Threshold Circuit based on Cyclic Codes

Syril Corneille Tchio Tchichelia, Hervé Talé Kalachi, Jules Waku, René Ndoundam

Threshold Circuit based on Cyclic Codes

Syril Corneille Tchio Tchichelia, Hervé Talé Kalachi,
Jules Waku and René Ndoundam
Department of Computer Sciences, University of Yaoundé 1,
P.O.Box 812 Yaoundé , Cameroon.
UMI 209 IRD - UPMC, UMMISCO, Bondy, France.
Department of Computer Engineering, National Advanced School of
Engineering-Yaoundé, University of Yaoundé 1, Cameroon.
E.mail: rene.ndoundam@facsciences-uy1.cm

Abstract

We study the model of a threshold circuit. By using the parity-check matrix:

- Firstly, we build a threshold circuit that recognizes the words belonging to a cyclic code C.
- Secondly, we build a threshold circuit that recognizes the words belonging to the set $C_1 \cap \overline{C_2}$, where C_1 and C_2 are cyclic codes.
- Thirdly, we build a threshold circuit that recognizes the words belonging to a symmetric difference of two cyclic codes.

We use these functions to characterize the followings sets: TC_4^0, TC_5^0 and TC_6^0.

Keywords: Threshold Circuit, Words, Symmetric Difference, Functions, Cyclic code, Parity-check Matrix.

1 Introduction

Let $\mathbb{B} = \{0,1\}$. A function f from $\mathbb{B}^n$ to $\mathbb{B}$ is a boolean function on n variables and a single value, in other terms:

$$f : \mathbb{B}^n \longrightarrow \mathbb{B}$$
$$x = (x_1, x_2, \cdots, x_n) \longmapsto y$$

A *circuit* is a directed acyclic graph. The sources are called *input nodes* and are labeled with 0, 1, $x_1, x_2, \cdots, x_n$. Non-input nodes are called gates and are labeled by boolean functions, whose arity is the in-degree of the nodes. The in-degree (out-degree) of a gate is called the *fan-in* (*fan-out*). Sink nodes have fan-out 0 and are called *output nodes* [1].

A threshold circuit C is a boolean circuit where each gate computes a threshold function. Threshold circuits are studied in Complexity Theory and Neural Networks [2].

A threshold function is a function that takes the value 1 if a specified function of the arguments exceeds or egals a given threshold and 0 otherwise.

The size of a circuit is the number of gates, while the depth is the length of the longest path from an input to an output node. Let us note $\alpha = (\alpha_1, \cdots, \alpha_n)$. The following basic functions (***threshold functions***) arise in the study of circuits:

$$T_k^{\alpha}(x_1, x_2, \cdots, x_m) = \begin{cases} 1, & if \quad \sum_{i=1}^{m} \alpha_i x_i \geq k; \\ \\ 0, & if \quad \sum_{i=1}^{m} \alpha_i x_i < k \end{cases} \tag{1}$$

When $\alpha = (1, 1, \cdots, 1)$, we also have the following threshold function:

$$TH_k^n(x_1, x_2, \cdots, x_n) = \begin{cases} 1, & if \quad \sum_{i=1}^{n} x_i \geq k; \\ \\ 0, & if \quad \sum_{i=1}^{n} x_i < k \end{cases} \tag{2}$$

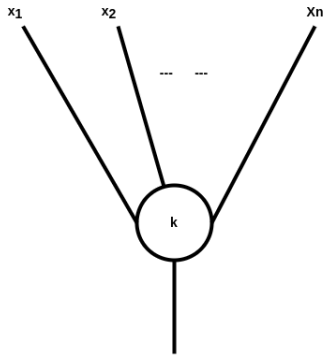

Figure 1: A threshold circuit computing the function $TH_k^n(x_1, x_2, \cdots, x_n)$.

The equal function is defined as follows:

$$EQUAL(x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_n) = \begin{cases} 1, & if\ x_i = y_i\ \forall\ 1 \leq i \leq n; \\ \\ 0, & \exists\ i\ \ 1 \leq i \leq n\ such\ that\ x_i \neq y_i \end{cases} \tag{3}$$

A boolean function f is symmetric if and only if

$$f(x_1, x_2, \cdots, x_n) = f(x_{\alpha(1)}, x_{\alpha(2)}, \cdots, x_{\alpha(n)})$$

for any permutation α on the set $\{1, 2, \cdots, n\}$.

Hajnal et al. [3] shown the following result:

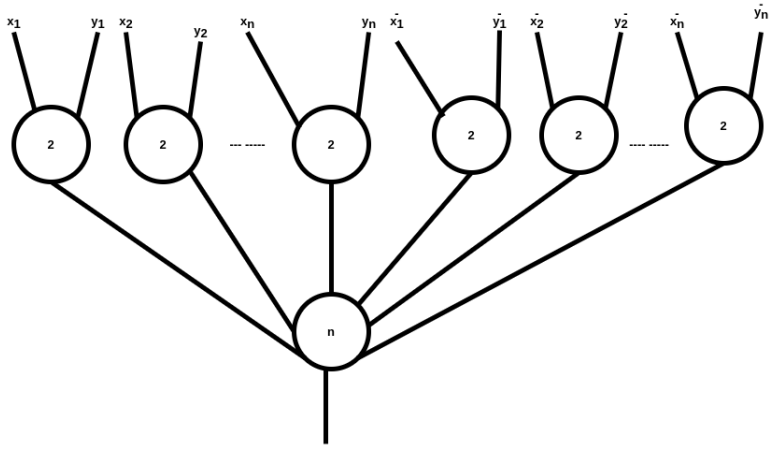

Figure 2: A threshold circuit computing the function $EQUAL(x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_n)$ of depth 2 and of size at least 2n + 1.

Proposition 1 *[3] Symmetric functions can be computed by depth-2 threshold circuits of linear size and weight 1.*

Parberry [2] shown the following theorems:

Theorem 1 *[2] Any symmetric function $f : \mathbb{B}^n \longrightarrow \mathbb{B}$ can be computed by a unit-weight threshold circuit with size 2n + 3 and depth 2.*

Theorem 2 *[2] Any threshold circuit of the weight w and depth 2 for IP: $\mathbb{B}^{2n} \longrightarrow \mathbb{B}$ must have size $\Omega(2^{n/2}/w^2)$.*

Corollary 1 *[2] $IP \notin TC_2^0$*

Proof 1 *[2] By Theorem 2, any depth 2 circuit of weight n^c for inner product must have size $\Omega(2^{n/2}/n^{2c})$, which is larger than any polynomial.* □

Let us consider the following symmetric function:

$$PARITY(x_1, x_2, \cdots, x_n) = x_1 \oplus x_2 \oplus \cdots \oplus x_i \oplus \cdots \oplus x_n = \bigoplus_{i=1}^{n} x_i$$

The complement of Parity is:

$$\overline{PARITY(x_1, x_2, \cdots, x_n)} = \overline{x_1 \oplus x_2 \oplus \cdots \oplus x_i \oplus \cdots \oplus x_n}$$

We easily observe that:

$$\overline{PARITY(x_1, x_2, \cdots, x_n)} = PARITY(x_1, x_2, \cdots, x_{n-1}, \overline{x}_n)$$

Inner Product is defined in [2, 3] as:

$$IP(x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_n) = \bigoplus_{i=1}^{n} (x_i \wedge y_i) \tag{4}$$

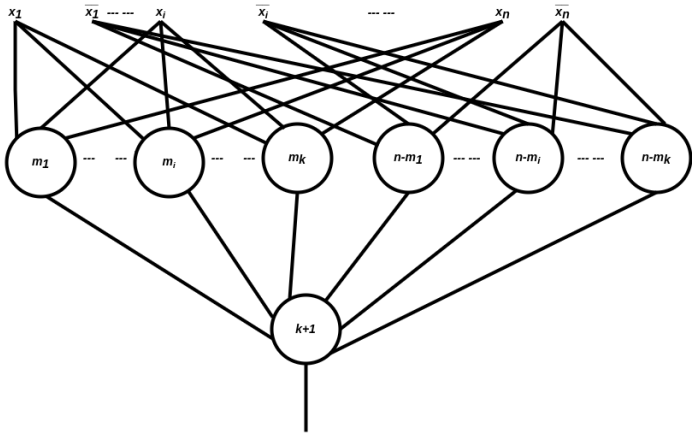

Figure 3: A threshold circuit computing the function $PARITY(x_1, x_2, \cdots, x_n) = x_1 \oplus x_2 \oplus \cdots \oplus x_i \oplus \cdots \oplus x_n = \bigoplus_{i=1}^{n} x_i$ with depth 2 and size at most 2n + 3.

