Mathematica
Balkanica

New Series Vol. 18, 2004, Fasc. 1-2

On the Strong Davenport Constant of Nonabelian Finite p-Groups

Vesselin Dimitrov

For a finite group G, the strong Davenport constant $D(G)$ is defined as the minimal integer s such that, for any sequence of (not necessarily pairwise different) elements $g_1, \dots, g_s \in G$, there exist indices $i_1 < \cdots < i_k$ with $g_{i_1} \cdots g_{i_k} = 1$. In the present paper, we use the theory of modular group algebras and, for an arbitrary finite p-group G, we show that $D(G) \leq L(G)$, where $L(G)$ is the Loewy length of $\mathbb{F}_pG$, i.e. the class of nilpotency of the Jacobson radical of $\mathbb{F}_pG$, with the obvious equality when G is abelian. We prove the equality $D(G) = L(G)$ also when $|G| = p^3$ and $p \equiv 3 \pmod 4$. Applying our methods, we prove our main result which is the strong version of the Erdős-Ginzburg-Ziv theorem for arbitrary finite p-groups, answering in the affirmative a conjecture of Olson in the special case of p-groups.

AMS Subj. Classification: 20D15, 11P99

Key Words: Davenport constant, zero-sum sequences, finite p-groups

1. Introduction

Davenport [3] posed the following problem which concerns the properties of the zero-sum sequences in finite groups:

For a finite group G, what is the maximal possible length $D(G)$ that a minimal zero-sum sequence in G can have?

The initial motivation of Davenport was his discovery [3] that if K is an algebraic number field and G is the ideal class group of K, then $D(G)$ is the maximal number of prime ideals (counting multiplicities) in the decomposition of an irreducible integer in K.

The precise definition of the Davenport constant of an arbitrary finite group G is given as follows. A *zero-sum* sequence in G is a sequence $g_1, \dots, g_s \in G$ such that $g_1 \cdots g_s = 1$, where, as usual, 1 denotes the identity of G. Such a sequence is called *minimal* if it does not contain proper nonempty zero-sum subsequences. Then, the strong Davenport constant $D(G)$ is defined to be the maximal length of a minimal zero-sum sequence in G. Equivalently, $D(G)$ is the minimal integer s such that, for any (not necessarily pairwise distinct) elements $g_1, \dots, g_s \in G$, there exist ordered indices $i_1 < \cdots < i_k$ with $g_{i_1} \cdots g_{i_k} = 1$.

The Davenport constant has been primarily investigated for abelian groups. We refer to [2] for a survey on the classical group-theoretic results in this direction, as well as for applications in factorization theory in Krull domains. For a discussion of the combinatorial aspects of the problem, see the survey article by Caro [1]. There are two natural ways of generalizing the Davenport constant to arbitrary finite groups, according to whether we are allowed to rearrange the elements of the sequence, or we have strictly to follow their order. The integer $D(G)$ which we defined is a generalization of the second type, and will be referred to as the *strong Davenport constant.* Similarly, the *weak Davenport constant* of a finite group G is the least s such that, for any $g_1, \dots, g_s \in G$, there exist distinct indices $i_1, \dots, i_k$ with $g_{i_1} \cdots g_{i_k} = 1$; we shall denote it by $D_0(G)$.

In what follows, we fix an arbitrary prime p. Olson [6] proved that if $G \cong \mathbb{Z}_{p^{e_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{e_r}}$ is a finite abelian p-group, then $D(G) = 1 + \sum_{j=1}^{r}(p^{e_j} - 1)$. Following an idea of Troi and Zannier [8], we propose the following generalization of Olson's result to the case of arbitrary p-groups. Let G be any (not necessarily abelian) finite p-group. The Jacobson radical J of the group algebra $\mathbb{F}_pG$ coincides with the augmentation ideal and is nilpotent. Its nilpotency class is called the *Loewy length* of $\mathbb{F}_pG$. We shall denote it by $L(G)$.

Theorem 1. *Let $S_1, \dots, S_k$ be sets of nonnegative integers such that, for each $i = 1, \dots, k$, the elements of S_i include 0 and are pairwise different modulo p. Suppose that*

$$\sum_{1 \le j \le k} (|S_j| - 1) \ge L(G). \tag{1.1}$$

Then, for arbitrary elements $g_1, \dots, g_k \in G$, the equation $g_1^{x_1} \cdots g_k^{x_k} = 1$ has a solution $(x_1, \dots, x_k) \in S_1 \times \cdots \times S_k$ different from the trivial solution $(0, \dots, 0)$.

By setting $k = L(G)$ and $S_i = \{0, 1\}$ for $1 \le i \le k$, we obtain immediately the following important corollary.

