THE EFFECT OF NULL-CHAINS ON THE COMPLEXITY OF CONTACT SCHEMES

Stasys P. Jukna

Institute of Mathematics and Cybernetics
Lithuanian Academy of Sciences
232600 Vilnius, MTP-1
Akademijos str., 4
Lithuania, USSR

Abstract

The contact scheme complexity of Boolean functions has been studied for a long time but its main problem remains unsolved: we have no example of a simple function (say in NP) that requires $\Omega(n^3)$ contact scheme size. The reason is, perhaps, that although the contact scheme model is elegantly simple, our understanding of the way it computes is vague.

On the other hand, it is known (see, e.g. [2,3]) that the main tool to reduce the size of schemes is to use "null-chains", i.e. chains with zero conductivity.(These chains enable one to merge non-isomorphic subschemes). So, in order to better understand the power of this tool, it is desirable to have lower bound arguments for schemes with various restrictions on null-chains.

In this report such an arguments are described for schemes without null-chains (Theorems 1-2), for schemes with restricted topology of null-chains (Theorem 3), and for schemes with restricted number and/or restricted length of null-chains (Theorem 4). In all these cases nearly-exponential lower bounds are established. Finally, we prove that null-chains do not help at all if schemes are required to realize sufficiently many prime implicants (Theorem 5).

1. Preliminaries

We deal with the standard model of contact schemes but we need some notations. Fix some set of Boolean variables $\mathbb{X}^+ = \{x_1,\dots,x_n\}$ and their negations $\mathbb{X}^- = \{\neg x_1,\dots,\neg x_n\}$. The elements of $\mathbb{X} = \mathbb{X}^+ \cup \mathbb{X}^-$ are called <u>contacts</u>. A contact scheme S is a labelled digraph with two distinguished nodes (the source and the output), and edges labelled by contacts. The <u>size</u> of S, size(S), is the number of edges in S. A chain is (a sequence of edges in)a path from the source to output. A <u>subchain</u> is a subsequence of (not necessarily consecutive) edges in a chain. A <u>cut</u> is a minimal set of edges which contains an edge from each chain. We will often identify a chain [cut] A with the set $A \subseteq \mathbb{X}$ of contacts it consists of; the current meaning will be clear from the context. A chain [cut] $A = \{y_1,\dots,y_m\} \subseteq \mathbb{X}$ (m ≤

2n) defines the monomial $K_A = \&_{i=1}^{m} y_i$ [the clause $D_A = \bigvee_{i=1}^{m} y_i$]. A chain [cut] A is <u>redundant</u> if $K_A \equiv 0$ [$D_A \equiv 1$]. Thus a chain (as well as a cut) is redundant iff it contains some pair of contrary contacts x_i and $\neg x_i$. Redundant chains [cuts] are also called <u>null-chains</u> [<u>one-cuts</u>]. A contact scheme <u>computes</u> a Boolean function f_S iff

$$f_S = \bigvee\{ K_A : A \text{ is a chain of } S \},$$

or equivalently, iff

$$f_S = \& \{ D_A : A \text{ is a cut of } S \}.$$

We will also need the following notions from extremal set theory. Let $\mathcal{F}$ be a family of subsets of a finite set N . For an integer i ($0 \le i \le |N|$), put

$$\#_i\mathcal{F} = \max \{ |\mathcal{G}| : \mathcal{G} \subseteq \mathcal{F} \text{ and } |\bigcap_{A\in\mathcal{G}} A| \ge i \}$$

i.e. $\#_i\mathcal{F}$ is the maximum number of sets in $\mathcal{F}$ that have at least i elements in common. Thus

$$|\mathcal{F}| = \#_0\mathcal{F} \ge \#_1\mathcal{F} \ge \dots \ge \#_{|N|}\mathcal{F} = 1 .$$

The rate to which $\#_i\mathcal{F} \longrightarrow 1$ as $i \longrightarrow |N|$ characterizes the "dispersion" of elements from N over the subsets of $\mathcal{F}$.