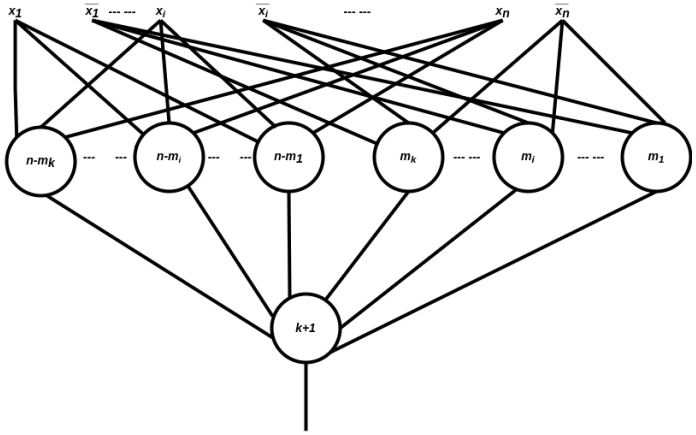

Figure 4: A threshold circuit computing the function $\overline{PARITY(x_1, x_2, \cdots, x_n)} = \overline{x_1 \oplus x_2 \oplus \cdots \oplus x_i \oplus \cdots \oplus x_n}$ with depth 2 and size at most 2n + 3.

We easily see that the complement of Inner Product is:

$$\overline{IP}(x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_n) = \overline{PARITY(x_1 \wedge y_1, \cdots, x_i \wedge y_i, \cdots, x_n \wedge y_n)} \tag{5}$$

We easily deduce that:

$$\overline{IP}(x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_n) = PARITY(x_1 \wedge y_1, \cdots, x_i \wedge y_i, \cdots, x_{n-1} \wedge y_{n-1}, \overline{x_n \wedge y_n}) \tag{6}$$

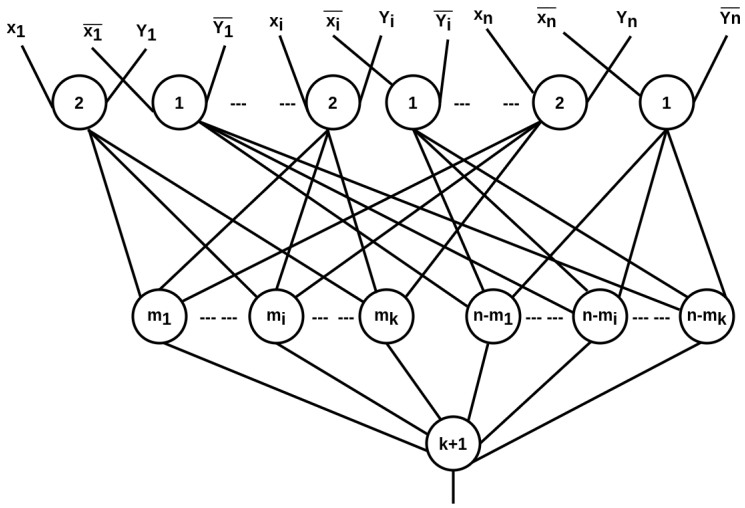

Figure 5: A threshold circuit computing the function $IP(x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_n) = x_1y_1 \oplus x_2y_2 \oplus \cdots \oplus x_iy_i \oplus \cdots \oplus x_ny_n$ of depth 3 and of size at most 2n(2n + 3).

Theorem 3 *[2]*

Any symmetric function $f: \mathbb{B}^n \longrightarrow \mathbb{B}$ can be computed by a unit-weight threshold circuit with 2n + 3 and depth 2.

Proof 2

Let $f: \{0,1\}^n \longrightarrow \{0,1\}$ be a symmetric function. f is fully(uniquely) defined by the set

$$S_f = \{m \in \mathbb{N} \mid f(x) = 1 \ for\ all\ x \in \mathbb{B}^n\ with\ exactly\ m\ ones\}.$$

Suppose $S_f = \{m_1, \cdots, m_k\}$.

The circuit uses k pairs of gates on the first level. The ith pair has one gate active when the number of ones in the input is at least m_i (this is a unit-weigth threshold-gate with threshold m_i connected to the inputs $x_1, \cdots, x_n$), and the other gate active when the number of ones in the input is at most m_i. When given an input x such that $f(x) = 0$, exactly one of each pair is active, therefore, exactly k gates are active. When given an input x such that $f(x) = 1$, one pair has both of its gates active, and all other pairs have exactly one of its gates active, therefore exactly $k + 1$ gates are active. The output gate therefore has threshold value $k + 1$ and inputs from all of the first level gates. This circuit has depth 2, and since $k \leq n + 1$, size at most 2(n + 1) + 1. □

For example, Figure 9 shows a threshold circuit for computing PARITY in depth 2 and size 7.

Figure 10 shows a threshold circuit for computing $\overline{PARITY}$ in depth 2 and size 9.

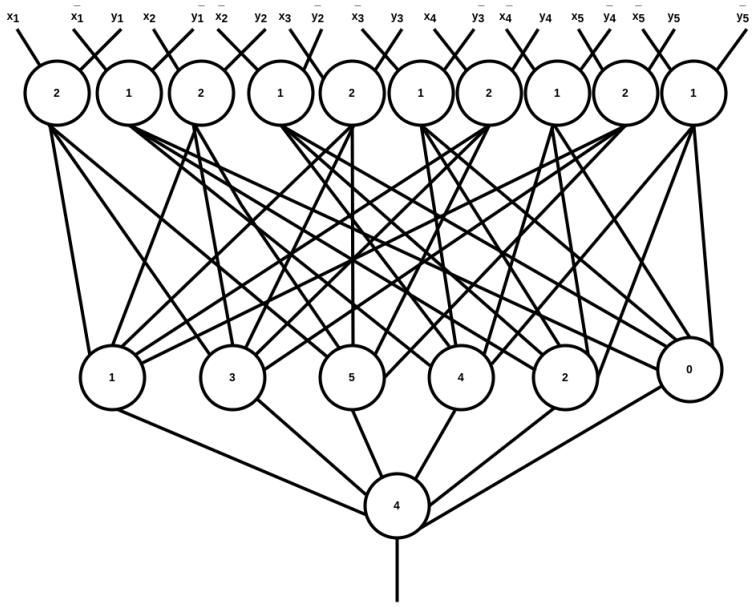

Figure 6: Example of a threshold circuit computing the function $IP(x_1, x_2, x_3, x_4, x_5, y_1, y_2, y_3, y_4, y_5) = x_1y_1 \oplus x_2y_2 \oplus x_3y_3 \oplus x_4y_4 \oplus x_5y_5$ of depth 3 and of size 17 .

Corollary 2 *[2]*

Any symmetric function $f: \mathbb{B}^n \longrightarrow \mathbb{B}^m$ can be computed by a unit-weight threshold circuit with size $2n + m + 2$ and depth 2.

Proof 3 *[2] Suppose $f: \mathbb{B}^n \longrightarrow \mathbb{B}^m$ is a symmetric function. Computing each individual bit of the output of f is a symmetric function, and hence by Theorem 1 can be computed in-depth 2 and size $2n + 1$. Thus, the obvious circuit for computing f uses m such circuits and has depth 2 and size $2nm + m$. However, the first layer of this combined circuit can have at most $2(n + 1)$ different gates, giving the required size bound.* □

Gates in the second layer of the threshold circuits constructed in Theorem 1 and Corollary 2 have an interesting property. They have unit weights, threshold k, and the number of ones in their input is guaranteed (by the rest of the circuit) to be either k or $k - 1$. Let us call this kind of Boolean linear threshold function a balanced one. The following result enables savings in depth whenever balanced threshold gates are used in any layer of a circuit but the last. This does not, of course, give savings in depth for the circuits constructed in Theorem 1 or Corollary 2, but it will enable a reduction in depth whenever these circuits are used as building blocks in the interior of another circuit [2].

