Disjoint difference families and their applications

S. -L. Ng[*], M. B. Paterson[†]

October 8, 2015

Abstract

Difference sets and their generalisations to difference families arise from the study of designs and many other applications. Here we give a brief survey of some of these applications, noting in particular the diverse definitions of difference families and the variations in priorities in constructions. We propose a definition of disjoint difference families that encompasses these variations and allows a comparison of the similarities and disparities. We then focus on two constructions of disjoint difference families arising from frequency hopping sequences and show that they are in fact the same. We conclude with a discussion of the notion of equivalence for frequency hopping sequences and for disjoint difference families.

Keywords: Frequency hopping sequences, difference families, m-sequences, finite geometry.

Classification: 94C30, 51E20, 94A62, 05B10.

1 Introduction

Difference sets and their generalisations to difference families arise from the study of designs and many other applications. In particular, the generalisation of difference sets to internal and external difference families arises from many applications in communications and information security. Roughly speaking, a difference family consists of a collection of subsets of an abelian group, and internal differences are the differences between elements of the same subsets, while external differences are the differences between elements of distinct subsets. Most of the definitions do not coincide exactly with each other, understandably since they arise from diverse applications, and the priorities of maximising or minimising various parameters are also understandably divergent. However, there is enough overlap in these definitions to warrant a study of how they relate to each other, and how the construction of one family may inform the construction of another. One of the aims of this paper is to perform a brief survey of these difference families, noting the variations in definitions and priorities, and to propose a definition that encompasses these definitions and allows a more unified study of these objects.

One particular class of internal difference family arises from frequency hopping (FH) sequences. FH sequences allow many transmitters to send messages simultaneously using a limited number of channels and it transpires that the question of how efficiently one can send messages has to do with the number of internal differences in a collection of subsets of frequency channels. The seminal paper of Lempel and Greenberger [51] gave optimal FH sequences using transformations of linear feedback shift register (LFSR) sequences. In another paper by Fuji-Hara *et al.* [28] various families of FH sequences were constructed using designs with particular automorphisms, and the question was raised there as to whether these constructions are the same as the LFSR constructions in [51]. Here we show a correspondence between one particular family of constructions in [28] and that of [51].

The relationship between the equivalence of difference families and the equivalence of the designs and codes that arise from them has been much studied. Here we will focus on the notion of equivalence for frequency hopping sequences and for disjoint difference families.

[*] Information Security Group, Royal Holloway University of London, Egham, Surrey TW20 0EX, United Kingdom. s.ng@rhul.ac.uk

[†] Department of Economics, Mathematics and Statistics, Birkbeck, University of London, Malet Street, Bloomsbury, London WC1E 7HX, United Kingdom. m.paterson@bbk.ac.uk

1.1 Definitions

Let $\mathcal{G}$ be an abelian group[1] of size v, and let $Q_0, \ldots, Q_{q-1}$ be disjoint subsets of $\mathcal{G}$, $|Q_i| = k_i$, $i = 0, \ldots, q-1$. We will call $(\mathcal{G}; Q_0, \ldots, Q_{q-1})$ a *disjoint difference family* $\mathrm{DDF}(v; k_0, \ldots, k_{q-1})$ over $\mathcal{G}$ with the following *external* $\mathcal{E}(\cdot)$ and *internal* $\mathcal{I}(\cdot)$ *differences*:

$$\begin{aligned}
\mathcal{E}_{i,j}(d) &= \{(a,b) \;:\; a-b=d, a \in Q_i, b \in Q_j, j \neq i\}, \\
\mathcal{E}_i(d) &= \{(a,b) \;:\; a-b=d, a \in Q_i, b \in Q_j, j = 0, \ldots, q-1, j \neq i\}, \\
\mathcal{E}(d) &= \{(a,b) \;:\; a-b=d, a \in Q_i, b \in Q_j, i,j = 0, \ldots, q-1, i \neq j\}, \\
\mathcal{I}_i(d) &= \{(a,b) \;:\; a-b=d, a,b \in Q_i, a \neq b\}, \\
\mathcal{I}(d) &= \{(a,b) \;:\; a-b=d, a,b \in Q_i, a \neq b, i = 0, \ldots, q-1\}.
\end{aligned}$$

We will call the DDF *uniform* if all the Q_i are of the same size, and we will say it is a *perfect*[2] internal (or external) DDF if $|\mathcal{I}(d)|$ (or $|\mathcal{E}(d)|$) is a constant for all $d \in \mathcal{G} \setminus \{0\}$. We will call the DDF a *partition type* DDF if $\{Q_0, \ldots, Q_{q-1}\}$ is a partition of $\mathcal{G}$.

Remark 1.1 As mentioned before and as will be pointed out in Section 2, there is by no means a consensus on the terms used to describe a DDF. Here we point out the disparity between our terms and those of [14], and in Section 2 we will point out the differences as they arise. In particular, the definition of difference family in [14] stipulates that the subsets Q_i are all of the same size, but does not insist that they are disjoint. We have defined a DDF to consist of disjoint subsets (of varying sizes) because we want to be able to define *external* differences. Using the term *uniform* to describe the subsets Q_i being of the same size is consistent with terminology used in design theory. □

Example 1.2 *A (v, k, λ)-difference set Q_0 over $\mathbb{Z}_v$ is a perfect internal* $\mathrm{DDF}(v; k)$ *with $|\mathcal{I}(d)| = \lambda = k(k-1)/(v-1)$. If we let $Q_1 = \mathbb{Z}_v \setminus Q_0$ then $(\mathbb{Z}_v; Q_0, Q_1)$ is an internal* $\mathrm{DDF}(v; k, v-k)$ *with $|\mathcal{I}_0(d)| = \lambda$ and $|\mathcal{I}_1(d)| = v - 2k + \lambda$ for all $d \in \mathbb{Z}_v^*$. In fact, $(\mathbb{Z}_v; Q_0, Q_1)$ has $|\mathcal{I}(d)| = v - 2k + 2\lambda$ and $|\mathcal{E}(d)| = v(v-1) - (v - 2k + 2\lambda)$ and is a perfect internal and external* DDF*.*

For example, the $(7, 3, 1)$ difference set $Q_0 = \{0, 1, 3\} \subseteq \mathbb{Z}_7$. We have $|\mathcal{I}(d)| = 1$. Let $Q_1 = \mathbb{Z}_7 \setminus Q_0 = \{2, 4, 5, 6\}$. Then $(\mathbb{Z}_7; Q_0, Q_1)$ has $|\mathcal{I}_0(d)| = 1$, $|\mathcal{I}_1(d)| = 2$, $|\mathcal{I}(d)| = 3$, $|\mathcal{E}_0(d)| = |\mathcal{E}_1(d)| = 2$ and $|\mathcal{E}(d)| = 4$ for all $d \in \mathbb{Z}_7^*$.

It is not hard to see that a perfect partition type internal DDF is also a perfect partition type external DDF and vice versa. However, this is not generally true for DDFs that are not partition type:

Example 1.3 *Let $\mathcal{G} = \mathbb{Z}_{25}$, $Q_0 = \{1, 2, 3, 4, 6, 15\}$, $Q_1 = \{5, 9, 10, 14, 17, 24\}$. This is a perfect external* $\mathrm{DDF}(25; 6, 6)$ *with $|\mathcal{E}(d)| = 3$ for all $d \in \mathbb{Z}_{25}^*$ given in [30]. However, it is not a perfect internal* DDF*:*

$$|\mathcal{I}(d)| = \begin{cases} 4 & \textit{for} \quad d = 1, 24, \\ 2 & \textit{for} \quad d = 7, 9, 10, 15, 16, 18, \\ 1 & \textit{for} \quad d = 6, 8, 17, 19, \\ 3 & \textit{for} \quad \textit{all other } d. \end{cases}$$

For many codes and sequences [28, 19, 30, 66, 12], desirable properties can be expressed in terms of (some) external or internal differences of DDFs. We give a brief survey of these applications and the properties required of the DDFs in the next section.

[1] The Handbook of Combinatorial Designs [14] has more material on difference families defined on non-abelian groups, but we will focus on abelian groups here since most of the applications we examine use abelian groups.

[2] The term *perfect* is used in [14] to refer to a specific type of difference family where half the differences cover half the ground set. Our usage is found in [74] in relation to self-synchronising codes.

2 Disjoint difference families in applications

This is not intended to be a comprehensive survey of where disjoint difference families arise in applications, nor of each application. We want to show that these objects arise in many areas of communications and information security research and that a study of their various properties may be useful in making advances in these fields.

2.1 Frequency hopping (FH) sequences

Let $F = \{f_0, \dots, f_{q-1}\}$ be a set of frequencies used in a frequency hopping multiple access communication system [24]. A frequency hopping (FH) sequence X of length v over F is simply $X = (x_0, x_1, \dots, x_{v-1})$, $x_i \in F$, specifying that frequency x_i should be used at time i. If two FH sequences use the same frequency at the same time (a collision), the messages sent at that time may be corrupted. Collisions are given by Hamming correlations: if a single sequence together with all its cyclic shifts are used then we are interested in its auto-correlation values (the number of positions in which each cyclic shift agrees with the original sequence). If two or more sequences are used then it is also necessary to consider the cross-correlation between pairs of sequences (the number of positions in which cyclic shifts of one sequence agree with the other sequence in the pair).

A single FH sequence X may be viewed in a combinatorial way: Define Q_i, $i = 0, \dots, q-1$, as subsets of $\mathbb{Z}_v$, with $j \in Q_i$ if $x_j = i$. Hence each Q_i corresponds to a frequency f_i, and the elements of Q_i are the positions in X where f_i is used. (For example, the frequency hopping sequence $X = (0, 0, 1, 0, 1, 1, 1)$ over $F = \{0, 1\}$ gives the DDF of Example 1.2.) In [28] it was shown that an FH sequence $(x_0, x_1, \dots, x_{v-1})$ with out-of-phase auto-correlation value of at most λ exists if and only if $(\mathbb{Z}_v; Q_0, \dots, Q_{q-1})$ is a partition type DDF$(v; k_0, \dots, k_{q-1})$ with $\mathcal{I}(d)$ satisfying

$$|\mathcal{I}(d)| \leq \lambda \text{ for all } d \in \mathbb{Z}_v^*.$$

In [28] $(\mathbb{Z}_v; Q_0, \dots, Q_{q-1})$ is called a partition type difference packing.

The aim in FH sequence design is to minimise collisions: we would like λ to be small. Lempel and Greenberger [51] proved a lower bound for λ, and in [69] bounds relating the size of sets of frequency hopping sequences with their Hamming auto- and cross-correlation values were given. Lempel and Greenberger [51] constructed optimal sequences using transformations of m-sequences (more details in Section 4.1). In [28] Fuji-Hara *et al.* also provided many examples of optimal sequences using designs with certain types of automorphisms. Other constructions of FHS include using cyclotomy [11, 56], random walks on expander graphs [26], and error-correcting codes [22, 23]. A survey of sequence design from the viewpoint of codes can also be found in [71]. Later in this paper we will show that one of the constructions in [28] by Fuji-Hara *et al.* gave the same sequences as those constructed by Lempel and Greenberger in [51]. It would be interesting to see how the other constructions relate to each other.

Note that in this correspondence to a difference family, the set of frequency hopping sequence is the rotational closure (Definition 5.2, Section 5) of one single frequency hopping sequence. Collections of DDFs were used to model more general sets of sequences in [4, 32, 80], referred to as balanced nested difference packings.

It is also to be noted that most of the published work considered either pairwise interference between two sequences (described above as Hamming correlation) or adversarial interference (jamming) [26, 82, 59], which may not reflect the reality of the application where more than two sequences may be in use. To this end Nyirenda *et al.* [60] modelled frequency hopping sequences as cover-free codes and considered additional properties required to resist jamming.

