THE POWER OF DESARGUESIAN SETS

Dr. W. W. Wu
Senior Staff Scientist
Advanced Systems
Communications Satellite Corporation
950 L’Enfant Plaza, S.W.
Washington, D. C. 20024

ABSTRACT

A Desarguesian set is a planar Euclidean geometry difference set which can be used to derive new cyclic block codes, convolutional self-orthogonal codes, and random multiple access codes. This paper discusses the usefulness of these codes and presents the step-by-step procedure for the purpose of constructing such sets. Comparisons are also made with planar projective geometry sets in which two types of existing codes were obtained.

1.0 INTRODUCTION

One of the reasons that the activity of coding applications has been relatively low perhaps is due to limited availability of high performance, high efficiency codes with low cost and simple decoders. Despite the flourishing of coding theory witnessed during the last decade, good codes are still too scarce to be useful in many practical situations. Based on such motivation this paper reports the finding of a construction procedure which can be used to generate not only one but three classes of completely different new codes. These three classes of codes are:

- One-step majority logic decodable block codes,
- Threshold decodable convolutional self-orthogonal codes, and
- Random multiple access codes.

The usefulness of each class of code will be discussed separately in Sections 3, 4, and 6. Because these three types of codes have a common origin from the geometry set, a discussion follows showing the differences between the existing codes and the newly derived ones from the necessary geometrical argument. In Section 2 the essential relations of geometries, sets, and codes will be presented from a simplified, hopefully clear and concise viewpoint. The main result will be presented in Section 5, in which the set construction procedure will be described step-by-step. Section 7 concludes with a remark
of the results which can be applied to frequency planning in order to avoid intermodulation interference problems in communications.

2.0 GEOMETRIES, SETS, AND CODES

Among other interesting subjects in finite geometry [1] are two fundamental classes called Euclidean and projective geometries. These geometries are traditionally represented by two quantities, the dimension \( D \) and a finite field \( F \). \( D \) is the size of ordered collection of elements which belong to \( F \). Euclidean and projective geometries are denoted as \( EG(D,F) \) and \( PG(D,F) \) respectively. It is known that error correcting codes can be derived from either geometries [2].

For example the Reed-Muller codes can be interpreted as \( EG(D,2) \).

The \( 2^D \) digits can be associated uniquely with \( 2^D \) points (collection of elements) in a \( D \)-dimensional Euclidean geometry over \( GF(2) \). The properties and construction method of other Euclidean geometry codes can be found in [2] along with a list of binary Euclidean geometry cyclic codes of length less than or equal to 63. Except for the code \( (n = 15, k = 7, d_{\text{min}} = 5) \) derived from \( EG(2,2) \) and for \( (63, 37, 9) \) code derived from \( EG(2,2^3) \), all other codes are derived from a dimension of other than 2.

Codes derivable from \( PG(D,F) \) also have been extensively investigated. Binary projective geometry codes of length up to 85 are listed in [2]. However the most useful projective geometry codes are derived from \( PG(2,F) \), i.e., the two dimensional, or planar geometry. Both convolutional codes and block codes can be constructed from \( PG(2,F) \). These two types of codes were independently derived through the common key characteristic of difference sets which have the origin from \( PG(2,F) \). Both types of codes have the common property of single step, simple majority logic decoding.

A difference set which can be derived from \( PG(2,F) \) is called planar projective geometry difference set (PPGDS). This is a collection of \( d_0, d_1, \ldots, d_u+1 \) integers such that among the set of integers no two differences (modulo - \( v \)) of the integers are the same. Difference sets in general are characterized by the parameters of \( v, u, \lambda \), while \( \lambda \) can be interpreted as the number of repeatable differences just mentioned. For PPGDS, \( \lambda \) always equals unity, i.e., no two differences are the same, or equivalently the differences of the set integers are all distinct. A necessary but not sufficient condition for a difference set to exist is that \( u(u+1) = \lambda(v-1) \) holds among the set parameters. There are other difference sets, but for useful code generations only the PPGDS have been proven of interest. PPGDS exist with parameters \( v = u^2 + u + 1 \), and \( \lambda = 1 \). The characteristics and construction procedures of PPGDS can be found in [3].
Although in theory both Euclidean and projective geometry codes have been
generalized into polynomial codes, they do not shed light as to the practical constructive
procedure for deriving good new codes.