Corollary 1. *The strong Davenport constant $D(G)$ of any finite p-group does not exceed the Loewy length of $\mathbb{F}_pG$.*

Corollary 1 generalizes Olson's theorem for $G = \mathbb{Z}_{p^{e_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{e_r}}$ because the lower bound $D(G) > \sum_{j=1}^{r}(p^{e_j} - 1)$ is obvious, and a classical result of Jennings [5] (see Lemma 2.1 below) easily implies that $L(G) = 1 + \sum_{j=1}^{r}(p^{e_j} - 1)$. The estimate $D(G) \le L(G)$ is the best possible upper bound of the Davenport constant of a finite p-group that can be extracted from the theory of modular group algebras. It seems plausible to conjecture that equality does hold for all finite p-groups:

Conjecture 1. *For all finite p-groups G, the strong Davenport constant is exactly equal to $L(G)$.*

We were not able to construct a sequence of length $L(G)-1$ and with no zero-sum subsequences in the general case, although we verified the conjecture in certain non-abelian cases, most notably when G is the non-abelian group of order p^3 and exponent $p \geq 3$, and $p \equiv 3 \pmod 4$. In Section 4, we discuss this problem, and describe some phenomena suggesting that there is no universal parametric construction even in the simplest non-abelian case when $|G| = p^3$.

Our main result is an application of Corollary 1 in a contribution to a well-known conjecture of Olson concerning the strong version of the Erdős-Ginzburg-Ziv theorem for arbitrary finite groups. Olson [7] proved in 1976 that if G is a finite group of order n, then from any $2n-1$ elements of G one can choose and rearrange some n elements whose product is 1. He further conjectured that the chosen elements can strictly follow any initial arrangement, but this is not known even for soluble groups. In this paper, we prove Olson's conjecture in the case of all finite p-groups. In fact, we establish a more precise result:

Theorem 2. *Let G be any finite non-cyclic p-group of order n, and let $s \geq \left(1 + \frac{2p-1}{p^2}\right)n - 1$ be an integer. Then, for any s elements $g_1, \dots, g_s \in G$, there exist n ordered indices $i_1 < \cdots < i_n$ such that $g_{i_1} \cdots g_{i_n} = 1$. Furthermore, for any $\varepsilon \in \mathbb{R}^+$, the constant $\left(1 + \frac{2p-1}{p^2}\right)n - 1$ may be replaced by $(1+\varepsilon)n - 1$, provided that the rank r of the Frattini factor $G/\Phi(G)$ satisfies $1+(p-1)r \leq \varepsilon p^r$.*

By using a well-known multiplicative method, we deduce the following result that deals with the weak version of the Erdős-Ginzburg-Ziv theorem for soluble groups.

Corollary 2. *Let G be a soluble group of order n. For each prime $p|n$, let r_p be the rank of the Frattini factor $H/\Phi(H)$ for a Sylow p-subgroup H of G. Let $s \geq (1 + \sum_{p|n} r_p/p^{r_p-1})n$ be an integer, and consider s elements $g_1, \dots, g_s \in G$. Then, there exist n distinct indices $i_1, \dots, i_n$ such that $g_{i_1} g_{i_2} \cdots g_{i_n} = 1$.*

Finally, as another application of our methods, we establish in Section 5 a result concerning orthogonality problems in finite-dimensional vector spaces over $\mathbb{F}_p$.

2. Preliminaries

Let G be a finite p-group, and denote by $J = J(\mathbb{F}_p G)$ the Jacobson radical of $\mathbb{F}_p G$. Since $\mathbb{F}_p$ is a field of characteristic p and G is a p-group, J is equal to the augmentation ideal span $\{g-1 \,|\, g \in G\}$ of $\mathbb{F}_p G$. The Jacobson radical of any finite-dimensional algebra is nilpotent. The nilpotency class of J is known as the *Loewy length* of $\mathbb{F}_p G$, and will be denoted by $L = L(G)$ throughout the paper.

We fix some standard notation. Throughout the paper, $[g, h] = g^{-1}h^{-1}gh$ is the commutator of $g, h \in G$; $[H_1, H_2]$ is the subgroup of G generated by $[h_1, h_2]$, where $h_1 \in H_1, h_2 \in H_2$ and H_1, H_2 are subgroups of G; $\langle \cdots \rangle$ is the subgroup of G generated by $\cdots$; $S^{(n)} = \{a^n \,|\, a \in S\}$ for an arbitrary set S. Also, it will be convenient to denote $J^0 = \mathbb{F}_pG$. We shall make use of the Brauer-Jennings-Zassenhaus M-series [5], defined by $M_1 = M_1(G) = G$ and, for $k > 1$, $M_k = M_k(G) = \langle [M_{k-1}, G], M^{(p)}_{\lceil k/p \rceil} \rangle$; note that M_k is a normal subgroup of M_{k-1}, and that $M_2(G) = \Phi(G)$ is the Frattini subgroup of G. Recall the following classical result.

