This is a post-peer-review, pre-copyedit version of an article published in Designs, Codes and Cryptography. The final authenticated version is available online at: https://doi.org/10.1007/s10623-022-01097-1

Bent Functions in the Partial Spread Class Generated by Linear Recurring Sequences

Maximilien Gadouleau[1], Luca Mariot[2], and Stjepan Picek[2]

[1]Department of Computer Science, Durham University, South Road, Durham, DH1 3LE, UK
m.r.gadouleau@dur.ac.uk

[2]Digital Security Group, Radboud University, PO Bus 9010, Nijmegen, 6500 GL, The Netherlands
{luca.mariot, stjepan.picek}@ru.nl

August 27, 2022

Abstract

We present a construction of partial spread bent functions using subspaces generated by linear recurring sequences (LRS). We first show that the kernels of the linear mappings defined by two LRS have a trivial intersection if and only if their feedback polynomials are relatively prime. Then, we characterize the appropriate parameters for a family of pairwise coprime polynomials to generate a partial spread required for the support of a bent function, showing that such families exist if and only if the degrees of the underlying polynomials are either 1 or 2. We then count the resulting sets of polynomials and prove that, for degree 1, our LRS construction coincides with the Desarguesian partial spread. Finally, we perform a computer search of all $\mathcal{PS}^-$ and $\mathcal{PS}^+$ bent functions of $n = 8$ variables generated by our construction and compute their 2-ranks. The results show that many of these functions defined by polynomials of degree $d = 2$ are not EA-equivalent to any Maiorana-McFarland or Desarguesian partial spread function.

Keywords bent functions, partial spreads, cyclic codes, linear recurring sequences, polynomials

1 Introduction

Boolean functions play an essential role in cryptography, coding theory, and combinatorial designs [15]. Among them, *bent functions* are of particular interest since they lie at the highest possible Hamming distance from the set of all affine functions, or equivalently they reach the highest possible nonlinearity. Even though bent

functions are unbalanced, highly nonlinear balanced functions can be derived from them [8]. For this reason, bent functions have been used in the past for designing stream and block ciphers since highly nonlinear Boolean functions are useful to withstand fast-correlation and linear cryptanalysis attacks [4]. Besides cryptography, bent functions are also studied in coding theory, as they are connected to the *covering radius* of first-order Reed-Muller codes, whose codewords are affine functions.

Over the last decades, many constructions of bent functions have been described in the related literature (see, e.g., [3, 15, 4] for a survey of the main ones). A distinction is usually made between *primary* and *secondary* constructions. Primary constructions build sets of bent functions from scratch, usually by leveraging on related combinatorial structures. Some of the most well-known primary constructions for bent functions include the *Maiorana-McFarland construction* [14], which exploits permutations over $\mathbb{F}_2^n$, and *Dillon's construction* [7], based on the class of *partial spreads* $\mathcal{PS}$. On the contrary, *secondary constructions* build new bent functions starting from existing ones. For example, the *Rothaus's construction* [17] takes three bent functions of n variables whose sum is also bent and yields a bent function of $n+2$ variables.

The search for novel methods to design bent functions is still an interesting and active research area nowadays, for a twofold motivation:

- *Discovering new functions*. Notwithstanding the multitude of existing constructions, they only cover a tiny fraction of the total number of bent functions [15], and the complete enumeration of bent functions remains an open question for $n \geq 10$ variables [16]. Therefore, finding new constructions that yield previously unknown bent functions is still an interesting research avenue to pursue. However, one must remark that this direction is becoming increasingly difficult precisely because many constructions are already in place. This makes the discovery of new bent functions both unlikely and cumbersome since, in principle, one has to check inequivalence against a large number of known classes.

- *Finding new constructions for known functions*. Novel constructions that generate already known bent functions are an interesting research line as well, for several reasons. For example, from an implementation point of view, such constructions could highlight more efficient ways to design the corresponding bent functions other than by classic lookup tables. More generally, a novel construction could provide a new perspective on understanding the structure of a known class of bent functions and spawning new research questions linked both to the construction of new bent functions and other interesting combinatorial objects. As we will argue in the following, we deem our work an example of this approach.

In this paper, we present a new primary construction of bent functions in the partial spread class $\mathcal{PS}$ by using the subspaces spanned by *Linear Recurring*

Sequences (LRS) over finite fields. The main idea is to define a linear mapping through the feedback polynomial of an LRS and then to use its kernel as a subspace in a partial spread. The main contributions of this paper can be summarized as follows:

- We prove that the kernels of two linear mappings have a trivial intersection if and only if the feedback polynomials of their LRS are pairwise coprime.
- We show that a family of pairwise coprime polynomials large enough to define a partial spread for a bent function exists if and only if the degree of the involved polynomials is either $d = 1$ or $d = 2$, assuming that all polynomials have a nonzero constant term.
- We prove that for degree $d = 1$, the functions given by our LRS construction coincide with the Desarguesian partial spread class.
- We perform a computer search of all bent functions of $n = 6, 8$ variables generated by our LRS construction, remarking that they always have maximal degree $n/2$. While for $\mathcal{PS}^-$ functions this is expected, the reason for $\mathcal{PS}^+$ functions lies in the fact that the corresponding partial spreads are not maximal.
- We analyze the distribution of the 2-ranks for the LRS bent functions of $n = 8$ variables. For degree $d = 1$, we independently verify and extend the distribution reported by Weng et al. [19] for functions in the Desarguesian partial spread. For degree $d = 2$, we remark that many of the obtained bent functions have a rank higher than 42. Thus, they are not EA-equivalent to any Maiorana-McFarland or Desarguesian partial spread function.

The remainder of this work is structured as follows. Section 2 reviews the background definitions on bent functions and linear recurring sequences. Section 3 defines our LRS construction, proving that the kernels of two LRS linear mappings have a trivial intersection if and only if the associated feedback polynomials are coprime. Section 4 characterizes the families of pairwise coprime polynomials that are required for the LRS construction and provides the corresponding counting result. Section 5 shows that the LRS construction equals the Desarguesian partial spread construction when using polynomials of degree 1. Section 6 discusses the computer search experiments for bent functions of $n = 6, 8$ variables generated by the LRS construction, reporting the distribution of the 2-ranks. Finally, Section 7 summarizes the main results of this paper, points out several avenues for future research, and discusses the connection with the cellular automata approach used in [9].

2 Background

This section covers the necessary background notions used throughout the paper. We begin by introducing the basic definitions and results related to bent Boolean

functions, describing the main known primary constructions (namely, the Maiorana-McFarland construction and Dillon's partial spread class), the extended affine equivalence relation, and a method to check the inequivalence of a bent function against a class of other known functions. We then move to linear recurring sequences and their vector spaces, representing the main combinatorial objects used to define our new construction of bent functions.

2.1 Bent Functions

We refer the reader to [4] for a thorough treatment of the results recalled in this section about Boolean functions. In what follows, let $\mathbb{F}_q$ be the finite field with q elements (where $q = p^\alpha$ is a power of a prime number) and denote by $\mathbb{F}_q^n$ the n-dimensional vector space over $\mathbb{F}_q$, with $\underline{0}$ being its null vector. For $q = 2$, sum and multiplication on $\mathbb{F}_2$ correspond to the XOR and logical AND operations, respectively. Following the literature convention about Boolean functions, we will denote the sum operation over $\mathbb{F}_2$ by $\oplus$, while for a generic finite field $\mathbb{F}_q$ we will adopt the normal sum symbol $+$. On the other hand, we will denote the multiplication operation in all finite fields by concatenation of the operands. A *Boolean function* of n variables is a mapping $f : \mathbb{F}_2^n \to \mathbb{F}_2$. The most natural way to uniquely represent a Boolean function f is by means of its *truth table*, which is the vector $\Omega_f \in \mathbb{F}_2^{2^n}$ that lists the output of f evaluated over all 2^n input vectors $x \in \mathbb{F}_2^n$ in lexicographic order. The *support* of f is the subset of input vectors that map to 1, that is, $supp(f) = \{x \in \mathbb{F}_2^n : f(x) \neq 0\}$, while the *Hamming weight* of f is defined as $w_H(f) = |supp(f)|$, i.e., the number of ones in the truth table of f. Functions with the Hamming weight equal to $w_H = 2^{n-1}$ are also called balanced since their truth table is composed of an equal number of zeros and ones, and they play an important role in the design of stream and block ciphers [4]. The *polarity truth table* $\Omega_{\hat{f}}$ of $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is the truth table of the function $\hat{f} : \mathbb{F}_2^n \to \{-1, +1\}$ defined as $\hat{f}(x) = (-1)^{f(x)}$ for all $x \in \mathbb{F}_2^n$.

