The exact bounds for the degree of commutativity of a $p$-group of maximal class, I

Antonio Vera-López, a,∗ J.M. Arregi, a M.A. García-Sánchez, a
F.J. Vera-López, b and R. Esteban-Romero c, 1

a Departamento de Matemáticas—Matematika Saila, Facultad de Ciencias—Zientzi Fakultatea, Universidad del País Vasco—Euskal Herriko Unibertsitatea, Apdo. 644, 48080 Bilbao, Spain
b Departamento de Matemática Aplicada y Estadística, Facultad de Informática, Campus de Espinardo, Universidad de Murcia, Murcia, Spain
c Departament d’Àlgebra, Facultat de Matemàtiques, Universitat de València, 46100 Burjassot, València, Spain

Received 9 May 2000
Communicated by Efim Zelmanov

Abstract

The first major study of $p$-groups of maximal class was made by Blackburn in 1958. He showed that an important invariant of these groups is the ‘degree of commutativity.’ Recently (1995) Fernández-Alcober proved a best possible inequality for the degree of commutativity in terms of the order of the group. Recent computations for primes up to 43 show that sharper results can be obtained when an additional invariant is considered. A series of conjectures about this for all primes have been recorded in [A. Vera-López et al., preprint]. In this paper, we prove two of these conjectures.

© 2002 Elsevier Science (USA). All rights reserved.

∗ This work has been supported by the DGICYT Grant PB97-0604 and by the University of the Basque Country.
∗ Corresponding author.
1 Supported by a Grant from the Generalitat Valenciana (Valencian Government).
1. Introduction

A group $G$ of order $p^m$ is said to be a $p$-group of maximal class if $Y_{m-1} \neq 1$, where

$$Y_0 = G, \quad Y_i = \underbrace{[G, \ldots, G]}_i$$

and $Y_1$ such that $Y_1/Y_4 = C_G/Y_4(Y_2/Y_4)$.

If $G$ is a $p$-group of maximal class, then $Y_i = 1$ for $i \geq m$ and $|Y_i : Y_{i+1}| = p$
for $i \in \{0, \ldots, m-1\}$.

The most important invariant of a $p$-group of maximal class $G$ is its degree of
commutativity, which is a measure of the commutativity among the members of
the lower central series of $G$. It was introduced by Blackburn (cf. [1]) and it is defined by

$$c = c(G) = \max\{k \leq m - 2 \mid [Y_i, Y_j] \leq Y_{i+j+k}, \forall i, j \geq 1\}.$$ 

We denote by $c_0$ the residue class of $c$ modulo $p - 1$ and $c_1$ is defined by
$c = c_1(p - 1) + c_0$. Another important invariant associated to a $p$-group of
maximal class is defined by

$$v = v(G) = \min\{k \in [2, m - c - 2] \mid [Y_1, Y_k] = Y_{1+k+c}\}.$$ 

In [4], it is proved that $v = v(G)$ is an even number $2l$ satisfying $v = 2l \leq p - 1$
and if $v + 2 = 2l + 2 \leq m - c - 1$, then $2l \leq p - 3$. Therefore, in the following,
we suppose $l \leq (p - 3)/2$.

Following N. Blackburn, we take a pair of elements $s \in G \setminus (Y_i \cup C_G(Y_{m-2}))$
and $s_1 \in Y_1 \setminus Y_2$, and define recursively $s_i = [s_{i-1}, s] \in Y_i \setminus Y_{i+1}$, for $i = 2, \ldots, m - 1$. For $i + j \leq m - c - 1$, let $\alpha_{i,j} \in \mathbb{F}_p$ be determined by the congruence

$$[s_i, s_j] \equiv s_{i+j+c}^{\alpha_{i,j}} \pmod{Y_{i+j+c+1}}.$$ 

It is known that $\alpha_{i,j}$ satisfies the following properties:

(P1) $\alpha_{i,j} = -\alpha_{j,i}$;
(P2) $\alpha_{i,i} = 0$, for $2i \leq m - c - 1$;
(P3) $\alpha_{i,j} = \alpha_{i+1,j} + \alpha_{i,j+1}$, for $i + j + 1 \leq m - c - 1$ (Bernoulli’s property);
(P4) $\alpha_{i,j} = \alpha_{i+p-1,j} + \alpha_{i,j+p-1}$, for $i + j + p - 1 \leq m - c - 1$ (periodicity
modulo $p - 1$);
(P5) $f(i, j, k) = \alpha_{i,j} \alpha_{i+j+c,k} + \alpha_{j,k} \alpha_{j+k+c,i} + \alpha_{k,i} \alpha_{k+i+c,j} = 0$, for any positive
integers $i, j, k$ satisfying $i + j + k \leq m - 2c - 1$ (Jacobi’s identity).

In this paper, we denote $x_\lambda = \alpha_{\lambda,\lambda+1}$, with $\lambda \geq 1$ and $y_j = \alpha_{1,2j+1}$, for $j \geq 0$.

By using $x_\lambda$, it is easy to check the following equality for $l$:

$$l = l(G) = \min\{k \in \{1, \ldots, (p - 3)/2\} \mid x_k \neq 0\}.$$
Moreover, if \( t \) is a positive integer such that \( t \leq m - 2c - 1 \), then \( S(t) \) denotes the system

\[
S(t) = \{ f(i, j, k) = 0 \mid i + j + k \leq t \}.
\]

For a positive integer \( t_1 \), we define \( T_{t_1} = \{ \alpha_{i,j} \mid i + j \leq t_1 \} \) and \( T_G = T_{m-c-1} \).

If we are interested in obtaining the defining relations of a \( p \)-group of maximal class, we need the best information about the degree of commutativity, because an improvement of only one unit in a lower bound allows us to eliminate a lot of unknowns in the commutator structure of the defining relations. Because of this, the researchers have focused on finding the best lower bound for the degree of commutativity. In fact, until now the main goal was to get an expression of type \( 2c \geq m - g(p) \), where \( g(p) \) was a function of \( p \), that is, an inequality in terms of the order of \( G \). The best one was given in [2] and it was \( 2c \geq m - 2p + 5 \).

However, if we consider also the invariants \( l \) and \( c_0 \), sharper inequalities can be obtained. Indeed, by implementing the algorithm described in [6], we have written a program which gives us the minimum value \( a \) such that \( 2c \geq m - a \), for a fixed prime \( p \), \( l \), and \( c_0 \). After running it for primes \( p \leq 43 \) and all possible values of \( l \) and \( c_0 \), we have made a table \( U_p \) that contains in the cell \((i, j)\) the corresponding \( a_{i,j} \) for \( c_0 = i - 1 \) and \( l = j \), when we works on prime \( p \). By observing the obtained results for the different primes \( p \), we have checked that \( 2p - 5 \) is the maximum obtained value, it only attains in two cells corresponding to \( l = (p - 3)/2 \) and \( c_0 = 2, 3 \) and the rest values are much lower. On other hand, we have detected a uniformity in the tables \( U_p \) and we have divided these tables in six different regions according to the obtained functions \( g(c_0, l, p) \), such that \( 2c \geq m - g(p, l, c_0) \). These regions have the following properties:

1. They keep on, when \( p \) changes.
2. The intersection of two different regions is the empty set.
3. Their union covers almost \( U_p \), except some particular values of \( c_0 \), for \( l \leq 3 \).

So, it deserves to prove the validity of the obtained functions in the considered regions for every prime \( p \), because the corresponding inequality is much sharper than the best one known until now.

In this paper, we prove the validity of two of obtained functions and in [7] we prove the other four. As it can be observed in the proofs of the six inequalities, the used techniques are different according to the considered regions.

The main results that we shall show in this paper are the following theorems.

**Theorem 1.** Suppose that one of the following statements holds:

1. \( p - 2 \geq c_0 \geq p - l \) and \( l \geq 2 \).
2. \( 2l = p - 3 \) and \( c_0 \geq 4 \) or \( c_0 = 2 \).
3. \( c_0 \geq 2p - 4l + 1 \).
4. \(2p - 4l - 1 \leq c_0 \leq 2p - 4l + 2\) and \(l > (p - 1)/3\).
5. \(c_0 \in \{2p - 4l - 2, 2p - 4l - 4\}\) and \(p \leq 3l - 1\).
6. \(l \geq (p + 5)/6\) and \(l + c_0 = (p + 1)/2\).

Then \(2c \geq m - p - 2l + c_0\) holds. Moreover, there exist \(p\)-groups of maximal class satisfying \(2c = m - p - 2l + c_0\) in cases 1–6.

**Theorem 2.** Suppose that \(l + c_0 = (p - 1)/2\) and \(l \geq (p + 5)/6\). Then, \(2c \geq m - 2l - c_0 - 1\) or \(c = c_0 = (p - 1)/2 - l\). In addition, if \(l + c_0 = (p - 1)/2\), there exist \(p\)-groups of maximal class satisfying \(2c = m - 2l - c_0 - 1\) for \(c_1 \geq 1\) or \(2c = m - 2l - c_0 - 2\) for \(c = c_0\).

The main part of Theorem 1 is an immediate consequence of Propositions 3.3–3.5, 3.7, 3.8, 3.10, and 3.15, which are shown in Section 3. The bound that states in Theorem 2 is shown in Section 4. Finally, the existence of \(p\)-groups of maximal class such that attain both bounds is justified by the examples of Theorem 4.5 of [8]. By using this theorem, we obtain the defining relations of the associated \(p\)-group of maximal class, which satisfy \(c(G) = c, l(G) = l, Y_1\) of class 2 and the exact values of our bounds in the regions we are working on. The existence of these \(p\)-groups of maximal class has been also checked by using GAP (cf. [3]) when \(p \leq 17\).

Moreover, in the particular case of \(G\) a \(p\)-group of maximal class with \(Y_1\) of class 2, it is shown in [8] that

1. If \(l \in \{1, \ldots, (p - 1)/2\}, c_0 \in \{1, \ldots, p - 2\}\), and \(l + c_0 \geq (p + 1)/2\), then \(2c \geq m - p - 2l + c_0\) is attained. That is, the region given in Theorem 1 can be enlarged to \(l \geq 1\).
2. If \(l + c_0 = (p - 1)/2\) and \(c_1 \geq 1\), the bound \(2c \geq m - 2l - c_0 - 1\) is attained. So, the hypothesis \(l \geq (p + 5)/6\) can be eliminated in Theorem 2.

