A general construction of Ordered Orthogonal Arrays using LFSRs

Daniel Panario, Mark Saaltink, Brett Stevens and Daniel Wevrick ∗†‡§

May 29, 2018

Abstract

In [2], \(q^t \times (q+1)t\) ordered orthogonal arrays (OOAs) of strength \(t\) over the alphabet \(\mathbb{F}_q\) were constructed using linear feedback shift register sequences (LFSRs) defined by primitive polynomials in \(\mathbb{F}_q[x]\). In this paper we extend this result to all polynomials in \(\mathbb{F}_q[x]\) which satisfy some fairly simple restrictions, restrictions that are automatically satisfied by primitive polynomials. While these restrictions sometimes reduce the number of columns produced from \((q+1)t\) to a smaller multiple of \(t\), in many cases we still obtain the maximum number of columns in the constructed OOA when using non-primitive polynomials. For small values of \(q\) and \(t\), we generate OOAs in this manner for all permissible polynomials of degree \(t\) in \(\mathbb{F}_q[x]\) and compare the results to the ones produced in [2], [15] and [16] showing how close the arrays are to being “full” orthogonal arrays. Unusually for finite fields, our arrays based on non-primitive irreducible and even reducible polynomials are closer to orthogonal arrays than those built from primitive polynomials.

1 Introduction

Let \(t, m, v, \lambda \in \mathbb{Z}^+\) with \(2 \leq t \leq m\), let \(n = \lambda v^t\) and let \(M\) be an \(n \times m\) array over a set \(V\) (the alphabet) of cardinality \(v\). An \(n \times t\) subarray of \(M\) is \(\lambda\)-covered if each \(t\)-tuple over \(V\) appears as a row of the subarray exactly \(\lambda\) times; the corresponding set of \(t\) columns of \(M\) is \(\lambda\)-covered. An orthogonal array (OA) of strength \(t\) and index \(\lambda\) is an \(n \times m\) array such that every set of \(t\) columns is \(\lambda\)-covered. We use \(OA_\lambda(n; t, m, v)\) to denote such an array.

A generalization of the concept of an OA is an ordered orthogonal array (OOA) [7], [11]. For \(s \in \mathbb{Z}^+\), let \(M\) be an \(n \times ms\) array with columns labeled by \(\{1, 2, \ldots, m\} \times \{1, 2, \ldots, s\} \)

∗D. Panario is with School of Mathematics and Statistics, Carleton University, Canada. Email: daniel@math.carleton.ca
†Mark Saaltink and Daniel Wevrick are Independent Researchers. Emails: mark.saaltink@gmail.com, dwevrick@gmail.com
‡B. Stevens is with School of Mathematics and Statistics, Carleton University, Canada. Email: brett@math.carleton.ca
§Daniel Panario and Brett Stevens are partially supported by NSERC of Canada.
and entries from a set $V$ (the alphabet) of cardinality $v$. For $1 \leq i \leq m$, the set of columns indexed by $\{i\} \times \{1, 2, \ldots, s\}$ is the block $B_{i}(M)$. Thus,

$$M = \begin{bmatrix} B_{1}(M) & B_{2}(M) & \cdots & B_{m}(M) \end{bmatrix}.$$ 

A subset $\Omega$ of columns of $M$ is left-justified if $(i, j) \in \Omega$ with $j > 1$ implies $(i, j-1) \in \Omega$. Thus, for each block $B_{i}(M)$, the columns in $\Omega$ that are in $B_{i}(M)$ are consecutive leftmost ones in $B_{i}(M)$, with indices $(i,1), (i,2), \ldots, (i,l_{i})$ where $l_{i}$ is the number of columns in $\Omega$ chosen from $B_{i}(M)$. We observe that $0 \leq l_{i} \leq s$ and so $l_{i}$ could be 0, which occurs when no columns of $\Omega$ are from $B_{i}(M)$. If $M$ has the property that every left-justified set $\Omega$ of $t$ columns of $M$ is $\lambda$-covered, then $M$ is an ordered orthogonal array, and is denoted $OOA(\lambda; n; t, m, s, v)$.

As before, $t$ is the strength of the OOA and $\lambda$ is the index. For both OAs and OOAs, if $\lambda = 1$, we simply say covered and write $OA(n; t, m, v)$ and $OOA(n; t, m, s, v)$ to denote such arrays. By setting $s = 1$, an $OOA(\lambda; n; t, m, 1, v)$ can easily be seen to be an $OA(\lambda; n; t, m, v)$ as every subset of $t$ columns is left-justified. As a concrete example, an $OOA(8; 3, 2, 3, 2)$ with 2 blocks of size 3 over the alphabet $F_{2}$ is shown in Figure 1.

$$OOA(8; 3, 2, 3, 2) = \begin{bmatrix} (1,1) & (1,2) & (1,3) & (2,1) & (2,2) & (2,3) \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Figure 1: A strength 3 OOA over alphabet $F_{2}$.

In an OA, all subsets of $t$ columns are $\lambda$-covered and in an OOA all left-justified subsets of $t$ columns are $\lambda$-covered. In an OOA, it is possible that additional subsets of $t$ columns, those that are not left-justified, are also $\lambda$-covered. An OOA that has a significant percentage of non left-justified subsets of $t$ columns $\lambda$-covered can be thought of as being closer to an OA and as having better coverage.

More information about OAs and OOAs can be found in [3, Section VI.59.3], [5] and [6, Chapter 3].

Earlier papers giving constructions of OOAs include [2], [15] and [16]. Our paper generalizes the construction given in [2] which uses linear feedback shift registers defined by primitive polynomials in $F_{q}[x]$. In our construction, primitivity is not required. Section 2
reviews, generalizes and simplifies a number of results from [2]. A key technical ingredient in [2] is the use of trace representation since, in that paper, only primitive polynomials are considered. Here we cannot use this ingredient since no trace representation is readily available for non-primitive polynomials. Section 3 gives the new construction and Section 4 provides a proof of the correctness of the construction. In place of the trace representation, we use the fact that the annihilating polynomial commutes with the left shift operator and scalar multiplication. In Section 5, we investigate the case of polynomials in \( \mathbb{F}_2[x] \), provide statistical data on the OOAs produced and compare these new OOAs to the ones produced in [2], [15] and [16]. Similar results for larger field sizes are provided in Appendix A. An initial analysis of the data shows that, on many occasions, the new construction produces OOAs that have better coverage than previously generated ones. In contrast to other situations in finite fields, here irreducible and reducible polynomials provide better coverage than primitive polynomials; see tables in Section 5 and Appendix A.

2 Linear Feedback Shift Registers

Let \( \mathbb{F}_q \) be a finite field of order \( q \) and let \( f \in \mathbb{F}_q[x] \) be a monic polynomial of degree \( t \). Writing \( f(x) = \sum_{i=0}^{t} b_i x^i \), define a linear feedback shift register (LFSR) whose output stream, \( S(f,T) = s = (s_n)_{n \geq 0} \) is given by

\[
s_{n+t} = -\sum_{i=0}^{t-1} b_i s_{n+i}, \quad n \geq 0,
\]

for a given initial \( t \)-tuple \( T = (s_0, s_1, \ldots, s_{t-1}) \in \mathbb{F}_q^t \).

This is equivalent to having \( \sum_{i=0}^{t} b_i s_{n+i} = 0 \) for all integers \( n \geq 0 \). Then, \( f \) annihilates such streams and such streams are annihilated by \( f \). Let \( G(f) \) denote the set of streams over \( \mathbb{F}_q \) that satisfy the recurrence defined by \( f \).

If \( b_0 \neq 0 \) we can “run the LFSR in reverse” by defining

\[
s_{n-t} = -b_0^{-1} \sum_{i=1}^{t} b_i s_{n-t+i}, \quad n \in \mathbb{Z},
\]

and so we can allow the indexing set for \( s \) to be \( \mathbb{Z} \) and not just the non-negative integers.

