Designs, Codes and Cryptography manuscript No.
(will be inserted by the editor)

Divisibility of Polynomials over Finite Fields and Combinatorial Applications

Daniel Panario · Olga Sosnovski · Brett Stevens · Qiang Wang †

September 1, 2011

Abstract Consider a maximum-length shift-register sequence generated by a primitive polynomial f over a finite field. The set of its subintervals is a linear code whose dual code is formed by all polynomials divisible by f. Since the minimum weight of dual codes is directly related to the strength of the corresponding orthogonal arrays, we can produce orthogonal arrays by studying divisibility of polynomials. Munemasa (Finite Fields Appl., 4(3):252-260, 1998) uses trinomials over $\mathbb{F}_2$ to construct orthogonal arrays of guaranteed strength 2 (and almost strength 3). That result was extended by Dewar *et al.* (Des. Codes Cryptogr., 45:1-17, 2007) to construct orthogonal arrays of guaranteed strength 3 by considering divisibility of trinomials by pentanomials over $\mathbb{F}_2$. Here we first simplify the requirement in Munemasa's approach that the characteristic polynomial of the sequence must be primitive: we show that the method applies even to the much broader class of polynomials with no repeated roots. Then we give characterizations of divisibility for binomials and trinomials over $\mathbb{F}_3$. Some of our results apply to any finite field $\mathbb{F}_q$ with q elements.

Keywords Polynomials over finite fields · divisibility of polynomials · orthogonal arrays.

Mathematics Subject Classification (2000) 12E20, 94A55, 05B15

1 Introduction

Maximum-length shift-register sequences are widely used in pseudo-random number generation and several engineering applications [9, 10]. The fewer nonzero terms in the characteristic polynomial of the shift-register sequence, the faster is the generation of the sequence. However, the number of nonzero terms in multiples of the characteristic polynomial determines the statistical bias in the sequence, fewer terms implying more bias [12, 16].

† The authors are supported in part by NSERC of Canada.

School of Mathematics and Statistics, Carleton University
1125 Colonel By Drive, Ottawa, ON, K1S 5B6

A classical result [7] relates the minimum weight of dual codes to the strength of the corresponding orthogonal arrays. In this paper we follow a method introduced by Munemasa [23] that constructs orthogonal arrays. The procedure first constructs a code with subintervals of a shift-register sequence generated by a polynomial f. Its dual code is characterized by all polynomials that are divisible by f. Hence, by studying the divisibility of polynomials we can produce dual codes, thus determining the strength of coverage in the arrays. This suggests studying the divisibility of polynomials over finite fields, and this is the focus of this paper.

This procedure was used by Munemasa [23] for the case trinomials (polynomials with three nonzero terms) dividing trinomials over $\mathbb{F}_2$ to produce orthogonal arrays with guaranteed strength 2 (and almost strength 3). Then, Dewar et al. [8] extended this to pentanomials (polynomials with five nonzero terms) dividing trinomials over $\mathbb{F}_2$ to give orthogonal arrays with guaranteed strength 3.

Dewar et al. [8] suggests extending the results to finite fields other than $\mathbb{F}_2$. Once we are not in $\mathbb{F}_2$ we can consider binomials (there are no irreducible binomials over $\mathbb{F}_2$). We focus on low weight polynomials since we can produce precise results in these cases. However, the general problem of when polynomials over a finite field of given weight divide polynomials of another given weight is interesting and not well understood. As concrete applications of this divisibility problem for ranges on the weight of the polynomials that exceed the results in this paper, see the cryptosystem TCHo [1,13] and the turbo codes applications [24]. Also of interest are some general results on the weights of multiples of polynomials over $\mathbb{F}_2$ which do not depend on the low weight of f [11,14,17,21].

This paper contains results similar to [8] and [23] but for binomials and trinomials over non-binary fields. In Section 2, we define notation and give previous results as well as we outline the general methodology. The most important result in this section is a simplification of Munemasa's conditions: we only require irreducible polynomials (or even reducible ones under the condition of no repeated roots) for the minimal polynomial of the LFSR instead of the primitive polynomial condition in previous results [8,23]. We also give some combinatorial applications for our results. The results in this section are valid for any finite field $\mathbb{F}_q$. Our main results are obtained for finite field $\mathbb{F}_3$. That is why throughout this paper, unless otherwise stated, we use the finite field $\mathbb{F}_3$. Moving from $\mathbb{F}_2$ to $\mathbb{F}_3$ has complicated the proofs considerably. Although in principle one could perhaps extend some of our results to other finite fields, the level of added complications would be even greater with our methodology. We believe that other techniques are needed to obtain similar results over larger finite fields, ideally techniques independent of the base fields. Section 3 focuses on divisibility of binomials by trinomials over $\mathbb{F}_3$. Section 4 deals with the case of trinomials dividing trinomials over $\mathbb{F}_3$. In Section 5, we conclude with some questions for further studies and research.

2 Background and preliminaries

2.1 Definitions and previous results

We give next some required definitions. A polynomial f of degree m is called *primitive* over $\mathbb{F}_q$ if $k = q^m - 1$ is the smallest positive integer such that f divides $x^k - 1$.

A *shift-register sequence* with characteristic polynomial $f(x) = x^m - \sum_{i=0}^{m-1} c_i x^i$ is the sequence $a = (a_0, a_1, \ldots)$ defined by

$$a_{n+m} = \sum_{i=0}^{m-1} c_i a_{i+n} \quad \text{for} \quad n \geq 0.$$

If f is primitive over $\mathbb{F}_q$ the sequence has period $q^m - 1$.

A subset C of $\mathbb{F}_q^n$ is called an *orthogonal array* of strength t if for any t-subset $T = \{i_1, i_2, \ldots, i_t\}$ of $\{1, 2, \ldots, n\}$ and any t-tuple $(b_1, b_2, \ldots, b_t) \in \mathbb{F}_q^t$ there exists exactly $|C|/q^t$ elements $c = (c_1, c_2, \ldots, c_n)$ of C such that $c_{i_j} = b_j$ for all $1 \leq j \leq t$. From the definition, if C is an orthogonal array of strength t, then it is also an orthogonal array of strength s for all $1 \leq s \leq t$.

Orthogonal arrays and codes are related by the next theorem.

Theorem 1 ([2]) *Let C be a linear code over $\mathbb{F}_q$. Then, C is an orthogonal array of maximal strength t if and only if $C^\perp$, its dual code, has minimum weight $t + 1$.*

Delsarte was able to generalize this result to non-linear codes [7]. The following theorem describes the dual code of the code generated by shift-register sequences in terms of multiples of its characteristic polynomial.

Theorem 2 ([23]) *Let f be a primitive polynomial of degree m over $\mathbb{F}_q$ and let $2 \leq n \leq q^m - 1$. Let C_n^f be the set of all subintervals of the shift-register sequence with length n generated by f, together with the zero vector of length n. The dual code of C_n^f is given by*

$$(C_n^f)^\perp = \{(b_1, \ldots, b_n) : \sum_{i=0}^{n-1} b_{i+1} x^i \text{ is divisible by } f\}.$$

Previous studies on divisibility of polynomials and combinatorial applications were done for polynomials over the binary field $\mathbb{F}_2$ [8,23]. Let f be a primitive polynomial of degree m over $\mathbb{F}_2$ and let $a = (a_0, a_1, \ldots)$ be a shift-register sequence with characteristic polynomial f. As in [8], we denote by C_n^f the set of all subintervals of this sequence with length n, where $m < n \leq 2m$, together with the zero vector of length n.

Munemasa [23] investigates the shift-register sequences when f is a trinomial, that is, a polynomial with three terms over $\mathbb{F}_2$.

Theorem 3 ([23]) *Let $f(x) = x^m + x^l + 1$ be a trinomial over $\mathbb{F}_2$ such that $\gcd(m, l) = 1$. If g is a trinomial over $\mathbb{F}_2$ of degree at most $2m$ that is divisible by f, then $g(x) = x^{\deg g - m} f(x)$, $g(x) = f(x)^2$, or $g(x) = x^5 + x^4 + 1 = (x^2 + x + 1)(x^3 + x + 1)$ or, its reciprocal, $g(x) = x^5 + x + 1 = (x^2 + x + 1)(x^3 + x^2 + 1)$.*

The main result in [23] implies that, in the case of a primitive trinomial f satisfying certain properties, C_n^f is an orthogonal array of strength 2 having the property of being very close to an orthogonal array of strength 3. Munemasa [23] shows that for most 3-tuples of $\{1, 2, \ldots, n\}$, the orthogonal property is satisfied, exception to this are the triples of coordinates corresponding to the exponents of trinomials of the form $x^i f$ and f^2.

Munemasa [23] suggested the extension of his results to polynomials f with more than three terms. Dewar et al. [8] extended Munemasa's result to shift-register sequences generated by primitive pentanomials, polynomials with five terms, over $\mathbb{F}_2$.

