# International Journal of Instrumentation Control and Automation 

Volume 1 | Issue 2
Article 7

July 2011

# Minimize Logic Synthesis FPGA - Extraction And Substitution Problems 

Nguyen Huu Khanh Nhan
Department of Electrical - Electronic, Ton Duc Thang University, Ho Chi Minh City, Vietnam, khanhnhan@tdt.edu.vn

Malinichev D.M.
2Department of Communications - Informatics, Moscow Technical University, Moscow, Russia, mmm-63@list.ru

Follow this and additional works at: https://www.interscience.in/ijica
Part of the Aerospace Engineering Commons, and the Mechanical Engineering Commons

## Recommended Citation

Nhan, Nguyen Huu Khanh and D.M., Malinichev (2011) "Minimize Logic Synthesis FPGA - Extraction And Substitution Problems," International Journal of Instrumentation Control and Automation: Vol. 1 : Iss. 2 , Article 7.
DOI: 10.47893/IJICA.2011.1020
Available at: https://www.interscience.in/ijica/vol1/iss2/7

This Article is brought to you for free and open access by the Interscience Journals at Interscience Research Network. It has been accepted for inclusion in International Journal of Instrumentation Control and Automation by an authorized editor of Interscience Research Network. For more information, please contact sritampatnaik@gmail.com.

# Minimize Logic Synthesis FPGA - Extraction And Substitution Problems 

Nguyen Huu Khanh Nhan ${ }^{1}$ \& Malinichev D.M. ${ }^{2}$<br>${ }^{1}$ Department of Electrical - Electronic, Ton Duc Thang University, Ho Chi Minh City, Vietnam<br>${ }^{2}$ Department of Communications - Informatics, Moscow Technical University, Moscow, Russia<br>E-mail : khanhnhan@tdt.edu.vn ${ }^{1}$,mmm-63@list.ru ${ }^{2}$


#### Abstract

The objective of multi-level logic synthesis of FPGA is to find the "best" multi-level structure, where "best" in this case means an equivalent presentation that is optimal with respect to various parameters such as size, speed or power consumption... Five basic operations are used in order to reach this goal: decomposition, extraction, factoring, substitution and collapsing. In this paper we propose a novel application of Walsh spectral transformation to the evaluation of Boolean function correlation. In particular, we present an algorithm with approach to solve the problems of extraction and substitution based on the use of Walsh spectral presentation. The method, operating in the transform domain, has appeared to be more advantageous than traditional approaches, using operations in the Boolean domain, concerning both memory occupation and execution time on some classes of functions.


Keywords - logic synthesis, Walsh spectral, boolean function, decomposition.

## I. INTRODUCTION

One of the promising directions of the element base of modern technical devices and systems for various applications are field programmable gate arrays (FPGA), which combine the advantages of standard or custom integrated circuits and gate array design with a convenience device, programmed by the user [1]. And FPGA contain a much larger number of logic gates than the complex programmable logic devices (CPLD), programmable logic arrays (PLA), etc. As a result, one FPGA can replace about 20 CPLDs in a variety of applications, thereby reducing the number of devices used in equipment. In addition, increases its reliability due to a decrease in the length of conductors on the circuit board and a smaller number of individual devices, while decreasing the required size of the circuits on the board and reduces the demands on the supply voltage. In this FPGA are the standard product, and users avoid many costs inherent in ASIC. But the problem of logic synthesis (LS) FPGA is much more complicated than traditional IP or gate array, due to their architectural features as the basic blocks and more complex interconnections between resources in the crystals.

The analysis of architecture and technology of FPGA allows us to conclude that, in addition to common for the entire microelectronics industry trends to increase the degree of integration, improving overall
performance, reduce costs, etc., the new trend is the increased ease of design and debug circuits. However, with increasing complexity of both the crystals and projects to the fore front more and more are questions of design and development of algorithms for automatic logic synthesis. It follows that the main problem of logic synthesis (LS) in the basis of FPGA is minimize the number of used logic blocks and reducing the complexity of the trace.

## II. KEY TASKS FOR FPGA LOGIC SYNTHESIS

When logic synthesis (LS) FPGA often use the technique of design separation into two distinct phases [3], the technology-independent and technologydependent (technology mapping).

We describe in more detail the mathematical problems that arise when considers are the basis of FPGA as well as possible and suggest solutions. Based on an analysis of FPGA architecture, we use methods based on five basic mathematical problems: Decomposition [8], factoring, extraction, substitution and collapsing.