2.1 Operations on streams

Fix a monic polynomial \( f \in \mathbb{F}_q[x] \) with non-zero constant term. For \( s = (s_n)_{n \geq 0} \in G(f) \) and \( \beta \in \mathbb{F}_q \), we define \( Ls \) to be the stream \( b = (s_{n+1})_{n \geq 0} \) and \( \beta s \) to be the stream \( b = (\beta s_n)_{n \geq 0} \). Here \( L \) is the left-shift operator and these operations can be extended in the
obvious way to define $g(L)s$ for $g \in \mathbb{F}_q[x]$. From [4], a stream $r$ has a run of zeroes of length $l$ at index $n$ if
\[ r_{n-1} \neq 0, r_n = r_{n+1} = \cdots = r_{n+l-1} = 0, r_{n+l} \neq 0. \]

For Lemmas 1-5 we always have the following context:
- $f \in \mathbb{F}_q[x]$ is a monic polynomial of degree $t$ with $f(x) = \sum_{i=0}^{t} b_i x^i$ and $b_0 \neq 0$;
- $\beta \in \mathbb{F}_q$ with $f(\beta) \neq 0$;
- $r, s \in G(f)$ with $r = (L - \beta)s$;
- $r$ has a run of $l \geq 0$ zeroes at index 0 (hence $r_l \neq 0$).

The following two lemmas follow easily.

Lemma 1. $(s_0, s_1, s_2, \ldots, s_l) = (s_0, \beta s_0, \beta^2 s_0, \ldots, \beta^l s_0)$.

Proof. This follows from $(L - \beta)s = r$ and the assumption that $r$ has a run of $l \geq 0$ zeroes at index 0.

Lemma 2. $s_0 = 0$ if and only if $s$ has a run of $l + 1$ zeroes starting at index 0.

Proof. This follows from Lemma 1.

From $r = (L - \beta)s$, it follows that if $s$ has a run of $l + 1$ zeroes at index 0 (i.e. when $s_0 = 0$), then $r$ has a run of $l$ zeroes at index 0. However, even if $s_0 \neq 0$, Lemma 1 shows that it is still possible to obtain a run of $l$ zeroes in $r$. In [2], a special polynomial was constructed from $r$ whose roots determine the exact conditions under which the run of $l$ zeroes in $r$ came from a run of $l + 1$ zeroes in $s$. This polynomial is:
\[ P_{l,r}(x) = \sum_{j=l+1}^{t} b_j \left( \sum_{m=l}^{j-1} r_m x^{j-1-m} \right). \]

The next 3 lemmas prove properties of $P_{l,r}$. These results were shown in [2], but the proofs given here are significantly shorter and less complicated than the ones given in [2]. These lemmas are used in the proof of the correctness of the OOA construction given in Section 3.

Lemma 3. The polynomial $s_0 f + P_{l,r}$ has $\beta$ as a root.

Proof. For $j \in \mathbb{Z}$, since $r = (L - \beta)s$, we have $r_j = s_{j+1} - \beta s_j$ or equivalently $s_{j+1} = r_j + \beta s_j$. Hence $s_1 = r_0 + \beta s_0$, $s_2 = r_1 + \beta s_1 = r_1 + \beta r_0 + \beta^2 s_0$, and so we have by induction
\[ s_j = s_0 \beta^j + \sum_{m=0}^{j-1} r_m \beta^{j-1-m} \quad \text{for all } j \in \mathbb{Z}. \]

Since $s$ is annihilated by $f$, we have
Hence \( \beta \leq 0 \) if \( r \neq 0 \). Since \( r = 0 \), the first \( l \) terms of the inner sum are 0 and so we have \( 0 = s_0 f(\beta) + \sum_{j=0}^{t} b_j \left( \sum_{m=0}^{j-1} r_m \beta^{j-1-m} \right) \).

If \( 0 \leq j \leq l \), the inner sum is empty and so \( 0 = s_0 f(\beta) + \sum_{j=l+1}^{t} b_j \left( \sum_{m=0}^{j-1} r_m \beta^{j-1-m} \right) = s_0 f(\beta) + P_{l,r}(\beta) \).

Hence \( \beta \) is a root of \( s_0 f + P_{l,r} \) as claimed. \( \Box \)

**Lemma 4.** The stream \( s \) has a run of zeroes of length \( l + 1 \) starting at index 0 if and only if \( \beta \) is root of \( P_{l,r}(x) \) if and only if \( s_0 = 0 \).

**Proof.** This follows from Lemmas 2 and 3 and the fact that \( f(\beta) \neq 0 \). \( \Box \)

To make the next results easier to understand, we re-write \( P_{l,r}(x) \) via a number of steps. First reverse the inner sum to get

\[
P_{l,r}(x) = \sum_{j=l+1}^{t} b_j \left( \sum_{m=0}^{j-1} r_m \beta^{j-1-m} \right).
\]

Then, switch the order of the two sums to get

\[
P_{l,r}(x) = \sum_{m=0}^{t-l-1} \left( \sum_{j=l+m+1}^{t} b_j r_{j-1-m} \right) x^m.
\]

Lastly re-index the inner sum to get

\[
P_{l,r}(x) = \sum_{m=0}^{t-l-1} \left( \sum_{j=0}^{t-m-l-1} b_{j+m+l+1} r_{j+l} \right) x^m. \tag{1}
\]

We observe that \( P_{l,r} \) has degree smaller than or equal to \( t - l - 1 \) and the coefficient of \( x^{t-l-1} \) is \( b_t r_t \). In fact, \( P_{l,r} \) has degree \( t - l - 1 \) since \( b_t = 1 \) and \( r_t \neq 0 \).

Now, if \( s \) has a run of \( l + 1 \) zeros starting at index 0, then we can express the polynomial \( P_{l+1,s}(x) \), for this tuple of zeroes, as

\[
P_{l+1,s}(x) = \sum_{m=0}^{t-l-2} \left( \sum_{j=0}^{t-m-l-2} b_{j+m+l+2} s_{j+l+1} \right) x^m. \tag{2}
\]

By Lemma 4 \( \beta \) is a root of \( P_{l,r} \). Hence \( P_{l,r}(x) = (x - \beta)A(x) \) for some \( A \in \mathbb{F}_q[x] \). We show that \( A \) is, in fact, \( P_{l+1,s}(x) \)
Lemma 5. Suppose $s$ has a run of at least $l + 1$ zeros starting at index 0. Then we have $P_{l,r}(x) = (x - \beta)P_{l+1,s}(x)$.

Proof. Let $H(x) = (x - \beta)P_{l+1,s}(x) - P_{l,r}(x)$ and consider $[x^m]H(x)$, the coefficient of $x^m$ in $H(x)$. We show that it is 0 and hence $H(x) = 0$. The constant term of $H(x)$ is

$$-\beta [x^0]P_{l+1,s}(x) - [x^0]P_{l,r}(x).$$

Using $P_{l,r}(x) = \sum_{j=0}^{t} b_j \left( \sum_{m=0}^{t-j} r_j - 1 - m x^m \right)$ and $P_{l+1,s}(x) = \sum_{j=0}^{t} b_j \left( \sum_{m=0}^{t-j-1} s_j - 1 - m x^m \right)$ which are equivalent formulae for $P_{l,r}$ and $P_{l+1,s}$ (see results shown after Lemma 4) this constant term is

$$-\beta \sum_{j=0}^{t} b_j R_j - \sum_{j=0}^{t} b_j r_j - 1 = -\sum_{j=0}^{t} b_j (r_j - 1 + \beta s_j) = -\sum_{j=0}^{t} b_j s_j$$

(since $r = (L - \beta)s$)

$$= 0$$

(since $f$ annihilates $s$).