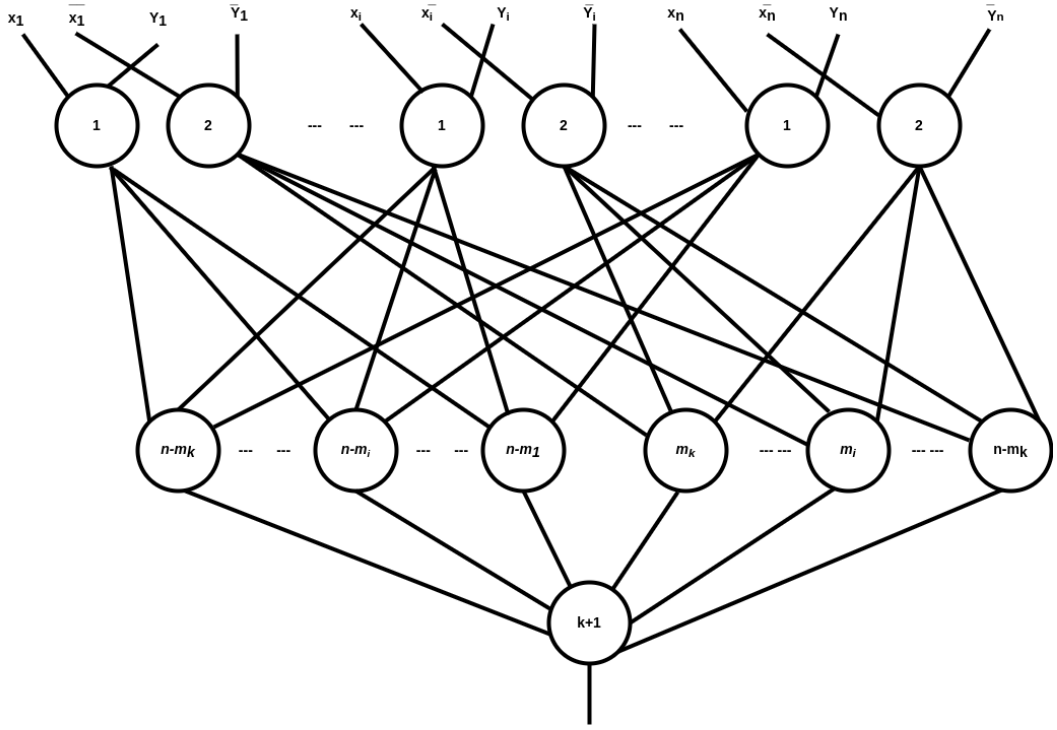

Figure 7: A threshold circuit computing the function $\overline{IP}(x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_n) = \overline{PARITY(x_1 \wedge y_1, \cdots, x_i \wedge y_i, \cdots, x_n \wedge y_n)}$ of depth 3 and of size at most 2n(2n + 3).

A threshold gate g is said to be balanced iff the number or sum of the ones at the input of the threshold-gate g is either k or k-1, with k $\in$ **N**, mathematically:

$$W_H(x) \in \{k, k-1\}.$$

If the number or the sum of the ones at the input of the threshold-gate of g is different from k or k-1, then g is said to be unbalanced, mathematically:

$$W_H(x) \notin \{k, k-1\}.$$

Lemma 1 *[2]*

Let g_0 be a unit-weight threshold-gate that has inputs only from balanced threshold-gates $g_1, \cdots, g_m$ where for all $1 \leq i < j \leq m$, gates g_i and g_j have distinct inputs. The gates $g_0, g_1, \cdots, g_m$ can be replaced by a single threshold-gate.

Proof 4 *[2]*

Let g_0 be a unit-weight threshold-gate that has inputs only from balanced threshold-gates $g_1, \cdots, g_m$. Suppose gates $g_1, \cdots, g_m$ collectively have inputs $x_1, \cdots, x_n$, and that for all $1 \leq i < j \leq m$, gates g_i and g_j have nonoverlapping

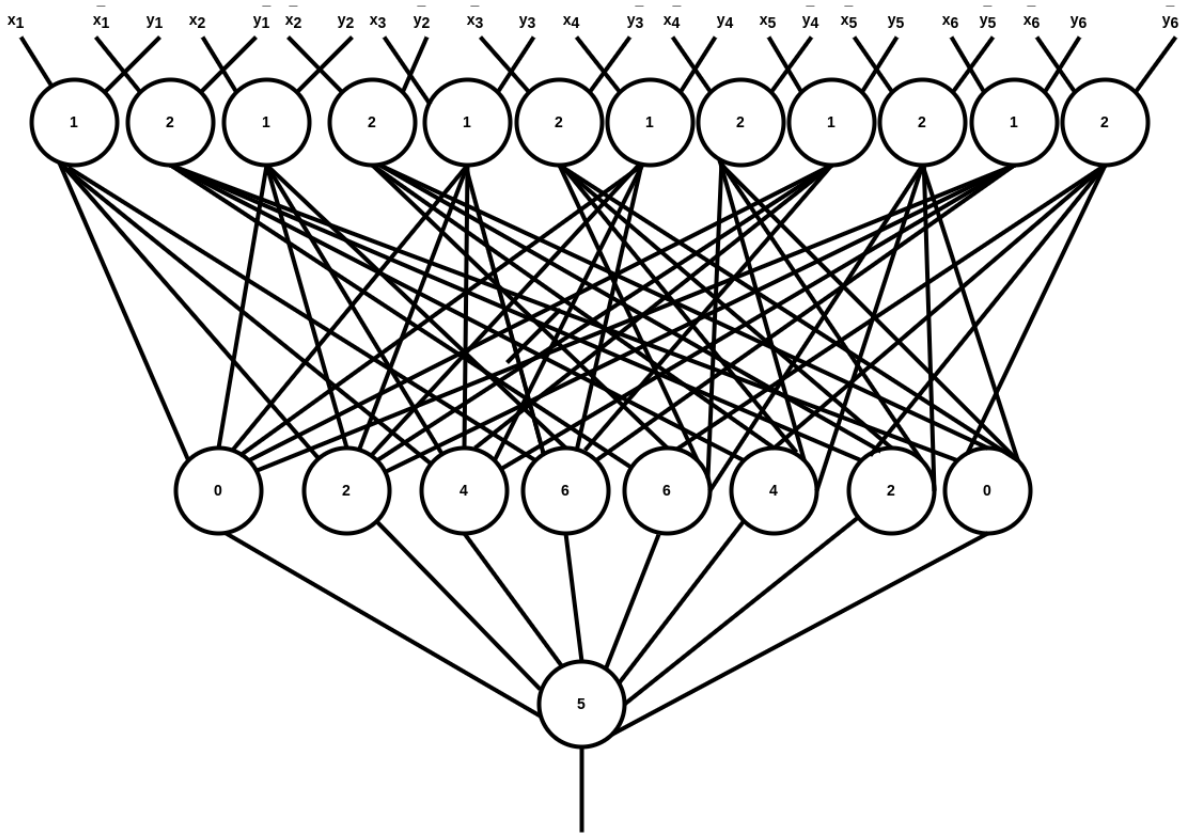

Figure 8: Example of a threshold circuit computing the function $\overline{IP}(x_1, x_2, x_3, x_4, x_5, x_6, y_1, y_2, y_3, y_4, y_5, y_6) = \overline{PARITY}(x_1 \wedge y_1, x_2 \wedge y_2, x_3 \wedge y_3, x_4 \wedge y_4, x_5 \wedge y_5, x_6 \wedge y_6)$ of depth 3 and of size 21.

input. Suppose g_i has weight k_i, for $0 \leq i \leq m$. We claim that the entire circuit can be replaced by a threshold-gate g with threshold $\sum_{i=0}^{m} k_i - m$ (see Figure 11).

Suppose g_0 outputs 0. Then, at most $k_0 - 1$ of the gates $g_1, \cdots, g_m$ output 1. Therefore, at most $k_0 - 1$ of the gates g_i for $1 \leq i < j \leq m$ see k_i ones, and the rest see $k_i - 1$ ones. Hence, $x_1, \cdots, x_n$ can have at most

$$\sum_{i=1}^{m} (k_i - 1) + (k_0 - 1) = \sum_{i=0}^{m} k_i - (m + 1)$$

ones. Therefore, g outputs 0.

Conversely, suppose g_0 outputs 1. Then, at least k_0 of the gates $g_1, \cdots, g_m$ output 1. Therefore, at least k_0 of the gates g_i for $1 \leq i \leq m$ see k_i ones, and the rest see $-1 + k_i$ ones. Hence, $x_1, \cdots, x_n$ must have at least

$$\sum_{i=1}^{m} (k_i - 1) + k_0 = \sum_{i=0}^{m} k_i - m$$

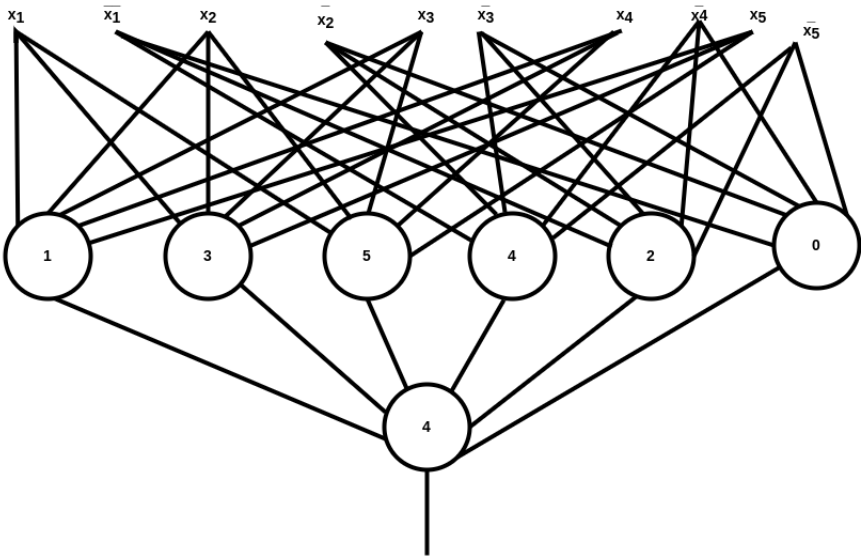

Figure 9: A threshold circuit computing the symmetric function $x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5$.

ones. Therefore, g outputs 1.