2. Previous lemmas

We shall use the notation
\[
\{a, b\} = \begin{cases} 
  a(a - 1) \cdots (a - b + 1) & \text{if } b \text{ is a positive integer}, \\
  1 & \text{if } b = 0, \\
  0 & \text{if } b \text{ is a negative integer}.
\end{cases}
\]

Similarly, we shall use the convention of the more general definition of the symbol of the combinatorial number,
\[
\binom{a}{b} = \frac{\{a, b\}/b!}{b} \quad \text{if } b \text{ is a non-negative integer},
\]
\[
0 \quad \text{if } b \text{ is a negative integer}.
\]
Suppose that \( i + j + p - c_0 - 1 \leq m - 2c - 1 \). Then the following factorization holds:

\[
 f(i, j, p - c_0 - 1) = \alpha_{i,j}(\alpha_{i+j+c_0,p-c_0-1} - \alpha_{i,p-c_0-1} - \alpha_{j,p-c_0-1}). \tag{1}
\]

Evidently, we have

\[
 \alpha_{i,j} = 0, \quad \text{for } i + j \leq 2l,
\]

\[
 \alpha_{i,2l+1-i} = (-1)^{l-i}x_l, \quad \text{for } i \leq l,
\]

\[
 \alpha_{i,2l+2-i} = (-1)^{l-i}(l + 1 - i)x_l, \quad \text{for } i \leq l,
\]

\[
 \alpha_{i,2l+3-i} = (-1)^{l-i}\left(\frac{l + 2 - i}{2}\right)x_l + (-1)^{l+1-i}\left(\begin{array}{c} l + 1 - i \\ 0 \end{array}\right)x_{l+1},
\]

\[
 \text{for } i \leq l + 1,
\]

\[
 \alpha_{i,2l+4-i} = (-1)^{l-i}\left(\frac{l + 3 - i}{3}\right)x_l + (-1)^{l+1-i}\left(\begin{array}{c} l + 2 - i \\ 1 \end{array}\right)x_{l+1},
\]

\[
 \text{for } i \leq l + 1. \tag{2}
\]

The following result, proved in [5, Lemma 1], can be used in order to prove some bounds.

**Lemma 2.1.** Let \( e \) and \( t \) be positive integers such that \( t \geq e \). Let us consider the matrix \( A = (a_{ij})_{1 \leq i,j \leq e} \), with

\[
 a_{ij} = \left(\frac{r - i}{t - 2i + j}\right).
\]

Then

\[
 \det A = \frac{F(r, t, e)}{F(t, t, e)}, \tag{3}
\]

where

\[
 F(r, t, e) = \prod_{w=1}^{t-1} (r - w)^{\min(w, t - w, e, t - e)} \\
 \cdot \prod_{w=t-e+1}^{t+e-3} (2r - w - 1)^{\min([\frac{e-1+w+1}{2}],[\frac{t+e-w-1}{2}])}.
\]

We have \( \alpha_{i,p} = \alpha_{i,1} = 0 \) for \( i \leq 2l - 1 \). Frequently we shall work with systems of \( e \) equations with \( e \) unknowns whose coefficient matrices are ones of the type of above lemma. These systems arise from considering equations

\[
 \alpha_{i_0,p+i_2} = \cdots = \alpha_{i_1,p+i_2} = 0,
\]

for suitable \( i_0, i_1 \) satisfying \( 1 \leq i_0 \leq i_1 \) and \( i_1 + i_2 - 1 \leq 2l \) and supposing the existence of the numbers \( i_3, i_4 \) satisfying \( x_{i_0} = \cdots = x_{i_3} = 0 \) and \( x_{i_4} = \).
\[ \cdots = x_{[(i_1 + p + i_2 - 1)/2]} = 0, \] otherwise, if there is not given \( i_3 \) (respectively \( i_4 \)) we define \( i_3 = i_0 - 1 \) (respectively \( i_4 \geq [(i_1 + p + i_2 - 1)/2] + 1 \)) satisfying \( i_1 - i_0 + 1 = i_4 - i_3 - 1 \).

In this case, for \( i_0 \leq i \leq i_1 \), we have

\[
0 = \sum_{\lambda = i}^{[(i+p+i_2-1)/2]} (-1)^{\lambda-i} \left( \frac{p + i_2 - \lambda - 1}{\lambda - i} \right) x_\lambda \\
= \sum_{\lambda = i_3 + 1}^{i_4 - i_2} (-1)^{\lambda-i} \left( \frac{p + i_2 - \lambda - 1}{\lambda - i} \right) x_\lambda \\
= \sum_{\mu = 1}^{i_4-i_2-1} (-1)^{\mu-(i_4+i_0-1)} \left( \frac{p + i_2 - i_3 - 1 - \mu}{\mu + i_3 - (i_4 + i_0 - 1)} \right) x_\mu',
\]

so

\[
0 = \sum_{\mu = 1}^{e} (-1)^{\mu-i'} \left( \frac{p + i_2 - i_3 - 1 - \mu}{p + i_2 - 2i_3 + i_0 - 2 - 2\mu + i'} \right) x_\mu', \tag{4}
\]

with \( 1 \leq i' \leq i_1 - i_0 + 1 \) and the parameters satisfying \( i_1 - i_0 + 1 = e = i_4 - i_3 - 1 \), because we will apply Lemma 2.1, when the number of equations and unknowns are equal.

So we consider the numbers

\[
r = p + i_2 - i_3 - 1, \\
t = p + i_2 - 2i_3 + i_0 - 2, \\
e = i_1 - i_0 + 1 = i_4 - i_3 - 1.
\]

If \( w \in [1, t - 1] \), then we have \( r - 1 \geq r - w \geq r - t + 1 \), and \( 1 \leq t - w \leq t - 1 \); that is

\[
i_3 - i_0 + 2 \leq r - w \leq p + i_2 - i_3 - 2 \quad \text{and} \\
1 \leq t - w \leq p + i_2 - 2i_3 + i_0 - 3.
\]

If \( w \in [t - e + 1, t + e - 3] \) then

\[
p + i_2 - i_1 + 1 = 2r - (t + e - 3) - 1 \leq 2r - w - 1 \\
\leq 2r - (t - e + 1) - 1 = p + i_2 + i_1 - 2i_0 - 1,
\]

and

\[
p + i_2 - 2i_3 + 2i_0 - i_1 - 1 = 2t - (t + e - 3) - 1 \leq 2t - w - 1 \\
\leq 2t - (t - e + 1) - 1 \\
= p + i_2 + i_1 - 2i_3 - 3.
\]
Thus, we consider the intervals

\[ I_1 = [i_3 - i_0 + 2, p + i_2 - i_3 - 2], \]
\[ I_2 = [1, p + i_2 - 2i_3 + i_0 - 3], \]
\[ I_3 = [p + i_2 - i_1 + 1, p + i_2 + i_1 - 2i_0 - 1], \]
\[ I_4 = [p + i_2 - 2i_3 + 2i_0 - i_1 - 1, p + i_2 - 2i_3 + i_1 - 3]. \quad (5) \]

So, if \( A \) is the coefficient matrix of system (4) and \( p \notin I_1 \cup I_2 \cup I_3 \cup I_4 \), it follows from Lemma 2.1 that \( \det A \not\equiv 0 \pmod{p} \).

The following lemma also will be used in Sections 3 and 4.

**Lemma 2.2.** If \( 3l \leq m - 2c - 1 \) and \( l \geq 2 \), then \( \alpha_{1,2l+c_0+k} = 0 \) for \( 1 \leq k \leq l - 1 \).

**Proof.** Suppose \( 3l \leq m - 2c - 1 \). For \( k \in \{1, \ldots, l - 1\} \), we have

\[ f(l - k, l, l + 1) = x_l \alpha_{2l+1+c_0,l-k} = 0 \]

because \( \alpha_{l-k,l} = \alpha_{l+1,l-k} = 0 \). But, \( x_l \neq 0 \), so \( -\alpha_{l-k,2l+1+c_0} = \alpha_{2l+1+c_0,l-k} = 0 \) for \( k \in \{1, \ldots, l - 1\} \). Now, by applying Bernoulli’s property, all the values of the triangle of vertices \((1, 2l + 1 + c_0), (1, 3l + c_0 - 1), (l - 1, 2l + 1 + c_0)\) are zero. In particular, \( \alpha_{1,2l+c_0+k} = 0 \), for \( 1 \leq k \leq l - 1 \). \( \square \)

If \( 2l + 2 \leq m - 2c - 1 \) and \( l \geq 2 \), we have \( f(1, l, l + 1) = x_l \alpha_{2l+1+c_0,1} = 0 \), so \( \alpha_{1,2l+1+c_0} = 0 \) and we can define the number \( l' \) by the following condition:

\[ \alpha_{1,2l+c_0+1} = \cdots = \alpha_{1,2l'+c_0+1'} = 0, \quad \alpha_{1,2l'+c_0+1'} \neq 0. \]

Evidently, in the case \( 3l \leq m - 2c - 1 \), from Lemma 2.2 we have \( l' \geq l \).

### 3. Region with bound \( 2c \geq m - p - 2l + c_0 \)

The following results are interesting in order to prove some bounds when \( c_0 \) and \( l \) are “big” in relation with \( p \), because in order to obtain information for a possible contradiction, we must fix our attention in the level \( i + j + k = p + 2l - c_0 \), bearing in mind that every Jacobi for the smaller levels is identically zero for every assignment of the \( x_l \).

In order to prove Theorem 1, when one of the first two statements holds, we need the following lemma.

**Lemma 3.1.** Suppose that \( p \leq 2l + c_0 + 1 \). If \( i + j + k \leq p + 2l - c_0 - 1 \), then we have \( \alpha_{i,j} \alpha_{i+j+c_0,k} = 0 \).

**Proof.** If \( i + j \leq 2l \), then we have \( \alpha_{i,j} = 0 \). Otherwise, if \( i + j \geq 2l + 1 \), then \( i + j + c_0 \geq 2l + 1 + c_0 \geq p \), so, by using periodicity \( p - 1 \), we get

\[ \alpha_{i+j+c_0,k} = \alpha_{i+j+c_0-(p-1),k} = 0 \]
because \( i + j + c_0 - (p - 1) + k \leq p + 2l - c_0 - 1 + c_0 - (p - 1) \leq 2l \). \( \square \)

As a consequence of this lemma, we obtain the following corollary.

**Corollary 3.2.** If \( p \leq 2l + c_0 + 1 \) and \( p + 2l - c_0 - 1 \leq m - 2c - 1 \), then \( f(i, j, k) = 0 \) whenever \( i + j + k \leq p + 2l - c_0 - 1 \), that is, the system \( S(t) \) for \( t = p + 2l - c_0 - 1 \) is satisfied for every assignment of the \( x_\lambda \), with \( l \leq \lambda \leq (p - 3)/2 \).

Therefore, under the conditions of above corollary, we can focus in the level \( p + 2l - c_0 \).

**Proposition 3.3.** If \( c_0 = p - 2 \) and \( l \geq 2 \), then \( 2c \geq m - 2l - p + c_0 = m - 2l - 2 \) holds. Moreover, there are Lie algebras of maximal class with \( 2c = m - 2l - 2 \).