No.	$f(x)$	$h(x)$	type
1	$x^5+x^4+x^3+x^2+1$	x^3+x^2+1	p
2	$x^5+x^3+x^2+x+1$	x^3+x+1	p
3	$x^5+x^3+x^2+x+1$	x^4+x+1	p
4	$x^5+x^4+x^3+x+1$	x^2+x+1	p
5	$x^6+x^5+x^4+x^3+1$	x^4+x^3+1	r
6	$x^6+x^4+x^2+x+1$	x^3+x+1	i
7	$x^6+x^4+x^3+x+1$	x^2+x+1	p
8	$x^6+x^5+x^2+x+1$	$x^5+x^4+x^3+x+1$	p
9	$x^6+x^5+x^3+x+1$	x^2+x+1	r
10	$x^7+x^4+x^2+x+1$	x^3+x+1	r
11	$x^7+x^4+x^3+x^2+1$	x^3+x^2+1	p
12	$x^7+x^5+x^2+x+1$	$x^7+x^6+x^5+x^4+x^3+x+1$	p
13	$x^7+x^5+x^3+x^2+1$	$x^5+x^4+x^3+x^2+1$	r
14	$x^8+x^5+x^3+x+1$	$x^5+x^4+x^2+x+1$	p
15	$x^8+x^5+x^3+x^2+1$	$x^8+x^7+x^5+x^4+x^3+x^2+1$	p
16	$x^8+x^6+x^3+x+1$	$x^6+x^4+x^2+x+1$	r
17	$x^8+x^7+x^5+x^2+1$	$x^6+x^5+x^4+x^2+1$	r
18	$x^9+x^6+x^5+x^2+1$	$x^8+x^5+x^4+x^2+1$	i
19	$x^9+x^7+x^4+x^3+1$	$x^8+x^6+x^4+x^3+1$	i
20	$x^9+x^8+x^5+x^2+1$	$x^6+x^5+x^4+x^2+1$	r
21	$x^{10}+x^4+x^3+x^2+1$	$x^8+x^7+x^4+x^2+1$	i
22	$x^{10}+x^7+x^2+x+1$	$x^6+x^4+x^3+x+1$	r
23	$x^{11}+x^7+x^6+x^2+1$	$x^8+x^7+x^4+x^2+1$	r
24	$x^{13}+x^{10}+x^2+x+1$	$x^9+x^7+x^6+x^4+x^3+x+1$	r
25	$x^{13}+x^{10}+x^9+x^2+1$	$x^{12}+x^9+x^8+x^6+x^4+x^2+1$	p

Table 1 Table of binary polynomial exceptions in the main theorem of [8]: 'p' in *type* indicates that the given polynomial $f(x)$ is primitive, 'i' indicates that $f(x)$ is irreducible and 'r' indicates that $f(x)$ is reducible.

Theorem 4 ([8]) *Let $f(x)=x^m+x^l+x^k+x^j+1$ be a pentanomial over $\mathbb{F}_2$ such that $\gcd(m,l,k,j)=1$. If g is a trinomial of degree at most $2m$ divisible by f, with $g=fh$, then*

1. *f is one of the polynomial exceptions given in Table 1;*
2. *$m\equiv 1 \bmod 3$ and f,g,h are as follows*

$$\begin{aligned} f(x) &= 1+x+x^2+x^{m-3}+x^m \\ &= (1+x+x^2)(1+x^{m-3}+x^{m-2}), \\ h(x) &= (1+x)+(x^3+x^4)+\cdots+(x^{m-7}+x^{m-6})+x^{m-4}, \\ f(x)h(x)=g(x) &= 1+x^{2m-6}+x^{2m-4}; \text{ or} \end{aligned}$$

3. *f is the reciprocal of one of the polynomials listed in the previous items.*

The result in [8] constructs orthogonal arrays of guaranteed strength at least 3.

2.2 Removing the primitivity condition

In this subsection, we generalize Theorem 2 by removing the primitivity condition for the characteristic polynomial f.

Theorem 5 *Let $\mathbf{a}=(a_0,a_1,a_2,\ldots)$ be a shift-register sequence over $\mathbb{F}_q$ with minimal polynomial $f\in\mathbb{F}_q[x]$, and suppose that f has degree m with m distinct roots. Let ρ be*

the period of f and $2 \leq n \leq \rho$. Let C_n^f be the set of all subintervals of the shift-register sequence $\mathbf{a}$ with length n. Then the dual code of C_n^f is given by

$$(C_n^f)^\perp = \{(b_1, \ldots, b_n) : \sum_{i=0}^{n-1} b_{i+1}x^i \text{ is divisible by } f\}.$$

PROOF. Since $\mathbf{a} = (a_0, a_1, a_2, \ldots)$ is the sequence with minimal polynomial f, the least period $per(a)$ of sequence $\mathbf{a}$ equals $per(f)$ which is denoted by t. Let $\alpha_1, \ldots, \alpha_m$ be all distinct roots of f. Then by Theorem 8.21 in [15], we have $a_n = \sum_{j=1}^{m} \beta_j \alpha_j^n$ for $n = 0, 1, \ldots$.

First we assume that all β_j are nonzero. Hence an element $w = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$ belongs to $(C_n^f)^\perp$ if and only if

$$\sum_{i=0}^{n-1} b_{i+1} \left(\sum_{j=1}^{m} \beta_j \alpha_j^{i+k} \right) = 0, \tag{1}$$

for $k = 0, 1, \ldots, t-1$. Equation (1) can be rewritten as

$$\sum_{j=1}^{m} \left(\sum_{i=0}^{n-1} b_{i+1} \alpha_j^i \right) \beta_j \alpha_j^k = 0, \quad k = 0, \ldots, t-1. \tag{2}$$

Consider the above system of equations with unknown variables $\sum_{i=0}^{n-1} b_{i+1}\alpha_j^i$ and coefficients $\beta_j \alpha_j^k$. There is at least 1 solution (the zero solution). Moreover, we have $t > m$. However, because all $\beta_j \neq 0$ and all α_j are distinct, the first m equations in (2) give a unique solution as the coefficient matrix is an invertible Vandermonde matrix. Therefore, there is only one solution in Equation (2). Hence $\sum_{i=0}^{n-1} b_{i+1}\alpha_j^i = 0$, for all $j = 1, \ldots, m$. This implies that the polynomial $w(x) = \sum_{i=0}^{n-1} b_{i+1}x^i$ is divisible by f.

If not all β_j are nonzero, then, without loss of generality, we assume that $a_n = \sum_{j=1}^{m'} \beta_j \alpha_j^n$ for $n = 0, 1, \ldots$ and $m' < m$. Namely, we assume $\beta_j = 0$ for $j = m'+1, \ldots, m$. We show that each α_j where $j = m'+1, \ldots, m$ must be a conjugate of one of α_j where $j = 1, \ldots, m'$. Otherwise, if there exists one α_{j_0} such that $m'+1 \leq j_0 \leq m$ and α_{j_0} is not a conjugate of any α_j where $j = 1, \ldots, m'$, then all conjugates of α_{j_0} must be in the set $\{\alpha_{m'+1}, \ldots, \alpha_m\}$. Let g be the minimal polynomial with roots α_{j_0} and its conjugates. Then $g \mid f$. Because $a_n = \sum_{j=1}^{m'} \beta_j \alpha_j^n$ for $n = 0, 1, \ldots$, we have that sequence $\mathbf{a}$ is derived by the polynomial f/g, which has degree $< m$, contradicting that f is the minimal polynomial of sequence $\mathbf{a}$. Hence each α_j where $j = m'+1, \ldots, m$ is a conjugate of one of α_j where $j = 1, \ldots, m'$.