A family $\mathcal{F}$ is (t,r)-<u>dispersed</u> if

$$\#_i\mathcal{F} / \#_{i+1}\mathcal{F} \ge t \quad \text{for all } i = 0,1,\dots,r-1.$$

A family $\mathcal{F}$ is (k,r)-<u>disjoint</u> ($k\ge2, r\ge0$) if $\#_r\mathcal{F} \le k - 1$. Notice that any (t,r)-dispersed family is also (k,r)-disjoint with $k = |\mathcal{F}|\cdot t^{-r}$.

In this report we show that for any sufficiently dispersed family $\mathcal{F}_o \subseteq 2^N$, the characteristic function $f_{\mathcal{F}} : 2^N \to \{0,1\}$ of any family $\mathcal{F} \subseteq 2^N$, given by

$$A \in \mathcal{F} \iff \exists B \in \mathcal{F}_o : A \supseteq B ,$$

requires super-polynomial size to be computed by contact schemes with various restrictions on null-chains and one-cuts. The consequence is that, under these restrictions, almost all NP-complete functions require super-polynomial contact scheme size.

2. Schemes Without Null-Chains

For a Boolean function f, let $L^*(f)$ denote the minimum size of a contact scheme without null-chains computing f .

The first non-trivial lower bound for π-schemes without null-chains has been proved by A.K. Pulatov in [8] and improved to contact schemes by S.E. Kuznetsov in [6]. Somewhat later similar results have been obtained for one-time-only branching programs - a special type of contact sheme without null-chains - by now a long list of authors (see, e.g. references in [3] or [12]).

Associate with a Boolean vector $\alpha = (\alpha_1, \ldots, \alpha_n)$ the set of contacts $N_\alpha = \{x_1^{\alpha_1}, \ldots, x_n^{\alpha_n}\} \subset \mathbb{X}$ where $x^1 = x$ and $x^0 = \neg x$, and put $\mathbb{N}_f = \{ N_\alpha : \alpha \in f^{-1}(1) \}$. Let

$$d(f) = 1 + \min \{ r : \mathbb{N}_f \text{ is } (2,n-r)\text{-disjoint} \} .$$

Notice that $d(f)$ is actually the minimal Hamming distance between any two vectors in $f^{-1}(1)$.

Theorem 1 (Pulatov [8], Kuznetsov [6]): For any Boolean function f

$$L^*(f) \geq |\mathbb{N}_f|^{d(f)/n} .$$

The theorem enables to obtain non-trivial lower bounds for functions f with $d(f)$ large enough with respect to $|\mathbb{N}_f|$. Recently, S.V. Zdobnov has announced in [13] the following improvement of this result.

Theorem 2 (Zdobnov [13]): If $d(f) \geq 3$ then

$$L^*(f) \geq |\mathbb{N}_f| . n^{(1/2-\varepsilon)\log n} \cdot 2^{-n} .$$

The theorem already yields super-polynomial lower bounds for some functions f with small $d(f)$, including the characteristic function of the Hamming code. Unfortunately, this argument (as well as Theorem 1) does not work for functions f with small $|\mathbb{N}_f|$.

Example 1 : Let $m \geq 2$ be a prime power and let $1 \leq s \leq m/2$. The Galois function is the following function $g_{m,s}(X)$ of $n=m^2$ Boolean variables $X = \{ x_{i,j} : i,j \in GF(m) \}$:

$g_{m,s}(X) = 1$ iff there exists a polynomial σ of degree at most $s-1$ over the Galois field $GF(m)$ such that $\forall i,j \in GF(m) \quad x_{i,j} = 1$ iff $j = \sigma(i)$.

Since $d(g) \leq 2m$, we have that

$$|\mathbb{N}_g|^{d(g)/n} \leq m^2 = n \qquad \text{and} \qquad \log |\mathbb{N}_g| = s\log m = o(n),$$

and therefore, both arguments fail for g, whereas it is known (see [2]) that $L^*(g_{m,s}) \geq m^s$.

