On the studies related to linear codes in generalized construction of resilient functions with very high nonlinearity

Subhamoy Maitra
Applied Statistics Unit
Indian Statistical Institute
e-mail: subho@isical.ac.in
Definitions and notations

• An $n$-variable Boolean function may be viewed as a mapping from $\{0, 1\}^n$ into $\{0, 1\}$.

• By $\Omega_n$ we mean the set of all Boolean functions of $n$ variables.

• We interpret a Boolean function $f(X_1, \ldots, X_n)$ as the output column of its truth table $f$, i.e., a binary string of length $2^n$, $f = [f(0, 0, \cdots, 0), f(1, 0, \cdots, 0), f(0, 1, \cdots, 0), \ldots, f(1, 1, \cdots, 1)]$.

• $f(X_1, \ldots, X_n)$ can be written in algebraic normal form as
  
  \[ a_0 + \sum_{i=1}^{n} a_i X_i + \sum_{1 \leq i < j \leq n} a_{ij} X_i X_j + \cdots + a_{12\ldots n} X_1 X_2 \cdots X_n, \]

  where $a_0, a_{ij}, \ldots, a_{12\ldots n} \in \{0, 1\}$.

  + here means addition over GF(2), i.e.,
  
  $0 + 0 = 0, 0 + 1 = 1, 1 + 0 = 1, 1 + 1 = 0$.

• $\text{wt}(f) = |\{x | f(x) = 1\}| = |\text{Supp}(f)|$.

  Balanced function: $\text{wt}(f) = 2^{n-1}$. 

Example

<table>
<thead>
<tr>
<th>$X_4$</th>
<th>$X_3$</th>
<th>$X_2$</th>
<th>$X_1$</th>
<th>$f$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Truth table of a 4-variable Boolean function.

Algebraic Normal Form $X_4 + X_3 + X_1X_2$. 
Definitions and notations (Contd.)

- Concatenation of TTs of \( f_1, f_2 \in \Omega_{n-1} \) to get \( f \in \Omega_n \). Denote by \( f = f_1||f_2 \). In ANF, \( f(X_1, \ldots, X_n) = (1 + X_n)f_1(X_1, \ldots, X_{n-1}) + X_nf_2(X_1, \ldots, X_{n-1}) \).

- For complement of \( f \) we use the notation \( \overline{f} \), i.e., in ANF, \( \overline{f} = 1 + f \).

- Functions of degree at most one are called affine functions. An affine function with constant term equal to zero is called a linear function: \( a_0 + a_1X_1 + \ldots a_nX_n, a_i \in \{0, 1\} \). Thus there are \( 2^{n+1} \) affine functions and \( 2^n \) linear functions (when \( a_0 = 0 \)).

The set of all \( n \)-variable affine (respectively linear) functions is denoted by \( A(n) \) (respectively \( L(n) \)). The nonlinearity of an \( n \)-variable function \( f \) is

\[
\text{nl}(f) = \min_{g \in A(n)}(d(f, g)),
\]

i.e., the distance from the set of all \( n \)-variable affine functions.
Walsh Transform

Let \( X = (X_1, \ldots, X_n) \) and \( \omega = (\omega_1, \ldots, \omega_n) \) both belong to \( \{0, 1\}^n \) and inner product
\( X \cdot \omega = X_1 \omega_1 + \ldots + X_n \omega_n \) (Linear Function).

Let \( f(X) \) be a Boolean function on \( n \) variables. Then the \textit{Walsh transform} of \( f(X) \) is a integer valued function over \( \{0, 1\}^n \) that can be defined as
\[
W_f(\omega) = \sum_{X \in \{0,1\}^n} (-1)^{f(X)+X \cdot \omega}.
\]

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th>f</th>
<th>(-1)^i</th>
<th>i = 0</th>
<th>i = 1</th>
<th>i = 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>-1</td>
<td>-2</td>
<td>-2</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-2</td>
<td>-4</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>-2</td>
<td>4</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>-1</td>
<td>0</td>
<td>2</td>
<td>-4</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>-2</td>
<td>-2</td>
<td>4</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>-2</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>-2</td>
<td>0</td>
</tr>
</tbody>
</table>

Fast Walsh Transform: requires \( O(n2^n) \) steps.

