On Welch-Gong Transformation Sequence Generators

G. Gong and A. M. Youssef

Center for Applied Cryptographic Research
Department of Combinatorics & Optimization
University of Waterloo
Waterloo, Ontario N2L 3G1, CANADA
{ ggong, a2youssef}@cacr.math.uwaterloo.ca

Abstract. Welch-Gong (WG) transformation sequences are binary sequences of period $2^n - 1$ with 2-level auto correlation. These sequences were discovered by Golomb, Gong and Gaal in 1998 and verified for $5 \leq n \leq 20$. Later on, No, Chung and Yun found another way to construct the WG sequences and verified their result for $5 \leq n \leq 23$. Dillon first proved this result for odd n in 1998, and finally, Dobbertin and Dillon proved it for even n in 1999. In this paper, we investigate a two-faced property of the WG transformation sequences for application in stream ciphers and pseudo-random number generators. One is to present randomness or unpredictability of the WG transformation sequences. The other is to exhibit the security property of the WG transformations regarded as Boolean functions. It is shown that the WG transformation sequences, in addition to the known 2-level auto correlation, have three-level cross correlation with m-sequences, large linear span increasing exponentially with n and efficient implementation. Thus this is the first type of pseudo-random sequences with good correlation and statistic properties, large linear span and efficient implementation. When the WG transformation are regarded as Boolean functions, it is proved that they have high nonlinearity. A criterion for whether the WG transformation regarded as Boolean functions are r-resilient is derived.

Key words. Stream cipher, pseudo-random sequence (number) generator, auto/cross correlation, linear span, Boolean function, non-linearity, r-resilient property.

1 Introduction

Pseudo-random sequences have been widely used in communications and cryptology. There are three major techniques of pseudo-random sequence generators as cryptographic algorithms: stream cipher algorithms, block cipher algorithms and pseudo-random number generators. The security of stream cipher systems and block cipher systems is directly determined by the randomness or unpredictability of the employed pseudo-random sequence generators. In practical applications, a secure communication system that uses public-key algorithms always employs a pseudo-random sequence generator as its session key or its private key generator. So, the security of the system not only depends on the public key algorithms, but also relies on the security of such a generator, which is realized by a pseudo-random sequence generator. In order to guarantee that the pseudo-random sequence generators have good randomness or unpredictability, we have the following criteria:

- Long period
- Balance property (Golomb Postulate 1 [4])
- Run property (Golomb Postulate 2)

- n-tuple distribution
- Two-level auto correlation (Golomb Postulate 3)
- Low-level cross correlation
- Large linear span and smooth increased linear span profiles

In the past two years, there has been a celebrated event in the design of binary sequences with 2-level auto correlation. The researchers [3] [5] [10] [12] [14] have found a number of new classes of binary sequences with 2-level auto correlation. In general, a pseudo-random sequence generator which generates sequences with 2-level auto correlation can be resistant to a correlation attack. However it is not easy to design a pseudo-random sequence generator which can generate sequences having both 2-level auto correlation and large linear span and be efficient to implement as well. Fortunately, it happened that one of classes of new sequences with 2-level auto correlation, so-called the Welch-Gong transformation sequences, possesses all these three properties. On the other hand, this type of sequences has period $2^n - 1$. Any binary sequence of period $2^n - 1$ is related to a function from the finite field $GF(2^n)$ to the finite field $GF(2)$. Thus it is automatically related to a Boolean function in n variables. Thus there is a connection among binary sequences with period $2^n - 1$, polynomial functions from $GF(2^n)$ to $GF(2)$ and Boolean functions in n variables. Chang, Dai and Gong [1] tried to use this connection. I.e., they applied m-sequences with three-level cross correlation to construct Boolean functions with the maximal non-linearity. In [8], Gong and Golomb successfully tried again to utilize this connection. They applied tools in pseudo-random sequence design and analysis to analyze the S-boxes in DES (Data Encryption Standard). When they considered the relationship between sequences and functions, they realized that monomials, which correspond to m-sequences, are not secure when used as component functions in block ciphers. This leads to a concept of linear span for polynomial functions introduced in their recent work [8] . In this paper, we will investigate the Welch-Gong transformation sequences in a two-faced aspect. One is to present their randomness, i.e., auto correlation, cross correlation with m-sequences, the balance property, and linear span when we consider them as sequences. The other is to derive the nonlinearity, the resilient property, linear span and degree when they are regarded as Boolean functions.

This paper is organized as follows. In section 2, we give the definition of Welch-Gong transformation sequences. In Section 3, we present the randomness properties of the Welch-Gong transformation sequences which include an irregular decimation property, statistic properties, cross correlation with m-sequences, the Hadamard transform, and the linear span. In section 4, we derive the nonlinearity and a criterion for the resilient property (Note. Since any Welch-Gong transformation is balanced, so the correlation immunity property becomes the resilient property). In section 5, we discuss linear span for the Welch-Gong transformations regarded as Boolean functions and show their degrees. Section 6 is a conclusion.

We conclude this section by providing some preliminaries for sequence designs. The reader is referred to [4] for shift register sequences, [9] for the theory of finite field, and [17] and [16] for the motivation and the original definitions of nonlinearity and the resilient property for Boolean functions.

We will use the following notation throughout the paper:

- $\mathbb{F}_q = GF(q)$, a finite field with q elements, and $\mathbb{F}_q^*$, the multiplication group of $\mathbb{F}_q$.
- $\mathbb{F}_2^n = \{\underline{\mathbf{x}} = (x_0, x_1, \cdots, x_{n-1}) | x_i \in \mathbb{F}_2\}$, a vector space over $\mathbb{F}_2$ of dimension n.
- $\underline{\mathbf{a}} = \{a_i\}$, a sequence over $\mathbb{F}_2$, i.e., $a_i \in \mathbb{F}_2$, is called a *binary sequence*. If $\underline{\mathbf{a}}$ is a periodic sequence with period v, then we also denote $\underline{\mathbf{a}} = (a_0, a_1, \cdots, a_{v-1})$, an element in $\mathbb{F}_2^v$.

A. Autocorrelation

If $\underline{\mathbf{a}} = (a_0, a_1, \cdots, a_{p-1})$ is a binary sequence with period p, its (periodic) autocorrelation function $C(\tau)$ is defined as

$$C(\tau) = \sum_{i=0}^{p-1} (-1)^{a_i + a_{i+\tau}}, \tau = 0, 1, \cdots.$$

Here τ is a phase shift of the sequence $\{a_i\}$.

Ideal (2-Level) Autocorrelation: If

$$C(\tau) = \begin{cases} p & \text{if } \tau \equiv 0 \bmod p, \\ -1 & \text{otherwise,} \end{cases}$$

then we say that the sequence $\{a_i\}$ has the idea two-level autocorrelation function.

B. Cross Correlation

If $\underline{\mathbf{a}} = (a_0, a_1, \cdots, a_{p-1})$ and $\underline{\mathbf{b}} = (b_0, b_1, \cdots, b_{p-1})$ are two binary sequences with period p, their (periodic) cross correlation function $C_{\underline{\mathbf{a}},\underline{\mathbf{b}}}(\tau)$ is defined as

$$C_{\underline{\mathbf{a}},\underline{\mathbf{b}}}(\tau) = \sum_{i=0}^{p-1} (-1)^{a_{i+\tau} + b_i}, \tau = 0, 1, \cdots.$$

Here τ is a phase shift of the sequence $\{b_i\}$.

C. Hamming Weight

Let

$$H(s) = |\{0 \le i < 2^n - 1 | s_i = 1\}|$$

if $s = \{s_i\}$ is a binary sequence with period $2^n - 1$ and

$$H(s) = |\{x \in \mathbb{F}_{2^n} | s(x) = 1\}|$$

if $s = s(x)$ is a polynomial function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. In both cases, we call $H(s)$ the *Hamming weight* of s. For a positive integer $r = r_0 + r_1 2 + \cdots r_{n-1}2^{n-1}, r_i \in \mathbb{F}_2$,

$$H(r) = |\{0 \le i < n | r_i = 1\}|$$

is also called the *Hamming weight* of the integer r.

2 Definition of Welch-Gong Transformation Sequence Generators

In this section, we will give the definition of the Welch-Gong transformation sequence generators. Hence after, we set $n \not\equiv 0 \bmod 3$.

Let $g(x) = x + x^{q_1} + x^{q_2} + x^{q_3} + x^{q_4}, x \in \mathbb{F}_{2^n}$, where q_i are defined by

$$\begin{aligned} q_1 &= 2^k + 1, \\ q_2 &= 2^{2k-1} + 2^{k-1} + 1, \\ q_3 &= 2^{2k-1} - 2^{k-1} + 1, \\ q_4 &= 2^{2k-1} + 2^k - 1, \end{aligned}$$

where $n = 3k - 1$ and

$$\begin{aligned} q_1 &= 2^{k-1} + 1, \\ q_2 &= 2^{2k-2} + 2^{k-1} + 1, \\ q_3 &= 2^{2k-2} - 2^{k-1} + 1, \\ q_4 &= 2^{2k-1} - 2^{k-1} + 1, \end{aligned}$$

where $n = 3k - 2$. Then a function, say $f(x)$, from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ defined by

$$f(x) = Tr(g(x+1)+1), x \in \mathbb{F}_{2^n} \tag{1}$$

is called the *Welch-Gong transformation* of $Tr(g(x))$ in [10], or the *WG transformation* for short.

Let α be a primitive element of $\mathbb{F}_{2^n}$. Let $\underline{\mathbf{a}} = \{a_i\}$ and $\underline{\mathbf{b}} = \{b_i\}$ whose elements are given by

$$a_i = Tr(g(\alpha^i)), i = 0, 1, \cdots \tag{2}$$

$$b_i = f(\alpha^i) = Tr(g(\alpha^i + 1) + 1), i = 0, 1, \cdots. \tag{3}$$

Then $\underline{\mathbf{b}}$ is called *Welch-Gong transformation sequence* of $\underline{\mathbf{a}}$, or *WG sequence* for short.

Any function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is related to a Boolean function (we will discuss an exact conversion of these two representations in Section 4). From a WG transformation, we have two types of pseudo-random sequence generators. One is WG sequences themselves. The other is to apply WG transformations regarded as Boolean functions to operate on a set of LFSRs for generating sequences. I.e., applying the WG transformations regarded as Boolean functions as combining functions or filtering functions in combinatorial function generators or filtering generators [15]. We refer to these two modes as *WG sequence generators*.

Remark 1. In fact, the transform given in (1) can be applied to any function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. But till now, we haven't found another type of $g(x)$ such that its WG transformation sequence has 2-level auto correlation. So, we restrict ourselves to this specific $g(x)$.

3 Randomness of WG Sequences

In this section, we will discuss the randomness properties of WG sequences, including their decimation, auto/cross correlation, statistic properties, and linear span.

A. Decimation Property

Lemma 1. *Let α be a primitive element of $\mathbb{F}_{2^n}$ and $\underline{\mathbf{b}}$ be the WG sequence of $\underline{\mathbf{a}}$. Then elements of $\underline{\mathbf{b}}$ can be obtained by operating an irregular decimation on $\underline{\mathbf{a}}$ as follows*

$$b_0 = a_0$$

for $i > 0$,

$$b_i = \begin{cases} a_{\tau(i)} & n \text{ even}, \\ a_{\tau(i)} + 1 & n \text{ odd}, \end{cases}$$

where $\tau(i)$ is determined by

$$\alpha^{\tau(i)} = \alpha^i + 1. \tag{4}$$

Proof. From the definition, $a_0 = Tr(g(1)) = n$ and $b_0 = Tr(g(0) + 1) = n$. Thus $a_0 = b_0$. For $i > 0$, if n is even, we have

$$b_i = Tr(g(\alpha^i + 1) + 1) = Tr(g(\alpha^i + 1)) + n = Tr(g(\alpha^i + 1)) = a_{t(i)}, i = 0, 1, \cdots.$$

Similarly, if n is odd, we have

$$b_i = Tr(g(\alpha^i + 1) + 1) = Tr(g(\alpha^i + 1)) + n = Tr(g(\alpha^i + 1)) = a_{t(i)} + 1, i = 0, 1, \cdots.$$

Thus the assertion is established.

