Necklaces: Generalizations

V Ch Venkaiah

V Ch Venkaiah is presently with the School of Computer and Information Sciences, University of Hyderabad. Prior to that he served in several organizations including the IIIT Hyderabad, IIT Delhi, Motorola, Tata Elxsi, and Central Research Laboratory of BEL. His research interests include cryptography, discrete mathematics, computational mathematics, algorithms, etc.

A q-ary necklace of length n is an equivalence class of q-coloured strings of length n under rotation. In this article, we study various generalizations and derive analytical expressions to count the number of these generalized necklaces. Also discussed are the various relations among the generalized necklaces, circulant matrices, and twistulant matrices.

1. Introduction

Consider the set of strings of length 4 consisting of the symbols a and b. That is, consider the set

$$S = \{aaaa, aaab, aaba, aabb, abaa, abab, abba, abbb,$$

$$baaa, baab, baba, babb, bbaa, bbab, bbba, bbbb\}.$$

Define a relation among the elements of S by declaring two elements to be related if either they are the same or one is a cyclic shift of the other. This can be easily verified to be an equivalence relation and hence partitions the set into equivalence classes. The resulting equivalence classes in our example are :

$$E_1 = \{aaaa\},\ E_2 = \{bbbb\},\ E_3 = \{aaab, baaa, abaa, aaba\},$$

$$E_4 = \{aabb, baab, bbaa, abba\},\ E_5 = \{abab, baba\},$$

$$E_6 = \{abbb, babb, bbab, bbba\}.$$

Each of these equivalence classes is called a *necklace* or, more precisely, a 2-ary necklace. In general, a q-ary necklace of length n is an equivalence class of q-ary strings of length n under rotation. So, a necklace is an equivalence class of a word under cyclic shift.

Keywords
q-ray necklaces, circulant matrices, linear codes, finite fields, twistulant.

An unlabelled necklace is an equivalence class of words under cyclic shift and permutation of alphabet of symbols. So, in our example, the unlabelled necklaces are $E_1^u = \{aaaa, bbbb\}$, $E_2^u = \{aaab, baaa, abaa, aaba, bbba, abbb, babb, bbab\}$, $E_3^u = \{aabb, baab, bbaa, abba\}$, $E_4^u = \{abab, baba\}$. These are the 2-ary unlabelled necklaces of length 4. A q-ary unlabelled necklace of length n is an equivalence class of q-ary strings under rotation and a permutation of the alphabet of symbols.

The necklaces studied here are combinatorial objects with applications to chemoinformatics, graph theory, and other fields.

In practice, a necklace (unlabelled or otherwise) is a representative of its equivalence class. It is lexicographically, the smallest element of its equivalence class. The necklaces studied here are combinatorial objects with applications to chemoinformatics, graph theory, and other fields.

The study of necklaces is facilitated by introducing finite fields. A *finite field* is a non-empty finite set equipped with two binary operations usually called addition and multiplication. The set is an abelian group with respect to addition and the non-zero elements of the set is also an abelian group with respect to multiplication. Also, the multiplication distributes over the addition. Note that the set of all real numbers as well as the set of all rational numbers are fields. But they are infinite fields. As an example of a finite field, consider the set of all non-negative integers less than 5 with addition modulo 5 and multiplication modulo 5 as the corresponding addition and multiplication operations, respectively. It may be noted, in this example, that 2 and 3 are the multiplicative inverses of each other and the remaining two non-zero elements, namely 1 and 4, have self inverses. Exactly similarly, for any prime number p, there is a field with p elements. In general, the number q of elements of a finite field, $\mathbb{F}_q$ is either a prime or a power of a prime.

Note that if, in the foregoing example, 0 and 1 replace the letters a and b then the 2-ary necklaces of length 4 over a binary field, $\mathbb{F}_2$, are obtained. In general, *q-ary necklaces of length n over a finite field* $\mathbb{F}_q$ are the equivalence classes of q-ary strings (vectors) of length n over $\mathbb{F}_q$ under a cyclic shift.

The necklaces we study are also related to linear codes over finite fields.

The necklaces we study are also related to linear codes over finite fields. A linear block code over a field F_q is a linear subspace of F_q^n, where n is the block length of the code. In other words, a block code of length n with q^k codewords is called a linear $[n, k]$ code if and only if its q^k codewords form a k-dimensional subspace of the vector space of all n-tuples over the field F_q. So, an $[n, k]$ block code can be specified by a $k \times n$ matrix, known as a generator matrix of the code.