For $m \geq 1$ we have:

$$[x^m]H(x) = [x^{m-1}]P_{l+1,s}(x) - \beta [x^m]P_{l+1,s}(x) - [x^m]P_{l,r}(x).$$

Now, from Equations 1 and 2 we get

$$[x^{m-1}]P_{l+1,s}(x) = \sum_{j=0}^{t-m-1} b_j + m+l+1 s_j + l+1 = b_{m+l+1} s_{l+1} + \sum_{j=1}^{t-m-l-1} b_j + m+l+1 s_j + l+1$$

$$[x^m]P_{l+1,s}(x) = \sum_{j=0}^{t-m-l-2} b_j + m+l+2 s_j + l+1 = 0 + \sum_{j=1}^{t-m-l-1} b_j + m+l+1 s_j + l$$

$$[x^m]P_{l,r}(x) = \sum_{j=0}^{t-m-l-1} b_j + m+l+1 r_j + l = b_r r_{l-1} + \sum_{j=0}^{t-m-l-2} b_j + m+l+1 r_j + l.$$

The first and third of these equations come from removing the first and last terms, respectively, from the sums, and the second equation comes from incrementing the index $j$ by 1. Thus we have

$$[x^m]H(x) = b_{m+l+1} s_{l+1} - b_r r_{l-1} + \sum_{j=1}^{t-m-l-1} b_j + m+l+1 (s_j + l+1 - \beta s_j + l) - \sum_{j=0}^{t-m-l-2} b_j + m+l+1 r_j + l.$$

Since, $r = (L - \beta)s$, $s_j + l+1 - \beta s_j + l$ holds for all $j$ and so

$$[x^m]H(x) = b_{m+l+1} s_{l+1} - b_r r_{l-1} + \sum_{j=1}^{t-m-l-1} b_j + m+l+1 r_j + l - \sum_{j=0}^{t-m-l-2} b_j + m+l+1 r_j + l$$

$$= b_{m+l+1} s_{l+1} - b_r r_{l-1} + (b_l r_{l-1} - b_{m+l+1} r_l)$$

$$= b_{m+l+1} (s_{l+1} - r_l)$$

$$= 0.$$

Thus $H(x) = 0$ and the claimed result holds.
2.2 Getting longer and longer runs

Let $\beta \in \mathbb{F}_q$ be such that $(x - \beta, f(x)) = 1$. Thus, there exists $g \in \mathbb{F}_q[x]$ such that $g(x)(x - \beta) \equiv 1 \pmod{f}$. Let $r_0$ be a stream that has a run of zeroes of length $l$ starting at index 0 and inductively define streams $r_{i+1} = g(L)r_i = (L - \beta)^{-1}r_i$ for $i \geq 1$. Equivalently, $r_i = (L - \beta)r_{i+1}$ for $i \geq 0$.

Let $P_{1,r_0}$ be the polynomial defined for the run of $l$ zeroes in $r_0$ and let $z$ be the multiplicity of $\beta$ as a root of $P_{1,r_0}$. From Lemma 5 for $i \geq 0$, $r_{i+1}$ has a run of zeros of length $l + i + 1$ as long as $r_i$ has a run of zeros of length $l + i$ starting at index 0 and $\beta$ is a root of $P_{i+1,r_i}$. If $\beta$ is not a root of $P_{i+1,r_i}$, then $r_{i+1}$ does not have a run of $l$ zeroes starting at index 0. Repeated application of Lemma 5 gives the following result.

**Lemma 6.** For $0 \leq i \leq z$, $r_i$ has a run of zeros of length $l + i$ starting at index 0 and $r_{z+1}$ is not 0 at index 0.

2.3 Starting at an index $\neq 0$

Next we show that, for the results given in the previous sections, the requirement that the run of zeroes occurs at index 0 is not essential. Specifically, suppose that $r$ has a run of $l$ zeroes starting at $n$ and that $r = (L - \beta)s$. Then, $L^n r = (L - \beta) L^n s$; $L^n r$ has a run of $l$ zeroes starting at index 0 and so the results given in the previous section can be applied to $L^n r$. Specifically, we would have:

- $(s_n, s_{n+1}, s_{n+2}, \ldots, s_{n+l}) = (s_n, \beta s_n, \beta^2 s_n, \ldots, \beta^l s_n)$;
- $s_n = 0$ if and only if $s$ has a run of $l + 1$ zeroes starting at index $n$;
- if $P_{l, L^n r}(x) = \sum_{j=l+1}^4 b_j \left( \sum_{m=1}^{j-1} r_{n+m} x^{j-1-m} \right)$; then, $\beta$ is a root of $s_n f + P_{l, L^n r}$;
- $\beta$ is root of $P_{l, r}$ if and only if $s_n = 0$ if and only if $s$ has a run of zeroes of length $l + 1$ starting at index $n$;
- suppose $s$ has a run of $l + 1$ zeros starting at index $n$; then $P_{l, r}(x) = (x - \beta)P_{l+1,s}(x)$.

These results will be used in the proof of the correctness of our new construction.

3 The Generalized Runs (GR) construction of OOAs

Let $f \in \mathbb{F}_q[x]$ be a monic polynomial with non-zero constant term. For a stream $s \in G(f)$ with period $\rho$ we define its orbit to be the set $\{s, Ls, L^2s, \ldots, L^{\rho-1}s\}$ which is the set of the $\rho$ different sequences of length $\rho$ obtained by applying the left shift operator $L$ to $s$ $i$ times, for $i = 0, \ldots, \rho - 1$. The orbits partition $G(f)$ into $s$ orbits $C_1, C_2, \ldots, C_s$. All streams in a given orbit $C_i$ have the same period, denoted $\rho(i)$. For each $C_i$ we choose one stream
\(a_i \in C_i\), the base for \(C_i\). Therefore, the elements of \(C_i\) are all the shifts of the base \(a_i\) and we consider our base \(a_i\) to start at index 0.

For each \(\beta \in \mathbb{F}_q\) and \(1 \leq j \leq s\), consider \(b = (L - \beta)a_j\). Since \(b\) is annihilated by \(f\), \(b \in G(f)\) and so lies in some orbit \(C_i\). Since any two elements of a given orbit are shifts of each other, the orbit that \(b\) lies in is independent of the choice of the base \(a_j\) for orbit \(C_j\).

### 3.1 RUNS construction from [2]

In [2] it was observed that if \(f \in \mathbb{F}_q[x]\) is a degree \(t\) primitive polynomial and \(a\) is a fixed non-zero stream in \(G(f)\) then, for each \(\beta \in \mathbb{F}_q^*\), there exists \(k_\beta \in \mathbb{Z}_{q^t - 1}\) such that, for all \(n \in \mathbb{Z}\), the following holds:

\[
a_{n+1} - \beta a_n = a_{n-k_\beta}. \tag{3}
\]

From this observation, an OOA\((q^t; t, q+1, t, q)\) over the alphabet \(\mathbb{F}_q\) was constructed as follows: for each \(\beta \in \mathbb{F}_q^*\), a block with \(t\) columns was constructed where the first column is \(L^{k_\beta}a\) and each subsequent column is a left shift by \(k_\beta\) places of the previous column.

When \(f\) is primitive there are exactly two orbits, one of which is the trivial orbit containing only the all zeroes stream and the other is the orbit containing \(a\). Equation (3) is equivalent to stating that \((L - \beta)a = L^{-k_\beta}a\) and so \((L - \beta)\) maps the non-trivial orbit to itself (and the trivial orbit to itself).

Since \(L^{k_\beta}a = (L - \beta)^{-1}a\), a left shift of \(k_\beta\) positions is equivalent to applying \((L - \beta)^{-1}\) to the stream. Hence, the \(j\)th column in the block is the first \(q^t - 1\) elements of \((L - \beta)^{-j}a\).

Two additional special blocks are constructed and these \(q + 1\) blocks in total, each with \(t\) columns per block, yield the OOA\((q^t; t, q+1, t, q)\).

