Division of Trinomials by Pentanomials and Orthogonal Arrays [*]

Michael Dewar
Department of Mathematics
University of Illinois
Urbana, IL 61801, USA
mdewar2@math.uiuc.edu

Lucia Moura
School of Information Technology and Engineering,
University of Ottawa,
Ottawa, ON, K1N 6N5
lucia@site.uottawa.ca

Daniel Panario, Brett Stevens, Qiang Wang
School of Mathematics and Statistics
Carleton University
1125 Colonel By Drive
Ottawa ON K1S 5B6, Canada
{daniel,brett,wang}@math.carleton.ca

November 7, 2006

Abstract

Consider a maximum-length binary shift-register sequence generated by a primitive polynomial f of degree m. Let C_n^f denote 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 [11] considered the case in which the polynomial f generating the sequence is a trinomial satisfying certain conditions. He proved that, in this case, C_n^f corresponds to an orthogonal array of strength 2 that has a property very close to being an orthogonal array of strength 3. Munemasa's result was based on his proof that very few trinomials of degree at most $2m$ are divisible by the given trinomial f. In this paper, we consider the case in which the sequence is generated by a pentanomial f satisfying certain conditions. Our main result is that no trinomial of degree at most $2m$ is divisible by the given pentanomial f, provided that f is not in a finite list of exceptions we give. As a corollary, we get that, in this case, C_n^f corresponds to an orthogonal array of strength 3. This effectively minimizes the skew of the Hamming weight distribution of subsequences in the shift-register sequence.

[*] The authors are supported by NSERC of Canada.

1 Introduction

Maximum-length shift-register sequences are widely used in pseudo-random number generation and have been shown in [11] to yield orthogonal arrays. The fewer non-zero terms in the characteristic polynomial, the faster is the generation of the sequence. However, the number of non-zero terms in multiples of the characteristic polynomial determines the statistical bias in the sequence, fewer terms implying more bias.

Let f be a primitive polynomial of degree m over $\mathbb{F}_2$ and let $a = (a_0, a_1, \dots)$ be a shift-register sequence with characteristic polynomial f. 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 [11] investigates the shift-register sequences when f is a trinomial, that is, a polynomial with three terms. His main result 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. More precisely, he shows that for most 3-tuples of $\{1, 2, \dots, n\}$, the orthogonal property is satisfied, except at those triple coordinates corresponding to the exponents of trinomials of the form $x^i f$ and f^2. This means that the third moment of the Hamming weight is small, as desired for less statistical bias [7, 9].

A natural extension of this work is the study of shift-register sequences generated by primitive pentanomials, polynomials with five terms. It is known that primitive trinomials over $\mathbb{F}_2$ do not exist for every degree (for example, see [3, 12]). There exists some empirical evidence that irreducible pentanomials over $\mathbb{F}_2$ do exist for every degree [3, 12]. Hansen and Mullen [5] conjectured that there exists a primitive polynomial of degree m over $\mathbb{F}_p$ of weight at most 5 for any prime p (the *weight* of a polynomial is the number of non-zero coefficients) and $m \geq 2$, and if p is not 2 or 3, then such a primitive polynomial exists with weight at most four (see also [10]). Pentanomials have the next smallest number of terms, after trinomials, that is possible in a primitive polynomial over $\mathbb{F}_2$, allowing a fast generation of a shift-register sequence when primitive trinomials are not available. In addition, the usage of pentanomials when trinomials do not exist is in the IEEE standard specifications for public-key cryptography [6].

In this paper, we extend Munemasa's study of bias in binary shift register sequences, primitive polynomials and orthogonal arrays. His main result is based on a theorem about the divisibility of trinomials by trinomials, which we state next in slightly modified form. Throughout this paper, unless otherwise stated, we are using the binary field $\mathbb{F}_2$. The *reciprocal* of a polynomial f of degree n is defined to be $\mathrm{rec}(f) = x^n f(\frac{1}{x})$.

Theorem 1.1 (Munemasa [11]). *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 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, $g(x) = x^5+x+1 = (x^2+x+1)(x^3+x^2+1)$.*

Munemasa [11] suggests the extension of his results to polynomials f with more than three terms. Our main theorem, which is on the divisibility of trinomials by pentanomials, is stated next. Note that Munemasa's result does not require the polynomial to be primitive or even irreducible although this is the primary application. Our results will be similar.

Theorem 1.2. *(Main Theorem) 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; or*

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.*

We observe that the polynomials in the infinite family in case 2. of Theorem 1.2, and their reciprocals, are reducible. We immediately get the following corollary since the largest degree among the irreducible polynomial exceptions f in Table 1 is 13.

Corollary 1.3. *If* $f(x) = x^m + x^l + x^k + x^j + 1$ *is irreducible over* $\mathbb{F}_2$ *with* $\gcd(m, l, k, j) = 1$ *and* $m \geq 14$, *then* f *does not divide any trinomials of degree less than or equal to* $2m$.

In particular, this is true for f primitive, since primitive polynomials are irreducible. In addition, it can be shown that for any primitive pentanomial f, the above GCD condition is satisfied; indeed, if d is a common divisor of m, l, k, j, then we can show that f divides $x^{d(2^{m/d}-1)} - 1$, but $d(2^{m/d} - 1) < 2^m - 1$. Using these facts, plus Theorems 2.1 and 2.2 (similarly used in [11]), we can now state a result about the strength of orthogonal arrays given by shift-register sequences generated by primitive pentanomials.

Corollary 1.4. *If* $f(x) = x^m + x^l + x^k + x^j + 1$ *is primitive over* $\mathbb{F}_2$ *and not one of the exceptions in Table 1 or their reciprocals, then, for* $m < n \leq 2m$,

1. C_n^f *is an orthogonal array of strength at least 3; or equivalently,*

2. $(C_n^f)^\perp$, *the dual code of* C_n^f, *has minimum weight at least* 4.

The fact that C_n^f has strength 3 implies that the third moment of the Hamming weight of the shift-register sequence is minimized [7, 9].

In Section 2, we give some basic definitions and results. In Section 3, we reprove Munemasa's result on divisibility of trinomials by trinomials, as a way of introducing our proof method. In Section 4, we divide the problem into cases (Lemma 4.1 and Lemma 4.2) and sketch the proof of our main result (Theorem 1.2). The complete proof can be found in the appendix. In Section 5, we conclude with some open questions.

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 polynomial exceptions: '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.

2 Shift-register sequences, codes and orthogonal arrays

Again, in this article, unless otherwise specified, we consider the binary field, $\mathbb{F}_2$. A polynomial f of degree m is called *primitive* if $k = 2^m - 1$ 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 the recurrence relation

$$a_{n+m} = \sum_{i=0}^{m-1} c_i a_{i+n},$$

for $n \geq 0$. We refer the reader to [4, 8] for more information on primitive polynomials and shift-register sequences.

A subset C of $\mathbb{F}_2^n$ 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 $(b_1, b_2, \ldots, b_t) \in \mathbb{F}_2^t$, there exists exactly $|C|/2^t$ 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 $1 \leq s \leq t$.

The next theorem, due to Delsarte [1], relates orthogonal arrays with codes.

Theorem 2.1. *[1] 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 $t+1$.*

The following result (Lemma 5.1 in [11]) describes the dual code of the code generated by shift register sequences in terms of multiples of its characteristic polynomial.

Theorem 2.2. *[11] Let f be a primitive polynomial of degree m over $\mathbb{F}_2$ and let $2 \leq n \leq 2^m - 1$. 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*

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

It is easy to see that $(C_{2^m-1}^f)^{\perp}$ is the Hamming code, which has minimum distance 3, and so, by Theorem 2.1, C_n^f is an orthogonal array of strength 2, for all $2 \leq n \leq 2^m - 1$. Therefore our main theorem together with the above two theorems give Corollary 1.4.

3 Trinomials dividing trinomials

In this section we give a different proof of Munemasa's result (Theorem 1.1) in order to illustrate the technique used for the proof of Theorem 1.2 in the next section. Before that, we briefly introduce some terminology that is frequently used in our proofs. To this end, let $f(x) = x^m + x^l + 1$ be a trinomial. If $g = hf$ is also trinomial for some h, then it is clear that h must have an odd number of non-zero terms. We write

$$h(x) = \sum_{s=0}^{t} x^{i_s},$$

where t is even, i_t is the degree of h and i_0=0. We often think of the picture in Figure 1 that illustrates $g = hf$.

The rows that are labeled i_s correspond to the three non-zero coefficients of $x^{i_s} f(x)$ in the sum $g(x) = h(x)f(x) = \sum_{s=0}^{t} x^{i_s} f(x)$. We refer to the $i_s - i_{s-1}$ as *shifts*. If g, the polynomial under the sum in Figure 1, is a trinomial, then there can only be three *columns* in Figure 1 that have an odd number of boxes

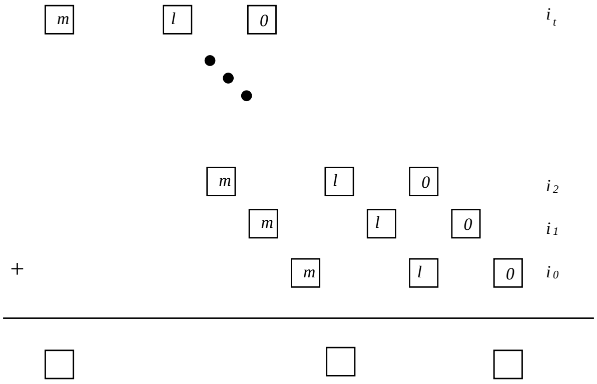

Figure 1: An illustration of equation $g(x) = \sum_{s=0}^{t} x^{i_s} f(x)$, with f, g trinomials.

in them. In this case, we say that one of the terms in that column is *left-over*. Since g is a trinomial, there are exactly three left-over terms including $0 + i_0$ and $m + i_t$. Also, by *stranded*, we mean a term that is left in such a position that nothing can cancel with it. Usually, it is already known that this term can not be the left-over and so a contradiction is automatic.

When a column has an even number of boxes we write that the terms *cancel* (in pairs). Any use of directional terminology *up*, *down*, *left*, *above*, *lower*, etc. is with respect to the layout in this figure. These terms can all be defined rigorously in terms of statements using m, l, i_s and relations $<$, $>$ and $\leq$, $\geq$. We use the relations in the equation form, but we also often use the intuitive prepositional phrases, for clarity. An example of two statements that have the same meaning is: "the l in the third row is to the left of the l in the first row" and "$l + i_2 > l + i_0$".

Next, we reprove Theorem 1.1 using this terminology.

Proof. (of Theorem 1.1)

Let f be the trinomial dividing g, where f and g are the ones given in the statement of the theorem. Recall that $g = fh$ if and only if $\text{rec}(g) = \text{rec}(f)\text{rec}(h)$. Thus by taking reciprocals, we can reduce the problem in two ways: the first is to assume that $m \geq 2l$ as Munemasa does; the second, which we use, is to assume that the middle term of $g(x)$ is either an "m" (that is, it equals $m + i_s$ for some s) or it is an "l" from the top $t/2$ rows.

Consider the box diagram for $g = fh$, as illustrated in Figure 1. The top 0 must cancel and it must cancel down. If it cancels down with an m, using the fact that $i_t \leq m$, we get $0 + i_t = m + i_0$. Since all 0's must cancel (with the exception of the 0 in row i_0), we get that $i_s - i_{s-1} = l$ for all $1 \leq s < t$. We have accounted for the cancellation of all 0's, all l's (save the one in row $t-1$) and only a single m. At most one of the remaining $t-1$ m's can be left-over and two m's cannot cancel themselves, so we have that $t \leq 3$ and its parity forces $t = 2$. In this case, it is easy to check that $h = f$ and $g = f^2$.

If the top 0 cancels down with an l then $0 + i_t = l + i_z$ for some $z < t$. We claim that in this case all 0's must cancel down with l's. Suppose that $0 + i_\Omega = m + i_y$, for some $y < \Omega < t$. We can show that the bounds on the degree of g force $y = 0$ and $\Omega = t$ which contradicts our assumption. There are exactly $t - 1$ 0's that cancel, which uses all but one l, namely $l + i_t$, the l in the top row. Thus we have that $i_s - i_{s-1} = l$ for all $1 \leq s \leq t$. Again, at most one m cancels up with an l and at most one m can be left-over. This gives us $t = 2$. If $l + i_2 = m + i_1$ then $m - l = l$. The GCD condition gives $l = 1$, $m = 2$ and $h = f$ and $g = f^2$. Finally, if $3l = l + i_2 = m + i_0$, then the GCD condition forces $l = 1$, $m = 3$ and we get $f(x) = 1 + x + x^3$, $h(x) = 1 + x + x^2$ and $g(x) = x^5 + x^4 + 1$, which is the only exception. Given our symmetry assumption, we get the reciprocal exception. □

4 Pentanomials dividing trinomials

In this section, we sketch the proof of our main theorem. First, we break our consideration into cases in a similar manner to our proof of Theorem 1.1. We separately consider the top-left portion and the bottom-right portion of the box diagram. The top and bottom portions are independent and the proof combines each possible top subcase with each possible bottom case. The next lemma, which considers the top-left portion of the box diagram, states the possible scenarios for m's and l's until the uppermost k enters the picture.

Lemma 4.1. *Let $f(x) = x^m + x^l + x^k + x^j + 1$ be a pentanomial over $\mathbb{F}_2$ with $m > l > k > j > 0$ that divides a trinomial of degree n with $m \leq n \leq 2m$ subject to our assumptions. Then, exactly one of the following cases occur and each one implies the corresponding equations given below:*

- *Case 1: $k + i_t = m + i_z$ for some $0 \leq z < t$.*
  - *Subcase 1.1: $m + i_t$ is the only left-over term to the left of $k + i_t$. Then,*

$$\begin{aligned} i_x - i_{x-1} &= m - l, \text{ for } z + 2 \leq x \leq t, & (1) \\ i_{z+1} - i_z &\leq m - l. & (2) \end{aligned}$$

  - *Subcase 1.2: $m + i_t$ and $l + i_\Omega$ are the left-over terms to the left of $k + i_t$ for some $z \leq \Omega < t$. Then, $\Omega = z + 1$ and*

$$\begin{aligned} i_x - i_{x-1} &= m - l, \text{ for } z + 2 \leq x \leq t, & (3) \\ i_{z+1} - i_z &> m - l. & (4) \end{aligned}$$

  - *Subcase 1.3: $m + i_t$ and $m + i_\Omega$ are the left-over terms to the left of $k + i_t$ for some $z + 1 \leq \Omega < t$. Then,*

$$\begin{aligned} i_x - i_{x-1} &= m - l, \text{ for } \Omega + 2 \leq x \leq t & (5) \\ i_x - i_{x-2} &= m - l, \text{ for } z + 3 \leq x \leq \Omega + 1, & (6) \\ i_{z+2} - i_z &< m - l. & (7) \end{aligned}$$

- *Case 2: $k + i_t = l + i_z$ for some $0 \leq z < t$.*
  - *Subcase 2.1: $m + i_t$ is the only left-over term to the left of $k + i_t$. Then,*

$$\begin{aligned} i_x - i_{x-1} &= m - l, \textit{ for } z+1 \leq x \leq t, & (8) \\ i_z - i_{z-1} &\geq m - l. & (9) \end{aligned}$$

  - *Subcase 2.2: $m + i_t$ and $l + i_\Omega$ are the left-over terms to the left of $k + i_t$ for some $z \leq \Omega < t$. This case does not occur.*
  - *Subcase 2.3: $m + i_t$ and $m + i_\Omega$ are the left-over terms to the left of $k + i_t$ for some $z \leq \Omega < t$. Then,*

$$\begin{aligned} i_x - i_{x-1} &= m - l, \textit{ for } \Omega+2 \leq x \leq t, & (10) \\ i_x - i_{x-2} &= m - l, \textit{ for } z+1 \leq x \leq \Omega+1, & (11) \\ i_z - i_{z-2} &> m - l, & (12) \\ z - 1 &\leq \Omega \leq t - 1. & (13) \end{aligned}$$

- *Case 3: $k+i_t$ is left-over. Let A be the highest 0, j or k that cancels down with an m or an l, and let B be its row.*
  - *Subcase 3.1: $A + i_B = m + i_z$. Then,*

$$\begin{aligned} i_x - i_{x-1} &= m - l, \textit{ for } z+2 \leq x \leq t, & (14) \\ i_{z+1} - i_z &\leq m - l, & (15) \\ i_t - i_z &> m - k. & (16) \end{aligned}$$

  - *Subcase 3.2: $A + i_B = l + i_z$. Then,*

$$\begin{aligned} i_x - i_{x-1} &= m - l, \textit{ for } z+1 \leq x \leq t, & (17) \\ i_t - i_z &> l - k, & (18) \\ i_z - i_{z-1} &> m - k. & (19) \end{aligned}$$

Proof. We include here Case 1 only; the other cases are similar and can be found in the appendix.

Subcase 1.1: $m + i_t$ is the only left-over term to the left of $k + i_t$. The terms $m+i_{t-1}, m+i_{t-2}, \ldots, m+i_{z+1}$ must cancel up. They cannot cancel with any 0, j, or k because they are all strictly greater than $k + i_t$, which is the leftmost of all the 0, j, and k terms. Thus they all cancel with an l from a row at least as high as i_{z+1}. Similarly, all of the l's to the left of $k + i_t$ must cancel down with some m. There must be exactly $t - z - 1$ l's to the left of $k + i_t$. That is, $l + i_t, \ldots, l + i_{z+2} > k + i_t \geq l + i_{z+1}$. Working from the top we get Equations 1 and 2. Figure 2 contains the pattern of cancellation for this subcase.

Subcase 1.2: $m+i_t$ and $l+i_\Omega$ are the left-over terms to the left of $k+i_t$ for some $z \leq \Omega < t$. This is similar to Subcase 1.1 except that we must now

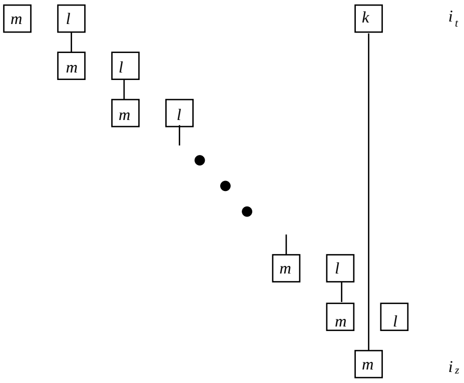

Figure 2: Pattern of cancellations for Subcase 1.1.

have $l + i_{z+1} > k + i_t$ so that the number of m's and l's which cancel are equal. Working from the top again we find,

$$i_x - i_{x-1} = m - l, \text{ for } \Omega + 1 \leq x \leq t.$$

We claim that $\Omega = z + 1$. By way of contradiction, let us assume that this is not the case. Then, since all the m's and l's in rows $i_t, \ldots, i_{\Omega+1}$ cancel, there is nothing above for $m + i_{\Omega-1}$ to cancel with, except $k + i_t$; contradiction. Furthermore, we have $i_{z+1} - i_z > m - l$, proving Equations 3 and 4. Figure 3 exemplifies this case. We always use Ω to represent the row containing the third left-over term.

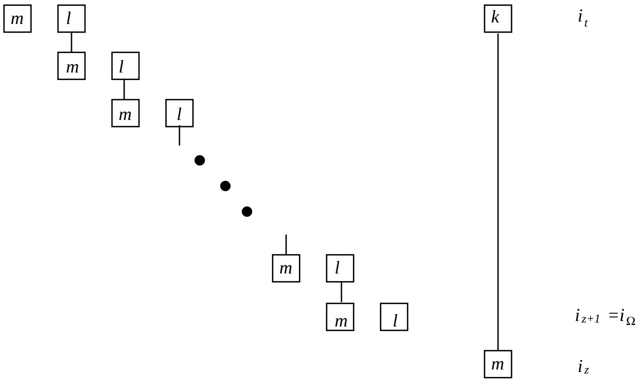

Figure 3: Pattern of cancellations for Subcase 1.2.

Subcase 1.3: $m + i_t$ and $m + i_\Omega$ are the left-over terms to the left of $k + i_t$ for some $z \leq \Omega < t$. There are exactly $t - z - 2$ m's to be canceled to the left of $k + i_t$. Hence $l + i_t, \ldots, l + i_{z+3} > k + i_t$. Working from the top, $l + i_t = m + i_{t-1}, \ldots, l + i_{\Omega+2} = m + i_{\Omega+1}$. Since $l + i_{\Omega+1}$ must cancel down, $i_{\Omega+1} - i_{\Omega} < m - l$ and $l + i_{\Omega+1} = m + i_{\Omega-1}, \ldots, l + i_{z+3} = m + i_{z+1}$, and $l + i_{z+1} < l + i_{z+2} < k + i_t$. We get Equations 5-7. We observe that $l + i_{z+2} \neq k + i_t$, since otherwise it would be left-over, but we already have enough left-over terms. Figure 4 shows this case.

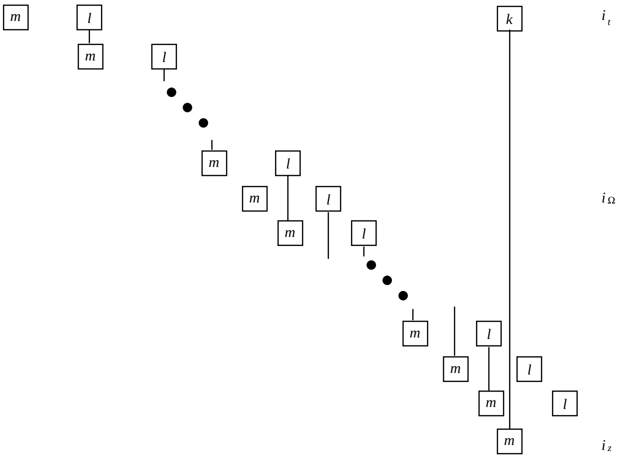

Figure 4: Pattern of cancellations for Subcase 1.3.

Figure 5 provides an insight on the cases not covered in this proof. □

In Lemma 4.2, we look at cases 4 and 5, which are not disjoint from the cases listed in Lemma 4.1 (subcases 1.1 to 3.2). The combinations between these two sets of cases form the complete case breakdown in the proof of Theorem 1.2.

Lemma 4.2 considers the bottom-right portion of the box diagram. More specifically, it analyzes the scenarios for the 0's and j's until the lower-most k enters the picture. The m in the top row and the 0 in the bottom row are left-overs. We make the assumption that the third left-over term is either a k in the top $t/2$ rows (since the number of rows is odd and start numbering at 0, t must be even), or an m or an l. In the proof of Theorem 1.2 we justify why this assumption is without any loss of generality. Therefore throughout the paper the third left-over will not be a j or a 0.

Lemma 4.2. *Let $f(x) = x^m + x^l + x^k + x^j + 1$ be a pentanomial over $\mathbb{F}_2$ with $m > l > k > j > 0$ that divides a trinomial g of degree n with $m \leq n \leq 2m$. Letting $g = fh$, with $g(x) = x^n + x^s + 1$ and $t+1$ being the number of terms in h, further assume that s corresponds to either a k on one of the top $t/2$ rows or an m or an l. Then, exactly one of the following cases must occur and they imply the corresponding equations given below:*

- *Case 4: j divides k. Then, we necessarily have $j + i_y = k + i_0$, for some*

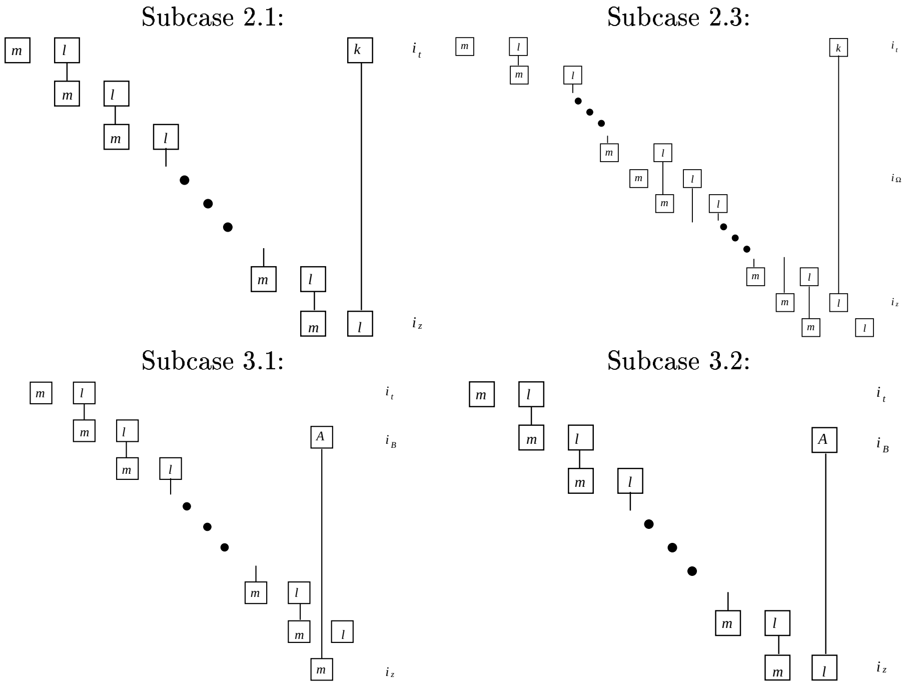

Figure 5: Pattern of cancellations for Subcases 2.1-3.2

$1 \le y \le t$, *and*

$$
\begin{aligned}
i_x &= xj, \textit{ for } 1 \le x \le y, && (20)\\
k &= (y+1)j, && (21)\\
i_{y+1} - i_y &> j, \textit{ if } y \ne t. && (22)
\end{aligned}
$$

- *Case 5: j does not divide k. Then, we necessarily have* $0 + i_y = k + i_0$, *for some* $1 \le y \le t$, *and*

$$
\begin{aligned}
i_x &= xj, \textit{ for } 1 \le x \le y-1, && (23)\\
i_y - i_{y-1} &< j. && (24)
\end{aligned}
$$

Figure 6 illustrates the cases considered in this lemma and gives an idea of its proof, which is given in the appendix.

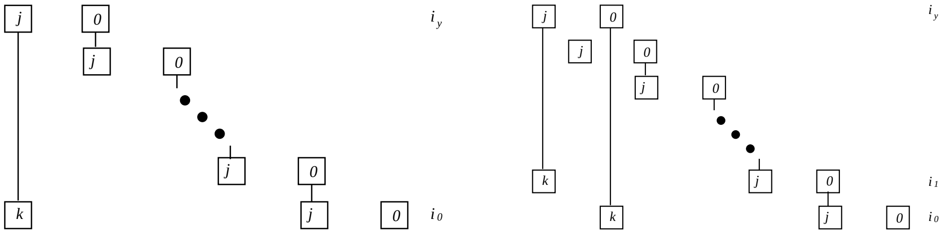

Figure 6: Pattern of cancellations for Cases 4 and 5.

	4	5
1.1	$z \le y \le z+2$	$z \le y \le z+1$
1.2	$y = z$	$z \le y \le z+2$
1.3	$z \le y \le z+2$	$z \le y \le z+3$
2.1	$y = z-1$	$z-1 \le y \le z+1$
2.3	$z-2 \le y \le z$	$z-1 \le y \le z+1$
3.1	$z \le y \le z+1$	$y = z+1$
3.2	$y = z-1$	$z \le y \le z+1$

Table 2: Bounds on y by subcases.

SKETCH OF THE PROOF OF OUR MAIN THEOREM (THEOREM 1.2)

The complete proof involves a great number of subcases. The complete case analysis can be found in the appendix.

Here we provide the main steps and a summary of findings for each case combination (subcases and cases follow the numbering given in Lemma 4.1 and Lemma 4.2).

Assume without loss of generality that the third left-over term (other than the m and the 0) is either a k in the top $t/2$ rows or an m or l; this assumption only requires that we later add the reciprocals of the polynomial exceptions found. Moreover if there exists a constant c with $i_x - i_{x-1} = c$ for all $1 \le x \le t$, then we can show that $c = j$ thus almost all of the m's cancel with l's, 0's with j's and the k's remain. This forces f to be one of the polynomial exceptions 4, 7 or 9 in Table 1. So for the rest of the proof we assume there exists no such c. We then can obtain the bounds given in Table 2 for the value of y for each possible combination of cases.

For each of the case combinations, we individually analyze the possible values of y permitted by the table above. For each situation, we either find a contradiction or conclude that f must be one of the listed polynomial exceptions. Tables 3 and 4 provide the polynomial exceptions with their related cases and the polynomial exceptions indexed by case, respectively.

In order to give a sample of the type of argument involved in the case analysis, we show some representative cases: Subcases 2.1/5 and 3.2. We also give a derivation of the bounds on the value of y from Table 2 for these cases.

No.	$f(x)$	z	y	t	Ω	Case
1	$x^5+x^4+x^3+x^2+1$	1	2	2	0,1	2.1/5
2	$x^5+x^3+x^2+x+1$	0	1	2	0,1	1.1/4
3	$x^5+x^3+x^2+x+1$	1	1	2	2	1.2/4
4	$x^5+x^4+x^3+x+1$	0,1,0	2	2	1,0,2	{1.1,2.1,3.2}/4
5	$x^6+x^5+x^4+x^3+1$	1	2	2	0	2.1/5
6	$x^6+x^4+x^2+x+1$	1	1	2	0	2.3/4
7	$x^6+x^4+x^3+x+1$	1	2	2	1	2.3/4
8	$x^6+x^5+x^2+x+1$	1	1	4	2	1.2/4
9	$x^6+x^5+x^3+x+1$	0	2	2	1	2.1/4
10	$x^7+x^4+x^2+x+1$	1	1	2	1	2.3/4
11	$x^7+x^4+x^3+x^2+1$	1	2	2	1	2.3/5
12	$x^7+x^5+x^2+x+1$	3	1	6	5	2.3/4
13	$x^7+x^5+x^3+x^2+1$	2	2	4	3	2.3/5
14	$x^8+x^5+x^3+x+1$	0	2	4	3	1.3/4
15	$x^8+x^5+x^3+x^2+1$	2	2	6	5	1.3/5
16	$x^8+x^6+x^3+x+1$	1	2	4	1,3,4	1.1/4
17	$x^8+x^7+x^5+x^2+1$	2	3	4	0	2.1/5
18	$x^9+x^6+x^5+x^2+1$	2	3	4	2,3,4	1.1/5
19	$x^9+x^7+x^4+x^3+1$	1	2	4	0	1.1/5
20	$x^9+x^8+x^5+x^2+1$	1	3	4	2	1.2/5
21	$x^{10}+x^4+x^3+x^2+1$	1	2	4	3	1.3/5
22	$x^{10}+x^7+x^2+x+1$	1	1	4	3	2.3/4
23	$x^{11}+x^7+x^6+x^2+1$	3	2	4	3	2.3/4
24	$x^{13}+x^{10}+x^2+x+1$	1	1	6	5	2.3/4
25	$x^{13}+x^{10}+x^9+x^2+1$	4	5	6	3	1.1/5

Table 3: Table of polynomial exceptions with subcases.

CASE 2.1/5
If $z \neq 0$, then

$$\begin{aligned} m &= (m-l)+(l-k)+k \\ &\leq (i_z - i_{z-1}) + (i_t - i_z) + i_y \\ &= i_t - i_{z-1} + i_y \\ &\leq m - i_{z-1} + i_y. \end{aligned}$$

Thus $i_{z-1} \leq i_y$ where equality holds if and only if $i_t = m$ and

$$i_z - i_{z-1} = m - l. \tag{25}$$

We observe that if equality holds, then we are also in Subcase 1.1/4 where the role of z is played by $z+1$.

The condition $z \neq 0$ is irrelevant since if $z = 0$ then all shifts are $m-l$, a situation already considered. We conclude that $z - 1 \leq y$.

Case	No.	z	y	t	Ω
1.1/4	2	0	1	2	0,1
1.1/4	4	0	2	2	1
1.1/4	16	1	2	4	1,3,4
1.1/5	18	2	3	4	2,3,4
1.1/5	19	1	2	4	0
1.1/5	25	4	5	6	3
1.2/4	3	1	1	2	2
1.2/4	8	1	1	4	2
1.2/5	20	1	3	4	2
1.3/4	14	0	2	4	3
1.3/5	15	2	2	6	5
1.3/5	21	1	2	4	3
2.1/4	4	1	2	2	0
2.1/4	9	0	2	2	1
2.1/5	1	1	2	2	0,1
2.1/5	5	1	2	2	0
2.1/5	17	2	3	4	0
2.3/4	6	1	1	2	0
2.3/4	7	1	2	2	1
2.3/4	10	1	1	2	1
2.3/4	12	3	1	6	5
2.3/4	22	1	1	4	3
2.3/4	23	3	2	4	3
2.3/4	24	1	1	6	5
2.3/5	11	1	2	2	1
2.3/5	13	2	2	4	3
3.2/4	4	0	2	2	2

Table 4: Table of polynomial exceptions indexed by subcase.

Since $i_x - i_{x-1} = m - l$ for $z+1 \leq x \leq t$ and $i_x - i_{x-1} = j$ for $1 \leq x \leq y-1$, if $z+1 \leq y-1$ then all shifts are $j = m - l$, contradicting $i_y - i_{y-1} < j$. Thus we take $z - 1 \leq y \leq z+1$. This completes the proof of the bounds on y.

Assume $y = z + 1$. Now $m - l = i_{z+1} - i_z = i_y - i_{y-1} < j$. Also, $0 + i_t = (0 + i_y) + (i_t - i_z) + (i_z - i_y) = k + (l - k) - (m - l) < l + i_0$. That is, $0 + i_t$ is strictly to the right of all l's and m's. What happens to $j + i_{y-1}$? It cancels up or down.

