



**AN ANALOGUE OF THE ERDŐS-GINZBURG-ZIV THEOREM
FOR QUADRATIC SYMMETRIC POLYNOMIALS**

Arie Bialostocki

Department of Mathematics, University of Idaho, Moscow ID 83844 USA
arieb@uidaho.edu

Tran Dinh Luong¹

Department of Mathematics, University of Idaho, Moscow ID 83844 USA
luongtran@vandals.uidaho.edu

Received: 12/23/08, Accepted: 5/20/09, Published: 9/25/09

Abstract

Let p be a prime and let $\varphi \in \mathbb{Z}_p[x_1, x_2, \dots, x_p]$ be a symmetric polynomial, where \mathbb{Z}_p is the field of p elements. A sequence T in \mathbb{Z}_p of length p is called a φ -zero sequence if $\varphi(T) = 0$; a sequence in \mathbb{Z}_p is called a φ -zero free sequence if it does not contain any φ -zero subsequence. Define $g(\varphi, \mathbb{Z}_p)$ to be the smallest integer l such that every sequence in \mathbb{Z}_p of length l contains a φ -zero sequence; if l does not exist, we set $g(\varphi, \mathbb{Z}_p) = \infty$. Define $M(\varphi, \mathbb{Z}_p)$ to be the set of all φ -zero free sequences of length $g(\varphi, \mathbb{Z}_p) - 1$, whenever $g(\varphi, \mathbb{Z}_p)$ is finite. The aim of this paper is to determine the value of $g(\varphi, \mathbb{Z}_p)$ and to describe the set $M(\varphi, \mathbb{Z}_p)$ for a quadratic symmetric polynomial φ in $\mathbb{Z}_p[x_1, x_2, \dots, x_p]$.

1. Introduction

This paper is motivated by the following theorem of Erdős, Ginzburg, and Ziv, [9], stated below in Theorem 1.1 (i) for a prime. Part (ii) of Theorem 1.1 addresses the inverse problem which corresponds to the first part. Several new proofs of (i) appear in [1], and a proof of (ii) appears in [16] and [5]; see also [15].

Theorem 1 (EGZ) *Let p be a prime and let \mathbb{Z}_p be the additive group of residue classes modulo p .*

- (i) *Every sequence in \mathbb{Z}_p of length $2p - 1$ contains a zero-sum subsequence of length p .*
- (ii) *The set of all sequences of maximal length in \mathbb{Z}_p that do not contain any zero-sum subsequence of length p is that of all sequences containing exactly two distinct elements, where each element appears $p - 1$ times.*

There were numerous generalizations and developments of the EGZ theorem in recent years; a comprehensive list of references on this topic can be found in the surveys [8], [2], [3], [10] and [11]. This paper diverts from most previous works, as it takes into consideration the field structure of \mathbb{Z}_p rather than being restricted to its additive structure. More precisely, we deal with symmetric polynomials in p variables

¹Partially supported by Project 322, Ministry of Education of Vietnam.
This paper is part of the second author's dissertation under the supervision of the first author.

over \mathbb{Z}_p , motivated by the fact that the sum in the EGZ theorem corresponds to the first elementary symmetric polynomial in $\mathbb{Z}_p[x_1, x_2, \dots, x_p]$. It is worthwhile to mention some historical origins to our approach. Two zero-sum problems concerning the ring \mathbb{Z}_n were raised in [4, p. 125], and independently the weighted version of the EGZ theorem, [13], was conjectured in [8, p. 96].

We start by introducing some definitions and notations. Let p be a prime and let \mathbb{Z}_p be the prime field of p elements. Let φ be a symmetric polynomial in $\mathbb{Z}_p[x_1, x_2, \dots, x_p]$. A sequence of p elements a_1, a_2, \dots, a_p in \mathbb{Z}_p is called a φ -zero sequence if $\varphi(a_1, a_2, \dots, a_p) = 0$; a sequence in \mathbb{Z}_p is called φ -zero free if it does not contain any φ -zero subsequence. Define $g(\varphi, \mathbb{Z}_p)$ to be the smallest integer l such that every sequence in \mathbb{Z}_p of length l contains a φ -zero subsequence; if l does not exist, we set $g(\varphi, \mathbb{Z}_p) = \infty$. Define $M(\varphi, \mathbb{Z}_p)$ to be the set of all φ -zero free sequences of length $g(\varphi, \mathbb{Z}_p) - 1$, whenever $g(\varphi, \mathbb{Z}_p)$ is finite. We consider two sequences in \mathbb{Z}_p to be identical if they differ by the order of their elements, and use the notation $[a_1]^{\alpha_1}[a_2]^{\alpha_2} \dots [a_k]^{\alpha_k}$ to denote a sequence in \mathbb{Z}_p where each element a_i appears α_i times.

