information

Article

On the Problem of the Existence of a Square Matrix U Such That $UU^T = -I$ over $\mathbb{Z}_{p^m}$

Sunghyu Han

School of Liberal Arts, KoreaTec, Cheonan 31253, Korea; sunghyu@koreatech.ac.kr; Tel.: +82-41-640-8611

Received: 17 May 2017; Accepted: 29 June 2017; Published: 4 July 2017

Abstract: Building-up construction is one of several methods for constructing self-dual codes. Recently, a new building-up construction method has been developed by S. Han, in which the existence of a square matrix U such that $UU^T = -I$ is essential. In this paper, we completely solve the existence problem for U over $\mathbb{Z}_{p^m}$, where p is an arbitrary prime number.

Keywords: building-up construction; self-dual code; $\mathbb{Z}_{p^m}$ code

1. Introduction

Coding theory has been developing since the 1950s. There are many interesting classes of codes, such as cyclic codes, MDS (Maximum Distance Separable) codes, algebraic geometry codes, and self-dual codes. Among them, self-dual codes are very interesting, as they are closely related to other areas of mathematics, such as block designs, lattices, modular forms, and sphere packings. Moreover, they are of interest in their own right (e.g., [1]).

There are many construction methods for self-dual codes, such as the gluing vector [2], balance principal [3], double circulant [4], and building-up construction methods. In this paper, we are concerned with the building-up construction method, which was introduced by M. Harada [5] and was subsequently formalized and named by J.-L. Kim for self-dual codes over the finite field $\mathbb{F}_2$ [6]. It was further developed for self-dual codes over the finite field $\mathbb{F}_q$, where q is a power of 2 or $q \equiv 1 \pmod 4$ [7] and $q \equiv 3 \pmod 4$ [8]. It was also applied to related rings [9–14].

However, there was an important missing case in previous building-up constructions; namely, $\mathbb{Z}_4$. This case was covered using matrices [15], where the method was formulated in the context of finite chain rings, including all previous cases as well as $\mathbb{Z}_4$. One of the key points is the existence of a square matrix U such that $UU^T = -I$. The corresponding problem over $\mathbb{Z}_{2^m}$ was completely solved, except for the following open case [15]: is there a $(4t+2) \times (4t+2)$ matrix U such that $UU^T = -I$ over $\mathbb{Z}_{2^m}$ $(m \geq 2)$ for all $t \geq 1$?

In this paper, we settle this open case. Furthermore, we solve the problem of the existence of a square matrix U such that $UU^T = -I$ over $\mathbb{Z}_{p^m}$, where p is an arbitrary prime number.

The paper is organized as follows. In Section 2, we state the preliminaries. In Section 3, we present the non-existence proof for a $(4t+2) \times (4t+2)$ matrix U such that $UU^T = -I$ over $\mathbb{Z}_{2^m}$ $(m \geq 2)$ for all $t \geq 0$. In Section 4, we study the existence problem for a matrix U over $\mathbb{Z}_{p^m}$, where p is an odd prime. Therefore, we completely solve the problem of the existence of a square matrix U such that $UU^T = -I$ over $\mathbb{Z}_{p^m}$, where p is an arbitrary prime number. In Section 5, we provide examples of the construction of self-dual codes using the result in Section 4.

Remark 1. *The square matrix U such that $UU^T = -I$ over finite fields was considered by J.L. Massey [16]. He called the matrix U antiorthogonal. Using the antiorthogonal matrix, he characterized the self-dual codes and constructed linear codes with complementary duals (LCD codes). In [17], Massey considered the existence problem of antiorthogonal matrices over finite fields.*

2. Preliminaries

Throughout this paper, R is a finite commutative ring with identity $1 \neq 0$. An R-submodule $C \subseteq R^n$ is called a linear code of length n over R. Unless otherwise specified, all codes are assumed to be linear.

For $\mathbf{x}, \mathbf{y} \in R^n$, we define the usual inner product by

$$\mathbf{x} \times \mathbf{y} = x_1 y_1 + \ldots + x_n y_n.$$

For a code C of length n over R, let

$$C^{\perp} = \{\mathbf{x} \in R^n \,|\, \mathbf{x} \times \mathbf{c} = 0, \forall\, \mathbf{c} \in C\}$$

be the dual code of C. If $C \subseteq C^{\perp}$, then we say that C is self-orthogonal, and if $C = C^{\perp}$, then C is self-dual.