Remark 2. This lemma shows that the WG sequence $\underline{\mathbf{b}}$ can be obtained by an irregular decimation from $\underline{\mathbf{a}}$ where the decimation is determined by (4). Note that $\underline{\mathbf{a}}$ is a 5-term sequence. So it can be generated by using five linear feedback shift registers and one AND gate. This property of the WG sequences allows them to have an efficient implementation for small n by operating decimation on $\underline{\mathbf{a}}$ together with a table look-up.

B. Auto Correlation, 2-Tuple Distribution, and Balance Property

Proposition 1. *Let $\underline{\mathbf{b}}$ be a WG sequence defined by (3). Then $\underline{\mathbf{b}}$ is a binary sequence of period $2^n - 1$ with (ideal) 2-level auto correlation.*

This result was first discovered by Golomb, Gong and Gaal in [10] and verified for $5 \leq n \leq 20$. Later on, No *et al* [14], found another way to construct the WG sequences and verified their result for $5 \leq n \leq 23$. Dillon proved it for the odd n case [2], and finally, Dobbertin and Dillon proved it for the even n case [3] which completely established Proposition 1.

Note. $\underline{\mathbf{a}}$ is also a 2-level auto correlation sequence. See [10] [3].

Let $\underline{\mathbf{s}}$ be a binary sequence of period $2^n - 1$. Assume that $1 \leq t \leq n$. In every period of $\underline{\mathbf{s}}$, if each nonzero t-tuple $(c_1, c_2, \cdots, c_t) \in F_2^t$ occurs 2^{n-t} times and zero t-tuple $(0, \cdots, 0)$ occurs $2^{n-t} - 1$ times, then we say that the sequence has an *ideal t-tuple distribution.*

Proposition 2. *Any WG sequence has ideal 2-tuple distribution.*

Proof. Let $\underline{\mathbf{b}}$ be a WG sequence of period $2^n - 1$. Since $\underline{\mathbf{b}}$ is a 2-level auto correlation sequence, then for any shift of $\underline{\mathbf{b}}$, say $L^\tau(\underline{\mathbf{b}}) = (b_\tau, b_{\tau+1}, \cdots)$, we have

$$|\{0 \leq k < 2^n - 1 | (b_k, b_{k+\tau}) = (i, j)\}| = \begin{cases} 2^{n-2} - 1 & \text{if } i = j = 0, \\ 2^{n-2} & \text{otherwise,} \end{cases} \tag{5}$$

where $i, j \in \mathbb{F}_2$. When $\tau = 1$ it establishes the assertion.

Proposition 3. *Any WG sequence is balanced. I.e., in every period $2^n - 1$, zeros occur $2^{n-1} - 1$ times and ones occur 2^{n-1} times.*

Proof. Applying Proposition 2, we have

$$H(\underline{\mathbf{b}} + L(\underline{\mathbf{b}})) = 2^{n-1} \text{ and } H(\underline{\mathbf{b}} \cdot L(\underline{\mathbf{b}})) = 2^{n-2} \tag{6}$$

where $\underline{\mathbf{b}} \cdot L(\underline{\mathbf{b}}) = \sum_{i=0}^{2^n-2} b_i b_{i+1}$, the inner product of $\underline{\mathbf{b}}$ and $L(\underline{\mathbf{b}})$. Since

$$H(\underline{\mathbf{b}} + \mathrm{L}(\underline{\mathbf{b}})) = H(\underline{\mathbf{b}}) + H(L(\underline{\mathbf{b}})) - 2H(\underline{\mathbf{b}} \cdot L(\underline{\mathbf{b}})).$$

Substituting (6) into the above identity, we get

$$2^{n-1} = 2H(\underline{\mathbf{b}}) - 2 \cdot 2^{n-2} \Longrightarrow H(\underline{\mathbf{b}}) = 2^{n-1}$$

which establishes the assertion.

C. Hadamard Transform and Cross Correlation

Let $f(x)$ be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. Then the Hadamard transform of $f(x)$ is defined by

$$\hat{f}(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda x) + f(x)}. \tag{7}$$

Let $S_v(x) = Tr(x^v)$.

Property 1. Let $n = 2m+1$ be odd and $v = 2^t + 1$ with $gcd(t, n) = 1$. Then the Hadamard transform of $S_{2^t+1}(x)$ is given by

$$\hat{S}_{2^t+1}(\lambda) = \begin{cases} 0 & \text{if } Tr(\lambda) = 0, \\ \pm 2^{m+1} & \text{if } Tr(\lambda) = 1. \end{cases}$$

This is established by Gold [6]. From the proof that the WG sequences are 2-level auto correlation sequences in [2], we can derive the following result:

Theorem 1. *For odd n, let $g(x)$ be defined as in Section 2.1, and let $f(x)$ be the Welch-Gong transform of $Tr(g(x))$, i.e., $f(x) = Tr(g(x+1)+1)$. Then $\hat{f}(\lambda)$, the Hadamard transform of $f(x)$, is given by*

$$\hat{f}(\lambda) = \hat{S}_{2^t+1}(\lambda^c),$$

where

$$c = d^{-1} \textit{ and } d = 2^{2t} - 2^t + 1 \textit{ for } 3t \equiv 1 \textit{ mod } n. \tag{8}$$

We now have the following corollaries.

Corollary 1. *(**Function Version**) Let $n = 2m+1$ odd, and let $f(x)$ be the Welch-Gong transformation function. Then the Hadamard transform of $f(x)$ is given by*

$$\hat{f}(\lambda) = \begin{cases} 0 & \textit{if } Tr(\lambda^c) = 0, \\ \pm 2^{m+1} & \textit{if } Tr(\lambda^c) = 1, \end{cases}$$

where c is defined in (8) in Theorem 1.

Proof. Applying Property 1 to Theorem 1, the result follows.

Corollary 2. *(**Sequence Version**) Let α be a primitive element of $\mathbb{F}_{2^n}$ and $f(x)$ be a Welch-Gong transformation function. Let $\underline{\mathbf{a}} = \{a_i\}$ be an m-sequence whose elements are defined by*

$$a_i = Tr(\alpha^i), i = 0, 1, \cdots$$

and $\underline{\mathbf{b}} = \{b_i\}$ be the WG sequence whose elements are given by (3). Then $C_{\underline{\mathbf{a}},\underline{\mathbf{b}}}(\tau)$, the cross correlation function between $\underline{\mathbf{a}}$ and $\underline{\mathbf{b}}$, is determined by

$$C_{\underline{\mathbf{a}},\underline{\mathbf{b}}}(\tau) = \begin{cases} -1 & \textit{if } Tr(\alpha^{\tau c}) = 0, \\ -1 \pm 2^{m+1} & \textit{if } Tr(\alpha^{\tau c}) = 1, \end{cases}$$

where c is defined in (8) in Theorem 1. I.e., the cross correlation function between $\underline{\mathbf{a}}$ and $\underline{\mathbf{b}}$ are three-valued.

Proof. By noticing that,

$$C_{\underline{\mathbf{a}},\underline{\mathbf{b}}}(\tau) = \sum_{i=0}^{2^n-2}(-1)^{a_{i+\tau}+b_i} = \sum_i (-1)^{Tr(\alpha^\tau \alpha^i)+f(\alpha^i)} = -1 + \sum_{x\in\mathbb{F}_{2^n}}(-1)^{Tr(\alpha^\tau x)+f(x)} = -1+\hat{f}(\alpha^\tau).$$

Applying Corollary 1, the result follows.

D. Linear Span of WG Sequences

The linear span of a sequence is defined to be the *shortest length* of the linear feedback shift registers which generate the sequence. Sequence with large linear span are resistant to attacks arising from employing the Berlekamp-Massey algorithm [13].

Proposition 4. *Let* $\underline{\mathbf{b}}$ *be a WG sequence of period* $2^n - 1$ *and* $LS(\underline{\mathbf{b}})$ *represent its linear span. Then*

$$LS(\underline{\mathbf{b}}) = n(2^{\lceil n/3 \rceil} - 3).$$

We will give a proof for this result after we derive the linear span of the WG transformations in Section 5. From Proposition 4, it is clear that the linear span of the WG sequences of period $2^n - 1$ increases exponentially with n.

Remark 3. WG sequences of period 2^n-1 are the first type of binary sequences of period 2^n-1 which have the balance property, ideal 2-tuple distribution, 2-level auto correlation, three-level cross correlation with m-sequences, linear span increased exponentially in n.

4 Non-linearity and Resilient Property of Welch-Gong Transformations

In this section, we will derive the non-linearity and the resilient property for the WG transformations when they are regarded as Boolean functions. First, we need to develop a result on the conversion of a polynomial function (from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$) to a Boolean function in n variables.

4.1 Isomorphism between $\mathbb{F}_{2^n}$ and $\mathbb{F}_2^n$

Since the finite field $\mathbb{F}_{2^n}$ can be regarded as a vector space of n dimension, then we have a linear space structure for $\mathbb{F}_{2^n}$. Let $B = \{\alpha_0, \alpha_1, \cdots, \alpha_{n-1}\}$ be a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, then $\forall x \in F_{2^n}$, we have

$$x = x_0\alpha_0 + x_1\alpha_1 + \cdots + x_{n-1}\alpha_{n-1}, x_i \in F_2.$$

Let

$$\delta : x \mapsto \underline{\mathbf{x}} = (x_0, x_1, \cdots, x_{n-1}) \tag{9}$$

then $\delta(x)$ is an isomorphism between $\mathbb{F}_{2^n}$ and $\mathbb{F}_2^n$ when both of them are regarded as vector spaces.

Lemma 2. *With the above notation. Let $f(x)$ be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. Then $f(x)$ defines a Boolean function in the following way:*

$$f(x) = f(x_0\alpha_0 + \cdots + x_{n-1}\alpha_{n-1}) = f_B(x_0, x_1, \cdots, x_{n-1})$$

Note that f and f_B in the above identity might not be same. We will write $f_B(x_0, x_1, \cdots, x_{n-1}) = f(x_0, x_1, \cdots, x_{n-1})$ for short if it will not cause any confusion in the context.

Proof. Since $f(x)$ is a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, then $f(x)$ can be represented by

$$f(x) = \sum_{i=1}^{r} Tr_1^{n_i}(\beta_i x^{t_i}), \beta \in \mathbb{F}_{2^{n_i}} \tag{10}$$

where t_i is a coset leader of a cyclotomic coset modulo $2^{n_i} - 1$ and $n_i|n$ the size of the cyclotomic coset containing t_i (*Note.* This can be obtained by the discrete Fourier transform [7]. Also it corresponds to the trace representation of a binary sequence with period $N|2^n - 1$). So it suffices to show that $Tr(\omega x^t)$ is a Boolean function in $x_0, x_1, \cdots, x_{n-1}$ when x is represented by $x = \sum_i x_i\alpha_i$. Let $\omega = \sum \omega_i\alpha_i, \omega_i \in F_2$. Then

$$\omega x^t = (\sum \omega_i\alpha_i)(\sum_i x_i\alpha_i)^t = \sum_i D_i\alpha_i$$

where $D_i = D_i(x_0, x_1, \cdots, x_{n-1}) \in \mathbb{F}_2$. Therefore

$$Tr(\omega x^t) = Tr(\sum_i D_i\alpha_i) = \sum_i Tr(D_i\alpha_i) = \sum_i D_i Tr(\alpha_i)$$

where $Tr(\alpha_i) \in F_2$. Since $D_i(x_0, \cdots, x_{n-1})$ is a Boolean function in variables $x_0, x_1, \cdots, x_{n-1}$, then $Tr(\omega x^t)$ is a Boolean function.

Example 1. Let $n = 3$ and $\mathbb{F}_{2^3}$ be defined by $t(x) = x^3 + x + 1$. Let α be a root of $t(x)$. Then $\{1, \alpha, \alpha^2\}$ is a basis of $\mathbb{F}_{2^3}$ over $\mathbb{F}_2$. Let $f(x) = Tr(x)$. For any $x \in F_{2^3}$, we write $x = x_0 + x_1\alpha + x_2\alpha^2$. Then

$$Tr(x) = Tr(x_0 + x_1\alpha + x_2\alpha^2) = Tr(x_0) + Tr(x_1\alpha) + Tr(x_2\alpha^2) = x_0 + x_1Tr(\alpha) + x_2Tr(\alpha^2) = x_0.$$

The last identity comes from $Tr(\alpha) = Tr(\alpha^2) = 0$.