Can we get a better algorithm?

\[
nl(f) = 2^{n-1} - \frac{1}{2} \max_{\omega \in \{0,1\}^n} |W_f(\omega)|.
\]

Why?

\[
W_f(\omega) = \#(f = \omega \cdot X) - \#(f \neq \omega \cdot X).
\]

\[
2^n = \#(f = \omega \cdot X) + \#(f \neq \omega \cdot X).
\]

So,

\[
d(f, \omega \cdot X) = \#(f \neq \omega \cdot X) = 2^{n-1} - \frac{1}{2}W_f(\omega).
\]

Minimum \( d(f, \omega \cdot X) \) comes from maximum \( |W_f(\omega)| \).
Correlation Immunity and Resiliency

A function \( f(x_1, \ldots, x_n) \) is \( t \)-th order correlation immune (CI) iff its Walsh transform \( W_f \) satisfies

\[
W_f(\omega) = 0,
\]
for all \( \omega \in \{0, 1\}^n \) such that \( 1 \leq wt(\omega) \leq t \).

If \( f \) is balanced then \( W_f(0) = 0 \). Balanced \( t \)-th order correlation immune functions are called \( t \)-resilient functions. Thus, a function \( f(x_1, \ldots, x_n) \) is \( t \)-resilient iff its Walsh transform \( W_f \) satisfies

\[
W_f(\omega) = 0,
\]
for all \( \omega \in \{0, 1\}^n \) such that \( 0 \leq wt(\omega) \leq t \).
Multiple Output Boolean Function

By $F^n_q$ we denote the vector space corresponding to the finite field $F_{q^n}$. We now introduce the concepts with respect to the multiple output Boolean functions $F^n_2 \rightarrow F^m_2$. In this case, the truth table contains $m$ different output columns, each of length $2^n$.

$F(x) : F^n_2 \rightarrow F^m_2$ such that $F(x) = (f_1(x), \ldots, f_m(x))$. 
Multiple Output Boolean Function
(Contd.)

The nonlinearity of $F$ is defined as,

$$nl(F) = \min_{\tau \in \mathbb{F}_2^m} nl\left( \bigoplus_{j=1}^m \tau_j f_j(x) \right).$$

Here, $\mathbb{F}_2^m = \mathbb{F}_2^m \setminus \{0\}$ and $\tau = (\tau_1, \ldots, \tau_m)$. Similarly the algebraic degree of $F$ is defined as,

$$deg(F) = \min_{\tau \in \mathbb{F}_2^m} deg\left( \bigoplus_{j=1}^m \tau_j f_j(x) \right).$$

Now we define an $n$-variable, $m$-output, $t$-resilient function, denoted by $(n, m, t)$, as follows. A function $F$ is an $(n, m, t)$ resilient function, iff $\bigoplus_{j=1}^m \tau_j f_j(x)$ is an $(n, 1, t)$ function ($n$-variable, $t$-resilient Boolean function) for any choice of $\tau \in \mathbb{F}_2^m$.

Since we are also interested in nonlinearity, we provide the notation $(n, m, t, w)$ for an $(n, m, t)$ resilient function with nonlinearity $w$. 
Works in this area

- Research on multiple output binary resilient functions has received attention from mid eighties.

- The concept of multiple output resilient functions had been introduced independently by Chor et. al. (FOCS 1985) and Bennett et. al. (SIAM Journal on Computing 1988).

- A similar concept was introduced at the same time for single output Boolean functions by Siegenthaler (IEEE-IT 1984).

- The nonlinearity issue for such multiple output resilient functions was discussed by Stinson and Massey (Journal of Cryptology 1995) It has been shown that it is possible to construct infinite classes of nonlinear resilient functions from Kerdock and Preparata codes.

Works in this area (Contd.)

- Gopalakrishnan and Stinson (DCC 1995) introduced three characterizations of non-binary correlation immune and resilient functions. They have considered \( t \)-th order correlation immune and resilient functions over \( F_q \). The characterizations were in terms of (i) structure of a certain associated matrix, (ii) Fourier transform and (iii) large sets of orthogonal arrays.

- Camion and Canteaut (DCC 1999) extended the results where they considered the functions over any finite alphabet \( \mathcal{A} \) endowed by the structure of an abelian group, i.e., a mapping \( F : \mathcal{A}^n \rightarrow \mathcal{A}^m \).

- Carlet (Crypto 1997) showed that applying a suitable modification to bent functions enables to construct correlation immune and resilient functions over Galois fields, in some cases over Galois rings.
A Result

Let $G$ be a generator matrix for an $(n, m, t + 1)$ linear code. Then the function $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$, given by $F(x) = xG^T$, is an $n$-input, $m$-output, $t$-resilient function.

