Research Journal of Applied Sciences, Engineering and Technology 5(5): 1848-1852, 2013
DOI:10.19026/rjaset.5.4948
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: August 11, 2012 Accepted: September 03, 2012 Published: February 11, 2013

Research Article

The Linear Orthomorphisms on the Ring Z_n

[1]Haiqing Han, [2]Yazhou Xiong and [3]Siru Zhu
[1]Department of Mathematics and Physics,
[2]Department of Economics and Management, Hubei Polytechnic University,
Huangshi 435003, Hubei, China
[3]Department of the Basics, AFRA, Wuhan 430019, Hubei, China

Abstract: Linear orthomorphism has the well diffusibility, which can be used to design P-permutation in cryptography. This paper presents the definition of the linear orthomorphisms and orthomorphic matrices on the integer residue class ring, whose counting formulas have been obtained too. They have provided a theoretical basis to research the nature of orthomorphisms on the ring in the cryptography.

Keywords: Linear orthomorphisms, orthomorphic matrix, the integer residue class ring, the orthomorphisms

INTRODUCTION

Shannon (1994) the well-known communications experts, has pointed out that the main idea of the cipher design is the diffusion and confusion. From the mathematical point of view, the combination of the linear and nonlinear permutations has a good role on diffusion and confusion. Complete mappings is widely used because of the good cryptographic properties, they have been proposed and studied as early as 1942 in Mann (1943) and shortly thereafter, they have been researched from the perspective of the algebraic geometry and group theory in Hall and Paige (1957). Then, the complete mappings have been widely used at the block design, statistical analysis, the areas of channel coding and so on. The orthomorphisms and Omni directional permutations are two important kinds of complete mappings. The concept of orthomorphisms was firstly formally presented in Jin-Ping and Shu-Wang (2006) for the study the orthogonal of Latin squares. Dr. L. (1995), in U.S., Mittenthal of TET (Teledyne Electronic Technology) has first studied orthomorphisms from the cryptography (Lohrop, 1995) and he also proved that the orthomorphisms over GF (2^n) have a good cryptographic property: completely balanced. The orthomorphisms over GF (2^n) have been also used on the design cipher, the digital signature and authentication algorithms. The commercial block cipher SMS4 has been designed on the round function based on the nonlinear orthomorphism (Shuwang *et al*., 2008). In addition to the commercial cipher, the orthomorphisms have the other related applications, such as:

- Teledyne Electronic Technology has researched and developed the cipher products DSD used orthomorphisms (Lohrop, 1995).
- In Qibin and Ken Cheng (1996) the linear orthomorphisms have been used to enhance the cipher security and improve cryptography properties.
- In Dawu *et al*. (1999) the orthomorphisms have been constructed Boolean functions, which meet the balance; algebraic degree is not less than 3.

The aspects of the nonlinearity, linear structure, the infusibility have good character.

In general, the orthomorphisms are classified into the linear and the nonlinear two kinds to study. This study focuses on the linear orthomorphisms over the ring Z_n.

The counting formula and generation algorithm (Yong and Qijun, 1996; Zongduo and Solonmen, 1999) of the linear orthomorphisms over the finite field F_2^n have been obtained, but they are very complex. In addition, the counting formula and generation algorithm of the nonlinear orthomorphisms have not been studied well. In order to explore orthomorphism more in cryptography applications, as well as to further study the mathematical properties and mathematical applications of them, this study have proceed the more extensive research of orthomorphisms over the ring instead of the finite field, because the nature of orthomorphisms over the ring is meet and it also must satisfy over the field. For simplicity, we have studied only the linear orthomorphisms over the ring Z_n, as the nonlinear orthomorphisms over Z_n will be researched later on.

Corresponding Author: Yazhou Xiong, Department of Economics and Management, Hubei Polytechnic University, Huangshi 435003, Hubei, China

In the design of modern cryptography, the linear orthomorphisms have been designed in the P-permutation (Haiqing and Huanguo, 2010). P-replacement the cryptography indicator to Measure the P-permutation is branch number. So the linear orthomorphisms with the largest branch number have been choose to design the cipher parts and the linear orthomorphisms over the ring Z_n is exactly the rich resources to design the P-permutations. We have studied the enumeration and construction problems of the linear orthomorphisms and the orthomorphic matrices over Z_n in this study.

