

A selection of divisible lexicographic codes

Harold N. Ward

Department of Mathematics,
University of Virginia,
Charlottesville, VA 22904, USA
E-mail: hnw@virginia.edu

Abstract: This paper presents a selection of lexicographic codes over a prime field \mathbb{F}_p , codes constructed so as to be linear and to have a prescribed minimum distance and divisor. The development of the code when the minimum distance is $3p$ and the divisor is p leads to questions involving the distribution of quadratic residues and non-residues modulo p . In the course of events, the Hall plane $H(p)$ emerges. This paper is dedicated to Vera Pless on the occasion of her retirement. She was in the audience when I presented a sketchy version of the material at a conference at Lehigh University many years ago. In my enthusiasm, I promised her a paper on the subject – and here it is, at last!

Keywords: lexicographic code; divisible code; quadratic residue; spread; translation plane; Hall plane; Griesmer bound.

Reference to this paper should be made as follows: Ward, H.N. (2010) 'A selection of divisible lexicographic codes', *Int. J. Information and Coding Theory*, Vol. 1, No. 4, pp.410–428.

Biographical notes: Harold N. Ward retired as a Professor Emeritus from the University of Virginia in 2007. He had taught there since 1967 after teaching at Brown University for five years. He was a student of Richard Brauer at Harvard University, earning his PhD in 1962.

1 Introduction

Lexicographic codes were introduced by Levenšteĭn (1960) as an application of a constructive algorithm due to V.I. Siforov. They were elaborated on considerably by Conway and Sloane (1986) in their prizewinning paper, in which they related them to impartial games. Later, Brualdi and Pless (1993) studied codes constructed from greedy algorithms more general than those dictated by lexicographic choices. The procedure is to order words in some way and specify a collection of properties the codes are to have, such as prescribed minimum distance. Then codes are produced by augmenting the code in hand at a particular step by the least word not used so far that makes the augmented code still satisfy the properties. A major result of the cited papers is that under fairly general conditions, the codes produced are linear.

A *divisible code* is a linear code in which all the word weights are multiples of a given divisor; the paper (Ward, 2001) provides a fairly recent survey of some of the features of divisible codes. In this paper, we shall take as the properties governing the codes both a

prescribed minimum weight and a selected divisor. Linearity is not a consequence of the constructions here, and we shall use the standard modification of the greedy algorithm: at each step, the augmenting word is chosen to be the least one not in the code at hand for which the span of it and that code has the desired properties.

Here is the underlying framework: the codes will be linear over the field \mathbb{F}_p , p an odd prime. We regard the space \mathbb{F}_p^n of words of length n over \mathbb{F}_p as being the subspace of words $(0, x_2, \dots, x_{n+1})$ of \mathbb{F}_p^{n+1} , for $n = 1, 2, \dots$. Then the union of the \mathbb{F}_p^n is the set of words from which the codes are constructed. What this amounts to is that the words can be taken as the non-negative integers written base p , the digit at p^n being the coordinate of the corresponding word at position $n + 1$. That realisation produces the ordering of the words – it is just numerical order. (Another common view is that the words are half-infinite sequences extending to the left, with components from \mathbb{F}_p . Each such sequence is required to have only finitely many non-zero entries.) This same natural ordering would appear if the codes were taken over a ring \mathbb{Z}_m . One can also use the alphabet \mathbb{Z} itself, as it was done in the two papers (Conway, 1990; Herscovici, 1991).

Given the properties required for the constructed codes, if code C has been produced by a certain step, the next code is the span $\langle C, \mathbf{c} \rangle$, where \mathbf{c} is the least word for which $\mathbf{c} \notin C$ and $\langle C, \mathbf{c} \rangle$ still has the desired properties. For example, the ATLAS (Conway et al., 1985, p.32) displays the extended ternary (12, 6) Golay code \mathcal{G} arising lexicographically at length 12 simply from the demand that the minimum weight be 6, with no divisibility requirement. Code \mathcal{G} has generator matrix

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

These rows correspond to the numbers 364, 2,960, 7,394, 20,554, 59,986 and 178,104. Since the covering radius of \mathcal{G} is 3 (Huffman and Pless, 2003, Theorem 10.4.2), the next code in the lexicographic sequence would have length 15. In fact, it is the span of \mathcal{G} and the word

$$1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1$$

(corresponding to 6,908,746). Although the new code is not divisible by 3, \mathcal{G} itself is. For ternary codes, divisibility by 3 is the same as self-orthogonality. Thus, if the requirements were divisibility by 3 along with minimum weight 6, the fact that \mathcal{G} is self-dual shows that the lexicographic code would continue in blocks, with generator matrix

$$\begin{matrix} \dots & 0 & 0 & 0 & 0 & G \\ \dots & 0 & 0 & 0 & G & 0 \\ \dots & 0 & 0 & G & 0 & 0 \\ \dots & 0 & G & 0 & 0 & 0 \\ \dots & G & 0 & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \end{matrix}$$

The codes we shall study are not like this, in that projections of the later codes onto the support of the span of the first two words will be divisible.

Our lexicographic codes over \mathbb{F}_p , p odd, are constructed subject to these two requirements:

- 1 the code is divisible by p
- 2 the minimum weight is rp , where $1 \leq r \leq p - 1$.

With p and r understood, \mathcal{L}_k will denote the code constructed at step k having dimension k , the whole lexicographic code being \mathcal{L} . Thus, $\mathcal{L}_k = \langle \mathcal{L}_{k-1}, \mathbf{g}_k \rangle$, where \mathbf{g}_k is the least word not contained in \mathcal{L}_{k-1} for which $\langle \mathcal{L}_{k-1}, \mathbf{g}_k \rangle$ is divisible by p and has minimum weight rp . This word will be called the *generator* at step k , and these generators must be linearly independent. As the paper develops, r will become more restricted. When we need to indicate r , we shall write $\mathcal{L}^{(r)}$.

One could let a computer that produce these codes up through some finite length, but the challenge is to give a description of how the codes evolve.

2 The initial codes and projection divisibility

The first code \mathcal{L}_1 is the span of the all-1 word of length rp . With $g = p - 1$ once and for all, the all-1 word is numerically $(p^{rp} - 1)/g$. By the Griesmer bound, the support length of \mathcal{L}_2 (the number of positions at which some word of \mathcal{L}_2 has a non-zero entry) must be at least $rp + r = r(p + 1)$. An $[r(p + 1), 2, rp]_p$ code divisible by p does exist, namely the r -fold replication of the two-dimensional Hamming dual (simplex code). In fact, any two-dimensional code of length $r(p + 1)$ with minimum weight rp and divisor p must be a constant weight code, that is, one in which all non-zero words have the same weight. By the often-reproved theorem of Bonisoli (1984), such a code is equivalent to the r -fold replicated Hamming dual. We shall consider this Hamming dual as the projective generalised Reed-Muller code $\text{PC}_1(1, p)$, in the notation of Sørensen (1991). However, since the code will appear frequently, we label it \mathcal{H} . Conventionally, we think of the projective line $\mathbb{P}^1(\mathbb{F}_p)$ over \mathbb{F}_p as $\mathbb{F}_p \cup \{\infty\}$, with $\infty = (0 : 1)$ and $z = (1 : z)$, $z \in \mathbb{F}_p$, in homogeneous coordinates $(x_1 : x_2)$. The coordinates are ordered $\infty, 0, 1, \dots, g$. Thus, \mathcal{H} is the set of evaluation vectors of the linear homogeneous polynomials in ξ_1 and ξ_2 on these points, where $\xi_i((x_1 : x_2)) = x_i$. Evaluation at z means evaluation at the pair $(x_1 : x_2)$ that z represents, and we shall say *homogeneous polynomials in z* . The evaluation vectors \mathbf{x}_1 and \mathbf{x}_2 of ξ_1 and ξ_2 form a basis of \mathcal{H} :

$$\mathbf{x}_1 = (0, 1, 1, 1, \dots, 1)$$

$$\mathbf{x}_2 = (1, 0, 1, 2, \dots, g)$$

Then \mathcal{L}_2 is the r -fold replication of \mathcal{H} , the replications being done at each coordinate position. We shall refer to the r coordinates replicating the coordinate at z as the *replication set* R_z . For example, the first two rows of the generator matrix G for the Golay code above span \mathcal{L}_2 for $p = 3$ and $r = 2$ (with a suggestive notation for replicated words):

$$\begin{array}{cccc} & R_\infty & R_0 & R_1 & R_2 \\ 2 \times \mathbf{x}_1 = & 0, 0 & 1, 1 & 1, 1 & 1, 1 \\ 2 \times \mathbf{x}_2 = & 1, 1 & 0, 0 & 1, 1 & 2, 2 \end{array}$$

With general r , the two words suggested are the first two generators of \mathcal{L} : $\mathbf{g}_1 = r \times \mathbf{x}_1$ and $\mathbf{g}_2 = r \times \mathbf{x}_2$.

For words \mathbf{c}_1 and \mathbf{c}_2 , let $\mathbf{c}_1\mathbf{c}_2$ be their componentwise product, and let $\sigma(\mathbf{c})$ be the sum of the entries in the word \mathbf{c} . Thus, the dot product of \mathbf{c}_1 and \mathbf{c}_2 is $\sigma(\mathbf{c}_1\mathbf{c}_2)$, and the Hamming weight $\text{wt}(\mathbf{c})$ of \mathbf{c} , when read modulo p , is $\sigma(\mathbf{c}^{p-1})$.