So, even for schemes without null-chains new arguments are desirable. General technique for schemes with restrictions on the topology of null-chains have been proposed in [2,3]. Let us briefly describe a modification of this argument .

3. Schemes With Free Subchains

Let $\mathcal{R}(S)$ be the set of all subchains in a contact scheme S . For $A\in\mathcal{R}(S)$, let $ext(A) = \{ C\in\mathcal{R}(S) : A\cup C$ is a chain in S $\}$ be the set of all extentions of A in S, and let $sp(S) = \{ B\in\mathcal{R}(S) : ext(B) = ext(A) \}$ be the "span" of A in S. For families of sets $\mathcal{F}$ and $\mathcal{G}$, set $\mathcal{F}\otimes\mathcal{G} = \{A\cup B : A\in\mathcal{F}$ and $B\in\mathcal{G} \}$. A subchain $A \in \mathcal{R}(S)$ is called to be <u>free</u> in S if it produces no new null-chain, i.e. if

$$\forall\ C \in ext(A) : \qquad K_C \neq 0 \ \Rightarrow\ K_{A\cup C} \neq 0 .$$

A collection of subchains $\mathcal{A} \subseteq \mathcal{R}(S)$ is a <u>separator</u> of S if

$$S_{\emptyset} = \bigcup_{A\in\mathcal{A}} S_A \quad \text{and} \quad |\mathcal{A}| \leq size(S).$$

where $S_A = sp(A) \otimes ext(A)$ (and hence, $S_{\emptyset}$ is the set of all chains in S). A separator $\mathcal{A}$ is an [a,b]-separator if $a \leq |A^+| \leq b$ for all $A\in\mathcal{A}$. (Throughout, A^+ stands for the set of all unnegated variables (not edges !) in a subchain A). Thus, any cut defines an obvious [0,1]-separator. Moreover, any scheme has at least one [a,b]-separator for any $0 \leq a \leq b \leq \min\{|A^+| : A\in S_{\emptyset} \}$.

We call a contact scheme S to be [a,b]-<u>separable</u> if there exists an [a,b]-separator $\mathcal{A}$ of S such that all $A\in\mathcal{A}$ are free in S . Let $L_{a,b}(f)$ denote the minimum size of an [a,b]-separable contact scheme computing f . It is clear that for all $a \leq b$

$$L^*(f) \geq L_{a,b}(f).$$

Let $\mathbb{N}_f(m) \subseteq \mathbb{N}_f$ be the m-th slice of f , i.e $\mathbb{N}_f(m) = \{ A\in\mathbb{N}_f : |A^+| = m \}$. A function f is called $(k,r)_m$-<u>disjoint</u> if the following two conditions are fulfilled :

(i) $\quad \#_r\{ A^+ : A \in \mathbb{N}_f(m) \} \leq k-1$,

(ii) $\quad$ if $A \in \mathbb{N}_f$ but $A \notin \mathbb{N}_f(m)$ then $|A^+| \geq 2m$.

Theorem 3 : If f is $(k,r)_m$-disjoint for some $k\geq 2$ and $m\geq 2r\geq 0$ then

$$L_{r,m-r}(f) \geq |\mathbb{N}_f(m)|\cdot(k-1)^{-2}$$

Proof : Let S be an [r,m-r]-separable scheme computing f, and let $\mathcal{A} \subseteq \mathcal{R}(S)$ be the corresponding free separator of S . Notation: for a set of chains $\mathcal{C}$ we will write $||\mathcal{C}||$ instead of $|\mathcal{C} \cap \mathbb{N}_f(m)|$. Then

$$|\mathbb{N}_f(m)| = ||S_\emptyset|| \le \sum_{A\in\mathcal{A}} ||S_A|| \le \delta\ |\mathcal{A}| \le \delta\ \mathrm{size}(S)\ ,$$

