PERMUTATION ROTATION-SYMMETRIC SBOXES, LIFTINGS AND AFFINE EQUIVALENCE

TRON OMLAND AND PANTELIMON STĂNICĂ

Abstract. In this paper, we investigate permutation rotation-symmetric (shift-invariant) vectorial Boolean functions on n bits that are liftings from Boolean functions on k bits, for $k \leq n$. These functions generalize the well-known map used in the current Keccak hash function, which is generated via the Boolean function $x_1 + x_1x_2 + x_3$.

We provide some general constructions, and also study the affine equivalence between rotation-symmetric Sboxes and describe the corresponding relationship between the Boolean function they are associated with. In the process, we point out some inaccuracies in the existing literature.

1. Introduction and motivation

One of the most basic primitives in symmetric cryptography is an Sbox, or a "substitution box", which, mathematically, is a map from the set of n-bit vectors to the set of m-bit vectors. Symmetric ciphers are often made up as a combination of Sboxes and only a few other operations that are usually linear. For example, the substitution-permutation networks are all of this type, including the current block cipher standard, AES. Therefore, as the main nonlinear part, Sboxes play a central role in providing the confusion to the robustness of ciphers, and therefore, the security of a cipher often relies heavily on the cryptographic properties of the Sbox involved.

Since lookup tables tend to have a large implementation cost, using an Sbox with an easy description is favorable. Let $\mathbb{F}_2^n$ denote the vector space of n-bits, let $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an Sbox and S be the (right) shift, that is, $S(x_1, x_2, \ldots, x_n) = (x_n, x_1 \ldots, x_{n-1})$. Then F is rotation-symmetric (or shift-invariant) if $F \circ S = S \circ F$, and such functions can be completely determined by a Boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$. Therefore, permutation rotation-symmetric Sboxes with good cryptographic properties are good candidates to be used as a primitives in symmetric ciphers. In particular, they are interesting for designing lightweight cryptography.

A Boolean function f on k bits determines a rotation-symmetric Sbox F on n bits, for $k \leq n$, by

$$F(x_1, x_2, \ldots, x_n) = \big(f(x_1, x_2, \ldots, x_k), f(x_2, x_3, \ldots, x_{k+1}), \ldots, f(x_n, x_1, x_2, \ldots, x_{k-1})\big),$$

and when F is a bijection we call such Sbox a (k, n)-*lifting*. The case where $k < n$ is especially interesting and the motivating example is the function $\chi(x_1, x_2, x_3) = x_1 + x_1x_2 + x_3$ (studied in Daemen's thesis [4]), which gives rise to $(3, n)$-liftings for

Date: March 1, 2022.

Key words and phrases. Boolean functions, vectorial Boolean, Sboxes, permutation, circulant matrices.

all odd $n \geq 3$. It has good cryptographic properties and is used in the current hash function Keccak.

Bijective rotation-symmetric Sboxes and liftings can also be viewed as reversible cellular automata, which are certain dynamical systems on the space of bi-infinite strings of 0's and 1's, thought of as cells. They are defined by local updates rules, depending on neighboring cells and uniformly applied to all cells at the same time. Reversible cellular automata have many applications in physics and biology, typically for simulation of microsystems.

Even though rotation-symmetric Sboxes (or cellular automata) are characterized by simple rules, designing them so that they are permutation is a difficult problem. There are only a few known classes and a limited number of available theoretical results. On the other hand, previous works (and existing computational data) shows that this is still a very rich class.

In this paper, we discuss various questions and techniques related to producing new classes of (k, n)-liftings, and methods to determine whether a candidate is in fact a lifting. We believe that finding the number of (k, n)-liftings is in general hard when $k < n$, but we explain how it can be computed for $k = n$. However, when k is small, computer experiments provide a bit of information. In Section 7 we present two families of Sboxes, one that consists of $(k, k+2)$-liftings for all odd k, and one that consists of (k, n)-liftings for all $4 \leq k \leq n$. The latter has a description by certain conserved landscapes. We also present a few theoretical results and bounds. Analysis of liftings that give rise to Sboxes with good cryptographic properties and cost-efficient implementation is a trade-off among the sizes of k and n, the number of nonzero terms, algebraic degree, and nonlinearity and differential uniformity.

Finally, let F and G be two bijective rotation-symmetric Sboxes determined by Boolean functions f and g, respectively. In Section 8, we investigate conditions for when F and G are affine equivalent, and in particular, what relationship this corresponds to between f and g. Some of our observations and results illustrate that the topic is more subtle than previous papers suggest. Most of this analysis is conducted in a slightly more general setting than rotation-symmetry, for so-called cyclic Sboxes, and in particular for k-shift-invariant permutations (both notions are explained below).

2. Background on Boolean functions

For a positive integer n, we let $\mathbb{F}_{2^n}$ denote the finite field with 2^n elements, and $\mathbb{F}_{2^n}^* = \mathbb{F}_{2^n} \setminus \{0\}$ (for $a \neq 0$, we write $\frac{1}{a}$ to mean the inverse of a in the considered finite field). Further, let $\mathbb{F}_2^m$ denote the m-dimensional vector space over $\mathbb{F}_2$. We call a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ a *Boolean function* on n variables. The cardinality of a set S is denoted by $\#S$. For $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ we define the *Walsh-Hadamard transform* to be the integer-valued function $W_f(u) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) - \mathrm{Tr}_n(ux)}$, $u \in \mathbb{F}_{2^n}$, where $\mathrm{Tr}_n : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is the absolute trace function, given by $\mathrm{Tr}_n(x) = \sum_{i=0}^{n-1} x^{2^i}$. If f is defined over the vector space $\mathbb{F}_2^n$, we then replace the trace by the scalar product $u \cdot x$ of $u, x \in \mathbb{F}_2^n$.

Given a Boolean function f, the derivative of f with respect to $a \in \mathbb{F}_{2^n}$ is the Boolean function $D_a f(x) = f(x + a) - f(x)$, for all $x \in \mathbb{F}_{2^n}$.

For positive integers n and m, any map $F:\mathbb{F}_2^n \to \mathbb{F}_2^m$ is called a *vectorial Boolean function*, or (n,m)*-function*. When $m=n$, F can be uniquely represented as a univariate polynomial over $\mathbb{F}_{2^n}$ (using the natural identification of the finite field with the vector space) of the form $F(x)=\sum_{i=0}^{2^n-1} a_i x^i,\ a_i\in\mathbb{F}_{2^n}$. The algebraic degree of F is then the largest weight (in the binary expansion) of the exponents i with $a_i\neq 0$. For an (n,m)-function F and $a\in\mathbb{F}_{2^n}, b\in\mathbb{F}_{2^m}$, we define the Walsh transform $W_F(a,b)$ to be the Walsh-Hadamard transform of its component function $\mathrm{Tr}_m(bF(x))$ at a, that is,

$$W_F(a,b)=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_m(bF(x))-\mathrm{Tr}_n(ax)},$$

with the same caveat that the traces are to be replaced by the regular scalar product when working over the corresponding vector spaces.

Given a vectors $x=(x_1,\ldots,x_n)\in\mathbb{F}_2^n$, its Hamming weight is $wt(x):=\sum_{i=1}^n x_i$, and for two vectors x,y, then *Hamming distance* is $d(x,y)=wt(x+y)$. For functions f,g, we let the Hamming weights/distance be the Hamming weights/distance of their truth (output) table. We define the *nonlinearity* for a Boolean functions to be $N_f=\min\{d(f,\ell):\ell \text{ affine function}\}$, which is known to be equal to $2^{n-1}-\dfrac{1}{2}\max_x|W_f(x)|$, and upper bounded by $N_f\leq 2^{n-1}-2^{n/2-1}$, attained for n even (by *bent* functions). We further define the nonlinearity of a vectorial Boolean (n,m)-function F to be the smallest nonlinearity among its component functions $b\cdot F$, for $b\in\mathbb{F}_2^m$. The largest nonlinearity of a Boolean function in odd dimension is n is odd is $\geq 2^{k-1}-2^{\frac{k-1}{2}}$ (this is known as the bent concatenation bound).

Given an (n,n)-function F, and $a,b\in\mathbb{F}_{2^n}$, we let $\Delta_F(a,b)=\#\{x\in\mathbb{F}_{2^n}: F(x+a)-F(x)=b\}$. Then $\Delta_F=\max\{\Delta_F(a,b)\,:\,a,b\in\mathbb{F}_{2^n}, a\neq 0\}$ is the *differential uniformity* of F. If $\Delta_F=\delta$, then we say that F is differentially δ-uniform. Since, for fixed a, any solution x_0 comes along with another, $a+x_0$, then we can have either $0,2$ and above solutions. If $\delta=2$, then F is called an *almost perfect nonlinear* (*APN*) function.

3. Cellular automata

Let $A=\{0,1\}^{\mathbb{Z}}=\{(x_i)_{i\in\mathbb{Z}}:i\in\mathbb{Z}\}$ be a bi-infinite string of 0's and 1's. Define the shift-operator $S\colon A\to A$ by $S(x)_i=x_{i-1}$. For a function $F\colon A\to A$, let $f_i\colon A\to\{0,1\}$ denote its i'th coordinate function, that is, $F(x)_i=f_i(x)$. Let $j,\ell\in\mathbb{Z}$. Then F satisfies the identity $F\circ S^j=S^\ell\circ F$ if and only if

$$f_i\circ S^j=f_{i-\ell},\ \text{for all } i\in\mathbb{Z}.$$

It follows that F is completely determined by $f_1,\ldots,f_\ell$. A function $F\colon A\to A$ is said to be *shift-invariant* if $F\circ S=S\circ F$, and is then determined by a single function $f\colon A\to\{0,1\}$, sometimes called a “local rule”.

In particular, let $k\geq 1$ and let $f\colon\{0,1\}^k\to\{0,1\}$ be any function. Then f induces $F\colon A\to A$ defined by

$$f_i(x)=f\circ S^{1-i-w}(x)=f(x_{i+w},\ldots,x_{i+w+k-1}),\ \text{for all } i\in\mathbb{Z},\ \text{and some } w\in\mathbb{Z}.$$

In this case F is called an infinite cellular automata. If we give A the product topology, then $F\colon A\to A$ is an infinite cellular automata if and only if it is shift-invariant and continuous (see [7, Theorem 3.4]). An infinite cellular automata $F\colon A \to A$ is reversible if it is bijective and F^{-1} is an infinite cellular automata.