Lemma 1: *Let $B = \{\mathbf{b}_1, \dots, \mathbf{b}_k\}$ be a spanning set for a code over \mathbb{F}_p . Then the code is divisible by p exactly when $\sigma(\mathbf{b}_{i_1} \cdots \mathbf{b}_{i_{p-1}}) = 0$ for all choices of members $\mathbf{b}_{i_1}, \dots, \mathbf{b}_{i_{p-1}}$ of B (repetitions allowed).*

Proof: This is a consequence of Ward (1990, Theorem 5.3), but it can be proved directly. If $\mathbf{c} = \sum_{i=1}^k b_i \mathbf{b}_i$ then

$$\sigma(\mathbf{c}^{p-1}) = \sum b_1^{i_1} b_2^{i_2} \cdots b_k^{i_k} \binom{p-1}{i_1, i_2, \dots, i_k} \sigma(\mathbf{b}_1^{i_1} \mathbf{b}_2^{i_2} \cdots \mathbf{b}_k^{i_k})$$

the sum over all choices of indices with $\sum i_j = p-1$. The multinomial coefficients are not 0 modulo p . Since the monomials in the b_i are independent over \mathbb{F}_p (Assmus and Key, 1992, p.154), the sum will be 0 for all choices of \mathbf{c} , that is, for all choices of the b_i , exactly when each factor $\sigma(\mathbf{b}_1^{i_1} \mathbf{b}_2^{i_2} \cdots \mathbf{b}_k^{i_k})$ is 0. \square

Now we can prove the key result used in the study of our lexicographic codes. Let \mathcal{C} be any code that has \mathcal{L}_2 as a subcode, the support of \mathcal{L}_2 being the last $r(p+1)$ coordinate positions of \mathcal{C} and being ordered as in the set-up for \mathcal{L}_2 . We write a typical word of \mathcal{C} as $\mathbf{c} = (\mathbf{c}_p, \mathbf{c}_\infty, \mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_{p-1})$, where \mathbf{c}_p is the projection of \mathbf{c} onto the complement of the support $\bigcup R_z$ of \mathcal{L}_2 and each other \mathbf{c}_z is the projection of \mathbf{c} onto R_z (the set of r coordinate positions where the original coordinate at z is replicated). Informally, we shall call \mathbf{c}_p the *left part* of \mathbf{c} and $(\mathbf{c}_\infty, \mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_{p-1})$ the *right part*, which is the projection of \mathbf{c} onto the support of \mathcal{L}_2 . Similarly, the left and right parts of \mathcal{C} are the sets of left and right parts of the words in \mathcal{C} . For example, if $\mathbf{0}_m$ and $\mathbf{1}_m$ are the all-0 and all-1 words of a length m , then if \mathcal{C} has length n ,

$$\begin{aligned} \mathbf{g}_1 &= (\mathbf{0}_{n-r(p+1)}, \mathbf{0}_r, \mathbf{1}_r, \mathbf{1}_r, \mathbf{1}_r, \dots, \mathbf{1}_r) \\ \mathbf{g}_2 &= (\mathbf{0}_{n-r(p+1)}, \mathbf{1}_r, \mathbf{0}_r, \mathbf{1}_r, 2\mathbf{1}_r, \dots, g\mathbf{1}_r) \end{aligned}$$

(As always, we augment words by 0s to their left when they are considered in longer codes.) In the proof, we need Lemma 1 in Ward (1981).

Lemma 2: *If \mathbf{a} and \mathbf{b} are two non-zero words in a code over \mathbb{F}_p that is divisible by p , let $f(\infty)$ be the number of coordinate positions where \mathbf{a} has a 0 and \mathbf{b} has a non-zero entry. Let $f(x)$ be the number of non-zero coordinates in \mathbf{a} for which the corresponding coordinate in \mathbf{b} is x times the one in \mathbf{a} . Then $f(x) \equiv f(\infty) \pmod{p}$ for all $x \in \mathbb{F}_p$, and $\sum f(x) = \text{wt}(\mathbf{a})$, the sum over \mathbb{F}_p .*

Theorem 1: *Suppose that $r < p-1$ and that \mathcal{L}_2 is a subcode of a code \mathcal{C} divisible by p . Then the projection of \mathcal{C} onto the support of \mathcal{L}_2 is also divisible by p . In fact, there is a set of r homogeneous linear polynomials $\lambda_0, \dots, \lambda_{r-1}$ such that the components of \mathbf{c}_z are the $\lambda_s(z)$ for $z \in \mathbb{P}^1(\mathbb{F}_p)$.*

Proof: Apply Lemma 1 to the set $\{\mathbf{g}_1, \mathbf{g}_2, \mathbf{c}\} : \sigma(\mathbf{g}_1^i \mathbf{g}_2^j \mathbf{c}^k) = 0$ for $i+j+k = p-1$. When $k < p-1$, at least one of i and j is positive, and the equation becomes $\sigma(\mathbf{x}_1^i \mathbf{x}_2^j (\sigma(\mathbf{c}_\infty^k), \sigma(\mathbf{c}_0^k), \sigma(\mathbf{c}_1^k), \dots, \sigma(\mathbf{c}_{p-1}^k))) = 0$, because each of \mathbf{g}_1 and \mathbf{g}_2 is constant

on the coordinate groups R_z of size r . As the products $\mathbf{x}_1^i \mathbf{x}_2^j$ with $i + j = p - 1 - k$ span the projective Reed-Muller code $\text{PC}_{p-1-k}(1, p)$, the word $(\sigma(\mathbf{c}_\infty^k), \sigma(\mathbf{c}_0^k), \sigma(\mathbf{c}_1^k), \dots, \sigma(\mathbf{c}_{p-1}^k))$ is in $\text{PC}_{p-1-k}(1, p)^\perp$. By Sørensen (1991, Theorem 2), the last code is $\text{PC}_k(1, p)$. So there is a homogeneous polynomial π_k of degree k for which $\sigma(\mathbf{c}_z^k) = \pi_k(z)$ for $z \in \mathbb{P}^1(\mathbb{F}_p)$, with $\pi_0(z) = r$.

These $\pi_k(z)$ are the power sum symmetric functions of the r components of the \mathbf{c}_z . Since $r < p$, we can solve for the elementary symmetric functions $\varepsilon_k(z)$ of the components, by Newton's identities; ε_k will also be a homogeneous polynomial of degree k (see the explicit formulas in Littlewood (1970, Chapter 5)). With the ε_k in hand, one can then continue with Newton's identities to conclude that $\sigma(\mathbf{c}_z^{p-1})$ is a homogeneous polynomial of degree $p - 1$ (in z). But for such a polynomial, the sum of its values over $\mathbb{P}^1(\mathbb{F}_p)$ is 0, again a consequence of Sørensen (1991, Theorem 2). Thus with $(\mathbf{c}_\infty, \mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_{p-1}) = \mathbf{c}'$, $\text{wt}(\mathbf{c}')$ is divisible by p . Since $\text{wt}(\mathbf{c})$ is also divisible by p , so is $\text{wt}(\mathbf{c}_p)$.

We prove the existence of the λ_s by induction on r (the range of indices on the λ_s is chosen to match a later construction). At $r = 1$, λ_0 is simply π_1 . For $r > 1$, subtract a multiple $b\mathbf{g}_2$ from \mathbf{c}' to make the leading entry in \mathbf{c}_∞ equal to 0. If the functions λ_s exist for the modified \mathbf{c}' , they exist for the original \mathbf{c}' in the form $\lambda_s + b\xi_2$. Apply Lemma 2 with $\mathbf{a} = \mathbf{g}_1$ (whose non-zero coordinates are all 1) and $\mathbf{b} = \mathbf{c}'$. As $f(\infty) < r$ and $\sum_x f(x) = \text{wt}(\mathbf{a}) = rp$, one of the $f(x)$ is at least p . Modify \mathbf{c}' again by subtracting a multiple of \mathbf{g}_1 (involving ξ_1) to make this x equal to 0. We claim that now there must be a 0 in each replication set. By arrangement, there is one 0 in R_∞ . Suppose there is none in R_z , $z \in \mathbb{F}_p$. The combination $\mathbf{x} = \mathbf{g}_2 - z\mathbf{g}_1$ has 0s on R_z . Apply Lemma 2 with $\mathbf{a} = \mathbf{x}$ and $\mathbf{b} = \mathbf{c}'$. Here $f(\infty) = r$, and as $\text{wt}(\mathbf{a}) = rp$ and each $f(x) \equiv r \pmod{p}$, all the $f(x)$ must be r . But that would mean \mathbf{c}' has only r zero entries; yet $r < p$. Thus, we can delete one coordinate in each replication set where \mathbf{c}' has a 0. Then the entries of \mathbf{c}' are given by the deleted 0 function and the $r - 1$ homogeneous linear polynomials provided by induction from $r - 1$. \square

For the Golay code, where $r = 3 - 1$, the projection is *not* divisible by 3. We shall assume from here on that $r < p - 1$.