where

$$\delta = \max\left\{ \ ||S_A|| \ :\ A\in\mathcal{A} \right\}.$$

So it remains to prove that $\delta \le (k-1)^2$. Take $A\in\mathcal{A}$. Then $r\le|A^+|\le m-r$ and A is free in S. Consider $\mathrm{Ext} = \{\ C \in \mathrm{ext}(A)\ :\ ||\mathrm{sp}(A)\otimes\{C\}|| \ge 1\ \}$. Ext is the set of all the extentions of A that are used to compute the m-th slice of f . Other extentions of A are of no interest for us since

$$||S_A|| = ||\mathrm{sp}(A)\otimes\mathrm{Ext}|| \ .$$

Let $\mathcal{D} := (\{A\}\otimes\mathrm{Ext}) \cap \mathbb{N}_f(m)$. Then $|\mathcal{D}| \le k-1$ since $|\cap\{D^+ : D\in\mathcal{D}\ \}| \ge |A^+| \ge r$. The crucial observation is that $\mathcal{D} = \{A\}\otimes\mathrm{Ext}$. This follows from (ii) because if $B = A\cup C$ with $C\in\mathrm{Ext}$, then $K_B \ne 0$ and $|B^+| \le |A^+| + |C^+| \le (m-r)+m \le 2m$. Hence, Ext may be partitioned into $|\mathcal{D}| \le k-1$ pairwise disjoint subsets $\mathrm{Ext}_D = \{\ C\in\mathrm{Ext}\ :\ A\cup C = D\ \}$, $D\in\mathcal{D}$. By (i) we have, for each $D\in\mathcal{D}$, that $||\mathrm{sp}(A)\otimes\mathrm{Ext}_D|| \le k-1$ because

$$|\cap\ \{C^+\ :\ C\in\mathrm{Ext}_D\ \}| \ge |D^+\setminus A^+| \ge m-(m-r) = r\ .$$

Therefore, $\delta \le |\mathcal{D}|(k-1) \le (k-1)^2$ and the theorem follows. ∎

The class of schemes without null-chains is not closed under the negation in a sense that $L^*(\neg f) \ll L^*(f)$ for some f . Let, for example, $\mathfrak{p}_n$ be the function of $n = m^2$ Boolean variables representing the elements of an mxm-matrix M, whose value is 1 iff each row and each column of M has exactly one 1. Then $|\mathbb{N}_{\mathfrak{p}}^+| = m!$ and, therefore, $\mathfrak{p}_n$ is $(k,r)_m$-disjoint for $r = m/2$ and $k = r!$. By Theorem 3, $L^*(\mathfrak{p}_n) \ge \exp(\Omega(\sqrt{n}))$, whereas one may easily verify that

$$L^*(\neg\mathfrak{p}_n) = O(n^{3/2}).$$

On the other hand, Theorem 3 enables one to construct an explicit functions f such that both f and ¬f are hard to compute by schemes without null-chains.(Notice that Theorems 1 and 2 both fail in this situation, because $d(\neg f) = 1$ for any function f with $d(f) \ge 3$).

Example 2 : Define the function $f_{m,s}$ of $n = m^2$ variables by :

$$f_{m,s}(\alpha)=\begin{cases} g_{m,s}(\alpha) & \text{if} \quad 0 \le |N_\alpha| < n/2, \\ g^*_{m,s}(\alpha) & \text{otherwise,} \end{cases}$$

where f^* stands for the dual of f, i.e. $f^* = \neg f(\neg x_1,,,.\neg x_n)$.

Since f is $(2,s)_m$-disjoint and self-dual (i.e. $f = f^*$), Theorem 3 immediately yields the following lower bound.