The following construction method for self-dual codes over R appears in [15].

Theorem 1. *[15] Let R be a finite chain ring, C_0 a self-dual code of length n over R, and G_0 a $k \times n$ generator matrix for C_0. Let $a \geq 1$ be an integer, and X an $a \times n$ matrix over R such that $XX^T = -I$. Let U be an $a \times a$ matrix over R such that $UU^T = -I$, and O the $a \times a$ zero matrix. Then, the matrix*

$$G = \left(\begin{array}{c|c|c} I & O & X \\ \hline -G_0 X^T & G_0 X^T U & G_0 \end{array}\right)$$

generates a self-dual code C of length $n + 2a$ over R.

To apply Theorem 1 to self-dual codes over R, we should have an $a \times a$ matrix U and an $a \times n$ matrix X such that $UU^T = -I$ and $XX^T = -I$. For $1 \leq a \leq n$, if there exists an $a \times a$ matrix U such that $UU^T = -I$, then there exists an $a \times n$ matrix X such that $XX^T = -I$. Here is the proof. Let $X = [U|O]$, where O is the $a \times (n - a)$ zero matrix. Then, $XX^T = UU^T + OO^T = -I$. Therefore, we focus on the problem of the existence of an $a \times a$ matrix U such that $UU^T = -I$.

In [15], the existence of an $a \times a$ matrix U such that $UU^T = -I$ over $\mathbb{Z}_{2^m}$ has been studied. We state the relevant result.

Theorem 2. *[15] For the existence of an $a \times a$ matrix U over $\mathbb{Z}_{2^m}$ such that $UU^T = -I$, we have the following.*

1. *If $m = 1$, then there exists such U for all $a \geq 1$.*
2. *If $m \geq 2$ and $a = 4t$, then there exists such U for all $t \geq 1$.*
3. *If $m \geq 2$ and $a = 2$, then no such U exists.*
4. *If $m \geq 2$ and $a = 2t + 1$, then no such U exists for all $t \geq 0$.*

In Theorem 2, the missing case is $m \geq 2$ and $a = 4t + 2, (t \geq 1)$. This leads to the following open problem [15]: Let $a = 4t + 2$ for some positive integer $t \geq 1$. Is there an $a \times a$ matrix U such that $UU^T = -I$ over $\mathbb{Z}_{2^m}$ $(m \geq 2)$? This problem is solved in the following section.

3. Nonexistence of a $(4t + 2) \times (4t + 2)$ Matrix U Such That $UU^T = -I$ over $\mathbb{Z}_{2^m}$ $(m \geq 2)$ for All $t \geq 0$

In this section, we solve the open problem in [15] by proving that there is no $(4t + 2) \times (4t + 2)$ matrix U such that $UU^T = -I$ over $\mathbb{Z}_{2^m}$ $(m \geq 2)$ for all $t \geq 0$. We start with the following lemma.

Lemma 1. *If there is an $a \times a$ matrix U such that $UU^T = -I$ over $\mathbb{Z}_{2^m}$, then U satisfies $UU^T = -I$ over $\mathbb{Z}_{2^n}$ for $1 \leq n \leq m$.*

Proof. Let $U = (u_{ij})$ $(1 \leq i, j \leq a)$. Suppose that $UU^T = -I$ over $\mathbb{Z}_{2^m}$. Then

$$u_{i1}u_{1j} + u_{i2}u_{2j} + \ldots + u_{ia}u_{aj} \equiv -\delta_{ij} \pmod{2^m} \ (1 \leq i, j \leq a), \tag{1}$$

where

$$\delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{else.} \end{cases} \tag{2}$$

Therefore, we have

$$u_{i1}u_{1j} + u_{i2}u_{2j} + \ldots + u_{ia}u_{aj} \equiv -\delta_{ij} \pmod{2^n} \ (1 \leq i, j \leq a) \tag{3}$$

for $1 \leq n \leq m$. So, $UU^T = -I$ over $\mathbb{Z}_{2^n}$ for $1 \leq n \leq m$. □

Corollary 1. *If there is no $a \times a$ matrix U such that $UU^T = -I$ over $\mathbb{Z}_4$, then there is no $a \times a$ matrix U such that $UU^T = -I$ over $\mathbb{Z}_{2^m}$ for $m \geq 2$.*

Proof. The statement is the contrapositive of Lemma 1. □

The proof of the main theorem in this section is related to self-dual binary codes. A self-dual binary code whose codewords have weight divisible by four is called doubly even or Type II; a self-dual code with at least one codeword of weight not divisible by 4 is called singly even or Type I. The following lemma is well-known (see [18] (p. 454) for example).