Case I: $j + i_z$ cancels down. If $t \geq y+1$, then since $i_{y+1} - i_y = i_{z+2} - i_{z+1} = m - l < j$, $0 + i_{y+1} < j + i_y$ and hence $0 + i_{y+1} < k + i_1$ and cannot cancel any k and from above, it cannot cancel any l or m. Therefore i_{y+1} cannot exist and $y = t$. Note that $m - l = i_{z+1} - i_z = l - k$ and hence $2(m-l) = (m-l) + (l-k) = m - k$. Because $j + i_z < j + i_{z+1} = k + i_1$, we consider the following two subcases.

Case IA: $j+i_z = m+i_0$. Then $l+i_0$ is left-over. If $i_z - i_{z-1} = m-l$ then $m-l=j$, a contradiction. Thus if $k+i_z$ cancels down, then since $i_z - i_{z-1} > m-l = l-k$, it does not cancel any l. So for some $a \geq 0$, $k+i_z = m+i_a$ and $m-k = i_z - i_a$ is a multiple of j. Since $j+i_t = k+i_1$ and $j+i_z < j+i_{z+1}$, we get that $m-k<j$ which is a contradiction. Therefore $k+i_z$ cancels up. Since the top j's and 0's are accounted for, $z=1, y=t=2$. Thus $f(x) = x^6+x^5+x^4+x^3+1$ and we have polynomial exception 5.

Case IB: $j+i_z = l+i_0$. Now $k = i_y = (i_y - i_{y-1}) + (i_{y-1}) = (l-k)+(l-j)$, since $i_y - i_{y-1} = l-k$. Hence $j = 2(l-k) = 2(m-l) = m-k$. Furthermore, $m+i_0 = (m-k)+k = j+k = k+i_1 (= j+i_t)$. The left-over must be in this column. Now $l+i_1$ must cancel and it can only cancel up with a k. So $i_2 - i_1$ cannot be $j = 2(l-k)$, so $2 = y = t$. We may deduce that $h(x) = x^3+x^2+1$ and $f(x) = x^5+x^4+x^3+x^2+1$ which is polynomial exception 1.

Case II: <u>$j+i_z$ **cancels up.**</u> Then $j+i_{y-1} = 0+i_{y+1}$ and $j = i_{z+2} - i_z = 2(m-l)$.

Case IIA: $t \geq y+2$. Consider $k+i_1 = j+i_y = 0+i_{y+2}$. Now either $k+i_1$ is left-over and thus $t=2$ (because a left-over k must be in the top $t/2$ rows) or $k+i_1 = \{l \text{ or } m\} + i_0$. However $t \geq y+2 \geq 4$ so it must be the latter. We have $l+i_0 > 0+i_t \geq 0+i_{y+2} = k+i_1$ so no l or m is available for $k+i_1$ to cancel with, a contradiction.

Case IIB: $t = y+1$. Since $j = 2(m-l) = i_t - i_z = l-k$, $l+i_0 = k+j = k+i_1 (= j+i_y)$, so $l+i_0$ is left-over. Now $m+i_0 = (l+i_0)+(m-l) = (j+i_y)+(i_t - i_{t-1}) = j+i_t$. We must have $m+i_{z-1} = k+i_y$, or else one of these will be stranded. Now we deduce $l+i_{z-1} = k+i_z$. If $z \geq 3$, then $m+i_{z-2}$ is stranded since everything above it is accounted except $k+i_{z-1}$ which is too far right since $m-k>j$. So $z = 0, 1,$ or 2. The subcase $z=0$ implies every shift is $m-l$ which was dealt with earlier. The case $z=1$ implies $y=2$, $t=3$, but t must be even. Thus we may take $z=2, y=3, t=4$. Now $f(x) = x^8+x^7+x^5+x^2+1$ which is polynomial exception 17.

Assume $y=z$. We have $0+i_t = (0+i_y)+(i_t-i_z)+(i_z-i_y) = k+(l-k)+0 = l+i_0$. Either $j+i_{y-1}$ cancels up (and hence $i_{y+1}-i_{y-1} = j$) or it cancels down with the l or m from i_0 and hence $i_{y+1}-i_{y-1} < j$. In the latter case $t=y$ or $t=y+1$. Note $m-l = i_{z+1}-i_z < i_{y+1}-i_{y-1} < j$. We divide into cases based on t relative to z.

Case I: <u>$t = z+1$.</u> From $z = y \geq 2$, we deduce $t \geq 3$. Since t must even, $t \geq 4$ and $y=z$ must be odd. So $y=z\geq 3$.

We easily deduce that $m-l = i_t - i_{t-1} = i_t - i_z = l-k$. Therefore $2(m-l) = (m-l)+(l-k) = m-k$. The only possible term with which $m+i_{z-1}$ may cancel is $k+i_z$. As well, $k+i_z$ must cancel down since the j's and

0's from rows i_t and $i_{t-1} = i_z$ are accounted for. Hence we break into subcases as follows:

Case IA: $m + i_{z-1} = k + i_z$**.** Here $2(m-l) = m-k = i_z - i_{z-1} < j$. The term $l + i_{z-1}$ has nothing above it with which to cancel. If $l + i_{z-1} = m + i_{z-2}$ then $m - l = i_{z-1} - i_{z-2} = i_{y-1} - i_{y-2} = j > 2(m-l)$ which is absurd. If $l + i_{z-1}$ cancels with an even lower m, say $m + i_{z-\alpha}$, then $(\alpha - 1)j = m - l < j$, which is a contradiction. We conclude that $l + i_{z-1}$ must be left-over. Now we require $k + i_{z-1} = m + i_{z-2}$ or else one of these will be stranded, leaving too many left-over terms. Thus $m - k = i_{z-1} - i_{z-2} = j$ contradicting with above.

Case IB: $m + i_{z-1}$ **is left-over,** $l + i_{z-1} = k + i_z$**.** We must have $k + i_{z-1} = m + i_{z-2}$ or else one of these will be stranded. Thus $m-k = i_{z-1} - i_{z-2} = j$. Hence $m + i_0 = k + i_1 = j + i_{t-1} \neq 0 + i_t$ and we have an "extra" left-over here, a contradiction.

Case IC: $m + i_{z-1}$ **is left-over,** $l + i_{z-1} \neq k + i_z$**.** We must have $k + i_z = m + i_{z-2}$ or else one of these will be left-over. Now $j = i_{z-1} - i_{z-2} = (m - k) - (i_z - i_{z-1}) < m - k = 2(m-l)$. What happens to $l + i_{z-1}$? It has nothing to cancel with unless $0 \leq z - 1 \leq 1$, i.e. $1 \leq z \leq 2$. However, $z = y \geq 2$ must be odd. Thus this subcase falls.

Case II: $t = z + 2$**.** We have, from before, that $j + i_{y-1} = 0 + i_{y+1}$. Consider $j + i_{z+1}$. It cannot cancel up since $0 + i_t$ is accounted for. Either it cancels down with $m + i_0$ or with some $k + i_\alpha$ for $\alpha \geq 2$. However $j + i_{z+1} = j + (m-l) + i_z = (m - l) + k + i_1 < j + k + i_1$.

Case IIA: $y > 2$**.** In this subcase, $j + i_1 = i_2$ so $j + i_{z+1} < k + i_2 \leq k + i_\alpha$ for $\alpha \geq 2$. Thus $j + i_{z+1} = m + i_0$. We have $l = (i_t - i_{z+1}) + i_{z+1} = (m - l) + (m - j)$ and we may deduce $j = 2(m - l) = l - k$. Hence $i_z = k = l - j$ so $k + i_1 = j + i_z = l + i_0 = 0 + i_t$. Therefore we have the left-over in the column with $k + i_2 = (k + j) + i_1 = l + i_1 = j + i_t$.

The term $0 + i_{z+1}$ must cancel with $j + i_{z-1}$ because all other possibilities (lower j's and l or k from i_0 or i_1) are impossible. Hence $2(m-l) = l-k = j = i_{z+1} - i_{z-1} = (m - l) + i_z - i_{z-1}$ and so $i_z - i_{z-1} = m - l$. Therefore there is an extra left-over in the column with $m + i_{z-1} = l + i_z = k + i_t$, a contradiction.

Case IIB: $y = 2$**.** Clearly $t = 4$. We have $j + i_4 = l + i_1$ and $j + i_1 = 0 + i_3$. When we draw the box diagram, there are five terms unaccounted for (of which four must cancel with each other): $m+i_0, m+i_1, k+i_2, k+i_3, j+i_3$.

Case IIB1: $j + i_3 = m + i_0$**.** Now $k - j = i_2 - i_1 < j$. So $k + i_3 = (k - j) + (j + i_3) < j + m = m + i_1$. Hence $m + i_1 > k + i_3 > k + i_2$ so we cannot complete the required cancellations.

Case IIB2: $j + i_3 \neq m + i_0$. Since $i_3 - i_1 = (m-l) + (k-j) < m - j$, $j + i_3 \neq m + i_1$ and so we must have $k - j = i_3 - i_2 = m - l$. Since $i_3 - i_1 = j - 0 < m - k$ we cannot have $m + i_1 = k + i_3$. This forces the left-over to be $m + i_1$. Hence $m + i_0 = k + i_3 (= j + i_4 = l + i_1)$. However, now $m - l = i_1 - i_0 = j$, contrary to earlier work.

Case III: $t \geq z + 3$.

Consider $0 + i_{z+1} < i_t = l + i_0 \leq \{l, m\} + i_\alpha$ for $\alpha \geq 0$ and $0 + i_{z+1} = (m - l) + i_z < j + i_z = k + i_1$ and we see that $0 + i_{z+1} = j + i_{z-1}$ because all other options are accounted for or impossible.

Since i_{z+2} is not the top row, $0 + i_{z+2} < 0 + i_t = l + i_0 \leq \{l, m\} + i_\alpha$ for $\alpha \geq 0$. Also, $0 + i_{z+2} = (m - l) + i_{z+1} < j + i_{z+1}$. Hence $0 + i_{z+2} = k + i_\alpha$ for $\alpha \geq 2$. (If $\alpha = 1$, then $0 + i_{z+2} = k + i_1 = j + i_z$ and so $k + i_1$ must be left-over and $2 \leq y < t = 2$.) That is, $i_\alpha = i_{z+2} - k = i_{z+2} - i_z = 2(m - l)$. However, $i_\alpha \geq i_2 = (i_2 - i_1) + i_1 = (i_2 - i_1) + j > (i_2 - i_1) + (m - l)$. We deduce $i_2 - i_1 < m - l$, but no shift is less than $m - l$ in 2.1/5 with $y = z$, thus a contradiction.

Assume $y = z - 1$. Similarly to the above, $0 + i_t = (0 + i_y) + (i_t - i_z) + (i_z - i_y) = k + (l - k) + (m - l) = m + i_0$ since $i_z - i_{z-1} = m - l$ from Equation 25. So $i_t = m, i_{t-1} = l$. Also, we conclude that $l + i_z = m + i_{z-1} = k + i_t$ and so the left-over must be in this column. Also, $l + i_{z-1} = (m + i_{z-1}) - (m - l) = (k + i_t) - (i_t - i_{t-1}) = k + i_{t-1}$. Now $j + i_{y-1} < j + i_y = k + i_1 \leq \{k, l, m\} + i_\alpha$ for $\alpha \geq 1$. Since m, l, k in i_0 are accounted for, and since the left-over is already determined, $j + i_{y-1}$ must cancel up. If $j + i_{y-1} = 0 + i_\alpha$ for $\alpha > y + 1$, then $0 + i_{y+1} < 0 + i_\alpha = j + i_{y-1}$ so $0 + i_{y+1}$ cannot cancel with anything, a contradiction. Thus $j + i_{y-1} = 0 + i_{y+1}$. In particular, $j = (i_{y+1} - i_y) + (i_y - i_{y-1}) = (m - l) + (i_y - i_{y-1}) > m - l$.

Consider $k + i_{t-2}$ which cannot cancel up since these 0's and j's are accounted for and the left-over is already fixed and to the left of $k + i_{t-2}$. This k also cannot be one of $k + i_0$ or $k + i_1$ since these cancel with row $i_y \leq i_{t-2}$.

Case I: $k + i_{t-2} < m + i_{y-1}$. Here $m + i_{y-1}$ is in danger of being stranded so we would actually need $y - 1 \leq 1$ which implies $2 \leq y \leq 2$ which further implies $y = 2$ and $z = 3$. But there is nothing lower remaining to actually cancel $k + i_{t-2}$, so we have a contradiction.

Case II: $k + i_{t-2} \geq m + i_{y-1}$. We require $k + i_{t-2} = m + i_{y-1}$ or else $k + i_{t-2}$ has nothing below with which to cancel. Hence $m - k = i_{t-2} - i_{y-1} = (i_t - i_y) - (i_t - i_{t-2}) + (i_y - i_{y-1}) = (m - k) - 2(m - l) + (i_y - i_{y-1})$ implying $2(m - l) = (i_y - i_{y-1}) < j$. Therefore $j = (i_{y+1} - i_y) + (i_y - i_{y-1}) = (m - l) + 2(m - l) = 3(m - l)$. So $0 + i_{z+1} = (i_{z+1} - i_z) + (i_z - i_{z-1}) + i_{z-1} = 2(m - l) + i_y < j + i_y = k + i_1 \leq \{k, l, m\} + i_\alpha$ for $\alpha \geq 1$ and m, l, k in rows i_1 and i_0 are taken unless $z + 1 = t$ or $t - 1$. Since $0 + i_{z+1} < j + i_y$ and $0 + i_{z+1} > 0 + i_z = j + i_{y-1}$, then $0 + i_{z+1}$ cannot cancel with any j. Since $0 + i_z$ is already taken, $0 + i_z \neq l + i_0 = 0 + i_{t-1}$. Therefore $z \neq t - 1$ and $z + 1 = t - 1$ implies $t = z + 2$. Thus $m - k = i_t - i_y = 3(m - l) = j = i_1$ implying $k + i_1 = m + i_0 = 0 + i_t = j + i_y$.

If $y \geq 3$, then $i_2 - i_1 = j = m - k$ so $k + i_2 = m + i_1 = j + i_t$ with no room for an l or 0. This triple cancellation contradiction proves $2 \leq y \leq 2$. Hence $y = 2, z = 3, t = 5$, but t must be even. This final contradiction concludes this subcase.

CASE 3.2
We prove this case by reduction to either Subcase 1.1 or Subcase 2.1. Let us recall that in this case $k + i_t$ is left-over. The starting point is $A + i_B = l + i_z$ where A is the highest $0, j, k$ that cancels with an l, and B is its row. We have

$$\begin{aligned} l + i_{z+t-B} &= (l + i_z) + (i_{z+t-B} - i_z) = (A + i_B) + (t - B)(m - l) \\ &= (A + i_B) + (i_t - i_B) = A + i_t. \end{aligned}$$

By the choice of B maximal, $B = t$. The case $A = k$ is dealt with in Subcase 2.1.

Assume $A = j$.
Now $l = (l - j) + j = (i_t - i_z) + i_1$ implying $m - l \geq i_t - (i_t - i_z + i_1) = i_z - i_1$. Recall $i_z - i_{z-1} > m - l$ for Subcase 3.2, and so if $z \geq 2$ then $m - l \geq i_z - i_1 \geq i_z - i_{z-1} > m - l$, a contradiction. If $z = 0$ then all shifts are the same and this was dealt with elsewhere. Thus $z = 1$ and $i_2 - i_1 = i_{z+1} - i_z = m - l$.

For either Case 4 or 5, if $y \geq 3$ then $m - l = i_2 - i_1 = j$ and actually all shifts are $j = m - l$, which has already been considered.

Case I: 3.2/4. If $y = 2$, then all shifts are $j = m - l$ which was dealt with elsewhere. If $y = z = 1$, then $m - l < i_z - i_{z-1} = i_y - i_{y-1} = j$ but $m - l = i_{z+1} - i_z = i_{y+1} - i_y > j$ and we have another contradiction. Case 4 implies that $y \geq 1$ so this exhausts the possibilities.

Case II: 3.2/5.

In Case 5, $y \geq 2$ and so $y = 2$. We have $i_2 = k, i_1 = j$ so $k - j = i_2 - i_1 = m - l$. However $k + i_t = (k - j) + (j + i_t) = (m - l) + (l + i_z) = m + i_z$ and we are in Subcase 1.1.

Assume $A = 0$.
In this case $l = i_t - i_z$, and hence we have

$$m = (m - l) + l < (i_z - i_{z-1}) + (i_t - i_z) \leq m - i_{z-1}$$

implying $i_{z-1} < 0$ which is a contradiction. □

5 Conclusion

In this paper we extended Munemasa's [11] results to obtain orthogonal arrays of guaranteed strength 3. Our main result also implies that shift-register sequences generated by primitive pentanomials offer less bias in terms of the third moment of the Hamming weight, than the ones generated by trinomials.

This research gives rise to some questions. Unlike Munemasa's result for divisibility of trinomials by trinomials, the choice of the restriction of $n \leq 2m$ in

Theorem 1.2 is somewhat arbitrary. It is desirable to have n as large as possible, as it gives a larger window for which the bias of the shift-register sequence is small. Can the upper bound on n be increased in Theorem 1.2?

Our results guarantee that the orthogonal arrays constructed, C_n^f, have strength at least 3. What can be said about strength 4? This requires the analysis of pentanomials dividing tetranomials.

Another question is concerned with generalizations of our main theorem for polynomials with more than five terms as well as for finite fields other than $\mathbb{F}_2$. Under which conditions, given t, does there exist a positive integer d such that if a polynomial f of degree m has precisely t non-zero coefficients and $m \geq d$, then f does not divide any polynomials with exactly s non-zero coefficients and degree less than or equal to some function of m, for all $s \leq t$?

We anticipate that approaching the last two questions using the techniques herein would be impossibly complex and long. We hope that a more global perspective exists that would make such results more amenable to proof.

References

[1] P. Delsarte. Four fundamental parameters of a code and their combinatorial significance. *Inform. Control*, 23:407–438, 1973.

[2] M. Dewar, L. Moura, D. Panario, B. Stevens and Q. Wang. Division of trinomials by pentanomials and orthogonal arrays. Submitted to *Designs, Codes and Cryptography*, 2006, 20 pages.

[3] J. von zur Gathen. Irreducible trinomials over finite fields. *Math. Comp.*, 72:1987–2000, 2003.

[4] S. W. Golomb. *Shift Register Sequences.* Aegean Park Press, 1982.

[5] T. Hansen and G. L. Mullen. Primitive polynomials over finite fields. *Math. Comp.*, 59:639–643, 1992.

[6] IEEE Standard Specifications for Public-Key Cryptography. Technical Report IEEE Std 1361-2000. IEEE Inc., 3 Park Ave., NY 10016-5997, USA.

[7] H. F. Jordan and D. C. M. Wood. On the distribution of sums of successive bits of shift-register sequences. *IEEE Trans. Computers*, 22:400–408, 1973.

[8] R. Lidl and H. Niederreiter. *Introduction to Finite Fields and Their Applications.* Cambridge University Press, Cambridge, first edition, 1994.

[9] J. H. Lindholm. An analysis of the pseudo-randomness properties of subsequences of long m-sequences. *IEEE Trans. Inform. Theory*, 14:569–576, 1968.

[10] I. H. Morgan and G. L. Mullen. Primitive normal polynomials over finite fields. *Math. Comp.* 63:759–765, 1993.

[11] A. Munemasa. Orthogonal arrays, primitive trinomials, and shift-register sequences. *Finite Fields and Their Applications*, 4(3):252–260, 1998.

[12] G. Seroussi. Table of low-weight binary irreducible polynomials. HP Labs Technical Report HPL-98–135, 1998.

Appendix: complete proofs of lemmas and main theorem

6 Full proofs of lemmas in Section 4

Case 1: $k+i_t = m+i_z$ for some $0 \leq z < t$

Subcase 1.1: $m+i_t$ is the only left-over term to the left of $k+i_t$.

The terms $m+i_{t-1}, m+i_{t-2}, \ldots, m+i_{z+1}$ must cancel up. They cannot cancel with any 0, j, or k because they are all strictly greater than $k+i_t$, which is the leftmost of all the 0, j, and k terms. Thus they all cancel with an l from a row at least as high as i_{z+1}. Similarly, all of the l's to the left of $k+i_t$ must cancel down with some m. There must be exactly $t-z-1$ l's to the left of $k+i_t$. That is, $l+i_t, \ldots, l+i_{z+2} > k+i_t, l+i_{z+1} \leq k+i_t$. Working from the top we have, for $z+2 \leq x \leq t$,

$$\begin{aligned} i_x - i_{x-1} &= m-l, \\ i_{z+1} - i_z &\leq m-l. \end{aligned}$$

Figure 2 contains the pattern of cancellation for this case.

Subcase 1.2: $m+i_t$ and $l+i_\Omega$ are the left-over terms to the left of $k+i_t$.

This is similar to Subcase 1.1 except that we must now have $l+i_{z+1} > k+i_t$ so that the number of m's and l's which cancel are equal. Working from the top again we find,

$$i_x - i_{x-1} = m-l, \text{ for } \Omega+1 \leq x \leq t.$$

We claim that $\Omega = z+1$. By way of contradiction, let us assume that this is not the case. Then, since all the m's and l's in rows $i_t, \ldots, i_{\Omega+1}$ cancel, there is nothing above for $m+i_{\Omega-1}$ to cancel with except $k+i_t$. Furthermore, we have $i_{z+1} - i_z > m-l$. Figure 3 exemplifies this case.

Subcase 1.3: $m+i_t$ and $m+i_\Omega$ are the left-over terms to the left of $k+i_t$.

There are exactly $t-z-2$ m's to be canceled. Hence $l+i_t, \ldots, l+i_{z+3} > k+i_t$. Working from the top, $l+i_t = m+i_{t-1}, \ldots, l+i_{\Omega+2} = m+i_{\Omega+1}$. Since $l+i_{\Omega+1}$ must cancel down, $i_{\Omega+1} - i_\Omega < m-l$ and $l+i_{\Omega+1} = m+i_{\Omega-1}, \ldots, l+i_{z+3} = m+i_{z+1}$, and $l+i_{z+1} < l+i_{z+2} < k+i_t$. That is,

$$\begin{aligned} i_x - i_{x-1} &= m-l, \text{ for } \Omega+2 \leq x \leq t, \\ i_x - i_{x-2} &= m-l, \text{ for } z+3 \leq x \leq \Omega+1, \\ i_{z+2} - i_z &< m-l, \\ \Omega &\geq z+1. \end{aligned}$$

We observe that $l + i_{z+2} \neq k + i_t$, since otherwise it would be left-over, but we already have enough left-over terms. Figure 4 shows this case.

Case 2: $k + i_t = l + i_z$ for some $0 \leq z < t$

There are three subcases, one of which never occurs. For the other two, $i_t - i_{z-2} > m - k$.

Subcase 2.1: $m + i_t$ is the only left-over term to the left of $k + i_t$.

The $m + i_{t-1}, \ldots, m + i_z$ require exactly $t - z$ l's. Hence $l + i_t = m + i_{t-1}, \ldots, l + i_{z+1} = m + i_z$. That is,

$$\begin{aligned} i_x - i_{x-1} &= m - l \text{ for } z + 1 \leq x \leq t, \\ i_z - i_{z-1} &\geq m - l. \end{aligned}$$

The pattern of cancellations for this case is in Figure 5.

Subcase 2.2: $m + i_t$ and $l + i_\Omega$ are the left-over terms to the left of $k + i_t$.

There are $t - z$ m's to cancel and there are exactly $t - z - 1$ l's to cancel. Hence this case is impossible.

Subcase 2.3: $m + i_t$ and $m + i_\Omega$ are the left-over terms to the left of $k + i_t$.

We need $m + i_{z-1} > k + i_t$ to ensure enough m's are available to cancel with the $t - z$ l's. Hence

$$\begin{aligned} i_x - i_{x-1} &= m - l, \text{ for } \Omega + 2 \leq x \leq t, \\ i_x - i_{x-2} &= m - l, \text{ for } z + 1 \leq x \leq \Omega + 1, \\ i_z - i_{z-2} &> m - l, \\ z - 1 &\leq \Omega \leq t - 1. \end{aligned}$$

Figure 5 gives the type of cancellation of this case.

Case 3: $k + i_t$ is left-over

Let $A + i_B$ be the largest 0, j, or k which cancels down with an m or l. Such an element must exist because $l + 0$ must cancel up with something.

Subcase 3.1: $A + i_B = m + i_z$.

There are $t - z - 1$ m's to cancel up with l's. Hence we have $l + i_{z+2} > A + i_B$ and $l + i_{z+1} \leq A + i_B$. Furthermore,

$$\begin{aligned} i_x - i_{x-1} &= m - l, \text{ for } z + 2 \leq x \leq t, \\ i_{z+1} - i_z &\leq m - l, \\ z &\leq t - 2. \end{aligned}$$

We observe that $i_B - i_z = m - A \geq m - k$, so $i_t - i_z > i_B - i_z \geq m - k$. Thus we have

$$i_t - i_z > m - k.$$

The pattern of cancellations for this case is in Figure 5.
Subcase 3.2: $A + i_B = l + i_z$.

There are $t - z$ m's to cancel. In this case,

$$i_x - i_{x-1} = m - l, \text{ for } z + 1 \leq x \leq t.$$

We note that $i_t - i_z \geq i_B - i_z = l - A \geq l - k$, where one of these inequalities is strict.

$$\begin{aligned} i_t - i_z &> l - k, \\ i_z - i_{z-1} &> m - k. \end{aligned}$$

Figure 5 gives the cancellation for this case.

Case 4: j divides k

We necessarily have $j + i_y = k + 0$, for some $1 \leq y \leq t$. We have

$$\begin{aligned} i_x &= xj, \text{ for } 1 \leq x \leq y, \\ k &= (y+1)j, \\ i_{y+1} - i_y &> j, \text{ if } y \neq t. \end{aligned}$$

Figure 6 provides the cancellation pattern for this case.

Case 5: j does not divide k

In this case, we necessarily have $0 + i_y = k + 0$, for some $1 \leq y \leq t$, and

$$\begin{aligned} i_x &= xj, \text{ for } 1 \leq x \leq y - 1, \\ i_y - i_{y-1} &< j. \end{aligned}$$

Figure 6 gives the pattern of cancellation for this case.

For all of the cases dealing with the upper-left cancellations, $i_t - i_{z-2} > m - k$. For all of the cases dealing with the lower-right cancellations, $i_{y+1} > k$. We conclude that $y + 1 > z - 2$. This can be tightened up for particular cases. We obtain an upper bound for y relative to z by noting that if there is too much overlap, every shift is $m - l = j$ and this either leads to a contradiction, or forces $f(x)$ to be one of the 25 polynomial exceptions. We deal with this situation now.

Suppose every shift is the same. For both cases 4 and 5, $i_1 = j$. That is, we deal with the situation when $i_x - i_{x-1} = j$ for $1 \leq x \leq t$. All of the 0's and j's will cancel with each other except for $0+i_0$ (left-over) and $j+i_t$ (which must cancel down). If $l+i_t$ is left-over (case 1.2), then $j=i_t-i_{t-1}=m-k$. In this case, all m's and k's cancel with each other except $m+i_t$ (left-over) and $k+i_0$ (which must cancel up). We have $j+i_t, k+i_0, l+i_0, l+i_1, \ldots, l+i_{t-1}$ to cancel. We must have $t=2$ and the l's must cancel up because all the m's are already taken. Since $k+i_0$ has nothing with which to cancel, we have a contradiction. Therefore we conclude that $l+i_t$ is not left-over. Furthermore, $l+i_t$ cancels with either $m+i_{t-1}$ or $m+i_{t-2}$. So either $j=i_t-i_{t-1}=m-l$ or $2j=i_t-i_{t-2}=m-l$. We deals with these situations separately.

If every shift is $j=(m-l)/2$ (i.e. if $m+i_{t-1}$ is left-over) then all m's and l's cancel with each other except $m+i_t$ and $m+i_{t-1}$ (both left-over) and $l+i_1$ and $l+i_0$, both of which must cancel up with the remaining $j+i_t, k+i_0, k+i_1, \ldots, k+i_t$. We conclude that $t=2$ and that $k+i_0=j+i_2$, $k+i_1=l+i_0$, and $k+i_2=l+i_1$. Thus we have the polynomial exception 7, $f(x)=x^6+x^4+x^3+x+1$.

If every shift is $j=m-l$ then all m's and l's cancel with each other except $m+i_t$ (left-over) and $l+i_0$ (cancels up). What must still be accounted for? $j+i_t, l+i_0, k+i_0, k+i_1, \ldots, k+i_t$. We must have $t=2$ and one of the k's is left-over. If $k+i_1$ is left-over, then we get polynomial exception 9. If $k+i_1=l+i_0$ then we get polynomial exception 4. If $k+i_1=j+i_2$ then we get the reciprocal of polynomial exception 4.

To summarize, if all shifts are the same, then we must have polynomial exception 4, 7 or 9. Henceforth, we assume that all shifts are not the same.

7 A few useful lemmas

In this section, we give several lemmas that are frequently used in the proof of Theorem 1.2.

Lemma 7.1. *If* $0+i_\beta=m+i_\alpha$ *then*

$$i_\beta=i_t=m,\ i_\alpha=i_0=0.$$

□

Lemma 7.2. *Suppose that* $m+i_\beta=j+i_\alpha$ *for* $1\le\beta<\alpha\le t$ *then*

$$i_\alpha=i_t=m,\ i_\beta=i_1=j.$$

Proof. We have

$$\begin{aligned} m &\ge i_t \\ &= i_t-i_\alpha+i_\alpha-i_\beta+i_\beta-i_1+i_1-i_0 \\ &\ge (i_t-i_\alpha)+m-j+(i_\beta-i_1)+j \\ &= m+(i_t-i_\alpha)+(i_\beta-i_1) \\ &\ge m. \end{aligned}$$

So equality must hold in all inequalities. □

Lemma 7.3. *Suppose that* $i_t - i_{t-2} \geq m - l$, $0 + i_\beta = l + i_\alpha$ *for* $0 \leq \alpha < \beta$ *and* $t - 2 \geq \beta$ *then*

$$i_t = m,\ i_{t-2} = i_\beta = l,\ \alpha = 0.$$

Proof. We have

$$\begin{array}{rcl} m & \geq & i_t \\ & = & i_t - i_{t-2} + i_{t-2} - i_\beta + i_\beta - i_\alpha + i_\alpha - i_0 \\ & \geq & m - l + (i_{t-2} - i_\beta) + l + i_\alpha \\ & = & m + (i_{t-2} - i_\beta) + i_\alpha \\ & \geq & m. \end{array}$$

So equality must hold in all inequalities. □

8 Full proof of the main theorem (Theorem 1.2)

After the preliminary assumptions in the sketch of the proof of Theorem 1.2, we proceed with the complete case analysis given below.

8.1 Case 1.1/4:

Subcase 1.1 implies $i_t - i_z = m - k$ and case 4 yields $i_{y+1} > k$, since $j + i_y = k$ and $i_{y+1} - i_y > j$. So $m < i_t - i_z + i_{y+1} \leq m - i_z + i_{y+1}$. Hence $z \leq y$.

If $y \geq z + 3$, then $j = i_y - i_{y-1} = m - l$. Hence the column $m + i_z = l + i_{z+1} = k + i_t$ gives a left-over. Now we show that $z = 0$. Otherwise, $m + i_{z-1} = l + i_z = k + i_{t-1}$ gives another left-over. Moreover, if $t > y$, then $k + i_0 = j + i_y = 0 + i_{y+1}$ gives another left-over. This implies that $t = y$. In this case, using $t = y \geq z + 3$ and $l + i_0 = l + i_z = k + i_{t-1} > k + i_{t-2} > k + i_z = j + i_t$, we conclude that $k + i_{t-2}$ must be another left-over, a contradiction. So $y \leq z + 2$. Therefore $z \leq y \leq z + 2$.

If $y = z + 2$, then we still have $j = i_y - i_{y-1} = i_{z+2} - i_{z+1} = m - l$. A similar discussion shows that $z = 0$ and $t = y = z + 2$. In this case, we have the polynomial exception 4: $f(x) = x^5 + x^4 + x^3 + x + 1$ and $h(x) = x^2 + x + 1$.

For the rest of this section, we consider $z \leq y \leq z + 1$. These bounds on y imply that m on row i_t is the only left over to the left of k on row i_t. As a result of case 1.1, we have $t \geq z + 2$, $m - l \geq j$, $i_t - i_z = m - k$, $i_t - i_{t-1} = m - l$, and $l + i_z = k + i_{t-1}$. We will frequently use these facts in the following subsections.

8.1.1 Assume $y = z$.

In this case, we have $j + i_{t-1} = l + i_0$ and $j + i_t = m + i_0$. Indeed, $y = z$ and case 4 imply that $j + i_z = k + i_0$. Together with $i_t - i_z = m - k$, we must have

$j + i_t = m + i_0$. Similarly, we have $j + i_{t-1} = l + i_0$ because of $k + i_{t-1} = l + i_z$ and $j + i_z = k + i_0$. This also shows that $0 + i_{z+1}$ can never cancel down with an l or an m. With the previously stated symmetry assumption that the third left-over term must be an m or an l or a k from the top half rows, $0 + i_{z+1}$ must cancel down with a k, so we consider the following two cases.

Case I: $0 + i_{z+1}$ cancels down with a k on row i_1. In this case, $2j = (k + i_1) - (k - j) = i_{z+1} - i_z \leq m - l$.

Case IA: $m - l = 2j$. In this case, $k + i_t = l + i_{z+1} = m + i_z$. So $m + i_{z-1}$ must cancel up with $j + i_t$. Hence we have $z = 1$. Also $0 + i_{z+1} = k + i_1$, $j + i_{z+1}$ is another leftover unless $t = z + 2$. But $t = z + 2$ and $z = 1$ contradicts the parity condition.

Case IB: $m - l > 2j$. We consider the following cases.