Corollary 1 : $\min\left\{ L_{s,m-s}(f),\ L_{s,m-s}(\neg f) \right\} \ge m^s.$

Specifically, both f and $\neg f$ are hard to compute if null-chains are forbidden

4. Schemes With Long Null-Chains

As we have seen above, there is an exponential gap between the complexity of schemes with and without null-chains. This means that although the usedge of null-chains and one-cuts has no influence on the function computed, such chains and cuts may lead to great reduction of size.

In this section we will show that null-chains and one-cuts do not help in both of the following situations:

(i) if we restrict the number of null-chains and one-cuts in a scheme, or

(ii) if we do not use "very short" null-chains or one-cuts.

Given a contact scheme S, let $\mathfrak{m}(S)$ $[\mathfrak{m}^\perp(S)]$ denote the number of all minimal subsets $A^+ \subseteq X^+$ where A ranges over all null-chains [one-cuts] in S . (Recall that A^+ is the set of unnegated variables in A). Let $\mathfrak{l}(S)$ $[\mathfrak{l}^\perp(S)]$ stand for $\min|A^+|$ where A ranges over all null-chains [one-cuts] in S . Thus for any contact scheme S , we have that

$$0 \le \mathfrak{l}(S) \le n \quad \text{and} \quad 0 \le \mathfrak{m}(S) \le \binom{n}{\mathfrak{l}}.$$

Define

$$L_{\mu,\lambda}(f) = \min\left\{ \text{size}(S) : S \text{ computes } f \text{ and } \mathfrak{m}(S) \le \mu \text{ and } \mathfrak{l}(S) \le \lambda \right\}.$$

In case of one-cuts we will write $L^\perp$ instead of L .Notice that $L_{\mu,\lambda}(f) = L(f)$, the unrestricted contact scheme complexity of f, if either $\lambda = n$ or $\lambda < n$ but $\mu = \binom{n}{\mathfrak{l}}$.

We will estimate these complexity functionals in terms of the dispersion of minterms and maxterms. A <u>minterm</u> [<u>maxterm</u>] of a Boolean function f is a minimal set, of contacts $A \subseteq \mathbb{X}$ such that

$$f \geq \underset{y\in A}{\&}\, y \neq 0 \qquad \left[\ f \leq \bigvee_{y\in A} y \neq 1\ \right].$$

Define $\mathit{min}(f)$, $\mathit{Max}(f)$ as the set of minterms, respectively maxterms of f . Let $\mathfrak{r}(f)$, $\mathfrak{R}(f)$ denote the minimum cardinality of a set in $\mathit{min}(f)$, respectively in $\mathit{Max}(f)$.

For integers $t,r \geq 1$ and real numbers $p,\aleph \in [0,1]$, let $H_f(t,r,p,\aleph)$ denote the following number:

$$H_f = t^{-r/2} \min\left\{ \Delta_f(r/2)\ ,\ \left[1- \aleph - \#_0\mathit{min}(f)p^{\mathfrak{r}(f)}\right]2^{tp^r - r\log\sqrt{t}} \right\},$$

where

$$\Delta_f(i) = \max_{\mathcal{F}} \left[\#_0\mathcal{F} \,/\, \#_i\mathcal{F}\right]$$

and $\mathcal{F}$ ranges over all (t,r)-dispersed subfamilies $\mathcal{F} \subseteq \mathit{min}(f)$.

Theorem 4 : For any monotone Boolean function f , the following bound holds:

$$L_{\mu,\lambda}(f) \geq \max_{p\in[0,1)} H_f(t,r,p,\aleph)$$

where

$$\aleph = \min\left\{ \mu p^{\lambda}\ ,\ np/\lambda \right\}.$$

The same bound holds also for $L^{\perp}_{\mu,\lambda}(f)$ with $\mathit{min}(f)$ and $\mathfrak{r}(f)$ replaced by $\mathit{Max}(f)$ and $\mathfrak{R}(f)$.

