On the variations of Maiorana-McFarland and (partial) spread class of Boolean functions

Razi Arshad and Alexander Pott

Otto von Guericke University, Magdeburg, Germany
razi.arshad@st.ovgu.de, alexander.pott@ovgu.de

A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is almost perfect nonlinear (APN), if $F(x+a)+F(x)=b$ has at most two solutions for all $a, b \in \mathbb{F}_2^n$, $a \neq 0$. APN functions have special importance in cryptography and related areas. For example, they can be used as S-boxes which guarantee a high resistance to differential cryptanalysis. The APN property of F is closely related to 2-dimensional affine subspaces of $\mathbb{F}_2^n$. APN functions (wipe out) all 2-dimensional affine subspaces of $\mathbb{F}_2^n$, that is, $F(a)+F(x+a)+F(y+a)+F(x+y+a) \neq 0$ for all distinct $a,\ x,\ y$. One can construct APN functions using n coordinate functions. First, we need to find a Boolean function $f_1(x)$ and determine the 2-dimensional affine subspaces of $\mathbb{F}_2^n$ which are not wiped out by $f_1(x)$, that is, $f_1(x)+f_1(x+a)+f_1(y)+f_1(y+a)=0$. Then, we try to find a Boolean function $f_2(x)$ that wipes out many of the 2-dimensional affine subspaces of $\mathbb{F}_2^n$ which are not wiped out by the Boolean function $f_1(x)$. We can continue in the same way and finally we try to find a Boolean function $f_n(x)$ that wipes out all the 2-dimensional affine subspaces of $\mathbb{F}_2^n$ which are not wiped out by the Boolean functions $f_1(x), \ldots, f_{n-1}(x)$. Many known APN functions consist of bent and plateaued coordinate functions. We observe that bent functions wipe out maximum number of 2-dimensional affine subspaces of $\mathbb{F}_2^n$. Bent functions are the best candidate of coordinate functions to construct APN functions. It has been proposed to search for more (non-quadratic) plateaued functions and somehow replace the quadratic plateaued function by non-quadratic plateaued function. In our approach, we want to replace the plateaued functions by non-quadratic functions which are actually better than plateaued functions with respect to "wiping out" 2-dimensional affine subspaces of $\mathbb{F}_2^n$. We know that bent functions can be constructed by using Maiorana-McFarland and partial spread construction method. It is a promising idea to look for Boolean functions which belong to Maiorana-McFarland and (partial) spread class and which wipe out large number of 2-dimensional affine subspaces of $\mathbb{F}_2^n$.

In this paper, we investigate variations of the Maiorana-McFarland and (partial) spread class of Boolean functions. First, we consider the case of (partial) spread Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, where $n=2m$. A spread of order k in $\mathbb{F}_2^n$ is a set of m-dimensional subspaces $H_1, \ldots, H_k$ of $\mathbb{F}_2^n$ such that $H_i \cap H_j = \{0\}$ for all $i \neq j$. We have two possible cases of m-dimensional subspaces $H_1, \ldots, H_k$ of $\mathbb{F}_2^n$. In the first case, we consider m-dimensional subspaces $H_1, \ldots, H_k$ of $\mathbb{F}_2^n$ without 0. The Boolean function f_k from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is the indicator function of $D = \cup_{i=1}^k H_i \setminus \{0\}$.

Theorem 1. *Assume that $f_k : \mathbb{F}_2^n \to \mathbb{F}_2$ is a Boolean function. The function f_k wipes out* $\frac{1}{24}\left(\frac{1}{2^{n+1}}[16((2^{n-1}-2^m k+k-1)^4+(2^n k^4-2^m k^5+k^5-k^4)+k(k-2^m)^4(2^m-1))]-3(2^{2n})+2^{n+1}\right)$ *number of 2-dimensional affine subspaces of $\mathbb{F}_2^n$.*

Note that for $k=2^{m-1}$, we have a bent function. We observe that for $k=2^{m-1}+1$ and $k=2^{m-1}-1$, the Boolean function f_k wipe out more 2-dimensional affine subspaces of $\mathbb{F}_2^n$ as compared with plateaued functions. The Boolean function f_k is a good candidate for coordinate function which can be used in the construction of APN functions. In the second case, we include 0 in the m-dimensional subspaces $H_1, \ldots, H_k$ of $\mathbb{F}_2^n$ and we have an analogue of Theorem 1. We can prove similar results for the Maiorana-McFarland class of Boolean functions.