ALGORITHM IN THE CONSTRUCTION OF THE DIFFERENCE SYSTEMS SETS

Editha Rivera Jorda
Technological University of the Philippines
Ayala Blvd., Ermita, Manila

Abstract. The paper aims to construct Difference System of Sets (DSS) through the algorithm of Tonchev’s theorem and developed a computer program in C++ language to facilitate constructing large prime number $n$ and exhausted all possible values of the number of sets ($q$) in DSS. The constructed DSS was obtained from the partitions of multiplicative group of $GF(n)^*$ for any prime number $n$ and difference set of quadratic residue for prime number $n \equiv 3(\text{mod} 4)$. The paper is descriptive in nature. It describes how to construct DSS through algorithm based on the proof of Tonchev’s theorem. DSS can be constructed by partitioning the multiplicative of group $GF(n)^*$ and the quadratic residue of $n \equiv 3(\text{mod} 4)$. The base blocks obtained from partitioning multiplicative of group $GF(n)^*$ and the quadratic residue of $n \equiv 3(\text{mod} 4)$ are collection of sets, and forms the perfect regular DSS with parameter $(n, m, q, \rho)$. Thus, DSS can be constructed from cyclic difference set based on the proof of Tonchev’s theorem and the partitions are collection of set and forms perfect regular DSS and the developed program can partition DSS from prime number $n$ from 3 to 3571. A construction of DSS for prime number $n \equiv 1(\text{mod} 4)$ through algorithm of another Tonchev’s theorem is recommended.

Key words: cyclic difference sets, difference system of sets, multiplicative group of $GF(n)^*$, quadratic residue
Introduction

The relationship of error-correcting codes to design theory was brought out by Mac Williams, Sloane, and Thompson (1973). With respect to practical problems in the communication of digitally encoded information, the subject of error-correcting codes also arises. Error–correcting codes were introduced to prove the theorem of Shannon (1948) that a virtually error-free communication could be observed over a noisy channel. The error-free communication is observable if the message to be communicated is converted first into codeword by adding “redundancy”. The codeword is sent through the channel where the received message is decoded to resemble the original message.

Tonchev (2005) used the process of transmitting data over a channel, as stream of symbols from a finite alphabet

$$\mathbb{F}_q = \{0, 1, \ldots, q-1\}$$

to a channel. The data stream contains consecutive messages. Each message is a sequence of \(n\) consecutive symbols

$$\ldots |0:10|10|10|10|0|1|1|1|1|1|0|1|0|0|0|\ldots$$

$$\ldots |x_1, \ldots, x_n|y_1, \ldots, y_n| \ldots$$

where \(x = x_1, \ldots, x_n\) and \(y = y_1, \ldots, y_n\) are two consecutive messages. These messages are decoded by the receiver in order to resemble the original message by synchronizing the codes. A synchronization problem occurs at the receiving end. That is, when a sequence of \(n\) symbols are expressed as a single message. Therefore, in order for the message decoded by the receiver to resembles, as closely as possible, the original message, the code should be synchronized. The synchronization problem that arises at the receiving end is the task of partitioning correctly the data stream into messages of length of \(n\), as opposed to expressing incorrectly a sequence of \(n\) symbols being linked together at the end of one message with the beginning of another message as a single message

$$\ldots |x_{n-1} \ldots x_n y_1 \ldots y_n| \ldots$$

to eliminate this problem, there is a need to partition the data stream correctly into message of length \(n\).

Crick and Orgel (1957) introduced comma-free codes, to solve the code synchronization problem and Crick and Orgel (1958), comma-free codes opened a new direction in coding theory, that is, investigation of combinatorial problems involving word synchronization for block codes.

But it was Levenshtein (1971) who showed that it is possible to combine error-correcting and word synchronization through the combinatorial problem on the Difference System of Sets (DSS).

Levenstein (1971) introduced DSS by using the parameter \((n, \{\tau_0, \tau_1, \ldots, \tau_{q-1}\}, \rho)\) defined as a collection of \(q\) disjoint sets \(Q \subseteq \{1, \ldots, n\}\), \(|Q| = \tau_i, 1 \leq i \leq q - 1, \) such that the multi-set of differences

$$\{a - b (mod n) | a \in Q_i, b \in Q_j, i \neq j\} \quad (1)$$

contains every number \(k, 1 \leq k \leq n - 1, \) at least \(\rho\) times. A DSS is perfect if every number \(i\) occurs exactly \(\rho\) times in the multi-set of difference and it is regular if all subsets \(Q_i\) are of the same size, that is, \(\tau_0 = \tau_1 = \cdots = \tau_{q-1} = m\). Hence, a perfect regular DSS on \(n\) points with \(q\) subsets of size \(m\) is denoted by \((n, m, q)\).