Lemma 2.1. *(Jennings [5])*

1. $M_k = \{g \in G \,|\, g - 1 \in J^k\}$ *and* M_k/M_{k+1} *is an elementary abelian* p*-group.*
2. *Let* $M_k/M_{k+1} = \langle f_{k1}M_{k+1} \rangle \oplus \cdots \oplus \langle f_{kd_k}M_{k+1} \rangle$*. Then* J^n *has a basis modulo* J^{n+1} *consisting of all products* $\prod_{k \geq 1} \prod_{i=1}^{d_k} (f_{ki} - 1)^{\alpha_{ki}}$ *such that* $0 \leq \alpha_{ki} < p$ *and* $\sum k\alpha_{ki} = n$*. In particular,*

$$\sum_{i \geq 0} t^i \dim J^i/J^{i+1} = \prod_j (1 + t^j + \cdots + t^{(p-1)j})^{d_j} \tag{2.1}$$

and the Loewy length of $\mathbb{F}_pG$ *equals* $L(G) = 1 + (p-1)\sum_j jd_j$*.*

We will need the following easy lemma, a variant of which appears in [8].

Lemma 2.2. *Let* p *be a prime number, and consider* $0 = k_0 < k_1 < \cdots < k_s$ *such that no two of the numbers* k_j $(0 \leq j \leq s)$ *are congruent modulo* p*. Then, there exist coefficients* $a_0 = 1, a_1, \ldots, a_s \in \mathbb{F}_p$ *such that the polynomial* $\sum_{j=0}^{s} a_j x^{k_j} \in \mathbb{F}_p[x]$ *is divisible by* $(1 - x)^s$*.*

Proof. By formal differentiation, the condition that $(1 - x)^s$ divides $1 + \sum_{j=1}^{s} a_j x^{k_j}$ is equivalent to the following system of s linear equations in s variables $a_1, \ldots, a_s$:

$$\begin{aligned} a_1 k_1^{\underline{0}} + a_2 k_2^{\underline{0}} + \cdots + a_s k_s^{\underline{0}} &= -1 \\ a_1 k_1^{\underline{1}} + a_2 k_2^{\underline{1}} + \cdots + a_s k_s^{\underline{1}} &= 0 \\ &\vdots \\ a_1 k_1^{\underline{s-1}} + a_2 k_2^{\underline{s-1}} + \cdots + a_s k_s^{\underline{s-1}} &= 0, \end{aligned}$$

where, as usual, $x^{\underline{m}} = x(x-1)\cdots(x-m+1)$ is the lowercase factorial. By Cramer's formula, it suffices to show that the matrix

$$M := \begin{pmatrix} k_1^{\underline{0}} & \ldots & k_s^{\underline{0}} \\ \vdots & \ddots & \vdots \\ k_1^{\underline{s-1}} & \cdots & k_s^{\underline{s-1}} \end{pmatrix} \tag{2.2}$$

has a nonzero determinant over $\mathbb{F}_p$, which follows from the formula

$$\det M = \prod_{1\le i<j\le s} (k_j - k_i)$$

and from the assumption that $k_1, \dots, k_s$ are pairwise distinct. The proof is complete. ■

Lemma 2.3 *Let G be a finite group such that $G/\Phi(G)$ is cyclic. Then, G is also cyclic.*

Proof. It is well-known that $\Phi(G)$ is the set of non-generators of G, i.e. the set of all $h \in G$ such that, for a subset $X \subseteq G$, $\langle X, h\rangle = G$ implies $\langle X\rangle = G$.

By assumption, $G/\Phi(G) = \langle g\Phi(G)\rangle$ for some $g \in G$. Let $X \subseteq G$ be such that $\langle X, g\rangle = G$, and consider an arbitrary element and $x \in X$. Then, x may be written as $x = g^i h$ with $h \in \Phi(G)$, so $\langle g, h, X \setminus \{x\}\rangle = \langle g, x, X \setminus \{x\}\rangle = G$. Since h is a non-generator, it follows that $\langle g, X \setminus \{x\}\rangle = G$. Now, starting with $X = G$ and successively deleting elements of X, we obtain that $G = \langle g\rangle$ is cyclic, proving the lemma. ■