**Proof.** Suppose that \( 2l + 2 \leq m - 2c - 1 \). Bearing in mind the periodicity modulo \( p - 1 = c_0 + 1 \) and that \( \alpha_{1,l} = \alpha_{l+1,1} = 0 \) we have

\[
f(1, l, l + 1) = \alpha_{l,l+1}\alpha_{2l,1} = (-1)^l x_l^2 = 0;
\]

whence \( x_l = 0 \), a contradiction.

As \( c_0 = p - 2 \), then \( 2l + c_0 + 1 = 2l + p - 1 \geq p \), so we are in the hypothesis of Corollary 3.2 and any assignment of the \( x_i \) for \( l \leq i \leq (p - 3)/2 \) satisfies \( S(t) \) for \( t = 2l + 1 \). \( \square \)

**Proposition 3.4.** Suppose that \( p - 3 \geq c_0 \geq p - l \), then \( 2c \geq m - 2l - p + c_0 \) holds. In addition, there are Lie algebras of maximal class with \( 2c = m - 2l - p + c_0 \).

**Proof.** Suppose that \( p + 2l - c_0 \leq m - 2c - 1 \). Since \( p - c_0 \leq l \), bearing in mind periodicity modulo \( p - 1 \), (1) and (2), it follows that

\[
f(c_0 - p + 2l + 3, p - c_0 - 2, p - c_0 - 1) = \alpha_{c_0-p+2l+3,p-c_0-2}(\alpha_{c_0+2l+1,p-c_0-1} - \alpha_{c_0-p+2l+3,p-c_0-1}) = (-1)^l(-p-c_0-1)x_l(-1)^l(-p-c_0)(x_l - (l + 1 - (p - c_0 - 1))x_l) = (c_0 + l + 1 - p)x_l^2 = 0,
\]

so \( x_l = 0 \), impossible.

We observe that \( 2l + c_0 + 1 \geq 2l + p - l + 1 = p + l - 1 \geq p \), so by Corollary 3.2 \( f(i, j, k) = 0 \), when \( i + j + k < p + 2l - c_0 \). \( \square \)

**Proposition 3.5.** Suppose that \( 2l = p - 3 \) and \( c_0 \geq 4 \) or \( c_0 = 2 \). Then \( 2c \geq m - p - 2l + c_0 \).
Proof. Suppose \( p + 2l - c_0 \leq m - 2c - 1 \). Set \( c_0 = 2k + e' \) with \( e' \in \{0, 1\} \). From Propositions 3.3 and 3.4 we can assume \( c_0 \leq p - 4 \), so we have \( k \leq l - 1 \). Bearing in mind periodicity modulo \( p \) and (2), we have

\[
0 = f(l - k, l - k + 1, p - 1 - e')
\]

\[
= (\alpha_{l-k+1,l-1-e'} + \alpha_{l-k,p-1-e'})(-1)^{l-(l-k)}x_l,
\]

whence

\[
\alpha_{l-k+1,l-1-e'} + \alpha_{l-k,p-1-e'} = 0. \tag{6}
\]

On the other hand, we have \( \alpha_{i,p} = \alpha_{i,1} = 0 \), for all \( i \leq 2l - 1 \), so \( \alpha_{i,p-1} = \alpha_{1,p-1} \) for \( i \leq 2l \) and

\[
\alpha_{i,p-2} = \alpha_{1,p-2} - (i - 1)\alpha_{1,p-1}, \quad \text{for } i \leq 2l + 1. \tag{7}
\]

If \( e' = 0 \), then from (6) it follows that \( \alpha_{i,p-1} = 0 \) for \( i \leq 2l \). In particular, from (2)

\[
0 = \alpha_{1,p-1} = \alpha_{1,2l+2} = (-1)^{l-1} \left( \binom{l+1}{2} \right) x_l + (-1)^{l} x_{l+1},
\]

\[
0 = \alpha_{2,p-1} = \alpha_{2,2l+2} = (-1)^{l-2} \left( \binom{l+1}{3} \right) x_l + (-1)^{l-1} x_{l+1}, \tag{8}
\]

whence \( x_l = 0 \), impossible.

If \( e' = 1 \), from (6) and (7), it follows

\[
\alpha_{1,p-2} = \frac{2l - c_0}{2} \alpha_{1,p-1} = \frac{2l - c_0}{2} x,
\]

with \( x = \alpha_{1,p-1} \). We have the following system in the unknowns \( x, x_l, x_{l+1} \):

\[
(-1)^{l-1} x_l = \alpha_{1,p-2} = \frac{2l - c_0}{2} x,
\]

\[
x = \alpha_{1,p-1} = \alpha_{1,2l+2} = (-1)^{l-1} \left( \binom{l+1}{2} \right) x_l + (-1)^{l} x_{l+1},
\]

\[
0 = \alpha_{1,p} = \alpha_{1,2l+3} = (-1)^{l-1} \left( \binom{l+2}{3} \right) x_l + (-1)^{l} (l+1) x_{l+1}, \tag{9}
\]

whence, working modulo \( p \), we get \( (c_0 - 3)x_l = 0 \), impossible. \( \square \)

The following lemma is quite useful in order to prove our bound when the statements 3 and 4 of Theorem 1 hold.

Lemma 3.6. If \( c_0 \geq 2p - 4l - 1 \) and \( p + 2l - c_0 \leq m - 2c - 1 \) hold, then we have \( x_r = 0 \) for \( p - c_0 \leq r \leq l + [(p - c_0)/2] - 1 \).

Proof. The condition \( c_0 \geq 2p - 4l - 1 \) implies \( l + [(c_0 - p)/2] - 1 \geq [(p - 2l - 1)/2] - 1 \geq 0 \). For \( 0 \leq k \leq l + [(c_0 - p)/2] - 1 \), we have

\[
(2l + c_0 - p - 2k - 1) + (p - c_0 + 1 + k) = 2l - k \leq 2l,
\]
so
\[ \alpha_{2l+c_0-p-2k-1,p-c_0+k} = 0 = \alpha_{p-c_0+k+1,2l+c_0-p-2k-1}; \]

consequently,
\[ f(2l + c_0 - p - 2k - 1, p - c_0 + k, p - c_0 + k + 1) \]
\[ = x_{p-c_0+k} \alpha_{2p-c_0+2k+1,2l+c_0-p-2k-1} = 0. \]

Bearing in mind periodicity modulo \( p - 1 \), we have
\[ \alpha_{2p-c_0+2k+1,2l+c_0-p-2k-1} = \alpha_{p-c_0+2k+2,2l+c_0-p-2k-1} \not= 0, \]

because it is at the level \( 2l + 1 \). Thus, we conclude, \( x_{p-c_0+k} = 0 \), as desired. \( \square \)

**Proposition 3.7.** Suppose that \( c_0 \geq 2p - 4l + 1 \) and \( p - c_0 - l \geq 1 \). Then, \( 2c \geq m - p - 2l + c_0 \) holds.

**Proof.** Suppose that \( p + 2l - c_0 \leq m - 2c - 1 \). From conditions \( c_0 \geq 2p - 4l + 1 \) and \( p - c_0 - l \geq 1 \), it follows that \( 1 \leq p - c_0 - l \leq l - (c_0 - 1)/2 \). Set
\[ u = \lfloor (l - (c_0 - 1)/2) \rfloor = l - [c_0/2]. \]

For \( i \leq u \), we have
\[ 0 = \alpha_{i,u} = \alpha_{i,p-1+u} \tag{10} \]

with \( (p - 2 + u + i)/2 \leq [(p - 2)/2 + u] = (p - 3)/2 + u \leq l + (p - c_0)/2 - 1 \).

So, bearing in mind Lemma 3.6, the above equations can be written in terms of \( x_l, x_{l+1}, \ldots, x_{p-c_0-1} \). Since \( 1 \leq p - c_0 - l \leq u \), we can consider the first \( p - c_0 - l \) equations of (10) in the \( p - c_0 - 1 \) unknowns \( x'_{\mu} = x_{\mu+1:l} \).

Set
\[ r = p - 1 + u - l, \quad t = p + u - 2l, \quad e = p - l - c_0, \]

and
\[ i_0 = 1, \quad i_1 = p - c_0 - l, \quad i_2 = l - \left\lfloor \frac{c_0}{2} \right\rfloor - 1 = u - 1, \]
\[ i_3 = l - 1, \quad i_4 = p - c_0. \]

The intervals (5) are
\[ I_1 = \left[ l, p - \left\lfloor \frac{c_0}{2} \right\rfloor - 2 \right], \quad I_2 = \left[ 1, p - l - \left\lfloor \frac{c_0}{2} \right\rfloor - 1 \right], \]
\[ I_3 = \left[ 2l + \left\lfloor \frac{c_0 + 1}{2} \right\rfloor, 2p - \left\lfloor \frac{3c_0}{2} \right\rfloor - 4 \right], \]
\[ I_4 = \left[ \left\lfloor \frac{c_0 + 1}{2} \right\rfloor + 2, 2p - 2l - \left\lfloor \frac{3c_0}{2} \right\rfloor - 2 \right]. \]

Consequently, \( I_1 \cup I_2 \cup I_3 \cup I_4 \subseteq [1, p - 1] \cup [p + 1, 2p - 1] \) and therefore \( p \not\in I_1 \cup I_2 \cup I_3 \cup I_4 \). The determinant is non-zero modulo \( p \) and thus, we have that \( x_l = 0 \), a contradiction. \( \square \)
Proposition 3.8. Suppose that $2p - 4l - 1 \leq c_0 \leq 2p - 4l + 2$ and $3l \geq p + 2$. Then $2c \geq m - p - 2l + c_0$.

Proof. Suppose $p + 2l - c_0 \leq m - 2c - 1$. From the hypothesis, as $c_0$ take four values, we have $[c_0/2] \in \{2l - p + c_0, 2l - p + c_0 - 1\}$. Therefore, $-[(c_0 + 1)/2] = [c_0/2] - c_0 \in \{2l - p, 2l - p - 1\}$. Moreover, we have $c_0 + [c_0/2] - 1 \leq p \leq 2l + c_0 - 1$. In fact, if $p \geq 2l + c_0$, then $c_0 \geq 2p - 4l - 1 \geq 2(2l + c_0) - 4l - 1 = 2c_0 - 1$, hence $c_0 \leq 1$ and $2p - 4l - 1 \leq c_0 \leq 1$, whence $2l \geq p - 1$, impossible. On the other hand, if $p \leq c_0 + [c_0/2] - 2$, we have $p \leq c_0 + [c_0/2] - 2$, but $c_0 + l \leq 2p - 3l + 2 \leq 2p - (p + 2) + 2 = p$, hence $p \leq c_0 + l + (c_0 + l - p) - 2 < p$, impossible.

We have $\alpha_{i,p} = 0$, for all $i \leq 2l - 1$. So, $\alpha_{i+p-c_0-1,p} = 0$, for all $1 \leq i < 2l - 1 - (p - c_0 - 1) = 2l - p + c_0$.