For the construction of codes with prescribed comma-free index that allow for the synchronization in the presence of errors, that is, the redundancy \((r)\) of a code counts the number of positions added for error detection and correction,

$$r = r_q(n, \rho) = \sum_{i=0}^{q-1} |Q_i| \quad (2)$$
where the value of \( r \) must be as small as possible. Levenshtein (1971) proved the
following bound on the minimum redundancy \( r_q(n, \rho) \) of a DSS with \( i \) parameters \( n, q, \rho \):
\[
r_q(n, \rho) \geq \sqrt{\frac{q \rho(n-1)}{q-1}}
\]  
(3)

In (2) and (3) the equality of the value of \( r \) occurs if and only if the DSS is perfect and
regular. Thus, degree of resemblance will depend on how good the code is with respect
to the channel. Wang (2006) improved the Levenstein bound considering difficulty in
achieving it in many cases.

Tonchev (2003) used a more general partition of cyclic difference sets. Furthermore,
various difference sets were obtained using cyclotomic classes by Tonchev and Mutoh
(2008) and cyclic balanced of weighing matrices by Jungnickel and Tonchev(2002). On
the other hand, Fuji-Hara, Munemasa and Tonchev (2006) obtained DSS from hyperplane
line spread and hyperplanes. Cummings (2006) provided a construction method for DSS
and conditions for a comma-free systematic code. While, Tonchev and Wang (2007)
developed an algorithms for constructing optimal DSS.

Tonchev (2005) surveyed the recent construction in DSS obtained as partitions of
cyclic difference sets. Such construction of the DSS obtained from the partitions of cyclic
difference sets for any prime numbers \( n \) are the multiplicative group \( GF(n)^* \) and partition
of difference sets of quadratic residue for \( n \equiv 3 (mod \ 4) \). It is time consuming to
construct DSS for a large prime number \( n \) and different number of sets \( (q) \) for every
partition. Hence, an algorithm for constructing DSS obtained from multiplicative group
\( GF(n)^* \) and quadratic residue facilitate the construction of perfect regular DSS.

The theory of combinatorial designs emphasizes its application in coding theory.
Combinatorial designs have been the subject of recent study, because of their numerous
applications in various branches of science such as: Statistical planning of experiments,
pattern recognition, construction of optimal error-correcting codes and the provision of
reliability in the transmission of digital information.

The connection between designs and codes leads to the construction of new designs
that can be used for decoding purposes. Codes are an efficient tool for the construction
and analysis of various combinatorial structures.

On the other hand, It is beneficial to students taking a course in Set Theory and
Discrete Mathematics wherein the concept of sets and partitions are the building block of
the course. Students will have a concrete idea of the concepts and its application in real
life. Computer science students can apply the concepts through the algorithms of the
theorems and develop computer program to facilitate partitioning large prime numbers \( n \).

**Statement of the problem**
There are several direct constructions of the difference systems of sets (DSS) obtained as
partitions of cyclic difference sets. The partitioning of cyclic difference sets in many cases
obtained a DSS that are perfect and regular. Hence, the paper sought

1. How to construct DSS using the algorithms based on Tonchev Theorems from the
    a. Multiplicative group \( GF(n)^* \) of a finite field of prime order \( n \); 
    b. Difference sets of Paley type (quadratic residue).
2. How to co construct DSS using program with given parameters \(n, m, q, \rho\) for any large prime number \(n\) and \(n \equiv 3 \mod(4)\) facilitate construction of DSS from multiplicative group \(GF(n)^*\) and difference sets of quadratic residues.

Methodology
The paper was descriptive in nature. The paper began by reviewing the preliminary concepts in Number Theory and Abstract algebra as building blocks in the algorithms of constructing DSS. Appropriate examples were presented to illustrate the definitions, lemma and theorems.

Two algorithms in constructing DSS from the Tonchev theorems were described and illustrated through examples.

A program in C++ was developed to facilitate the construction of 1 DSS for a large prime numbers \(n\) in partitioning the multiplicative group of finite field of prime number \(n\) and difference sets of quadratic residues for prime \(n \equiv 3 \mod(4)\). Moreover, the computer program was utilized to give examples in constructing the partitioning of perfect regular DSS.