Lemma 2.4. *Let G be a finite p-group of order n, and let r be the rank of the (abelian) group $G/\Phi(G)$. Then,*

$$L(G) \le \frac{1 + (p-1)r}{p^r} n.$$

Proof. Clearly, $r = d_1 = \operatorname{rank} M_1/M_2$. Suppose that $L(G) > \varepsilon n$, where $n = |G|$ and $\varepsilon > 0$ is fixed. Let S be the set of indices i for which $d_i \neq 0$. Then, S is finite, and let $S = \{i_1 < i_2 < \cdots < i_m\}$. Since $d_i = 0$ for $i \notin S$, we have

$$n = p^{\sum_{i\ge 1} d_i} = p^{d_{i_1} + \cdots + d_{i_m}}.$$

For $1 \le j \le m$, consider the set $A_j = \{t i_j \,|\, 0 \le t \le (p-1)d_{i_j}\}$.

Since $L(G) > \varepsilon n$, we have $\dim J^i/J^{i+1} \ge 1$ for $0 \le i < \varepsilon n$. On the other hand, by Jennings' Dimension formula (2.1), $\dim J^i/J^{i+1} \ge 1$ implies that i is expressible under the form $i = s_1 + \cdots + s_m$ with $s_j \in A_j$. We conclude that each integer x satisfying $0 \le x < \varepsilon n$ belongs to the set $A_1 + \cdots + A_m$ of all such sums $s_1 + \cdots + s_m$. In particular, $|A_1 + \cdots + A_m| \ge \varepsilon n$, so

$$\varepsilon p^{d_{i_1} + \cdots + d_{i_m}} \le |A_1 + \cdots + A_m| \le |A_1| \cdots |A_m|. \tag{2.3}$$

It is clear that $1 \in S$, i.e. $i_1 = 1$. Using (2.3), the equality $|A_1| = 1 + (p-1)d_1$ and the inequalities $|A_j| \le p d_{i_j}$ for $j \ge 2$, we get that

$$\varepsilon p^{d_1} p^{(d_{i_2}-1) + \cdots + (d_{i_m}-1)} \le (1 + (p-1)d_1) d_{i_2} \cdots d_{i_m}. \tag{2.4}$$

By the obvious inequalities $p^{d_{i_j}-1} \geq d_{i_j}$ for $j > 1$, we get that $\varepsilon \leq \frac{1+(p-1)r}{p^r}$, implying the desired inequality $L(G) \leq \frac{1+(p-1)r}{p^r}n$. ■

3. Proofs of the main results

In this section we present proofs of Theorem 1, Theorem 2 and Corollary 2.

Proof of Theorem 1. Let $S_i = \{k_{i0} = 0, k_{i1}, \dots, k_{is_i}\}$, $1 \leq i \leq k$. By Lemma 2.2, for each $i \in \{1, \dots, k\}$, there exist elements $a_{i0} = 1, a_{i1}, \dots, a_{is_i} \in \mathbb{F}_p$ such that

$$\sum_{0 \leq j \leq s_i} a_{ij} x^{k_{ij}} = (1-x)^{s_i} f_i(x)$$

for some polynomials $f_i \in \mathbb{F}_p[x]$. This implies that

$$\sum_{0 \leq j \leq s_i} a_{ij} g_i^{k_{ij}} = (1-g_i)^{s_i} I_i, \tag{3.1}$$

where $I_i = f_i(g_i) \in \mathbb{F}_p G$. Now, consider the element

$$I := \prod_{1 \leq i \leq k} \Big(\sum_{0 \leq j \leq s_i} a_{ij} g_i^{k_{ij}} \Big) \tag{3.2}$$

of the group algebra $\mathbb{F}_p G$. By (3.1), we have $I \in J^{s_1+\cdots+s_k}$, where $J = J(\mathbb{F}_p G)$. But, by assumption, we have $s_1 + \cdots + s_k \geq L(G)$, so $J^{s_1+\cdots+s_k} = 0$, implying $I = 0$. On the other hand, by expanding (3.2) to its normal form and using that $a_{10} = \cdots = a_{k0} = 1$, we have

$$I = 1 + \sum_x b(x) g_1^{x_1} g_2^{x_2} \cdots g_k^{x_k} \tag{3.3}$$

for some coefficients $b(x)$, where the sum is over all $x = (x_1, \dots, x_k) \in S_1 \times \cdots \times S_k, x \neq (0, \dots, 0)$. Since $I = 0$, it follows that the sum in (3.3) has a nonzero contribution to the identity of G, for otherwise the coefficient of 1 in I would be $1 \neq 0$. Therefore, some equation of the form $g_1^{x_1} g_2^{x_2} \cdots g_k^{x_k} = 1$ has a non-trivial solution $(x_1, \dots, x_k) \in S_1 \times \cdots \times S_k$, completing the proof. ■

