NEW CONSTRUCTIONS OF CIRCULANT AND INVOLUTORY MDS MATRICES

Bocong Chen¹, Martianus Frederic Ezerman², San Ling², Buket Özkaya²

¹ School of Mathematics, South China University of Technology, Guangzhou, Guangdong, 510641, China,
² School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, Singapore 637371

Abstract. Circulant MDS matrices are important, not only as a topic in coding theory but also due to their cryptographic applications, particularly in the design of hash functions and block ciphers. In this letter, we propose a new construction of circulant MDS matrices from double-circulant codes over finite fields. As a consequence, we explicitly construct circulant involutory MDS matrices over finite fields of odd size.

1. Introduction

Maximum distance separable (MDS) codes are optimal. They have the best error correction capability among linear codes of fixed length and size over a given finite field. As a coding theoretical object, an MDS matrix is the redundant part of the standard generator matrix of an MDS code. Such matrices are crucial in the design of numerous hash functions and block ciphers. Their maximal diffusion property injects a strong defense into the substitution and permutation network against differential and linear cryptanalyses. The MixColumn step in the Advanced Encryption System (AES) [1, Section 3.4.3], for example, uses a 4 × 4 circulant MDS matrix over \( \mathbb{F}_{2^8} \). Note that MDS matrices derived from Generalized Reed Solomon (GRS) codes are generally not circulant.

An involutory matrix is its own inverse. Many deployment scenarios require both the MixColumn and its inverse operations to be carried out. To implement the two inverse operations in lightweight devices, where storage and the number of available logic gates are severely constrained, circulant and involutory MDS matrices are strongly preferred [2]. However, over any field of characteristic 2, except for \( M = (1) \), such a matrix does not exist [3]. Cauchois and Loidreau gave a simpler algebraic proof of the nonexistence result in [4]. For fields of odd characteristic, they conjectured the parameters for which circulant involutory MDS matrices exist.

Rich literature has grown out of the sustained interest in constructing MDS matrices with desirable properties such as being circulant or involutory or with small XOR counts. Lacan
and Fimes [5] constructed MDS matrices using two Vandermonde matrices over any finite field. Sajadieh et al. also used two Vandermonde matrices to build an involutory MDS matrix in [6]. Other notable prior proposals can be found in [3, Refs. 1, 12–14, 17, 20, 25] and in [4, Refs. 2, 9, 12–14]. The above nonexistence result also led researchers to consider recursive MDS matrices, which can be written as a power of some companion matrices, e.g., in [7], or skew-circulant MDS matrices, e.g., in [4].

Double-circulant codes are particular quasi-cyclic (QC) codes of index 2 with systematic generator matrices. They are known to be asymptotically good [8, 9]. In this work, we characterize MDS double-circulant codes using their parity-check matrices, which are constructed via the spectral method given by Semenov and Trifonov in [10]. Cyclic MDS codes have been extensively studied in the literature. To our best knowledge, however, not much is known about the QC codes that are MDS, beyond the treatment given in [11].

The paper is organized as follows. We begin with basic notation and known results in Section 2. Section 3 presents a new construction of circulant MDS matrices over finite fields from double-circulant MDS codes. As a corollary, a class of circulant involutory MDS matrices over fields of odd characteristic is derived. Section 4 provides a conclusion.

2. Preliminaries

Let \( \mathbb{F}_q \) denote the finite field with \( q \) elements, where \( q \) is a power of a prime number. A linear \([n, k, d]_q\) code \( C \) is a \( k \)-dimensional subspace of \( \mathbb{F}_q^n \) with minimum (Hamming) distance \( d \). Such a code \( C \) is commonly represented by either its \( k \times n \) generator matrix \( G \) with entries in \( \mathbb{F}_q \) or its \((n - k) \times n\) parity-check matrix \( H \) with entries in \( \mathbb{F}_q \) or in some extension \( \mathbb{F}_{q^r} \) of \( \mathbb{F}_q \), where \( r \geq 1 \) (see [12, Ch. 7. §7]). Using Gaussian elimination, the generator matrix \( G \) can be given in the standard (or systematic) form \( G = (I_k \mid M) \) and \( H = (-M^T \mid I_{n-k}) \) is a corresponding parity-check matrix (see [12, Ch. 1. §2]), where \( I_t \) denotes the \( t \times t \) identity matrix, for any integer \( t > 0 \).