An important subclass of linear block codes is the class of linear cyclic codes. In a cyclic code, a cyclic shift of a codeword is again a codeword. Associated with a linear $[n, k]$ cyclic code is the generator polynomial of degree $n - k$. Among several generator matrices of a linear $[n, k]$ cyclic code, the simplest is the one in which the rows are the codewords corresponding to the generator polynomial and its first $k - 1$ cyclic shifts.

A quasi-cyclic (QC) code of index p is a code in which a cyclic shift of a codeword by p positions is another codeword. A cyclic code is a QC code with $p = 1$.

Let $\mathbb{F}_q$ be a finite field. Consider a vector

$$\mathbf{a} = (a_0, a_1, \cdots a_{n-1})$$

of length n, where $a_i \in \mathbb{F}_q, 0 \leq i \leq n - 1$. Now define a matrix A to be the one whose first row is the vector $\mathbf{a}$, second row is the right cyclic shift of the first row, third row is the right cyclic shift of the second row and so on. In general, the i^{th} row of the matrix is the right cyclic shift of the $(i - 1)^{th}$ row, for $2 \leq i \leq n$. That is,

$$A = \begin{bmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 & \cdots & a_{n-3} \\ \vdots & \vdots & \vdots & & \vdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{bmatrix}.$$

A matrix of this form is called a circulant matrix of order n over $\mathbb{F}_q$.

The study of circulants has a very long history in the theory of matrices and determinants. Orthogonal circulant matrices over finite fields are of interest in coding theory. Linear binary codes whose generating vectors are partitioned in the form (I, A), where I and A are identity and circulant matrices respectively of order n, are of particular interest. This is because of the fact that several of the known best codes can be put into this form and it seems possible that there are good codes for larger values of n. Also they have connections with other abstract constructs such as polynomial ideals over a finite field, linear difference equations, and generalized Hadamard matrices.

Orthogonal circulant matrices over finite fields are of interest in coding theory. This is because of the fact that several of the known best codes can be put into this form and it seems possible that there are good codes for larger values of *n.* Also they have conections with other abstract constructs such as polymonial ideals over a finite field, linear difference equations, and generalized Hadamard matrices.

Define a mapping from the set of all circulant matrices over $\mathbb{F}_q$ to q-ary strings of length n in such a way that a circulant matrix gets mapped to its first row. This mapping can be quickly verified to be a bijection. So, the relation on words that was defined earlier induces a relation on the set of all circulant matrices. As per this relation, two circulant matrices are equivalent if the first row of one of the circulants is a circular shift of the first row of the other circulant.

The number of q-ary necklaces of length n is given by the following McMahon (or the M le colonel C Moreau) formula

$$N_q(n) = \frac{1}{n} \sum_{d|n} \varphi(n/d) q^d \,,$$

where φ is the Euler's totient function.

A q-ary Lyndon word of length n is an n-character string over an alphabet of size q, and which is the minimum element in the lexicographical ordering of all its rotations. In other words, it is a form of a q-ary necklace. Being the smallest, a Lyndon word differs from any of its non-trivial rotations, and is therefore aperiodic. Lyndon words have applications to free Lie algebras. The number of Lyndon words of length n over a finite field is equal to the number of irreducible polynomials of degree n over that field. Various other forms of necklaces exist in the literature. On concatenating all the Lyndon words with length dividing a given number, we get a de Bruijn sequence. In the study of necklaces, several interesting variants arise such as the unlabelled necklaces, Lyndon words, primitive necklaces, deBruijn sequence, necklaces with fixed density, necklaces with a certain sequence string forbidden, and bracelets, etc.

Lyndon words have applications to free Lie algebras. The number of Lyndon words of length *n* over a finite field is equal to the number of irreducible polynomials of degree *n* over that field.

This article discusses the various generalizations and the corresponding analytical expressions to count their numbers. Also discussed are the various relations among the necklaces, generalized necklaces, circulant matrices, and twistulant matrices. Further, the article briefly touches upon some applications of these objects.

2. Generalizations

This section discusses various generalizations of the necklaces, illustrates each with some examples, and some of their applications.