Although both convolutional and block codes can be constructed from PPGDS, yet the
properties of the two types of codes are different. As of to date there are more useful
PPGDS convolutional codes than PPGDS block codes, and it does not seem possible to
generate any more useful block codes from PPGDS. But the PPGDS block codes are more
powerful in terms of error correcting capability per code length (either block length or
constrained length). These remarks will be further discussed separately in the next two
sections.

3.0 PLANAR PROJECTIVE GEOMETRY DIFFERENCE SET BLOCK CODES

Through the properties of PPGDS, Weldon derived a class of block codes which are
not only as powerful as some known random error correcting codes, but simple in
decoding implementation. For example, the (1057, 813, 34) PPGDS code can correct up to
16 errors in a code block of 1057 bits with a code rate of 0.77. The decoder consists of a
244 stage syndrome shift register, 813 bit message register, 30 3-input adders for threshold
decision, and 122 modulo-2 adders for feedbacks connected to the syndrome shift register.
Less than 14 AND gates are used for message controls. The decoding procedure is simple
indeed. For Gaussian channel signaling with a BPSK modem, a coding gain of 3.0 dB is
possible at $10^{-4}$ bit error rate without soft decision. At $10^{-9}$ it requires less than 7.0 dB
$E_b/N_0$ by calculation.

In addition to Weldon, the attractiveness of PPGDS codes was at least recognized by
Wu in 1969 (COMSAT Lab Record) and by Dorsch and Dolainsky in 1974 (DFVLR -
Institute für Satellitenlektionik, Oberpfaffenhofen, Germany). At COMSAT we have
computer simulated with hard decision only both the (73, 45, 10) and the (1057, 813, 34)
codecs and verified their expected performances. The other existing binary difference set
cyclic codes available are (7, 3, 4), (21, 11, 6), and (273, 191, 18). Unfortunately, as
observed by Weldon, there exist extremely few codes with useful parameters in this class.
It seems safe to conclude that it is not possible to derive additional powerful block codes
from PPGDS, unless there will be new PPGDS to be discovered.

4.0 PLANAR PROJECTIVE GEOMETRY DIFFERENCE SET
CONVOLUTIONAL CODES

PPGDS have been used successfully to generate a large number of convolutional self-
orthogonal codes [4], which provide a remarkable decoding property that does not seem to
be shared by other most powerful decoders known today. It is the property of not
producing additional and bursty errors at the outputs of the decoders when the capability of the decoders is exceeded. This property suggests itself attractively to the concatenations of this class of high rate codes.

The usefulness and derivations of PPGDS convolutional codes have been described in [4]. For global commercial satellite communication a high rate PPGDS code has been implemented in an operational digital carrier INTELSAT system. The author has been recently informed that the concatenations of PPGDS codes has been considered by Jet Propulsion Laboratory for a deep space mission.

The planar projective difference set convolutional codes differ from the planar projective difference set block codes in that more than a single convolutional code of different rate and different error correcting capability can be derived from a single planar geometry set. Thus the number of available projective planar difference set convolutional codes, which can be one step threshold decoded, exceeds the limited number of planar projective difference set block codes. But with the availability of Desarguesian sets, additional self-orthogonal convolutional codes can be provided with variety of code constraint lengths, rates and the number of correctable errors for future coding system design selections.

5.0 DESARGUESIAN SETS

The usefulness and limitations of PPGDS codes have been discussed. From a practical coding standpoint, more PPGDS are desirable in order to generate more useful codes. However due to the rigid structure of the PG(2,F) geometry it appears impossible to obtain more PPGDS; and it seems that it is a very unrewarding task to pursue the geometrical set approach for the purpose of code generation. As it turns out, the projective geometry difference set approach is indeed fruitless. But analogous to the difference sets derivable from PG(2,F) there exist difference sets which can be obtained from EG(2,F). This planar Euclidean geometry has been referred to as Desarguesian plane in the mathematical literature; thus we call the difference sets which can be derived from EG(2,F) Desarguesian sets. Unfortunately among the most recent and comprehensive treatments of difference sets in the literature, none suggested the possibility or existence of the planar Euclidean geometry difference sets (PEGDS, or Desarguesian sets), which essentially have the same characteristics as PPGDS. In this section the properties of Desarguesian sets are discussed and the construction procedure of Desarguesian sets is then demonstrated.