PRELIMINARIES

Let $Z_n = \{\bar{0}, \bar{1}, \cdots, \overline{n-1}\}$ be the residue class ring of integers modulo n, where $\bar{i}$ represents the class of all integers that the remainder is i divided by n, Consider the following permutation.

Definition 1: Let $\sigma : Z_n \to Z_n$ be the permutation on Z_n, σ is called the orthomorphism on Z_n, if σ + I (I is a unit transformation) is the permutation on Z_n too. σ is called the Omnidirectional permutation, if σ - I is also the permutation on Z_n.

For the every integer l (l<n), σ is called the l - generalized orthomorphism, if σ + lI are all the permutations on Z_n. $\forall x, y \in Z_n$, if σ(x + y) = σ(x) + σ(y) then σ is said as the linear orthomorphism.

Let F be the finite field, the polynomial $f \in F[X]$ So $\forall c \in F$, $f(c) \in F$.

The Polynomial f ϵ F[X] is a transformation on F. If f (X) is one to one transformation, then it is said a permutation on F. It is easy to the following facts: that f(X) is a permutation on Fif and only if $f : c \mapsto f(c)$ is injective on F, if and only if f is a subjective on F, if and only if $\forall a \in F$ the equation f (X) = a has the solution, if and only if $\forall a \in F$ the equation f(X) = a has a unique solution.

Definition 2: Let $f \in F[X]$ and $f(X) = a_0 + a_1X + \ldots + a_nX^n$, if $a_n \neq 0$, then f(X) = is said the polynomial of the degree n. Denote deg(f(X)) = n.

By the Lagrange interpolation formula, and a permutation on F can be expressed into the polynomial of the degree not more then (|F| - 1). Where |F| is the cardinality of the finite field F.

Definition 3: Let A be a matrix on Z_n, that is the entries of A come from Z_n, the determinant of A is defined as usual, so the value of the determinant of A is an element in Z_n. If this element is invertible about the multiplication (or the addition generator), then it is said by invertible. The matrix A is said the orthomorphic matrix on the ring Z_n, if the matrices A and A + I are all invertible.

By the definition 2, the matrix A on Z_n is the orthomorphic matrix if and only if det A and det (A + I) are the invertible element (or generators) in Z_n, if and only if gcd (det A, n) = 1 and gcd (det A, n) = 1 set up at the same time by the definition of the invertible element in Z_n.

The linear orthomorphism and the orthomorphic matrix are one to one over the finite field (Yun and Hongwei, 2002). But the linear orthomorphism and the orthomorphic matrix are not satisfied the one-one corresponding over the ring Z_n. And it is also difficult to express the orthomorphism into the polynomial over the ring Z_n. The evidence shows that the research method of orthomorphisms over the finite field cannot be used to study the orthomorphisms over the ring Z_n.

In order to understand the algebraic structure properties of the ring, the isomorphism theorem of the ring Z_n is firstly given.

Lemma 1: Let n be the order of the ring Z_n, the standard decomposition is $n = p^{r1}{}_1\, p^{r2}{}_2 \ldots p^{rs}{}_s$, where p_1, $p_2, \ldots, p_s$ p_1, are the distinct prime numbers, denote $m_i = p^{ri}{}_i (1 \leq i \leq s)$, then there is the ring isomorphism: $Z_n \cong Z_{m_1} \oplus Z_{m_2} \oplus \cdots \oplus Z_{m_s}$.

This is the famous Chinese Remainder Theorem, we need not give the proof because of it can be found in many textbooks. In Shuwang *et al*. (2008), it has pointed out there is the one to one corresponding relationship between the orthomorphism and the Omni directional permutation over the ring Z_n, as long as an orthomorphism is constructed, it is easy to get an Omni directional permutation over the ring Z_n, so they are uniform to study for simplicity. We have only studied the linear orthomorphism on the ring Z_n (that is equivalent to study the linear Omni directional permutation on the ring Z_n). From the algebra, the ring Z_n is a cyclic group on its addition, the isomorphism number of the cyclic group is determined by its generators. And $\forall \bar{a} \in Z_n$, $\bar{a}$ is an additive generator if and only if gcd (a, n) = 1, where a is one representative of the remaining class $\bar{a}$. It is easy that the number of the additive generators in the ring Z_n is φ(n) (φ is the Euler function).