### 3.2 Generalized RUNS construction

By using the analysis in Section 3.1 to describe the construction in [2], we generalize this construction to include non-primitive polynomials satisfying some simple properties. For these polynomials, an OOA\((q^t; t, \gamma + 1, t, q)\) over the alphabet \(\mathbb{F}_q\) is constructed, where \(\gamma\) is the number of \(\beta \in \mathbb{F}_q^*\) that are not roots of \(f\). When \(f\) is primitive, \(\gamma = q\) and the resulting OOA\((q^t; t, q+1, t, q)\) is essentially the one produced in [2].

For \(f \in \mathbb{F}_q[x]\), a monic polynomial with non-zero constant term, let \(\Gamma_f = \{\beta_1, \beta_2, \ldots, \beta_\gamma\} \subseteq \mathbb{F}_q\) be the set of those \(\beta\) such that \((x - \beta, f(x)) = 1\). For each such \(\beta\), \((x - \beta)^{-1} \pmod{f}\) exists and so \((L - \beta)^{-1}\) is a well-defined function on \(G(f)\).

For each \(\beta_k \in \Gamma_f\) and each orbit \(C_i\), \(1 \leq i \leq s\), we construct a \(\rho_i \times t\) matrix \(M(i, \beta_k)\) with \(t\) columns and \(j\)th column defined by the first \(\rho(i)\) elements of \((L - \beta_k)^{-j}a_i\).
For each orbit $C_i$, we also have a special $\rho_i \times t$ matrix $M(i, \infty)$ with $t$ columns and $j$th column defined by the first $\rho(i)$ elements of

$$L^{j-1}a_i.$$ 

Define a matrix $M$ consisting of the submatrices $M(i, \beta_j), i \in \{1, 2, \ldots, s\}, \beta_j \in \{\infty\} \cup \Gamma_f$ arranged as below, where $\gamma = |\Gamma_f|$.

\[
\begin{array}{cccc}
C_1 \{ & M(1, \infty) & M(1, \beta_1) & M(1, \beta_2) \ldots M(1, \beta_\gamma) \\
C_2 \{ & M(2, \infty) & M(2, \beta_1) & M(2, \beta_2) \ldots M(2, \beta_\gamma) \\
& \ldots & \ldots & \ldots \ldots \ldots \ldots \\
C_s \{ & M(s, \infty) & M(s, \beta_1) & M(s, \beta_2) \ldots M(s, \beta_\gamma) \\
& Bl_M(0) & Bl_M(1) & Bl_M(2) & Bl_M(\gamma)
\end{array}
\]

In the next section, we prove that $M$ is an $OOA(q^t; t, t, \gamma + 1, q)$. In Section 3.1 we noted that two additional blocks were included in the RUNS construction. The Generalized RUNS construction shows that one of these blocks corresponds to the set of matrices $\{M(i, \infty) \mid 1 \leq i \leq s\}$ and the second corresponds to the set of matrices $\{M(i, 0) \mid 1 \leq i \leq s\}$ (note that $0 \in \Gamma_f$ always holds).

4 Correctness of the construction

The following result can be found in [13].

**Lemma 7.** The following are equivalent:

1. A set of $t$ columns $\{i_1, \ldots, i_t\}$ is covered in $M$.
2. There is no row $R = (r_0, r_1, \ldots, r_{t(\gamma + 1) - 1})$ other than the all-zero row of $M$ such that $r_{i_1} = \cdots = r_{i_t} = 0$.

One thing to note about the rows of the $M(i, \infty)$ submatrices is that their $s$th row, with rows indexed $0 \leq s \leq \rho(i) - 1$, is the first $t$ entries of $L^s a_i$. Equivalently these are the entries $s, s + 1, \ldots, s + t - 1$ of $a_i$. This is used in Case 1 in the following proof showing that the construction is valid.

**Theorem 8.** $M$ is an $OOA(q^t; t, t, \gamma + 1, q)$.

**Proof.** With needed changes, the proof follows the one given in [2] for primitive $f$.

Let $L$ be a left-justified set of $t$ columns in $M$ and let $B$ be the $q^t \times t$ array induced by the columns of $L$. Partition $L$ into sets $L_0, L_1, \ldots, L_\gamma$ where the columns of $L_i$ are in the $i$th block $Bl_M(i)$ and let $l_i = |L_i|, 0 \leq i \leq \gamma$. Thus, $0 \leq l_i \leq t$ and $t = \sum_{i=0}^{\gamma} l_i$. This implies $t - l_0 = \sum_{i=1}^{\gamma} l_i$, which is used a number of times in the proof.
Let \( R = (r_0, r_1, \ldots, r_{l-1}) \) be a row of \( B \). This row corresponds to some orbit \( C_t \) which, after a re-labeling of the orbits, we can assume to be \( C_1 \) having base \( \mathbf{a} \). This row corresponds to a row \( S = (s_0, s_1, \ldots, s_{l(\gamma+1)-1}) \) of the full matrix \( M \).

Suppose that \( S \) is not the all zeroes row. Hence, the base \( \mathbf{a} \) is not the all zeroes stream. We claim that \( R \) is not all zeroes. By way of contradiction, suppose that it is all zeroes and consider 3 cases: Case 1: \( l_0 > 0 \), Case 2: \( l_0 = 0 \) and \( s_0 \neq 0 \) and Case 3: \( l_0 = 0 \) and \( s_0 = 0 \).

In all cases, we find a run of zeroes of length \( l \geq 0 \) starting at some index \( n \) and create the polynomial \( P_l \) of degree \( t - l - 1 \) for this run. Then, letting \( z_k \) be the multiplicity of \( \beta_k \) as a root of \( P_l \), we use that fact that \( \sum_{k=1}^{\gamma} z_k \leq \deg(P_l) = t - l - 1 \) to derive the required contradiction.

Case 1: \((l_0 > 0)\) : Then, \((r_0, r_1, \ldots, r_{l_0-1}) = (s_0, s_1, \ldots, s_{l_0-1})\) and from what we noted earlier about \( M(0, \infty) \), this \( l_0 \)-tuple is \((\mathbf{a}_r, \mathbf{a}_{r+1}, \ldots, \mathbf{a}_{r+l_0-1})\), the first \( l_0 \) elements of \( L^\omega \mathbf{a} \) where \( \omega \) is the row index of \( R \) in the matrix \( M(1, \infty) \) (with indexing starting at 0).

If \( r_j \neq 0 \) for some \( 0 \leq j \leq l_0 - 1 \), we are done. So suppose that \( r_0 = r_1 = \cdots = r_{l_0-1} = 0 \). Thus, \( \mathbf{a} \) has a run of zeroes of length \( l' \geq l_0 \) starting at index \( n \leq \omega \) and ending at index \( n + l' - 1 \). Let \( P_{l'} \) be our polynomial of degree \( t - l' - 1 \) for this run of \( l' \) zeroes starting at index \( n \).

By Lemma 5 the \( z_k \) entries in matrix \( M(0, \beta_k) \) corresponding to the row \( S \) are all zero and the \((z_k + 1)\)st entry is not. Thus, since \( R \) is the all zeroes row, we must have \( l_k \leq z_k \) for \( 1 \leq k \leq \gamma \), giving \( \sum_{k=1}^{\gamma} l_k \leq \sum_{k=1}^{\gamma} z_k \). Hence, \( t - l_0 = \sum_{k=1}^{\gamma} l_k \leq \sum_{k=1}^{\gamma} z_k \leq t - l' - 1 \). This gives, \( l_0 \geq l' + 1 \), a contradiction.

Case 2 \((l_0 = 0, s_0 \neq 0)\) : Then \( \mathbf{a} \) contains a run of \( l_0 = 0 \) zeroes starting at index \( \omega \). Let \( P_0 \) be our polynomial of degree \( t - l_0 - 1 = t - 1 \) for this run of 0 zeroes starting at index \( \omega \).

By Lemma 6 the \( z_k \) entries in matrix \( M(i, \beta_k) \) corresponding to the row \( S \) are all zero and the \((z_k + 1)\)st entry is not. Since \( R \) is the all zeroes row, as before, we have \( l_k \leq z_k \) for all \( k \).