Lemma 2. *Type II codes exist only for lengths that are multiples of eight.*

We are ready to prove the main theorem of this section.

Theorem 3. *Let $a = 4t + 2$ for some non-negative integer $t \geq 0$. Then, there is no $a \times a$ matrix U such that $UU^T = -I$ over $\mathbb{Z}_{2^m}$ $(m \geq 2)$.*

Proof. By Corollary 1, it is sufficient to prove that there is no $a \times a$ matrix U such that $UU^T = -I$ over $\mathbb{Z}_4$. We assume that there is an $a \times a$ matrix U such that $UU^T = -I$ over $\mathbb{Z}_4$. Let

$$\mathbf{u}_i = (u_{i1}, u_{i2}, \ldots, u_{ia}) \tag{4}$$

be the i-th row of U. Since $\mathbf{u}_i \times \mathbf{u}_i = -1$ over $\mathbb{Z}_4$, we have

$$u_{i1}^2 + u_{i2}^2 + \ldots + u_{ia}^2 \equiv -1 \pmod{4}. \tag{5}$$

Let

$$A = \{j \mid u_{ij} \equiv \pm 1 \pmod{4}\} \tag{6}$$

and

$$B = \{j \mid u_{ij} \equiv 0, 2 \pmod{4}\}. \tag{7}$$

By Equation (5), we have

$$|A| \equiv -1 \pmod{4}. \tag{8}$$

Since $UU^T = -I$ over $\mathbb{Z}_4$, we have $UU^T = I$ over $\mathbb{Z}_2$. For $j \in A$, we have $u_{ij} \equiv 1 \pmod{2}$, and for $j \in B$, we have $u_{ij} \equiv 0 \pmod{2}$. Let $wt(\mathbf{u}_i)$ be the weight of $\mathbf{u}_i$ over $\mathbb{Z}_2$. By Equation (8), we have

$$wt(\mathbf{u}_i) \equiv -1 \pmod{4}. \tag{9}$$

We consider the matrix $G = [I \mid U]$ over $\mathbb{Z}_2$. Then, G is $a \times 2a$; i.e., $(4t+2) \times (8t+4)$ matrix. By Equation (9), each row of G has weight $w \equiv 0 \pmod 4$ over $\mathbb{Z}_2$. Let C be the binary code generated by G. Then, C is a doubly even self-dual (Type II) code, since $GG^T = O$ and the weight of each row of G is doubly even over $\mathbb{Z}_2$. By Lemma 2, the code length of C should be a multiple of eight. However, the code length of C is $8t+4$. This leads to a contradiction. Therefore, there is no $a \times a$ matrix U such that $UU^T = -I$ over $\mathbb{Z}_4$. This completes the proof. □

We update Theorem 2 using the previous theorem, and the case $\mathbb{Z}_{2^m}$ is settled.

Theorem 4. *For the existence of an $a \times a$ matrix U over $\mathbb{Z}_{2^m}$ such that $UU^T = -I$, we have the following.*

1. *If $m = 1$, then there exists such U for all $a \geq 1$.*
2. *If $m \geq 2$, then there exists such U if and only if a is a multiple of four.*

4. On the Problem of the Existence of a Matrix U Such That $UU^T = -I$ over $\mathbb{Z}_{p^m}$, Where p Is an Odd Prime

In this section, we consider the existence problem of a matrix U such that $UU^T = -I$ over $\mathbb{Z}_{p^m}$, where p is an odd prime. We start with the following lemma, which can be found in elementary number theory books (see, for example, [19] (Theorem 8.10)).

Lemma 3. *An integer $n > 1$ has a primitive root if and only if*

$$n = 2, 4, p^k, or\ 2p^k, \tag{10}$$

where p is an odd prime.

We consider two cases: $p \equiv 1 \pmod 4$ and $p \equiv -1 \pmod 4$. If $p \equiv 1 \pmod 4$, we need the following lemma whose proof can be made using elementary number theory (see, for example, [14] (Lemma 2.1)).

