information

Article

Vector-Circulant Matrices and Vector-Circulant Based Additive Codes over Finite Fields

Somphong Jitman

Department of Mathematics, Faculty of Science, Silpakorn University, Nakhon Pathom 73000, Thailand; jitman_s@silpakorn.edu; Tel.: +66-897-378-538

Received: 21 April 2017; Accepted: 6 July 2017; Published: 10 July 2017

Abstract: Circulant matrices have attracted interest due to their rich algebraic structures and various applications. In this paper, the concept of vector-circulant matrices over finite fields is studied as a generalization of circulant matrices. The algebraic characterization for such matrices has been discussed. As applications, constructions of vector-circulant based additive codes over finite fields have been given together with some examples of optimal additive codes over $\mathbb{F}_4$.

Keywords: circulant matrices; vector-circulant matrices; additive-codes; half-rate codes

---

1. Introduction

Classical and quantum information media, such as storage devices and communication systems, are not one hundred percent reliable in practice because of noise or interference. Coding theory has been introduced to deal with this problem since the 1960s. Additive codes constitute an important class of codes due to their rich algebraic structures and wide applications in both classical and quantum communications (see [1–5], and references therein).

For a prime power q and a positive integer n, $\mathbb{F}_q$ denotes the finite field of order q and $M_n(\mathbb{F}_q)$ denotes the $\mathbb{F}_q$-algebra of all $n \times n$ matrices whose entries are from $\mathbb{F}_q$. Given $\alpha \in \mathbb{F}_q \setminus \{0\}$, a matrix $A \in M_n(\mathbb{F}_q)$ is said to be *α-twistulant* [6] if

$$A = \begin{bmatrix} a_0 & a_1 & \dots & a_{k-2} & a_{n-1} \\ \alpha a_{n-1} & a_0 & \dots & a_{n-3} & a_{n-2} \\ \alpha a_{n-2} & \alpha a_{n-1} & \dots & a_{n-4} & a_{n-3} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha a_1 & \alpha a_2 & \dots & \alpha a_{n-1} & a_0 \end{bmatrix}$$

for some $(a_0, a_1, \dots, a_{n-1}) \in \mathbb{F}_q^n$. Such a matrix is called *circulant* (resp., *negacirculant*) *matrix* when $\alpha = 1$ (resp., $\alpha = -1$). The set of all $n \times n$ circulant (resp., α-twistulant, negacirculant) matrices over $\mathbb{F}_q$ is isomorphic to $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ (respectively, $\mathbb{F}_q[x]/\langle x^n - \alpha\rangle$, $\mathbb{F}_q[x]/\langle x^n + 1\rangle$) as commutative algebras [6]. Circulant matrices over finite fields and their well-known generalizations in the notions of twistulant and negacirculant matrices have widely been studied and applied in many branches of Mathematics. Recently, they have been applied to construct circulant based additive codes [3] and double circulant codes [7] with optimal and extremal parameters.

In this paper, the concept of vector-circulant matrices over finite fields is studied as a generalization of circulant matrices. We focus on the algebraic characterization of such matrices as well as their applications. Constructions of vector-circulant based additive codes over finite fields are given together with some examples of optimal additive codes over $\mathbb{F}_4$.

The paper is organized as follows. In Section 2, vector-circulant matrices over finite fields $\mathbb{F}_q$ are studied together with the characterization of their algebraic structures. In Section 3, applications of vector-circulant matrices in constructing vector-circulant based additive codes over finite fields are given. Examples of some optimal additive codes derived from vector-circulant matrices are provided as well. In Section 4, suggested ideas for constructions of quantum codes based on these additive codes are discussed.

2. Vector-Circulant Matrices over Finite Fields

In this section, a general concept of circulant matrices over finite fields is given. Properties of such matrices are studied together with the algebraic characterizations.