Let φ be a symmetric polynomial in $\mathbb{Z}_p[x_1, x_2, \dots, x_p]$. It is clear that if we have $\varphi(0, 0, \dots, 0) \neq 0$, then for every integer m , where $m \geq 1$, the sequence $[0]^m$ is φ -zero free, which implies $g(\varphi, \mathbb{Z}_p) = \infty$. We now suppose $\varphi(0, 0, \dots, 0) = 0$. If φ is a linear symmetric polynomial, then, by the EGZ theorem, we have $g(\varphi, \mathbb{Z}_p) = 2p - 1$ and $M(\varphi, \mathbb{Z}_p)$ is the set of all sequences in \mathbb{Z}_p of the form $[u]^{p-1}[v]^{p-1}$, where $u, v \in \mathbb{Z}_p$ and $u \neq v$. In this paper, we will determine the value of $g(\varphi, \mathbb{Z}_p)$ and describe the set $M(\varphi, \mathbb{Z}_p)$ for a quadratic symmetric polynomial φ in $\mathbb{Z}_p[x_1, x_2, \dots, x_p]$.

Throughout the paper we will denote by $d(T)$ the number of distinct elements of a sequence T in \mathbb{Z}_p , and denote by s_k , for $k \geq 1$, the power-sum symmetric polynomial of degree k in $\mathbb{Z}_p[x_1, x_2, \dots, x_p]$, which is defined by the formula $s_k(x_1, x_2, \dots, x_p) = x_1^k + x_2^k + \dots + x_p^k$.

2. Main Result

Let p be a prime, where $p \geq 3$, and let $\varphi \in \mathbb{Z}_p[x_1, x_2, \dots, x_p]$ be a quadratic symmetric polynomial with $\varphi(0, 0, \dots, 0) = 0$. Then φ can be written in the form $as_1^2 + bs_2 + cs_1$, where $a, b, c \in \mathbb{Z}_p$, and either $a \neq 0$ or $b \neq 0$.

The main result of the paper is the following theorem.

Theorem 2 *Let p be a prime, where $p \geq 3$, and let $\varphi = as_1^2 + bs_2 + cs_1$, where $a, b, c \in \mathbb{Z}_p$, and either $a \neq 0$ or $b \neq 0$, be a quadratic symmetric polynomial in $\mathbb{Z}_p[x_1, x_2, \dots, x_p]$. Then the following assertions hold:*

- (i) *If $a = 0$ and $b \neq 0$, then $g(\varphi, \mathbb{Z}_p) = 2p - 1$, and $M(\varphi, \mathbb{Z}_p)$ is the set of all sequences of the form*

$$[u]^\alpha[-u - cb^{-1}]^{p-1-\alpha}[v]^\beta[-v - cb^{-1}]^{p-1-\beta},$$

where $u, v \in \mathbb{Z}_p, u \neq v, u + v \neq -cb^{-1}$ and $0 \leq \alpha \leq p - 1, 0 \leq \beta \leq p - 1$.

- (ii) If $a \neq 0, b = 0$ and $c = 0$, then $g(\varphi, \mathbb{Z}_p) = 2p - 1$, and $M(\varphi, \mathbb{Z}_p)$ is the set of all sequences of the form $[u]^{p-1}[v]^{p-1}$, where $u, v \in \mathbb{Z}_p$ and $u \neq v$.
- (iii) If $a \neq 0, b = 0$ and $c \neq 0$, then $g(\varphi, \mathbb{Z}_p) = 2p - 2$, and $M(\varphi, \mathbb{Z}_p)$ is the set of all sequences of the form $[u]^{p-1}[u + ca^{-1}]^{p-2}$, where $u \in \mathbb{Z}_p$.
- (iv) If $a \neq 0, b \neq 0$ and $p \geq 5$, then

$$2(p - 1) + n(p) \leq g(\varphi, \mathbb{Z}_p) \leq 4p - 3,$$

where $n(p)$ denotes the least quadratic non-residue modulo p .