Remark 4. For a given function $f(x)$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, by representing $x = \sum_i x_i\alpha_i, x_i \in \mathbb{F}_2$ where $\{\alpha_0, \cdots, \alpha_{n-1}\}$ is a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, we obtain a Boolean function, still written as $f(x_0, x_1, \cdots, x_{n-1})$, by evaluating $f(x_0\alpha_0 + \cdots + x_{n-1}\alpha_{n-1})$. We call $f(x_0, x_1, \cdots, x_{n-1})$ a Boolean representation of $f(x)$ (with respect to the basis $\{\alpha_i\}$). When the defining polynomial of the finite field $\mathbb{F}_{2^n}$ is fixed, a Boolean form of the function depends on a basis used for computation in $\mathbb{F}_{2^n}$ regarded as a vector space. Since there are

$$B_n = \prod_{i=0}^{n-1}(2^n - 2^i)$$

different bases, then there are B_n (not necessarily distinct) Boolean forms for a given function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. Conversely, for a given Boolean function in n variables, we can obtain its polynomial representation which is a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ by using so-called the Fourier transform, see [8].

In the following two subsections, we will discuss the non-linearity and the resilient property of the WG transformations when they are regarded as Boolean functions.

4.2 Non-linearity of WG Transformations

Let $f(\underline{\mathbf{x}})$, $\underline{\mathbf{x}} = (x_0, x_1, \cdots, x_{n-1}) \in F_{2^n}$, be a Boolean function. A Boolean function $a(\underline{\mathbf{x}})$ is said to be *affine* if

$$a(\underline{\mathbf{x}}) = \sum_{i=0}^{n-1} w_i x_i + c, w_i \in \mathbb{F}_2, c \in \mathbb{F}_2.$$

Let

$$A = \{\sum_i w_i x_i + c \mid w_i \in \mathbb{F}_2, c \in \mathbb{F}_2\}.$$

I.e., A is the set consisting of all affine Boolean functions in n variables. Then the non-linearity of $f(\underline{\mathbf{x}})$, denoted by N_f, is defined as

$$N_f = min_{a \in A} d(f, a)$$

where

$$d(f, a) = |\{\underline{\mathbf{x}} \in F_2^n | f(\underline{\mathbf{x}}) \neq a(\underline{\mathbf{x}})\}|$$

which is called the *distance* of f from a.

Remark 5. From the definition of the distance, we have $d(f, a) = H(f + a)$, where $H(f + a)$ is the Hamming weight of $f + a$ defined in Section 1.

Note that

$$d(f, a) = |\{x \in \mathbb{F}_{2^n} | f(x) \neq a(x)\}|$$

where $f(x)$ and $a(x)$ are polynomial forms of the Boolean functions $f(\underline{\mathbf{x}})$ and $a(\underline{\mathbf{x}})$ respectively. I.e., the distance of f from a is not changed whenever either a Boolean form or a polynomial form are applied. From this observation, we can derive the following lemma.

Let

$$\hat{f}(\underline{\mathbf{w}}) = \sum_{\underline{\mathbf{x}} \in \mathbb{F}_2^n} (-1)^{\underline{\mathbf{w}} \cdot \underline{\mathbf{x}} + f(\underline{\mathbf{x}})} \tag{11}$$

which is called the *Walsh transform* of the Boolean function f.

Lemma 3. *Let $f(\underline{\mathbf{x}})$ be a Boolean function and $a(\underline{\mathbf{x}})$ be a linear Boolean function. Let $f(x)$ and $a(x)$ be a polynomial representation of $f(\underline{\mathbf{x}})$ and $a(\underline{\mathbf{x}})$ respectively.*

1. *$a(\underline{\mathbf{x}}) = \sum_i w_i x_i = \underline{\mathbf{w}} \cdot \underline{\mathbf{x}}$ where $\underline{\mathbf{w}} = (w_0, w_1, \cdots, w_{n-1}) \in \mathbb{F}_2^n$. Moreover, there exists some $\lambda \in \mathbb{F}_{2^n}$ such that*
$$a(x) = Tr(\lambda x). \tag{12}$$
2. *The Hadamard transform of $f(x)$ and the Walsh transform of $f(\underline{\mathbf{x}})$ have the following relation:*
$$\hat{f}(\underline{\mathbf{w}}) = \hat{f}(\lambda), \underline{\mathbf{w}} \in \mathbb{F}_2^n, \lambda \in \mathbb{F}_{2^n} \tag{13}$$
where $\underline{\mathbf{w}} \cdot \underline{\mathbf{x}} = Tr(\lambda x)$.
3. *The Hadamard transform of f and the distance of $f(\underline{\mathbf{x}})$ from $a(\underline{\mathbf{x}})$ are related by*
$$\hat{f}(\lambda) = 2^n - 2d(f, a)$$
where λ is determined by (12). Or equivalently,
$$d(f, a) = \frac{2^n - \hat{f}(\lambda)}{2}.$$

Proof. The first assertion can be found in a coding book, for example [11]. We now consider the second assertion. Note that $f(x) = f(\underline{\mathbf{x}})$. Thus for $\underline{\mathbf{x}} = (x_0, x_1, \cdots, x_{n-1}) \in F_2^n$, we have

$$\begin{aligned}
\hat{f}(\underline{\mathbf{w}}) &= \sum_{\underline{\mathbf{x}} \in \mathbb{F}_2^n} (-1)^{\underline{\mathbf{w}} \cdot \underline{\mathbf{x}} + f(\underline{\mathbf{x}})} \\
&= \sum_{x \in F_{2^n}} (-1)^{Tr(\lambda x) + f(x)} \\
&= \hat{f}(\lambda)
\end{aligned}$$

where $\underline{\mathbf{w}} \in \mathbb{F}_2^n, \lambda \in \mathbb{F}_{2^n}$ and $\underline{\mathbf{w}} \cdot \underline{\mathbf{x}} = Tr(\lambda x)$. So the second result is true. Note that

$$\begin{aligned}
\hat{f}(\lambda) &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda x) + f(x)} \\
&= 2^n - 2d(f, Tr(\lambda x)) = 2^n - 2d(f, a).
\end{aligned}$$

The last identity comes from $a(\underline{\mathbf{x}}) = Tr(\lambda x)$. This confirms the third result.

Lemma 4. *Let $f(\underline{\mathbf{x}})$ be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Let $a(\underline{\mathbf{x}})$ be a linear function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Then*

$$d(f, a+1) = 2^n - d(f, a).$$

Moreover

$$d(f, a+1) = \frac{2^n + \hat{f}(\lambda)}{2}$$

where λ satisfies that $a(\underline{\mathbf{x}}) = Tr(\lambda x)$.

Theorem 2. *Let $n = 2m + 1$ odd. Let $f(x)$ be the Welch-Gong transformation defined by (1). Let $f(\underline{\mathbf{x}})$ be the Boolean form of $f(x)$. Then the non-linearity of $f(\underline{\mathbf{x}})$, denoted by N_f, is given by*

$$N_f = 2^{n-1} - 2^m.$$

Proof. Let $a(\underline{\mathbf{x}})$ be a linear Boolean function. Applying Lemma 3-(3) and Corollary 1, we have

$$d(f, a) = \frac{2^n - \hat{f}(\lambda)}{2} = \begin{cases} 2^{n-1} & \text{if } \hat{f}(\lambda) = 0 \\ 2^{n-1} - 2^m & \text{if } \hat{f}(\lambda) = 2^{m+1} \\ 2^{n-1} + 2^m & \text{if } \hat{f}(\lambda) = -2^{m+1}. \end{cases}$$

Applying Lemma 4 together with Lemma 3-(3) and Corollary 1, we get

$$d(f, a+1) = \frac{2^n + \hat{f}(\lambda)}{2} = \begin{cases} 2^{n-1} & \text{if } \hat{f}(\lambda) = 0 \\ 2^{n-1} + 2^m & \text{if } \hat{f}(\lambda) = 2^{m+1} \\ 2^{n-1} - 2^m & \text{if } \hat{f}(\lambda) = -2^{m+1}. \end{cases}$$

Thus

$$N_f = min_{a \in A} d(f, a) = 2^{n-1} - 2^m.$$

Remark 6. Chang, Dai and Gong [1] discussed how to construct Boolean functions with the maximal non-linearity in terms of binary m-sequences with three-valued cross correlation. In particular, they discussed the case $Tr(x^r)$ for some special choices of r. Gong and Golomb [8], pointed out that the monomial functions $Tr(x^r)$ are not secure when used as combining functions or filtering functions in stream cipher systems or block cipher modes, because they correspond to m-sequences. However, the WG transformations are not monomials. We will come back to this question in the next section.

4.3 Resilient Property of WG Transformations

In this subsection, we will give a criterion for whether Welch-Gong Transformations satisfy the resilient property.

Let $f(\underline{\mathbf{x}}), \underline{\mathbf{x}} \in F_2^n$, be a Boolean function. For $r > 0$, $f(\underline{\mathbf{x}})$ is said to be *r-order correlation immune* if

$$\hat{f}(\underline{\mathbf{w}}) = 0 \text{ for all } \underline{\mathbf{w}} \in F_2^n : 1 \leq H(\underline{\mathbf{w}}) \leq r. \tag{14}$$

This definition comes from the result obtained by Xiao and Massey [18] which is equivalent to Siegenthaler's original definition [16]. If $f(\underline{\mathbf{x}})$ satisfies (14) and $f(\underline{\mathbf{x}})$ is balanced, i.e., $H(f(\underline{\mathbf{x}})) = 2^{n-1}$, then $f(\underline{\mathbf{x}})$ is said to be r-resilient.

Let

$$D = \{x \in F_{2^n}^* | Tr(x^c) = 0\} \tag{15}$$

where c is defined in Theorem 1. Then $|D| = 2^{n-1} - 1$. Recall that $\{\alpha_0, \alpha_1, \cdots, \alpha_{n-1}\}$ is the basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. Let

$$R = \{(Tr(\lambda\alpha_0), \cdots, Tr(\lambda\alpha_{n-1})) \in \mathbb{F}_2^n | \lambda \in D\}. \tag{16}$$

Theorem 3. *With the above notation. Let n be odd. Let $f(\underline{\mathbf{x}})$ be the Boolean form of the WG transformation $f(x) = Tr(g(x+1)+1)$ defined by (1). Then $f(\underline{\mathbf{x}})$ is r-resilient if and only if all vectors in $W_r = \{\underline{\mathbf{w}} | 1 \leq H(\underline{\mathbf{w}}) \leq r\}$ appear in R. I.e., $W_r \subset R$.*

Proof. Applying Lemma 3, we have

$$\hat{f}(\underline{\mathbf{w}}) = \hat{f}(\lambda)$$

where

$$a(\underline{\mathbf{x}}) = \sum_{i=0}^{n-1} w_i x_i = Tr(\lambda x). \tag{17}$$

Notice that

$$\lambda x = \lambda \sum_i x_i \alpha_i \Longrightarrow Tr(\lambda x) = \sum_{i=0}^{n-1} Tr(\lambda \alpha_i) x_i.$$

Combining with (17), we have

$$w_i = Tr(\lambda \alpha_i), 0 \leq i < n. \tag{18}$$

According to Corollary 1, $\hat{f}(\lambda) = 0$ if and only if $Tr(\lambda^c) = 0$ where c is defined by (8). Together with the definition of the resilient property, we have the following reasoning process.

$$\begin{aligned} f \text{ is } r\text{-resilient} &\Longleftrightarrow \hat{f}(\underline{\mathbf{w}}) = 0 \text{ for all } \underline{\mathbf{w}} \in W_r \\ &\Longleftrightarrow \hat{f}(\lambda) = 0 \text{ for all } \lambda \text{ corresponding to } \underline{\mathbf{w}} \cdot \underline{\mathbf{x}} = Tr(\lambda x), \underline{\mathbf{w}} \in W_r \\ &\Longleftrightarrow \text{ for such } \lambda\text{'s}, \lambda \in D \text{ and } (Tr(\lambda\alpha_0), \cdots, Tr(\lambda\alpha_{n-1})) \in W_r \\ &\Longleftrightarrow W_r \subset R. \end{aligned}$$

Remark 7. Theorem 3 provides a method to find r-resilient WG transformations regarded as Boolean functions. Since the number of bases of $\mathbb{F}_{2^n}$ is huge and $|R| = 2^{n-1} - 1$, it is possible to find Boolean forms of the WG transformations have r-resilient property where r is in the range of $1 \leq r \leq n - \lceil n/3 \rceil$ (We will prove this inequality in the next section).