We now proceed to the

Proof of Theorem 2. Remark that $L(G \oplus H) = L(G) + L(H) - 1$ for all finite p-groups G, H. This is straightforward to prove, but we just note that it follows immediately from the formula for L in Lemma 2.1, since $M_k(G \oplus H) = M_k(G) \oplus M_k(H)$. By Theorem 1, we have

$$D(G \oplus H) \leq L(G \oplus H) = L(G) + L(H) - 1.$$

In view of the obvious inequality $L(H) \le |H|$, we have

$$D(G \oplus H) \le L(G) + |H| - 1. \tag{3.4}$$

Now, choose H to be the cyclic group of order $n = |G|$. Embed G into $E = G \oplus H$, and consider arbitrary elements $g_1, \dots, g_{k+n-1} \in G$, where $k = L(G)$. Fix a generator x of H, and consider the sequence $xg_1, \dots, xg_{k+n-1} \in E$. By (3.4), $D(E) \le k+n-1$, so the latter sequence has a zero-sum subsequence. In other words, there are ordered indices $i_1 < \cdots < i_l$ such that $(xg_{i_1}) \cdots (xg_{i_l}) = 1$. Since x commutes with each g_i, this is equivalent to $x^l(g_{i_1} \cdots g_{i_l}) = 1$, so $x^l = 1$ and $g_{i_1} \cdots g_{i_l} = 1$. But x has order n, so $n|l$ which, in view of $l \le k+n-1 \le 2n-1$, gives $l = n$. Therefore, we obtain the existence of exactly n ordered indices $i_1 < \cdots < i_n$ with $g_{i_1} \cdots g_{i_n} = 1$.

Since G is non-cyclic, Lemma 2.3 implies that $\operatorname{rank} G/\Phi(G) \ge 2$. By Lemma 2.4, we have $k \le \frac{2p-1}{p^2}n$, giving $k+n-1 \le \left(1 + \frac{2p-1}{p^2}\right)n - 1$, and the first part of the theorem follows immediately from the above argument. For the strengthening, note that $k \le \varepsilon n$ implies that the constant $\left(1 + \frac{2p-1}{p^2}\right)n - 1$ may be improved to $(1+\varepsilon)n - 1$, and the assertion follows immediately from Lemma 2.4. ■

Proof of Corollary 2. For a finite group H, let $f(H)$ be the least s so that, from any s elements of H, one can choose and arrange exactly $|H|$ elements multiplying to 1. If $H \lhd G$, it is straightforward to observe the following inequality:

$$f(G) \le f(H) + |H|(f(G/H) - 1). \tag{3.5}$$

Let $n = p_1^{k_1} \cdots p_s^{k_s}$ be the prime factorization of n. By Hall's theorem, $p_1, \dots, p_s$ can be numbered in such a manner that there exists a subnormal series

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_s = \langle 1 \rangle$$

satisfying $|G_{i-1}/G_i| = p_i^{k_i}$ for $i \in \{1, \dots, s\}$. By Theorem 2 and the assumption on the Sylow p_i-subgroups of G, we have $f(G_{i-1}/G_i) \le r_{p_i} p_i^{k_i}/p_i^{r-1}$, and the desired inequality $f(G) < (1 + \sum r_{p_i}/p_i^{r_{p_i}-1})n$ follows by successive applications of (3.5). ■

4. Lower bounds on $D(G)$

Unlike in the case of arbitrary abelian groups where we have trivial lower bounds, the difficulty in proving the conjecture $D(G) = L(G)$ is the construction of an appropriate sequence of length $L(G) - 1$ with no zero-sum ordered subsequences. In this section, we provide such a construction in some particular cases, present some heuristic arguments in favor of the conjecture, and discuss the difficulties in the general situation.

There are only two non-isomorphic non-abelian groups of order p^3. For $p = 2$ these groups are the dihedral group D_8 of order 8 and the quaternion group Q. For $p > 2$, one of the non-abelian groups of order p^3 is of exponent p^2 and the other is of exponent p.

Start with the following very simple observation.