Case IB1: $z \geq 3$ **and** $t > z + 2$. We first show that $m - l = i_{z+1} - i_{z-1}$. Indeed, because $z \geq 3$, case $0 + i_{z+1} = k + i_1$ and the fact $i_2 - i_1 = j$ imply that $j + i_{z+1} = k + i_2$. Since $i_3 - i_2 = j$ and $i_{z+2} - i_{z+1} = m - l > 2j$, $k + i_3$ must be a left over. Hence $m + i_{z-1}$ must be canceled up. Using $i_z - i_{z-1} = j < m - l$, $l + i_z = k + i_{t-1}$, and $m + i_0 = j + i_t$, we obtain that the cancellation must be $m + i_{z-1} = l + i_{z+1}$. Hence $m - l = i_{z+1} - i_{z-1} = (i_{z+1} - i_z) + (i_z - i_{z-1}) = 2j + j = 3j$. Moreover, $z \geq 3$ and $i_z - i_{z-2} = 2j$ force that $m + i_{z-2} > l + i_z = k + i_{t-1}$ and thus $m + i_{z-2}$ is another left-over, a contradiction.

Case IB2: $z \geq 3$ **and** $t = z + 2$. The fact $t = z + 2$ implies $l - k = 2j$ and thus $k + i_2 = l + i_0$. Because $t = z + 2$, we have $j + i_{z+1} = j + i_{t-1} = l + i_0 = k + i_2$. This shows that we have a left-over term from the column $j + i_{z+1} = l + i_0 = k + i_2$. Hence $m + i_{z-1}$ must be canceled up. Moreover, we must have $m + i_{z-1} = l + i_{z+1}$ and thus $m - l = 3j$ by using a similar argument as in case IB1. Then $l + i_3 = m + i_0 = j + i_{z+2}$ gives another left-over, a contradiction.

Case IB3: $z \leq 2$ **and** $t > z + 2$. If $z = 1$, then $k = 2j$. The fact that $m - l > 2j$ implies that $l + i_0 = j + i_{t-1}$ is to the left of $k + i_{z+1}$ and $0 + i_{z+2}$ is to the left of $k + i_{z+1}$. Then both $k + i_{z+1}$ and $j + i_{z+1}$ can't cancel out with anything, so they are leftovers, a contradiction. If $z = 2$, then $k - j = 2j$. The fact that $l + i_z = k + i_{t-1}$, $j + i_{t-1} = l + i_0$ and $j + i_t = m + i_0$ implies that $l + i_{z+1}$ can not cancel up. It must cancel down with $m + i_{z-1} = m + i_1$ or it is a left-over. Consider the case that $l + i_{z+1} = m + i_{z-1}$, then $m - l = 3j$. Then $0 + i_t = k + i_{t-1} = l + i_2$ gives a left-over. Moreover, $l + i_1$ is another left-over, a contradiction. Consider now the case that $l + i_{z+1}$ is a left over. Then the fact that $l + i_z = k + i_{t-1}$, $m + i_0 = j + i_t$, and $i_z - i_{z-1} = i_2 - i_1 = j$ implies that $m + i_{z-1}$ is to the left of $l + i_z = k + i_{t-1}$, which shows that $m + i_{z-1}$ is another left-over, a contradiction.

Case IB4: $z \le 2$ **and** $t = z + 2$**.** Note $l - k = 2j$. If $z = 1$, then $t = 3$ and thus it contradicts the parity condition. If $z = 2$, then $k - j = 2j$ implies that $j + i_{z+1} = k + i_z$. Moreover, $j + i_{z+1} = j + i_{t-1} = l + i_0$. Hence $j + i_{z+1} = k + i_z = l + i_0$ gives a left-over. But $l + i_1$ is another leftover, a contradiction.

Case II: $0 + i_{z+1}$ **cancels down with a** k **on row** i_p **with** $p > 1$**.**

The fact that $l - k = l + i_t - (k + i_t) = m + i_{t-1} - (m + i_z) = i_{t-1} - i_z \ge i_{z+1} - i_z$, $j + i_z = k + i_z$, $0 + i_{z+1} = k + i_p$ with $p > 1$ implies that $k + i_1$ must be a left-over. Moreover, $p = 2$. Otherwise, both $k + i_1$ and $k + i_2$ are left-overs because $j + i_{t-1} = l + i_0$ is to the left of $j + i_{z+1}$. In this case, $z \ge 2$. Using that $k + i_1$ is a left-over and $z \ge 2$, we can show that $m - l = i_{z+1} - i_{z-1}$. Since $0 + i_{z+1} = k + i_2$ and $j + i_z = k + i_0$, we have $i_{z+1} - i_z = 3j$. Hence $m - l = i_{z+1} - i_{z-1} = 4j$. If $z > 2$, then $m - l = 4j$ implies that $m + i_{z-2}$ is to the left of $l + i_z = k + i_{t-1}$ and thus $m + i_{z-2}$ is another left-over, a contradiction. Therefore we have $z = 2$. Moreover, $t = z + 2$, for otherwise, $k + i_{z+2}$ is a leftover. Using $z = 2$, $t = z + 2$ and $m - l = 4j$, we have that $l + i_1$ is to the right of $0 + i_t$ and thus $l + i_1$ is another left over, a contradiction.

8.1.2 Assume $y = z + 1$

Case 4 and $y = z + 1$ imply that $i_{i+1} - i_i = j$ for any $0 \le i \le z$ and $j + i_{z+1} = k + i_0$. We also have $m + i_0 > j + i_t$ because $i_t - i_z = m - k$ and $j + i_{z+1} = k + i_0$. Similarly, $l + i_0 > j + i_{t-1}$ because $i_{t-1} - i_z = l - k$ and $j + i_{z+1} = k + i_0$. With the previously stated symmetry assumption that the third left-over term must be an m or l or a k from the top half rows, $0 + i_{z+2}$ must cancel down. Hence $m + i_0 > j + i_t$ and $l + i_0 > j + i_{t-1}$ imply that $0 + i_{z+2}$ can never cancel down with an l or an m if $t > z + 2$. If $t = z + 2$, then $0 + i_{z+2}$ could cancel down with an l or a k, but not an m. We consider the following two cases.

Case I: $t = z + 2$**.** In this case $l - k = i_{t-1} - i_z = j$. Because $i_{z+2} - i_{z+1} = m - l < m - k$ and $k + i_0 = j + i_{z+1}$, we have $m > k + i_{z+2} - i_{z+1} = j + i_{z+1} + i_{z+2} - i_{z+1} = j + i_{z+2}$. This means that $m + i_0$ is to the left of $j + i_{z+2}$.

Case IA: $0 + i_{z+2} = k + i_p$ **for some** $1 \le p \le z$**.** Since $m + i_0$ is to the left of $j + i_{z+2}$, $0 + i_{z+2} = k + i_p = l + i_{p-1}$ and $j + i_{z+2} = k + i_{p+1} = l + i_p$ give two left overs, a contradiction.

Case IB: $0 + i_{z+2} = k + i_{z+1}$**.** In this case, $0 + i_{z+2} = k + i_{z+1} = l + i_z$ gives a left-over. Since $l - k = j$, we have $j + i_{z+2} = l + i_{z+1}$. If $z \ge 1$, then $m + i_0$ is another left-over, a contradiction. If $z = 0$, then $k - j = j$. Hence $k = 2j$, $l = 3j$, and $m = 5j$. From the greatest common divisor condition, we have $j = 1$. Hence we obtain the polynomial exception 2: $f(x) = x^5 + x^3 + x^2 + x + 1$ and $h(x) = x^3 + x + 1$.

Case IC: $0 + i_{z+2} = l + i_p$ **for some** $1 \le p \le z$**.** In this case, $l - k = i_{z+1} - i_z = j$. Moreover, $m - l = i_{z+2} - i_{z+1} = (l + i_p) - (k + i_0 - j) = (p+2)j$. We now consider all possible values of p. If $p \geq 2$, then $m - l \geq 4j$. Together with $m + i_0 > j + i_t$, we conclude that both $m + i_{z-1}$ and $m + i_{z-2}$ are left overs, a contradiction. If $p = 1$, i.e., $0 + i_{z+2} = l + i_1$, then $m - l = 3j$. We show that $z \leq 1$. Indeed, if $z \geq 2$, then both $m + i_{z-1}$ and $m + i_{z-2}$ are left-overs, a contradiction. Since $z = 1$ contradicts the parity condition, we conclude further that $z = 0$. In this case, $j = 1$, $k = 2$, $l = 3$, $m = 6$, which implies $j + i_t$ is a leftover, contradicting the symmetry assumption that the third leftover is an m or an l or a k. Finally if $p = 0$, i.e., $0 + i_{z+2} = l + i_0$, then $m - l = 2j$. So $l - k = j$ implies that $k + i_1 = l + i_0 = 0 + i_{z+2}$, which gives a left-over. Moreover, if $z \geq 2$, then $k + i_1 = l + i_0 = 0 + i_{z+2}$ and $l - k = j$ imply that $k + i_2 = l + i_1 = j + i_{z+2}$, which gives another left-over, a contradiction. Hence $z \leq 1$. Since $z = 1$ contradicts the parity condition, we must have $z = 0$. In this case, we have the polynomial exception 2: $f(x) = x^5 + x^3 + x^2 + x + 1$ and $h(x) = x^3 + x + 1$.

Case II: $t \geq z + 3$.

We note that $0 + i_{z+2}$ can't cancel down with an l or an m as explained earlier.

Case IIA: $0 + i_{z+2}$ cancels down with k on row i_1.

To prove that $t \leq z + 3$, we assume that $t \geq z + 4$. Then $l - k = (t - z - 2)(m - l) + j \geq 2(m - l) + j$. In this case, $m - l = i_{z+2} - i_{z+1} = k + i_1 - (k - j) = 2j$. Moreover, $0 + i_t = (i_t - i_{t-1}) + (i_{t-1} - i_z) - (i_{z+1} - i_z) + i_{z+1} = (m - l) + (l - k) - j + (k - j) = 2j + (l - k) - j + (k - j) = l = l + i_0$. Therefore $j + i_t = l + i_1$.

If z is very small (say, $z + 1 < 2(t - z - 2)$), then there is at least 1 left-over j or 0 from row i_{z+2} to row i_{t-1} (those j's or 0's can only be canceled down with k's from row i_2 to row i_{z+1} and we don't have enough k's). This contradicts our symmetry assumption that the third leftover is not a 0 nor j.

So $z \geq 2(t - z - 1) - 1 \geq 3$. In this case, the column $m + i_{z-2} = l + i_z = k + i_{t-1}$ gives a left-over. Consider the column of $0 + i_t = l + i_0$. If there was a $k + i_p$ in this column, then there would be a left-over from this column, a contradiction. On the other hand, if there was no $k + i_p$ in the column of $0 + i_t$, then $j + i_{t-1} = k + i_a$ for some $a \geq z + 1$ because each shift is either a j shift or $2j$ shift. Hence $k + i_{a+1} = j + i_t = l + i_1$ gives a left-over.

Therefore the previous discussion gives $t = z + 3$. Then $l - k = (m - l) + j = 3j$ and $0 + i_{z+3} = l + i_0$. It is easy to use parity condition to exclude $z = 0$ and $z = 2$. If $z = 1$, then we have the polynomial exception 16: $f(x) = x^8 + x^6 + x^3 + x + 1$ and $h(x) = x^6 + x^4 + x^2 + x + 1$. If $z \geq 3$, then $0 + i_{z+3} = k + i_3 = l + i_0$ and $j + i_{z+3} = k + i_4 = l + i_1$ give a contradiction.

Case IIB: $0 + i_{z+2}$ cancels down with k on row i_p with $p \geq 2$.

Since $t > z + 2$, we have $l - k \geq (m - l) + j$. In this case, k on row i_1 is left-over. We claim that $0 + i_{z+2}$ cancels down with k on row i_2. Suppose $p > 2$, then $k+i_{p-1}$ can only be canceled down with $l+i_c$ for $c \leq p-2$. Hence $0+i_{z+2}=k+i_p=l+i_{c+1}$ and thus we have two left overs. Therefore, we must have $p=2$. This implies $m-l=i_{z+2}-i_{z+1}=k+i_2-(k-j)=3j$ and $z \geq 1$.

We show that $t=z+3$. Assume that $t \geq z+4$. Note that $z \geq 1$ and $l-k=(t-z-2)(m-l)+j \geq 7j$. If $z \geq 3$, using $m-l=3j$, one get $0+i_{z+2}=k+i_2=(z+4)j$, $j+i_{z+2}=k+i_3=(z+5)j$, and $0+i_{z+3}=(z+7)j$. This implies that $k+i_4=(z+6)j<0+i_{z+3}$ and thus k on row i_4 can not cancel up with a j or 0. Moreover $l-k=7j$ implies that k on row i_4 can not cancel down with an l or m. Hence k on row i_4 must be another left-over, a contradiction. If $z=2$, then 0 on row i_{z+3} must be a left-over, a contradiction. If $z=1$, then j on row i_{z+2} must be a left-over.

Therefore $t=z+3$. In this case, $l-k=4j$ and $m-l=i_{z+2}-i_{z+1}=k+i_2-(k-j)=3j$. If $z=1$, then $0+i_{z+2}=k+i_2=k+i_{z+1}$ implies that $k=i_{z+2}-i_{z+1}=m-l=3j$. Using $l-k>m-l$, we have $l+i_0>(k+i_0)+(m-l)=(j+i_{z+1})+(i_{z+2}-i_{z+1})=j+i_{z+2}$. Hence $l+i_0$ is to the left of $j+i_{z+2}$ and $j+i_{z+2}$ is another left-over, a contradiction. Note that $z=2$ is excluded by parity condition. If $z>2$, then we have $0+i_{z+3}=l+i_1$ and $j+i_{z+3}=l+i_2$ by using $i_{z+3}-i_{z+2}=m-l=3j$, $l-k=4j$, and $0+i_{z+2}=k+i_2$. Because $0+i_t=0+i_{z+3}=l+i_1$ and $j+i_t=j+i_{z+3}=l+i_2$ and $m+i_{z-1}>l+i_z=k+i_{t-1}$, we must have $m+i_{z-1}=l+i_{z+1}$. In this case, $m-l=i_{z+1}-i_{z-1}=2j$, a contradiction.

8.2 Case 1.1/5:

First suppose that $y \leq z-1$. Then $m \geq i_t=i_t-i_z+i_z-i_y+i_y-i_0=m-k+(i_z-i_y)+k-0>m$ is a contradiction. On the other hand if $y \geq z+2$ then $j=i_{z+1}-i_z \leq m-l$ but $m-l=i_y-i_{y-1}<j$ which is a contradiction. We break into two initial cases.

8.2.1 Assume $y=z$

First we note that in this case $z=y \geq 2$ and $t \geq z+2$. With this in mind and $m \geq i_t=i_t-i_z+i_z-i_0=m-k+k-0=m$, we get that $i_t=m$, $i_{t-1}=l$, $m+i_0=0+i_t$, $l+i_0=0+i_{t-1}$, $m+i_1=j+i_t$, $l+i_1=j+i_{t-1}$, $k+i_1=j+i_z$, and $k+i_{t-1}=l+i_z$. Also we can determine what cancels with $j+i_{z-1}$. If it canceled down then since $k+i_1=j+i_z>j+i_{z-1}$, it would have to cancel with $l+i_0$ or $m+i_0$, the cancellation of these has been accounted for. Therefore it must cancel up with $0+i_\alpha$. If $\alpha>z+1$ then the $0+i_{z+1}$ must cancel down. Again since $k+i_0=0+i_z<0+i_{z+1}<0+i_\alpha=j+i_{z-1}<j+i_z=k+i_1$ it can only cancel down with $l+i_0$ or $m+i_0$ implying that $t=z+1$ or $z+2$. By the assumption that $\alpha>z+1$ we have that $t=\alpha=z+2$. Then $0+i_{z+2}=j+i_{z-1}=m+i_0$ and since $k+i_1=j+i_z>j+i_{z-1}$ there is nothing else to cancel in this column. Thus one of these must be left-over and by assumption it must be $m+i_0$. So $fg = h = 1 + x^m + x^{2m}$. We have $j + i_t = m + i_1$ so $l + i_{z+1}$ must cancel down with $m = i_{z-1}$ and $j = 2(m-l)$. Now considering $l + i_{z-1} > m + i_{z-2}$ so $l + i_{z-1}$ must cancel up with $k + i_z$, and $m - l = 2(l-k)$. We have $j = 4(l-k)$, $m - l = 2(l-k)$, $m = zj = 4z(l-k)$ and $k = m-(m-l)-(l-k) = 4z(l-k)+2(l-k)+(l-k) = (4z+3)(l-k)$, so by the GCD condition, $l-k = 1$, $m-l = 2$ and $j = 4$. Similarly we have that $k + i_{z-1}$ must cancel up and so we can conclude that $z = 2$. This gives $k = 5$, $l = 6$ and $m = 8$. But now fg is pentanomial which is a contradiction.

So $j + i_{z-1} = 0 + i_{z+1}$. If either $z = 2$ or $z > 2$ we have accounted for the cancellation of $j + i_1$. We will make good use of the fact that we have found all the cancellations of all the elements on rows 0, 1, t and $t-1$ (except $l + i_{t-1}$ when $t = z+2$).

What cancels with $l + i_{z+1}$. Since $k + i_{t-1} < l + i_{z+1} \leq k + i_t$ and $z + 1 \geq 3$, it cannot cancel up (unless it cancels up with $k + i_t$ but this is the same as being left-over) so it must cancel down with an m or be left-over.

Case I: $l + i_{z+1}$ is left-over. We ask what does $j + i_{z+1}$ cancel with.

Case IA: $j + i_{z+1} = l + i_\alpha$ or $j + i_{z+1} = m + i_\alpha$. If $0 + i_t = m + i_0$, then $j + i_t = m + i_1$. This is therefore the only possible cancellation of an m and a j so $\alpha = 1$. Similarly if $0 + i_{t-1} = l + i_0$ then $j + i_{t-1} = l + i_1$ we also get that $\alpha = 1$. In either case this implies that $t = z+2$. Now $0 + i_{z+1} = j + i_{z-1} = l + i_0$ so this must be the left-over term. But this contradicts fact that $l + i_{z+1}$ is left-over.

Case IB: $j + i_{z+1} = 0 + i_\alpha$. In this case we will have that $m - l$ divides j.

Case IB1: $\alpha > z+2$. We consider $0 + i_{z+2}$. It must cancel down but all j's below it are taken. If $z > 2$ then $k + i_2 = k + i_1 + j = j + i_z + j > j + i_{z+1} > 0 + i_{z+2}$ so the only k available is $k + i_2$ if $z = 2$. Other wise it cancels with an l or m.

Case IB1a: $0 + i_{z+2} = k + i_z$. We have $z = 2$. We have $m = i_t = i_t - i_{z+1} + i_{z+1} = 2j + (t-z-1)(m-l) = i_t - i_{z+2} + i_{z+2} = 2k + (t-z-2)(m-l)$ so we have j, $2k$, l and m divisible by $m-l$. The GCD condition gives $2k - 2j = m - l = 2$. If $\alpha > z+3$ then $0 + i_{z+3}$ must cancel down with an l (m is impossible by the parity of t). This gives $t = 6$, $j = 3(m-l) = 6$, $k = 7$ and $f = 1 + x^6 + x^7 + x^{16} + x^{18}$ and $h = 1 + x^6 + x^7 + x^{12} + x^{14} + x^{16} + x^{18}$ and $g = fh$ is not a trinomial.
If $\alpha = z+3$ then $j + i_{z+1} = j + i_3 = 0 + i_5$. Now $j = 2(m-l) = 4$ and $k = 5$. We have $k + i_{z+1} = 5 + 8 = 13$, but for $\beta > z+1$ all $0 + i_\beta$ and $j + i_\beta$ are even. All m's and l's below i_{z+1} are accounted for so $k + i_{z+1} = k + i_3$ is left-over. But $l + i_{z+1}$ has nothing to cancel with and must be left-over too. Thus fg is not a trinomial.

Case IB1b: $0 + i_{z+2} = l + i_\beta$. In this case $t = z+3$ and $\beta = 0$. We have $j + i_{z+1} = 0 + i_{z+3} = m + i_0$ so $j = 2(m-l)$ and we must have another thing to cancel in this column. It can only be k but since k is not divisible by j it must be $k+i_z$. We have $m = 2k = (z+1)j = 2(z+1)(m-l)$. The GCD condition now gives that $m-l = 1, j = 2, m-k = 2(m-l)+i_{z+1}-i_z = 2+1 = 3$, $k = 3$, $l = 5$, $m = 6$, and $t = 5$ which is a contradiction.

Case IB1c: $0 + i_{z+2} = m + i_\beta$**.** In this case $t = z+2$ and $\beta = 0$. But this contradicts the assumption that $j + i_{z+1} = 0 + i_\alpha$ and $\alpha > z+2$.

Case IB2: $\alpha = z+2$**.** In this case we have $m - l = i_{z+2} - i_{z+1} = j$ and $l + i_{z+1}$ being left-over implies that $m + i_{z-1}$ must cancel up with something else and the only possibility forces $z = 2$ and $m+i_1 = j+i_t$. We can also conclude that $0 + i_{t-1} = j + i_{t-2} = l + i_0 = k + i_\beta$ for some β. The fact that j does not divide k forces $\beta = z$. So $2k = k + i_2 = l + i_0$. We have $k - j < j$ since $i_2 - i_1 < j$. We also have that $i_{t-2} - i_2 = k - j < j = m - l$. This implies that $i_{t-2} = i_3$ which violates the even parity of t.

Case IC: $j + i_{z+1} = k + i_\alpha$**,** $\alpha < z$**.** In this case we get that $k = j + i_{z+1} - i_\alpha$ is a multiple of j which cannot happen.

Case ID: $j + i_{z+1} = k + i_\alpha$**,** $\alpha = z$**.** Now $k - j = i_{z+1} - i_z < j$ so $z = 2$, and $k = 3j/2$. We now examine $0 + i_{z+2}$. It must cancel down and if $t - 1 > z + 2 = 4$ we have nothing below to cancel with. So $t \leq 5$ and by parity $t = 4$, $l = 2j$ and $0 + i_3 = j + i_1 = l + i_0$ but none of these can be left-over.

Case II: $l + i_{z+1} = m + i_{z-1}$**.** Now we have that $m - l = j$ and so the cancellation of all m's, l's, j's and 0's is accounted for. We have $j + i_t = l + i_2 = m + i_1$ and $0 + i_{t-1} = j + i_{t-2} = l + i_0$. At most one of these can furnish the left-over term, so we must have $k + i_\beta = l + i_0$ or $m + i_1$. If β is not z then i_β is a multiple of $j = m - l$ and we have k as a multiple of j which cannot happen in case 5. So we must have $k = i_z = l - k$ or $k = i_z = m - k + j$. In either case j divides $2k$ and so the GCD condition gives that $j = 2$. Because we know the cancellations of all m's, l's, j's and 0's, the only k's that appear are the ones already accounted for and possibly one left-over, thus $4 \leq t \leq 6$ and even. If $t = 4$ then $z = 2$, $f = 1 + x^2 + x^3 + x^4 + x^6$ and $h = f$ so $fh = g$ is not trinomial. If $t = 6$ and $z = 2$, $f = 1 + x^2 + x^3 + x^8 + x^{10}$ and $h = 1 + x^2 + x^3 + x^4 + x^6 + x^8 + x^{10}$ and $g = fh$ is not a trinomial. Similarly if $t = 6$ and $z = 4$ which is just the reciprocal case. If $t = 6$ and $z = 3$ then $f = 1 + x^2 + x^5 + x^8 + x^{10}$, $h = 1 + x^2 + x^4 + x^5 + x^6 + x^8 + x^{10}$ and again $g = fh$ is not trinomial.

Case III: $l + i_{z+1} = m + i_\alpha$**,** $\alpha < z - 1$**.**

In this case we have that $m + i_{z-1} = j + i_t$ thus $z = 2$ and $m + i_{z-1} = m + i_1$. Also, $l + i_{z+1} = l + i_3 = m + i_0 = 0 + i_t$. But nothing else cancels in this column since $k + i_{t-1} = l + i_z < l + i_{z+1}$. So one of these is left-over (by our assumptions it is either the l or m). Since $i_{z+1} - i_0 = m - l$, we have that $m - 0 = (t-2)(m-l)$,

$m-l=2j$. Since $i_{z+2}-i_{z+1}=m-l>j$ we can conclude that $j+i_{z+1}$ must cancel down and either with $k+i_z$ or with $l+i_1$ (in which case $t=4$ since $l+i_0=0+i_{z-1}$). If $k-j=i_{z+1}-i_z$ then $j=2(k-j)$ and we have $k-j=1$ by the GCD condition and $j=2$, $k=3$, $l=4(t-3)$ and $m=4(t-2)$. If $t>4$ then $0+i_4$ is left-over which is a contradiction.

If $t=4$ then $f=1+x^2+x^3+x^4+x^8$, $h=1+x^2+x^3+x^4+x^8$ and $g=fh$ is pentanomial.

Case IV: $l+i_{z+1}=m+i_\alpha$, $\alpha<z-1$ and $m+i_{z-1}$ is left-over.

In this case we have that $m-l=i_{z+1}-i_\alpha=i_{z+1}-i_{z-1}+i_{z-1}-i_\alpha=j+i_{z-1}-i_\alpha>j$ so $j+i_{z+1}$ cannot cancel up. There are three cases

Case IVA: $j+i_{z+1}=k+i_\beta$. If $\beta\leq z-1$ then we can show that k is divisible by j, so $\beta=z$. Now $k-j=i_{z+1}-i_z<i_{z+1}-i_{z-1}=j$ so $z=2$ and $2(k-j)=j$ and $k=3j/2$. Now $0+i_4$ must cancel down.

CASE IVA1: $0+i_4=k+i_\gamma$. The only possible γ is 3 and $k-0=m-l$ and $j+i_4$ also cannot cancel up. There are no available k's below so it cancels with an l or m and we get $t=4$ (we use parity forbid $t=5$). We have $f=1+x^2+x^3+x^4+x^7$, $h=f$ and thus $g=hf$ is not trinomial.

CASE IVA2: $0+i_4=l+i_\gamma$. In this case the parity of t forces $t=4$ and $0+i_4=l+i_1=j+i_3$ which is a contradiction.

CASE IVA3: $0+i_4=m+i_\gamma$. In this case $t=4$, and $2j=0+i_3=l+i_0$ and so $l+i_0$ is left-over which is a contradiction.

Case IVB: $j+i_{z+1}=l+i_\beta$. Considering the 0, j and m, l cancellations on top two and bottom two rows we get $t=z+2$ and $\beta=1$. This implies that $0+i_{z+1}=j+i_{z-1}=l+i_0$. One of these must be left-over which contradicts the assumption that $m+i_{z-1}$ is left-over.

Case IVC: $j+i_{z+1}=m+i_\beta$. Considering the 0, j and m, l cancellations on top two and bottom two rows we get the contradiction that $t=z+1$.

8.2.2 Assume $y=z+1$

In this case we have $z\geq 1$ and $t\geq z+2$. Also $0+i_t<m+i_0$ so 0's never cancel with m's. We first split into three cases depending on the position of $0+i_{z+2}$.

Case I: $0+i_{z+2}<j+i_z$.

We have that $0+i_{z+2}$ must cancel down with $l+i_0$. If $t>z+2$ then $m>i_t=i_t-i_{z+2}+i_{z+2}-i_0\geq m-l+l-0=m$ which is impossible so $t=z+2$. Now $j+i_z$ must cancel down with $m+i_0$ and $m=(z-1)j$, $i_{z+2}-i_{z+1}=l-k=m-l$. We have $j=j+i_{z+1}-(j+i_z)+j+i_z-(0+i_{z+2})+0+i_{z+2}-(0+i_{z+1})=i_{z+1}-i_z+m+i_0-(l+i_0)+i_{z+2}-i_{z+1}=3(l-k)$. Thus we have that $j/3$ divides j, k, l and m so the GCD condition gives that $j=3$, $m-l=l-k=1$. $k+i_{z+2}=l+i_{z+1}=m+i_z$ and there is nothing else in this column so the left-over is here. Thus if $z>1$ the $m+i_1$ must cancel up with something. Since $m+i_1>j+i_{z+2}$ it must cancel up with a k, but if

$z > 1$ then $m + i_1 < k + i_2$, so we can conclude that $z = 1$. This gives $t = 3$ which violates parity.

Case II: $0 + i_{z+2} = j + i_z$.

Here $j = i_{z+2} - i_z = m - l + i_{z+1} - i_z > m - l$ so $l + i_{z+1}$ either cancels up or is left-over.

Case IIA: $l + i_{z+1}$ **cancels up.** Since $l + i_{z+1} > l + i_z = k + i_{t-1}$ we get that $l + i_{z+1} = j + i_t$ or $l + i_{z+1} = 0 + i_1$. In the later case we get the contradiction $m > i_t = i_t - i_{z+1} + i_{z+1} - i_z + i_z - i_0 = l + (i_{z+1} - i_z) + zj > l + (i_{z+1} - i_z) + m - l > m$. In the former case a similar consideration gives that $z = 1$. Since $l + i_2 = j + i_t = k + i_t - (k - j) = m + i_1 - (k - j)$, $i_2 - i_1 = m - l - k + j$ and we have $j = i_3 - i_2 + i_2 - i_1 = 2m - 2l - k + j$ so $k = 2(m - l)$. Since t is even and it is at least $z + 2 = 3$ we have $t \geq 4$ and this gives $l + i_0 = j + i_{t-2}$, $0 + i_t = k + i_{t-2}$ and $j + i_{t-1} = m + i_0$. Now $k - j = k + i_{t-1} - (j + i_{t-1}) = l + i_1 - (m - i_0) = l + j - m$ so $2j = k + m - l = 3(m-l)$ and $m = j + i_{t-1} = j + (t-1-2)(m-l) + i_2 = j + (t-3)(m-l) + k = 3(m-l)/2 + (t-3)(m-l) + 2(m-l) = t(m-l) + (m-l)/2$. The GCD condition now gives that $m - l = 2$, $k = 4$, $j = 3$. We have $0 + i_4 < j + i_3$ and either $t = 4$ or $j + i_3 < 0 + i_5$ so $j + i_3$ must cancel down with an l or m, but we know all cancellations of m and l on the first three rows. So we can conclude that $t \leq 5$ which implies that $t = 4$ and $f = 1 + x^3 + x^4 + x^7 + x^9$, $h = 1 + x^3 + x^4 + x^6 + x^8$ and $g = fh = 1 + x^7 + x^{17}$ which is polynomial exception 19.

CASE IIB: $l + i_{z+1}$ **is left-over.** We consider $m + i_{z-1}$. This must cancel up. We have $i_z - i_{z-1} = j > m - l$ so $l + i_z > m + i_{z-1}$ and $l + i_z = k + i_{t-1}$. If $m + i_{z-1} = j + i_\alpha$ and $z \geq 2$ then $m > i_t = i_t - i_\alpha + i_\alpha - i_{z-1} + i_{z-1} = i_t - i_\alpha + m - j + j > m$ so we have that $z = 1$. Now $2(m - l) > m - l + i_{z+1} - i_z = j$ so $\alpha = t$ or $t - 1$. If the latter then where does $j + i_t$ cancel? We have $k - j < j \leq 2(m - l)$ so since $t \geq 4 = z + 3$, $k + i_{t-2} < j + i_t$ and $j + i_t$ has nowhere to cancel. So we have $m + i_1 = j + i_t$ which contradicts $m + i_1 = m + i_z = k + i_t$.

So we can conclude that $m + i_{z-1} = k + i_\alpha$, $\alpha \leq t - 2$. If $\alpha < t - 2$ then we consider $k + i_{t-2}$. It has nothing to cancel down with so it must cancel up. It cannot cancel up with a 0 since this would imply that $0 + i_t > m + i_{z-1}$. It must cancel up with a j. If $k + i_{t-2} = j + i_{t-1}$ we get $m - l = i_{t-1} - i_{t-2} = k - j$ but $k - j = i_{z+1} - i_z < m - l$, so $k + i_{t-2} = j + i_t$, giving $k - j = 2(m - l)$. If $z > 1$ we have $m > i_t = i_t - i_{t-2} + i_{t-2} - i_\alpha + i_\alpha - i_{z-1} + i_{z-1} = k - j + (i_{t-2} - i_\alpha) + m - k + (z-1)j > m$ so $z = 1$. We now have that $k - j = i_{z+1} - i_z < m - l$ and $k - j = 2(m - l)$ which contradict each other.

So we can conclude that $m + i_{z-1} = k + i_{t-2}$. This gives that $2(m - l) = k + i_t - (k + i_{t-2}) = m + i_z - (m + i_{z-1}) = j$ which implies that $k - zj = i_{z+1} - i_z = m - l$. The GCD condition now gives that $j = 2$, $m - l = 1$, $k = 2z + 1$, $l = t + z$ and $m = t + z + 1$.

If $t \geq z+3$ then $0+i_{z+3}=j+i_{z+1}=k+i_1$ but none of these is left-over so they also equal $l+i_0$, which in turn forces $t=z+3$, $l=2z+3$ and $m=2z+4$. Now if $z \geq 2$ then $m+i_{z-2}$ must cancel up with a j which forces $z=2$, $t=5$ which cannot happen. If $z=1$ then $t=4$, $f=1+x^2+x^3+x^5+x^6$, $h=1+x^2+x^3+x^4+x^5$ and $g=fh$ is not a trinomial.

So we have that $t=z+2$, $l=2z+2$ and $m=2z+3$. By parity z is even so must be at least 2 and $l+i_{z-1}$ must cancel up with a j. Since $0+i_t < m+i_{z-2}$ we must have $l+i_{z-1}=j+i_t$. Thus $z=2$, $f=1+x^2+x^5+x^6+x^7$, $h=1+x^2+x^4+x^5+x^6$ and $g=fh$ is not trinomial.