A linear \([n, k, d]_q\) code is called MDS if its parameters attain equality in the Singleton bound, which states \( d \leq n - k + 1 \) (e.g., see [12, Theorem 11 in Ch. 1. §10.]). A \( k \times m \) matrix \( M \) over \( \mathbb{F}_q \) is MDS if \( G = (I_k \mid M) \) is a generator matrix of an MDS code in the standard form, i.e., \( M \) is the redundant part of \( G \). Despite this easy characterization, the problem of finding the longest possible MDS code with a given dimension and base field size is not completely solved so far. The MDS conjecture, posed by Segre in 1957, states that the length \( n \) of a linear MDS code of dimension \( 2 \leq k \leq q \) over \( \mathbb{F}_q \) must satisfy \( n \leq k + q \), unless \( k = 3 \) or \( k = q - 1 \) and \( q \) is even, in which case \( n \leq k + q + 2 \). If \( k > q \), then \( n \leq k + 1 \), which was shown by Bush in [13]. For a nice survey on the MDS conjecture together with some partial cases that are proven (e.g., \( k = 2 \) and \( k = q \) cases), we refer the reader to Chapter 11 in [12]. The conjecture is proven for \( k \leq \text{char}(\mathbb{F}_q) \) in [14] and for \( k \leq 2 \cdot \text{char}(\mathbb{F}_q) - 2 \) when \( q \) is not prime in [15].

An \( m \times m \) circulant matrix is generated by a vector \( \vec{a} = (a_0, a_1, \ldots, a_{m-1}) \) or, equivalently, by the coefficients of a polynomial \( A(x) \in \mathbb{F}_q[x] \) of degree at most \( m - 1 \). More formally, given
\( \vec{a} \in \mathbb{F}_q^m \) or its corresponding polynomial \( A(x) = a_0 + a_1 x + \cdots + a_{m-1} x^{m-1} \in \mathbb{F}_q[x] \), the matrix

\[
A = \begin{pmatrix}
  a_0 & a_1 & \cdots & a_{m-2} & a_{m-1} \\
  a_{m-1} & a_0 & \cdots & a_{m-3} & a_{m-2} \\
  \vdots & \vdots & \ddots & \vdots & \vdots \\
  a_2 & a_3 & \cdots & a_0 & a_1 \\
  a_1 & a_2 & \cdots & a_{m-1} & a_0
\end{pmatrix}
\]  

is the \textit{circulant matrix} associated with the vector \( \vec{a} \) or the polynomial \( A(x) \). Consider the ideal \( (x^m - 1) = \{ f(x) (x^m - 1) \mid f(x) \in \mathbb{F}_q[x] \} \) of \( \mathbb{F}_q[x] \) and define the quotient ring \( R := \mathbb{F}_q[x]/(x^m - 1) \), which contains the polynomials of degree up to \( m - 1 \). Observe that the ring of \( m \times m \) circulant matrices over \( \mathbb{F}_q \) is isomorphic to \( R \) by the association \( A \hookrightarrow A(x) \).

Let \( m \) and \( \ell \) be positive integers. A linear code \( C \subseteq \mathbb{F}_q^{m \ell} \) is \textit{quasi-cyclic} of index \( \ell \) if its codewords are closed under cyclic shift by \( \ell \) positions and \( \ell \) is the smallest number with this property. The code \( C \) is cyclic when \( \ell = 1 \). A general theory of QC codes over finite fields can be found in [16, 17, 10]. The polynomial description of QC codes plays a central role in all of these works. To establish this description, we first write each element in \( \mathbb{F}_q \) as an \( m \times \ell \) array

