IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Modular arithmetic, Galois's fields and Vector space components and their partial relation to Graph Theory.

Dr Fakhruddin Khan

Assistant Professor, Applied Mathematics, Amity University, Rupaspur, Baily Road, Near police station, Patna.

ABSTRACT

In this paper I have worked to provide an introduction to the Modular arithmetic, Galois field and Vector space components and its relation to graph theory. Graph theory is an area of mathematics where modular arithmetic and vector space components are used for undirected graph. Vector and vector space discussed in the two-dimensional Euclidean space. The concept of representing vectors is now extended to representation of k- dimensional space by means of an ordered k-tuple. Vector space associated with graph and total number of subgraphs are discussed in relation to their edges. Linearly dependent and independent vectors are also explained following an example.

KEY WORDS: Modular Arithmetic, Galois Field GF(2), Vector Space, Euclidean Space, Basis Vector

Introduction: Modular arithmetic is a kind of integer arithmetic that reduces all numbers to a number belongs to the set of natural numbers [0, 1, 2, ……. n-1] by using mod function rule of arithmetic dealing with remainders. In this rule Galois field arises by the prime numbers that is a field formed by modulo of prime numbers. A vector space is defined in the form of vector addition '+' and scaler multiplication 'X'.

Concept: A system of numbers that has only three numbers in it viz 0, 1, 2 only and ordinary algebraic rules of addition and multiplication holds on them. The following exception is given below that if a number Q>= 3, it is to be divided by 3, the quotient is discarded, and the remainder is used in place of Q. The addition and multiplication table for such a number is given in the following table and are called **addition modulo 3** and **multiplication modulo 3.** Together they are called modulo 3 arithmetic. We can define any

modulo m arithmetic system consisting of m elements 0, 1, 2, 3, ……., m – 1 and the relationship for any q>m – 1:

Q = m.P + R = R (mod m) and R < m.

Table for addition modulo 5: Q = R (mod 5)

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3
5	0	1	2	3	4

Table for multiplication modulo 5: Q = R (mod 5)

x	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1
5	0	0	0	0	0

It can be verified that the set {0, 1, 2, 3, 4} with addition or multiplication modulo 5 is a field. The identity element with respect to addition is 0 and with respect to multiplication n is 1. Every element has unique additive inverse and with respect to multiplication it has a unique inverse. So, it can be easily verified that tables like tables of 2, 5 and 7 is a field. It results that every finite set Zm = {0, 1, 2, 3, --------, m - 1} with modulo m addition or multiplication is a field if and only if, m is a prime number. As these modulo of prime numbers forms a field the kind of field is called Galois field modulo m or GF(m).

As we see by representing graphs, we are concerned only with GF (2) = Galois modulo 2, which consisting of only two numbers {0, 1} and the addition modulo 2 and multiplication modulo 2 operations. The two arithmetic tables are given below:

+	0	1
0	0	1
1	1	0

x	0	1
0	0	0
1	0	1

The above two table logic is same as computer logic “Exclusive OR” and AND gate logic.

Vectors and vector spaces:

The vector and vector space are considered in a two-dimensional Euclidean plane, a point can be represented by an ordered pair X = (α_1 , α_2). This is regarded as a point X = (α_1 , α_2) emanating from the origin O = (0, 0) in a vector space. Similarly, in 3D Euclidean space the point X = (α_1 , α_2, α_3) represents a vector in the plane. All points belong to the field of real numbers. Let us suppose we are working with GF (2), then every number in the triplet can be either 0 or 1 and number of possible vectors are 8. These are (0, 0, 0), (0, 0, 1), (0, 1, 0), (1, 0, 0), (0, 1, 1), (1, 0, 1), (1, 1, 0), (1, 1, 1).

This concept of representing vectors can be extended to representation of k- dimensional space by means of an ordered k-tuple. For example, a 5- tuple (0, 1, 1, 0, 0) represents a vector in a fifth dimensional space over the field GF (2).

