Introduction and Outlook into the Aspects of Conjugate Multisets

Suma P¹, Dr. Sunil Jacob John²

¹Assistant Professor, Department of Mathematics, Government Engineering College, Sreekrishnapuram, Palakkad 678633, Kerala, India
²Associate 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 triangular 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 operations 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 multipliers, 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 n increasing sequence of positive integers that add up to 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, . . ., 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

Definition 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 CM defined as CM : X → N, where N is the set of non negative integers. For each x, CM(x) is its 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 x1 appearing k1 times, x2 appearing k2 times and so on xn appearing kn times. Then M is written as M = \{k1|x1, k2|x2, · · · , kn|xn\}.

Definition 2.3. The root set of an mset M = \{k1|x1, k2|x2, · · · , kn|xn\} is the classical set S = \{x1, x2, · · · , xn\}.

Definition 2.4. [1] Let M1 and M2 be two mssets drawn from a set X. M1 is a submultiset of M2 (M1 ⊆ M2) if CM1(x) ≤ CM2(x) for all x in X.

Definition 2.5. [1] Two mssets M1 and M2 are equal if M1 ⊆ M2 and M2 ⊆ M1.

Definition 2.6. [1] Addition of two multisets M1 and M2 drawn from a set X results in a new multiset M = M1 ⊕ M2 such that ∀ x ∈ X, CM(x) = CM1(x) + CM2(x).
Definition 2.7. [1] Subtraction of two multisets $M_1$ and $M_2$ drawn from a set $X$ results in a new multiset $M = M_1 - M_2$ such that $\forall x \in X$, $CM(x) = \max f CM_1(x) - CM_2(x), 0$.

Definition 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 $\lambda_i$ 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

Definition 3.1. [8] Conjugate of a partition $\lambda$ of a positive integer $n$ is that whose diagram is the transpose (in the sense of matrices) of that of $\lambda$.

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

Definition 3.2. If $M_1$ is an mset corresponding to a partition $\lambda$, and $M_2$ is the mset corresponding to the conjugate partition of $\lambda$, then $M_2$ is called conjugate 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 $\lambda$ 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 $M = \{a_1|x_1, a_2|x_2, \cdots, a_k|x_k\}$ is an mset and if

\[
y_i = \sum_{j=1}^{k} a_j, \text{ for } i = 1, 2, \cdots, k.
\]

\[
b_i = x_k-(i-1) - x_k-(i-2), \text{ for } i = 2, 3, \cdots, k.
\]

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, $b_1y_1 + b_2y_2 + \cdots + b_ky_k = n$.

If $\lambda$ is the partition corresponding to $M$ and $\bar{\lambda}$ is that of $M^C$, then it is easy to verify that $\lambda$ and $\bar{\lambda}$ are conjugate partitions and hence $M^C$ is the conjugate mset of $M$.

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

\[
y_i = \sum_{j=1}^{k} a_j, \text{ for } i = 1, 2, \cdots, k.
\]

\[
b_i = x_k-(i-1) - x_k-(i-2), \text{ for } i = 2, 3, \cdots, k.
\]

Then root set of $M$ is $\{y_1, y_2, \cdots, y_p\}$. 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 $a_1 + a_2 + \cdots + a_k = y_2$. 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 3.6. (Construction of a Matrix from an Mset and its conjugate) :-

Let $M = \{a_1|x_1, a_2|x_2, \cdots, a_k|x_k\}$ be a mset 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.

Construct a square matrix $A$ of order $k$ as follows:

\[
\begin{array}{cccc}
a_1b_1 & a_1b_2 & \cdots & a_1b_k \\
0 & a_2b_1 & a_2b_2 & \cdots & a_2b_{k-1} \\
0 & 0 & a_3b_1 & \cdots & a_3b_{k-2}
\end{array}
\]

Then $A$ is upper triangular and non-singular.

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

Moreover, Determinant of $A = \sum_{j=1}^{k} a_j b_j$

$$= b_1(a_1 + a_2 + \cdots + a_k)$$

$$= b_1y_1$$

**Corollary 3.7.** Let $M = \{a_1 | x_1, a_2 | x_2, \ldots, a_k | x_k\}$ be a multiset that belongs to $P(n)$ for some positive integer $n$ and let $M^c = b_1 | y_1, b_2 | y_2, \ldots, b_k | y_k$ 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

$$\sum_{j=1}^{k} a_j b_j$$

Similarly, sum of the elements of second row is

$$\sum_{j=2}^{k} a_j b_j$$

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

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

$$= n.$$
Introduction and Outlook into the Aspects of Conjugate Multisets

\[
\begin{array}{cccc}
\begin{array}{cccc}
\begin{array}{cccc}
0 & b_{2a1} & b_{2a2} & \ldots & b_{2ak-1} \\
\end{array}
\end{array}
\end{array}
\end{array}
\]
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 $MA = MB$.