2.1 *First Category of Generalized Necklaces*

Influenced by its relevance in the construction of quasi-cyclic codes, we defined a first category of generalized q-ary necklace of length n as an equivalence class of q-ary strings (vectors) of length n under cyclic rotation and multiplication by a non-zero constant.

Example 1. Let $q = 5$ and $n = 2$. Then the set of 5-ary strings of length 2 is $\{(i, j) : 0 \leq i, j \leq 4\}$.

The above-mentioned relation gives rise to the following five equivalence classes:

$$\begin{aligned} E_1 &= \{[0\ 1], [1\ 0], [0\ 2], [2\ 0], [0\ 4], [4\ 0], [0\ 3], [3\ 0]\}, \\ E_2 &= \{[1\,1], [2\,2], [3\,3], [4\,4]\}, \\ E_3 &= \{[1\,2], [2\,1], [2\,4], [4\,2], [3\,1], [1\,3], [3\,4], [4\,3]\}, \\ E_4 &= \{[1\,4], [4\,1], [2\,3], [3\,2]\}, \\ \text{and } E_5 &= \{[0\,0]\}. \end{aligned}$$

Note that in E_1, the elements $[0\,2]$,$[0\,3]$,$[0\,4]$ are constant multiples of the element $[0\,1]$ and the elements $[1\,0]$, $[2\,0]$, $[3\,0]$, $[4\,0]$ are the cyclic shifts of $[0\,1]$, $[0\,2]$, $[0\,3]$, and $[0\,4]$ respectively. Similarly, the other equivalence classes are obtained.

Representatives of each of these equivalence classes will be the first category of generalized necklaces.

Note: Arithmetic of each component of a vector is performed modulo q. So in Example 1, the vector $[2\,3]$ is twice the vector $[1\,4]$.

Example 2. Let $q = 11$ and $n = 2$. That is, the set consists of all $11-$ary strings of length 2, which is the set $\{(i, j) : 0 \leq i, j \leq 10\}$.

The above relation gives rise to the following eight equivalence classes:

$$\begin{aligned} E_1 = &\ \{[0\,1], [1\,0], [0\,2], [2\,0], [0\,3], [3\,0], [0\,4], [4\,0], \\ &[0\,5], [5\,0], [0\,6], [6\,0], [0\,7], [7\,0], [0\,8], [8\,0], [0\,9], [9\,0], \\ &[0\,10], [10\,0]\}, \\ E_2 = &\ \{[1\,1], [2\,2], [3\,3], [4\,4], [5\,5], [6\,6], [7\,7], \\ &[8\,8], [9\,9], [10\,10]\}, \end{aligned}$$

$$\begin{aligned}
E_3 &= \{[1\,2],[2\,1],[2\,4],[3\,6],[4\,8],[5\,10],\\
&\quad [6\,1],[7\,3],[8\,5],[9\,7],\\
&\quad [10\,9],[4\,2],[6\,3],[8\,4],[10\,5],[1\,6],[3\,7],\\
&\quad [5\,8],[7\,9],[9\,10]\},\\
E_4 &= \{[1\,3],[3\,1],[2\,6],[3\,9],[4\,1],[5\,4],[6\,7],[7\,10],\\
&\quad [8\,2],[9\,5],[10\,8],[6\,2],[9\,3],[1\,4],[4\,5],[7\,6],[10\,7],\\
&\quad [2\,8],[5\,9],[8\,10]\},\\
E_5 &= \{[1\,5],[5\,1],[2\,10],[3\,4],[4\,9],[5\,3],[6\,8],[7\,2],\\
&\quad [8\,7],[9\,1],[10\,6],[10\,2],[4\,3],[9\,4],[3\,5],[8\,6],[2\,7],\\
&\quad [7\,8],[1\,9],[6\,10]\},\\
E_6 &= \{[1\,7],[7\,1],[2\,3],[3\,10],[4\,6],[5\,2],[6\,9],[7\,5],\\
&\quad [8\,1],[9\,8],[10\,4],[3\,2],[10\,3],[6\,4],[2\,5],[9\,6],[5\,7],\\
&\quad [1\,8],[8\,9],[4\,10]\},\\
E_7 &= \{[1\,10],[10\,1],[2\,9],[3\,8],[4\,7],[5\,6],[6\,5],\\
&\quad [7\,4],[8\,3],[9\,2]\},\\
E_8 &= \{0\}.
\end{aligned}$$

As in the previous example, representatives of each of these equivalence classes will be the first category of generalized necklaces.