The following two results will be used in the proof of Theorem 2.1.

Lemma 3 Let $m \geq 4$, and let S be a sequence in \mathbb{Z}_m of length $2m - 3$.

- (i) ([7]) If S has at least four distinct elements, then it contains a zero-sum subsequence of length m .
- (ii) ([6, 11]) If S does not contain any zero-sum subsequence of length m , then it either has the form $[u]^{m-1}[v]^{m-2}$ or $[u]^{m-1}[v]^{m-3}[2v - u]^1$, where $u, v \in \mathbb{Z}_m$, and $\gcd(u - v, m) = 1$.

Lemma 4 ([12, 14]) Every sequence in $\mathbb{Z}_m \oplus \mathbb{Z}_m$ of length $4m - 3$ contains a zero-sum subsequence of length m .

Proof of Theorem 2. (i) Suppose $a = 0$ and $b \neq 0$. Then we have $\varphi = bs_2 + cs_1$. Let $f(x) = bx^2 + cx \in \mathbb{Z}_p[x]$. Then

$$\varphi(x_1, x_2, \dots, x_p) = f(x_1) + f(x_2) + \dots + f(x_p).$$

Let $a_1, a_2, \dots, a_{2p-1}$ be a sequence in \mathbb{Z}_p of length $2p - 1$. Then, by the EGZ theorem, the sequence $f(a_1), f(a_2), \dots, f(a_{2p-1})$ contains a zero-sum subsequence of length p . It follows that the former sequence contains a φ -zero subsequence, which implies $g(\varphi, \mathbb{Z}_p) \leq 2p - 1$.

Next let $b_1, b_2, \dots, b_{2p-2}$ be a sequence in \mathbb{Z}_p of length $2p - 2$. It is clear that this sequence is φ -zero free if and only if the sequence $f(b_1), f(b_2), \dots, f(b_{2p-2})$ does not contain any zero-sum subsequence of length p . By the EGZ theorem, this is equivalent to the fact that the later sequence is of the form $[y]^{p-1}[z]^{p-1}$, where $y, z \in \mathbb{Z}_p$ and $y \neq z$. Since the value set of $f(x)$ for $x \in \mathbb{Z}_p$ contains at least two distinct elements, it follows that there exists a φ -zero free sequence in \mathbb{Z}_p of length $2p - 2$. Hence $g(\varphi, \mathbb{Z}_p) = 2p - 1$. Furthermore, a simple computation shows that for $u, v \in \mathbb{Z}_p, u \neq v$, the equality $f(u) = f(v)$ holds if and only if $u + v = -cb^{-1}$. Therefore $M(\varphi, \mathbb{Z}_p)$ is the set of all sequences of the form in (i).

(ii) Suppose $a \neq 0, b = 0$ and $c = 0$. Then $\varphi = as_1^2$, and (ii) follows by the EGZ theorem.

(iii) Suppose $a \neq 0$, $b = 0$ and $c \neq 0$. Without loss of generality, we may assume that $a = 1$. Then we have $\varphi = s_1^2 + cs_1$.

Let S be a sequence in \mathbb{Z}_p of length $2p - 2$. We will show that S contains a φ -zero subsequence, which implies $g(\varphi, \mathbb{Z}_p) \leq 2p - 2$. The case $d(S) = 1$ is trivial; the case $d(S) \geq 3$ follows by the EGZ theorem (ii). We now consider the case $d(S) = 2$. If S has an element appearing more than $p - 1$ times, then it is clear that S contains a zero-sum subsequence of length p , which is also a φ -zero subsequence. So we may assume that $S = [u]^{p-1}[v]^{p-1}$, where $u, v \in \mathbb{Z}_p$ and $u \neq v$. Let α be the integer such that $0 \leq \alpha \leq p - 1$ and $\alpha \equiv c(v - u)^{-1} \pmod{p}$, and let $T = [u]^\alpha[v]^{p-\alpha}$. It is clear that $\alpha \neq 0$, and hence T is a subsequence of S of length p . A simple computation shows that $s_1(T) = \alpha(u - v) = -c$. It follows that $\varphi(T) = 0$, and hence T is a φ -zero subsequence of S .