Proof (sketch): Let S be a minimal contact scheme computing f with $\mathfrak{m}(S) \leq \mu$ and $\mathfrak{l}(S) \leq \lambda$. Replace in S all the negated contacts by constant 1 (or by 0 in case of one-cuts). Let f^+ be the monotone function computed by the resulting scheme S^+. Then $\text{size}(S) \geq \text{size}(S^+)$ and $f^+ \geq f$. From ([4], Theorem 4) it follows that

$$\text{size}(S^+) \geq \max_{p\in[0,1)} H_{f^+}(t,r,p,\aleph_+),$$

where

$$\aleph_+ = \text{Prob}\left[\ K_A \leq f^+\&\neg f\ \right] \leq \text{Prob}\left[\ K_A \leq f^+\ \right]$$

and $A \subseteq \{x_1,\ldots,x_n\}$ is a random monomial in which each variable x_i appears independently and with equal probability $p\in[0,1)$.

Let g be the disjunction of all the monomials in $min(f^+)\setminus min(f)$. Then $f^+ = f \vee g$, $\mathfrak{r}(g) \geq \mathfrak{l}(S)$ and $\#_0 min(g) \leq \mathfrak{m}(S)$. So,

$$\aleph_+ \leq \text{Prob}\left[K_A \leq f \right] + \text{Prob}\left[K_A \leq g \right].$$

It remains to notice that for any monotone f, we have that

$$\text{Prob}\left[K_A \leq f \right] \leq \#_0 min(f)\ p^{\mathfrak{r}(f)}$$

and, by Chebyshev's inequality,

$$\text{Prob}\left[K_A \leq f \right] \leq \text{Prob}\left[|A| \geq \mathfrak{r}(f) \right] \leq np/\mathfrak{r}(f). \quad \blacksquare$$

Example 3: Let f_n be the monotone function of $n = \binom{m}{2}$ Boolean variables representing the edges of an undirected graph G, which is 1 iff G contains an s-clique where $s = \lceil (m/\ln m)^{2/3} \rceil$. Then $\#_i min(f_n) = \binom{m-i}{s-i}$, and hence $min(f_n)$ is (t,r)-dispersed for any $t \leq \lceil m/3 \rceil$ and $r \leq s$.

Corollary 2 : If $\lambda = \Omega(n^{1-1/s})$ or $\mu \leq (1-\varepsilon)n^{\lambda/s}$, $\varepsilon > 0$, then

$$L_{\mu,\lambda}(f_n) \geq \exp(\Omega(n^{1/6-o(1)})).$$

Proof: Take $r = \lceil \sqrt{s} \rceil$, $t = \lceil 4r \ln m \rceil$ and $p = m^{-2/s}$. Then $\#_0 min(f) p^{\mathfrak{r}(f)} \leq \binom{m}{s} p^{s^2} < m^{-s}$, and by Theorem 4, the bound holds for any μ,λ such that $\min\{\mu p^{\lambda}, np/\lambda\} \leq const < 1$. $\blacksquare$

Example 4 : Define

$$g_n^+ = \mathop{\&}_{\sigma \in \Pi} \bigvee_{i \in GF(m)} x_{i,\sigma(i)}$$

where Π is the set of all polynomials over GF(m) of degree at most s-1, and $s = \lceil \ln m \rceil$. As $\#_i Max(g_n^+) = m^{s-i}$, the family $\#_i Max(g_n^+)$ is (t,r)-dispersed for any $t \leq m/3$ and $r \leq s$.

Corollary 3: If $\lambda = \Omega(n)$ or $\log_2 \mu \leq O(\lambda)$ then

$$L^{\perp}_{\mu,\lambda}(g_n^+) \geq n^{\Omega(\log n)}.$$

Proof: Take $t = \lceil \sqrt{m} \rceil$, $r = \lceil s/2 \rceil$ and $p = (t^{-1}\ln^2 t)^{1/s}$, and apply Theorem 4. ∎

This bound is almost tight because g_n^+ is computable by a trivial contact scheme S with $\mathfrak{m}^{\perp}(S) = 0$ and $size(S) \le n^{\log n}$.