Now an element $w = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$ belongs to $(C_n^f)^\perp$ if and only if

$$\sum_{i=0}^{n-1} b_{i+1} \left(\sum_{j=1}^{m'} \beta_j \alpha_j^{i+k} \right) = 0, \tag{3}$$

for $k = 0, 1, \ldots, t-1$. Equation (3) can be rewritten as

$$\sum_{j=1}^{m'} \left(\sum_{i=0}^{n-1} b_{i+1} \alpha_j^i \right) \beta_j \alpha_j^k = 0, \quad k = 0, \ldots, t-1. \tag{4}$$

Consider the above system of equations with unknown variables $\sum_{i=0}^{n-1} b_{i+1}\alpha_j^i$ and coefficients $\beta_j\alpha_j^k$. There is at least 1 solution (the zero solution). Moreover, we have $t > m > m'$. However, because all $\beta_j \neq 0$ for all $1 \leq j \leq m'$ and all α_j are distinct, the first m' equations in (4) give a unique solution as the coefficient matrix is an invertible Vandermonde matrix. Therefore, there is only one solution in Equation (4). Hence $\sum_{i=0}^{n-1} b_{i+1}\alpha_j^i = 0$, for all $j = 1, \ldots, m'$. Furthermore, we obtain $\sum_{i=0}^{n-1} b_{i+1}(\alpha_j^q)^i = (\sum_{i=0}^{n-1} b_{i+1}\alpha_j^i)^q = 0$ because $b_{i+1} \in \mathbb{F}_q$. This implies that a conjugate of α_j where $j = 1, \ldots, m'$ is still a root of w. Because each α_j satisfies that $m' + 1 \leq j \leq m$ is a conjugate of one of α_j such that $1 \leq j \leq m'$, we therefore obtain $f \mid w$. □

Suppose $f = f_1 \cdots f_k$ such that $f_1, \ldots, f_k$ are irreducible polynomials and f satisfies the conditions in Theorem 5. Let (C_n^f) be the code generated by f and $C_n^{f_i}$ be the code generated by each f_i as in Theorem 5. Let C be the union of C_n^f and $C_n^{f_i}$, together with the zero vector of length n. The dual code $C^\perp$ of C is contained in the dual code $(C_n^f)^\perp$ of C_n^f. Therefore, if $(C_n^f)^\perp$ has minimum weight $t+1$, then $C^\perp$ has minimum weight at least $t+1$ as well. If C can be generated by a primitive polynomial of degree m as in Theorem 2, then C is an orthogonal array of strength at least t.

Remarks about combinatorial applications. One of the primary applications suggested by Munemasa [23] was the construction of orthogonal arrays when f is primitive. Theorem 5 shows that orthogonal arrays can be constructed from a far larger class of polynomials. However, the characterization of the dual code in terms of the multiples of the polynomial f demonstrates that other interesting combinatorial objects can be built from these methods. Arrays which have orthogonal or covering properties for a selected collection of subsets of columns, rather than all subsets of columns of a fixed size t, have recently been studied. Indeed, the investigation of *partial orthogonal arrays* [22] was motivated directly by Munemasa's original paper. Another well-known example of arrays which are orthogonal for selected subsets of columns are the (t, m, s)-nets [18]. A *covering array* is a generalization of orthogonal arrays which in its simplest definition requires that for any given set of t columns, every t-tuple appears at least λ times [5]. These are used extensively in reliability testing where each column corresponds to an input or parameter of the system under test and each row corresponds to the settings for one test. This is typically used in a black-box manner assuming nothing about the internal structure of the system. But when internal knowledge of the system is known we can relax the requirement that all t-subsets of columns should be covered and only require coverage for those known to interact. This setting can even be generalized to collections of column subsets of various sizes. There has been a substantial amount of recent work in this area, for examples and more references see [3, 4, 19, 20]. Arrays constructed from shift-register sequences offer a means to construct such objects with coverage over algebraically determined collections of column subsets.

2.3 Notation

In this section, we introduce some notations that are widely used in the remainder of the paper. Also, in the next sections we use the same terminology as in [8]. In particular, when the sum of coefficients in the same column of our figures is 0 we write that corresponding terms x^i *cancel*. Any use of the terminology *up, down, left, above, lower*, etc., is with respect to the layout in the figure.

Notation 1 *Let $\mathbb{F}$ be a field, $f, g, h \in \mathbb{F}[x]$. Let $f(x) = a + bx^k + x^m$ divide $g(x) = c + dx^l + x^n$ such that $n \leq 3m$, $a \neq 0, c \neq 0$ and $fh = g$, where $h(x) = \sum_{i=0}^{d-1} h_i x^i$. We say that l is the "left-over" of g. Moreover, in the expansion of $fh = g$ we get:*

$$\begin{aligned} d &= h_{l-m} + bh_{l-k} + ah_l, \\ h_i &= 0 \quad i \notin [0, 2m], \\ c &\neq 0. \end{aligned}$$

If only $ah_l \neq 0$, then the left-over is of Type 0.
If only $bh_{l-k} \neq 0$, then the left-over is of Type K.
If only $h_{l-m} \neq 0$, then the left-over is of Type M.
If only $h_{l-m} = 0$ and $bh_{l-k} + ah_l \neq 0$, then the left-over is of Type $0K$.
If only $bh_{l-k} = 0$ and $h_{l-m} + ah_l \neq 0$, then the left-over is of Type $0M$.
If only $ah_l = 0$ and $h_{l-m} + bh_{l-k} \neq 0$, then the left-over is of Type KM.
If $ah_l \neq 0$, $bh_{l-k} \neq 0$, $h_{l-m} \neq 0$ and $h_{l-m} + bh_{l-k} + ah_l \neq 0$, then the left-over is of Type $0KM$.

The above notation is given for the case when f is trinomial. If f is binomial we do not have bh_{l-k} term when calculating dx^l. Thus, we do not have left-overs of Type K, $0K$, KM and $0KM$.

In order to better understand all the definitions and notations let us consider the following example in $\mathbb{F}_3$: $f(x) = 2+x^2$, $h(x) = 2+2x^2+x^4$, $g(x) = 1+x^4+x^6$. The example illustrates the case when f is binomial and the term bh_{l-k} is omitted. The product fh corresponds to the left box diagram from Fig. 1, where a column indicates the degree of the monomial in the expansion fh. The boxes in row i correspond to the nonzero coefficients in $f(x) \cdot (h_i x^i)$, $0 \leq i < d$, and the entries in the boxes come from the exponents of the monomials from f yielding this term in the expanded product. The box diagram on the right of Fig. 1 gives the explanation of the figure on the left but using the variable x. Throughout this paper the notation A_b is used to refer to a box in column b containing the label A. For example, in Fig. 1 we say that 0_2 is canceled up with 2_2, since the sum of coefficients is 0. We can see it on the right diagram, $2x^2 + x^2 = 0$. On the diagram, 2_4 is not canceled down with 0_4 since the sum of coefficients in this column is not 0. In this case we have left-over $l = 4$ of Type $0M$.

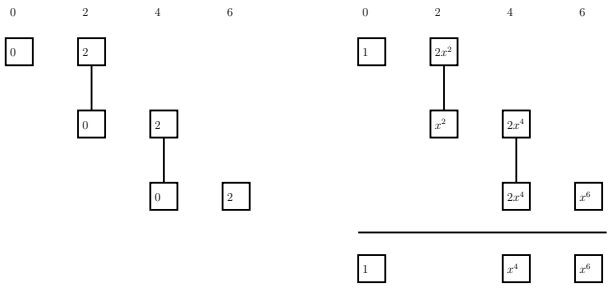

Fig. 1 An illustration of the notation in equation $g(x) = h(x)f(x) = (\sum a_i x^i)f(x)$ with $f(x) = 2 + x^2$, $h(x) = 2 + 2x^2 + x^4$ and $g(x) = 1 + x^4 + x^6$ over $\mathbb{F}_3$.

2.4 Reductions of the problem

In this section, we introduce a result that is used to reduce the problems in the next sections. Let $w(f)$ denote the weight of f, that is, the number of nonzero terms of f.

Theorem 6 *Let $f, g, h \in \mathbb{F}[x]$, $fh = g$, $w(f) = n > 1$ and $w(g) = m$. If there exists an $f_0 \in \mathbb{F}[x]$ such that $f(x) = f_0(x^k)$ for $k > 1$ then there exist $g_i \in \mathbb{F}[x]$, $w(g_i) = m_i$ for $0 \leq i < k$ such that*

$$g(x) = \sum_{i=0}^{k-1} g_i(x^k)x^i, \quad m = \sum_{i=0}^{k-1} m_i, \text{ and } m_i \neq 1. \tag{5}$$

Proof. Suppose that $h(x) = \sum_{i=0}^{d} a_i x^i$ and define $h_i(x) = \sum_{j=0}^{\lceil d/k \rceil} a_{jk+i} x^j$, for $0 \leq i < k$. Thus we have that

$$h(x) = \sum_{i=0}^{k-1} h_i(x^k)x^i. \tag{6}$$

Let $g_i = f_0 h_i$ and define m_i to be the weight of g_i. Equation (5) now follows from $g = fh$ and Equation (6). Since the powers of x in each $g_i(x^k)x^i$ are disjoint sets, m is partitioned into m_i and since every g_i is a multiple of f_0 whose weight is more than 1, we have that $m_i \neq 1$. □

When f is a binomial divisibility by $x - a$ is equivalent to a being a root. We can use this to derive an instance of Theorem 6 for the case when f has weight 2.

