IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X.
PP 19-24
www.iosrjournals.org

Introduction and Outlook into the Aspects of Conjugate Multisets

Suma P[1], Dr. Sunil Jacob John[2]
[1]*Assistant Professor, Department of Mathematics, Government Engineering College, Sreekrishnapuram, Palakkad 678633, Kerala, India*
[2]*Associate Professor, Department of Mathematics, National Institute of Technology Calicut, Calicut 673601, Kerala, India*

Abstract: *In this paper, we define conjugate multisets and establish some of its properties. Corresponding to every multiset, a unique upper triangu- lar nonsingular matrix is formed by making use of this conjugate multiset. A novel approach in encryption and decryption is made using multisets and conjugate multisets.*
Keywords: *Multiset, Integer partition, Conjugate partition, Conjugate multiset, Encryption, Decryption*

I. Introduction

Multiset is a collection of elements in which elements are allowed to repeat.[1] In some situations, the classical definition of set proves inadequate and multisets become a very useful tool in such situations. Multisets are of interest in many areas of mathematics and Computer Science.

Research in multiset theory is still in infant stage. The relations and opera- tions with multisets [4] , relations and functions in multiset context [1], multiset representations in prime factorization, zeros and poles of meromorphic functions and in many other situations [5], multisets having negative integers as multi- pliers , known as Hybrid sets [3], Partition of multisets [6] etc. are some of the studies in the area of multisets.

A partition of a positive integer n is any non increasing sequence of positive integers that add upto n[13]. Integer partition and multisets are closely related. Many properties of integer partition can be proved with the help of multiset theory. The partition set M of a positive integer n is a multiset whose elements are from the set $\{1, 2, \ldots, n\}$. For example, 15 = 4 + 3 + 3 + 2 + 2 + 1. The corresponding multiset is $\{4, 3, 3, 2, 2, 1\}$.

Cryptography is the science of using mathematics to encrypt and decrypt data. Matrices are widely used in cryptography.[9] [12] [7] This paper is an attempt to introduce conjugate multiset by connecting multisets with integer partition. An application of multiset in cryptography is explained and illus- trated.

II. Multisets And Integer Partitions

Deftnition 2.1.[1] A collection of elements containing duplicate is called mul- tiset. If X is a set of elements, a multiset M drawn from X is represented by a function C_M defined as $C_M : X \to N$, where N is the set of non negative inte- gers. For each $x \in X$, $C_M(x)$ is the characteristic value of x in M and indicates the number of occurrence of x in M.
The word multiset often shortened to mset.

Notation 2.2. Let M be an mset from X with x_1 appearing k_1 times, x_2 appearing k_2 times and so on x_n appearing k_n times. Then M is written as $M = \{k_1|x_1, k_2|x_2, \cdots, k_n|x_n\}$.
Deftnition 2.3. The root set of an mset $M = \{k_1|x_1, k_2|x_2, \cdots, k_n|x_n\}$ is the classical set $S = \{x_1, x_2, \cdots, x_n\}$.
Deftnition 2.4.[1] Let M_1 and M_2 be two msets drawn from a set X. M_1 is a *submultiset* of M_2 ($M_1 \subseteq M_2$) if $C_{M_1}(x) \le C_{M_2}(x)$ for all x in X.

Deftnition 2.5.[1] Two msets M_1 and M_2 are *equal* if $M_1 \subseteq M_2$ and $M_2 \subseteq M_1$.

Deftnition 2.6.[1] Addition of two multisets M_1 and M_2 drawn from a set X results in a new multiset $M = M_1 \oplus M_2$ such that $\forall x \in X$, $C_M(x) = C_{M_1}(x) + C_{M_2}(x)$.

Deftnition 2.7.[1] Subtraction of two multisets M_1 and M_2 drawn from a set X results in a new multiset $M = M_1 \ominus M_2$ such that $\forall x \in X$, $C_M(x) = \max\{C_{M_1}(x) - C_{M_2}(x), 0\}$.