Proposition 5.1. *If D_8 is the dihedral group of order 8 and Q is the quaternion group of order* 8, *then Conjecture 1 holds, i.e. $D(D_8) = D(Q) = 5$.*

Proof. By Corollary 1, we have $D(D_8), D(Q) \leq 5$, and it suffices to give examples of sequences in D_8 and Q of length 4 with no zero-sum subsequences. It is well-known that D_8 has the following presentation:

$$D_8 = \langle a, b \,|\, a^4 = b^2 = 1, [a, b] = a^2 \rangle.$$

Then, the sequence a, a, a, b obviously has the required properties. Similarly, Q has the presentation

$$Q = \langle a, b \,|\, a^4 = 1, [a, b] = a^2 = b^2 \rangle,$$

and the sequence a, a, a, b satisfies the requirements. ■

A similar observation easily yields Conjecture 1 in the case when G is the non-abelian group of order p^3 and exponent $p^2, p \geq 3$. Far more interesting is the case when G is the non-abelian group of order p^3 and exponent p. We provide the following construction in the case $p \equiv 3 \pmod 4$:

Theorem 3. *Let $p \equiv 3 \pmod 4$ be a prime and G be the non-abelian group of order p^3 and exponent p. Then, $D(G) = 4p - 3$.*

Proof. It is well-known that G has the following presentation:

$$G = \langle a, b, c \,|\, a^p = b^p = c^p = [a, c] = [b, c] = 1, [a, b] = c \rangle.$$

By Corollary 1, we have $D(G) \leq L(G) = 4p - 3$, so it suffices to prove the lower bound. We claim that the sequence

$$(p-1) \times abc^{1/2}, (p-1) \times ab^3c^{3/2}, (p-1) \times b^{-1}, (p-1) \times a^{-1}bc^{-1/2}$$

has no (ordered) zero-sum subsequences; here, the fractional exponents are reduced modulo p, i.e. $\pm 1/2$ and $3/2$ are, respectively, $\pm 2^{p-2}$ and $3 \cdot 2^{p-2}$ modulo p. Suppose that it has some zero-sum subsequence S. Then, S is of the form $S = x \times abc^{1/2}, y \times ab^3c^{3/2}, z \times b^{-1}, t \times a^{-1}bc^{-1/2}$, where $0 \leq x, y, z, t < p$ are not all zero. Therefore, $(abc^{1/2})^x(ab^3c^{3/2})^y(b^{-1})^z(a^{-1}bc^{-1/2})^t = 1$. A direct computation shows that this is equivalent to

$$c^{x^2+3y^2-t^2+2xy-2xt-6yt+2zt}a^{x+y-t}b^{x+3y-z+t} = 1.$$

Therefore, in $\mathbb{F}_p$ we have the following system in x, y, z, t:

$$\begin{aligned} x + 3y - z + t &= 0 \\ x + y - t &= 0 \\ x^2 + 3y^2 - t^2 + 2xy - 2xt - 6yt + 2zt &= 0. \end{aligned}$$

By expressing z and t from the first two equations and replacing in the third, we obtain that

$$x^2 + 2y^2 + 2xy = 0,$$

which implies $x = y = 0$, since the quadratic form x^2+2y^2+2xy has discriminant -4 which is not a quadratic residue in $\mathbb{F}_p$ as $p \equiv 3 \pmod 4$. Therefore, $x = y = z = t = 0$, a contradiction, proving the claim. ∎

In fact, by the proof of Theorem 3 and by the fact that there does not exist an universal $a \in \mathbb{Q}$ which is a quadratic non-residue modulo all sufficiently large primes, a sequence of the form

$$(p-1) \times a^{\alpha_1} b^{\beta_1} c^{\gamma_1}, \ldots, (p-1) \times a^{\alpha_4} b^{\beta_4} c^{\gamma_4}$$

with $\alpha_i, \beta_i, \gamma_i \in \mathbb{Q}$ cannot give a construction for all primes p to complete the proof of the Conjecture for all groups of order p^3. Moreover, it is easy to see that no partitioning of the primes into residue classes (as we did for $p \equiv 3 \pmod 4$) can be done to give a construction in finitely many steps. Therefore, a construction of the form $(p-1) \times g_1, \ldots, (p-1) \times g_4$ is specific for each prime p, and would require one to introduce a symbolic non-residue v modulo p so that the problem can be solved. For more complicated groups G, the situation becomes much more difficult to parametrize. In view of a similar observation to the above, the approach of applying induction on $|G|$ and deducing a construction for G from a construction for the commutator subgroup $G' = [G, G]$ seems hopeless.

5. An application: Orthogonality problems in finite-dimensional vector spaces over $\mathbb{F}_p$

As the final part of the proof of Theorem 2 shows, we can study properties of zero-sum sequences in finite abelian p-groups by considering an appropriate embedding into a larger group. This section is intended to provide an example of a result, obtained by embedding an abelian p-group into a non-abelian p-group with easily computed Loewy length of its $\mathbb{F}_p$-algebra; this result is inaccessible through abelian embeddings.