Hence \( \sum_{k=1}^{\gamma} l_k \leq \sum_{k=1}^{\gamma} z_k \) and, since \( t = \sum_{k=1}^{\gamma} l_k \), we have \( t \leq \sum_{k=1}^{\gamma} z_k \leq t - 1 \), a contradiction.

Case 3 \((l_0 = 0, s_0 = 0)\): Since \( S \) is not the all zeroes row, there exists a smallest \( t \geq 1 \) such that \( s_0 = s_1 = \cdots = s_{l-1} = 0 \), but \( s_l \neq 0 \). Thus, \( \mathbf{a} \) has a run of \( l' \geq l \) zeroes starting at index \( n \leq 0 \) and ending at index \( n + l' - 1 \). Let \( P_{l'} \) be our polynomial of degree \( t - l' - 1 \) for this run of \( l' \) zeroes starting at index \( n \).

By Lemma 6 the \( z_k \) entries in matrix \( M(i, \beta_k) \) corresponding to the row \( S \) are all zero and the \((z_k + 1)\)st entry is not. Since \( R \) is the all zeroes row, we must have \( l_k \leq z_k \) for \( 1 \leq k \leq \gamma \). As in Case 2, we get \( t = \sum_{k=1}^{\gamma} l_k \leq \sum_{k=1}^{\gamma} z_k \leq t - l' - 1 \) which gives \( l' \leq -1 \), a contradiction.

Thus all cases lead to a contradiction and so \( R \) is not the all zeroes row and hence \( L \) is covered by Lemma 7. Thus, \( M \) is an OOA\((q^t; t, t, \gamma + 1, q)\) as claimed.

As a corollary to this theorem, we have one of the main results of [2].
**Corollary 9.** An OOA\((q^t; t, q+1, t, q)\) over the alphabet \(\mathbb{F}_q\) can be derived from the LFSR defined by a degree \(t \geq 2\) primitive polynomial \(f \in \mathbb{F}_q[x]\).

**Proof.** Since \(f\) is primitive, \(f\) has no roots in \(\mathbb{F}_q\) and so \((x - \beta, f(x)) = 1\) for all \(\beta \in \mathbb{F}_q\). Thus, \(\Gamma_f = \mathbb{F}_q\) and Theorem 8 provides the required OOA\((q^t; t, q+1, t, q)\).

**Example 10.** Let \(f(x) = x^3 + x^2 + x + 1 = (x+1)^3 \in \mathbb{F}_2[x]\). Then \(G(f)\) is partitioned into 4 orbits, as shown in the following table along with its (arbitrarily chosen) base.

| \(j\) | \(a_j\) | period |
|------|--------|--------|
| 0    | 0011...| 4      |
| 1    | 01...  | 2      |
| 2    | 0...   | 1      |
| 3    | 1...   | 1      |

Hence, \(\Gamma_f = \{0\}\) and our OOA is the following \(8 \times 6\) matrix, partitioned into the 8 submatrices \(M(i, \beta)\) for \((i, \beta) \in \{0, 1, 2, 3\} \times \{\infty, 0\}\).

\[
\begin{array}{cccc}
M(0, \infty) & M(0, 0) & M(1, \infty) & M(1, 0) \\
0 & 0 & 1 & 1 \\
0 & 1 & 1 & 0 \\
1 & 1 & 0 & 0 \\
1 & 0 & 1 & 1 \\
M(2, \infty) & M(2, 0) & M(3, \infty) & M(3, 0) \\
0 & 0 & 1 & 1 \\
0 & 1 & 1 & 0 \\
1 & 1 & 1 & 0 \\
1 & 1 & 1 & 1 \\
\end{array}
\]

By Theorem 8, this is an OOA\((8; 3, 2, 3, 2)\) and is the one shown at the start of the paper.

**Example 11.** Let \(f(x) = x^4 + x^3 + 1 \in \mathbb{F}_2[x]\). Since \(f\) is primitive, \(G(f)\) is partitioned into 2 orbits. The following table shows their (arbitrarily chosen) bases.

| \(j\) | \(a_j\) | period |
|------|--------|--------|
| 0    | 000111101011001...| 15     |
| 1    | 0...   | 1      |

Hence, \(\Gamma_f = \mathbb{F}_2\) and our OOA is the following \(16 \times 12\) matrix which is partitioned into the 6 submatrices \(M(i, \beta)\), one for each for \((i, \beta) \in \{0, 1\} \times (\Gamma_f \cup \{\infty\})\).

\[
\begin{array}{cccc}
M(0, \infty) & M(0, 0) & M(0, 1) & M(1, \infty) \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 \\
1 & 1 & 0 & 1 \\
1 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 \\
\end{array}
\]
By Theorem 8, this is an OOA(16; 4, 3, 4, 2) and is essentially the one that would be constructed by the RUNS construction of [2].

5 Comparison of constructions in \( \mathbb{F}_2[x] \)

In this section we provide some data about the OOA\( s \) produced by our new construction. First, in Table 1 when the GR construction provides an OOA with \( t(q+1) \) columns, as the RUNS construction and the Rosenbloom/Tsfasman/Skriganov (RTS) construction do, we compare the percentage of \( t \)-sets covered.

In this table, \# is the number of OOA\( s \) produced by the method, \( R_{\min}, R_{\max}, R_{\text{avg}} \), \( GR_{\min}, GR_{\max} \) and \( GR_{\text{avg}} \) give the minimum, maximum and average percentage coverage for the RUNS and GR constructions, respectively. For the RUNS construction, \# is the number of primitive polynomial in \( \mathbb{F}_2[x] \) of degree \( t \) and for the GR construction, \# is the number of polynomials of degree \( t \) with no roots in \( \mathbb{F}_2 \). The RTS construction produces exactly one OOA and the corresponding entry in the table is the percentage of \( t \)-sets covered for this OOA. Boldfaced entries indicate when a non-primitive polynomial gives an OOA with coverage that is at least as good as when only primitive polynomials are used.

Secondly, for those OOA\( s \) produced by the GR construction which have the maximum number of \( t \)-sets of columns covered, Table 2 provides the polynomial(s) that produce the corresponding OOA\( (s) \). In the “Property” column of these table, \( P \) denotes a primitive polynomial, \( I \) denotes an irreducible but not primitive polynomial and \( R \) denotes a reducible polynomial, whose factorization is provided. Observe that when \( t = 8 \), the unique polynomial that provides the best coverage is reducible and shows that, in general, primitivity is not essential for best coverage.

| \( t \) | \( \text{cols} \) | \# | \( GR_{\min} \) | \( GR_{\max} \) | \( GR_{\text{avg}} \) | \( \# \) | \( R_{\min} \) | \( R_{\max} \) | \( R_{\text{avg}} \) | \( \# \) | \( \text{RTS} \) |
|-------|------------|-----|-------------|-------------|-------------|-----|-------------|-------------|-------------|-----|------------|
| 2     | 6          | 1   | 0.7333      | 0.7333      | 0.7333      | 1   | 0.7333      | 0.7333      | 0.7333      | 1   | 0.7333     |
| 3     | 9          | 2   | 0.5952      | 0.5952      | 0.5952      | 2   | 0.5952      | 0.5952      | 0.5952      | 1   | 0.4643     |
| 4     | 12         | 4   | 0.3556      | 0.5232      | 0.4323      | 2   | 0.4848      | 0.5232      | 0.5040      | 1   | 0.3455     |
| 5     | 15         | 8   | 0.3413      | 0.4695      | 0.4186      | 6   | 0.3862      | 0.4695      | 0.4444      | 1   | 0.1968     |
| 6     | 18         | 16  | 0.2265      | 0.4465      | 0.3627      | 6   | 0.3891      | 0.4465      | 0.4100      | 1   | 0.1357     |
| 7     | 21         | 32  | 0.3088      | 0.4237      | 0.3660      | 18  | 0.3088      | 0.4237      | 0.3631      | 1   | 0.0897     |
| 8     | 24         | 64  | 0.0814 \( \textbf{0.4174} \) | 0.3364      | 16  | 0.3471      | 0.3984      | 0.3777      | 1   | 0.0736     |
Table 2: Polynomials in $\mathbb{F}_2[x]$ giving maximum coverage.