To illustrate the features of the problem consider in the basis of FPGA, look at an example. Let's the number of inputs $B F$ is $m=5$, and $f_{1}=\operatorname{abcdeg}$ and $f_{2}=$ $a b c+b d e+a e+c d$. The functions $f_{1}$ and $f_{2}$ in its implementation are 6 and 10 literals, respectively. In addition, the function $f_{1}$ requires for its optimal
implementation of two CLB, while $\mathrm{f}_{2}$ - only one, since $\mathrm{f}_{2}$ - function of 5 variables.
we introduce some definitions.
Definition 1. Expression is a free cube if there is another cube, this expression is divisible by precisely: ie, $a b+c-$ is free of a cube, $a b+a c-n o$.
Definition 2. The main divider expression f - a set of expressions of the form $D(f)=\{f / C \mid C$-free cube $\}$.
Definition 3. The core of the expression $f$ is the set of expressions of the form $K(f)=\{g \mid g \in D$ (f) and $g$ free cube $\}$.
Definition 4. The balance of the original function f, associated with the nucleus K , obtained by replacing the variable of this function for all occurrences of $K$ in the $f$.

Definition 5. The basis function f, denoted as sup (f) - a set of variables which it depends on. In this case, using the operation $|\sup (\mathrm{f})|$ can find the inverse function.

Definition 6. The feature is called feasible if $|\sup (\mathrm{f})|<$ m , ie. feasible function can be implemented in one CLB.
Definition 7. Boolean network is realizable if every intermediate node implements a workable option.

The number of intermediate nodes implemented Boolean network gives an upper bound on the number CLB, necessary for its implementation. Thus, a fairly obvious looks conclusion in [2] that the synthesis algorithm can be divided into two phases, the first of which involves the construction of realizable networks, and the second - to minimize the number of nodes. And the first step usually involves the use of decomposition and extraction procedures, and the second is factoring, substitution and collapsing.

The above problems arise in the design of any architecture of FPGA. Some of their aspects were considered in [4] in terms of spectral processing BF. These studies showed promise using spectral analysis of BF for solving problems of use FPGA. In this case, the gain occurs mainly in the processing of large amounts of input data.

Note that the complexity of solving all of these math problems can be significantly reduced with the use of spectral representations of BF in the basis of Walsh functions. As a result, methods of implement FPGA can be optimized on the basis of this presentation. In this paper to solve the problems of extraction and substitution.

Extraction is process of identifying and creating some intermediate functions and variables, and reexpressing the original functions in term of the
intermediate plus the original variables. The process is used to identify the common sub-expressions.

Substitution is the process of expressing a function $F$ as a function of second function G, plus the original inputs to the function $F$. This is done by substituting $G$ into $F$ where ever possible.

## III. SPECTRAL ANALYSIS OF BOOLEAN FUNCTIONS

We use the definition of BF in the monographs [4], where they are treated as multi-dimensional functions with $m$-inputs and k-outputs, and carry out mapping of the form:

$$
\begin{equation*}
f:\{0,1\}^{m} \rightarrow\{0,1\}^{k} \tag{1}
\end{equation*}
$$

Set of outputs is denoted as BF $f_{k-1}, \ldots f_{0}$, and used the decimal indices $x=\left(X_{m-l, \ldots,} X_{0}\right) €\{0,1\}^{m}$ are calculated

$$
\begin{align*}
& \text { the formula: } \\
& \qquad x=\sum_{i=0}^{m-1} x_{i}  \tag{2}\\
& f=\left(f_{k-1}, \ldots ., f_{0}\right) \in\{0,1\}^{k}, f=\sum_{i=0}^{m-1} 2^{i}  \tag{3}\\
& f_{i} 2^{i}
\end{align*}
$$

Where x and f can be interpreted as the coordinates of the binary vectors to decimal numbers.

Note that the expressions (2) and (3) describe the BF as a piecewise constant function $F(x)$ of real argument on the half-open interval $\left[0,2^{m}\right]$. With this notation system of BF (1) can be represented as a lattice of $y=f(x)$, defined at the points $0,1 \ldots, 2^{m}-1$ interval $\left[0,2^{m}\right]$.

Extend the function $y=f(x)$ to piecewise constant function $F(x)$ as follows:

$$
\begin{equation*}
F(x)=f(\delta) \text { variations } x \in[\delta, \delta+1] \tag{4}
\end{equation*}
$$

We say that a piecewise constant function $F(x)$ represents the original system of BF, if it satisfies the condition (4) and $\mathrm{f}(\mathrm{x})$ is constructed by formulas (1) and (3). Thus, the foundation can be described as a vector:

$$
F=\left[f(0), f(l) \ldots . . f\left(2^{m}-l\right)\right]^{T}
$$

where $X=\left(\begin{array}{lll}x_{m}-1 & \ldots & X_{0}\end{array}\right),\left(0<x<2^{m}-l\right)$ - a set of input vectors, and $f(x)$ is an integer value, where $F_{i}=\left[f_{i}(0)\right.$, $\left.f_{i}(l) \ldots . f_{i}\left(2^{m}-l\right)\right]^{T}$, and $f_{i}(x), 0<i<k-l$, a binary value.