Lemma 4. *Let p be an odd prime and m a positive integer. Then, -1 is a square in $\mathbb{Z}_{p^m}$ if and only if $p \equiv 1 \pmod 4$.*

Proof. -1 is a square in $\mathbb{Z}_{p^m}$ if and only if $(-1)^{\frac{\phi(p^m)}{2}} \equiv 1 \pmod{p^m}$, where ϕ is an Euler-phi function (see, for example, [19] (Theorem 8.12)). Equivalently, $(-1)^{\frac{p^{m-1}(p-1)}{2}} \equiv 1 \pmod{p^m}$ if and only if $p \equiv 1 \pmod 4$. □

If $p \equiv -1 \pmod 4$, we first prove the following lemma, which is an integral part of the main theorem in this section.

Lemma 5. *Let $p \equiv -1 \pmod 4$. Then, every unit of $\mathbb{Z}_{p^m}$ can be written as a sum of two squares in $\mathbb{Z}_{p^m}$.*

Proof. Let $\mathbb{Z}_{p^m}^*$ be the set of units of $\mathbb{Z}_{p^m}$. By Lemma 3, there is a primitive root β such that $\mathbb{Z}_{p^m}^* = \langle \beta \rangle$. Then, $|\beta| = p^{m-1}(p-1)$. We define Q, N, M by the following:

$$Q = \{0,\ \beta^{2i} \mid i = 1, 2, \ldots, \frac{p^{m-1}(p-1)}{2}\} \tag{11}$$

$$N = \{\beta^{2i+1} \mid i = 1, 2, \ldots, \frac{p^{m-1}(p-1)}{2}\} \tag{12}$$

$$M = \{p \times i \mid i = 1, 2, \ldots, p^{m-1} - 1\} \tag{13}$$

Then, $\mathbb{Z}_{p^m} = Q \cup N \cup M$.

We claim that Q is not closed under addition. We assume the contrary towards a contradiction. Since Q is finite, Q is an additive subgroup in $\mathbb{Z}_{p^m}$. Therefore, $|Q|$ divides $|\mathbb{Z}_{p^m}|$; i.e.,

$$(p^{m-1} \times \frac{p-1}{2} + 1) \mid p^m. \tag{14}$$

Then,

$$p \mid (p^{m-1} \times \frac{p-1}{2} + 1). \tag{15}$$

This is a contradiction. Therefore, Q is not closed under addition. Thus, there are i and j such that $\beta^{2i} + \beta^{2j} \notin Q$.

We claim that $\beta^{2i} + \beta^{2j} \in N$. We assume that $\beta^{2i} + \beta^{2j} \notin N$. Then, $\beta^{2i} + \beta^{2j} \in M$ and $\beta^{2i} + \beta^{2j} = pk$ for some k. Hence, $\beta^{2i} + \beta^{2j} \equiv 0 \pmod{p}$. Consequently, $\beta^{2i} \equiv -\beta^{2j} \pmod{p}$. Thus, $-1 \equiv (\beta^{i-j})^2 \pmod{p}$. This is a contradiction, since -1 is not a square by Lemma 4. Therefore, $\beta^{2i} + \beta^{2j} \in N$.

Thus, $\beta^{2i} + \beta^{2j} = \beta^{2k+1}$ for some k. Therefore, $\beta = (\beta^{i-k})^2 + (\beta^{j-k})^2$. Hence, for any l, $\beta^{2l} = (\beta^l)^2 + 0^2$ and $\beta^{2l+1} = (\beta^l \times \beta^{i-k})^2 + (\beta^l \times \beta^{j-k})^2$. This completes the proof. □

We now state the main results in this section.

Theorem 5. *Let p be an odd prime. Then, for the existence of an $a \times a$ matrix U over $\mathbb{Z}_{p^m}$ such that $UU^T = -I$, we have the following for all $m \geq 1$.*

1. *If $p \equiv 1 \pmod{4}$, then there exists such U for all $a \geq 1$.*
2. *If $p \equiv -1 \pmod{4}$, then there exists such U if and only if a is even.*

Proof. We assume that $p \equiv 1 \pmod{4}$. By Lemma 4, there is an element c in $\mathbb{Z}_{p^m}$ such that $c^2 = -1$. Let U be an $a \times a$ diagonal matrix with all diagonal elements c; i.e,

$$U = \begin{pmatrix} c & & 0 \\ & \ddots & \\ 0 & & c \end{pmatrix}.$$

Then, $UU^T = -I$. This proves the first statement.

