Remarks on the Lie derived lengths of group algebras of groups with cyclic derived subgroup

Zsolt Balogh\textsuperscript{a}, Tibor Juhász\textsuperscript{b}

\textsuperscript{a}Institute of Mathematics and Informatics, College of Nyíregyháza
e-mail: baloghzs@nyf.hu

\textsuperscript{b}Institute of Mathematics and Informatics, Eszterházy Károly College
e-mail: juhaszti@ektf.hu

Submitted 20 June 2007; Accepted 10 November 2007

\textit{In memoriam Professor Péter Kiss}

Abstract

The aim of this paper is to give a new elementary proof for our previous theorem, in which the Lie derived length and the strong Lie derived length of group algebras are determined in the case when the derived subgroup of the basic group is cyclic of odd order.

Keywords: Group algebras, Lie derived length

MSC: 16S34, 17B30

1. Introduction

The group algebra $FG$ of a group $G$ over a field $F$ may be considered as a Lie algebra with the usual bracket operation $[x, y] = xy - yx$. Denote by $[X, Y]$ the additive subgroup generated by all Lie products $[x, y]$ with $x \in X$ and $y \in Y$, and define the Lie derived series and the strong Lie derived series of the group algebra $FG$ respectively, as follows: let $\delta^{(0)}(FG) = \delta^{(0)}(FG) = FG$ and

\[
\delta^{[n+1]}(FG) = [\delta^{[n]}(FG), \delta^{[n]}(FG)], \\
\delta^{(n+1)}(FG) = [\delta^{(n)}(FG), \delta^{(n)}(FG)]FG.
\]

We say that $FG$ is Lie solvable if $\delta^{[m]}(FG) = 0$ for some $m$ and the number $dl_L(FG) = \min\{m \in \mathbb{N} \mid \delta^{[m]}(FG) = 0\}$ is called the Lie derived length of $FG$. 

Similarly, $FG$ is said to be strongly Lie solvable of derived length $\text{dll}(FG) = m$ if $\delta^{(m)}(FG) = 0$ and $\delta^{(m-1)}(FG) \neq 0$. Evidently, $\delta^{[i]}(FG) \subseteq \delta^{(i)}(FG)$ for all $i$.

For $m \geq 0$ let

$$s^{(m)}_l = \begin{cases} 
1 & \text{if } l = 0; \\
2s^{(m)}_{l-1} + 1 & \text{if } s^{(m)}_{l-1} \text{ is divisible by } 2^m; \\
2s^{(m)}_{l-1} & \text{otherwise}.
\end{cases}$$

In [1] we proved the following

**Theorem 1.1** (Z. Balogh and T. Juhász [1]). Let $G$ be a group with cyclic derived subgroup of order $p^n$, where $p$ is an odd prime, and let $F$ be a field of characteristic $p$. If $G/C_G(G')$ has order $2^n p^s$, then

$$\text{dll}(FG) = \text{dll}(F) = d + 1,$$

where $d$ is the minimal integer for which $s^{(m)}_d \geq p^n$ holds. Otherwise,

$$\text{dll}(FG) = \text{dll}(F) = \lfloor \log_2(2p^n) \rfloor.$$

This article can be considered as a supplement to [1]. In the original proof of the theorem, at the discussion of the cases when either $G/C_G(G')$ has order $2p^s$, or the order of $G/C_G(G')$ is divisible by some odd prime $q \neq p$, Theorem A and B from [3] play the central role. Two lemmas are shown here, which enable us to construct a new (elementary) proof of Theorem 1.1 avoiding the use of above-mentioned results of A. Shalev. For a change, we prove these two lemmas by two different ways (the first was proposed by the referee, whereat we wish to thank him), although both statements could be proved by both methods which will be presented here.

We denote by $\omega(FG)$ the augmentation ideal of $FG$. It is well-known that $\omega(FG)$ is nilpotent if and only if $G$ is a finite $p$-group and $\text{char}(F) = p$. The nilpotency index of $\omega(FG)$ will be denoted by $t(G)$. For a normal subgroup $H \subseteq G$ we mean by $\mathfrak{l}(H)$ the ideal $FG \cdot \omega(FH)$. For $x, y \in G$ let $x^y = y^{-1}xy$ and $(x, y) = x^{-1}x^y$, furthermore, denote by $\zeta(G)$ the center of the group $G$. We shall use freely the identities

$$[x, yz] = [x, y]z + y[x, z], \quad [xy, z] = x[y, z] + [x, z]y,$$

and for units $a, b$ the equality $[a, b] = ba((a, b) - 1)$.