Corollary 1 *Let $f(x) = x^k + a \in \mathbb{F}[x]$. Then f divides g with $w(g) = m$ if and only if there exist $g_i \in \mathbb{F}[x]$ with weights $w(g_i) = m_i \neq 1$ such that $g_i(a) = 0$ and*

$$g(x) = \sum_{i=0}^{k-1} g_i(x^k)x^i, \quad m = \sum_{i=0}^{k-1} m_i.$$

Corollary 2 *Let $f, g, h \in \mathbb{F}[x]$, $fh = g$, $w(f) = n$ and $w(g) \leq 3$. If there exists $f_0 \in \mathbb{F}[x]$ such that $f(x) = f_0(x^k)$ for $k > 1$ then there exists $g_0 \in \mathbb{F}[x]$ such that $g(x) = g_0(x^k)$.*

Proof. There are no integer partitions of 2 or 3 that contain more than one nonzero part and that do not contain any part of size 1. □

Thus, considering $w(g) \leq 3$, we may assume that gcd of the exponents of f is 1. This will be used frequently in our proofs.

For example in the case that $w(f) = 2$ and $w(g) \leq 3$, Corollaries 1 and 2 give for binomials dividing binomials:

$$f(x) = x^m + a, \quad g(x) = x^{dm} - (-a)^d;$$

and for binomials dividing trinomials

$$f(x) = x^m + a, \quad g(x) = x^{dm} + \left(-(-a)^{d-k} - c(-a)^{-k}\right) x^{mk} + c, \quad 1 \leq k \leq d-1.$$

3 Trinomials dividing binomials

3.1 Polynomials dividing binomials

There are some general comments which can be given about polynomials dividing binomials. Let $f, g, h \in \mathbb{F}[x]$, where $\mathbb{F}$ is a field, $fh = g$, $w(f) = n > 1$, ρ is the period of f, and $w(g) = 2$. If the degree of g is greater than ρ then Sadjadpour *et al.* [24] describe all possible binomial g in terms of binomial multiples of f whose degree is less than ρ. We start with a couple simple facts. First, if f divides a polynomial of degree d and weight w then f must divide a monic polynomial of the same degree and weight. If f divides two monic polynomials of the same degree then it must divide their difference. These combined with the fact that a non-monomial cannot divide a monomial gives the following fact.

Fact 1 *Let $f \in \mathbb{F}[x]$ and $w(f) > 1$. The polynomial f can divide at most one monic binomial with nonzero constant of any fixed degree.*

A simple induction gives the next fact.

Fact 2 *In $\mathbb{F}[x]$ the following divisibility always holds for any $i \geq 1$:*

$$x^k - a \mid x^{ik} - a^i.$$

Proposition 1 *Let $f \in \mathbb{F}[x]$, $w(f) > 1$ and the period of f be ρ. If f divides a binomial of degree $k < \rho$ with a nonzero constant term, then it must divide a binomial of degree* $\gcd(\rho, k)$.

Proof. If k is not a divisor of ρ then we have $\rho = sk + r$ where $0 < r < k$. Fact 2 now gives that f divides a monic binomial h of degree sk with a nonzero constant term. Now $x^\rho - 1 - x^r h$ results in a binomial of degree r with a nonzero constant term. An induction and the Euclidean algorithm complete the proof. □

We can now conclude that to know everything about f dividing binomials it is sufficient to restrict the attention to monic binomials with nonzero constant terms and degrees that are divisors of the period ρ of f. Fact 2 also gives constraints as to what the constant terms can be as a function of roots of unity in the field $\mathbb{F}$. On this topic there is much known [15]. Sadjadpour *et al.* [24] and Fact 2 construct all others with nonzero constant terms and multiplication by non-trivial monomials yields the rest.

Of course these are quite general statements. In this paper we give more precise statements about binomials as multiples of a polynomial f, of degree m, for a small range of degrees, namely those not more than $\text{char}(\mathbb{F}) \cdot m$.

3.2 Trinomials dividing binomials over $\mathbb{F}_3$

This section focuses on the divisibility of binomials by trinomials over $\mathbb{F}_3$. The main result is given in Theorem 7. As in previous sections, results are derived for monic polynomials f and g such that f divides g. Since we work with $\mathbb{F}_3$, results in Theorem 7 can be extended to that f divides $2g$, $2f$ divides g and $2f$ divides $2g$.

If a polynomial $f \in \mathbb{F}_3[x]$ with $f(0) = 1$ divides polynomial $g(x) = x^n - 1$ then the smallest such n is the period of f and periods of polynomials are well studied [15]. All

other binomials g with $f|g$ and $\deg(g)$ greater than the period of f are characterized by Sadjadpour *et al.* [24].

Next we give results for trinomials dividing binomials over $\mathbb{F}_3$. To enhance readability of the paper we use K's and M's although they are k's and m's.

Theorem 7 *Let $f(x) = a + bx^k + x^m$ $(a, b \neq 0)$ be a monic trinomial over $\mathbb{F}_3$. If $g(x) = c + x^n$ $(c \neq 0)$ is a monic binomial over $\mathbb{F}_3$ with degree at most $3m$ divisible by f, with $g = fh$, then f and g are as given in Table 2.*

Case	$f(x)$	$g(x)$
1.1	$1 + bx^{m/2} + x^m$	$-b + x^{3m/2}$
1.2	$-1 + bx^{m/2} + x^m$	$1 + x^{2m}$
1.3	$1 + bx^{m/2} + x^m$	$-1 + x^{3m}$
1.4	$a + x^{m/3} + x^m$	$-1 + x^{8m/3}$
1.5	$b + bx^{2m/3} + x^m$	$-1 + x^{8m/3}$

Table 2 Polynomials over $\mathbb{F}_3$ such that $g = fh$ for monic trinomial f and monic binomial g.

Proof. The idea is similar to the previous section. If there exists f_0 and $f(x) = f_0(x^k)$ for some integer value k, the problem is reduced to finding binomials g_0 divisible by trinomials f_0.

Thus, we assume that $f_0(x) = a + bx^k + x^m$ and $\gcd(k, m) = 1$. First we consider the case that $m \geq 4$ and $2k > m$. Consider the box diagram in Fig. 2. In order to get the binomial g_0 the left-most and the right-most terms must remain and the rest of the terms must be canceled. So we must have row [1] and row [2] to cancel K_k down with 0_k. Since $(k, m) = 1$, M_m can only be canceled down with 0_m and we must have row [3]. Also row [4] must occur because K_{2k} cancels down with 0_{2k}. Since we have row [4] we have to cancel M_{2m} and K_{3k}. After we cancel them, we get $\deg(g) \geq m + 2k$. Therefore, we need row [5] to cancel M_{m+2k} down with K_{m+2k}. Cancelation with 0_{m+2k} gives $\deg(g) \geq 3m$. Also row [6] must exist to cancel M_{2m} and M_{2m+k} as in Fig. 2.

If $2m \neq 3k$, there are more rows on Fig. 2 to complete all cancelations to get the binomial. If we cancel K_{3k} up, we get a left-over term of Type 0 to the left of M_m. If we cancel K_{3k} down, we get M_{m+3k} term that is not canceled. If we cancel M_{m+3k} down with 0_{m+3k}, we get $\deg(g) > 3m$. If we cancel M_{m+3k} down with K_{m+3k}, we get 0_{m+2k} to the right of M_{2m} and $\deg(g) > 3m$. Therefore, there is no solution in this case.

If $2m = 3k$, and $(k, m) = 1$, we have $m = 3$ and $k = 2$. This contradicts to $m \geq 4$. Therefore, there is no solution in this case.

We have thus proved that for $m \geq 4$, and $2k > m$ there are no trinomials f_0 dividing binomials g_0. Using reciprocity we can state that there are no trinomials f_0 dividing binomials g_0 when $m \geq 4$.

The problem is now reduced to finding those trinomials f_0 of degree at most 3 dividing binomials of degree at most 9. This is a finite problem and can be exhaustively computed. The results are shown in Table 3. The generalization of Table 3 to arbitrary m such that $\gcd(k, m)$ is not necessarily 1 is given in Table 2. □

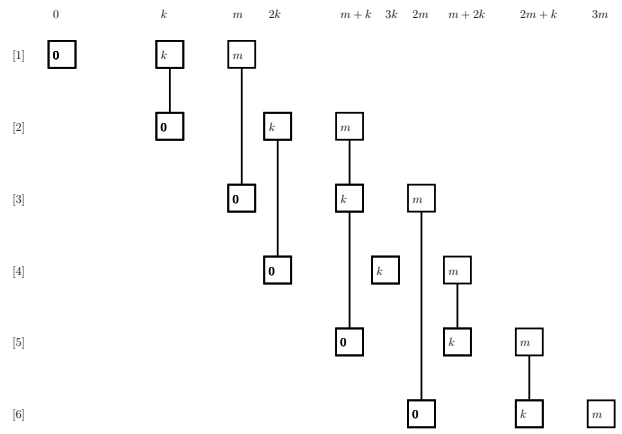

Fig. 2 An illustration of equation $g_0(x) = (\sum a_i x^i) f_0(x)$ with trinomial f_0 and binomial g_0 when $\deg(g) \in [m+1, 3m]$ and $2k > m$ over $\mathbb{F}_3$.