We now assume that $p \equiv -1 \pmod{4}$. By Lemma 5, there exist α, β such that $\alpha^2 + \beta^2 = -1$ in $\mathbb{Z}_{p^m}$. Let

$$U_2 = \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix}.$$

Then, $U_2 U_2^T = -I$. This proves that there is a 2×2 matrix U such that $UU^T = -I$. For $a = 2t$, where $t \geq 1$, let

$$U_a = \begin{pmatrix} U_2 & & 0 \\ & \ddots & \\ 0 & & U_2 \end{pmatrix}.$$

Then, $U_a U_a^T = -I$.

Finally, we assume that there is an $a \times a$ matrix U such that $UU^T = -I$. Then, $\det(UU^T) = \det(-I)$, $(\det U)^2 = (-1)^a$. Therefore, a should be even. This completes the proof. □

5. Examples

In this section, we provide examples of construction of self-dual codes over $\mathbb{Z}_{p^m}$ using Theorem 1. For $p = 2$, examples can be found in [15]. For $p \equiv 1 \pmod 4$, they can be found in [14]. Therefore, we provide examples for $p \equiv -1 \pmod 4$. All computations were performed with Magma [20].

Example 1. *A classification of self-dual codes over $\mathbb{Z}_9$ appears in [21]. For code length $n = 2$, there is unique self-dual code with generator matrix*

$$G_0 = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}.$$

We apply Theorem 1 with

$$U = X = \begin{pmatrix} 1 & 4 \\ 4 & -1 \end{pmatrix}.$$

Then, we have

$$G = \left(\begin{array}{cc|cc|cc} 1 & 0 & 0 & 0 & 1 & 4 \\ 0 & 1 & 0 & 0 & 4 & 8 \\ \hline 6 & 6 & 6 & 0 & 3 & 0 \\ 6 & 3 & 0 & 6 & 0 & 3 \end{array}\right). \tag{16}$$

By elementary row operation in G, we obtain the standard form

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 4 \\ 0 & 1 & 0 & 0 & 4 & 8 \\ 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 \end{pmatrix}. \tag{17}$$

Let C be the code generated by G_1. Then, it is easy to see that it is equivalent to the following code in [21]

$$C_{9,1,1} \bigoplus C_{9,1,1} \bigoplus C_{9,4,3}, \tag{18}$$

where $C_{9,1,1}$ is the code generated by the 1×1 matrix

$$(3) \tag{19}$$

and $C_{9,4,3}$ is the code generated by the 2×4 matrix

$$\begin{pmatrix} 1 & 0 & 8 & 5 \\ 0 & 1 & 5 & 1 \end{pmatrix}. \tag{20}$$

Example 2. *$C_{49,4,3}$ in [21] is the self-dual code of length 4 over $\mathbb{Z}_{49}$ generated by the matrix*

$$G_0 = \begin{pmatrix} 1 & 4 & 4 & 4 \\ 0 & 7 & 0 & 42 \\ 0 & 0 & 7 & 42 \end{pmatrix}. \tag{21}$$

We apply Theorem 1 with

$$U = \begin{pmatrix} 2 & 17 \\ 17 & -2 \end{pmatrix} \text{ and } X = \begin{pmatrix} 1 & 1 & 39 & 17 \\ 10 & 17 & 1 & 48 \end{pmatrix}. \tag{22}$$

Then, we have

$$G = \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 1 & 1 & 39 & 17 \\ 0 & 1 & 0 & 0 & 10 & 17 & 1 & 48 \\ \hline 16 & 20 & 20 & 13 & 1 & 4 & 4 & 4 \\ 14 & 21 & 7 & 0 & 0 & 7 & 0 & 42 \\ 42 & 35 & 7 & 42 & 0 & 0 & 7 & 42 \end{array}\right) \tag{23}$$

By elementary row operation in G, we obtain the standard form

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 39 & 17 \\ 0 & 1 & 0 & 0 & 3 & 24 & 29 & 27 \\ 0 & 0 & 1 & 1 & 5 & 23 & 45 & 45 \\ 0 & 0 & 0 & 7 & 0 & 0 & 7 & 7 \\ 0 & 0 & 0 & 0 & 7 & 42 & 21 & 21 \end{pmatrix}. \tag{24}$$