For each $n \geq 1$ define $A_n \subseteq A$ to be the subset of n-periodic strings. That is,

$$A_n = \{x \in A : S^n(x) = x\} = \{x \in A : x_i = x_{i+n}, \text{ for all } i \in \mathbb{Z}\}.$$

Then F restricts to a function $A_n \to A_n$ if and only if $f_{i+n}(x) = f_i(x)$ for all $x \in A_n$ and all $i \in \mathbb{Z}$. Suppose that $F \circ S = S^\ell \circ F$ for some $\ell \geq 1$ and that F restricts to A_n for some $n \geq 1$ with $\gcd(\ell, n) = 1$. Then F is completely determined by a single function $f\colon A_n \to \{0,1\}$. Indeed, let m be the inverse of ℓ modulo n and it follows that (see Lemma 8.5 below)

$$f_i(x) = f \circ S^{(1-i)m}(x), \text{ for all } i \in \mathbb{Z}.$$

A function $F\colon A_n \to A_n$ is called a (finite) cellular automata if it is induced from a Boolean function $f\colon \{0,1\}^n \to \{0,1\}$, i.e., with $\operatorname{diam}(f) = n$, by

$$f_i(x) = f \circ S^{1-i}(x) = f(x_i, \ldots, x_{i+n-1}), \text{ for all } i \in \mathbb{Z},$$

and in this case, F is a cellular automata if and only if it is shift-invariant. Moreover, F is a reversible cellular automata if it is bijective on A_n.

Let f be a Boolean function defining F by setting $f_i = f \circ S^{1-i}$. Then (somewhat counter intuitively) f is called locally invertible if F is a reversible infinite cellular automata on A, and globally invertible if there is some $n \geq \operatorname{diam}(f)$ such that F is a reversible cellular automata on A_n. It can be shown that f is locally invertible on A if and only if it is globally invertible on A_n for every $n \geq \operatorname{diam}(f)$ (see [9, Theorem 4]).

3.1. **Rotation-symmetric Sboxes and liftings.** If a function $F\colon A \to A$ restricts to a function $A_n \to A_n$, it is natural to identify A_n with $\mathbb{F}_2^n$ via the map $x \mapsto (x_1, \ldots, x_n)$, and also identify F with a function $\mathbb{F}_2^n \to \mathbb{F}_2^n$.

Henceforth, we let S denote the shift on $\mathbb{F}_2^n$, that is,

$$S(x_1, \ldots, x_n) = (x_n, x_1, \ldots, x_{n-1}).$$

A function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called a rotation-symmetric Sbox if $S \circ F = F \circ S$, i.e., if F is shift-invariant. For every rotation-symmetric Sbox F, it is easily checked that there is a unique Boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ such that (we let $x = (x_1, \ldots, x_n)$)

$$\begin{aligned} F(x) &= \Big(f(x), f \circ S^{-1}(x), f \circ S^{-2}(x), \ldots, f \circ S^{-n+1}(x)\Big) \\ &= \left(f(x_1, x_2 \ldots, x_n), f(x_2, \ldots, x_n, x_1), \ldots, f(x_n, x_1, \ldots, x_{n-1})\right). \end{aligned}$$

Let f be a Boolean function on k variables. Then f induces rotation-symmetric Sboxes $F\colon \mathbb{F}_2^n \to \mathbb{F}_2$ for all $n \geq k$. Our goal is to study situations where F is a permutation .

Definition 3.1. We say that a rotation-symmetric (shift-invariant) F is a (k,n)-lifting for $k \leq n$ if $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is induced from a Boolean function $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ by

$$F(x_1, x_2, \ldots, x_n) = \big(f(x_1, x_2, \ldots, x_k), f(x_2, x_3, \ldots, x_{k+1}), \ldots, f(x_k, x_1, \ldots, x_{k-1})\big).$$

This setup is a special case of the above approach, where we restrict to Boolean functions $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ that only depend on the first k arguments.

For $1 \leq k < n \leq 4$ there are no nonlinear (k, n)-liftings, and in general it seems hard to compute the number of (k, n)-liftings when $k < n$. However, partial nontrivial results can be obtained. For example, there are four nonlinear $(3, 5)$-liftings without a constant term that are all essentially equivalent (see Section 5), and one of them is

$$x_1 + x_1x_2 + x_3,$$

which is used in the current hash function Keccak, see e.g., [14, mid-p. 8] and [6, p. 3]. In fact, we suspect that there are no nonlinear $(3, n)$-liftings when $n > 3$ is even, and for every odd $n > 3$, all the $(3, n)$-liftings are coming from the $(3, 5)$-liftings described above.

All new classes of (k, n)-liftings should be of interest, and we will display our findings below. The task is to find shift-invariant permutations with sufficiently "good" cryptographic properties. Moreover, we would like to determine when such functions give rise to affine equivalent Sboxes. It is also of interest to investigate the cryptographic properties of the Boolean functions that induce such permutations, the nonlinearity, their differential uniformity, etc.

4. Finding all bijections

For an element $x = (x_1, x_2, \dots, x_n) \in \mathbb{F}_2^n$, the cycle $c(x)$ of x is the set

$$\begin{aligned} c(x) &= \{S^i(x) : i = 0, \dots, n-1\} \\ &= \{(x_1, x_2, \dots, x_n), (x_2, \dots, x_n, x_1), \dots, (x_n, x_1, \dots, x_{n-1})\}. \end{aligned}$$

The size of this set is called the length of the cycle. In particular, that there are exactly two elements with a cycle of length 1, namely,

$$0 = (0, 0, \dots, 0) \text{ and } 1 = (1, 1, \dots, 1),$$

and we call these the trivial cycles.

The cycles are the smallest sets X that are shift-invariant, i.e., that satisfy $S(X) = X$.

If F is shift-invariant, then

$$S(F(c(x))) = F(S(c(x))) = F(c(x)),$$

for every cycle $c(x)$, that is, the image of every cycle is contained in a cycle.

Henceforth, we assume that F is shift-invariant and bijective. Since the set $X = F(c(x))$ must have the same size as $c(x)$, and since it satisfies $S(X) = X$, it must be a cycle of the same length as $c(x)$. Let

$$c_\ell = \{X \subseteq \mathbb{F}_2^n : X = c(x) \text{ for some } x \text{ and } |X| = \ell\}.$$

A function F that maps cycles to cycles of the same length induces a function $c_\ell \to c_\ell$ given by $X \mapsto F(X)$. We conclude that:

Proposition 4.1. *A shift-invariant function F is bijective if and only if it maps cycles to cycles and induces bijections on c_ℓ for every ℓ.*

For example, c_1 consists of $0 = (0, 0, \dots, 0)$ and $1 = (1, 1, \dots, 1)$, so a shift-invariant bijection F must either satisfy $F(0) = 0$ and $F(1) = 1$ or vice versa, i.e., $F(0) = 1$ and $F(1) = 0$.

For $n = 3$ the nontrivial cycles can be represented by elements $(1, 0, 0)$ and $(1, 1, 0)$, each of length 3. There are $2^3 = 8$ elements in $\mathbb{F}_2^3$, so F is determined by its values at these elements, together with the trivial cycles. There are 2 possibilities for $F(0)$, then 1 possibilty for $F(1)$, then 6 possibilities for $F(1, 0, 0)$, determining also $F(0, 1, 0)$ and $F(0, 0, 1)$, and then finally 3 possibilities for $F(1, 1, 0)$. Thus, in total there are $2 \cdot 1 \cdot 6 \cdot 3 = 36$ bijections.

For $n = 4$ the nontrivial cycles are $(1, 0, 1, 0)$ of length 2 and $(1, 0, 0, 0)$, $(1, 1, 0, 0)$, and $(1, 1, 1, 0)$, each of length 4. Counting bijections as above, starting with the cycles of smallest length, we get that there are $2 \cdot 1 \cdot 2 \cdot 12 \cdot 8 \cdot 4 = 1536$ bijections.

Here are a list of some more computation results:

n	decomposed bijection count	number of bijections
1	$2 \cdot 1$	2
2	$2 \cdot 1 \cdot 2$	4
3	$2 \cdot 1 \cdot 6 \cdot 3$	36
4	$2 \cdot 1 \cdot 2 \cdot 12 \cdot 8 \cdot 4$	1536
5	$2 \cdot 1 \cdot 30 \cdot 25 \cdot 20 \cdot 15 \cdot 10 \cdot 5$	22 500 000
6	$2 \cdot 1 \cdot 2 \cdot 6 \cdot 3 \cdot 54 \cdot 48 \cdots 12 \cdot 6$	263 303 591 362 560
7	$2 \cdot 1 \cdot 126 \cdot 119 \cdots 14 \cdot 7$	large number

Obviously, one can easily reduce these numbers by splitting the count into equivalence classes. For example, just by requiring $F(0) = 0$ and $F(1) = 1$, we can divide all counts by 2.

The above does not seem to be well known (see [13, Table 3]), although a formula was given in [10, Proposition 14]. Following the above approach and inspired by [10, Proposition 14], we can give a more general result.

Let X be a set of n elements and let G be a subgroup of the symmetric group S_n. Let H denote the group of permutations on X that are invariant under G, that is, $H = C_{S_n}(H)$, the centralizer of G in S_n. To compute the number of elements in H, recall that the orbits $Gx = \{gx : g \in G\}$ form a partition of X. Let d be the number of distinct sizes $s_1, \dots, s_d$ of the sets Gx, $x \in X$, and let t_i be the number of orbits of size s_i for $1 \le i \le d$, so that

$$\sum_{i=1}^{d} t_i s_i = n.$$

Then the size of H is

$$\prod_{i=1}^{d} s_i^{t_i} \, (t_i!).$$

One situation that is of particular interest is when p is a prime number and $X = \mathbb{F}_{p^k}^m$, so $n = p^{km}$, and $G = \{S^j : 0 \le j < m\}$, where S denotes the permutation on X given by $S(x_1, x_2 \dots, x_m) = (x_m, x_1, \dots, x_{m-1})$ for $x_i \in \mathbb{F}_{p^k}$. In this case, one may also define the subgroups L and A of S_n consisting of all linear and affine bijections $X \to X$, respectively, when X is viewed as an m-dimensional vector space over $\mathbb{F}_{p^k}$.

The size of L is given by

$$\prod_{i=1}^{m}\left(p^{km}-p^{k(i-1)}\right),$$

where the reasoning is that the first row can be any nonzero element, and for $i \geq 2$, the $i+1$'th row must be outside the span of the first i rows. The size of A is then p^{km} times the size of L. We remark that the group of invertible circulant matrices coincides with $C_L(G) = C_{S_n}(G) \cap L$, and its size is computed above in Theorem 8.12 in the case $p^k = 2$.

5. Liftings and some open questions

Computing the number of (k,n)-liftings for $k < n$ seems much more difficult than the computation for $k = n$. In general, if f is a (k,n)-lifting there may be other m's such that f is also a (k,m)-lifting, so we define the set

$$\mathrm{inv}(f) = \{n \geq k : f \text{ induces a bijection } \mathbb{F}_2^n \to \mathbb{F}_2^n\}.$$

Then f is locally invertible if $\mathrm{inv}(f) = \{n : n \geq d\}$ and globally invertible if $\mathrm{inv}(f) \neq \varnothing$. In the latter case it is natural to distinguish between the functions f for which the set $\mathrm{inv}(f)$ is finite or infinite.