The *Algebraic Normal Form* (ANF) is another useful representation that expresses a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ as a multivariate polynomial over the quotient ring $\mathbb{F}_2[x_1, \cdots, x_n]/(x_1^2 \oplus x_1, \cdots, x_n^2 \oplus x_n)$:

$$P_f(x) = \bigoplus_{I \in \mathcal{P}([n])} a_I \left(\prod_{i \in I} x_i \right) \quad , \tag{1}$$

with $\mathcal{P}([n]) = 2^{[n]}$ being the power set of $[n] = \{1, \cdots, n\}$, and a_I being the coefficient of the monomial defined by the subset $I \in \mathcal{P}([n])$. The *algebraic degree* of f is defined as the cardinality of the largest subset I such that $a_I \neq 0$. In particular, *affine functions* are defined as those Boolean functions with degree at most 1. Notice that the ANF is a unique representation of a Boolean function, and in particular, one can retrieve the truth table back from the ANF coefficients through the *Möbius*

transform:

$$f(x) = \bigoplus_{I \in \mathcal{P}[n]: I \subseteq supp(x)} a_I \ , \tag{2}$$

A third common method to uniquely represent Boolean functions used in cryptography is the *Walsh-Hadamard transform*. Formally, the Walsh-Hadamard transform of a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is the mapping $W_f : \mathbb{F}_2^n \to \mathbb{Z}$ defined for all $a \in \mathbb{F}_2^n$ as

$$W_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus a \cdot x} \ , \tag{3}$$

where $a \cdot x = \bigoplus_{i=1}^{n} a_i x_i$ is the *scalar product* between a and x. One may easily see that a function f is balanced if and only if its Walsh-Hadamard transform vanishes on the null vector, i.e., if and only if $W_f(\underline{0}) = 0$. In particular, the Walsh-Hadamard coefficient $W_f(a)$ quantifies the correlation between f and the linear function $a \cdot x$. The lower the absolute value of $W_f(a)$, the lower will be the correlation of f from $a \cdot x$ (and from its affine counterpart $1 \oplus a \cdot x$), and thus the higher will be the Hamming distance between the truth tables of the two functions. In particular, the *nonlinearity* of a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is defined as the minimum Hamming distance of f from the set of all affine functions, and it can be computed as follows:

$$Nl_f = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} (|W_f(a)|) \ . \tag{4}$$

Therefore, a Boolean function with high nonlinearity must be characterized by a low maximum absolute value among its Walsh-Hadamard coefficients. *Parseval's relation* states that the sum of the squared Walsh-Hadamard spectrum is constant for any Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, and it equals:

$$\sum_{a \in \mathbb{F}_2^n} [W_f(a)]^2 = 2^{2n} \ . \tag{5}$$

From Parseval's relation, one can remark that the lowest maximum absolute value of the Walsh-Hadamard transform occurs when the constant 2^{2n} is uniformly "spread" among all 2^n coefficients, that is, when each coefficient in absolute value equals $2^{\frac{n}{2}}$. This observation yields the *covering radius bound* for the nonlinearity of an n-variable Boolean function:

$$Nl_f \leq 2^{n-1} - 2^{\frac{n}{2}-1} \ . \tag{6}$$

Functions satisfying with equality Equation (6) – or equivalently, whose Walsh-Hadamard coefficients all equal $2^{\frac{n}{2}}$ in absolute value – are called *bent functions*. Such functions exist only when n is even since the Walsh-Hadamard coefficients must be integer numbers. Although achieving the highest possible nonlinearity granted by the covering radius bound, bent functions cannot be employed directly in the design of stream or block ciphers since they are always unbalanced. As a matter of fact, we have $W_f(\underline{0}) = \pm 2^{\frac{n}{2}}$ for any bent function, which means that its Hamming weight is $2^{n-1} \pm 2^{\frac{n}{2}-1}$.

There are several ways to construct bent functions proposed in the literature. Usually, such methods are divided in *primary* and *secondary constructions*. Recall that a primary construction builds "from scratch" new bent functions by leveraging other kinds of combinatorial objects. On the other hand, a secondary construction derives new bent functions starting from already existing ones. This paper focuses on the former case.

One of the main primary constructions investigated in the literature is the *Maiorana-McFarland construction*, which is the set $\mathcal{M}$ of all Boolean functions $f : \mathbb{F}_2^n \to \mathbb{F}_2$, with $n = 2m$, defined as:

$$f(x,y) = x \cdot \pi(y) \oplus g(y) \quad , \tag{7}$$

for all $x, y \in \mathbb{F}_2^m$, where $\pi : \mathbb{F}_2^m \to \mathbb{F}_2^m$ is any permutation of $\mathbb{F}_2^m$ and g is any Boolean function on $\mathbb{F}_2^m$. Therefore, for any $m \in \mathbb{N}$ there are $(2^m)! \cdot 2^{2^m}$ bent functions of $2m$ variables in $\mathcal{M}$.

A second well-known primary construction that gives rise to a large number of bent functions was introduced by Dillon in his PhD thesis [7], and it is based on *partial spreads*. A partial spread of $\mathbb{F}_2^n$, with $n = 2m$, is a family P of m-dimensional subspaces $S_1, S_2, \cdots, S_t \subseteq \mathbb{F}_2^n$ with pairwise trivial intersection (i.e., for all $i \neq j$ one has $S_i \cap S_j = \{\underline{0}\}$). Further, a partial spread is a *spread* if the union of its subspaces results in the whole space $\mathbb{F}_2^n$. The main result proved by Dillon is that one can construct a bent function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, with $n = 2m$, from a partial spread P of $\mathbb{F}_2^n$ by defining the support of f as the *union* of the subspaces in P. Remark that the partial spread must be large enough to reach the Hamming weight required for a bent function. In particular, a bent function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, $n = 2m$, belongs to the class $\mathcal{PS}^-$ if $f(0) = 0$ and its support is the union of $t = 2^{m-1}$ subspaces of a partial spread P of $\mathbb{F}_2^n$. Functions in the $\mathcal{PS}^-$ class reach the maximum possible algebraic degree for a bent function of $n = 2m$ variables, namely m. Bent functions belonging to the class $\mathcal{PS}^+$ are defined similarly, with $f(0) = 1$ and their support being the union of $t = 2^{m-1} + 1$ m-dimensional subspaces of a partial spread of $\mathbb{F}_2^n$. The union of $\mathcal{PS}^-$ and $\mathcal{PS}^+$ gives the whole partial spread class $\mathcal{PS}$. We formally summarize this in the following definition:

Definition 1. *Let $n = 2m$. A bent function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is of type $\mathcal{PS}^-$ (respectively, $\mathcal{PS}^+$) if its support is defined as:*

$$supp(f) = \bigcup_{S \in P} (S \setminus \{\underline{0}\}) \quad \left(\textit{respectively, } supp(f) = \bigcup_{S \in P} S \right) \quad , \tag{8}$$

where P is a partial spread of size 2^{m-1} (respectively, $2^{m-1} + 1$).

Hence, from a practical point of view, the support of a $\mathcal{PS}^+$ function is obtained by taking the union of the elements in the partial spread. For a $\mathcal{PS}^-$ function, the support is also the union, with the exception that the null vector is always discarded from the elements in the partial spread.

Contrarily to $\mathcal{PS}^-$, functions in $\mathcal{PS}^+$ can have algebraic degrees other than m. More precisely, this depends on whether a $\mathcal{PS}^+$ function is defined by a *non-maximal* partial spread (i.e., a partial spread that can be extended by adjoining another subspace) or not. In the former case, the resulting $\mathcal{PS}^+$ function also has degree m. In the latter, the degree might be different, and in particular, when m is even, $\mathcal{PS}^+$ contains the quadratic bent functions. We summarize the relationship between algebraic degree and $\mathcal{PS}$ bent functions in the result below, whose proof can be found in Dillon's thesis [7]:

Proposition 1. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$, with $n = 2m$, be a bent function in the partial spread class $\mathcal{PS}$. Then, the following hold:*

- *If $f \in \mathcal{PS}^-$, then f has algebraic degree m.*
- *If $f \in \mathcal{PS}^+$ and its partial spread is not maximal, then f has degree m.*