It is known that between BF and Walsh functions, there is a relationship, which explains the possibility of effective use of spectral analysis in the basis of Walsh functions to analyze the fleet. In order to determine this relationship, we consider details of the Walsh function.

These functions are piecewise constant and are given on the half-open interval $\left[0,2^{m}\right]$ expression:

$$
\begin{equation*}
W_{\omega}(x)=(-1)^{\sum_{i=0}^{\omega-1} \omega_{(m-i-i)^{2}}} \tag{5}
\end{equation*}
$$

where $0<\omega<2^{m}-1, m \in N$, and $\omega_{i}$ and $x_{i}$ are determined from the binary representations $\omega$ and $x$.

$$
\begin{align*}
& \omega=\sum_{i=0}^{m-1} \omega_{i} 2^{m-1-i}  \tag{6}\\
& \text { a. } x=\sum_{i=0}^{\infty} x_{i} 2^{m-1-i} \tag{7}
\end{align*}
$$

$\omega$ number for the function $W_{\omega}(x)$ is called its index, and the number of units in the binary expansion $\omega$, ie. Quantity $\|\omega\|=\sum_{i=0}^{m-1} \omega_{i}$ called weight index or rank.

Consider a subset of Walsh functions with the weight index of 1 . Denote their symbols $R_{i}(x)(i=l, 2$, ... $m$ ). Then (5) (6) we obtain:

$$
\begin{gather*}
R_{j}(x)=W_{2^{(i-1)}}(x)=(-1)^{x^{i-1}}=\exp \left(j \frac{2 \pi}{2} x^{(i-1)}\right)  \tag{8}\\
j=\sqrt{-1} \quad R_{0}(x)=W_{0}(x)=1
\end{gather*}
$$

Function $R_{i}(x)$, defined by (8) are called Rademacher functions. As shown in [4], as a product of Rademacher functions can be represented by any Walsh function, ie:

$$
\begin{equation*}
W_{\omega}(x)=\prod_{i=0}^{m-1}\left(R_{i+1}(x)\right)^{\omega^{(m-1-i)}} \tag{9}
\end{equation*}
$$

Fast algorithms of spectral transformations in the basis Walsh similar fast discrete multiplicative transformations, using as a basis of trigonometric functions, i.e. in particular, fast Fourier transform (FFT). Issues of generalization of discrete multiplicative transformations over finite fields are considered in some detail [5], where the main theorem and in this area.
Theorem 1. Let $\Phi(x)$ - a step function representing a system of BF in m variables and $S(\omega)\left(\omega=0,1, \ldots 2^{m}-1\right)$ its spectrum by Walsh.

Then $S(\omega)=2^{-m} a_{m}(\varpi)$, where if $\omega=\sum_{i=0}^{m-1} \omega_{i} 2^{m-1-i}$, then $\varpi=\sum_{i=0}^{m-1} \omega_{i} 2^{i}$, and

$$
a_{0}(\omega)=\Phi(\omega)
$$

$$
\begin{align*}
& a_{0}\left(2^{m-1}+\omega\right)=\Phi\left(2^{m-1}+\omega\right) \\
& a_{s}(\omega)=a_{s-1}(2 \omega)+a_{s-1}(2 \omega+1)  \tag{10}\\
& a_{s}\left(2^{m-1}+\omega\right)=a_{s-1}(2 \omega)-a_{s-1}(2 \omega+1) \\
& \left(\omega=0,1, \ldots 2^{m-1}-1\right) ;(s=1,2, \ldots m)
\end{align*}
$$

The number of operations $N_{w}$, you want to produce this algorithm for computing $S(\omega)$, as in the case of calculating the FFT is equal to $N \cdot \log _{2} N$, where $N$ - number of arguments, or because the actions are performed with a binary representation of the arguments, $N_{w}=2^{m} * m$, Where $m$ - number of bits of the arguments.

Walsh spectrum $\hat{F}$ can be calculated as follows:

$$
\begin{gathered}
\hat{F}=[W]_{m} * F, \text { where } \\
{[W]_{m}=\left[\begin{array}{ll}
{[W]_{m-1}} & +[W]_{m-1} \\
{[W]_{m-1}} & -[W]_{m-1}
\end{array}\right], \text { where }[W]_{1}=\left[\begin{array}{cc}
1 & +1 \\
1 & -1
\end{array}\right]}
\end{gathered}
$$

There is also the inverse Walsh, with which you can restore the BF using the relation:

$$
\hat{F}: F=\hat{F} *[W]_{m}
$$

This method of computing the Walsh spectrum is more suitable for the calculation of matrices of small dimensions. In this case, the above-introduced the matrix $[W]_{m}$ are the Hadamard matrices.