The numbers in the field is also called Scalers in the field GF (2) and are 0 and 1. A vector space also satisfies some of the vector operations like vector addition, scalar multiplication etc.

Theorem: A k- dimensional vector space over the field F, is an object consisting of a Field F, A set W of K-tuples, A binary operation + and · such that. A vector P is called the scaler product of τ and X and it is given by

$$P = \tau \cdot X = (\tau \cdot \alpha_1, \tau \cdot \alpha_2, \tau \cdot \alpha_3 \ldots\ldots\ldots\ldots\ldots\ldots\ldots, \tau \cdot \alpha_k)$$

Also, the scaler multiplication satisfies the following laws:

i) $\tau_1 \cdot (\tau_2 \cdot X) = (\tau_1 \cdot \tau_2) \cdot X$ --------- Associative Law

ii) $\tau_1 \cdot (X + Y) = (\tau_1 \cdot X) + (\tau_1 \cdot Y)$ ----------Distributive Law

iii) $1 \cdot X = X = X \cdot 1$ ----------Identity Law

iv) $\tau_1 \cdot X = X \cdot \tau_1$ -------Commutative Law

Vector space associated with a graph:

A graph G with four vertices and five edges e_1, e_2, e_3, e_4, e_5. The subset of these five edges can be represented by a 5-tuple set X:

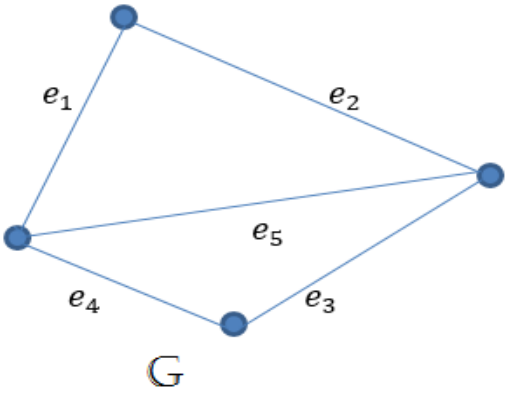
$$X = (\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$$

Such that $x_i = 1$ if e_i is in g

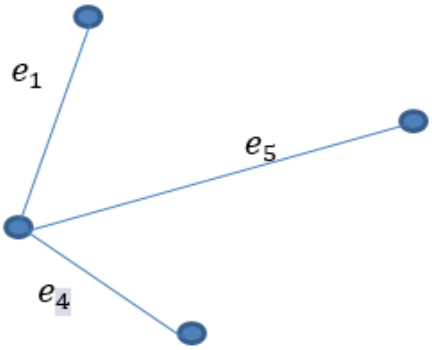
$x_i = 0$ if e_i is not in g

Illustration: The following graph g_1 will be represented by the tuple (1, 0, 0, 1, 1),

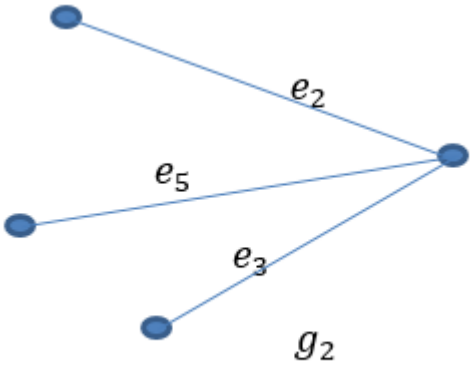
Similarly, g_2 by the tuple (0, 1, 1, 0, 1).



G



g1



Here Graph G has two sub-graphs g1 and g2.

The total numbers of subgraphs of graph G altogather will be equal to 2^5 or 32 such five tuple is possible. It includes a null graph (0, 0, 0, 0, 0) and a grpah itself (1, 1, 1, 1, 1) and other graphs are of the form (0, 0, 0, 0, 1) , (0, 0, 0, 1, 0) and so on.