Currently, the structure of the class $\mathcal{PS}$ is still far from being completely characterized, and several methods have been investigated to define partial spreads that are large enough to obtain $\mathcal{PS}^-$ and $\mathcal{PS}^+$ bent functions. Here, we introduce only the *Desarguesian spread*, which is perhaps the best-known example of spread used to construct $\mathcal{PS}^-$ bent functions (see, e.g., [6] for a general overview of other partial spreads). Given $n = 2m$, one can use the *bivariate form* to represent the Desarguesian spread [15]. The vector space $\mathbb{F}_2^n$ is identified with the Cartesian product $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, and the Desarguesian spread is defined as:

$$\begin{aligned} DS &= \{E_a \subseteq \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} : \ a \in \mathbb{F}_{2^m}\} \cup E_\infty \ \text{, where :} \\ E_a &= \{(x, ax) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} : \ x \in \mathbb{F}_{2^m}\} \ , \\ E_\infty &= \{(0, y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} : \ y \in \mathbb{F}_{2^m}\} \ . \end{aligned} \tag{9}$$

Then, any subset of 2^{m-1} elements of DS is a partial spread whose union defines the support of a bent function. More in particular, these functions belong to the so-called class $\mathcal{PS}_{ap}$ (where ap stands for "affine plane"), which is a subset of $\mathcal{PS}^-$. Besides reaching maximal degree $n/2$, functions in the $\mathcal{PS}_{ap}$ class have the additional interesting property of being *hyper-bent*, as shown, e.g., in [5]. A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$, n even, is called hyper-bent if the function $f(x^i)$ is bent for all exponent i coprime with $2^n - 1$ [20]. As such, hyper-bent functions have the highest possible distance not only from all affine functions (which corresponds to the case $i = 1$) but also from all *bijective monomial functions*.

Given the great variety of primary constructions available in the literature, a crucial question when investigating a new construction is to assess whether the bent functions produced by it are essentially different from those belonging to other known classes. This is accomplished by using equivalence relations. The underlying idea is to classify the bent functions produced by the known constructions up to equivalence and then verify if the bent functions generated by a new construction belong to any of these classes or to different ones. The main equivalence relation

used in this context is the *extended affine equivalence* (EA-equivalence). Two Boolean functions $f, g : \mathbb{F}_2^n \to \mathbb{F}_2$ are EA-equivalent if there exists a linear permutation $L : \mathbb{F}_2^n \to \mathbb{F}_2^n$, two vectors $u, v \in \mathbb{F}_2^n$, and an element $c \in \mathbb{F}_2$ such that, for all $x \in \mathbb{F}_2^n$,

$$g(x) = f(L(x) \oplus u) \oplus (v \cdot x) \oplus c \quad . \tag{10}$$

A bent function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, with $n = 2m$, belongs to the *completed Maiorana-McFarland class* $\mathcal{M}^\#$ if it is EA-equivalent to a function in $\mathcal{M}$.

One possible method to check the EA-inequivalence of a function against other classes resorts to the notion of rank, introduced by Weng et al. [19]. More precisely, the 2-rank of a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is the rank of the $2^n \times 2^n$ binary matrix A_f whose rows and columns are indexed by the vectors of $\mathbb{F}_2^n$, and which is defined as $A_f(x,y) = f(x \oplus y)$ for all $x, y \in \mathbb{F}_2^n$. In particular, if f is a bent function, then A_f is the incidence matrix of a symmetric 2-design, and it is called the *translate design* of the difference set, which is the support of f. Weng et al. proved that EA-equivalent bent functions have the same rank. Therefore, one can prove that two bent functions are not equivalent by checking that their ranks differ. The paper by Weng et al. further characterizes the lower and upper bounds for different types of bent functions. In particular, the rank of any Maiorana-McFarland bent function of $n = 2m$ variables ranges between $LB_{\mathcal{M}} = 2m + 2$ and $UB_{\mathcal{M}} = 2^{m+1} - 2$. On the other hand, bent functions defined over the Desarguesian partial spread have ranks between $LB_{DS} = 2^{m+1} - 2$ and $UB_{DS} = \sum_{i=0}^{m} \binom{m}{i} 2^{\min\{i, m-i\}}$. An interesting consequence of the fact that the two intervals overlap only on $2^{m+1} - 2$ is that almost all bent functions arising from the Desarguesian partial spread class are inequivalent to any Maiorana-McFarland function. Moreover, one can show that a bent function is inequivalent to all Maiorana-McFarland and Desarguesian spread functions by showing that its rank is higher than UB_{DS}.

2.2 Linear Recurring Sequences

This section covers only the basic notions of linear recurring sequences essential to present our construction. An excellent overview of this topic can be found in the book by Lidl and Niederreiter on finite fields [11].

Let $d \in \mathbb{N}$, and $a, a_0, \cdots, a_{d-1} \in \mathbb{F}_q$. A sequence $\{x_i\}_{i \in \mathbb{N}}$ of elements in $\mathbb{F}_q$ is called a *linear recurring sequence* (LRS) of order d if it satisfies the following relation:

$$a + a_0 x_i + a_1 x_{i+1} + \ldots + a_{d-1} x_{i+d-1} = x_{i+d} \quad , \tag{11}$$

for all $i \in \mathbb{N}$. The first d elements $x_0, \cdots, x_{d-1}$ act as the *initial values* of the sequence, while all subsequent ones are determined by applying the linear recurrence defined in Equation (11). In what follows, we will assume that $a = 0$, i.e., that the LRS is *homogeneous*, and that $\mathbb{F}_q$ is a field of characteristic 2. In this case, the *feedback polynomial* of the LRS (11) can be defined as:

$$f(X) = a_0 + a_1 X + \cdots a_{d-1} X^{d-1} + X^d \quad , \tag{12}$$

that is, $f(X)$ is the monic polynomial in $\mathbb{F}_q[X]$ of degree d whose monomials are defined by the coefficients of the LRS.

It is known that the family $S(f(X))$ of all sequences $\{x_i\}$ satisfying the linear recurrence with feedback polynomial $f(X)$ as in (12) forms a d-dimensional vector space over $\mathbb{F}_q$ (see Chapter 6, Section 5 in [11]). In this work, we consider the projection of such sequences onto their first $2d$ coordinates. Therefore, we obtain a subspace $S_f \subseteq \mathbb{F}_q^{2d}$ of dimension d which is the kernel of the linear map $F : \mathbb{F}_q^{2d} \to \mathbb{F}_q^d$ defined as:

$$F(x_0, \cdots, x_{2d-1})_i = a_0 x_i + a_1 x_{i+1} + \ldots + a_{d-1} x_{i+d-1} + x_{i+d} \ , \tag{13}$$

for all output coordinates $i \in \{0, \cdots, d-1\}$. Since the map F is linear, we can describe it as $F(x) = M_F \cdot x^\top$, where M_F is the $d \times 2d$ matrix of the form:

$$M_F = \begin{pmatrix} a_0 & \cdots & a_{d-1} & 1 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & a_0 & \cdots & a_{d-1} & 1 & 0 & \cdots & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & a_0 & \cdots & a_{d-1} & 1 \end{pmatrix} \ , \tag{14}$$

Therefore, we can compactly represent the linear map F by the coefficients of the feedback polynomial f, i.e., $f \mapsto M_F$. Notice that M_F has the form of the *parity-check matrix* of a cyclic code, with f playing the role of the *parity check polynomial*. However, the code associated with f is not cyclic in general. This happens, in particular, if and only if the *generator polynomial* (which is defined as the reciprocal of f) divides $X^N - 1$, where $N = 2d$. On the other hand, evaluating F on a particular vector $x \in \mathbb{F}_q^{2d}$ corresponds to computing the *syndrome* of x. In what follows, we will also consider the special cases where the feedback polynomial is respectively X^d and 1. The former is still a feedback polynomial of degree d—although not a typical one—and thus, the definition of the $d \times 2d$ matrix in Equation (14) still holds. In particular, the linear map F is defined by the matrix $M_F = [0|I]$, where I denotes the $d \times d$ identity matrix; the corresponding kernel is the subspace $\{(x_0, \cdots, x_{d-1}, 0, \cdots, 0) : x_i \in \mathbb{F}_q\}$, i.e. all those vectors whose right half is set to 0. On the other hand, the case $f(X) = 1$ is different since here we have a polynomial of degree 0. However, we can still define a $d \times 2d$ matrix with $d \geq 1$ of the form (14) as $M_F = [I|0]$. The function F maps each vector of dimension $2d$ to its first d coordinates. Therefore, symmetrically to the case of X^d, the kernel of the linear map for $f(X) = 1$ is the subspace $\{(0, \cdots, 0, x_d, \cdots x_{2d-1}) : x_i \in \mathbb{F}_q\}$, that is, all vectors whose left half is set to 0.