## 2. Proof of Theorem 1.1

Let $G$ be a group with derived subgroup $G' = \langle x \mid x^{p^n} = 1 \rangle$ where $p$ is an odd prime, and let $F$ be a field of characteristic $p$. As it is well-known, the automorphism group of $G'$ is isomorphic to the unit group $U(\mathbb{Z}_{p^n})$ of $\mathbb{Z}_{p^n}$. Furthermore, $U(\mathbb{Z}_{p^n})$ is cyclic, so the factor group $G/C_G(G')$, which is isomorphic to a subgroup of $U(\mathbb{Z}_{p^n})$, is cyclic, too. We distinguish the following two cases according to the order of $G/C_G(G')$. 

2.1. $G/C$ has order $2^mp^r$

Let $d$ be the minimal integer for which $s_d^{(m)} \geq p^n$ holds.

First suppose that $m = 0$. Then, as is easy to check (see [1]), the group $G$ is nilpotent, and by [2], $dl_L(FG) = dl^L(FG) = \lceil \log_2 (p^n + 1) \rceil$. Since

$$2^d - 1 = s_d^{(0)} < p^n \leq s_d^{(0)} = 2^{d+1} - 1,$$

we have $d < \log_2 (p^n + 1) \leq \lceil \log_2 (p^n + 1) \rceil \leq d + 1$, thus Theorem 1.1 is proved for the case in point.

Let now $m \geq 1$. To prove that $d + 1$ is an upper bound on $dl^L(FG)$ it is sufficient to show that

$$\delta^{(l+1)}(FG) \subseteq \mathcal{J}(G')^{s_l^{(m)}} \text{ for all } l \geq 0.$$  

This is clear for $l = 0$. For the induction we need Lemma 2 from [1], which states that

$$\mathcal{J}(G')^{j2^m}, \mathcal{J}(G')^{j2^m} \subseteq \mathcal{J}(G')^{j2^m + j2^m + 1}. \quad (2.1)$$

Hence, assuming that $\delta^{(l)}(FG) \subseteq \mathcal{J}(G')^{s_{l-1}^{(m)}}$, we obtain

$$\delta^{(l+1)}(FG) = [\delta^{(l)}(FG), \delta^{(l)}(FG)]FG \subseteq [\mathcal{J}(G')^{s_{l-1}^{(m)}}, \mathcal{J}(G')^{s_{l-1}^{(m)}}]FG \subseteq \mathcal{J}(G')^{s_l^{(m)}}.$$  

Therefore, $dl^L(FG) \leq d + 1$. Now, we shall prove that $d + 1 \leq dl_L(FG)$. Let us choose an element $aC_G(G')$ of order $2^m$ from $G/C_G(G')$ and consider the group $H = \langle x, a \rangle$ and set $x^k = x^a$. In particular, when $m = 1$, we have that $a^2 \in \zeta(H)$, $x^a = x^{-1}$, and the quotient group $H = H/\zeta(H)$ is isomorphic to the dihedral group of order $2p^n$. This case is treated in the next lemma.

**Lemma 2.1.** Let $G$ be the dihedral group of order $2p^n$ for some odd prime $p$, and let $\text{char}(F) = p$. Then $dl_L(FG) \geq d + 1$, where $d$ is the minimal integer such that $s_d^{(1)} \geq p^n$.

**Proof.** Write the group $G$ as $\langle a, x \mid a^2 = x^{2^n} = 1, xa = ax^{-1} \rangle$ and set $s_1 = s_1^{(1)}$. We shall show that $(x - x^{-1})^{s_l - 1} \in \delta^{[l]}(FG)$ if $l$ is odd, and $(x - x^{-1})^{s_l - 1 + 1} \in \delta^{[l]}(FG)$ if $l$ is even; further

$$a(x - x^{-1})^{s_l - 1} \in \delta^{[l]}(FG) \quad \text{and} \quad ax(x - x^{-1})^{s_l - 1} \in \delta^{[l]}(FG).$$

For, if $l = 1$ then $x - x^{-1} = [a, ax] \in \delta^{[1]}(FG)$, $a(x - x^{-1}) = [a, x] \in \delta^{[1]}(FG)$ and $ax(x - x^{-1}) = [ax, x] \in \delta^{[1]}(FG)$.