Case III: $0+i_{z+2} > j+i_z$ **.**

We ask what $j+i_z$ cancels down with. If $j+i_z=m+i_0$ then we have $m > i_t \geq i_t - i_{z+2} + i_{z+2} - i_z + i_z > i_t - i_{z+2} + j + m - j > m$ so $j+i_z=l+i_0$. But $0+i_t < m+i_0$ implies that $0+i_{t-1} < l+i_0 = j+i_z < 0+i_{z+2}$, so $t-1 < z+2$ which gives that $t=z+2$. Now $0+i_{z+2}$ cancels down with either a k or l.

Case IIIA: $0+i_{z+2}=k+i_\alpha$. If $\alpha > 2$ then what does $k+i_2$ cancel with? It must cancel down with $l+i_1$ or $m+i_0$ or be left-over. If $k+i_2=m+i_0$ then we get the contradiction that $0+i_{z+2} > m+i_0$. So we have $l-k=i_2-i_1$ This combined with $l-k=i_{z+1}-i_z < j$ forces $z=1$ and $t=3$ violates the parity of t.

So $0+i_{z+2}=k+i_2$ and we get that $m-l=2j$. We have that $k=zj+i_{z-1}-i_z=zj+l-k$, $l=(z+1)j$ and thus j divides $2k$, l, and m so the GCD condition gives that $j=2$, $m-l=4$, $l=2z+2$, $k=(2z+1)$ and $m=2z+6$. One of $l+i_{z+1}$ or $m+i_{z-1}$ must cancel and it must be up with a j. If $m+i_{z-1}=j+i_t$ this implies $k-j=j$. Alternatively if $l+i_{z+1}=j+i_t$ then $k-j < m-l$. In either case $k-j \leq 3$. If $k-j=1$ then $z=1$ and $t=3$ is the wrong parity. If $k-j=2$ then j divides k which is a contradiction. So $k-j=3$ and $f=1+x^2+x^5+x^6+x^{10}$, $h=1+x^2+x^4+x^5+x^9$ and their product is not trinomial.

If $k+i_2$ does not cancel and is left-over then $t=4$ and $0+i_4=k+i_3$. This gives that $k=m-l$. Now $l+i_1$ is not left-over but cannot cancel up because if it did we would have $l+i_1=j+i_t$ implying $l+i_0=0+i_t$, contradicting $j+i_z=l+i_0$. Thus it must cancel down with $m+i_0$ and this gives $k=m-l=j$ which is a contradiction.

Case IIIB: $0+i_{z+2}=l+i_\alpha$. If $\alpha > 1$ then $l+i_1$ is left-over or must cancel. If it cancels it must be down with $m+i_0$ or up with a k.

Case IIIB1: $l+i_1=m+i_0$. In this case $m-l=i_1-i_0=j$ and thus $0+i_{z+2}=j+i_{z+1}$ contradicting $j+i_{z+1}=k+i_1$.

Case IIIB2: $l+i_1=k+i_\beta$. We have $l-k=l+i_0-(k+i_0)=j+i_z-(0+i_{z+1})=j-(i_{z+1}-i_z) < j$. So if $z \geq 2$ then $l+i_1 < k+i_2$ and there are no k's with which to cancel. So $z = 1$ which gives $t = 3$ in violation of ts parity.

Case IIIB3: $l + i_1$ is left-over. If $\alpha > 2$ then $l + i_2$ must cancel. If $z \geq 3$ then $l + i_2 < k + i_3$ and there are no k's with which to cancel up. If $z = 2$ then $t = 4$, $0 + i_4 = l + i_3$, $l = m - l$, $l = 3j$, $m = 6j$ and $2k = k + i_{z+1} = +i_z = l + 2j = 5j$. The GCD condition now gives that $f = 1 + x^2 + x^5 + x^6 + x^{12}$, $h = 1 + x^2 + x^4 + x^5 + x^{11}$ and $g = fh$ is not trinomial.

We can now conclude that $l + i_2$ must cancel down. If with $m + i_1$ this gives the contradiction that $j = m - l > j$. If $l + i_2 = m + i_0$ then $m - l = 2j$. This implies that $0 + i_{z+2} = 0 + i_{z+1} + 2j = k + 2j = k + i_2$ which cannot possibly be equal to $l + i_\alpha$ as we are assuming here.

Now we have that $0 + i_{z+2} = l + i_2$. Now $k + i_2$ cannot cancel up and so must cancel down with $m + i_1$ or $m + i_0$. If the former we get that $m - k = j$ which contradicts $m - l > j$. If the latter we have that $m - k = 2j$ and then $0 + i_{z+2} = 0 + i_z + (i_{z+2} - i_z) = 0 + i_z + m - k = 0 + i_z + 2j = j + i_z + j = l + i_0 + j = l + i_1$ which is left-over by assumption.

Case IIIB4: $0 + i_{z+2} = l + i_1$. We have $0 + i_{z+2} = l + i_1 = l + j$ and $l - j = i_2$, thus $m - k = i_{z+2} - i_z = 2j$. We also have that $2k = k + i_{z+1} = l + i_z = (z + 1)j + zj = (2z + 1)j$. The GCD condition now gives that $j = 2$, $k = 2z + 1$, $l = 2z + 2$ and $m = 2z + 5$. Now if $z \geq 4$, $l + i_{z-1}$ and $l + i_{z-2}$, cannot cancel down with an m because below i_z all m's are opposite in parity to all l's. Only one can be left-over so one must cancel up, giving that $k - j = k + i_t - (j + i_t) < m + i_z - (l + i_{z-2}) = m - l + 2j = 7$. This translates to $z \leq 4$, and by the parity of t, z must be even. If $z = 2$ then $f = 1 + x^2 + x^5 + x^6 + x^9$, $h = 1 + x^2 + x^4 + x^5 + x^8$ and $g = fh = 1 + z^{10} + x^{17}$. This is polynomial exception 18.

If $z = 4$ then $f = 1 + x^2 + x^9 + x^{10} + x^{13}$, $h = 1 + x^2 + x^4 + x^6 + x^8 + x^9 + x^{12}$ and $g = fh = 1 + x^{16} + x^{25}$. This is polynomial exception 25.

8.3 Case 1.2/4:

If $z + 2 = \Omega + 1 \leq y$ then all shifts are $j = m - l$. If $y = z + 1$ then $m - l < i_{z+1} - i_z = i_y - i_{y-1} = j < i_{y+1} - i_y = i_{z+2} - i_{z+1} = m - l$, which is ridiculous. Hence $y \leq z$. Now $m = (m-k)+(k-j)+j = (i_t - i_z) + (i_y - i_0) + j \leq m - i_z + i_y + j$. Thus $i_z \leq i_y + j < i_y + (i_{y+1} - i_y) = i_{y+1}$. Therefore $z < y + 1$ and we conclude $y = z$. Furthermore, $m + i_0 = i_t - i_z + i_y + j = j + i_t$.

Suppose $t \geq z + 3$. Then since $i_t - i_{t-1} = m - l$, $j + i_{t-1} = l + i_0$ and $k + i_{t-1} = l + i_z$. What happens to $k + i_1$? It must cancel up since the m,l in row i_0 are taken. To prevent $0 + i_{y+1}$ from being left-over, we must have $k + i_1 = 0 + i_{y+1}$. Hence $i_{y+1} - i_y = (k + j) - (k - j) = 2j$. Now consider $m + i_{z-1}$. If it cancels with a k, then we deduce $m + i_{z-1} = k + i_{t-2}$ or else $k + i_{t-2}$ is stranded to the left of anything with which to cancel. Hence $j = i_z - i_{z-1} + (m - k) - (m - k) = i_z - i_{z-1} + (i_t - i_z) - (i_{t-2} - i_{z-1}) = i_t - i_{t-2} = 2(m - l)$. Now $0 + i_{z+2} \leq 0 + i_{t-1} < j + i_{t-1} = l + i_0$ so $0 + i_{z+2}$ cannot cancel down with an l or m. Also, $0 + i_{z+2} > 0 + i_{z+1} = k + i_1$ and $k + i_2 \geq k + i_1 + j = 0 + i_{z+1} + j > 0 + i_{z+1} + (m - l) = 0 + i_{z+2}$ and so $0 + i_{z+2}$ cannot cancel with a k or j. This is impossible and so we deduce that $m + i_{z-1}$ cancels with a j. This forces $z = 1$ since $m + i_0 = j + i_t$. In particular, $k = j + i_1 = 2j$. Now $j + i_2 = 0 + i_3$ (m,l,k in rows i_0, i_1 are accounted for) and so $m - l = i_{z+2} - i_{z+1} = i_3 - i_2 = j$. If $t \neq z + 3$ then $t \geq z + 5$ since z is odd. In this case $0 + i_{t-1} = j + i_{t-2} = k + i_{t-3}$ and there cannot be an m or l to complete a quadruple cancellation in this column. Therefore $t = z + 3 = 4$. We get polynomial exception 8.

Suppose $t = z+2$. Now consider $m+i_{t-3}$. Since t is even, $t-3$ is not zero and hence $m+i_{t-3}$ cannot cancel with a j. Since no m cancels a 0 in Case 1.2/4 and since the only l or k unaccounted for in rows i_t, i_{t-1}, or i_{t-2} is $k+i_{t-2}$, we must have $m - k = i_{t-2} - i_{t-3} = i_z - i_{z-1} = j = i_1$. Therefore $k + i_1 = m + i_0 = j + i_t$ but there is no room to complete a quadruple cancellation.

Finally, suppose $t = z + 1$. The term $l + i_{t-1}$ must cancel and there are only two possibilities: $m + i_{t-2}$ and $0 + i_t$. In the former case, $m - l = i_{t-1} - i_{t-2} = i_z - i_{z-1} = j$. So $l + i_1 = m + i_0$. Every m and l will cancel in consecutive rows to form a "staircase", as will the j's and 0's. We require some k below $j + i_t$ to complete the quadruple cancellation with $m + i_0$, $l + i_1$ and $j + i_t$. But now we have accounted for this k, along with $k + i_t$ and $k + i_0$, so there can only be three rows, i.e. $t = 2$. But now there are not enough rows for the quadruple cancellation. This contradiction leaves only the case where $l + i_{t-1} = 0 + i_t$. Thus $m - k = i_t - i_{t-1} = l$, and so $m - l = k$. If $k + i_{t-1} = m + i_{t-2}$, then $m - k = i_{t-1} - i_{t-2} = i_z - i_{z-1} = j$. So $k = m - j = i_t - i_0$. i.e. $0 + i_t = k + i_0 = j + i_z$, a contradiction. Now since $m + i_{t-2}$ doesn't cancel down with $k + i_{t-1}$, it will be stranded unless $t = 2$ and $m + i_{t-2} = j + i_t$. We conclude $k + i_1 = l + i_0$ and $l - k = j = k - j$, $m - l = 2j$. So $f(x) = x^5 + x^3 + x^2 + x + 1$, $h(x) = x^4 + x + 1$ which is polynomial exception 3.

8.4 1.2/5

We note that m on row i_t and l on row i_{z+1} are only two left-over terms on the left of $k + i_t$. If $y - 1 \geq z + 2$, i.e., $y \geq z + 3$, then $j = m - l$. On the other hand, $i_y - i_{y-1} = m - l < j$, a contradiction. Hence $y \leq z + 2$. Note $k + i_t = m + i_z$. Hence $m = k + i_t - i_z = i_y + i_t - i_z \leq m + i_y - i_z$. Hence $y \geq z$. Therefore $z \leq y \leq z + 2$.

8.4.1 Assume $y = z$.

¿From $i_y - i_{y-1} < j$, we know that $(y - 1)j < k < yj$. Note $k + i_t = m + i_z$ and $0 + i_z = k + i_0$, we obtain that $0 + i_t = m + i_0$.

<u>**Case I:** $t = y + 1$.</u>

In this case, $0+i_{y+1}=m+i_0$ and $j+i_z=k+i_1$ follow that $j+i_{y-1}=l+i_0$. Then $l=yj$ and $m-k>m-l=m-yj$.

Case IA: $m+i_{y-1}=k+i_y$**.** In this case, $l+i_y=j+i_{y+1}$.

First we have $m=2k-(y-1)j<2yj-(y-1)j=(y+1)j$. Next $l-j=i_{y+1}-i_y=m-k<m-(y-1)j$ implies that $m>l+(y-2)j$. Hence $l<3j$. Because $l=yj$, we have $y<3$. Note $y-1>0$, we have $y=2$. In this case, $t=3$, a contradiction.

Case IB: $m+i_{y-1}=l+i_y$**.** Hence $m-l=i_y-i_{y-1}<j$. Because l on row i_0 cancels up with j on row i_{y-1}, m and k on row i_1 cancels up with j on row i_{y+1} and i_y respectively. Hence l on row i_1 cancels up with a k. If this k is on row i_y, then $l-k=k-j$. Since $l-k<j$, we have $k-j=i_z-i_1<j$. Hence $z=2$ and $t=3$, a contradiction. If this k is on other rows, then $l-k$ is a multiple of j. Since l is a multiple of j, then k must be a multiple of j, a contradiction.

Case IC: $m+i_{y-1}=j+i_{y+1}$**.** In this case, $m-j=i_{y+1}-i_{y-1}=m-(y-1)j$ follows that $y=2$, a contradiction.

Case II: $t\geq y+2$**.**

If $t=y+2$, then $0+i_{t-1}=l+i_0$ implies that $j+i_{y-1}$ is a left-over.

Let $t\geq y+3$. So $0+i_{y+1}=j+i_{y-1}$, $m+i_0=0+i_t$, $l+i_0=0+i_{t-1}$, $j+i_t=m+i_1$, $l+i_y=k+i_{t-1}$. Moreover, $m-l<i_{y+1}-i_y<i_{y+1}-i_{y-1}=j$.

Case IIA: $m+i_{y-1}$ **cancels up with a** j**.** In this case, $y=2$ because $m+i_1=j+i_t$.

Case IIA1: suppose $i_y-i_{y-1}=m-l$**.** We have $2(k-j)=2(m-l)<m-l+i_{y+1}-i_y=j$. Hence $k+i_y$ is to the right of $j+i_{y+1}$ and thus $k+i_y$ is a left-over, a contradiction.

Case IIA2: suppose $i_y-i_{y-1}<m-l$**.** That is, $k-j<m-l$. If $t\geq z+4$, then $0+i_{z+2}$ is to the right of $j+i_{z+1}$ (because $m-l<j$) and thus $0+i_{z+2}=k+i_z$. Then $m-l=i_{z+2}-i_{z+1}=2(k-j)$, a contradiction. Hence $t=z+3$ and thus $t=5$, a contradiction.

Case IIA3: suppose $i_y-i_{y-1}>m-l$**.** So we have $m-l<k-j<j$. If $t\geq z+4$, then $0+i_{z+2}$ is to the right of $j+i_z=k+i_{z-1}$ and it is a left-over, a contradiction. If $t=z+3$, then $t=5$, another contradiction.

Case IIB: $m+i_{y-1}$ **cancels up with a** k **or** l**.** So $i_y-i_{y-1}\geq m-l$. We have $i_{y+2}-i_y=i_{y+2}-i_{y+1}+i_{y+1}-i_y=m-l+i_{y+1}-i_y\leq i_y-i_{y-1}+i_{y+1}-i_y\leq j$. Hence $0+i_{z+2}$ is to the right or above of $j+i_z=k+i_1$. If $t\geq z+4$, then $0+i_{z+2}$ is a left-over, a contradiction. If $t=z+3$, then $t=5$, another contradiction.

8.4.2 Assume $y = z + 1$.

We have $i_{z+2} - i_{z+1} = m - l$, $m - l < i_{z+1} - i_z < j$, and $i_z - i_{z-1} = j$. From case 5, we have $j + i_y = k + i_1$, i.e., j on row i_{z+1} cancels with k on row i_1. If $t = z + 1$, then j on row i_z must cancel with l on row i_0. Because $m - k < j$, m on row i_0 is to the right of k on row i_1. This m is left-over, a contradiction.

Let $t > z + 1$. Note that the 0 on row i_{z+2} is to the right of j on row i_{z+1}. Because $t > z + 1$, we have $l - k > m - l$. Hence 0 on row i_{z+2} is to the right of bottom l. So 0 on the row i_{z+2} must cancel down with j on row i_z. That is $j = (m - l) + (i_{z+1} - i_z)$. We observe that in this case we also have $l - k \geq (i_{z+1} - i_z)$.

Case I: $l - k < j$.

To cancel the bottom l, we need a 0 on row i_{z+3}. Therefore $t \geq z + 3$ and $l - k = 2(m - l)$ (from the distance of 0's on row i_{z+3} and i_{z+1}). But $l - k > 2(m - l)$ when $t \geq z + 3$ (from the left-top corner – case 1.2), a contradiction.

Case II: $l - k \geq j$.

That is, the bottom l is to the left of k on row i_1. In this case, $t = z + 2$. Otherwise, 0 on row i_{z+3} is to the right of j on row i_{z+1} because $2(m - l) < (m-l) + (i_{z+1} - i_z) = j$ and this 0 must be a left-over, a contradiction. Consider $t = z + 2$. Hence $m - k = j = (m - l) + (i_{z+1} - i_z)$. This contradicts to $l - k \geq j$.

8.4.3 Assume $y = z + 2$.

We note that $j = i_{y-1} - i_{y-2} = i_{z+1} - i_z > m - l$.

Case I: $t = z + 2$.

Then $j + i_{z+1} = l + i_0$. Note that k on row i_1 cancels up with j on row i_{z+2}, l on row i_1 must cancel up with a k. It can not cancel down with m on row i_0 because in that case we have a contradiction $m - k = l - k + j > l - k + m - l = m - k$. Then $l - k = i_\alpha - i_1$ must be a multiple of j. And l is a multiple of j, we conclude k is a multiple of j, a contradiction.

Case II: $t > z + 2$.

We have $l - k > j$. Hence the bottom l is to the left of k on row i_1. Then $0 + i_{z+3} = j + i_{z+1}$. Hence $j = 2(m - l)$. If $t > z + 3$, then $0 + i_{z+4} = j + i_{z+2} = k + i_1$, a contradiction. If $t = z + 3$, then $l - k = (m - l) + j$. Note that $k - j = (m - l) + zj$ and $m - k = j + 2(m - l) = 2j$, we have $l = (z + 3)j$. That is, the bottom l cancels with the top j. Hence $l - k = 2j - (m - l)$. Consider l on row i_1, it cancels up with a k or it it a left-over because it can not cancel down with a m nor up with a j (all j's are accounted). If $l + i_1$ is a left-over, $z + 1 = 1$ and $t = 3$, a contradiction. If $l + i_1$ cancels with a k, k must be on row i_{z+2}. Otherwise, k is a multiple of j. If $l + i_1 = k + i_{z+2}$, then $l - k = (z + 1)j + m - l - j = zj + m - l$. Hence $z = 1$. This is the polynomial exception 20.

8.5 Case 1.3/4:

If $z \geq y+1$ then $m \geq i_t - i_z + i_z - i_{y+1} + i_{y+1} - i_y + i_y - i_0 > m$ so we have $z \leq y$. If $y \geq z+3$ then $2j = i_y - i_{y-2} \geq m - l$ but $2j = i_{z+2} - i_z < m - l$ so we have $y \leq z+2$. We note that $t > \Omega > z$ and further, $t \geq z+3$ otherwise $l + i_{z+2}$ to be another left-over term to the left of $k + i_{z+2}$.

8.5.1 Assume $y = z$.

<u>**Case I:** $\Omega < t-1$.</u>

Then $l + i_z = k + i_{t-1}$, $l + i_{z+2} = m + i_{z-1}$. Note that $l + i_0 = j + i_{t-1}$ and $m + i_0 = j + i_t$. It follows that $0 + i_{z+1} = k + i_1$ and thus $i_{z+1} - i_z = 2j$. If $z \geq 4$, then $l + i_{z+1} = m + i_{z-2}$ and $m + i_{z-3}$ must be a left-over because $i_{z+1} - i_z = 2j$. If $z = 3$, then $m - l = i_{z+1} - i_1 = k = 4j$. But $0 + i_t = k + i_{t-1} = l + i_z$, a contradiction. If $z = 2$, then $l + i_{z+2} = m + i_{z-1}$, $j + i_t = m + i_0$, and $l + i_{z+1} = 0 + i_t$. Hence $m - l = i_z - i_{z-2} + j + i_{z+1} - i_z = 5j$. Thus it follows that $i_x - i_{x-1}$ is either $3j$ or $2j$ for all $z+1 \leq x \leq \Omega+1$. If $\Omega < t-2$, then $l + i_1$ must be a left-over because $m - l > j$, $l + i_2 = k + i_{t-1}$ and $l + i_0 = j + i_{t-1}$. If $\Omega = t-2$, then $l + i_1 = k + i_\Omega$ and thus $i_{t-1} - i_{t-2} = j$, a contradiction. If $z = 1$, then one of $l + i_{z+1}$ and $l + i_{z+2}$ must be left-over.

<u>**Case II:** $\Omega = t-1$.</u> We have $l + i_z = k + i_{t-2}$, $l + i_0 = j + i_{t-2}$ and $m + i_0 = j + i_t$.

Case IIA: $z = \Omega - 2$. So $t - 2 = z + 1$, $0 + i_{z+1} = k + i_1$ and $l - k = 2j$. Hence $i_{z+1} - i_z = 2j$. Note that $l + i_{z+2} = m + i_{z-1}$. We have $i_t - i_{t-1} = i_{z+1} - i_z = 3j$.

Case IIA1: $k - j \geq m - l$. In this case, $l + i_{z+2} = m + i_{z-1}$. It follows that $i_t - i_{t-1} = i_{z+1} - i_{z-1} = 3j$. Consider $l + i_{z+1}$.

Case IIA1a: $l + i_{z+1} = k + i_{t-1}$. Since $l - k = i_{z+2} - i_{z+1} = i_{z+1} - i_z = 2j$, we have $m - l = i_t - i_{t-2} = i_{z+3} - i_{z+1} = 5j$. Hence $z = 2$ or otherwise, $m + i_{z-2}$ is a left-over. This implies that $k - j = 2j < m - l$, a contradiction.

Case IIA1b: $l + i_{z+1}$ **is to the left of** $k + i_{t-1}$. In this case, $z \geq 3$, $l + i_{z+1} = m + i_{z-2}$ and $k + i_{t-1} = m + i_{z-3}$. Hence $m - l = i_{z+1} - i_{z-2} = 2j + j + j = 4j$. Therefore $i_{t-1} - i_{t-2} = j$. Hence $z = 4$ and $k - j = m - l = 4j$. In this case, $j + i_{t-1} = k + i_{z-1} = l + i_1$ gives a left-over, a contradiction.

Case IIA1c: $l + i_{z+1}$ **is to the right of** $k + i_{t-1}$. In this case, $l + i_{z+1} = m + i_{z-3}$ and $k + i_{t-1} = m + i_{z-2}$. So $l - k = j$, which contradict to $l - k = i_{z+1} - i_z = 2j$.

Case IIA2: $k - j < m - l$. Note that $j + i_t = m + i_0$, we have $l + i_{z+2} = m + i_{z-1}$. Consider $m + i_{z-2}$.

Case IIA2a: $m + i_{z-2}$ **cancels up with** $l + i_{z+1}$. Hence $m - l = i_{z+1} - i_{z-2} = 4j$. So $i_{z+2} - i_{z+1} = i_{t-1} - i_{t-2} = j$. Since

$k - j < m - l$, $k - j$ is either $2j$ or $3j$ because $k - j \neq j$. If $k - j = 3j$, then $k + i_{t-1}$ is a left-over. If $k - j = 2j$ (i.e., $z = 2$), then we must have $j + i_t = k + i_{t-1} = l + i_{z+1} = m + i_0$. Then $0 + i_{t-1}$ is a left-over.

Case IIA2b: $m + i_{z-2}$ cancels up with $k + i_{t-1}$. Hence $m - k = i_{t-1} - i_{z-2} = i_t - i_z$ and it follows that $i_t - i_{t-1} = 2j$, contradicts to $i_t - i_{t-1} = 3j$.

Case IIA2c: $m + i_{z-2}$ cancels up with $j + i_t$. We have that $z = 2$ so $t = 5$ is odd which is a contradiction.

Case IIB: $z < \Omega - 2$. we consider two cases depending on the relationship between $k - j$ and $m - l$.

Case IIB1: $k - j \geq m - l$. Consider $l + i_{z+2}$.

Case IIB1a: $l + i_{z+2} = k + i_{t-1}$. In this case, $l + i_{z+1} = m + i_{z-1}$. Hence $m - l = 3j$. Since $i_z - i_{z-1} = j$, $m + i_{z-2}$ must be a left-over if $z > 2$. If $z = 2$, then $k - j = 2j < m - l$, a contradiction.

Case IIB1b: $l + i_{z+2} = m + i_{z-1}$. We have $0 + i_{z+1} = k + i_1$ which implies that $i_{z+1} - i_z = 2j$. We now consider 3 cases for $l + i_{z+1}$.

Case IIB1bi: $l + i_{z+1} = k + i_{t-1}$. This case is impossible because $m - l = i_{z+2} - i_{z-1} > i_{z+1} - i_z = 2j$.

Case IIB1bii: $l + i_{z+1}$ is to the left of $k + i_{t-1}$. In this case, $l + i_{z+1} = m + i_{z-1}$ and $k + i_{t-1} = m + i_{z-2}$. Thus $m - l = i_{z+1} - i_{z-1} = 4j$ and $z = 4$. That is, $k - j = m - l = 4j$. Moreover, $i_{z+2} - i_{z+1} = 4j - 3j = j$. Hence $0 + i_{z+2} = j + i_{z+1} = k + i_2$ gives a left-over.

Case IIB1biii: $l + i_{z+1}$ is to the right of $k + i_{t-1}$. We have $l + i_{z+1} = m + i_{z-2}$ and $k + i_{t-1} = m + i_{z-1}$. Hence $m - l = i_{z+1} - i_{z-3} = 5j$. Note that $k - j \geq m - l$, $m + i_{z-4}$ must be a left-over, a contradiction.

Case IIB2: $k - j < m - l$. Since $j + i_t = m + i_0$, z is at most 4.

Case IIB2a: $l + i_{z+2} = j + i_t$. In this case, we must have $z = 1$ and $j + i_t = k + i_{t-1} = l + i_{z+2} = m + i_0$. Hence $i_t - i_{t-1} = j$. Now $0 + i_t = j + i_{t-1} = l + i_{z+1}$ gives a left-over, a contradiction.

Case IIB2b: $l + i_{z+2} = k + i_{t-1}$ and $l + i_{z+2} \neq j + i_t$. Let us consider the position of $j + i_t = m + i_0$.

Case IIB2bi: $j + i_t = m + i_0$ is to the left of $l + i_{z+2} = k + i_{t-1}$. Again, $z = 1$ follows that $i_{z+2} - i_{z+1} = j$ and $i_{z+1} - i_z = 2j$. Hence $m - l > 4j$. If $m - l \geq 5j$, then $0 + i_t$ is to the left or above $k + i_{t-1} = l + i_{z+2}$ and thus a left-over. If $m - l < 5j$, then $0 + i_t$ is to the right of $k + i_{t-1} = l + i_{z+2}$. But from $k - j = j$ it follows that $0 + i_t$ is left-over.

Case IIB2bii: $j + i_t = m + i_0$ is to the right of $l + i_{z+2} = k + i_{t-1}$ and to the left of $l + i_{z+1}$. In this case, $z = 1$. Note that $i_{z+1} - i_z = 2j$, $0 + i_t$, $j + i_{t-1}$, $0 + i_{t-1}$, and $l + i_{z+1}$ are to the left of $k + i_{t-2} = l + i_z$. None of these can be left-over so $0 + i_t = j + i_{t-1}$ and $0 + i_{t-1} = l + i_{z+1}$. This implies that $i_t - i_{t-1} = j = i_3 - i_2$. The fact that t must be even now gives that $i_x - i_{x-1} = j$ for all $x \geq 3$. We have $m - l = 2j$ but $m - j = i_t = i_t - i_{t-1} + i_{t-1} - i_{z+1} + i_{z+1} - i_0 = l + 4j$.

Case IIB2biii: $j + i_t = m + i_0$ is to the right of $l + i_{z+1}$. In this case, $l + i_{z+1} = m + i_{z-1}$ and $z = 2$. Hence $m - l = 3j$. Then $k - j = 2j$ and thus $0 + i_t = k + i_{t-2} = l + i_z$. Note $l + i_{z+2}$ is to the left of $l + i_{z+1}$ and $i_z - i_{z-1} = j$, we have $i_t - i_{t-1} < j$. Hence $0 + i_t = k + i_{t-2} = l + i_z$ gives a left-over, a contradiction.

Case IIB2c: $l + i_{z+2} = m + i_{z-1}$. Again, we consider $l + i_{z+1}$.

Case IIB2ci: $l + i_{z+1} = k + i_{t-1}$. If $\Omega = z + 3$, then $l - k = i_{z+3} - i_{z+1} = m - l$ contradicts to $l - k = i_{z+2} - i_z < i_{z+2} - i_{z-1} = m - l$. If $\Omega > z + 3$ and $\Omega - z = \alpha$ is odd, then $l - k = i_{t-1} - i_{z+1} = ((\alpha - 3)/2)(m - l) + i_{z+3} - i_{z+1} = i_{t-2} - i_z = ((\alpha - 3)/2)(m - l) + i_{z+2} - i_z$ but $i_{z+3} - i_{z+1} \geq m - l > i_{z+2} - i_z$.

If $\Omega > z + 3$ and $\Omega - z = \alpha$ is even, then $l - k = i_{t-1} - i_{z+1} = ((\alpha - 2)/2)(m - l) + i_{z+2} - i_{z+1} = i_{t-2} - i_z = ((\alpha - 2)/2)(m - l) + i_{z+1} - i_z$ and it follows that $i_{z+2} - i_{z+1} = i_{z+1} - i_z = 2j$. Hence $m - l = i_{z+2} - i_{z-1} = 5j$ and $i_t - i_{t-1} = 3j$. It then follows that $0 + i_t$ is a left-over.

Case IIB2cii: $l + i_{z+1}$ is to the left of $k + i_{t-1}$. We consider the position of $j + i_t = m + i_0$.

Case IIB2cii1: $j + i_t = m + i_0$ is to the left of $l + i_{z+1}$. In this case $0 + i_t = l + i_{z+1}$ and $k + i_{t-1}$ is a left-over, a contradiction.

Case IIB2cii2: $j + i_t = m + i_0$ is to the right of $l + i_{z+1}$ and to the left of $k + i_{t-1}$. In this case, $l + i_{z+1} = m + i_{z-2}$ and $0 + i_t = k + i_{t-1}$. Hence $m - l = 4j$ and thus $i_{z+2} - i_{z+1} = j$. Moreover, $z = 3$ and $k - j = 3j$. Hence $k = 4j$. But $k = 4j = i_t - i_{t-1} < m - l = 4j$, a contradiction.

Case IIB2cii3: $j + i_t = m + i_0$ is to the right of $k + i_{t-1}$. In this case, $z = 4$, $l + i_{z+1} = m + i_{z-2}$ and $k + i_{t-1} = m + i_{z-3}$. Note $m - l = i_{z+1} - i_{z-2} = 4j$ and $z = 4$, we have $k - j = m - l = 4j$, a contradiction to $k - j < m - l$.

Case IIB2ciii: $l + i_{z+1}$ is to the right of $k + i_{t-1}$. Similar to the above we have

Case IIB2ciii1: $j + i_t = m + i_0$ is to the left of $k + i_{t-1}$. In this case, we must have $z = 2$, $0 + i_t = k + i_{t-1}$, and $j + i_{t-1} = l + i_{z+1}$. Hence $0 + i_{t-1}$ is a left-over.

Case IIB2ciii2: $j + i_t = m + i_0$ is to the left of $l + i_{z+1}$ and to the right of $k + i_{t-1}$. In this case, $z = 3$ and $k + i_{t-1} = m + i_{z-2}$, and $0 + i_t = l + i_{z+1}$. Hence $i_t - i_{t-1} = i_z - i_{z-2} = 2j$. Therefore $j + i_{t-1}$ is to the left of $l + i_z = k + i_{t-2}$ and it is a left-over.

Case IIB2ciii3: $j + i_t = m + i_0$ is to the right of $l + i_{z+1}$. In this case, $z = 4$, $k + i_{t-1} = m + i_{z-2}$ and $l + i_{z+1} = m + i_{z-3}$. Hence $m - l = 5j$. Hence $0 + i_t = k + i_{t-2} = l + i_z$ gives a left-over.

8.5.2 Assume $y = z + 1$.

Case I: $\Omega = z + 1$.

In this case, $i_t = m - 2j$ and $l + i_0 = m + i_0 - (m - l) = i_t + 2j - (m - l) = i_{t-1} + 2j$. Hence $0 + i_{z+2} = k + i_1$. That is, $i_{z+2} - i_{z+1} = 2j$. Therefore $0 + i_t = m + i_{z-1}$. So $z = 1$. In this case, $l + i_{z+1}$ is a left-over.

Case II: $t - 1 > \Omega > z + 1$.

Similarly to the previous case, $l + i_0 = i_{t-1} + 2j$. If $l + i_{z+2} = j + i_t$, then $i_{z+2} - i_0 = i_t - i_{t-1} = m - l$. Hence $z = 1$ and $j + i_t = l + i_{z+2} = m + i_0$, a contradiction. Hence $l + i_{z+2} \neq j + i_t$ and $l + i_{z+2} = m + i_{z-1}$. Because $0 + i_{z+2} = k + i_1$, we have $i_{z+2} - i_{z+1} = 2j$. Hence $m - l = i_{z+2} - i_{z-1} = 4j$. Therefore $j + i_t = m + i_{z-2}$ and $0 + i_t = l + i_{z+1} = m + i_{z-3}$ if $z \geq 3$. This implies that $z = 2$. However, $l + i_2 = k + i_{t-1}$, $l + i_0 = j + i_{t-1}$, and $k - j = 2j$ imply that $\Omega = t - 2$ and $l + i_1 = k + i_\Omega$. But $i_{\Omega+1} - i_\Omega = 2j$, a contradiction to $i_2 - i_1 = j$.