Theorem 4 yieds also the following criterion for the monotone scheme complexity $L^+(f)$. For a random monomial $\mathcal{A} \subseteq \mathbb{X}^+$, put

$P_{\mathcal{A}}(r) = \max\left\{ \text{Prob} [\mathcal{A} \supseteq B] : B \subseteq \mathbb{X}^+ \text{ and } |B| = r \right\}.$

We say $\mathcal{A}$ islocally independent if for any two monomials $B_1, B_2 \subseteq \mathbb{X}^+$, the events $\{ \mathcal{A} \supseteq B_i \mid \mathcal{A} \supseteq B_1 \cap B_2 \}$ are independent. We say f is (t,r)-good if there exists a locally independent monomial $\mathcal{A}$ such that

$$\text{Prob} [K_{\mathcal{A}} \le f] \le \text{const} < 1 \quad \text{and} \quad P_{\mathcal{A}}(r) \gg t^{-1} \ln \Delta_f(r).$$

Criterion: If f is (t,r)-good and $min(f)$ is (t,r)-dispersed for some t and r such that $\ln t \ll r^{-1} \ln \Delta_f(r)$, then

$$L^+(f) \ge \Delta_f(r) t^{-r} .$$

5. Shemes With Necessary Minterms

For a contact scheme S, let f_S denote the Boolean function it computes, and let $\mathcal{D}_S$ denote the set of all monomials corresponding to non-null chains of S. A minterm $\mathcal{A} \in min(f)$ is <u>necessary</u> if there exists a vector $\alpha \in \{0,1\}^n$ with $K_{\mathcal{A}}(\alpha) = 1$ but $K_{\mathcal{B}}(\alpha) = 0$ for all other minterms $\mathcal{B} \in min(f) - \{\mathcal{A}\}$. (These minterms belong necessarily to each shortest DNF of f). Define $nec(f)$ as the set of all necessary minterms of f .

A contact scheme S is called to be a δ-<u>scheme</u> ($\delta \in [0,1]$) if

$$|\mathcal{D}_S \cap nec(f_S)| \ge \delta \, |nec(f_S)|,$$

i.e. if S realizes at least δ fraction of all the necessary minterms of f_S . A scheme S is ω-<u>scheme</u> if

$$nec(f_S) \subseteq \mathcal{D}_S \subseteq min(f_S).$$

Note that any scheme is δ-scheme for some $\delta \in [0,1]$. An ω-scheme is a special type of δ-scheme for $\delta = 1$.

For $\delta \in [0,1] \cup \{\omega\}$, let $L_\delta(f)$ denote the minimum size of a δ-scheme computing f . Thus, $L_0(f)$ is the unrestricted contact scheme complexity of f .

The functional $L_\delta(f)$ has been studied for a long time. The first non-trivial result in this direction has been obtained by E. A. Okol'nishnikova in [7], where a sequence of functions $f_n(x_1,\dots,x_n)$ is given such that

$$L_1(f_n) \le 2n \qquad \text{but} \qquad L_\omega(f_n) \ge \exp(\Omega(n^{1/4})) .$$

The next major development was made by A. A. Razborov [9,10] and A. E. Andreev [1] where super-polynomial lower bounds for $L^+(f)$, the monotone scheme complexity of f, have been proved . One may transfere these bounds also to $L_1(f)$, because any minimal 1-scheme for monotone f has no null-chains, and therefore $L_1(f) = L^+(f)$.

However, we have seen before that the presence of null-chains may substantially reduce the size of schemes (see also [2,3,6,8-11]). Thus we need a technique to prove lower bounds for $L_\delta(f)$ with $\delta < 1$, as well as for $L_1(f)$ and non-monotone f (in these cases null-chains may be used in a non-trivial manner to reduce the size of schemes).

We say f is $(t,r)_\delta$-dispersed if each sub-family $\mathscr{A} \subseteq nec(f)$ with $|\mathscr{A}| \ge \delta\,|nec(f)|$ is a (t,r)-dispersed family.