\[
\vec{c} = \begin{pmatrix}
  c_{0,0} & \cdots & c_{0,\ell-1} \\
  \vdots & \ddots & \vdots \\
  c_{m-1,0} & \cdots & c_{m-1,\ell-1}
\end{pmatrix},
\]

so that being closed under shift by \( \ell \) units in \( \mathbb{F}_q^{m \ell} \) corresponds to being invariant under row shift in \( \mathbb{F}_q^{m \times \ell} \). We can associate \( \vec{c} \in \mathbb{F}_q^{m \times \ell} \) as in (2) with an element of \( R^\ell \) by mapping each column to a polynomial in \( R \) as \( \vec{c}(x) := (c_0(x), c_1(x), \ldots, c_{\ell-1}(x)) \in R^\ell \), where for each \( 0 \leq t \leq \ell - 1 \),

\[
c_t(x) := c_{0,t} + c_{1,t} x + c_{2,t} x^2 + \cdots + c_{m-1,t} x^{m-1} \in R.
\]

Then, the map \( \phi : \mathbb{F}_q^{m \ell} \rightarrow R^\ell \) such that \( \phi(\vec{c}) = \vec{c}(x) \) is an \( R \)-module isomorphism.

Note that the row shift in \( \mathbb{F}_q^{m \times \ell} \) amounts to componentwise multiplication by \( x \) in \( R^\ell \). Thus, a QC code \( C \) of length \( m \ell \) and index \( \ell \) over \( \mathbb{F}_q \) is an \( R \)-submodule in \( R^\ell \).

Now we describe the Discrete Fourier Transform (or the Mattson-Solomon transform) induced by the polynomials in \( R \). For the details and the proofs of the results presented below, we refer the reader to [17, §V.] and [12, Ch. 8. §6.]. Henceforth, we assume that \( \gcd(m, q) = 1 \). Let \( \lambda \) be a primitive \( m^{th} \) root of unity and let \( \Omega := \{ \lambda^i : 0 \leq i \leq m - 1 \} \) be the collection of all \( m^{th} \) roots of unity. The smallest extension of \( \mathbb{F}_q \) containing \( \Omega \) is denoted by \( \mathbb{F}_{q^r} \), i.e., \( \mathbb{F}_{q^r} = \mathbb{F}_q(\lambda) \) is the splitting field of \( x^m - 1 \). The Fourier transform of \( A(x) = a_0 + a_1 x + \cdots + a_{m-1} x^{m-1} \in R \) is \( \tilde{A}(x) = a_0 + a_1 x + \cdots + a_{m-1} x^{m-1} \), where the Fourier coefficient \( \alpha_\ell \) is defined as \( \alpha_\ell := A(\lambda^\ell) \), for \( \ell \in \{0, \ldots, m - 1 \} \). The inverse transform is given by

\[
a_\ell = \frac{1}{m} \sum_{i=0}^{m-1} \alpha_i \lambda^{-i} = \frac{1}{m} \tilde{A}(\lambda^{-\ell}).
\]
Note that the inverse transform is also characterized by the following linear transformation in an equivalent way (see [18])

\[
\begin{pmatrix}
  a_0 \\
  a_1 \\
  \vdots \\
  a_{m-1}
\end{pmatrix}
= 
\begin{pmatrix}
  1 & 1 & \cdots & 1 & \lambda & \lambda^2 & \cdots & \lambda^{m-1} \\
  1 & \lambda & \lambda^2 & \cdots & \lambda^{2(m-1)} \\
  \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
  1 & \lambda^{m-1} & \lambda^{2(m-1)} & \cdots & \lambda^{(m-1)^2}
\end{pmatrix}^{-1}
\begin{pmatrix}
  \alpha_0 \\
  \alpha_1 \\
  \vdots \\
  \alpha_{m-1}
\end{pmatrix}
\]

(4)

\[
= \frac{1}{m}
\begin{pmatrix}
  1 & \delta & \cdots & \delta^{m-1} \\
  1 & \delta^2 & \cdots & \delta^{2(m-1)} \\
  \vdots & \vdots & \ddots & \vdots \\
  1 & \delta^{m-1} & \cdots & \delta^{(m-1)^2}
\end{pmatrix}
\begin{pmatrix}
  \alpha_0 \\
  \alpha_1 \\
  \vdots \\
  \alpha_{m-1}
\end{pmatrix}
\]

where \( \delta := \lambda^{-1} \) is also an \( m \text{th} \) root of unity in \( \mathbb{F}_{q^r} \).