Results and discussion
In this section, preliminary concepts were discussed such as the definitions of primitive root modulo, quadratic residues, cyclic difference set, simple construction of DSS obtained as partition of cyclic difference sets and the generalization of the simple construction of singletons into general partition of the cyclic difference set through lemma by Tonchev (2005). Two theorems that are the basis for the algorithm in constructing DSS from the partition of the Multiplicative Group \(GF(n)^*\) of a finite field of prime order \(n\) and difference sets of Paley type (quadratic residue) are enumerated and lastly, the output of the developed program and its tables were presented.

Preliminary concepts
The following concepts are used in the development of the construction of DSS.

Primitive root
Definition: Let \(n\) be a prime number and \(Z_n^*\) be the multiplicative group modulo \(n\), then \(\alpha \in Z_n^*\) is said to be a primitive root if \(n - 1\) is the smallest positive integer such that \(\alpha^{n-1} \equiv 1 \mod(n)\).

For \(n = 5\). Let \(Z_5^* = \{1,2,3,4\}\). Note that
\[2^1 \equiv 2 \mod(5); \quad 2^2 \equiv 4 \mod(5); \quad 2^3 \equiv 3 \mod(5); \quad 2^4 \equiv 1 \mod(5)\]
By definition, 2 is a primitive root modulo 5

Quadratic Residue
Definition: Let \(p\) be a prime and \(\alpha \in Z_p^*\). Then, is a quadratic residues modulo \(p\) if there exits \(x \in Z_p^*\) such that \(x^2 \equiv a \mod(p)\). Otherwise, it is called quadratic nonresidue modulo \(p\).

For \(n = 7\). Let \(Z_7^* = \{1,2,3,4,5,6\}\). Clearly by the above definition elements \(1,2,4\) are quadratic residue since
\[1^2 \equiv 1 \mod(7); \quad 2^2 \equiv 4 \mod(7); \quad 3^2 \equiv 2 \mod(7).\]
Cyclic difference sets and quadratic residue

Two mathematicians, Kirk (1857) who studied the difference set by considering the case where the difference of two elements in given set occurred only once and Paley(1933), used the quadratic residues in constructing difference sets.

Cyclic difference set

Definition: A \( (v, k, \lambda) \) difference set \( (mod \ v) \) or a cyclic \( (v, k, \lambda) \) difference set is a set

\[ D = \{d_1, \ldots, d_k\} \] of distinct elements of \( Z_v \) such that each nonzero \( d \in Z_v \) can be expressed in the form \( d = d_i - d_j, i \neq j \) in precisely \( \lambda \) ways.

For \( n = 11 \). Let \( D = \{1,3,4,5,9\} \) be a subset of \( Z_{11}^* \). Observe that differences of the elements of \( D \) occurs twice.

\[
\begin{align*}
1 &= 4 - 3 = 5 - 4 \\
2 &= 3 - 1 = 5 - 3 \\
3 &= 1 - 9 = 4 - 1 \\
4 &= 9 - 5 = 5 - 1 \\
5 &= 3 - 9 = 9 - 4 \\
6 &= 9 - 3 = 4 - 9 \\
7 &= 1 - 5 = 5 - 9 \\
8 &= 1 - 4 = 9 - 1 \\
9 &= 1 - 3 = 3 - 5 \\
10 &= 3 - 4 = 4 - 5
\end{align*}
\]

Thus, by definition \( D \) is \( (11,5,2) \) a cyclic difference set.

Quadratic Residue difference set

Theorem: Let \( q \equiv 3(mod \ 4) \). Then the nonzero squares in \( GF(n) \) form a \( (q, \frac{1}{2}(q - 1), \frac{1}{4}(q - 3)) \) difference sets.

For \( n = 31 \). Let \( q = 31 = 4(7) + 3 \) and let \( \alpha = 3 \) be the primitive element of \( GF(n) \) and the quadratic residue \( Q = \{9, 19, 16, 20, 25, 8, 10, 28, 4, 5, 14, 2, 18, 7, 1\} \). By the previous theorem, \( Q \) forms a \( (31, 15, 7) \) difference set, that is, \( q = 31, k = \frac{1}{2}(31 - 1) = 15, \lambda = \frac{1}{4}(31 - 3) = 7 \).

Algorithms in constructing DSS from Partition of the Multiplicative Group \( GF(n)^* \) of a finite field of prime order \( n \) difference sets of Paley type or quadratic residue

In this paper, lemma was applied to construct DSS from partition of the multiplicative group \( GF(n)^* \) of a finite field of prime of a finite field of order \( n \) defined by a subgroup of \( GF(n)^* \) and its cosets and partitioning the difference sets of Paley type, or equivalently, by partitioning the set of quadratic residues \( Q \) modulo a prime number \( n \equiv 3(mod \ 4) \).