In the following we will prove that any WG-transformation regarded as a Boolean function with 1-resilient property is always possible by a proper basis conversion.

Lemma 5. *There are n linearly independent vectors in R, defined by (16).*

Proof. Since the number of (distinct) vectors in $R \cup \{0\}$ is 2^{n-1}, then the number of linearly independent vectors in $R \cup \{0\}$ is $\geq n-1$ with equality if and only if $R \cup \{0\}$ is a linear space. Now we will prove that $R \cup \{0\}$ is not a linear space. Assume that $R \cup \{0\}$ is a linear space of dimension $n-1$ and let

$$\sigma(\lambda) = (Tr(\lambda), Tr(\lambda\alpha), \cdots, Tr(\lambda\alpha^{n-1})).$$

Thus $\forall \lambda_1, \lambda_2 \in D$, we have $\sigma(\lambda_1)$ and $\sigma(\lambda_2) \in R$. Since R is a linear space, then $\sigma(\lambda_1) + \sigma(\lambda_2) \in R$. But

$$\sigma(\lambda_1) + \sigma(\lambda_2) =$$

$$(Tr(\lambda_1) + Tr(\lambda_2), Tr(\lambda_1\alpha) + Tr(\lambda_2\alpha), \cdots, Tr(\lambda_1\alpha^{n-1}) + Tr(\lambda_2\alpha^{n-1})) \in R$$

and hence $\lambda_1 + \lambda_2 \in D$. Thus $D \cup \{0\}$ is a linear space of dimension $n-1$. Let $\lambda \in D$ and hence for any $x \in D$ we have $\lambda + x \in D$ and hence $Tr((\lambda + x)^c) = 0$ if $x \in D$ and $Tr((\lambda + x)^c) = 1$ if $x \notin D$. I.e., we have

$$Tr((\lambda + x)^c) = \begin{cases} 0 \text{ if } Tr(x^c) = 0, \\ 1 \text{ if } Tr(x^c) = 1, \end{cases}$$

Thus $Tr((\lambda + x)^c) = Tr(x^c)$ which is a contradiction since $H(c) > 1$.

Theorem 4. *Let $f(x)$ be a WG-transformation. Then there exists at least one basis of $\mathbb{F}_{2^n}$ such that the Boolean function representation of $f(x)$ under this basis is 1-resilient*

Proof. According to Lemma 5, we can assume that $\{\alpha_0, \cdots, \alpha_{n-1}\}$ is a subset of $R_{\underline{\alpha}}$ which is linearly independent over $\mathbb{F}_2$. Let

$$A = \begin{pmatrix} \alpha_0 \\ \cdot \\ \cdot \\ \cdot \\ \alpha_{n-1} \end{pmatrix}$$

where α_i is a row vector of A. Let $B = A^{-1}$ and let β_j denote the jth column vector of B, $j = 0, \cdots, n-1$. Then $\underline{\beta} = \{\beta_0, \cdots, \beta_{n-1}\}$ is a basis of $\mathbb{F}_{2^n}$. Then $R_{\underline{\beta}}$ is given by

$$R_{\underline{\beta}} = \{\sigma_{\underline{\alpha}}(\lambda)B | \lambda \in D\}.$$

Therefore the row vectors of $BA = A^{-1}A = I_n$, the identity matrix, belong to $R_{\underline{\beta}}$. Hence $f_{\underline{\beta}}(x_0, \cdots, x_{n-1})$, the Boolean representation of $f(x)$ under the basis $\underline{\beta}$, is a 1-resilient function.

5 Linear Span and Degree of WG Transformations

Let $f(x) = \sum_i c_i x^i$ be a polynomial function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. Let

$$I = \{0 \le i \le 2^n - 1 | c_i \ne 0\}.$$

The *algebraic degree* of $f(x)$, denoted as $alg(f)$, is defined as

$$alg(f) = max_{\{i \in I\}} alg(x_i) \text{ where } alg(x_i) = H(i).$$

Let $f(\underline{\mathbf{x}})$ be the Boolean form of $f(x)$ and denote the degree of $f(\underline{\mathbf{x}})$ as $deg(f(\underline{\mathbf{x}}))$.

Fact 1 *The algebraic degree of $f(x)$, a polynomial function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, is equal to the degree of the Boolean form of the function. I.e.,*

$$alg(f) = deg((f(\underline{\mathbf{x}})).$$

Linear span of $f(x)$ is said to be the number of non-zero coefficients in $f(x) = \sum_i c_i x^i$, which is introduced by Gong and Golomb in [8]. We denote it as $LS(f(x))$ or simply $LS(f)$ if the context is clear. I.e.,

$$LS(f) = |I|.$$

Remark 8. The linear span of a polynomial function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is equal to the linear span of the sequence corresponding to the function.

Let $f(\underline{\mathbf{x}})$ be a Boolean function, we will define the linear span of the Boolean function $f(\underline{\mathbf{x}})$ in terms of its polynomial representations. Let

$$\Pi = \{ \text{ all bases of } \mathbb{F}_{2^n} \text{ over } \mathbb{F}_2 \}.$$

For $B = \{\alpha_0, \cdots, \alpha_{n-1}\} \in \Pi$, we denote $f_B(x)$ a polynomial representation of $f(\underline{\mathbf{x}})$ with respect to the basis B. We define a *linear span* of $f(\underline{\mathbf{x}})$, denoted by $LS(f(\underline{\mathbf{x}}))$, as

$$LS(f(\underline{\mathbf{x}})) = min_{B \in \Pi} LS(f_B(x)).$$

Note that for a given polynomial function $f(x)$, the linear span of any Boolean representation of $f(x)$ is equal to the linear span of $f(x)$ itself. We will write this observation as a lemma for later reference.

Lemma 6. *With the above notation. Let $f(x)$ be a polynomial function of $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. Let $f_B(\underline{\mathbf{x}})$ be its Boolean form with respect to a basis B of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. Then*

$$LS(f_B(\underline{\mathbf{x}})) = LS(f(x))$$

for all $B \in \Pi$.

As Youssef and Gong pointed it out in their recent work [19], the polynomial representation a complicated Boolean function might be just a monomial function (here monomial means that it has only one trace term in (10) which is different from the concept of the ordinary monomial which only has exactly one term). Thus a Boolean function must have a large linear span so that it can be resistant to the interpolation attack. In the following, we will show that the linear span of the Boolean forms of the WG transformations increases exponentially with n.

The following result is extracted from [10].

Fact 2 *Let $f(x) = Tr(g(x+1)+1)$ be the WG transformation defined by (1), then*

$$f(x) = \sum_{i \in I} Tr(x^i) \tag{19}$$

where $I = I_1 \cup I_2$ for $n = 3k-1$, where

$$I_1 = \{2^{2k-1} + 2^{k-1} + 2 + i | 0 \leq i \leq 2^{k-1} - 3\} \tag{20}$$

$$I_2 = \{2^{2k} + 3 + 2i | 0 \leq i \leq 2^{k-1} - 2\} \tag{21}$$

and where $I = \{1\} \cup I_3 \cup I_4$ for $n = 3k-2$, where

$$I_3 = \{2^{k-1} + 2 + i | 0 \leq i \leq 2^{k-1} - 3\} \tag{22}$$

$$I_4 = \{2^{2k-1} + 2^{k-1} + 2 + i | 0 \leq i \leq 2^{k-1} - 3\}. \tag{23}$$

Moreover, in each case, all the elements in I belong to distinct cyclotomic cosets modulo $2^n - 1$.

Note that the trace functions appeared in (19) depend on the coset size of i in I.

Theorem 5. *Let $f(x) = Tr(g(x+1)+1)$ be the WG transformation defined by (1), then $LS(f(x))$, the linear span of f, is given by*

$$LS(f(x)) = n(2^{\lceil n/3 \rceil} - 3).$$

Proof. According to Fact 2, all numbers in I belong to different cyclotomic cosets modulo $2^n - 1$ and $|I| = 2^k - 3$. So we only need to show that any coset containing a number in I has full size n. Here we only give a proof for $n = 3k-1$ and $s \in I_1$, since proofs for the other cases are similar. Note that for $s \in I_1$, the binary representation of s has the following pattern

$$\begin{array}{rcccccccc} Index & 0\ 1 \cdots k-1 & k \cdots & 2k-2 & 2k-1 & 2k \cdots & 3k-2 = n-1 \\ BinaryRep. & * * \cdots \quad * & 0 \cdots & 0 & 1 & 0 \cdots & 0 \end{array} \tag{24}$$

where * can take any value from $\{0,1\}$. Let C_s be a coset containing s, then

$$C_s = \{s, s2, \cdots, s2^{n_s - 1}\}$$

where n_s is the smallest integer satisfying $s2^{n_s} \equiv s \bmod 2^n - 1$. According to (24), $n_s = n$. I.e., C_s has full size n. Thus for each $s \in I$, we have the trace function appeared in Fact 2 is the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. Thus $LS(Tr(x^i)) = n$ for each $i \in I$. Therefore the result follows.

Proof of Proposition 4 in Section 3. Since the linear span of a WG sequence $\underline{\mathbf{b}}$ is equal to the linear span of the corresponding WG transformation f. I.e., we have $LS(\underline{\mathbf{b}}) = LS(f)$. Applying Theorem 5, the result follows.

Theorem 6. *Let $f(x)$ be the WG transformation defined by (1). Then the linear span of any Boolean form of $f(x)$ is equal to the linear span of $f(x)$. I.e.,*

$$LS(f(\underline{\mathbf{x}})) = n(2^{\lceil n/3 \rceil} - 3).$$

Proof. The result follows from Lemma 6 and Theorem 5.

Theorem 7. *Let $f(x) = Tr(g(x+1)+1)$ be the WG transformation defined by (1) and $f(\underline{\mathbf{x}})$ be its Boolean form. Then $deg(f(\underline{\mathbf{x}}))$, the degree of $f(\underline{\mathbf{x}})$, is given by*

$$deg(f(\underline{\mathbf{x}})) = \lceil n/3 \rceil + 1.$$

Proof. According to Fact 1, the degree of $f(\underline{\mathbf{x}})$ is equal to the algebraic degree of $f(x)$. From the definition, the algebraic degree of $f(x)$ is determined by the largest Hamming weight among the numbers appeared in the set I in Fact 2.

Case 1. $n = 3k - 1$. In this case, I is defined by (20) and (21). Considering $i \in I_1$,

$$i = 2^{2k-1} + 2^{k-1} + 2 + 2^{k-1} - 3 = 2^{2k-1} + 2^k - 1 \Longrightarrow H(i) = k + 1$$

which is the number in I_1 has the largest Hamming weight among all the numbers in I_1. For I_2, the number in I_2 which has the the largest Hamming weight is

$$i = 2^{2k} + 3 + 2(2^{k-1} - 2) = 2^{2k} + 2^k - 1 \Longrightarrow H(i) = k + 1.$$

Therefore $A_f = k + 1$. So that $deg(f(\underline{\mathbf{x}})) = k + 1$.

Case 2. $n = 3k - 2$. Similarly, we have

$$\begin{aligned} i &= 2^{k-1} + 2 + 2^{k-1} - 3 = 2^k - 1 \in I_3 \Longrightarrow H(i) = k \text{ and} \\ i &= 2^{2k-1} + 2^{k-1} + 2 + 2^{k-1} - 3 = 2^{2k-1} + 2^k - 1 \in I_4 \Longrightarrow H(i) = k + 1 \end{aligned}$$

So, $i = 2^{2k-1} + 2^k - 1 \in I$ has the maximal Hamming weight among the all numbers in I. Therefore $A_f = k + 1$. So that $deg(f(\underline{\mathbf{x}})) = k + 1$.

Corollary 3. *For a given WG transformation regarded as a Boolean function in n variables, r, the order of the resilient property of the function, is bounded by the following inequality*

$$r \leq n - \lceil n/3 \rceil.$$

Proof. Let d be the degree of the function. According to the Siegenthaler inequality [16], r, the order of the resilient property of the function, d, the degree of the function, and n, the number of the variables have the following relation,

$$r + d \leq n - 1.$$

Applying Theorem 7, we have $d = \lceil n/3 \rceil + 1$. Therefore

$$r \leq n - 1 - (\lceil n/3 \rceil + 1) = n - \lceil n/3 \rceil.$$

Or equivalently,

$$r \leq \begin{cases} 2k-2 & \text{for } n = 3k-1 \\ 2k-3 & \text{for } n = 3k-2. \end{cases}$$

6 Examples

In this section, we will give an example to illustrate the randomness properties of WG transformations regarded as both WG sequences and Boolean functions, which we obtained in the previous sections. Let $n = 7$, then $k = 3$, and

$$q_1 = 5, q_2 = 21, q_3 = 13, \text{ and } q_4 = 29.$$

So,

$$g(x) = x + x^5 + x^{21} + x^{13} + x^{29}$$

and we have the WG transformation $f(x)$ given by:

$$f(x) = Tr(g(x+1)+1) = Tr(x + x^3 + x^7 + x^{19} + x^{29}).$$

Let $\mathbb{F}_{2^7}$ be defined by a primitive polynomial $h(x) = x^7 + x + 1$. Let α be a root of $h(x)$. Then α is a primitive element of $\mathbb{F}_{2^7}$.