Let p be a prime. Consider a vector space V over $\mathbb{F}_p$ with $\dim V = d < \infty$, and let $w_1, \ldots, w_d$ be a fixed basis of V. Let us write $\mathbf{1} = \sum_{j=1}^{d} w_j$. As usual, if $x = x_1 w_1 + \cdots + x_d w_d, y = y_1 w_1 + \cdots + y_d w_d \in V$, we denote by $x \cdot y = x_1 y_1 + \cdots + x_d y_d$ the *dot product* of x and y. Two vectors $x, y \in V$ are *orthogonal* if their dot product is zero, i.e. $x \cdot y = 0$. Also, for the subspace $U = U_I$ of V spanned by $\{w_i \,|\, i \in I\}$ for a given set of indices $I \subseteq \{1, \ldots, d\}$, the *projection* of $x = x_1 w_1 + \cdots + x_d w_d$ in U is the vector $\sum_{i \in I} x_i w_i \in U$, and will be denoted by $\pi(x) = \pi_U(x)$.

A set $S \subset V$ of pairwise orthogonal elements of V will be referred to as an *orthogonal set* (with respect to V); note that an orthogonal set with respect to V is not necessarily an orthogonal set with respect to a given subspace U_I of V. An interesting combinatorial problem is to determine the minimal possible dimension of V so that each sufficiently small set of vectors in V is projected to an orthogonal set in some nontrivial subspace of V. In this direction, we observe the following result that follows immediately by Olson's p-groups theorem [6], together with an appropriate embedding of $\mathbb{Z}_p^r$ in some larger abelian p-group.

Theorem 4. *Let p be a prime and r be a positive integer. Consider a vector space V over $\mathbb{F}_p$ of finite dimension at least $1 + (p-1)\binom{r+1}{2}$, and let $v_0 = \mathbf{1}, v_1, \ldots, v_r$ be $r+1$ vectors in V. Then, there exists a nontrivial subspace $U = U_I$ of V such that $\{\pi_U(v_0), \ldots, \pi_U(v_r)\}$ forms an orthogonal subset of U.*

Proof. Consider the group $G \cong \mathbb{Z}_p^r$, and let $G = \langle a_1 \rangle \oplus \cdots \oplus \langle a_r \rangle$. Embed G into the group

$$E = G \oplus \Big(\bigoplus_{1 \le i < j \le r} \langle a_{i,j} \rangle \Big),$$

where $a_{i,j}$ has order p, $1 \le i < j \le r$. Clearly, $E \cong \mathbb{Z}_p^{\binom{r+1}{2}}$.

Now, suppose that the dimension of V is $d \ge 1 + (p-1)\binom{r+1}{2}$, and let

$$v_j = \sum_{1 \le i \le d} x_{i,j} w_i, 1 \le j \le r.$$

Consider the elements

$$g_s := a_1^{x_{s,1}} \cdots a_r^{x_{s,r}} \prod_{1 \le i < j \le r} a_{i,j}^{x_{s,i} x_{s,j}}, 1 \le s \le d.$$

These elements form a sequence in G of length $d \ge 1 + (p-1)\binom{r+1}{2} = D(E)$, so there exist some indices $i_1 < \cdots < i_k$ with $g_{i_1} \cdots g_{i_k} = 1$. It is then easy to see that the non-trivial subspace U of V spanned by $\{w_{i_1}, \cdots, w_{i_k}\}$ satisfies $\pi_U(v_i) \cdot \pi_U(v_j) = 0$ for $0 \le i < j \le r$, proving the claim. ■

The dot product is a symmetric bilinear form defined by the identity $d \times d$ matrix. We can define a bilinear form using any fixed matrix with entries from $\mathbb{F}_p$. For example, using the upper triangular matrix with zero diagonal and all entries from the upper corner equal to 1, we define the product

$$x \star y = \sum_{1 \le i < j \le d} x_i y_j,$$

where $x = \sum_{i=1}^{d} x_i w_i, y = \sum_{i=1}^{d} y_i w_i$. Clearly, we have the identity

$$(x \cdot \mathbf{1})(y \cdot \mathbf{1}) = x \star y + x \cdot y + y \star x.$$

The following result is similar in concept to Theorem 4, but cannot be handled directly by Olson's p-group theorem.