Case III: $\Omega = t - 1$.

We consider two cases:

Case IIA: $z = \Omega - 2$. We know that $t = z + 3$ and $l + i_z = k + i_{z+1}$. If $z = 0$, then we have an even number of rows. Hence $z \geq 1$ and then $k - j \geq 2j$. So $j + i_t \neq l + i_{t-1}$. Otherwise, $k - j$ on row i_t is less than the distance (j) of m's on row i_z and i_{z-1}. Hence we have $l + i_{t-1} (= l + i_{z+2}) = m + i_{z-1}$. We know that $l - k = j$, $i_{t-1} - i_{z+1} > j$ and $i_t - i_{t-1} = 2j$. From this we get that $k + i_{t-1} = m + i_{z-2}$ and $l + i_{z+1} < k + i_{t-1}$. All k's below row $z + 1$ cancel with l's. Thus we have accounted for the cancellation of all k's, all l's except $l + i_{z+1}$ and all 0's and j's except $0 + i_t$, $j + i_t$, $0 + i_{t-1}$ and $j + i_{t-1}$. But $i_t = m - 2j$ so all m's are to the left of all 0's and j's leaving at least four left-over terms.

Case IIIB: $z < \Omega - 2$. Note that $l + i_0$ is to the left of $j + i_{t-2}$. Hence $0 + i_{z+2} = k + i_1$ and $j + i_{z+2} = k + i_2$. So $l - k \geq 3j$. Consider $m + i_{z-1}$. We know that $j + i_t \neq m + i_{z-1}$ because $j + i_t$ is to the right of $m + i_0$. Also $k + i_{t-1} \neq m + i_{z-1}$. Otherwise, $i_{t-1} - i_{t-2} = 3j$ and thus $m - l = 5j$. This contradicts to that all j's and 0's between row i_{t-2} and row i_{z+2} are canceled with k's. Again, we have $l + i_{z+2} = m + i_{z-1}$ and $m - l = 4j$. So $i_{z+3} - i_{z+1} = 2j$ and all the distances between two consecutive rows above are $2j$. Hence $l-k=(2(t-2-z)-1)j$. Also we have $k+i_{t-1}=m+i_{z-2}$. Thus $j+i_t=l+i_{z+1}$. If $z\geq 3$ then $j+i_t=l+i_{z+1}=m+i_{z-3}$ is a contradiction.

If $z=2$ then $0+i_t=k+i_{t-2}=l+i_z$, a contradiction. If $z=1$ then $l+i_{z+1}=0+i_t$. The even parity (because they must cancel in pairs) of remaining terms between $k+i_t$ and $k+i_{t-2}$ and the fact that $0+i_{t-1}<k+i_{t-2}$ give that $j+i_{t-1}<k+i_{t-2}$ also. Four terms remain but $k+i_{t-1}<j+i_t<m+i_0$ so at least two are left-over.

Finally if $z=0$ then $i_t-i_{t-1}=2j=i_{t-1}-i_{t-2}$. We obtain the contradiction $0+i_{t-1}=k+i_{t-2}=l+i_0$.

8.5.3 Assume $y=z+2$.

We note that $t\geq z+3$ and $i_t=m-3j$. What does $0+i_{z+3}$ cancel with?

Case I: $0+i_{z+3}=m+i_\alpha$.

Lemma 7.1 gives that $t=z+3$ and $\alpha=0$. In this case $l+i_0$ must cancel up with a k. Since $k+i_1$ is not left over we must have $l+i_0=k+i_1$. But now $i_{z+3}-i_{z+2}=m-k+j>m-l$ which cannot happen in case 1.3.

Case II: $0+i_{z+3}=l+i_\alpha$.

Lemma 7.3 gives us that $t\leq z+5$.

Case IIA: $t=z+5$. Lemma 7.3 gives us that $\alpha=0$, $\Omega=z+4$ and $i_t=m$ which contradicts $i_t=m-3j$.

Case IIB: $t=z+4$. If $\Omega\leq z+2$, then $\alpha=0$ and $i_{z+4}=m$. Now we get the contradiction that $m-k=i_{z+4}-i_z=m-l+l-k+j+2j=m-k+3j$. So we assume that $\Omega=z+3$.

Now we have that $m-k=i_{z+4}-i_z=m-l+2j$. Since $k+i_1<l+i_0\leq l+i_\alpha=0+i_{z+3}$ we have the contradiction that $k+i_1$ must be left-over.

Case IIC: $t=z+3$. If $\Omega=z+1$ then we have that $m-k=i_{z+3}-i_z=m-l+2j$. This gives $k+i_1<l+i_0\leq l+i_\alpha=0+i_{z+3}$ we have the contradiction that $k+i_1$ must be left-over.

So we assume that $\Omega=z+2$. If $z\geq 1$ then $m+i_{z-1}$ must cancel up with something. It can only be $j=i_{z+3}$ or $l+i_{z+2}$. The former implies that $k=2j$ and thus $z=-1$ and the later implies that $m-l=3j$. This gives $0+i_{z+3}=k+i_1=l+i_0$ with nothing else in this column but none of these are left-over.

Thus $z=0$, but then $t=3$ violates parity.

Case III: $0+i_{z+3}=k+i_\alpha$.

If $\alpha\geq 2$, then we ask what does $k+i_1$ cancel with. There is nothing available above it so it must cancel down with $m=i_0$ or $l+i_0$. The former implies that $0+i_{z+3}>m+i_0$ and the latter gives that $0+i_{z+3}$ also cancels with an l. This was covered in Case II.

So $i + i_{z+3} = k + i_1$. We now break into two cases depending on the value of Ω.

Case IIIA: $\Omega = z + 1$. Here $m - l = i_{z+3} - i_{z+2} = 2j$ and $m - k = 2j + (t - z - 2)(m - l) = 2(t - z - 1)j$. Now we get the contradiction that $k + i_t = l + i_{z+2} = m + i_z$ but none of these may be left-over.

Case IIIB: $\Omega > z + 1$. Here $m - l = i_{z+3} - i_{z+1} = 3j$. Also $i_t = i_t - i_z + i_z - i_{z+2} + i_{z+2} - i_0 = m - 3j = l$. We also note that all shifts above $z + 3$ are j, $2j$ or $3j$ and thus the GCD condition gives that $j = 1$. What does $l + i_2$ cancel with? Not with an m since $l + i_2 = l + 2j < m + i_0$. Not j or 0 since $j + i_t = l + i_1 < l + i_2$ so it must cancel with a $k + i_\beta$ since it is not left-over. If $i_\beta - i_{\beta-1} = 1$ then $j + i_t = k + i_{\beta-1} = l + i_1$ but none of these can be left-over. This gives that $\beta \geq z + 3$.

If $i_\beta - i_{\beta-1} = 2$ then $0 + i_t = k + i_{\beta-1} = l + i_0$ but none of these can be left-over so we must have that $i_t - i_{t-1} = j$ which implies that $\Omega = t - 1$ and t and z are the same parity. Now if $\beta \geq z + 4$ then $0 + i_{t-1} = k + i_{\beta-2}$ but $j + i_{t-2} > k + i_{\beta-3}$ but it cannot be left-over and thus we have that $\beta = z + 3$. In this case $l = 2k - 1$, $m = 2k + 2$.

Now if $t \geq z + 4$ then $0 + i_{z+4} = j + i_{z+3} = k + i_2$ but none of these are left-over so $0 + i_{z+4} = l + i_0$ This gives $f = 1 + x + x^3 + x^5 + x^8$, $h = 1 + x + x^2 + x^4 + x^5$ and $g = fh = 1 + x^{12} + x^{13}$ Which is polynomial exception 14. Lastly, if $t = z + 3$, then $l - k = 1$ implying $k = 2$ and $z = -1$.

If $i_\beta - i_{\beta-1} = 3$ then $\beta \geq \Omega + 2$. Now $i_t - i_{t-1} = 3$ and $j + i_{t-1} < k + i_{\beta-1} < 0 + i_t$ which contradicts the fact that $k + i_{\beta-1}$ cannot be left-over.

8.6 1.3/5

If $y \leq z - 1$, then $m \geq i_t = i_t - i_z + i_z - i_{z-1} + i_{z-1} - i_0 \geq m - k + i_z - i_{z-1} + k > m - k + k = m$, a contradiction. Hence $y \geq z$.

Assume that $y \geq z + 3$. We assume that $i_y - i_{y-1} = j - \epsilon < j$ for some small positive number ϵ by case 5. If $\Omega > z + 2$, then $i_{z+2} - i_z = 2j < m - l$. But $i_{z+3} - i_{z+1} = m - l$ is either $2j$ or $2j - \epsilon$, a contradiction. If $\Omega = z + 1$, then $i_{z+2} - i_z = 2j < m - l$. But $i_{z+3} - i_{z+2} = m - l$ is either j or $j - \epsilon$, a contradiction. Hence $y \leq z + 2$.

Therefore $z \leq y \leq z + 2$.

8.6.1 Assume $y = z + 2$.

Using $k + i_t = m + i_z$, $0 + i_{z+2} = k + i_0$, $i_{z+2} - i_z > j$, we conclude that $m + i_0 > j + i_t$. Hence $m + i_0$ is to the left of $j + i_t$.

<u>**Case I:** $\Omega < t - 1$.</u>

Since $\Omega < t - 1$, we have $l + i_z = k + i_{t-1}$. If $z = 0$, then we must have $l + i_{z+2} = j + i_t$ and $l + i_{z+1} = 0 + i_t$. So $i_{z+2} - i_{z+1} = j$, a contradiction. If $z = 1$, then $l + i_{z+2} = m + i_{z-1}$ and $l + i_{z+1} = j + i_t$. Therefore $0 + i_t = l + i_z = k + i_{t-1}$

gives another left-over, a contradiction. If $z \geq 2$, then $l + i_{z+2} = m + i_{z-1}$ and $l + i_{z+1} = m + i_{z-2}$ by using the fact that $m + i_0$ is to the left of $j + i_t$. Hence $m - l = i_{z+1} - i_{z-2} = 3j$ contradicts to $m - l = i_{z+2} - i_{z-1} < 3j$.

Case II, $\Omega = t - 1$ and $\Omega > z + 2$.

Here $l - k = i_{t-2} - i_z \geq i_{z+2} - i_z > j$ implies that $j + i_{z+1} = 0 + i_{z+3}$. Hence $m - l = i_{z+3} - i_{z+1} = j$.

Assume that $z = 0$. Using $m - l = j$ and $l - k = i_{t-2} - i_z > i_{t-2} - i_{z+2} + j = i_t - i_{z+2} > i_{t-1} - i_{z+2}$, we obtain that $l + i_{z+2} > k + i_{t-1}$ and thus $l + i_{z+2} = j + i_t$. Moreover, $l + i_{z+1} = k + i_{t-1}$. Using $i_{t-2} - i_z = l - k = i_{t-1} - i_{z+1}$ and $i_{z+1} - i_z = j$, we have $i_{t-1} - i_{t-2} = j$, contradicts to $i_t - i_{t-2} = m - l = j$. Hence $z \geq 1$. Then $m + i_{z-1} = l + i_z = k + i_{t-2}$. Using $j = m - l = i_t - i_{t-2}$ and $k - j > j$, we conclude that $k + i_{t-2}$ can not cancel up with any one of $0 + i_t$, $j + i_{t-1}$ and $0 + i_{t-1}$. Hence $m + i_{z-1} = l + i_z = k + i_{t-2}$ gives a left over, a contradiction.

Case III: $\Omega = t - 1$ and $\Omega = z + 2$.

In this case, we have $k + i_{z+3} = m + i_z$ and $k + i_{z+1} = l + i_z$. So $l - k = i_{z+1} - i_z = j$. This implies that $j + i_{z+2} = k + i_1 = l + i_0$. Hence $0 + i_{z+3} = j + i_{z+2} = k + i_1 = l + i_0$. Moreover, $z \geq 1$ and $l + i_{z+1} = m + i_{z-1}$ imply that $2j < m - l = i_{z+1} - i_{z-1} < 3j$. So $l + i_{z+1} > m + i_{z-2}$. Since $i_{z+2} - i_{z+1} < j = l - k$, we have $l + i_{z+1} > k + i_{t-1}$. This implies that $l + i_{z+1}$ must be a left-over if $z \geq 2$. If $z = 1$, then $l + i_{z+1} = j + i_t$. But then $k + i_{t-1}$ is a left-over because $k + i_{t-1} > k + i_{t-2} = l + i_z$.

8.6.2 Assume $y = z + 1$.

In this case, we have $j + i_t > m + i_0 > 0 + i_t$ because $i_{z+1} - i_z < j$, $k + i_t = m + i_z$, and $0 + i_{z+1} = k + i_0$. That is, $j + i_t$ is to the left of $m + i_0$ and $m + i_0$ is to the left of $0 + i_t$. This also implies that $z \geq 1$.

Case I: $\Omega < t - 1$.

Since $i_t - i_{t-1} = m - l$ and $k + i_t = m + i_z$, we have $l + i_z = k + i_{t-1}$. In this case, $t \geq z + 3$. Using $l - k = i_{t-1} - i_z \geq i_{z+2} - i_z$ and $0 + i_{z+1} = k + i_0$, we conclude that $l + i_0 > 0 + i_{z+2}$. Since $j + i_{z+1} = k + i_1$, we must have $0 + i_{z+2} = j + i_z$ to cancel $j + i_z$. That is, $i_{z+2} - i_z = j$.

Case IA: $m - l \geq j$. In this case, we note that $l + i_{z+2}$ cannot cancel up with $0 + i_t$, nor cancel down with $m + i_p$ such that $p < z - 1$. Indeed, in both cases, $j + i_t$ has to be canceled down with $m + i_{z-1}$. Then $k - j = (m + i_z) - (m + i_{z-1}) = j$, a contradiction. Hence we have either $l + i_{z+2} = j + i_t$ or $l + i_{z+2} = m + i_{z-1}$.

In either case, $0 + i_{z+2} = j + i_z$ because $l - k > m - l \geq j$. If $l + i_{z+2} = j + i_t$, then $l + i_{z+1} = m + i_{z-1}$. Otherwise, $m + i_{z-1}$ can only cancel up with $0 + i_t$, a contradiction. Since $0 + i_{z+2} = j + i_z$, we obtain $i_{z+2} - i_z = i_t - i_{t-1} + i_{t-1} - i_z - (i_t - i_{z+2}) = (m - l) + (l - k) - (l - j) = m - l - k + j = j$. Hence $m - l = k$ and thus $z = 1$. Then $0 + i_t = k + i_{t-1} = l + i_1$, a contradiction. If $l + i_{z+2} = m + i_{z-1}$, then $m - l = 2j$. Here $l + i_{z+1}$ cannot cancel down with an $m + i_p$ with $p < z - 1$, for otherwise, $m - l = i_{z+1} - i_p > 2j$, a contradiction. Also $l + i_{z+1}$ can not cancel up with $0 + i_t$, for otherwise, $j + i_t$ must be cancel down with some $m + i_q$ and thus $k - j = i_z - i_q$ is a multiple of j, a contradiction. So we have $l + i_{z+1} = j + i_t$. Hence $z = 1$, otherwise, $m + i_{z-2}$ is right below $l + i_z = k + i_{t-1}$, a left-over. Hence $j + i_t = l + i_{z+1} < l + i_{z+2} = m + i_{z-1} = m + i_0$, which contradicts to $m + i_0 > j + i_t$.

Case IB: $m - l < j$. In this case, $l + i_{z+2} = j + i_t$ and $l + i_{z+1} = 0 + i_t$ imply that $m - l > j$, a contradiction.

Case II, $\Omega = t - 1$ and $\Omega > z + 2$.

In this case, $l + i_z = k + i_{t-2}$. Using $l - k = i_{t-2} - i_z \geq i_{z+2} - i_z$ and $0 + i_{z+1} = k + i_0$, we conclude that $l + i_0 > 0 + i_{z+2}$. Moreover, since $j + i_{z+1} = k + i_1$, we must have $0 + i_{z+2} = j + i_z$ to cancel $j + i_z$. That is, $i_{z+2} - i_z = j$.

Case IIA: $m - l \geq j$. We consider seven cases for $l + i_{z+2}$.

Case IIA1: $l + i_{z+2} = m + i_{z-1}$. In this case $m - l = 2j$. We claim that $z = 1$. Otherwise, suppose $z > 1$, then $m + i_{z-2}$ is right below $l + i_z = k + i_{t-2}$ and $j + i_{t-1}$ must be above $l + i_z = k + i_{t-2}$. Indeed, $k + i_{t-2} \neq j + i_t$ because $i_t - i_{t-2} = m - l = 2j \neq k - j$ and $k + i_{t-2} \neq 0 + i_t$ because $i_t - i_{t-2} = m - l = 2j < k$. Moreover, since $k > m - l$, one of $j + i_t$, $k + i_{t-1}$ and $l + i_{z+1}$ must be a leftover, a contradiction. Therefore $z = 1$. So $j + i_t = k + i_{t-1}$ must be to the left of $m + i_{z-1} = l + i_{z+2}$. Using $z = 1$ again, we have $k - j < j$ and thus $j + i_{t-1}$ is to the left of $0 + i_t$. This implies that $j + i_{t-1}$ cancels down with $l + i_{z+1}$. But $k < m - l$ implies that $0 + i_t$ is a left-over because $0 + i_t$ is to the left of $k + i_{t-2} = l + i_z$, a contradiction.

Case IIA2: $l + i_{z+2} = k + i_{t-1}$. In this case, $i_{t-1} - i_{t-2} = i_{z+2} - i_z = j$. Note that $m + i_{z-1} < l + i_{z+2}$, for otherwise, $m + i_{z-1}$ must be canceled up with $j + i_t$. This implies that $k - j = j$, a contradiction. Therefore $j < m - l < i_{z+2} - i_{z-1} = 2j$. This also implies that $i_t - i_{t-1} < j$ because $i_t - i_{t-2} = m - l < 2j$ and $i_{t-1} - i_{t-2} = j$.

Case IIA2a: $m + i_{z-1} \neq l + i_{z+1}$. Again, we know that $j + i_t \neq m + i_{z-1}$, for otherwise, $k - j = i_z - i_{z-1} = j$, a contradiction. Hence we have $j + i_t = l + i_{z+1}$. Since $i_t - i_{t-1} < j$, we must have $j + i_{t-1} = m + i_{z-1}$. Therefore $k - j < i_{z+2} - i_z = j$, which implies that $z = 1$. Since t must be even and $z = 1$, we should have $i_{z+3} - i_{z+2} < j$ and $i_{z+2} - i_{z+1} = j$, this contradicts to that $i_{z+2} - i_{z+1} < i_{z+2} - i_z = j$.

Case IIA2b: $m + i_{z-1} = l + i_{z+1}$. If $k - j < m - l$, then $i_{z+1} - i_1 < i_{z+1} - i_{z-1}$ and thus $z = 1$. But $j + i_t > m + i_0 = m + i_{z-1}$, $j + i_t$ is a left-over, a contradiction. Hence $k - j \geq m - l$. Again, $k - j = i_{z+1} - i_1 = i_{z+1} - i_{z-1} + (i_{z-1} - i_1) = (m - l) + (i_{z-1} - i_1) = m - l + (i_z - i_2)$. This shows that $j + i_t = j + m - k + i_z = l + i_2$ and thus $j + i_t$ must cancel down with $l + i_2$. Hence $z \geq 3$.

Since all j's must be to the right of $l + i_2 = j + i_t$ and $m + i_{z-2}$ is to the left of $l + i_2$, we must have $m + i_{z-2} = k + i_{t-3}$. So $m - k = i_{t-3} - i_{z-2}$. Since $i_z - i_{z-2} = 2j$ and $m + i_z = k + i_t$, we have $i_t - i_{t-3} = 2j$. Together with $i_{t-1} - i_{t-2} = j$, we have $i_t - i_{t-1} = i_{t-2} - i_{t-3} = j/2$. Hence $m - l = 3j/2$. If $t - z$ is odd, then $i_{z+3} - i_{z+2} = j/2$ and $i_{z+2} - i_{z+1} = j$, which contradicts to $i_{z+2} - i_z = j$. Consider the case that $t - z$ is even. Assume that $t - z = 4$. Then $l - k = i_{z+2} - i_z = j$ and thus $k + i_z = l + i_{z-1}$. If $z > 3$, then $m + i_{z-3}$ is a left-over by using $m + i_{z-2} = k + i_{t-3} = k + i_{z+1}$ and $m + i_{z-3} > l + i_2 = j + i_t$, a contradiction. If $z = 3$, then $k + i_3 = l + i_2 = j + i_t$ gives another left-over, a contradiction. So $t - z \geq 6$. In this case, we still have $k + i_{t-3} = m + i_{z-2}$ and $k + i_{t-4} = m + i_{z-3}$. If $z > 3$, then $l + i_{z-1} > m + i_{z-3} > l + i_2$ and thus $l + i_{z-1}$ is a left-over, a contradiction. Let $z = 3$. Using $j + i_t = l + i_2 = l + 2j$, $m - l = 3j/2$, and $i_t - i_{t-1} = j/2$, we then have $j + i_{t-1} = m + i_0$, contradicts to $k + i_{t-4} = m + i_0$.

Case IIA3: $l + i_{z+2} = j + i_t$. Then $m - l = i_t - i_{t-2} = (i_t - i_{z+2}) + (i_{z+2} - i_z) - (i_{t-2} - i_z) = l - j + j - (l - k) = k$ implies that $0 + i_t = k + i_{t-2} = l + i_z$, which gives an additional left-over because $m + i_0$ is to the left of $0 + i_t$, a contradiction.

Case IIA4: $l + i_{z+2} = 0 + i_t$. In this case, $j + i_t$ either cancels down with $k + i_{t-1}$ or an $m + i_p$ with $p \leq z - 1$. If $j + i_t = m + i_p$ with some $p \leq z - 1$, then $k - j = i_z - i_p$ is a multiple of j, a contradiction. If $j + i_t = k + i_{t-1}$, then $m + i_{z-1}$ is to the left of $0 + i_t = l + i_{z+2}$ as $i_z - i_{z-1} = j < k$. So $j = i_z - i_{z-1} = k + i_t - (j + i_{t-1}) = 2(k - j)$. Hence $i_z - i_{z-1} = k - j = j/2$ and $z = 1$. Moreover, $i_{z+2} - i_{z+1} = j/2$. Since t is even, we have $i_{t-1} - i_{t-2} = j/2$. Using $z = 1$, we also obtain $l + i_{z+1} = 0 + i_{t-1}$. Hence $i_t - i_{t-1} = i_{z+2} - i_{z+1} = j/2$. Therefore $m - l = j$, contradicts to $m - l > i_z - i_{z-1} = j$.

Case IIA5: $l + i_{z+2} = m + i_p$ **for some** $p < z - 1$. In this case, $z \geq 2$. Since $i_t \leq m$, $m + i_{z-1}$ can not cancel up with a 0. It must be canceled up with a j or k. Again, $m + i_{z-1} \neq j + i_t$ for otherwise, $k - j = i_z - i_{z-1} = j$, a contradiction. Also $m + i_{z-1} \neq j + i_{t-1}$, for otherwise, $j + i_t = k + i_{t-1}$. So $j = i_z - i_{z-1} = 2(k - j)$, contradicts to $z \geq 2$. Hence $m + i_{z-1} = k + i_{t-1}$. This implies that $i_t - i_{t-1} = i_z - i_{z-1} = j$. We now claim that $p = z - 2$. Otherwise, $m + i_{z-2}$ must be a left-over. So $m - l = i_{z+2} - i_{z-2} = 3j$. Using this and $i_t - i_{t-1} = j$, we conclude that $i_x - i_{x-1}$ is either a j or $2j$ for any $x \geq z + 2$, which contradicts to $i_{z+2} - i_z = j$.

Case IIA6: $l + i_{z+2} = j + i_{t-1}$. Using $l - j = i_{t-1} - i_{z+2}$, $l - k = i_{t-2} - i_z$, and $i_{z+2} - i_z = j$, we have $i_{t-1} - i_{t-2} = k$. So $0 + i_{t-1} = k + i_{t-2} = l + i_z$. There must exist an $m + i_p$ with $p < z$ such that $0 + i_{t-1} = k + i_{t-2} = l + i_z = m + i_p$. Hence $m - l$ is a multiple of j. This implies that $l+i_{z+1}$ can not cancel down with an m. Hence $l+i_{z+1}=0+i_t$. Therefore $i_t > i_t - i_{z+1} + i_z - i_p = l + (m-l) = m$, a contradiction.

Case IIA7: $l+i_{z+2}=0+i_{t-1}$**.** In this case, $l+i_{z+1}$ must be canceled down with some $m+i_p$ with $p<z$. So $i_t > i_{t-1} - i_{z+2} + i_{z+1} - i_p = l + (m-l) = m$, a contradiction.

Case IIB: $m-l<j$**.** In this case, $m+i_{z-1}$ is to the right of $l+i_z$ and $0+i_t$ is to the right of $m+i_{z-1}$.

Assume $\Omega = t-1 = z+3$. We note that $j+i_t$ can not cancel with $k+i_{t-1}$, for otherwise, one of $l+i_{z+2}$ and $l+i_{z+1}$ must be a left-over. Hence $j+i_t$ cancels down with $l+i_{z+2}$ or $l+i_{z+1}$. In either case, $k-j<m-l<j$. But $k-j=i_{z+1}-i_1$. Hence $z=1$ and t is odd, a contradiction.

Assume $\Omega = t-1 > z+3$. Hence $l-k = i_{t-2} - i_z > i_{z+2} - i_z = j$. Since $l+i_{z+2}$ and $l+i_{z+1}$ must be canceled up, either $j+i_t$ or $j+i_{t-1}$ cancels down with one of $l+i_{z+2}$ and $l+i_{z+1}$ (recall that $0+i_t$ is to the right of $m+i_0$). Using $m+i_z=k+i_t$ and $l+i_z=k+i_{t-2}$, we must have that $k-j<m-l<j$. Hence $z=1$. If $k+i_{t-1}=l+i_{z+2}$, then $j+i_{t-1}$ is to the left of $k+i_{t-2}=l+i_z$. If $k+i_{t-1}=l+i_{z+1}$, then $k-j=i_{z+1}-i_z$ implies that $j+i_{t-1}=k+i_{t-2}=l+i_z$. In both bases, $j+i_{t-1}$ is a left-over.

Case III: $\Omega = t-1$ **and** $\Omega = z+2$**.**

In this case, we have $t=z+3$ and $l+i_{t-1}$, $k+i_{t-1}$ are to the left of $l+i_z=k+i_{z+1}$. Moreover, $l-k<j$.

Case IIIA: $m-l\geq j$**.** We first note that $l+i_{z+2}$ can not cancel up with $0+i_t$ nor cancel down with $m+i_p$ with $p<z-1$. Because in both cases, $j+i_t$ must be canceled down with an $m+i_q$ with $q<z$. This implies that $k-j=i_z-i_q$ is a multiple of j, a contradiction. Therefore we have either $l+i_{z+2}=m+i_{z-1}$ or $l+i_{z+2}=j+i_{z+3}$.

Let $l+i_{z+2}=m+i_{z-1}$. (i) Assume that $k+i_{z+2}=j+i_t$ and $l+i_{z+1}=m+i_{z-2}$. Since $m-l=i_{z+1}-i_{z-2}=i_{z+2}-i_{z-1}$, we have $i_{z+2}-i_{z+1}=j$. Hence $0+i_{z+2}=j+i_{z+1}=k+i_1$, a contradiction. (ii) Assume that $k+i_{z+2}=l+i_{z+1}$ and $j+i_t=m+i_{z-2}$. If $l+i_{z+1}=k+i_{z+2}$, then $l-k=i_{z+2}-i_{z+1}<j$ and $0+i_{k+1}=k+i_0$ imply that $0+i_{z+2}=l+i_0$. Therefore $j+i_z$ is a left-over, a contradiction. (iii) Assume that $k+i_{z+2}=m+i_{z-2}$ and $j+i_t=l+i_{z+1}$. A contradiction similar to (ii) because $i_{z+2}-i_{z+1}<l-k<j$. (iv) Assume that $k+i_{z+2}=j+i_t$ and $l+i_{z+1}=j+i_{t-1}$. Using $i_{z+2}-i_{z-1}=m-l=i_{z+3}-i_{z+1}$ and $i_{z+3}-i_{z+2}=k-j$, we conclude that $i_{z+1}-i_{z-1}=k-j$ and thus $z=2$. Then t is odd, a contradiction.

Let $l+i_{z+2}=j+i_{z+3}$. We have $m+i_{z-1}=l+i_{z+1}$ or $m+i_{z-1}=k+i_{z+2}$ because $0+i_{z+3}$ is to the right of $m+i_0$. In the former case, $m-l=l-k+j<2j$. Using $k+i_{z+3}=m+i_z$, $j+i_{z+3}=l+i_{z+2}$, and $m+i_{z-1}=l+i_{z+1}$, we have $k-j<i_z-i_{z-1}=j$. Hence $z=1$.

Moreover, $m - l = k$. So $0 + i_{z+2} = k + i_{z+1} = l + i_z$ gives a left-over, a contradiction. Now we assume that $m + i_{z-1} = k + i_{z+2}$. Using $m-k = i_t - i_z = i_{t-1} - i_{z-1}$ and $i_z - i_{z-1} = j$, we have $l - j = j$ and also $0+i_t = j+i_{t-1}$. Hence $z = 1$. Therefore we have the polynomial exception 21. That is, $f = x^{10} + x^4 + x^3 + x^2 + 1$ and $h = x^9 + x^7 + x^3 + x^2 + 1$.

Case IIIB: $m - l < j$. In this case, $l + i_{t-1} = j + i_t$ and $l + i_{t-2} = k + i_{t-1}$. Also $l - k < m - l < j$. So $l + i_0$ can not cancel up with $0 + i_t$. Hence $0 + i_{z+3} = j + i_z$. That is, $m - k = j$. So $m + i_0 = k + i_1 = j + i_{z+1}$ gives a left-over, a contradiction.

8.6.3 Assume $y = z$.

We must have $0 + i_t = m + i_0$ and $j + i_t = m + i_1$. Moreover, $z \geq 2$.

Case I: $\Omega < t - 1$.

In this case, we have $l + i_z = k + i_{t-1}$ and $0 + i_{z+1} = j + i_{z-1}$. Because $0 + i_t = m + i_0$ and $j + i_t = m + i_1$, we have $l + i_{z+2} = m + i_{z-1}$ and $l + i_{z+1} = m + i_{z-2}$. Hence $z \geq 4$ and $m - l = i_{z+1} - i_{z-2} = 2j$. Moreover, $i_{z+2} - i_{z+1} = j$. It implies that $i_x - i_{x-1} = j$ for all $z + 2 \leq x \leq \Omega + 1$.

Note that all l's below row z and above i_1 cancel down with m's. Then there must be left-overs in columns $j+i_t = l+i_3 = m+i_1$ and $0+i_t = l+i_2 = m+i_0$. So there exists k on row α such that $j+i_t = k+i_\alpha = l+i_3 = m+i_1$. If $\alpha \geq z+1$, then $k-j = i_t - i_\alpha$ is a multiple of j, a contradiction. If $\alpha \leq z$, then there exists $\beta \leq z-1$ such that $k+i_\beta = 0+i_t = l+i_2 = m+i_0$. Hence $l-k = i_\beta - i_2$ must be a multiple of j, which contradicts to that $l - k = i_{t-1} - i_z$ is not a multiple of j.

Case II: $\Omega = t - 1$ and $\Omega > z + 2$.

In this case, $t \geq z + 4$. So $m + i_0 = 0 + i_t$ and $l + i_0 = 0 + i_{t-2} > 0 + i_{z+2}$. Hence $0 + i_{z+1} = j + i_{z-1}$.

Case IIA: $\Omega = z + 3$. Note that $m - l \geq j$. Otherwise, one of $k + i_{t-1}$, $l + i_{z+1}$ and $l + i_{z+2}$ is left-over because $j + i_t = m + i_1$.

Case IIA1: $m - l \geq j$ **and** $k - j \geq m - l$. We consider $l + i_{z+2}$.

Case IIA1a: $l + i_{z+2} = m + i_{z-1}$. Note $l - k = i_{z+2} - i_z < m - l$. Hence $k+i_{t-1}$ is to the left of $l+i_{z+1}$. Since $k-j > m-l$, we have $k + i_{t-1} = m + i_{z-2}$ and $l + i_{z+1} = m + i_{z-3}$. Because $0 + i_{z+1} = j + i_{z-1}$, we obtain that $m - l = 3j$. Hence $i_{z+2} - i_{z+1} = 2j$. Note that all l's from row i_{z-1} to row i_4 cancel down with m and $k - j$ is not a multiple of j, $k + i_{z+1}$ is a left-over if $k - j > 5j$ and $j + i_t = l + i_4 = m + i_1$ gives a left-over if $3j < k - j < 5j$.

Case IIA1b: $l + i_{z+2} = k + i_{t-1}$. In this case, $l + i_{z+1} = m + i_{z-1}$ and thus $m - l = j$. Since $i_{z+2} - i_{z+1} < m - l = j$ and $i_z - i_1 = k - j$ is not a multiple of j, $k + i_{z+1}$ is a left-over if $k - j > 2j$. If $k - j < 2j$, the only possible situation is $z = 3$ or $z = 2$. If $z = 3$, the t is odd, a contradiction. If $z = 2$, the $j + i_t = m + i_1 = m + i_{z-1} = l + i_{z+1}$ gives a left-over, a contradiction.