Remark 1. *Suppose that we have a feedback polynomial $g(X)$ of degree $d \geq 1$ and $f(X) = 1$. Then, the kernels of the linear maps G and F respectively defined by $g(X)$ and $f(X)$ have a trivial intersection. In fact, the rightmost d coordinates of the vectors in the kernel of F are linear functions of the leftmost d ones. The only vector in this kernel that also has its left half equal to 0 is thus the null vector.*

As a final note, remark that F may also be regarded as a linear *cellular automaton* (CA) [13]. The connection between the LRS used here to define bent functions, and the CA approach will be briefly discussed in the conclusions.

3 The LRS Construction

The first step of our construction requires characterizing when the kernels of two LRS subspaces have a trivial intersection. The next result shows that this is equivalent to computing the greatest common divisor of the respective feedback polynomials.

Lemma 1. *Let $f,g \in \mathbb{F}_q[X]$ be two polynomials over $\mathbb{F}_q$ both of degree $d \geq 1$, respectively defined as:*

$$f(X) = a_0 + a_1 X + \cdots + a_{d-1}X^{d-1} + X^d \ , \tag{15}$$

$$g(X) = b_0 + b_1 X + \cdots + b_{d-1}X^{d-1} + X^d \ , \tag{16}$$

with $a_i, b_i \in \mathbb{F}_q$. Further, let $F,G : \mathbb{F}_q^{2d} \to \mathbb{F}_q^d$ be the linear maps defined by the polynomials f and g, respectively. Then, the kernels of F and G have trivial intersection if and only if $\gcd(f,g) = 1$*, i.e., if and only if f and g are coprime.*

Proof. The linear maps F and G are respectively defined as $F(x) = M_F \cdot x^\top$ and $G(x) = M_G \cdot x^\top$ for all $x \in \mathbb{F}_q^{2d}$, where M_F and M_G are the two $d \times 2d$ matrices of the form (14). Define now the linear function $H : \mathbb{F}_q^{2d} \to \mathbb{F}_q^{2d}$ as $H = M_H \cdot x^\top$ for all $x \in \mathbb{F}_q^{2d}$, where

$$M_H = \begin{pmatrix} M_F \\ M_G \end{pmatrix} = \begin{pmatrix} a_0 & \cdots & a_{d-1} & 1 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & a_0 & \cdots & a_{d-1} & 1 & 0 & \cdots & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & a_0 & \cdots & a_{d-1} & 1 \\ b_0 & \cdots & b_{d-1} & 1 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & b_0 & \cdots & b_{d-1} & 1 & 0 & \cdots & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & b_0 & \cdots & b_{d-1} & 1 \end{pmatrix} . \tag{17}$$

In other words, the matrix M_H is simply the *superposition* of the two matrices M_F and M_G. It is clear that the nullspace of M_H is the intersection of the nullspaces of M_F and M_G. Hence, the kernels of F and G have trivial intersection if and only if M_H is invertible. Remark that M_H is also the *Sylvester matrix* of the polynomials f and g. It is a well-known fact that the determinant of the Sylvester matrix (also called the *resultant* in this context) is nonzero if and only if f and g do not have a common factor [10]. Therefore, one has that $ker(F) \cap ker(G) = \{\underline{0}\}$ if and only if f and g are coprime. □ □

Consequently, we need to find a family of pairwise coprime polynomials that is large enough to define a bent function. Following what we recalled in Section 2.1, for a $\mathcal{PS}^-$ function we need $t = 2^{m-1}$ coprime polynomials of degree d. To this aim, let us take the finite field $\mathbb{F}_q$ with $q = 2^l$, for $l \in \mathbb{N}$. This is because a partial spread for a bent function must be defined over the vector space $\mathbb{F}_2^n$, $n = 2m$. In particular, each vector $x \in \mathbb{F}_{2^l}^{2d}$ must also be converted into a corresponding binary vector $x \in \mathbb{F}_2^n$ since the union of the vectors in the partial spread will form the support of the bent function. In other words, we require that $ld = m$. By identifying $\mathbb{F}_{2^l}$ with the vector space $\mathbb{F}_2^l$, a vector x in $\mathbb{F}_{2^l}^{2d}$ is a $2d$-tuple whose components are in turn binary l-tuples:

$$x = ((x_{0,0}, \cdots, x_{0,l-1}), \cdots, (x_{2d-1,0}, \cdots, x_{2d-1,l-1})) \ . \tag{18}$$

We now associate to each element $x \in \mathbb{F}_{2^l}^{2d}$ an element of $\mathbb{F}_2^{2ld}$ through the *flattening* operator $\varphi : \mathbb{F}_{2^l}^{2d} \to \mathbb{F}_2^{2ld}$, which simply drops the parentheses inside the vector representation of x:

$$\varphi(x) = (x_{0,0}, \cdots, x_{0,l-1}, \cdots, x_{2d-1,0}, \cdots, x_{2d-1,l-1}) \ . \tag{19}$$

It is then easy to see that φ is bijective. We can now characterize the partial spreads arising from our construction:

Theorem 1. *Let $m, l, d \in \mathbb{N}$ such that $m = ld$. If there are $t = 2^{ld-1}$ (respectively, $t = 2^{ld-1} + 1$) coprime polynomials of degree $d \geq 1$ over $\mathbb{F}_q$ where $q = 2^l$, possibly including the constant polynomial 1 of degree 0, then there exists a partial spread P over $\mathbb{F}_2^n$, $n = 2m$, whose union of its subspaces with the null vector discarded (respectively, with the null vector included) defines a bent function in the class $\mathcal{PS}^-$ (respectively, $\mathcal{PS}^+$).*

Proof. Let us first consider the case where $f_1, \cdots, f_t$ are all coprime polynomials of degree $d \geq 1$ over $\mathbb{F}_q$, and let $F_1, \cdots, F_t : \mathbb{F}_q^{2d} \to \mathbb{F}_q^d$ be the corresponding linear maps associated to them. Define the following family of subspaces of $\mathbb{F}_2^n$, with $n = 2m = 2ld$:

$$P = \{\Phi(ker(F_i)) \subseteq \mathbb{F}_2^n : 1 \leq i \leq t\} \ , \tag{20}$$

where $\Phi(ker(F_i)) = \{y \in \mathbb{F}_2^n : y = \varphi(x), x \in ker(F_i)\}$, for $1 \leq i \leq t$. In other terms, the subspace $\Phi(ker(F_i))$ is obtained by taking the kernel of F_i and applying the flattening operator to each vector in it. Since the polynomials $f_1, \cdots, f_t$ are pairwise coprime, by Lemma 1, the kernels of the F_i have pairwise trivial intersection. Clearly, the same property holds for the subspaces $\Phi(ker(F_i))$ in P since they are just a different representation of the same kernels through the flattening operator. Therefore, P is a partial spread over $\mathbb{F}_2^n$, and depending on its size ($t = 2^{ld-1}$ or $t = 2^{ld-1} + 1$), it can be used to define the support of a $\mathcal{PS}^-$ or $\mathcal{PS}^+$ bent function as per Definition 1.

Suppose now that one of the t polynomials is $f_i(X) = 1$, while all others $f_j(X)$ for $j \neq i$ are pairwise coprime polynomials of degree $d \geq 1$. By Remark 1, the

kernel of F_i has trivial intersection with the kernel of F_j for all $j \neq i$. Thus, one can construct a partial spread also in this case using Equation (20). □ □

An alternative way of considering the inclusion of the constant polynomial $f(X) = 1$ in Theorem 1 is that one can define a variant of the Sylvester resultant for two polynomials of different degrees $e < d$, with $d \geq 1$, such that the corresponding matrix still has size $2d \times 2d$. The idea, explained by Sylvester in [18, pp. 425–426], is to augment the matrix of the linear map related to the polynomial of smaller degree e by postpending $d - e$ ghost terms equal to zero in the first row and then sliding as usual to construct the rows below. Equivalently, in the polynomial notation the additional ghost terms are $0 \cdot x^i$ for $e + 1 \leq i \leq d$. This is precisely how we defined the matrix in Section 2.2 for $f(X) = 1$, i.e. as $M_F = [I|0]$.

In the remainder of this section, we show two examples of bent functions obtained through our construction.