(a). Sequence Aspects of the WG transformation:

We obtain a WG sequence $\underline{\mathbf{b}} = \{b_i\}$ as follows:

$\underline{\mathbf{b}} =$

```
1 0 0 0 0 0 0 1 0 1 0 0 0 0 1 1 0 1 1 1 0 0 0 1 0 1 0 0 1 0 1 1
0 0 1 0 1 0 1 0 0 0 0 1 0 1 1 0 0 0 1 0 0 1 0 1 1 1 0 1 1 0 1 1
0 0 0 1 1 0 0 1 1 1 0 1 1 0 0 1 0 0 0 0 0 1 1 0 0 0 1 1 1 1 0 1
0 1 0 1 1 1 0 1 0 0 1 0 0 1 1 1 1 1 1 1 0 0 1 1 1 1 0 1 1 1 1
```

where $b_i = f(\alpha^i), i = 0, 1, \cdots$.

The WG sequence $\underline{\mathbf{b}}$ has the following profiles:

1. Balance property.
2. Ideal 2-tuple distribution.
3. 2-level auto correlation

4. 3-valued cross correlation with an m-sequence $\{a_i\}$, $a_i = Tr(\alpha^i), i = 0, 1, \cdots$, belongs to the set $\{-1, 15, -17\}$.
5. the Hadamard transform spectrum belonging to the set $\{0, \pm 16\}$.
6. Linear span 35.

(b). Boolean Function Aspects of the WG transformation:

Using the polynomial basis $(1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6)$, where $\alpha^7 + \alpha + 1 = 0$, the algebraic normal form of the Boolean function that corresponds to $f(x)$ is given by

$$x_0 \oplus x_1x_3 \oplus x_0x_1x_3 \oplus x_2x_3 \oplus x_0x_2x_3 \oplus x_1x_2x_3 \oplus x_0x_3x_4 \oplus x_2x_3x_4 \oplus x_0x_5 \oplus x_0x_1x_5 \oplus$$

$$x_0x_2x_5 \oplus x_1x_2x_5 \oplus x_3x_5 \oplus x_1x_3x_5 \oplus x_1x_4x_5 \oplus x_2x_4x_5 \oplus x_2x_3x_4x_5 \oplus x_1x_6 \oplus x_2x_6 \oplus x_0x_2x_6 \oplus x_0x_3x_6 \oplus x_4x_6 \oplus x_0x_4x_6 \oplus$$

$$x_2x_4x_6 \oplus x_1x_3x_4x_6 \oplus x_0x_5x_6 \oplus x_1x_5x_6 \oplus x_1x_2x_5x_6 \oplus x_0x_3x_5x_6.$$

Changing the basis using the following basis conversion matrix

$$\begin{pmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \beta_3 \\ \beta_4 \\ \beta_5 \\ \beta_6 \end{pmatrix} = \begin{pmatrix} 1\,1\,1\,0\,0\,0\,1 \\ 0\,1\,0\,0\,0\,0\,0 \\ 0\,0\,1\,1\,1\,0\,1 \\ 0\,0\,0\,1\,0\,1\,0 \\ 0\,0\,0\,0\,1\,0\,0 \\ 0\,0\,0\,0\,0\,1\,0 \\ 0\,0\,0\,0\,0\,0\,1 \end{pmatrix} \begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \\ \alpha^3 \\ \alpha^4 \\ \alpha^5 \\ \alpha^6 \end{pmatrix}$$

we obtain

$$x_0 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_0x_3 \oplus x_0x_1x_3 \oplus x_2x_3 \oplus x_0x_2x_3 \oplus x_1x_2x_3 \oplus x_3x_4 \oplus x_1x_3x_4 \oplus$$

$$x_2x_3x_4 \oplus x_5 \oplus x_0x_5 \oplus x_1x_5 \oplus x_1x_3x_5 \oplus x_0x_4x_5 \oplus x_3x_4x_5 \oplus x_2x_3x_4x_5 \oplus x_6 \oplus x_0x_6 \oplus x_0x_2x_6 \oplus x_1x_2x_6 \oplus x_0x_3x_6 \oplus$$

$$x_1x_3x_6 \oplus x_2x_4x_6 \oplus x_1x_3x_4x_6 \oplus x_5x_6 \oplus x_0x_5x_6 \oplus x_1x_5x_6 \oplus x_2x_5x_6 \oplus x_1x_2x_5x_6 \oplus x_3x_5x_6 \oplus x_0x_3x_5x_6 \oplus x_2x_3x_5x_6 \oplus x_3x_4x_5x_6$$

which is 1-resilient function with nonlinearity 56, algebraic degree 4 and linear span 35.

Another example for $n = 11$ is given in the appendix.

7 Conclusion

We provide a table which contains the profiles that we obtained in previous sections as a conclusion of this paper.
Notations used in Table 1:

- NC means that there is no corresponding concept between them.

Table 1. Profiles of WG Transformations

WG Sequences Profile	WG Sequence		WG Trans. as Boolean Func.	WG Trans. Boolean Profile
$2^n - 1$	Period	$\longleftrightarrow$	Boolean	n variables
Yes	Balance property	$\longleftrightarrow$	Balance property	Yes
Yes	2-tuple distribution		NC	
2-level	Auto correlation		NC	
$\{-1, -1 \pm 2^{\frac{n+1}{2}}\}$, n odd optimal w.r.t. the Welch bound,	cross correlation with m-sequences	$\longleftrightarrow$	Non-linearity	$2^{n-1} - 2^{\frac{n-1}{2}}$, n odd
$0, \pm 2^{(n+1)/2}$, n odd	Hadamard transform spectrum			$0, \pm 2^{(n+1)/2}$, n odd
$n(2^{\lceil n/3 \rceil} - 3)$ increased exponentially in n	Linear span	$\Longleftrightarrow$	Linear span	$n(2^{\lceil n/3 \rceil} - 3)$ increased exponentially in n
	NC		Degree	$\lceil n/3 \rceil + 1$
	NC		r-resilient	possible $r : 1 \le r \le n - \lceil n/3 \rceil$, n odd
easy*	Implementation			easy
Ideal candidates for Pseudo-random sequence generators	Applications			Ideal candidates for use as combining functions or filtering functions operating on a set of LFSRs

– *: There are two methods to implement WG sequences. One is to use 5 LSFRs together with a table look-up (Lemma 1 method). The other is to use a finite field configuration. The complexity of implementation of WG sequences by using the finite field configuration only depends on evaluation of four exponentiations listed in Section 2. Especially, it only depends on the evaluating the exponents q_3 and q_4 where each of them has $k-1$ consecutive 1's. We will discuss how to efficiently compute these two exponentiations at a separate paper. (*Note.* Implementation of the trace function has no cost.)

References

1. Xingong Chang, Zongduo Dai and Guang Gong, Some cryptographic properties of exponential functions, *Advances in Cryptology -ASIA CRYPT'94*, Lecture Notes in Computer Science, No. 917, Springer-Verlag, 1994, pp. 415-418.
2. John Dillon, Multiplicative difference sets via additive characters, *Designs, Codes and Cryptography.* **17** (1999), no. 1-3, 225–235.
3. J. Dillon and H. Dobbertin, New cyclic difference sets with Springer parameters, preprint, August 1999.
4. S.W. Golomb, *Shift Register Sequences*, Revised Edition, Aegean Park Press, 1982, pp. 39.
5. G. Gong, P. Gaal and S.W. Golomb, A suspected infinity class of cyclic Hadamard difference sets, *the Proceedings of 1997 IEEE Information Workshop*, July 6-12, 1997, Longyearbyen, Svalbard, Norway.
6. R. Gold, Maximal recursive sequences with 3-valued recursive cross-correlation functions, *IEEE Trans. on Inform. Theory*, January 1968, pp. 154-156.
7. G. Gong, Lecture notes, http://cacr.math.uwaterloo.ca/ ggong/CO739x/739xcover.html
8. G. Gong and S.W. Golomb, Transform domain analysis of DES, *IEEE Trans. on Inform. Theory*, vol. 45, No.6, September 1999, pp. 2065-2073.
9. R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, Volume 20, Addison-Wesley, 1983.
10. J.S. No, S.W. Golomb, G. Gong, H.K. Lee, and P. Gaal, New binary pseudo-random sequences of period $2^n - 1$ with ideal autocorrelation, *IEEE Trans. on Inform. Theory*, vol. 44, No. 2, March 1998, pp.814-817.

11. F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Company, 1977.
12. A. Maschietti, Difference sets and hyperovals, *Designs, Codes and Cryptography*, **14**, pp. 89-98, 1998.
13. J. M. Massey, *Shift register synthesis and BCH decoding*, IEEE transactions on Information Theory. Vol. 15, no. 1, pp. 122-127, January, 1969.
14. Jong-Seon No, Hagong Chung and Min-Seon Yin, Binary pseudo-random sequences of period $2^m - 1$ with ideal autocorrelation generated by the polynomial $z^d + (z+1)^d$, *IEEE Trans. Inform. Theory*, vol. 44, no. 3, 1998, pp.1278-1282.
15. R.A. Rueppel, *Analysis and Design of Stream Ciphers*, Springe-Verlag, 1986, pp.53.
16. T. Siegenthaler, Correlation-immunity of nonlinear combining functions for cryptographic applications, *IEEE Trans. on Inform. Theory*, vol. IT-30, No. 5, September 1984, pp.776-780.
17. A.F. Webster and S.E. Tavares, On the design of S-boxes, *Advances in Cryptology-Crypto'85*, Lecture Notes in Computer Science, No. 218, Springer-Verlag, 1985, pp. 523-534.
18. Guozheng Xiao and James Massey, A spectral characterization of correlation immune combining functions, *IEEE Trans. on Inform. Theory*, vol. 34, No. 3, May 1988, pp.569-571.
19. A. M. Youssef and G. Gong, On the interpolation attacks on block ciphers, Proceedings of *Fast Software Encryption 2000* , April 13-14, 2000, New York, Lecture Notes in computer science, to appear.