Simple construction of DSS

The application of lemma is based from the simple construction of DSS from the partition of difference. The following definition described how to construct DSS from the collection of singletons.

Definition: Letting \( D = \{x_1, x_2, \ldots, x_k\} \) be a cyclic difference set, that is, a subset of \( k \) residues modulo \( v \) such that every positive residue modulo \( n \) occurs exactly \( \lambda \) times in the multi-set of differences

\[
M = \{x_i - x_j(mod \ n) | x_i, x_j \in D, x_i \neq x_j \} \quad (1)
\]

Then the collection of singletons \( Q_0 = \{x_1\}, \ldots, Q_{k-1} = \{x_k\} \) is a perfect regular DSS with parameters \( (n = v, m = 1, q = k, \rho = \lambda) \). Thus, DSS are a generalization of cyclic difference sets.
The following illustrated the simple construction of DSS. For every integer modulo $n$, $Z_n$ and a cyclic different set $D$ which is a subset of $Z_n$, the difference of every positive residue modulo $n$ in $D$ appears exactly $\lambda$ times. Hence, the collection of singletons $Q_0, Q_1, Q_2, \ldots, Q_{k-1}$ is a perfect regular DSS with parameters $(\nu, 1, k, \lambda)$.

For $n = 6$. Let $Z_6 = \{0, 1, 2, 3, 4, 5\}$ and $D = \{1, 2, 3, 4, 5\}$ a cyclic difference set which is the subset of $Z_6$. Obviously, the difference of every positive residue in $D$ appears exactly four times.

\[
\begin{align*}
1 - 2 &= 2 - 3 = 3 - 4 = 4 - 5 = 1 - 5 = 3 - 1 = 4 - 2 = 5 - 3 = 2 \\
1 - 3 &= 2 - 4 = 3 - 5 = 5 - 1 = 4 - 3 = 2 - 1 = 3 - 2 = 4 - 3 = 5 - 4 = 1 \\
1 - 4 &= 2 - 5 = 4 - 1 = 5 - 2 = 3
\end{align*}
\]

Thus from the lemma, the collection of singletons $Q_0 = \{5\}, Q_1 = \{4\}, Q_2 = \{3\}, Q_3 = \{2\}, Q_4 = \{1\}$ form a perfect regular DSS with parameters $(5, 1, 5, 4)$.

**Lemma in constructing DSS**

To generalize the definition of simple construction, Tonchev (2005) replaced the singletons with a more general partition of the given difference set through the following lemma.

Lemma: Let $D \subset \{1, 2, \ldots, n\}$, $|D| = k$, be a cyclic $(n, k, \lambda)$ difference set. Assume that $D$ is partitioned into $q$ disjoint subsets $Q_0, \ldots, Q_{q-1}$ that are the base blocks of a cyclic design $B$ with block sizes $\tau_i = |Q_i|, i = 0, \ldots, q-1$ such that every two points are contained in at most $\lambda_1$ blocks. Then the sets $Q_0, \ldots, Q_{q-1}$ form a DSS with parameters $(n, \tau_0, \ldots, \tau_{q-1}, \rho = \lambda - \lambda_1)$. The DSS $\{Q_i\}_{i=0}^{q-1}$ is perfect if and only if $B$ is a pairwise balanced design with every two points occurring together in exactly $\lambda_1$ blocks.

The following illustrates the lemma

For $n = 5$. Let $Z_5 = \{0, 1, 2, 3, 4\}, D = \{1, 2, 3, 4\}$ cyclic difference set which is a subset of $Z_5$ and let $B = \{Q_0, Q_1\}$ as the cyclic base block design with $Q_0 = \{1, 4\}, Q_1 = \{3, 2\}$.

First, show that $D$ is a cyclic difference set with $\lambda = (5 - 2) = 3$, since every positive residue modulo in $D$ appears exactly thrice.

\[
\begin{align*}
1 &= 2 - 1 = 3 - 4 = 4 - 3; \\
2 &= 3 - 1 = 1 - 4 = 4 - 2; \\
4 &= 1 - 2 = 2 - 3 = 3 - 4
\end{align*}
\]

Thus, $D$ is $(5, 4, 3)$ cyclic difference set.