We have shown that g outputs 1 iff g_0 outputs 1. Therefore, the circuit containing $g_0, g_1, \cdots, g_m$ can be replaced by the threshold-gate g, as claimed. □

Definition 1
TC^0 is the class of languages accepted by threshold circuits of polynomial size and depth O(1).

TC^0_k is the class of languages accepted by threshold circuits of depth k and size $O((\log(n))^k)$.

Hajnal et al.[3] have shown the following result:

Lemma 2 *[3]*
Fix any $\epsilon > 0$ and polynomial p. Assume that C is a depth-2 threshold circuit with weight $\leq p(n)$ computing INNER PRODUCT MOD 2 to two n-bit strings. Then if n is sufficiently large, the size of C is at least $2^{(1/2-\epsilon)n}$.

From the Lemma 2, Hajanal et al.[3] deduce that:

Lemma 3 *[3]*
INNER PROD MOD 2 is not in TC^0_2, INNER PROD MOD 2 is in TC^0_3

Hajnal et al.[3] deduce the following strict inclusion:

Theorem 4 *[3]*
$TC^0_1 \subseteq TC^0_2 \subseteq TC^0_3$

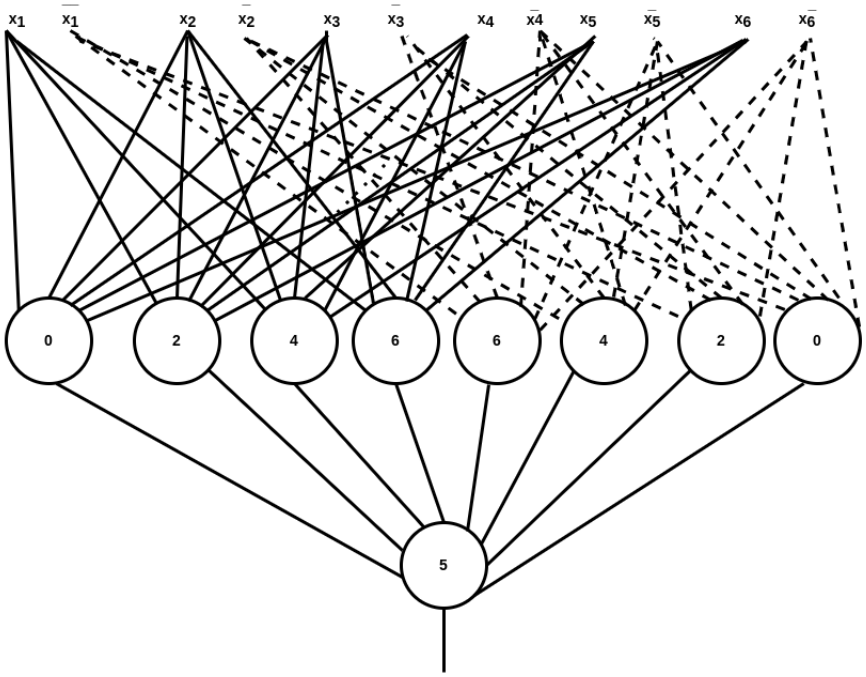

Figure 10: A threshold circuit computing the symmetric function $\overline{PARITY}(x_1, x_2, x_3, x_4, x_5, x_6)$.

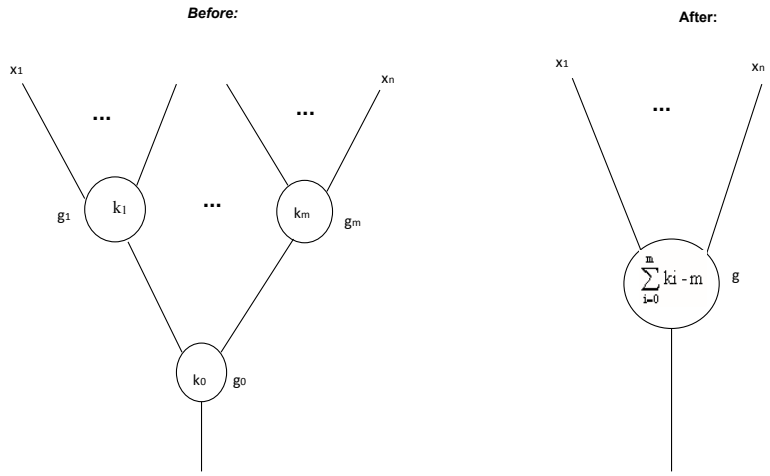

Figure 11: Before and after pictures for Lemma [2]

It was conjectured in [4, 5] that:

$$TC^0 \neq TC^0_k, \ for\ any\ k$$

Parberry stated in [2] that:

It is an open problem as to whether the TC^0 hierarchy collapses, that is, whether more than three layers of threshold gates are needed to compute all functions in TC^0 in polynomial size.

Krause and Wegener [6] have said that:

Indeed, no proof is known that a function is contained in $NP \setminus TC^0_3$.

Our aim is to show that the sets $NP \setminus TC^0_3$, $NP \setminus TC^0_4$ and $NP \setminus TC^0_5$ are not empty.

The paper is organized as follows. Section 2 is concerned with the presentation of linear codes and cyclic codes, matrix generators, and parity-check matrix of linear codes. Section 3, we present our contribution. Concluding remarks are stated in Section 4.

2 Linear Codes and Cyclic Codes

2.1 Linear Codes

Definition 2

$\mathcal{C}$ is a linear code if $\mathcal{C}$ is a linear subspace of $\mathbb{F}_q^n$. $\mathcal{C}$ is then called a $[k, n]$-code if dim($\mathcal{C}$)= k. If the minimal distance of $\mathcal{C}$ is d, we say that $\mathcal{C}$ is a $[k, n, d]$-code

A linear code can be described by each of the following matrices :

- A *generator* matrix G for an $[k, n, d]$-code $\mathcal{C}$ is a $k \times n$ matrix whose rows form a basis for $\mathcal{C}$. The lines of a generator matrix form a base for the code $\mathcal{C}$.

$$\mathrm{G} = \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_k \end{pmatrix}$$

  The generator matrix in systematic form have the following structure:

$$G = [I_k | P],$$

  where I_k is the $k \times k$ identity matrix and P $\in$ $\mathbb{F}_q^{k\times(n-k)}$.

- A *parity-check* matrix H for an $[k, n, d]$ code $\mathcal{C}$ is an $(n-k) \times n$ matrix of rank $n-k$ sastisfying:

$$\forall\ \mathbf{x} \in \mathcal{C}, \quad H\ {}^t\mathbf{x} = 0.$$

  From a generator matrix in systematic form, one can compute the parity-check matrix as follos :

$$H = \left[\ {}^tP | I_{n-k}\right].$$

If G is a generator matrix and H a parity-check matrix of the same code, then

$$G\ {}^tH = 0.$$

Example 1

We construct a binary $[6,3]$*-code by choosing three vectors linearly independent of* $\mathbb{F}_2^6$.

$$\mathrm{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

We obtain all the codewords of $\mathcal{C}$ *by calculating all the products* $m\mathrm{G}$ *with* $m \in \mathbb{F}_2^3$.

The words of the code $\mathcal{C}$ *is given by:*

			$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$
0	*0*	*0*	$(\mathbf{0\ 0\ 0\ 0\ 0\ 0})$
0	*0*	*1*	$(\mathbf{1\ 1\ 0\ 1\ 1\ 0})$
0	*1*	*0*	$(\mathbf{0\ 1\ 1\ 1\ 0\ 1})$
0	*1*	*1*	$(\mathbf{1\ 0\ 1\ 0\ 1\ 1})$
1	*0*	*0*	$(\mathbf{1\ 0\ 0\ 1\ 0\ 1})$
1	*0*	*1*	$(\mathbf{0\ 1\ 0\ 0\ 1\ 1})$
1	*1*	*0*	$(\mathbf{1\ 1\ 1\ 0\ 0\ 0})$
1	*1*	*1*	$(\mathbf{0\ 0\ 1\ 1\ 1\ 0})$

We transform the matrix G in the systematic form(**Gaussian elimination**)

$$\mathrm{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix} \longmapsto \cdots \longmapsto \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} = (I_3|P)$$

Example 2

Starting from the generator matrix defined as follow:

$$\mathrm{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} = (I_3|A)$$

We find the parity-check matrix $\mathrm{H} = ({}^tA|I_3)$ *of* $\mathcal{C}$ *which yields:*

$$\mathrm{H} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

From H*, we obtain the codewords of* $\mathcal{C}^\perp$

			$\begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$
0	*0*	*0*	$(\mathbf{0\ 0\ 0\ 0\ 0\ 0})$
0	*0*	*1*	$(\mathbf{1\ 1\ 0\ 0\ 0\ 0})$
0	*1*	*0*	$(\mathbf{0\ 1\ 1\ 0\ 1\ 0})$
0	*1*	*1*	$(\mathbf{1\ 0\ 1\ 0\ 1\ 1})$
1	*0*	*0*	$(\mathbf{1\ 0\ 1\ 1\ 0\ 0})$
1	*0*	*1*	$(\mathbf{0\ 1\ 1\ 1\ 0\ 1})$
1	*1*	*0*	$(\mathbf{1\ 1\ 0\ 1\ 1\ 0})$
1	*1*	*1*	$(\mathbf{0\ 0\ 0\ 1\ 1\ 0})$

2.2 Cyclic Codes

Definition 3 *[11]*

A code C is cyclic if

a) C is a linear code;

b) any cyclic shift of a codeword is also a codeword, i.e. whenever $v_o v_1 \cdots v_{n-1} \in C$*, then also* $v_{n-1} v_0 v_1 \cdots v_{n-2} \in C$ *and* $v_1 v_2 \cdots v_{n-1} v_0 \in C$

Example 3

a) $\{0\}$ *is a trivial cyclic code;*

b) Code $C = \{000, 101, 011, 110\}$ *is cyclic*

c) Hamming code Ham(3, 2): with the generator matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

is equivalent to a cyclic code.