Note that the weight of the right part \mathbf{c}' is p times the number of non-zero λ_s . Thus, the weight of any coset of \mathcal{L}_2 in \mathcal{C} is less than rp , since on subtracting an appropriate combination of \mathbf{g}_1 and \mathbf{g}_2 from a coset representative, as in the proof, one can arrange that one of the λ_s for the representative is 0. In particular, any word having left part $\mathbf{0}$ must already be in \mathcal{L}_2 . We record an evident corollary, stemming from the fact that if λ is a non-zero linear homogeneous polynomial, then the word whose components are $\lambda(z)$, $z \in \mathbb{P}^1(\mathbb{F}_p)$, has weight p .

Corollary 1: If \mathcal{L}_2 is a subcode of a code \mathcal{C} with coordinates arranged as in the theorem, and each word of \mathcal{C} has left part divisible by p and right part described by a set of linear homogeneous polynomials λ_s , again as in the theorem, then \mathcal{C} is divisible by p .

3 The codes for $r = 1$ and $r = 2$

As suggested, the left part of any additional word beyond \mathcal{L}_2 must have weight at least p . Conceivably, the left part could be selected from \mathcal{H} itself; we shall see how that plays out.

When $r = 1$, the right parts of additional words are always $\mathbf{0}_{p+1}$. It follows that the lexicographic code is simply the direct sum of copies of \mathcal{L}_2 , each shifted to the left by a

4 Preliminaries for $r \geq 3$

Any word in $\mathcal{L}^{(2)}$ is *coherent* in the sense that for its projection onto $\bigcup R_z$, the homogeneous linear polynomials λ_0 and λ_1 have the property that if $\lambda_0(\infty)$ and $\lambda_1(\infty)$ appear in that order in R_∞ , then $\lambda_0(z)$ and $\lambda_1(z)$ appear in that order in each R_z . We need to see to what extent coherence holds when $r > 2$. The first three generators are

$$\begin{array}{rcccccc}
 & R_\infty & R_0 & R_1 & R_2 & \dots & R_g \\
 \mathbf{g}_1 = \mathbf{0}_{p+1} & 0, 0, 0, \dots & 1, 1, 1, \dots & 1, 1, 1, \dots & 1, 1, 1, \dots & \dots & 1, 1, 1, \dots \\
 \mathbf{g}_2 = \mathbf{0}_{p+1} & 1, 1, 1, \dots & 0, 0, 0, \dots & 1, 1, 1, \dots & 2, 2, 2, \dots & \dots & g, g, g, \dots \\
 \mathbf{g}_3 = \mathbf{x}_1 & 0, 0, 0, \dots & 0, 1, 2, \dots & 0, 1, 2, \dots & 0, 1, 2, \dots & \dots & 0, 1, 2, \dots
 \end{array}$$

The reason for \mathbf{g}_3 is that any lower choice for the λ_s of \mathbf{g}_3 would still have all the $\lambda_s(\infty) = 0$. But if two of the λ_s were the same, then some combination with \mathbf{g}_1 would have at least two λ_s equal to 0 and have weight less than rp . We see a pattern of coherence developing, and we wish to show that it continues. Index the coordinates in each R_z , $z \in \mathbb{F}_p$, by the entries of \mathbf{g}_3 in those sets (R_∞ will be indexed later). For $\mathbf{c} \in \mathcal{L}$, let the s th entry of \mathbf{c} in R_z be $\varphi_s(z)$, $0 \leq s \leq r - 1$. These functions φ_s can be represented by polynomials in z with degrees at most $p - 1$.

Lemma 3: *If $r \leq (p + 1)/2$, then each φ_s has degree at most 1 as a polynomial in z .*

Proof: The right part of \mathcal{L} is divisible by p , by Theorem 1. We apply Lemma 1 to the right part \mathbf{r} of \mathbf{c} and the right parts $\mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3$ of $\mathbf{g}_1, \mathbf{g}_2, \mathbf{g}_3$:

$$\sigma(\mathbf{r}_1^{m_1} \mathbf{r}_2^{m_2} \mathbf{r}_3^{m_3} \mathbf{r}^c) = 0 \text{ for } m_1 + m_2 + m_3 + c = p - 1$$

If $m_1 + m_3 > 0$, there is no contribution from R_∞ to the sum involved in σ . Thus, if $m_2 + c \leq p - 2$,

$$0 = \sigma(\mathbf{r}_1^{m_1} \mathbf{r}_2^{m_2} \mathbf{r}_3^{m_3} \mathbf{r}^c) = \sum_{s=0}^{r-1} s^{m_3} \sum_{z \in \mathbb{F}_p} z^{m_2} \varphi_s^c(z) \quad \text{for } m_3 \leq p - 1 - m_2 - c$$

In fact $m_2 + c \leq p - r$, then the double sum is 0 for $0 \leq m_3 \leq r - 1$. Then it follows that the interior sum is 0, since the coefficient matrix in s is Vandermonde. Taking $r \geq 2$, we now have $\sum_{z \in \mathbb{F}_p} z^{m_2} \varphi_s^c(z) = 0$ if $m_2 + c \leq p - r$. In terms of generalised Reed-Muller codes (not projective – see Assmus and Key (1992, Section 5.4)), this means that $\varphi_s^c \in \mathcal{R}_{\mathbb{F}_p}(p - r - c, 1)^\perp$, so that $\varphi_s^c \in \mathcal{R}_{\mathbb{F}_p}(r + c - 2, 1)$, by Assmus and Key (1992, Theorem 5.4.2). That is, for the degree of φ_s^c , $\deg(\varphi_s^c) \leq r + c - 2$, and this is valid for $c \leq p - 2$.

Now assume that $r \leq (p + 1)/2$, so that $\deg(\varphi_s^c) \leq c + (p - 3)/2$, and let $\deg(\varphi_s^c) = d$. We wish to show that $d \leq 1$. As long as $cd \leq p - 1$, $\deg(\varphi_s^c) = cd$ (in realising the function φ_s^c as a polynomial, one computes the polynomial power and then reduces it modulo $z^p - z$). We claim that if $1 \leq c \leq (p - 3)/2$ and $cd \leq p - 1$, then $(c + 1)d \leq p - 1$, too. For $cd \leq p - 1$ implies that $cd = \deg(\varphi_s^c) \leq c + (p - 3)/2$. Then $d \leq 1 + (p - 3)/(2c)$ and $(c + 1)d \leq (c + 1)(1 + (p - 3)/(2c))$. However,

$$p - 1 - (c + 1) \left(1 + \frac{p - 3}{2c} \right) = (c - 1) \frac{((p - 3/2) - c)}{c} \geq 0$$

since the factors on the right are non-negative. As $d \leq p - 1$, finite induction from $c = 1$ shows that $d(p - 1)/2 \leq p - 1$ and so $d \leq 2$. But if $d = 2$, $c = (p - 1)/2$ gives the contradiction $p - 1 = cd \leq c + (p - 3)/2 = p - 2$. \square

Continuing to take $r \leq (p + 1)/2$, we can now produce a candidate for \mathbf{g}_4 having left part \mathbf{x}_2 . The entries in R_∞ must all be different, otherwise a selected combination with \mathbf{g}_1 , \mathbf{g}_2 and \mathbf{g}_3 would produce two 0s in R_∞ and a matching two 0s in R_0 to make two of the λ_s of the combination equal to 0 and give total weight less than rp . So the R_∞ entries are $0, 1, 2, \dots, r - 1$ in that order. The lowest available entries for R_0 are simply 0s. Then for R_1 and R_2 the lowest entries are $0, 1, 2, \dots, r - 1$ and $0, 2, 4, \dots, 2r - 2$, conforming to the facts that the λ_s for \mathbf{g}_4 are all different and $2(r - 1) \leq p - 1$. For \mathbf{g}_4 , $\varphi_s(z) = sz$ (and $\lambda_s((x_1 : x_2)) = sx_2$). The display is

	R_∞	R_0	R_1	R_2	...	R_g
$\mathbf{g}_1 = \mathbf{0}_{p+1}$	0, 0, 0, ...	1, 1, 1, ...	1, 1, 1, ...	1, 1, 1,	1, 1, 1, ...
$\mathbf{g}_2 = \mathbf{0}_{p+1}$	1, 1, 1, ...	0, 0, 0, ...	1, 1, 1, ...	2, 2, 2,	g, g, g, \dots
$\mathbf{g}_3 = \mathbf{x}_1$	0, 0, 0, ...	0, 1, 2, ...	0, 1, 2, ...	0, 1, 2,	0, 1, 2, ...
$\mathbf{g}_4 = \mathbf{x}_2$	0, 1, 2, ...	0, 0, 0, ...	0, 1, 2, ...	0, 2, 4,	0, $g, g - 1, \dots$

We need to show that all members of \mathcal{L} are coherent. Let $\mathbf{r} = (\mathbf{c}_\infty, \mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_g)$ be the right part of a word \mathbf{c} in \mathcal{L} , as before, with $\mathbf{c}_\infty = c_0c_1c_2 \dots$ and $\varphi_s(z) = d_s z + e_s$, as in Lemma 3. The coherence sought is that $c_s = d_s$ for $0 \leq s \leq r - 1$. By Lemma 1, $\sigma(\mathbf{r}_2^{m_2} \mathbf{r}_4^{m_4} \mathbf{r}) = 0$, where \mathbf{r}_2 and \mathbf{r}_4 are the right parts of $\mathbf{g}_2, \mathbf{g}_4$ and $m_2 + m_4 + 1 = p - 1$. The equation is

$$\begin{aligned}
 0 &= \sigma(\mathbf{r}_2^{m_2} \mathbf{r}_4^{m_4} \mathbf{r}) = \sum_s s^{m_4} c_s + \sum_s \sum_z z^{m_2} (sz)^{m_4} (d_s z + e_s) \\
 &= \sum_s s^{m_4} c_s + \sum_s s^{m_4} \left(\sum_z z^{p-1} d_s + \sum_z z^{p-2} e_s \right)
 \end{aligned}$$

Since $\sum_z z^m = 0$ for $1 \leq m \leq p - 2$ and $\sum_z z^{p-1} = -1$, the equation is $\sum_s s^{m_4} (c_s - d_s) = 0$, and this holds for $m_4 \leq p - 2$. As the number r of s is at most $(p + 1)/2$, $c_s - d_s$ must be 0 (by the standing assumption that $r < p - 1$, we have $p \geq 5$, so that indeed $(p + 1)/2 \leq p - 2$). We can thus write $\lambda_s((x_1 : x_2)) = e_s x_1 + d_s x_2$.