Consider the two commuting maps $\mathbb{F}_2^n \to \mathbb{F}_2^n$ given by complementing and reflecting, i.e.,

$$(x_1, x_2, \ldots, x_n) \mapsto (\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n}) \quad \text{and} \quad (x_1, x_2, \ldots, x_n) \mapsto (x_n, x_{n-1}, \ldots, x_1).$$

We say that f and g are *essentially equivalent* (surely, a subclass of the well known extended affine equivalence notion) if g can be formed by composing f with any combination of these two maps, modulo adding a constant term. Clearly, the invertibility properties are preserved under essential equivalence.

The functions $f(x_1, \ldots, x_k) = x_j$ for $1 \leq j \leq k$ generate invertible (k,n)-liftings, for all $n \geq k$, and for $k = 1, 2, 3$ there are no other locally invertible functions. For $k = 4$ the following function, originally described by Patt [15], is the only locally invertible up to essential equivalence:

$$x_2 + x_1\overline{x_3}x_4.$$

Below we present what we believe are all functions $f\colon \mathbb{F}_2^4 \to \mathbb{F}_2$ for which $\mathrm{inv}(f)$ is infinite, found by experiments, up to essential equivalence. The following induce permutations for all odd n, but not for even n, i.e., $\mathrm{inv}(f) = \{5, 7, 9, 11, \ldots\}$:

$$x_2 + x_1x_3\overline{x_4}, \quad x_1 + x_2\overline{x_3}, \quad x_2 + x_3\overline{x_4},$$

the latter two coming from a 3-variable function. The following induce permutations for all n not divisible by 3, i.e., $\mathrm{inv}(f) = \{4, 5, 7, 8, 10, 11, \ldots\}$:

$$x_1 + x_2x_3\overline{x_4}, \quad x_1 + \overline{x_2}x_3x_4.$$

For $n \geq 5$ some examples are given in [4, Appendix A.3].

The table below shows the number of (k,n)-liftings for $k=4$ and 5 on the left and right, respectively.

n	# liftings	deg ≤ 1	deg ≤ 2
4	768	8	32
5	236	8	40
6	22	6	14
7	30	6	14
8	20	8	8
9	22	6	14
10	20	8	8
11	32	8	16
12	10	6	6
13	32	8	16
14	18	6	6
15	22	6	14

n	# liftings	deg ≤ 1	deg ≤ 2
5	11250000	15	1890
6		12	336
7		12	89
8		16	16
9		12	33
10		15	19
11		16	40
12		12	12
13		16	40
14		12	16
15		9	25

An exhaustive search reveals that there are 94 functions of deg ≤ 2 that are $(5,n)$-liftings for some $7 \leq n \leq 15$. In other words, there are only 5 functions amongst these that are not $(5,7)$-liftings. Some of these are $(5,9)$-liftings, but not $(5,m)$-liftings for any other $5 \leq m \leq 15$.

Question 5.1. There are several counting problems related to (k,n)-liftings.

(i) How many locally invertible functions in k variables are there?
(ii) How many globally invertible functions in k variables with infinite $\mathrm{inv}(f)$ are there?
(iii) Can one find upper bounds on the number of liftings of various types? We provide partial results below for $(3,n)$ and $(4,n)$-liftings.
(iv) Does there exist a bound, say $\tau(k)$, such that if f is a (k,n)-lifting for some $n \geq k$, then there exists $m < \tau(k)$ such that f is a (k,m)-lifting?

Remark 5.2. If f is a (k,n)-lifting and $k \leq m \leq n$ such that m divides n, then f is also a (k,m)-lifting. In [4, after Proposition 6.1] it is explained that this leads to a way of describing $\mathrm{inv}(f)$ by a set of integers denoted by ξ. Experiments indicate that ξ may be finite for many functions f, but the same experiments also indicate that this is not always the case. We note that for every example in [4, after Proposition 6.1], the set ξ is given as a small finite set. In general, it seems difficult to find a proof that determines $\mathrm{inv}(f)$ based on partial knowledge of $\mathrm{inv}(f)$. In fact, even proving whether or not $\mathrm{inv}(f)$ is infinite seems hard.

6. General results and bounds on (k,n)-liftings

We observed computationally and then showed (see also [3, Theorem 2.5] that if a Boolean function f is a (k,n)-lifting, then the algebraic degree of f is smaller than k.

Theorem 6.1. *Let f be a (k,n)-lifting, $n \geq k \geq 3$. Then* $\deg(f) < k$.

Proof. Let the vectorial function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be the lift of f. Since F is a permutation , then (at least) its first component must be balanced. We will show that if f contains the term $x_1 x_2 \cdots x_k$, then f cannot be balanced (this last claim can be shown from what we know about the weight distribution of Reed-Muller codes, but we provide below an argument avoiding that).

Let $f(x) = f_k(x) + x_1x_2\cdots x_k$, where f_k has degree less than k. It suffices to show that

$$\sum_{x\in\mathbb{F}_2^k} f_k(x) \equiv 0 \pmod 2, \tag{1}$$

for each $k = 2, 3, \dots$, since then the truth table of $x_1x_2\cdots x_k + f_k(x)$ will have an odd number of 1's.

We shall prove (1) by induction. The initial case $k = 2$ is obviously true, so we assume (1) holds for k and prove it for $k+1$. Given $f(x) = f_{k+1}(x) + x_1x_2\cdots x_{k+1}$, $\deg(f_{k+1}) < k+1$, we distinguish two cases in the proof.

Case 1. If there exists x_i which occurs in every term of degree n in $f_{k+1}(x)$ then

$$f_0 = f_{k+1}(x_1, \cdots, x_{i-1}, 0, x_{i+1}, \cdots, x_{k+1})$$

and

$$f_1 = f_{k+1}(x_1, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_{k+1})$$

have degrees $\le k-1$. So (below, we let $x = (x_1, \dots, x_{k+1})$) by the induction hypothesis

$$\sum_{x\in\mathbb{F}_2^{k+1}} f_{n+1}(x) = \sum_{\substack{x\in\mathbb{F}_2^{k+1}\\ x_i=0}} f_0 + \sum_{\substack{x\in\mathbb{F}_2^{k+1}\\ x_i=1}} f_1 \equiv 0 + 0 \equiv 0 \pmod 2.$$

Case 2. If there is no x_i as in Case 1, then $f_{k+1}(x)$ contains all $\binom{k+1}{k}$ possible terms of degree k. Remove the term $t(x) = x_2\cdots x_{k+1}$ from $f_{k+1}(x)$ and let the resulting function of degree $\le k$ be $g_{k+1}(x)$. Define

$$g_0 = g_{k+1}(0, x_2, \dots, x_{k+1})$$

and

$$g_1 = g_{k+1}(1, x_2, \dots, x_{k+1}).$$

Then g_0 and g_1 have degrees $\le k-1$, as in Case 1 and we have, using the induction hypothesis twice

$$\begin{aligned}\sum_{x\in\mathbb{F}_2^{k+1}} f_{k+1}(x) &= \sum_{\substack{x\in\mathbb{F}_2^{k+1}\\ x_1=0}} g_0 + \sum_{\substack{x\in\mathbb{F}_2^{k+1}\\ x_1=1}} g_1 + \sum_x t(x)\\ &\equiv 0 + \sum_{\substack{x\in\mathbb{F}_2^{k+1}\\ x_{k+1}=0}} t(x) + \sum_{\substack{x\in\mathbb{F}_2^{k+1}\\ x_{k+1}=1}} t(x) \equiv 0 \pmod 2.\end{aligned}$$

The claim is shown. □

In the course of the previous proof, we used the fact that the first coordinate (or any other, for that matter) must be balanced. We shall use this idea in the proof of the next result, which gives bounds for the number of $(3, n)$-liftings, $n \ge 4$.

Proposition 6.2. *Let $n \geq 4$. The number of $(3,n)$-liftings (with no constant term) is upper bounded by 8, and the bound is attained. The number of $(4,n)$-liftings, $n \geq 6$, is upper bounded by 146 (it is unknown, if attained). If $3 \leq n \leq 15$, the number of $(3,n)$-liftings is ≤ 8. If $6 \leq n \leq 15$, the number of $(4,n)$-liftings is ≤ 32. The exact counts up to $n = 15$ is given in Section 9.*

Proof. Let f be a (k,n)-lifting and $F = (f_1, f_2, \ldots, f_n)$ be the bijection on $\mathbb{F}_2^n$ obtained from f, where $f_i = f \circ S^{i-1}$. Surely, the coordinates of any bijection must be balanced, and in fact, any block of coordinates $(f_{i_1}, f_{i_2}, \ldots, f_{i_t})$ (for some $t \geq 1$) must be balanced, that is, each vector of $\mathbb{F}_2^t$ must be attained the same number of times, namely, the frequency of each block must be 2^{n-t}. We also note that each coordinate of a bijection F, hence the (k,n)-lifting f must contain an odd number of terms. We will use these observations to prune down the list of potential liftings.

There are 20 balanced functions in 3 variables (with no constant term) containing an odd number of terms, namely,

$$\begin{aligned}
&x_2, x_1x_3 + x_2 + x_3, x_2x_3 + x_1 + x_3, x_1x_2 + x_1x_3 + x_2x_3 + x_1 + x_2,\\
&x_1x_3 + x_2x_3 + x_1, x_1, x_1x_2 + x_1x_3 + x_2x_3 + x_2 + x_3, x_1x_2 + x_2 + x_3, x_3,\\
&x_1x_2 + x_1x_3 + x_2, x_1x_2 + x_1x_3 + x_2x_3 + x_1 + x_3, x_1x_2 + x_2x_3 + x_1,\\
&x_1x_2 + x_1 + x_3, x_2x_3 + x_1 + x_2, x_1x_2 + x_2x_3 + x_3, x_1 + x_2 + x_3,\\
&x_1x_2 + x_1x_3 + x_2x_3, x_1x_3 + x_1 + x_2, x_1x_2 + x_1x_3 + x_3, x_1x_3 + x_2x_3 + x_2.
\end{aligned}$$

Among these, there are 10 balanced functions, namely,

$$\begin{aligned}
&x_1, x_2, x_3, x_1 + x_2 + x_3, x_1x_2 + x_1 + x_3, x_1x_2 + x_2 + x_3, x_2x_3 + x_1 + x_2,\\
&x_2x_3 + x_1 + x_3, x_1x_2 + x_1x_3 + x_2x_3 + x_1 + x_2, x_1x_2 + x_1x_3 + x_2x_3 + x_2 + x_3,
\end{aligned}$$

for which a block of two consecutive coordinates of F, namely $(f(x_1, x_2, x_3), f(x_2, x_3, x_4))$, which are balanced, for $n = 4$. Increasing to a block of size $3, 4$, for $n = 5, 6$, the set of potential (k,n)-liftings does not get pruned down, however, for $n \geq 7$, the block

$$(f(x_1, x_2, x_3), f(x_2, x_3, x_4), f(x_3, x_4, x_5), f(x_4, x_5, x_6), f(x_5, x_6, x_7)),$$

is not balanced anymore for two out of ten functions, as the set of values (running with $(x_1, x_2, \ldots, x_7)$ through $\mathbb{F}_2^7$) contains only 30 values in lieu of $2^5 = 32$. Surely, the same block, if $n > 7$ is also not balanced. The surviving lifters are

$$\begin{aligned}
&x_1, x_2, x_3, x_1 + x_2 + x_3, x_1x_2 + x_1 + x_3,\\
&x_1x_2 + x_2 + x_3, x_2x_3 + x_1 + x_2, x_2x_3 + x_1 + x_3.
\end{aligned}$$