For a given vector $\boldsymbol{\lambda} = (\lambda_0, \lambda_1, \ldots, \lambda_{n-1}) \in \mathbb{F}_q^n$, let $\rho_{\boldsymbol{\lambda}} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be an $\mathbb{F}_q$-linear transformation defined by

$$\begin{aligned} \rho_{\boldsymbol{\lambda}}((v_0, v_1, \ldots, v_{n-1})) &= (0, v_0, v_1, \ldots, v_{n-2}) + v_{n-1}\boldsymbol{\lambda} \\ &= (v_{n-1}\lambda_0, v_0 + v_{n-1}\lambda_1, \ldots, v_{n-2} + v_{n-1}\lambda_{n-1}). \end{aligned} \tag{1}$$

The map $\rho_{\boldsymbol{\lambda}}$ defined above is called the $\boldsymbol{\lambda}$*-vector-cyclic shift* on $\mathbb{F}_q^n$ and it is called the *cyclic shift* on $\mathbb{F}_q^n$ if $\boldsymbol{\lambda} = (1, 0, 0, \ldots, 0) \in \mathbb{F}_q^n$.

For a fixed vector $\boldsymbol{\lambda} \in \mathbb{F}_q^n$, a matrix $A \in M_n(\mathbb{F}_q)$ is said to be *vector-circulant*, or specifically, $\boldsymbol{\lambda}$*-vector-circulant* if

$$\begin{aligned} A = &\begin{bmatrix} a_0 \;\; a_1 \;\; \cdots \;\; a_{n-1} \\ \rho_{\boldsymbol{\lambda}}(a_0 \;\; a_1 \;\; \cdots \;\; a_{n-1}) \\ \rho_{\boldsymbol{\lambda}}^2(a_0 \;\; a_1 \;\; \cdots \;\; a_{n-1}) \\ \vdots \\ \rho_{\boldsymbol{\lambda}}^{n-1}(a_0 \;\; a_1 \;\; \cdots \;\; a_{n-1}) \end{bmatrix} \\ =: &\operatorname{cir}_{\boldsymbol{\lambda}}(a_0, a_1, \ldots, a_{n-1}) \end{aligned}$$

for some $(a_0, a_1, \ldots, a_{n-1}) \in \mathbb{F}_q^n$.

Clearly, a $\boldsymbol{\lambda}$-vector-circulant matrix becomes the classical circulant and α-twistulant matrices when the vectors $\boldsymbol{\lambda}$ are $(1, 0, \ldots, 0)$ and $(\alpha, 0, \ldots, 0)$, respectively.

Example 1. *Consider the finite field $\mathbb{F}_4 = \{0, 1, \alpha, \omega^2 = 1 + \omega\}$. The matrices*

$$\begin{bmatrix} 1 & \omega & 0 \\ 0 & 1 & \omega \\ \omega & 0 & \omega^2 \end{bmatrix} = \operatorname{cir}_{(1,0,1)}(1, \omega, 0)$$

and

$$\begin{bmatrix} 1 & \omega & 0 & \omega \\ \omega^2 & 1 & \omega & \omega \\ \omega^2 & \omega & 1 & 0 \\ 0 & \omega^2 & \omega & 1 \end{bmatrix} = \operatorname{cir}_{(\omega,0,0,1)}(1, \omega, 0, \omega)$$

are 3×3 and 4×4 vector-circulant matrices, respectively. They are obviously not circulant.

For a vector $\boldsymbol{\lambda} = (\lambda_0, \lambda_1, \ldots, \lambda_{n-1}) \in \mathbb{F}_q^n$, let

$$\boldsymbol{\lambda}(x) = \lambda_0 + \lambda_1 x + \cdots + \lambda_{n-1}x^{n-1} \in \mathbb{F}_q[x]$$

be the corresponding polynomial representation of $\boldsymbol{\lambda}$.

The linear transformation $\rho_{\boldsymbol{\lambda}}$ is key to determining the algebraic structures of vector-circulant matrices. Some necessary properties of $\rho_{\boldsymbol{\lambda}}$ are determined in terms of $\boldsymbol{\lambda}(x)$ as follows. From