Similar to PPGDS, Desarguesian sets are also characterized by the three parameters $v$, $u$, and $\lambda=1$. Different from PPGDS, Desarguesian sets always have $v = u^2 - 1$. Thus for sets of $v$ values not available in PG(2,F), they can be in existence in EG(2,F).
The detailed studies of EG(2,F) difference sets and its application to one type of coding can be found in [4]. In the following, only the essential steps in order to obtain such sets are presented. Desarguesian sets are derived based on the interaction of two F’s. Or if one prefers, a ground field and its subfield. Let them be denoted as $F_2 = GF(p^m)$ and $F_2 = GF(p^{2m})$ for any positive integer $m$ and prime $p$. $\alpha$ and $\sigma$ are the primitive elements of $F_1$ and $F_2$ respectively. The construction method proceeds as follows.

Step 1: Given a prime or prime power $n = p^m$, then $p^{2m} = n^2$. Identify the non-zero elements of the corresponding finite field $GF(p^{2m})$ in terms of the primitive element $\sigma$ satisfying a primitive polynomial $F_0(\sigma)$ of degree $2m$. Let
\[
F_0(\sigma) = \sigma^{2m} + f_{2m-1} \sigma^{2m-1} + \ldots + f_1 \sigma + f_0 = 0
\]  
then
\[
\sigma^{2m} = -(f_{2m-1} \sigma^{2m-1} + \ldots + f_1 \sigma + f_0)
\]

Step 2: With the selected integer $u$ form two sets of integers $z = 1, 2, \ldots, u$; and $k = 0, 1, \ldots, u-2$. Each value of $z$ provides a Desarguesian set $\{D\}$. Choose a value of $z$ and run through the $k$ values to obtain
\[
d(z,k) = z + k(u+1)
\]
That is,
\[
d(z,0) = z + 0(u+1)
\]
\[
d(z,1) = z + 1(u+1)
\]
\[
\vdots
\]
\[
d(z,u-2) = z + (u-2)(u+1)
\]
The set of exponents $d_{k+1}$ can be obtained from $d(z,k)$ through the element $\sigma$ as in (4)
\[
\sigma^{d_{k+1}} = 1 + \sigma^d(z,k)
\]
for $k = 0, 1, \ldots, u-2$

Step 3: With $d_0 = 0$, the set is the collection of $d$’s, i.e.,
\[
\{D\} = \{0, d_1, d_2, \ldots, d_{u-1}\}\]
Example: Step 1: Let $p = 3$, $m = 1$, $u = p^m = 3$, then in terms of the primitive root $\sigma$ the non-zero elements of $GF(3^2) = F_2$ can be obtained by finding a primitive polynomial of degree 2 which is irreducible over $GF(3)$. Choose

$$F_0(x) = x^2 - 2x - 1 \quad (5)$$

Since $\sigma$ is a root of (5) we have $F_0(\sigma) = 0$ or,

$$\sigma^2 = 2\sigma + 1 \quad (6)$$

Then the other elements of $GF(3^2)$ are:

$$\sigma^0 = 1$$

$$\sigma^1 = \sigma$$

$$\sigma^2 = 2\sigma + 1$$

$$\sigma^3 = \sigma \cdot \sigma^2 = \sigma(2\sigma + 1)$$

$$= 2\sigma^2 + \sigma = 2(2\sigma + 1) + \sigma$$

$$= 2(\sigma + 1)$$

$$\sigma^4 = \sigma \cdot \sigma^3 = 2$$

$$\sigma^5 = 2\sigma$$

$$\sigma^6 = \sigma + 2$$

$$\sigma^7 = \sigma + 1$$

Step 2: Choose $z = 2$ and $k = 0$, we have

$$d(2,0) = 2 + 0 (3+1) = 2 \quad (7)$$

$$\sigma^{d_{1}} = 1 + \sigma d(2,0) = 1 + \sigma^2 = 1 + 2\sigma + 1$$

$$= 2\sigma + 2 = \sigma^3 \quad (8)$$
Therefore $d_1 = 3$. Next with $k = 1$ and the same value $z$ we have

$$d(2,1) = 2 + (3+1) = 6 \quad (9)$$

Therefore $d_2 = 1$

**Step 3:** With $d_0 = 0$, the set is

$$\{D\} = \{0, 3, 1\} \quad (11)$$

$\{D\}$ has the parameter of $v = u^2 - 1 = 8$, $u = 3$, and $\lambda = 1$.