A similar method works on the $(4,n)$-liftings, though we could not go below 146 (see below) potential "lifters". Out of the 3432 balanced functions in 4 variables, containing an odd number of terms (recall that this is necessary, otherwise they cannot lift to a permutation), going to $n = 8$, and taking consecutive blocks, we pruned down the list to 146 potential lifters. The computational results regarding the $(3,n)$, and $(4,n)$-liftings (exact counts up to $n = 15$ are displayed in Section 9) were obtained (and rechecked) via some SageMath programs. The claims of our proposition are shown. ∎

7. New classes of liftings

We start with some considerations from Daemen's thesis [4, Appendix A.2]. The Boolean function, or the rule, f that determines an infinite cellular automata can either be described by a polynomial, or by "landscapes" (or "complementing landscapes" as Daemen calls them [4, Section 6.6]). More precisely, a landscape is a sequence $L = (\ell_i)_{i=0}^{k-1}$ with an origin $\ell_j = *$ for some j and the other elements being denoted by $0, 1$ or $-$. If a rule is defined by one such landscape, then the bit in position $\star$ is flipped if it fits into the landscape.

A landscape is called conserved if remains unchanged after one iteration, in other words if the rule defines an idempotent bijection.

In [4, Appendix A.2], the technique used to show that certain shift-invariant functions are invertible, is to apply a method called "seed and leap", which constructs the inverse of any element, i.e., the method shows that the function is surjective.

We start with a family of $(k, k+2)$-liftings, for any $k \geq 3$ odd.

Theorem 7.1. *For an odd number $k \geq 3$, consider the Boolean function $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ given by*

$$f(x_1, \ldots, x_k) = x_1 + x_2 + x_{k-1} + x_k + \sum_{i=1}^{k-2} x_i x_{i+1},$$

and the corresponding S-box on $\mathbb{F}_2^n, n = k+2$, given by

$$F(x_1, x_2, \ldots, x_n) = (f(x_1, \ldots, x_k), f(x_2, \ldots, x_{k+1}), \ldots, f(x_k, x_1, \ldots, x_{k-1}))\,.$$

Then, F is a bijection on $\mathbb{F}_2^n$. Moreover, f is balanced and its nonlinearity is $N_f = 2^{k-1} - 2^{\frac{k-1}{2}}$ (matching the bent concatenation bound). Furthermore, $N_F \leq 2^{n-2}$ and $2^{n-3} \leq \delta_F \leq 2^{n-2}$.

Proof. To show the bijectivity of F, we will describe a transformation on the coordinates of F rendering a simpler system (for the one to one property). Let $f_i(x_1, \ldots, x_k, x_{k+1}, x_n) = S^{i-1} \circ f = f(x_i, x_{i+1}, \ldots, x_{k+i-1})$, and so $f_i(x_1, \ldots, x_k, x_{k+1}, x_n) = f(x_1, \ldots, x_k)$. The transformations (and their rotation symmetries) depend upon $k \pmod 8$, precisely, they are

$$\text{For } k \equiv 1 \pmod 8,\ f_1 + \sum_{i=1}^{\frac{k-1}{4}} f_{4i} = x_{k+2} + x_{k+2}x_1 + x_2,$$

$$\text{For } k \equiv 3 \pmod 8,\ \sum_{i=0}^{\frac{k-3}{4}} f_{4i+1} = x_k + x_k x_{k+1} + x_{k+2},$$

$$\text{For } k \equiv 5 \pmod 8,\ \sum_{i=0}^{\frac{k-5}{4}} (f_{4i+1} + f_{4i+2} + f_{4i+3}) + f_k + f_{k+1} = x_{k-2} + x_{k-2}x_{k-1} + x_k,$$

$$\text{For } k \equiv 7 \pmod 8,\ f_1 + \sum_{i=0}^{\frac{k-3}{4}} (f_{4i+2} + f_{4i+3} + f_{4i+4}) = x_{k+2} + x_{k+2}x_1 + x_2.$$

We shall show that the transformation renders the claimed trinomial, only in the case $k \equiv 1 \pmod 8$, as the others are rather similar.

We let $k \equiv 1 \pmod 8$ and write the expanded version of the sum $f_1 + \sum_{i=1}^{\frac{k-1}{4}} f_{4i}$, splitting the sum (for better understanding) at $n = k+2$. We get

$$
\begin{aligned}
&x_1 + x_2 + (x_1x_2 + \cdots + x_{k-2}x_{k-1}) + x_{k-1} + x_k \\
&+x_4 + x_5 + (x_4x_5 + \cdots + x_{k+1}x_{k+2}) + x_{k+2} + x_1 \\
&+x_8 + x_9 + (x_8x_9 + \cdots + x_{k+1}x_{k+2}) + x_{k+2}x_1 + (x_1x_2 + x_2x_3 + x_3x_4) + x_4 + x_5 \\
&\qquad\qquad\qquad\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
&+x_{k-1} + x_k + (x_{k-1}x_k + x_kx_{k+1} + x_{k+1}x_{k+2}) \\
&\qquad\qquad\qquad\qquad\qquad + x_{k+2}x_1 + (x_2x_2 + \cdots + x_{k-6}x_{k-5}) + x_{k-5} + x_{k-4}.
\end{aligned}
$$

We then see that when these equations are added, all terms cancel out (because of the parity of $k-1$) except for $x_2, x_{k+2}, x_{k+2}x_1$ from the first, second, respectively, third lines.

We therefore recover the $(3, k+2)$-lifting of [4], which we know is a bijection.

Surely, any function $g(x_1, \ldots, x_t) + x_{t+1}$ is balanced, hence f is balanced, since it is of this form. We now concentrate on the nonlinearity of f. We shall use now a result of Dickson [12, p. 438], which states that a (balanced) quadratic Boolean function in k variables is affine equivalent to $x_1x_2 + x_3x_4 + \cdots + x_{2d-1}x_{2d} + x_{2d+1}$, for some $d \le \frac{k-1}{2}$ (d is called the *Dickson rank*). Moreover, the nonlinearity of such a function is $2^{k-1} - 2^{k-1-d}$. We shall show that our function f has its Dickson rank equal to $\frac{k-1}{2}$, which will render our claim.

We therefore write

$$
\begin{aligned}
&f(x_1, \ldots, x_k) \\
&= x_1 + x_2 + x_1x_2 + x_2x_3 + x_3x_4 + \cdots + x_{k-3}x_{k-2} + x_{k-2}x_{k-1} + x_{k-1} + x_k \\
&= x_1 + x_2 + x_1x_2 + x_3(x_2 + x_4) + x_5(x_4 + x_6) + \cdots + x_{k-2}(x_{k-3} + x_{k-1}) + x_{k-1} + x_k \\
&= x_1 + x_1x_2 + x_3y_4 + \cdots + x_{k-2}y_{k-1} + y_2 + y_4 + \cdots + y_{k-1} + x_k,
\end{aligned}
$$

where

$$
\begin{aligned}
x_4 &= x_2 + y_4 \\
x_6 &= x_2 + y_4 + y_6 \\
&\cdots\cdots \\
x_{k-1} &= x_2 + y_4 + y_6 + \cdots + y_{k-1}.
\end{aligned}
$$

Since $k - 2 = 2\frac{k-1}{2} - 1$, then the Dickson rank of f is $\frac{k-1}{2}$ and the first claims are shown.

We now concentrate on the nonlinearity and differential uniformity of F. We first use the fact that F is affine equivalent the rotation-symmetric function generated by $h(x_1, x_2, x_3) = x_1 + x_1x_2 + x_3$, so the nonlinearity and differential uniformity is preserved.

It is easy to show that $h(x_1, x_2, x_3) = x_1 + x_1x_2 + x_3$ is APN (as a classical Boolean function), since, for $a = (a_1, a_2, a_3) \in \mathbb{F}_2^3, b \in \mathbb{F}_2$, $a \neq 0$, the equation

$$h\left((x_1, x_2, x_3) + (a_1, a_2, a_3)\right) + h(x_1, x_2, x_3) = b,$$

is equivalent to

$$a_1x_2 + a_2x_1 = b + a_1 + a_1a_2 + a_3,$$

which has at most two (bound attained for $a_1a_2 \neq 0$) solutions, and so, $\delta_h = 2$ (APN). By [13, Lemma 1], we know that $N_{\tilde{h}} = 2^{n-3} \cdot 2 = 2^{n-2}$, where $\tilde{h}(x_1, \ldots, x_n) = h(x_1, x_2, x_3)$. Further, the differential uniformity of $\tilde{h}$ is $\delta_{\tilde{h}} = 2^{n-3}\delta_h = 2^{n-2}$. Using [13, Theorem 1], we then get that (we denote by $h_i = h \circ S^{-1}$)

$$N_F \leq \min\{N_{h_1}, N_{h_2}, \ldots, N_{h_n}\} = N_h = 2^{n-2}$$

(in fact, this is attained) and

$$2^{n-3} \leq \delta_F \leq 2^{n-2}$$

(the upper bound is attained). The proof of our theorem is shown. □

Remark 7.2. The function $f(x_1, \ldots, x_k) = x_1 + x_2 + x_{k-1} + x_k + \sum_{i=1}^{k-2} x_ix_{i+1}$ has higher nonlinearity, namely $2^{k-1} - 2^{\frac{k-1}{2}}$, compared to nonlinearity of 2 (in dimension 3) for $x_1 + x_1x_2 + x_3$, or even 2^{k-2} (considered in dimension k, like our f). Moreover, with a bit more work, one can show that the differential uniformity of f is in fact 2^{k-2}, since the equation $f((x_1, \ldots, x_k) + (a_1, \ldots, a_k)) + f(x_1, \ldots, x_k) = b, (a_1, \ldots, a_k) \in \mathbb{F}_2^k, b \in \mathbb{F}_2$, is equivalent to

$$a_2x_1 + (a_1 + a_3)x_2 + \cdots + (a_{k-3} + a_{k-2})x_{k-2} + a_{k-2}x_{k-1} = b + f(a_1, \ldots, a_k),$$

whose maximum (attained) number of solutions is 2^{k-2}. Furthermore, both f, h generate equivalent S-boxes, hence having the same nonlinearity and differential uniformity.

