/4}\right)\ +$$

$$+\ k\ O(1)|\ \mathcal{A}\ |^{3/4+\Theta(|\mathcal{A}|)}\ |\ \mathcal{U}\ |^{O(1)}\ +\ \mathbf{L}(\mathrm{HOM}^{m(k+1)}(\mathcal{A},\mathcal{U}))\ .$$

We suppose that $m \le |\ \mathcal{A}\ |\log|\ \mathcal{U}\ |$, because

$$\max_{\mathbf{F}\in\mathrm{HOM}(\mathcal{A},\mathcal{U})}\mathbf{H}(\mathbf{F})\ =|\ \mathcal{A}\ |\ \log|\ \mathcal{U}\ |\ .$$

We change minimal k such that $m(k+1)\le|\ \mathcal{A}\ |^{3/4}$. In our conditions we have

$$\frac{3}{2}\left(\frac{\log|\ \mathcal{U}\ |}{\log|\ \mathcal{A}\ |}\right)^{1/2}\ \le\ \frac{3}{2}\left(\frac{1}{4}\right)^{1/2}\ =\ \frac{3}{4}\ <\ 1\ ,$$

consequently

$$k\ \le\ O(1)\ \log\frac{|\ \mathcal{A}\ |\log|\ \mathcal{U}\ |}{|\ \mathcal{A}\ |^{3/4}}\ \le\ O(1)\ \log|\ \mathcal{A}\ |\ ,$$

$$\sum_{i=1}^{k}\frac{m(k)}{\log m(k)}\ \le\ \frac{m}{\log m}\left(1+\Theta(|\ \mathcal{A}\ |)+O(1)\left(\frac{\log|\ \mathcal{U}\ |}{\log|\ \mathcal{A}\ |}\right)^{1/2}\right)\ .$$

By combining this bound with (18) we obtain the necessary result.

□

2.7 General case

We suppose, that conditions (2) and (3) are true.

Lemma 14 *If the following conditions are true*

$$\mathbf{H}(\mathbf{F})\ \le\ m\ ,\qquad 2\ \le\ m\le|\ \mathcal{C}\ |\log|\ \mathcal{U}\ |\ ,$$

$$1\ \le\ \frac{|\ \mathcal{A}\ |}{m\ |\ \mathcal{U}\ |^{4}\log^{4}m}\le\ 2\ ,\qquad \frac{\log|\ \mathcal{U}\ |}{\log|\ \mathcal{C}\ |}\ \le\ 1\ ,$$

then there exists a mapping ϕ from $\mathcal{HL}(\mathcal{A}\times\mathcal{B},\mathcal{C})$ such that

$$\mathbf{L}\left(\mathbf{F}\ |_{\psi_1\circ\mathbf{Q}_{\mathbf{F},\phi,\mathcal{A}}=0}\right)\ +\ \mathbf{L}\left(\mathbf{Q}_{\mathbf{F},\phi,\mathcal{A}}\right)\ \le\ \Theta(m)\frac{m}{\log m}\ .$$

Proof. We define the function $\mathbf{J}$ from $\mathrm{Hom}(\mathcal{C}, \{0,1\})$ by the following

$$\mathbf{J}(c) \ = \ \begin{cases} 1 & \textbf{if } \mathbf{F}(c) \neq \mathcal{U} \\ 0 & \textbf{otherwise} \end{cases} \ .$$

We suppose, that

$$\mathbf{F}_0 \ = \ \mathbf{F} \mid_{\psi_1 \circ \mathbf{Q}_{\mathbf{F},\phi,\mathcal{A}}=0} \ ,$$

$$\mathcal{D} \ = \ \left\{ a \mid \ a \in \mathcal{A} \ , \ \Sigma_{\{a\} \times \mathcal{B}} \ \phi \circ \mathbf{J} \ > \ 1 \right\} \ .$$

Earlier we have defined the function $\mathbf{Q}_{\mathbf{F},\phi,\mathcal{A}}$ such that

$$\mathbf{Q}_{\mathbf{F},\phi,\mathcal{A}}(c) = 0 \ \iff \ c \in \mathcal{D} \ ,$$

consequently

$$\mid \mathcal{M}(\mathbf{F}_0) \mid \ = \ \sum_{a \in \mathcal{D}} \Sigma_{\{a\} \times \mathcal{B}} \ \phi \circ \mathbf{J} \ .$$

We suppose, that for the function ϕ assumption of Lemma 9 is true. In this case we have

$$\mid \mathcal{M}(\mathbf{F}_0) \mid \leq \ \frac{1}{\mid \mathcal{A} \mid} (\Sigma_{\mathcal{C}} \ \mathbf{J})^2 \ = \ \frac{1}{\mid \mathcal{A} \mid} (\mid \mathcal{M}(\mathbf{F}) \mid)^2$$

We has noticed in Lemma 1 that

$$\mid \mathcal{M}(\mathbf{F}) \mid \leq \ \mathbf{H}(\mathbf{F}) \mid \mathcal{U} \mid \ .$$

Consequently

$$\mid \mathcal{M}(\mathbf{F}_0) \mid \leq \ \frac{1}{\mid \mathcal{A} \mid} m^2 \mid \mathcal{U} \mid^2 \ \leq \ \frac{m^2 \mid \mathcal{U} \mid^2}{m \mid \mathcal{U} \mid^4 \log^4 m} \ = \ \frac{m}{\mid \mathcal{U} \mid^2 \log^4 m} \ .$$

In that way we have, that

$$\mathbf{H}(\mathbf{F}_0) \ \leq \mid \mathcal{M}(\mathbf{F}_0) \mid \log \mid \mathcal{U} \mid \leq \ \frac{m \log \mid \mathcal{U} \mid}{\mid \mathcal{U} \mid^2 \log^4 m} \ .$$