This result was given by Bennett et. al. (SIAM Journal on Computing 1988); also been studied by Stinson (Congressus Numerantium 1993) using the orthogonal array characterization.
A Result by Johansson-Pasalic (ISIT 2000)

Let $c_0, \ldots, c_{m-1}$ be a basis of a binary $[u, m, t + 1]$ linear code $C$. Let $\beta$ be a primitive element in $\mathbb{F}_{2^m}$ and $(1, \beta, \ldots, \beta^{m-1})$ be a polynomial basis of $\mathbb{F}_{2^m}$. Define a bijection $\phi : \mathbb{F}_{2^m} \mapsto C$ by $\phi(a_0 + a_1\beta + \cdots a_{m-1}\beta^{m-1}) = a_0c_0 + a_1c_1 + \cdots a_{m-1}c_{m-1}$. Consider the matrix

$$A^* = \begin{pmatrix}
\phi(1) & \phi(\beta) & \cdots & \phi(\beta^{m-1}) \\
\phi(\beta) & \phi(\beta^2) & \cdots & \phi(\beta^m) \\
\vdots & \vdots & \ddots & \vdots \\
\phi(\beta^{2^{m-2}}) & \phi(1) & \cdots & \phi(\beta^{2^{m-2}})
\end{pmatrix}.$$ 

For any linear combination of columns (not all zero) of the matrix $A^*$, each nonzero codeword of $C$ will appear exactly once.

- There are $2^m - 1$ rows in the matrix $A^*$.
- For convenience, we use a standard index notation to identify the elements of $A^*$. That is, $a_{i,j}$ denotes the element in $i$-th row and $j$-th column of $A^*$, for $i = 0, \ldots, 2^m - 2$, and $j = 0, \ldots, m - 1$. 
Result by Johansson-Pasalic (Contd.)

• Since each entry $a_{i,j}$ of $A^*$ is a nonzero codeword of a linear $[u, m, t + 1]$ linear code $C$, the corresponding linear function $a_{i,j}(x) = x \cdot a_{i,j}$ on $L_u$ will be nondegenerate on at least $t + 1$ variables. This linear function is $t$-resilient.

• Any column of the matrix $A^*$ can be seen as a column vector of $2^m - 1$ distinct $t$-resilient linear functions on $u$ variables.

• Thus to get $n$-variable function we need $\left\lceil \frac{2^n - u}{2^m - 1} \right\rceil$ many such matrices one below the other. To get high nonlinearity, one needs nonintersecting codes.

• The nonlinearity will be $2^n - 1 - 2^u - 1$.

• A set of linear $[u, m, t + 1]$ codes $\mathcal{C} = \{C_1, C_2, \ldots, C_s\}$ such that $C_i \cap C_j = \{0\}, 1 \leq i < j \leq s$, is called a set of linear $[u, m, t + 1]$ nonintersecting codes.
Further ideas by Pasalic and Maitra (SAC 2001)

- Computer search is used to get the set $\mathcal{C}$ and good results could be obtained for small size of $n$.
- May not be efficient for larger $n$ as the search becomes complicated.
- Good theoretical approach to find a set of nonintersecting codes will be interesting in this area.
- The new idea uses a single code to construct the resilient functions, instead of searching for nonintersecting codes.
- We remove some rows of $A^*$ towards this new construction.
Result by Pasalic-Maitra (Contd.)

- Let us only concentrate on the first $2^q$ rows of $A^*$ for $0 \leq q \leq m - 1$.
- We introduce the matrix $D$ with entries $d_{i,j} = a_{i,j}$, $i = 0, \ldots, 2^q - 1$, and $j = 0, \ldots, m - 1$. Note that the entries of $D$ are elements from $\mathbb{F}_2^u$ given by $d_{i,j} = \phi(\beta^{i+j})$.
- For any linear combination of columns (not all zero) of the matrix $D$, each nonzero codeword of $C$ will either appear exactly once or not appear at all.
- Let the set $\{g_1, \ldots, g_m\}$ of Boolean functions on $u + q$ variables be defined as,
  
  $$g_{j+1}(y, x) = \bigoplus_{\tau \in \mathbb{F}_2^u} (y_1 \oplus \tau_1) \cdots (y_q \oplus \tau_q)(d_{[\tau],j} \cdot x),$$

  where $[\tau]$ denotes the integer representation of vector $\tau$, and $j = 0, \ldots, m - 1$. That is, to the $j$-th column of $D$ we associate the function $g_{j+1}$.
- Any nonzero linear combination of the functions $g_1, \ldots, g_m$ is a $t$-resilient function with nonlinearity $2^{u+q-1} - 2^{u-1}$. 