Multiplication by a non-zero element does not change the weight of a codeword. So the construction of quasi-cyclic codes makes use of these generalized necklaces. The number of these generalized q-ary necklaces of length n can be computed empirically. An expression for an approximation to their number is given in [4, 6]. Only recently, the following analytical expression for the exact number of these generalized necklaces was obtained by the author and T Aaron Gulliver [8]

$$b(n,q) = \frac{1}{(q-1)n}\sum_{d|n}\varphi(d)\gcd(d,q-1)(q^{n/d}-1)+1,$$

where φ is the Euler's totient function and gcd denotes the greatest common divisor function.

Example 3. In Example 2, $q = 11$, $n = 2$. So,

$$b(2,11) \;=\; \frac{1}{20}\sum_{d|2}\varphi(d)\gcd(d,10)(11^{2/d}-1)+1 = 8.$$

2.2 *Second Category of Generalized Necklaces*

An $n \times n$ twistulant matrix (also known as a constacyclic matrix) over $\mathbb{F}_q$ is a matrix of the form

$$B = \begin{bmatrix} b_0 & b_1 & b_2 & \cdots & b_{n-1} \\ \lambda b_{n-1} & b_0 & b_1 & \cdots & b_{n-2} \\ \lambda b_{n-2} & \lambda b_{n-1} & b_0 & \cdots & b_{n-3} \\ \vdots & \vdots & \vdots & & \vdots \\ \lambda b_1 & \lambda b_2 & \lambda b_3 & \cdots & b_0 \end{bmatrix}.$$

where λ is a non-zero element and $b_i, 0 \le i \le n-1$, are elements of $\mathbb{F}_q$. When $\lambda = -1$, a twistulant matrix is known as a negacirculant matrix. Twistulant (negacirculant) matrices are the basic components in the generator matrix for a quasi-twisted (QT) (negacirculant (NC)) code.

A constacyclic shift of $(x_1, x_2, \cdots, x_n)$ is a vector

$$(\lambda x_n, x_1, x_2, \cdots, x_{n-1}),$$

where λ is some non-zero element of the field $\mathbb{F}_q$.

A quasi-twisted code of index p is a code in which a constacyclic shift of a codeword by p places is another codeword. Note that a quasi-twisted code generalize the class of constacyclic codes ($p = 1$), quasi-cyclic codes ($\lambda = 1$) and the class of cyclic codes ($\lambda = 1$, $p = 1$)

The constacyclic codes are a generalization of cyclic codes and have practical applications as they can be encoded with shift registers.

The constacyclic codes are a generalization of cyclic codes and have practical applications as they can be encoded with shift registers.

Consider the set of vectors of length n over $\mathbb{F}_q$ and their constacyclic shifts with a non-zero constant λ. Now define a relation among these vectors by declaring that two vectors are related if they are the same or one is a constacyclic shift with constant λ of the other. This relation can be easily verified to be an equivalence relation and hence partitions the set. So, we define each such equivalence class as a second category of generalized q-ary necklace of length n over $\mathbb{F}_q$.

Example 4. In this example we consider the set of 2$-$vectors over $\mathbb{F}_5$ and their constacyclic shifts with constant 2. That is $q = 5$, $n = 2$, and $\lambda = 2$. But this turns out to be the set of all vectors of length 2 over $\mathbb{F}_5$, which is given in Example 1. The relation that two vectors are related if one is the same or it is a constacyclic shift with constant $\lambda = 2$ gives rise to the following four equivalence classes of the set considered above:

$$E_1 = \{[0\,1], [1\,0], [0\,2], [2\,0], [0\,4], [4\,0], [0\,3], [3\,0]\},$$

$$E_2 = \{[1\,1], [1\,2], [2\,2], [2\,4], [4\,4], [4\,3], [3\,3], [3\,1]\},$$

$$E_3 = \{[1\,3], [3\,2], [2\,1], [1\,4], [4\,2], [2\,3], [3\,4], [4\,1]\}, \text{and}$$

$$E_4 = \{0\}.$$

Representatives of each of these equivalence classes will then be the second category of generalized necklaces.