It turns out that one can give a general class of (n, k)-liftings that happen to be conserved landscapes for any dimension $n \geq k \geq 4$. For a binary string B, we let $\mathrm{len}(B)$ be its length. Further, we take the concatenation of two binary strings (of arbitrary length), B_2B_1 and a shift to the right $s_\ell(B_2B_1)$ (by an arbitrary step, say ℓ) of B_2B_1 and we find the length of the largest overlap of consecutive bits between B_2B_1 and $s_\ell(B_2B_1)$, which we denote by $ov(B_2B_1 \cap s_\ell(B_2B_1))$. For example, if $B_1 = 11, B_2 = 10$, then $ov(1011 \cap s_1(1011)) = 1$, $ov(1011 \cap s_2(1011)) = 1$, $ov(1011 \cap s_3(1011)) = 1$.

Theorem 7.3. *For a fixed k, and $s \leq k$, we shall denote the polynomial*

$$x_s + (x_1 + \epsilon_1)(x_2 + \epsilon_2) \cdots (x_{s-1} + \epsilon_{s-1})(x_{s+1} + \epsilon_{s+1}) \cdots (x_d + \epsilon_k), \epsilon_i \in \{0, 1\},$$

by

$$\epsilon_1 \ldots \epsilon_{s-1} \star \epsilon_{s+1} \ldots \epsilon_k.$$

We now let $1 \leq s \leq k$ and f of the above form, that is, $f(x_1, \ldots, x_k) = x_s + (x_1 + \epsilon_1)(x_2 + \epsilon_2) \cdots (x_{s-1} + \epsilon_{s-1})(x_{s+1} + \epsilon_{s+1}) \cdots (x_d + \epsilon_k) = B_1 \star B_2$ (in the above notation), where $B_1 = \epsilon_1 \ldots \epsilon_{s-1}, B_2 = \epsilon_{s+1} \ldots \epsilon_k$ are binary strings satisfying $ov(B_2B_1 \cap s_\ell(B_2B_1)) < \min\{\mathrm{len}(B_1), \mathrm{len}(B_2)\}$. Then the rotation symmetric vectorial function $F(x_1, \ldots, x_n) = (f(x_1, \ldots, x_k), \ldots, f(x_k, x_1, \ldots, x_{k-1}))$ is a permutation (k, n)-lifting Sbox.

Proof. The function f was chosen this way, since for any binary string $\alpha = (\alpha_1, \dots, \alpha_n)$ as an input to $F(x_1, \dots, x_n) = (f(x_1, \dots, x_k), f(x_2, \dots, x_{k+1}), \dots, f(x_n, x_1, \dots, x_{k-1}))$, the value of F will not flip the bits in α unless the occur in the position of $\star$ with B_1 to the left and B_2 to the right. Moreover, the imposed condition on B_1, B_2 ensures that the function F is 1-1, since there are no instances when the "flipped" bit occurs in blocks in other than the $\star$ positions, which never overlap with non-*star* positions. This show that the vectorial function F is injective, and therefore bijective. ☐

We give below some precise examples.

Corollary 7.4. *The following are (k, n)-liftings for all $n \geq k \geq 4$:*

$$\begin{aligned}
k = 4: &\quad 1 \star 01 = x_2 + x_3 + x_1x_3 + x_3x_4 + x_1x_3x_4 \\
k = 5: &\quad 10 \star 10 = x_3 + x_2x_5 + x_1x_2x_5 + x_2x_4x_5 + x_1x_2x_4x_5 \\
k = 6: &\quad 110 \star 01 = x_4 + x_3x_5 + x_1x_3x_5 + x_2x_3x_5 + x_1x_2x_3x_5 + x_3x_5x_6 \\
&\qquad + x_1x_3x_5x_6 + x_2x_3x_5x_6 + x_1x_2x_3x_5x_6 \\
k = 7: &\quad 1110 \star 10 = x_5 + x_4x_7 + x_1x_4x_7 + x_2x_4x_7 + x_1x_2x_4x_7 + x_3x_4x_7 + x_1x_3x_4x_7 \\
&\qquad + x_2x_3x_4x_7 + x_1x_2x_3x_4x_7 + x_4x_6x_7 + x_1x_4x_6x_7 + x_2x_4x_6x_7 \\
&\qquad + x_1x_2x_4x_6x_7 + x_3x_4x_6x_7 + x_1x_3x_4x_6x_7 + x_2x_3x_4x_6x_7 + x_1x_2x_3x_4x_6x_7
\end{aligned}$$

are all liftings for any dimension $n \geq k$. More generally, for $k \geq 5$,

$$\begin{aligned}
k \text{ even}: &\quad \overbrace{(11\dots1)}^{k-4 \text{ times}}\, 0 \star 01 \\
k \text{ odd}: &\quad \overbrace{(11\dots1)}^{k-4 \text{ times}}\, 0 \star 10.
\end{aligned}$$

8. Affine equivalence and cyclic functions

The cycle of an element $x \in \mathbb{F}_2^n$ is the set $c(x) = \{S^j(x) : j \in \mathbb{Z}\}$, whose size must divide n. Two cycles are either equal or disjoint, so the collection of cycles $X = \{c(x) : x \in \mathbb{F}_2^n\}$ forms a partition of $\mathbb{F}_2^n$. A map $\mathbb{F}_2^n \to \mathbb{F}_2^n$ is called *cyclic* if it restricts to a map $X \to X$, for every cycle X, that is, if the image of every cycle is contained in a cycle.

Lemma 8.1. *If $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is a function satisfying $FS = S^kF$ for some $1 \leq k \leq n$, then F is cyclic.*

Moreover, for every $1 \leq j, \ell \leq n$, consider the set $X_{j,\ell} = \{F \colon \mathbb{F}_2^n \to \mathbb{F}_2^n \mid FS^j = S^\ell F\}$. Then $X_{j,\ell}$ is a subset of the set of all cyclic functions if and only if $\gcd(j, n) = 1$.

If $\gcd(j, n) = 1$, *then there is some $1 \leq k \leq n$ such that $X_{j,\ell} = X_{1,k}$.*

Proof. Suppose that $FS = S^kF$ and let $x \in \mathbb{F}_2^n$. Then $S^{ki}F(x) = F(S^ix)$, for all i, that is, the image of the cycle of x belongs to the cycle of $F(x)$.

If $\gcd(j, n) > 1$, then define the element x to be the element formed by repeating the string $1, 0 \dots, 0$ of length $\gcd(j, n)$ a number of $n/\gcd(j, n)$ times. Define F by taking $F(S^{i\gcd(j,n)}x) = (1, 1, \dots, 1)$ for $i \geq 0$, and $F(y) = (0, 0, \dots, 0)$ for all other $y \in \mathbb{F}_2^n$. Then F satisfies $FS^j = S^\ell F$ for all ℓ and maps $c(x)$ to $\{(0, 0, \dots, 0), (1, 1, \dots, 1)\}$, so it is not cyclic.

If $\gcd(j,n)=1$, then there exists $1 \le k \le n$ such that $jk=\ell$, and computations show that $FS = S^kF$ if and only if $FS^j = S^\ell F$. $\square$

Note that there exists a cyclic function F and integers j,ℓ with $\gcd(j,n)>1$ such that $FS^j = S^\ell F$, but there is no k such that $FS = S^kF$ holds (for this particular F), so the above result only applies to this class of functions.

Definition 8.2. A function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called k-shift-invariant if it satisfies $FS = S^kF$ for some $1 \le k \le n$. If $k=1$, then F is shift-invariant, as above.

Remark 8.3. We want to point out that the concept of k-rotation-symmetric Sboxes has been previously defined (see [10]): a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ satisfying $S^kF = FS^k$ (for k dividing n) is called k-rotation symmetric. However, as we point out below, for us it is more natural (given the connection with circulant matrices) to consider the above definition. If $\gcd(k,n)=1$ and $FS^k = S^kF$, let m be so that $mk = 1 \pmod n$, and then $FS = FS^{mk} = S^{mk}F = SF$, so F is shift-invariant. If $\gcd(k,n)>1$, then we can potentially be in a rather different setting, e.g., if

$$A = \begin{pmatrix} a & b & c & d \\ e & f & g & h \\ c & d & a & b \\ g & h & e & f \end{pmatrix},$$

then $AS^2 = S^2A$, but A (or A^T) is not necessarily k-circulant for any k.

The set of cyclic functions and the set of shift-invariant functions are both closed under composition, while a product of an m- and k-shift-invariant function is mk-shift-invariant. Thus the set of all functions that are k-shift-invariant for some k is also closed under composition.

We denote a k-circulant matrix by

$$C_k(a_1,\dots,a_n) = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_{n-k+1} & a_{n-k+2} & \cdots & a_{n-k} \\ a_{n-2k+1} & a_{n-2k+2} & \cdots & a_{n-2k} \\ \vdots & \vdots & \vdots & \vdots \\ a_{k+1} & a_{k+2} & \cdots & a_k \end{pmatrix}.$$

Lemma 8.4. *Let A be a matrix. The following are equivalent:*

(i) *the linear transformation $x \mapsto Ax$ is cyclic,*

(ii) *there exists a vector $b \in \mathbb{F}_2^n$ and an integer $1 \le k \le n$ such that*

$$\text{column } i \text{ of } A = S^{(i-1)k}b \textit{ for all } 1 \le i \le n,$$

that is A^T is k-circulant.

(iii) *there is an integer $1 \le k \le n$ such that $AS = S^kA$, that is, the linear transformation $x \mapsto Ax$ is k-shift-invariant.*

We say that the matrix A is cyclic if any of these equivalent conditions hold.

Proof. The equivalence between (ii) and (iii) follows from [5, Theorem 5.1.1].

Suppose that $x \mapsto Ax$ is cyclic. Then the image of the cycle $\{e_1, \ldots, e_n\}$ must be a cycle. The image $Ae_1, \ldots, Ae_n$, that is, the columns of A, therefore make up a cycle, and thus (ii) holds.

Suppose (iii) holds, i.e., $AS = S^k A$ for some k, and let $x \in \mathbb{F}_2^n$. Then, since $Sc(x) = c(x)$, we have $Ac(x) = ASc(x) = S^k Ac(x)$, that is, S^k maps the set $Ac(x)$ to $Ac(x)$, and thus $Ac(x)$ must be contained in a cycle. □

An affine transformation $x \mapsto Ax + c$ is k-shift-invariant if and only if $x \mapsto Ax$ is k-shift-invariant and $S^k c = c$. Indeed, assuming $FS = S^k F$, and setting $x = 0$, gives that $S^k c = c$, and then the k-shift-invariance of the linear part follows.

If $AS = S^k A$ with $\gcd(k, n) = 1$, then there exists a unique $1 \le m \le n$ such that $SA = AS^m$. Indeed, given such a k, there is a unique m such that $mk = 1$ and then $SA = S^{mk} A = AS^m$. In particular, by using that $S^T = S^{-1}$, this means that $A^T S = S^m A^T$, so the transpose of A also induces a cyclic linear transformation $x \to A^T x$.