Case IIA1c: $l + i_{z+2} = m + i_{z-2}$, $m + i_{z-1} = k + i_{t-1}$. So $z \geq 4$. We have $m - k = i_{t-1} - i_{z-1} = i_{z+3} - i_{z-1} = i_{z+3} - i_{z+1} + i_{z+1} - i_{z-1} = m - l + j$. So $l - k = j$. Using $i_{z+2} - i_z = l - k$, we obtain that $0 + i_{z+2} = j + i_z = k + i_1 = l + i_0$. This implies that $i_{z+2} - i_{z+1} = i_z - i_{z-1}$. Moreover, $m - l = i_{z+2} - i_{z-1} = (i_{z+2} - i_{z+1}) + (i_{z+1} - i_{z-1}) + (i_{z-1} - i_{z-2}) = i_{z+2} - i_{z+1} + 2j = i_z - i_{z-1} + 2j$. So $l + i_z = m + i_{z-3}$. If $z = 4$, then $j + i_t = l + i_z = k + i_{z+2} = m + i_1$ and thus $l + i_{z+1}$ is a left-over, a contradiction. If $z > 4$, then $k + i_{z+2} = l + i_z = m + i_{z-3}$ gives a left-over, a contradiction.

Case IIA2: $m - l \geq j$ **and** $k - j < m - l$. Note that $j + i_t = m + i_1$, z is at most 5 to cancel $k + i_{t-1}$, $l + i_{z+1}$ and $l + i_{z+2}$. But $z = 5$ is impossible because t is not odd. Hence $z \leq 4$.

Case IIA2a: $l + i_{z+2} = m + i_{z-1}$. In this case, $l - k = i_{z+2} - i_z < i_{z+2} - i_{z-1} = m - l$. Then $k + i_{t-1}$ must be to the left of $l + i_{z+1}$. We must have $k + i_{t-1} = m + i_{z-2}$. Moreover, if $l + i_{z+1} = j + i_{t-1}$ implies that $k - j < 2j$ and thus $z = 3$, a contradiction. Hence $l + i_{z+1} = m + i_{z-3}$. Therefore $z = 5$ in this case. However, we have a even number of rows , a contradiction.

Case IIA2b: $l + i_{z+2} = k + i_{t-1}$. In this case, $z \leq 2$. Otherwise, $l + i_{z+1} = m + i_{z-1}$ and thus $m - l = i_{z+1} - i_{z-1} = j$. But $k - j < m - l = j$, contradicts to $z \geq 3$ (i.e. $k - j > j$). Hence $z = 2$ and $l + i_{z+1} = j + i_{t-1}$. That is, we must have $l + i_{z+2} = k + i_{z+3}$ and $l + i_{z+1} = j + i_{z+3}$. So $m - l = l - j$ and thus $i_t - i_{t-1} = (m - l) - (l - k) = (l - j) - (l - k) = k - j$. This means $j + i_t = k + i_{t-1} = l + i_{z+2} = m + i_1$. Hence $i_{z+2} - i_{z-1} = m - l = i_{z+3} - i_{z+1} = i_{z+3} - i_{z+2} + i_{z+2} - i_{z+1} = l - k + i_{z+2} - i_{z+1}$. On the other hand, $i_{z+2} - i_{z-1} = i_{z+2} - i_{z+1} + j$, we have $l - k = j$. Then $m - l = i_t - i_{t-2} = k$. That is, $0 + i_t = k + i_{t-2} = l + i_z = m + i_0$. In this case, we have the polynomial exception 15: $f(x) = x^8 + x^5 + x^3 + x^2 + 1$ and $h(x) = x^8 + x^7 + x^5 + x^4 + x^3 + x^2 + 1$.

Case IIA2c: $l + i_{z+2} = j + i_{t-1}$. So $k + i_{t-1} = m + i_{z-1}$ and $j + i_t = m + i_{z-2}$. Hence $z = 3$, a contradiction.

Case IIB: $\Omega > z + 3$. We also have $m - l \geq j$. Moreover, $t > z + 4$.

Case IIB1: $m - l \geq j$ **and** $k - j \geq m - l$. We consider $l + i_{z+2}$.

Case IIB1a: $l + i_{z+2} = m + i_{z-1}$. Consider $l + i_{z+1}$, we have 3 cases:

Case IIB1ai: $l + i_{z+1} = k + i_{t-1}$. If $\Omega - z = \alpha$ is odd, then $l - k = i_{t-1} - i_{z+1} = (\alpha - 1)(m - l)/2$, a multiple of $m - l$, but $l - k = i_{t-2} - i_z < (\alpha - 1)(m - l)/2$, a contradiction.

If $\Omega - z = \alpha$ is even, $l - k = i_{t-1} - i_{z+1} = \alpha(m-l)/2 + i_{z+2} - i_{z+1}$ and $l - k = i_{t-2} - i_z = \alpha(m-l)/2 + i_{z+1} - i_z$ follow that $i_{z+2} - i_{z+1} = i_{z+1} - i_z < j$. Because $j + i_z = k + i_1$, $0 + i_{z+2}$ must be a left-over because $i_{z+2} - i_z < 2j$ and $l - k > 2j$, a contradiction.

Case IIB1aii: $k + i_{t-1}$ is to the left of $l + i_{z+1}$. We note that $k + i_{t-1} = m + i_{z-2}$ and $l + i_{z+1} = m + i_{z-3}$. Since $i_{z+1} - i_{z-1} = j$, we obtain $m - l = 3j$ and thus $i_{z+2} - i_{z+1} = 2j$. So $i_x - i_{x-1} = 2j$ or j for all $x \geq z + 3$. Since $i_z - i_4$ is not a multiple of j and $i_{t-2} - i_{t-3} = 2j$ or j, $j + i_t = l + i_4 = m + i_1$ gives a left-over.

Case IIB1aiii: $k + i_{t-1}$ is to the right of $l + i_{z+1}$. In this case $m - l = i_{z+1} - i_{z-1} = 2j$ and thus $i_x - i_{x-1} = j$ for all $x \geq z + 2$. Since $i_z - i_4$ is not a multiple of j and $i_{t-2} - i_{t-3} = j$, $j + i_t = l + i_4 = m + i_1$ gives a left-over.

Case IIB1b: $l + i_{z+2} = k + i_{t-1}$. In this case, $l + i_{z+1} = m + i_{z-1}$ and thus $m - l = j$. Note that $i_{t-2} - i_{t-3} < j$ and $l - k \geq m - l = j$. If $k - j > 2j$, then $k + i_{t-3}$ must be a left-over. If $j < k - j < 2j$, then the only possible situation is $z = 2$. So $j + i_t = m + i_1 = m + i_{z-1} = l + i_{z+1}$ implies that $k - j < m - l$, a contradiction.

Case IIB1c: $l + i_{z+2} = m + i_{z-2}$. In this case, $k + i_{t-1} = m + i_{z-1}$ and $l + i_{z+1} = m + i_{z-3}$. So $m - l = i_{z+1} - i_{z-3} = 3j$ and then $i_{z+2} - i_{z+1} = j$. This implies that $i_t - i_{t-1}$ is j or $2j$, contradicts to $i_t - i_{t-1} = i_z - i_{z-1} < j$.

Case IIB2: $m - l \geq j$ and $k - j < m - l$. Similarly, $z \leq 5$.

Case IIB2a: $l + i_{z+2} = k + i_{t-1}$. If $\Omega - z = \alpha$ is even, then $l - k = i_{t-1} - i_{z+2} = (\alpha - 2)(m-l)/2$ contradicts to $l - k = i_{t-2} - i_z = (\alpha - 2)(m-l)/2 + i_{z+1} - i_z$. If $\Omega - z = \alpha$ is odd, then a similar argument follows that $i_{z+3} - i_{z+2} = i_{z+2} - i_z$. Note $0 + i_t = m + i_0$ and $j + i_t = m + i_1$, we have 2 cases on $l + i_{z+1}$.

Case IIIB2ai: $l + i_{z+1} = m + i_{z-1}$. Hence $m - l = j$. Because $k - j < m - l = j$, we know $z = 2$ as well. Hence $j + i_t = l + i_{z+1} = m + i_1$ gives a left-over.

Case IIB2aii: $l + i_{z+1} = j + i_{t-1}$ and $z = 2$. This is the case such that $j + i_t$ is to the left of $l + i_{z+1}$. Using $k - j < j$, we have $k - j = i_z - i_{z-1}$. Also from $z = 2$ it follows that $0 + i_t = k + i_{t-2} = l + i_z = m + i_0$ and $m - l = k$. Hence $i_{z+2} - i_{z+1} = m - l - j = k - j$ and then $i_{z+3} - i_{z+2} = j$. In general, we have $i_{z+x} - i_{z+x-1}$ is $k - j$ if x is even and j if x is odd. Because $\Omega - z = \alpha$ is odd, we have $i_t - i_{t-1} = k - j$ and $i_{t-1} - i_{t-2} = j$. Because $i_{z+3} - i_{z+2} = i_{z+2} - i_z$, $i_{z+2} - i_z = j$ and then $0 + i_{z+2} = j + i_z = k + i_1$, a contradiction.

Case IIB2b: $l + i_{z+2} = m + i_{z-1}$. Same as the case IIIB1ai, we have $l + i_{z+1} \neq k + i_{t-1}$.

Case IIB2bi: $k + i_{t-1}$ is to the left of $l + i_{z+1}$. Note $z \leq 5$ in this case.

Case IIB2bi1: Assume $j + i_t = m + i_1$ is to the right of $l + i_{z+1}$. Then we have $k + i_{t-1} = m + i_{z-2}$ and $l + i_{z+1} = m + i_{z-3}$. Since $i_{z+1} - i_{z-1} = j$, we obtain $m - l = 3j$. But $k - j < m - l$ follows that $m - l > 3j$, a contradiction.

Case IIB2bi2: Assume $j + i_t = m + i_1$ is to the left of $l + i_{z+1}$ and to the right of $k + i_{t-1}$. Then $k + i_{t-1} = m + i_{z-2}$ and $l + i_{z+1} = j + i_{t-1}$. In this case, $z = 4$. Note that $k - j = i_z - i_1 > 2j$ implies that $0 + i_t = m + i_0$ is to the left of $j + i_{t-1} = l + i_{z+1}$. Hence $i_{z+2} - i_{z+1} = m - l - j > j$. Hence $j + i_{z+1}$ can't cancel up with $0 + i_{z+2}$. Of course, $j + i_{z+1}$ can't cancel down with $k + i_2$, so $j + i_{z+1}$ is a left-over.

Case IIB2bi3 Assume $j + i_t = m + i_1$ is to the left of $k + i_{t-1}$. Then $k + i_{t-1}$ must be a left-over because $0 + i_t = m + i_0$.

Case IIB2bii: $k + i_{t-1}$ is to the right of $l + i_{z+1}$. If $j + i_t$ is to the left of $l + i_{z+1}$, then $l + i_{z+1}$ must be a left-over. If $j + i_t$ is to the right of $l + i_{z+1}$ and to the left of $k + i_{t-1}$, then $k + i_{t-1}$ must be a left-over because $0 + i_t = m + i_0$. If $j + i_t$ is to the right of $k + i_{t-1}$, then $l + i_{z+1} = m + i_{z-2}$ and $k + i_{t-1} = m + i_{z-3}$. So $k - j = i_z - i_1 < m - l$ follows that $m - l > 3j$, it contradicts to $m - l = i_{z+1} - i_{z-1} = 2j$.

Case IIB2c: $l + i_{z+2} = m + i_{z-2}$, $k + i_{t-1} = m + i_{z-1}$. We obtain $z \geq 4$ because $j + i_t = m + i_1$. Using $m - k = i_{t-1} - i_{z-1}$ and $m - k = i_t - i_z$, we have $i_t - i_{t-1} = i_z - i_{z-1} < j$. Since $m - l = i_{z+2} - i_{z-2} = i_{z+2} - i_{z+1} + 2j$ and $m - l = i_{z+3} - i_{z+1}$, we have $i_{z+3} - i_{z+2} = 2j$.

If $z = 4$, then $j + t = m + i_1$ must be to the left of $l + i_{z+1}$, moreover, $l + i_{z+1} = j + i_{t-1}$. Hence $k - j = (m + i_{z-1}) - (l + i_{z+1}) = m - l - j$ and thus $m - l = k$. Then $l + i_0 = 0 + i_{t-2} = k + i_{t-4}$. Using $3j < m - l = k < 4j$ and $i_{z+3} - i_{z+2} = 2j$, we have that either $i_{t-2} - i_{t-3} = 2j$ or $j < i_{t-2} - i_{t-3} < 2j$. In both cases, we have $l + i_0 = 0 + i_{t-2} = k + i_{t-4} \neq j + i_{t-3}$. Hence we have a left-over, a contradiction. If $z = 5$, then $l + i_{z+1} = m + i_{z-3}$ is to the left of $j + i_t = m + i_1$. So $m - l = 3j$ and $i_{z+2} - i_{z+1} = i_{z-2} - i_{z-3} = j$. Each $i_x - i_{x-1}$ for any $x \geq z + 2$ is either j or $2j$. In particular, $i_t - i_{t-1} = 2j$ because t is even. This shows that one of $m + i_1 = l + i_4 = j + i_t$ and $m + i_0 = l + i_3 = 0 + i_t$ gives a left-over, a contradiction.

Case III: $\Omega = t - 1$ and $\Omega = z + 2$.

In this case, $l + i_z = k + i_{z+1}$, $0 + i_{z+1} = l + i_0$, and $l + i_{t-1} = m + i_{z-1}$ ($l + i_{t-1}$ can't cancel up with $j + i_t$ because $j + i_t = m + i_1$). Hence $0 + i_{z+2} = j + i_{z-1}$

and $m - l = j$. All l's below row $z - 1$ are canceled with m's. Then we have $k+i_{t-1} = l+i_{t-2}$. Because $l-k < j$, $z = 3$ and $j+i_t = k+i_z = l+i_{z-1} = m+i_{z-2}$ (in this case, $t = 6$ and $z = 3$). Otherwise $j + i_t = l + i_2 = m + i_1$ gives a left-over, a contradiction. Hence $l - k = j/3$ and $k - j = 4j/3$. Therefore $k + i_{z-1} = k + i_2$ is a left-over, a contradiction.

8.7 Case 2.1/4:

Here we assume $t > y$ and $z > 0$. Otherwise all shifts are the same and this has been dealt with producing polynomial exceptions 4 and 9. If $y \geq z$, then $j < i_{y+1} - i_y = m - l$ but $j = i_y - i_{y-1} \geq m - l$. If $y \leq z - 2$, then $m \geq i_t = i_t - i_z + i_z - i_{z-1} + i_{z-1} - i_{y+1} + i_{y+1} - i_y + i_y - i_0 > l - k + m - l + (i_{z-1} - i_{y+1}) + j + k - j \geq m$. So we can conclude that $y = z - 1$.

We consider what cancels with $0+i_z$. Since $t \geq z+1$, Lemma 7.1 gives that it cannot cancel with an m. It cannot cancel with an j because $i_{y+1} - i_y > j$ in subcase 4.

Case I: $0 + i_z = l + i_\alpha$.

Since $i_{z+1} - i_z = m - l$, Lemma 7.3 gives that $\alpha = 0$, $i_t = i_{z+1} = m$ and we get $l - k = m - l$. We also have that $j + i_z = l + i_1$, $0 + i_{z+1} = m + i_0$ and $j + i_{z+1} = m + i_1$. We now consider what cancels with $k + i_1$. We know that $j + i_z = l + i_1 > k + i_1 > k + i_0 = j + i_{z-1}$. Thus it can only be in the same column as $0 + i_z = l + i_0$ or $0 + i_{z+1} = m + i_0$, and thus it is left-over. This implies that $t/2 \leq 1$ since left-over k's must be in the top half of the diagram. But this implies that $y = 0$ which cannot happen.

Case II: $0 + i_z = k + i_\alpha$.

Case IIA: $\alpha \geq 2$. We consider $k+i_1$. Since $j+i_z > 0+i_z > k+i_1 > k+i_0 = j + i_{z-1} > 0 + i_{z-1}$ it cannot cancel up. Thus it must cancel down or be left-over. Again if it is left over then $t = 2$ which is incompatible with $t \geq z+1$ and $y \geq 1$. If $k+i_1 = l+i_0$, then $m \geq 0+i_{z+1} = 0+i_z+m-l = k+i_\alpha+m-l > k+i_1+m-l = l+i_0+m-l = m$ which is a contradiction. If $k + i_1 = m + i_0$, then $m \geq 0 + i_z = k + i_\alpha > k + i_1 = m + i_0 = m$ is a contradiction.

Case IIB: $\alpha = 1$. We start with two cases depending on the size of y.

Case IIB1: $y = 1$. We consider the relative positions of $j + i_z$ and $0 + i_{z+1}$.

Case IIB1a: $0 + i_{z+1} < j + i_z$. First note that $m - l = i_{z+1} - i_z < j$. If $0 + i_{z+1} = m + i_\beta$ then $t = 3$ which violates parity. $k + i_2 = k + i_z > j + i_z > 0 + i_{z+1} > 0 + i_z = k + i_1$. So we must have $0 + i_{z+1} = l + i_\beta$, $\beta = 0, 1$. If $\beta = 1$ then $0 + i_3 = l + i_1 = l + i_2 - 2j = k + i_t - 2j = 0 + i_t$ which implies the contradiction that $t = 3$. So $\beta = 0$ and $0 + i_{z+1} = l + i_0$ and by Lemma 7.3 and parity we have that $t = z + 2 = 4$. We have $0 + i_4 = m + i_0 < j + i_3 = l + i_1$ and $j + i_4 = m + i_1$.

We can account for the cancellation of everything except $j + i_2$, $k + i_2$ and $k + i_3$. No pair of these can cancel which produces a contradiction.

Case IIB1b: $0 + i_{z+1} = j + i_z$. Here we have $m - l = j$ and thus $j + i_t = k + i_{t-1} = m + i_1$ and nothing else cancels in this column. So one of these (the k or the m) must be left-over. Since $t \geq 4$, we have $0 + i_t = j + i_{t-1} = k + i_{t-2} = l + i_1 = m + i_0$ but none of these can be left-over.

Case IIB1c: $0 + i_{z+1} > j + i_z$. In this case $m - l = i_{z+1} - i_z > j$. We ask what $j + i_2$ cancels with. It must cancel down. If it cancels down with an m then $m \geq i_t = 0 + i_t \geq 0 + i_{z+1} > j + i_2 \geq m$. If $j + i_2 = l + i_1$, then $l - k = j = (m - l)(t - z) > j(t - z) \geq j$, a contradiction. So $j + i_2 = l + i_0$. If $t \geq z + 2$ then $m \geq i_t = 0 + i_t = 0 + i_{t-1} + m - l > j + i_2 + m - l = l + i_0 + m - l = m$. Finally if $t \leq z + 1 = 3$ we get an immediate contradiction.

Case IIB2: $y \geq 2$. We have $j + i_z = k + i_2$. We consider $0 + i_{z+1}$. If $0 + i_{z+1} = m + i_\gamma$ then Lemma 7.1 gives that $i_t = i_{z+1} = m$ and $m - l = l - k$. Now $m - k = m - l + l - k = 2(m - l)$ and $m - l = i_{z-1} - i_z = m - (k + j) = m - k - j = 2(m - l) - j$ implying that $m - l = l - k = j$. So $0 + i_z = k + i_1 = l + i_0$ and $0 + i_{z+1} = j + i_z = k + i_2 = l + i_1 = m + i_0$ but we cannot have a left-over in both of these.

So we can break into three cases.

Case IIB2i: $0 + i_{z+1} = l + i_\beta$. Lemma 7.3 gives that either $t = z + 1$ or $\beta = 0$ and $t = z + 2$.

In the first case $m - l = l - k$ and $l - 0 = i_{z+1} - i_\beta = l - k + 2j + (y - \beta)j$ and since $k = j(y + 1)$, we get $\beta = 1$. Also $m - l \leq i_z - i_{z-1} = 2j$. We now consider $l + i_0$. If it cancels it can only cancel up with a k. If it cancels up with $k + i_\gamma$ with $\gamma \geq 3$ then each of the three cases $\gamma > 3$, $\gamma = z = 3$ and $\gamma = 3 < z$ gives that $2j \geq m - l = l - k = i_\gamma - i_0 \geq 3j$. Therefore we can conclude that $l + i_0$ is left-over. Now $m + i_y$ must cancel up and the only available cancellation is $m + i_y = k + i_z$. This gives that $m - l = l - k = j$. We know the left-over is $l + i_0$ but $0 + i_t = j + i_z = k + i_2 = l + i_1 = m + i_0$ ans so something must cancel in this column too. Thus $fh = g$ cannot be a trinomial.

In the later case we have $0 + i_{z+1} = l + i_0$ and $i_t = i_{z+2} = m$. We can calculate that $l - k = 2(m - l)$, $l - 0 = m - l + 2j + k - j$ and thus $m - l = j$ This gives $l = k + 2j$, $m = k + 3j$. The GCD condition gives that $j = 1$, $k = y + 1$, $l = y + 3$ and $m = y + 4$. If $y \geq 3$. If $y \geq 3$ then $k + i_z = l + i_{z-1} = m + i_{z-2}$ and $0 + i_{z+2} = j + i_{z+1} = k + i_3 + l + i_1 = m + i_0$. But both of these columns cannot have a left-over. We can therefore conclude that $y = 2$ which implies the parity contradiction that $t = 5$.

Case IIB2ii: $0 + i_{z+1} = k + i_\beta$. Since $2j = i_z - i_{z-1} \geq m - l$ we get that if $\beta = z$ then $m - l = 2j$. Similarly if $y \geq \beta \geq 3$, then $m - l \geq 2j$ and $m - l = 2j$. Thus $m + i_{z-1} = l + i_z = k + i_t$ is left-over. The GCD condition now gives that $j = 1$. We consider $m + i_{z-2}$. It is not left-over and must cancel up. But $k + i_t = l + i_z > m + i_{z-2} > l + i_{z-1} = k + i_{t-1}$ so it must cancel up with a 0 or j in row t.
If with a 0 then $m + i_{z-2} = m + i_0 = 0 + i_t$ and $j + i_t$ has nowhere to cancel. So $m + i_{z-2} = j + i_t$. This implies that $k = 2$, $z = 2$. Now $0 + i_t = k + i_{t-1} = l + i_{z-1}$ but these are not left-over which is a contradiction.

Case IIB2iii: $0 + i_{z+1} = j + i_z$. If it cancels with $j + i_z = k + i_2$ then there is either something else in the column or $k + i_2$ is left-over. In the former it must be an l and we are in Case IIB2i. Thus $k + i_2$is left-over and $t \leq 4$. Considering that $t > z > y > 0$ we see that $t = 4$ and also that $m - l = l - k = j$. This gives $fh = (1 + x + x^3 + x^4 + x^5)(1 + x + x^2 + x^4 + x^5) = 1 + x^4 + x^5 + x^6 + x^{10}$ is not trinomial.

8.8 Case 2.1/5:

If $z \neq 0$, then

$$\begin{aligned} m &= (m - l) + (l - k) + k \\ &\leq (i_z - i_{z-1}) + (i_t - i_z) + i_y \\ &= i_t - i_{z-1} + i_y \\ &\leq m - i_{z-1} + i_y. \end{aligned}$$

Thus $i_{z-1} \leq i_y$ where equality holds if and only if $i_t = m$ and

$$i_z - i_{z-1} = m - l.$$

We observe that if equality holds, then we are also in Subcase 1.1/4 where the role of z is played by $z + 1$.

The condition $z \neq 0$ is irrelevant since if $z = 0$ then all shifts are $m - l$, a situation already considered. We conclude that $z - 1 \leq y$.

Since $i_x - i_{x-1} = m - l$ for $z + 1 \leq x \leq t$ and $i_x - i_{x-1} = j$ for $1 \leq x \leq y - 1$, if $z + 1 \leq y - 1$ then all shifts are $j = m - l$, contradicting $i_y - i_{y-1} < j$. Thus we take $z - 1 \leq y \leq z + 1$. This completes the proof of the bounds on y.

Assume $y = z + 1$. Now $m - l = i_{z+1} - i_z = i_y - i_{y-1} < j$. Also, $0 + i_t = (0 + i_y) + (i_t - i_z) + (i_z - i_y) = k + (l - k) - (m - l) < l + i_0$. That is, $0 + i_t$ is strictly to the right of all l's and m's. What happens to $j + i_{y-1}$? It cancels up or down. Because $j + i_z < j + i_{z+1} = k + i_1$, we consider the following two subcases.

Case I: $j + i_z$ **cancels down.** If $t \geq y + 1$, then since $i_{y+1} - i_y = i_{z+2} - i_{z+1} = m - l < j$, $0 + i_{y+1} < j + i_y$ and hence $0 + i_{y+1} < k + i_1$ and cannot cancel any k and from above, it cannot cancel any l or m. Therefore i_{y+1} cannot exist and $y = t$. Note that $m-l = i_{z+1}-i_z = l-k$ and hence $2(m-l) = (m-l)+(l-k) = m-k$.

Case IA: $j + i_z = m + i_0$. Then $l + i_0$ is left-over. If $i_z - i_{z-1} = m - l$ then $m - l = j$, a contradiction. Thus if $k + i_z$ cancels down, then since $i_z - i_{z-1} > m - l = l - k$, it does not cancel any l. So for some $a \geq 0$, $k+i_z = m+i_a$ and $m-k = i_z - i_a$ is a multiple of j. Since $j+i_t = k+i_1$ and $j + i_z < j + i_{z+1}$, we get that $m - k < j$ which is a contradiction. Therefore $k + i_z$ cancels up. Since the top j's and 0's are accounted for, $z = 1, y = t = 2$. Thus $f(x) = x^6+x^5+x^4+x^3+1$ and we have polynomial exception 5.

Case IB: $j + i_z = l + i_0$. Now $k = i_y = (i_y - i_{y-1}) + (i_{y-1}) = (l - k) + (l - j)$, since $i_y - i_{y-1} = l-k$. Hence $j = 2(l-k) = 2(m-l) = m-k$. Furthermore, $m + i_0 = (m - k) + k = j + k = k + i_1(= j + i_t)$. The left-over must be in this column. Now $l + i_1$ must cancel and it can only cancel up with a k. So $i_2 - i_1$ cannot be $j = 2(l - k)$, so $2 = y = t$. We may deduce that $h(x) = x^3 + x^2 + 1$ and $f(x) = x^5 + x^4 + x^3 + x^2 + 1$ which is polynomial exception 1.

<u>Case II: $j + i_z$ cancels up.</u> Then $j + i_{y-1} = 0 + i_{y+1}$ and $j = i_{z+2} - i_z = 2(m - l)$.

Case IIA: $t \geq y + 2$. Consider $k + i_1 = j + i_y = 0 + i_{y+2}$. Now either $k + i_1$ is left-over and thus $t = 2$ (because a left-over k must be in the top $t/2$ rows) or $k + i_1 = \{l \text{ or } m\} + i_0$. However $t \geq y + 2 \geq 4$ so it must be the latter. We have $l + i_0 > 0 + i_t \geq 0 + i_{y+2} = k + i_1$ so no l or m is available for $k + i_1$ to cancel with, a contradiction.

Case IIB: $t = y + 1$. Since $j = 2(m - l) = i_t - i_z = l - k$, $l + i_0 = k + j = k + i_1(= j + i_y)$, so $l + i_0$ is left-over. Now $m + i_0 = (l + i_0) + (m - l) = (j + i_y) + (i_t - i_{t-1}) = j + i_t$. We must have $m + i_{z-1} = k + i_y$, or else one of these will be stranded. Now we deduce $l + i_{z-1} = k + i_z$. If $z \geq 3$, then $m + i_{z-2}$ is stranded since everything above it is accounted except $k + i_{z-1}$ which is too far right since $m - k > j$. So $z = 0, 1$, or 2. The subcase $z = 0$ implies every shift is $m - l$ which was dealt with earlier. The case $z = 1$ implies $y = 2$, $t = 3$, but t must be even. Thus we may take $z = 2, y = 3, t = 4$. Now $f(x) = x^8 + x^7 + x^5 + x^2 + 1$ which is polynomial exception 17.

Assume $y = z$. We have $0+i_t = (0+i_y)+(i_t-i_z)+(i_z-i_y) = k+(l-k)+0 = l+i_0$. Either $j+i_{y-1}$ cancels up (and hence $i_{y+1}-i_{y-1} = j$) or it cancels down with the l or m from i_0 and hence $i_{y+1} - i_{y-1} < j$. In the latter case $t = y$ or $t = y+1$. Note $m-l = i_{z+1}-i_z < i_{y+1}-i_{y-1} < j$. We divide into cases based on t relative to z.

<u>Case I: $t = z + 1$.</u> From $z = y \geq 2$, we deduce $t \geq 3$. Since t must even, $t \geq 4$ and $y = z$ must be odd. So $y = z = 3$.

We easily deduce that $m - l = i_t - i_{t-1} = i_t - i_z = l - k$. Therefore $2(m - l) = (m - l) + (l - k) = m - k$. The only possible term with which $m + i_{z-1}$ may cancel is $k + i_z$. As well, $k + i_z$ must cancel down since the $j, 0$ from rows $i_t, i_{t-1} = i_z$ are accounted for. Hence we break into subcases as follows:

Case IA: $m + i_{z-1} = k + i_z$. Here $2(m-l) = m-k = i_z - i_{z-1} < j$. The term $l + i_{z-1}$ has nothing above it with which to cancel. If $l + i_{z-1} = m + i_{z-2}$ then $m - l = i_{z-1} - i_{z-2} = i_{y-1} - i_{y-2} = j > 2(m - l)$ which is absurd. If $l + i_{z-1}$ cancels with an even lower m, say $m + i_{z-\alpha}$, then $(\alpha - 1)j = m - l < j$, which is a contradiction. We conclude that $l + i_{z-1}$ must be left-over. Now we require $k + i_{z-1} = m + i_{z-2}$ or else one of these will be stranded, leaving too many left-over terms. Thus $m - k = i_{z-1} - i_{z-2} = j$ contradicting with above.

Case IB: $m + i_{z-1}$ **is left-over,** $l + i_{z-1} = k + i_z$. We must have $k + i_{z-1} = m+i_{z-2}$ or else one of these will be stranded. Thus $m-k = i_{z-1} - i_{z-2} = j$. Hence $m + i_0 = k + i_1 = j + i_{t-1} \neq 0 + i_t$ and we have an "extra" left-over here, a contradiction.

Case IC: $m + i_{z-1}$ **is left-over,** $l + i_{z-1} \neq k + i_z$. We must have $k+i_z = m+i_{z-2}$ or else one of these will be left-over. Now $j = i_{z-1} - i_{z-2} = (m - k) - (i_z - i_{z-1}) < m - k = 2(m - l)$. What happens to $l + i_{z-1}$? It has nothing to cancel with unless $0 \leq z - 1 \leq 1$, i.e. $1 \leq z \leq 2$. However, $z = y \geq 2$ must be odd. Thus this subcase falls.

<u>**Case II:** $t = z + 2$.</u> We have, from before, that $j + i_{y-1} = 0 + i_{y+1}$. Consider $j + i_{z+1}$. It cannot cancel up since $0 + i_t$ is accounted for. Either it cancels down with $m + i_0$ or with some $k + i_\alpha$ for $\alpha \geq 2$. However $j + i_{z+1} = j + (m-l) + i_z = (m - l) + k + i_1 < j + k + i_1$.

Case IIA: $y > 2$. In this subcase, $j + i_1 = i_2$ so $j + i_{z+1} < k + i_2 \leq k + i_\alpha$ for $\alpha \geq 2$. Thus $j + i_{z+1} = m + i_0$. We have $l = (i_t - i_{z+1}) + i_{z+1} = (m - l) + (m - j)$ and we may deduce $j = 2(m - l) = l - k$. Hence $i_z = k = l - j$ so $k + i_1 = j + i_z = l + i_0 = 0 + i_t$. Therefore we have the left-over in the column with $k + i_2 = (k + j) + i_1 = l + i_1 = j + i_t$.

The term $0 + i_{z+1}$ must cancel with $j + i_{z-1}$ because all other possibilities (lower j's and l or k from i_0 or i_1) are impossible. Hence $2(m-l) = l-k = j = i_{z+1} - i_{z-1} = (m - l) + i_z - i_{z-1}$ and so $i_z - i_{z-1} = m - l$. Therefore there is an extra left-over in the column with $m + i_{z-1} = l + i_z = k + i_t$, a contradiction.

Case IIB: $y = 2$. Clearly $t = 4$. We have $j + i_4 = l + i_1$ and $j + i_1 = 0 + i_3$. When we draw the box diagram, there are five terms unaccounted for (of which four must cancel with each other): $m+i_0, m+i_1, k+i_2, k+i_3, j+i_3$.

Case IIB1: $j + i_3 = m + i_0$. Now $k - j = i_2 - i_1 < j$. So $k + i_3 = (k - j) + (j + i_3) < j + m = m + i_1$. Hence $m + i_1 > k + i_3 > k + i_2$ so we cannot complete the required cancellations.

Case IIB2: $j + i_3 \neq m + i_0$. Since $i_3 - i_1 = (m - l) + (k - j) < m - j$, $j + i_3 \neq m + i_1$ and so we must have $k - j = i_3 - i_2 = m - l$. Since $i_3 - i_1 = j - 0 < m - k$ we cannot have $m + i_1 = k + i_3$. This forces the left-over to be $m + i_1$. Hence $m + i_0 = k + i_3 (= j + i_4 = l + i_1)$. However, now $m - l = i_1 - i_0 = j$, contrary to earlier work.

Case III: $t \geq z + 3$.

Consider $0 + i_{z+1} < i_t = l + i_0 \leq \{l, m\} + i_\alpha$ for $\alpha \geq 0$ and $0 + i_{z+1} = (m - l) + i_z < j + i_z = k + i_1$ and we see that $0 + i_{z+1} = j + i_{z-1}$ because all other options are accounted for or impossible.