From Lemma 3.6, we have that $x_r = 0$ for $p - c_0 \leq r \leq l + [(p - c_0)/2] - 1$. Therefore, for $1 \leq i \leq 2l - p + c_0$, it follows that

$$0 = \alpha_{i+p-c_0-1,p} = \sum_{\lambda=l+[p-c_0/2]} (-1)^{i-l} \left( \frac{p-\lambda-1}{\lambda - (i + p - c_0 - 1)} \right) x_{\lambda}. \quad (11)$$

We have

$$[(i + p - c_0 + p - 2)/2] \leq [(2l - p + c_0 + p - c_0 + p - 2)/2] = l + (p - 1)/2 - 1,$$

so (11) is a system of $2l - p + c_0$ linear equations with $l + (p - 1)/2 - 1 - (l + [(p - c_0)/2]) + 1 = [c_0/2]$ unknowns $x_{l+[(p-c_0)/2]}, \ldots, x_{l+(p-1)/2}-1$. Since $[c_0/2] \leq 2l - p + c_0$, we can consider the first $[c_0/2]$ equations of (11) in $[c_0/2]$ unknowns. Let $r = p - l - [(p - c_0)/2]$, $t = p - 2l + 1 - e'$, where $e' \in [0, 1]$ is the parity of $c_0$ and

$$i_0 = p - c_0, \quad i_1 = p - c_0 + \left[ \frac{c_0}{2} \right] - 1, \quad i_2 = 0,$$

$$i_3 = l + \left[ \frac{p - c_0}{2} \right] - 1, \quad i_4 = l + \frac{p - 1}{2}.$$ The intervals (5) are

$$I_1 = \left[ \frac{-p + c_0 + e' + 1}{2} + l, \frac{p + c_0 - e' - 1}{2} - l \right],$$

$$I_2 = [1, p - 2l - e'], \quad I_3 = \left[ \frac{c_0 + e'}{2} + 2, \frac{3c_0 - e'}{2} - 2 \right],$$

$$I_4 = \left[ p + 3 - 2l - \frac{c_0 + e'}{2}, p - 1 - 2l + \frac{c_0 - 3e'}{2} \right].$$
Consequently $I_1 \cup I_2 \cup I_3 \cup I_4 \subseteq [1, p - 1]$ and $\det A \neq 0 \pmod{p}$. Thus, we conclude

$$0 = x_{p-c_0} = \cdots = x_{l+[(p-c_0)/2]-1} = x_{l+[(p-c_0)/2]} = \cdots = x_{l+(p-1)/2-1},$$

and so $\alpha_{i,j} = 0$ for $i \geq p - c_0$, $j \geq p - c_0 + 1$ and $i + j \leq 2l + p - 1$. In particular, $\alpha_{i,2l+p-1-i} = 0$ for $p - c_0 \leq i \leq l + (p - 1)/2 - 1$. In addition, in the level $2l + p - 1$, also we have $\alpha_{i,2l+p-1-i} = 0$ for $1 \leq i \leq 2l - 1$. Furthermore, $2l - 1 \geq p - c_0$, so the two zero triangles must intersect one another and consequently $\alpha_{i,2l+p-1-i} = 0$ for $1 \leq i \leq l + (p - 1)/2 - 1$; hence $x_l = 0$, impossible. \hfill \Box

Next, we study the diagonal $l + c_0 = (p + 1)/2$. We need the next lemma.

**Lemma 3.9.** Suppose that $l + c_0 = (p + 1)/2$, $4l + c_0 - 1 \leq m - 2c - 1$, and $l \geq 2$. Then $\alpha_{i,2l+c_0} = 0$ for $1 \leq i \leq 2l - 2$.

**Proof.** From Lemma 2.2 we have $\alpha_{i,2l+c_0+1} = 0$, for $1 \leq i \leq l - 1$. Bearing in mind periodicity modulo $p - 1 = 2l + 2c_0 - 2$ and (2), we have

$$f(i, 2l - 2 - i, 2l + c_0 + 1) = \alpha_{2l-2-i,2l+c_0+1}(-1)^{l-i-1}x_l$$

$$+ \alpha_{2l+c_0+1,i}(-1)^{l-i-3}x_l.$$  

Consequently,

$$\alpha_{2l-2-i,2l+c_0+1} = \alpha_{i,2l+c_0+1},$$

and we conclude $\alpha_{2l-2-i,2l+c_0+1} = 0$ for $1 \leq i \leq 2l - 3$; that is

$$\alpha_{j,2l+c_0} = \alpha_{1,2l+c_0} \quad \text{for} \quad 1 \leq j \leq 2l - 2. \quad (12)$$

Now

$$f(1, 2l - 2, 2l + c_0) = \alpha_{2l-2,2l+c_0}\alpha_{2l,1} + \alpha_{2l+c_0,1}\alpha_{3,2l-2} = 0.$$  

So,

$$\alpha_{2l-2,2l+c_0} + \alpha_{1,2l+c_0} = 0$$

and, from (12), we obtain $\alpha_{1,2l+c_0} = 0$ as desired. \hfill \Box

**Proposition 3.10.** Suppose that $l \geq (p + 5)/6$ and $l + c_0 = (p + 1)/2$. Then $2c \geq m - p - 2l + c_0$ holds.

**Proof.** Suppose $p + 2l - c_0 = 4l + c_0 - 1 \leq m - 2c - 1$. From the hypothesis, we have $2l \geq c_0 + 2$, so, from Lemma 3.9, we obtain $\alpha_{i,2l+c_0} = 0$ for $1 \leq i \leq c_0$. This is a system of $c_0$ equations with $c_0$ unknowns whose coefficient matrix is one of the type given in Lemma 2.1, for $r = l + c_0$, $t = c_0 + 1$, and $e = c_0$. In addition,
Therefore, the determinant of this coefficient matrix does not vanish and the system has a unique solution, \( x_l = 0 \) for \( l \leq i < l + c_0 - 1 \), a contradiction with the condition \( x_l \neq 0 \).

Next we study the case \( c_0 \in \{2p - 4l - 2, 2p - 4l - 4\} \).

**Lemma 3.11.** If \( c_0 \leq 2l - 2 \) and \( 2l - c_0 + p \leq m - 2c - 1 \), then
\[
\alpha_{2l-c_0+i,p-1-i} = (-1)^{c_0-i-1} \alpha_{1,p-1-i} \quad \text{for } 0 \leq i \leq c_0 - 1.
\]

**Proof.** For \( 0 \leq i \leq c_0 - 1 \), and by using periodicity modulo \( p - 1 \), we have
\[
0 = f(1, 2l - c_0 + i, p - 1 - i) = \alpha_{2l-c_0+i,p-1-i}(-1)^{i}x_l + \alpha_{p-1-i,1}(-1)^{l-c_0-i}x_l,
\]
so the desired result.

**Lemma 3.12.** If \( c_0 \leq 2l - 2 \), \( 2l - c_0 + p \leq m - 2c - 1 \), and \( c_0 \geq p - 2l + 1 \), then
\begin{enumerate}
\item \( x_{p-c_0} = \cdots = x_{l-1+[(p-c_0)/2]} = 0 \). \quad (13)
\item \( x_{p-c_0-1} = (-1)^{l+c_0}x_l \) and \( x_{p-c_0-2} = (-1)^{l+c_0}(l - (p - c_0) + 2)x_l \).
\end{enumerate}

**Proof.** For \( p - 2l \leq i \leq c_0 - 1 \), it is \( p - 1 - i + 1 \leq p - 1 - (p - 2l) + 1 = 2l \), so from Lemma 3.11 \( \alpha_{2l-c_0+i,p-1-i} = 0 \) and we have
\[
\alpha_{p-c_0,2l-1} = \alpha_{p-c_0+1,2l-2} = \cdots = \alpha_{2l-1,p-c_0},
\]
that is
\[
\alpha_{i,j} = 0, \quad \text{for } i \geq p - c_0, j \geq p - c_0 + 1, i + j \leq p - c_0 + 2l - 1,
\]
or equivalently
\[
x_{p-c_0} = \cdots = x_{l-1+[(p-c_0)/2]} = 0.
\]
Consequently, if \( x = \alpha_{p-c_0-1,2l} \) and \( y = \alpha_{p-c_0-2,2l+1} \) then Bernoulli’s property yields
\[
\alpha_{p-c_0-1,j} = x, \quad \text{for } p - c_0 \leq j \leq 2l,
\]
and
\[ \alpha_{p-c_0-2,j} = y + (2l + 1 - j)x, \quad \text{for } p - c_0 - 1 \leq j \leq 2l + 1. \]

On the other hand, from Lemma 3.11 for \( i = p - 2l - 1 \), we have
\[ \alpha_{p-c_0-1,2l} = (-1)^{c_0+l}x_l, \]
hence \( x_{p-c_0-1} = x = (-1)^{c_0+l}x_l \), and also for \( i = p - 2l - 2 \) we have
\[ \alpha_{p-c_0-2,2l+1} = (-1)^{c_0-p-1}\alpha_{1,2l+1} = (-1)^{c_0+l-1}(l + 1 - 1)x_l, \]
therefore
\[ \alpha_{p-c_0-2,p-c_0-1} = y + (2l + 1 - (p - c_0 - 1))x \]
\[ = (-1)^{c_0+l-1}(l + 1 - 1)x_l \]
\[ + (2l + 1 - (p - c_0 - 1))(-1)^{c_0+l}x_l, \]
whence the desired value of \( x_{p-c_0-2} \). \( \square \)

**Lemma 3.13.** Suppose that \( c_0 \) is even, \( c_0 < 2l \) and \( p + 2l - c_0 \leq m - 2c - 1 \), then \( \alpha_{1,p-1} = 0 \).

**Proof.** We have \( c_0 \leq 2l - 2 \) and from Lemma 3.11 we get \( \alpha_{2l-c_0,p-1} = -\alpha_{1,p-1} \).
In addition, \( \alpha_{i,p} = 0 \), for \( i \leq 2l - 1 \), hence \( \alpha_{2l-c_0,p-1} = \alpha_{1,p-1} \), and therefore we conclude \( \alpha_{1,p-1} = 0 \). \( \square \)

**Lemma 3.14.** Consider the matrix \( A = (a_{ij}) \) defined as follows:
\[ a_{i,j} = \begin{cases} 
  x - i & \text{if } i = 1, \ldots, e - 1, \ j = 1, \ldots, e, \\
  t - 2i + j & \text{if } i = e, \ j = 1, \ldots, e,
\end{cases} \]
where \( t = e - 1 \). Set
\[ h(x,e) = \prod_{w=2}^{2(e-1)} \left( x - \frac{w}{2} \right)^{\min([w/2],[2(e-w)/2])}. \]
Then
\[ \det A = (-1)^e e(e-1) \frac{h(x,e)}{h(e,e)(2x-e)}. \]

**Proof.** We apply to \( A \) the following column transformations:
\[ A^j \mapsto A^j + 2A^{j+1}, \quad A^j \mapsto \frac{1}{2x - t - j + e - s} A^j, \]
for \( j = 3, \ldots, s, s = e - 1, e - 2, \ldots, 3 \). The resulting matrix \( B \) has its two first columns and the last row equal to the ones of \( A \) and the rest elements of \( B \) satisfy

\[
\left( x + e - j - i \right) \quad \left( t + e - 2i \right)
\]

for \( i = 1, \ldots, e - 1 \) and \( j = 3, \ldots, e \).