Moreover, if F is k-shift-invariant and $\gcd(k, n) = 1$, then the image under F of a cycle is always equal to a cycle (not just contained in one), and for a k-shift-invariant function to be bijective it is necessary that $\gcd(k, n) = 1$, otherwise the elements e_1 takes the same value as e_i for some $i > 1$, where e_i denotes the vector with 1 on position i, and 0 else. Indeed, $F(e_2) = S^k F(e_1)$, $F(e_3) = S^k F(e_2) = S^{2k} F(e_1)$, etc.

Lemma 8.5. *Let F be k-shift-invariant and $\gcd(k, n) = 1$. Then F is completely determined by a single Boolean function f by*

$$F = (f, f \circ S^{-m}, f \circ S^{-2m}, \ldots, f \circ S^{-(n-1)m}),$$

where m is the inverse of k modulo n.

Proof. As usual, let f_i denote the coordinate functions of F so that $f_1 = f$. Then the identity $f_i \circ S = f_{i-k \pmod n}$ leads to

$$f_{\ell k+1} \circ S^{\ell} = f_{(\ell-1)k+1} \circ S^{\ell-1} = \cdots f_{k+1} \circ S^{-1} = f_1,$$

for $0 \le \ell \le n-1$, so $f_{\ell k+1} = f \circ S^{-\ell}$. Now set $i = \ell k + 1 \pmod n$, so that $\ell = m(i-1) \pmod n$, where m is the inverse of k, and then we get that $f_i = f \circ S^{-m(i-1)}$. □

In general, two functions $F, G \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ are said to be affine equivalent if there exist invertible matrices $A, B \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ and elements $d, e \in \mathbb{F}_2^n$ such that

$$F(Ax + e) = BG(x) + d.$$

Lemma 8.6. *Let F, G be two functions $\mathbb{F}_2^n \to \mathbb{F}_2^n$ with $F(Ax + e) = BG(x) + d$ and assume that A and B are invertible and satisfy $AS = S^k A$, $BS = S^k B$ for some $1 \le k \le n$. Assume also that d, e belong to $\{(0, 0, \ldots 0), (1, 1, \ldots, 1)\}$. Then*

(i) *For every $1 \le m \le n$, F is m-shift-invariant if and only if G is m-shift-invariant,*
(ii) *F is cyclic if and only if G is cyclic,*
(iii) *F is bijective if and only if G is bijective.*

Proof. If F is m-shift-invariant, then

$$\begin{aligned}S^m G(x) + B^{-1}d &= S^m B^{-1} F(Ax+e) = B^{-1} S^{km} F(Ax+e) \\ &= B^{-1}F(S^k Ax + e) = B^{-1}F(ASx+e) \\ &= G(Sx) + B^{-1}d,\end{aligned}$$

so G is m-shift-invariant, and the same argument applies in the opposite direction. The cyclic and the permutation properties follow by the composition of functions. □

In light of the above we introduce the following notion.

Definition 8.7. Two functions $F, G\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ are said to be cyclically equivalent if there exist invertible cyclic matrices $A, B\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ and elements $d, e \in \{(0,0,\ldots 0), (1,1,\ldots,1)\}$ such that

$$F(Ax+e) = BG(x) + d.$$

Let F and G be two cyclically equivalent bijections, and let A and B be the two implementing matrices. Suppose that F, G, A, B have degrees j, k, ℓ, m, respectively. Then

$$S^{j\ell}F(Ax+e) = F(ASx+e) = BG(Sx) + d = S^{km}BG(x) + d = S^{km}F(Ax+e),$$

so $j\ell = km \pmod n$, and in particular, F and G have the same degree if and only if A and B have the same degree.

Lemma 8.8. *If F and G are two affine equivalent cyclic bijections, and F is affine, then F and G are cyclically equivalent.*

Proof. If F is affine and cyclic, then $F(x) = Dx + b$ for some k-circulant matrix D^T with $\gcd(k, n) = 1$ and some $b \in \{(0,0,\ldots 0), (1,1,\ldots,1)\}$. Indeed, evaluating S^kF and FS at 0 gives that $S^kb = b$, and it follows that $SD = DS$. Since G is affine equivalent to F, then G is also affine, and therefore of the same type. Now just pick $Ax + e$ to be $G(x)$ and $Bx + d$ to be $F(x)$. □

Question 8.9. Clearly, if two functions are cyclically equivalent, then they are affine equivalent. Does the converse hold in the k-shift-invariant case? That is, F and G are k-shift-invariant and affine equivalent, are they necessarily cyclically equivalent? If not, can we produce a counter-example?

Experimenting in small dimensions suggests that affine equivalence may imply cyclically equivalence, but finding a proof in general seems hard.

Note that in [10, Theorem 10] it is indirectly claimed that the result holds, since the author attempts to compute the number of elements in the affine equivalence classes, but only attempts to compute it for the cyclic equivalence classes, and the number computed is also incorrect (see Remark 8.14 below). The result is also cited and used several places, e.g., on [13, p. 58] and on [2, p. 362].

Lemma 8.10. *The number of k-shift-invariant functions in the affine equivalence class of the identity matrix I is two times the number of invertible k-circulant matrices of dimension n.*

Proof. Suppose that $I(Ax+e) = BG(x)+d$ for all x, i.e., $G(x) = B^{-1}Ax + c$ for some c and all x. Setting $x = 0$, this gives that $G(0) = c$, so $c = (0,0,\ldots,0)$ or $(1,1,\ldots,1)$. This again implies that the transpose of $B^{-1}A$ is k-circulant.

The factor 2 comes from the two choices for c, and the result follows. □

The union of sets of all invertible k-circulant matrices forms a group under matrix multiplication and inverses, containing the set of invertible circulant matrices as a commutative subgroup.

If A is k-circulant and invertible, then $\gcd(k,n) = 1$, the cycle of the first row has maximal length n, and the Hamming weight of the first row is odd. If $\gcd(k,n) = 1$, then the number of invertible k-circulant matrices is the same as the number of circulant matrices. If n is a power of two, then the circulant matrices are precisely those coming from a first row with odd Hamminf weight, i.e., the number is $\sum_{\text{odd } i\, <\, n} \binom{n}{i} = 2^{n-1}$.

More generally, we can exactly characterize invertibility of circulant matrices. The following result can be found, for instance, in [1, Theorem 2.2], or [17], although the result appears much earlier in [8].

Theorem 8.11. *Let C be a (binary) circulant $n \times n$ matrix whose first row is $(a_1,\ldots,a_n)$, and $F(z) = a_1 + a_2z + \cdots + a_nz^{n-1} \in \mathbb{F}_2[z]$ be its generating polynomial. Then C is invertible if and only if $\gcd(F(z), z^n - 1) = 1$. Moreover, the first row $(\alpha_1,\ldots,\alpha_n)$ of the inverse C^{-1} is a solution of*

$$(\alpha_1,\ldots,\alpha_n)\cdot C = (1,0,\ldots,0),$$

and furthermore, if $F^*(z) = \alpha_1 + \alpha_2z + \cdots + \alpha_nz^{n-1}$ is the generating polynomial of C^{-1}, then $F(z)\cdot F^*(z) \equiv 1 \pmod{z^n - 1}$.

If $k = 1$, then $C_k(a_1,\ldots,a_n) = C(a_1,\ldots,a_n)$. When $\gcd(k,n) = 1$, then the rows of the k-circulant matrix A cycle through every shift of the first row in *some order* and so, there is a permutation matrix P such that $PA = PC_k(a_1,\ldots,a_n) = C(a_1,\ldots,a_n)$. Therefore, the invertibility of a k-circulant matrix A, under $\gcd(k,n) = 1$, is described by Theorem 8.11. When $\gcd(k,n) > 1$, a k-circulant matrix is never invertible. The following result follows easily.

We recall now the notion of cyclotomic cosets. If $\gcd(n,q) = 1$, then the *cyclotomic coset of q modulo n containing i* is $C_i = \{i \cdot q^j \pmod{n}, j = 0,1,\ldots\}$. A subset $\{i_1,\ldots,i_t\}$ is called a *complete set of representatives* of cyclotomic cosets of q modulo n if $C_{i_1},\ldots,C_{i_t}$ are distinct and $\mathbb{Z}_n = \cup_{j=1}^{t} C_{i_j}$. For example, the cyclotomic cosets of 2 modulo 15 are:

- $C_0 = \{0\}$;
- $C_1 = \{1,2,4,8\}$;
- $C_3 = \{3,6,9,12\}$;
- $C_5 = \{5,10\}$;
- $C_7 = \{7,11,13,14\}$;
- the set $\{0,1,3,5,7\}$ is a complete set of representatives of cyclotomic cosets of 2 modulo 15.

Theorem 8.12. *Let n be odd, m be the order of 2 modulo n, t be the number of distinct cyclotomic cosets of 2 modulo $2^m - 1$, of sizes $\ell_1, \ell_2, \dots, \ell_t$. The number c_n of invertible circulant $n \times n$ matrices over $\mathbb{F}_2$ is*

$$c_n = (2^{\ell_1} - 1)(2^{\ell_2} - 1) \cdots (2^{\ell_t} - 1).$$

If $2^t \| n$ (that means that $2^t \mid n$ and $2^{t+1} \nmid n$), $t > 1$, the number of invertible circulant $n \times n$ matrices over $\mathbb{F}_2$ is

$$2^{\frac{n(2^t-1)}{2^t}} c_{\frac{n}{2^t}}.$$

Proof. We shall use Theorem 8.11 and what is known about the factorization of $x^n - 1$ over a finite field to derive formulas about the number of invertible circulant matrices over $\mathbb{F}_2$.

It is known that if α is a primitive element of $\mathbb{F}_{q^m}$ then the *minimal polynomial* of α^i with respect to $\mathbb{F}_q$ is

$$m^{(i)}(x) = \prod_{j \in C_i} (x - \alpha^j),$$

where C_i is the unique cyclotomic coset of q modulo $(q^m - 1)$ containing i. For example, if α is a root of $x^2 + x + 2 \in \mathbb{F}_3[x]$, $\mathbb{F}_{3^2} = F_3(\alpha)$, then the minimal polynomial of α^2 is $m^{(2)}(x) = (x - \alpha^2)(x - \alpha^6)$, since the cyclotomic coset of $q = 3$ modulo $n = 3^2 - 1$ containing 2 is $C_2 = \{2, 6\}$. Moreover, the factorization of $x^n - 1$ over $\mathbb{F}_q$ is therefore

$$x^n - 1 = \prod_{i=1}^{t} m^{((q^m-1)s_i/n)}(x),$$

where m is the least integer such that $n \mid q^m - 1$, and $s_1, \dots, s_t$ is a complete set of representatives of q modulo n.