Theorem 5 *[11]*

Every nontrivial cyclic (n,k)-code contains a codeword g(x) of degree n-k. Then code words are precisely all the multiples q(x)g(x), where q(x) is any polynomial of degree smaller than k. The code has the following generator matrix:

$$\mathrm{G} = \begin{bmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{bmatrix} = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-k} & & 0 & & 0 & \cdots & 0 & 0 & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & & g_{n-k} & & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \cdots & & g_{n-k} & & \cdots & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & & \cdots & & & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & 0 & 0 & & \cdots & & & g_0 & g_1 & g_2 \cdots & g_{n-k} \end{bmatrix}$$

Example 4

The even-parity code of length n is cyclic. The codeword of degree n— k = 1 is just one: 1 + x. The generator matrix is

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 1 \end{bmatrix}$$

Proposition 2 *[11]*

A cyclic code with the parity check polynomial $h(x) = h_0 + h_1 x + \cdots + h_{k-1}x^{k-1} + x^k$ *has the following parity check matrix:*

$$H = \begin{bmatrix} 0 & 0 & \cdots & 0 & 0 & 0 & 1 & h_{k-1} & \cdots & h_2 & h_1 & h_0 \\ 0 & 0 & \cdots & 0 & 0 & 1 & h_{k-1} & h_2 & & h_1 & h_0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & h_{k-1} & h_2 & h_1 & & h_0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & h_{k-1} & \cdots & h_2 & h_1 & h_0 & 0 & 0 & \cdots & 0 & 0 & 0 \end{bmatrix}$$

Example 5

The Hamming cyclic code of length 7 with the generator polynomial $g(x) = 1 + x + x^3$ *has the parity check polynomial* $h(x) = (x^7 - 1) \div (x^3 + x + 1) = x^4 + x^2 + x + 1$*. Thus, it has the following parity check matrix:*

$$H = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}$$

Remark 1

If we denote H the control matrix of a cyclic code C

$$H = \begin{bmatrix} h_{1*} \\ h_{2*} \\ \vdots \\ h_{(n-k)*} \end{bmatrix} = \begin{bmatrix} 0 & 0 & \cdots & 0 & 0 & 0 & 1 & h_{k-1} & \cdots & h_2 & h_1 & h_0 \\ 0 & 0 & \cdots & 0 & 0 & 1 & h_{k-1} & h_2 & & h_1 & h_0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & h_{k-1} & h_2 & h_1 & & h_0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & h_{k-1} & \cdots & h_2 & h_1 & h_0 & 0 & 0 & \cdots & 0 & 0 & 0 \end{bmatrix}$$

Based on Proposition 2 and on the structure of H, we easily observe that:

$$h_{i*} = S(h_{(i+1)*});\ 1 \leq i \leq\ n - k - 1$$

where S is the right circular shift defined as:

$$S(e_p, e_{p-1}, \cdots, e_2, e_1) = (e_1, e_p, e_{p-1}, \cdots, e_3, e_2)$$

sometimes, right circular shift is noted as : $\gg$

It follows that

$$h_{(n-k-i)*} = S^i(h_{(n-k)*});\ 1 \leq i \leq\ n-k-1$$

where

$$S^i = \underbrace{SoSoSoSoSo\cdots oS}_{i\ times}$$

we easily deduce that:

$$H = \begin{bmatrix} h_{1*} \\ h_{2*} \\ \vdots \\ h_{(n-k-2)*} \\ h_{(n-k-1)*} \\ h_{(n-k)*} \end{bmatrix} = \begin{bmatrix} S^{(n-k-1)}(h_{(n-k)*}) \\ S^{(n-k-2)}(h_{(n-k)*}) \\ \vdots \\ S^2(h_{(n-k)*}) \\ S(h_{(n-k)*}) \\ h_{(n-k)*} \end{bmatrix}$$

3 Our Contribution

In the following subsection, we characterize a function that testing if a word belonging to a code by using a generator matrix.

3.1 Testing belonging of a word to a code by using Generator Matrix

We consider two cases of Generator Matrix: Generator Matrix in a systematic form and Generator Matrix in a general form.

3.1.1 Generator Matrix in a systematic form

Subsequently, without loss of generality we suppose that the generator matrix has the form:

$$G = (I_k|B) = \left(\begin{array}{ccccc|cccc} 1 & 0 & 0 & \cdots & 0 & b_{11} & b_{12} & \cdots & b_{1,n-k} \\ 0 & 1 & 0 & \cdots & 0 & b_{21} & b_{22} & \cdots & b_{2,n-k} \\ 0 & 0 & 1 & \cdots & 0 & b_{31} & b_{32} & \cdots & b_{3,n-k} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & b_{k1} & b_{k2} & \cdots & b_{k,n-k} \end{array}\right) \tag{7}$$

$\forall\ V = (v_1, v_2, \cdots, v_n) \in C$, we have

$$Coor(V) = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{pmatrix}$$

From the fact that G is a generator matrix of C, we can write:

$$V \in C \Longleftrightarrow Coor(V).G = V$$

This is equivalent to:

$$V \in C \Longleftrightarrow (v_1, v_2, v_3 \cdots, v_k) \left(\begin{array}{ccccc|cccc} 1 & 0 & 0 & \cdots & 0 & b_{11} & b_{12} & \cdots & b_{1,n-k} \\ 0 & 1 & 0 & \cdots & 0 & b_{21} & b_{22} & \cdots & b_{2,n-k} \\ 0 & 0 & 1 & \cdots & 0 & b_{31} & b_{32} & \cdots & b_{3,n-k} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & b_{k1} & b_{k2} & \cdots & b_{k,n-k} \end{array}\right) = (v_1, v_2, v_3 \cdots, v_n)$$

This implies that:

$$V \in C \Longleftrightarrow (v_1, v_2, v_3 \cdots, v_k, \bigoplus_{l=1}^{k} v_l \times b_{l,1}, \bigoplus_{l=1}^{k} v_l \times b_{l,2}, \cdots, \bigoplus_{l=1}^{k} v_l \times b_{l,n-k}) = (v_1, v_2, v_3 \cdots, v_n)$$

We conclude that:

$$V \in C \Longleftrightarrow \bigoplus_{l=1}^{k} v_l \times b_{l,j} \ = \ v_{k+j}, \ 1 \leq j \leq n-k$$

It follows that:

$$V \in C \Longleftrightarrow IP(b_{*j}, V) \ = \ v_{k+j}, \ 1 \leq j \leq n-k \tag{8}$$

By using Equation (8), we define the following function

$$f_1(V, G) \ = \ EQUAL((IP(b_{*1}, V), IP(b_{*2}, V), \cdots, IP(b_{*n-k}, V)), (v_{k+1}, v_{k+2}, \cdots, v_n))$$

which testing if the word V belonging to a code C by using the generator matrix in the systematic form.