We have the relationship between determinants:

\[
\det A = \prod_{s=3}^{e-1} \prod_{j=3}^{s} (2x - j - s + 1) \cdot \det B.
\]

If we multiply now the rows \( i = 1, \ldots, e - 1 \) by \((2e - 1 - 2i)!/\left\{x - i, e - 2i\right\}\), we obtain the matrix \( C = (c_{ij}) \), with

\[
c_{ij} = \begin{cases} 
\begin{aligned}
\left( e - 2i, e - 1 \right) & \text{for } i = 1, \ldots, e - 1 \text{ and } j = 1, \\
\left( x - (t + 1 - i), j - 1 \right) & \text{for } i = 1, \ldots, e - 1 \text{ and } j = 3, \ldots, e,
\end{aligned}
\end{cases}
\]

being

\[
\det B = \prod_{i=1}^{e-1} \frac{x - i, e - 2i}{(2e - 1 - 2i)!} \det C.
\]

Now we make some transformations:

\[
C^j \mapsto C^j - (x - j + 1)C^{j-1}, \quad j = e, e - 1, \ldots, s, s = 4, \ldots, e,
\]

and, by canceling the signs \(-1\) we obtain a matrix \( D = (d_{ij}) \) with

\[
d_{ij} = \begin{cases} 
\begin{aligned}
\left( 2e - 1 - 2i, e - 1 \right) & \text{for } i = 1, \ldots, e - 1, \text{ and } j = 1, \\
\delta_{i,e} & \text{for } i = 1, \ldots, e, \text{ and } j = 2, \\
\left( e - 1 - i, j - 3 \right) \cdot \left( x - (e - i), 2 \right) & \text{for } i = 1, \ldots, e - 1, \text{ and } j = 3, \ldots, e, \\
\delta_{2,j} & \text{for } i = e, \text{ and } j = 1, \ldots, e.
\end{aligned}
\end{cases}
\]

Set \( b_1 = [e/2] - 1, b_2 = [(e+1)/2] - 1 \). The above matrix has a block structure of \((b_1 + 1) + b_2 + 1 \) rows and \(1 + 1 + b_2 + b_1 \) columns:

\[
D = \begin{pmatrix}
D_{11} & 0 & D_{13} & D_{14} \\
0 & 0 & D_{23} & 0 \\
0 & 1 & 0 & 0
\end{pmatrix},
\]

where \( D_{23} \) is a square block such that \( d_{ij} = 0 \) if \( i + j > e + 2 \).

Consequently,

\[
\det D = \pm \det D_{23} \cdot \det([D_{11}, D_{14}])
\]

with

\[
\det D_{23} = \pm \prod_{i=b_1+2}^{e-1} (e - 1 - i)! \cdot (x - (e - i), 2).\]
The matrix $T = [D_{11}, D_{14}] = (t_{ij})$ is one of size $b_1 + 1$. Set $F(x) = \det T$. We observe that the entries of the column $D_{11}$ are constant, and the ones from the $b_1$ columns of $D_{14}$ are polynomials of the form $x - (e - i), 2\}$ of degree 2. Therefore, the degree of the polynomial $F(x)$ is at most $2b_1$.

Let us see that

$$F(x) = cte \cdot \prod_{w=b_2+2}^{e-1} (x - w) \cdot \prod_{w=1}^{b_1} (x - w - 1/2).$$

(14)

In order to prove it, it is enough to show that $\det T$ vanishes in the points

$$\lambda = b_2 + 2, \ldots, e - 1 \quad \text{and} \quad \mu = w + 1/2, \quad \text{for} \ w = 1, \ldots, b_1.$$

Indeed, for $2 \leq j \leq b_1 + 1$ the factor $x - (e - i), 2\} = (x - e + i)(x - e + i - 1)$ divides to $t_{ij}$, therefore if $b_2 + 2 \leq \lambda \leq e - 1$, then $t_{ij}(\lambda) = 0$ for $e - \lambda \leq i \leq e - \lambda + 1$ and $2 \leq j \leq b_1 + 1$ and, consequently, $F(\lambda) = 0$, since when we replace $x$ with $\lambda$, the rows $T_{e-\lambda}$ and $T_{e-\lambda+1}$ are linear combination of $(1, 0, \ldots, 0)$.

We see that $F(\mu) = 0$ for $\mu = w + 1/2$, with $w = 1, \ldots, b_1$. We notice that the following equalities:

$$2e - 2i - 1, e - 1\}
= 2e - 1\} e - i - 1/2, \left[\begin{array}{c} e \\ 2 \end{array}\right] \cdot e - i - 1, \left[\begin{array}{c} e - 1/2 \\ 2 \end{array}\right] \}
= 2^{b_1+1} e - i - 1/2, b_1 + 1 \cdot 2^{b_2} e - i - 1, b_2 \},
\mu - e + i, 2\} = \frac{1}{2^2} 2^2 e - i - 1/2 + 1 - w, 2\},
\mu - e - i, j + b_2 - 2\} = e - 1 - i, b_2 \cdot e - 1 - i - b_2, j - 2\}$$

hold. Therefore $2^2 e - i - 1/2 + 1 - w, 2\} \cdot e - 1 - i, b_2 \}$ is a common factor in the row $i$. If we take out this factor, we obtain the matrix $R = (r_{ij})$ of size $(b_1 + 1) \times (b_1 + 1)$, with its first column defined by

$$r_{i1} = \frac{2^{b_1+1} e - i - 1/2, b_1 + 1 \cdot 2^{b_2}}{2^2 e - i - 1/2 + 1 - w, 2\},$$

and the rest ones by

$$r_{ij} = \frac{1}{2^2} e - 1 - i - b_2, j - 2\}.$$
matrices is lower than or equal to the rank of factors and the rank of these matrices is at most \( b_1 \), then the rank of \( R \) is lower than or equal to \( b_1 \) and therefore its determinant is zero. So, \( \mu \) is a root of \( F(x) \).

Consequently, the determinant of the matrix \( T \) is one of the type (14).

In order to obtain the value of the constant \( cte \), we calculate the value of the determinant in the point \( b_2 + 1 \) to conclude:

\[
\det T = (2b_2 + 1)! \cdot \prod_{w=2}^{e-2} w^{\min(w-1,e-1-w)} \cdot \prod_{w=1}^{b_1+1} w^{\min(w,2,b_1+2-w)} \\
\times \prod_{k=2}^{b_1-1} k! \cdot \frac{2^{b_1}}{(e-2)!} \cdot \prod_{w=1}^{b_1} (x - w - 1/2) \cdot \prod_{w=b_2+2}^{e-1} (x - w).
\]

Summarizing the above results and reordering the factors, we obtain the desired expression. \( \square \)

Now, we can prove our bound when the last statement of Theorem 1 holds.

**Proposition 3.15.** Suppose that \( 3l \geq p + 1 \) and \( c_0 \in \{2p - 4l - 2, 2p - 4l - 4\} \), then \( 2c \geq m - p - 2l + c_0 \).

**Proof.** Suppose that \( p + 2l - c_0 \leq m - 2c - 1 \). We have \( \alpha_{i,p} = 0 \), for all \( i \leq 2l - 1 \). In addition, \( c_0 \leq 2l - 2 \) because \( 3l \geq p + 1 \). As \( c_0 \) is even, by using Lemma 3.13, we conclude \( \alpha_{i,p-1} = 0 \), for all \( i \leq 2l \). If \( 2l = p - 3 \) and \( c_0 = 2 \), then from [1] we have \( 2c \geq m - 2p + 5 = m - p - 2l + c_0 \), impossible. So \((2l, c_0) \neq (p - 3, 2)\) and necessarily \( c_0 \geq p - 2l + 1 \), so, from Lemma 3.12, we get \( x_{p-c_0} = \cdots = x_{l+1+\lceil(p-c_0)/2\rceil} = 0 \). Let us consider the following equations:

\[
0 = \alpha_{i+p-c_0-1,p-1} \quad \text{for } i + p - c_0 - 1 \leq 2l.
\]

In the case \( c_0 = 2p - 4l - 2 \), we have a system of \( c_0/2 \) equations and \( c_0/2 \) unknowns, whose coefficient matrix is one of the type given in Lemma 2.1, for \( e = c_0/2, r = (p - 1)/2 - l + c_0/2, \) and \( t = p - 2l \). In this case, we have

\[
i_0 = p - c_0, \quad i_1 = 2l, \quad i_2 = -1, \\
i_3 = l + \frac{p - c_0 - 1}{2} - 1, \quad i_4 = l + \frac{p - 1}{2},
\]

and the intervals

\[
I_1 = \left[ -\frac{p + c_0 + 1}{2} + l, \frac{p - 3 + c_0}{2} - l \right], \quad I_2 = [1, p - 1 - 2l], \\
I_3 = [p - 2l, 3p - 6l - 6], \quad I_4 = [3, 2p - 4l - 3].
\]

Consequently, \( I_1 \cup I_2 \cup I_3 \cup I_4 \subseteq [1, p - 1] \) and the determinant is non-zero modulo \( p \) and thus, we arrive to the contradiction \( xl = 0 \).
In the case \( c_0 = 2p - 4l - 4 \), we consider the \( c_0/2 + 1 = 2l - (p - c_0 - 2) + 1 \) equations \( \alpha_{i,p-1} = 0 \), \( p - c_0 - 2 \leq i \leq 2l \), in the \( c_0/2 + 1 \) unknowns \( x'_1 = x_{l+(p-c_0-1)/2}, \ldots, x'_{c_0/2} = x_{l+(p-3)/2} \), and \( x'_{c_0/2+1} = x_l \), bearing in mind that \( x_p-c_0-1 = (-1)^{l+c_0}x_l \) and \( x_{p-c_0-2} = (-1)^{l+c_0}(l - (p - c_0) + 2)x_l \). Replacing these values and putting \( e = c_0/2 + 1, \ r = (3p - 5)/2 - 3l \), and \( t = p - 2l - 2 = c_0/2 \), the coefficient matrix is \( A = (a_{ij}) \) with

\[
a_{ij} = \begin{cases} 
\left( \frac{r - j}{t - 2j + i} \right), & \text{if } 1 \leq j \leq e, \\
\frac{l - p + 3}{t}, & \text{if } j = e \text{ and } i = 1, \\
1, & \text{if } j = e \text{ and } i = 2, \\
0, & \text{if } j = e \text{ and } 3 \leq i \leq e.
\end{cases}
\]