The circulant $n \times n$ matrices over $\mathbb{F}_2$ form a ring which is isomorphic to the factor ring $\mathbb{F}_2[x]/\langle x^n + 1 \rangle$. We apply the previous considerations to our situation. We let $q = 2$, n odd, and m be the order of 2 modulo n, that is, the smallest integer such that $n \mid 2^m - 1$. Let t be the number of distinct cyclotomic cosets, whose sizes we label by $\ell_1, \ell_2, \dots, \ell_t$. Since $x^n + 1$ can be factored over $\mathbb{F}_2$ as a product of irreducible polynomials of degree, which is the size of the cyclotomic cosets, we conclude that the ring R is isomorphic to a product of fields $R \cong F_{2^{\ell_1}} \times \cdots \times F_{2^{\ell_t}}$. A similar argument works for n not coprime to the characteristic, since $c_{2s} = 2^s c_s$ (see also [11]). Thus, if $2^t \| n$, so $n = 2^t s$, then

$$c_n = 2^{\frac{n}{2}} c_{\frac{n}{2}} = 2^{\frac{n}{2} + \frac{n}{4}} c_{\frac{n}{4}} = \ldots = 2^{\frac{n}{2} + \frac{n}{4} + \cdots + \frac{n}{2^t}} c_{\frac{n}{2^t}}.$$

We can compress the exponent using the sum of a geometric sequence and the claims are shown. $\square$

Remark 8.13. We can easily get the count for the number of invertible circulant matrices using the above theorem, and we display below this count for $1 \le n \le 32$: 1, 2, 3, 8, 15, 24, 49, 128, 189, 480, 1023, 1536, 4095, 6272, 10125, 32768, 65025, 96768, 262143, 491520, 583443, 2095104, 4190209, 6291456, 15728625, 33546240, 49545027, 102760448, 268435455, 331776000, 887503681, 2147483648, 3211797501, 8522956800, 12325233375, 25367150592, 68719476735, 137438429184, 206007472125.

Remark 8.14. In [10, Theorem 10] it is claimed that the number of elements in an affine equivalence class is given by a particular formula. Computing the number for $1 \leq n \leq 5$ gives 4, 8, 96, 128, 720 elements, respectively. This is claimed to hold for all equivalence classes, including the one for the identity, which contradicts our result above. Note also that the number of elements in an affine equivalence class is not constant.

Although the result [10, Theorem 10] is incorrect, it is possible that the formula gives an upper bound for the number of elements in an affine equivalence class.

The number of invertible circulant $n \times n$-matrices is a multiple of n, since shifting all elements of the matrix one step to the right produces another invertible circulant matrix.

Thus, the number of invertible circulant matrices divided by n is the number of "basis cycles", that is, cycles that spans the whole $\mathbb{F}_2^n$. More generally, one may consider the dimension of the span of a cycle, and note that a bijective cyclic linear transformation must take a cycle to a cycle with the same dimension.

If two shift-invariant bijections F and G are affine equivalent, what can we say about the equivalences of the corresponding Boolean function f and g? This result gives a precise condition for cyclic equivalence.

Theorem 8.15. *Let f and g be two Boolean functions inducing shift-invariant functions F and G. Then F and G are cyclically equivalent if and only if there are an invertible cyclic matrix A, a vector $(b_j)_{j=1}^n$ with the property that any cyclic matrix it defines is invertible, $d' \in \{0,1\}$, and $e \in \{(0,0,\dots 0),(1,1,\dots,1)\}$ such that*

$$\sum_{j=1}^{n} b_j (g \circ S^{1-j})(x) + d' = f(Ax+e). \tag{2}$$

Proof. Let F and G be cyclically equivalent, i.e., there exist A, B, d, e such that $F(Ax+e) = BG(x)+d$ for all x. Recall that A and B must be invertible and cyclic of the same degree, i.e., there is a k (which is here equal to the inverse of the degree) such that $AS^k = SA$ and $BS^k = SB$. Then the i'th coordinate function f_i for the map $x \mapsto F(Ax+e)$ is given by

$$f_i(x) = (f \circ S^{1-i})(Ax+e) = f(AS^{(1-i)k}x+e).$$

Let $(b_j)_{j=1}^n$ be the first row of B. To compute the i'th coordinate function g_i for the map $x \mapsto BG(x)+d$, we first note that the i'th row of B has b_1 in column $1+(i-1)k$. Thus g_i is given by

$$\begin{aligned} g_i(x) &= (\text{row } i \text{ of } B)\cdot(g \circ S^{1-i})(x) + d' \\ &= \sum_{j=1}^{n} b_j (g \circ S^{1-j-(1-(1+(i-1)k))})(x) + d' = \sum_{j=1}^{n} b_j (g \circ S^{1-j+(1-i)k})(x) + d', \end{aligned}$$

where d' is the first entry of d. For each i, we replace $S^{(1-i)k}x$ by y, and then $f_i(y) = g_i(y)$ coincides with the equation (2).

For the converse direction, if (2) holds, then we construct B from letting $(b_j)_{j=1}^n$ be its first row and shift by k, where k is the degree of A, and d is constructed the obvious way from d'. Then the define $f_i(x) = (f \circ S^{1-i})(Ax+e)$ and $g_i(x) =$

(row i of B) $\cdot (g \circ S^{1-i})(x) + d'$. The above computations give that $f_i = g_i$ for all i, hence $F(Ax+e) = BG(x) + d$. □

The above result also holds when F and G are k-shift-invariant with $\gcd(k,n) = 1$, just by replacing S^{1-j} by $S^{(1-j)m}$ in (2), where m is the inverse of k.

Recall that two Boolean functions f and g are said to be affine equivalent if there is an invertible matrix A such that $g(x) + d = f(Ax+e)$. It is also known that in the degree 2 case, then f is equivalent to g if and only if $N_f = N_g$ and $\mathrm{wt}(f) = \mathrm{wt}(g)$.

Definition 8.16. We say that two functions F and G are strongly affine equivalent if there is an invertible matrix A such that

$$F(Ax+e) = G(x) + d$$

for some $d, e \in \{(0,0,\dots 0),(1,1,\dots,1)\}$.

Lemma 8.17. *Two cyclic bijections F and G are strongly affine equivalent if and only if the corresponding Boolean functions f and g satisfies*

$$f(Ax+e) = g(x) + d$$

for some circulant matrix A, $d' \in \{0,1\}$, and $e \in \{(0,0,\dots 0),(1,1,\dots,1)\}$.

Proof. Note first that if F and G are strongly affine equivalent, then

$$Ax + e = F^{-1}G(x) + F^{-1}d,$$

so $F^{-1}G(x)$ is cyclic and affine, that is, equals $Dx+b$ for some k-circulant matrix D^T and $b \in \{(0,0,\dots 0),(1,1,\dots,1)\}$. Thus A^T is also k-circulant and $d, e \in \{(0,0,\dots 0),(1,1,\dots,1)\}$.

Moreover, the i'th coordinate functions of F and G are given by

$$f \circ S^{(1-i)k}(Ax+e) = f(AS^{(1-i)k}x + e) \quad \text{and} \quad g \circ S^{(1-i)k}(x) + d',$$

where d' is the constant entry of d. Since these are equal for all $y = S^{-ik}x$, we must have that $f(Ay+e) = g(y) + d'$, so f and g are affine equivalent.

The converse is similar. □

Question 8.18. Let F and G be shift-invariant bijections with corresponding Boolean functions f and g and define the Boolean function g_b by (2), that is,

$$g_b(x) = \sum_{j=1}^{n} b_j (g \circ S^{1-j})(x) + d'.$$

Clearly, if $b = e_1$, then $g = g_b + d'$, but is it possible that g and g_b are affine equivalent also when this is not the case? It follows from Theorem 8.15 that affine equivalence of f and g and cyclic equivalence of F and G are related via affine equivalence of g and g_b.

8.1. **Does affine equivalence imply cyclic equivalence?** The following discussion is meant to shed some light on Question 8.9, and to simplify notation, we ignore the constants and say that F and G are linearly equivalent if there exist invertible matrices A and B such that $FA = BG$.

If $FA = BG$ for some A, B, there are also many other pairs of matrices A', B' such that $FA' = B'G$. If F and G are cyclic and $FA = BG$, the question is whether one can always find a pair of cyclic matrices A', B' such that $FA' = B'G$. Clearly, if $FA = BG$, this also holds when the maps are restricted to the set of cycles. While F and G potentially can have any possible cycle map, for linear transformations the number of possible cycle maps is fairly small, so there must be a strong relationship between the cycle maps of F and G.

Suppose that F and G are two linearly equivalent shift-invariant bijections. We define the intertwiner sets

$$\begin{aligned}\operatorname{int}(F, G) &= \{(A, B) \in \mathrm{GL}(n, \mathbb{F}_2) \times \mathrm{GL}(n, \mathbb{F}_2) : FA = BG\}\\ \operatorname{int}(F) &= \{(A, B) \in \mathrm{GL}(n, \mathbb{F}_2) \times \mathrm{GL}(n, \mathbb{F}_2) : FA = BF\}\\ \operatorname{int}(G) &= \{(A, B) \in \mathrm{GL}(n, \mathbb{F}_2) \times \mathrm{GL}(n, \mathbb{F}_2) : GA = BG\}.\end{aligned}$$

We may note that the last two sets are actually groups under the pointwise product $(A, B)(A', B') = (AA', BB')$. Moreover, suppose that (A, B) and (A', B') belong to $\operatorname{int}(F, G)$. Then

$$FA'A^{-1} = B'GA^{-1} = B'B^{-1}F,$$

that is, the pair $(A'A^1, B'B^{-1})$ belongs to $\operatorname{int}(F)$. Similarly, $(A^1A', B^{-1}B)$ belongs to $\operatorname{int}(G)$.

In other words, there is a one-to-one-correspondence (bijection) between any two of the above sets. Indeed, fix some $(A, B) \in \operatorname{int}(F, G)$ and consider the map

$$\operatorname{int}(F) \to \operatorname{int}(F, G), \quad (A_F, B_F) \mapsto (A_F A, B_F B).$$

It is also straightforward to compute that if $(A, B) \in \operatorname{int}(F, G)$, $(A_F, B_F) \in \operatorname{int}(F)$, and $(A_G, B_G) \in \operatorname{int}(G)$, then $(A_F AA_G, B_F BB_G) \in \operatorname{int}(F, G)$, and thus

$$\operatorname{int}(F, G) = \operatorname{int}(F) \cdot (A, B) = (A, B) \cdot \operatorname{int}(G) = \operatorname{int}(F) \cdot (A, B) \cdot \operatorname{int}(G).$$

For example, if $F = I$, and $FA = BG$, then $G = B^{-1}A$ must be linear and cyclic, and in this case, $\operatorname{int}(F) = \{(A, A) : A \in \mathrm{GL}(n, \mathbb{F}_2)\}$.

The above at least indicates that $\operatorname{int}(F, G)$ is typically a fairly large set.