Note that all the above properties of Walsh functions can be formulated in terms of Hadamard matrices, so that the Walsh transform is sometimes called the Walsh-Hadamard transform.

## IV. CORRELATION ANALYSIS OF BOOLEAN FUNCTIONS

Autocorrelation function of $\operatorname{BF} f\left(x_{0}, x_{1}, \ldots, x_{m-1}\right)$ is determined on the basis of relations:

$$
\begin{equation*}
B_{2}^{(f ; f)}(\tau)=\sum_{x=0}^{2^{m}-1} f(x) f(x \oplus \tau) \tag{11}
\end{equation*}
$$

where $\tau \in\left\{0,1, \ldots, 2^{m}-1\right\}$.
As seen from (11), the original function is related to the autocorrelation function of convolution transforms.

Cross-correlation or simply the correlation function of two $\operatorname{BF} f_{1}(x)$ and $f_{2}(x)$ is the function:

$$
\begin{equation*}
B_{2}^{(f 1 ; f 2)}(\tau)=\sum_{x=0}^{2^{m}-1} f_{1}(x) f_{2}(x \oplus \tau) \tag{12}
\end{equation*}
$$

where $\tau \in\left\{0,1, \ldots, 2^{m}-1\right\}$

Establish a connection between the correlation functions and features considered earlier Walsh. To consider the following two theorems.

Theorem 2. Dual application of Walsh transform to the piecewise constant function $F(x)$ does not alter this function up to a normalizing factor of $2^{-m}$. Indeed,

$$
\begin{equation*}
S_{\overline{S_{f(x)}}}(x)=2^{-m} f(x) \tag{13}
\end{equation*}
$$

Proof: due to the symmetry

$$
\begin{aligned}
& \overline{S_{f(x)}(\omega)}=2^{-m} \sum_{x=0}^{2^{m}-1} f(x) W_{\omega}(x) \\
& S_{\overline{S_{f(x)}}}(x)=2^{-m} \sum_{\omega=0}^{2^{m}-1} S_{f(x)}(\omega) W_{x}(\omega)= \\
& =2^{-m} \sum_{\omega=0}^{2^{m}-1}\left(2^{-m} \sum_{g=0}^{2^{m}-1} f(g) W_{\omega}(g)\right) W_{\omega}(x)=
\end{aligned}
$$

by shifting the argument

$$
\begin{aligned}
& =2^{-m} \sum_{\omega=0}^{2^{m}-1} \sum_{g=0}^{2^{m}-1} f(g) W_{\omega}(g \oplus x)= \\
& =2^{-2 m} \sum_{\omega=0}^{2^{m}-1} f(g) \sum_{g=0}^{2^{m}-1} W_{\omega}(g \oplus x)=
\end{aligned}
$$

From the orthogonal condition

$$
=2^{-m} \sum_{g=0}^{2^{m}-1} f(g)=2^{-m} f(x)
$$

Theorem 3. Let two BF of $m$ arguments, and two lattice functions $f_{1}(x)$ and $f_{2}(x)$, corresponding to them. Then

$$
\begin{equation*}
B_{2,2}^{(f 1, f 2)}=2^{2 m} \overline{W\left(W\left(f_{1}\right) \overline{W\left(f_{2}\right)}\right)} \tag{14}
\end{equation*}
$$

Proof:

$$
S_{1}(\omega) \overline{S_{2}(\omega)}=2^{-2 m} \sum_{x 1, x 2=0}^{2^{m}-1} f_{1}\left(x_{1}\right) f_{2}\left(x_{2}\right) W\left(x_{1}\right) W\left(x_{2}\right)
$$

Then, in view of theorems on the completeness and orthogonality, symmetry index and the argument of the argument and shift operations involution [8], we have:

$$
\begin{aligned}
& \overline{W\left(W\left(f_{1}\right) \overline{W(\tau)}\right.}=2^{-m} \sum_{\omega=0}^{2^{m}-1} S(\omega) \overline{S_{2}(\omega)} W(\omega)= \\
& =2^{-3 m} \sum_{\omega=0}^{2^{m}-1} \sum_{x 1, x 2=0}^{2^{m}-1} f_{1}\left(x_{1}\right) f_{2}\left(x_{2}\right) \overline{W_{\omega}\left(x_{1} \oplus x_{2} \oplus \tau\right)}=
\end{aligned}
$$

$$
\begin{aligned}
& =2^{-2 m} \sum_{x 1, x 2=0}^{2^{m}-1} f_{1}\left(x_{1}\right) f_{2}\left(x_{1} \oplus \tau\right)+ \\
& 2^{-3 m} \sum_{x 2 \neq x 1 \oplus \tau} f_{1}\left(x_{1}\right) f_{2}\left(x_{2}\right) \sum_{\omega=0}^{2^{m}-1} W_{\omega}\left(x_{1} \oplus x_{2} \oplus \tau\right)=
\end{aligned}
$$