Equation (1), it is easily verified that $\rho_{\boldsymbol{\lambda}}$ is an $\mathbb{F}_q$-linear transformation defined corresponding to the matrix

$$T_{\boldsymbol{\lambda}} = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ \lambda_0 & \lambda_1 & \lambda_2 & \dots & \lambda_{n-1} \end{bmatrix}$$

which is the companion matrix of the polynomial $-\boldsymbol{\lambda}(x) + x^n$ in $\mathbb{F}_q[x]$, i.e., $\rho_{\boldsymbol{\lambda}}(\boldsymbol{v}) = \boldsymbol{v}T_{\boldsymbol{\lambda}}$, for all $\boldsymbol{v} \in \mathbb{F}_q^n$. Consequently, for $1 \leq i$, $\rho^i_{\boldsymbol{\lambda}}$ is an $\mathbb{F}_q$-linear transformation defined corresponding to $T^i_{\boldsymbol{\lambda}}$. By convention, we set $\rho^0_{\boldsymbol{\lambda}}$ to be the identity map and $T^0_{\boldsymbol{\lambda}} = I_n$. It follows that

$$\mathrm{cir}_{\boldsymbol{\lambda}}(a_0, a_1, \dots, a_{n-1}) = \sum_{i=0}^{n-1} a_i \mathrm{cir}_{\boldsymbol{\lambda}}(E_{i+1}), \tag{2}$$

where $E_i = (0, \dots, 0, \underbrace{1}_{ith}, 0, \dots, 0) \in \mathbb{F}_q^n$ for $1 \leq i \leq n$.

Observe that the matrix $T_{\boldsymbol{\lambda}}$ does not need to be invertible. For $\boldsymbol{\lambda} = (\lambda_0, \lambda_1, \dots, \lambda_{n-1}) \in \mathbb{F}_q^n$, the singularity of $T_{\boldsymbol{\lambda}}$ depends on λ_0. By applying a suitable sequence of elementary row operations, $T_{\boldsymbol{\lambda}}$ is equivalent to an $n \times n$ diagonal matrix $\mathrm{diag}(\lambda_0, 1, 1, \dots, 1)$. Then, the next proposition follows.

Proposition 1. *Let $\boldsymbol{\lambda} = (\lambda_0, \lambda_1, \dots, \lambda_{n-1}) \in \mathbb{F}_q^n$. Then $T_{(\lambda_0, \lambda_1, \dots, \lambda_{n-1})}$ is invertible if and only if $\lambda_0 \neq 0$.*

$\mathrm{Cir}_{n,\boldsymbol{\lambda}}(\mathbb{F}_q)$ denotes the set of all $n \times n$ $\boldsymbol{\lambda}$-vector-circulant matrices over $\mathbb{F}_q$. Consider $M_n(\mathbb{F}_q)$ as a noncumulative algebra over $\mathbb{F}_q$, $\mathrm{Cir}_{n,\boldsymbol{\lambda}}(\mathbb{F}_q)$ is a commutative subalgebra of $M_n(\mathbb{F}_q)$. It follows directly from the linearity of $\rho_{\boldsymbol{\lambda}}$ that $\mathrm{Cir}_{n,\boldsymbol{\lambda}}(\mathbb{F}_q)$ is a subspace of the $\mathbb{F}_q$-vector space $M_n(\mathbb{F}_q)$. Moreover, by Equation (1), the set $\{\mathrm{cir}_{\boldsymbol{\lambda}}(E_1), \mathrm{cir}_{\boldsymbol{\lambda}}(E_2), \dots, \mathrm{cir}_{\boldsymbol{\lambda}}(E_n)\}$ can be verified to be a basis of $\mathrm{Cir}_{n,\boldsymbol{\lambda}}(\mathbb{F}_q)$.

The following properties of companion matrices and vector-circulant based matrices are well-known and play a role in applications.

Lemma 1. *Let $\boldsymbol{\lambda} \in \mathbb{F}_q^n$. Then, the following statements hold.*

(i) $T^m_{\boldsymbol{\lambda}} = \mathrm{cir}_{\boldsymbol{\lambda}}(\rho^m_{\boldsymbol{\lambda}}(E_1))$ *for all integers* $0 \leq m$.
(ii) $T^i_{\boldsymbol{\lambda}} = \mathrm{cir}_{\boldsymbol{\lambda}}(E_{i+1})$ *for all integers* $0 \leq i < n$.