2.2 Self-synchronising codes

Self-synchronising codes are also called comma-free codes and have the property that no codeword appears as a substring of two concatenated codewords. This allows for synchronisation without external help. Codes achieving self-synchronisation in the presence of up to $\lfloor \frac{\lambda-1}{2} \rfloor$ errors can be constructed from a DDF$(v; k_0, \dots, k_{q-1})$ $(\mathbb{Z}_v; Q_0, \dots, Q_{q-1})$ with $|\mathcal{E}(d)| \geq \lambda$. In [30], this DDF was called a *difference system of sets* of index λ over $\mathbb{Z}_v$. The sets $Q_0, \dots, Q_{q-1}$ give the markers for self-synchronisation and are a redundancy, hence we would like $k = \sum_{i=0}^{q-1} k_i$

to be small. Other optimisation problems include reducing the rate k/v, reducing λ, and reducing the number q of subsets.

An early paper by Golomb *et al.* [36] took the combinatorial approach to the subject of self-synchronising codes, and [52] gave a survey of results, constructions and open problems of self-synchronising codes. More recent work on self-synchronising codes can be found in [13] which gave some variants on the definitions, and in [6] in the guise of non-overlapping codes, giving constructions and bounds. Further constructions can be found in [30], including constructions from the partitioning of cyclic difference sets and partitioning of hyperplanes in projective geometry, as well as iterative constructions using external and internal DDFs.

2.3 Splitting A-codes and secret sharing schemes with cheater detection

In authentication codes (A-codes), a transmitter and a receiver share an encoding rule e, chosen according to some specified probability distribution. To authenticate a source state s, the transmitter encodes s using e and sends the resulting message $m = e(s)$ to the receiver. The receiver receives a message m' and accepts it if it is a valid encoding of some source, *i.e.* when $m' = e(s')$ for some source s'. In a splitting A-code, the message is computed with an input of randomness so that a source state is not uniquely mapped to a message. An adversary (who does not know which encoding rule is being used) may send their own message m to the receiver in the hope that it will be accepted as valid. This is known as an *impersonation attack*, and succeeds if m is a valid encoding of some source s. Also of concern are *substitution attacks*, in which an adversary who has seen an encoding m of a source s replaces it with a new value m'. This attack succeeds if m' is a valid encoding of some source $s' \neq s$. We refer to [66] for further background. It was shown in [66] that optimal splitting A-codes can be constructed from a perfect uniform external DDF$(v; k_0 = k, \ldots, k_{q-1} = k)$ with $|\mathcal{E}(d)| = 1$. This gives an A-code with q source states, v encoding rules, v messages, and each source state can be mapped to k valid messages. This type of DDF was called an external difference family (EDF) in [66]. The probability of an adversary successfully impersonating the transmitter is given by kq/v and the probability of successfully substituting a message being transmitted is given by $1/kq$ (which also happens to equal $k(q-1)/(v-1)$ in this particular context). These are parameters to be minimised.

An extensive list of A-code references prior to 1998 is given in [72]. More recent work on splitting authentication codes includes [7, 17, 18, 31, 43, 44, 45, 46, 47, 50, 53, 54, 63, 68, 75, 76]

A *secret sharing scheme* is a means of distributing some information, known as *shares*, to a set of *players* so that authorised subsets of players are able to combine their shares to reconstruct a unique secret, whereas the shares belonging to unauthorised subsets reveal no information about the secret. If some of the players are dishonest, however, then they may *cheat* by submitting false values that are not their true shares and thereby causing an incorrect value to be obtained during secret reconstruction. Such attacks were first discussed by Tompa and Woll in [73]. Various types of difference family have been used in constructing schemes which allow such cheating to be detected with high probability. In [65], difference sets were used to construct schemes that were optimal with respect to certain bounds on the sizes of shares. In [66], EDFs were used in a similar manner to construct optimal schemes. Other schemes that permit detection of cheaters include those proposed in [3, 9, 42, 62, 61, 64]. Many of these constructions can be interpreted as involving particular types of difference family; this observation has led to the definition of the concept of *algebraic manipulation detection codes* [15] (see Section 2.4).

2.4 Weak algebraic manipulation detection (AMD) codes

An AMD code is a tool that can be combined with a cryptographic system that provides some form of secrecy in order to incorporate extra robustness against an adversary who can actively change values in the system. The notion was proposed in [15] as an abstraction of techniques used in the construction of robust secret sharing schemes. In the basic setting for a weak AMD code, a *source* is chosen uniformly from a finite set S of sources with $|S| = k$. It is then encoded using a (possibly randomised) encoding map $E \colon S \to \mathcal{G}$ where $\mathcal{G}$ is an abelian group of order $v \geq k$. We require the sets of possible encodings of different sources to be disjoint, so that $E(s)$ uniquely determines s. An adversary is able to manipulate this encoded value by adding a group element $d \in \mathcal{G}$ of its choosing. (We suppose the adversary knows the details of the encoding function, but does not know what source has been chosen, nor the specific value of any randomness used in the encoding.) After this manipulation, an attempt is made to decode the resulting value. If the altered value $E(s) + d$ is a valid encoding $E(s')$ of some source s' then it is decoded to s'. Otherwise, decoding fails and the symbol $\perp$ is returned; this represents the situation where the adversary's manipulation has been detected. The adversary is deemed to have succeeded if $E(s) + d$ is decoded to $s' \neq s$, that is if they have caused the stored value to be decoded to a source other than the one that was initially stored.

A set of sources S with $|S| = k$, abelian group $\mathcal{G}$ with $|\mathcal{G}| = v$ and encoding rule E constitute a *weak* (k, v, ϵ)*-AMD (algebraic manipulation detection) code* if for any choice of $d \in \mathcal{G}$ the adversary's success probability is at most ϵ. (The probability is taken over the uniform choice of source, and over the randomness used in the encoding.)

In [15], it was shown that a weak (k, v, ϵ)-AMD code with deterministic encoding is equivalent to a DDF$(v; k)$ with

$$|\mathcal{I}(d)| \leq \lambda, \ \lambda \leq \epsilon k \ \text{ for all } d \in \mathcal{G}.$$

In [15] these were called (v, k, λ)-bounded difference sets. It is easy to see that these are generalisations of difference sets, allowing general abelian groups and with an upper bound for the number of differences.

Weak AMD codes were introduced in [15], with further detail on constructions, bounds and applications provided in the full version of the paper [16]. Bounds on the adversary's success probability in a weak AMD code were given in [19] and several families with good asymptotic properties were constructed using vector spaces. Additional bounds were given in [67], and constructions and characterisations were given relating weak AMD codes that are optimal with respect to these bounds to a variety of types of external DDF. It is desirable to minimise the tag length ($\log v - \log k$, the number of redundant bits) as well as ϵ.

2.5 Stronger forms of algebraic manipulation detection (AMD) code

Strong AMD codes were defined in [15]; these are able to limit the success probability of an adversary even when the adversary knows which source has been encoded. Specifically, for every source $s \in S$ and every element $d \in \mathcal{G}$, the probability that $(E(s) + d)$ is decoded to a value $s' \notin \{s, \perp\}$ is at most ϵ. (Here the probability is taken over the randomness in the encoding rule E. Unlike the case of a weak AMD code, a strong AMD code cannot use a deterministic encoding rule.)

Write $Q_i = \{g \in \mathcal{G} \ : \ D(g) = s_i\}$ for each $s_i \in S$, $i = 0, \ldots, k-1$, and $|Q_i| = k_i$. In the case where the encoding $E(s_i)$ is uniformly distributed over Q_i for every s_i, we have that $(\mathcal{G}; Q_0, \ldots, Q_{k-1})$ forms a DDF$(v; k_0, \ldots, k_{k-1})$ with $|\mathcal{E}_i(d)| \leq \lambda_i = \epsilon k_i$ and $|\mathcal{E}(d)| \leq \lambda = \sum_{i=0}^{k-1} \lambda_i$.

Constructions from vector spaces and caps in projective space were given in [19]. Additional bounds and characterisations were given in [67]. A construction based on a polynomial over a finite field was given in [15] and applied to the construction of robust secret sharing schemes, and robust fuzzy extractors. This construction has since been used for a range of applications, including the construction of anonymous message transmission schemes [8], non-malleable codes [25], strongly decodeable stochastic codes [37], secure communication in the presence of a byzantine relay [38, 39], and codes for the adversarial wiretap channel [77]. New constructions, including an asymptotically optimal randomised construction were given in [20].

AMD codes that resist adversaries who learn some limited information about the source were constructed and analysed in [1], and their application to tampering detection over wiretap channels was discussed.

AMD codes secure in a stronger model in which an adversary succeeds even when producing a new encoding of the original source have been used in the design of secure cryptographic devices and related applications [33, 34, 49, 58, 57, 78, 79].

2.6 Optical orthogonal codes (OOCs)

Optical orthogonal codes (OOCs) are sequences arising from applications in code-division multiple access in fibre optic channels. OOC with low auto- and cross-correlation values allow users to transmit information efficiently in an asynchronous environment. A $(v, w, \lambda_a, \lambda_c)$-OOC of size q is a family $\{X_0, \ldots, X_{q-1}\}$ of q $(0,1)$-sequences of length v, weight w, such that auto-correlation values are at most λ_a and cross-correlation values are at most λ_c. For each sequence X_i, let Q_i be the set of integers modulo v denoting the positions of the non-zero bits. Then $(\mathbb{Z}_v; Q_0, \ldots, Q_{q-1})$ is a uniform DDF$(v; k_0 = w \ldots, k_{q-1} = w)$ with

$$\begin{aligned} |\mathcal{I}_i(d)| &\leq \lambda_a, \\ |\mathcal{E}_{i,j}(d)| &\leq \lambda_c, \text{ for all } d \in \mathbb{Z}_v^*. \end{aligned}$$

Background and motivation to the study of OOC were given in [12], which also included constructions from designs, algebraic codes and projective geometry. In [5] constant weight cyclically permutable codes, which are also uniform DDFs, were used to construct OOC, and a recursive construction was given. In [83] OOC were used to construct compressed sensing matrix and a relationship between OOC and modular Golomb rulers ([14]) was given - a (v, k) modular Golomb ruler is a set of k integers $\{d_0, \ldots, d_{k-1}\}$ such that all the differences are distinct and non-zero modulo v - in fact, a DDF$(v; k)$ with $|I(d)| \leq 1$ for all $d \neq 0$.

A generalisation to two-dimensional OOC with a combinatorial approach can be found in [10, 21]. Combinatorial and recursive constructions as well as bounds can be found in [27], and [48] allowed variable weight OOC and used various types of difference families and designs to construct such OOCs.

2.7 Other applications

The list of applications discussed in this section is by no means exhaustive, and DDFs arise in a variety of other areas of combinatorics and coding theory. For example, in [29], complete sets of disjoint difference families (in fact, partition type perfect uniform DDFs where the subsets are grouped) were used in constructing *1-factorisations of complete graphs* and in constructing *cyclically resolvable cyclic Steiner systems*. In [81], *high-rate quasi-cyclic codes* were constructed using perfect internal uniform DDF, and a generalisation to families of sets of non-negative integers with specific internal differences was given. *$\mathbb{Z}$-cyclic whist tournaments* correspond to perfect internal DDFs over $\mathbb{Z}_v$ [2]. In addition, various types of sequences and arrays with specified correlation properties have been proposed for a wide range of applications [35, 40]. Many of these can be studied in terms of a relationship with appropriate forms of DDFs [70].

3 A geometrical look at a perfect partition type disjoint difference family

In [28] a perfect partition type DDF$(q^n - 1; k_0 = q - 1, k_1 = q, \ldots, k_{q^{n-1}-1} = q)$ over $\mathbb{Z}_{q^n-1}$ was constructed from line orbits of a cyclic perspectivity τ in the n-dimensional projective space $PG(n, q)$ over GF(q). In [51] another construction with the same parameters was given. In the next section we will show a correspondence between the two constructions. Before that we will describe in greater detail the the construction of [28, Section III].