Example 1. *Let $m = 2$, $n = 2m = 4$, $l = 1$, and $d = 2$. Since $ld = m$, in this case we need to find $t = 2^{m-1} = 2$ relatively prime polynomials $f_1, f_2 \in \mathbb{F}_2[X]$ of degree $d = 2$ to apply our construction. Let $f_1(X) = X^2 + 1$ and $f_2(X) = X^2 + X + 1$. In this case, there is no need to apply the flattening operator since the ground field for the polynomials is already $\mathbb{F}_2$. The two linear maps $F_1, F_2 : \mathbb{F}_2^4 \to \mathbb{F}_2^2$ are respectively defined by the following two matrices:*

$$M_{F_1} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}, \; M_{F_2} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

The kernels of F_1 and F_2 are the following ones:

$$ker(F_1) = \{0000, 1010, 0101, 1111\},$$
$$ker(F_2) = \{0000, 1011, 0110, 1101\},$$

which clearly have a trivial intersection. Therefore, the union of $ker(F_1)$ and $ker(F_2)$ (excluding the null vector) defines the support of the Boolean function $g : \mathbb{F}_2^4 \to \mathbb{F}_2$ with the following truth table:

$$\Omega_g = (0,0,0,0,0,1,1,0,0,0,1,1,0,1,0,1) \; .$$

The ANF of g is defined as follows:

$$g(x_1, x_2, x_3, x_4) = x_1x_3 \oplus x_2x_3 \oplus x_2x_4.$$

It is possible to verify that this function is bent in a number of ways. For example, by applying the linear transformation $x_4 \leftarrow x_3 \oplus x_4$ the function g is equivalent to the canonical nondegenerate quadratic form $g'(x_1, x_2, x_3, x_4) = x_1x_3 \oplus x_2x_4$, which by Equation (7) *is a Maiorana-McFarland function.*

Example 2. *The bent function g defined in Example 1 belongs to the $\mathcal{PS}^-$ class, since its support is the union of $2^{2-1}=2$ subspaces of dimension 2 with trivial intersection, stripping out the null vector. If we want to obtain a $\mathcal{PS}^+$ function, we need an additional polynomial of degree $d=2$ that is coprime both to f_1 and f_2. To this end, we can select for instance $f_3(X)=X^2$. The kernel of the associated linear map F_3 is as follows:*

$$ker(F_3)=\{0000,0100,1000,1100\} \ ,$$

which again has trivial intersection with both $ker(F_1)$ and $ker(F_2)$. Therefore, we can define a $\mathcal{PS}^+$ bent function $h:\mathbb{F}_2^4\to\mathbb{F}_2$ by setting $h(0000)=1$ and defining the rest of its support as the union of the three kernels minus their trivial intersection. We thus obtain the following truth table:

$$\Omega_h=(1,1,1,1,0,1,1,0,0,0,1,1,0,1,0,1) \ ,$$

with the ANF of h being:

$$h(x_1,x_2,x_3,x_4)=x_1x_2\oplus x_1x_3\oplus x_2x_3\oplus x_2x_4\oplus x_1\oplus x_2\oplus 1 \ .$$

4 Counting Bent Functions in the LRS Construction

Recall from Theorem 1 that, given $m,l,d\in\mathbb{N}$ such that $m=ld$, one can construct a $\mathcal{PS}^-$ (respectively, $\mathcal{PS}^+$) bent function if there are at least $t=2^{ld-1}$ (respectively, $t=2^{ld-1}+1$)) coprime polynomials of degree d over $\mathbb{F}_q$ where $q=2^l$. Thus, the first research question is whether for all even $n\in\mathbb{N}$ there are enough pairwise coprime polynomials to obtain a bent function. In what follows, we focus on the case of monic polynomials with *nonzero constant term* that are pairwise coprime to exploit the counting results proved in [12]. There, the authors proposed construction for such families of polynomials based on the multiplication of two irreducible polynomials of degree k and $d-k$, respectively. In particular, they showed that the maximum size of the families that can be generated through this construction equals:

$$N_d=I_d+\sum_{k=1}^{\lfloor\frac{d}{2}\rfloor}I_k \ . \tag{21}$$

In the formula above, I_k denotes the number of irreducible monic polynomials of degree k and with a nonzero constant term over $\mathbb{F}_q$, which is $I_k=q-1$ for $k=1$, while for $k\geq 2$ it is given by *Gauss's formula*:

$$I_k=\frac{1}{k}\sum_{e|k}\mu(e)\cdot q^{\frac{k}{e}} \ , \tag{22}$$

with μ denoting the *Möbius function*. Further, in [12], it is proved that such construction is optimal, meaning that N_d actually corresponds to the maximum size

attainable by any family of monic coprime polynomials of degree d with a nonzero constant term over $\mathbb{F}_q$. Thus, one can study Equation (21) with respect to the parameters l, d, and m to address the existence question for families of polynomials that satisfy the conditions of Theorem 1. We now characterize such families for the case of $\mathcal{PS}^-$ functions in terms of the degrees of their polynomials:

Theorem 2. *Let $l,d,m \in \mathbb{N}$ such that $ld = m$, and let $q = 2^l$. Then there exists a family of $t = 2^{m-1}$ pairwise coprime polynomials of degree d and nonzero constant term over $\mathbb{F}_q$ if and only if $d \in \{1,2\}$.*

Proof. We need to show that $N_d \geq \frac{1}{2}q^d$ if and only if $d \leq 2$. We first settle the cases of $d \leq 4$ one by one.

For $d = 1$, we obtain

$$N_1 = I_1 = q - 1 \geq \frac{1}{2}q.$$

For $d = 2$, we obtain

$$N_2 = I_2 + I_1 = \frac{1}{2}(q^2 - q) + (q-1) = \frac{1}{2}q^2(1 + q^{-1} - 2q^{-2}) \geq \frac{1}{2}q^2.$$

For $d = 3$, we obtain

$$\begin{aligned} N_3 = I_3 + I_1 &= \frac{1}{3}\left(q^3 - q\right) + (q-1) \\ &< \frac{1}{3}q^3\left(1 + 2q^{-2}\right) \leq \frac{1}{3}q^3\frac{3}{2} \\ &= \frac{1}{2}q^3. \end{aligned}$$

For $d = 4$, we obtain

$$\begin{aligned} N_4 = I_4 + I_2 + I_1 &= \frac{1}{4}\left(q^4 - q^2\right) + \frac{1}{2}(q^2 - q) + (q-1) \\ &< \frac{1}{4}q^4\left(1 + q^{-2} + 2q^{-3}\right) \leq \frac{1}{4}q^4\frac{3}{2} \\ &= \frac{3}{8}q^4. \end{aligned}$$

We now move on to the case where $d \geq 5$. Denoting the smallest nontrivial divisor of d by p, we first get the following upper bound on I_d:

$$I_d \leq \frac{1}{d}\left\{q^d - q^{d/p} + (q^{d/p-1} + \cdots + q + 1)\right\} < \frac{1}{d}q^d.$$

We also obtain the following upper bound:

$$\sum_{k=1}^{\lfloor d/2 \rfloor} I_k \leq q^{\lfloor d/2 \rfloor + 1} \leq q^{d-2} \leq \frac{1}{4}q^d \quad .$$

Combining, we obtain

$$N_d = I_d + \sum_{k=1}^{\lfloor d/2 \rfloor} I_k < q^d \left(\frac{1}{d} + \frac{1}{4} \right) < \frac{1}{2} q^d \ .$$

□ □

Hence, bent functions can be obtained from our LRS construction using polynomials with nonzero constant terms for all number of variables $n = 2m$, where $m = l$ when $d = 1$, and $m = 2l$ when $d = 2$. This leads us to the following counting result:

Theorem 3. *Let $l, m \in \mathbb{N}$ and $d \in \{1,2\}$ such that $ld = m$, and let $q = 2^l$. Then, the number of $\mathcal{PS}^-$ bent functions of $n = 2m$ variables that can be obtained by Theorem 1 with polynomials of degree d and nonzero constant term is $\binom{2^m-1}{2^{m-1}}$ when $d = 1$ and*

$$\sum_{A=0}^{I_2} \binom{I_2}{A} \sum_{B=0}^{2^{m-1}-A} \binom{I_1}{B} \binom{I_1 - B}{2(2^{m-1} - B - A)} \frac{(2(2^{m-1} - B - A))!}{(2^{m-1} - B - A)! 2^{2^{m-1}-B-A}}, \tag{23}$$

where $I_2 = \frac{1}{2}(q^2 - q)$ and $I_1 = q - 1$, when $d = 2$.