We apply Lemma 1 for the function $\mathbf{F}_0$ and obtain the following bound for its complexity

$$\mathbf{L}(\mathbf{F}_0) \ \leq \ 8 \ \mathbf{H}(\mathbf{F}_0) \mid \mathcal{U} \mid \log \mid \mathcal{U} \mid \leq$$

$$\leq \ \frac{m \log^2 \mid \mathcal{U} \mid}{\mid \mathcal{U} \mid \log^4 m} \ \leq \ \frac{2m}{\log^4 m} \ = \ \Theta(m) \frac{m}{\log m} \ . \qquad (19)$$

It is easy to see, that for the complexity of any boolean function $\mathbf{f}$ from $\mathrm{Hom}(\mathcal{A},\{0,1\})$ the following bound is true

$$\mathbf{L}(\mathbf{f}) \ \leq \ O(1) \mid \{a \mid \ a \in \mathcal{A} \ , \ \mathbf{f}(a) = 0\} \mid \log \mid \mathcal{A} \mid \ .$$

By the construction we have

$$\mid \{a \mid \ a \in \mathcal{A} \ , Q_{\mathbf{F},\phi,\mathcal{A}}(a) = 0\} \mid \leq \mid \mathcal{M}(\mathbf{F}_0) \mid \leq \ \frac{m}{\mid \mathcal{U} \mid^2 \log^4 m}$$

Consequently

$$\mathbf{L}(\mathbf{Q}_{\mathbf{F},\phi,\mathcal{A}}) \ \leq \ \frac{m \log \mid \mathcal{A} \mid}{\mid \mathcal{U} \mid^2 \log^4 m} \ \leq \ O(1) \ \frac{m}{\log^3 m} \ = \ \ \Theta(m) \ \frac{m}{\log m} \ .$$

We combine this bound with the bound (19) and obtain the necessary result.

□

Theorem 1 *If* $\mid \mathcal{C} \mid \geq 2$, $\mid \mathcal{U} \mid \geq 2$, *then*

$$\mathbf{L}(\mathrm{HOM}^m(\mathcal{C},\mathcal{U})) \ \geq \ \frac{m}{\log m} \ (1 - \Theta(m)) + O(1) \log \mid \mathcal{C} \mid \ ,$$

$$\mathbf{L}(\mathrm{HOM}^m(\mathcal{C},\mathcal{U})) \ \leq \ \frac{m}{\log m} \left(1 + \Theta(m) + O(1) \left(\frac{\log \mid \mathcal{U} \mid}{\log m}\right)^{1/4}\right) \ + \\ + \ O(1) \ \log(\mid \mathcal{C} \mid) \ + \ \mid \mathcal{U} \mid^{O(1)} \ .$$

Proof. The lower bound can be obtained analogical by to Sholomov (1969).

At the first step we suppose, that $\mathcal{C} = \{0,1\}^r$ and $r \geq 2$. We can suppose without loss of generality that

$$m \geq 2 \ , \qquad \frac{\log \mid \mathcal{U} \mid}{\log m} \ \leq \ \frac{1}{2} \ ,$$

because in other case our theorem follow from Lemma 1. Let $\mathbf{F}$ be some function from $\mathrm{HOM}(\mathcal{C},\mathcal{U})$. We have, that

$$\mathbf{H}(\mathbf{F}) \ \leq \mid \mathcal{C} \mid \log \mid \mathcal{U} \mid \ ,$$

Consequently we can suppose also, that

$$m \ \leq \mid \mathcal{C} \mid \log \mid \mathcal{U} \mid \ .$$

We choosee the sets $\mathcal{A}$ and $\mathcal{B}$ such that

$$\mathcal{A} = \{0,1\}^p \ , \ \mathcal{B} = \{0,1\}^s \ , \qquad p \geq 1 \ , \ s \geq 1 \ , \qquad p + s = r \ ,$$

$$1 \ \leq \ \frac{|\ \mathcal{A}\ |}{m\ |\ \mathcal{U}\ |^4 \log^4 m} \leq \ 2 \ , \tag{20}$$

It is impossible only in the case when

$$m\ |\ \mathcal{U}\ |^4 \log^4 m \ \geq \ \frac{1}{4} \ |\ \mathcal{C}\ | \ .$$

In this case our theorem follow immediately from Lemma 13 and we suppose, that (20) is true.

We compute our function $\mathbf{F}$ according to Lemma 5. We have that $\mathbf{L}(\mathbf{F})$ is at most

$$\mathbf{L}\left(\mathbf{C}_{\mathbf{F},\phi,\mathcal{A}}\right) \ + \ \mathbf{L}\left(\mathbf{F}\ |_{\psi_1 \circ \mathbf{Q}_{\mathbf{F},\phi,\mathcal{A}}=0}\right) \ + \ \mathbf{L}\left(\mathbf{Q}_{\mathbf{F},\phi,\mathcal{A}}\right) \ + \ \mathbf{L}(\psi_1) \ + \ \mathbf{L}(\mathbf{w}) \ .$$

It is easy to see, that

$$\mathbf{L}(w) \ \leq \ O(1) \log |\ \mathcal{U}\ | \ . \tag{21}$$

The function ψ_1 is some boolean linear (r,p)-operator. Consequently according to Lupanov (1956) bounds for matrix complexity we have

$$\mathbf{L}(\psi_1) \ \leq \ \frac{rp}{\log r} + O(r) \ = \ \frac{\log |\ \mathcal{C}\ | \log |\ \mathcal{A}\ |}{\log\log |\ \mathcal{C}\ |} + O(1) \log |\ \mathcal{C}\ | =$$

$$\Theta(m) \frac{m}{\log m} + O(1) \log |\ \mathcal{C}\ | \ . \tag{22}$$

From Lemma 14 we have that there exists a mapping ϕ from $\mathcal{HL}(\mathcal{A} \times \mathcal{B}, \mathcal{C})$ such that

$$\mathbf{L}\left(\mathbf{F}\ |_{\psi_1 \circ \mathbf{Q}_{\mathbf{F},\phi,\mathcal{A}}=0}\right) \ + \ \mathbf{L}\left(\mathbf{Q}_{\mathbf{F},\phi,\mathcal{A}}\right) \ \leq \ \Theta(m) \frac{m}{\log m} \ . \tag{23}$$