5 The code for $r = 3$

With $r = 3$, the first four generators of \mathcal{L} are as in Section 4:

	R_∞	R_0	R_1	R_2	...	R_g
$\mathbf{g}_1 = \mathbf{0}_{p+1}$	0, 0, 0	1, 1, 1	1, 1, 1	1, 1, 1	...	1, 1, 1
$\mathbf{g}_2 = \mathbf{0}_{p+1}$	1, 1, 1	0, 0, 0	1, 1, 1	2, 2, 2	...	g, g, g
$\mathbf{g}_3 = \mathbf{x}_1$	0, 0, 0	0, 1, 2	0, 1, 2	0, 1, 2	...	0, 1, 2
$\mathbf{g}_4 = \mathbf{x}_2$	0, 1, 2	0, 0, 0	0, 1, 2	0, 2, 4	...	0, $g, g - 1$

We wish to see how long we can take the left parts of further generators alternately to be \mathbf{x}_1 and \mathbf{x}_2 . Because of their coherence, the right parts of the generators are entirely specified by the entries in R_∞ and R_0 . If those six entries are $[d_0, d_1, d_2; e_0, e_1, e_2]$, then the entries in R_z are $d_0 z + e_0, d_1 z + e_1, d_2 z + e_2$, in that order. If two right parts \mathbf{r} and \mathbf{r}' are represented by $[d_0, d_1, d_2; e_0, e_1, e_2]$ and $[d'_0, d'_1, d'_2; e'_0, e'_1, e'_2]$, then \mathbf{r} is less than \mathbf{r}' exactly when $[d_0, d_1, d_2; e_0, e_1, e_2]$ is less than $[d'_0, d'_1, d'_2; e'_0, e'_1, e'_2]$. In creating a generator with

the six entries $[d_0, d_1, d_2; e_0, e_1, e_2]$, we can adjust by multiples of \mathbf{g}_1 and \mathbf{g}_2 and take d_0 and e_0 both to be 0, the least possibility. The remaining four entries will make up the foreword of the generator (in the lexicographic spirit).

Definition 1: *If for $k \geq 2$ we succeed in finding a k th pair of generators \mathbf{g}_{2k-1} and \mathbf{g}_{2k} whose left parts are shifts of \mathbf{x}_1 and \mathbf{x}_2 into the same set of $p + 1$ positions immediately to the left of those for \mathbf{g}_{2k-3} and \mathbf{g}_{2k-2} , we shall say that the index k is booked.*

When k is booked, we shall display the forewords of \mathbf{g}_{2k-1} and \mathbf{g}_{2k} in the rows of a matrix

$$M_k = \begin{bmatrix} d_1 & d_2 & e_1 & e_2 \\ d'_1 & d'_2 & e'_1 & e'_2 \end{bmatrix}$$

These rows span a subspace \mathcal{P}_k of \mathbb{F}_p^4 . Along with k , we shall also say that M_k and \mathcal{P}_k , are booked. If k is booked, then so are all the lower indices. Thus, the second booked index is 2, with

$$M_2 = \begin{bmatrix} 0 & 0 & 1 & 2 \\ 1 & 2 & 0 & 0 \end{bmatrix}$$

No non-zero word \mathbf{c} in $\langle \mathbf{g}_{2k-1}, \mathbf{g}_{2k} \rangle$ can be in a coset of \mathcal{L}_2 of weight $2p$ or less. As the left part of \mathbf{c} has weight p , the right part $(\mathbf{c}_\infty, \mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_g)$ cannot be in a coset of weight p (or 0). Such cosets consisting of coherent words are represented by forewords in the three planes that are the spans of the following matrices:

$$\mathcal{P}_\infty: M_\infty = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

$$\mathcal{P}_0: M_0 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

$$\mathcal{P}_1: M_1 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

We shall also consider these three planes (and their matrices and indices) as booked. Any two of these planes intersect trivially, in the sense that they meet only in 0.

Lemma 4: *Suppose that $k \geq 2$ is a booked index. Then the following properties hold:*

- 1 \mathcal{P}_k is a plane – that is, M_k has rank 2
- 2 If $k \neq l$ and l is also booked, then \mathcal{P}_k and \mathcal{P}_l intersect trivially.

Proof: If a linear combination of the rows of M_k is equal to $\mathbf{0}$, the same combination of \mathbf{g}_{2k-1} and \mathbf{g}_{2k} would have weight p . Similarly, if some non-zero combination of the rows of M_k lay in $\mathcal{P}_\infty, \mathcal{P}_0$ or \mathcal{P}_1 , then that combination of \mathbf{g}_{2k-1} and \mathbf{g}_{2k} would have weight $2p$. Finally, if \mathcal{P}_k and \mathcal{P}_l share a non-zero word (and here $l \geq 2$), combinations of \mathbf{g}_{2k-1} and \mathbf{g}_{2k} and of \mathbf{g}_{2l-1} and \mathbf{g}_{2l} would be equal, contradicting the independence of generators. \square

The lemma implies that the booked planes form a partial spread (see Lüneburg (1980), among others). In searching to book the next k , the possible forewords for \mathbf{g}_{2k-1} can be limited to have leading coefficient 1. For because of the disjointedness of the support of the left part of \mathbf{g}_{2k-1} from the supports of the earlier \mathbf{g}_j , the needed independence from those \mathbf{g}_j depends only on the right part of \mathbf{g}_{2k-1} . Accordingly, that can be scaled to be as low

as possible. The same holds for possible forewords for \mathbf{g}_{2k} , independence of any non-zero combination of \mathbf{g}_{2k-1} and \mathbf{g}_{2k} from the earlier \mathbf{g}_j being assured; but these forewords can also be modified by a multiple of the foreword for \mathbf{g}_{2k-1} , since the only criterion for success is the trivial intersections of \mathcal{P}_k with the preceding planes.

Lemma 5: *The numbers 0 to $p - 1$ ($= g$) are booked.*

Proof: Suppose that 0 through $k - 1$ are booked and that for $0 \leq h \leq k - 1$, $M_h = \begin{bmatrix} 0 & 0 & 1 & h \\ 1 & h & 0 & 0 \end{bmatrix}$. This is true for $k = 3$. The least foreword available for \mathbf{g}_{2k-1} has the form $[0, 0; \quad 1, a]$ for some a , with $a > k - 1$ to avoid membership in a previous plane. The least choice is then $a = k$. The least apparent choice for the foreword for \mathbf{g}_{2k} is $[0, 1; \quad 0, b]$ for some b . But for such a choice, \mathcal{P}_k would not intersect \mathcal{P}_∞ trivially. Thus, one searches for a foreword $[1, c; \quad 0, d]$, making that intersection trivial. Then triviality of intersection of \mathcal{P}_k with \mathcal{P}_h , $0 \leq h < k$, requires that

$$\det \begin{bmatrix} 0 & 0 & 1 & h \\ 1 & h & 0 & 0 \\ 0 & 0 & 1 & k \\ 1 & c & 0 & d \end{bmatrix} = (h - k)(c - h)$$

not be 0. The least successful choice is $c = k$ and $d = 0$. Thus, the forewords for \mathbf{g}_{2k-1} and \mathbf{g}_{2k} exist and have the desired form $[0, 0; \quad 1, k]$ and $[1, k; \quad 0, 0]$. \square

A complete spread in \mathbb{F}_p^4 contains $p^2 + 1$ planes, and we could conceivably book all the way to $p^2 - 1$; so we make these definitions:

Definition 2: *The prime p is called complete if all the indices k up through $p^2 - 1$ are booked.*

Definition 3: *By run h we mean the longest consecutive sequence $hp, hp + 1, \dots, hp + j$, $j < p$, whose terms are booked (we allow the sequence to be empty); and if $j = g$, we shall say the run is fully booked.*

So far, only run 0 is fully booked!

For $k \geq p$, the least candidate for the foreword of \mathbf{g}_{2k-1} is $[0, 1; \quad a, b]$ for some a and b , since the forewords starting with two 0s have all been used. Here $a \neq 0$, to avoid membership in \mathcal{P}_∞ . If a successful foreword exists, then the least possible foreword for \mathbf{g}_{2k} has the form $[1, 0; \quad c, d]$.