3.1.2 Generator Matrix in a general form

We consider the general case:

$$G = \begin{pmatrix} g_{11} & g_{12} & g_{13} & \cdots & g_{1n} \\ g_{21} & g_{22} & g_{23} & \cdots & g_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ g_{k1} & g_{k2} & g_{k3} & \cdots & g_{kn} \end{pmatrix}$$

where G is a $k \ \times \ n$ matrix such that $g_{ij} \in \{0, 1\}, \ for \ 1 \leq i \leq k$ and $1 \ \leq j \leq \ n$.
We have to determine

$$(z_1, z_2, z_3 \cdots, z_k) \in \{0, 1\},$$

such that

$$\bigoplus_{i=1}^{k} z_i \times g_{i,*} \ = \ V$$

This is equivalent to:

$$V \in C \Longleftrightarrow (z_1, z_2, z_3 \cdots, z_k) \begin{pmatrix} g_{11} & g_{12} & g_{13} & \cdots & g_{1n} \\ g_{21} & g_{22} & g_{23} & \cdots & g_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ g_{k1} & g_{k2} & g_{k3} & \cdots & g_{kn} \end{pmatrix} = (v_1, v_2, v_3 \cdots, v_n)$$

This implies that:

$$V \in C \Longleftrightarrow ((z_1 \times g_{11} + z_2 \times g_{21} + z_3 \times g_{31} + \cdots + z_k \times g_{k1}), (z_1 \times g_{12} + z_2 \times g_{22} + z_3 \times g_{32} + \cdots + z_k \times g_{k2}), \cdots,$$

$$(z_1 \times g_{1n} + z_2 \times g_{2n} + z_3 \times g_{3n} + \cdots + z_k \times g_{kn})) = (v_1, v_2, \cdots, v_n)$$

$$V \in C \Longleftrightarrow (\sum_{t=1}^{k} z_t \times g_{k1}, \sum_{t=1}^{k} z_t \times g_{k2}, \cdots, \sum_{t=1}^{k} z_t \times g_{kn}) = (v_1, v_2, \cdots, v_n)$$

$$V \in C \Longleftrightarrow (\bigoplus_{t=1}^{k} z_t \wedge g_{t,1}, \bigoplus_{t=1}^{k} z_t \wedge g_{t,2}, \cdots, \bigoplus_{t=1}^{k} z_t \wedge g_{k,n}) = (v_1, v_2, \cdots, v_n)$$

We conclude that:

$$V \in C \Longleftrightarrow \bigoplus_{j=1}^{k} z_j \wedge g_{j,i} \ = \ v_i, \ 1 \leq i \leq n$$

It follows that:

$$V \in C \Longleftrightarrow IP(g_{*i}, V) \ = \ v_i, \ 1 \leq i \leq n \tag{9}$$

By using Equation (9), we define the following function

$$f_2(V, G) \ = \ EQUAL((IP(g_{*1}, V), IP(g_{*2}, V), \cdots, IP(g_{*n}, V)), (v_1, v_2, \cdots, v_n))$$

which testing if the word V belonging to a code C by using the generator matrix in the general form.

3.2 Testing belonging of a word to a code by using Parity-check Matrix

Let us denote $C^{\perp}$ the dual code of a code C. We note H the generator matrix of $C^{\perp}$. Let us note a word $V = (v_1, v_2, \cdots, v_n) \in C$ and let us express $H^t V$ in terms of IP:

$$H^t V = \begin{pmatrix} h_{11} & h_{12} & \cdots & h_{1n} \\ h_{21} & h_{22} & \cdots & h_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ h_{(n-k)1} & h_{(n-k)2} & \cdots & h_{(n-k)n} \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^{n} h_{1j} \times v_j \\ \vdots \\ \sum_{j=1}^{n} h_{ij} \times v_j \\ \vdots \\ \sum_{j=1}^{n} h_{(n-k)j} \times v_j \end{pmatrix}$$

$$= \begin{pmatrix} \bigoplus_{j=1}^{n} h_{1j} \wedge v_j \\ \vdots \\ \bigoplus_{j=1}^{n} h_{ij} \wedge v_j \\ \vdots \\ \bigoplus_{j=1}^{n} h_{(n-k)j} \wedge v_j \end{pmatrix} = \begin{pmatrix} IP(h_{1*}, V) \\ \vdots \\ IP(h_{i*}, V) \\ \vdots \\ IP(h_{(n-k)*}, V) \end{pmatrix}$$

By definition, we have:

$$V \ \in \ C \iff H^t V \ = \ \vec{0} \tag{10}$$

This implies that:

$$V \ \in \ C \iff \sum_{i=1}^{n-k} IP(h_{i*}, V) = 0 \tag{11}$$

$$V \ \notin \ C \iff \sum_{i=1}^{n-k} IP(h_{i*}, V) \geq 1 \tag{12}$$

It follows that:

$$V \ \in \ C \iff \sum_{i=1}^{n-k} \overline{IP}(h_{i*}, V) = (n-k) \tag{13}$$

We deduce that:

$$V \ \in \ C \iff TH_{(n-k)}^{(n-k)}(\overline{IP}(h_{1*}, V), \overline{IP}(h_{2*}, V), \cdots, \overline{IP}(h_{(n-k)*}, V)) = 1 \tag{14}$$

By using Equation (14), we define the following function:

$$f_3(V, H) = TH_{(n-k)}^{(n-k)}(\overline{IP}(h_{1*}, V), \overline{IP}(h_{2*}, V), \cdots, \overline{IP}(h_{(n-k)*}, V))$$

where the vector

$$h_{i*} \ = \ \big(h_{i1}, h_{i2}, \cdots, h_{in}\big) \quad 1 \leq i \leq n-k \tag{15}$$

are the generator of the dual space of $C^{\perp}$ (or the parity-check matrix of C).

The function f_3 tests if the word V belonging to a code C by using the parity-check matrix.

$$V \ \in \ C \iff f_3(V, H) = 1 \tag{16}$$

Let us consider the following function:

$$\tilde{f}_3(V, H) = TH_1^{(n-k)}(IP(h_{1*}, V), IP(h_{2*}, V), \cdots, IP(h_{(n-k)*}, V)) \tag{17}$$

It is easy to see that:

$$V \ \notin \ C \iff \tilde{f}_3(V, H) = 1$$

Example 6

Let $n = 3, k = 1$ *from where* $n - k = 2$ *construct the threshold circuit corresponding to the function*

$$f_4(V, H) = TH^{(2)}_{(2)}(\overline{IP}(h_{1*}, V), \overline{IP}(h_{2*}, V))$$

where the vector

$$h_{i*} = \left(h_{i1}, h_{i2}, h_{i3}\right) \quad 1 \leq i \leq 2 \tag{18}$$

with

$$\overline{IP}(h_{1*}, V) = h_{11} \wedge v_1 \oplus h_{12} \wedge v_2 \oplus h_{13} \wedge v_3$$

and

$$\overline{IP}(h_{2*}, V) = h_{21} \wedge v_1 \oplus h_{22} \wedge v_2 \oplus h_{23} \wedge v_3$$

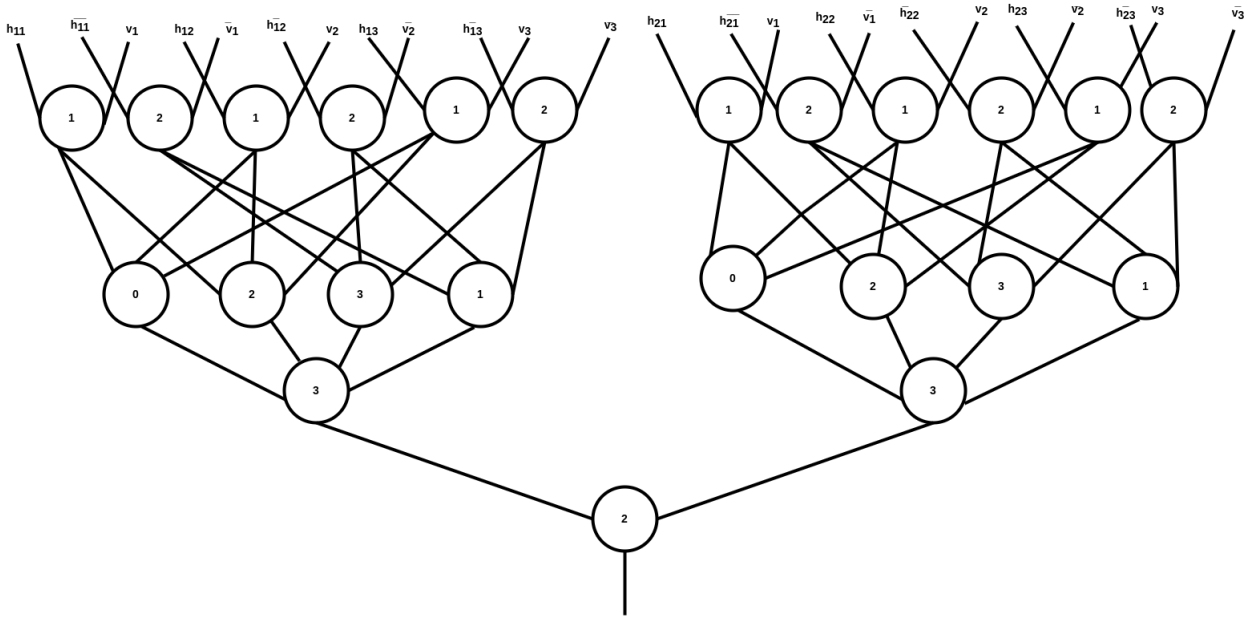

Figure 12: A threshold circuit of the function $f_4(V) = TH^{(2)}_{(2)}(\overline{IP}(h_{1*}, V), \overline{IP}(h_{2*}, V))$ testing belonging of a word of length 3 to a code by using the parity-check-matrix of dimension 2. Here the function $f_2(v)$ is **balanced**, this circuit is size 23 and depth 4 .