It is easy to see, that

$$\mathbf{C}_{\mathbf{F},\phi,\mathcal{A}} \in \mathrm{HOM}^m(\mathcal{A}, \mathcal{U}) \ ,$$

consequently by applying Lemma 13 to this function we have

$$\mathbf{L}(\mathbf{C}_{\mathbf{F},\phi,\mathcal{A}}) \ \leq \ \frac{m}{\log m} \left(1 + \Theta(|\ \mathcal{A}\ |) + O(1) \left(\frac{\log |\ \mathcal{U}\ |}{\log |\ \mathcal{A}\ |}\right)^{1/4}\right) \ +$$

$$+ O(1)|\,\mathcal{A}\,|^{3/4+\Theta(|\mathcal{A}|)}\,|\,\mathcal{U}\,|^{O(1)} \leq$$

$$\leq \frac{m}{\log m}\left(1+\Theta(m)+O(1)\left(\frac{\log|\,\mathcal{U}\,|}{\log m}\right)^{1/4}\right)+|\,\mathcal{U}\,|^{O(1)}\ . \qquad (24)$$

The sum of (21), (22), (23), (24) is the necessary bound.

In the following we do not suppose that $\mathcal{C}=\{0,1\}^r$. Let

$$\mathcal{C}\subseteq\mathcal{D}=\{0,1\}^r\ , \qquad 2^{r-1}<|\,\mathcal{C}\,|\leq 2^r\ .$$

Let $\mathbf{F}$ be some function from $\mathrm{HOM}^m(\mathcal{A},\mathcal{U})$. We define a function $\mathbf{G}$ from $\mathrm{HOM}(\mathcal{D},\mathcal{U})$ such that

$$\mathbf{G}(c) \ = \ \begin{cases} \mathbf{F}(c) & \textbf{if} \quad c\in\mathcal{C} \\ \mathcal{U} & \textbf{otherwise}\ . \end{cases}$$

It is easy to see, that

$$\mathbf{H}(\mathbf{G}) \ = \ \mathbf{H}(\mathbf{F})\ , \qquad \mathbf{G}\in\mathrm{HOM}^m(\mathcal{D},\mathcal{U})\ .$$

Also it is easy, that some circuit $\mathbf{S}$ compute the function $\mathbf{G}$ if and only if this circuit compute the function $\mathbf{F}$. Consequently $\mathbf{L}(\mathbf{G}) \ = \ \mathbf{L}(\mathbf{F})$, and we have, that

$$\mathbf{L}(\mathrm{HOM}^m(\mathcal{C},\mathcal{U})) \ \leq \ \mathbf{L}(\mathrm{HOM}^m(\mathcal{D},\mathcal{U}))\ .$$

It is not difficult to check, that necessary bounds are true, because

$$|\,\mathcal{C}\,|\leq|\,\mathcal{D}\,|\leq\ 2\,|\,\mathcal{C}\,|\ \ .$$

□

3 Hitting set construction

3.1 The case of not too small entropy

By $\mathcal{N}$ we denote the set of all natural numbers.

Lemma 15 *There exists a function* $\mathbf{l}(n,k,p,q)$ *from* $\mathrm{Hom}(\mathcal{N}^4,\mathcal{N})$ *computable in the time polynomial of*

$$\log n+\log k+\log p+\log q\ ,$$

such that

$$\mathbf{L}(\mathrm{HOM}_{p/q}(\mathcal{A},\mathcal{U})) \ \le \ \mathbf{l}(|\ \mathcal{A}\ |,|\ \mathcal{U}\ |,p,q)\ ,$$

and $\mathbf{l}(n,k,p,q)$ *at most*

$$\frac{\log(q/p)}{\log\log(q/p)}\left(1+\Theta\left(\frac{q}{p}\right)+O(1)\left(\frac{\log k}{\log\log(q/p)}\right)^{1/4}\right)+O(1)\log n+k^{O(1)}\ .$$

Proof. This fact follow from the proof of Theorem 1.

□

By $\mathrm{Hom}^{\mathrm{hit}}_{p,q}(\mathcal{A},\mathcal{U})$ we denote the set of all functions $\mathbf{f}$ from $\mathrm{Hom}(\mathcal{A},\mathcal{U})$ such that

$$\mathbf{L}(\mathbf{f}) \ \le \ \mathbf{l}(|\ \mathcal{A}\ |,|\ \mathcal{U}\ |,p,q)\ .$$

Lemma 16 *The set* $\mathrm{Hom}^{\mathrm{hit}}_{p,q}(\mathcal{A},\mathcal{U})$ *is a hitting set for the system* $\mathrm{HOM}_{p/q}(\mathcal{A},\mathcal{U})$. *If*

$$\Theta(|\ \mathcal{A}\ |)\ \log\frac{q}{p}\ \ge\ \log|\ \mathcal{A}\ |\ \ \log\log|\ \mathcal{A}\ |\ ,$$
$$\log|\ \mathcal{U}\ |\ \le\ \Theta(|\ \mathcal{A}\ |)\ \log\log(q/p)\ , \qquad (25)$$

then

$$|\ \mathrm{Hom}^{\mathrm{hit}}_{p,q}(\mathcal{A},\mathcal{U})\ |\ \le\ \left(\frac{q}{p}\right)^{1+\Theta(|\mathcal{A}|)}\ .$$

Proof. It is easy to see, that $\mathrm{Hom}^{\mathrm{hit}}_{p,q}(\mathcal{A},\mathcal{U})$ is a hitting set. Let

$$|\ \mathcal{A}\ |=n\ ,\qquad |\ \mathcal{U}\ |=k\ ,\qquad l=\mathbf{l}(n,k,p,q)\ .$$

It easy to see, that our bound is at most $NS(\lceil\log n\rceil,\lceil\log k\rceil,l)$, i.e. the number of circuits with $\lceil\log n\rceil$ inputs, $\lceil\log k\rceil$ outputs and with complexity at most l. Lupanov (1965) has proved that this number is at most

$$(O(1)(\log n+l))^{l+\log k+O(1)}\ .$$

From this bound and conditions (25) we obtain, that

$$\log NS(\lceil\log n\rceil,\lceil\log k\rceil,l)\ \le\ (1+\Theta(n))\ \log\frac{q}{p}\ .$$

Consequently the necessary bound is true.