Consider the polynomial \( h = h(x,e) \) defined in Lemma 3.14. Developing the determinant of the above matrix by the last column we have

\[
\det A = (l - p + 3) \cdot \Delta_1 + 1 \cdot \Delta_2,
\]

with

\[
\Delta_1 = (-1)^{e-1} \frac{h(r,e)}{h(e,e)}
\]

by using Lemma 2.1, and also from Lemma 3.14 and bearing in mind that a matrix and its transposed have the same determinant, we have

\[
\Delta_2 = (-1)^e e(e-1) \frac{h(r,e)}{h(e,e)(2r-e)}.
\]

Thus,

\[
\det A = (-1)^{e-1} \frac{h(r,e)}{h(e,e)(2r-e)} \left( (l - p + 3)(2r - e) - e(e - 1) \right).
\]

Further \( (l - p + 3)(2r - e) - e(e - 1) = -(3p - 4l - 7)(p - 2l - 2) \not\equiv 0 \pmod{p} \), because \( c_0 = 2p - 4l - 4 < p \). In addition, the integer factors of the numerator and denominator of \( \det A \) have, respectively, the following bounds:

\[
1 \leq p - 2l - 1 = 2r - 2(e - 1) \leq 2r - w \leq 2r - 2 = 3p - 6l - 7 < p
\]

and

\[
2 \leq 2r - w \leq 2p - 4l - 4 = c_0 < p.
\]

Consequently, the determinant is non-zero modulo \( p \) and thus, we arrive to the contradiction \( x_l = 0 \).  \( \Box \)

4. Region with bound \( 2c \geq m - 2l - c_0 - 1 \)

We consider the invariant \( l' \) defined below Lemma 2.2. We have the following lemma.
Lemma 4.1. If $2l + l' + 1 \leq m - 2c - 1$ and $l \geq 2$, then
\[
\alpha_{l,l'+k+1} = (-1)^k \alpha_{l-k,l'+k+1} \quad \text{for } 1 \leq k \leq l - 1
\]  
holds.

Proof. Set $\alpha_{1,2l+c_0+l'} = z \neq 0$. Then $\alpha_{i,2l+c_0+l'+1-i} = (-1)^{l-1}z \neq 0$. We have
\[
0 = f(l - k, l, l' + k + 1) = \alpha_{l,l'+k+1}(-1)^{l-k}z + \alpha_{l'+k+1,l-k}(-1)^l z,
\]
for $k = 1, \ldots, l - 1$, whence the desired equality holds. \hfill \Box

Lemma 4.2. If $3l + 2 \leq m - 2c - 1$ and $l \geq 2$, then one of the following conditions holds:

1. $\alpha_{1,2l+c_0+l} \neq 0$ and $\alpha_{i,j} = (-1)^{l-i}(j-l-1) x_l$ for $i + j \leq 3l$.
2. $\alpha_{1,2l+c_0+l} = 0$, $\alpha_{1,2l+c_0+l+1} \neq 0$, and
\[
\alpha_{i,j} = (-1)^{l-i} \binom{j-l-1}{l-i} x_l, \quad \text{for } i + j \leq 3l + 1.
\]
3. $\alpha_{1,2l+c_0+l} = \alpha_{1,2l+c_0+l+1} = 0$.

Proof. We have three possibilities according as $l' = l$, $l' = l + 1$, and $l' \geq l + 2$. In the first case, from (15), we get
\[
\alpha_{l,l+k+1} = (-1)^k \alpha_{l-k,l+k+1} = (-1)^k(-1)^{l-k-1} \alpha_{1,2l} = (-1)^{l-1} \alpha_{1,2l} = x_l,
\]
for $1 \leq k \leq l - 1$. Therefore, as the values of the $l$th column are equal, we get $x_{l+k} = 0$ for $1 \leq k \leq [(l - 1)/2]$. Consequently,
\[
\alpha_{i,j} = \sum_{\lambda = i}^{[i+j-1]} (-1)^{l-i} \binom{j-\lambda-1}{\lambda-i} x_{\lambda} = (-1)^{l-i} \binom{j-l-1}{l-i} x_l,
\]
for $i + j \leq 3l$.

Suppose $l' = l + 1$. From (15) and (2) it follows
\[
\alpha_{l,l+k+2} = (-1)^k \alpha_{l-k,l+k+2} = (-1)^k(-1)^{l-l-k}(l + 1 - (l - k)) x_l
= (k + 1) x_l,
\]
for $k = 1, \ldots, l - 1$. Therefore
\[
x_{l+1} = \alpha_{l+1,l+2} = \alpha_{l,l+2} - \alpha_{l,l+3} = x_l - 2x_l = -x_l
\]
and
\[
\alpha_{l+1,l+k+2} = \alpha_{l,l+k+2} - \alpha_{l,l+k+3} = (k + 1) x_l - (k + 2) x_l
= -x_l, \quad 1 \leq k \leq l - 2.
\]
so we have the same value in the \((l+1)\)th column and this implies that \(x_{l+k} = 0\) for \(2 \leq k \leq \lfloor l/2 \rfloor\). We obtain

\[
\alpha_{i,j} = \sum_{\lambda=i}^{[i+j-1]} (-1)^{\lambda-i} \binom{j-\lambda-1}{\lambda-i} x_{l^+}
\]

\[
= (-1)^{l-i} \binom{j-l-1}{l-i} x_l + (-1)^{l+1-i} \binom{j-l-2}{l+1-i} x_{l+1}
\]

\[
= (-1)^{l-i} \left( \binom{j-l-1}{l-i} + \binom{j-l-2}{l+1-i} \right) x_l,
\]

for \(i + j \leq 3l + 1\). Finally, the third case, \(l' \geq l + 2\), follows directly from the definition of \(l'\) \(\square\)

**Lemma 4.3.** Suppose that \(2l + c_0 + 1 \leq m - 2c - 1\), \(c_0 > l \geq 5\), and \(p \notin [c_0 + 2l - 2, c_0 + 2l + 2]\), then \(\alpha_{1,2l+c_0+i} = 0\) for \(1 \leq i \leq l\).

**Proof.** Suppose, by contradiction, that \(\alpha_{1,3l+c_0} \neq 0\). As \(c_0 > l\), we can write \(2l + c_0 + 1 = 3l + 2\mu + e\), with \(e \in \{0, 1\}\) and \(\mu \geq 1\). As \(3l \leq m - 2c - 1\), from Lemma 2.2 we obtain \(l' = l\). Consequently, from Lemma 4.2 we have that all the values of the submatrix \(T_{3l}\) are given by the formula

\[
\alpha_{i,j} = (-1)^{l-i} \binom{j-l-1}{l-i} x_l. \tag{16}
\]

The following assertion holds:

If \(3l + \lambda \leq m - 2c - 1\) and \(2 \leq \lambda \leq 2\mu + e\) then \(\alpha_{l+1,2l+c_0+i} = 0\), for \(1 \leq i \leq \lambda - 1\), and \(x_{l+j} = 0\), for \(1 \leq j \leq \lfloor l/2 \rfloor + \lfloor \lambda/2 \rfloor - 1\).

We prove that assertion by induction on \(\lambda\). Set \(l = 2l'' + e''\), with \(e'' \in \{0, 1\}\). For \(\lambda = 2\), we have \(3l + 2 \leq m - 2c - 1\), and, from Lemma 4.2, \(x_{l+j} = 0\), for \(1 \leq j \leq \lfloor (l - 1)/2 \rfloor\). So

\[
f(l-1,l+1,l+2) = \alpha_{l+2,l-1}\alpha_{2l+1+c_0,l+1} = 0,
\]

whence \(\alpha_{2l+1+c_0,l+1} = 0\). By using this zero and from the definition of the number \(l'\) we have

\[
\alpha_{i,3l+c_0+1-i} = (-1)^{l-i} z \neq 0, \quad \alpha_{i,3l+c_0+2-i} = (-1)^{l-1}(l+1-i)z \neq 0,
\]

for \(z = \alpha_{1,2l+c_0+l}\). Consequently

\[
f(1,l+[l/2],l+[l/2]+1) = x_{l+[l/2]l} \alpha_{3l+c_0+1-e'',1} = 0,
\]

whence \(x_{l+[l/2]} = 0\). So, for \(\lambda = 2\), the result is true.
Suppose $\lambda < 2\mu + e$, and that the assertion holds for $\lambda$. Let us prove it for $\lambda + 1$. The inductive hypothesis origins $\alpha_{l+1,2l+c_0+i} = 0$, for $1 \leq i \leq \lambda - 1$ and $x_{l+j} = 0$, for $1 \leq j \leq \lfloor l/2 \rfloor + \lfloor \lambda/2 \rfloor - 1$. It remains to prove that $\alpha_{l+1,2l+c_0+\lambda} = 0$, and $x_{l+(l/2)+[(\lambda+1)/2]-1} = 0$. Set $w = \alpha_{l+1,2l+c_0+\lambda}$. Clearly the following equality holds:

$$\alpha_{l+k,2l+c_0+\lambda+1-k} = (-1)^{k-1}w, \quad \text{for } 1 \leq k \leq \lambda.$$ 

Let us denote $\lambda = 2\lambda' + e'$. Then

$$3l + 2[\lambda/2] + e' + 1 = 3l + \lambda + 1 \leq m - 2e - 1,$$

and so,

$$f(l-e',l+[\lambda/2]+e',l+[\lambda/2]+1+e')$$

$$= \alpha_{l-e',l+[\lambda/2]+e'}\alpha_{2l+[\lambda/2]+c_0,l+[\lambda/2]+1+e'} + \alpha_{l+[\lambda/2]+1+e',l-e'}\alpha_{2l+[\lambda/2]+1+c_0,l+[\lambda/2]+e'}$$

$$= \alpha_{l-e',l+[\lambda/2]+e'}(-1)^{l+[\lambda/2]+1+e'}w$$

$$+ \alpha_{l+[\lambda/2]+1+e',l-e'}(-1)^{l+[\lambda/2]+e'}w$$

$$= (-1)^{l+[\lambda/2]+1+e'}(\alpha_{l-e',l+[\lambda/2]+e'} + \alpha_{l-e',l+[\lambda/2]+1+e'})w = 0.$$ 

But $\alpha_{l-e',l+[\lambda/2]+e'} + \alpha_{l-e',l+[\lambda/2]+1+e'}$ is equal to $2x_l$ or $-(2[\lambda/2]+1)x_l$ according to $e' = 0$ or $e' = 1$, respectively. As $\lambda + 1 \leq 2\mu + e = c_0 + 1 - l < p$, we necessarily have $w = 0$. We conclude:

$$\alpha_{1,2l+c_0+1} = \cdots = \alpha_{l-1,2l+c_0+1} = 0, \quad \alpha_{l,2l+c_0+1} = (-1)^{l-1}z,$$

$$\alpha_{l+1,2l+c_0+1} = \cdots = \alpha_{l+\lambda,2l+c_0+1} = 0.$$ 

Therefore

$$\alpha_{i,j} = \sum_{u=1}^{l+\lambda} (-1)^{u-i} \binom{j-(2l+c_0+1)}{u-i} \alpha_{u,2l+c_0+1}$$

$$= (-1)^{-i} \binom{j-(2l+c_0+1)}{l-i} \alpha_{l,2l+c_0+1}$$

$$= (-1)^{i+1} \binom{j-(2l+c_0+1)}{l-i} z,$$

for $1 \leq i \leq l+\lambda$, $j \geq 2l + c_0 + 1$, $i + j \leq 3l + c_0 + \lambda + 1$.