Corollary 1. *Let n be a positive integer and let $\boldsymbol{\lambda} \in \mathbb{F}_q^n$. Then $T^m_{\boldsymbol{\lambda}} \in \mathrm{Cir}_{n,\boldsymbol{\lambda}}(\mathbb{F}_q)$ for all $0 \leq m$.*

It is well know that the set of $n \times n$ circulant matrices over $\mathbb{F}_q$ is a commutative subalgebra of $M_n(\mathbb{F}_q)$ and it is isomorphic to $\mathbb{F}_q[x]/\langle x^n - \boldsymbol{\lambda}(x)\rangle$ as commutative algebras (see [6]). These results can be easily generalized to the case of vector-circulant matrices as follows.

Theorem 1. *Let n be a positive integer and let $\boldsymbol{\lambda} \in \mathbb{F}_q^n$. Then, $\mathrm{Cir}_{n,\boldsymbol{\lambda}}(\mathbb{F}_q)$ is a commutative subalgebra of $M_n(\mathbb{F}_q)$ with identity I_n.*

Using the algebra isomorphism $\varphi : \mathrm{Cir}_{n,\boldsymbol{\lambda}}(\mathbb{F}_q) \to \mathbb{F}_q[x]/\langle x^n - \boldsymbol{\lambda}(x)\rangle$ defined by

$$\mathrm{cir}_{\boldsymbol{\lambda}}(a_0, a_1, \dots, a_{n-1}) \mapsto \sum_{i=0}^{n-1} a_i x^i + \langle x^n - \boldsymbol{\lambda}(x)\rangle,$$

we have the following relation.

Theorem 2. *Let n be a positive integer and let $\boldsymbol{\lambda} \in \mathbb{F}_q^n$. Then, $\mathrm{Cir}_{n,\boldsymbol{\lambda}}(\mathbb{F}_q)$ is isomorphic to $\mathbb{F}_q[x]/\langle x^n - \boldsymbol{\lambda}(x)\rangle$ as commutative algebras.*

3. Vector-Circulant Based Additive Codes over Finite Fields

In this section, we restrict our study to a finite field $\mathbb{F}_{p^2}$ and focus on applications of vector-circulant matrices over $\mathbb{F}_{p^2}$ in constructing additive codes over $\mathbb{F}_{p^2}$. Since additive codes over finite fields have applications in both classical and quantum communications (see, for example, [1–5]), it is of natural interest to study this family of codes. Constructions of good/optimal additive codes have been widely studied (see [3,8–10], and references therein). Characterizations of self-dual and formally self-dual additive codes have been given in [11,12], respectively. Circulant based additive codes and cyclic additive codes have been studied in [1,8], respectively. Here, we focus on the construction of additive codes based on vector-circulant matrices. Examples of some additive codes with good/optimal parameters derived from vector-circulant matrices are given as well.

A *code of length* n over $\mathbb{F}_{p^2}$ is defined to be a non-empty subset of $\mathbb{F}_{p^2}^n$. A code C is said to be *additive* if it is an additive subgroup of the additive group $(\mathbb{F}_{p^2}^n, +)$. Throughout, every code is assumed to be additive. It is known (see [3]) that C contains p^k codewords for some $0 \leq k \leq 2n$, and can be defined by a $k \times n$ generator matrix, with entries from $\mathbb{F}_{p^2}$, whose rows span C additively. We regard an additive code of length n over $\mathbb{F}_{p^2}$ containing p^k codewords as an $(n, p^k)_{p^2}$ code. The rate of an $(n, p^k)_{p^2}$ code is defined to be $\mathrm{rate}(C) := \frac{k}{2n}$. The *Hamming weight* of $\boldsymbol{v} \in \mathbb{F}_{p^2}^n$, denoted by $\mathrm{wt}(\boldsymbol{v})$, is defined to be the number of nonzero components of $\boldsymbol{v}$. The *Hamming distance* between $\boldsymbol{u} \neq \boldsymbol{v} \in \mathbb{F}_{p^2}^n$ is defined as $\mathrm{wt}(\boldsymbol{u} - \boldsymbol{v})$. The *minimum distance* of the code C, denoted by $d(C)$, is the minimal Hamming distance between any two distinct codewords of C. As C is additive, the minimum distance equals the smallest nonzero weight of any codewords in C. An $(n, p^k)_{p^2}$ code with minimum distance d is called an $(n, p^k, d)_{p^2}$ code. The efficiency of codes is determined by their minimum distances. Precisely, a code with high minimum distance is more useful in practice.