□

3.2 Hash classes of functions

In this section we are constructing the classes of the special hash mappings. Let $\mathcal{A}$ and $\mathcal{B}$ finite sets. Let $\mathcal{S}$ be a subset of $\mathcal{A}$.

We say that mapping ϕ from $\mathrm{Hom}(\mathcal{A},\mathcal{B})$ is hash function for $\mathcal{S}$, if

$$a_1, a_2 \in \mathcal{S}\ ,\ a_1 \neq a_2 \qquad \Longrightarrow \qquad \phi(a_1) \neq \phi(a_2)\ .$$

Let $\mathcal{F}$ be a mapping set, $\mathcal{F} \subseteq \mathrm{Hom}(\mathcal{A},\mathcal{B})$. The set $\mathcal{F}$ is hash class for the set $\mathcal{S}$, if in $\mathcal{F}$ there exists some hush function for $\mathcal{S}$.

The set $\mathcal{F}$ is μ-hash class, if it is hash class for any μ-elements subset of $\mathcal{A}$.

Such function classes has been considered in Poljak, Pultr and Rodl (1983) and in Krichevsky (1985). In this subsection we construct special μ-hash class for our goals.

Let

$$\mathcal{F}_1 \circ \mathcal{F}_2 \ = \ \{\phi_1 \circ \phi_2 \mid \ \phi_1 \in \mathcal{F}_1\ ,\ \phi_2 \in \mathcal{F}_2\}$$

for

$$\mathcal{F}_1 \subseteq \mathrm{Hom}(\mathcal{A},\mathcal{B})\ , \qquad F_2 \subseteq \mathrm{Hom}(\mathcal{B},\mathcal{C})\ .$$

By $\mathbf{GF}(q)$ we denote the q-elements Galua field. For a natural $\eta \geq 2$ and $g \in \mathbf{GF}(q)$ we let

$$\phi_{\eta,g} \ \in \ \mathrm{Hom}(\mathbf{GF}(q)^\eta, \mathbf{GF}(q))\ ,$$

$$\phi_{\eta,g}(a_1, a_2, ..., a_\eta) \ = \ a_1 + a_2 g + a_3 g^2 + ... + a_\eta g^{\eta-1}\ ,$$

$$\mathcal{LF}_\eta(\mathcal{G}) \ = \ \{\phi_{\eta,g} \mid \ g \in \mathcal{G}\}\ , \qquad \mathcal{G} \subseteq \mathbf{GF}(q)\ .$$

The following Lemma 17 and Lemma 18 has been proved by Krichevsky (1985).

Lemma 17 *If*

$$\mid \mathcal{G} \mid \geq \ \left(\begin{array}{c} \mu \\ 2 \end{array} \right) (\eta - 1) + 1\ , \qquad \eta \geq 2\ ,$$

then $\mathcal{LF}_\eta(\mathcal{G})$ is μ-hash class.

Lemma 18 *If*

$$\mathcal{F}_1 \subseteq \mathrm{Hom}(\mathcal{A},\mathcal{B})\ , \qquad \mathcal{F}_2 \subseteq \mathrm{Hom}(\mathcal{B},\mathcal{C})\ ,$$

are μ-hash classes, then

$$\mathcal{F}_1 \circ \mathcal{F}_2 \subseteq \mathrm{Hom}(\mathcal{A}, \mathcal{C})$$

is μ-hash class also.

Lemma 19 *For any finite sets $\mathcal{A}$, $\mathcal{B}$ and natural numbers μ, η, such that*

$$| \mathcal{A} | \geq | \mathcal{B} | \geq \mu^2 \eta \ , \qquad \eta \geq 2 \ , \ \mu \geq 1 \ ,$$

there exists μ-hash class $\mathrm{Hom}^{\mathrm{hash}}_{\mu,\eta}(\mathcal{A}, \mathcal{B})$ such that

$$\mathrm{Hom}^{\mathrm{hash}}_{\mu,\eta}(\mathcal{A}, \mathcal{B}) \ \subseteq \ \mathrm{Hom}(\mathcal{A}, \mathcal{B}) \ ,$$

$$| \mathrm{Hom}^{\mathrm{hash}}_{\mu,\eta}(\mathcal{A}, \mathcal{B}) | \leq \ \mu^2 \eta \left(\frac{\log | \mathcal{A} |}{\lfloor \log | \mathcal{B} | \rfloor} \right)^{1+2 \log \mu / \log \eta} \ .$$

There exist an algorithm for this class construction with working time at most

$$| \mathrm{Hom}^{\mathrm{hash}}_{\mu,\eta}(\mathcal{A}, \mathcal{B}) | \ | \mathcal{A} |^{1+o(1)} \ .$$

Proof. We have

$$2 \left(\left(\begin{array}{c} \mu \\ 2 \end{array} \right) (\eta - 1) + 1 \right) - 1 \ =$$

$$= \ \mu^2 \eta - \mu^2 - \mu(\eta - 1) + 1 \ \leq \ \mu^2 \eta \ \leq | B | \ .$$