Let $V = [u]^{p-1}[u + c]^{p-2}$, where $u \in \mathbb{Z}_p$. If T is a subsequence of V of length p , then it has the form $[u]^{p-\alpha}[u + c]^\alpha$, where $1 \leq \alpha \leq p - 2$. A simple computation shows that

$$\varphi(T) = \alpha c(\alpha c + c) = c^2 \alpha(\alpha + 1) \neq 0,$$

and hence V is φ -zero free. Thus we have proved that $g(\varphi, \mathbb{Z}_p) = 2p - 2$.

We now describe the set $M(\varphi, \mathbb{Z}_p)$. The argument above shows that all the sequences of the form $[u]^{p-1}[u + c]^{p-2}$, where $u \in \mathbb{Z}_p$, belong to $M(\varphi, \mathbb{Z}_p)$. Now let U be a φ -zero free sequence in \mathbb{Z}_p of length $2p - 3$. It is clear that if $d(U) = 1$, then U contains a φ -zero sequence, a contradiction. If $d(U) \geq 4$, then, by Lemma 2.2 (i), it contains a zero-sum subsequence of length p , which is also a φ -zero sequence, a contradiction.

We claim that $d(U) \neq 3$. Suppose, to the contrary, that $d(U) = 3$. If $p = 3$, then $U = [0]^1[1]^1[2]^1$, and it is clear that U is a φ -zero sequence, a contradiction. So we may assume $p \geq 5$. Since U is φ -zero free, it follows that U does not contain any zero-sum subsequence of length p . Hence, by Lemma 2.2 (ii), it must be of the form

$$U = [u]^{p-1}[u + w]^{p-3}[u + 2w]^1,$$

where $u, w \in \mathbb{Z}_p$ and $w \neq 0$. We consider three cases of w .

Case 1 : $w \neq c$ and $w \neq c2^{-1}$. Let α be the integer such that $0 \leq \alpha \leq p - 1$ and $\alpha \equiv cw^{-1} \pmod{p}$, and let $T = [u]^\alpha[u + w]^{p-\alpha}$. It is clear that $\alpha \notin \{0, 1, 2\}$, and hence T is a subsequence of U of length p . A simple computation shows that $\varphi(T) = -\alpha w(-\alpha w + c) = 0$. Hence T is a φ -zero subsequence of U , a contradiction.

Case 2 : $w = c$. Let $T = [u]^2[u + w]^{p-3}[u + 2w]^1$. A simple computation shows that $\varphi(T) = -w(-w + c) = 0$. Hence T is a φ -zero subsequence of U , a contradiction.

Case 3 : $w = c2^{-1}$. Let $T = [u]^3[u + w]^{p-4}[u + 2w]^1$. A simple computation shows that $\varphi(T) = -2w(-2w + c) = 0$. Hence T is a φ -zero subsequence of U , a contradiction.

Thus we have proved that $d(U) \neq 3$, and our claim follows. Hence we must have $d(U) = 2$. Since U is a φ -zero free sequence, it does not contain any zero-sum subsequence of length p . Hence, by Lemma 2.2 (ii) again, it must be of the form

$$U = [u]^{p-1}[v]^{p-2},$$

where $u, v \in \mathbb{Z}_p$ and $u \neq v$. We will show that $v - u = c$. Suppose, to the contrary, that $v - u \neq c$. Let α be the integer such that $0 \leq \alpha \leq p - 1$ and $\alpha \equiv c(v - u)^{-1} \pmod{p}$, and let $T = [u]^\alpha[v]^{p-\alpha}$. It is clear that $\alpha \notin \{0, 1\}$, and hence T is a subsequence of U of length p . A simple computation shows that

$$\varphi(T) = \alpha(u - v)(\alpha(u - v) + c) = 0.$$

Hence T is a φ -zero subsequence of U , a contradiction. Thus we have $v - u = c$, and (iii) follows.