The ring sum operation of two sub-graph corresponding to modulo 2 addition for g1 and g2 is

g1 = {e1, e4, e5} representing (1, 0, 0, 1, 1), and

g2 = {e2, e3, e5} representing (0, 1, 1, 0, 1).

The ring sum g1 $\oplus$ g2 = {e1, e1, e3, e4} representing (1, 1, 1, 1, 0), which is a modulo 2 addition of the 5-tuples of g1 and g2.

Basis vector of a graph

Linearly Dependence Vector Equations: A set of vectors X_1, X_2 , X_3, ……., X_r over a field F is said to be independent if for scalers a_1, a_2, a_3, ……, a_r in F satisfies the expression:

$$a_1X_1 + a_2X_2 + a_3X_3 + \ldots\ldots\ldots\ldots\ldots + a_rX_r = 0$$

holds only if $a_1 = a_2 = a_3 = \ldots\ldots\ldots\ldots\ldots = a_r = 0$.

Otherwise the set is said to be linearly Dependent. In that case coefficients are not null and hence, linear combination is not zero.

Illustration-1: $X_1 = \begin{pmatrix}1\\4\\0\end{pmatrix}$, $X_2 = \begin{pmatrix}0\\1\\2\end{pmatrix}$, $X_3 = \begin{pmatrix}3\\0\\0\end{pmatrix}$.

An arbitrary linear combination is zero then

$$a_1X_1 + a_2X_2 + a_3X_3 = \begin{pmatrix}a_1\\4a_1\\0\end{pmatrix} + \begin{pmatrix}0\\a_2\\2a_2\end{pmatrix} + \begin{pmatrix}3a_3\\0\\0\end{pmatrix} = \begin{pmatrix}0\\0\\0\end{pmatrix}$$

$$= \begin{pmatrix}a_1 + 3a_3\\4a_1 + a_2\\2a_2\end{pmatrix} = \begin{pmatrix}0\\0\\0\end{pmatrix}$$

$\Rightarrow$ $a_1 + 3a_3 = 0$

$4a_1 + a_2 = 0$

$2a_2 = 0$

$\Rightarrow$ $a_1 = a_2 = a_3 = 0$

Pertaining to the above result, I can conclude that the set of vectors { X_1, X_2 , X_3} are Linearly Independent.

Illustration-2: $X_4 = \begin{pmatrix}0\\2\\-2\end{pmatrix}$, $X_5 = \begin{pmatrix}1\\2\\0\end{pmatrix}$, $X_6 = \begin{pmatrix}0.5\\0\\1\end{pmatrix}$.

An arbitrary linear combination is zero then

$$a_4X_4 + a_5X_5 + a_6X_6 = \begin{pmatrix}0\\2a_4\\-2a_4\end{pmatrix} + \begin{pmatrix}a_5\\2a_5\\0\end{pmatrix} + \begin{pmatrix}0.5a_6\\0\\a_6\end{pmatrix} = \begin{pmatrix}0\\0\\0\end{pmatrix}$$

$$= \begin{pmatrix} a_5 + 0.5a_6 \\ 2a_4 + 2a_5 \\ -2a_4 + a_6 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

⇨ $a_5 + 0.5a_6 = 0$
$2a_4 + 2a_5 = 0$
$-2a_4 + a_6 = 0$

On solving we get $a_4 = -a_5 = 0.5a_6 \neq 0$ and it may be any real number other than zero. Hence, we conclude that the set of vectors $\{X_1, X_2, X_3\}$ are Linearly dependent.

Representation of linearly independent and dependent vector in graphical format for more generalisation of vector space.

Basis Vector:

Let V be a subspace of R^n for some n. A collection of vectors B = $\{X_1, X_2, X_3, \ldots\ldots\ldots\ldots\ldots\ldots X_n\}$ of vector V is called basis vector of B if linearly independent and spans V. If either one of these criteria is not satisfied, then collection is not basis for V. If a collection of vectors spans V, then it contains enough vectors so that every vector in V can be written as a linear combination of those in the collection.
[1]

To the set of linearly independent vectors $\{X_1, X_2, X_3\}$.