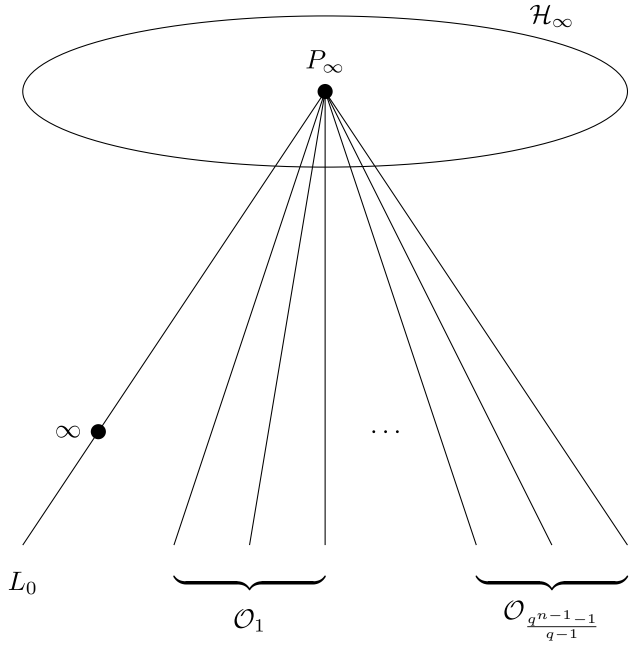
An n-dimensional projective space $PG(n, q)$ over the finite field of order q admits a cyclic group of perspectivities $\langle\tau\rangle$ of order $q^n - 1$ that fixes a hyperplane $\mathcal{H}_\infty$ and a point $\infty \notin \mathcal{H}_\infty$. (We refer the reader to [41] for properties of projective spaces and their automorphism groups.) This group $\langle\tau\rangle$ acts transitively on the points of $\mathcal{H}_\infty$ and regularly on the points of $PG(n, q) \setminus (\mathcal{H}_\infty \cup \{\infty\})$. We will call the points (and spaces) not contained in $\mathcal{H}_\infty$ the affine points (and spaces).

The point orbits of $\langle\tau\rangle$ are $\{\infty\}$, $\mathcal{H}_\infty$, and $PG(n, q) \setminus (\mathcal{H}_\infty \cup \{\infty\})$. Dually, the hyperplane orbits are $\mathcal{H}_\infty$, the set of all hyperplanes through ∞, and the set of all hyperplanes of $PG(n, q) \setminus \mathcal{H}_\infty$ not containing ∞. Line orbits under $\langle\tau\rangle$ are:

(A) One orbit of affine lines through ∞ - this orbit has length $\frac{q^n-1}{q-1}$; and

(B) $\frac{q^{n-1}-1}{q-1}$ orbits of affine lines not through ∞ - each orbit has length $q^n - 1$, and $\langle\tau\rangle$ acts regularly on each orbit; and

Figure 1: The parallel class $\mathcal{P}$.



(C) One orbit of lines contained in $\mathcal{H}_\infty$.

A set of parallel (affine) lines through a point $P_\infty \in \mathcal{H}_\infty$ consists of one line L_0 from the orbit of type (A) and $q-1$ lines from each of the $(q^{n-1}-1)/(q-1)$ orbits of type (B). We will write this set of q^{n-1} lines $\mathcal{P} = \{L_0, L_1, \ldots, L_{q^{n-1}-1}\}$ as follows (See Figure 1):

- L_0, a line through ∞ and $P_\infty \in \mathcal{H}_\infty$;
- $\mathcal{O}_i = \{L_{(i-1)(q-1)+1}, L_{(i-1)(q-1)+2}, \ldots, L_{(i-1)(q-1)+(q-1)}\}$, $i = 1, \ldots, \frac{q^{n-1}-1}{q-1}$, each $\mathcal{O}_i$ belonging to a different orbit under $\langle \tau \rangle$.

We consider the two types of $d \in \mathbb{Z}^*_{q^n-1}$ depending on the action of τ^d on L_0:

(I) There are $q-2$ values of τ^d, $d \in \mathbb{Z}^*_{q^n-1}$, fixing the line L_0 (and the points P_∞ and ∞) and permuting the points of L_0. These τ^d permute but do not fix the lines within each $\mathcal{O}_i$. Hence we have, for these $d \in \mathbb{Z}^*_{q^n-1}$,

$$L_0^{\tau^d} \cap L_0 = L_0 \text{ and } L_i^{\tau^d} \cap L_i = \{P_\infty\}. \tag{1}$$

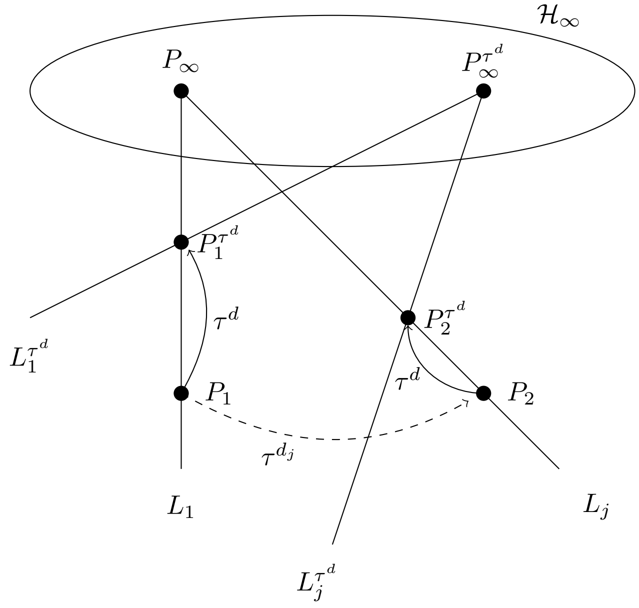
(II) The remaining $(q^n-1)-(q-2)$ values of τ^d map lines in $\mathcal{P}$ to affine lines not in $\mathcal{P}$. Hence we have

$$L_0^{\tau^d} \cap L_0 = \{\infty\} \text{ and } |L_i^{\tau^d} \cap L_i| = 0 \text{ or } 1. \tag{2}$$

Without loss of generality consider $L_1 \in \mathcal{O}_1$. Suppose $|L_1^{\tau^d} \cap L_1| = 1$, say $L_1^{\tau^d} \cap L_1 = \{P\}$. Let $L_k \in \mathcal{O}_1$ be another line in the same orbit as L_1, so there is a d_k such that $L_1^{\tau^{d_k}} = L_k$. It is not hard to see that $\{P^{\tau^{d_k}}\} = L_k^{\tau^d} \cap L_k$, since

$$\begin{aligned} P \in L_1 \quad &\Rightarrow \quad P^{\tau^{d_k}} \in L_1^{\tau^{d_k}} = L_k, \\ P \in L_1^{\tau^d} \quad &\Rightarrow \quad P^{\tau^{d_k}} \in (L_1^{\tau^d})^{\tau^{d_k}} = (L_1^{\tau^{d_k}})^{\tau^d} = L_k^{\tau^d}. \end{aligned}$$

Figure 2: L_1, L_j in different orbits



Hence for any orbit $\mathcal{O}_i$, if $|L_j^{\tau^d} \cap L_j| = 1$ for some $L_j \in \mathcal{O}_i$ then $|L_k^{\tau^d} \cap L_k| = 1$ for all $L_k \in \mathcal{O}_i$

Now, suppose again that $|L_1^{\tau^d} \cap L_1| = 1$. Let P_1 be the point on L_1 such that $P_1^{\tau^d} \in L_1^{\tau^d} \cap L_1$. Consider $L_j \in \mathcal{O}_k$, $k \neq 1$. Suppose $|L_j^{\tau^d} \cap L_j| = 1$. Let P_2 be the point on L_j such that $P_2^{\tau^d} \in L_j^{\tau^d} \cap L_j$. (See Figure 2.) Since $\langle\tau\rangle$ is transitive on affine points (excluding ∞), there is a d_j such that $P_1^{\tau^{d_j}} = P_2$. Then

$$(P_1^{\tau^d})^{\tau^{d_j}} = (P_1^{\tau^{d_j}})^{\tau^d} = P_2^{\tau^d}.$$

This means that τ^{d_j} maps P_1 to P_2 and $P_1^{\tau^d}$ to $P_2^{\tau^d}$ and hence maps the line L_1 to L_j. But this is a contradiction since L_1 and L_j belong to different orbits under $\langle\tau\rangle$. Hence if $|L_j^{\tau^d} \cap L_j| = 1$ for any L_j in some orbit $\mathcal{O}_i$ then $|L_k^{\tau^d} \cap L_k| = 0$ for all L_k in all other orbits.

It is also clear that for any L_i in any orbit, there is a d such that $|L_i^{\tau^d} \cap L_i| = 1$, because $\langle\tau\rangle$ is transitive on affine points (excluding ∞). Indeed, $\langle\tau\rangle$ acts regularly on these points, so that for any pair of points (P, Q) on L_i there is a unique d such that $P^{\tau^d} = Q$. There are $q(q-1)$ pairs of points and so there are $q(q-1)$ such values of d. These $q(q-1)$ values of d for each $\mathcal{O}_i$ in $\mathcal{P}$, together with the $q-2$ values of d where τ^d that fixes L_0, account for all of $\mathbb{Z}^*_{q^n-1}$.

Now, the points of $PG(n,q) \setminus (\mathcal{H}_\infty \cup \{\infty\})$ can be represented as $\mathbb{Z}_{q^n-1}$ as follows: pick an arbitrary point P_0 to be designated 0. The point $P_0^{\tau^i}$ corresponds to $i \in \mathbb{Z}_{q^n-1}$. The action of τ^d on any point P is thus represented as $P + d$. Affine lines are therefore q-subsets of $\mathbb{Z}_{q^n-1}$. Let $Q_0 \subseteq \mathbb{Z}_{q^n-1}$ contain the points of $L_0 \setminus \{\infty\}$, and let Q_i contain the points of L_i. It follows from the intersection properties of the lines (properties (1), (2)) that $\{Q_0, \ldots, Q_{q^{n-1}-1}\}$ forms a perfect partition type DDF$(q^n-1; q-1, q, \ldots, q)$ over $\mathbb{Z}_{q^n-1}$, with $|\mathcal{I}(d)| = q-1$ for all $d \in \mathbb{Z}^*_{q^n-1}$.

3.1 A perfect external DDF

Given that a partition type perfect internal DDF over $\mathbb{Z}_v$ with $|\mathcal{I}(d)| = \lambda$ must be a perfect external DDF with $|\mathcal{E}(d)| = v - \lambda$, the intersection properties $|L_i^{\tau^d} \cap L_j|$, $i \neq j$ can be deduced as follows for the two different types (I), (II) of d:

(I) For the $q-2$ values of τ^d of type (I) fixing L_0, we have:

(a) L_0 is fixed, so $|L_0^{\tau^d} \cap L_i| = 0$ for all $L_i \neq L_0$.

(b) If L_i and L_j are in different orbits then $|L_i^{\tau^d} \cap L_j| = 0$ (since τ^d fixes $\mathcal{O}_i$).

(c) If L_i and L_j are in the same orbit, then since τ^d acts regularly on an orbit of type (B), there is a unique d that maps L_i to L_j, so $|L_i^{\tau^d} \cap L_j| = q$, and for all other L_k in the same orbit, $|L_i^{\tau^d} \cap L_k| = 0$. This applies to each orbit, so that for each of the $q-2$ values of d, there are $((q^{n-1}-1)/(q-1)) \times (q-1) = q^{n-1}-1$ cases where $|L_i^{\tau^d} \cap L_j| = q$.

(II) For the $(q^n-1)-(q-2)$ values of τ^d of type (II) not fixing L_0, we have:

(a) Pick any point $P \in L_0 \setminus \{\infty\}$, $P^{\tau^d} \in L_i$ for some $L_i \neq L_0$, so $|L_0^{\tau^d} \cap L_i| = 1$ for some L_i. There are $q-1$ points on $L_0 \setminus \{\infty\}$, so there are $q-1$ lines L_i such that $|L_0^{\tau^d} \cap L_i| = 1$.

(b) Consider $L_i \neq L_0$. Take any point $P \in L_i$. We have $P^{\tau^d} \in L_j$ for some L_j, so $|L_i^{\tau^d} \cap L_j| = 1$. This applies for all L_i, so that for any of the $(q^n-1)-(q-2)$ values of d, there are $(q^{n-1}-1)q$ cases of $|L_i^{\tau^d} \cap L_j| = 1$, $q-1$ of which are when $L_j = L_i$.