Theorem 5. *Let p be a prime and $r \in \mathbb{N}$, and consider a vector space V over $\mathbb{F}_p$ of finite dimension at least $1 + (p-1)r^2$. Then, for any r vectors $v_1, \dots, v_r \in V$, there exists a non-trivial subspace U of V such that their projections $\pi_U(v_1), \dots, \pi_U(v_r)$ in U are orthogonal to $\mathbf{1}$, and satisfy $\pi(v_i) \star \pi(v_j) = 0$ for $1 \le i < j \le d$.*

Proof. Consider the group

$$G = \langle a_1, \dots, a_r; b_{ij} \mid a_i^p = b_{ij}^p = [a_k, b_{ij}] = [b_{kl}, b_{ij}] = 1, [a_i, a_j] = b_{ij}^{-1} \rangle,$$

where $1 \le i < j \le r, 1 \le k \le l \le r$. This is the factor group of the free nilpotent of class 2 group freely generated by $a_1, \dots, a_r$, modulo the relations $a_i^p = [a_i, a_j]^p = 1$. This is a group of exponent p and order $p^{r+\binom{r}{2}} = p^{\binom{r+1}{2}}$.

A direct computation easily gives the M-series of G: we have $M_1(G) = G, M_2(G) = \bigoplus_{i<j} \langle b_{ij} \rangle$, and $M_k(G) = \langle 1 \rangle$ for $k \ge 3$. Therefore, $d_1 = r, d_2 = \binom{r}{2}$, and $d_k = 0$ for $k \ge 3$. Hence, $L(G) = 1 + (p-1)r^2$, giving $D(G) \le 1 + (p-1)r^2$.

Suppose that V has dimension $d \ge 1 + (p-1)r^2$, and let

$$v_j = \sum_{1 \le i \le d} x_{i,j} w_i, 1 \le j \le r.$$

Consider the elements

$$g_s := a_1^{x_{s,1}} \cdots a_r^{x_{s,r}} \in G, 1 \le s \le d.$$

They form a sequence in G of length at least $D(G)$, so there exist ordered indices $i_1 < \cdots < i_k$ with $g_{i_1} \cdots g_{i_k} = 1$. Let U be the (non-trivial) subspace of V spanned by $\{w_{i_1}, \dots, w_{i_k}\}$. For $x \in V$, let $\pi(x) = \pi_U(x)$. A direct computation then shows that

$$1 = g_{i_1} g_{i_2} \cdots g_{i_k} = a_1^{\mathbf{1}\cdot\pi(v_1)} \cdots a_r^{\mathbf{1}\cdot\pi(v_r)} \prod_{1 \le i < j \le r} b_{ij}^{\pi(v_i)\star\pi(v_j)}.$$

Therefore, $\mathbf{1} \cdot \pi(v_l) = \pi(v_i) \star \pi(v_j) = 0$ for $1 \le i, j, l \le d; i < j$, which is exactly what we needed to show. ■

Acknowledgements

The author wishes to express his sincere gratitude to: Pavlo Pylyavskyy for his mentorship during the Research Science Institute, where the biggest part of this research was carried out; Prof. Hartley Rogers for finding such a mentor; Prof. Vesselin Drensky for help with the theory of modular group algebras and useful directions; Dr. John Rickert and Dr. Jenny Sendova for their valuable help and encouragement; Gabriel Carroll for numerous suggestions. The author is also greatly indebted to the Center for Excellence in Education and the Massachusetts Institute of Technology for making this research possible.

References

[1] Y. Caro. Zero-sum problems — A survey, *Discrete Mathematics*, **152** (1996), 93–113.

[2] S. T. Chapman. On the Davenport Constant, the Cross Number, and Their Applications in Factorization Theory, *Zero-dimensional commutative rings*, Lecture notes in Pure and Applied Math., **171** (1995), 167–190.

[3] H. Davenport. *Proceedings of the Midwestern Conference on Group theory and Number theory*, Ohio State University, April 1966.

[4] P. Erdős, A. Ginzburg, A. Ziv. Theorem in additive number theory, *Bull. Research Council Israel*, **10** (1961), 41–43.

[5] S. A. Jennings. The structure of the group ring of a p-group over a modular field, *Trans. Amer. Math. Soc.*, **50** (1941), 175–185.

[6] J. E. Olson. A combinatorial problem in finite abelian groups I, *Journal of Number Theory*, **1** (1969), 8–10.

[7] J. E. Olson. On a combinatorial problem of Erdős, Ginzburg and Ziv, *Journal of Number Theory*, **8** (1976), 52–57.

[8] G. Troi, U. Zannier. On a theorem of J.E. Olson and an application (vanishing sums in finite abelian p-groups), *Finite Fields Appl.*, **3** (1997), no. 4, 378–384.

Highschool Institute of Mathematics
and Informatics, IMI
Bulgarian Academy of Sciences
Sofia 1113, BULGARIA
e-mail: vessel@mit.edu

Received 30.09.2003