| $t$ | cols | Polynomial | Property | Factorization |
|-----|------|------------|----------|---------------|
| 2   | 6    | $x^2 + x + 1$ | P        |               |
| 3   | 9    | $x^3 + x + 1$ | P        | $x^2 + 1$     |
|     |      | $x^3 + x^2 + 1$ | P        |               |
| 4   | 12   | $x^4 + x^3 + 1$ | P        |               |
| 5   | 15   | $x^5 + x^4 + x^3 + x + 1$ | P        |               |
| 6   | 18   | $x^6 + x^4 + x^3 + x + 1$ | P        |               |
| 7   | 21   | $x^7 + x^5 + x^2 + x + 1$ | P        |               |
| 8   | 24   | $x^8 + x^6 + x^4 + x^3 + 1$ | R        | $(x^2 + x + 1)(x^6 + x^5 + x^4 + x + 1)$ |

For some applications, there may not be a need for the OOA to have the maximum number of columns, but it may be that the percentage of covered $t$-sets of columns is more important. Table 3 provide statistics on the coverage in the OOAs produced by the GR construction when the maximum number of columns is not produced.

Table 3: Percentage of covered $t$-sets for OOAs using GR construction in $\mathbb{F}_2$.

| $t$ | cols | #   | $GR_{min}$ | $GR_{max}$ | $GR_{avg}$ |
|-----|------|-----|------------|------------|------------|
| 2   | 4    | 1   | 0.6667     | 0.6667     | 0.6667     |
| 3   | 6    | 2   | 0.4000     | 0.6000     | 0.5000     |
| 4   | 8    | 4   | 0.2286     | 0.6286     | 0.4893     |
| 5   | 10   | 8   | 0.1270     | 0.6190     | 0.4719     |
| 6   | 12   | 16  | 0.2265     | 0.5541     | 0.4467     |
| 7   | 14   | 32  | 0.0373     | 0.5035     | 0.3957     |
| 8   | 16   | 64  | 0.0199     | 0.4867     | 0.3717     |

In Appendix A we provide similar analyses for $\mathbb{F}_q[x]$ when $q = 3, 4, 5, 7, 8, 9$.

6 Summary

In this paper we generalize the construction of OOAs given in [2] from using LFSRs defined by primitive polynomials to LFSRs using a far larger class of polynomials. While doing so, we also significantly simplify the proofs from [2]. For small field size and small degree, we provide data on how close the OOAs constructed are to being full OAs and compare the results to earlier constructions. Provided examples show that primitivity is not a requirement for the construction of OOAs having best coverage.
References

[1] R. C. Bose, “Mathematical theory of the symmetrical factorial design”, *Sankhya*, vol. 8, no. 2, pp. 107-166, 1947.

[2] A. G. Castoldi, L. Moura, D. Panario and B. Stevens, “Ordered orthogonal array construction using LFSR sequences,” *IEEE Trans. Info. Theory*, vol. 63, no. 2, pp. 1336-1347, 2017.

[3] C. J. Colbourn and J. H. Dinitz, *Handbook of Combinatorial Designs*. Second Edition, Chapman & Hall/CRC, Boca Raton, 2006.

[4] S. W. Golomb and G. Gong, *Signal Design for Good Correlation for Wireless Communication, Cryptography, and Radar*. Cambridge University Press, Cambridge, 2005.

[5] A. S. Hedayat, N. J. A. Sloane and J. Stufken, *Orthogonal Arrays: Theory and Applications*. Springer, 1999.

[6] T. Krikorian, *Combinatorial Constructions of Ordered Orthogonal Arrays and Ordered Covering Arrays*. MSc. Thesis, Ryerson University, 2011.

[7] K. M. Lawrence, “A combinatorial characterization of \((t, m, s)\)-nets in base \(b\),” *J. Combin. Des.*, vol. 4, pp. 275–293, 1996.

[8] R. Lidl and H. Niederreiter, *Finite Fields*. Cambridge University Press, Cambridge, 1997.

[9] L. Moura, G. L. Mullen and D. Panario, “Finite field constructions of combinatorial arrays,” *Des. Codes Cryptogr.* vol. 78, pp. 197–219, 2016.

[10] G. L. Mullen and D. Panario, *Handbook of Finite Fields*. Chapman & Hall/CRC, Boca Raton, 2013.

[11] G. L. Mullen and W. Ch. Schmid, “An equivalence between \((t, m, s)\)-nets and strongly orthogonal hypercubes,” *J. Combin. Theory A*, vol. 76, pp. 164–174, 1996.

[12] A. Munemasa, “Orthogonal arrays, primitive trinomials, and shift-register sequences,” *Finite Fields Appl.*, vol. 4, pp. 252–260, 1998.

[13] S. Raaphorst, L. Moura, and B. Stevens, “A construction for strength-3 covering arrays from linear feedback shift register sequences,” *Des. Codes Cryptogr.*, vol. 73, pp. 949–968, 2014.

[14] S. Roman, *Coding and Information Theory*. Springer, 1992.

[15] M. Y. Rosenbloom and M. A. Tsfasman, “Codes for \(m\)-metric,” *Probl. Inf. Transm.*, vol. 33, pp. 45–52, 1997.
A Statistical data for OOA produced by GR in $\mathbb{F}_q$, $q = 3, 4, 5, 7, 8, 9$

As was done in Section 5, we provide data about the OOA(s) produced by our new construction for larger fields. For some fields and polynomial degree, when the number of polynomials giving the OOA(s) with best coverage is large, we do not provide the polynomials but only a count.

| $t$ cols | Polynomial | Property | Factorization |
|---------|------------|----------|---------------|
| 2 8     | $x^2 + x + 2$ | $P$ |                 |
| 3 12    | $x^3 + 2x^2 + 1$ | $P$ |                 |
|         | $x^3 + x^2 + 2$ | $I$ |                 |
| 4 16    | $x^4 + x^3 + x^2 + 2x + 2$ | $P$ |                 |
|         | $x^4 + 2x^3 + 2x^2 + x + 2$ | $P$ |                 |
| 5 20    | $x^5 + 2x^4 + x^3 + 2x^2 + 2x + 1$ | $I$ |                 |
|         | $x^5 + 2x^3 + 2x^2 + 2x + 1$ | $I$ |                 |
| 6 24    | $x^6 + 2x^5 + x^4 + 2x^3 + 2x^2 + x + 1$ | $R$ | $(x^2 + 1)(x^4 + x^3 + x + 1)$ |
|         | $x^6 + 2x^5 + 2x^4 + 2x^3 + 2x^2 + 2x + 1$ | $R$ | $(x^2 + 1)(x^4 + x^2 + 2x + 1)$ |

Table 6: Percentage of covered $t$-sets for OOA using GR construction in $\mathbb{F}_3$.

| $t$ cols | # | $G_{\text{min}}$ | $G_{\text{max}}$ | $G_{\text{avg}}$ |
|---------|---|----------------|----------------|----------------|
| 2 6     | 2 | 0.7351         | 0.7333         | 0.7333         |
| 4 1     | 2 | 0.6667         | 0.6667         | 0.6667         |
| 3 6     | 8 | 0.5457         | 0.7262         | 0.6256         |
| 9 2     | 2 | 0.9000         | 0.9000         | 0.9000         |
| 4 12    | 24| 0.4808         | 0.7455         | 0.6535         |
| 8 6     | 22| 0.2286         | 0.8571         | 0.5405         |
| 5 15    | 72| 0.3613         | 0.7081         | 0.6037         |
| 10 18   | 5 | 0.2540         | 0.7098         | 0.6332         |
| 8 18    | 216| 0.1872        | 0.8740         | 0.6975         |
| 12 54   | 0.0693        | 0.7370         | 0.5853         |
Table 7: Comparison between GR and RUNS constructions in $F_4$.