Let us prove that $x_{l+[l/2]+[(\lambda+1)/2]-1} = 0$. We can suppose that $\lambda$ is odd, otherwise $[(\lambda+1)/2] = [\lambda/2]$ and the result follows from the induction hypothesis. We have $\alpha_{i+1,2l+c_0+i} = 0$, for $1 \leq i \leq \lambda$. Therefore $\alpha_{i,j} = 0$, for $i \geq l+1$, $j \geq 2l + c_0 + 1$, and $i + j \leq 3l + c_0 + \lambda + 1$.

We have $\lambda + 1 = 2(\lambda' + 1)$, and we have to show that $x_{l+[l/2]+\lambda'} = 0$. 


Let us consider the triple \((1, l + [l/2] + \lambda', l + [l/2] + \lambda' + 1)\) in the level \(2l + 2[l/2] + 2\lambda' + 2 \leq 3l + \lambda + 1 \leq m - 2c - 1\). We consider three cases:

1. If \(\lambda' \leq [l/2] - 2 + e''\), then \(2 + l + [l/2] + \lambda' \leq 2l\) and \(\alpha_{1,l+[l/2]+\lambda'} = 0 = \alpha_{l+[l/2]+\lambda'+1,1}\), so

\[
0 = f\left(1, 1 + [l/2] + \lambda', l + [l/2] + \lambda' + 1\right)
= x_{l+[l/2]+\lambda'}\alpha_{2l+[l/2]+2\lambda'+1+c_0,1},
\]

but

\[
\alpha_{1,3l+c_0+i} = \binom{l + i - 1}{i} z \neq 0, \quad \text{for } 0 \leq i \leq \lambda.
\]

In particular, \(\alpha_{2l+2[l/2]+2\lambda'+1+c_0,1} \neq 0\), whence \(x_{l+[l/2]+\lambda'} = 0\).

2. Suppose now \(\lambda' \geq [l/2] + e''\). Then \(l + [l/2] + \lambda' \geq l + 1, l + [l/2] + \lambda' + 1 + c_0 \geq 2l + c_0 + 1\) and \(2l + 2[l/2] + 2\lambda' + 2 + c_0 \leq 3l + c_0 + \lambda + 1\), so

\[
\alpha_{l+[l/2]+\lambda'+1,l+[l/2]+\lambda'+2+c_0} = \alpha_{l+[l/2]+\lambda'+1,l+[l/2]+\lambda'+1+c_0} = 0,
\]

and consequently

\[
0 = f\left(1, 1 + [l/2] + \lambda', l + [l/2] + \lambda' + 1\right)
= x_{l+[l/2]+\lambda'}\alpha_{2l+[l/2]+2\lambda'+1+c_0,1},
\]

and again, \(x_{l+[l/2]+\lambda'} = 0\).

3. Finally, we consider the case \(\lambda' = [l/2] - 1 + e''\). Then \(\lambda = 2\lambda' + 1 = 2[l/2] + 2e'' = l + 1 + e''\), and

\[
0 = f\left(1, 1 + [l/2] + \lambda', l + [l/2] + \lambda' + 1\right) = f\left(1, 2l - 1, 2l\right)
= x_{2l-1}\alpha_{4l-1+c_0,1},
\]

because \(\alpha_{1+2l+c_0,2l-1} = -\alpha_{2l-1,1+2l+c_0} = 0\), since \(2l - 1 \leq l + \lambda = 2l - 1 + e''\), and it is a value in the portion of diagonal \(2l + c_0 + 1\), from \(l + 1\) to \(l + \lambda\). Therefore, \(x_{2l-1} = 0\).

From the above, the assertion holds for \(\lambda + 1\). Setting \(\lambda = 2\mu + e\), the submatrix \(T_{2l+c_0+1-e-e''}\) is determinated and consequently also the submatrix \(T_{2l+c_0+1-e-e''}\). In fact,

\[
\alpha_{i,j} = \sum_{\eta=i}^{[i+j-1]/2} (-1)^{\eta-i} \binom{j-\eta-1}{\eta-i} x_{\eta} = (-1)^{l-i} \binom{j-l-1}{l-i} x_{l},
\]

for \(i + j \leq 2l + c_0 - 1\),

being \(x_{l+j} = 0\) for \(j \leq [(c_0 - 2)/2]\). In addition, also we have determinated the triangle lying on the portion of diagonal from \(\alpha_{1,2l+c_0+1}\) to \(\alpha_{l+\lambda'-1,2l+c_0+1} = \alpha_{c_0,2l+c_0+1}\).
As $l \geq 5$, we can consider the zeroes
\[ \alpha_{i, 2l + c_0 + 1} \sum_{\eta=i}^{l+[(c_0+i)/2]} (-1)^{\eta-i}(2l + c_0 + 1 - \eta - 1) x_\eta = 0, \]
for $i = 1, 2, 3, 4$. If $c_0$ is even, the first three zeroes constitute a system of three equations in the unknowns $x_l, x_{l+c_0}/2, x_{l+c_0/2+1}$ whose determinant is
\[ \frac{1}{24} \frac{1}{c_0+3} \left( \frac{l+c_0}{l-1} \right) c_0(2l + c_0 + 1)(2l + c_0)(2l + c_0 - 1) \equiv 0 \pmod{p}. \]
If $c_0$ is odd, the four zeroes constitute a system of four equations in the unknowns $x_l, x_{l+(c_0-1)/2}, x_{l+(c_0+1)/2}, x_{l+(c_0+3)/2}$ whose determinant is
\[ \frac{1}{4!} \frac{1}{5!} \frac{1}{(c_0+4)(c_0+2)} \left( \frac{l+c_0}{l-1} \right) (c_0-1)(c_0+1)(2l + c_0 - 2)
\cdot (2l + c_0 - 1)(2l + c_0)^2 (2l + c_0 + 1)(2l + c_0 + 2) \equiv 0 \pmod{p}. \]
In any case, we get $p \in [2l+c_0-2, 2l+c_0+2]$, contradicting the hypothesis. \qed

Let us denote $y_j = \alpha_{1, 2l+j}$.

**Lemma 4.4.** If $3l + \mu \leq m - 2c - 1$ and $l \geq \mu + 2 \geq 2$, then one of the following cases holds:

1. $y_{c_0+l} \neq 0$, \quad $y_i = \left( \frac{l+i-1}{l-1} \right) y_0$, \quad $x_{l+i} = 0$ \quad for $1 \leq i \leq \lfloor (l-1)/2 \rfloor$.

2. $y_{c_0+l+i} = 0$ \quad for $0 \leq i \leq \mu - 2$, \quad $y_{c_0+l+\mu-1} \neq 0$,
\[ x_{l+\mu-1} + (-1)^\mu x_l = 0, \quad x_{l+\mu-2} - (-1)^\mu (\mu - 1) x_l = 0, \quad \text{and} \]
\[ x_{l+i} = 0 \quad \text{for} \quad \mu \leq i \leq \lfloor (l + \mu - 2)/2 \rfloor. \]

3. $y_{c_0+l+i} = 0$ \quad for $0 \leq i \leq \mu \leq l - 1$.

Moreover, in any case $y_{c_0+i} = 0$ for $1 \leq i \leq l - 1$.

**Proof.** As $3l \leq 3l + \mu \leq m - 2c - 1$, from Lemma 2.2 we deduce that $y_{c_0+i} = 0$ for $1 \leq i \leq l - 1$.

In order to prove the other assertion, we argue by induction. For $\mu = 2$, the statement holds by Lemma 4.2. Suppose that it is true for $\lambda < \mu$, and let us prove it for $\lambda + 1 \leq \mu$. As $3l + \lambda \leq 3l + \lambda + 1 \leq 3l + \mu \leq m - 2c - 1$, from the inductive hypothesis we deduce that one of the following cases can hold:

1. $y_{c_0+l} \neq 0$, \quad $y_k = \left( \frac{l+k-1}{l-1} \right) y_0$, \quad $x_{l+k} = 0$ \quad for $1 \leq k \leq \lfloor (l-1)/2 \rfloor$.

2. $y_{c_0+l+i} = 0$ \quad for $0 \leq i \leq \lambda - 2$, \quad $y_{c_0+l+\lambda-1} \neq 0$,
\[ x_{l+\lambda-1} + (-1)\lambda x_l = 0, \quad x_{l+\lambda-2} - (-1)\lambda (\lambda - 1) x_l = 0 \quad \text{and} \]
\[ x_{l+i} = 0 \quad \text{for } \lambda \leq i \leq \left( l + \lambda - 2 \right) / 2. \]

3. \( y_{c_0+l+i} = 0 \quad \text{for } 0 \leq i \leq \lambda \leq l - 1. \)

We claim that if \( y_{c_0+i} = 0 \) and \( 3l + \lambda + 1 \leq m - 2c - 1 \), then \( y_{c_0+l+\lambda-1} = 0 \), and, consequently, the second possibility does not hold. Effectively, suppose \( y_{c_0+l+\lambda-1} = z \neq 0 \) and set \( w = y_{c_0+l+\lambda-1+l+\lambda} \). Then we have \( \alpha_{l,3l+c_0+\lambda-1} = (-1)^{l-1}z \), for \( 1 \leq i \leq l + \lambda - 1 \), and \( \alpha_{l+1,3l+c_0+\lambda-1+i} = (-1)^{l-1}w + (-1)^{l+1}(i-1)z \), for \( 1 \leq i \leq l + \lambda \). In addition, bearing in mind that the second possibility holds, we have \( x_{l+\lambda-1} = (-1)^{l-1}x_l \) and consequently

\[
\begin{align*}
f(l - \lambda, l + \lambda, l + \lambda + 1) &= (-1)^{l-\lambda-1}y_0(-1)^{l+\lambda}(l + \lambda - 1)z - (l + \lambda)z \\
&= (-y_0)(-z) = y_0z,
\end{align*}
\]

therefore \( y_0 = 0 \) or \( z = 0 \), which is impossible. Consequently, if \( y_{c_0+l} = 0 \) and \( 3l + \lambda + 1 \leq m - 2c - 1 \), then \( y_{c_0+l+\lambda-1} = 0 \).