Next, show that $Q_0 = \{1, 4\}, Q_1 = \{3, 2\}$ are the base blocks of a cyclic design with two points contained in exactly $\lambda_1$ block or equivalently, the differences contained in exactly $\lambda_1$ times. Obviously, the difference appears exactly once, that is $\lambda_1 = 1$ times.

\[
\begin{align*}
1 &= 3 - 2 = 2 - 1 = 4 - 3; \\
2 &= 1 - 4 = 3 - 4 = 4 - 2; \\
3 &= 1 - 3 = 4 - 1 = 2 - 4
\end{align*}
\]

Hence, $Q_0$ and $Q_1$ are the base blocks of a cyclic difference set.

Lastly, if we let $a \in Q_0, b \in Q_1$, then the number $a - b$ appears exactly $\rho = \lambda - \lambda_1 = 2$.

\[
\begin{align*}
1 &= 4 - 3 = 2 - 1; \\
2 &= 4 - 2 = 3 - 1
\end{align*}
\]

Therefore, by lemma, the sets $Q_0$ and $Q_1$ form a perfect regular $(5, 2, 2)$ DSS.
Multiplicative Group of $GF(n)^*$ and the set of quadratic residues $Q$ modulo for prime number $n \equiv 3 (mod\ 4)$

The following algorithms are the first applications of the lemma:

**Algorithm of the Multiplicative Group of $GF(n)^*$**

For the construction of DSS obtained from the partition of multiplicative group of $GF(n)^*$, Tonchev (2005) gave the following theorem which states that:

Theorem: Let $n = mq + 1$ for some $m, q \in \mathbb{Z}$ and let $\alpha$ be a primitive element of the finite field order $n$, $GF(n)$. The collections of sets:

- $Q_0 = \{\alpha^q, \alpha^{2q}, \ldots, \alpha^{mq} = 1\}$,
- $Q_1 = \alpha Q_0, \ldots, Q_{q-1} = \alpha^{q-1} Q_0$

is a perfect regular $(n, m, q, \rho)$DSS.

Based on the theorem above, the following steps are the algorithm in constructing DSS from the Multiplicative group of $GF(n)^*$ for any prime number $n$.

Let $n = mq + 1$ be any prime number and $q$ be any positive integer

Set $m = \frac{n-1}{q}$.

If $m$ is an integer or $n - 1$ is divisible by $q$,

Set $\alpha^{n-1} \equiv 1 \mod n$

Else

Let $q$ be any positive integer.

Calculate $m$ and check if $m$ is an integer

Set $Q_0 = \{\alpha^q, \alpha^{2q}, \ldots, \alpha^{mq} = 1\}$ and $j = 1$

Repeat

- $Q_j = \{\alpha^j Q_0\}$
- $j = j + 1$

Until

- $j = j + 1$

Set $\rho = (n - m - i)$

The collection $Q_0, Q_1, \ldots, Q_{q-1}$ is a perfect regular $(n, m, q, \rho)$DSS

Figure 1. Algorithm in constructing DSS for any prime number $n$

In figure 1, the steps described the algorithm in constructing DSS if the prime number $n$ can be rewritten as $n = mq + 1$. According to the lemma, if $GF(n)^*$ is a cyclic difference set, then cyclic base blocks difference can be constructed, and the theorem states that if $n = mq + 1$, then the collection of sets formed from the base blocks is a perfect regular DSS with parameter $(n, m, q, \rho)$.

The following illustrated the application of the algorithm.

For $n = 7$. Let $n = 7 = 3 \cdot 2 + 1$, $m = 3$ and $q = 2$. The primitive element of $\mathbb{Z}_7$ is, $\alpha = 3$. $D = \{1, 2, \ldots, 6\}$ is a cyclic $(7, 6, 5)$ difference set. The base blocks $B = \{Q_0, Q_1\}$ are the following:

- $Q_0 = \{3^2, 3^4, 3^6\} = \{2, 4, 1\}$
- $Q_1 = \{3^3, 3^4, 3^6\} = \{3, 3^3, 3^5\} = \{6, 5, 3\}$

Thus, $GF(n)^* = Q_0 \cup Q_1$ is a cyclic $(7, 3, 2)$ design. That is,

- $1 = 2 - 1 = 6 - 5$
- $2 = 4 - 2 = 5 - 3$
- $3 = 4 - 1 = 6 - 3$
- $4 = 1 - 4 = 3 - 6$
- $5 = 2 - 4 = 3 - 5$
- $6 = 1 - 2 = 5 - 6$
Hence, the collection of sets $Q_0$ and $Q_1$ with $\rho = 7 - 3 - 1 = 3$ form a perfect regular DSS with parameter $(7, 3, 2, 3)$.