Defining the sets $Q_0, \dots, Q_{q-1}$ as before, we see that $\{Q_0, \dots, Q_{q-1}\}$ forms a perfect partition type DDF with $\mathcal{E}(d) = q(q^{n-1}-1)$.

4 A correspondence between two difference families

In [28], Fuji-Hara *et al.* constructed the perfect partition type DDF$(q^n-1; q-1, q, \dots, q)$ over $\mathbb{Z}_{q^n-1}$ with $|\mathcal{I}(d)| = q-1$ described in Section 3. Using parallel t-dimensional subspaces (we described the case when $t=1$), perfect partition type DDF$(q^n-1; q^t-1, q^t, \dots, q^t)$ with $|\mathcal{I}(d)| = q^t-1$ can also be constructed.

This construction gives DDF with the same parameters as those constructed using m-sequences in [51], though [51] restricted their constructions to the case when q is a prime. It was asked in [28] whether these are "essentially the same" constructions. In this section we show a correspondence between these two constructions, and in Section 5 we discuss what "essentially the same" might mean. This correspondence also shows that the restriction to q prime in [51] is unnecessary. (Indeed it was pointed out in [71] that the assumption that the field must be prime is not necessary.)

4.1 The Lempel-Greenberger m-sequence construction

We refer the reader to [55] for more details on linear recurring sequences. Here we sketch an introduction. Let $(s_t) = s_0 s_1 s_2 \dots$ be a sequence of elements in GF(q), q a prime power, satisfying the n^{th} order linear recurrence relation

$$s_{t+n} = c_{n-1}s_{t+n-1} + c_{n-2}s_{t+n-2} + \cdots + c_0 s_t,\ c_i \in \text{GF}(q),\ c_{n-1} \neq 0.$$

Then (s_t) is called an (n^{th} order) linearly recurring sequence in GF(q). Such a sequence can be generated using a *linear feedback shift register (LFSR)*. An LFSR is a device with n *stages*, which we denote by $S_0, \dots, S_{n-1}$. Each stage is capable of storing one element of GF(q). The contents s_{t+i} of all the registers S_i $(0 \leq i \leq n-1)$ at a particular time t are known as the *state* of the LFSR at time t. We will write it either as $s(t,n) = s_t s_{t+1} \dots s_{t+n-1}$ or as a vector $\mathbf{s}_t = (s_t, s_{t+1}, \dots, s_{t+n-1})$. The state $\mathbf{s}_0 = (s_0, s_1, \dots, s_{n-1})$ is the *initial state.*

At each clock cycle, an output from the LFSR is extracted and the LFSR is updated as described below.

- The content s_t of the stage S_0 is output and forms part of the *output sequence.*
- For all other stages, the content s_{t+i} of stage S_i is moved to stage S_{i-1} $(1 \leq i \leq n-1)$.

- The new content s_{t+n} of stage S_{n-1} is the value of the *feedback function*

  $$f(s_t, s_{t+1}, \ldots, s_{t+n-1}) = c_0 s_t + c_1 s_{t+1} + \cdots c_{n-1} s_{t+n-1},\ c_i \in \mathrm{GF}(q).$$

  The new state is thus $\mathbf{s}_{t+1} = (s_{t+1}, s_{t+2}, \ldots, s_{t+n})$. The constants $c_0, c_1, \ldots, c_{n-1}$ are known as the *feedback coefficients* or *taps.*

A diagrammatic representation of an LFSR is given in Figure 3.

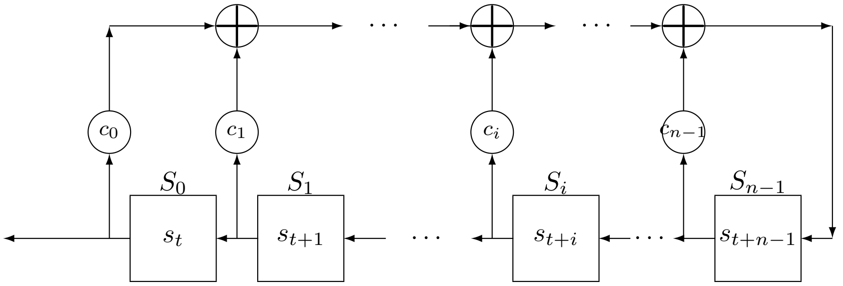


Figure 3: Linear Feedback Shift Register

The *characteristic polynomial* associated with the LFSR (and the linear recurrence relation) is

$$f(x) = x^n - c_{n-1}x^{n-1} - c_{n-2}x^{n-2} - \cdots - c_0.$$

The state at time $t+1$ is also given by $\mathbf{s}_{t+1} = \mathbf{s}_t C$, where C is the *state update matrix* given by

$$C = \begin{pmatrix} 0 & 0 & \ldots & 0 & c_0 \\ 1 & 0 & \ldots & 0 & c_1 \\ 0 & 1 & \ldots & 0 & c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & c_{n-1} \end{pmatrix}.$$

A sequence (s_t) generated by an n-stage LFSR is periodic and has maximum period $q^n - 1$. A sequence that has maximum period is referred to as an *m-sequence.* An LFSR generates an m-sequence if and only if its characteristic polynomial is primitive. An m-sequence contains all possible non-zero states of length n, hence we may use, without loss of generality, the *impulse response sequence* (the sequence generated using initial state $(0 \cdots 01)$).

Let $S = (s_t) = s_0 s_1 s_2 \ldots$ be an m-sequence over a prime field GF(p) generated by an n-stage LFSR with a primitive characteristic polynomial $f(x)$. Let $s(t,k) = s_t s_{t+1} \ldots s_{t+k-1}$ be a subsequence of length k starting from s_t.

The σ_k-transformations, $1 \leq k \leq n-1$ introduced in [51] are described as follows:

$$\sigma_k : s(t,k) = s_t s_{t+1} \ldots s_{t+k-1} \rightarrow \sum_{i=0}^{k-1} s_{t+i} p^i \in \mathbb{Z}_{p^k} = \{0, 1, \ldots, p^k - 1\}.$$

We write the σ_k-transform of S as $U = (u_t)$, $u_t = \sigma_k(s(t,k))$, which is a sequence over $\mathbb{Z}_{p^k}$.

In [51, Theorem 1] it is shown that the sequence U forms a frequency hopping sequence with out-of-phase autocorrelation value of $p^{n-k} - 1$, and hence a partition type perfect DDF with $|\mathcal{I}(d)| = p^{n-k} - 1$ (Section 2.1). We see in the next section that this corresponds to the geometric construction of [28] described in Section 3.

4.2 A geometric view of the Lempel-Greenberger m-sequence construction.

We refer the reader to [41] for details about coordinates in finite projective spaces over GF(q). Here we only sketch what is necessary to describe the m-sequence construction of Section 4.1 from the projective geometry point of view.

Let $PG(n,q)$ be an n-dimensional projective space over GF(q). Then we may write

$$PG(n,q) = \{(x_0, x_1, \ldots, x_n) \mid x_i \in \mathrm{GF}(q) \text{ not all zero}\},$$

with the proviso that $\rho(x_0, x_1, \ldots, x_n)$ as ρ ranges over GF$(q) \setminus \{0\}$ all refer to the same point. Dually a hyperplane of $PG(n,q)$ is written as $[a_0, a_1, \ldots, a_n]$, $a_i \in$ GF(q) not all zero, and contains the points $(x_0, x_1, \ldots, x_n)$ satisfying the equation

$$a_0x_0 + a_1x_1 + \cdots + a_nx_n = 0.$$

Clearly $\rho[a_0, a_1, \ldots, a_n]$ as ρ ranges over GF$(q) \setminus \{0\}$ refers to the same hyperplane. A k-dimensional subspace is specified by either the points contained in it, or the equations of the $n-k$ hyperplanes containing it.

Now, let $S = (s_t) = s_0s_1s_2\ldots$ be an m-sequence over GF(p), p prime, generated by an n-stage LFSR with a primitive characteristic polynomial $f(x)$ and state update matrix C, as described in the previous section. For $t = 0, \ldots, p^n - 2$, let $P_t = (s_t, s_{t+1}, \ldots, s_{t+n-1}, 1)$. Then the set $\mathcal{O} = \{P_t \mid t = 0, \ldots p^n - 2\}$ are the points of $PG(n,p) \setminus (\mathcal{H}_\infty \cup \{\infty\})$ where $\mathcal{H}_\infty$ is the hyperplane $x_n = 0$ and ∞ is the point $(0, \ldots, 0, 1)$.

Let τ be the projectivity defined by

$$A = \left(\begin{array}{cccc} & & & 0 \\ & C & & \vdots \\ & & & 0 \\ 0 & \ldots & 0 & 1 \end{array}\right).$$

Then τ fixes $\mathcal{H}_\infty$ and ∞, acts regularly on $\mathcal{O} = \{P_t \mid t = 0, \ldots, p^n - 2\}$, and maps P_t to P_{t+1}. Now we consider what a σ_k-transformation means in $PG(n,p)$.

Firstly we consider σ_{n-1}. This takes the first $n-1$ coordinates of the point $P_t = (s_t, s_{t+1}, \ldots, s_{t+n-1}, 1)$ and maps them to $\sum_{i=0}^{n-2} s_{t+i}p^i \in \mathbb{Z}_{p^{n-1}}$. There are p^{n-1} distinct $z_i \in \mathbb{Z}_{p^{n-1}}$ and for each $z_i \neq 0$, there are p points $Z_i = \{P_{t_0}, \ldots, P_{t_{p-1}}\} = \{(s_t, s_{t+1}, \ldots, s_{t+n-2}, \alpha, 1) \mid \alpha \in \mathrm{GF}(p)\}$ which are mapped to z_i by σ_{n-1}. For $z_i = 0$ there are $p-1$ corresponding points in Z_0 since the all-zero state does not occur in an m-sequence.

It is not hard to see that the sets $Z_0 \cup \{\infty\}$, $Z_1, \ldots Z_{p^{n-1}-1}$ form the set of parallel (affine) lines through the point $(0, \ldots, 0, 1, 0) \in \mathcal{H}_\infty$, since Z_i is the set $\{(s_t, \ldots, s_{t+n-2}, \alpha, 1) \mid \alpha \in \mathrm{GF}(p)\}$ for some $(n-1)$-tuple $(s_t, \ldots, s_{t+n-2})$ and this forms a line with $(0, \ldots, 0, 1, 0) \in \mathcal{H}_\infty$ (the line defined by the $n-1$ hyperplanes $x_0 - s_tx_n = 0$, $x_1 - s_{t+1}x_n = 0$, $\ldots$, $x_{n-2} - s_{t+n-2}x_n = 0$). This is precisely the construction given by [28] described in Section 3. For each $Z_i = \{P_{t_0}, \ldots, P_{t_{p-1}}\}$, $i = 1, \ldots, p^{n-1} - 1$, let $D_i = \{t_0, \ldots, t_{p-1}\}$, and for $Z_0 = \{P_{t_0}, \ldots, P_{t_{p-2}}\}$, let $D_0 = \{t_0, \ldots, t_{p-2}\}$. Then the sets D_i form a partition type perfect internal DDF$(p^n; p-1, p, \ldots, p)$ over $\mathbb{Z}_{p^n}$ with $|\mathcal{I}(d)| = p - 1$ for all $d \in \mathbb{Z}_{p^n}^*$.

Similarly, for σ_k, $1 \leq k \leq n-1$, the set of points

$$Z_i = \{(s_t, \ldots, s_{t+n-k-1}, \alpha_1, \ldots, \alpha_k, 1) \mid \alpha_1, \ldots, \alpha_k \in \mathrm{GF}(p)\}$$

corresponding to each $z_i \in \mathbb{Z}_{p^k}$ form an $(n-k)$-dimensional subspace and the set of Z_i forms a parallel class. These are the constructions of [28, Lemma 3.1, 3.2].