Using an extention of Andreev-Razborov argument [1,9] to non-monotone circuits, given in [4,5], one may prove the following lower bound. Let H^*_f stand for H_f with $min(f)$ replaced by $nec(f)$.

Theorem 5: For any $\delta \in [0,1]$ and any $(t,r)_\delta$-dispersed Boolean function f , we have that

$$L_\delta(f) \ge \delta \min_{p\in[0,1)} H^*_f(t,r,p,0).$$

Example 5: Let us consider the following non-monotone version of $\mathfrak{g}_n^+$ (see Example 4):

$$\mathfrak{h}_n = \bigvee_{\sigma\in\Pi} K_\sigma \qquad \text{where} \qquad K_\sigma = \mathop{\&}_{i\in GF(m)} (x_{i,\sigma(i)} \,\&\, \neg x_{i,\sigma(i)\oplus 1}) .$$

Then $nec(\mathfrak{h}_n) = \{ K_\sigma : \sigma \in \Pi \}$ and $\mathfrak{h}_n$ is $(t,r)_\delta$-dispersed for any $t \le \delta m/3$ and $r < s$ ([5]). Taking t,r and $p\in[0,1)$ as in Corollary 3, we obtain from Theorem 5 the following lower bound.

Corollary 4 :For any $\delta \geq n^{-\sigma(\log n)}$, and hence, for any constant $\delta \in (0,1]$, we have that

$$L_{\delta}(\mathfrak{h}_n) \geq n^{\Omega(\log n)} .$$

Thus, for an arbitrary small constant $\delta \in (0,1]$, the δ-scheme size of $\mathfrak{h}_n$ is almost the same as the size $|nec(\mathfrak{h}_n)| = \mathcal{O}(n^{\log n})$ of its shortest DNF $nec(\mathfrak{h}_n)$, and so, if $\delta \geq$ const>0 then, for some Boolean functions, null-chains do not help at all.

References

[1] A. E. Andreev, On one method of obtaining lower bounds of individual monotone function complexity, Dokl. Akad. Nauk SSSR, 282 (1985).

[2] S. P. Jukna, Lower bounds on the complexity of local circuits, Springer Lecture Notes in Comput. Sci., 233 (1986).

[3] S. P. Jukna, Entropy of contact circuits and lower bounds on their complexity, Theoretical Computer Science, 57, n.1 (1988).

[4] S. P. Jukna, Two lower bounds for circuits over the basis (&,V,¬), Springer Lecture Notes in Comput. Sci., 324 (1988).

[5] S. P. Jukna, Method of approximations for obtaining circuit size lower bounds, Preprint n.6 (Vilnius, 1988).

[6] S. E. Kuznetsov, The influence of null-chains on the complexity of contact circuits, in : Probabilistic Methods in Cybernetics, 20 (Kazan, 1984).

[7] E. A. Okol'nishnikova, On the influence of one type of restrictions to the complexity of combinational circuits, in : Discrete Analysis, 36 (Novosibirsk, 1981).

[8] A. K. Pulatov, Lower bounds on the complexity of implementation of characteristic functionds of group codes by π-schemes, in : Combinatorial-Algebraic Methods in Applied Mathematics (Gorki, 1979).

[9] A. A. Razborov, Lower bounds on the monotone complexity of some Boolean functions, Dokl. Akad. Nauk SSSR, 281 (1985).

[10] A. A. Razborov, A lower bound on the monotone network complexity of the logical permanent, Mat. Zametki,37,n.5 (1985).

[11] E. Tardos, The gap between monotone and non-monotone circuit complexity is exponential, Combinatorica 7 (1987).

[12] I. Wegener, The complexity of Boolean functions, Wiley-Teubner, 1987.

[13] S. V. Zdobnov, Lower bounds on the complexity of schemes without null-chains, in : Proc. 9th All-Union Conf. on Math. Logic (Leningrad, 1988).