| $t$ | cols | # | $GR_{min}$ | $GR_{max}$ | $GR_{avg}$ | # | $R_{min}$ | $R_{max}$ | $R_{avg}$ | # | $RTS$ |
|-----|------|---|------------|------------|------------|---|------------|------------|------------|---|-------|
| 2   | 10   | 6 | 0.8667     | 0.8667     | 0.8667     | 4 | 0.8667     | 0.8667     | 0.8667     | 1 | 0.7556 |
| 3   | 15   | 20| 0.6505     | 0.8210     | 0.7585     | 12| 0.7604     | 0.8220     | 0.7912     | 1 | 0.4879 |
| 4   | 20   | 81| 0.5317     | 0.7670     | 0.7279     | 32| 0.7397     | 0.7641     | 0.7524     | 1 | 0.4017 |
| 5   | 25   | 324| 0.6165     | 0.7423     | 0.7141     | 120| 0.6165     | 0.7423     | 0.7133     | 1 | 0.2268 |

Table 8: Polynomials in $F_4[x]$ giving maximum coverage.

| $t$ | cols | Polynomial | Property |
|-----|------|------------|----------|
| 2   | 10   | $x^2 + \omega x + \omega$ | P |
|     |      | $x^2 + (\omega + 1)x + \omega + 1$ | P |
|     |      | $x^2 + x + \omega$ | P |
|     |      | $x^2 + x + 1$ | I |
|     |      | $x^2 + \omega x + 1$ | I |
|     |      | $x^2 + (\omega + 1)x + 1$ | I |
| 3   | 15   | $x^3 + \omega x^2 + (\omega + 1)x + \omega$ | P |
|     |      | $x^3 + \omega x^2 + (\omega + 1)x + \omega + 1$ | P |
|     |      | $x^3 + (\omega + 1)x^2 + \omega x + \omega$ | P |
|     |      | $x^3 + (\omega + 1)x^2 + \omega x + 1$ | P |
|     |      | $x^3 + x^2 + x + \omega$ | P |
|     |      | $x^3 + x^2 + x + 1$ | P |
| 4   | 20   | $x^4 + \omega x^3 + (\omega + 1)x^2 + \omega + 1$ | I |
|     |      | $x^4 + \omega x^3 + x^2 + \omega + 1$ | I |
|     |      | $x^4 + (\omega + 1)x^3 + (\omega + 1)x^2 + \omega + 1$ | I |
|     |      | $x^4 + (\omega + 1)x^3 + (\omega + 1)x + 1$ | I |
|     |      | $x^4 + x^3 + \omega x^2 + \omega + 1$ | I |
|     |      | $x^4 + x^3 + (\omega + 1)x^2 + \omega + 1$ | I |
|     |      | $x^4 + x^3 + (\omega + 1)x^2 + (\omega + 1)x + 1$ | I |
| 5   | 25   | $x^5 + \omega x^4 + x^3 + \omega x^2 + \omega$ | P |
|     |      | $x^5 + (\omega + 1)x^4 + x^3 + (\omega + 1)x^2 + \omega + 1$ | P |
|     |      | $x^5 + x^4 + \omega x^3 + \omega x^2 + \omega + 1$ | P |
|     |      | $x^5 + x^4 + (\omega + 1)x^3 + (\omega + 1)x^2 + \omega$ | P |
|     |      | $x^5 + x^4 + (\omega + 1)x^3 + (\omega + 1)x + 1$ | P |
|     |      | $x^5 + (\omega + 1)x^4 + (\omega + 1)x^3 + \omega x^2 + 1$ | I |

Table 9: Percentage of covered $t$-sets for OOA$s using GR construction in $F_4$.

| $t$ | cols | # | $GR_{min}$ | $GR_{max}$ | $GR_{avg}$ |
|-----|------|---|------------|------------|------------|
| 2   | 8    | 3 | 0.7500     | 0.7500     | 0.7500     |
|     | 6    | 3 | 0.7333     | 0.7333     | 0.7333     |
| 3   | 12   | 21| 0.7545     | 0.7591     | 0.7558     |
|     | 9    | 6 | 0.8214     | 0.8214     | 0.8214     |
|     | 6    | 1 | 0.4000     | 0.4000     | 0.4000     |
| 4   | 16   | 81| 0.3868     | 0.7573     | 0.7263     |
|     | 12   | 27| 0.3556     | 0.8564     | 0.7542     |
|     | 8    | 3 | 0.4714     | 0.4714     | 0.4714     |
| 5   | 20   | 324| 0.4717     | 0.7608     | 0.7135     |
|     | 15   | 108| 0.3413     | 0.7812     | 0.7016     |
|     | 10   | 12| 0.2540     | 0.7063     | 0.5714     |
Table 10: Comparison between GR and RUNS constructions in $\mathbb{F}_5$.

| $t$ | cols | $GR_{min}$ | $GR_{max}$ | $GR_{avg}$ | $R_{min}$ | $R_{max}$ | $R_{avg}$ | # RTI |
|-----|------|------------|------------|------------|-----------|-----------|-----------|-------|
| 2   | 12   | 100.00     | 0.8788     | 0.8667     | 4         | 0.8788    | 0.8788    | 1      |
| 3   | 18   | 0.8100     | 0.8395     | 0.8244     | 20        | 0.8100    | 0.8395    | 1      |
| 4   | 24   | 0.6763     | 0.8095     | 0.7808     | 48        | 0.7768    | 0.8015    | 1      |

Table 11: Polynomials in $\mathbb{F}_5[x]$ giving maximum coverage.

| $t$ | cols | Polynomial | Property |
|-----|------|------------|----------|
| 2   | 12   | $x^2 + x + 2$ | P        |
|     |      | $x^2 + 2x + 3$ | P        |
|     |      | $x^2 + 3x + 3$ | P        |
|     |      | $x^2 + 4x + 2$ | P        |
|     |      | $x^2 + 2$     | I        |
|     |      | $x^2 + 3$     | I        |
| 3   | 18   | $x^3 + 3x + 2$ | P        |
|     |      | $x^3 + 3x + 3$ | P        |
|     |      | $x^3 + x^2 + 2$ | P        |
|     |      | $x^3 + 4x^2 + 3$ | P        |
|     |      | $x^3 + 2x + 1$ | I        |
|     |      | $x^3 + 2x + 4$ | I        |
|     |      | $x^3 + 2x^2 + 1$ | I        |
|     |      | $x^3 + 3x^2 + 4$ | I        |
| 4   | 24   | $x^4 + x^3 + 2x^2 + x + 3$ | I        |
|     |      | $x^4 + 2x^3 + 3x^2 + 3x + 3$ | I        |
|     |      | $x^4 + 3x^3 + 3x^2 + 2x + 3$ | I        |
|     |      | $x^4 + 4x^3 + 2x^2 + 4x + 3$ | I        |

Table 12: Percentage of covered $t$-sets for OOA$s using GR construction in $\mathbb{F}_5$.

| $t$ | cols | # | $GR_{min}$ | $GR_{max}$ | $GR_{avg}$ |
|-----|------|---|------------|------------|------------|
| 2   | 10   | 4 | 0.8667     | 0.8667     | 0.8667     |
| 3   | 15   | 44| 0.7739     | 0.8505     | 0.8096     |
|     | 12   | 12| 0.7455     | 0.7636     | 0.7530     |
|     | 9    | 4 | 0.7619     | 0.7619     | 0.7619     |
| 4   | 20   | 204| 0.7129    | 0.8233     | 0.7845     |
|     | 16   | 78 | 0.7412     | 0.8495     | 0.8067     |
|     | 12   | 12| 0.7939     | 0.8364     | 0.8222     |
|     | 8    | 1 | 0.2286     | 0.2286     | 0.2286     |
Table 13: Comparison between GR and RUNS constructions in $\mathbb{F}_7$.