From the orthogonal condition.

$$
=2^{-2 m} \sum_{x 1=0}^{2^{m}-1} f_{1}\left(x_{1}\right) f_{2}\left(x_{1} \oplus \tau\right)
$$

Note that Theorem 3 is also known as WienerKhinchin theorem [6].

In view of Theorems 2 and 3, we find that for BF, the following relation:

$$
\begin{equation*}
B_{2,2}{ }^{(f 1, f 2)}=2^{2 m} W\left(W\left(f_{1}\right) W\left(f_{2}\right)\right) \tag{15}
\end{equation*}
$$

Properties of the correlation characteristics of BF determined by the properties of convolution transforms of the original features. In particular, the form of these transformations implies the invariance of the correlation characteristics to shift the argument of the original. Converse is also true that the autocorrelation function of the original function can be restored up to a shift of the argument.

For the BF shift of the argument is equivalent to $\alpha$ inversion of those arguments, which correspond to the nonzero components of the binary expansion of $\alpha$. Therefore, the complexity of realizing the foundation in any basis, is completely determined by its autocorrelation function up to $m$ elements of the inversion, where $m$ - number of arguments of BF. This makes it possible to solve all the problems associated with minimizing the complexity of circuits that implement the system of BF , the language of the correlation characteristics, which is done in this paper.

## V. RECOGNITION OF BOOLEAN FUNCTIONS

Obviously, for the recognition the linearity of BF is sufficient to calculate its Walsh spectrum, and if this range contains only one non-zero point $\omega=c$ (not counting the point $\omega=0$ ), then BF is linear and is represented in the form.

$$
\begin{equation*}
f(x)=\bigoplus_{i=0}^{m-1} c_{i} x_{i} \tag{16}
\end{equation*}
$$

Recognition of the self-dual (anti self-duality) BF [9] reduces to the calculation of the value of its autocorrelation function at a point $2^{m}-1$.

Recall that a $\operatorname{BF} f\left(x_{0}, \ldots, x_{n}\right)$ is called self-dual (anti self-duality) then only when it takes on the opposite
sets of opposite (or same anti self-duality function) values. A set of self-dual and anti self-duality functions form the class of functions closed under composition [9]. Since the properties self-dual (anti self-duality) are invariant to a shift in the arguments of BF, their detection may be accomplished by analyzing the autocorrelation function of $B F$.

Theorem 4. To BF $f(x)=f\left(x_{0}, \ldots, x_{n}\right)$ has been self-dual (anti self-duality) is necessary and sufficient that:

$$
\begin{align*}
& B\left(2^{m}-1\right)=0  \tag{17}\\
& \left(B\left(2^{m}-1\right)=\sum_{x=0}^{2^{m}-1} f(x)\right) \tag{18}
\end{align*}
$$

In addition, in the literature the notion $\alpha$ self-dual (anti self-duality). For BF, it would take place if and only if there is , $\alpha$ such that:

$$
\begin{align*}
& f\left(x_{0}, \ldots, x_{m-1}\right)=\overline{f\left(x_{0}^{\alpha_{0}}, \ldots, x_{m-1}^{\alpha_{m-1}}\right)}  \tag{19}\\
& \left(f\left(x_{0}, \ldots, x_{m-1}\right)=\overline{f\left(x_{0}^{\alpha_{0}}, \ldots, x_{m-1}^{\alpha_{m-1}}\right)}\right)  \tag{20}\\
& \qquad x_{j}^{\alpha_{j}}=\left\{\begin{array}{l}
\overline{x_{j}}-\alpha_{j}=0 \\
x_{j}-\alpha_{j}=1 \quad \text { with }
\end{array}\right. \\
& \text { Where }
\end{align*}
$$

$$
\alpha=\sum_{i=0}^{m-1} \alpha_{i} \cdot 2^{m-1-i} \text { and } \bar{\alpha}=\sum_{i=0}^{m-1} \bar{\alpha}_{i} \cdot 2^{m-1-i}
$$