Deftnition 2.8.[11] Partition of a positive integer n is a non increasing sequence $\lambda = (\lambda_1, \lambda_2, \cdots, \lambda_k)$ of non negative integers λ_i such that $\lambda_1 + \lambda_2 + \cdots + \lambda_k = n$.

Partition diagram(Ferrers Diagram) 2.9.[8] The Ferrers diagram of an integer partition gives us a very useful tool for visualizing partitions, and some- times for proving identities. It is constructed by stacking left-justified rows of cells, where the number of cells in each row corresponds to the size of a part. The first row corresponds to the largest part, the second row corresponds to the second largest part, and so on

III. Conjugate Multisets

Deftnition 3.1.[8] *Conjugate of a partition* λ of a positive integer n is that whose diagram is the transpose (in the sense of matrices) of that of λ.

Every mset represents an integer partition and every integer partition can be written as an mset.

Deftnition 3.2. If M_1 is an mset corresponding to a partition λ, and M_2 is the mset corresponding to the conjugate partition of λ, then M_2 is called con- jugate mset of M_1.

Notation 3.3. Conjugate multiset of M is denoted as M^C.

As in the case of complex numbers, there is a unique conjugate for every multiset.

Theorem 3.4. If M is an mset corresponding to a partition λ of a positive integer n and M^C is the conjugate mset of M, then the cardinality of the root sets of M and M^C are same.

Proof :- Suppose $M = \{a_1|x_1, a_2|x_2, \cdots, a_k|x_k\}$ and $M^C = \{b_1|y_1, b_2|y_2, \cdots b_p|y_p\}$. Then root set of $M = \{x_1, x_2, \cdots, x_k\}$ and that of $M^C = \{y_1, y_2, \cdots, y_p\}$. So,

$|M| = k$ and $|M^C| = p$. From the definition of conjugacy, $a_1 + a_2 + \cdots + a_k = y_1$. If we remove the term $a_k|x_k$ from M and comparing its conjugate, we have $a_1 + a_2 + \cdots + a_{k-1} = y_2$. Proceeding like this, after removing $a_k|x_k, a_{k-1}|x_{k-1}, \cdots, a_2|x_2$, and comparing with its conjugate, we get $a_1 = y_p$.

Here, as we move from $a_1 + a_2 + \cdots + a_k$ to a_1 by successively removing one term in one step, the other side moves from y_1 to y_p and this completes the proof that $k = p$.

Theorem 3.5. If $M = \{a_1|x_1, a_2|x_2, \cdots, a_k|x_k\}$ is an mset and if

$y_i = \sum_{j=1}^{k-(i-1)} a_j$, for $i = 1, 2, \cdots, k$.

$b_i = x_{k-(i-1)} - x_{k-(i-2)}$, for $i = 2, 3, \cdots, k$. and

$b_1 = x_k$, then, $M^C = \{b_1|y_1, b_2|y_2, \cdots b_k|y_k\}$ is the conjugate mset of M.

Proof:- Suppose $M \in P(n)$ for some positive integer n. Then, $a_1x_1 + a_2x_2 + \cdots + a_kx_k = n$.

Now,

$b_1y_1 + b_2y_2 + \cdots + b_ky_k$

$= a_1x_1 + a_2x_2 + \cdots + a_kx_k$, by substituting $b_1, b_2, b_k, y_1, y_2, y_k$ and sim- plifying.

So, $M^C \in P(n)$.

If λ is the partition corresponding to M and λ^* is that of M^C, then it is easy to verify that λ and λ^* are conjugate partitions and hence M^C is the conjugate mset of M.

Theorem 3.6. (Construction of a Matrix from an Mset and its conju- gate) :-

Let $M = \{a_1|x_1, a_2|x_2, \cdots, a_k|x_k\}$ be a multiset that belongs to $P(n)$ for some positive integer n and let $M^C = \{b_1|y_1, b_2|y_2, \cdots b_k|y_k\}$ be the conjugate multiset of M.