Example 5. Let $q = 11$, $n = 2$, and $\lambda = 3$. That is, the set consists of vectors of length 2 and their constacyclic shifts with constant 3 over the field $\mathbb{F}_{11}$. But this again turns out to be list of vectors specified in Example 2. The relation gives rise to the following fourteen equivalence classes:

$$\begin{aligned} E_1 \;&=\; \{[0\,1], [1\,0], [0\,3], [3\,0], [0\;9], [9\,0], [0\,5], [5\,0], [0\,4], \\ &\quad [4\,0]\}, \end{aligned}$$

$$
\begin{aligned}
E_2 &= \{[0\,2],[2\,0],[0\,6],[6\,0],[0\,7],[7\,0],[0\,10],[10\,0],[0\,8],\\
&\quad [8\,0],\},\\
E_3 &= \{[1\,1],[1\,3],[3\,3],[3\,9],[9\,9],[9\,5],[5\,5],[5\,4],\\
&\quad [4\,4],[4\,1],\},\\
E_4 &= \{[1\,2],[2\,3],[3\,6],[6\,9],[9\,7],[7\,5],[5\,10],[10\,4],\\
&\quad [4\,8],[8\,1]\},\\
E_5 &= \{[1\,4],[4\,3],[3\,1],[1\,9],[9\,3],[3\,5],[5\,9],[9\,4],\\
&\quad [4\,5],[5\,1]\},\\
E_6 &= \{[1\,5],[5\,3],[3\,4],[4\,9],[9\,1]\},\\
E_7 &= \{[1\,6],[6\,3],[3\,7],[7\,9],[9\,10],[10\,5],[5\,8],[8\,4],\\
&\quad [4\,2],[2\,1]\},\\
E_8 &= \{[1\,7],[7\,3],[3\,10],[10\,9],[9\,8],[8\,5],[5\,2],[2\,4],\\
&\quad [4\,6],[6\,1]\},\\
E_9 &= \{[1\,8],[8\,3],[3\,2],[2\,9],[9\,6],[6\,5],[5\,7],[7\,4],[4\,10],\\
&\quad [10\,1]\},\\
E_{10} &= \{[1\,10],[10\,3],[3\,8],[8\,9],[9\,2],[2\,5],[5\,6],[6\,4],\\
&\quad [4\,7],[7\,1]\},\\
E_{11} &= \{[2\,2],[2\,6],[6\,6],[6\,7],[7\,7],[7\,10],[10\,10],[10\,8],\\
&\quad [8\,8],[8\,2]\},\\
E_{12} &= \{[2\,7],[7\,6],[6\,10],[10\,7],[7\,8],[8\,10],[10\,2],[2\,8],\\
&\quad [8\,6],[6\,2]\},\\
E_{13} &= \{[2\,10],[10\,6],[6\,8],[8\,7],[7\,2]\},\\
E_{14} &= \{0\}.
\end{aligned}
$$

Representatives of each of these equivalence classes will then be the second category of generalized necklaces.

Define a map from the set of all twistulant matrices with λ as the non-zero constant and the set of all q-ary vectors of length n and their constacyclic shifts with constant λ by sending a twistulant matrix to its first row. Clearly this is a bijection. So the relation defined above on the set of q-ary vectors of length n and their constacyclic shifts with constant λ induces a relation on the set of all twistulant matrices with constant λ. According to this relation two twistulant matrices are equivalent if the first row of one of the twistulant matrix is either same or is a constacyclic shift of the first row of the other.

The number of second category of generalized q-ary necklaces of length n can be computed empirically. An attempt was made to arrive at an analytic expression for a special (ternary) case of this category of generalized necklaces. In [9], the author obtained the following analytical expression for the number of second category of generalized necklaces over $\mathbb{F}_q$ with λ as the constant in the constacyclic shift operation:

$$d(n,q) = \frac{1}{\mathrm{ord}(\lambda)n} \sum_{\substack{i=1 \\ \lambda^{\frac{i}{\gcd(n,i)}}=1}}^{\mathrm{ord}(\lambda)n} (q^{\gcd(n,i)} - 1) + 1 \qquad (1)$$