For $n = 19$: Let $n = 19 = 3 \cdot 6 + 1$ with $m = 3, q = 6$. With $\alpha = 2$ as its primitive element. $D = \{1, 2, 3, \ldots, 16, 17, 18\}$ is a cyclic $(19, 18, 17)$ difference set. The base blocks are the following:

$Q_0 = \{2^6, 2^{12}, 2^{18}\} = \{7, 11, 1\}$
$Q_1 = 2\{2^6, 2^{12}, 2^{18}\} = \{14, 3, 2\}$
$Q_2 = 2^2\{2^6, 2^{12}, 2^{18}\} = \{9, 6, 4\}$
$Q_3 = 2^3\{2^6, 2^{12}, 2^{18}\} = \{18, 12, 8\}$
$Q_4 = 2^4\{2^6, 2^{12}, 2^{18}\} = \{17, 5, 16\}$
$Q_5 = 2^5\{2^6, 2^{12}, 2^{18}\} = \{15, 10, 13\}$

Hence, by lemma $GF(n)^*$ is a cyclic $2 - (19, 3, 2)$ design. Thus, the collection of sets $Q_0, Q_1, Q_2, Q_3, Q_4, Q_5$ form a perfect regular $(19, 3, 6, 15)$ DSS.

Algorithm for quadratic residue from prime number $n \equiv 3 (mod \ 4)$

For the construction of DSS obtained from the set of quadratic residue for prime number $n \equiv 3 (mod 4)$. Tonchev (2005) stated the following theorem,

Theorem: For every prime $n = 2mq + 1 \equiv 3 (mod \ 4)$ there exists a perfect regular DSS with parameters $(n, m, q, \rho = \frac{n-2m-1}{4}).$

Based on the theorem above, the following steps are the algorithm in constructing DSS from the set of quadratic residue for prime number $n \equiv 3 (mod \ 4)$.

Let $n = mq + 1$ be any prime number such that $n \equiv 3 (mod \ 4)$
Let $q$ be any positive integer
Set $m = \frac{n-1}{2q}$
If $m$ is an integer or $n - 1$ is divisible by $2q$,
Set $\alpha^{n-1} \equiv 1 \mod n$
Else
Let $q$ be any positive integer.
Calculate $m$ and check if $m$ is an integer
Set $Q_0 = \{\alpha^{2i} \mid 1 \leq i \leq \frac{n-1}{2}\}, D_m = \{\alpha^{2iq} \mid 1 \leq i \leq m\}$ and $j = 1$
Let $Q_0 = D_m$
Repeat
$Q_j = D_m\alpha^{2j}$
$j = j + 1$
Until
$j = q - 1$
Set $(n, m, q, \rho = \frac{n-2m-1}{4})$.
The collection $Q_0, Q_1, \ldots, Q_{q-1}$ is a perfect regular $(n, m, q, \rho)$ DSS

Figure 2. Algorithm in constructing DSS for prime number $n = 2mq + 1 \equiv 3 (mod \ 4)$

Based on figure 2, if any prime number $m$ can be rewritten as $n \equiv 3 (mod \ 4)$, then the set of quadratic residue is a cyclic difference set by the Paley (1933). The base blocks constructed by the algorithm are collection of sets that form a perfect regular DSS with parameter $(n, m, q, \rho)$.

The following illustrate the construction of DSS based on the algorithm.
For $n = 19$. Consider $n = 19 = 2 \cdot 3 \cdot 3 + 1, m = 3, q = 3$. Then $\alpha = 2$ is a primitive element $\mathbb{Z}_{19}$.

Set $Q = \{\alpha^{2i} | 1 \leq i \leq 9\} = \{2^2, 2^4, 2^6, 2^8, 2^{12}, 2^{14}, 2^{16}, 2^{18}\} = \{4, 16, 7, 9, 17, 11, 6, 5, 1\}$ By Paley(1933), $Q$ is cyclic $(19, 9, 4)$ difference set.

Let $D_m = \{\alpha^{2i} | 1 \leq i \leq m\} = D_3 = \{\alpha^{6j} | 1 \leq i \leq 3\}$. Then the following base blocks is a $2 - (19, 3, 1)$ design: $Q_0 = D_m = \{7, 11, 1\}, Q_1 = \{9, 6, 4\}, Q_2 = \{17, 5, 16\}$.

By Tonchev (2005), the collection of sets $Q_0, Q_1, Q_2$ forms a perfect regular $(19, 3, 3, 3)$ DSS.

For $n = 31$. Let $n = 31 = 2 \cdot 5 \cdot 3 + 1$. where $m = 5, q = 3$ and $\alpha = 3$ as a primitive element modulo $13$.