Let C be the code generated by G_1. Then, C is a self-dual code of length 8*. We cannot compare this code with those in [21], since the classification in [21] has been carried out up to code length* 6*.*

Acknowledgments: The author wish to thank the reviewers for valuable remarks which helped to improve this article. The author was supported by the 2017 Professor Education and Research Promotion Program of KoreaTech.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Rains, E.; Sloane, N.J.A. Self-Dual Codes. In *Handbook of Coding Theory*; Pless, V.S., Huffman, W.C., Eds.; Elsevier: Amsterdam, The Netherlands, 1998.
2. Conway, J.H.; Pless, V. On the enumeration of self-dual codes. *J. Comb. Theory Ser. A* **1980**, *28*, 26–53.
3. Huffman, W.C.; Pless, V.S. *Fundamentals of Error-correcting Codes*; Cambridge University Press: Cambridge, UK, 2003.
4. Grassl, M.; Gulliver, T.A. On circulant self-dual codes over small fields. *Des. Codes Cryptogr.* **2009**, *52*, 57–81.
5. Harada, M. The existence of a self-dual $[70, 35, 12]$ code and formally self-dual codes. *Finite Fields Appl.* **1997**, *3*, 131–139.
6. Kim, J.-L. New extremal self-dual codes of lengths 36, 38, and 58. *IEEE Trans. Inf. Theory* **2001**, *47*, 386–393.
7. Kim, J.-L.; Lee, Y. Euclidean and Hermitian self-dual MDS codes over large finite fields. *J. Comb. Theory Ser. A* **2004**, *105*, 79–95.
8. Kim, J.-L.; Lee, Y. An Efficient Construction of Self Dual Codes. *Bull. Korean Math. Soc.* **2015**, *52*, 915–923.
9. Alfaro, R.; Dhul-Qarnayn, K. Constructing Self-Dual codes over $\mathbb{F}_q[u]/(u^t)$. *Des. Codes Cryptogr.* **2015**, *74*, 453–465.
10. Dougherty, S.T.; Kim, J.-L.; Kulosman, H.; Liu, H. Self-dual codes over commutative Frobenius rings. *Finite Fields Appl.* **2010**, *16*, 14–26.
11. Dougherty, S.T.; Kim, J.-L.; Liu, H. Constructions of Self-dual Codes over Finite Commutative Chain Rings. *Int. J. Inf. Codin. Theory* **2010**, *1*, 171–190.
12. Han, S.; Lee, H.; Lee, Y. Construction of Self Dual Codes over $\mathbb{F}_2 + u\mathbb{F}_2$. *Bull. Korean Math. Soc.* **2012**, *49*, 135–143.
13. Kim, J.-L.; Lee, Y. Construction of MDS Self-dual codes over Galois rings. *Des. Codes Cryptogr.* **2007**, *45*, 247–258.
14. Lee, H.; Lee, Y. Construction of self-dual codes over finite rings $\mathbb{Z}_{p^m}$. *J. Comb. Theory Ser. A* **2008**, *115*, 407–422.
15. Han, S. A method for costructing self-dual codes over $\mathbb{Z}_{2^m}$. *Des. Codes Cryptogr.* **2015**, *75*, 253–262.
16. Massey, J.L. Orthogonal, antiorthogonal and self-orthogonal matrices and their codes. *Commun. Codin.* **1998**, *2*, 3.
17. Massey, J.L. On Antiorthogonal Matrices and Their Codes. In Proceedings of the 1998 IEEE International Symposium on Information Theory (ISIT), Cambridge, MA, USA, 16–21 August 1998.
18. Huffman, W.C. On the classification and enumeration of self-dual codes. *Finite Fields Appl.* **2005**, *11*, 451–490.

19. Burton, D.M. *Elementary Number Theory*, 6th ed.; McGraw-Hill International Edition; McGraw-Hill: New York, NY, USA, 2007.
20. Bosma, W.; Cannon, J.; Playoust, C. The Magma algebra system. I. The user language. *J. Symbolic Comput.* **1997**, *24*, 235–265.
21. Balmaceda, J.M.P.; Betty, R.A.L.; Nemenzo, F.R. Mass formula for self-dual codes over $\mathbb{Z}_{p^2}$. *Discret. Math.* **2017**, *308*, 2984–3002.