Example 4.1 *Let $S = (s_t)$ be an m-sequence over* GF(3) *satisfying the linear recurrence relation $x_{t+3} = 2x_t + x_{t+2}$. The state update matrix is therefore*

$$C = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

The impulse response sequence is $S = (00111021121010022201221202)$*, and the* σ_3*-,* σ_2*- and* σ_1*-transformations give*

P_t	$s(t,3)$	$\sigma_3(s(t,3))$	$s(t,2)$	$\sigma_2(s(t,2))$	$s(t,1)=\sigma_1(s(t,1))$
P_0	001	9	00	0	0
P_1	011	12	01	3	0
P_2	111	13	11	4	1
P_3	110	4	11	4	1
P_4	102	19	10	1	1
P_5	021	15	02	6	0
P_6	211	14	21	5	2
P_7	112	22	11	4	1
P_8	121	16	12	7	1
P_9	210	5	21	5	2
P_{10}	101	10	10	1	1
P_{11}	010	3	01	3	0
P_{12}	100	1	10	1	1
P_{13}	002	18	00	0	0
P_{14}	022	24	02	6	0
P_{15}	222	26	22	8	2
P_{16}	220	8	22	8	2
P_{17}	201	11	20	2	2
P_{18}	012	21	01	3	0
P_{19}	122	25	12	7	1
P_{20}	221	17	22	8	2
P_{21}	212	23	21	5	2
P_{22}	120	7	12	7	1
P_{23}	202	20	20	2	2
P_{24}	020	6	02	6	0
P_{25}	200	2	20	2	2

Writing this in $PG(3,3)$, $P_t = (s_t, s_{t+1}, s_{t+2}, 1)$*, and* $\mathcal{H}_\infty$ *is the hyperplane* $x_3 = 0$*, and* ∞ *is the point* $(0,0,0,1)$*. The projectivity* τ *maps* P_t *to* P_{t+1}*, where* τ *is represented by the matrix* A*,*

$$A = \begin{pmatrix} 0 & 0 & 2 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

The σ_2 *transformation maps 3 points to every* $z_i \in \mathbb{Z}_9^*$*. These form the affine lines of* $PG(3,3)$ *through the point* $(0,0,1,0)$*. For example, the points* P_1, P_{11}, P_{18} *lie on the line defined by* $x_0 = 0$, $x_1 - x_3 = 0$*. The set* $\{1,11,18\}$ *would be one of the subsets of the difference family. This gives* $Q_0 = \{0,13\}$, $Q_1 = \{1,11,18\}$, $Q_2 = \{5,14,24\}$, $Q_3 = \{4,10,12\}$, $Q_4 = \{2,3,7\}$, $Q_5 = \{8,19,22\}$, $Q_6 = \{17,23,25\}$, $Q_7 = \{6,9,21\}$, $Q_8 = \{15,16,20\}$*.*

The σ_1 *transformation maps 9 points to every* $z_i \in \mathbb{Z}_3^*$*. These form the affine planes of* $PG(3,3)$ *through the point* $(0,0,1,0)$*. For example, the points* P_2, P_3, P_4, P_7, P_8, P_{10}, P_{12}, P_{19}, P_{22} *lie on the plane* $x_0 - x_3 = 0$*. The sets*

$$\begin{aligned} Q_0 &= \{0,1,5,11,13,14,18,24\}, \\ Q_1 &= \{2,3,4,7,8,10,12,19,22\}, \\ Q_2 &= \{6,9,15,16,17,20,21,23,25\} \end{aligned}$$

form a difference family over $\mathbb{Z}_3$*.*

4.3 The other way round?

We see that the m-sequence constructions of [51] gives the projective geometry constructions of [28]. Here we consider how the constructions of [28] relate to m-sequences.

In $PG(n,q)$ we may choose any $n+2$ points (every set of $n+1$ of which are independent) as the *simplex of reference* (there is an automorphism that maps any set of such $n+2$ points to any other set). Hence we may choose the hyperplane $x_n = 0$ (denoted $\mathcal{H}_\infty$) and the point $(0,0,\ldots,0,1)$ (denoted ∞).

Now, consider a projectivity τ represented by an $(n+1)\times(n+1)$ matrix A that fixes $\mathcal{H}_\infty$ and ∞. It must take the form

$$A = \left(\begin{array}{ccccc} & & & & 0 \\ & & C & & \vdots \\ & & & & 0 \\ 0 & \ldots & & 0 & 1 \end{array}\right),$$

and we see that

$$A^i = \left(\begin{array}{ccccc} & & & & 0 \\ & & C^i & & \vdots \\ & & & & 0 \\ 0 & \ldots & & 0 & 1 \end{array}\right).$$

So the order of A is given by the order of C. Let the characteristic polynomial of C be $f(x)$. The order of A is hence the order of $f(x)$.

Consider the action of $\langle\tau\rangle$ on the points of $PG(n,q)\setminus(\mathcal{H}_\infty\cup\infty)$. For $\langle\tau\rangle$ to act transitively on these points A must have order q^n-1, which means that $f(x)$ must be primitive. If we use this $f(x)$ as the characteristic polynomial for an LFSR we generate an m-sequence, as in Section 4.1. For prime fields, this is precisely the construction of [51].

Projectivities in the same conjugacy classes have matrices that are similar and therefore have the same characteristic polynomial. There are $\frac{\phi(q^n-1)}{n}$ primitive polynomials of degree n over GF(q) and this gives the number of conjugacy classes of projectivities fixing $\mathcal{H}_\infty$ and ∞ and acting transitively on the points of $PG(n,q)\setminus(\mathcal{H}_\infty\cup\infty)$.

For a particular $\langle\tau\rangle$ with characteristic polynomial $f(x)$ and difference family $\{Q_0,\ldots,Q_{q^{n-1}-1}\}$, there are q^n-1 choices for the point P_0 to be designated 0 in the construction described in Section 3. Each choice gives Q_i+d for each Q_i, $i=1,\ldots,q^{n-1}-1$, $d\in\mathbb{Z}^*_{q^n-1}$. This corresponds to the q^n-1 shifts of the m-sequence generated by the LFSR with characteristic polynomial $f(x)$. The choice of parallel class (the point $P_\infty\in\mathcal{H}_\infty$) gives the difference family $\{Q_i+d\ :\ d\in\mathbb{Z}_{q^n-1}, i=1,\ldots,q^{n-1}-1\}$. (There are $q-1$ values of d such that $\{Q_i+d\}=\{Q_i\}$.) This corresponds to a permutation of symbols and a shift of the m-sequence. If the set of shifts of an m-sequence is considered as a cyclic code over GF(q) then this gives equivalent codes (more on this in Section 5). The group $\langle\tau\rangle$ has $\phi(q^n-1)$ generators, and each of the generators τ^i, $(i,q^n-1)=1$ corresponds to a multiplier w such that $\{wQ_i\ :\ i=1,\ldots,q^{n-1}-1\}=\{Q_i\ :\ i=1,\ldots,q^{n-1}-1\}$.

We have described this correspondence in terms of the lines of $PG(n,q)$ but this also applies to the correspondence between higher dimensional subspaces and the σ_k-transformations.

Example 4.2 *In $PG(3,3)$, the group of perspectivities generated by τ, represented by the matrix*

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

fixes the plane $x_3 = 0$ and fixes the point $\infty = (0,0,0,1)$. An affine point $(x,y,z,1)$ is mapped to the point $(y,x+z,y+z,1)$ and a plane $[a,b,c,d]$ is mapped to the plane $[a+b-c,a,-a+c,d]$. Taking the point $(1,0,0,1)$

as 0*, we have the affine lines through* $P_\infty = (1,0,0,0)$ *in* $x_3 = 0$ *as*

$$\begin{array}{lll}
Q_0 = \{0,13\}, & Q_1 = \{1,19,4\}, & Q_2 = \{2,22,23\}, \\
Q_3 = \{3,5,12\}, & Q_4 = \{6,14,17\}, & Q_5 = \{7,11,21\}, \\
Q_6 = \{8,24,20\}, & Q_7 = \{9,10,15\}, & Q_8 = \{16,18,25\}.
\end{array}$$

If we consider the action of τ^5*, we have*

$$\begin{array}{ll}
Q'_0 = \{0,13\} = Q_0 \times 7, & Q'_1 = \{6,9,21\} = Q_3 \times 7, \\
Q'_2 = \{16,20,15\} = Q_4 \times 7, & Q'_3 = \{11,1,18\} = Q_7 \times 7, \\
Q'_4 = \{22,8,19\} = Q_8 \times 7, & Q'_5 = \{17,23,25\} = Q_5 \times 7, \\
Q'_6 = \{12,10,4\} = Q_6 \times 7, & Q'_7 = \{2,3,7\} = Q_1 \times 7, \\
Q'_8 = \{24,14,5\} = Q_2 \times 7. &
\end{array}$$

If we choose a different parallel class, say, $P'_\infty = (0,0,1,0)$*, we will instead have*

$$\begin{array}{lll}
Q''_0 = \{10,23\}, & Q''_1 = \{1,24,16\}, & Q''_2 = \{2,0,9\}, \\
Q''_3 = \{3,14,11\}, & Q''_4 = \{4,8,18\}, & Q''_5 = \{5,17,21\}, \\
Q''_6 = \{6,7,12\}, & Q''_7 = \{13,15,22\}, & Q''_8 = \{19,20,25\},
\end{array}$$

and $\{Q'_0,\ldots,Q'_8\} = \{Q_0+10,\ldots,Q_8+10\}$.

The characteristic polynomial of A *is* $f(x) = x^3 - x^2 - 2x - 2$*. Using* $f(x)$ *as the characteristic polynomial of an LFSR we have the update matrix* C *as*

$$C = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 2 \\ 0 & 1 & 1 \end{pmatrix}.$$

Using the process described in Section 4.2, we obtain (with $(0,0,1,1)$ *as* 0*) the difference family* $\{Q_i - 1 \ : \ i = 0,\ldots 8\}$.

It is clear from this correspondence that the m-sequence constructions of [51] also works over a non-prime field. The σ_k transform is essentially assigning a unique symbol to each k-tuple from the initial m-sequence.

5 Equivalence of FH sequences

In [28], Fuji-Hara *et al.* stated "Often we are interested in properties of FH sequences, such as auto-correlation, randomness and generating method, which remain unchanged when passing from one FH sequence to another that is essentially the same. Providing an exact definition for this concept and enumerating how many non 'essentially the same' FH sequences are also interesting problems deserving of attention." Here we discuss the notion of equivalence of FH sequences.

Firstly we adopt the notation of [60] for frequency hopping schemes: An (n,M,q)-frequency hopping scheme (FHS) $\mathcal{F}$ is a set of M words of length n over an alphabet of size q. Each word is an FH sequence.

Elements of the symmetric group S_n can act on $\mathcal{F}$ by permuting the coordinate positions of each word in $\mathcal{F}$. Let ρ_n denote the permutation $\begin{pmatrix}1 & 2 & \cdots & n\end{pmatrix} \in S_n$. We say that an element of S_n is a *rotation* if it belongs to $\langle \rho_n \rangle$, the subgroup generated by ρ_n.

Example 5.1 *Consider the* $(7,1,2)$*-FHS* $\mathcal{F}$ *consisting of the single word* $(0,0,0,1,0,1,1)$*. We have* $(0,0,0,1,0,1,1)^{\rho_7} = (1,0,0,0,1,0,1)$.

Definition 5.2 *Let* Q *be a finite alphabet. Given a set* $S \subseteq Q^n$ *we define the* rotational closure *of* S *to be the set*

$$\overset{\Leftrightarrow}{S} = \{\mathbf{w}^\sigma \mid \mathbf{w} \in S,\ \sigma \in \langle \rho_n \rangle\}.$$

If $\overset{\Leftrightarrow}{S} = S$ *then we say that* S *is* rotationally closed*.*

Example 5.3 *Consider again the binary $(7,1,2)$-FHS $\mathcal{F}$ consisting of the single word $(0,0,0,1,0,1,1)$. Its rotational closure is the orbit of the word $(0,0,0,1,0,1,1)$ under the action by the subgroup $\langle \rho_7 \rangle$:*

$$\begin{aligned}\overset{\Leftrightarrow}{\mathcal{F}} = \{ \quad & (0,0,0,1,0,1,1),\\ & (1,0,0,0,1,0,1),\\ & (1,1,0,0,0,1,0),\\ & (0,1,1,0,0,0,1),\\ & (1,0,1,1,0,0,0),\\ & (0,1,0,1,1,0,0),\\ & (0,0,1,0,1,1,0)\}.\end{aligned}$$

If $\mathcal{F}$ is a FHS then $\overset{\Leftrightarrow}{\mathcal{F}}$ is precisely the set of sequences available to users for selecting frequencies. An important property of a FHS is the Hamming correlation properties of the sequences in $\mathcal{F}$.