Set $Q = \{3^2, 3^4, 3^6, 3^8, 3^{10}, 3^{12}, 3^{14}, 3^{16}, 3^{18}, 3^{20}, 3^{22}, 3^{24}, 3^{26}, 3^{28}, 3^{30}\}$

$= \{9, 19, 16, 20, 25, 8, 10, 28, 4, 5, 14, 2, 18, 7, 1\}$. By Paley, $Q$ is a cyclic $(31, 15, 2)$ difference set.

Let $D_5 = \{\alpha^{6j} | 1 \leq i \leq 5\}$. Then the following base blocks form a $2 - (31, 5, 2)$ design:

$Q_0 = D_5 = \{16, 8, 4, 2, 1\}, Q_1 = \{20, 10, 5, 18, 9\}, Q_2 = \{25, 28, 14, 7, 19\}$.

By Tonchev (2005), the collection of sets $Q_0, Q_1, Q_2$ form a perfect regular $(31, 5, 3, 3)$ DSS.

The first application of lemma was used to construct a perfect regular DSS and the algorithms for constructing DSS were based on Tonchev (2005). The theorems stated that the collection of sets which are the base blocks of the cyclic difference form a DSS with parameter $(n, m, q, p)$ from the multiplicative group of $GF(n^*)$ and quadratic residue.

**Output of the Computer program**

The developed program used C++ and the minimum requirements to run C++ were the following: it must be at least Windows 98 operating system, the executable file (DSSv6.exe) may be run in DOS mode and the program (DSSv6.cpp) was developed using Bloodshed Dev C++. The concept of modular programming was utilized and there were five modules or procedure namely: accept(), testrange(), testprime(), primitive(), and findalpha() and findalpha2(). Figure 3 is the interface of the program.
Figure 3. The example screenshot of the interface of the developed program

Based on figure 3, any numbers can enter from 3 to 3571. If the input number is valid, two options are given to partition the difference set, the test to indicate whether the input number of partition sets ($q$) is an integer, the primitive element that will comprise the elements of the set, and finally the collection of sets that forms DSS with parameter $(n, m, q, p)$.

The following tables summarized the output of the developed program from 3 to 23.

Table 1: Partition of any prime number $n$ or multiplicative group of a finite field