If $l$ is even then, by induction, the elements

$$(x - x^{-1})^{s_l - 2}, a(x - x^{-1})^{s_l - 2}, ax(x - x^{-1})^{s_l - 2}$$

are
belong to \(\delta^{[l-1]}(FG)\). Since \((x - x^{-1})^2\) is central and \(s_{l-2}\) is odd,
\[
[ax(x - x^{-1})^{s_{l-2}}, a(x - x^{-1})^{s_{l-2}}] = [ax(x - x^{-1}), a(x - x^{-1})](x - x^{-1})^{2s_{l-2} - 2} \\
= a(x - x^{-1})[x, a(x - x^{-1})](x - x^{-1})^{2s_{l-2} - 2} \\
= (x - x^{-1})^{2s_{l-2} + 1} = (x - x^{-1})^{s_{l-1} + 1},
\]
Thus \((x - x^{-1})^{s_{l-1} + 1} \in \delta^{[l]}(FG)\). Furthermore,
\[
\left[\frac{1}{2} a(x - x^{-1})^{s_{l-2}}, (x - x^{-1})^{s_{l-2}}\right] = \left[\frac{1}{2} a(x - x^{-1})^{s_{l-2}}, (x - x^{-1})^{s_{l-2}}\right]x \\
= \frac{1}{2} ax(x - x^{-1})^{s_{l-2}}, (x - x^{-1})^{s_{l-2}} \\
= ax(x - x^{-1})^{s_{l-1}},
\]
so the elements \(a(x - x^{-1})^{s_{l-1}}\) and \(ax(x - x^{-1})^{s_{l-1}}\) belong to \(\delta^{[l]}(FG)\).

Now, if \(l\) is odd then \(s_{l-2}\) is even, and by the inductive hypothesis
\((x - x^{-1})^{s_{l-1} + 1}, a(x - x^{-1})^{s_{l-2}}, ax(x - x^{-1})^{s_{l-2}} \in \delta^{[l-1]}(FG)\).

As above,
\[
[a(x - x^{-1})^{s_{l-2}}, ax(x - x^{-1})^{s_{l-2}}] = [a, ax](x - x^{-1})^{2s_{l-2}} \\
= (x - x^{-1})^{2s_{l-2} + 1} \\
= (x - x^{-1})^{s_{l-1}} \in \delta^{[l]}(FG),
\]
and
\[
\frac{1}{2} a(x - x^{-1})^{s_{l-2}}, (x - x^{-1})^{s_{l-2} + 1}] = \frac{1}{2} a(x - x^{-1})(x - x^{-1})^{2s_{l-2}} \\
= a(x - x^{-1})^{2s_{l-2}} \\
= a(x - x^{-1})^{s_{l-1}} \in \delta^{[l]}(FG),
\]
and finally
\[
\frac{1}{2} ax(x - x^{-1})^{s_{l-2}}, (x - x^{-1})^{s_{l-2} + 1}] = \frac{1}{2} a(x - x^{-1})^{s_{l-2}}, (x - x^{-1})^{s_{l-2} + 1}][x \\
= ax(x - x^{-1})^{s_{l-1}} \in \delta^{[l]}(FG).
\]

Induction is complete.

Let \(d\) be the minimal integer such that \(s_d \geq p^n\). Then \(s_{d-1} < p^n\) and
\(a(x - x^{-1})^{s_{d-1}} = ax^{-s_{d-1}}(x^2 - 1)^{s_{d-1}}\)
is nonzero element of \(\delta^{[d]}(FG)\) (by the binomial theorem as the order of \(x^2\) is \(p^n\)).
Thus \(d\ll(FG) > d\) and the statement follows. \(\square\)
The following line shows the truth of Theorem 1.1 for the case \( m = 1 \):

\[
d + 1 \leq dl_L(FH) \leq dl_L(FG).
\]

Let us turn to the case \( m > 1 \). Since \((x, a) = x^{-1+k} \in H'\) and \( k \not\equiv 1 \pmod{p} \), we have that \( H' \) has order \( p^n \). Moreover, \( H/C_H(H') \) has order \( 2^m \). Lemma 4 in [1] forces

\[
a \omega_i^{(m)}(FH') \oplus a^{-1} \omega_i^{(m)}(FH') \subseteq \delta^{[l+1]}(FH)
\]

for all \( l \geq 0 \), therefore \( \delta^{[d]}(FH) \neq 0 \), so \( d + 1 \leq dl_L(FH) \leq dl_L(FG) \), as asserted.