Proof. By Theorem 2 the only cases we need to address are $d = 1$ and $d = 2$. Let $d = 1$ (and thus $m = l$). Then, by Equation (21), the largest family $\mathcal{F}_1$ of coprime polynomials of degree 1 with nonzero constant term over $\mathbb{F}_q$ is composed of $N_1 = q - 1 = 2^m - 1$ elements. The number of subsets of 2^{m-1} elements of $\mathcal{F}_1$ that can be selected to apply Theorem 1 is $\binom{2^m-1}{2^{m-1}}$. For $d = 2$, any family of $t = 2^{m-1}$ coprime polynomials of degree 2 with nonzero constant term over $\mathbb{F}_q$ consists of:

1. $A \leq I_2$ irreducible polynomials of degree 2;
2. $B \leq I_1$ polynomials of the form f^2, where f is an irreducible polynomial of degree 1;
3. $C = t - B - A$ polynomials of the form gh, where g and h are irreducible polynomials of degree 1;

and obviously, the same irreducible polynomial of degree 1 only appears once. There are $\binom{I_2}{A}$ choices for the first part of the family, $\binom{I_1}{B}$ choices for the second part of the family, and

$$\frac{1}{C!} \binom{I_1 - B}{2} \binom{I_1 - B - 2}{2} \cdots \binom{I_1 - B - 2C + 2}{2} = \binom{I_1 - B}{2C} \frac{(2C)!}{C! 2^C}$$

choices for the third part of the family. Combining all three parts, we obtain the formula. □ □

The results above refer to the number of families of coprime polynomials with a nonzero constant term that is large enough to construct $\mathcal{PS}^-$ bent functions. Although such functions will be the focus of our computer investigations in the next sections, one could also augment such families with other types of polynomials, as long as they are pairwise coprime with all the others. This could be used, for instance, to construct further $\mathcal{PS}^-$ functions or $\mathcal{PS}^+$ functions with polynomials of degree $d = 1, 2$. Additionally, one could combine these other types of coprime polynomials with families of degrees higher than 2.

One simple idea to achieve this is to augment each family with the constant polynomial 1 and the polynomial X^d, which we already treated in Section 2.2 and considered in Theorem 1. Although the former is not of degree d while the latter does not have a constant term, it is easy to see that they are coprime both among themselves and to all other polynomials in the families considered in Theorems 2 and 3. This idea spawns from the orthogonal array (OA) characterization of our construction adopted in [9], where the first two columns of the OA correspond to the LRS subspaces defined by 1 and X^d. We will elaborate further on this connection in the conclusions section.

We already used in Example 2 the polynomial X^2 to construct a $\mathcal{PS}^+$ function of 4 variables, by adding it to the family $\{X^2+1, X^2+X+1\}$. One could also add the constant polynomial 1, thereby obtaining a family of 4 coprime polynomials. Since to define a $\mathcal{PS}^+$ function of 4 variables with our LRS construction we need $2^{2-1}+1 = 3$ pairwise coprime polynomials, we can build $\binom{4}{3} = 4$ $\mathcal{PS}^+$ functions by selecting all subsets of three polynomials in $\{1, X^2, X^2+1, X^2+X+1\}$. Alternatively, one could build $\binom{4}{2} = 6$ $\mathcal{PS}^-$ functions since, in this case, we only need a subset of two polynomials.

The next example shows how the two polynomials 1 and X^d can be used to augment a family of coprime polynomials with a nonzero constant term of degree $d > 2$ so that we have enough of them to apply our construction.

Example 3. *Let $m = 3$, and l, d such that $ld = m$. There are only two possibilities, namely $l = 3$ and $d = 1$, and $l = 1$ and $d = 3$. The first one is already covered by Theorem 2 since $d = 1$. Let us consider the case $l = 1$ and $d = 3$. From Equation* (21)*, we have $N_3 = I_3 + I_1 = 2 + 1 = 3$ coprime polynomials of degree* 3 *over $\mathbb{F}_2$ with nonzero constant term, which are the following ones:*

$$
\begin{aligned}
f_1(X) &= X^3 + X^2 + 1 \\
f_2(X) &= X^3 + X + 1 \\
f_3(X) &= (X+1)(X^2+X+1) = X^3 + X^2 + X + 1 \quad .
\end{aligned}
$$

To obtain a $\mathcal{PS}^-$ (respectively, a $\mathcal{PS}^+$) function we need $2^{3-1} = 4$ (respectively, $2^{3-1}+1 = 5$) coprime polynomials. By adding 1 *and X^3 to the set $\{f_1, f_2, f_3\}$, we can thus build $\binom{5}{4} = 5$ $\mathcal{PS}^-$ functions and one $\mathcal{PS}^+$ function.*

This is a post-peer-review, pre-copyedit version of an article published in Designs, Codes and Cryptography. The final authenticated version is available online at: https://doi.org/10.1007/s10623-022-01097-1

5 Equivalence to *DS* Functions for Degree $d = 1$

We now show that our LRS construction coincides with the Desarguesian partial spread class when considering polynomials of degree $d = 1$. In this case, to generate a bent function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ of $n = 2m$ variables, by Theorem 1 we need to find a set of $t = 2^{m-1}$ irreducible polynomials of degree 1 over $\mathbb{F}_{2^m}$. This basically amounts to choosing a subset of cardinality t from the family:

$$I_1 = \{a + X \in \mathbb{F}_{2^m}[X] : a \in \mathbb{F}_{2^m}^*\} \ . \tag{24}$$

Thus, let $P = \{f_1(X), \cdots, f_t(X)\}$ be a subset of I_1. Recall that each polynomial is used as an abstract representation for the coefficients of an LRS of order $d = 1$, used to define the corresponding linear map. In particular, for $f_i(X) = a_i + X$, we have that F_i equals:

$$F_i(x_0, x_1) = a_i x_0 + x_1 \ , \tag{25}$$

for all pairs $(x_0, x_1) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. By Theorem 1, the kernels of $F_i \equiv f_i$ for $i \in \{1, \cdots, t\}$ form a partial spread, and each of them is obtained by taking all pairs $(x_0, x_1) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ such that $x_1 = a_i x_0$, since $\mathbb{F}_{2^m}$ is a field of characteristic 2. We have that:

$$\begin{aligned} ker(F_i) &= \{(x_0, x_1) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} : x_1 = a_i x_0\} \\ &= \{(x, a_i x) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} : x \in \mathbb{F}_{2^m}\} = E_{a_i} \ , \end{aligned} \tag{26}$$

where E_{a_i} is a member of the Desarguesian spread as defined by Equation (9) in bivariate form. We have thus obtained the following result:

Lemma 2. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$, $n = 2m$, be a bent function defined as in Theorem 1 with degree $d = 1$. Then, $f \in \mathcal{PS}_{ap}$.*

Therefore, when considering the family I_1 of $2^l - 1$ irreducible polynomials of degree 1 over $\mathbb{F}_{2^l}$ with a nonzero constant term, our LRS construction is a particular case of the partial spread induced by the Desarguesian spread. Further, the two classes coincide if one adds the polynomials 1 and X to the family I_1 since in that case, one can construct $\binom{2^l+1}{2^{l-1}}$ $\mathcal{PS}_{ap}$ functions.

However, the above reasoning on the Desarguesian spread does not hold for degree 2. In this case, the LRS is defined by three coefficients instead of two, with the input vector of the linear map consisting of 4 coordinates. Consequently, the LRS is evaluated over three variables x_0, x_1, x_2, and there does not seem to be a straightforward way to express the kernel of the linear map as a set of pairs of the type (x, ax). To the best of our knowledge, there are no other constructions in the literature that represent partial spreads in a way analogous to our construction with degree $d = 2$.

Table 1: Distribution of 2-ranks for bent functions of $n = 8$ variables in the Desarguesian spread, obtained through the LRS construction with irreducible polynomials of degree $d = 1$ over $\mathbb{F}_{2^4}$. The bold value corresponds to the upper bound for the rank of a Maiorana-McFarland function.

Rank	#Functions
30	510
36	4080
40	2040
42	17680
Total	24310

6 Computational Results on Ranks and EA-Equivalence for $n = 8$

To investigate more in detail the bent functions induced by our LRS construction, we performed a computer search for $n = 6$ and $n = 8$ variables, with polynomials of degrees $d = 1, 2$, generating only $\mathcal{PS}^-$ functions for $d = 1$ and both $\mathcal{PS}^-$ and $\mathcal{PS}^+$ functions for $d = 2$. This is due to the fact that for degree $d = 1$ the $\mathcal{PS}^+$ functions are the complements of $\mathcal{PS}^-$ functions. For degree $d = 2$, we noticed that all $\mathcal{PS}^+$ functions also have degree $n/2$. This is because the partial spreads which define these functions are not maximal, and therefore by Proposition 1, they must have the same algebraic degree of $\mathcal{PS}^-$ functions. Moreover, it is known that up to $n = 6$ variables, all bent functions belong to the completed Maiorana-McFarland class [17]. Therefore, the smallest interesting case to consider is $n = 8$ variables.