Since i_{z+2} is not the top row, $0 + i_{z+2} < 0 + i_t = l + i_0 \leq \{l, m\} + i_\alpha$ for $\alpha \geq 0$. Also, $0 + i_{z+2} = (m - l) + i_{z+1} < j + i_{z+1}$. Hence $0 + i_{z+2} = k + i_\alpha$ for $\alpha \geq 2$. (If $\alpha = 1$, then $0 + i_{z+2} = k + i_1 = j + i_z$ and so $k + i_1$ must be left-over and $2 \leq y < t = 2$.) That is, $i_\alpha = i_{z+2} - k = i_{z+2} - i_z = 2(m - l)$. However, $i_\alpha \geq i_2 = (i_2 - i_1) + i_1 = (i_2 - i_1) + j > (i_2 - i_1) + (m - l)$. We deduce $i_2 - i_1 < m - l$, but no shift is less than $m - l$ in 2.1/5 with $y = z$, thus a contradiction.

Assume $y = z - 1$. Similarly to the above, $0 + i_t = (0 + i_y) + (i_t - i_z) + (i_z - i_y) = k + (l - k) + (m - l) = m + i_0$ since $i_z - i_{z-1} = m - l$ from Equation 25. So $i_t = m, i_{t-1} = l$. Also, we conclude that $l + i_z = m + i_{z-1} = k + i_t$ and so the left-over must be in this column. Also, $l + i_{z-1} = (m + i_{z-1}) - (m - l) = (k + i_t) - (i_t - i_{t-1}) = k + i_{t-1}$. Now $j + i_{y-1} < j + i_y = k + i_1 \leq \{k, l, m\} + i_\alpha$ for $\alpha \geq 1$. Since m, l, k in i_0 are accounted for, and since the left-over is already determined, $j + i_{y-1}$ must cancel up. If $j + i_{y-1} = 0 + i_\alpha$ for $\alpha > y + 1$, then $0 + i_{y+1} < 0 + i_\alpha = j + i_{y-1}$ so $0 + i_{y+1}$ cannot cancel with anything, a contradiction. Thus $j + i_{y-1} = 0 + i_{y+1}$. In particular, $j = (i_{y+1} - i_y) + (i_y - i_{y-1}) = (m - l) + (i_y - i_{y-1}) > m - l$.

Consider $k + i_{t-2}$ which cannot cancel up since these 0's and j's are accounted for and the left-over is already fixed and to the left of $k + i_{t-2}$. This k also cannot be one of $k + i_0$ or $k + i_1$ since these cancel with row $i_y \leq i_{t-2}$.

Case I: $k + i_{t-2} < m + i_{y-1}$. Here $m + i_{y-1}$ is in danger of being stranded so we would actually need $y - 1 \leq 1$ which implies $2 \leq y \leq 2$ which further implies $y = 2$ and $z = 3$. But there is nothing lower remaining to actually cancel $k + i_{t-2}$, so we have a contradiction.

Case II: $k + i_{t-2} \geq m + i_{y-1}$. We require $k + i_{t-2} = m + i_{y-1}$ or else $k + i_{t-2}$ has nothing below with which to cancel. Hence $m - k = i_{t-2} - i_{y-1} = (i_t - i_y) - (i_t - i_{t-2}) + (i_y - i_{y-1}) = (m - k) - 2(m - l) + (i_y - i_{y-1})$ implying $2(m - l) = (i_y - i_{y-1}) < j$. Therefore $j = (i_{y+1} - i_y) + (i_y - i_{y-1}) = (m - l) + 2(m - l) = 3(m - l)$. So $0 + i_{z+1} = (i_{z+1} - i_z) + (i_z - i_{z-1}) + i_{z-1} = 2(m - l) + i_y < j + i_y = k + i_1 \leq \{k, l, m\} + i_\alpha$ for $\alpha \geq 1$ and m, l, k in rows i_1 and i_0 are taken unless $z + 1 = t$ or $t - 1$. Since $0 + i_{z+1} < j + i_y$ and $0 + i_{z+1} > 0 + i_z = j + i_{y-1}$, then $0 + i_{z+1}$ cannot cancel with any j. Since $0 + i_z$ is already taken, $0 + i_z \neq l + i_0 = 0 + i_{t-1}$. Therefore $z \neq t - 1$ and $z + 1 = t - 1$ implies $t = z + 2$. Thus $m - k = i_t - i_y = 3(m - l) = j = i_1$ implying $k + i_1 = m + i_0 = 0 + i_t = j + i_y$.

If $y \geq 3$, then $i_2 - i_1 = j = m - k$ so $k + i_2 = m + i_1 = j + i_t$ with no room for an l or 0. This triple cancellation contradiction proves $2 \leq y \leq 2$. Hence $y = 2, z = 3, t = 5$, but t must be even. This final contradiction concludes this subcase.

8.9 Case 2.3/4:

If $y < z-2$ then $i_t \geq i_t - i_z + i_z - i_{z-2} + i_{z-2} - i_y + i_y - i_0 > l - k + m - l + j + k - j = m$ gives a contradiction. Now suppose that $y > z$. Then if $\Omega = z - 1$ then $j = i_{z+1} - i_z = m + l$ but $j = i_z - i_{z-1} < m - l$. If $\Omega > z - 1 > 0$ then $2j = i_{z+1} - i_{z-1} = m - l$ but $2j = i_z - i_{z-2} > m - l$ gives a contradiction. The only remaining cases to check are $\Omega > z - 1$ and $z = 1, 0$. If $z = 0$ then $l + i_1$ has nothing to cancel with since all k j and 0 are to its right, all the m are to the left. If $z = 1$ and $\Omega > 0$ then $y \geq 2$ and it can easily be verified that all shifts are either j or $2j$. In particular $m - l = 2j$ and $l - k = i_t - i_z$ is a multiple of j. The GCD condition now gives that $j = 1$ and since $i_{y+1} - i_y$ is the first shift strictly larger than j we have that $\Omega = y - 1$. $l + i_0$ must cancel up with a k, j or 0. But $k + i_t = l + i_1$, $l + i_1 = l + i_0 + j$ and unless $t = y$, $i_t - i_{t-1} = 2j$ so all remaining k, j and 0 are to the right of $l + i_0$.

If $t = y$, then $j = 1, k = y + 1, l - k = y - 1, l = 2y$, and $m = 2y + 2$. If $t > 2$ then $k + i_1$ has nothing to cancel with and so $t = 2$. This is polynomial exception 7.

From now on we can assume $z - 2 \leq y \leq z$. Also we know that that the left-overs are two m's to the left of $l + i_z$ and the $0 + i_0$. We use this frequently to derive contradictions from k's or l's having nowhere to cancel.

8.9.1 Assume $y = z$

First $i_t = i_t - i_z + i_z - i_0 = l - k + k - j = l - j$ so the bottom l cancels with the top j

If $\Omega > z - 1 > 0$ then $2j = i_z - i_{z-2} > m - l$ but $m - l > i_z - i_{z-1} > 2j$. If $\Omega > z - 1 = 0$ then $k = 2j$. If $\Omega < t - 1$ then $i_t - i_{t-1} = m - l > 2j$ and so $0 + i_t$ cannot cancel with any k or j. Neither with m nor l since $m + i_0 > l + i_0 = j + i_t > 0 + i_t$. So $\Omega = t - 1$ and $0 + i_{z+1} = k + i_z$ is forced, so $i_{z+1} - i_z = k = 2j$ and $m - l = i_{z+1} - i_{z-1} = 3j$ and so $i_x - i_{x-1} = m - l - j > j$ if x is even and j if x is odd, $1 \leq x \leq t$. So $0 + i_t = k + i_{t-1}$ and $m - l = 3j$. $l - j = i_t - i_0 = (t/2)(m - l) = 3jt/2$ and thus all m, l, k are multiples of j so $j = 1$, $k = 2$, $l = (3t/2 + 1)$ and $m = (3t/2 + 4)$. Thus

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

where $m \equiv 1 \bmod 3$. This is the only infinite family of exceptions and all these f are reducible so not primitive. Exceptions 10, 22 and 24 are members of this family.

Thus we can now assume that $\Omega = z - 1$, $i_x - i_{x-1} = m - l > j$ for $z + 1 \leq x \leq t$, $i_z - i_{z-1} < m - l$ and if $z \geq 2$ then $2j = i_z - i_{z-2} > m - l$.

If $z = 1$ then we condition on the size of $m - l$ with respect to j. $k + i_1$ must cancel with $0 + i_2$ since everything else in i_1 and i_0 is accounted for. Thus $m - l = 2j$ then $l - k = 2(t - z)j$ and the GCD condition gives $j = 1$, $k = 2$, $l = 2(t - z + 1) = 2t$ and $m = 2(t + 1)$. $j + i_2$ must cancel down with $l + i_1$ since $l + i_0 = j + i_t$. So $4 = j + i_2 = l + i_0 = l$ This gives

$$\begin{aligned} f &= 1 + x + x^2 + x^4 + x^6 \\ h &= 1 + x + x^3 \\ fh = g &= 1 + x^6 + x^9 \end{aligned}$$

Which is polynomial exception 6.

Finally if $z > 1$, then $2j > m - l > j$. So $k + i_1 > 0 + i_{y+1}$ and $0 + i_{y+1}$ must cancel down with an m or an l. However $0 + i_{y+1} < j + i_t = l + i_0 \leq \{m, l\} + i_\alpha \forall \alpha$.

8.9.2 Assume $y = z - 1$

First, $i_z - i_{z-1} = i_{y+1} - i_y \leq m - l$ and $i_z - i_{z-2} = i_z - i_{z-1} + j > m - l$. If $\Omega = z - 1$ then $i_z - i_{z-1} < m - l$ and if $\Omega > z - 1$ then $i_z - i_{z-1} < i_{z+1} - i_{z-1} = m - l$ so in either case $m - l > j$. Also since $i_z - i_{z-1} < m - l$, $i_t = i_t - i_0 = i_t - i_z + i_z - i_{z-1} + i_{z-1} - i_0 < l - k + m - l + k - j = m - j$

We condition on what $0 + i_z$ will cancel down with. If $0 + i_z = m + i_\alpha$ then Lemma 7.1 implies that $i_t = i_z$, but this contradicts the fact that $t > z$. If $0 + i_z = l + i_\alpha$ Then Lemma 7.3 gives that $t \leq z + 2$ and if equality is achieved then $i_t = i_{z+2} = m$, which contradicts $i_t < m - j$. So $i_t = i_{z+1}$. If $\alpha > 0$ then $l + i_0 = k + i_\beta$, $\beta \geq 1$. If $\beta > 1$ then $k + i_1$ has nothing, up nor down, to cancel with. So $\beta = 1$ and $l - k = j < m - l$ gives that $\Omega = z$, $i_{z+1} - i_z = j$, $i_z - i_{z-1} = m - l - j$ and all other shifts are by j. So $m - l = i_z - i_{z-2} > m - l$ So we may conclude that $\alpha = 0$. If $l - k > j$ then $k + i_1$ has nothing to cancel with since $0 + i_z > k + i_1 > j + i_y$. We also consider where $k + i_1$ cancels when $l - k \leq j$. It can only cancel down with $m + i_0$ but this contradicts the fact that $m - l > j$. So it must cancel up. Since $j + i_z > k + i_1 > j + i_{z-1}$ it must cancel with $0 + i_{z+1}$. Now $i_{z+1} = k + j$, $l - k = i_{z+1} - i_z = k + j - l$ and $l - k = j/2$. Now $m - l = i_{z+1} - i_z$ or $i_{z+1} - i_{z-1}$ so $m - l = j/2$ or $2j$ In either case $j/2$ divides k, l and m so the GCD condition gives that $j = 2$. If $m - l = j/2 = 1$ then $i_z - i_{z-1} < m - l$ is impossible. Otherwise $j = 2$, $k = 2y + 2$, $l = 2y + 3$, $m = 2y + 7$ and $\Omega = z$. If $y > 2$ then $j + i_t = j + i_{z+1} = k + i_2 < k + i_3$ and $m + i_0 = l + i_2 < k + i_3 < m + i_1$ so $k + i_3$ has nothing to cancel with. This implies that $y = 1, 2$. The former is impossible because $t = z + 1 = y + 2$ must be even. We get

$$\begin{aligned} f &= 1 + x^2 + x^6 + x^7 + x^{11} \\ h &= 1 + x^2 + x^4 + x^7 + x^8 \\ fh = g &= 1 + x^{18} + x^{19}. \end{aligned}$$

This is polynomial exception 23.

So we may finally assume that $0 + i_z = k + i_\alpha$. If $\alpha > 1$ then $k + i_1 = l + i_0$ and $j = l - k$. If $t \geq z + 2$ or $t = z + 1$ and $\Omega = z - 1$ then $l - k > m - l > j$. So $t = z + 1$, $i_{z+1} - i_z = j$, $\Omega = z$, and $m - l = i_{z+1} - i_{z-1} = i_z - i_{z-2} > m - l$.

Now we may assume that $0 + i_z = k + i_1$ and therefore that $i_z - i_{z-1} = 2j$. If $y = 1$ then $j + i_2$ could cancel down with an m or l and up with a 0. If $j + i_2$ cancels with an m, then since $j + i_t = m + i_0$, $t = 2$ and this j cancels with bottom m. But then $z \leq 1$ and so $y \leq 0$.

If $j + i_2 = l + i_\alpha$ and $\alpha = 1$ then $0 + i_2 = k + i_1 = l + i_0$ and so one is not canceled. If $j + i_2 = l + i_0$ then $l - k = 2j$ and $m + i_0 = m + i_{z-2} < l + i_z = l + 3j$ so $m - l < 3j$. $i_{z+1} - i_z < i_t - i_z = l - k = 2j$ and so $0 + i_{z+1}$ will have nothing to cancel with. Thus $j + i_z$ must cancel up with $0 + i_\alpha$. If $\alpha > z + 1$ then $0 + i_{z+1}$ must cancel down with an l and $l - k < 2j$. If $t - 2 \geq z + 1$, then Lemma 7.3 gives $m = i_t$, contrary to $m - j = i_t$. Thus $t \leq z + 2$ and parity gives $t = z + 2 = 4$ and this gives that $l - k = j$ which leaves one of $0 + i_z = k + i_y = l + i_0$ left-over. Thus $j + i_z = 0 + i_{z+1}$ and $m - l = i_{z+1} - i_z = j$, which is impossible or $i_{z+1} - i_{z-1} = 3j$. Now $m + i_{z-2} = l + i_z$ which is not permitted.

Thus $y > 1$ and $j + i_z = k + i_2$. Now we condition on where the $0 + i_{z+1}$ cancels. If with an m the Lemma 7.1 tells us that $t = z + 1$, $i_{z+1} = m$ but $i_t < m$.

If $0 + i_{z+1} = l + i_\alpha$. Lemma 7.3 gives that $t \leq z + 2$. If $t = z + 1$ then $l - k = i_{z+1} - i_z = l + \alpha j - (y + 2)j$, $\alpha = 1$ and $l + i_0$ must cancel up with a $k + i_\beta$, $\beta \geq 3$. Thus $m - l \geq l - k \geq 3j$ but $3j = i_z - i_{z-2} > m - l$.

If $t = z + 2$, $i_{z+2} = i_z + l - k = l + j$ and $i_{z+1} = l + \alpha j$. So $\alpha = 0$, $i_{z+2} = l + j$, $i_{z+1} = l$ and we have $0 + i_{z+2} = j + i_{z+1} = l + i_1$ but none of these can be left-over so there must be $m + i_0$ or $k + i_\beta$ to cancel with. If the m then $j = m - l > j$. If $j + i_{z+1} = k + i_\beta$ then j divides $l - k$ and so all shifts are divisible by j and this implies that $m - l$ is divisible by j so $j = 1$ but then it is impossible that $m + z - 2 = m + (z-2)j = m + i_{z-2} - i_0 = m + i_{z-2} < l + i_z < m + i_{z-1} = m + z - 1$.

Finally, if $0 + i_{z+1} = k + i_\alpha$ with $\alpha > 3$ and $y > 2$ then $k + i_3$ cancels down with an l or an m. If an m then $0 + i_{z+1} > k + i_3 \geq m$. So $k + i_3 = l + i_\beta$ with $\beta = 0, 1, 2$. But $l - k = i_t - i_z \geq i_{z+1} - i_z \geq 3j$ and $l - k = i_3 - i_\beta = (3 - \beta)j$ so $l - k = 3j$, $\alpha = 4$ and $0 + i_{z+1} = l + i_1$ and this case has been previously dealt with.

If $0 + i_{z+1} = k + i_3$ and $y = 2$, then $k = 3j$, $i_z = 4j$, $i_{z+1} = 7j$. If $\Omega = z - 1$ then $m - l = 3j$ and $m + i_{z-2} = l + i_z$ which is a contradiction. If $\Omega \geq z$ then $m - l = 5j$ and $m + i_{z-2} > l + i_z$ which is a contradiction.

So $0 + i_{z+1} = k + i_3$ and $y \geq 3$. We have $0 + i_{z+1} = k + 3j$ and $i_{z+1} - i_z = 2j$. But $i_z - i_{z-2} = 3j > m - l$. Hence $\Omega \neq z - 1$. Thus $m + i_{z-1} = l + i_{z+1}$ and so $m - l = 4j$. Then $m + i_{z-2}, m + i_{z-3}, m + i_{z-4} > l + i_{z-1}$ so these m's must cancel up with a 0, j, or k. But $i_t < m - j$ implies these three m's must cancel with k's. However $i_t - i_{t-2} \geq m - l$, so at most $k + i_{t-1}$ is available to cancel these m's, so we have a contradiction.

8.9.3 Assume $y = z - 2$

First $m - l < i_z - i_{z-2} = m - l + \delta$, $m \geq i_t - i_z + i_z - i_y + i_y - i_0 = l - k + m - l + \delta + k - j = m + \delta - j$ and $\delta \leq j$. We will first condition on what $m + i_y$ cancels up with. Lemma 7.2 precludes the possibility of it canceling up with a j or a 0 except $j + i_t$. We will also examine what $0 + i_{y+1}$ cancels with. Lemma 7.1 and fact that $t \geq z + 1$ imply that it cannot cancel with an m. Lemma 7.3 shows that if it cancels with an l then $i_{z+1} = i_t = m$, $i_{z-1} = l$, $\Omega = t - 1 = z$ and $\delta = j$.

Case I: $m + i_y = l + i_\alpha$.

Since $l + i_z > m + i_y$ we have that $\alpha = y + 1 = z - 1$, $i_{z-1} - i_{z-2} = m - l$ and $i_z - i_{z-1} = \delta \leq j$. We now condition on what cancels with $0 + i_{z-1}$.

Case IA: $0 + i_{z-1} = l + i_0$. Recall that $i_{z+1} = i_t = m$, $i_{z-1} = l$, $\Omega = t - 1 = z$ and $\delta = j$. Since $y \geq 1$, $j + i_{z-1} = l + i_1$. Since $j + i_{z-2} < k + i_1 < l + i_1 = j + i_{y+1} = 0 + i_z$ the only thing that can cancel with $k + i_1$ is $m + i_0$. In this case $m - k = j$ which contradicts fact that $m - k > m - l = i_{z+1} - i_z + i_z - i_{z-1} > j$.

Case IB: $0 + i_{z-1} = k + i_\alpha$. If $\alpha > 1$ then $k + i_1$ must cancel down with $l + i_0$ or $m - i_0$. If m then we calculate that $i_{z-1} - i_0 > m$ which is impossible. If $k + i_1 = l + i_0$ then $m \geq i_t \geq i_{z+1} \geq m - l + i_{z-1} = m - l + k - 0 + i_\alpha = m - l + k + (\alpha - 1)j + l - k > m$, which is a contradiction.

So $\alpha = 1$ and $i_{z-1} = k + j$, $i_{z-2} = k - j$ and $m - l = 2j$. We break into two cases:

Case IB1: $y = 1$. We have $y = 1$, $k = 2j$, $m - l = 2j$. Where does $j + i_{z-1}$ cancel. If it cancels down to $l + i_1$ then $l + i_0 = 0 + i_z$ and by Lemma 7.3 we get that $t = 5$ which violates t's parity. If $j + i_{z-1} = m + i_0$ then $l = k$ which is not allowed. If $j + i_{z-1} = l + i_0$ then $l = 4j$, $m = 6j$, $j = 1$ and consider what $0 + i_z$ cancels with. This forces $i_z = m$ but $t > z$.

So this j cancels up, $j + i_{z-1} = 0 + i_\beta$, $\beta \geq z$. If $\beta > z$ then $0 + i_z$ must cancel down. Lemma 7.1 shows that it must cancel down with an l. If $0 + i_z = l + i_1$ then $l + i_0$ has nothing to cancel. If $0 + i_z = l + i_0$ then $i_z = l$. No matter the value of Ω, $i_{z+1} - i_{z-1} > j$ and there is no $0 + i_\beta = j + i_{z-1}$.

Thus we may assume that $j + i_{z-1} = 0 + i_z = 4j$. $k + i_t = l + i_z$ implies that $0 + i_t = l - k + i_z = l - 2j + 4j = l + 2j = m$. We have $j + i_t = m + i_1 = l + i_{z-1}$, but none of these are left-over so we must have a $k + i_\beta = j + i_t$, $z \leq \beta < t$. The fact that $i_t - i_{t-2} \geq m - l = k$ forces $\beta = t - 1$ and $i_t - i_{t-1} = k - j = j$ which in turn implies that

$\Omega = t - 1$. Also, $i_{t-1} - i_{t-2} = m - l - j = j$ so $i_x - i_{x-1} = j$ for all $z + 1 \leq x \leq t$. The fact that $0 + i_{z+1} < k + i_z$ but still must cancel means that $0 + i_{z+1} = m + i_0$, $l + i_1$ or $l + i_0$. In the former two cases $l + i_0$ has nothing to cancel with. In the latter all $m = 7j$, l and k are divisible by j and we have

$$\begin{aligned} f &= 1 + x + x^2 + x^5 + x^7 \\ h &= 1 + x + x^3 + x^4 + x^5 + x^6 + x^7 \\ fh = g &= 1 + x^{13} + x^{14} \end{aligned}$$

which is polynomial exception 12.

Case IB2: $y > 1$, $j + i_{z-1} = k + i_2$. We ask what $0 + i_z$ cancels down with. Lemma 7.1 gives the contradiction of $t = z$ if $0 + i_z = m + i_\alpha$. If $0 + i_z = l + i_\beta$, $0 \leq \beta \leq z - 1$. Lemma 7.3 gives that $t \leq z + 2$. We split into three cases

Case IB2a: $0 + i_z = l + i_\beta$ **and** $t = z + 2$. From Lemma 7.3 we get that $i_{z+2} = m$, $i_{z+2} - i_z = m - l = l - k = 2j$, $0 + i_z = l + i_0$, $\Omega = z + 1$. From this we obtain that $j = 1$. Now $k + i_{z+1} = l + i_{z-1} = m + i_{z-2}$ but none of these is left-over so $j + i_{z+2} = k + i_{z+1}$ and by Lemma 7.2, $y = 1$. But this gives t an odd parity and contradicts the assumption of Case IB2 that $y > 1$.

Case IB2b: $0 + i_z = l + i_\beta$ **and** $t = z + 1$. If $\Omega = z - 1$ then $i_{z+1} - i_z = m - l = l - k = 2j$ and Lemma 7.3 gives that $0 + i_z = l + i_0$. The GCD condition gives that $j = 1$, $k = y + 1$, $l = y + 3$ and $m = y + 5$. Recall since $z - 2 = y > 1$ then $m + i_{z-4}$ is well defined and $m + i_{z-4} = l + i_{z-2} = k + i_{z-1}$ but none are left-over. Recall that $j + i_z = l + i_1$. So $m + i_{z-4} = j + i_{z+1}$, or $0 + i_{z+1}$. If $m + i_{z-4} = 0 + i_{z+1}$ then $t = z + 1 = 5$ which violates parity. So $m + i_{z-4} = j + i_{z+1}$ and Lemma 7.2 gives $j = 1$, $k = 4$, $l = 6$ and $m = 8$ but then $0 + i_{z+1}$ has nothing to cancel with.

If $\Omega = z$, $0 + i_z = l + i_\beta$ and $\beta > 0$ then the fact that $l - k < m - l = 2j$ gives that $l + i_0 < k + i_2$ and $l + i_0$ has nothing to cancel with. So $\beta = 0$ and $i_{z+1} = k + 3j = 2l - k$. This implies that $j/2$ divides k, l and m and we get $j = 2$, $m - l = 4$, $l = k + 3$, $i_{z+1} = k + 6$, $i_z = k + 3$, $i_{y+1} = k + 2$, $i_y = k - 2$. We must cancel $k + i_{z-1}$ with something.

If $k + i_{z-1} = j + i_z$ then $k - j = 1$ but k is a multiple of 2. If $k + i_{z-1} = 0 + i_z$ then $k = 1$. If $k + i_{z-1} = 0 + i_{z+1}$ then $j + i_{z+1}$ has nothing to cancel with. If $k + i_{z-1} = j + i_{z+1}$ then $k = 6$ but $0 + i_{z+1}$ has nothing to cancel with. These are all the possibilities since canceling down is impossible: $l + i_{z-2} < k + i_{z-1}$ and $m + i_{z-4} < k + i_{z-1} < m + i_{z-3}$.

Case IB2c: $0 + i_z = k + i_\beta$. First $\beta \geq 3$ and if $\beta > 3$ then $k + i_3$ must cancel down with $l + i_\gamma$. An adjusted (to take into account the extra $i_\gamma - i_3$ shift) application of Lemma 7.3 gives $t = z+1$ and $3j = l - k = i_{z+1} - i_z < i_{z+1} - i_{z-1} = m - l = 2j$. So $0 + i_z = k + i_3$ and $m - l = 2j = i_z - i_{z-1} < m - l$ which is a contradiction.

Case II: $m + i_y = k + i_\alpha$.

Here we break into two cases

Case IIA: $m + i_y = k + i_{z-1}$. We have $i_{z-1} = m - j$, $j + i_{z-1} = m + i_0$, $l - k + i_z - i_{y+1} = \delta \leq j$ and $l - k < j$. We condition on what $0 + i_{z-1}$ cancels with.

Case IIA1: $0 + i_{z-1} = l + i_\beta$. Lemma 7.3 gives that $i_{z+1} = i_t = m$, $i_{z+1} - i_{z-1} = m - l = j$, $0 + i_{z-1} = l + i_0$. The only available cancellation for $k + i_1$ is $0 + i_z$. We need to find something to cancel with $l + i_{z-1}$. Up with a k is the only possibility since $l + i_{z-1} > k + i_{z-1} = m + i_{z-2} > m + i_1 = j + i_t$. So $l + i_{z-1} = k + i_z$ and we get $2(l-k) = j$ which implies by the GCD condition $l - k = 1$ and so $j = 2$, $k = 2(y+1)$, $l = 2y+3$ and $m = 2y+5$.

If $y = 1$ then $fh = (1 + x^2 + x^4 + x^5 + x^7)(1 + x^2 + x^5 + x^6 + x^7 = 1 + x^8 + x^9 + x^{13} + x^{14}$ which is not a trinomial.

If $y > 1$, we look for what cancels with $k + i_{z-2}$. Nothing down is available since $l + i_{z-3} < k + i_{z-2} < m + i_{z-3} = l + i_{z-2}$ and if $z \geq 4$, $m + i_{z-4} = l + i_{z-3}$. The only things available above are $j + i_z$ and $j + i_t$. If $j + i_t = k + i_{z-2}$ then $k = j + (i_t + i_{z-2}) = j + (j + l - k + j) = 3j + 1 = 7$, but k should be even. If $j + i_z = k + i_{z-2}$, then $i_y = i_{z-2} = j - k + i_z = j - k + k + i_1 = j + i_1 = i_2$ which gives $t = 5$ which violates parity.

Case IIA2: $0 + i_{z-1} = k + i_\beta$. We have $\beta \geq 1$ but $l - k < j$ so $l + i_0$ has nothing to cancel with.

Case IIB: $m + i_y = k + i_\alpha$, $\alpha \geq z$. Again we condition on what cancels with $0 + i_{z-1}$.

Case IIB1: $0 + i_{z-1} = l + i_\beta$. Lemma 7.3 gives that $i_t = i_{z+1} = m$, $i_{z+1} - i_z = l - k$, $i_{z+1} - i_{z-1} = m - l$, $i_z - i_{z-2} = m - k$, and $0 + i_{z-1} = l + i_0$. Thus $l - k = j$ and $0 + i_{z-1} = k + i_1 = l + i_0$ but none of these can be left-over.

Case IIB2: $0 + i_{z-1} = k + i_\beta$. If $\beta > 1$ then $k + i_1 = l + i_0$, $l - k = j$ and so $k + i_\beta = l + i_{\beta-1}$ but there cannot be an m here (0 is not at the top because $z - 1 \neq t$) and j's below i_{z-1} are accounted for. Thus $\beta = 1$, $i_{z-1} = k + j$. Also $j \geq i_t - i_\alpha$. We break into two cases

Case IIB2a: $y \geq 2$. We have $j + i_{z-1} = k + i_2$ and examine what $0 + i_z$ cancels with. m is impossible by Lemma 7.1.

Case IIB2ai: $0 + i_z = l + i_\gamma$. Lemma 7.3 gives that $t \leq z + 2$. If equality holds then $i_{z+2} = m$, $i_{z+2} - i_z = m - l = l - k$,

$0+i_z = l+i_0$. We have $k+i_{z+1} = l+i_{z-1}$, so if $\alpha = z+1$, then $m+i_{z-2} = l+i_{z-1}$, and we are in case IA. So $m+i_{z-2} = k+i_z$ and $m-k = i_z - i_{z-2} = l-k+j$. Thus $l-k = m-l = j$, but now $0+i_z = l+i_0 = k+i_1 = 0+i_{z-1}$ and so $i_z = i_{z-1}$. We may assume $t = z+1$. If $\Omega = z-1$ then $0+i_z = l+i_0$, $m-l = l-k = i_{z+1}-i_z$, $i_{z+1} = m$. We have $m+i_{z-2} = k+i_z$ then $m-k = 2(l-k) = l-k+j$ and $l-k = m-l = j$ but then $i_z = i_{z-1}$.

Thus we may assume that $\Omega = z$. Again $m+i_{z-2} = k+i_z$ and $i_z = m-j$. If $\gamma > 0$ then $l+i_0$ cancels up with a k giving $l-k > j$ and $i_{z+1} = i_z+l-k > m$. So $0+i_z = l+i_0$. But now $l-k = i_{z+1}-i_z \leq m-m-j = j$ gives that $0+i_z = l+i_0 \leq k+i_0+j = k+i_1 = 0+i_{z-1}$ which is a contradiction.

Case IIB2aii: $0+i_z = k+i_\gamma$. Similarly to case IB2c, $\gamma > 3$ gives $t = z+1$, $3j = l-k = i_{z+1}-i_z < i_{z+1}-i_{z-1} = m-l$. We have $m+i_{z-2} = k+i_z$ and $m \geq i_{z+1}-i_z+i_z-i_{z-2}+i_{z-2}-i_0 = 3j+m-k+k-j = m+2j$. So $\gamma = 3$ and $0+i_z = k+i_3$. If $\alpha \leq t-2$ then $k+i_{t-1}$ must cancel up with $0+i_t$ or $j+i_t$ and $m \geq i_t - i_{t-1} + i_{t-1} - i_\alpha + i_\alpha - i_{z-2} + i_{z-2} - i_0 \geq k-j+(i_{t-1}-i_\alpha)+m-k+k-j > m$. So $m+i_{z-2} = k+i_{t-1}$ and $i_t - i_{t-1} \leq j$. Since $2j = i_z - i_{z-1} < m-l$, if $\Omega < t-1$ then $i_t - i_{t-1} = m-l > j$. So we have $\Omega = t-1$. General considerations give $l+i_{z-1} > m+i_{z-2} = k+i_{t-1}$ and so $l+i_{z-1}$ must cancel up with $\{j,0\}+i_t$. So $i_t - i_{z-1} \geq l-j$, $i_{z-1}-i_{z-2} = 2j$, $i_y = yj$. If $y > 2$ then $i_z - i_{z-1} = 2j$ (since $0+i_z = k+i_3$) and thus $4j = i_z - i_{z-2} > m-l$ and $m \geq i_t \geq (l-j)+2j+3j = l+4j > m$, a contradiction. Hence $y = 2$, $i_z - i_{z-1} = k = 3j$, and so $i_z - i_{z-2} = 5j$. Furthermore, $j \geq i_t - i_{t-1} = (k+i_t)-(k+i_{t-1}) = (l+i_z)-(m+i_{z-2}) = 5j-(m-l)$. We deduce $4j \leq m-l$ and the shifts above i_z alternate between $j \leq i_{z+1}-i_z = (m-l)-3j$ and $i_z - i_{z-1} = 3j$. In particular, since t and z are both even, $i_t - i_{t-1} = i_z - i_{z-1} = 3j$. But we also have $i_t - i_{t-1} = (l-k+i_z)-(m-k+i_{z-2}) = (i_z-i_{z-2})-(m-l) = 5j-(m-l)$ implying $m-l = 2j$ contrary to the earlier deduction $m-l \geq 4j$.

Case IIB2b: $y = 1$. We break into two cases depending on what cancels with $0+i_z$.