$f_0(x)$	$g_0(x)$	Case in Table 2
$1 + bx + x^2$	$-b + x^3$	1.1
$-1 + bx + x^2$	$1 + x^4$	1.2
$1 + bx + x^2$	$-1 + x^6$	1.3
$a + x + x^3$	$-1 + x^8$	1.4
$b + bx^2 + x^3$	$-1 + x^8$	1.5

Table 3 Polynomials over $\mathbb{F}_3$ with $g_0 = f_0 h_0$ for monic trinomial $f_0(x) = a + bx^k + x^m$, such that $\gcd(k, m) = 1$, and monic binomial g_0.

4 Trinomials dividing trinomials over $\mathbb{F}_3$

This section focuses on the divisibility of trinomials by trinomials over $\mathbb{F}_3$. The main results are shown in Theorem 8. Results are derived for monic polynomials f and g such that f divides g. As before, since we work with $\mathbb{F}_3$, results in Theorem 8 can be extended to f divides $2g$, $2f$ divides g and $2f$ divides $2g$. Again, to enhance readability of the paper we use K's and M's as though they are k's and m's.

Definition 1 Let $f(x) = a + bx^k + x^m$ divide $g(x) = c + dx^l + x^n$ such that $fh = g$ in $\mathbb{F}_3[x]$, and $n \leq 3m$. Let N_k denote the number of K's to the right of $2m$ and N_m denote the number of M's to the right of $2m$.

For example, Fig. 2 shows the case when $N_k = 2$ and $N_m = 3$.

Lemma 1 *Let f, g, h be as above. If $\deg(g) > 2m$, N_k and N_m as defined, then:*

- $N_m = N_k + 1$, *if $l \in (0, 2m]$ of any Type or $l \in (2m, 3m)$ and of Type MK;*
- $N_m = N_k$, *if $l \in (2m, 3m)$ and of Type K;*
- $N_m = N_k + 2$, *if $l \in (2m, 3m)$ and of Type M.*

Proof. All the M's to the right of $2m$ can only be canceled with K's, since canceling with a 0 implies $\deg(g) > 3m$.

If $l \in (0, 2m]$ of any type or $l \in (2m, 3m)$ of Type MK, all but one M to the right of $2m$ can only be canceled (or paired) with K's. The other one corresponds

to the leading term of g. Therefore, for the given condition on the left-over l, we get $N_m = N_k + 1$.

If $l \in (2m, 3m)$ of Type K, all the M's to the right of $2m$ can only be canceled with K's. We have one K for the left-over and one M for the leading term of trinomial g. Therefore, in this case we get $N_m = N_k$.

If $l \in (2m, 3m)$ of Type M, all but two M's to the right of $2m$ can only be canceled with K's: two remain for left-over and for the leading term of trinomial g. Therefore, in this case we get $N_m = N_k + 2$. □

Lemma 2 *Let f, g, h be as above and N_k and N_m as defined. If* $\deg(g) > 2m$ *then:*

- $N_k \leq 1$, *if* $k = 1$;
- $N_k \leq 1$, *if* $l \in (0, 2m]$ *of any Type or* $l \in (2m, 3m)$ *of Type* MK;
- $N_k \leq 2$, *if* $l \in (2m, 3m)$ *of Type* M;
- $N_k = 1$, *if* $l \in (2m, 3m)$ *of Type* K.

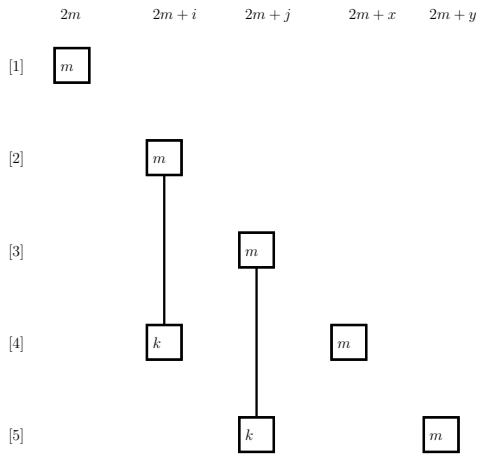

Fig. 3 An illustration of relationship of N_k and left-over in g.

Proof. Let $m > 2k$, otherwise we use the reciprocal of f. Consider the portion of the box diagram for $g = fh$ in Fig. 3. Since we only work with N_k and N_m as defined before, we need to check only what happens to the right of $2m$.

- $l \in (0, 2m]$ of any type or $l \in (2m, 3m)$ of Type MK or $k = 1$
  We assume that $N_k \geq 1$, and therefore row [5] exists and it is the last row in Fig. 3. If $l \in (0, 2m]$ of any type or $l \in (2m, 3m)$ of Type MK we must have row [3] to cancel K_{2m+j} up with M_{2m+j}. If $N_k > 1$ ($l \in (2m, 3m)$ of Type MK) and [4] is the second to last row, we have more M's that are not canceled. If $k = 1$ and l is of any type then the existence of row [5] and the fact that $\deg(g) \leq 3m$ imply that $j = 1$ and row [4] cannot exist. Therefore, $N_k \leq 1$.
- $l \in (2m, 3m)$ of Type M
  Assume [5] is the last row on Fig. 3. Then we have row [3] to cancel K_{2m+j} up with M_{2m+j}. If we have row [4] then we have [2] to cancel K and M in column

$2m+i$. If we have more rows with K's to the right of $2m$ it gives more M's to the right of $2m+j$ that are not canceled. Therefore, $N_k \leq 2$.

– $l \in (2m, 3m)$ of Type K
Assume [5] is the last row on Fig. 3. If $N_k > 1$ then we have more rows above [5] and it gives M's that are not canceled, given that left-over is of Type K. Therefore, $N_k = 1$.

□

Theorem 8 *Let $f(x) = a + bx^k + x^m$ $(a \neq 0, b \neq 0)$ be a monic trinomial over $\mathbb{F}_3$. If $g(x) = c + dx^l + x^n$ $(c \neq 0, d \neq 0)$ is a monic trinomial over $\mathbb{F}_3$ with degree at most $3m$ divisible by f, with $g = fh$, then*

1. *$g = f^3$;*
2. *f and g are as in Table 4; or*
3. *f and g are reciprocals of polynomials listed in Table 4.*

Case	$f(x)$	$g(x)$
1.1	$-1 + bx^{m/2} + x^m$	$1 - bx^{m/2} + x^{3m}$
1.2	$1 + bx^{m/2} + x^m$	$b + x^{m/2} + x^{5m/2}$
1.3	$-1 + bx^{m/2} + x^m$	$b - bx^m + x^{5m/2}$
1.4	$-1 + bx^{m/2} + x^m$	$-b - x^{3m/2} + x^{5m/2}$
1.5	$1 + bx^{m/2} + x^m$	$b + bx^{4m/2} + x^{5m/2}$
1.6	$1 + bx^{m/2} + x^m$	$1 + x^m + x^{2m}$
1.7	$-1 + bx^{m/2} + x^m$	$b + x^m + x^{3m/2}$
1.8	$-1 + bx^{m/2} + x^m$	$-b - bx^m + x^{3m/2}$
1.9	$a - x^{m/3} + x^m$	$-a - x^{m/3} + x^{3m}$
1.10	$a - x^{m/3} + x^m$	$1 + x^{2m/3} + x^{8m/3}$
1.11	$a + x^{m/3} + x^m$	$a + ax^{2m/3} + x^{7m/3}$
1.12	$a - x^{m/3} + x^m$	$a - ax^{4m/3} + x^{7m/3}$
1.13	$a - x^{m/3} + x^m$	$-a + x^{5m/3} + x^{7m/3}$
1.14	$a + x^{m/3} + x^m$	$1 + ax^{5m/3} + x^{2m}$
1.15	$a - x^{m/3} + x^m$	$a + ax^{4m/3} + x^{5m/3}$
1.16	$-1 + bx^{m/4} + x^m$	$-b + bx^{6m/4} + x^{11m/4}$
1.17	$1 + bx^{m/4} + x^m$	$1 + bx^{9m/4} + x^{10m/4}$

Table 4 Table of polynomials such that $g = fh$ with f and g monic trinomials over $\mathbb{F}_3$.

Proof. Let f be a trinomial dividing a trinomial g, where f and g are as given in the statement of the theorem. Let $h(x) = a_0 + a_1x + a_2x^2 + \cdots$ $(a_0 \neq 0)$ such that $g = fh$.

The proof is split into parts. The idea is similar to the proof in the previous section. If there exists $f_0(x)$ and $f(x) = f_0(x^k)$ for some integer value k, the problem is reduced to finding trinomials g_0 divisible by trinomials f_0. Thus, we assume that $\gcd(m, k) = 1$. We get two cases:

1. $(k, m) = 1, \quad k \neq 1$;
2. $k = 1$.