THE MAIN CONCLUSIONS

With this basic knowledge, we can get some conclusions on the linear orthomorphisms over the ring Z_n.

Theorem 1: Let σ be a linear orthomorphism over the ring Z_n, if and only if σ and (σ + I) are the automorphism of the additive group Z_n.

Proof: σ is a linear orthomorphism over the ring Z_n, if and only if σ and (σ +I) are the linear permutations over the ring Z_n. As Z_n is an additive group, $\forall x, y \in Z_n$, it is satisfied σ(x + y) = σ(x) + σ(y). Hence, σ is the group orthomorphisms on Z_n. Similarly, (σ + I) are also the group orthomorphisms.

The linear orthomorphisms over the ring Z_n are linked into the group orthomorphisms by theorem 1. Here is the decomposition property of the ring auto morphisms.

Lemma 2 (Yun and Hongwei, 2002): Let $Z_n \cong Z_{m_1} \oplus Z_{m_2} \oplus \cdots \oplus Z_{m_s}$, where $n = p^{r1}{}_1\, p^{r2}{}_2 \ldots p^{rs}{}_s$ and $m_i = p^{ri}{}_i$ (1≤i≤s), then σ is the orthomorphisms of the additive group if and only if σ $|Z_{mi}$ is the orthomorphisms of Z_{mi}(1≤i≤s). Where σ $|_{Zmi}$ is indicated that the automorphisms σ on $Z_n$is restricted on Z_{mi}.

Lemma 2 demonstrates that if the automorphism σ $|Z_{mi}$ = σ_i on Z_{mi}(1≤i≤s) are found, then the group automorphism σ = (σ_1, σ_2, … , σ_s) on Z_n satisfied σ$|Z_{mi}$ = σ on Z_{mi}(1≤i≤s) can be determined. The linear orthomorphism over the ring Z_n can be transformed the group automorphism on Z_n, and the group automorphism σ = (σ_1, σ_2,…, σ_s) on Z_n can be transformed the group automorphism on Z_{mi}(1≤i≤s). Thus the whole question is to find the additive group automorphism on Z_{mi} (where $m_i = p^{ri}{}_i$ is a prime power). But, the additive group automorphism on Z_{mi} is determined entirely by the additive generator. $\forall x, y \in Z_{m_i}$, they are any two additive generators on Z_{mi}, then σ (x) = y determines an additive group automorphism σ on Z_{mi}. The number of generators in Z_{mi} is φ(m_i), where φ(m_i) is the Euler function, which the number of the elements are coprime to m_i in the set {0, 1, … , m_i - 1}.

Theorem 2: The number of the linear orthomorphisms over the ring $Z_p{}^r$ (p is prime) is:

$$\varphi(p^r)\phi(p^r) = p^{r-1}(p-1)p^{r-1}(p-2)$$

Proof: From the previous analysis, σ is the linear orthomorphisms over the ring Z_{pr} if and only if σ and (σ + I) are both the additive group orthomorphisms over the ring $Z_p{}^r$, if and only if σ and (σ + I) become the generators into the generators. Note $\overline{a}, \overline{b}$ are in the ring $Z_p{}^r$, then $\overline{a}, \overline{b}$ are the residue class, a, b are respectively representative element in $\overline{a}, \overline{b}$. $\overline{a}, \overline{b}$ are the generators if and only if a, b are prime to n. Without loss of generality, suppose $\sigma(\overline{a}) = \overline{b}$, then $(\sigma + I)(\overline{a}) = \overline{b} + \overline{a}$. The number of the linear orthomorphisms are completely determined by the pairs {a, b} (0≤a, b≤p^r - 1), they satisfied:

$$\begin{cases} \gcd(a, p^r) = 1 & (1) \\ \gcd(b, p^r) = 1 & (2) \\ \gcd(a+b, p^r) = 1 & (3) \end{cases}$$

a and b are respectively expressed into p-hexadecimal numbers:

$$a = a_0 + a_1 p + \cdots + a_{r-1} p^{r-1}$$

where,

$$0 \le a_i \le p-1 (0 \le i \le r-1)$$

$$b = b_0 + b_1 p + \cdots + b_{r-1} p^{r-1}$$

where,

$$0 \le b_i \le p-1 (0 \le i \le r-1)$$

If the Eq. (1) is establishment, then $a_0 \neq 0$; the Eq. (2) is establishment, then $b_0 \neq 0$; the Eq. (3) is establishment, then $a_0 + b_0 \neq p$. And the other a_i, b_i are only satisfied 0≤a_i≤p - 1(1≤i≤r - 1) and 0≤a_i≤ p - 1(1≤i≤ r - 1). a is entirely decision by {a_0, a_1, … , a_{r-1}}, there are (p - 1) choices to a_0 and there are p choices to each a_1, a_2, …. , a_{r-1}. There are φ(p^r) selection methods to a, namely φ(p^r) = p^{r-1} (p - 1); b is also completely determined by {b_0, b_1, … , b^{r-1}}. However, when a is selected well, there are (p - 2) choices to b_0 and there are p choices to each b_1, b_2,…, b_{r-1}. So there are ϕ(p^r) selection methods to b, that is ϕ(p^r) = p^{r-1} (p - 2). The linear orthomorphism σ is determined by a pair of numbers {a, b} with $\sigma(\overline{a}) = \overline{b}$.

In summary, the number of the linear orthomorphisms over the ring Zp^r is:

$$\varphi(p^r)\phi(p^r) = p^{r-1}(p-1)p^{r-1}(p-2)$$

It is easy to get the counting formula of the linear orthomorphisms over the ring Z_n Combined with Theorem 1 and 2.

Theorem 3: Let Z_n be the ring met $n = p^{r1}{}_1\, p^{r2}{}_2 \ldots p^{rs}{}_s$, the number of the linear orthomorphisms Z_n is:

$$\prod_{i=1}^{s} \varphi(p_i^{r_i})\phi(p_i^{r_i}) = \prod_{i=1}^{s} [p_i^{r_i-1}(p_i-1)p_i^{r_i-1}(p_i-2)]$$

Proof: Let $Z_n \cong Z_{m_1} \oplus Z_{m_2} \oplus \cdots \oplus Z_{m_s}$, where $m_i = p^{ri}{}_i$ (1≤i≤s). By Lemma 2, the linear orthomorphism over the ring Z_n is entirely determined by the set of the linear orthomorphisms {σ$|Z_{mi}$} over {Z_{mi} (1≤i≤s)}. The linear orthomorphism over Z_n can be formed, as long as the linear orthomorphisms are constructed over each Z_{mi} ($1 \le i \le s$). That is $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_s)$, where $\sigma |Z_{mi} = \sigma_i$. By the Multiplication combination principle, the number of the linear orthomorphisms Z_n is:

$$\prod_{i=1}^{s} \varphi(p_i^{r_i})\phi(p_i^{r_i}) = \prod_{i=1}^{s} [p_i^{r_i-1}(p_i-1)p_i^{r_i-1}(p_i-2)]$$

With above results, it is basically clear to the construction and enumeration of the linear orthomorphisms over the ring Z_n, which is the linear Omni directional permutation over the ring Z_n is all clear. But sometimes it needs to study the orthomorphic matrix over the ring. By the preceding discussion, the linear orthomorphism and the orthomorphic matrix are not satisfied the one-one corresponding over the ring Z_n. It must be researched.

Let $A = (a_{ij})_{k\times k}$ be the k×k matrix on Z_n, that is $a_{ij} \in Z_n$. By the definition of the determinant:

$$\det A = \sum_{i_1 i_2 \cdots i_k} (-1)^{\tau(i_1 i_2 \cdots i_k)} a_{i_1 1} a_{i_2 2} \cdots a_{i_k k}$$

where the sum is the all arrangement ($i_1 i_2 \dots i_k$) of 1, 2, … k. $\tau(i_1 i_2 \dots i_k)$ represents the inverse ordered number of the arrangement ($i_1 i_2 \dots i_k$). By definition, if $A = (a_{ij})_{k\times k}$ is the matrix on the ring Z_n, then $\det A \in Z_n$.