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 $\in P(23)$.

The matrices $A$ and $B$ are respectively, and

\[
A = \begin{pmatrix}
2 & 4 & 2 & 2 \\
0 & 1 & 2 & 1 \\
0 & 0 & 2 & 4 \\
0 & 0 & 0 & 3
\end{pmatrix}
\]

\[
B = \begin{pmatrix}
2 & 1 & 2 & 3 \\
0 & 4 & 2 & 4 \\
0 & 0 & 2 & 1 \\
0 & 0 & 0 & 2
\end{pmatrix}
\]

$MA = MB = \{2[4, 1][3, 5][2, 2][1]\}$ which also $\in P(23)$.

### 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:

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

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

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

$b_1 = x_k$, and

$b_i = x_k-(i-1)-x_k-(i-2)$ for $i = 2, 3, \ldots, k$

\[
j_f = \sum_{k-(i-1)}^a a_f, \text{ for } i = 1, 2, \ldots, k.
\]

- Split the numerical equivalent of $P$ into blocks $P_1, P_2, \ldots P_m$, 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 negative elements is constructed as discussed in theorem 2.15.

- Form the block diagonal matrix \( B \) of order \( l \) as
  \[
  A \begin{array}{cccc}
  0 & & & \\
  \Sigma & & & I \\
  0 & & & \\
  \end{array}
  \]
- Take \( C_i = P_i B \), for \( i = 1, 2, \ldots, m \).
- Let \( c_{ij} = q(\mathbf{i} - 1)\mathbf{k} + j \mathbf{26} + r(\mathbf{i} - 1)\mathbf{k} + j \), for \( i = 1, 2, \ldots, m \) and \( j = 1, 2, \ldots, k \), where \( c_{ij} \) is the \( j^{th} \) digit of \( C_i \) and \( 1 \leq r(\mathbf{i} - 1)\mathbf{k} + j \leq 26 \).
- Form the cipher text as an mset \( M_1 = \{d_{11} | z_{11}, d_{12} | z_{12}, \ldots, d_{mk} | z_{mk}\} \).
- \( d_{ij} = q_{ij} + 1 \), 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 \( C_i \), \( i = 1, 2, \ldots, m \).
- From \( M \), Write \( A \) and find \( A^{-1} \) and write \( B^{-1} \).
- Calculate \( P_i = C_i B^{-1} \), for \( i = 1, 2, \ldots, m \)
- 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 \( P = \text{YOUR PIN NUMBER IS 41265} \). 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

\[
\begin{pmatrix}
2 & 1 & 1 & 1 \\
0 & 2 & 1 & 1 \\
0 & 0 & 2 & 1 \\
\end{pmatrix}
\]

\( P_1, P_2 \) and \( P_3 \) are respectively

\[
\begin{pmatrix}
0 & 0 & 0 & 1 \\
0 & 0 & 0 & 2 \\
\end{pmatrix}
\]

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

The block diagonal matrix \( B \) is

\[
\begin{pmatrix}
A & & & \\
0 & & & \\
I_3 & & & \\
\end{pmatrix}
\]

\( C_1, C_2 \) and \( C_3 \) are

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

\[
\begin{pmatrix}
\Sigma & \Sigma & \Sigma & \Sigma & \Sigma & \Sigma & \Sigma & \Sigma \\
\Sigma & \Sigma & \Sigma & \Sigma & \Sigma & \Sigma & \Sigma & \Sigma \\
\Sigma & \Sigma & \Sigma & \Sigma & \Sigma & \Sigma & \Sigma & \Sigma \\
\end{pmatrix}
\]
The cipher text \( M_1 = \{2|x, 3|c, 4|d, 4|s, 4|a, 1|p, 1|i, 1|m, 0|z, 2|h, 3|i, 2|z, 1|r, 1|l, 0|z, 1|r, 2|u, 4|d, 3|k, 3|i, 1|h, 1|f, 1|e, j\} \).

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 nonsingular 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

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