1. $(k, m) = 1, \quad k \neq 1$

In this part we only consider the case when $m > 2k$; using reciprocity we can extend the results to $m < 2k$. The proof in this part is divided into subcases according to the

type and position of the left-over, l. We assume for the whole case 1 that $m = jk + i$ and $i < k$.

(a) $l \in (0, m)$ of Type K
Consider the box diagram for $g = fh$ from Fig. 4. In order to get the trinomial g, the left-most, the right-most and one of the middle terms must remain and the rest of the terms must cancel. On the diagram we always have row [1]. Since left-

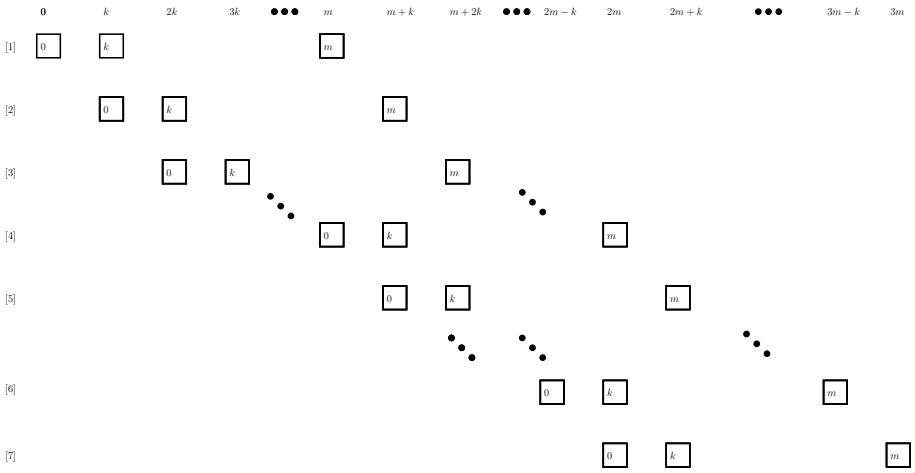

Fig. 4 An illustration of $g(x) = (\sum a_i x^i) f(x)$ with f, g trinomials over $\mathbb{F}_3$ for case 1(a).

over is of Type K and $\gcd(k, m) = 1$ and $k \neq 1$, we need row [4] to cancel M_m (corresponds to M in column m) with 0_m.
Assume that K_{m+k} is canceled up only by M_{m+k}, thus we have row [2]. We get the following system of equations:

$$\begin{aligned} ba_m + a_k &= 0, && \text{column m+k,} \\ aa_m + a_0 &= 0, && \text{column m,} \\ aa_k + ba_0 &= 0, && \text{column k.} \end{aligned}$$

Rearranging the above equations we get

$$aba_m = 0,$$

contradicting that $a \neq 0$, $b \neq 0$ and $a_m \neq 0$, since we always have row [4].
We have shown that K_{m+k} cannot be canceled up only, and we have row [5]. According to Lemmas 1 and 2, $N_k \leq 1$ and $N_m \leq 2$. Therefore, we can only have at most 1 more row after [5]. We must have row [7] to cancel M_{2m} down by 0_{2m} and cancel M_{2m+k} down by K_{2m+k}. There are no more rows between [5] and [7]. Thus, K_{m+2k} cancels up with M_{m+2k} in row [3]. Next, row [2] must be present to cancel 0_{2k} up with K_{2k} and 0_k up with K_k. There are no rows between [3] and [4] because otherwise we get extra M's between m and $2m$. They cannot be canceled since no more rows are possible between [5] and [7]. The solution in this case is

$$f(x) = a + bx^k + x^m, \quad g(x) = a + bx^{3k} + x^{3m},$$

corresponding to the trivial case $g(x) = f^3(x)$.

(b) $l \in (0, m)$ of Type $K0$ or 0
Consider the box diagram for $g = fh$ from Fig. 5. In order to get the trinomial g, the left-most, the right-most and one of the middle terms must remain and the rest of the terms must cancel.

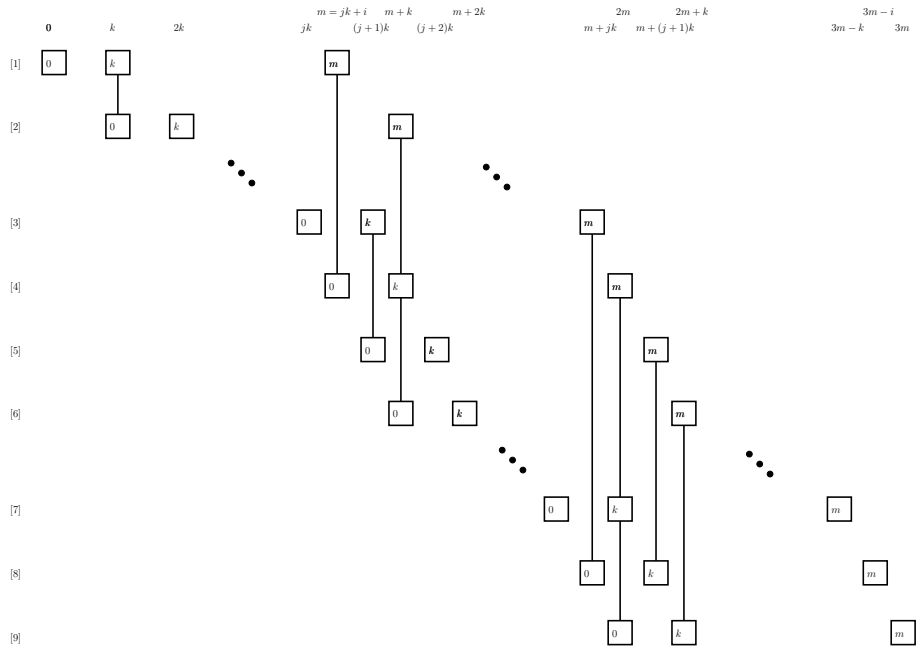

Fig. 5 An illustration of $g(x) = (\sum a_i x^i) f(x)$ with f, g trinomials over $\mathbb{F}_3$ for cases 1(b)-1(g).

On the diagram we always have rows [1]-[3], since $m > 2k$ and left-over is of Type $K0$ or 0, all the K's must be canceled with 0's or matched with 0's (in case left-over is of Type $K0$). There are some rows possible between [1]-[2] and [2]-[3]. For now the type of l does not matter, since we have to cancel or match all K's to the left of m. According to Lemma 2, $N_k \leq 1$. According to Lemma 1, $N_m = N_k + 1$, i.e. at most 2 rows are possible below [4].
Assume $N_k = 0$. If we have row [4] then M_{m+jk} cancels down with K_{m+jk} (observe that if M_{m+jk} cancels down with a 0, then there is a k to the right of $2m$) and M_{2m} cancels down with row [7]. We have at least one M between $2m$ and $3m - k$ that is not canceled. If we do not have row [4] then row [6] must exist to cancel M_{m+k} down. Also M_m cancels down with K_m and it gives one more M between $m + k$ and $m + jk$. We still have to cancel at least two M's between $m + k$ and $m + jk$ and cancel M_{2m+k}. However, only one more row is allowed below [4]. Therefore, there is no solution for this case when $N_k = 0$.
Assume $N_k = 1$. If we have row [8] then row [5] must exist and there is no row [4]. Therefore, M_m is not canceled. If we have row [9] then rows [4] and [6] must exist. No more rows are allowed below [4] and therefore $K_{(j+1)k}$ must be canceled

up. Therefore, there will be more rows between [2] and [3] to cancel all extra K's which will give more M's between $m+k$ and $2m$ that are not canceled. Therefore, there is no solution in this case when $l \in (0, m)$ of Type $K0$ or 0.

(c) $l = m$
Consider the box diagram for $g = fh$ from Fig. 5. On the diagram we always have row [1]-[3], since $m > 2k$. There are some possible rows between [2] and [3]. Then we have row [5] to cancel $K_{(j+1)k}$ down and row [8] to cancel $M_{m+(j+1)k}$ down. Thus, we have $N_m \geq 2$ and Lemmas 1 and 2 give $N_m = 2$, $N_k = 1$ and no other rows below [4] other than [5] and [8]. Therefore, $K_{(j+2)k}$ is not canceled (it cannot be canceled up since $(k, m) = 1$) and there is no solution in this case.