Consequently, if we let $d = \lfloor \log | \mathcal{B} | \rfloor$ then

$$\left(\begin{array}{c} \mu \\ 2 \end{array} \right) (\eta - 1) + 1 \ \leq \ 2^d \ \leq | \mathcal{B} | \ . \qquad (26)$$

Let s minimal nonnegative integer number such that

$$| \mathcal{A} | \leq \ \exp_2(d \ \eta^s) \ , \qquad \text{where} \qquad \exp_2(x) \ = \ 2^x \ . \qquad (27)$$

Let

$$\mathcal{C}_i \ = \ \mathbf{GF}(\exp_2(d \ \eta^i)) \ , \qquad i = 0, 1, ..., s \ .$$

In this case we may suppose that

$$\mathcal{C}_{i+1} \ = \ (\mathcal{C}_i)^\eta \ , \qquad i = 0, 1, ..., s - 1 \ .$$

By (26) there exist sets $\mathcal{G}_i$, such that

$$\mathcal{G}_i \subseteq \mathcal{C}_i \ , \qquad | \mathcal{G}_i | = \ \left(\begin{array}{c} \mu \\ 2 \end{array} \right) (\eta - 1) + 1 \ , \qquad (28)$$

$$i = 0, 1, ..., s-1 \ .$$

According to Lemma 17 the function sets

$$\mathcal{LF}_\eta(\mathcal{G}_i) \ \subseteq \ \mathrm{Hom}(\mathcal{C}_{i+1}, \mathcal{C}_i) \ , \qquad i = 0, 1, ..., s-1 \ ,$$

are μ-hash classes. Let

$$\mathrm{Hom}^{\mathrm{hash}}_{\mu,\eta}(\mathcal{C}_s, \mathcal{C}_0) \ = \ \mathcal{LF}_\eta(\mathcal{G}_{s-1}) \circ \mathcal{LF}_\eta(\mathcal{G}_{s-2}) \circ ... \circ \mathcal{LF}_\eta(\mathcal{G}_0) \ .$$

By Lemma 18 we have, that this function set is μ-hash class. By (28) we have the following upper bound for the class size

$$\mid \mathrm{Hom}^{\mathrm{hash}}_{\mu,\eta}(\mathcal{C}_s, \mathcal{C}_0) \mid \ \leq \ \prod_{i=0}^{s-1} \mid \mathcal{G}_i \mid \ \leq \ (\mu^2\eta)^s \ . \qquad (29)$$

By (27) we have that

$$s \ = \ \left\lceil \frac{\log \frac{\log|A|}{d}}{\log \eta} \right\rceil \ \leq \ \frac{\log \frac{\log|A|}{\lfloor \log|B| \rfloor}}{\log \eta} + 1 \ ,$$

$$(\mu^2\eta)^s \ \leq \ \mu^2\eta \ \exp\left(\frac{(2\log\mu + \log\eta)}{\log\eta} \ \log \frac{\log \mid A \mid}{\lfloor \log \mid B \mid \rfloor} \right) \ =$$

$$= \ \mu^2\eta \ \left(\frac{\log \mid A \mid}{\lfloor \log \mid B \mid \rfloor} \right)^{1 + 2\log\mu/\log\eta} \ .$$

Consequently, by (29),

$$\mathrm{Hom}^{\mathrm{hash}}_{\mu,\eta}(\mathcal{C}_s, \mathcal{C}_0) \ \leq \ \mu^2\eta \ \left(\frac{\log \mid A \mid}{\lfloor \log \mid B \mid \rfloor} \right)^{1 + 2\log\mu/\log\eta} \ .$$

We let

$$\mathrm{Hom}^{\mathrm{hash}}_{\mu,\eta}(\mathcal{A}, \mathcal{B}) \ = \ \{\phi\} \circ \mathrm{Hom}^{\mathrm{hash}}_{\mu,\eta}(\mathcal{C}_s, \mathcal{C}_0) \circ \{\psi\} \ ,$$

where ϕ some injection from $\mathrm{Hom}(\mathcal{A}, \mathcal{C}_s)$ and ψ some injection from $\mathrm{Hom}(\mathcal{C}_0, \mathcal{B})$.

The upper bound for algorithm working time is trivial.

□

3.3 The case of small entropy

Lemma 20 *If* $\mathcal{Q} \subseteq \mathrm{Hom}(\mathcal{B},\mathcal{U})$ *is a hitting set for the system* $\mathrm{HOM}_\epsilon(\mathcal{B},\mathcal{U})$ *and* $\mathcal{F} \subseteq \mathrm{Hom}(\mathcal{A},\mathcal{B})$ *is* $\left\lfloor |\,\mathcal{U}\,| \log \frac{1}{\epsilon} \right\rfloor$*-hash function class, then the set* $\mathcal{F} \circ \mathcal{Q}$ *is hitting for the set system* $\mathrm{HOM}_\epsilon(\mathcal{A},\mathcal{U})$.

Proof. Let $\mathbf{F}$ be some function from $\mathrm{HOM}_\epsilon(\mathcal{A},\mathcal{U})$. We know, that

$$|\,\mathcal{M}(\mathbf{F})\,| \leq\ \mu(\epsilon)\ , \qquad \text{where} \qquad \mu(\epsilon)\ =\ \left\lfloor |\,\mathcal{U}\,| \log \frac{1}{\epsilon} \right\rfloor\ .$$

Let a mapping ϕ from $\mathcal{F}$ be hash function for $\mathcal{M}(\mathbf{F})$. There exists such hash function, because the set $\mathcal{F}$ is $\mu(\epsilon)$-hash class. By ϕ and $\mathbf{F}$ we define new function $\mathbf{G}$ such that

$$\mathbf{G}\ \in\ \mathrm{HOM}(\mathcal{B},\mathcal{U})\ , \qquad\qquad \mathbf{G}(b)\ =\ \bigcap_{a \in \phi^{-1}(b)} \mathbf{F}(a)\ .$$