Lemma 6: *Let \mathbf{N} be the set of non-squares in \mathbb{F}_p . If $M_k = \begin{bmatrix} 0 & 1 & a & b \\ 1 & 0 & c & d \end{bmatrix}$, then for \mathcal{P}_k to intersect trivially all the \mathcal{P}_h in run 0, $(b - c)^2 + 4ad$ must be in \mathbf{N} .*

Proof: Trivial intersection requires that

$$\det \begin{bmatrix} 0 & 0 & 1 & j \\ 1 & j & 0 & 0 \\ 0 & 1 & a & b \\ 1 & 0 & c & d \end{bmatrix} = -aj^2 + (b - c)j + d$$

be non-zero for all j , $0 \leq j \leq p - 1$ (i.e. all $j \in \mathbb{F}_p$). Thus, the discriminant of this quadratic in j must be a nonsquare, and that is the stated condition. In particular, a and d must be non-zero. That $a \neq 0$ also covers trivial intersection with \mathcal{P}_∞ . \square

At index p , the least foreword for \mathbf{g}_{2p-1} is now $[0, 1; \quad 1, 0]$. For \mathbf{g}_{2p} , the least foreword is then $[1, 0; \quad 0, n_1]$, where n_1 is the least member of \mathbf{N} . For future use, we set $n_0 = 0$.

Proposition 1: *Run 1 is fully booked. Moreover, $M_{p+j} = \begin{bmatrix} 0 & 1 & 1 & j \\ 1 & 0 & j & n_1 \end{bmatrix}$ for $0 \leq j \leq p - 1$.*

Proof: Suppose the indices from p to $p + j - 1$ are booked for $j < p$; we seek to book $p + j$. By the remarks above, the supposition holds at $j = 1$. The least foreword that works for $\mathbf{g}_{2(p+j)-1}$ is $[0, 1; \quad 1, j]$, the third entry needing to be non-zero. Then for the foreword $[1, 0; \quad c, d]$ for $\mathbf{g}_{2(p+j)}$, Lemma 6 requires $(j - c)^2 + 4d \in \mathbf{N}$. The least choice for c is j , and the least d is still n_1 . With these choices, one must check for trivial intersections of \mathcal{P}_{p+j} with the previous \mathcal{P}_{p+i} . That requirement is

$$\det \begin{bmatrix} 0 & 1 & 1 & j \\ 1 & 0 & j & n_1 \\ 0 & 1 & 1 & i \\ 1 & 0 & i & n_1 \end{bmatrix} = (j - i)^2 \neq 0$$

for $i < j$, and it is clearly met. □

Suppose now that runs 0 through $k - 1$ are fully booked with the matrices for run h , $1 \leq h < k$, being $M_{hp+j} = \begin{bmatrix} 0 & 1 & h & j \\ 1 & 0 & j & n_h \end{bmatrix}$, $0 \leq j \leq p - 1$. Here n_h depends only on the run. For brevity, we may use $M_k^* = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ in place of $M_k = \begin{bmatrix} 0 & 1 & a & b \\ 1 & 0 & c & d \end{bmatrix}$. The least foreword available for \mathbf{g}_{2kp-1} at the start of run k is $[0, 1; \quad k, 0]$. If a matching least available foreword for \mathbf{g}_{2kp} exists, it is $[1, 0; \quad c, d]$ for some c and d ; $M_{kp}^* = \begin{bmatrix} k & 0 \\ c & d \end{bmatrix}$. Lemma 6 implies that $c^2 + 4kd \in \mathbf{N}$. Trivial intersections for runs 1 to $k - 1$ require that

$$\det \begin{bmatrix} 0 & 1 & k & 0 \\ 1 & 0 & c & d \\ 0 & 1 & h & j \\ 1 & 0 & j & n_h \end{bmatrix} = j^2 - cj - (k - h)(d - n_h) \neq 0$$

for all $j \in \mathbb{F}_p$ (as in Lemma 6). Thus, the discriminant $c^2 + 4(k - h)(d - n_h)$ must be in \mathbf{N} . With $n_0 = 0$, this condition includes the previous one when $h = 0$. We search for $[1, 0; \quad c, d]$ in two steps: find the least c for which $c^2 + 4(k - h)(d - n_h) \in \mathbf{N}$ for $0 \leq h < k$ for some d , and then take the least d that works. Suppose the result is $[1, 0; \quad c_0, d_0]$.

Theorem 2: *If $k \geq 1$ and kp is booked, with foreword $[1, 0; \quad c_0, d_0]$ for \mathbf{g}_{2kp} , then run k is fully booked if and only if $c_0 = 0$.*

Proof: Suppose run k is fully booked but $c_0 \neq 0$. Then $M_{kp+l}^* = \begin{bmatrix} k & l \\ c_l & d_l \end{bmatrix}$ for certain c_l, d_l . As before, trivial intersections with the planes of an earlier run $h, h \geq 1$, requires that

$$\det \begin{bmatrix} 0 & 1 & k & l \\ 1 & 0 & c_l & d_l \\ 0 & 1 & h & j \\ 1 & 0 & j & n_h \end{bmatrix} = j^2 - (c_l + l)j - (k - h)(d_l - n_h) + lc_l \neq 0$$

for all $j \in \mathbb{F}_p$. The discriminant is

$$(c_l + l)^2 + 4(k - h)(d_l - n_h) - 4lc_l = (c_l - l)^2 + 4(k - h)(d_l - n_h)$$

so the *discriminant condition* is

$$(c_l - l)^2 + 4(k - h)(d_l - n_h) \in \mathbf{N} \tag{1}$$

Again, setting $h = 0$ gives the demand of Lemma 6. Trivial intersection with the planes for run k itself requires

$$\det \begin{bmatrix} 0 & 1 & k & j \\ 1 & 0 & c_j & d_j \\ 0 & 1 & k & l \\ 1 & 0 & c_l & d_l \end{bmatrix} = -(j - l)(c_j - c_l) \neq 0$$

for $j \neq l$; that is, $c_j \neq c_l$. Since at $l = 0$ the discriminant condition is $c_0^2 + 4(k - h)(d_0 - n_h) \in \mathbf{N}$ and only c_0^2 is involved, minimality of c_0 implies that $c_0 \leq (p - 1)/2$. Now suppose that $[1, 0; c, d]$ is a candidate foreword for \mathbf{g}_{2kp+l} , $0 < l < p$. If $c \leq l$, then by (1), $[1, 0; l - c, d]$ is a candidate foreword for \mathbf{g}_{2kp} . Consequently, $l - c \geq c_0$, that is, $c \leq l - c_0$. Similarly, if $l \leq c$, then $c \geq l + c_0$. Moreover, $[1, 0; l - c_0, d_0]$ satisfies (1) if $l \geq c_0$ and $[1, 0; l + c_0, d_0]$ does so if $l < p - c_0$.

Let $2mc_0 < p < 2(m + 1)c_0$. Then using the observations just made, and recalling that the c_l must be distinct, we obtain the M_{2kp+l}^* for $0 \leq l \leq 2mc_0 - 1$:

$$\begin{aligned} & \begin{bmatrix} k & 0 \\ c_0 & d_0 \end{bmatrix}, \begin{bmatrix} k & 1 \\ c_0 + 1 & d_0 \end{bmatrix}, \begin{bmatrix} k & 2 \\ c_0 + 2 & d_0 \end{bmatrix}, \dots, \begin{bmatrix} k & c_0 - 1 \\ 2c_0 - 1 & d_0 \end{bmatrix} \\ & \begin{bmatrix} k & c_0 \\ 0 & d_0 \end{bmatrix}, \begin{bmatrix} k & c_0 + 1 \\ 1 & d_0 \end{bmatrix}, \begin{bmatrix} k & c_0 + 2 \\ 2 & d_0 \end{bmatrix}, \dots, \begin{bmatrix} k & 2c_0 - 1 \\ c_0 - 1 & d_0 \end{bmatrix} \\ & \begin{bmatrix} k & 2c_0 \\ 3c_0 & d_0 \end{bmatrix}, \begin{bmatrix} k & 2c_0 + 1 \\ 3c_0 + 1 & d_0 \end{bmatrix}, \dots, \begin{bmatrix} k & 3c_0 - 1 \\ 4c_0 - 1 & d_0 \end{bmatrix} \\ & \begin{bmatrix} k & 3c_0 \\ 2c_0 & d_0 \end{bmatrix}, \begin{bmatrix} k & 3c_0 + 1 \\ 2c_0 + 1 & d_0 \end{bmatrix}, \dots, \begin{bmatrix} k & 4c_0 - 1 \\ 3c_0 - 1 & d_0 \end{bmatrix}, \dots \end{aligned}$$

the suggested pattern continuing. In particular, the c_l for $0 \leq l \leq 2mc_0 - 1$ also fill up the interval $0 \leq c_l \leq 2mc_0 - 1$.

If $p < (2m + 1)c_0$, then at $l = 2mc_0$ there is a problem: if a candidate foreword $[1, 0; c, d]$ had $c > l$, then as $c < p$, $c - l < c_0$; so that is out. But for $c \leq l$, $c \leq l - c_0 = (2m - 1)c_0$, and those values have been used. If $p > (2m + 1)c_0$, the suggested pattern could continue until $l = p - c_0$, when the only candidate forewords would have to have $c < l$ and then $c \leq l - c_0 < 2mc_0$, again among the used values.