A corresponding threshold circuit the function f_2 *is the following figure 12*

It follows by application of the Lemma 1 of Parberry that the function f_4 *belongs to* TC^0_3 *and it becomes* ***unbalanced****.*

A corresponding threshold circuit is the following figure 13

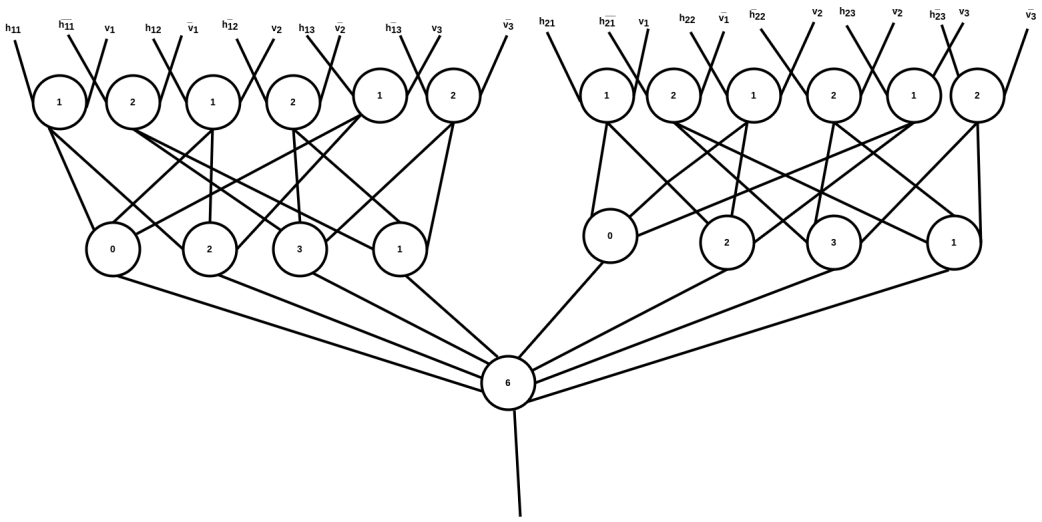

Figure 13: A threshold circuit of the function $f_4(v) = TH^{(2)}_{(2)}(\overline{IP}(h_{1*}, V), \overline{IP}(h_{2*}, V))$ testing belonging of a word of length 3 to a code by using the parity-check-matrix of dimension 2 reduced by one level by using the Lemma 1 of Parberry[2]. This circuit is size 21 and depth 3.

3.3 Element of TC^0_4

In this paragraph, we want to show that there exists a function which belongs to TC^0_4.

We consider a cyclic code $\mathcal{C}$.

Problem 1
Data : *a cyclic code $\mathcal{C}$, H its parity-check matrix , a word w.*

Question : $w \in C$ *?*

Let us build a boolean function f_5 such that:

$$f_5(w, h_{(n-k)*}) = 1 \Longleftrightarrow w \in \mathcal{C}$$

$$H = \begin{pmatrix} h_{1*} \\ h_{2*} \\ \vdots \\ h_{(n-k)*} \end{pmatrix} = \begin{pmatrix} h_{11} & h_{12} & \cdots & h_{1n} \\ h_{21} & h_{22} & \cdots & h_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ h_{(n-k)1} & h_{(n-k)2} & \cdots & h_{(n-k)n} \end{pmatrix}$$

is the parity-check matrix of the cyclic code C.

$$f_5(w, h_{(n-k)*}) = TH^{(n-k)}_{(n-k)}(\overline{IP}(S^{(n-k-1)}(h_{(n-k)*}), w), \overline{IP}(S^{(n-k-2)}(h_{(n-k)*}), w), \cdots ,$$

$$\overline{IP}(S(h_{(n-k)*}), w), \overline{IP}(h_{(n-k)*}, w))$$

Theorem 6

$$for\ k\ =\ n - \lceil \log_2(n) \rceil$$
$$f_5\ \in TC^0_4.$$

Proof 5

Based on the depth of evaluation of $\overline{IP}$, we consider two cases:

First case: $\overline{IP}$ is evaluated by a circuit of depth 2.

From the fact that $\overline{IP}$ is evaluated by a circuit of depth 2 and from Lemma 2*, we conclude that the size of $\overline{IP}$ is exponential in n, it follows that the size of the function f_5 is also exponential in n.*

$$then\ f_5\ \notin TC^0_3.$$

Second case: $\overline{IP}$ is evaluated by a circuit of depth 3.

From the fact that the depth of $\overline{IP}$ is 3, we deduce that the depth of the function f_5 is 4.

From the Theorem 1*, the size of the circuit which evaluates*

$$\overline{IP}(h_{i*}, w)\ =\ \overline{IP}(S^{(n-k-i)}(h_{(n-k)*}), w)\ is\ \mathcal{O}((\log n)^3).$$

It follows that the size of

$$f_5\ is\ \mathcal{O}((\log n)^4),\ because\ n - k = \lceil \log_2(n) \rceil.$$

We easily conclude that

$$f_5\ \in\ TC^0_4.$$

□

Let us consider a cyclic code C, H is parity-check matrix where

$$H\ =\ \begin{pmatrix} h_{1*} \\ h_{2*} \\ \vdots \\ h_{(n-k)*} \end{pmatrix}\ =\ \begin{pmatrix} h_{11} & h_{12} & \cdots & h_{1n} \\ h_{21} & h_{22} & \cdots & h_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ h_{(n-k)1} & h_{(n-k)2} & \cdots & h_{(n-k)n} \end{pmatrix}$$

Problem 2
Data : *a cyclic code $\mathcal{C}$, H its parity-check matrix , a word w.*

Question : $w\ \notin\ C$ *?*

Let us build a boolean function $\tilde{f}_5$ such that:

$$\tilde{f}_5(w, h_{(n-k)*}) = 1 \Longleftrightarrow w \notin \mathcal{C}$$

$$\tilde{f}_5(w, h_{(n-k)*}) = TH_1^{(n-k)}(IP(S^{(n-k-1)}(h_{(n-k)*}), w), IP(S^{(n-k-2)}(h_{(n-k)*}), w), \cdots,$$
$$IP(S(h_{(n-k)*}), w), IP(h_{(n-k)*}, w))$$

The following result characterizes the function $\tilde{f}_5$.

Theorem 7

For n sufficiently large, we define

$$k \ = \ n - \lceil \log_2(n) \rceil$$

$$\tilde{f}_5 \ \in TC_4^0.$$

Proof 6

Based on the depth of evaluation of IP, we consider two cases:

First case: IP is evaluated by a circuit of depth 2.

From the fact that IP is evaluated by a circuit of depth 2 and from Lemma 2, we conclude that the size of IP is exponential in n, it follows that the size of the function $\tilde{f}_5$ is also exponential in n.

$$\textit{then } \tilde{f}_5 \ \notin TC_3^0.$$

Second case: IP is evaluated by a circuit of depth 3.

From the fact that the depth of IP is 3, we deduce that the depth of the function $\tilde{f}_5$ is 4.

From the Theorem 1, the size of the circuit which evaluates

$$IP(h_{i*}, w) \ = \ IP(S^{(n-k-i)}(h_{(n-k)*}), w) \textit{ is } \mathcal{O}((\log n)^3).$$

It follows that the size of

$$\tilde{f}_5 \textit{ is } \mathcal{O}((\log n)^4), \textit{ because } n - k = \lceil \log_2(n) \rceil.$$

We easily conclude that

$$\tilde{f}_5 \ \in \ TC_4^0.$$

□

3.4 Element of TC_5^0

We tackle the existence of a function in the set TC_5^0. Let us consider two cyclic codes C_1 and C_2

Problem 3

- *Two cyclic codes C_1 and C_2,*
- *H_1 parity-check matrix of C_1,*

$$H_1 = \begin{bmatrix} L_1 \\ L_2 \\ \vdots \\ L_{(n-k)} \end{bmatrix} = \begin{bmatrix} 0 & 0 & \cdots & 0 & 0 & 0 & 1 & h_{k-1} & \cdots & h_2 & h_1 & h_0 \\ 0 & 0 & \cdots & 0 & 0 & 1 & h_{k-1} & h_2 & & h_1 & h_0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & h_{k-1} & h_2 & h_1 & & h_0 & 0 & 0 \\ \cdots & \cdots & & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & & \cdots & \cdots \\ 1 & h_{k-1} & \cdots & h_2 & h_1 & h_0 & 0 & 0 & \cdots & 0 & 0 & 0 \end{bmatrix}$$