Given $\boldsymbol{\lambda} \in \mathbb{F}_{p^2}^n$, a *$\boldsymbol{\lambda}$-vector-circulant based additive code* over $\mathbb{F}_{p^2}$ is defined to be the code additively spanned by the rows of a $\boldsymbol{\lambda}$-vector-circulant matrix of the form

$$G := \mathrm{cir}_{\boldsymbol{\lambda}}(a_0, a_1, \ldots, a_{n-1}) = \begin{bmatrix} a_0 \ a_1 \ \cdots \ a_{n-1} \\ \rho_{\boldsymbol{\lambda}}(a_0 \ a_1 \ \cdots \ a_{n-1}) \\ \rho_{\boldsymbol{\lambda}}^2(a_0 \ a_1 \ \cdots \ a_{n-1}) \\ \vdots \\ \rho_{\boldsymbol{\lambda}}^{n-1}(a_0 \ a_1 \ \cdots \ a_{n-1}) \end{bmatrix}.$$

Such a code is called a *circulant based additive code* if $\boldsymbol{\lambda} = (1, 0, \ldots, 0)$ and it is called a *λ-twistulant based additive code* if $\boldsymbol{\lambda} = (\lambda, 0, \ldots, 0)$. An advantage of this construction is that there are typically much more additive codes than circulant based or twistulant based additive codes [3] due to the various choices of $\boldsymbol{\lambda}$.

Remark 1. *We have made the following observations for the number of possible choices of generator matrices for additive codes of length n over $\mathbb{F}_{p^2}$.*

1. *The number of $n \times n$ circulant matrices over $\mathbb{F}_{p^2}$ is $|\mathrm{Cir}_{n,(1,0,\ldots,0)}(\mathbb{F}_{p^2})| = p^{2n}$.*
2. *The number of $n \times n$ vector-circulant matrix over $\mathbb{F}_{p^2}$ is $p^{2n}|\mathrm{Cir}_{n,(1,0,\ldots,0)}(\mathbb{F}_{p^2})| = p^{4n}$.*
3. *The number of $n \times n$ matrices over $\mathbb{F}_{p^2}$ is $|M_n(\mathbb{F}_{p^2})| = p^{2n^2}$.*

We note that each value above does not determine explicitly the number of its corresponding additive codes since two different matrices in $M_n(\mathbb{F}_{p^2})$ can generate the same additive code. The advantage of searching for good additive codes from vector-circulant matrices is that there are much more choices of generator matrices than circulant matrices and the search space is not too large as $M_n(\mathbb{F}_{p^2})$.

It is not difficult to see that the rate of a vector-circulant based additive code is

$$\text{rate}(C) = \frac{\text{the number of maximal } \mathbb{F}_p - \text{linearly independent rows of } G}{2n} \leq \frac{1}{2}.$$

In the case where $k = n$, an $(n, p^n)_{p^2}$ code has rate $\frac{1}{2}$ and it is called a *half-rate code*. It follows from the Singleton bound [1] that any half-rate additive code over $\mathbb{F}_{p^2}$ must satisfy

$$d \leq \left\lfloor \frac{n}{2} \right\rfloor + 1.$$

An $(n, p^n)_{p^2}$ code C is said to be *extremal* if it attains the equality in the Singleton bound, and *near-extremal* if it has minimum distance $\lfloor \frac{n}{2} \rfloor$.

Using the computer algebra system Magma [13], a procedure to generate vector-circulant based additive codes of small lengths over $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2 = 1 + \alpha\}$ is implemented. Half-rate additive codes over $\mathbb{F}_4$ with highest minimum distances of length up to 13 are shown in Table 1. We note that the codes of length 2 to 7 are extremal and the codes of length 8 to 13 are near-extremal. Comparing Table 5 in [1], and Table 1 in [9], the codes given in Table 1 are optimal.