If $c_0 = 0$, then the proof that run k is fully booked proceeds much as the proof of Proposition 1, with $M_{kp+l}^* = \begin{bmatrix} k & l \\ l & d_0 \end{bmatrix}$. □

Recall that p is called complete if all $m \leq p^2 - 1$ are booked. By Theorem 2, a complete prime entails that the first matrix for run k is of the form $M_{kp} = \begin{bmatrix} 0 & 1 & k & 0 \\ 1 & 0 & 0 & n_k \end{bmatrix}$ for some

n_k (labelled d_0 in the proof above). Lemma 6 pointed out that n_1 is the least member of \mathbf{N} (the non-squares of \mathbb{F}_p). Condition 1, applied with $l = 0$, $c_0 = 0$ and $d_0 = n_k$, requires that $4(k - h)(n_k - n_h) \in \mathbf{N}$, that is, that

$$(k - h)(n_k - n_h) \in \mathbf{N} \tag{2}$$

The n -sequence $0 = n_0, n_1, \dots$ is defined recursively by requiring that n_k be the least member of \mathbb{F}_p for which $(k - h)(n_k - n_h) \in \mathbf{N}$ for all $h < k$ (so the n_k are distinct). By the discussion preceding Theorem 2, the existence of n_k is equivalent to the fact that kp is booked, with $M_{kp} = \begin{bmatrix} 0 & 1 & k & 0 \\ 1 & 0 & 0 & n_k \end{bmatrix}$. Thus, by Theorem 2 itself, the determination whether p is complete amounts to determining whether the n -sequence is defined for all $k < p$.

Theorem 3: *If prime p is complete, then $n_k \equiv kn_1 \pmod{p}$.*

Proof: With $k \neq h$, $(k - h)(n_k - n_h) \in \mathbf{N}$ can also be written $(n_k - n_h)/(k - h) \in \mathbf{N}$. Thus, the difference quotient of the function $k \rightarrow n_k$ on \mathbb{F}_p takes on at most $|\mathbf{N}| = (p - 1)/2$ values. By Rédei (1973, Theorem 24') (see also Carlitz, 1960), the function must be linear. As $n_0 = 0$, $n_k = kn_1$ in \mathbb{F}_p . □

5.1 Checking for completeness

Call the sequence of residues modulo p of $0, n_1, 2n_1, \dots, (p - 1)n_1$ the $n_1 \times$ -sequence. Completeness of p amounts to the equality of the n -sequence and the $n_1 \times$ -sequence. We have no number-theoretic test for whether an odd prime p is complete. However, some observations help the computational determination of completeness.

If the n -sequence is not the $n_1 \times$ -sequence, let the first departure occur at position k , with value n : $n_i \equiv in_1 \pmod{p}$ for $i < k$, but $n \not\equiv kn_1 \pmod{p}$. From $(n - in_1)(k - i) \in \mathbf{N}$ for $i < k$, we get $(n - jn_1 - (i - j)n_1)(k - j - (i - j)) \in \mathbf{N}$ for $i - j < k - j$. Therefore, $n - jn_1 \pmod{p}$ would be a candidate for n_{k-j} . Let a be the remainder modulo p of $n - kn_1$; $a > 0$. Then member $a + ln_1$, $1 \leq l < k$, of the progression starting at a and having difference n_1 (the entries in this a -sequence taken modulo p) is a candidate for n_l .

Suppose the first numerical drop in the $n_1 \times$ -sequence occurs at position m ; that is, $(m - 1)n_1 < p$ but $p < mn_1$. By a result of A. Brauer (ascribed to his teacher, I. Schur) in Brauer (1931), $n_1 \leq \lceil \sqrt{p} \rceil$, so that $m \geq n_1 - 2$. However, suppose that $k \geq m$ (this can not happen if $n_1 = 2$, because then n must be 1, the only possibility below $2!$ As $mn_1 - p$ must also be 1, k has to be less than m .) Compare the $n_1 \times$ -sequence with the a -sequence (entries modulo p):

index	0	1	...	m	...	k
$n_1 \times$ -sequence	0	n_1	...	$mn_1 - p$...	$kn_1 \pmod{p}$
a -sequence	a	$a + n_1$...	$a + mn_1$...	$n \equiv a + kn_1 \pmod{p}$

Then it must be that $a < n_1$. Otherwise, numerically, $a + (m - 1)n_1 \geq mn_1 > p$, and when read modulo p , the a -sequence must drop somewhere before position m , say at position l . The value of the entry at the drop is less than n_1 and so less than the multiple of n_1 there. Thus, there would be a departure from the $n_1 \times$ -sequence sooner than position k , the a -sequence value at l being a candidate for n_l .

Now for $0 \leq i \leq n_1 - 2$ ($\leq m$), we have $(a + (n_1 - 1)n_1 - in_1)(n_1 - 1 - i) \in \mathbf{N}$, since $a + (n_1 - 1)n_1$ is a candidate for n_{n_1-1} . With $z = n_1 - 1 - i$, this says that $(a + zn_1)z \in \mathbf{N}$,

for $1 \leq z \leq n_1 - 1$. As all such z are squares, $a + zn_1 \in \mathbf{N}$. In particular, $a + an_1 \in \mathbf{N}$. But n_1 must be an odd prime, by the comment above; and $a + an_1 = a \times 2 \times (n_1 + 1)/2$. All three factors here are less than n_1 , so they are squares modulo p ; but then $a + an_1 \notin \mathbf{N}$ after all. Thus $k < m$. That is, if a departure occurs, it happens *before* the first drop in the $n_1 \times$ -sequence.

Continuing with the supposed departure at position k , let $n \equiv tn_1 \pmod{p}$, with $t > k$. Then, $(n - in_1)(k - i) \in \mathbf{N}$ for $i < k$ becomes $(t - i)(k - i)n_1 \in \mathbf{N}$. As $n_1 \in \mathbf{N}$, $(t - i)(k - i) \in \mathbf{S}$, the set of non-zero squares in \mathbb{F}_p . Setting $z = k - i$, we have $(t - k + z)z \in \mathbf{S}$ for $1 \leq z \leq k$. That is, if χ is the quadratic character modulo p (1 on \mathbf{S} , -1 on \mathbf{N} and $\chi(0) = 0$), the sequences $\chi(1), \chi(2), \dots, \chi(k)$ and $\chi(t - (k - 1)), \chi(t - (k - 2)), \dots, \chi(t)$ must be the same. Note that $k < m = \lfloor (p - 1)/n_1 \rfloor + 1$, making $k \leq \lfloor (p - 1)/n_1 \rfloor$. In \mathbb{F}_p , $t = n/n_1$. Let $t_n n_1 \equiv n \pmod{p}$, where $1 \leq t_n \leq p - 1$; necessarily $t_n \geq \lfloor (p - 1)/n_1 \rfloor$.

On the basis of these remarks, here is a procedure for checking p for completeness:

Algorithm 1: For n from 1 to $n_1 - 1$, look for k in the range $2 \leq k \leq \lfloor (p - 1)/n_1 \rfloor$ making the two sequences

$$\begin{array}{ccccccc} \chi(1) & & \chi(2) & & \dots & & \chi(k) \\ \chi(1 + t_n - k) & & \chi(2 + t_n - k) & & \dots & & \chi(t_n) \end{array}$$

agree. If for each n there is no such k , then p is complete.

5.2 Completeness for $p \equiv 5 \pmod{8}$

Consider the case that $n_1 = 2$ and $\chi(-1) = 1$ in Algorithm 1. This happens exactly when $p \equiv 5 \pmod{8}$, by quadratic reciprocity (see Niven et al. (1991, Chapter 3)). Here the only n to check is $n = 1$, with $t_1 = (p + 1)/2$. We look for the smallest k for which the two sequences

$$\begin{array}{ccccccc} \chi(1) & & \chi(2) & & \dots & & \chi(k) \\ \chi((p + 1)/2 - k + 1) & & \chi((p + 1)/2 - k + 2) & & \dots & & \chi((p + 1)/2) \end{array}$$

agree, and if $k = (p + 1)/2$, then p is complete. Agreement just means $\chi(j) = \chi((p + 1)/2 - k + j)$ for $1 \leq j \leq k$. This is the same as $\chi(2j) = \chi(2k - 1 - 2j)$, $1 \leq j \leq k$, from $\chi(-1) = 1$. Let $q = 2k - 1$. The requirement is $\chi(i) = \chi(q - i)$ for even i from 2 to $q - 1$. Switching i and $q - i$ gives the same relation for odd i . Thus, the sequence agreement amounts to the demand that $\chi(i) = \chi(q - i)$ for $1 \leq i \leq q - 1$.

It must be that q is a prime. For if not, we can write $q = eq'$, where $1 < q' < q$ and q' is odd. Then, $\chi(eq' - ej) = \chi(ej)$ for $1 \leq j \leq q' - 1$, so that $\chi(q' - j) = \chi(j)$ for that range, thereby giving $(q' + 1)/2$ for a smaller k . Completeness of p will mean that $p = q$.

Theorem 4: *With $p \equiv 5 \pmod{8}$ and q the smallest odd prime for which $\chi(i) = \chi(q - i)$ for all i with $1 \leq i \leq q - 1$, one has $\chi(i) = (i/q)$ (the Legendre symbol) for those i . That is, on the interval $1 \leq i \leq q - 1$, χ is the quadratic character for q .*

Proof: Let $Q = \{1, 2, \dots, q - 1\}$, and regard Q as the group of non-zero members of \mathbb{F}_q under multiplication. What we need to show is that χ is a character on Q . If that is so, then since $\chi: Q \rightarrow \{1, -1\}$ and χ is surjective (from $\chi(2) = -1$), χ must be the only such character on Q , namely, the quadratic character.