Construct a square matrix A of order k as follows:

$$\begin{bmatrix} a_1b_1 & a_1b_2 & .. & .. & a_1b_k \\ 0 & a_2b_1 & a_2b_2 & .. & a_2b_{k-1} \\ 0 & 0 & a_3b_1 & .. & a_3b_{k-2} \\ .. & .. & .. & .. & .. \\ 0 & 0 & 0 & 0 & a_kb_1 \end{bmatrix}$$

..

Then A is upper triangular and non singular.

Proof:- The construction itself proves the upper triangulariry of A. Determinant of A is the product of the diagonal elements and is nonzero because $a_1, a_2, \cdots a_k$ and b_1 are positive. So A is nonsingular.

Moreover, Determinant of $A = \sum_{i=1}^{k} a_i b_1$
$= b_1(a_1 + a_2 + \cdots + a_k)$
$= b_1 y_1$

Corollary 3.7. Let $M = \{a_1|x_1, a_2|x_2, \cdots, a_k|x_k\}$ be a multiset that belongs to $P(n)$ for some positive integer n and let $M^c = \{b_1|y_1, b_2|y_2, \cdots b_k|y_k\}$ be the conjugate multiset of M. Then the elements of the matrix A of theorem 3.6 is also an mset that belongs to $P(n)$ for the same n.

Proof :- The sum of the elements of the first row of A is $\sum_{j=1}^{k} a_1 b_j$
$= a_1(b_1 + b_2 + \cdots + b_k)$
$= a_1 x_1$

Similarly, sum of the elements of second row is $\sum_{j=1}^{k-1} a_2 b_j$
$= a_2(b_1 + b_2 + \cdots + b_{k-1})$
$= a_2 x_2$

Proceeding like this, sum of the elements of i^{th} row is $a_i x_i$ and sum of the ele- ments of the last row is $a_k x_k$

So sum of the elements of A is $a_1 x_1 + a_2 x_2 + \cdots + a_k x_k$
$= n$.

Corollary 3.8. Let M be an mset that belongs to $P(n)$ and A be the corre- sponding unique upper triangular matrix. Let M_A be the mset of the elements of A. Starting from M^c, let B be the matrix and M_B is the mset. Then $M_A = M_B$, where the equality is the multiset equality.

Proof . Let $M = \{a_1|x_1, a_2|x_2, \cdots, a_k|x_k\}$ and $M^c = \{b_1|y_1, b_2|y_2, \cdots b_k|y_k\}$

Then A

Then A

$$A = \begin{pmatrix} a_1b_1 & a_1b_2 & .. & .. & a_1b_k \\ 0 & a_2b_1 & a_2b_2 & .. & a_2b_{k-1} \\ 0 & 0 & a_3b_1 & .. & a_3b_{k-2} \\ .. & .. & .. & .. & .. \\ .. & .. & .. & .. & .. \\ 0 & 0 & 0 & 0 & a_kb_1 \end{pmatrix}$$

and B =

$b_1 a_1 \quad b_1 a_2 \quad .. \quad .. \quad b_1 a_k$

$0 \qquad b_2 a_1 \quad b_2 a_2 \quad .. \quad b_2 a_{k-1}$

$$\begin{array}{ccccc} 0 & 0 & b_3a_1 & .. & b_3a_{k-2} \\ .. & .. & .. & .. & .. \\ .. & .. & .. & .. & .. \\ 0 & 0 & 0 & 0 & b_ka_1 \end{array}$$

The elements of the first row of A is exactly same as that of the elements of the main diagonal of B, second row of A is that just above the main diagonal of B and so on. That is, all the elements of A are there in B also and hence $M_A = M_B$.