Let $\mathcal{F}$ be an (n, M, q)-FHS and let $\mathbf{x} = (x_0, \ldots, x_{n-1})$, $\mathbf{y} = (y_0, \ldots, y_{n-1}) \in \mathcal{F}$. The Hamming correlation $H_{\mathbf{x},\mathbf{y}}(t)$ at relative time delay t, $0 \leq t < n$, between $\mathbf{x}$ and $\mathbf{y}$ is

$$H_{\mathbf{x},\mathbf{y}}(t) = \sum_{i=0}^{n-1} h(x_i, y_{i+t}),$$

where

$$h(x,y) = \begin{cases} 1 & \text{if } x = y, \\ 0 & \text{if } x \neq y. \end{cases}$$

Note that the operations on indices are performed modulo n. If $\mathbf{x} = \mathbf{y}$ then $H_{\mathbf{x}}(t) = H_{\mathbf{x},\mathbf{x}}(t)$ is the Hamming auto-correlation. The maximum out-of-phase Hamming auto-correlation of $\mathbf{x}$ is

$$H(\mathbf{x}) = \max_{1 \leq t < n} \{H_{\mathbf{x}}(t)\}$$

and the maximum Hamming cross-correlation between any two distinct FH sequences $\mathbf{x}$, $\mathbf{y}$ is

$$H(\mathbf{x},\mathbf{y}) = \max_{0 \leq t < n} \{H_{\mathbf{x},\mathbf{y}}(t)\}.$$

We define the maximum Hamming correlation of an (n, M, q)-FHS $\mathcal{F}$ as

$$M(\mathcal{F}) = \max_{\mathbf{x},\mathbf{y} \in \mathcal{F}} \{H(\mathbf{x}), H(\mathbf{y}), H(\mathbf{x},\mathbf{y})\}.$$

Theorem 5.4 *Let $\mathbf{w} \in Q^n$. The maximum out-of-phase Hamming auto-correlation $H(\mathbf{w})$ of $\mathbf{w}$ is equal to $n - d$, where d is the minimum (Hamming) distance of $\overset{\Leftrightarrow}{\mathbf{w}}$.*

Theorem 5.5 *Let $\mathcal{F}$ be an (n, M, q)-FHS. The minimum distance of $\overset{\Leftrightarrow}{\mathcal{F}}$ is equal to $n - M(\mathcal{F})$.*

The proofs of these theorems are trivial, but the theorems suggest that taking the rotational closure of a frequency hopping sequence allows us to work with the standard notion of Hamming distance in place of the Hamming correlation.

Theorem 5.6 *Let $\mathbf{w} \in Q^n$. If $|\overset{\Leftrightarrow}{\mathbf{w}}| < n$ then $H(\mathbf{w}) = n$.*

Proof: We observe that $|\overset{\Leftrightarrow}{\mathbf{w}}|$ is the size of the orbit of $\mathbf{w}$ under the action of the subgroup $\langle \rho_n \rangle$, which has order n. By the orbit-stabiliser theorem, if $|\overset{\Leftrightarrow}{\mathbf{w}}| < n$ then the stabiliser of $\mathbf{w}$ is nontrivial. That is, there is some (non-identity) rotation that maps $\mathbf{w}$ onto itself. This implies that its maximum out-of-phase Hamming auto-correlation is n. □

In other words, unless a given sequence of length n has worst possible Hamming auto-correlation, its rotational closure always has size n.

The following lemma is also straightforward to prove:

Lemma 5.7 Let $\mathbf{w} \in Q^n$. If $|\overset{\Leftrightarrow}{\mathbf{w}}| < n$ then for $i = 0, 1, \ldots, n-1$ we have $\overset{\Leftrightarrow}{\mathbf{w}^{\rho_n^i}} = \overset{\Leftrightarrow}{\mathbf{w}}$. □

In coding theory, two codes are equivalent if one can be obtained from the other by a combination of applying an arbitrary permutation to the alphabet symbols in a particular coordinate position and/or permuting the coordinate positions of the codewords. These are transformations that preserve the Hamming distance between any two codewords. In the case of frequency hopping sequences, it is the maximum Hamming correlation that we wish to preserve. This is a stronger condition, and hence the set of transformations that are permitted in the definition of equivalence will be smaller. For example, we can no longer apply different permutations to the alphabet in different coordinate positions, as that can alter the out-of-phase Hamming correlations. Because the rotation of coordinate positions is inherent to the definition of Hamming correlation, if we wish to permute the alphabet symbols then we must apply the same permutation to the symbols in each coordinate position. Similarly, not all permutations of coordinates preserve the out-of-phase Hamming auto-correlation of a sequence.

Example 5.8 *Consider the sequence* $(0, 0, 0, 1, 0, 1, 1)$*. Its maximum out-of-phase Hamming auto-correlation is 3. However, if we swap the first and last column we obtain the sequence* $(1, 0, 0, 1, 0, 1, 0)$*, which has maximum out-of-phase Hamming auto-correlation 5.*

However, we can use the notion of rotational closure to determine an appropriate set of column permutations that will preserve Hamming correlation. Recall that for a given word, its out-of-phase Hamming auto-correlation is uniquely determined by the minimum distance of its rotational closure. Now, any permutation of coordinates preserves Hamming distance, so if we can find a set of permutations that preserve the property of being rotationally closed, then these will in turn preserve the out-of-phase Hamming auto-correlation of individual sequences.

Suppose a word $\mathbf{w}$ of length n has $H(\mathbf{w}) < n$. Then its rotational closure consists of the elements

$$\overset{\Leftrightarrow}{\mathbf{w}} = \{\mathbf{w}, \mathbf{w}^{\rho_n}, \mathbf{w}^{\rho_n^2}, \ldots, \mathbf{w}^{\rho_n^{n-1}}\}.$$

Applying a permutation $\gamma \in S_n$ to the coordinates of these words gives the set

$$\left(\overset{\Leftrightarrow}{\mathbf{w}}\right)^{\gamma} = \{\mathbf{w}^{\gamma}, \mathbf{w}^{\rho_n\gamma}, \mathbf{w}^{\rho_n^2\gamma}, \ldots, \mathbf{w}^{\rho_n^{n-1}\gamma}\}.$$

We wish to establish conditions on γ that ensure that $\left(\overset{\Leftrightarrow}{\mathbf{w}}\right)^{\gamma}$ is itself rotationally closed.

Theorem 5.9 *Suppose* $\mathbf{w} \in Q^n$ *has out-of-phase Hamming auto-correlation less than* n*. Then* $\left(\overset{\Leftrightarrow}{\mathbf{w}}\right)^{\gamma}$ *is rotationally closed if and only if* $\gamma \in N_{S_n}(\langle\rho_n\rangle)$*, that is* γ *is an element of the normaliser of* $\langle\rho_n\rangle$ *in* S_n*.*

Proof: Suppose $\gamma \in N_{S_n}(\langle\rho_n\rangle)$. Then $\gamma\langle\rho_n\rangle\gamma^{-1} = \langle\rho_n\rangle$. This implies that

$$\overset{\Leftrightarrow}{\mathbf{w}} \;=\; \{\mathbf{w}^{\gamma\rho_n^i\gamma^{-1}} \mid i = 0, 1, 2, \ldots, n-1\},$$

and so

$$\begin{aligned} \left(\overset{\Leftrightarrow}{\mathbf{w}}\right)^{\gamma} &= \{\mathbf{w}^{\gamma\rho_n^i} \mid i = 0, 1, 2, \ldots, n-1\} \\ &= \overset{\Leftrightarrow}{\mathbf{w}^{\gamma}}. \end{aligned}$$

Conversely, if $\left(\overset{\Leftrightarrow}{\mathbf{w}}\right)^{\gamma}$ is rotationally closed, then

$$\begin{aligned} \left(\overset{\Leftrightarrow}{\mathbf{w}}\right)^{\gamma} &= \{\mathbf{w}^{\gamma}, \mathbf{w}^{\rho_n\gamma}, \mathbf{w}^{\rho_n^2\gamma}, \ldots, \mathbf{w}^{\rho_n^{n-1}\gamma}\} \\ &= \{\mathbf{w}', \mathbf{w}'^{\rho_n}, \mathbf{w}'^{\rho_n^2}, \ldots, \mathbf{w}'^{\rho_n^{n-1}}\}, \end{aligned}$$

where $\mathbf{w}' = \mathbf{w}^{\rho_n^i\gamma}$ for some i. So we have

$$\left(\overset{\Leftrightarrow}{\mathbf{w}}\right)^{\gamma} = \{\mathbf{w}^{\rho_n^i\gamma}, \mathbf{w}^{\rho_n^i\gamma\rho_n}, \mathbf{w}^{\rho_n^i\gamma\rho_n^2}, \dots, \mathbf{w}^{\rho_n^i\gamma\rho_n^{n-1}}\}.$$

This means that $\mathbf{w}^{\gamma} = \mathbf{w}^{\rho_n^i\gamma\rho_n^j}$ for some j, and so $\mathbf{w}^{\gamma\rho_n^{-j}\gamma^{-1}} = \mathbf{w}^{\rho_n^i}$. Clearly this applies to all i, j, and we have $\gamma \in N_{S_n}(\langle\rho_n\rangle)$. □

Example 5.10 *Consider the permutation* $\gamma = \begin{pmatrix}2 & 5 & 3\end{pmatrix}\begin{pmatrix}4 & 6 & 7\end{pmatrix} \in S_7$. *We have* $\gamma^{-1} = \begin{pmatrix}2 & 3 & 5\end{pmatrix}\begin{pmatrix}4 & 7 & 6\end{pmatrix}$, *and*

$$\begin{aligned}\gamma\rho_7\gamma^{-1} &= \begin{pmatrix}2 & 5 & 3\end{pmatrix}\begin{pmatrix}4 & 6 & 7\end{pmatrix}\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7\end{pmatrix}\begin{pmatrix}2 & 3 & 5\end{pmatrix}\begin{pmatrix}4 & 7 & 6\end{pmatrix}\\ &= \begin{pmatrix}1 & 3 & 5 & 7 & 2 & 4 & 6\end{pmatrix}\\ &= \rho_7^2.\end{aligned}$$

Since ρ_7^2 *generates* $\langle\rho_7\rangle$ *this shows that* $\gamma \in N_{S_7}(\langle\rho_7\rangle)$.

Now consider the word (A, B, C, D, E, F, G). *The rows of the following matrix give its rotational closure:*

$$\begin{bmatrix} A & B & C & D & E & F & G\\ G & A & B & C & D & E & F\\ F & G & A & B & C & D & E\\ E & F & G & A & B & C & D\\ D & E & F & G & A & B & C\\ C & D & E & F & G & A & B\\ B & C & D & E & F & G & A \end{bmatrix}.$$

If we apply γ *to the columns of this matrix, we obtain*

$$\begin{bmatrix} A & C & E & G & B & D & F\\ G & B & D & F & A & C & E\\ F & A & C & E & G & B & D\\ E & G & B & D & F & A & C\\ D & F & A & C & E & G & B\\ C & E & G & B & D & F & A\\ B & D & F & A & C & E & G \end{bmatrix},$$

which is easily seen to be the rotational closure of any of its rows.

We now look at applying these ideas to the sequence $(0, 0, 0, 1, 0, 1, 1)$. *Permuting its coordinates with* γ *in fact yields* $(0, 0, 0, 1, 0, 1, 1)$, *which is trivially equivalent to the original sequence. Less trivially,* $\begin{pmatrix}2 & 4 & 3 & 7 & 5 & 6\end{pmatrix}$ *is another example of an element of the normaliser of* $\langle\rho_7\rangle$, *and applying this permutation to the coordinates yields the sequence* $(0, 1, 1, 0, 1, 0, 0)$. *This is an example of an 'equivalent' frequency hopping sequence that is not simply a rotation of the original sequence.*

Definition 5.11 *We say that two* (n, M, q)*-FHSs are* equivalent *if one can be obtained from the other by a combination of permuting the symbols of the underlying alphabet and/or applying to the coordinates of its sequences any permutation that is an element of* $N_{S_n}(\langle\rho_n\rangle)$.