Now we show that the inverse transform (4) maps vectors in \( \mathbb{F}_{q^r}^m \) to vectors in \( \mathbb{F}_q^m \). We assume that \( x^m - 1 \) factorizes into irreducibles in \( \mathbb{F}_{q}[x] \) as

\[
x^m - 1 = f_1(x)f_2(x) \cdots f_s(x).
\]

Since \( m \) and \( q \) are relatively prime, there are no repeated factors in (5). Let \( u_j \) be the smallest nonnegative integer with \( f_j(\lambda^{u_j}) = 0 \), for all \( j \in \{1, 2, \ldots, s\} \). The \( \mathbb{F}_q \)-conjugacy (or \( q \)-cyclotomic) class containing \( \lambda^{u_j} \) in \( \Omega \) is defined as

\[
[\lambda^{u_j}] = \left\{ \lambda^{u_j}, \lambda^{qu_j}, \lambda^{q^2u_j}, \ldots, \lambda^{q^{e_j-1}u_j} \right\} \subseteq \Omega,
\]

where \( e_j = \deg(f_j) \) and, hence, \( [\lambda^{u_j}] \) contains all roots of the irreducible polynomial \( f_j \), for each \( j \). Note that \( \Omega \) is a disjoint union of these \( q \)-cyclotomic classes. We set \( \mathbb{E}_j := \mathbb{F}_q(\lambda^{u_j}) \), for each \( 1 \leq j \leq s \), where \( \mathbb{E}_j \) is an intermediate field between \( \mathbb{F}_{q^r} \) and \( \mathbb{F}_q \) such that \( [\mathbb{E}_j : \mathbb{F}_q] = e_j \). Recall that the trace map from the extension \( \mathbb{E}_j \) onto \( \mathbb{F}_q \), for \( 1 \leq j \leq s \), is defined as

\[
\text{Tr}_{\mathbb{E}_j/\mathbb{F}_q}(x) := x + x^q + \cdots + x^{q^{e_j-1}}.
\]

We now rewrite (3) as

\[
a_f = \frac{1}{m} \sum_{i=0}^{m-1} \alpha_i \lambda^{-fi} = \frac{1}{m} \sum_{j=1}^{s} \sum_{b=0}^{e_j-1} \alpha_{q^b u_j} \lambda^{-q^b u_j} = \frac{1}{m} \sum_{j=1}^{s} \text{Tr}_{\mathbb{E}_j/\mathbb{F}_q}(\alpha_{u_j} \lambda^{-u_j})
\]

and this proves that \( a_f \in \mathbb{F}_q \), for any \( f \in \{0, \ldots, m - 1\} \).