<table>
<thead>
<tr>
<th>$n$</th>
<th>$GF(n)^*$</th>
<th>$q$</th>
<th>$m$</th>
<th>$\alpha$</th>
<th>DSS</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>${1,2}$</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>$Q_0 = {1}; \ Q_1 = {2}$</td>
<td>$(3,1,2,1)$</td>
</tr>
<tr>
<td>5</td>
<td>${1,2,3,4}$</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>$Q_0 = {4,1}; \ Q_1 = {3,2}$</td>
<td>$(5,2,2,2)$</td>
</tr>
<tr>
<td>5</td>
<td>${1,2,3,4}$</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>$Q_0 = {1}; \ Q_1 = {2}$; $Q_2 = {3}; \ Q_4 = {4}$</td>
<td>$(5,13,2)$</td>
</tr>
<tr>
<td>7</td>
<td>${1,2,3,4,5,6}$</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>$Q_0 = {2,4,1}; \ Q_1 = {6,5,3}$</td>
<td>$(7,3,2,3)$</td>
</tr>
<tr>
<td>7</td>
<td>${1,2,3,4,5,6}$</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>$Q_0 = {6,1}; \ Q_1 = {4,3}; \ Q_2 = {5,2}$</td>
<td>$(7,2,3,4)$</td>
</tr>
<tr>
<td>11</td>
<td>${1,2,3,4,5,6,7,8,9,10}$</td>
<td>2</td>
<td>5</td>
<td>2</td>
<td>$Q_0 = {4,5,9,3,1}$; $Q_1$ $= {8,10,7,6,2}$</td>
<td>$(11,5,2,5)$</td>
</tr>
<tr>
<td>11</td>
<td>${1,2,3,4,5,6,7,8,9,10}$</td>
<td>5</td>
<td>2</td>
<td>2</td>
<td>$Q_0 = {10,1}; \ Q_1 = {9,2}; \ Q_2 = {7,4}; \ Q_3 = {3,8}; \ Q_4 = {6,5}$</td>
<td>$(11,2,5,8)$</td>
</tr>
<tr>
<td>13</td>
<td>${1,2,3,4,5,6,7,8,9,10,11,12}$</td>
<td>2</td>
<td>6</td>
<td>2</td>
<td>$Q_0 = {4,3,12,9,10,1}$; $Q_1 = {8,6,11,5,7,2}$</td>
<td>$(13,6,2,6)$</td>
</tr>
<tr>
<td>13</td>
<td>${1,2,3,4,5,6,7,8,9,10,11,12}$</td>
<td>3</td>
<td>4</td>
<td>2</td>
<td>$Q_0 = {8,12,5,2}; \ Q_1 = {3,11,10,2}; \ Q_2 = {6,9,7,4}$</td>
<td>$(13,4,3,8)$</td>
</tr>
<tr>
<td>13</td>
<td>${1,2,3,4,5,6,7,8,9,10,11,12}$</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>$Q_0 = {3,9,1}; \ Q_1 = {6,5,2}; \ Q_2 = {12,10,4}; \ Q_3 = {11,7,8}$</td>
<td>$(13,2,6,10)$</td>
</tr>
<tr>
<td>17</td>
<td>${1,2,3,4,5,6,7,8,9,10,11,12}$</td>
<td>2</td>
<td>8</td>
<td>3</td>
<td>$Q_0 = {12,1}; \ Q_1 = {11,2}; \ Q_2 = {9,4}; \ Q_3 = {5,8}; \ Q_4 = {10,3}; \ Q_5 = {7,6}$</td>
<td>$(17,8,2,8)$</td>
</tr>
<tr>
<td>17</td>
<td>${1,2,3,4,5,6,7,8,9,10,11,12}$</td>
<td>8</td>
<td>2</td>
<td>3</td>
<td>$Q_0 = {9,13,15,16,8,4,2,1}; \ Q_1 = {10,5,11,14,7,12,6,3}$</td>
<td>$(17,2,8,14)$</td>
</tr>
<tr>
<td>17</td>
<td>${1,2,3,4,5,6,7,8,9,10,11,12}$</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>$Q_0 = {16,1}; \ Q_1 = {14,3}; \ Q_2 = {8,9}$</td>
<td>$(17,4,4,12)$</td>
</tr>
<tr>
<td>$n$</td>
<td>${QR}^*$</td>
<td>$q$</td>
<td>$m$</td>
<td>$\alpha$</td>
<td>DSS</td>
<td>Parameters</td>
</tr>
<tr>
<td>-----</td>
<td>-------------</td>
<td>-----</td>
<td>-----</td>
<td>---------</td>
<td>-----</td>
<td>------------</td>
</tr>
<tr>
<td>3</td>
<td>${1}$</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>$Q_0 = {1}$</td>
<td>(3,1,1,1)</td>
</tr>
<tr>
<td>7</td>
<td>${2,4,1}$</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>$Q_0 = {2,4,1}$</td>
<td>(7,3,1,3)</td>
</tr>
<tr>
<td>7</td>
<td>${2,4,1}$</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>$Q_0 = {1}, Q_1 = {2}, Q_2 = {4}$</td>
<td>(7,1,3,5)</td>
</tr>
<tr>
<td>11</td>
<td>${4,5,9,3,1}$</td>
<td>1</td>
<td>5</td>
<td>2</td>
<td>$Q_0 = {4,5,9,3,1}$</td>
<td>(11,5,1,5)</td>
</tr>
<tr>
<td>11</td>
<td>${4,5,9,31}$</td>
<td>5</td>
<td>1</td>
<td>2</td>
<td>$Q_0 = {4,5,9,31}$</td>
<td>(11,1,5,9)</td>
</tr>
</tbody>
</table>
Table 1 and 2, summarized the number of elements in a set, the subsets of the given set, the number of sets formed ($q$), the number of elements in the set ($m$), the primitive element, the collection of sets that form a DSS and parameters.

**Conclusion**

The paper aimed to construct DSS from the algorithms of Tonchev’s theorem from the partition of cyclic difference set. Two cyclic difference sets namely: the multiplicative group of $GF(n)^*$ and quadratic residue were used for the construction of DSS.

DSS can be constructed from the multiplicative group of $GF(n)^*$ and quadratic residue if both are cyclic differences and the collection of the base blocks from the subset of the multiplicative group of $GF(n)^*$ and quadratic residue are the sets that form the DSS. Tonchev (2005) concluded that the collection of sets has the parameter $(n, m, q, \rho)$. To facilitate the constructing of DSS from multiplicative group of $GF(n)^*$ and quadratic residue particularly for large prime $n$, a computer program in C++ was developed.

According to Levenshtein (1971), the combination of error-correcting and word-synchronization is possible in considering combinatorial problem on the DSS. Combinatorial designs is been the subject of study based on the various application in science, namely: Statistical planning of experiments, pattern recognition, construction of optimal error-correcting codes and the provisions of reliability in the transmission of digital information.
References