- *H_2 parity-check matrix of C_2,*

$$H_2 = \begin{bmatrix} \tilde{L}_1 \\ \tilde{L}_2 \\ \vdots \\ \tilde{L}_{(n-k)} \end{bmatrix} = \begin{bmatrix} 0 & 0 & \cdots & 0 & 0 & 0 & 1 & \tilde{h}_{k-1} & \cdots & \tilde{h}_2 & \tilde{h}_1 & \tilde{h}_0 \\ 0 & 0 & \cdots & 0 & 0 & 1 & \tilde{h}_{k-1} & \tilde{h}_2 & & \tilde{h}_1 & \tilde{h}_0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & \tilde{h}_{k-1} & \tilde{h}_2 & \tilde{h}_1 & & \tilde{h}_0 & 0 & 0 \\ \cdots & \cdots & & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & & \cdots & \cdots \\ 1 & \tilde{h}_{k-1} & \cdots & \tilde{h}_2 & \tilde{h}_1 & \tilde{h}_0 & 0 & 0 & \cdots & 0 & 0 & 0 \end{bmatrix}$$

- *a word w.*

Question : $w \in C_1 \cap \overline{C_2}$ *?*
Let us consider the function

$$f_6(w, L_{(n-k)}, \tilde{L}_{(n-k)}) = TH_2^2(f_5(w, L_{(n-k)}), \tilde{f}_5(w, \tilde{L}_{(n-k)}))$$

Theorem 8

For n sufficiently large, we define

$$k = n - (\lceil \log_2(n) \rceil)^2$$
$$f_6 \in TC_5^0.$$

Proof 7
Based on the depth of $\overline{IP}$ and IP we consider two cases:
First case: $\overline{IP}$ and IP are evaluated by a circuit of depth 2.

From the fact that $\overline{IP}$ and IP are evaluated by a circuit of depth 2 and from Lemma 2, we conclude that the size of IP or $\overline{IP}$ is exponential in n. It follows that the size of the function f_6 is also exponential in n.
Then

$$f_6 \notin TC_4^0.$$

Second case: $\overline{IP}$and IP are evaluated by a circuit of depth 3.

From the fact the depth of $\overline{IP}$ and IP is 3, we deduce that the depth of the function f_6 is 5.

From the Theorem 1 the size of the circuit which evaluates:

- $IP(h_{(i*)}, w) \ = \ IP(S^{(n-k-i)}(h_{(n-k)}), w)$ *is* $\mathcal{O}((\log n)^3)$,
- $\overline{IP}(h_{(i*)}, w) \ = \ \overline{IP}(S^{(n-k-i)}(h_{(n-k)}), w)$ *is* $\mathcal{O}((\log n)^3)$.

It follows that the size of f_6 *is* $\mathcal{O}((\log n)^5)$ *, because* $n - k \ = (\lceil \log_2(n) \rceil)^2$. *We easily deduce that*

$$f_6 \ \in TC_5^0.$$

□

The next subsection is denoted to the study of the set TC_6^0

3.5 Element of TC_6^0

In this subsection, we are interested by the function who characterize the symmetric difference of two cyclic codes.

Problem 4

- *Two cyclic codes* C_1 *and* C_2,
- H_1 *parity-check matrix of* C_1,

$$H_1 = \begin{bmatrix} L_{(1)} \\ L_{(2)} \\ \vdots \\ L_{(n-k)} \end{bmatrix} = \begin{bmatrix} 0 & 0 & \cdots & 0 & 0 & 0 & 1 & h_{k-1} & \cdots & h_2 & h_1 & h_0 \\ 0 & 0 & \cdots & 0 & 0 & 1 & h_{k-1} & h_2 & & h_1 & h_0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & h_{k-1} & h_2 & h_1 & & h_0 & 0 & 0 \\ \cdots & \cdots & & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & h_{k-1} & \cdots & h_2 & h_1 & h_0 & 0 & 0 & \cdots & 0 & 0 & 0 \end{bmatrix}$$

- H_2 *parity-check matrix of* C_2,

$$H_2 = \begin{bmatrix} \tilde{L}_{(1)} \\ \tilde{L}_{(2)} \\ \vdots \\ \tilde{L}_{(n-k)} \end{bmatrix} = \begin{bmatrix} 0 & 0 & \cdots & 0 & 0 & 0 & 1 & \tilde{h}_{k-1} & \cdots & \tilde{h}_2 & \tilde{h}_1 & \tilde{h}_0 \\ 0 & 0 & \cdots & 0 & 0 & 1 & \tilde{h}_{k-1} & \tilde{h}_2 & & \tilde{h}_1 & \tilde{h}_0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & \tilde{h}_{k-1} & \tilde{h}_2 & \tilde{h}_1 & & \tilde{h}_0 & 0 & 0 \\ \cdots & \cdots & & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \tilde{h}_{k-1} & \cdots & \tilde{h}_2 & \tilde{h}_1 & \tilde{h}_0 & 0 & 0 & \cdots & 0 & 0 & 0 \end{bmatrix}$$

- *a word* w.

Question : $w \ \in \ C_1 \ \Delta \ C_2$ *?*

Let us consider the function

$$f_7(w, L_{(n-k)}, \tilde{L}_{(n-k)}) = \overline{PARITY}(f_5(w, L_{(n-k)}), f_5(w, \tilde{L}_{(n-k)}))$$

We characterize the function f_7 in the next result.

Theorem 9
For n sufficiently large, define

$$k \ = \ n - (\lceil \log_2(n) \rceil)^3$$

$$f_7 \ \in TC_6^0.$$

Proof 8
Based on the depth of evaluation of $\overline{IP}$ and IP, we consider two cases:

First case: IP and $\overline{IP}$ are evaluated by a circuit of depth 2.

From the fact that the size IP and $\overline{IP}$ is exponential in n, it follows that the size of the function f_7 is also exponential in n. We deduced that:

$$f_7 \notin TC_5^0.$$

Second case: IP and $\overline{IP}$ are evaluated by a circuit of depth 3.

From the fact that the depth of IP or $\overline{IP}$ in 3, we deduce that the depth of the function f_7 is 6.

a) From the Theorem 1*, the size of the circuit which*

- *evaluates* $\overline{IP}(L_{(i)}, w) = \overline{IP}(S^{(n-k-i)}(L_{(n-k)}), w)$ *is* $\mathcal{O}((\log n)^3)$.
- *evaluates* $\overline{IP}(\tilde{L}_{(i)}, w) = \overline{IP}(S^{(n-k-i)}(\tilde{L}_{(n-k)}), w)$ *is* $\mathcal{O}((\log n)^3)$.

b) It follows that the size of

$$f_7 \text{ is } \mathcal{O}((\log n)^6), \quad \text{because } n-k = (\lceil \log_2(n) \rceil)^3.$$

We easily deduce that

$$f_7 \in TC_6^0.$$

□

4 Conclusion

In this paper, by using cyclic codes and their parity check matrix, we have shown that the sets $NP \setminus TC_3^0$, $NP \setminus TC_4^0$ and $NP \setminus TC_5^0$ are not empty.

Acknoweldgments

The authors thanks Professor Marcos KIWI(University of Chile) for useful suggestions.

References

[1] Peter Clote and Evangelos Kranakis, *Boolean Functions and Computation Models* Springer, 2002.

[2] Ian Parberry, *Circuit Complexity and Neural Networks* , *The MIT Press*, 1994.

[3] A. Hajnal, W. Maass, P. Pudlak, M. Szegedy and G. Turan , "Threshold Circuits of Bounded Depth ", *Journal of Computer and System Sciences*, **46**, pp. 129-154, 1993.pp. 207-227, 1994.

[4] D. A. Mix Barrington, N. Immerman and H. Straubing, *On uniformity with in* NC^1, *Journal of Computer and System Sciences*, **41**, pp. 274-306, 1990.

[5] A. C. Yao, *Circuits and local computation* , *Proc. 21st ACM Symposium on Theory of Computing*, pp. 186-196, 1989.

[6] M. Krause and I. Wegener, *Circuit Complexity in Boolean Models and Methods in Mathematics, Computer Science and Engineering* edited by Y. Crama and P.L. Hammer, Cambridge University Press, pp. 506-530, 2010.

[7] Kai Yeung Siu and Jehoshua Bruck, "*On the power of threshold circuits with small weights*", *Siam J. Disc. Math.*, **Vol. 4**,N^o 3, pp. 423-435, 1991.

[8] Reed. I. S., "A class of Multiple-Error Correcting Codes and the Decoding Scheme", *IEEE Trans.Inf. Theory*, **Vol. 4**, pp. 38-49, 1954.

[9] Alberto Ravagnani, "Coding Theory", *Eindhoven University of Technology*, pp. 18-37, February 7, 2022.

[10] Van Lint, J.H., "Introduction to Coding Theory", *Springer, New York-Heidelberg-Berlin*, pp. 5-14, 1982.

[11] Jiri Adamek, "Theory and Applications of Error-Correcting Codes with an Introduction to Cryptography and Information Theory ", *A Wiley-Interscience Publication JOHN WILEY & SONS, INC. Chichester · New York · Brisbane · Toronto · Singapore* , pp. 161-195, 1991