As a first assessment, we generated all $\mathcal{PS}^-$ functions by using families of coprime polynomials of degree $d = 1$. Although by Lemma 2, we know that all such functions are in $\mathcal{PS}_{ap}$ and coincide with the Desarguesian spread class, we computed their ranks to independently verify the count reported by Weng et al. [19]. In this case, we have $m = l = 4$ and $t = 2^{m-1} = 8$. Hence, to construct a function from the Desarguesian spread, we need 8 coprime polynomials. Since there are 16 irreducible polynomials of degree $d = 1$ with coefficients over $\mathbb{F}_{2^4}$ and the constant polynomial 1, one can obtain $\binom{17}{8} = 24310$ $\mathcal{PS}_{ap}$ functions with our construction. Table 1 reports the distribution of the 2-ranks for all such functions. The upper bound on the rank of a Maiorana-McFarland function of $n = 8$ variables given in [19] is $2^{m+1} - 2 = 30$. Hence, one can see from Table 1 that most of the functions in the Desarguesian spread are inequivalent to Maiorana-McFarland functions. Remark also that the numbers in Table 1 are higher than those reported by Weng et al. in [19] because we are actually considering more functions. As a matter of fact, Weng et al. computed the $\binom{16}{8} = 12870$ bent functions in the class $\mathcal{PS}^-$ arising from the Desarguesian spread components $x_1 = ax_0$, with $a \in \mathbb{F}_{2^4}$. This corresponds to our LRS construction when considering only the $2^4 - 1$ irreducible polynomials

of degree 1 over $\mathbb{F}_{2^4}$ with nonzero constant term and the polynomial X. On the other hand, here, as mentioned above, we also consider the polynomial 1, which is coprime with all such polynomials, although it does not have degree 1. This allows us to construct $\binom{16}{7} = 11440$ additional functions. Therefore, the distribution reported in Table 1 independently verifies and extends Weng et al.'s result in [19]. Moreover, since the functions of $\mathcal{PS}^+$ type are the complements of those of type $\mathcal{PS}^-$, Table 1 actually gives a complete account of the rank distribution of all $\mathcal{PS}_{ap}$ functions in 8 variables.

Next, we focused our attention on coprime polynomials of degree $d = 2$. As we discussed in Section 5, this case is not directly amenable to the Desarguesian spread, and it is, therefore, an interesting candidate to find potentially new $\mathcal{PS}^-$ and $\mathcal{PS}^+$ functions. By Theorem 2, we have $m = 4$, $t = 8$, and $l = 2$. Consequently, a $\mathcal{PS}^-$ bent function is obtained by finding a set of eight pairwise coprime polynomials over $\mathbb{F}_4$ of degree 2. Let $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$, where α is a root of a primitive polynomial $p(X) \in \mathbb{F}_2[X]$ of degree 2. Then, by Gauss's formula, there are six irreducible polynomials of degree 2 over $\mathbb{F}_4$:

$$\begin{aligned}
p_1(X) &= X^2 + \alpha^2 X + \alpha^2 \ , \\
p_2(X) &= X^2 + \alpha^2 X + 1 \ , \\
p_3(X) &= X^2 + \alpha X + \alpha \ , \\
p_4(X) &= X^2 + X + \alpha^2 \ , \\
p_5(X) &= X^2 + \alpha X + 1 \ , \\
p_6(X) &= X^2 + X + \alpha \ .
\end{aligned}$$

These polynomials are, of course, pairwise coprime since they are irreducible. Let us denote them by $I_2 = \{p_1, p_2, p_3, p_4, p_5, p_6\}$. Further, there are three irreducible polynomials of degree 1 and nonzero constant term over $\mathbb{F}_4$ that can be squared to obtain polynomials of degree 2 that are coprime among themselves and with those in I_2:

$$\begin{aligned}
p_7(X) &= (X+1)^2 = X^2 + 1 \ , \\
p_8(X) &= (X+\alpha)^2 = X^2 + \alpha^2 \ , \\
p_9(X) &= (X+\alpha^2)^2 = X^2 + \alpha \ .
\end{aligned}$$

Analogously, we denote by I_1^2 the set $\{p_7, p_8, p_9\}$. Moreover, we can augment our set with the polynomials 1 and X^2. Although the former is not of degree 2 and the latter does not have a constant term, they are coprime with all polynomials in $I_2 \cup I_1^2$. Finally, we can take the $\binom{3}{2} = 3$ pairs of I_1 and multiply the polynomials in them, obtaining:

$$\begin{aligned}
p_{10}(X) &= (X+1)(X+\alpha^2) = X^2 + \alpha X + \alpha^2 \ , \\
p_{11}(X) &= (X+1)(X+\alpha) = X^2 + \alpha^2 X + \alpha \ , \\
p_{12}(X) &= (X+\alpha)(X+\alpha^2) = X^2 + X + 1 \ ,
\end{aligned}$$

Table 2: Distribution of 2-ranks for $\mathcal{PS}^-$ and $\mathcal{PS}^-$ bent functions of $n = 8$ variables obtained through the LRS construction with coprime polynomials of degree $d = 2$ over $\mathbb{F}_4$. The bold value corresponds to the upper bound for the rank of the Desarguesian bent function.

Type	Rank	#Functions
$\mathcal{PS}^-$	36	20
	40	24
	42	28
	44	123
	46	78
	Total	273
$\mathcal{PS}^+$	40	45
	44	19
	46	18
	Total	82

with $I_{1,1} = \{p_{10}, p_{11}, p_{12}\}$. These three polynomials are not pairwise coprime among themselves, but each of them is relatively prime to all polynomials in $I_2 \cup \{1, X^2\}$, and to exactly one polynomial in I_1^2. Summarizing, for the $\mathcal{PS}^-$ case, we can construct 273 functions with the following families of $t = 8$ pairwise coprime polynomials:

- $\binom{11}{8} = 165$ subsets of 8 elements in the union $I_2 \cup I_1^2 \cup \{1, X^2\}$.
- $\binom{3}{1}\binom{9}{7} = 108$ families obtained by choosing one element p from $I_{1,1}$ and adjoining to it 7 polynomials from $I_2 \cup \{1, X^2\} \cup \{p_1'\}$, where p_1' is the one element in I_1^2 which is coprime to p.

Similarly, we can obtain 82 $\mathcal{PS}^+$ functions by the following families of $t = 9$ pairwise coprime polynomials:

- $\binom{11}{9} = 55$ subsets of 9 elements in the union $I_2 \cup I_1^2 \cup \{1, X^2\}$.
- $\binom{3}{1}\binom{9}{8} = 108$ families obtained by choosing one element p from $I_{1,1}$ and adjoining to it 8 polynomials from $I_2 \cup \{1, X^2\} \cup \{p_1'\}$, where p_1' is again the one element in I_1^2 that is coprime to p.

Table 2 reports the distribution of the ranks for the $\mathcal{PS}^-$ and $\mathcal{PS}^+$ functions obtained from the families of polynomials described above. The first significant observation that can be drawn from the table is that *none of these bent functions is equivalent to a Maiorana-McFarland function*, since the smallest rank is 36. It is even more interesting to observe that *many functions are inequivalent to the ones*

induced by the Desarguesian spread, namely those reaching a rank higher than 42. In particular, of the 355 $\mathcal{PS}$ bent functions given by our construction, 238 have a rank greater than 42, so they are not equivalent to either Maiorana-McFarland or Desarguesian spread functions. While this is not sufficient to conclude that we found a class of previously unknown bent functions, we consider it the first step toward that goal. Hopefully, our results will motivate further research in this direction.

7 Conclusions and Perspectives

This paper described a method to construct bent functions from linear recurring sequences. The construction leverages on the subspaces spanned by linear mappings defined by a family of LRS. In particular, we proved that if the polynomials defining the linear recurrence equations are pairwise coprime, the kernels of the corresponding linear mappings have a pairwise trivial intersection. This result depends on the observation that the superposition of two LRS mappings is the Sylvester matrix associated with their polynomials, which is invertible if and only if the polynomials are coprime. Consequently, the kernels induced by a family of LRS subspaces whose polynomials are pairwise coprime form a partial spread, and thus a bent function in the class $\mathcal{PS}$.

The key question concerning our LRS construction is to determine when a large enough family of LRS kernels exists, depending on the number of variables of the function, the degree of the polynomials, and the extension field of their coefficients. Assuming that all polynomials have a nonzero constant term, we showed that such families exist if and only if the degree of the polynomials is either 1 or 2, and we derived the counting formulas for both cases. We then remarked that at least two other polynomials can always be added to these families, namely X^d and 1. This allows one to obtain also $\mathcal{PS}^+$ functions and, in certain situations, to employ families of polynomials with degrees larger than 2. We then proved that our LRS construction coincides with the Desarguesian partial spread when the degree of the involved polynomials is $d = 1$, and thus the functions obtained in this case all belong to the class $\mathcal{PS}_{ap}$. Therefore, candidates for potentially new bent functions generated by our construction should be sought with polynomials of degree $d = 2$.