Indian Statistical Institute
Result by Pasalic-Maitra (Contd.)

- Given a \([u, m, t + 1]\) linear code, it is possible to construct \((u + q, m, t, 2^{u+q-1} - 2^{u-1})\) resilient functions, for \(0 \leq q \leq m - 1\).

- There exists an \([m + 1, m, 2]\) linear code. Thus, it is possible to construct an \((n = 2m, m, 1, nl(F) = 2^{n-1} - 2^{\frac{n}{2}})\) function \(F(x)\). Putting \(u = m + 1\) and \(q = m - 1\), we get \((n, m, 1, 2^{n-1} - 2^{m})\) resilient functions.

- With \(m = 16\), one can construct 1-resilient function \(F(x) : \mathbf{F}_2^{32} \mapsto \mathbf{F}_2^{16}\) with \(nl(F) = 2^{n-1} - 2^{\frac{n}{2}} = 2^{31} - 2^{16}\). This function can be used in a stream cipher system where at each clock it is possible to get 2-byte output.

- Each column of \(D\) can be seen as a \((u + q)\)-variable function with order of resiliency \(t\) and nonlinearity \(2^{u+q-1} - 2^{u-1}\). These functions are referred as \(g_1, \ldots g_m\).

- Any nonzero linear combination of these functions will provide \((u + q)\)-variable function \(g\) with order of resiliency \(t\) and nonlinearity \(2^{u+q-1} - 2^{u-1}\).
Composing with Highly Nonlinear Functions

• The \((u + q)\)-variable function need to be repeated \(2^{n-u-q}\) times to make an \(n\)-variable function. We will thus use an \((n - u - q)\)-variable function and XOR it with the \((u + q)\)-variable function to get an \(n\)-variable function.

• To get the maximum possible nonlinearity in this method, the \((n - u - q)\)-variable function must be of maximum possible nonlinearity.

• We will use \(m\) different functions \(h_1, \ldots, h_m\) and use the compositions 
  \[ f_1 = h_1 \oplus g_1, \ldots, f_m = h_m \oplus g_m, \]
  to get \(m\) different \(n\)-variable functions.

• Any nonzero linear combination of \(f_1, \ldots, f_m\) can be seen as the XOR of linear combinations of \(h_1, \ldots, h_m\) and linear combinations of \(g_1, \ldots, g_m\).

• In order to get a high nonlinearity of the vector output function we will need high nonlinearity of the functions \(h_1, \ldots, h_m\) and also high nonlinearity for their linear combinations.
Nonlinearity of Direct Sum

• Let \( h(y) \in V_k \) and \( g(x) \in V_{n_1} \). Then the nonlinearity of \( f(y, x) = h(y) \oplus g(x) \) is given by,
\[
\text{nl}(f) = 2^k \text{nl}(g) + 2^{n_1} \text{nl}(h) - 2^{\text{nl}(g) \text{nl}(h)}.
\]

• Let \( h(y) \) be a bent function on \( V_k, k = 2m \). Let \( g(x) \in V_{n_1} \) with \( \text{nl}(g) = 2^{n_1-1} - 2^u - 1 \), for \( u \leq n_1 \). Then the nonlinearity of \( f(y, x) = h(y) \oplus g(x) \) is given by,
\[
\text{nl}(f) = 2^{n_1+k-1} - 2^{k}2^u - 1.
\]

• Let \( h'(y') \) be a bent functions on \( V_k, k = 2r \), and let \( h(y) \) be a function on \( V_{k+1} \) given by \( h(y) = x_{k+1} \oplus h'(y') \). Let \( g(x) \in V_{n_1} \) with \( \text{nl}(g) = 2^{n_1-1} - 2^u - 1 \), for \( u \leq n_1 \). Then the nonlinearity of \( f(y, x) = h(y) \oplus g(x) \) is given by,
\[
\text{nl}(f) = 2^{n_1+k-1} - 2^{k+1}2^u - 1.
\]
How to get $h_1, \ldots, h_m$

- If $(n - u - q)$ is even, we can use bent functions $h_1, \ldots, h_m$. We require $m$ different bent functions such that the nonzero linear combinations will also produce bent functions. For this we need $n - u - q \geq 2m$.