This definition is correct because ϕ is hash function for the set $\mathcal{M}(\mathbf{F})$ and consequently in this case for any x from $\mathcal{B}$ it is true

$$|\,\mathcal{M}(\mathbf{F}) \cap \phi^{-1}(b)\,| \leq\ 1\ . \tag{30}$$

We have, that

$$|\,\mathcal{M}(\mathbf{G})\,| = |\,\mathcal{M}(\mathbf{F})\,|\ , \qquad \mathbf{H}(\mathbf{G})\ =\ \mathbf{H}(\mathbf{F})\ .$$

consequently

$$\mathbf{G}\ \in\ \mathrm{HOM}_\epsilon(\mathcal{B},\mathcal{U})\ .$$

Because $\mathcal{Q}$ is hitting set for the system $\mathrm{HOM}_\epsilon(\mathcal{B},\mathcal{U})$, there exist some function $\mathbf{g}$ from $\mathcal{Q}$ such that $\mathbf{g} \in \mathbf{G}$. We consider

$$\mathbf{f}\ =\ \phi \circ \mathbf{g}\ \in\ \mathcal{F} \circ \mathcal{Q}\ ,$$

and will be checking that $\mathbf{f} \in \mathbf{F}$. It means, that

$$\forall a \in \mathcal{A}\ :\ \mathbf{f}(a) \in \mathbf{F}(a)\ . \tag{31}$$

Let $a \in \mathcal{A}$, $b = \phi(a)$. If $\mathbf{F}(a) = \mathcal{U}$, then (31) is true for any value of $\mathbf{f}(a)$. Suppose, that $\mathbf{F}(a) \neq \mathcal{U}$. Then, in the correspondence with function $\mathbf{G}$ definition, and (30) we have

$$\forall x \in \phi^{-1}(b) \setminus \{a\}\ :\ \mathbf{F}(x) = \mathcal{U}\ .$$

Consequently

$$\mathbf{G}(b) \ = \ \bigcap_{x \in \phi^{-1}(b)} \mathbf{F}(x) \ = \ \mathbf{F}(a) \ ,$$

and we have

$$\mathbf{f}(a) \ = \ (\phi \circ \mathbf{g})(a) \ = \ \mathbf{g}(\phi(a)) \ = \ \mathbf{g}(b) \in \mathbf{G}(b) = \mathbf{F}(a) \ ,$$

$$\mathbf{f}(a) \ \in \ \mathbf{F}(a) \ .$$

□

In the following we suppose

$$n = \mid \mathcal{A} \mid \ , \qquad k = \mid \mathcal{U} \mid \ , \qquad \mu = \left\lfloor k \ \log \frac{q}{p} \right\rfloor \ ,$$

$$\eta = \mu^{\log\log\log\log n} \ , \qquad \theta = \lceil \log(\mu^2 \eta) \rceil \ .$$

$$\mathrm{Hom}_{p,q}^{\mathrm{hit}*}(\mathcal{A},\mathcal{U}) \ = \ \begin{cases} \mathrm{Hom}_{p,q}^{\mathrm{hit}}(\mathcal{A},\mathcal{U}) & \textbf{if } \theta \geq \sqrt{\log n} \\ \mathrm{Hom}_{\mu,\eta}^{\mathrm{hash}}(\mathcal{A},\{0,1\}^{\theta}) \circ \mathrm{Hom}_{p,q}^{\mathrm{hit}}(\{0,1\}^{\theta},\mathcal{U}) & \\ & \textbf{if } \theta < \sqrt{\log n} \end{cases}$$

Theorem 2 *The set* $\mathrm{Hom}_{p,q}^{\mathrm{hit}*}(\mathcal{A},\mathcal{U})$ *is a hitting set for the system* $\mathrm{HOM}_{p/q}(\mathcal{A},\mathcal{U})$. *If*

$$\log \mid \mathcal{U} \mid \ \leq \ \Theta(\mid \mathcal{A} \mid) \ \log\log(q/p) \ , \tag{32}$$

then

$$\mid \mathrm{Hom}_{p,q}^{\mathrm{hit}*}(\mathcal{A},\mathcal{U}) \mid \ \leq \ \left(\frac{q}{p} \log \mid \mathcal{A} \mid \right)^{1+\Theta(|\mathcal{A}|)} \ .$$

There exists a algorithm for this set construction with the working time at most

$$\mid \mathcal{A} \mid^{1+o(1)} \ \left(\frac{\log \mid \mathcal{A} \mid}{p/q} \right)^{1+o(1)}$$

Proof. Suppose that $\theta \geq \sqrt{\log n}$. In this case we have

$$\theta \ \leq \ 2\log\mu + \log\eta \ \leq \ (1+o(1)) \log\mu \log\log\log\log n \ ,$$

consequently

$$\log \mu \ \geq \ (1 - o(1)) \ \frac{\sqrt{\log n}}{\log \log \log \log n} \ \geq \ (\log n)^{1/4} \ .$$

By (32) we have

$$(\log n)^{1/4} \ \leq \ \log \mu \ \leq \ (1 - \Theta(n)) \log \log \frac{q}{p} \ ,$$

$$\Theta(n) \log \frac{q}{p} \ \geq \ \log n \ \log \log n \ ,$$

and necessary result follows from Lemma 16.

Consider the second case: $\theta < \sqrt{\log n}$. The set $\mathrm{Hom}^{\mathrm{hit}*}_{p,q}(\mathcal{A}, \mathcal{U})$ is hitting by Lemma 19 and Lemma 20.