(d) $l \in (m, 2m]$
Consider the box diagram for $g = fh$ from Fig. 5. On the diagram, as before, we always have row [1]-[3], since $m > 2k$. There are some possible rows between [2] and [3]. Since $(k, m) = 1$ and $k \neq 1$ we have row [4]. Let $m = jk + i$, $j \geq 2$, $1 \leq i < k$. This holds for remaining cases when $k \neq 1$.
According to Lemmas 1 and 2, $N_k \leq 1$, $N_m = N_k + 1$ and at most 2 rows are possible below [4]. If $l \neq (j+1)k$ then we have [5] to cancel $K_{(j+1)k}$ down and row [8] to cancel $M_{m+(j+1)k}$ down, since only one row is possible between [4] and [8] and we have [5]. Therefore $K_{(j+2)k}$ and M_{2m} are not canceled and there is no solution in this case.
Let $l = (j+1)k$. If l is of Type $K0$ then again we have [5] and [8] and therefore $K_{(j+2)k}$ and M_{2m} are not canceled and there is no solution in this case. If l is of Type K then we do not have [5] and [8]. Now we need to cancel M_{m+jk} and we get $\deg(g) > 2m$. Therefore, we also need to cancel M_{2m}. Since we do not have [8], we can only cancel M_{m+jk} down with K_{m+jk}. This implies the existence of a row beneath row [4] which, because of the gcd condition, cannot be row [7]. If we also have row [7] to cancel M_{2m} down with K_{2m}, we get two M's to the right of M_{2m} that are not canceled. Therefore, [7] does not exist and we have [9] to cancel M_{2m} down with 0_{2m}. The row [6] must exist to cancel K_{2m+k} up with M_{2m+k} and M_{m+jk} down with K_{m+2k}. We have $m + 2k = m + jk$ and $j \geq 2$ gives $j = 2$. Therefore, the solution in this case is

$$f(x) = a + bx^k + x^m, \quad g(x) = a + bx^{3k} + x^{3m},$$

corresponding to the trivial case $g(x) = f^3(x)$.

(e) $l \in (2m, 3m]$ of Type K
According to Lemmas 1 and 2, $N_m = N_k = 1$. Therefore, no rows are possible between [4] and [8]. Therefore, $K_{(j+1)k}$ is not canceled and there is no solution in this case.

(f) $l \in (2m, 3m]$ of Type M
According to Lemma 1, $N_m = N_k + 2$. Therefore, we have at most two rows between [4] and [8]. If we have [9], then we must have [6] to cancel K_{2m+k} up. We have [5] to cancel $K_{(j+1)k}$ down. We already have two rows between [4] and [8] and $K_{(j+2)k}$ is not canceled down. Also $K_{(j+2)k}$ cannot cancel up with $M_{(j+2)k}$ because $\gcd(k, m) = 1$. Therefore, there is no solution in this case.
If we do not have [9], then we have [7] to cancel M_{2m} down. We have [5] to cancel $K_{(j+1)k}$ down. We already have two rows between [4] and [8] and $K_{(j+2)k}$ has to be canceled. We can cancel it only with 0_{2m-k} and get

$$(j+2)k = 2m - k,$$

Solving for $(k, m) = 1$, $m = jk + i$ and $j \geq 2$ we get $m = 5$, $k = j = 2$ and $i = 1$. We should have row [8] to cancel M_{m+jk} and $M_{m+(j+1)k}$ down. We can write the following system of equations:

$$
\begin{array}{rrrrrrrrrrl}
a_9 & & & & & & & & = 1, & \text{column 3m-i,} \\
 & a_8 & & & & & & & \neq 0, & \text{column 3m-k,} \\
ba_9 + & & a_6 & & & & & & = 0, & \text{column m+(j+1)k,} \\
aa_9 + & & & & a_4 & & & & = 0, & \text{column m+jk,} \\
 & ba_8 + & & a_5 & & & & & = 0, & \text{column 2m,} \\
 & aa_8 + & ba_6 & & & & & & = 0, & \text{column (j+2)k,} \\
 & & aa_6 + & & ba_4 & & & & = 0, & \text{column (j+1)k,} \\
 & & & ba_5 + & & a_2 & & & = 0, & \text{column m+k,} \\
 & & & aa_5 + & & & a_0 & = 0, & \text{column m=jk+i,} \\
 & & & & aa_4 + & ba_2 & & & = 0, & \text{column 2k=jk,} \\
 & & & & & aa_2 + & ba_0 & = 0, & \text{column k.}
\end{array}
$$

Rearranging the above equations we get

$$ab = 0,$$

contradicting that $a \neq 0$, $b \neq 0$. Therefore, there is no solution in this case.

(g) $l \in (2m, 3m]$ of Type MK
According to Lemma 1, $N_m = N_k + 1$. Therefore, we have at most two rows below [4]. Again we cannot have [8] and [9] at the same time.
Assume we have [9]. Then we have [6] and this is the only row between [4] and [9]. Therefore, $K_{(j+1)k}$ is not canceled and there is no solution in this case.
Assume we have [8]. Then we have [5] and this is the only row between [4] and [8]. Therefore, M_{2m} is not canceled and there is no solution in this case.

2. $k = 1$. First suppose $m \geq 6$. According to Lemma 1 and Lemma 2 we have

- if $l \leq 2m$, then $N_k \leq 1$ and $N_m \leq 2$;
- if $l > 2m$, then
  . l is Type M: $N_k \leq 1$ and $N_m \leq 3$;
  . l is Type K: $N_k = 1$ and $N_m = 1$;
  . l is Type MK: $N_k \leq 1$ and $N_m \leq 2$.

This means that, for $k = 1$, $N_m \leq 3$. Therefore, we can consider the following cases according to N_m (the number of nonzero coefficients a_i of polynomial $h(x)$, $i \in [m + 1, 2m]$, where $fh = g$):

(a) $N_m = 3$
According to the above statement, this case is possible only if $l > 2m$ and l is of Type M. Consider the box diagram for $g = fh$ from Fig. 6. We always have rows [1]-[4] to cancel all 0's and 1's to the left of M_m. In general, the total of m rows must exist between [1] and [4] inclusive. Since $N_m = 3$, one of the M's to the right of $2m$ has to be canceled down with 1. Since $N_k \leq 1$, we have row [7] and row [6] to cancel 1_{2m+1} up with M_{2m+1} and only one more row must exist between [6] and [7] inclusive to give left-over of Type M. Since $m \geq 6$, there are at least three M's between $m + 3$ and $2m - 1$ inclusive that are not canceled. All three of them cannot be canceled with a single row. Therefore, there is no solution in this case.

(b) $N_m = 2$
This case is possible if either $l \leq 2m$ of any type, or $l > 2m$ and l of Type MK or M.

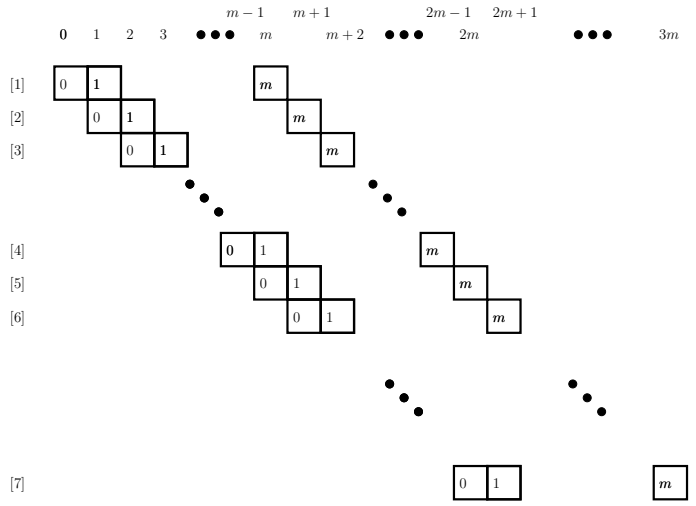

Fig. 6 An illustration of $g(x) = (\sum a_i x^i) f(x)$ with f, g trinomials over $\mathbb{F}_3$ and $k = 1$.

i. $l \leq 2m$
If $l \geq m$ or $l < m$ and of Type $0K = 01$ then consider the box diagram for $g = fh$ from Fig. 6. Here we have a similar situation as in 2(a). There are at least two M's between $m+3$ and $2m-2$ (inclusive) that are not canceled. One of them can be part of left-over, but others are not canceled. Therefore, there is no solution in this case.
Consider $l < m$ of Type $K = 1$. Here we have a similar situation as in 1(a). The flow of the proof is exactly the same and we get trivial solution $g(x) = f^3(x)$. The case when $l < m$ of Type $K = 0$ cannot happen because $k = 1$ and either all 1's canceled with 0's or there are 2 left-overs 0 and 1.

ii. $l > 2m$ and l of Type MK
We have a similar situation as in 2(b)i. and the same box diagram for $g = fh$ from Fig. 6 that contains rows as discussed earlier. The difference is that there are no more rows allowed between [6] and [7]. This means that for given $m \geq 6$, there are at least two M's between $m+3$ and $2m-2$ (inclusive) that are not canceled. Therefore, there is no solution in this case.

iii. $l > 2m$ and l of Type M
Here we have a similar situation as in previous part. Again there are at least five M's between $m+2$ and $2m$ that need to be canceled by at most two rows below [5]. Therefore, there is no solution in this case.