Equivalent FHSs have the same maximum Hamming correlation.

5.1 Comparison with the notion of equivalence for DDFs

Two distinct difference families are said to be equivalent if there is an isomorphism between the underlying groups that maps one DDF onto a translation of the other. In Section 2.1 we discussed the correspondence between a partition type DDF and an FHS. In fact, we will see that two partition type DDFs over $\mathbb{Z}_n$ are equivalent in this sense if and only if the corresponding FHSs are equivalent in the sense of Definition 5.11. We begin by noting that the automorphism group of $\mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_n^*$. As in Section 5 let $\rho_n \in S_n$ be the permutation $\begin{pmatrix}1 & 2 & \cdots & n\end{pmatrix}$. Any element $\gamma \in N_{S_n}(\langle \rho_n \rangle)$ induces a map $\phi_\gamma \colon \mathbb{Z}_n \to \mathbb{Z}_n$ by sending $i \in \mathbb{Z}_n$ to the unique element $j \in \mathbb{Z}_n$ for which $\gamma^{-1}\rho_n^i\gamma = \rho^j$. The map ϕ_γ is a homomorphism, since if $\phi_\gamma(i_1) = j_1$ and $\phi_\gamma(i_2) = j_2$ then $\gamma^{-1}\rho_n^{i_1+i_2}\gamma = \gamma^{-1}\rho_n^{i_1}\gamma\gamma^{-1}\rho_n^{i_2}\gamma = \rho_n^{j_1}\rho_n^{j_2} = \rho_n^{j_1+j_2}$, so $\phi_\gamma(i_1 + i_2) = \phi_\gamma(i_1) + \phi_\gamma(i_2)$; in fact it is an automorphism. Every automorphism of $\langle \rho_n \rangle$ can be obtained in this fashion.

Theorem 5.12 *Let $\mathcal{F}$ be a length n FHS consisting of a single word, and let $\mathcal{D}$ be the corresponding partition type* DDF *over $\mathbb{Z}_n$. Then the FHS obtained by applying a permutation $\gamma \in N_{S_n}(\langle \rho_n \rangle)$ to the coordinate positions of $\mathcal{F}$ corresponds to a* DDF *that is a translation of the* DDF *obtained from $\mathcal{D}$ by applying the automorphism ϕ_γ to the elements of $\mathbb{Z}_n$.*

Proof: It is straightforward to verify that $\gamma^{-1}\rho_n\gamma$ is the cycle $\begin{pmatrix}1^\gamma & 2^\gamma & \ldots & n^\gamma\end{pmatrix}$. For $\gamma \in N_{S_n}(\langle \rho_n \rangle)$ this is equal to ρ_n^k for some k. It follows that for $i = 1, 2, \ldots, n-1$ we have

$$(i+1)^\gamma = i^\gamma + k. \tag{3}$$

The correspondence between $\mathcal{F}$ and $\mathcal{D}$ is obtained by associating positions in the sequence with elements of $\mathbb{Z}_n$. For example, the FHS $\mathcal{F} = (1,1,2,3,2)$ corresponds to the DDF $(\mathbb{Z}_5; \{0,1\}, \{2,4\}, \{3\})$:

$$\begin{array}{c|ccccc} \mathbb{Z}_5 & 0 & 1 & 2 & 3 & 4 \\ \hline \mathcal{F} & 1 & 1 & 2 & 3 & 2 \end{array}.$$

We observe that in this representation, the $i + 1^{\text{th}}$ element of the sequence $\mathcal{F}$ is in correspondence with the element $i \in \mathbb{Z}_n$. If we apply γ to the positions of $\mathcal{F}$, then the entry in the $j+1^{\text{th}}$ position is mapped to the $i+1^{\text{th}}$ position when $(j+1)^\gamma = i+1$. Repeatedly applying the relation in (3) tells us that in this case we have $i + 1 = 1^\gamma + jk$, so $i = (1^\gamma - 1) + jk$.

If we apply ϕ_γ to $\mathbb{Z}_n$ then element $j \in \mathbb{Z}_n$ is replaced by element i when $\gamma^{-1}\rho_n^j\gamma = \rho^i$. But we have that

$$\begin{aligned} \gamma^{-1}\rho_n^j\gamma &= (\gamma^{-1}\rho_n\gamma)^j \\ &= (\rho_n^k)^j \\ &= \rho_n^{kj}, \end{aligned}$$

so it must be the case that $i = kj$. It follows that if we then translate this DDF by adding $1^\gamma - 1$ to each element of $\mathbb{Z}$ we obtain the same overall transformation that was effected by applying γ to $\mathcal{F}$. □

Example 5.13 *For example, let $\gamma = \begin{pmatrix}1 & 5 & 3 & 4\end{pmatrix} \in N_{S_5}(\langle \rho_5 \rangle)$. Applying γ to $\mathcal{F} = (1,1,2,3,2)$ we have*

$$\begin{array}{c|ccccc} \mathbb{Z}_5 & 0 & 1 & 2 & 3 & 4 \\ \hline \mathcal{F}^\gamma & 3 & 1 & 2 & 2 & 1 \end{array},$$

with resulting FHS $(3,1,2,2,1)$ and corresponding DDF *$(\mathbb{Z}_5; \{0\}, \{1,4\}, \{2,3\})$. We observe that $1^\gamma = 5$, so that $1^\gamma - 1 = 4$. Alternatively, we note that $\gamma^{-1}\rho_5\gamma = \begin{pmatrix}1 & 3 & 5 & 2 & 4\end{pmatrix} = \rho_5^2$. Hence ϕ_γ gives*

$$\begin{array}{c|ccccc} \phi_\gamma(\mathbb{Z}_5) & 0 & 2 & 4 & 1 & 3 \\ \hline \mathcal{F} & 1 & 1 & 2 & 3 & 2 \end{array},$$

which we can rewrite in order as

$$\begin{array}{c|ccccc} \phi_\gamma(\mathbb{Z}_5) & 0 & 1 & 2 & 3 & 4 \\ \hline \mathcal{F} & 1 & 3 & 1 & 2 & 2 \end{array}.$$

The resulting FHS is $(1,3,1,2,2)$, which is simply a cyclic shift of the one obtained previously. The DDF *is $(\mathbb{Z}_5; \{1\}, \{0,2\}, \{3,4\})$. If we add 4 to each element, we recover the previous* DDF.

6 Conclusion

We have given a general definition of a disjoint difference family, and have seen a range of examples of applications in communications and information security for these difference families, with different applications placing different constraints on the associated properties and parameters. Focusing on the case of FHSs and their connection with partition type disjoint difference families, we have shown that a construction due to Fuji-Hara *et al.* [28] gives rise to precisely the same disjoint difference families as an earlier construction of Lempel and Greenberger [51], thus answering an open question in [28]. In response to the question of Fuji-Hara *et al.* as to when two FHSs can be considered to be "essentially the same" we have established a notion of equivalence of frequency hopping schemes. FHSs based on a single sequence correspond to partition type disjoint difference families, and in this case we have shown that our definition of equivalence corresponds to an established notion of equivalence for difference families, although our definition also applies more generally to schemes based on more than one sequence.

References

[1] H. Ahmadi and R. Safavi-Naini. Detection of algebraic manipulation in the presence of leakage. In C. Padró, editor, *Information Theoretic Security: 7th International Conference, ICITS 2013, Proceedings*, volume 8317 of *Lecture Notes in Computer Science*, pages 238–258. Springer, 2013.

[2] I. Anderson and N. J. Finizio. Whist tournaments. In C. J. Colbourn and J. H. Dinitz, editors, *Handbook of Combinatorial Designs*, chapter 64, pages 663–668. Chapman and Hall/CRC, Boca Raton, FL, 2007.

[3] T. Araki and S. Obana. Flaws in some secret sharing schemes against cheating. In J. Pieprzyk, H. Ghodosi and E. Dawson, editors, *Information Security and Privacy, 12th Australasian Conference, ACISP 2007, Townsville, Australia, July 2-4, 2007, Proceedings*, volume 4586 of *Lecture Notes in Computer Science*, pages 122–132. Springer, 2007.

[4] J. Bao and L. Ji. New families of optimal frequency hopping sequence sets. *CoRR*, abs/1506.07372, 2015.

[5] S. Bitan and T. Etzion. Constructions for optimal constant weight cyclically permutable codes and difference families. *IEEE Transactions on Information Theory*, 41(1):77–87, 1995.

[6] S. R. Blackburn. Non-overlapping codes. *IEEE Transactions on Information Theory*, 61(9):4890–4894, Sept 2015.

[7] C. Blundo, A. De Santis, K. Kurosawa and W. Ogata. On a fallacious bound for authentication codes. *Journal of cryptology*, 12(3):155–159, 1999.

[8] A. Broadbent and A. Tapp. Information-theoretic security without an honest majority. In K. Kurosawa, editor, *Advances in Crypotology: 13th International Conference on Theory and Application of Cryptology and Information Security, ASIACRYPT 2007, Proceedings*, volume 4833 of *Lecture Notes in Computer Science*, pages 410–426. Springer, 2007.

[9] S. Cabello, C. Padró and G. Sáez. Secret sharing schemes with detection of cheaters for a general access structure. *Designs, Codes and Cryptography*, 25(2):175–188, 2002.

[10] H. Cao and R. Wei. Combinatorial constructions for optimal two-dimensional optical orthogonal codes. *IEEE Transactions on Information Theory*, 55(3):1387–1394, March 2009.

[11] W. Chu and C. J. Colbourn. Optimal frequency-hopping sequences via cyclotomy. *IEEE Transactions on Information Theory*, 51(3):1139–1141, March 2005.

[12] F. R. K. Chung, J. A. Salehi and V. K. Wei. Optical orthogonal codes: design, analysis and applications. *IEEE Transactions on Information Theory*, 35(3):595–604, May 1989.

[13] A. L. Churchill. Restrictions and generalizations on comma-free codes. *The Electronic Journal of Combinatorics*, 16(1), 2009. Research Paper R25.

[14] C. J. Colbourn and J. H. Dinitz. *Handbook of Combinatorial Designs (Discrete Mathematics and Its Applications).* Chapman & Hall/CRC, 2nd edition, 2006.

[15] R. Cramer, Y. Dodis, S. Fehr, C. Padró and D. Wichs. Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors. In N. P. Smart, editor, *Advances in Cryptology : 27th International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2008, Proceedings*, volume 4965 of *Lecture Notes in Computer Science*, pages 471–488. Springer, 2008.

[16] R. Cramer, Y. Dodis, S. Fehr, C. Padró and D. Wichs. Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors. *IACR Cryptology ePrint Archive*, 2008:30, 2008.

[17] C. Ding, A. Salomaa, P. Solé and X. Tian. Three constructions of authentication/secrecy codes. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pages 24–33. Springer, 2003.

[18] C. Ding and X. Tian. Three constructions of authentication codes with perfect secrecy. *Designs, Codes and Cryptography*, 33(3):227–239, 2004.

[19] R. Cramer, S. Fehr and C. Padró. Algebraic manipulation detection codes. *Science China Mathematics*, 56(7):1349–1358, 2013.

[20] R. Cramer, C. Padró and C. Xing. Optimal algebraic manipulation detection codes in the constant-error model. In Y. Dodis and J. B. Nielsen, editors, *Theory of Cryptography : 12th Theory of Cryptography Conference, TCC 2015, Proceedings*, volume 9014 of *Lecture Notes in Computer Science*, pages 481–501. Springer, 2015.

[21] P Dai, J. Wang and J. Yin. Combinatorial constructions for optimal 2-D optical orthogonal codes with AM-OPPTS property. *Designs, Codes and Cryptography*, 71(2):315–330, 2014.

[22] C. Ding, R. Fuji-Hara, Y. Fujiwara, M. Jimbo and M. Mishima. Sets of frequency hopping sequences: Bounds and optimal constructions. *IEEE Transactions on Information Theory*, 55(7):3297–3304, July 2009.