Illustration 3.9 . Consider the mset $M = \{2|5, 1|4, 2|3, 3|1\}$ Then $M^C = \{1|8, 2|5, 1|3, 1|2\}$

Here both M and M^C are ϵ P (23).The matrices A and B are respectively,

and

$$\begin{array}{cccc} 2 & 4 & 2 & 2 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 2 & 4 \\ 0 & 0 & 0 & 3 \end{array}$$

$$\begin{array}{cccc} 2 & 1 & 2 & 3 \\ 0 & 4 & 2 & 4 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{array}$$

$M_A = M_B = \{2|4, 1|3, 5|2, 2|1\}$ which also ϵ P (23).

IV. Application Of Multisets And Conjugate Multisets In Cryptography

Here, we are giving an application of multiset in the field of Cryptography. Encryption and decryption are performed with the help of the matrix formed from multiset.

Encryption Algorithm 4.1

- Take the message (Plain text) as P

Translate the letters of P into their numerical equivalent by the rule $a = 1$, $b = 2$, $z = 26$, 0 for space between two alphabets and 27, the space between an alphabet and a digit or space between two digits. The digits are taken as it is.

- Form an Mset M from P as follows:

$M = \{a_1|x_1, a_2|x_2, \cdots a_k|x_k\}, x_1 > x_2 > \cdots x_k$

where $x_1, x_2, \cdots, x_k$ are the number of letters in the words of P having multiplicities $a_1, a_2, \cdots, a_k$.

- Write the conjugate mset $M^C = \{b_1|y_1, b_2|y_2, \cdots, b_k|y_k\}$ of M. Then,

$b_1 = x_k$, and

$b_i = x_{k-(i-1)} - x_{k-(i-2)}$ for $i = 2, 3, \cdots, k$

$$y_i = \sum_{j=1}^{k-(i-1)} a_j, \text{ for } i = 1, 2, \cdots, k.$$

- Split the numerical equivalent of P into blocks $P_1, P_2, \cdots P_m$, of size $l = 2^n$ digits, where n is chosen in such a way that $2^{n-1} < k \leq 2^n$, by adding sufficient number of zeros at the end of P_m.

Using M and M^c, an upper triangular nonsingular and having non neg- ative elements is constructed as discussed in theorem 2.15.

- Form the block diagonal matrix B of order l as $\begin{bmatrix} A & 0 \\ 0 & I \end{bmatrix}$
- Take $C_i = P_i B$, for $i = 1, 2, \cdots, m$.
- Let $c_{ij} = q_{(i-1)k+j} 26 + r_{(i-1)k+j}$, for $i = 1, 2, \cdots, m$ and $j = 1, 2, \cdots, k$, where c_{ij} is the j^{th} digit of C_i and $1 \le r_{(i-1)k+j} \le 26$.
- Form the cipher text as an mset $M_1 = \{d_{11}|z_{11}, d_{12}|z_{12}, \cdots, d_{mk}|z_{mk},$ where : $d_{ij} = q_{ij} + 1$, and z_{ij} is the r_{ij} th alphabet by taking $1st$ as a, $2nd$ as b etc.

Decryption algorithm 4.2

- From M_1, write C_i, $i = 1, 2, \cdots, m$.
- From M, Write A and find A^{-1} and write B^{-1}.
- Calculate $P_i = C_i B^{-1}$., for $i = 1, 2, \cdot, m$
- Write $P = [P_1 P_2 \cdots P_m]$.

Note 4.3 :- Both the cipher text and key are multisets. M_1 is the cipher text and M is the key

2. Illustration

Consider the message P = **YOUR PIN NUMBER IS 41265**. Then $M = \{1|6, 1|5, 1|4, 1|3, 1|2\}$ and $M^c = \{2|5, 1|4, 1|3, 1|2, 1|1\}$.