Note that for the same $\operatorname{BF} f(x)$ there may be several $\alpha_{l}, \ldots, \alpha_{g}$ such that $f(x) \quad \alpha_{i}-\operatorname{self-dual}(i=1, \ldots, g)$ and a few $\beta_{1}, \beta_{2}, \ldots, \beta_{h}$ such that $f(x) \beta_{i}$ - anti self-duality $(i=$ $1, \ldots, h)$. In this case, any BF 0 - anti self-duality, and if it $\beta_{i}$ - anti self-duality and $\beta_{j}$ - anti self-duality, then $\left(\beta_{i}\right.$ $\oplus \beta_{j}$ ) anti self-duality. Thus, the set of points for any anti self-duality foundation is a group (with group operation $\oplus$ ) and the number of points anti selfduality (order of) is equal to $2^{i}, i \in\{0,1\}$. Point group, anti self-duality group called the inversion of variables. If $f\left(x_{0}, x_{2} \ldots, x_{m-1}\right) 2^{s}$ - self-duality, then $f\left(x_{0}, x_{2} \ldots, x_{m-1}\right)$ does not depend on $x_{s}$.

Theorem 5. The function $f(x)=\left(x_{0}, \ldots ., x_{m-1}\right)$ has points self-dual $\alpha_{l}, \ldots, \alpha_{g}$ and the points anti self-duality $\beta_{l}, \ldots, \beta_{h}$, if and only if when
$B\left(\alpha_{i}\right)=0 \quad(i=1,2, \ldots, g)$
$B\left(\beta_{i}\right)=\sum_{x=0}^{2^{m}-1} f(x) \quad(i=1,2, \ldots, h)$
It is obvious that Theorem 5 generalizes Theorem 4 in $\alpha=2 m-1(\beta=2 m-1)$.
consequence. For any BF $f(x)$ the number of points at which the autocorrelation function takes a value $\sum_{x=0}^{2^{m}-1} f(x)$
, equal to $2^{i}, i \in\{0,1\}$, and the corresponding samples of the autocorrelation function of a group. Thus, the zeros of the autocorrelation function is determined self-dual point, and the maximum count equal to $\sum_{x=0}^{2^{m}-1} f(x)$ - point anti self - duality. These results are used in particular for the analysis of linear codes [12].

Since monotone functions represent the other pole of complexity in their implementation of linear functions, the language of correlation functions is not very suitable for implementation. Although, by some weakening of the notion of monotony, which is the concept of a threshold of BF, you can get some interesting results. Thus, in [13] was proposed to implement the foundation for the linear-threshold network, described in terms of Walsh spectral coefficients, and in [14], a tabulation the spectra of threshold functions. In addition, known techniques that allow, in specific cases to obtain engineering solutions for a number of arguments, not exceeding six. In [15] introduced the condition of n-monotony of BF using the Walsh spectral coefficients, but it requires too many definitions and intermediate results and therefore not included here. Some practical results of work [15] can be found in [16].

In order to further address issues of recognition of BF using the Walsh spectra, we introduce additional notation:

$$
\begin{equation*}
S(W)=\left(S\left(W_{0}\right), \ldots ., S\left(W_{2^{n}-1}\right)\right. \tag{23}
\end{equation*}
$$

where $S$ - range of functions; $W$ - domain transformation of BF, in addition, $d_{0}\left(W_{\omega}\right)$ - the number of constituents of $\mathrm{BF} \mathrm{f}(\mathrm{x})$ for each value of $W_{\omega}$.

Then $S\left(W_{j}\right)=d_{0}\left(W_{j}\right)-d_{l}\left(W_{j}\right)$ for any $W_{j} \in W$. We divide the region transform into subsets and call their levels, i.e. $W^{n}=\left\{W^{(0)}, \ldots ., W^{(n)}\right\}$. In addition, we say that $W^{j} \in W^{(l)}, l=1 \div n$, if $\left\|W_{j}\right\|=1$. Consequently, the set of spectral coefficients are also divided into levels $S(W)=\left\{S^{(0)}, \ldots ., S^{(n)}\right\}$, where $S\left(W_{j}\right) \in S^{(1)}$, if $\left\|W_{j}\right\|=l$. The coefficient $S\left(W_{0}\right)$ indicates the number constituents of the unit BF.

The function $f(x)$ partially symmetric with respect to $x_{m}$ and $x_{k}$, if the permutation $x_{m}$ and $x_{k} f\left(x_{i}\right)=f\left(x_{i}\right.$ * $\left.P_{m, k}\right)=f\left(x_{j}\right)$, for all $x_{j} \in X^{n}$, where $P_{m, k}$ - substitution matrix dimension $n \times n$, and $\operatorname{det} P_{m, k}=1 ; p_{i, j} \in\{0$; $1\}$; In addition, $P_{m, k}^{-1}=P_{m, k}^{-T}$. Then obviously $\left\|x_{i}\right\|=$ $\left|\left|x_{j}\right|\right|$.