We will be considering two subcases:

$$\mu \ > \ \log \log \log n \qquad \text{and} \qquad \mu \ \leq \ \log \log \log n \ .$$

In the first subcase

$$\log \theta \log \log \theta \ \leq \ (1 + \Theta(n)) \ ((\log \eta) + 2 \log \mu)^2 \ \leq$$

$$\leq \ (1 + \Theta(n)) \ \log^2 \eta \ \leq \ (1 + \Theta(n)) \ (\log \log \log \log n \ \log \mu)^2 \ \leq$$
$$\leq \ (1 + \Theta(n)) \ (\log \log \mu \log \mu)^2 \ \leq \ \Theta(n) \mu \ = \ \Theta(n) \log \frac{q}{p} \ .$$

Consequently by the Lemma 16 we have

$$| \ \mathrm{Hom}^{\mathrm{hit}}_{p,q}(\{0,1\}^{\theta}, \mathcal{U}) \ | \leq \ \left(\frac{q}{p} \right)^{1 + \Theta(n))} \ . \tag{33}$$

By the bounds of the Lemma 19 we have

$$| \ \mathrm{Hom}^{\mathrm{hash}}_{\mu,\eta}(\mathcal{A}, \{0,1\}^{\theta})) \ | \leq \ \mu^2 \eta \ (\log n)^{1 + 2(\log \mu)/ \log \eta} \ \leq$$

$$\leq \ \mu^{2 + \log \log \log \log n} (\log n)^{1 + \Theta(n)} \ \leq \ \mu^{2 + \log \mu} (\log n)^{1 + \Theta(n)} \ \leq$$
$$\leq \ \left(\frac{q}{p} \right)^{\Theta(n)} (\log n)^{1 + \Theta(n)} \ . \tag{34}$$

By multiplication (33) and (34) we have necessary bound.

In the second subcase also by Lemma 19 we have the following bounds

$$| \ \mathrm{Hom}^{\mathrm{hash}}_{\mu,\eta}(\mathcal{A}, \{0,1\}^{\theta})) \ | \leq \ \mu^2 \eta \ (\log n)^{1 + 2 \log k / \log m} \ \leq$$

$$\leq \ (\log\log\log n)^{2+\log\log\log\log n}(\log n)^{1+\Theta(n)} \ \leq \ (\log n)^{1+\Theta(n)} \ . \qquad (35)$$

It is easy to see, that in this subcase

$$| \ \mathrm{Hom}^{\mathrm{hash}}_{\mu,\eta}(\mathcal{A}, \{0,1\}^{\theta})) \ | \leq | \ \mathrm{Hom}(\mathcal{A}, \{0,1\}^{\theta})) \ | \leq$$

$$\leq \ k^{(2^{\theta})} \ \leq \ (\mu+1)^{\mu+1} \ = \ (\log n)^{\Theta(n)} \ . \qquad (36)$$

By multiplication (35) and (35) we have necessary bound.

□

Acknowledgments

The author thanks V.B.Kudrjavcev, A.A.Bolotov (Moscow university) and S.Skyum, S.Soloviev (Aarhus university) for very helpful discussions.

References

[1] Shennon, C.E. (1949), The synthesis of two-terminal swiching circuits, Bell. Syst. Tech. J. 28, pp.59-98.

[2] Jablonsky, S.V. (1957), About of classes of boolean functions with small complexity, Uspekhi Mat. Nauk 12, pp.1273-1276. (In Russian) Inglish translation in Russian Math. Surveys.

[3] Lupanov, O.B. (1956) About gating and contact-gating circuits, Dokl. Akad. Nauk SSSR 111, pp.1171-11744. (In Russian), English translation in Soviet Math. Docl.

[4] Lupanov, O.B. (1965) About a method circuits design – local coding principle, Problemy Kibernet. 10, pp.31-110. (in Russian). English Translation in Systems Theory Res. v.10, 1963.

[5] Nechiporuk, E.I. (1965), About the complexity of gating circuits for the partial boolean matrix, Dokl. Akad. Nauk SSSR 163, pp.40-42. (In Russian). English translation in Soviet Math. Docl.

[6] Sholomov, L.A. (1969) About realization of partial boolean functions by circuits from functional elements, Problemy Kibernet. 21, pp.215-226. (in Russian). English Translation in Systems Theory Res. v.21, 1971.

[7] Ugolnikov, A.B. (1976), Circuit design for monotone functions, Problemy Kibernet. 31, pp.167-185. (in Russian). English Translation in Systems Theory Res. v.21, 1971.

[8] Pippenger, N. (1977) Information theory and the complexity of Boolean functions, Math. Systems Theory 10, pp.129-167.

[9] Pippenger, N. (1978), The complexity of monotone boolean functions, Math. Systems Theory 11, pp.289-316.

[10] Andreev, A.E. (1985) A universal principle of self-correction, Mat. Sb. 127(169), pp.147-172.(In Russian), English translation in Math. USSR-Sb. 55, pp.145-169.

[11] Andreev, A.E. (1988), Circuit design in full monotone basis, Matem. Voprosy Kibernet. 1, pp.114-139. (In Russian).

[12] Andreev, A.E. (1989), On the complexity of the realization of partial Boolean functions by circuits of functional elements, Diskret. mat. 1, pp.36-45. (In Russian). English translation in Discrete Mathematics and Applications 1, pp.251-262.

[13] Andreev, A.E.(1994), Almost optimal hitting set. Dokl. Akad. Nauk RUSSIA (accepted).

[14] Krichevsky, R.E. (1994), Occam's Razor, Partially Specified Boolean Functions, String Matching, and Independent Sets, Inform. and Comput. 108, pp.158-174.

[15] Nisan, N. (1990), Pseudo-random generators for space-bounded computation, in "Proceedings of 22th ACM Symposium on Theory of Computation," pp.204-212.

[16] Sipser, M. (1986), Expanders, Randomness or Time vs. Space, in "Proceedings of 1th conference on Structure in Complexity Theory", Lecture Notes in Computer Science 223, pp.325-329.

[17] Chor, B., and Goldreich, O. (1989), On the power of Two-Point Based Sampling, J. Complexity 5, pp.96-106.

[18] Luby, M., and Velickovic, B. (1991), On deterministic approximation of DNF, in "Proceedings of 23th ACM Symposium on Theory of Computation," pp.430-438.