### 2.2. The order of \( G/C_G(G') \) is divisible by some odd prime \( q \neq p \)

In the proof of the next lemma we will use the well-known congruence

\[
x^k - 1 \equiv k(x - 1) \quad \left( \text{mod } \mathfrak{I}(G')^2 \right) \quad \text{for all } k \in \mathbb{Z}.
\]

(2.2)

Set \( G/C_G(G') = \langle bC_G(G') \rangle \) and \( x^k = x^b \). The congruence

\[
[(x - 1)^{2^l}, b] \equiv (k^{2^l} - 1)b(x - 1)^{2^l} \quad \left( \text{mod } \mathfrak{I}(G')^{2^l+1} \right) \quad \text{for all } l \geq 0
\]

(2.3)

can be obtained as a simple consequence of (2.2).

**Lemma 2.2.** Let \( G \) be a group with cyclic derived subgroup of order \( p^n \) and let \( \text{char}(F) = p \). If the order of \( G/C_G(G') \) is divisible by an odd prime \( q \neq p \), then \( dl_L(FG) \geq \lceil \log_2(2p^n) \rceil \).

**Proof.** Let \( G' = \langle x \mid x^{p^n} = 1 \rangle \) and let us choose an element \( bC \in G/C_G(G') \) of order \( q \) and set \( x^k = x^b \). Evidently, \( k^{2^m} \not\equiv 1 \pmod{p} \) for all \( m \). Set \( H = \langle b, C_G(G') \rangle \). Clearly, \( x^{k^{2^l}} = (x, b) \in H' \) is of order \( p^n \), so \( H' \) has order \( p^n \), too. Since \( H' = \langle b, C_G(G') \rangle \) and the map \( c \mapsto (b, c) \) is an epimorphism of \( C_G(G') \) onto \( H' \), we can choose \( c \) from \( C_G(G') \) such that \( (b, c) = x \). Define the following three series in \( FG \): let

\[
u_0 = b, \quad v_0 = c, \quad w_0 = c^{-1}b^{-1},
\]

and, for \( l \geq 0 \), let

\[
u_{l+1} = [u_l, v_l], \quad v_{l+1} = [u_l, w_l], \quad w_{l+1} = [w_l, v_l].
\]

Using induction we show for odd \( l \) that

\[
u_l \equiv t^{(l)}_{\nu} cb(x - 1)^{2^{l-1}} \quad \left( \text{mod } \mathfrak{I}(G')^{2^{l-1}+1} \right)
\]

\[
u_l \equiv t^{(l)}_{\nu} c^{-1}(x - 1)^{2^{l-1}} \quad \left( \text{mod } \mathfrak{I}(G')^{2^{l-1}+1} \right)
\]

(2.4)