Case IIB2bi: $0+i_z \neq j+i_{z-1}$.)$+i_z$ cannot cancel down with an m, by Lemma 7.1. If $0+i_z = l+i_1$ then the contrapositive of Lemma 7.3 gives that $t = z+1 = 4$. If $\Omega = z$ then $fh = (1+x+x^2+x^4+x^5)(1+x+x^3+x^4+x^5) = 1+x^3+x^4+x^9+x^{10}$ which is not a trinomial. If $\Omega = z-1$ then $fh = (1+x+x^2+x^4+x^6)(1+x+x^3+x^5+x^7)$ which has $i_t > m$. So

$0 + i_z = l + i_0$, $3j < l$ and $j < l - k$. Lemma 7.3 gives that $t \le z + 2$ and parity forces $t = z + 1$, $m + i_{z-2} = k + i_z$ and $i_z = l = m - j$. But $m \ge i_{z+1} = i_z + l - k > m$.

Case IIB2bii: $0 + i_z = j + i_{z-1}$. We have $j = i_3 - i_2 < m - l < i_3 - i_1 = 3j$. If $\alpha \le t - 2$ then $m \ge i_t - i_{t-2} + i_{t-2} - i_\alpha + i_\alpha - i_1 + i_1 - i_0 \ge m - l + (i_{t-2} - i_\alpha) + m - k + j > m$, so $m + i_1 = k + i_{t-1}$.

If $i_t - i_{t-1} = m - l$ then $m \ge i_t - i_{t-1} + i_{t-1} - i_1 + i_1 - i_0 = m - l + m - k + k - j > m$. So $\Omega = t - 1$. Since t and $z + 1$ are even, $i_t - i_{t-1} = i_{z+1} - i_z = m - l - j$. $m \ge i_t - i_{t-1} + i_{t-1} - i_1 + i_1 - i_0 = m - l - j + m - k + k - j$ gives that $m - l \le 2j$. We also have that $m - l + l - k = m - k = i_{t-1} - i_{z-2} = i_{t-1} - i_z + i_z - i_{z-2} = i_{t-1} - i_z + 3j = l - k - (m - l - j) + 3j$ which gives $m - l = 2j$. Once again we have that $m + i_{z-2} = l + i_{z-1}$ which is Case IB1.

Case III: $m + i_y = j + i_\alpha$.

First, $j \ge l + i_z - m + i_y = k + i_t - (j + i_\alpha) \ge k + i_t - (j + i_t) \ge j$ which implies that $m + i_y = j + i_t$. Lemma 7.2 gives that $y = 1$, $z = 3$ $i_t = m$ and $\delta = j$ so $i_z - i_{z-2} = m - l + j$.

If $t \ge z + 2$ then there exists an $z \le \alpha \le t$ such that $i_t - i_\alpha = m - l$ and thus $0 + i_\alpha = l + i_0$. Further, we get that $j + i_\alpha = l + i_1$. Thus $0 + i_{z-1} = k + i_1$ implying that $i_{z-1} - i_{z-2} = 2j$ and thus $i_z - i_{z-1} = m - l - j$. So $j + i_{z-1}$ has nothing below to cancel with. Thus $j + i_{z-1} = 0 + i_z$ and $m - l = 2j$.

So $m + i_{z-2} = l + i_{z-1} = j + i_t$. Since none of these is left-over, there must be a k in this column. But $k + i_\alpha = 0 + i_t < j + i_t$ implying that $\alpha = t - 2$. This in turn gives that $0 + i_t = j + i_{t-2} = l + i_1$ which is a contradiction.

We now know that $t = z + 1 = 4$. If $\Omega = z - 1$ then $0 + i_z = l + i_0$ and $j + i_z = l + i_1$ which forces $0 + i_2 = k + i_1$. We have found cancellations for all except $k + i_3$, $j + i_2$, $k + i_2$ and $l + i_2$ but clearly at least two of these must be left-over which is a contradiction.

Finally we know that $\Omega = z$. This implies that $i_1 = j$, $i_2 = l$, $i_3 = k + j$ and $i_4 = m$. But we also have that $m - l = 2(l - k)$ which implies $k - j = l - k = j$ and the contradiction now that $i_2 = i_3$.

8.10 2.3/5

If $y \le z - 2$, then $m \ge i_t \ge i_t - i_z + i_z - i_{z-2} + i_{z-2} - i_y + i_y \ge (l - k) + (m - l) + i_{z-2} - i_y + k \ge m$. So $y \ge z - 1$.

If $y \ge z + 2$, then $i_x - i_{x-1} = j$ for $1 \le x \le y - 1$ implies that $i_x - i_{x-2} = 2j$ for $1 \le x \le z + 1$. In particular, $i_{z+1} - i_{z-1} = m - l = 2j$. (Indeed, if $\Omega = z - 1$, then $i_{z+1} - i_z = m - l = j$ and thus $m + i_{z-1} = l + i_z = k + i_t$, a contradiction. Hence $\Omega > z - 1$ and thus $i_{z+1} - i_{z-1} = m - l = 2j$.) Consider z: we have either $z \ge 2$ or $z = 1$. When $z \ge 2$, we have $k + i_t = l + i_z = m + i_{z-2}$, a contradiction. Let $z = 1$. If $\Omega = z - 1$, then $m - l = i_{z+1} - i_z = j$ and thus $k + i_t = l + i_1 = m + i_0$, a contradiction. If $\Omega = t - 1$, then $i_{y-1} - i_{y-3} = m - l = 2j$ but $i_y - i_{y-2} = m - l <$

$2j$, a contradiction. If $z-1 < \Omega < t-1$, then from $m-l = i_{z+1} - i_{z-1} = 2j$ and $i_{z+1} - i_z = j$ we have that $l-k = (i_t - i_{z+1}) + i_{z+1} - i_z$ is a multiple of j. This means that each shift above i_z is either j or $2j$, contradicting to $i_y - i_{y-1} < j$. Hence $y \leq z+1$.

8.10.1 $y = z - 1$

Case I: $\Omega = z - 1$.

We observe that $z-1 \geq 2$ (i.e., $z \geq 3$) and $j + i_{z-1} = k + i_1$. We have $i_{z-1} - i_{z-2} \leq k - j$.

We note that $l + i_{z-1}$ can only be canceled with $0 + i_t$, $j + i_t$, or $m + i_{z-2}$. Indeed, because $m - l = i_t - i_{t-1}$, $k + i_{t-1} = l + i_z - (m-l) < l + i_{z-1}$, $k + i_{t-1}$ must be to the right of $l + i_{z-1}$. If $l + i_{z-1} = 0 + i_t$, then $m + i_{z-2} = j + i_t$. Then $i_{z-1} - i_{z-2} = m + i_{z-1} - (m + i_{z-2}) > k - j$ because $m + i_{z-1}$ is to the left of $k + i_t$, a contradiction. If $l + i_{z-1} = j + i_t$, then either $m + i_{z-2}$ is a left-over or $i_{z-1} - i_{z-2} = m + i_{z-1} - (m + i_{z-2}) > k - j$, a contradiction.

Let $l + i_{z-1} = m + i_{z-2}$. Since $m - l = i_{z-1} - i_{z-2} < j$, $m + i_{z-3} = m - l + l + i_{z-3} < j + l + i_{z-3} = i_{z-2} - i_{z-3} + l + i_{z-3} = l + i_{z-2}$ and thus $m + i_{z-3}$ is to the right of $l + i_{z-2}$. Since $k + i_{t-1}$ is to the left of $l + i_{z-2}$, $j + i_t$ must be to the left of $l + i_{z-2}$ and $j + i_t = k + i_{t-1}$. Hence $k - j = i_t - i_{t-1} = m - l < j$. If $z \geq 4$, then $k - j = i_{z-1} - i_1 > j$, a contradiction.

Let $z = 3$; we split the analysis into 2 cases:

Case IA: Assume $t = 4$. In this case we have $m - l = l - k = i_t - i_{t-1}$ and $i_{z-1} - i_{z-2} = m - l = i_y - i_1 = k - j$. Hence $m - l = l - k = k - j < j$. Then $0 + i_z = j + i_{z-2}$. Moreover, $0 + i_t$ must be canceled with $l + i_0$ and $j + i_{t-1}$ must be canceled with $m + i_0$. In this case, we obtain $m = 3j$, $l = \frac{5j}{2}$, and $k = 2j$. This contradicts to $k - j < j$.

Case IB: Assume $t > 4$. Since $l + i_z < m + i_{z-1}$, we have $i_z - i_{z-1} < m - l < l - k = i_t - i_z$. So $0 + i_z < l - k + i_{z-1} = l - k + i_y = l + i_0$ and thus $0 + i_z$ is to the right of $l + i_0$. We have $0 + i_z = j + i_{z-2} = j + i_1$. Again, $m - l = k - j = i_{z-1} - i_{z-2} < j$. Therefore $i_{z+1} - i_z = m - l = k - j$. Now, since $i_z - i_{z-2} = j$ and $i_{z-1} - i_{z-2} = i_{z+1} - i_z = m - l$, we have $0 + i_{z+1} = j + i_{z-1} = k + i_{z-2}$. Moreover, $l + i_0$ must be in that column or we have too many left-overs, thus $l + i_0 = 0 + i_{z+1} = j + i_{z-1} = k + i_{z-2}$. Hence $l - k = i_z - i_{z-2} = j$, so $j = k + i_{z-2} - i_{z-1} = m - l + j + i_{z-2} - i_{z-1} = m - l + i_z - i_{z-1} < 2(m-l)$. We now have $l + i_{z-2} = k + i_z = j + i_{z+1}$ and they are to the left of $m + i_0$ and $j + i_z = 0 + i_t$, a contradiction.

Case II: $t - 1 > \Omega \geq z$.

If $m - l < j$, then $0 + i_{z+1}$ is a left-over because $l - k > m - l$ and $j + i_{y-1} = 0 + i_z$, a contradiction. Hence $m - l \geq j$. We observe that $j + i_{z-1} = k + i_1$ and $m + i_{z-2} = j + i_t$ (because $k + i_{t-1}$ is to the right of $m + i_{z-2}$). If $z > 3$, then $k - j = i_{z-1} - i_1 > j$. This contradicts to $k - j < m + i_{z-1} - (m + i_{z-2}) = i_y - i_{y-1} < j$. If $z = 3$, then $k - j = i_2 - i_1$

which contradicts to $k - j < m + i_{z-1} - (m + i_{z-2}) = i_2 - i_1$.

Case III: $\Omega = t - 1$. We consider two cases.

Case IIIA: Assume $t > z + 1$. Then $l - k \geq m - l$. Let $m - l < j$. If $l - k > m - l = i_{z+1} - i_{z-1}$, then $0 + i_{z+1}$ is a left-over, a contradiction. If $l - k = m - l$, then $t = z + 2$ and $m - k > i_t - i_{z-1}$ implies that $m + i_0$ is to the left of $0 + i_t$. Moreover, $l + i_0 = 0 + i_{z+1}$, $j + i_{z-1} = l + i_0$, and $l - k = m - l < j$ imply that $0 + i_{z+2}$ is a left-over, a contradiction.

Let $m - l \geq j$. Then $l - k \geq m - l \geq j$. Since $j + i_{z-2} = 0 + i_z$, we have $m + i_{z-2} > l + i_z = k + i_t$. Then $m + i_{z-2}$ is another left-over, a contradiction.

Case IIIA: Assume $t = z + 1$. Then $l - k < m - l$. If $m - l < j$, then $0 + i_{z+1} = j + i_{z-2}$ and $0 + i_z = l + i_0$ (if $0 + i_{z+1} = l + i_0$ and $0 + i_z = j + i_{z-2}$, then $l - k = i_{z+1} - i_{z-1} > i_{z+1} - i_z = l - k$, a contradiction). Since $m - l < j$, $m + i_0 < l + j = l + i_1$. Also, $0 + i_z = l + i_0$ implies $l + i_1 = j + i_z$ and thus $m + i_0$ is to the right of $l + i_1 = j + i_z$. If $z > 3$, then $m + i_0$ must be a left-over because $l - k < m - l < j$. If $z = 3$, then $m + i_0 = k + i_{z-1} = k + i_2$. In this case, $m + i_1 \neq j + i_4$ because $m + i_2 - (m + i_1) = k - j$. If $m + i_1 = l + i_2$, then $j + i_4 = k + i_3$ and thus $k - j = l - k$. Therefore $m - l = k - j = l - k$ which contradicts to $l - k < m - l$. If $m + i_1 = k + i_3$, then $m - k = l - j$. Hence $i_3 - i_2 = l - (m - k) = j$, contradicts to $i_3 - i_2 < i_4 - i_1 < j$.

Now we assume that $m - l \geq j$. In this case, we have $m + i_{z-2} = k + i_{t-1}$ (otherwise, $k - j < i_{z-1} - i_{z-2}$). If $j + i_{z-2} = 0 + i_z$, then $m - k = j$, a contradiction to $m - l \geq j$. Hence we have $j + i_{z-2} = l + i_0$. Now, $0 + i_z$ cancels either with $l + i_1$ or $k + i_2$. In the former case, $i_z = l + i_1 = l + j$ and $j + i_{z-2} = l + i_0$ imply that $m - k = i_z - i_{z-2} = 2j$. Because $i_y - i_{y-1} = 2(l - k)$ and $j = i_y - i_{y-1} + l - k$, we have $l - k = j/3$ and thus $i_y - i_{y-1} = 2j/3$, $i_z - i_{z-1} = 4j/3$. Moreover, $m - l = 5j/3$, $m - k = 2j$, and $m + i_0$ is to the left of $0 + i_t$. Because $y \geq 2$, $k + i_2$ is always a left-over, a contradiction. In the latter case, that is, $0 + i_z = k + i_2$, we first consider $z \geq 4$. Since $0 + i_z = k + i_2$, we have $i_z - i_{z-1} = 2j$. Moreover, $m + i_0$ is to the left of $0 + i_t$. Therefore $l - k = j/3 < j$ implies that $l + i_1$ must be a left-over. If $z = 3$, then $0 + i_3 = k + i_2$ and $j + i_2 = k + i_1$. Moreover, $l - j = j$ means $l = 2j$. Then $i_4 - i_2 = l - k + k = l = 2j$. So $i_4 - i_1 > 2j$. So $l + i_1$ is to the right of $0 + i_4$. Again, $m + i_0$ is to the left of $0 + i_t$. Furthermore, $l - k = j/3 < j$ implies that $j + i_3$ is also to the left of $0 + i_z$. We have that $l + i_1$ is a left-over, a contradiction.

8.10.2 $y = z$

Case I: $\Omega = z - 1$. If $t = z + 1$, then $l - k = m - l$ and thus $0 + i_t = l + i_0$. We have that $j + i_{z-1}$ is to the right of $k + i_1$. Hence $j + i_{z-1}$ is a left-over. Now assume $t > z + 1$. Again we have $0 + i_t = l + i_0$. Since $j + i_z = k + i_1$, we have $j + i_{z-1} = 0 + i_{z+1}$ and $j = (i_{z+1} - i_z) + (i_z - i_{z-1}) = (m - l) + (i_z - i_{z-1})$. So

$m - l < j$ and thus $l + i_{z-1} = j + i_t$. That is, $z = 2$. So $m + i_0$ must cancel up with $k + i_{t-1}$ and we also have $j + i_2 = k + i_1$. Because $k - j = i_2 - i_1 < m - l$, $j + i_{t-1}$ must be a left-over.

Case II: $t - 1 > \Omega \geq z$. In this case, we also have $0 + i_t = l + i_0$ and $j + i_t = l + i_1$. We must have $0 + i_{z+1} = j + i_{z-1}$ and thus $j = m - l$. So $l + i_{z-1} = m + i_{z-2}$ and all the way down to $l + i_1 = m + i_0$. If $z \geq 3$, then $k + i_{t-1}$ must be a left-over because it is to the left of $j + i_t = l + i_1$. If $z = 2$, then $j + i_t = l + i_{z-1} = m + i_0$ gives a left-over.

Case III: $\Omega = t - 1$.

If $\Omega = z$, then $j + i_{z-1} = m + i_0$ because $0 + i_t = 0 + i_{z+1} = l + i_0$ and $0 + i_z = k + i_0$. Since $m - l < m - k < j$, we can only have 4 rows in total. This contradicts to the parity.

If $\Omega = z + 1$, then we have $l - k = m - l$. Since $0 + i_{z+2} = l + i_0$ and $k + i_{z+1} = l + i_{z-1}$, we have $0 + i_{z+1} = j + i_{z-1}$ and thus $m - l = j$. This implies that $z = 2$. Hence we have the polynomial exception 13: $f(x) = x^7 + x^5 + x^3 + x^2 + 1$ and $h(x) = x^5 + x^4 + x^3 + x^2 + 1$.

If $\Omega > z + 1$, then we have $m - l = i_{z+1} - i_{z-1} = j$. Hence $0 + i_{z+2} = j + i_z = k + i_1$ gives a left-over.

8.10.3 $y = z + 1$

Case I: $\Omega = z - 1$. In this case, $i_{z+1} - i_z = m - l < j$ contradicts to $i_z - i_{z-1} = j < m - l$.

Case II: $t - 1 > \Omega \geq z$. we consider two cases:

Case IIA: $\Omega = z$. We have $j < m - l < 2j$. If $t = z + 1$, then we have $z = 1$ and the polynomial exception 11: $f = x^7 + x^4 + x^3 + x^2 + 1$ and $h = x^3 + x^2 + 1$. Assume $t > z + 1$. Because $0 + i_t$ is to the right of $l + i_0$, 0's and j's from row i_{z+1} to row i_{t-1} must be canceled down with k's except $0 + i_{z+2} = j + i_z$. Therefore $z > 2$. Since $m + i_{z-2}$ is to the left of $l + i_{z-1}$ and $k + i_{t-1}$, $m + i_{z-2} = j + i_t$. Also $l + i_{z-1}$ is to the left of $m + i_{t-3}$ and $k + i_{t-1}$, then $l + i_{z-1} = 0 + i_t$. Hence $i_z - i_{z-1} = (i_t - i_{z-1}) - (i_t - i_z) = l - (l - k) = k$ and also $i_z - i_{z-1} = j$. Therefore $k = j$, a contradiction.

Case IIB: $t - 1 > \Omega > z$. In this case, $m - l > j$. If $z \geq 2$, then $m + i_{z-2} = j + i_t$. Since $m - l < 2j$, we must have $0 + i_t = l + i_{z-1}$. Hence we have again $k - 0 = j$, a contradiction. If $z = 1$, then $j + i_t$ must be a left-over because $m - l > j > k - j$.

Case III: $\Omega = t - 1$. Note $m - l = i_{z+1} - i_{z-1} = i_y - i_{z-1} < 2j$. If $t = z + 1$ and $z > 1$, then $j + i_z = l + i_0$ and thus $l + i_1$ is a left-over because $j + i_t = k + i_1$, $0 + i_t = k + i_0$, $m - l > j$ and $l - k < j$. If $t > z + 1$, then $0 + i_{z+2} = j + i_z$ and thus $m - l = i_{z+2} - i_z = j$. This contradicts to $m - l = i_{z+1} - i_{z-1} > j$.

8.11 Case 3.1/4:

If $z \leq y - 2$ and $y = t$ then all shifts are a constant, j and this has been dealt with previously. If $z \leq y - 2$ and $y < t$ then $m - l = i_{y+1} - i_y > j$ and

$m - l = i_y - i_{y-1} = j$ which is a contradiction. So we have that $z \geq y - 1$. However if $z \geq y+1$ then $m \geq i_t = i_t - i_B + i_B - i_z + i_z - i_{y+1} + i_{y+1} - i_y + i_y - i_0 = (i_t - i_B) + m - A + (i_z - i_{y+1}) + (i_{y+1} - i_y) + k - j > (i_t - i_B) + m - k + (i_z - i_{y+1}) + j + k - j \geq m$. So we have that $z \leq y \leq z + 1$.

8.11.1 Assume $y = z$.

Since $m \geq i_t = i_t - i_{t-1} + i_{t-1} - i_B + i_B - i_z + i_z - i_0 \geq m - l + (i_{t-1} - i_B) + m - k + k - j = m - l + (i_{t-1} - i_B) + m - j$, we have a contradiction if $t > B$ and $m - l > j$. If $t = B$ then $A = 0$ or j (recall that subcase 3.1 assumes that $y + i_t$ is left-over). In the former $0 = z = y > 0$. In the latter, Lemma 7.2 gives that $z = 1$, $i_t - i_z = i_t - i_1 = m - j$, and $k = 2j$. We have $t \geq z + 2 = 3$ and since t must be even, $t \geq 4$ and $j + i_t = m + i_1$, $0 + i_t = m + i_0$, $j + i_{t-1} = l + i_1$, $0 + i_{t-1} = l + i_0$. Additionally we have that $m - l \geq i_2 - i_1 > j$ so $m + i_2 = m + i_1 + i_2 - i_1 > m + i_1 + j = j + i_t + j = k + i_t$. Also $l + i_2 > l + i_1 = j + i_{t-1}$ cannot be left-over so it must cancel up with $k + i_{t-1}$. This gives $j < i_2 - i_1 = l + i_2 - (l + i_1) = k + i_{t-1} - (j + i_{t-1}) = k - j = j$. So we can assume that $t > B$ and thus $m - l \leq j$. But this contradicts the fact that $j \geq m - l \geq i_{z+1} - i_z = i_{y+1} - i_y > j$.

8.11.2 Assume $y = z + 1$.

We have $m - l = i_{z+2} - i_{z+1} = i_{y+1} - i_y > j$. If $B \leq t - 2$ then $m \geq i_t - i_B + i_B - i_z + i_z - i_{z+1} + i_{z+1} - i_0 \geq 2(m - l) + m - A - (i_{z+1} - i_z) + k - j = 2(m - l) + m - A - j + k - j > 2j + m - k - j + k - j = m$, so $B \geq t - 1$.

<u>Case I: $B = t$.</u> If $A = 0$, then Lemma 7.1 implies that $i_z = i_0$, $k = 2j$, $j + i_t = k + i_t - j > k + i_t - (m - l) = k + i_{t-1}$. So $j + i_t = m + i_1 = l + i_2$ and nothing else is in this column but none of these is left-over. Thus we have $A = j$ and $z = 0$ or 1.

If $z = 1$ we have that $j + i_t = m + i_1$, $0 + i_t = m + i_0$, $j + i_{t-1} = l + i_1$, $0 + i_{t-1} = l + i_0$ and $k = 3j$. We have that $l + i_2$ must cancel but there is nothing available below it. There are no 0 or j for it to cancel up with so it must cancel up with a k. We have $k + i_{t-1} = j + i_{t-1} + 2j = l + i_1 + 2j > l + i_1 = j + i_{t-1} = j + i_{t-3} + 2(m - l) > j + i_{t-3} + 2j = k + i_{t-3}$. So $l + i_2 = k + i_{t-2}$ and this implies that $k + i_{t-1} = m + i_2 = l + i_3$ and nothing else is in this column. But none of these can be left-over.

So we can assume that $z = 0$, $k = 2j$ and thus $k + i_t = m + i_1$. But we know that $k + i_t$ is left-over so $m + i_1 = l + i_2$. Also we have $k + i_{t-1} = l + i_1$, $j + i_{t-1} = l + i_0$ and $0 + i_t = j + i_t - j = j + i_{t-1} + (m - l) - j > j + i_{t-1}$. We have $0 + i_t = 0 + i_{t-2} + 2(m - l) > k + i_{t-2}$ which shows that there is nothing for $0 + i_t$ to cancel with and it cannot be left-over.

<u>Case II: $B = t - 1$.</u>

If $A = 0$ then $i_{t-1} = i_B$ which forces $i_{t-1} = i_t$, a contradiction. If $A = j$ then $m \geq i_t - i_{t-1} + i_{t-1} - i_z + i_z = m - l + m - j + i_z > m$ so $A = k$. Now $m \geq i_t = m - l + m - k + k - 2j$ so $m - l \leq 2j$ If $t - 2 \geq z + 2$ then $l + i_{z+1} > l + i_z = k + i_{t-2}$. If $z \geq 1$ then $l + i_{z+1} = m + i_{z+1} - (m - l) =$

$m + i_{z-1} + 2j - (m - l) \geq m + i_{z-1}$. Since $l + i_{z+1}$ cannot be left-over we must have it canceling down with $m + i_{z-1}$ or up with a 0 or j in row t or $t - 1$.

Case IIA: $l + i_{z+1} = m + i_{z-1}$. We have $m - l = 2j$ and $m = m - k + k = i_{t-1} - i_z + k = i_{t-1} - i_{z+1} + i_{z+1} - i_z + k = (t-1-z-1)(m-l) + j + k = (t - z - 2)(2j) + j + (z + 2)j = (2t - z - 1)j$. The GCD condition gives that $j = 1$, $k = z + 2$, $l = 2t - z - 3$ and $m = 2t - z - 1$. We can also calculate that $i_t = (t - z - 1)(m - l) + (z + 1)j = 2t - z - 1 = m$. This gives $j + i_t = m + i_1$, $0 + i_t = m + i_0$, $j + i_{t-1} = l + i_1$ and $0 + i_{t-1} = l + i_0$. Since $t \geq z + 3$, if we have $z \geq 2$ then $k + i_{t-2} = l + i_z = m + i_{z-2}$ but none of these is left-over so they cancel with a 0 or j in row t or $t - 1$. The cancellation of 0 and j in rows t and $t-1$ has already been accounted for so we can conclude that $z = 1$. Here $0 + i_{z+3} = 0 + i_4 = 6$ must cancel down with an l or m. The parity of l and m are even and so we get $f = 1+x+x^3+x^4+x^6$, $h = 1+x+x^2+x^4+x^6$ or $f = 1+x+x^3+x^6+x^8$, $h = 1 + x + x^2 + x^4 + x^6 + x^8$. In neither case is $g = fh$ a trinomial.

Case IIB: $l + i_{z+1} = 0 + i_{t-1}$. This case is impossible since $m \geq i_t = i_t - i_{t-1} + i_{t-1} - i_{z+1} + i_{z+1} \geq m - l + l - 0 + j > m$.

Case IIC: $l + i_{z+1} = j + i_{t-1}$. Here we must have that $m = i_t$ and $z = 0$. Thus $0 + i_t = k + i_{t-1} = m + i_0$ but there is nothing else to cancel in this column and none of these is left-over.

Case IID: $l + i_{z+1} = 0 + i_t$. What does $j + i_t$ cancel with? Not an l since $l + i_{z+1} = 0 + i_t < 0 + i_t + j = l + i_{z+1} + j = l + i_{z+2} - (m - l) + j < l + i_{z+2}$ thus $j + i_t$ is to the left of $l + i_{z+2}$ and all other l's are accounted for. Not a k since $k + i_{t-1}$ already cancels with $m + i_z$ and $k + i_{t-2} = k + i_{t-1} - (m - l) = m + i_z - (m - l) = m + i_{z+1} - j - (m - l) = l + i_{z+1} + m - l - j - (m - l) < l + i_{z+1} = 0 + i_t < j + i_t$ if $t \geq z + 4$ and $k + i_{t-2} = k + i_{z+1} < l + i_{z+1} = 0 + i_t < j + i_t$ if $t = z + 3$ (Note $t \geq z + 3$ since $m + i_z = k + i_{t-1} > l + i_{z+1}$). So the only remaining possibility for $j + i_t$ to cancel with is m. But $m + i_z$ already cancels with $k + i_{t-1}$ and $m + i_{z-1} = m + i_{z+1} - 2j = l + i_{z+1} + m - l - 2j \leq l + i_{z+1} = 0 + i_t < j + i_t$. So $j + i_t$ is left-over which is a contradiction.

Case IIE: $l + i_{z+1} = j + i_t$. Here we have $0 + i_t = l + i_z$ and $2(m - l) = k + i_t - (k + i_{t-1}) + m + i_z - (l + i_z) = k + i_t - (k + i_{t-1}) + k + i_{t-1} - (0 + i_t) = k$. So $k = 3j$ or $4j$ (k = 2j implies that all shifts are a constant, $m - l$ which has been dealt with before).

Case IIE1: $k = 3j$. We have $z = 1$, $m - l = 3j/2$, $m - k = i_{t-1} - i_1 = (t - 1 - 2)(m - l) + j = (3t - 7)j/2$ and the GCD condition gives that $j = 2$, $k = 6$, $l = 3t - 4$ and $m = 3t - 1$. What does $0 + i_{z+2} = 7$ cancel down with? The only possibility is that $l + i_0 = 7$ but this violates the fact that $l \equiv 2 \bmod 3$.

Case IIE2: $k = 4j$. We have $z = 2$, $m - l = 2j$, $m - k = i_{t-1} - i_2 = (t - 1 - 2 - 1)(m - l) + j = (t - 4)(2j) + j = (2t - 7)j$ and the GCD condition gives $j = 1$, $k = 4$, $l = 2t - 5$ and $m = 2t - 3$. Since $t \geq z + 3$ because $l + i_{z+1} \leq m + i_z = k + i_{t-1}$, parity gives $t \geq 6$. We ask what $j + i_{z+3} = j + 7j = 8$ cancels with. Since $t \geq z + 4$, then $j + i_{z+3} < 2j + i_{z+3} = 0 + i_{z+4}$. The fact that $k + i_{z+1} < j + i_{z+3} < k + i_{z+2}$ means it must cancel down with an l or m in row 0 or 1. Since $j + i_{z+3}$ is even and $l + i_0$ and $m + i_0$ are odd, it must cancel in row 1. We get either $f = 1 + x^1 + x^4 + x^5 + x^7$ and $h = 1 + x + x^2 + x^3 + x^5 + x^7$ or $f = 1 + x + x^4 + x^7 + x^9$ and $h = 1 + x + x^2 + x^3 + x^5 + x^7 + x^9$. In neither case is $g = fh$ a trinomial.

8.12 Case 3.1/5:

We have $i_t - i_z \geq i_B - i_z = m - A \geq m - k$, but we cannot have equality all the way through or else we are in Subcase 1.1. Now $m = (m - k) + k < (i_t - i_z) + i_y \leq m - i_z + i_y$ and hence $z \leq y - 1$.

Now suppose $z \leq y - 2$, i.e. $y \geq z + 2$. Recall that

$$i_x - i_{x-1} = \begin{cases} m - l & \text{if } y \leq x \leq t, \\ j & \text{if } 1 \leq x \leq y - 1. \end{cases}$$

Then $m - l \geq i_{z+1} - i_z = j > i_y - i_{y-1} = m - l$, a clear contradiction. We conclude that $y = z+1$. Also note that for Case 5, $y \geq 2$ and hence $1 \leq z \leq t-2$ implies that $t \geq 3$. Since t must be even, $t \geq 4$.

8.12.1 Assume $A = 0$.

We have $m \geq i_B - i_0 \geq i_B - i_z = m - 0$. This implies that $i_z = 0$ which is a contradiction with $z \geq 1$.

8.12.2 Assume $A = j$.

Then $m = (m - j) + j = (i_B - i_z) + i_1 \leq m + i_1 - i_z$ which implies $i_z \leq i_1$. But $z \geq 1$, so we have equality throughout and so $m = i_t = i_B$, $z = 1$, $y = 2$. Consider $m = (i_t - i_{t-1}) + (i_{t-1} - i_2) + i_2 = (m - l) + (i_{t-1} - i_2) + k$ and so $l + i_2 = k + i_{t-1}$. Now $k + i_t = k + i_{t-1} + i_t - i_{t-1} = l + i_2 + m - l = m + i_2$. Thus $k + i_t$ cancels with $m + i_2$ and we are in case 1 or 2.

8.12.3 Assume $A = k$.

If $B = t$ then we are in case 1.1/5, so $t - B \geq 1$. Now $i_t \leq m = m - k + k = i_B - i_z + i_{z+1}$. Hence $i_t - i_B \leq i_{z+1} - i_z$. From this we conclude that $m - l \leq (t - B)(m - l) = i_t - i_B \leq i_{z+1} - i_z < m - l$, a contradiction.

8.13 Case 3.2:

We prove this case by reduction to either Subcase 1.1 or Subcase 2.1. Let us recall that in this case $k + i_t$ is left-over. The starting point is $A + i_B = l + i_z$ where A is the highest $0, j, k$ that cancels with an l, and B is its row. We have

$$\begin{aligned} l + i_{z+t-B} &= (l + i_z) + (i_{z+t-B} - i_z) = (A + i_B) + (t - B)(m - l) \\ &= (A + i_B) + (i_t - i_B) = A + i_t. \end{aligned}$$

By the choice of B maximal, $B = t$. The case $A = k$ is dealt with in Subcase 2.1.

Assume $A = j$.
Now $l = (l - j) + j = (i_t - i_z) + i_1$ implying $m - l \geq i_t - (i_t - i_z + i_1) = i_z - i_1$. Recall $i_z - i_{z-1} > m - l$ for Subcase 3.2, and so if $z \geq 2$ then $m - l \geq i_z - i_1 \geq i_z - i_{z-1} > m - l$, a contradiction. If $z = 0$ then all shifts are the same and this was dealt with elsewhere. Thus $z = 1$ and $i_2 - i_1 = i_{z+1} - i_z = m - l$.

For either Case 4 or 5, if $y \geq 3$ then $m - l = i_2 - i_1 = j$ and actually all shifts are $j = m - l$, which has already been considered.

Case I: 3.2/4. If $y = 2$, then all shifts are $j = m - l$ which was dealt with elsewhere. If $y = z = 1$, then $m - l < i_z - i_{z-1} = i_y - i_{y-1} = j$ but $m - l = i_{z+1} - i_z = i_{y+1} - i_y > j$ and we have another contradiction. Case 4 implies that $y \geq 1$ so this exhausts the possibilities.

Case II: 3.2/5.

In Case 5, $y \geq 2$ and so $y = 2$. We have $i_2 = k, i_1 = j$ so $k - j = i_2 - i_1 = m - l$. However $k + i_t = (k - j) + (j + i_t) = (m - l) + (l + i_z) = m + i_z$ and we are in Subcase 1.1.

Assume $A = 0$.
In this case $l = i_t - i_z$, and hence we have

$$m = (m - l) + l < (i_z - i_{z-1}) + (i_t - i_z) \leq m - i_{z-1}$$

implying $i_{z-1} < 0$ which is a contradiction.
End of Proof of Theorem 1.2! □