- If $(n - u - q)$ is odd, we can use bent functions $b_j$ of $(n - u - q - 1)$ variables and take $h_j = x_n \oplus b_j$. This requires the condition $n - u - q - 1 \geq 2m$ to get $m$ distinct bent functions.

- It may very well happen that the value of $n - u - q$ may be less than $2m$ and in such a scenario it is not possible to get $2m$ bent functions with the desired property.

- It is possible to obtain $m$ distinct bent functions on $2p$ variables ($p \geq m$), say $b_1, \ldots, b_m$, such that any nonzero linear combination of these bent functions will provide a bent function. Also, $\deg(\oplus_{i=1}^{m} \tau_i b_i) = p$, for $\tau \in \mathbb{F}_2^m$. 
An example

Let $m = 2$ and $c_0 = (01)$, $c_1 = (10)$. We use an irreducible polynomial $p(z) = z^2 + z + 1$ to create the field $\mathbb{F}_{2^2}$. Then it can be shown that the matrix $A$ is given by,

$$
A = \begin{pmatrix}
0 & 0 \\
c_0 & c_1 \\
c_1 & c_0 + c_1 \\
c_0 + c_1 & c_0
\end{pmatrix}.
$$

In the truth table notation, let us consider the 4-variable bent function $h_1(x)$ as the concatenation of the 2-variable linear functions $0, x_1, x_2, x_1 \oplus x_2$ and similarly, $h_2(x)$ as concatenation of $0, x_2, x_1 \oplus x_2, x_1$. Then the function $h_1(x) \oplus h_2(x)$ is also bent, which is a concatenation of $0, x_1 \oplus x_2, x_1, x_2$.

Notations: We denote $\pi = n - u - m + 1$. Also we consider the availability of $(n - u - m + 1)$-variable functions $h_1, \ldots, h_m$ such that any linear combination of them will provide a nonlinearity at least $\nu(n - u - m + 1, m)$. 
Summarized Results

**Theorem 1** Given a linear \([u, m, t + 1]\) code, it is possible to construct \((n, m, t, nl(F))\) function \(F = (f_1, \ldots, f_m)\), where \(nl(F) =\)

\[
\begin{cases}
2^{n-1} - 2^{u-1}, \\
u \leq n < u + m, \\
2^{n-1} - 2^{n-m}, \\
u + m \leq n < u + m + 2, \\
2^{n-1} - 2^{n-m} + 2^u \nu(n - u - m + 1, m), \\
u + m + 2 \leq n < u + 2m - 1, \\
2^{n-1} - 2^{\frac{n+u-m+1}{2}}, \\
u + 2m - 1 \leq n < u + 3m - 3, \pi \text{ even}, \\
2^{n-1} - 2^{\frac{n+u-m+2}{2}}, \\
u + 2m \leq n < u + 3m - 3, \pi \text{ odd}, \\
2^{n-1} - 2^{u+m-1}, \\
u + 3m - 3 \leq n < u + 3m, \\
2^{n-1} - 2^{\frac{n+u-m-1}{2}}, \\
\pi \text{ even}, \\
n \geq u + 3m - 1, \\
2^{n-1} - 2^{\frac{n+u-m}{2}}, \\
n \geq u + 3m, \pi \text{ odd}.
\end{cases}
\]
Results

A: Pasalic-Maitra, B: Johansson-Pasalic.

Table 1: Results for 1-resilient functions.

<table>
<thead>
<tr>
<th>m</th>
<th>n = 9</th>
<th>n = 10</th>
<th>n = 11</th>
<th>n = 12</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>B</td>
<td>A</td>
<td>B</td>
<td>A</td>
</tr>
<tr>
<td>2</td>
<td>224</td>
<td>240*</td>
<td>480</td>
<td>480</td>
</tr>
<tr>
<td>3</td>
<td>224</td>
<td>224</td>
<td>480</td>
<td>480</td>
</tr>
<tr>
<td>4</td>
<td>224</td>
<td>224</td>
<td>480#</td>
<td>448</td>
</tr>
<tr>
<td>5</td>
<td>224</td>
<td>224</td>
<td>480#</td>
<td>448</td>
</tr>
<tr>
<td>6</td>
<td>192</td>
<td>192</td>
<td>448</td>
<td>448</td>
</tr>
</tbody>
</table>

Table 2: Results for 2-resilient functions.

