Semi-bent Boolean Functions Arising from CA

Luca Mariot, Martina Saletta, Alberto Leporati, Luca Manzoni

L.Mariot@tudelft.nl

ACRI 2020 – December 2-4, 2020
Boolean functions $f : \{0, 1\}^n \rightarrow \{0, 1\}$ are used in:

- **Stream ciphers**, to design the *keystream generator* (KSG)
- **Block ciphers**, as the coordinate functions of *S-boxes* ($S_i$)
**Boolean Functions - Basic Representations**

- **Truth table**: a $2^n$-bit vector $\Omega_f$ specifying $f(x)$ for all $x \in \{0, 1\}^n$

<table>
<thead>
<tr>
<th>$(x_1, x_2, x_3)$</th>
<th>000</th>
<th>100</th>
<th>010</th>
<th>110</th>
<th>001</th>
<th>101</th>
<th>011</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\Omega_f$</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

- **Algebraic Normal Form (ANF)**: Sum (XOR) of products (AND)

$$f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3 \oplus x_2 x_3$$

- **Walsh Transform**: correlation with linear functions $a \cdot x$,

$$W(f, a) = \sum_{x \in \{0, 1\}^n} (-1)^{f(x) \oplus a \cdot x} \text{ for all } a \in \{0, 1\}^n$$

![Graph showing Walsh Transform values for different inputs]
Boolean functions with as "flat" as possible Walsh spectrum:

- **Bent functions:** $W(f, a) = \pm 2^{\frac{n}{2}}$ for all $a \in \{0, 1\}^n$
  - Reach the highest possible nonlinearity
  - Exist only for $n$ even and they are *unbalanced*

- **Semi-bent functions:**
  - Can be balanced, and exist for every $n$
  - Good trade-off of nonlinearity and other properties

- **Plateaued functions:** $W(f, a) \in \{-2^r, 0, 2^r\}$
Constructions of good Boolean Functions

- Number of Boolean functions of $n$ variables: $2^{2n}$
- ⇒ too huge for exhaustive search when $n > 5$

In practice, one can resort to *algebraic constructions*

- *Primary constructions*: (semi-)bent functions are built from scratch (e.g., Maiorana-McFarland construction [M73])
- *Secondary constructions*: new (semi-)bent functions are obtained from existing ones (e.g., Rothaus’s construction [R76])

⇓

**Focus of our work**: Secondary constructions of semi-bent functions based on **Cellular Automata**
Cellular Automata (CA)

- Each cell updates its state \( s \in \{0, 1\} \) by applying a local rule \( f : \{0, 1\}^m \rightarrow \{0, 1\} \) to itself and the \( m-1 \) cells to its right.

Example: \( n = 6, m = 3, f(s_i, s_{i+1}, s_{i+2}) = s_i \oplus s_{i+1} \oplus s_{i+2} \)

\[
\begin{array}{cccccc}
1 & 0 & 0 & 0 & 0 & 1 \\
\end{array}
\]

\( f(1, 0, 0) = 1 \)

\[
\begin{array}{ccc}
1 & 0 & 0 \\
\end{array}
\]

No Boundary CA – NBCA

\[
\begin{array}{cccccc}
1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
\end{array}
\]

\( f(1, 1, 0) = 0 \)

\[
\begin{array}{ccc}
1 & 0 & 0 \\
\end{array}
\]

Periodic Boundary CA – PBCA

- Uses of PBCA: S-boxes [SS08, MPLJ19], PRNG [W86, LM14]
- Uses of NBCA: Secret Sharing Schemes [MGLF20]
**Idea:** Define a function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ by XORing all $n - m + 1$ output cells of a NBCA.

Recursive construction parameterized on $n$, with $n = m$ being the base case (= local rule).
Preservation of Algebraic Degree

Definition

Given a CA of length \( n \geq m \) with the local rule \( f : \{0, 1\}^m \rightarrow \{0, 1\} \), define \( f^* : \{0, 1\}^n \rightarrow \{0, 1\} \) for all \( x \in \{0, 1\}^n \) as:

\[
f^*(x) = \bigoplus_{i=1}^{n-m+1} f(x_i, \cdots, x_{i+m-1}) = f(x_1, \cdots, x_m) \oplus \cdots \oplus f(x_{n-m+1}, \cdots, x_n)
\]

Algebraic degree: degree of the ANF of \( f \)

\[
f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3 \oplus x_2 x_3 \Rightarrow \text{degree 2}
\]

Lemma

Let \( f : \mathbb{F}_2^m \rightarrow \mathbb{F}_2 \) be a Boolean function of \( m \) variables. For any \( n \geq m \), the function \( f^* \) has the same algebraic degree of \( f \).
Goal: characterize semi-bent rules $f$ of $m$ variables generating semi-bent functions $f^*$ for all $n \in \mathbb{N}$ under our construction

Empirical search of such rules based on these ideas:

- For each considered rule, check semi-bentness of $f^*$ only up to a certain $n$ (in our case, $n = 20$)
- To reduce the search space, check only quadratic functions (degree 2), since they are all plateaued [C10]
- \( \Rightarrow \) Combinatorial algorithm to exhaustively search the space of quadratic ANF
Search Algorithm

\textbf{SEARCH-ANF}(m, n, d)

\textbf{Init:} For \(1 \leq k \leq d\), build the family \(I_k\) of monomials of degree \(k\), set all \(2^m\) ANF coefficients of \(f\) to 0 and initialize \(L\) as the empty list.

\textbf{Loop:} For all subsets \(T \subseteq I_d\) do:

\textbf{Init:} Reset all \(d\)-degree terms in the ANF to 0

\textbf{Inst:} For all \(T \in T\), set the ANF coefficient \(a_T\) to 1

\textbf{Loop:} For all subsets \(P \subseteq \bigcup_{k=1}^{d-1} I_k\) do:

1. Reset all terms of degree less than \(d\) to 0
2. For all \(P \in P\), set \(a_P\) to 1
3. Recover the truth table of \(f\) from the ANF
4. If \(f\) is semi-bent, then for \(m < i \leq n\) apply the CA construction with \(i\) cells
5. If \(f^*\) is semi-bent for all \(m < i \leq n\), add \(f\) to \(L\)

\textbf{Output:} return \(L\)
We exhaustively enumerated the space of quadratic local rules of $3 \leq m \leq 6$ variables.

For each $m$, we further filtered those semi-bent rules that always generate balanced functions.

<table>
<thead>
<tr>
<th>$m$</th>
<th>$2^{2m}$</th>
<th>$S_{m,2}$</th>
<th>QSB</th>
<th>Bal</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>256</td>
<td>56</td>
<td>24</td>
<td>8</td>
</tr>
<tr>
<td>4</td>
<td>65536</td>
<td>1008</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>$\approx 4.3 \cdot 10^9$</td>
<td>32736</td>
<td>2208</td>
<td>280</td>
</tr>
<tr>
<td>6</td>
<td>$\approx 1.84 \cdot 10^{19}$</td>
<td>$2.1 \cdot 10^6$</td>
<td>12208</td>
<td>1937</td>
</tr>
</tbody>
</table>
Conclusions and Open Problems

Remarkable findings:

▶ For $m = 4$, our construction always fails. No semi-bent rule generates semi-bent functions of up to 20 variables
▶ All filtered balanced rules generate semi-bent functions with the same number of linear structures
▶ For $m = 3$ rule 30 and rule 210 occurred in the filtered set

Open problems:

▶ Investigate if our construction fails for other values of $m$
▶ Theoretical characterization of the rules in the filtered set
▶ Analyze the periods of spatially periodic preimages in quadratic CA [MLDF17]