[19] Even, G., Goldreich, O., Luby, M., Nisan, N., and Velickovic, B. (1992), Approximation of general independent distributions, in "Proceedings of 24th ACM Symposium on Theory of Computation," pp.10-16.

[20] Linial, N., Luby, M., Saks, M., and Zuckerman, D. (1993), Efficient construction of a small hitting set for combinatorial rectangles in high dimension, in "Proceedings of 25th ACM Symposium on Theory of Computation," pp.258-267.

[21] Karpinski, M., and Luby, M. (1993), Approximating the number of solutions to a GF(2) Formula, J. Algorithms, 14, pp.280-287.

[22] Markowsky, G., Carter, J.L., and Wegman, M.N. (1978) Analysis of a universal class of hash functions, Lecture Notes in Computer Science 64, pp.345-354.

[23] Carter, J.L., and Wegman, M.N. (1979) Universal Classes of Hash Functions, J. Comput. System Sci. 18, pp.143-154.

[24] Poljak,, S., Pultr, A., and Rodl V. (1983), On qualitatively independent partitions and related problems, Discrete Appl. Math. 6, pp.193-205.

[25] Krichevsky, R.E. (1985), Optimal hashing, Inform. and Control 62, pp.64-92.

Figures

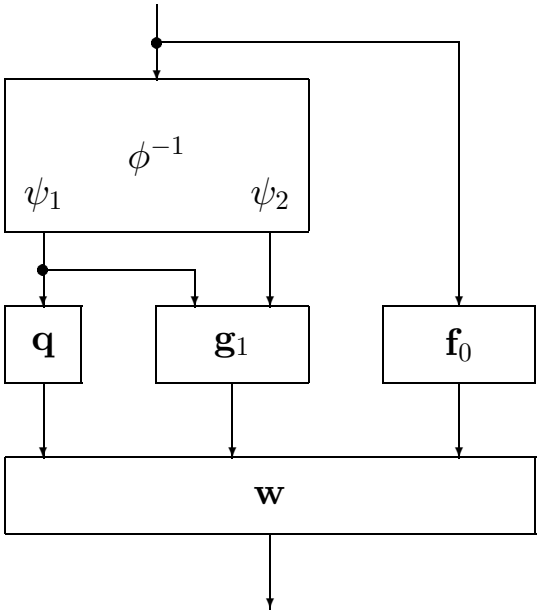

Figure 1

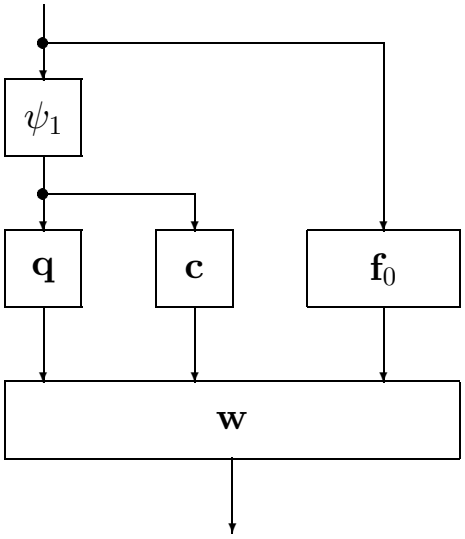

Figure 2

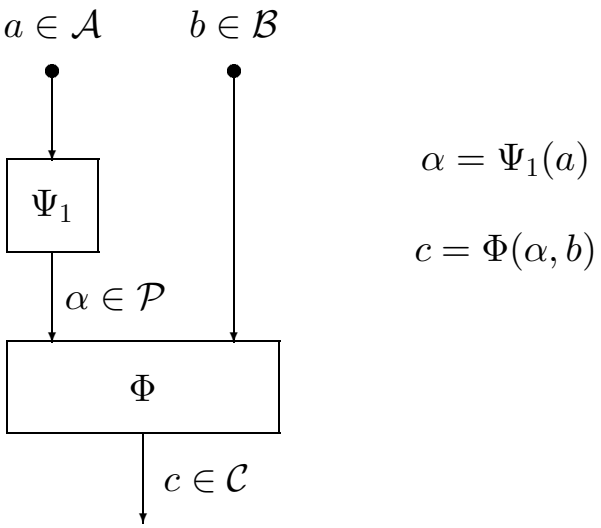
$a \in \mathcal{A}$
$b \in \mathcal{B}$
Ψ_1
$\alpha \in \mathcal{P}$
Φ
$c \in \mathcal{C}$
$\alpha = \Psi_1(a)$
$c = \Phi(\alpha, b)$

Figure 3

Recent Publications in the BRICS Report Series

RS-94-1 **Glynn Winskel.** ***Semantics, Algorithmics and Logic: Basic Research in Computer Science. BRICS Inaugural Talk*****. February 1994, 8 pp.**

RS-94-2 **Alexander E. Andreev.** ***Complexity of Nondeterministic Functions*****. February 1994, 47 pp.**

RS-94-3 **Uffe H. Engberg and Glynn Winskel.** ***Linear Logic on Petri Nets*****. February 1994, 54 pp.**

RS-94-4 **Nils Klarlund and Michael I. Schwartzbach.** ***Graphs and Decidable Transductions based on Edge Constraints*****. February 1994, 19 pp. Appears in:** ***Trees in Algebra and Programming CAAP '94*** **(ed. S. Tison), LNCS 787, 1994.**

RS-94-5 **Peter D. Mosses.** ***Unified Algebras and Abstract Syntax*****. March 1994, 21 pp. To appear in:** ***Recent Trends in Data Type Specification*** **(ed. F. Orejas), LNCS 785, 1994.**

RS-94-6 **Mogens Nielsen and Christian Clausen.** ***Bisimulations, Games and Logic*****. April 1994, 37 pp. Full version of paper to appear in:** ***New Results and Trends in Computer Science*****, LNCS, 1994.**