To check whether (11) is a Desarguesian set we list the differences (modulo-8) among the three elements of the set,

$$0 - 3 \equiv 5 \pmod{8}$$
$$0 - 1 \equiv 7 \pmod{8}$$
$$3 - 0 \equiv 3 \pmod{8} \quad (12)$$
$$3 - 1 \equiv 2 \pmod{8}$$
$$1 - 0 \equiv 1 \pmod{8}$$
$$1 - 3 \equiv 6 \pmod{8}$$

It can be observed in (12) that the differences, i.e., 5, 7, 3, 2, 1, 6 occur once with no repeat. Thus $\lambda = 1$. $u = 3$ implies the fact the set contains three elements, i.e., 0, 3, 1.

### 6.0 RANDOM MULTIPLE ACCESS CODES

For multiple users, communications access schemes have been proven efficient for resources sharing. Random multiple access (RMA) technique is a signaling scheme which utilizes both time and frequency combination. If the inefficient usage of radio frequency system bandwidth can be tolerated and knowing that the number of baseband receivers is proportional to the number of users, then the advantages of a RMA system are
• The capability of accommodating a very large number of users.

• Bandwidth and time sharing. Without the need for retransmission when two or more messages collide.

• Enhance data security and resist jamming.

• System degrades gracefully.

• Low flux density of the received signal.

• Simple implementation

• Flexibility in future system expansion.

• Minimal amount of message control and supervision, and freedom of access.

• When signaling frequencies are spaced to avoid intermodulation products in FDMA, wideband low level RMA may be used in the same FDMA frequency band without the significant degradation of the FDMA signals to noise ratio.

Thus for some future tactical, mobile, data collection, maritime, computer data, and small to miniature size earth station operations in satellite communications RMA systems can be useful. Coding is essential in RMA systems. However the coding requirements differ from those for error correcting codes. Due to the nature of code generation and detection processes, the minimum distance measure of a RMA code differs from Hamming or Lee distance measures, because the disagreements (or agreements) of code symbols between any pair of code words span over the entire code word length and not just merely for the corresponding symbol position comparisons. For this reason, powerful nonbinary codes, such as Reed-Solomon codes, can not be optimally applied. The algorithm for generating RMA codes from Desarguesian sets has been demonstrated and the validity of the code properties has been proven [5]. It may be concluded after a long series effort that it is not possible to generate RMA codes from planar projective geometry. However it has been demonstrated thus far that RMA codes with the desirable properties can only be derived from Desarguesian sets. Without going into detail of the derivations and proofs only the properties of RMA codes are stated below

    Code length = n.

    Number of code symbols n^3
Code minimum distance n-1.

Number of frequency divisions = n^2.

Number of time divisions = n.

Number of code words = n^2 (n^2 + n + l)

The verification of these properties can also be found in [5].

Besides presenting the motivation and mentioning the connection to Desarguesian sets, no attempt will be made here as to the detail of RMA code construction.

7.0 CONCLUDING REMARKS

In this paper the power and usefulness of a Desarguesian set related to practical codes have been discussed. The procedure to construct such sets has been demonstrated. The method presented can generate a large number of cyclic block codes, convolutional self-orthogonal codes and random multiple access codes. All these three different classes of codes can be obtained from the same Desarguesian set.

From planar projective geometry it has been pointed out in this paper that the existing cyclic one-step majority decodable block codes and the threshold decodable convolutional codes have a common origin. Unfortunately codes derivable from planar projective geometry are few and exhausted. It also mentioned the unsuccessful attempt to generate random multiple access codes from PG(2,F). It seems at present that random multiple access codes can only be derived from Desarguesian sets which belong to EG(2,F).

In this paper we have used F to denote a finite field qualitatively and denote GF(n) quantitatively of the same field.

Through the distinct property of difference triangles Fang and Sandrin (Known 1975, published in COMSAT Technical Review 1977) established the connection between the triangles and frequency spacings in order to avoid intermodulation products in satellite communication. These triangles are originally derived from planar projective geometries. The set parameter v can be interpreted as the number of frequencies needed for spacing. The parameter u (in the case of Desarguesian set), or u + 1 (in the case of PPGDS) can be viewed as the number assigned frequency spacings. The values of the set elements are the actual assigned frequencies. A measure of effectiveness in frequency spacing is to have larger number of u with a smaller value v. Thus comparison in terms of the ratio u/v may be a reasonable criterion between Desarguesian sets and PPGDS. By comparison of
u/u^2 - 1 to (u+1)/(u^2+u +1) for the two classes of sets one can easily conclude that asymptotically Desarguesian sets are superior to planar projective geometry difference sets.

**REFERENCES**