From this point on, we will consider QC codes of index \( \ell = 2 \) only. Using what Lally and Fitzpatrick had established in [16], any QC code \( C \) in \( \mathbb{F}_q^{2m} \) has a generating set obtained from the rows of a reduced \( 2 \times 2 \) polynomial matrix.
Consider the ring homomorphism
\begin{equation}
\Psi : \mathbb{F}_q[x]^2 \rightarrow R^2
\end{equation}
\[(f_0(x), f_1(x)) \mapsto (f_0(x) + I, f_1(x) + I).\]
Let \(\vec{y}_0 := (1, 0)\) and \(\vec{y}_1 := (0, 1)\). The preimage \(\tilde{C} \subseteq \mathbb{F}_q[x]^2\) of a given QC code \(C \subseteq R^2\) under (7) is an \(\mathbb{F}_q[x]\)-submodule, which contains \(\tilde{K} := \{(x^m - 1)\vec{y}_0, (x^m - 1)\vec{y}_1\}\). Observe that \(\mathbb{F}_q[x]^2\) is a finitely generated free module over \(\mathbb{F}_q[x]\), which is a principal ideal domain. Hence, \(\tilde{C}\) is generated by \(\{\vec{w}_1, \vec{w}_2, (x^m - 1)\vec{y}_0, (x^m - 1)\vec{y}_1\}\), where \(\vec{w}_z = (w_{z,0}(x), w_{z,1}(x)) \in \mathbb{F}_q[x]^2\), for each \(z \in \{1, 2\}\). Hence, the rows of
\begin{equation}
\mathcal{G} = \begin{pmatrix}
w_{1,0}(x) & w_{1,1}(x) \\
w_{2,0}(x) & w_{2,1}(x) \\
x^m - 1 & 0 \\
0 & x^m - 1
\end{pmatrix}
\end{equation}
form a generating set for \(\tilde{C}\). We triangularize \(\mathcal{G}\) using elementary row operations and we get another set of generators from an upper-triangular \(2 \times 2\) matrix with entries in \(\mathbb{F}_q[x]\),
\begin{equation}
\tilde{G}(x) = \begin{pmatrix}
g_{0,0}(x) & g_{0,1}(x) \\
0 & g_{1,1}(x)
\end{pmatrix},
\end{equation}
where the following conditions are satisfied:

1. We have \(\deg(g_{1,1}(x)) > \deg(g_{0,1}(x))\).
2. Both \(g_{0,0}(x)\) and \(g_{1,1}(x)\) are divisors of \(x^m - 1\).
3. If \(g_{0,0}(x) = x^m - 1\), then \(g_{0,1}(x) = 0\).

A generating set for \(C\) is obtained by considering the rows of \(\tilde{G}(x)\) under the image of \(\Psi\) in (7). Viewed as an \(R\)-submodule, \(C\) is said to be a 1-generator QC code if \(g_{1,1}(x) = x^m - 1\) and \(C\) is 2-generator if both \(g_{0,0}(x)\) and \(g_{1,1}(x)\) are different from \(x^m - 1\). It was proven in [16, Corollary 2.4] that \(C\) has the \(\mathbb{F}_q\)-dimension
\begin{equation}
2m - (\deg(g_{0,0}(x)) + \deg(g_{1,1}(x)))
\end{equation}

Using the polynomial matrix \(\tilde{G}(x)\) in (8) above, a spectral theory has been developed for QC codes by Semenov and Trifonov in [10]. It provides an efficient method to build a parity-check matrix for the corresponding code \(C\). The determinant of \(\tilde{G}(x)\) is \(\det(\tilde{G}(x)) := g_{0,0}(x)g_{1,1}(x)\) and an eigenvalue \(\beta\) of \(C\) is a root of \(\det(\tilde{G}(x))\). Observe that all eigenvalues are elements of \(\Omega \subseteq \mathbb{F}_q^\ast\), since \(g_{t,t}(x) \mid x^m - 1\), for each \(t \in \{0, 1\}\). The biggest integer \(a\) satisfying \((x - \beta)^a \mid \det(\tilde{G}(x))\) is called the algebraic multiplicity of \(\beta\). The eigenspace of \(\beta\) is denoted by \(\mathcal{V}_\beta\), which is the null space of \(\tilde{G}(\beta)\). In other words,
\[
\mathcal{V}_\beta := \{\vec{v} \in \mathbb{F}_q^2 : \tilde{G}(\beta)\vec{v}^\top = \vec{0}_2\}
\]
where \(\vec{0}_q\) denotes the zero vector of length \(\mathbb{F}_q\), for any \(\mathbb{F}_q \geq 1\). The geometric multiplicity of \(\beta\) is the dimension of \(\mathcal{V}_\beta\). It was shown in [10, Lemma 1] that the algebraic and geometric
multiplicities of an eigenvalue $\beta$ are equal, i.e. $a = \dim_{\mathbb{F}_q}(V_\beta)$. Let $\beta_1, \ldots, \beta_p$ be all the distinct eigenvalues of $C$. For each $1 \leq i \leq p$, let $n_i$ denote the multiplicity of $\beta_i$ and let the associated eigenspace $V_i$ be spanned by the basis $\{\vec{v}_{i,0}, \ldots, \vec{v}_{i,n_i-1}\}$. We construct the matrix