Example 6. In Example 5, $q = 11$, $n = 2$, and $\lambda = 3$. Since 5 is the least integer so that, $\lambda^5 = 3^5 = 1$, we have $\mathrm{Ord}(\lambda) = \mathrm{Ord}(3) = 5$. Then

$$d(2,11) = \frac{1}{10} \sum_{\substack{i=1 \\ 3^{\frac{i}{\gcd(2,i)}}=1}}^{10} (11^{\gcd(2,i)} - 1) + 1 = 14.$$

2.3 *Third Category of Generalized Necklaces*

The set of vectors considered here is the same as that considered for the second category of generalized necklaces. In this case, two elements are related if one is the same or it is a constant multiple or it is a consta cyclic shift with constant λ or it is a constant multiple of a consta cyclic shift with constant λ of the other.

Example 7. Let q, n, and λ be as in the Example 5, so that the set of vectors is as in that example. This relation gives rise to eight equivalence classes which we leave for the reader to write down. Representatives of these equivalence classes comprise the third category of generalized necklaces.

Similar to the way the first category of generalized necklaces are used in the construction of quasicyclic codes, necklaces of the third category are used in the construction of quasi-twisted codes. Empirical methods were being employed in counting the number of the third category of generalized necklaces. An attempt was made in [5] to arrive at an expression for the special ternary case of the third category of generalized necklaces. The following analytical expression for the exact number of the general case of the third category of generalized necklaces was obtained in [10].

Similar to the way the first category of generalized necklaces are used in the construction of quasicyclic codes, necklaces of the third category are used in the construction of quasi-twisted codes.

$$e(n,q) = \frac{1}{(q-1)\mathrm{ord}(\lambda)n} \sum_{i} (q^{\gcd(n,i)} - 1) + 1 \qquad (2)$$

where the summation is over i which are between 1 and $\mathrm{ord}(\lambda)n$ and satisfy $t^{\frac{n}{\gcd(n,i)}} \lambda^{\frac{i}{\gcd(n,i)}} = 1$.

Example 8 In Example 5, $q = 11$, $n = 2$, and $\lambda = 3$. Since 5 is the least integer so that, $\lambda^5 = 3^5 = 1$, we have $\mathrm{ord}(\lambda) = \mathrm{ord}(3) = 5$. Then one can compute and obtain

$$e(2, 11) = 8.$$

3. Relation to Polynomial Rings

Let $\mathbb{F}_q$ be a field and let $R_n = \mathbb{F}_q[x]/(x^n - 1)$ be an algebra of polynomials modulo $(x^n - 1)$ over $\mathbb{F}_q$. In other words, its elements are the remainders of polynomials when divided by $x^n - 1$; thus, the elements can be identified with all polynomials of degree $< n$. Define a map from R_n to the set of vectors of length n over $\mathbb{F}_q$ by sending an element of R_n gets mapped to its coefficient vector. It is easy to see that this is a natural bijection. So the relation defined among these vectors in the context of necklaces induces a relation among the elements of

The algebra of polynomials in the ring R_n is isomorphic to the algebra of circulants over $\mathbb{F}_q$.

R_n. As per this relation two elements $r_1(x)$ and $r_2(x)$ of R_n are related if and only if $r_1(x) = x^\ell r_2(x) \bmod (x^n-1)$ for some integer ℓ. As mentioned earlier, this is an equivalence relation and partitions the set R_n into equivalence classes. The set of these equivalence classes is in one-to-one correspondence with the set of necklaces of length n over $\mathbb{F}_q$. Similarly, the relation defined among the vectors of length n over $\mathbb{F}_q$ in the context of first category of generalized necklaces induces a relation among the elements of R_n. As per this relation two elements $r_1(x)$ and $r_2(x)$ of R_n are related to each other if, and only if,

$$r_1(x) = \gamma x^\ell r_2(x) \bmod (x^n - 1)$$

for some integer ℓ and $\gamma \in \mathbb{F}_q \setminus \{0\}$. Again, as in the case of the first category of generalized necklaces, this is an equivalence relation and partitions the set R_n into equivalence classes. These equivalence classes are in one-to-one correspondence with the first category of generalized necklaces of length n over $\mathbb{F}_q$. Also, since there is a bijection between the set of all circulants over $\mathbb{F}_q$ and the set of vectors of length n over $\mathbb{F}_q$, it follows that there is a bijection between the elements of R_n and the set of all circulants over $\mathbb{F}_q$. In fact, the algebra of polynomials in the ring R_n is isomorphic to the algebra of circulants over $\mathbb{F}_q$.