8 Appendix

Let $n = 11$, then $k = 4$, and

$$q_1 = 17, q_2 = 137, q_3 = 121, \text{ and } q_4 = 143.$$

So,

$$g(x) = x + x^{17} + x^{121} + x^{137} + x^{143}$$

and the WG transformation is given by

$$\begin{aligned} f(x) &= Tr(g(x+1)+1) \\ &= Tr(x^{25} + x^{35} + x^{41} + x^{57} + x^{69} + x^{71} + x^{73} + x^{89} + x^{105} + x^{121} + x^{139} + x^{141} + x^{143}). \end{aligned}$$

Let $\mathbb{F}_{2^{11}}$ be defined by a primitive polynomial $h(x) = x^{11} + x^2 + 1$. Let α be a root of $h(x)$. Then α is a primitive element of $\mathbb{F}_{2^{11}}$. We obtain a WG sequence $\underline{\mathbf{b}} = \{b_i\}$, $b_i = f(\alpha^i), i = 0, 1, \cdots$, as follows:

```
1 0 0 0 0 1 0 1 0 0 1 1 0 0 1 0 0 1 0 0 1 0 1 0 0 0 0 0 1 1
0 0 0 0 1 1 0 1 0 1 1 1 0 1 1 0 0 0 0 0 0 1 0 0 0 0 1 0 1 1
0 1 0 0 0 0 0 0 1 0 1 1 0 0 1 0 0 1 1 1 1 1 1 1 0 0 1 0 1 0
0 1 0 1 0 0 0 0 0 0 0 1 1 1 0 1 0 1 0 0 0 0 1 0 0 0 1 1 1 0
0 1 1 1 0 0 0 0 0 1 0 0 0 1 0 0 1 1 0 1 1 1 1 1 0 1 0 1 1 0
0 0 0 0 1 0 1 1 1 1 1 0 1 0 1 0 1 0 0 1 0 0 1 1 0 0 1 1 0 1
0 1 1 1 0 1 1 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 1 0 1 0 1 1 0 1
1 0 0 0 1 0 0 1 0 1 0 0 0 1 1 1 0 1 0 0 0 0 1 1 1 1 1 1 0 0
0 1 1 1 1 1 1 1 0 0 0 1 0 1 0 1 0 0 1 0 0 1 0 0 0 0 1 0 0 1
0 1 1 1 1 0 0 1 1 1 1 0 1 1 1 1 1 0 0 0 1 0 0 1 1 1 1 1 0 0


0 1 0 0 0 1 0 0 1 0 0 1 1 1 1 0 1 1 1 0 1 1 0 1 1 0 0 0 1 1
0 1 1 0 0 1 0 0 1 0 0 0 0 0 1 0 1 0 0 1 0 1 1 0 1 0 0 1 1 1
0 1 1 1 1 1 1 1 0 0 1 0 1 0 1 1 0 0 0 0 0 1 0 0 0 0 1 1 0 1
```

0 0 0 1 0 1 0 0 1 1 0 0 0 0 1 0 0 0 1 0 0 0 1 1 1 0 0 1 1 0
1 0 0 1 0 0 0 1 1 1 0 1 0 0 1 0 0 0 1 1 0 1 0 1 0 0 1 1 1 1
1 1 0 0 1 0 0 1 0 1 0 1 0 1 1 1 1 1 1 0 1 0 1 0 1 1 0 1 0 1
0 1 1 1 1 1 1 1 1 1 1 0 1 1 1 0 0 1 0 0 0 1 1 0 0 0 1 1 0 0
1 0 0 1 0 0 1 0 0 1 0 1 1 0 0 0 0 1 0 0 0 1 1 0 0 1 0 1 1 0
0 1 1 0 1 1 1 1 1 0 0 1 0 0 1 1 1 1 1 0 1 0 0 0 1 0 1 0 1 0
1 1 1 1 0 1 0 1 0 1 1 1 0 1 0 1 1 1 1 0 1 1 1 0 1 0 0 0 0 1

0 1 1 1 0 0 0 1 0 1 1 0 0 0 0 1 1 0 0 1 0 0 1 0 1 0 1 1 1 0
0 1 1 1 1 1 1 1 0 0 1 0 1 0 0 0 1 1 1 0 0 1 0 0 0 1 1 1 1 0
0 0 1 0 1 0 0 0 0 0 1 1 0 0 0 0 1 0 0 0 0 0 0 1 0 1 0 1 1 0
0 1 1 1 0 1 0 0 1 1 0 1 1 0 1 1 0 1 1 0 0 1 0 0 1 1 1 1 1 0
0 1 1 1 1 1 1 0 1 0 1 0 1 1 1 0 0 0 0 0 1 0 0 0 1 1 0 0 1 1
1 0 0 0 0 1 0 1 0 0 0 1 1 0 0 0 0 0 0 1 0 0 1 1 1 1 0 0 1 1
0 1 0 1 0 1 1 0 0 0 1 1 0 0 0 1 1 1 1 1 0 0 0 1 0 0 0 0 1 1
0 0 0 1 0 0 1 1 0 0 0 1 0 1 1 1 1 1 1 0 0 1 0 0 1 0 1 1 0 1
1 1 0 1 0 1 1 1 0 1 0 0 0 1 1 1 1 1 1 0 0 0 1 0 0 1 0 1 1 0
0 1 0 1 0 0 1 0 1 1 0 1 1 1 0 1 1 1 0 1 0 1 1 0 1 1 1 0 1 0

1 0 1 0 0 0 0 1 1 0 0 1 0 1 1 1 0 0 1 1 0 0 1 1 0 0 1 0 1 1
1 0 1 1 1 1 1 0 0 1 1 0 0 0 1 1 0 1 1 1 1 1 0 1 1 1 0 0 1 0
0 0 1 0 1 0 1 0 1 0 1 1 1 1 1 0 1 0 1 0 1 1 0 0 1 0 1 1 1 0
0 0 0 0 1 1 0 1 0 1 0 1 1 0 1 0 0 0 0 0 0 1 1 0 1 0 0 0 0 1
1 0 0 1 0 0 1 1 0 1 0 0 1 0 0 0 0 0 1 0 0 1 1 1 1 1 0 0 0 1
0 0 0 1 1 0 0 0 0 1 0 0 1 1 1 1 0 0 0 1 1 0 0 0 1 1 1 1 0 0
0 0 1 0 1 1 0 0 1 0 1 0 1 1 1 1 1 1 0 0 0 0 1 1 0 0 0 0 1 0
1 0 1 1 1 1 1 1 0 0 1 0 0 1 0 0 0 1 1 0 0 0 1 1 0 1 1 1 0 0
1 1 1 0 1 1 1 1 0 1 1 1 0 0 1 0 0 0 1 1 1 0 1 1 0 1 1 0 0 0
1 1 1 0 1 0 1 0 0 1 1 0 1 0 1 1 0 0 1 1 0 1 0 0 0 0 0 0 1 1

0 0 1 1 1 1 1 1 0 0 0 1 0 0 1 0 0 1 1 0 1 1 0 1 0 0 0 0 0 0
1 0 1 0 0 1 0 1 1 1 0 0 0 1 1 1 0 1 1 1 0 0 1 1 1 1 1 1 0 0
0 1 1 1 1 1 1 1 1 0 1 0 1 0 1 0 0 1 0 0 1 0 0 1 1 0 0 1 0 1
0 1 1 0 1 0 1 1 0 1 0 1 1 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 0 1
0 0 0 1 1 1 0 1 1 0 0 1 0 1 0 0 0 1 0 1 1 1 1 0 0 0 0 1 0 1
0 1 1 0 0 0 0 0 0 1 0 0 0 0 0 1 1 1 0 1 1 1 0 1 1 0 1 1 0 1
0 1 1 0 1 1 1 0 0 0 1 0 0 0 0 0 1 0 1 0 0 1 1 0 1 0 0 0 1 0
1 1 0 1 1 1 1 0 0 1 0 1 1 1 0 1 0 0 1 0 1 0 1 0 1 1 1 1 0 1
0 0 1 1 1 1 1 1 1 0 1 1 1 0 0 0 1 1 0 1 1 0 0 1 1 1 1 1 1 1
0 1 0 0 0 0 0 1 0 1 1 1 0 1 0 1 0 0 1 0 1 1 0 1 0 0 1 1 1 1

1 1 0 0 0 0 0 0 0 1 1 0 0 0 1 0 0 1 0 0 0 1 1 1 1 0 0 0 0 1
0 0 0 1 0 1 0 1 1 0 0 0 0 0 1 1 1 0 1 0 1 0 0 1 0 1 1 0 1 0
0 1 1 0 0 0 1 0 0 0 1 1 1 0 0 1 0 0 0 0 1 1 1 0 0 1 0 1 0 0
1 1 1 0 1 0 1 1 1 1 0 0 0 1 0 1 1 0 0 1 0 0 0 1 0 0 1 0 1 1
0 0 0 1 0 1 1 1 0 1 0 0 1 0 1 1 0 0 0 0 0 1 1 1 0 1 1 1 1 0
1 1 1 0 1 1 1 1 0 0 0 0 1 0 0 1 0 1 1 1 0 0 1 1 1 0 0 0 1 1
1 1 1 1 0 1 1 1 0 1 1 0 1 1 1 0 0 1 1 1 0 0 0 1 0 0 1 1 1 1
1 0 1 1 1 0 1 0 0 0 0 0 0 0 1 0 0 0 0 1 1 1 0 1 1 1 1 0 0 0
0 1 1 1 0 1 1 1 0 1 0 0 1 1 0 1 1 1 1 1 0 0 1 1 1 1 1 0 0 1
1 0 1 1 1 0 0 0 1 0 0 0 1 0 1 1 0 0 1 0 1 1 1 0 0 0 1 0 0 0

```
1 1 0 0 1 0 0 0 0 1 0 1 0 0 1 0 1 1 0 1 0 0 1 1 0 1 1 0 1 0
1 0 0 1 0 1 1 1 1 0 0 1 0 0 1 1 1 1 0 1 0 1 1 0 0 0 1 1 1 0
1 0 0 1 1 1 1 1 1 0 1 0 1 1 0 1 0 1 1 0 1 0 0 0 0 0 0 0 1 1
1 1 0 0 1 1 1 1 1 0 1 1 1 1 0 1 1 0 1 0 1 0 0 0 0 0 1 0 0 1
0 0 0 0 1 0 0 0 1 1 0 0 1 1 0 1 1 0 0 0 1 1 1 0 1 0 1 1 1 1
0 0 1 0 0 1 1 1 0 0 1 1 1 0 0 0 0 0 1 1 0 1 1 0 1 1 1 0 0 0
0 0 0 1 0 0 0 0 1 0 1 1 0 0 1 0 0 1 1 0 0 1 1 0 1 0 0 0 1 1
0 1 0 0 0 1 0 0 0 1 0 0 1 0 1 0 0 0 1 1 0 1 0 1 0 0 0 0 1 1
1 0 0 1 0 1 1
```

$\underline{\mathbf{b}}$ is balanced, has ideal 2-tuple distribution, 2-level auto correlation, 3-valued cross correlation with the m-sequence $\{a_i\}, a_i = Tr(\alpha^i), i = 0, 1, \cdots$, which belongs to the set $\{-1, 63, -65\}$, the Hadamard transform spectra belong to the set $\{0, \pm 64\}$ and linear span 143. The algebraic normal form (ANF) of the Boolean representation of $f(x)$ under the basis $B_1 = \{1, \alpha, \cdots, \alpha^{10}\}$ is given by Table 1. Note that in the following tables we list a monomial $x_{i_1}x_{i_2}\cdots x_{i_s}$ of $f(x_0, x_1, \cdots, x_{10})$ as $(i_1, i_2, \cdots, i_s)$.

Table 1. ANF of the Boolean Representation of $f(x)$ under the Basis B_1

(0) (5) (7) (10)

(0,3) (1,4) (3,4) (1,5) (2,5) (4,5) (0,6) (1,6) (3,6)
(5,6) (1,7) (3,7) (6,7) (2,8) (3,8) (6,8) (7,8) (5,9)
(6,9) (7,9) (2,10) (4,10) (7,10) (8,10)

(1,2,3) (0,1,4) (1,2,4) (0,3,4) (0,1,5) (0,2,5) (0,3,5)
(0,4,5) (2,4,5) (0,1,6) (1,3,6) (2,4,6) (0,5,6) (2,5,6)
(3,5,6) (0,2,7) (1,2,7) (2,3,7) (0,4,7) (1,4,7) (2,4,7)
(2,5,7) (1,6,7) (4,6,7) (5,6,7) (0,2,8) (1,2,8) (1,3,8)
(2,3,8) (2,4,8) (3,4,8) (0,5,8) (1,5,8) (2,5,8) (3,5,8)
(4,5,8) (0,6,8) (3,6,8) (5,6,8) (0,7,8) (5,7,8) (0,1,9)
(1,2,9) (0,3,9) (1,3,9) (2,3,9) (1,4,9) (3,4,9) (2,5,9)
(4,5,9) (0,6,9) (1,6,9) (3,6,9) (4,6,9) (1,7,9) (3,7,9)
(5,7,9) (2,8,9) (3,8,9) (4,8,9) (5,8,9) (7,8,9) (0,2,10)
(1,2,10) (1,3,10) (0,4,10) (3,4,10) (2,5,10) (0,6,10) (1,6,10)
(3,6,10) (0,7,10) (1,7,10) (4,7,10) (5,7,10) (0,8,10) (4,8,10)
(5,8,10) (0,9,10) (1,9,10) (2,9,10) (3,9,10)