Theorem 6. BF $f(x)$ partially symmetric if and only if $S\left(W_{j}\right)=S\left(W_{q}\right)$, where $W_{q}=W_{j} * P_{m, k}, W_{q}, W_{j} \in W^{(l)}$.
BF called completely symmetric if $f\left(x_{j}\right)=f\left(x_{j} * P\right)$ for any $X_{i} \in P$, where $P$ - the matrix any permutation of the permutation group of order $n!$. Since any permutation matrix can be represented as a product, then using Theorem 6, we obtain proof of the corollary below.

Consequence. BF is symmetric if and only if $\left|S\left(W_{j}\right)\right|=$ $\left|S\left(W_{q}\right)\right|$ for all $W_{q}, W_{j} \in W^{(t)}$, where $1=1 \div n$, i.e. symmetric function is equal in absolute Walsh coefficients at each level.

Thus, the basic properties of the BF, i.e. linearity, self-dual (anti self- duality) different with orders of symmetry and partial symmetry, can be identified using the Walsh spectrum.

## VI. PROBLEMS OF EXTRACTION AND SUBSTITUTION.

To describe the algorithm for extraction recall that the autocorrelation function of a Boolean function (BF) [9] is the similarity measure of its output at a certain distance in the space of BF. At the same time unit in the binary representation of addresses maximum ratio BF indicate what arguments are involved in its formation, therefore, the minimum number in the value of the autocorrelation function corresponds to the minimum BF coupling between its arguments. Based on these general considerations, the authors propose an algorithm for solving the problem of extraction, described below.

Initially formed by the coefficients of the autocorrelation function of BF. Then take into account factors "first tier", ie depending on one variable, and among them is sought with a minimum rate. If you have coefficients with the same value, then made advanced search of the coefficients of the relevant variables at the next tier. Depending on the results of this search and select and the minimum ratio. After finding the minimum rate and to determine the original function arguments, on which it depends, there is a transition to the coefficients of the "second tier", that is dependent on two variables. In this case the coefficients in the formation of which was attended by the same arguments as in the formation of a minimum ratio of the first tier, we seek the minimum ratio. Then jumps to the next tier, etc. After completing the loop through all tiers of the above algorithm is repeated for the other variable.

Note that the above algorithm for solving the extraction is the matrix analogue of the well-known algorithm "branch and bound", which guarantees finding is not necessarily better, but quite a good result. A very strong positive aspect of the proposed algorithm from the standpoint of reduction of brute force is the fact that the minimum ratio is sought not the entire table length
$2^{n}$, but only among $\mathrm{C}_{\mathrm{n}}^{\mathrm{i}}$ coefficients, where n - total number of arguments, and i- number of arguments on a particular tier.

Thus, the proposed algorithm for solving the division consists of the following:

1. Verified by the simultaneous fulfillment of conditions $B\left(\tau_{0}\right)=\max _{|\tau| \neq 0} B(\tau)$ and $\|\tau\|=1$;
2. Determined $\|\tau\|=x_{i 1}, \ldots, x_{i n}$;
3. Verified that the inequality $\sum_{j=1}^{n} x_{i j} \leq M$ and $\tau \leq n ;$
4. Determined $B\left(\tau_{i}\right)=\min _{|\tau| \leq i} B(\tau)$;
5. Go to step 1 .

In the above procedures sequence $\|\tau\|$ - capacity expansion, $\tau$ - binary address, $M$ - number of inputs of CLB.

We describe an algorithm for extraction example of the following functions: $f\left(x_{3}, x_{2}, x_{1}, x_{0}\right)=\left(x_{0} \oplus X_{l}\right) \&\left(X_{2} \oplus\right.$ $\left.X_{3}\right)$. Define $F=[0,0,0,0,0,1,1,2,0,1,1,2,0,2,2,4]^{T}$, that is $B=[36,24,24,16,24,12,12,8,24,12,12,8,16,8,8,4]$. From the analysis in that all the functions of the first tier of the same, ie value of the autocorrelation function of BF in these points is 24 . By viewing the advanced find out that the function is symmetrical. Therefore, as the first variable we take $x_{0}$, having minimum values of the autocorrelation of the variables $x_{3}$ and $x_{2}$. This means that the separation (cutting) of the original BF should be performed by separating the variable $x_{0}$ from $x_{3}$ and $x_{2}$. After a similar operation for the variable $x_{l}$, we obtain a similar result: $x_{1}$ requires separation of $x_{3}$ and $x_{2}$. Given the fact that the restriction on the number of variables is two, we find that this feature should be implemented by cutting into two parts $-x_{3}$ and $x_{2}$, as well as $x_{0}$ and $x_{1}$.