In what follows, congruences will all be modulo q , and for an integer z , $[z]$ will mean the member of $Q \cup \{0\}$ for which $z \equiv [z]$. Let

$$Q_0 = \{a \in Q : \chi([ax]) = \chi(a)\chi(x), \text{ for all } x \in Q\}$$

Then Q_0 is a subgroup of Q : let $a, b \in Q_0$ with $[ab] = c$; we must show that $c \in Q_0$. Suppose that $[cx] = y$. Let $[bx] = x'$, so that $[ax'] = y$. Then $\chi(a)\chi(b) = \chi(c)$, $\chi(b)\chi(x) = \chi(x')$ and $\chi(a)\chi(x') = \chi(y)$. Thus

$$\chi(c)\chi(x) = \chi(a)\chi(b)\chi(x) = \chi(a)\chi(x') = \chi(y)$$

as needed. Certainly $1 \in Q_0$; but we also have $2 \in Q_0$. For suppose that $[2x] = y$. If $2x < q$, then $y = 2x$ and $\chi(y) = \chi(2)\chi(x)$. And if $2x > q$, then $y = 2x - q$, as $2x < 2q$. So $\chi(y) = \chi(q - (2x - q)) = \chi(2(q - x))$. Since $2(q - x) < q$, $\chi(y) = \chi(2)\chi(q - x) = \chi(2)\chi(x)$. Finally, if $a \in Q_0$, then $q - a \in Q_0$. For with $[ax] = y$, $(q - a)x \equiv q - y$; that is, $[(q - a)x] = q - y$. Since $\chi(a)\chi(x) = \chi(y)$, and $\chi(q - a) = \chi(a)$, $\chi(q - y) = \chi(y)$, then $\chi(q - a)\chi(x) = \chi(q - y)$. Of course, $q - a = [-a]$.

To show that χ is a character on Q , we must prove that $Q_0 = Q$. We do this by a double finite induction: let $h \in Q$ be such that for all h' with $1 \leq h' < h$, $h' \in Q_0$. We may assume that $h \geq 3$ and that h is odd – if not, $h/2 \in Q_0$ and then $h \in Q_0$. Next, let x be such that when $x' < x$, $\chi(h)\chi(x') = \chi([hx'])$. We wish to show from this that if $[hx] = y$, then $\chi(h)\chi(x) = \chi(y)$. Here we may assume that $x \notin Q_0$, so $x \geq 3$. We may take x odd like h : if $x = 2x'$ and $[hx'] = y'$, then $y = [2y']$. As $x' < x$, $\chi(h)\chi(x') = \chi(y')$. Then $\chi(h)\chi(2)\chi(x') = \chi(2)\chi(y')$. Since $\chi(x) = \chi(2)\chi(x')$ and $\chi(y) = \chi(2)\chi(y')$ (from $2 \in Q_0$), $\chi(h)\chi(x) = \chi(y)$.

If $h < q/x$, then $hx < q$ and $[hx] = hx$, hence $\chi(h)\chi(x) = \chi([hx])$. We may thus assume that $h > q/x$. We may also assume that $3 < q/x$. For if not, let $[hx] = y$ and $[h(q - x)/2] = y'$. Then $[2y'] = q - y$. As $3 > q/x$ means that $(q - x)/2 < x$, $\chi(h)\chi((q - x)/2) = \chi(y')$ and $\chi(h)\chi(q - x) = \chi(2)\chi(y') = \chi(q - y)$, making $\chi(h)\chi(x) = \chi(y)$.

Now let m be odd with $m < q/x < m + 2$. Then $m \geq 3$ and $m + 2 \leq h$. As $mx < q$ and $q - mx$ is even, $x' = (q - mx)/2$ is a positive integer. Moreover, $x' < x$. Let $[hx'] = y'$, so that $\chi(h)\chi(x') = \chi(y')$. Since $m < h$, $m \in Q_0$ and $[(q - 1)m] \in Q_0$. Therefore $j = [((q - 1)/2)m] \in Q_0$ also. We have $jx \equiv ((q - 1)/2)mx \equiv (q - mx)/2 = x'$. Let $[jy] = y'$. Then $\chi(j)\chi(x) = \chi(x')$ and $\chi(j)\chi(y) = \chi(y')$. So $\chi(h)\chi(x') = \chi(y')$ becomes $\chi(h)\chi(j)\chi(x) = \chi(j)\chi(y)$, and thus $\chi(h)\chi(x) = \chi(y)$.

We may, therefore, conclude that $\chi([hx]) = \chi(h)\chi(x)$ for all $x \in Q$, so that $h \in Q_0$. Then the induction on h shows that $Q_0 = Q$. \square

From the theorem, $(2/q) = -1$ and $(-1/q) = ((q - 1)/q) = (1/q) = 1$. Thus, q itself is a prime with $q \equiv 5 \pmod{8}$. If q were not complete, there would be a smaller prime q' , also with $q' \equiv 5 \pmod{8}$, whose quadratic character is that of q on the interval $1 \leq x \leq q' - 1$ and therefore χ itself on that interval. But then q' would be a smaller prime showing the incompleteness of p . In summary:

Corollary 2: If $p \equiv 5 \pmod{8}$ and p is not complete, then there is a smaller complete prime q , with $q \equiv 5 \pmod{8}$, for which the quadratic character of p restricted to the interval $1 \leq x \leq q - 1$ gives the quadratic character of q .

Corollary 3: *There are an infinite number of complete primes p with $p \equiv 5 \pmod{8}$.*

Proof: Suppose not, and let p_1, \dots, p_t be the list in ascending order, with $p_1 = 5$ (which is complete). By Dirichlet's theorem on primes in arithmetical progressions, there are an infinite number of primes satisfying the congruences

$$p \equiv 5 \pmod{8}, \quad p \equiv 1 \pmod{3} \quad \text{and} \quad p \equiv 2p_j \pmod{p_{j-1}} \quad \text{for} \quad 2 \leq j \leq t$$

Suppose that such a p is not complete, and let q be the prime of Corollary 2. Then $q = p_j$ for some j , and for $1 \leq x \leq q - 1$, $(x/p) = (x/q)$. If $j = 1$, so that $q = 5$, then $(3/p) = (3/5) = -1$. But $(3/p) = (p/3) = (1/3) = 1$, by quadratic reciprocity, since $p \equiv 1 \pmod{4}$. If $j > 1$, then $((p_{j-1})/p) = ((p_{j-1})/p_j)$. Again by reciprocity, $(p/(p_{j-1})) = (p_j/p_{j-1})$. But $p \equiv 2p_j \pmod{p_{j-1}}$ makes $(p/(p_{j-1})) = (2p_j/(p_{j-1})) = -(p_j/(p_{j-1}))$. Thus, there would be an infinite number of complete primes after all. \square

The complete primes p with $p \equiv 5 \pmod{8}$ below 1,000 are

5, 13, 37, 61, 109, 157, 181, 229, 277, 349, 373, 397, 421, 541,
613, 661, 709, 757, 829, 877

The least primes $p \equiv 5 \pmod{8}$ that are not complete, as verified by the q listed for $q \leq 61$, are

$p = 29$	733	136,453	4,565,629
$q = 5$	13	37	61

The search for patterns of quadratic residues and non-residues has been conducted for some time. See Peralta (1992) for fairly recent results and a short survey, as well as the related article by Brauer (1969) (from which reference Brauer (1931) was obtained).

5.3 Complete primes below 4,000

3, 5, 7, 13, 17, 23, 37, 41, 61, 71, 73, 89, 97, 109, 113, 137, 157, 181, 191, 193, 229, 233, 241, 257, 277, 281, 311, 313, 337, 349, 353, 373, 397, 401, 409, 421, 433, 449, 457, 479, 521, 541, 569, 577, 601, 613, 617, 641, 661, 673, 709, 719, 757, 761, 769, 809, 829, 839, 863, 877, 881, 911, 929, 937, 953, 977, 1,009, 1,021, 1,033, 1,049, 1,069, 1,093, 1,103, 1,117, 1,129, 1,151, 1,153, 1,193, 1,201, 1,213, 1,237, 1,249, 1,289, 1,297, 1,319, 1,321, 1,361, 1,367, 1,381, 1,409, 1,429, 1,433, 1,439, 1,453, 1,481, 1,489, 1,511, 1,549, 1,559, 1,597, 1,601, 1,607, 1,609, 1,621, 1,657, 1,669, 1,697, 1,721, 1,741, 1,753, 1,777, 1,789, 1,801, 1,861, 1,871, 1,873, 1,889, 1,913, 1,933, 1,993, 2,017, 2,029, 2,053, 2,081, 2,089, 2,113, 2,129, 2,137, 2,153, 2,161, 2,221, 2,269, 2,281, 2,293, 2,297, 2,341, 2,351, 2,377, 2,389, 2,399, 2,417, 2,423, 2,437, 2,441, 2,473, 2,521, 2,557, 2,593, 2,609, 2,617, 2,633, 2,657, 2,677, 2,689, 2,713, 2,729, 2,749, 2,753, 2,777, 2,797, 2,801, 2,833, 2,857, 2,879, 2,897, 2,927, 2,953, 2,969, 2,999, 3,001, 3,037, 3,041, 3,049, 3,061, 3,089, 3,109, 3,121, 3,137, 3,169, 3,181, 3,191, 3,209, 3,217, 3,229, 3,257, 3,301, 3,313, 3,329, 3,359, 3,361, 3,433, 3,449, 3,457, 3,469, 3,529, 3,541, 3,593, 3,613, 3,617, 3,637, 3,671, 3,673, 3,697, 3,709, 3,733, 3,761, 3,769, 3,793, 3,833, 3,853, 3,877, 3,881, 3,889, 3,911, 3,929.