(0,1,2,3)	(0,1,2,4)	(0,2,3,4)	(1,2,3,4)	(0,1,3,5)	(0,2,3,5)
(1,2,3,5)	(1,2,4,5)	(0,3,4,5)	(0,1,3,6)	(0,2,3,6)	(1,2,3,6)
(0,2,4,6)	(1,2,4,6)	(0,3,4,6)	(2,3,4,6)	(0,1,5,6)	(0,3,5,6)
(1,3,5,6)	(2,3,5,6)	(0,4,5,6)	(1,4,5,6)	(3,4,5,6)	(0,1,2,7)
(1,2,3,7)	(0,3,4,7)	(1,3,4,7)	(2,3,4,7)	(0,1,5,7)	(2,3,5,7)
(0,4,5,7)	(1,4,5,7)	(2,4,5,7)	(3,4,5,7)	(0,2,6,7)	(0,3,6,7)
(3,4,6,7)	(0,5,6,7)	(0,1,2,8)	(0,2,3,8)	(0,2,4,8)	(0,2,5,8)
(1,2,5,8)	(1,3,5,8)	(2,3,5,8)	(0,4,5,8)	(1,4,5,8)	(3,4,5,8)
(1,2,6,8)	(0,3,6,8)	(1,3,6,8)	(0,4,6,8)	(2,4,6,8)	(3,4,6,8)
(0,1,7,8)	(0,2,7,8)	(0,3,7,8)	(1,3,7,8)	(0,4,7,8)	(3,4,7,8)
(1,5,7,8)	(2,5,7,8)	(3,5,7,8)	(0,6,7,8)	(2,6,7,8)	(3,6,7,8)
(0,2,3,9)	(0,1,4,9)	(0,2,4,9)	(1,3,4,9)	(2,3,4,9)	(0,3,5,9)
(3,4,5,9)	(0,2,6,9)	(1,2,6,9)	(0,3,6,9)	(1,3,6,9)	(0,4,6,9)
(2,4,6,9)	(3,4,6,9)	(3,5,6,9)	(4,5,6,9)	(1,2,7,9)	(0,3,7,9)
(0,4,7,9)	(1,4,7,9)	(3,4,7,9)	(3,5,7,9)	(4,5,7,9)	(2,6,7,9)
(4,6,7,9)	(5,6,7,9)	(1,2,8,9)	(0,3,8,9)	(1,3,8,9)	(0,5,8,9)
(2,5,8,9)	(4,5,8,9)	(1,6,8,9)	(2,6,8,9)	(5,6,8,9)	(0,7,8,9)
(1,7,8,9)	(3,7,8,9)	(4,7,8,9)	(5,7,8,9)	(6,7,8,9)	(0,1,2,10)
(0,1,3,10)	(0,2,3,10)	(1,2,3,10)	(0,3,4,10)	(2,3,4,10)	(1,3,5,10)
(2,3,5,10)	(0,2,6,10)	(1,2,6,10)	(1,3,6,10)	(0,4,6,10)	(1,4,6,10)
(2,4,6,10)	(3,4,6,10)	(0,5,6,10)	(3,5,6,10)	(0,1,7,10)	(0,2,7,10)
(2,4,7,10)	(3,4,7,10)	(3,5,7,10)	(1,6,7,10)	(2,6,7,10)	(3,6,7,10)
(5,6,7,10)	(0,1,8,10)	(0,3,8,10)	(2,3,8,10)	(1,4,8,10)	(2,4,8,10)
(1,5,8,10)	(2,5,8,10)	(3,5,8,10)	(0,6,8,10)	(1,6,8,10)	(0,7,8,10)
(1,7,8,10)	(2,7,8,10)	(3,7,8,10)	(4,7,8,10)	(1,2,9,10)	(1,3,9,10)
(1,4,9,10)	(3,4,9,10)	(0,5,9,10)	(2,5,9,10)	(4,5,9,10)	(1,6,9,10)
(2,6,9,10)	(5,6,9,10)	(2,7,9,10)	(5,7,9,10)	(0,8,9,10)	(1,8,9,10)
(2,8,9,10)	(3,8,9,10)	(6,8,9,10)	(7,8,9,10)		

(0,1,2,4,5)	(1,2,3,4,6)	(0,1,2,5,6)	(0,1,3,5,6)	(0,2,3,5,6)
(1,2,3,5,6)	(0,1,4,5,6)	(1,2,4,5,6)	(0,1,2,4,7)	(0,1,3,4,7)
(1,2,3,4,7)	(0,1,2,5,7)	(0,1,3,5,7)	(0,2,3,5,7)	(1,2,3,5,7)
(0,1,4,5,7)	(0,2,4,5,7)	(0,1,2,6,7)	(0,2,3,6,7)	(0,1,4,6,7)
(1,3,4,6,7)	(0,1,5,6,7)	(0,2,5,6,7)	(1,2,5,6,7)	(1,4,5,6,7)
(3,4,5,6,7)	(0,1,2,4,8)	(0,1,3,4,8)	(0,2,3,4,8)	(1,2,3,4,8)
(0,1,2,5,8)	(1,2,4,5,8)	(0,3,4,5,8)	(1,3,4,5,8)	(1,2,3,6,8)
(1,2,4,6,8)	(0,2,5,6,8)	(1,2,5,6,8)	(2,3,5,6,8)	(2,4,5,6,8)
(0,1,2,7,8)	(0,1,3,7,8)	(0,2,4,7,8)	(0,3,4,7,8)	(1,3,4,7,8)
(1,2,5,7,8)	(2,3,5,7,8)	(0,4,5,7,8)	(1,2,6,7,8)	(2,3,6,7,8)
(0,4,6,7,8)	(0,5,6,7,8)	(1,5,6,7,8)	(2,5,6,7,8)	(3,5,6,7,8)
(0,1,2,3,9)	(0,1,3,4,9)	(0,2,3,4,9)	(1,2,3,4,9)	(1,2,3,5,9)
(1,2,4,5,9)	(0,3,4,5,9)	(1,3,4,5,9)	(2,3,4,5,9)	(0,1,3,6,9)
(0,2,3,6,9)	(0,1,4,6,9)	(0,2,4,6,9)	(0,3,4,6,9)	(1,3,4,6,9)
(0,2,5,6,9)	(0,3,5,6,9)	(1,4,5,6,9)	(2,4,5,6,9)	(3,4,5,6,9)
(0,2,3,7,9)	(1,2,3,7,9)	(0,1,4,7,9)	(0,2,4,7,9)	(1,3,4,7,9)
(2,3,4,7,9)	(0,1,5,7,9)	(0,2,5,7,9)	(1,2,5,7,9)	(0,3,5,7,9)
(1,3,5,7,9)	(0,4,5,7,9)	(1,4,5,7,9)	(0,1,6,7,9)	(0,3,6,7,9)
(1,3,6,7,9)	(1,4,6,7,9)	(2,4,6,7,9)	(3,4,6,7,9)	(3,5,6,7,9)
(0,1,4,8,9)	(0,2,4,8,9)	(0,3,4,8,9)	(1,3,4,8,9)	(0,2,5,8,9)
(1,2,5,8,9)	(0,3,5,8,9)	(1,4,5,8,9)	(0,1,6,8,9)	(0,2,6,8,9)
(1,2,6,8,9)	(1,3,6,8,9)	(2,4,6,8,9)	(0,5,6,8,9)	(1,5,6,8,9)
(2,5,6,8,9)	(3,5,6,8,9)	(4,5,6,8,9)	(0,1,7,8,9)	(2,3,7,8,9)
(1,4,7,8,9)	(3,4,7,8,9)	(0,5,7,8,9)	(1,5,7,8,9)	(2,5,7,8,9)
(4,5,7,8,9)	(0,6,7,8,9)	(2,6,7,8,9)	(4,6,7,8,9)	(5,6,7,8,9)
(0,1,2,3,10)	(0,1,2,4,10)	(0,1,3,4,10)	(1,2,3,4,10)	(0,1,3,5,10)
(1,2,3,5,10)	(0,1,4,5,10)	(0,2,4,5,10)	(1,2,4,5,10)	(0,3,4,5,10)
(1,3,4,5,10)	(2,3,4,5,10)	(0,1,2,6,10)	(0,1,3,6,10)	(0,3,4,6,10)
(1,3,4,6,10)	(2,3,4,6,10)	(0,2,5,6,10)	(0,3,5,6,10)	(1,3,5,6,10)
(1,4,5,6,10)	(0,1,2,7,10)	(0,2,3,7,10)	(1,2,3,7,10)	(0,1,4,7,10)
(1,2,4,7,10)	(0,1,5,7,10)	(0,2,5,7,10)	(0,3,5,7,10)	(2,3,5,7,10)
(0,4,5,7,10)	(1,4,5,7,10)	(3,4,5,7,10)	(0,1,6,7,10)	(0,2,6,7,10)
(0,5,6,7,10)	(1,5,6,7,10)	(3,5,6,7,10)	(4,5,6,7,10)	(0,1,2,8,10)
(0,1,3,8,10)	(0,1,4,8,10)	(0,2,4,8,10)	(1,2,4,8,10)	(0,3,4,8,10)
(1,3,4,8,10)	(0,1,5,8,10)	(0,2,5,8,10)	(2,3,5,8,10)	(3,4,5,8,10)
(0,1,6,8,10)	(1,2,6,8,10)	(0,3,6,8,10)	(2,3,6,8,10)	(0,5,6,8,10)
(2,5,6,8,10)	(3,5,6,8,10)	(0,2,7,8,10)	(1,2,7,8,10)	(0,3,7,8,10)
(1,3,7,8,10)	(2,4,7,8,10)	(2,5,7,8,10)	(3,5,7,8,10)	(4,5,7,8,10)
(1,6,7,8,10)	(5,6,7,8,10)	(0,1,2,9,10)	(0,2,3,9,10)	(2,3,4,9,10)
(0,1,5,9,10)	(1,2,5,9,10)	(0,3,5,9,10)	(2,3,5,9,10)	(0,1,6,9,10)
(0,2,6,9,10)	(1,2,6,9,10)	(0,3,6,9,10)	(1,3,6,9,10)	(2,3,6,9,10)
(2,4,6,9,10)	(0,5,6,9,10)	(4,5,6,9,10)	(0,2,7,9,10)	(1,2,7,9,10)
(0,3,7,9,10)	(2,3,7,9,10)	(1,4,7,9,10)	(2,4,7,9,10)	(3,5,7,9,10)
(0,6,7,9,10)	(1,6,7,9,10)	(5,6,7,9,10)	(0,1,8,9,10)	(0,2,8,9,10)
(3,4,8,9,10)	(0,6,8,9,10)	(2,6,8,9,10)	(4,6,8,9,10)	(5,6,8,9,10)
(1,7,8,9,10)	(3,7,8,9,10)	(4,7,8,9,10)	(5,7,8,9,10)	

Using the following basis conversion matrix

$$A = \begin{pmatrix} 0&0&0&0&1&1&0&0&0&0&0 \\ 0&0&0&1&0&1&1&1&0&0&0 \\ 0&0&0&0&0&0&1&1&0&0&0 \\ 0&0&0&0&1&0&0&1&0&0&0 \\ 0&0&0&0&0&1&1&0&0&1&1 \\ 0&1&1&1&1&1&0&1&0&0&0 \\ 0&1&0&0&0&0&1&0&1&1&1 \\ 1&0&0&0&1&1&1&0&1&0&0 \\ 1&1&1&0&1&0&1&0&0&1&0 \\ 0&0&1&0&1&1&0&1&0&0&1 \\ 0&1&0&1&0&1&1&0&0&1&1 \end{pmatrix}$$

the algebraic normal form of of a Boolean representation of $f(x)$ under the basis $B_2 = A(1, \alpha, \cdots, \alpha^{10})^T$ is listed in Table 2, which is 1-resilient with nonlinearity 992, degree 5 and linear span 143. (Note that there are 505 and 534 monomials in the ANF of the Boolean representations of $f(x)$ under the bases B_1 and B_2 respectively.)