Lemma 3: Shengyuan (1999), Let $A = (a_{ij})_{k\times k}$ be an invertible matrix on the ring Z_n, if and only if $\det A$ is the multiplication invertible element in Z_n. Let $Z_n \cong Z_{m_1} \oplus Z_{m_2} \oplus \cdots \oplus Z_{m_s}$ and $A = (a_{ij})_{k\times k}$ is an invertible matrix on the ring Z_n, after the every element in the residue class a_{ij} is modulo m_t, $A = (a_{ij})_{k\times k}$ can regard as a matrix on Z_{mt}, then A is invertible matrix on the ring Z_{mt}. On the contrary, find an invertible matrix $A_t = (a^{(t)}_{ij})_{k\times k}$ on the each ring Z_{mt}($1 \le t \le s$), through the isomorphism $f: Z_n \to Z_{m_1} \oplus Z_{m_2} \oplus \cdots \oplus Z_{m_s}$, we have obtained the matrix $A = (a_{ij})_{k\times k}$, satisfied $aij = f(a^{(1)}_{ij}, a^{(2)}_{ij}, \dots, a^{(s)}_{ij})$, then $A = (a_{ij})_{k\times k}$ is invertible on the ring Z_n. Then the invertible matrix on the ring Z_n can be converted into the invertible matrix on the ring $Z_p^{\ r}$ (p is prime). A matrix $A = (a_{ij})_{k\times k}$ on the ring Z_n is invertible if and only if gcd (det A, p^r) = 1, so gcd(det A, p) = 1, which is indicated that the matrix $A = (a_{ij})_{k\times k}$ is invertible regarded on the ring Z_p. While the ring Z_p is a finite field, the number of the invertible matrices with the order k is $\prod_{i=0}^{k-1}(p^k - p^i)$ on the finite field Z_p. Further, any invertible matrix with the order k on the ring Z_p can be extended into the invertible matrix on the ring $Z_p^{\ r}$, only let $A' = (a_{ij} + lp)_{k\times k}, 0 \le l \le p^{r-1} - 1$. Then an invertible matrix with the order k on the ring Z_p can be extended into $p^{k2(r-1)}$ invertible matrices on the ring Z_{pr}. So the number of the invertible matrices with the order k on the ring Z_{p^r} is $\prod_{i=0}^{k-1}(p^k - p^i)p^{k^2(r-1)}$. With a similar method, we have determined the number of the orthomorphic matrix with the order k on the ring Z_{pr}.

Theorem 4: The number of the orthomorphic matrices with the order k on the ring Z_{pr} is $T_k(p)$ ($k \ge 2$), then:

$$T_k(p) = (\sum_{l=2}^{k} \prod_{i=1}^{l-1} (p^k - p^i) p^{k(k-l)+l-2} L_{k-l}(p)) p^{k^2(r-1)}$$

where, $L_{k-l}(p)$ = the number of the matrices with the order (k - I) on the ring Z_p and they have no the Eigen values 0 and 1. Regulate: $L_0(p) = 1$ and $L_1(p) = p - 1$.

Proof: The orthomorphic matrices with the order k on the ring Z_{pr} can be extended from orthomorphic matrices on the ring Z_p. The matrix $A = (a_{ij})_{k\times k}$, on the ring Z_{pr} is the orthomorphic matrices with the order k if and only if A, A + I are invertible, A, A + I can be entirely expanded from invertible matrices on the ring Z_p. Hence, it only needs to find out invertible matrix A with the order k on the ring Z_p satisfied that (A + I) is invertible; it can be extended to invertible matrix A with the order k on the ring Z_{pr}.

Imitate the proof method in Shengyuan (1999), it is easy to get the number of the matrices with the order (kI) on the ring Z_p and they have no the eigenvalues 0 and 1, that is:

$$\sum_{l=2}^{k} \prod_{i=1}^{l-1} (p^k - p^i) p^{k(k-l)+l-2} L_{k-l}(p)$$

where, $L_{k-I}(p)$ is the number of the matrices with the order (k - I on the ring Z_p and they have no the eigenvalues 0 and 1. Then they can be extended to the ring Zp^r, the number of the orthomorphic matrices with the order k on the ring Zp^r is:

$$T_k(p) = (\sum_{l=2}^{k} \prod_{i=1}^{l-1} (p^k - p^i) p^{k(k-l)+l-2} L_{k-l}(p)) p^{k^2(r-1)}$$

The proof is end.