Algorithm for solving the extraction.
Another task logic synthesis FPGA - the task of the substitution (merge) - is proposed to solve by analyzing the autocorrelation function of the table corresponding

BF. In this case there are two possible levels of addressing the merge. At a higher level problem is solved not only the merge of the original BF , but also because of previously conducted its decomposition. The task becomes much more complicated because of the substantial increase in the number of searched options.

As one of the possible methods of solving the above problems we propose the following hierarchical algorithm. The first step is the analysis of the autocorrelation function table for BF couples find its values in the formation of which involved no more than three input CLB. The analysis is performed by an algorithm similar to the proposed decomposition, and, if not the subsequent stages, then this problem can be regarded as a special case of decomposition. Obtained for pairs of candidates for a merge originally carried out to verify that the terms of the presence in each pair no more than four inputs. The next step is to check the condition limiting the total number of entries to five. This order of testing candidates for a possible merge due to the fact that the total number of inputs is always restricted by the inequalities: $C_{n}{ }^{3} \leq C_{n}{ }^{4} \leq C_{n}{ }^{5}$, which leads to a reduction in the total number of options searched.

## VII. CONCLUTION.

It follows that the use of spectral analysis techniques in the basis of the Walsh representation for solving problems of extraction and substitution is highly effective. In the future the author envisions the building of the upper bounds of the spectral algorithms in their application for synthesis of FPGA.

This problem arise in the design of any architecture of FPGA. Some of their aspects were considered in $[10,11]$ in terms of spectral processing BF. These studies showed promise using spectral analysis of BF for solving problems of use FPGA. In this case, the gain occurs mainly in the processing of large amounts of input data.

## REFERENCES

[1] Goldenberg LM,Matyushkin BD,Polak MN "Digital Signal Processing." Moscow: Radio Svyaz, 1985.
[2] Murgai R., Nishizaki Y., Shenoy N., Brayton R. K., Sangiovanni-Vlncentelli A. "Logic synthesis algorithms for programmable gate arrays" In Proc. of the CM/IEEE Design Autom. Conf. (Orlando, FL, June), 620-625. 1990.
[3] F. Mailhot and G. De Micheli, "Algorithms for technology mapping based on binary decision diagrams and on Boolean operations", IEEE

Trans. On CAD, vol. 12, no. 3, pp. 599-620, May 1993.
[4] Darrlnger J., Joyner W., Berman L, Trellyan L "Logic Synthesis through local transformation" IBM J. Res. Develop., v.25, №4, pp.272-280, July 1981.
[5] Muzio J.C. "Composite Spectra and the Analysis of Switching Circuits" IEEE Trans. On Comput Vol. C-29, № 8 Aug. 1980.
[6] Karpovsky M.G. "Finite Ortogonal Series In the Design of Digital Devices" NY.:Wiley, 1976.
[7] Zeidman B. "All about FPGAs / Logic Design Line". March 21. 2006.
[8] Karp R. M. "Functional decomposition and switching circuit design" J. SIAM 11,2, 291-335. 1963.
[9] Preparata F.P. "VLSI algorithms and architecture" In M.P. Chytil, V. Koubek (ed.;Lecture notes In Computer Science 176), Springer-Verlag, 1984.
[10] Pratt W., Kane J., Andrews H.C., "Hadamard transform image coding" Proc. IEEE Vol. 57, № 1 pp. 58-68, 1969.
[11] Trimberg S."Reprogrammable Gate Arrays and Applications" Proc. of the IEEE,V.81,N 7, July 1993.
[12] Karp R.M. "deducibility among combinatorial problem on Complexity of Computer computation" ,1972.
[13] Gary M. D. Johnson, "Computers and Intractability problem" ed. AA Friedman - Mir, 1982.
[14] M. Dertouzos, "Threshold Logic," Trans. from English. edited by VI Warsaw, Moscow, Mir.ZhT. - pp. 342.
[15] Sapozhenko AA, "On the complexity of disjunctive normal forms obtained by the gradient algorithm," Discrete Analysis. Vyp.21, Novosibirsk, 1972 -pp.62-71.
[16] Proc. IEEE, "Custom Integrated Circuits conference", Boston, Mass., May 13-16, 1990 (N.Y.).1990, pp. 27.5.1-27.5.4.
[17] M. J. Ciesielski. S. Yang, and M. A. Perkowski, "Minimization of multiple-valued logic based on graph coloring," Tech. Rep. TR-CSE- 90.13, Dep. Elect. Comp. Eng., Univ. of Massachusetts. Amherst, Sept. 1990.