| $t$ | cols | GR_{min} | GR_{max} | GR_{avg} | RUNS_{min} | RUNS_{max} | RUNS_{avg} | # | RTS |
|-----|------|----------|----------|----------|-------------|-------------|-------------|---|-----|
| 2   | 16   | 21       | 0.9017   | 0.9083   | 0.9083      | 0.9083      | 0.9083      | 1 | 0.7583 |
| 3   | 24   | 112      | 0.8375   | 0.8898   | 0.8671      | 0.8671      | 0.8671      | 1 | 0.5830 |
| 4   | 32   | 819      | 0.8175   | 0.8643   | 0.8643      | 0.8643      | 0.8643      | 1 | 0.4654 |

Table 14: Polynomials in $\mathbb{F}_7[x]$ giving maximum coverage.

| $t$ | cols | Polynomial | Property |
|-----|------|------------|----------|
| 2   | 16   | $x^2 + x + 3$ | P        |
|     |      | $x^2 + 2x + 3$ | P        |
|     |      | $x^2 + 2x + 5$ | P        |
|     |      | $x^2 + 3x + 5$ | P        |
|     |      | $x^2 + 4x + 5$ | P        |
|     |      | $x^2 + 5x + 3$ | P        |
|     |      | $x^2 + 5x + 5$ | P        |
|     |      | $x^2 + 6x + 3$ | P        |
|     |      | $x^2 + x + 6$  | I        |
|     |      | $x^2 + 3x + 6$  | I        |
|     |      | $x^2 + 4x + 6$  | I        |
|     |      | $x^2 + 6x + 6$  | I        |
| 3   | 24   | $x^3 + x^2 + 5x + 2$ | P        |
|     |      | $x^3 + 2x^2 + 6x + 2$ | P        |
|     |      | $x^3 + 4x^2 + 3x + 2$ | P        |
|     |      | $x^3 + 3x^2 + 3x + 5$ | I        |
|     |      | $x^3 + 5x^2 + 6x + 5$ | I        |
|     |      | $x^3 + 6x^2 + 5x + 5$ | I        |
| 4   | 32   | $x^4 + x^3 + 6x^2 + 2x + 5$ | P        |
|     |      | $x^4 + 2x^3 + 3x^2 + 2x + 3$ | P        |
|     |      | $x^4 + 5x^3 + 3x^2 + 5x + 3$ | P        |
|     |      | $x^4 + 6x^3 + 6x^2 + 5x + 5$ | P        |
|     |      | $x^4 + 3x^3 + 5x^2 + 5x + 6$ | I        |
|     |      | $x^4 + 4x^3 + 5x^2 + 2x + 6$ | I        |

Table 15: Percentage of covered $t$-sets for OOA(s) using GR construction in $\mathbb{F}_7$.

| $t$ | cols | # | GR_{min} | GR_{max} | GR_{avg} |
|-----|------|---|----------|----------|----------|
| 2   | 14   | 6 | 0.9121   | 0.9121   | 0.9121   |
|     | 12   | 15| 0.8485   | 0.8788   | 0.8667   |
| 3   | 21   | 132 | 0.8146 | 0.8925 | 0.8629 |
|     | 18   | 30 | 0.8407 | 0.8824 | 0.8652 |
|     | 15   | 20 | 0.8750 | 0.8879 | 0.8681 |
| 4   | 28   | 804 | 0.8232 | 0.8666 | 0.8505 |
|     | 24   | 360 | 0.7987 | 0.8667 | 0.8459 |
|     | 20   | 60 | 0.8285 | 0.8716 | 0.8498 |
|     | 16   | 15 | 0.7396 | 0.8071 | 0.7809 |
Table 16: Comparison between $GR$ and $RUNS$ constructions in $\mathbb{F}_8$.

| $t$ | $cols$ | $GR_{min}$ | $GR_{max}$ | $GR_{avg}$ | $R_{min}$ | $R_{max}$ | $R_{avg}$ | # | RTS |
|-----|--------|------------|------------|------------|------------|------------|------------|---|-----|
| 2   | 18     | 28         | 0.9346     | 0.9346     | 0.9346     | 18         | 0.9346     | 0.9346 | 0.9346 | 1     | 0.7582 |
| 3   | 27     | 168        | 0.8776     | 0.8916     | 0.8844     | 144        | 0.8776     | 0.8916 | 0.8844 | 1     | 0.4909 |

Table 17: Polynomials in $\mathbb{F}_8[x]$ giving maximum coverage.

| $t$ | $cols$ | # polynomials | Property |
|-----|--------|---------------|----------|
| 2   | 18     | 18            | P        |
|     |        | 10            | I        |
|     |        | 0             | R        |
| 3   | 27     | 18            | P        |
|     |        | 10            | I        |
|     |        | 0             | R        |

Table 18: Percentage of covered $t$-sets for $OOAs$ using $GR$ construction in $\mathbb{F}_8$.

| $t$ | $cols$ | $GR_{min}$ | $GR_{max}$ | $GR_{avg}$ | $R_{min}$ | $R_{max}$ | $R_{avg}$ | # | RTS |
|-----|--------|------------|------------|------------|------------|------------|------------|---|-----|
| 2   | 16     | 7          | 0.7583     | 0.7583     | 0.7583     |            |            | 1     |     |
|     | 14     | 21         | 0.9121     | 0.9121     | 0.9121     |            |            | 1     |     |
| 3   | 24     | 203        | 0.8518     | 0.8528     | 0.8569     |            |            | 1     |     |
|     | 21     | 42         | 0.8789     | 0.8805     | 0.8797     |            |            | 1     |     |
|     | 18     | 35         | 0.8505     | 0.8615     | 0.8571     |            |            | 1     |     |

Table 19: Comparison between $GR$ and $RUNS$ constructions in $\mathbb{F}_9$.

| $t$ | $cols$ | $GR_{min}$ | $GR_{max}$ | $GR_{avg}$ | $R_{min}$ | $R_{max}$ | $R_{avg}$ | # | RTS |
|-----|--------|------------|------------|------------|------------|------------|------------|---|-----|
| 2   | 20     | 36         | 0.9158     | 0.9263     | 0.9263     | 16         | 0.9263     | 0.9263 | 0.9263 | 1     | 0.7579 |
| 3   | 30     | 240        | 0.8702     | 0.9086     | 0.9015     | 96         | 0.8704     | 0.9086 | 0.9015 | 1     | 0.5872 |

Table 20: Polynomials in $\mathbb{F}_9[x]$ giving maximum coverage.

| $t$ | $cols$ | # polynomials | Property |
|-----|--------|---------------|----------|
| 2   | 20     | 16            | P        |
|     |        | 1             | I        |
|     |        | 0             | R        |
| 3   | 30     | 8             | P        |
|     |        | 8             | I        |
|     |        | 0             | R        |

Table 21: Percentage of covered $t$-sets for $OOAs$ using $GR$ construction in $\mathbb{F}_9$.

| $t$ | $cols$ | $GR_{min}$ | $GR_{max}$ | $GR_{avg}$ | $R_{min}$ | $R_{max}$ | $R_{avg}$ | # | RTS |
|-----|--------|------------|------------|------------|------------|------------|------------|---|-----|
| 2   | 18     | 8          | 0.9346     | 0.9346     | 0.9346     |            |            | 1     |     |
|     | 16     | 28         | 0.8917     | 0.9083     | 0.9012     |            |            | 1     |     |
| 3   | 27     | 296        | 0.5874     | 0.9121     | 0.8908     |            |            | 1     |     |
|     | 24     | 56         | 0.8933     | 0.9032     | 0.8991     |            |            | 1     |     |
|     | 21     | 56         | 0.8421     | 0.9105     | 0.8922     |            |            | 1     |     |