$$V_i := \begin{pmatrix} \vec{v}_{i,0} \\ \vdots \\ \vec{v}_{i,n_i-1} \end{pmatrix} = \begin{pmatrix} v_{i,0,0} & v_{i,0,1} \\ \vdots & \vdots \\ v_{i,n_i-1,0} & v_{i,n_i-1,1} \end{pmatrix},$$

whose rows contain the basis elements, for each $i$. We set

$$H_i := (1, \beta_i, \ldots, \beta_i^{m-1}) \otimes V_i$$

and

$$H := \begin{pmatrix} H_1 \\ \vdots \\ H_p \end{pmatrix} = \begin{pmatrix} V_1 & \beta_1 V_1 & \ldots & \beta_1^{m-1} V_1 \\ \vdots & \vdots & \vdots & \vdots \\ V_p & \beta_p V_p & \ldots & \beta_p^{m-1} V_p \end{pmatrix}.$$ 

The equality of algebraic and geometric multiplicities shown in [10, Lemma 1] implies that $H$ has $n := \sum_{i=1}^{p} n_i = \deg(g_{0,0}(x)) + \deg(g_{1,1}(x))$ rows. It was proven in [10, Lemma 2] that these $n$ rows are linearly independent. Combined with (9), we obtain that $H$ has rank $2m - \dim_{\mathbb{F}_q}(C)$. One can easily verify that $H \vec{c}^\top = \vec{0}_n$, for all $\vec{c} \in C$, and therefore $H$ serves as a parity-check matrix.

Proposition 1. [10, Theorem 1] An element $\vec{c} \in \mathbb{F}_q^{2m}$ is a codeword of $C$ if and only if $H \vec{c}^\top = \vec{0}_n$.

3. The Main Results

A double-circulant code $C$ is a $[2m, m]_q$-code with systematic generator matrix $G = (I_m | A)$ such that $A$ is an $m \times m$ circulant matrix as in (1). Our aim is to explicitly find $a_i \in \mathbb{F}_q$, for $0 \leq i \leq m-1$, such that the double-circulant code $C$ is MDS. We accomplish this by constructing a suitable parity-check matrix $H$ for $C$.

Observe that we can regard $C$ as a QC code of length $2m$ and index 2 over $\mathbb{F}_q$ via the following isomorphism

$$\mathbb{F}_q^m \times \mathbb{F}_q^m \cong \mathbb{F}_{2q}^{m \times 2}$$

$$(c_0, c_1, \ldots, c_{m-1}, c_0', c_1', \ldots, c_{m-1}') \leftrightarrow \begin{pmatrix} c_0 & c_0' \\ \vdots & \vdots \\ c_{m-1} & c_{m-1}' \end{pmatrix},$$

which provides a rearrangement of codewords in $C$ as in (2). For the details and the rearrangement in higher indices we refer to Section II.1. in [8].
Clearly, $C$ is generated by $(1, A(x)) \in R^2$ as an $R$-module, where $A(x) \in R$ is the associated polynomial of $A$. Therefore,

$$
\tilde{G}(x) = \begin{pmatrix} 1 & A(x) \\ 0 & x^m - 1 \end{pmatrix}
$$

is the $2 \times 2$ reduced matrix related to $C$. We have $\det(\tilde{G}(x)) = x^m - 1$ and, therefore, $1, \lambda, \ldots, \lambda^{m-1}$ are all eigenvalues of $C$, each of them with multiplicity 1, since $\gcd(m, q) = 1$. Let $A(\lambda^i) := -\alpha_i$, for $0 \leq i \leq m - 1$. Then

$$
V_i = \left\{ \bar{v} \in \mathbb{F}_q^2 \mid \tilde{G}(\lambda^i) \bar{v}^T = \bar{0}_2 \right\} = \{ \theta(\alpha_i, 1) \mid \theta \in \mathbb{F}_q \}.
$$