The corresponding matrix A is

$$\begin{bmatrix} 2 & 1 & 1 & 1 & 1 \\ 0 & 2 & 1 & 1 & 1 \\ 0 & 0 & 2 & 1 & 1 \\ 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 2 \end{bmatrix}$$

P_1, P_2 and P_3 are respectively

$$\begin{bmatrix} 25 & 15 & 21 & 18 & 0 & 16 & 9 & 14 \end{bmatrix}$$
$$\begin{bmatrix} 0 & 14 & 21 & 13 & 2 & 5 & 18 & 0 \end{bmatrix}$$
$$\begin{bmatrix} 9 & 19 & 27 & 4 & 1 & 2 & 6 & 5 \end{bmatrix}$$

The block diagonal matrix B is

$$\begin{bmatrix} A & 0 \\ 0 & I_3 \end{bmatrix}$$

C_1, C_2 and C_3 are

$$\begin{bmatrix} 50 & 55 & 82 & 97 & 79 & 16 & 9 & 14 \end{bmatrix}$$
$$\begin{bmatrix} 0 & 28 & 56 & 61 & 52 & 5 & 18 & 0 \end{bmatrix}$$
$$\begin{bmatrix} 18 & 47 & 82 & 63 & 61 & 2 & 6 & 5 \end{bmatrix}$$

The cipher text $M_1 = \{2|x, 3|c, 4|d, 4|s, 4|a, 1|p, 1|i, 1|n, 0|z, 2|b, 3|d, 3|i, 2|z, 1|e, 1|r, 0|z, 1|r, 2|u, 4|d, 3|k, 3|i, 1|b, 1|f, 1|e, \}$.

V. Conclusion And Future Work

Here in this paper, Conjugacy is introduced in Multiset theory. Like complex number and integer partition, conjugate mset is also unique for every mset. The matrix formed using mset and conjugate mset is upper triangular and nonsin- gular having diagonal elements as eigen values and all elements nonnegative. So this matrix can be used in many practical situations. In most of the methods of encryption and decryption, an invertible matrix is needed. In such situations also, the newly created matrix can be used.

References

[1]. K. P. Girish and Sunil Jacob John. (2009). *Relations and functions in multiset context*. Information sciences. **179**. 758–768.

[2]. Chris Brink. (1988). *Multisets and the Algebra of Relevance logic*. Non- Classical Logic. **5**. 75–95.

[3]. C. S. Calude , G. Paun , G. Rozenberg and A. Salomaa. (2001).

[4]. *Mathematics of Multisets*. Springer Verlag. 347–358

[5]. N.J.Wildberger. (2003). *A new look at multisets*. School of Mathematics UNSW Sydney 2053.

[6]. D. Singh , A. M. Ibrahim, T. Yohanna and J. N. Singh. (2007). *An overview of the application of multise*. Novi Sad J. Math. **37**. 73–92

[7]. Edward A.Bender. (1974). *Partitions of Multisets*. Discrete mathematics. 301–311

[8]. Penmetsa V Krishna Raja , A S N Chakravarthy and Prof. P S Avadhani (2011) *A cryptosystem based on Hilbert Matrix using cipher block chaining mode*. International Journal of Mathematics Trends and Technol- ogy.

[9]. Herbert S. Wilf (2000). *Lectures on Integer Partitions*. Delivered at the University of Victoria Canada

[10]. Dinesh P. Baviskar1, Sidhhant N. Patil2, and Onkar K. Pawar3. (2013). *Android based message encryption/decryption using matrix*. Interna- tional Journal of Research in Engineering and Technology. eISSN: 2319-1163- pISSN: 2321-7308

[11]. H. L. Alder (1969). *Partition Identities – From Euler to the Present*. Amer, math monthly. **76**. 733–746.

[12]. AlexanderD.Healy. (2001). *Partition Identities*. www.alexhealy.net/papers/math 192.pdf

[13]. M. Yamuna1, S. Ravi Rohith2, Pramodh Mazumdar3and Avani Gupta4. (2013). *Text Encryption Using Matrices*. International Journal of Application or Innovation in Engineering and Management.**2**. ISSN 2319 - 4847

[14]. G. E. Andrews (1985). *The Theory of Partitions*. Encyclopedia of Math and Its Applications. **2**.