Table 1. Half-rate vector-circulant based additive codes of length n over $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2 = 1 + \alpha\}$ generated by $\text{cir}_\lambda(v)$.

n	λ	v	$d(C)$
2	$(1,1)$	$(\alpha,1)$	2
3	$(1,0,\alpha)$	$(\alpha,1,1)$	2
4	$(1,0,0,1)$	$(1,\alpha,1,1)$	3
5	$(1,0,0,0,\alpha)$	$(1,0,\alpha,1,1)$	3
6	$(1,0,0,0,0,0)$	$(\alpha,\alpha^2,\alpha,1,1,1)$	4
7	$(1,0,1,0,0,0,0)$	$(0,1,\alpha,1,1,1,1)$	4
8	$(1,0,0,0,0,0,0,\alpha)$	$(0,\alpha,\alpha^2,\alpha^2,1,1,1,1)$	4
9	$(1,0,0,0,0,0,0,0,1)$	$(a^2,\alpha,1,1,1,1,1,1,1)$	4
10	$(1,0,0,0,0,0,0,0,0,0)$	$(0,\alpha,\alpha,1,\alpha,1,1,1,1,1)$	5
11	$(1,0,0,0,1,0,0,0,0,0,0)$	$(0,\alpha,\alpha^2,\alpha,1,1,1,1,1,1,1)$	5
12	$(1,0,0,0,0,0,0,0,0,0,0,0)$	$(0,1,\alpha^2,\alpha^2,1,\alpha,1,1,1,1,1,1)$	6
13	$(1,0,0,0,0,0,0,0,0,0,0,0,0)$	$(0,\alpha,\alpha^2,1,1,\alpha,1,1,1,1,1,1,1)$	6

Examples of good vector-circulant based additive codes with rate less than $\frac{1}{2}$ are presented in Table 2. Compared with Table 1 in [9], the codes given in Table 2 are optimal.

Table 2. Vector-circulant based $(n, 2^k)_4$ codes over $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2 = 1 + \alpha\}$ generated by $\text{cir}_\lambda(v)$.

n	k	λ	v	*d(C)*
5	4	$(1,0,0,0,0)$	$(\alpha,0,\alpha,1,1)$	4
6	4	$(1,0,0,0,0,0)$	$(\alpha^2,0,\alpha,1,1,1)$	4
	5	$(1,0,0,0,0,0)$	$(\alpha^2,\alpha,0,1,1,1)$	4
7	4	$(\alpha,0,0,0,0,0,1)$	$(0,\alpha^2,1,\alpha^2,\alpha^2,0,1)$	5
	6	$(1,\alpha,0,0,0,0,0)$	$(\alpha,\alpha,0,0,1,1,1)$	4
8	4	$(1,0,0,0,0,0,0,\alpha)$	$(\alpha,\alpha^2,\alpha,\alpha,0,\alpha^2,1,0)$	6
	6	$(1,1,0,0,0,0,0,0)$	$(\alpha^2,1,0,0,\alpha^2,1,\alpha,\alpha^2)$	5
9	6	$(1,0,0,0,0,0,0,0,0)$	$(1,\alpha,1,1,\alpha,1,0,0,0)$	6
	8	$(1,0,0,0,0,0,0,0,0)$	$(\alpha^2,1,1,\alpha,1,0,0,0,0)$	5
10	8	$(1,0,0,0,0,0,0,0,0,0)$	$(\alpha,1,\alpha,0,1,1,1,0,0,0)$	6
11	8	$(0,1,0,0,0,0,0,0,0,0,0)$	$(0,0,0,1,0,0,\alpha,\alpha^2,1,\alpha,\alpha^2)$	6
	10	$(1,0,0,0,0,0,0,0,0,0,0)$	$(1,\alpha^2,\alpha^2,0,\alpha,\alpha,1,0,0,0,0)$	6
13	12	$(0,1,0,0,0,0,0,0,0,0,0,0,0)$	$(0,\alpha^2,1,\alpha,\alpha,1,0,1,1,1,1,1,1)$	6

4. Future Works

Additive codes and their duals defined with respect to the trace Hermitian inner product (see [2]) can be applied in constructing quantum codes (see [2,3,5]). In [5], symmetric quantum codes were constructed from self-orthogonal additive codes. Nested pairs of additive codes were used in constructing asymmetric quantum codes [2]. In [14], the hull of codes and complementary dual codes were applied for constructions of entanglement-assisted quantum codes. We note that the said properties for vector-circulant based additive codes can be determined directly from their corresponding vector-circulant matrices. Let C be an additive code additively generated by a vector-circulant matrix G and let B be a matrix whose rows form maximal $\mathbb{F}_p$-linearly independent rows of G. For a given matrix $A := [a_{ij}]$ over $\mathbb{F}_{p^2}$, let $\overline{A} = [a_{ij}^p]$. Then, the following characterizations can be derived using ideas from [15].