After remarking that the bent functions of $n = 6, 8$ variables given by our LRS construction always have maximal degree $n/2$ even for the $\mathcal{PS}^+$ case (which is explained by the non-maximality of the related partial spreads), we performed a computational analysis of the 2-ranks of the functions for the $n = 8$ case, to determine the rank distributions. In particular, for degree $d = 1$, we verified and extended the rank distribution reported by Weng et al. [19] for bent functions in the Desarguesian spread, remarking that most of them are not EA-equivalent to any Maiorana-McFarland function. For degree $d = 2$, we generated both $\mathcal{PS}^-$ and $\mathcal{PS}^+$ types of functions and remarked that many of them have a rank greater than 42, which means that they are not EA-equivalent to functions in the Desarguesian spread either. Hence, such bent functions are the most promising candidates to be

potentially novel.

There are several open questions for future research on this LRS construction. The first interesting direction is to investigate more in detail the functions obtained by polynomials of degree $d = 2$. Indeed, although we showed that many of them are inequivalent to both Maiorana-McFarland and Desarguesian spread functions, it could still be the case that they are EA-equivalent to some other known classes. To this end, it would be interesting to compare our functions to those generated by other partial spread-based constructions, a list of which can be found in [15]. Besides computing the 2-rank, employing more discriminating invariants would also be interesting. These include, for instance, the *Smith normal form* of the development of the graph G_f of a Boolean function f, which is used by Polujan and Pott in [16] to classify homogeneous cubic bent functions. The goal here would be to find a complete invariant that allows one to give a complete classification of the equivalence classes arising from our construction of bent functions.

We conclude by discussing the connection of our LRS construction with the cellular automata (CA) approach that we adopted in [9]. Our initial idea was to start from a recent construction of *Mutually Orthogonal Latin Squares* (MOLS) based on linear CA that we set forth in [12]. A cellular automaton can be defined as a shift-invariant vectorial transformation, where the same *local rule* is applied at all sites (or cells) of the input array. If the local rule is linear, then the CA global function is defined by a transition matrix with the same form of the matrix in Equation (14). In particular, the CA global function may be regarded as the linear map induced by an LRS kernel, with Equation (13) representing the application of the local rule on the i-th cell of the input.

In [12], we first showed that such a linear CA $F : \mathbb{F}_q^{2d} \to \mathbb{F}_q^d$ defines a Latin square of order q^d if and only if the leftmost and rightmost coefficients a_0, a_{d-1} of its local rule are not null. Further, they proved that the Latin squares generated by two such CA are orthogonal if and only if the polynomials associated with their local rules are relatively prime. Thus, determining the maximum size of a family of pairwise coprime polynomials of degree d and the nonzero constant term is equivalent to finding the size of the largest family of MOLS of order q^d induced by linear CA[1].

The connection between MOLS generated by linear CA and bent functions traces back to a theorem proved by Bush [2], where he showed that a large enough orthogonal array (OA, which is equivalent to a set of MOLS) could be used to define a Hadamard matrix. It is well known that a Boolean function is bent if and only if the polar form of its translate design is a Hadamard matrix. What we proved in [9] is that the Hadamard matrix defined by the MOLS of a family of linear CA indeed has the translate design structure required for a bent function. This result is the "CA version" of Theorem 1 proved here.

[1]Remark that in [12] d is used to denote the *diameter* of the CA rather than the degree of the polynomials, which there is denoted by b with $b = d - 1$. For the sake of consistency, in this paper, we used the letter d directly for the degree since it coincides with the LRS order. Hence the d in this paragraph should be interpreted as a $d - 1$ in [12].

The characterization through kernels of LRS is clearly a much more compact way to describe our construction than the CA approach, and it is also more general. Indeed, in this paper, we focused on the assumption that the feedback polynomials of the LRS have a nonzero constant term to leverage on the counting results proved in [12] for CA-based MOLS. However, Lemma 1 does not need this hypothesis to characterize LRS kernels with a trivial intersection, which is what matters in the end to construct a partial spread. In particular, one can use *any* family of pairwise coprime polynomials with degree d, regardless of their constant term. This is enough to guarantee that the associated Sylvester matrix is invertible. We implicitly dropped this assumption by augmenting our families with the polynomials X^d and 1 since they are easily seen to be coprime with all other polynomials. However, besides those analyzed here, several other families of coprime polynomials can be considered. We plan to investigate this issue in future research, as we suspect that this would simplify the counting results reported in Section 4 by using the q-to-1 relationship between non-coprime and coprime pairs of polynomials over $\mathbb{F}_q$ proved in [1].

Acknowledgements

The authors wish to thank the anonymous reviewers for their helpful comments to improve the presentation of the paper, as well as for pointing out the connection between linear CA and subspaces of linear recurring sequences and the use of rank invariants to classify our bent functions.

Data Availability

The experimental data discussed in this paper (including the truth tables of the functions generated through the LRS construction and their ranks) are available at `https://github.com/rymoah/bent-functions-lrs`.

References

[1] A. T. Benjamin and C. D. Bennett. The probability of relatively prime polynomials. *Mathematics Magazine*, 80(3):196–202, 2007.

[2] K. Bush. Construction of symmetric Hadamard matrices. In *A survey of combinatorial theory*, pages 81–83. Elsevier, 1973.

[3] C. Carlet. Boolean Functions for Cryptography and Error Correcting Codes. In Y. Crama and P. L. Hammer, editors, *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, pages 257–397. Cambridge University Press, New York, NY, USA, 1st edition, 2010.

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

[5] C. Carlet and P. Gaborit. Hyper-bent functions and cyclic codes. *J. Comb. Theory, Ser. A*, 113(3):466–482, 2006.

[6] C. Carlet and S. Mesnager. Four decades of research on bent functions. *Des. Codes Cryptogr.*, 78(1):5–50, 2016.

[7] J. F. Dillon. *Elementary Hadamard difference sets*. PhD thesis, Univ. of Maryland, 1974.

[8] H. Dobbertin. Construction of bent functions and balanced boolean functions with high nonlinearity. In B. Preneel, editor, *Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings*, volume 1008 of *Lecture Notes in Computer Science*, pages 61–74. Springer, 1994.

[9] M. Gadouleau, L. Mariot, and S. Picek. Bent functions from cellular automata. *IACR Cryptol. ePrint Arch.*, page 1272, 2020.

[10] I. M. Gelfand, M. Kapranov, and A. Zelevinsky. *Discriminants, resultants, and multidimensional determinants*. Springer Science & Business Media, 2008.

[11] R. Lidl and H. Niederreiter. *Introduction to finite fields and their applications*. Cambridge University Press, 1994.

[12] L. Mariot, M. Gadouleau, E. Formenti, and A. Leporati. Mutually orthogonal latin squares based on cellular automata. *Designs, Codes and Cryptography*, 88(2):391–411, 2020.

[13] L. Mariot, A. Leporati, A. Dennunzio, and E. Formenti. Computing the periods of preimages in surjective cellular automata. *Nat. Comput.*, 16(3):367–381, 2017.

[14] R. L. McFarland. A family of difference sets in non-cyclic groups. *J. Comb. Theory, Ser. A*, 15(1):1–10, 1973.

[15] S. Mesnager. *Bent Functions - Fundamentals and Results*. Springer, 2016.

[16] A. A. Polujan and A. Pott. Cubic bent functions outside the completed Maiorana-McFarland class. *Des. Codes Cryptogr.*, 2020.

[17] O. S. Rothaus. On "bent" functions. *J. Comb. Theory, Ser. A*, 20(3):300–305, 1976.

[18] J. J. Sylvester. Xviii. on a theory of the syzygetic relations of two rational integral functions, comprising an application to the theory of sturm's functions, and that of the greatest algebraical common measure. *Philosophical transactions of the Royal Society of London*, (143):407–548, 1853.

[19] G. Weng, R. Feng, and W. Qiu. On the ranks of bent functions. *Finite Fields Their Appl.*, 13(4):1096–1116, 2007.

[20] A. M. Youssef and G. Gong. Hyper-bent functions. In B. Pfitzmann, editor, *Advances in Cryptology - EUROCRYPT 2001, International Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, Austria, May 6-10, 2001, Proceeding*, volume 2045 of *Lecture Notes in Computer Science*, pages 406–419. Springer, 2001.