\[
u_l \equiv t^{(l)}_{\nu} b^{-1}(x - 1)^{2^{l-1}} \quad \left( \text{mod } \mathfrak{I}(G')^{2^{l-1}+1} \right)
\]
and if \( l \) is even then
\[
\begin{align*}
u_l &\equiv t_u^{(l)}b(x-1)^{2^{l-1}} \pmod{\mathcal{I}(G')^{2^{l-1}+1}}; \\
v_l &\equiv t_v^{(l)}c(x-1)^{2^{l-1}} \pmod{\mathcal{I}(G')^{2^{l-1}+1}}; \\
w_l &\equiv t_w^{(l)}c^{-1}b^{-1}(x-1)^{2^{l-1}} \pmod{\mathcal{I}(G')^{2^{l-1}+1}},
\end{align*}
\]
where \( t_u^{(l)}, t_v^{(l)}, t_w^{(l)} \) are nonzero elements in the field \( F \) while \( 2^{l-1} < p^n \). Evidently, \( u_1 = [b,c] = cb(x-1) \), and applying (2.2) we have
\[
u_1 = [b, c^{-1}b^{-1}] = c^{-1}((x^{-1})b^{-1} - 1) = c^{-1}(x-k' - 1) \equiv -k'c^{-1}(x-1) \pmod{\mathcal{I}(G')^2},
\]
and similarly, \( w_1 = [c^{-1}b^{-1}, c] \equiv -k'b(x-1) \pmod{\mathcal{I}(G')^2}, \) where \( x^{k'} = x^{b^{-1}} \). Therefore (2.4) holds for \( l = 1 \). Now assume that (2.4) is true for some odd \( l \). Then, using the congruences (2.3) and \( kk' \equiv 1 \pmod{p} \), we have
\[
\begin{align*}
u_{l+1} &\equiv t_u^{(l)}t_v^{(l)}[cb(x-1)^{2^{l-1}}, c^{-1}(x-1)^{2^{l-1}}] \\
&\equiv -t_u^{(l)}t_v^{(l)}[(x-1)^{2^{l-1}}, b](x-1)^{2^{l-1}} \\
&\equiv -t_u^{(l)}t_v^{(l)}(k^{2^{l-1}} - 1)b(x-1)^{2^{l}} \pmod{\mathcal{I}(G')^{2^{l+1}}},
\end{align*}
\]
\[
\begin{align*}
v_{l+1} &\equiv t_u^{(l)}t_w^{(l)}[cb(x-1)^{2^{l-1}}, b^{-1}(x-1)^{2^{l-1}}] \\
&\equiv t_u^{(l)}t_w^{(l)}(-b^{-1}c[(x-1)^{2^{l-1}}, b](x-1)^{2^{l-1}} \\
&\quad + cb[(x-1)^{2^{l-1}}, b^{-1}](x-1)^{2^{l-1}}) \\
&\equiv t_u^{(l)}t_w^{(l)}k^{2^{l-1}}(k^{2^{l-1}} - 1)c(x-1)^{2^{l}} \pmod{\mathcal{I}(G')^{2^{l+1}}}
\end{align*}
\]
and
\[
\begin{align*}
w_{l+1} &\equiv t_w^{(l)}t_v^{(l)}[b^{-1}(x-1)^{2^{l-1}}, c^{-1}(x-1)^{2^{l-1}}] \\
&\equiv -t_w^{(l)}t_v^{(l)}c^{-1}[(x-1)^{2^{l-1}}, b](x-1)^{2^{l-1}} \\
&\equiv -t_w^{(l)}t_v^{(l)}(k^{2^{l-1}} - 1)c^{-1}b^{-1}(x-1)^{2^{l}} \pmod{\mathcal{I}(G')^{2^{l+1}}}.
\end{align*}
\]
The assumption on \( k \) (see at the beginning of the proof) ensures that the coefficients of the element \( u_{l+1}, v_{l+1} \) and \( w_{l+1} \) are nonzero in the field \( F \). Supposing that (2.5) is true for some even \( l \) we can similarly get the required congruences. So, (2.4) and (2.5) are valid for any \( l > 0 \).

Assume that \( l < \lceil \log_2(2p^n) \rceil \). Then \( 2^{l-1} < p^n \) and the elements \( u_l, v_l, w_l \) are nonzero in \( \delta^{[l]}(FH) \), thus \( dl_L(FH) \geq dl_L(FH) \geq \lceil \log_2(2p^n) \rceil \). \( \square \)

The inequality \( dl^L(FG) \leq \lceil \log_2(2p^n) \rceil \) is well-known, thus the lemma completes the proof of Theorem 1.1.
3. Remarks on the theorem

(i) If $G$ is a non-nilpotent group with cyclic derived subgroup of order $p^n$ and $\text{char}(F) = p$, then

$$\left\lfloor \log_2(3p^n/2) \right\rfloor \leq d_l(FG) = d_l^L(FG) \leq \left\lceil \log_2(2p^n) \right\rceil.$$ 

In order to prove these inequalities it remains to show that if $G/C_G(G')$ has order $2^mp^r$, then $\left\lfloor \log_2(3p^n/2) \right\rfloor \leq d_l(FG)$. Since $G$ is not nilpotent, $m > 0$, and, as we have already seen, the dihedral group of order $2p^h$ can be embedded into $G$. Hence, by Lemma 2.1, we have $d + 1 \leq d_l(FG)$, where $d$ is the minimal integer such that $s_d^{(1)} \geq p^n$. At the same time, it is easy to verify that

$$s_l^{(1)} = \begin{cases} 
(2l+2 - 1)/3 & \text{if } l \text{ is even;} \\
(2l+2 - 2)/3 & \text{if } l \text{ is odd.} 
\end{cases} \quad (3.1)$$

Thus, $(2d+2 - 1)/3 > s_d^{(1)} > p^n$, whence $d + 1 \geq \left\lceil \log_2(3p^n/2 + 1/2) \right\rceil$ follows. Since $\left\lfloor \log_2(3p^n/2 + 1/2) \right\rfloor = \left\lfloor \log_2(3p^n/2) \right\rfloor$, the required inequality is guaranteed.