The percentage of odd primes below 10,000 that are complete is about 39.3, and the percentage below 50,000 is about 39. All the computations for this and the preceding subsection were done with Maple.

5.4 *The translation plane for a complete prime*

When the prime p is complete, we obtain a spread in \mathbb{F}_p^4 of planes consisting of the planes \mathcal{P}_k , $0 \leq k \leq p^2 - 1$ and \mathcal{P}_∞ . They produce an affine plane (again, see Lüneburg (1980)) whose points are the members of \mathbb{F}_p^4 and whose lines are the translates of the \mathcal{P}_k . What plane is this? Recall that \mathcal{P}_k is the row space of the matrix M_k , where

$$M_\infty = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, M_h = \begin{bmatrix} 0 & 0 & 1 & j \\ 1 & j & 0 & 0 \end{bmatrix}, \text{ for } 0 \leq j \leq p - 1$$

$$M_{hp+j} = \begin{bmatrix} 0 & 1 & h & j \\ 1 & 0 & j & hn_1 \end{bmatrix}, \text{ for } 1 \leq h \leq p - 1 \text{ and } 0 \leq j \leq p - 1$$

The plane is a Hall plane, and we can prove that in a more general setting.

Theorem 5: *Let q be a power of an odd prime and let n be a non-square in \mathbb{F}_q . Define the matrices M_k almost as above:*

$$M_\infty = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, M_j = \begin{bmatrix} 0 & 0 & 1 & j \\ 1 & j & 0 & 0 \end{bmatrix}, \text{ for } j \in \mathbb{F}_q$$

$$M_{h,j} = \begin{bmatrix} 0 & 1 & h & j \\ 1 & 0 & j & hn \end{bmatrix}, \text{ for } h \in \mathbb{F}_q, h \neq 0 \text{ and } j \in \mathbb{F}_q$$

Then the planes that are the row spaces of the matrices form a spread in \mathbb{F}_q^4 whose corresponding affine plane \mathcal{A} is isomorphic to the Hall plane $H(q)$ (Lüneburg, 1980, Section 13).

Proof: That the planes form a spread is proved the same way as for the planes in the discussion of the lexicographic codes (or more simply from what follows). The planes can be described succinctly by using \mathbb{F}_{q^2} realised as the extension $\mathbb{F}_q(\sqrt{n})$. Think of \mathbb{F}_q^4 as $\mathbb{F}_{q^2}^2$ by identifying (x_1, y_1, x_2, y_2) with $(x_1\sqrt{n} + y_1, x_2\sqrt{n} + y_2)$. Then the member

$$y(0, 1, h, j) + x(1, 0, j, hn) = (x, y, xj + yh, xhn + yj)$$

of the row span of $M_{h,j}$ can be written as $(\zeta, \omega\zeta)$, where $\zeta = x\sqrt{n} + y$ and $\omega = h\sqrt{n} + j$; we denote this plane by \mathcal{P}_ω , the restriction on the slope ω being that $\omega \notin \mathbb{F}_q$. Each of the other $q + 1$ planes comprises the points $(x\alpha, y\alpha)$, where $x, y \in \mathbb{F}_q$ and either $\alpha = 1$ or $\alpha = \sqrt{n} + z$ for some $z \in \mathbb{F}_q$ (an unnecessary restriction serving only to label the planes). Call such a plane \mathcal{B}_α . The planes \mathcal{P}_ω are lines in the affine plane $\mathbb{F}_{q^2}^2$ over \mathbb{F}_{q^2} . The \mathcal{B}_α , on the other hand, are Baer subplanes of $\mathbb{F}_{q^2}^2$. It is easy to see that the conditions (1) and (2) of Lüneburg (1980, p.57) are met by the collection of translates of the \mathcal{B}_α , so that \mathcal{A} is a derived plane of $\mathbb{F}_{q^2}^2$. By the results of Lüneburg (1980, Section 13), \mathcal{A} is isomorphic to the Hall plane $H(q)$. □

6 **Questions**

Questions like the following will probably have occurred to the reader:

- Is there a number-theoretic description of complete primes?
- Lacking that, can one give an asymptotic count of complete primes? By Corollary 3, there are an infinite number of them.

- Does Theorem 4 generalise? Computer exploration might be worthwhile.
- For a complete prime p , how does $\mathcal{L}^{(3)}$ continue beyond $\mathcal{L}_{p^2+1}^{(3)}$, the code described in Section 5?
- For an incomplete prime, how does $\mathcal{L}^{(3)}$ continue in the first run that is not fully booked?
- Is there a succinct description of the development of $\mathcal{L}^{(r)}$ for $r > 3$?
- What happens when $p = 2$? The original work in Conway and Sloane (1986) should figure prominently here. For example, are the corresponding games interesting? One special case is the lexicographic code with divisor 2^m and minimum weight 2^{m+1} , where connections with Reed-Muller codes emerge.
- Are there analogues of the codes for non-prime alphabets? The divisibility criterion in Ward (1990) is rather elaborate for fields of non-prime size.

References

- Assmus, E.F. Jr. and Key, J.D. (1992) *Designs and their Codes, Cambridge Tracts in Mathematics*, Vol. 103, Cambridge: Cambridge University Press.
- Bonisoli, A. (1984) 'Every equidistant linear code is a sequence of dual Hamming codes', *Ars Combinatoria*, Vol. 18, pp.181–186.
- Brauer, A. (1931) 'Ueber den kleinsten quadratischen Nichtrest', *Mathematische Zeitschrift*, Vol. 33, pp.161–176.
- Brauer, A. (1969) 'Combinatorial methods in the distribution of k th power residues', *Combinatorial Mathematics and its Applications (Proceeding Conference, University of North Carolina, Chapel Hill, N.C., 1967)*, University of North Carolina Press, Chapel Hill, N.C., pp.14–37.
- Brualdi, R.A. and Pless, V.S. (1993) 'Greedy codes', *Journal of Combinatorial Theory Series A*, Vol. 64, No. 1, pp.10–30.
- Carlitz, L. (1960) 'A theorem on permutations in a finite field', *Proceeding American Mathematical Society*, Vol. 11, pp.456–459.
- Conway, J.H. (1990) 'Integral lexicographic codes', *Discrete Mathematics*, Vol. 83, Nos. 2–3, pp.219–235.
- Conway, J.H., Curtis, R.T., Norton, S.P., Parker, R.A. and Wilson, R.A. (with computational assistance from J.G. Thackray) (1985) *Atlas of Finite Groups*, Eynsham: Oxford University Press.
- Conway, J.H. and Sloane, N.J.A. (1986) 'Lexicographic codes: error-correcting codes from game theory', *IEEE Transactions on Information Theory*, Vol. 32, No. 3, pp.337–348.
- Herscovici, D.S. (1991) 'Minimal distance lexicographic codes over an infinite alphabet', *IEEE Transactions on Information Theory*, Vol. 37, No. 5, pp.1366–1368.
- Huffman, W.C. and Pless, V. (2003) *Fundamentals of Error-Correcting Codes*. Cambridge: Cambridge University Press.
- Levenštejn, V.I. (1960) 'A class of systematic codes', *Dokl. Akad. Nauk SSSR*, Vol. 131, pp.1011–1014 (Russian); translated as *Soviet Mathematics Doklady*, Vol. 1, pp.368–371.
- Littlewood, D.E. (1970) *A University Algebra*, New York: Dover Publications, Inc.
- Lüneburg, H. (1980) *Translation Planes*. Berlin, New York: Springer-Verlag.
- Niven, I., Zuckerman, H.S. and Montgomery, H.L. (1991) *An Introduction to the Theory of Numbers*. (5th ed.), New York: John Wiley and Sons, Inc.

- Peralta, R. (1992) 'On the distribution of quadratic residues and nonresidues modulo a prime number', *Mathematical Computing*, Vol. 58, No. 197, pp.433–440.
- Rédei, L. (1973) *Lacunary Polynomials over Finite Fields*, Translated from the German by I. Földes, Amsterdam, London: North-Holland Publishing Co.; New York: American Elsevier Publishing Co., Inc.
- Sørensen, A.B. (1991) 'Projective Reed-Muller codes', *IEEE Transactions on Information Theory*, Vol. 37, No. 6, pp.1567–1576.
- Ward, H.N. (1981) 'Divisible codes', *Archiv der Mathematik (Basel)*, Vol. 36, No. 6, pp.485–494.
- Ward, H.N. (1990) 'Weight polarization and divisibility', *Discrete Mathematics*, Vol. 83, Nos. 2–3, pp.315–326.
- Ward, H.N. (2001) 'Divisible codes — a survey', *Serdica Mathematical Journal*, Vol. 27, No. 4, pp.263–278.