[23] C. Ding, Y. Yang and X. Tang. Optimal sets of frequency hopping sequences from linear cyclic codes. *IEEE Transactions on Information Theory*, 56(7):3605–3612, July 2010.

[24] R. C. Dixon. *Spread Spectrum Systems.* Wiley-Blackwell, 2nd edition, 1984.

[25] S. Dziembowski, K. Pietrzak and D. Wichs. Non-malleable codes. In A. C. Yao, editor, *Innovations in Computer Science, ICS 2010, Proceedings*, pages 434–452. Tsinghua University Press, 2010.

[26] Y. Emek and R. Wattenhofer. Frequency hopping against a powerful adversary. In Y. Afek, editor, *Distributed Computing*, volume 8205 of *Lecture Notes in Computer Science*, pages 329–343. Springer Berlin Heidelberg, 2013.

[27] T. Feng and Y. Chang. Combinatorial constructions for optimal two-dimensional optical orthogonal codes with $\lambda = 2$. *IEEE Transactions on Information Theory*, 57(10):6796–6819, Oct 2011.

[28] R. Fuji-Hara, Y. Miao and M. Mishima. Optimal frequency hopping sequences: a combinatorial approach. *IEEE Transactions on Information Theory*, 50(10):2408–2420, Oct 2004.

[29] R. Fuji-Hara, Y. Miao and S. Shinohara. Complete sets of disjoint difference families and their applications. *Journal of Statistical Planning and Inference*, 106(1-2):87-103, August 2002.

[30] Y. Fujiwara and V. D. Tonchev. High-rate self-synchronizing codes. *IEEE Transactions on Information Theory*, 59(4):2328–2335, April 2013.

[31] G. Ge, Y. Miao and L. Wang. Combinatorial constructions for optimal splitting authentication codes. *SIAM Journal on Discrete Mathematics*, 18(4):663–678, 2005.

[32] G. Ge, Y. Miao and Z. Yao. Optimal frequency hopping sequences: Auto- and cross-correlation properties. *IEEE Transactions on Information Theory*, 55(2):867–879, Feb 2009.

[33] S. Ge, Z. Wang, M. Karpovsky and P. Luo. Reliable and secure memories based on algebraic manipulation detection codes and robust error correction. In *Proceedings of the Sixth International Conference on Dependability, DEPEND 2013.*

[34] S. Ge, Z. Wang, P. Luo and M. Karpovsky. Secure memories resistant to both random errors and fault injection attacks using nonlinear error correction codes. In *Proceedings of the 2nd International Workshop on Hardware and Architectural Support for Security and Privacy*, page 5. ACM, 2013.

[35] S. W. Golomb and G. Gong. *Signal design for good correlation: for wireless communication, cryptography, and radar.* Cambridge University Press, 2005.

[36] S. W. Golomb, B. Gordon and L. R, Welch. Comma-free codes. *Canadian Journal of Mathematics*, 10(2):202–209, 1958.

[37] V. Guruswami and A. Smith. Optimal-rate code constructions for computationally simple channels. *CoRR*, abs/1004.4017, 2010.

[38] X. He and A. Yener. Secure communication with a byzantine relay. In *IEEE International Symposium on Information Theory ISIT 2009*, pages 2096–2100. IEEE, 2009.

[39] X. He and A. Yener. Strong secrecy and reliable byzantine detection in the presence of an untrusted relay. *IEEE Transactions on Information Theory*, 59(1):177–192, 2013.

[40] T. Helleseth. Sequence correlation. In C. J. Colbourn and J. H. Dinitz, editors, *Handbook of Combinatorial Designs*, chapter 7, pages 313–317. Chapman and Hall/CRC, Boca Raton, FL, 2007.

[41] J. W. P. Hirschfeld. *Projective Geometries over Finite Fields.* Oxford Mathematical Monographs, 2nd edition, 1998.

[42] H. Hoshino and S. Obana. Almost optimum secret sharing schemes with cheating detection for random bit strings. In K. Tanaka and Y. Suga, editors, *Advances in Information and Computer Security : 10th International Workshop on Security, IWSEC 2015, Proceedings*, volume 9241 of *Lecture Notes in Computer Science*, pages 213–222. Springer, 2015.

[43] M. Huber. Authentication and secrecy codes for equiprobable source probability distributions. In *IEEE International Symposium on Information Theory, ISIT 2009*, pages 1105–1109. IEEE, 2009.

[44] M. Huber. Combinatorial bounds and characterizations of splitting authentication codes. *Cryptography and Communications*, 2(2):173–185, 2010.

[45] M. Huber. Combinatorial designs for authentication and secrecy codes. *Foundations and Trends in Communications and Information Theory*, 5(6):581–675, 2010.

[46] M. Huber. *Combinatorial Designs for Authentication and Secrecy Codes.* Foundations and trends in communications and information theory. Now Publishers, 2010.

[47] M. Huber. Information theoretic authentication and secrecy codes in the splitting model. *CoRR*, abs/1112.0038, 2011.

[48] J. Jiang, D. Wu and P. Fan. General constructions of optimal variable-weight optical orthogonal codes. *IEEE Transactions on Information Theory*, 57(7):4488–4496, July 2011.

[49] M. Karpovsky and Z. Wang. Design of strongly secure communication and computation channels by nonlinear error detecting codes. *IEEE Transactions on Computers*, 63(11):2716–2728, 2014.

[50] K. Kurosawa and S. Obana. Combinatorial bounds on authentication codes with arbitration. *Designs, Codes and Cryptography*, 22(3):265–281, 2001.

[51] A. Lempel and H. H. Greenberger. Families of sequences with optimal Hamming-correlation properties. *IEEE Transactions on Information Theory*, 20(1):90–94, Jan 1974.

[52] V. I. Levenshtein. Combinatorial problems motivated by comma-free codes. *Journal of Combinatorial Designs*, 12(3):184–196, 2004.

[53] M. Liang and B. Du. A new class of splitting 3-designs. *Designs, Codes and Cryptography*, 60(3):283–290, 2011.

[54] M. Liang and B. Du. A new class of 3-fold perfect splitting authentication codes. *Designs, Codes and Cryptography*, 62(1):109–119, 2012.

[55] R. Lidl and H. Niederreiter. *Finite Fields*, volume 20 of *Encyclopedia of Mathematics and its applications.* Cambridge University Press, Cambridge, UK, 2nd edition, 1997.

[56] F. Liu, D. Peng, Z. Zhou and X. Tang. A new frequency-hopping sequence set based upon generalized cyclotomy. *Designs, Codes and Cryptography*, 69(2):247–259, 2013.

[57] P. Luo, A. Y.-L. Lin, Z. Wang and M. Karpovsky. Hardware implementation of secure Shamir's secret sharing scheme. In *IEEE 15th International Symposium on High-Assurance Systems Engineering (HASE) 2014, Proceedings*, pages 193–200. IEEE, 2014.

[58] P. Luo, Z. Wang and M. Karpovsky. Secure NAND flash architecture resilient to strong fault-injection attacks using algebraic manipulation detection code. In *Proceedings of the International Conference on Security and Management (SAM) 2013.* The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2013.

[59] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos and G. Pantziou. A survey on jamming attacks and countermeasures in WSNs. *IEEE Communications Surveys Tutorials*, 11(4):42–56, 2009.

[60] M. Nyirenda, S. L. Ng and K. M. Martin. A combinatorial model of interference in frequency hopping schemes. *CoRR abs/1508.02570*, 2015.

[61] S. Obana. Almost optimum t-cheater identifiable secret sharing schemes. In K. G. Paterson, editor, *Advances in Cryptology : 30th International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2011, Proceedings*, volume 6632 of *Lecture Notes in Computer Science*, pages 284–302. Springer, 2011.

[62] S. Obana and T. Araki. Almost optimum secret sharing schemes secure against cheating for arbitrary secret distribution. In X. Lai and K. Chen, editors, *Advances in Cryptology : 12th International Conference on the Theory and Application of Cryptology and Information Security,ASIACRYPT 2006, Proceedings*, volume 4284 of *Lecture Notes in Computer Science*, pages 364–379. Springer, 2006.

[63] S. Obana and K. Kurosawa. Bounds and combinatorial structure of (k, n) multi-receiver A-codes. *Designs, Codes and Cryptography*, 22(1):47–63, 2001.

[64] S. Obana and K. Tsuchida. Cheating detectable secret sharing schemes supporting an arbitrary finite field. In M. Yoshida and K. Mouri, editors, *Advances in Information and Computer Security : 9th International Workshop on Security, IWSEC 2014, Proceedings*, volume 8639 of *Lecture Notes in Computer Science*, pages 88–97. Springer, 2014.

[65] W. Ogata, K. Kurosawa and D. R. Stinson. Optimum secret sharing scheme secure against cheating. *SIAM Journal of Discrete Mathematics*, 20(1):79–95, 2006.

[66] W. Ogata, K. Kurosawa, D. R. Stinson and H. Saido. New combinatorial designs and their applications to authentication codes and secret sharing schemes. *Discrete Mathematics*, 279(13):383–405, 2004. In Honour of Zhu Lie.

[67] M. B. Paterson and D. R. Stinson. Combinatorial characterizations of algebraic manipulation detection codes involving generalized difference families. *CoRR abs/1506.02711*, 2015.

[68] D. Pei. *Authentication Codes and Combinatorial Designs.* Discrete Mathematics and Its Applications. CRC Press, 2006.

[69] D. Peng and P. Fan. Lower bounds on the hamming auto- and cross correlations of frequency-hopping sequences. *IEEE Transactions on Information Theory*, 50(9):2149–2154, Sept 2004.

[70] A. Pott, V. Kumaran, T. Helleseth, and D. Jungnickel. *Difference Sets, Sequences and their Correlation Properties*. Nato Science Series C:. Springer Netherlands, 1999.

[71] D. V. Sarwate. Optimum PN sequences for CDMA systems. In S. G. Glisic, P. A. Leppänen, editors, *Code Division Multiple Access Communications*, pages 53–78. Springer US, 1995.

[72] D. R. Stinson and R. Wei. Bibliography on authentication codes. http://cacr.uwaterloo.ca/ dstinson/acbib.html, 1998.

[73] M. Tompa and H. Woll. How to share a secret with cheaters. *Journal of Cryptology*, 1(2):133–138, 1988.

[74] V. D. Tonchev. Difference systems of sets and code synchronization. *Rendiconti del Seminario Matematico di Messina Series II*, 9:217226, 2003.

[75] J. Wang. A new class of optimal 3-splitting authentication codes. *Designs, Codes and Cryptography*, 38(3):373–381, 2006.

[76] J. Wang and R. Su. Further results on the existence of splitting BIBDs and application to authentication codes. *Acta applicandae mathematicae*, 109(3):791–803, 2010.

[77] P. Wang and R. Safavi-Naini. An efficient code for adversarial wiretap channel. In *IEEE Information Theory Workshop (ITW) 2014*, pages 40–44. IEEE, 2014.

[78] Z. Wang and M. Karpovsky. New error detecting codes for the design of hardware resistant to strong fault injection attacks. In *Proceedings of the International Conference on Security and management ((SAM) 2012*. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2012.

[79] Z. Wang and M. G. Karpovsky. Algebraic manipulation detection codes and their applications for design of secure cryptographic devices. In *17th IEEE International On-Line Testing Symposium (IOLTS 2011), Proceedings*, pages 234–239. IEEE, 2011.

[80] B. Wen. Construction of optimal sets of frequency hopping sequences. *ISRN Combinatorics*, 2013(Article ID 479408), 2013.

[81] T. Xia and B. Xia. Quasi-cyclic codes from extended difference families. In *Proceedings of the IEEE Wireless Communications and Networking Conference*, pages 1036–1040. IEEE, 2005.

[82] W. Xu, W. Trappe, Y. Zhang and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, MobiHoc '05, pages 46–57, New York, NY, USA, 2005. ACM.

[83] N. Y. Yu and N. Zhao. Deterministic construction of real-valued ternary sensing matrices using optical orthogonal codes. *IEEE Signal Processing Letters*, 20(11):1106–1109, Nov 2013.