Hence, $V_i$ is a one-dimensional vector subspace of $\mathbb{F}_q^2$ with basis $V_i = (\alpha_i, 1)$. We have

$$
(H) = \left( \begin{array}{cccccc}
\alpha_0 & 1 & \alpha_0 & 1 & \alpha_0 & 1 \\
\alpha_1 & 1 & \lambda \alpha_1 & \lambda & \lambda^2 \alpha_1 & \lambda^2 \\
\alpha_2 & 1 & \lambda^2 \alpha_2 & \lambda^2 & \lambda^4 \alpha_2 & \lambda^4 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\alpha_{m-1} & 1 & \lambda^{m-1} \alpha_{m-1} & \lambda^{m-1} & \lambda^{2(m-1)} \alpha_{m-1} & \lambda^{2(m-1)} \\
\end{array} \right).
$$

and using (11) we obtain the parity-check matrix $H$ in the form specified by (10) as

$$
H = \left( \begin{array}{cccccc}
\alpha_0 & 1 & \alpha_0 & 1 & \alpha_0 & 1 \\
\alpha_1 & 1 & \lambda \alpha_1 & \lambda & \lambda^2 \alpha_1 & \lambda^2 \\
\alpha_2 & 1 & \lambda^2 \alpha_2 & \lambda^2 & \lambda^4 \alpha_2 & \lambda^4 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\alpha_{m-1} & 1 & \lambda^{m-1} \alpha_{m-1} & \lambda^{m-1} & \lambda^{2(m-1)} \alpha_{m-1} & \lambda^{2(m-1)} \\
\end{array} \right).
$$

What remains for us to do is to choose suitable elements $\alpha_i \in \mathbb{F}_q$, for $0 \leq i \leq m - 1$, such that $C$ becomes an MDS code. Once this is done, we recover $A(x)$ by solving for its coefficients in (4) or in (6).

Theorem 2. Given a prime power $q$, choose a positive integer $1 < m \leq \lfloor \frac{q+1}{2} \rfloor$ such that $\gcd(m, q) = 1$ and there exists $\alpha \in \mathbb{F}_q \setminus \{0, 1\}$ with an order in the multiplicative group of $\mathbb{F}_q$ that is relatively prime to $m$, where $\mathbb{F}_q$ is the splitting field of $x^m - 1$. Let $A(x) \in R$ satisfy $A(\lambda^i) = -\alpha^i$, for all $0 \leq i \leq m - 1$, such that the coefficients of $A(x)$ are obtained by the inverse Fourier transform given in (4) or (6). Then, the associated circulant matrix $A$ is an MDS matrix over $\mathbb{F}_q$.

Proof. The condition $m \leq \lfloor \frac{q+1}{2} \rfloor$ is coherent with the MDS conjecture. We use the well-known result that $C$ is a $[2m, m, m + 1]_q$ MDS code if and only if any $m$ columns of $H$ are linearly independent ([12, Theorem 10 in Ch. 1, §10]). Observe that any $m$ columns of $H$ form an $m \times m$ Vandermonde matrix. Thus, it suffices to show that the $2m$ elements $1, \lambda, \ldots, \lambda^{m-1}$, $\alpha, \lambda \alpha, \ldots, \lambda^{m-1} \alpha$ are distinct.

Suppose, for a contradiction, that $\lambda^i = \alpha \lambda^j$ for some $0 \leq i, j \leq m - 1$, implying $\alpha = \lambda^{i-j}$. Let $h$ be the order of $\alpha$ in the multiplicative group of $\mathbb{F}_q$. Thus, $1 = \alpha^h = \lambda^{h(i-j)}$, and hence, $m$ divides $h(i-j)$. Since $h$ and $m$ are relatively prime, $m$ must divide $i - j$. This forces $i = j$, which contradicts the assumption that $\alpha \neq 1$. \qed
Remark 3. Note that $A$ is an MDS matrix over $\mathbb{F}_q$ if and only if all of its minors are nonzero [4, Definition 3]. More formally, all minors of an MDS matrix are also MDS, as proven in [19, Theorem 2]. In the design of symmetric ciphers, because of the software implementation efficiency, MDS matrices of even size over finite fields of characteristic 2 are preferred. Using our method, one can construct $m \times m$ MDS matrices where $m$ is odd and $q$ is even, and even size MDS matrices can be obtained easily by their minors of desired size.