There is an isomorphism between the algebra of polynomials in the ring S_n and the algebra of twistulant matrices of order n over $\mathbb{F}_q$.

Let $S_n = \mathbb{F}_q[x]/(x^n - \lambda)$, $\lambda \in \mathbb{F}_q \setminus \{0\}$. Similar to the ring of R_n, there is a one-to-one correspondence between the elements of S_n and the set of all vectors of length n over $\mathbb{F}_q$ and between the elements of S_n and the set of all twistulant matrices of order n over $\mathbb{F}_q$ with constant of cyclic shift as λ. In fact, there is an isomorphism between the algebra of polynomials in the ring S_n and the algebra of twistulant matrices of order n over $\mathbb{F}_q$. Here also, the relation defined in the context of second category of generalized necklaces induces a relation on the elements of S_n. As per this relation two elements, namely $s_1(x)$ and $s_2(x)$, of S_n are related if and only if $s_1(x) = x^\ell s_2(x) \bmod (x^n - \lambda)$ for some integer ℓ. Similarly the relation in the context of the third category of generalized necklaces induces a relation among the elements of S_n in such a way that two elements $s_1(x)$ and $s_2(x)$ of S_n are related if and only if $s_1(x) = \gamma x^\ell s_2(x) \bmod (x^n - \lambda)$ for some integer ℓ and $\gamma \in \mathbb{F}_q \setminus \{0\}$.

To summarize, we have defined and studied certain generalized necklaces. Apart from other applications, these generalized necklaces are used in the construction of quasi-cyclic and quasi-twisted codes. There are no analytical expressions for the number of each of these generalized necklaces. So, they are counted empirically. An expression for an approximate number of the first category of generalized necklaces is given in [4, 6]. An attempt was made in [5] to arrive at an expression for the special, ternary case of the third category of generalized necklaces. The exact numbers of the categories of generalized necklaces were given above as equations 1,2 and 3. Examples that illustrate the use of these equations are also worked out here.

Acknowledgments

The author would like to acknowledge the suggestions received from an anonymous referee, to improve the readability of the article. This article is dedicated to my wife Anuradha, who has been with me throughout.

Address for Correspondence
V Ch Venkaiah
School of Computer and
Information Sciences
University of Hyderabad
Gachibowli
Hyderabad 500 046, India.
Email:venkaiah@hotmail.com

Suggested Reading

[1] K A Byrd and T P Vaughan, Counting and constructing orthogonal circulants, *Journal of Combinatorial Theory*, Series A, Vol.24, pp.34–49, 1978.

[2] Eric Z Chen, An explicit construction of 2-generator quasi-twisted codes, *IEEE Trans. on Inform.Theory*, Vol.54, pp.5770–5773, 2008.

[3] P P Greenough and R Hill, Optimal ternary quasi-cyclic codes, *Designs, Codes and Crypt*., Vol.2, pp.81–91, 1992.

[4] T A Gulliver and V K Bhargava, Some best rate 1/p and rate (p-1)/p systematic quasi-cyclic codes over GF(3) and GF(4), *IEEE Trans. Inform. Theory*, Vol.38, pp.1369–1374, 1992.

[5] T A Gulliver, New optimal ternary linear codes, *IEEE Trans. Inform. Theory*, Vol.41, pp.1182–1185, 1995.

[6] T A Gulliver and V K Bhargava, New good rate (m-1)/pm ternary and quaternary quasi-cyclic codes, *Designs, Codes and Crypt*, Vol.7, pp.223–233, 1996.

[7] F J Macwilliams, Orthogonal circulant matrices over finite fields, and how to find them, *Journal of Combinatorial Theory*, Vol.10, pp.1–17, 1971.

[8] V Ch Venkaiah and T A Gulliver, Quasi-cyclic codes over FF_{13} and enumeration of defining polynomials, *Journal of Discrete* Algorithms, Vol.16, pp.249–257, 2012.

[9] V Ch Venkaiah, *Generalized necklaces – twistulant matrices: A count*, under preparation.

[10] V Ch Venkaiah and T A Gulliver, Generalized necklaces -twistulant matrices: A count – Part II, under preparation.