If \( y_{c_0+l+\lambda} = 0 \), we have case 3 of the lemma for \( \lambda + 1 \). If \( u = y_{c_0+l+\lambda} \neq 0 \), we must prove the conditions given in the second case of the lemma for \( \lambda + 1 \). Effectively, if we take the triples \( (l-k, l+\lambda, l+k+1) \), with \( \lambda \leq k \leq l - 1 \), we deduce that \( f(l-k, l+\lambda, l+k+1) = (-1)^{l-k-1}u(-\alpha_{l+\lambda,l+k+1} + (-1)^{l+1}x_l) \), and so \( \alpha_{l+\lambda,l+k+1} = (-1)^\lambda x_l \). Consequently, we get that \( x_{l+\lambda} = (-1)^\lambda x_l \) and \( x_{l+i} = 0 \) for \( \lambda + 1 \leq i \leq [(l + \lambda - 1) / 2] \).

Moreover,

\[
f(l - \lambda + 2, l + \lambda - 1, l + \lambda) = (-1)^l u((-1)^\lambda x_{l+\lambda-1} + \lambda x_l) = 0,
\]

therefore \( x_{l+\lambda-1} = (-1)^{l+1}x_l \) and the lemma is satisfied for \( \lambda + 1 \). That completes the proof. \( \square \)

**Lemma 4.5.** Suppose that \( 2l + c_0 + 1 \leq m - 2c - 1 \), \( l \geq (p + 5) / 6 \), \( c_0 > l \geq 5 \), and \( l + c_0 = (p - 1) / 2 \). Then, \( y_{c_0+\delta} = 0 \) for \( 1 \leq \delta \leq c_0 - 1 \).

**Proof.** Let \( 2l + c_0 + 1 = 3l + \mu \), with \( \mu \geq 0 \). Clearly the condition \( l \geq \mu + 2 \) is equivalent to \( l \geq (p + 5) / 6 \), given in the hypothesis.
As \( l \geq \mu + 2 \) and \( 3l + \mu \leq m - 2c - 1 \), we have, from Lemma 4.4, that one of the conditions 1–3 holds.

Moreover, \( 3l \leq m - 2c - 1 \), so \( y_{c_0+1} = \cdots = y_{c_0+l-1} = 0 \). In addition, we have \( 2l + c_0 + 1 \leq m - 2c - 1 \), \( c_0 > l \geq 5 \), and \( p \notin [2l + c_0 - 2, 2l + c_0 + 2] \), because \( 2l + c_0 = p - c_0 - 1 \). So, from Lemma 4.3, we obtain \( y_{c_0+l} = 0 \) and case 1 of Lemma 4.4 cannot hold. So we have the second or the third condition. Anyway, we have that \( y_{c_0+\delta} = 0 \) for \( 1 \leq \delta \leq \mu - 2 + l \). But \( l + \mu = c_0 + 1 \), therefore,

\[
y_{c_0+\delta} = 0, \quad \text{for } 1 \leq \delta \leq c_0 - 1. \quad \square
\]

We can prove the main part of Theorem 2.

**Proof.** The cases \( p \leq 19 \) are analysed in [6]. So we can assume \( p > 19 \), whence \( l \geq 5 \). Suppose that \( 2l + c_0 + 1 \leq m - 2c - 1 \). If \( c_0 \leq l \), arguing as in Lemma 2.2, we get

\[
f(c_0 - k, l, l + 1) = \alpha_{l,l+1} \alpha_{2l+c_0+1,c_0-k} = 0, \quad \text{for } 1 \leq k \leq c_0 - 1.
\]

Consequently,

\[
\alpha_{1,2l+c_0+1} = \cdots = \alpha_{1,2l+c_0+c_0-1} = 0. \tag{17}
\]

Suppose \( c_0 > l \geq 5 \). From Lemma 4.5, we have that (17) also holds. Therefore (17) holds in any case. Let us call \( \alpha_{1,2l+2c_0} = \alpha_{1,p-1} = z \). In addition, \( \alpha_{1,2l+2c_0+i} = \alpha_{1,p-1+i} = \alpha_{1,i} = 0 \) for \( 1 \leq i \leq 2l - 1 \). We have that \( 2l + c_0 + 1 \leq m - 2c - 1 \), so \( 2l + c_0 + 1 + c \leq m - c - 1 \). We have two possibilities: either \( c = c_0 = (p - 1)/2 - l \) or \( c > c_0 \); so \( c \geq c_0 + p - 1 \) and \( 2l + 2c_0 + p \leq m - c - 1 \). Suppose that the last case happens. We have

\[
\alpha_{1,2l+c_0+1} = 0, \quad \cdots, \quad \alpha_{1,p-2} = 0, \quad \alpha_{1,p-1} = z, \quad \alpha_{1,p} = 0, \quad \cdots, \quad \alpha_{1,p+2l-2} = 0,
\]

namely, a portion of 1st column of length \( c_0 + 2l - 1 \), that creates a triangle with sides of length \( c_0 + 2l - 1 \), that is, \( c_0 + 2l - 1 \) columns. The extreme step of the row \( i + j = p + 2l - 1 = 4l + 2c_0 \) corresponds to \( i + i + 2 = 4l + 2c_0 \), therefore \( i = 2l + c_0 - 1 \) and, so, the triangle \( T_{2l+2c_0+2l} = T_{p-1+2l} \) can be given in terms of \( z \), in particular, from the definition of \( l, z \neq 0 \).

We have a formula that gives us the values of the triangle as a function of its first column,

\[
\alpha_{i,j} = \sum_{w=j}^{j+i-1} (-1)^{w-j} \binom{i-1}{w-j} \alpha_{1,w}.
\]

The values \( \alpha_{1,2l+c_0}, \alpha_{1,2l+c_0-1}, \alpha_{1,2l+c_0-2} \) can be given in terms of \( z \). We have:
Simplifying, we get

\[ (-1)^{c_0-1} \left( \frac{c_0 + 2l - 2}{c_0 - 1} \right) z = \alpha_{c_0 + 2l - 1, c_0 + 2l + 1} \]

\[ = \alpha_{c_0 + 2l - 1, c_0 + 2l} = (-1)^{c_0} \left( \frac{c_0 + 2l - 2}{c_0} \right) z + \alpha_{1, c_0 + 2l}. \]

\[ (-1)^{c_0} \left( \frac{c_0 + 2l - 3}{c_0} \right) z + \alpha_{1, c_0 + 2l} \]

\[ = \alpha_{c_0 + 2l - 2, c_0 + 2l} = \alpha_{c_0 + 2l - 2, c_0 + 2l - 1} \]

\[ = (-1)^{c_0 + 1} \left( \frac{c_0 + 2l - 3}{c_0 + 1} \right) z + \alpha_{1, c_0 + 2l - 1} - \left( \frac{c_0 + 2l - 3}{1} \right) \alpha_{1, c_0 + 2l}, \]

\[ (-1)^{c_0 + 1} \left( \frac{c_0 + 2l - 4}{c_0 + 1} \right) z + \alpha_{1, c_0 + 2l - 1} - \left( \frac{c_0 + 2l - 4}{1} \right) \alpha_{1, c_0 + 2l} \]

\[ = \alpha_{c_0 + 2l - 3, c_0 + 2l - 1} = \alpha_{c_0 + 2l - 3, c_0 + 2l - 2} \]

\[ = (-1)^{c_0} \left( \frac{c_0 + 2l - 4}{c_0 + 2} \right) z + \alpha_{1, c_0 + 2l - 2} - \left( \frac{c_0 + 2l - 4}{2} \right) \alpha_{1, c_0 + 2l - 1} \]

\[ + \left( \frac{c_0 + 2l - 4}{2} \right) \alpha_{1, c_0 + 2l}. \]

Simplifying, we get

\[ \alpha_{1, c_0 + 2l} = (-1)^{c_0 + 1} \left( \frac{c_0 + 2l - 1}{c_0} \right) z, \]

\[ \alpha_{1, c_0 + 2l - 1} = \left( \frac{c_0 + 2l - 2}{1} \right) \alpha_{1, c_0 + 2l} + (-1)^{c_0} \left( \frac{c_0 + 2l - 2}{c_0 + 1} \right) z, \]

\[ \alpha_{1, c_0 + 2l - 2} = \left( \frac{c_0 + 2l - 3}{1} \right) \alpha_{1, c_0 + 2l - 1} - \left( \frac{c_0 + 2l - 3}{2} \right) \alpha_{1, c_0 + 2l} \]

\[ + (-1)^{c_0 + 1} \left( \frac{c_0 + 2l - 3}{c_0 + 2} \right) z. \] (18)

On the other hand, we have that

\[ f(1, 2, c_0 + 2l - 2) = \alpha_{2, c_0 + 2l - 2}(-z) + \alpha_{1, c_0 + 2l - 2}(-z) = 0, \]

so \( \alpha_{2, c_0 + 2l - 2} = -\alpha_{1, c_0 + 2l - 2} \), but \( \alpha_{1, c_0 + 2l - 1} + \alpha_{2, c_0 + 2l - 2} = \alpha_{1, c_0 + 2l - 2} \); that is,

\[ 2\alpha_{1, c_0 + 2l - 2} = \alpha_{1, c_0 + 2l - 1}. \] (19)

From (18) and (19), we get a system of four equations in the unknowns \( z, \alpha_{1, c_0 + 2l}, \alpha_{1, c_0 + 2l - 1}, \alpha_{1, c_0 + 2l - 2} \), whose coefficient matrix is

\[
\begin{pmatrix}
0 & 0 & 1 & -2 \\
(1)^{c_0-1} \left( \frac{c_0 + 2l - 1}{c_0} \right) & 1 & 0 & 0 \\
(1)^{c_0} \left( \frac{c_0 + 2l - 2}{c_0 + 1} \right) & c_0 + 2l - 2 & -1 & 0 \\
(1)^{c_0} \left( \frac{c_0 + 2l - 3}{c_0 + 2} \right) & \left( \frac{c_0 + 2l - 3}{2} \right) & -(c_0 + 2l - 3) & 1
\end{pmatrix}.
\] (20)
Since $2l \equiv -2c_0 - 1 \pmod{p}$, the determinant of this matrix modulo $p$ is
\[
-1)^{c_0}(c_0 + 2l - 3)!/(c_0 + 1)^3
\]

This number is non-zero modulo $p$, so $x_l = 0$, that is impossible. □

Acknowledgment

We thank the referee his suggestions and comments on the final version of this paper.

References