(c) $N_m = 1$
This case is possible if $l > 2m$ and l is of Type K or $l \leq 2m$.

i. $l > 2m$ and l is of Type K
Here we have a similar situation as in 2(a). We have the same box diagram for $g = fh$ from Fig. 6 that contains rows as discussed earlier. The difference is that there are no more rows allowed between [5] and [7] (row [7] is required in order to get left-over of Type K). This means that for given $m \geq 6$, there are at least four M's between $m+2$ and $2m-1$ (inclusive) that are not canceled. Therefore, there is no solution in this case.

ii. $l \leq 2m$
If $l \geq m$ or $l < m$ of Type 01 then consider the box diagram for $g = fh$ from Fig. 6. We always have rows [1]-[4] to cancel or match all 0's to the left of M_m. All m rows between [1] and [4] inclusive are present. Even if there is row [5] to cancel M_{m+1} down with 1_{m+1}, for given $m \geq 6$ there are at least five M's between $m+2$ and $2m$ or $m+1$ and $2m-1$ (inclusive). Only one row is allowed below row [5] that can cancel two M's, one M is left-over and there are still $m-1-3 \geq 2$ M's that are not canceled. Thus, there is no solution in this case.
Consider $l < m$ of Type $K = 1$ and the box diagram for $g = fh$ from Fig. 6. Since $l < m$, we have row [1] and [5] to cancel M_m down with 0_m. If row [6] is present then $N_m = 1$ shows this is the last row. Also M_{2m} must cancel down and this cannot be done. Therefore, row [6] is absent and we must have row [2] to cancel 1_{m+1} up with M_{m+1} and 1_1 down with 0_1. Having one more row below [5] leads to cancelation of M_{2m} and existence of row [4] and therefore we have to cancel all 0's to the left of M_m. This contradicts that the left-over is of Type 1. Therefore, there is no solution in this case.
The case $l < m$ of Type 0 is not possible since it gives K to the left of M_m that is not canceled.

(d) $N_m = 0$
In this case we get that no rows exist below [5]. In 1(a) we proved that the case with only rows [1], [2] and [5] is not possible. If we have other rows between [2] and [5] we get M's between M_{m+1} and M_{2m} and K's to the left of M_m that are not canceled. Therefore, there are no solutions in this case.

According to the above results, given $m \geq 6$, there is only one case possible for trinomial f diving trinomial g, when $g = f^3$. This means the problem is reduced to $m \leq 5$ which is a finite problem and can be computed with our program. Running the program, the results in Table 5 are obtained. □

$f_0(x)$	$g_0(x)$	Case in Table 4
$-1+bx+x^2$	$1-bx+x^6$	1.1
$1+bx+x^2$	$b+x+x^5$	1.2
$-1+bx+x^2$	$b-bx^2+x^5$	1.3
$-1+bx+x^2$	$-b-x^3+x^5$	1.4
$1+bx+x^2$	$b+bx^4+x^5$	1.5
$1+bx+x^2$	$1+x^2+x^4$	1.6
$-1+bx+x^2$	$b+x^2+x^3$	1.7
$-1+bx+x^2$	$-b-bx^2+x^3$	1.8
$a-x+x^3$	$-a-x+x^9$	1.9
$a-x+x^3$	$1+x^2+x^8$	1.10
$a+x+x^3$	$a+ax^2+x^7$	1.11
$a-x+x^3$	$a-ax^4+x^7$	1.12
$a-x+x^3$	$-a+x^5+x^7$	1.13
$a+x+x^3$	$1+ax^5+x^6$	1.14
$a-x+x^3$	$a+ax^4+x^5$	1.15
$-1+bx+x^4$	$-b+bx^6+x^{11}$	1.16
$1+bx+x^4$	$1+bx^9+x^{10}$	1.17

Table 5 Polynomials over $\mathbb{F}_3$ such that $g_0 = f_0 h_0$ with monic trinomial f_0 and monic trinomial g_0.

5 Conclusion

Divisibility of polynomials over finite fields with control of their weights is not well understood, even though it has many concrete practical applications. In this paper we study the divisibility of binomials and trinomials by binomials and trinomials over finite fields. We mostly focus in $\mathbb{F}_3$. Natural extensions are to consider polynomials with more monomials and larger finite fields.

The overall goal of the area is to completely characterize when polynomials of certain weight divide polynomials of another weight. Unfortunately, this seems to be out of reach with the known methods. We cannot use our methods for an arbitrary field as the field grows, the number of ways of cancelling explodes; this causes the system of equations to have many solutions. New techniques are required to go beyond fewnomials (polynomials with few monomials) dividing fewnomials as the ones presented in this paper. We feel it is important that the next steps in the research should be to find a method which works over an arbitrary field and not just a method to solve the next largest field or the next highest weight.

References

1. J. Ph. Aumasson, M. Finiasz, W. Meier and S. Vaudenay, TCHo: a Hardware-Oriented Trapdoor Cipher, *Proc. ACISP'07*, LNCS 4586, 184–199, 2007.
2. R. C. Bose, On some connections between the design of experiments and information theory, *Bull. Inst. Internat. Statist.*, 38:257–271, 1961.
3. C. T. Cheng, The test suite generation problem: optimal instances and their implications, *Discrete Applied Mathematics*, 155:1943–1957, 2007.
4. M. B. Cohen, C. J. Colbourn, J. S. Collofello, P. B. Gibbons and W. B. Mugridge, Variable strength interaction testing of components, *Proc. 27th Internat. Comp. Softw. and Applications*, 413–418, 2003.
5. C. J. Colbourn, Covering arrays, *Handbook of Combinatorial Designs*, Chapter VI.10, 361–364, 2007.
6. C. J. Colbourn and J. H. Dinitz (eds.), Handbook of Combinatorial Designs, *Discrete Mathematics and its Applications, Chapman & Hall/CRC*, second edition, 2007.
7. P. Delsarte, Four fundamental parameters of a code and their significance, *Information and Control*, 23:407–438, 1973.
8. M. Dewar, L. Moura, D. Panario, B. Stevens and Q. Wang, Division of trinomials by pentanomials and orthogonal arrays, *Designs, Codes and Cryptography*, 45:1–17, 2007.
9. S. Golomb, Shift Register Sequences, *Aegean Park Press*, 1982.
10. S. Golomb and G. Gong, Signal Design for Good Correlation, *Cambridge University Press*, 2005.
11. K. C. Gupta and S. Maitra, Multiples of primitive polynomials over GF(2), In *Progress in cryptology—INDOCRYPT 2001 (Chennai)*, volume 2247 of *Lecture Notes in Comput. Sci.*, pages 62–72. Springer, Berlin, 2001.
12. H. F. Jordan and D. C. M. Wood, On the distribution of sums of successive bits of shift-register sequences, *IEEE Transactions on Computers*, C-22:400–408, 1973.
13. M. Herrmann and G. Leander, A practical key recovery attack on basic TCHo, *Proc. PKC 2009*, LNCS 5443, 411–424, 2009.
14. K. Jambunathan, On choice of connection-polynomials for LFSR-based stream ciphers, In *Progress in cryptology—INDOCRYPT 2000 (Calcutta)*, volume 1977 of *Lecture Notes in Comput. Sci.*, pages 9–18. Springer, Berlin, 2000.
15. R. Lidl and H. Niederreiter, Introduction to Finite Fields and their Applications, *Cambridge University Press*, 1994.
16. J. H. Lindholm, An analysis of the pseudo-randomness properties of subsequences of long m-sequences, *IEEE Transactions on Information Theory*, IT-14, 569-576, 1968.
17. S. Maitra, K. C. Gupta, and A. Venkateswarlu, Results on multiples of primitive polynomials and their products over GF(2), *Theoretical Computer Science*, 341(1-3):311–343, 2005.

18. W. J. Martin, (t, m, s)-nets, *Handbook of Combinatorial Designs*, Chapter VI.59, 361–364, 2007.
19. K. Meagher, L. Moura and L. Zekaoui, Mixed covering arrays on graphs, *Journal of Combinatorial Designs*, 15: 393–404, 2007.
20. K. Meagher and B. Stevens, Covering arrays on graphs, *Journal of Combinatorial Theory, Series B*, 95: 134–151, 2005.
21. G. L. Mullen and D. Panario (eds.), Handbook of Finite Fields, *Discrete Mathematics and its Applications, Chapman & Hall/CRC*, to appear.
22. G. L. Mullen and J. Yucas, private communication.
23. A. Munemasa, Orthogonal arrays, primitive trinomials, and shift-register sequences, *Finite Fields and their Applications*, 4(3):252–260, 1998.
24. H. Sadjadpour, N. Sloane, M. Salehi and G. Nebe, Interleaver Design for Turbo Codes, *IEEE Journal On Selected Areas In Communications*, 19(5):831–837, 2001.