(i) C is self-orthogonal with respect to the trace Hermitian inner if and only if $B\overline{B}^T - \overline{B}B^T = 0$.

(ii) C is complementary dual with respect to the trace Hermitian inner if and only if $B\overline{B}^T - \overline{B}B^T$ is invertible.

(iii) If B' is a matrix whose rows are chosen from the rows of B, then the additive code C' generated by B' is a subcode of C, i.e., $C' \subseteq C$ form a nested pair of additive codes.

Based on these properties, quantum codes can be constructed using suitable vector-circulant based additive codes and methods in [2,5,14].

For future studies, characterizations and constructions of vector-circulant based additive codes with additional properties such as self-dual, self-orthogonal, and complementary dual are therefore interesting problems. Computations for vector-circulant based additive codes with larger lengths are also interesting.

Acknowledgments: This research was supported by the Thailand Research Fund under Research Grant MRG6080012. The author would like to thank the anonymous referees for there helpful comments.

Conflicts of Interest: The authors declare no conflict of interest. The founding sponsors had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, and in the decision to publish the results.

References

1. Danielsen, L.E.; Parker, M.G. Directed graph representation of half-rate additive codes over $GF(4)$. *Des. Codes Cryptogr.* **2011**, *59*, 119–130.
2. Ezerman, M.F.; Jitman, S.; Ling, S.; Pasechnik, D.V. CSS-like constructions of asymmetric quantum codes. *IEEE Trans. Inf. Theory* **2013**, *59*, 6732–6754.
3. Gulliver, T.A; Kim, J.-L. Circulant based extremal additive self-dual codes over $GF(4)$. *IEEE Trans. Inf. Theory* **2004**, *50*, 359–366.
4. Han, S. Triple circulant codes based on quadratic residues. *J. Chungcheong Math. Soc.* **2010**, *23*, 91–98.
5. Ketkar, A.; Klappenecker, A.; Kumar, S.; Sarvepalli, P.K. Nonbinary stabilizer codes over finite fields. *IEEE Trans. Inf. Theory* **2006**, *52*, 4892–4914.
6. Davis, P.J. *Circulant Matrices*, 2nd ed.; Chelesa Publishing: New York, NY, USA, 1994.
7. Kiermaier, M.; Wassermann, A. Double and bordered α-circulant self-dual codes over finite commutative chain rings. In Proceedings of the Eleventh International Workshop on Algebraic and Combinatorial Coding Theory, Pamporovo, Bulgaria, 16–22 June 2008; pp. 144–150.
8. Bierbrauer, J. Cyclic additive codes. *J. Algebra* **2012**, *372*, 661–672.
9. Bierbrauer, J.; Edel, Y.; Faina, G.; Marcugini, S.; Pambianco, F. Short additive quaternary codes. *IEEE Trans. Inf. Theory* **2009**, *55*, 952–954.
10. Blokhuis, A.; Brouwer, A.E. Small additive quaternary codes. *Eur. J. Comb.* **2004**, *25*, 161–167.
11. Danielsen, L.E.; Parker, M.G. On the classification of all self-dual additive codes over $GF(4)$ of length up to 12. *J. Comb. Theory Ser. A* **2006**, *113*, 1351–1367.
12. Han, S.; Kim, J.-L. Formally self-dual additive codes over $\mathbb{F}_4$. *J. Symb. Comput.* **2010**, *45*, 787–799.

13. Bosma, W.; Cannon, J.J.; Playoust, C. The Magma algebra system I: The user language. *J. Symb. Comput.* **1997**, *24*, 235–265.
14. Guenda, K.; Jitman, S.; Gulliver, T.A. Constructions of good entanglement-assisted quantum error correcting codes. *Des. Codes Cryptogr.* **2017**, doi:10.1007/s10623-017-0330-z.
15. Boonniyom, K.; Jitman, S. Complementary daul subfield linear codes over finite fields. *arXiv* **2016**, arXiv:1605.06827.