9. New classes found computationally

In the below, when f is a Boolean function in (at most) k variables and $k \le m$, we let $\operatorname{inv}(f) \cap \{k, k+1, \dots, m\}$ be denoted by $\operatorname{inv}_m(f)$. There are probably a great deal of overlap between the classes we present and the ones listed in [4, Appendix A.3] with a different description, but there are certainly examples below that are not in [4].

There are 82 nonlinear functions that are $(5, n)$-lifting for some $7 \le n \le 15$ and coming from a Boolean function with only quadratic terms. We display below the equivalence class representatives with at most five quadratic terms (we will also compute the permutation (PP) or non-permutation (N-PP) properties, nonlinearity (nl), differential/boomerang uniformity (DU/BU) and plateaued (p) or non-plateaued property for $n = 7$). We shall not compute the boomerang uniformity if the Sbox is not a permutation. Recall that the largest nonlinearity for $n = 7$ is 48 (some of our examples below achieve that). To have a benchmark, we compute these parameters for the Patt function, $x_1 + x_1x_2 + x_3$, for $n = 7$, obtaining $(PP, nl, p, DU, BU) = (1, 32, 1, 32, 96)$ (we put a 1 (respectively, 0) in the respective positions if the function is (respectively, it is not) a permutation, or plateaued).

$\mathrm{inv}_{15}(f)$	polynomial	(PP, nl, p, DU, BU)
odd	$x_1 + x_3 + x_1x_2$	$(1, 32, 1, 32, 96)$
$n \nmid 4$	$x_1 + x_5 + x_1x_3$	$(1, 32, 1, 32, 96)$
odd	$x_1 + x_2 + x_2x_3$	$(1, 32, 1, 32, 96)$
odd	$x_2 + x_4 + x_2x_3$	$(1, 32, 1, 32, 96)$
7	$x_1 + x_5 + x_1x_4$	$(1, 32, 1, 32, 96)$
$5, 7$	$x_1 + x_2 + x_1x_5$	$(1, 32, 1, 32, 96)$
$n \nmid 2, 3$	$x_2 + x_5 + x_1x_2 + x_2x_3 + x_3x_4$	$(1, 32, 1, 32, 96)$
7	$x_1 + x_5 + x_1x_2 + x_2x_4 + x_3x_4$	$(1, 48, 1, 16, 44)$
$5, 6, 7$	$x_2 + x_1x_3 + x_2x_4 + x_1x_5 + x_3x_5$	$(1, 48, 1, 8, 48)$
7	$x_2 + x_1x_3 + x_1x_4 + x_2x_5 + x_3x_5$	$(1, 0, 1, 16, 80)$
7	$x_2 + x_4 + x_5 + x_1x_2 + x_1x_3 + x_1x_4 + x_2x_4$	$(1, 48, 1, 8, 24)$
$n \nmid 2, 3$	$x_3 + x_5 + x_1x_2 + x_1x_3 + x_1x_4 + x_2x_4 + x_3x_4$	$(1, 32, 1, 32, 96)$
$5, 7$	$x_1 + x_4 + x_1x_2 + x_1x_3 + x_1x_4 + x_2x_4 + x_2x_5$	$(1, 32, 1, 16, 128)$
$6, 7$	$x_1 + x_2 + x_3 + x_4 + x_1x_3 + x_2x_3 + x_2x_4 + x_3x_4 + x_3x_5$	$(1, 48, 1, 8, 40)$

We note that the above function $x_2+x_5+x_1x_2+x_2x_3+x_3x_4$ is essentially equivalent to the one from Theorem 7.1, for $k = 5$.

The below table is, up to essential equivalence, a complete list of all nonlinear $(5, 9)$-liftings that come from a Boolean function with only quadratic terms:

$\mathrm{inv}_{15}(f)$	polynomial	(PP, nl, p, DU, BU) for $n = 9$
odd	$x_1 + x_3 + x_1x_2$	$(1, 128, 1, 128, 448)$
$n \nmid 4$	$x_1 + x_5 + x_1x_3$	$(1, 128, 1, 128, 448)$
odd	$x_1 + x_2 + x_2x_3$	$(1, 128, 1, 128, 448)$
odd	$x_2 + x_4 + x_2x_3$	$(1, 128, 1, 128, 448)$
$6, 9$	$x_3 + x_1x_2 + x_2x_4 + x_1x_5 + x_4x_5$	$(1, 128, 1, 512, 512)$
9	$x_1 + x_4 + x_2x_5$	$(1, 128, 1, 128, 448)$

There are 92 function that are $(5, 7)$-liftings coming from a Boolean function with exactly one cubic term (and no term with higher degree), divided into 23 essential equivalence classes, and here is a complete list of representatives:

$\mathrm{inv}_{15}(f)$	polynomial	(PP, nl, p, DU, BU)
$n \nmid 3$	$x_4 + x_1x_2 + x_1x_2x_3$	$(1, 16, 0, 56, 100)$
$n \nmid 3$	$x_4 + x_2x_3 + x_1x_2x_3$	$(1, 16, 0, 56, 94)$
$n \nmid 3$	$x_2 + x_5 + x_1x_2 + x_2x_4 + x_1x_2x_3$	$(1, 32, 0, 32, 104)$
7	$x_1 + x_4 + x_1x_2 + x_1x_5 + x_1x_2x_3$	$(1, 32, 0, 20, 56)$
$6, 7, 11$	$x_5 + x_1x_2 + x_1x_2x_4$	$(1, 16, 0, 54, 86)$
all	$x_3 + x_1x_4 + x_1x_2x_4$	$(1, 16, 0, 54, 94)$
odd	$x_2 + x_3 + x_4 + x_5 + x_2x_3 + x_1x_4 + x_1x_2x_4$	$(1, 32, 0, 24, 50)$
odd	$x_3 + x_2x_4 + x_1x_2x_4$	$(1, 16, 0, 54, 86)$
odd	$x_5 + x_2x_4 + x_1x_2x_4$	$(1, 16, 0, 54, 94)$
$n \nmid 6$	$x_4 + x_5 + x_2x_4 + x_3x_4 + x_1x_2x_4$	$(1, 32, 0, 28, 96)$
odd	$x_3 + x_4 + x_1x_4 + x_4x_5 + x_1x_2x_4$	$(1, 32, 0, 28, 80)$
odd	$x_4 + x_1x_5 + x_1x_2x_5$	$(1, 16, 0, 56, 100)$
7	$x_4 + x_2x_5 + x_1x_2x_5$	$(1, 16, 0, 56, 100)$
7	$x_1 + x_2 + x_3 + x_4 + x_5 + x_1x_3 + x_2x_5 + x_3x_5 + x_1x_2x_5$	$(1, 32, 0, 30, 30)$
$n \nmid 3$	$x_1 + x_2x_3 + x_2x_3x_4$	$(1, 16, 0, 56, 100)$
$n \nmid 3$	$x_5 + x_2x_3 + x_2x_3x_4$	$(1, 16, 0, 56, 100)$
odd	$x_2 + x_1x_3 + x_1x_3x_4$	$(1, 16, 0, 54, 86)$
odd	$x_5 + x_1x_3 + x_1x_3x_4$	$(1, 16, 0, 54, 90)$
all	$x_2 + x_1x_4 + x_1x_3x_4$	$(1, 16, 0, 54, 94)$
$n \nmid 4$	$x_5 + x_1x_4 + x_1x_3x_4$	$(1, 16, 0, 54, 90)$
$6, 7, 11$	$x_5 + x_3x_4 + x_1x_3x_4$	$(1, 16, 0, 54, 90)$
odd	$x_1 + x_3 + x_4 + x_1x_2 + x_1x_3 + x_4x_5 + x_1x_3x_4$	$(1, 40, 0, 24, 56)$
odd	$x_1 + x_5 + x_1x_2 + x_2x_3 + x_1x_4 + x_4x_5 + x_1x_3x_4$	$(1, 40, 0, 24, 52)$

References

[1] D. Bini, G. M. Del Corso, G. Manzini, and L. Margara, Inversion of circulant matrices over $\mathbb{Z}_m$. *Math. Comp.* 70 (2001), 1169–1182.

[2] C. Carlet. Boolean Functions for Cryptography and Coding Theory. Cambridge University Press, 2021.

[3] T. W. Cusick and Y. Cheon. Counting balanced Boolean functions in n variables with bounded degree. *Experimental Math.* 16:1 (2007), 101–105.

[4] J. Daemen. Cipher and hash function design strategies based on linear and differential cryptanalysis. PhD thesis, KU Leuven, 1995. `https://cs.ru.nl/~joan/papers/JDA_Thesis_1995.pdf`.

[5] P.J. Davis, Circulant Matrices, John Wiley and Sons, New York, 1979.

[6] L. Grassi, D. Khovratovich, S. Rønjom, and M. Schofnegger. The Legendre symbol and the modulo-2 operator in symmetric schemes over $\mathbb{F}_p^n$. to appear in *IACR Trans. Symmetric Cryptology*, 2022; Cryptology ePrint Archive, Report 2021/1533, 2021. `https://ia.cr/2021/1533`.

[7] G. A. Hedlund Endomorphisms and automorphisms of the shift dynamical system. *Math. Systems Theory* 3 (1969), 320–375.

[8] A. W. Ingleton, The rank of circulant matrices. *J. Lond. Math. Soc.* s1-31 (4) (1956) 445–460.

[9] J. Kari, Reversible Cellular Automata: From Fundamental Classical Results to Recent Developments. *New Gener. Comput.* 36 (2018), 145–172.

[10] S. Kavut, Results on rotation-symmetric S-boxes. *Information Sciences* 201 (2012), 93–113.

[11] F. J. MacWilliams, Orthogonal circulant matrices over finite fields and how to find them. *J. Combin. Theory - Ser.* A 10 (1971), 1–17.

[12] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes (North-Holland, Amsterdam, 1977).

[13] L. Mariot, S. Picek, D. Jakobovic, and A. Leporati. Cellular automata based S-boxes. *Cryptogr. Commun.* 11 (2019), 41–62.

[14] L. Mariot, S. Picek, D.Jakobovic, and A. Leporati. Evolutionary algorithms for designing reversible cellular automata. *Genetic Programming and Evolvable Machines* 22 (2021), 429–461.

[15] Y. N. Patt. Injections of Neighborhood Size Three and Four on the Set of Configurations from the Infinite One-Dimensional Tessellation Automata of Two-State Cells. *US Army Electronics Command, Fort Monmouth, NJ* (1972).

[16] T. Toffoli and N. H. Margolus. Invertible cellular automata: a review. *Phys. D* 45 (1990), 229–253.

[17] J.-Q. Wang and C.-Z. Dong, Inverse matrix of symmetric circulant matrix on skew field. *Int. J. Algebra* 1 (11) (2007), 541–546.

Digital Defense Department, Norwegian National Security Authority, NO-1306 Sandvika, Norway

Email address: tron.omland@gmail.com

Department of Applied Mathematics, Naval Postgraduate School, Monterey, CA 93943-5212, U.S.A.;

Email address: pstanica@nps.edu