Let us consider another vector Y = $\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}$.

Now it can be seen that the new vector $\{X_1, X_2, X_3, Y\}$ is linearly dependent regardless of what is the vector Y. In other words

$$aX_1 + bX_2 + cX_3 + dY = 0.$$

The above vector X_1, X_2, X_3 can be expressed as the linear combination of vectors $\{X_1, X_2, X_3\}$ so as to the vectors are called basis vector in the vector space.

$$\text{Or, } Y = -\frac{a}{d}X_1 - \frac{b}{d}X_2 - \frac{c}{d}X_3$$

* This is uploaded on the website link:
[1] https://www.cliffsnotes.com/study-guides/algebra/linear-algebra/real-euclidean-vector-spaces/a-basis-for-a-vector-space
Downloaded on 2nd March, 2020.

Or $Y = \left(-\frac{a}{d}\right)X_1 + \left(-\frac{b}{d}\right)X_2 + \left(-\frac{c}{d}\right)X_3$ ----------(i)

Let us consider,

$$K_1 = -\frac{a}{d}$$

$$K_2 = -\frac{b}{d}$$

$$K_3 = -\frac{c}{d}$$

Then from equation (i):

$Y = K_1X_1 + K_2X_2 + K_3X_3$ ----------(ii)

Now, In case when the vector is dependent then the linear combination will be of the form:

$aX_1 + bX_2 + cX_3 + dY = d'$.

i.e. $dY = d' - aX_1 - bX_2 - cX_3$

or, $Y = \left(\frac{d'}{d}\right) - \left(\frac{a}{d}\right)X_1 - \left(\frac{b}{d}\right)X_2 - \left(\frac{c}{d}\right)X_3$

$Y = D + K_1X_1 + K_2X_2 + K_3X_3$ ----------(iii)

It shows that if the vector is dependent then the linear combination of the dependent and independent vector space consists of a constant term.

If every vector in a vector space can be expressed as a linear combination of a given set of vectors, this set is said to span the vector space W. The minimal number of linearly independent vectors is the dimension of the vector space.

References:

1. Chen, W. K., "On vector spaces associated with a Graph," SIAM J. Applied Mathematics, vol. 20, No. 3 May 1971, 526 – 529.
2. Deo, Narsingh. *Graph theory with applications to engineering and computer science*. Courier Dover Publications, 2017.
3. Goldman, J., G. C. Rota, "The number of Subspaces of a Vector space," Academia press, Inc., New York, 1969.
4. Goncharov, A.B., 2001. Multiple ζ-values, Galois groups, and geometry of modular varieties. In *European Congress of Mathematics* (pp. 361-392). Birkhäuser, Basel.
5. Halmos, P. R., "Finite Dimensional Vector Spaces," Van Nostrand Reinhold Company, New York, 1958.
6. Miller, K. S., Elements of Modern Abstract Algebra, Harper & Row, Inc., New York, 1958.
7. Ocneanu, Adrian. "Quantized groups, string algebras and Galois theory for algebras." *Operator algebras and applications* 2 (1988): 119-172.
8. Ringel CM. Report on the Brauer-Thrall conjectures: Rojter's theorem and the theorem of Nazarova and Rojter (on algorithms for solving vectorspace problems. I). InRepresentation Theory I 1980 (pp. 104-136). Springer, Berlin, Heidelberg
9. Ringel, C.M., 1980. Report on the Brauer-Thrall conjectures: Rojter's theorem and the theorem of Nazarova and Rojter (on algorithms for solving vectorspace problems. I). In *Representation Theory I* (pp. 104-136). Springer, Berlin, Heidelberg.
10. Schweigert, Christoph, Jürgen Fuchs, and Ingo Runkel. "Categorification and correlation functions in conformal field theory." *Proceedings of the ICM*. European Mathematical Society Zürich, 2006.