As the difference of the integers $\left\lfloor \log_2(3p^n/2) \right\rfloor$ and $\left\lfloor \log_2(2p^n) \right\rfloor$ is at most one, the values of $d_l(FG)$ and $d_l^L(FG)$ are almost uniquely determined by this inequality. In some cases we are able to determine explicitly the values of $d_l(FG)$ and $d_l^L(FG)$:

(ii) We claim that if $G/C_G(G')$ has order $2p^r$, then

$$d_l(FG) = d_l^L(FG) = \left\lfloor \log_2(3p^n/2) \right\rfloor.$$ 

Indeed, according to Theorem 1.1, if $l = d_l^L(FG)$ then $s_{l-2}^{(1)} < p^n$. From (3.1) it follows that $(2l - 1)/3 < p^n$. Hence $l < \log_2(3p^n/2 + 1/2) + 1$, and therefore $l \leq \left\lfloor \log_2(3p^n/2 + 1/2) \right\rfloor$. Since $\left\lfloor \log_2(3p^n/2 + 1/2) \right\rfloor = \left\lfloor \log_2(3p^n/2) \right\rfloor$, the proof is complete.

(iii) Since the order of $G/C_G(G')$ divides the order of $U(\mathbb{Z}_{p^n})$, which is equal to $p^{n-1}(p-1)$, for primes $p$ of the form $4k - 1$ the order of $G/C_G(G')$ is either $p^r$ for some $r$ (then $d_l(FG) = d_l^L(FG) = \left\lfloor \log_2(p^n + 1) \right\rfloor$), or $2p^r$ (then by part (ii), $d_l(FG) = d_l^L(FG) = \left\lfloor \log_2(3p^n/2) \right\rfloor$), or it has an odd prime divisor $q \neq p$ (then $d_l(FG) = d_l^L(FG) = \left\lfloor \log_2(2p^n) \right\rfloor$).

(iv) Let $G$ be a non-nilpotent group with derived subgroup of order $p > 3$, where $p$ is a Fermat prime (i.e. it can be written in the form $2^s + 1$ for some $s \geq 0$), and let $\text{char}(F) = p$. Then

$$d_l(FG) = d_l^L(FG) = \begin{cases} 
\left\lceil \log_2(2p) \right\rceil & \text{if } G/C_G(G') \text{ has order } p - 1; \\
\left\lceil \log_2(3p/2) \right\rceil & \text{otherwise.} 
\end{cases}$$
Indeed, let us write $p$ in the form $2^r + 1$ ($r > 1$). If $G/C_G(G')$ has order $p - 1 = 2^r$, then $s_{r}^{(r)} = 2^r$, and by Theorem 1.1,

$$dl_L(FG) = dl^{L'}(FG) = r + 2 = \lceil \log_2 (2p) \rceil,$$

as asserted. In the other case $G/C_G(G')$ has order $2^m$ for some $0 < m < r$. Since $\lceil \log_2 (3p/2) \rceil = r + 1$, by Theorem 1.1 it is enough to show that $s_{r}^{(m)} \geq p$. But this is true, because $s_{r-1}^{(r-1)} = 2^{r-1}$, furthermore, for $m = r - 1$ we have

$$s_{r}^{(m)} = s_{r}^{(r-1)} = 2 s_{r-1}^{(r-1)} + 1 = 2^r + 1 = p,$$

and if $m < r - 1$ then $s_{r-1}^{(m)} > s_{r-1}^{(r-1)}$. This implies

$$s_{r}^{(m)} \geq 2 s_{r-1}^{(m)} > 2 s_{r-1}^{(r-1)} = 2^r = p - 1$$

and the proof is done.

References


Zsolt Balogh
Institute of Mathematics and Informatics
College of Nyíregyháza
H-4410 Nyíregyháza
Sóstói út 31/B
Hungary

Tibor Juhász
Institute of Mathematics and Informatics
Eszterházy Károly College
H-3300 Eger
Leányka út 4
Hungary