Example 4. Let $q = 2^6$, $m = 7$ and let $\theta$ be a generator of the multiplicative group of $\mathbb{F}_{2^6}$ given by the computer algebra system GAP [20]. Let $\lambda = \theta^9$ and $\alpha = \theta^{21}$. By Theorem 2, the circulant matrix associated with $A(x) = \sum_{i=0}^{6} a_i x^i$ is MDS. We obtain the coefficients of $A(x)$

$$(a_0, a_1, a_2, a_3, a_4, a_5, a_6) = (1, \theta^{53}, \theta^{20}, \theta^{22}, \theta^{29}, \theta^{23}, \theta^{37})$$

by solving

$$\begin{pmatrix}
  a_0 \\
  a_1 \\
  \vdots \\
  a_6
\end{pmatrix} = \begin{pmatrix}
  1 & 1 & \ldots & 1 \\
  1 & \delta & \ldots & \delta^6 \\
  \vdots & \vdots & \ddots & \vdots \\
  1 & \delta^6 & \ldots & \delta^{36}
\end{pmatrix} \begin{pmatrix}
  1 \\
  \alpha \\
  \vdots \\
  \alpha^6
\end{pmatrix}.$$ 

A square matrix $M$ is involutory if $M = M^{-1}$. By the isomorphism between the ring of $m \times m$ circulant matrices over $\mathbb{F}_q$ and the quotient ring $R$, a circulant matrix $A$ is involutory if and only if $A(x)^2 \equiv 1 \pmod{x^m - 1}$, i.e., $x^m - 1$ is a divisor of $(A(x) - 1)(A(x) + 1)$.

As a corollary of Theorem 2, we derive a construction of circulant involutory MDS matrices over any finite field of odd characteristic. Let $\alpha = -1$ so that $\alpha_i = \alpha^i = (-1)^i$. In our notation, $A(\lambda^i) = -\alpha_i = (-1)^{i+1}$, for $0 \leq i \leq m-1$, which guarantees that $x^m - 1$ divides $(A(x) - 1)(A(x) + 1)$. Note that $m$ must be odd since $-1$ has an even order in the multiplicative group of $\mathbb{F}_q$.

Corollary 5. Let $q$ be odd and $\alpha = -1$. Choose an odd integer $m$ with $1 < m \leq \lfloor \frac{q+1}{2} \rfloor$ and $\gcd(m, q) = 1$. Let $A(x) \in R$ satisfy $A(\lambda^i) = -\alpha^i$, for $0 \leq i \leq m-1$, where $A(x)$ is obtained using (4) or (6). Then, the matrix $A$ associated with $A(x)$ is a circulant involutory MDS matrix over $\mathbb{F}_q$.

4. Conclusion

In this work, we introduced a method to construct circulant and circulant involutory MDS matrices over finite fields, which builds upon the theory of 1-generator QC codes of index 2. Extending this approach to multicirculant codes of higher indices and to general QC codes with 2 or more generators are worthy goals.

5. Acknowledgement

The work of B. Chen is supported by the National Natural Science Foundation of China Grant Numbers 11871025, 11971175, and 11601158, as well as by Science and Technology Program of
Guangzhou Grant Number 201804010102. Nanyang Technological University Grant Number M4080456 supports the research carried out by M. F. Ezerman, S. Ling, and B. Özkaya. This paper was written while B. Chen was visiting Nanyang Technological University.

REFERENCES


E-mail address: bocong.chen@yahoo.com, {fredezerman, lingsan, buketozkaya}@ntu.edu.sg