Table 2. ANF of the Boolean Representation of $f(x)$ under the Basis B_2

(1) (2) (3) (4) (5) (6) (7) (9)

(0,3) (3,4) (0,5) (1,5) (2,5) (3,5) (4,5) (2,6) (3,6)
(4,6) (5,6) (0,7) (3,7) (4,7) (5,7) (6,7) (0,8) (2,8)
(6,8) (2,9) (5,9) (6,9) (7,9) (0,10) (1,10) (5,10) (6,10)
(9,10)

(0,1,2) (0,2,3) (0,1,4) (0,2,4) (1,2,4) (1,3,4) (2,3,4)
(0,1,5) (0,3,5) (1,3,5) (0,4,5) (0,1,6) (0,2,6) (0,3,6)
(2,3,6) (1,4,6) (2,4,6) (3,4,6) (0,5,6) (1,5,6) (3,5,6)
(4,5,6) (1,2,7) (0,3,7) (1,3,7) (0,4,7) (2,4,7) (3,4,7)
(3,5,7) (4,5,7) (0,6,7) (1,6,7) (2,6,7) (4,6,7) (5,6,7)
(0,2,8) (1,2,8) (1,3,8) (2,4,8) (3,4,8) (0,5,8) (1,5,8)
(2,5,8) (3,5,8) (0,6,8) (4,6,8) (1,7,8) (6,7,8) (0,2,9)
(1,2,9) (0,3,9) (0,4,9) (1,4,9) (0,5,9) (3,5,9) (0,6,9)
(2,6,9) (4,6,9) (5,6,9) (1,7,9) (3,7,9) (4,7,9) (1,8,9)
(2,8,9) (5,8,9) (6,8,9) (7,8,9) (0,1,10) (1,2,10) (0,3,10)
(2,3,10) (1,4,10) (3,4,10) (0,5,10) (1,5,10) (2,5,10) (4,5,10)
(2,6,10) (4,6,10) (0,7,10) (3,7,10) (0,8,10) (6,8,10) (0,9,10)
(2,9,10) (4,9,10) (6,9,10)

(0,1,2,3)	(0,1,2,4)	(0,2,3,4)	(1,2,3,4)	(0,1,3,5)	(0,2,3,5)
(0,2,4,5)	(1,2,4,5)	(1,3,4,5)	(2,3,4,5)	(0,1,2,6)	(0,1,3,6)
(0,3,4,6)	(2,3,4,6)	(0,1,5,6)	(1,2,5,6)	(1,3,5,6)	(1,4,5,6)
(0,1,3,7)	(0,2,3,7)	(0,1,4,7)	(0,2,4,7)	(1,2,4,7)	(0,3,4,7)
(2,3,5,7)	(0,4,5,7)	(1,4,5,7)	(2,4,5,7)	(3,4,5,7)	(0,2,6,7)
(0,3,6,7)	(1,3,6,7)	(1,4,6,7)	(0,5,6,7)	(1,5,6,7)	(2,5,6,7)
(0,1,2,8)	(0,1,3,8)	(0,1,4,8)	(0,2,4,8)	(0,3,4,8)	(1,3,4,8)
(0,1,5,8)	(1,2,5,8)	(0,3,5,8)	(1,3,5,8)	(2,3,5,8)	(0,2,6,8)
(1,2,6,8)	(1,3,6,8)	(1,4,6,8)	(2,4,6,8)	(0,5,6,8)	(4,5,6,8)
(0,1,7,8)	(0,2,7,8)	(0,3,7,8)	(1,3,7,8)	(2,3,7,8)	(0,4,7,8)
(1,4,7,8)	(2,4,7,8)	(3,4,7,8)	(0,5,7,8)	(1,5,7,8)	(2,5,7,8)
(4,5,7,8)	(0,6,7,8)	(1,6,7,8)	(2,6,7,8)	(3,6,7,8)	(4,6,7,8)
(0,1,2,9)	(0,2,3,9)	(1,2,3,9)	(1,2,4,9)	(2,3,4,9)	(0,1,5,9)
(0,2,5,9)	(1,3,5,9)	(0,4,5,9)	(1,2,6,9)	(0,3,6,9)	(2,3,6,9)
(0,4,6,9)	(2,4,6,9)	(3,4,6,9)	(2,5,6,9)	(1,3,7,9)	(2,3,7,9)
(0,4,7,9)	(2,4,7,9)	(3,4,7,9)	(2,5,7,9)	(0,6,7,9)	(1,6,7,9)
(2,6,7,9)	(4,6,7,9)	(1,2,8,9)	(0,3,8,9)	(1,3,8,9)	(2,4,8,9)
(3,4,8,9)	(0,5,8,9)	(1,5,8,9)	(2,5,8,9)	(4,5,8,9)	(0,6,8,9)
(1,6,8,9)	(2,6,8,9)	(4,6,8,9)	(1,7,8,9)	(3,7,8,9)	(5,7,8,9)
(0,1,2,10)	(0,1,3,10)	(0,2,3,10)	(0,1,4,10)	(1,3,4,10)	(0,1,5,10)
(1,2,5,10)	(0,3,5,10)	(2,3,5,10)	(0,2,6,10)	(1,2,6,10)	(0,3,6,10)
(1,3,6,10)	(2,3,6,10)	(0,4,6,10)	(1,4,6,10)	(2,4,6,10)	(0,5,6,10)
(2,5,6,10)	(3,5,6,10)	(0,1,7,10)	(1,3,7,10)	(2,3,7,10)	(0,4,7,10)
(1,4,7,10)	(0,5,7,10)	(1,5,7,10)	(3,5,7,10)	(4,5,7,10)	(0,6,7,10)
(1,6,7,10)	(3,6,7,10)	(5,6,7,10)	(1,2,8,10)	(1,3,8,10)	(2,3,8,10)
(1,4,8,10)	(3,4,8,10)	(2,5,8,10)	(3,5,8,10)	(4,5,8,10)	(1,6,8,10)
(4,6,8,10)	(5,6,8,10)	(1,7,8,10)	(5,7,8,10)	(0,1,9,10)	(3,4,9,10)
(1,5,9,10)	(0,6,9,10)	(2,6,9,10)	(3,6,9,10)	(5,6,9,10)	(1,7,9,10)
(2,7,9,10)	(3,7,9,10)	(4,7,9,10)	(5,7,9,10)	(0,8,9,10)	(3,8,9,10)
(5,8,9,10)	(6,8,9,10)	(7,8,9,10)			

(0,1,2,3,4)	(0,1,2,3,5)	(0,1,2,4,5)	(0,1,3,4,6)	(0,2,3,4,6)	(0,1,3,5,6)
(0,2,3,5,6)	(0,1,4,5,6)	(0,3,4,5,6)	(2,3,4,5,6)	(0,1,2,3,7)	(1,2,3,4,7)
(1,2,3,5,7)	(0,1,4,5,7)	(1,2,4,5,7)	(2,3,4,5,7)	(0,1,2,6,7)	(1,2,3,6,7)
(0,2,4,6,7)	(0,3,4,6,7)	(2,3,4,6,7)	(0,1,5,6,7)	(1,2,5,6,7)	(2,3,5,6,7)
(1,4,5,6,7)	(2,4,5,6,7)	(0,1,2,3,8)	(0,1,3,4,8)	(0,2,3,4,8)	(1,2,3,4,8)
(0,2,3,5,8)	(1,2,3,5,8)	(0,1,4,5,8)	(0,2,4,5,8)	(1,2,4,5,8)	(0,3,4,5,8)
(2,3,4,5,8)	(0,1,2,6,8)	(0,1,3,6,8)	(1,2,3,6,8)	(0,1,4,6,8)	(0,3,4,6,8)
(2,3,4,6,8)	(0,2,5,6,8)	(1,2,5,6,8)	(1,3,5,6,8)	(2,3,5,6,8)	(1,4,5,6,8)
(2,4,5,6,8)	(0,1,3,7,8)	(0,1,4,7,8)	(0,2,4,7,8)	(1,2,4,7,8)	(0,3,4,7,8)
(0,1,5,7,8)	(2,3,5,7,8)	(0,1,6,7,8)	(0,2,6,7,8)	(1,2,6,7,8)	(1,3,6,7,8)
(2,3,6,7,8)	(0,4,6,7,8)	(1,4,6,7,8)	(4,5,6,7,8)	(0,1,2,4,9)	(1,2,3,4,9)
(1,2,3,5,9)	(0,2,4,5,9)	(1,2,4,5,9)	(0,3,4,5,9)	(1,3,4,5,9)	(0,1,2,6,9)
(0,1,3,6,9)	(0,2,3,6,9)	(1,2,4,6,9)	(1,3,4,6,9)	(2,3,4,6,9)	(0,1,5,6,9)
(0,2,5,6,9)	(1,2,5,6,9)	(1,3,5,6,9)	(1,4,5,6,9)	(2,4,5,6,9)	(0,1,3,7,9)
(1,2,3,7,9)	(0,2,4,7,9)	(2,3,4,7,9)	(1,2,5,7,9)	(1,3,5,7,9)	(1,4,5,7,9)
(3,4,5,7,9)	(0,1,6,7,9)	(0,2,6,7,9)	(0,3,6,7,9)	(1,3,6,7,9)	(2,3,6,7,9)
(0,4,6,7,9)	(3,4,6,7,9)	(0,5,6,7,9)	(1,5,6,7,9)	(2,5,6,7,9)	(3,5,6,7,9)
(4,5,6,7,9)	(0,2,3,8,9)	(1,2,3,8,9)	(0,2,4,8,9)	(0,1,5,8,9)	(0,2,5,8,9)
(1,2,5,8,9)	(0,3,5,8,9)	(2,3,5,8,9)	(0,4,5,8,9)	(1,4,5,8,9)	(2,4,5,8,9)
(3,4,5,8,9)	(0,1,6,8,9)	(0,2,6,8,9)	(1,2,6,8,9)	(0,3,6,8,9)	(2,3,6,8,9)
(0,4,6,8,9)	(1,4,6,8,9)	(1,5,6,8,9)	(2,5,6,8,9)	(3,5,6,8,9)	(0,1,7,8,9)
(0,3,7,8,9)	(1,3,7,8,9)	(1,4,7,8,9)	(2,5,7,8,9)	(0,6,7,8,9)	(1,6,7,8,9)
(4,6,7,8,9)	(0,1,2,3,10)	(0,1,2,4,10)	(1,2,3,4,10)	(0,1,2,5,10)	(0,1,3,5,10)
(1,2,3,5,10)	(0,2,4,5,10)	(0,3,4,5,10)	(2,3,4,5,10)	(0,1,2,6,10)	(0,1,3,6,10)
(0,2,3,6,10)	(0,1,4,6,10)	(0,2,4,6,10)	(1,2,4,6,10)	(0,3,4,6,10)	(0,1,5,6,10)
(1,2,5,6,10)	(0,3,5,6,10)	(1,3,5,6,10)	(1,4,5,6,10)	(2,4,5,6,10)	(3,4,5,6,10)
(0,2,3,7,10)	(0,2,4,7,10)	(1,2,4,7,10)	(1,3,4,7,10)	(2,3,4,7,10)	(1,2,5,7,10)
(0,3,5,7,10)	(1,3,5,7,10)	(3,4,5,7,10)	(0,1,6,7,10)	(1,2,6,7,10)	(1,3,6,7,10)
(2,4,6,7,10)	(3,4,6,7,10)	(0,5,6,7,10)	(1,5,6,7,10)	(2,5,6,7,10)	(4,5,6,7,10)
(1,3,4,8,10)	(0,2,5,8,10)	(1,2,5,8,10)	(0,3,5,8,10)	(2,3,5,8,10)	(0,3,6,8,10)
(1,3,6,8,10)	(0,4,6,8,10)	(2,4,6,8,10)	(3,4,6,8,10)	(0,5,6,8,10)	(2,5,6,8,10)
(3,5,6,8,10)	(1,2,7,8,10)	(0,3,7,8,10)	(2,3,7,8,10)	(2,4,7,8,10)	(1,5,7,8,10)
(2,5,7,8,10)	(5,6,7,8,10)	(0,1,2,9,10)	(1,2,3,9,10)	(0,2,4,9,10)	(1,3,4,9,10)
(2,3,4,9,10)	(0,1,5,9,10)	(0,3,5,9,10)	(2,3,5,9,10)	(2,4,5,9,10)	(0,1,6,9,10)
(2,3,6,9,10)	(0,4,6,9,10)	(1,4,6,9,10)	(3,4,6,9,10)	(0,5,6,9,10)	(2,5,6,9,10)
(3,5,6,9,10)	(0,2,7,9,10)	(1,2,7,9,10)	(0,3,7,9,10)	(1,3,7,9,10)	(2,3,7,9,10)
(1,4,7,9,10)	(3,4,7,9,10)	(1,5,7,9,10)	(2,5,7,9,10)	(1,6,7,9,10)	(4,6,7,9,10)
(5,6,7,9,10)	(0,3,8,9,10)	(2,3,8,9,10)	(0,4,8,9,10)	(1,4,8,9,10)	(2,4,8,9,10)
(0,6,8,9,10)	(2,6,8,9,10)	(3,6,8,9,10)	(4,6,8,9,10)	(1,7,8,9,10)	(5,7,8,9,10)