<table>
<thead>
<tr>
<th>m</th>
<th>n = 9</th>
<th>n = 10</th>
<th>n = 11</th>
<th>n = 12</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>B</td>
<td>A</td>
<td>B</td>
<td>A</td>
</tr>
<tr>
<td>2</td>
<td>192</td>
<td>240*</td>
<td>448</td>
<td>480*</td>
</tr>
<tr>
<td>3</td>
<td>192</td>
<td>192</td>
<td>448</td>
<td>448</td>
</tr>
<tr>
<td>4</td>
<td>192#</td>
<td>128</td>
<td>448#</td>
<td>384</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>256</td>
<td>256</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 3: Results for 3-resilient functions.

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>A</th>
<th>B</th>
<th>A</th>
<th>B</th>
<th>A</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>192</td>
<td>192</td>
<td>384</td>
<td>448*</td>
<td>896</td>
<td>960*</td>
<td>1792</td>
</tr>
<tr>
<td>3</td>
<td>192</td>
<td>192</td>
<td>384</td>
<td>384</td>
<td>896</td>
<td>896</td>
<td>1792</td>
</tr>
<tr>
<td>4</td>
<td>128</td>
<td>128</td>
<td>384#</td>
<td>256</td>
<td>896#</td>
<td>768</td>
<td>1792</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>256</td>
<td>256</td>
<td>512</td>
<td>512</td>
<td>1536</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>512*</td>
<td>1024</td>
</tr>
</tbody>
</table>
## Results

Table 4: Nonlinearity of $(36, 8, t)$ resilient functions.

<table>
<thead>
<tr>
<th>(A) Order of resiliency $t$</th>
<th>7</th>
<th>6</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>(B) NL (Kurosawa et. al.)</td>
<td>$2^{35} - 2^{27}$</td>
<td>$-$</td>
<td>$2^{35} - 2^{26}$</td>
</tr>
<tr>
<td>(C) NL-B</td>
<td>$2^{35} - 2^{22}$</td>
<td>$-$</td>
<td>$2^{35} - 2^{23}$</td>
</tr>
<tr>
<td>(D) NL-A</td>
<td>$2^{35} - 2^{25}$</td>
<td>$2^{35} - 2^{24}$</td>
<td>$2^{35} - 2^{23}$</td>
</tr>
<tr>
<td>(E) The codes</td>
<td>[20, 8, 8]</td>
<td>[19, 8, 7]</td>
<td>[17, 8, 6]</td>
</tr>
<tr>
<td>(F) NL-C</td>
<td>$2^{35} - 2^{24}$</td>
<td>$2^{35} - 2^{24}$</td>
<td>$2^{35} - 2^{23}$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(A)</th>
<th>4</th>
<th>3</th>
<th>2</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>(B)</td>
<td>$2^{35} - 2^{25}$</td>
<td>$2^{35} - 2^{24}$</td>
<td>$2^{35} - 2^{25}$</td>
<td>$2^{35} - 2^{24}$</td>
</tr>
<tr>
<td>(C)</td>
<td>$2^{35} - 2^{22}$</td>
<td>$2^{35} - 2^{22}$</td>
<td>$2^{35} - 2^{21}$</td>
<td>$2^{35} - 2^{21}$</td>
</tr>
<tr>
<td>(D)</td>
<td>$2^{35} - 2^{23}$</td>
<td>$2^{35} - 2^{20}$</td>
<td>$2^{35} - 2^{19}$</td>
<td>$2^{35} - 2^{18}$</td>
</tr>
<tr>
<td>(E)</td>
<td>[16, 8, 5]</td>
<td>[13, 8, 4]</td>
<td>[12, 8, 3]</td>
<td>[9, 8, 2]</td>
</tr>
<tr>
<td>(F)</td>
<td>$2^{35} - 2^{24}$</td>
<td>$2^{35} - 2^{20}$</td>
<td>$2^{35} - 2^{19}$</td>
<td>$2^{35} - 2^{18}$</td>
</tr>
</tbody>
</table>

The work of Gupta-Sarkar gives better results for $n \geq 13$ in some (not all) cases.

NL-A: Pasalic-Maitra, NL-B: Johansson-Pasalic, NL-C: Gupta-Sarkar.
Concluding Remarks

- We have presented an outline of three related works where linear codes are used to construct resilient functions.


- We believe there is further scope of improvement in this area given the new results related to single output Boolean functions that appeared after these works.

- Fast Software or Efficient Hardware Implementation of these functions may also be an interesting area of study.

Thank you