Next, we give the counting formula of the orthomorphic matrices with the order k on the ring Z_n.

Theorem 5: Let $Z_n \cong Z_{m_1} \oplus Z_{m_2} \oplus \cdots \oplus Z_{m_s}$ and $n = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}$, $m_i = p_i^{r_i} (1 \le i \le s)$, then the counting formula of the orthomorphic matrices with the order k on the ring Z_n is:

$$T_k(n) = \prod_{j=1}^{s} [p_j^{k^2(r-1)} (\sum_{l=2}^{k} \prod_{i=1}^{l-1} (p_j^k - p_j^i) p_j^{k(k-l)+l-2} L_{k-l}(p_j))]$$

where, $L_{k-l}(p_j)$ ($1 \le j \le s$) is the number of the matrices with the order (k - l) on the ring Z_{pj} and they have no the Eigen values 0 and 1. Regulate: $L_0(p_j) = 1$ and $L_1(p_j) = p_j - 1$.

The proof of theorem 5 is mainly that the orthomorphic matrices on the ring Z_n are transformed onto the ring Z_{pj}. Then the orthomorphic matrices on all the rings $\{Z_{pj}| \ 1 \leq j \leq s\}$ are isomorphism into the orthomorphic matrix on the ring Z_n, which is the result of the theorem. For simplicity, we have not proved this theorem.

CONCLUSION

We have mainly studied the linear orthomorphisms and the orthomorphic matrices on the ring Z_n in this study and given the counting formula. Because there exist the zero factors in the ring Z_n, the linear orthomorphisms and the orthomorphic matrices are not satisfied the one-one corresponding relationship over the ring Z_n. In cryptography, the linear orthomorphisms have mainly been designed the P-permutation. The important cryptography quality indicator to measure P-permutation is the branch number (Haiqing and Huanguo, 2010), it is still an important issue to research the linear orthomorphisms and the orthomorphic matrices on the ring Z_n. In addition, the nonlinear orthomorphisms have mainly been designed the S-box, which is the core of the cipher security.

ACKNOWLEDGMENT

This study is supported by the national natural science foundation of Hubei Polytechnic University (11YJZ10R) (801-8852).

REFERENCES

Dawu, G., L. Jihong and X. Guozhen, 1999. Construction of cryptographic functions based on orthomorphic permutation. J. XiDian Univ., 26: 40-43.

Haiqing, H. and Z. Huanguo, 2010. Research on the branch number of P-permutation in block cipher. J. Chinese Comput. Syst., 31: 921-926.

Hall, M. and L.J. Paige, 1957. Complete mappings of finite groups. Pacif. J. Math., 5: 541-54.

Jin-Ping, R. and L. Shu-Wang, 2006. Enumerations and counting of orthomorphic permutations. J. Comp. Res. Dev., 43: 1071-1075.

Lohrop, M., 1995. Block substitution using orthormorphic mapping. Adv. Appl. Math., 16: 59-71.

Mann, H.B., 1943. The construction of orthogonal latin squares. Ann. Math. Statist., 13: 418-423.

Qibin, Z. and Z. Ken Cheng, 1996. On transformations with halving effect on certain subvarieties of the space vm (F2). Proceedings of China Crypt, ZhengZhou, China.

Shannon, C.E., 1949. Communication theory of secrecy system. Bell. Syst. Technic. J., 27: 656-715.

Shengyuan, Z., 1999. The number of invertible matrices of order m over. J. Fujian Normal University (Natural Science). 15: 13-15.

Shuwang, L., F. Xiubin, *et al*., 2008. Complete Mapping and Application in Cryptography. China University of Technology Press, Hefei, China.

Yong, L. and L. Qijun, 1996. The construction and enumeration of the affine orthemorphisms. J. Ciphers Inform., 2: 23-25.

Yun, F. and L. Hongwei, 2002. Group and Combination Coding. Wuhan University Press, Wuhan, China.

Zongduo, D. and W.G. Solonmen, 1999. Generating all linear orthemorphisms without repetition. Discrete Math., 5: 47-55.