(iv) Suppose $a \neq 0, b \neq 0$ and $p \geq 5$. Without loss of generality, we may assume that $a = 1$. Then we have $\varphi = s_1^2 + bs_2 + cs_1$. By the change of variables $x_i \mapsto x_i - c(2b)^{-1}$ for $1 \leq i \leq p$, the polynomial φ becomes $s_1^2 + bs_2$. So, without loss of generality, we may also assume that $c = 0$. We first prove that $g(\varphi, \mathbb{Z}_p) \leq 4p - 3$. Let $a_1, a_2, \dots, a_{4p-3}$ be a sequence in \mathbb{Z}_p of length $4p - 3$. By Lemma 2.3, the sequence $(a_1, a_1^2), (a_2, a_2^2), \dots, (a_{4p-3}, a_{4p-3}^2)$ in $\mathbb{Z}_p \oplus \mathbb{Z}_p$ contains a zero-sum subsequence of length p . It follows that the former sequence contains a subsequence, say T , that is an s_1 -zero and s_2 -zero sequence simultaneously. It is clear that T is also a φ -zero sequence, and hence the required inequality follows.

We now establish the lower bound for $g(\varphi, \mathbb{Z}_p)$.

Claim *There exists $u \in \mathbb{Z}_p$ such that $b(1 - u^2)$ is a quadratic non-residue in \mathbb{Z}_p .*

Let A be the set of all squares in \mathbb{Z}_p and let $B = \{b(1 - x) \mid x \in A\}$. Since $p \geq 5$, there exists a quadratic non-residue w in \mathbb{Z}_p with $w \neq -1$. Then we have $\sum_{x \in A} x + w \sum_{x \in A} x = \sum_{y \in \mathbb{Z}_p} y = 0$. Since $w \neq -1$, it follows that

$$\sum_{x \in A} x = 0.$$

Hence,

$$\sum_{y \in B} y = \sum_{x \in A} b(1 - x) = b \sum_{x \in A} 1 - b \sum_{x \in A} x = b(p + 1)/2.$$

If $A = B$, then $\sum_{y \in B} y = \sum_{x \in A} x = 0$, which implies $b(p + 1)/2 = 0$, a contradiction. Hence $A \neq B$. Since $|A| = |B|$, it follows that there exists an element $u \in \mathbb{Z}_p$ such that $b(1 - u^2) \notin A$, and our claim follows.

Let us consider the sequence

$$U = [1]^{p-1}[-1]^{p-1}[u]^{n(p)-1}$$

where u is chosen so that $b(1-u^2)$ is a quadratic non-residue in \mathbb{Z}_p , and $n(p)$ denotes the least quadratic non-residue modulo p . To prove $g(\varphi, \mathbb{Z}_p) \geq 2(p-1) + n(p)$, we show that the sequence U is φ -zero free. Suppose, to the contrary, that U contains a φ -zero subsequence of length p , say

$$T = [1]^\alpha [-1]^\beta [u]^\gamma,$$

where $0 \leq \alpha, \beta \leq p-1$, $0 \leq \gamma \leq n(p)-1$ and $\alpha + \beta + \gamma = p$. A simple computation shows that $\varphi(T) = 0$ implies the equality

$$(\alpha - \beta + u\gamma)^2 - b(1 - u^2)\gamma = 0.$$

If $\gamma = 0$, then it follows that $\alpha - \beta \equiv 0 \pmod{p}$, which is impossible since $0 \leq \alpha, \beta \leq p-1$ and $\alpha + \beta = p$. If $1 \leq \gamma \leq n(p)-1$, then γ is a quadratic residue in \mathbb{Z}_p . Hence $b(1-u^2)\gamma$ is a quadratic non-residue in \mathbb{Z}_p , a contradiction. Thus we have proved that the sequence U is φ -zero free, and (iv) follows.

The proof of the theorem is complete. □

Remark Let us consider the case that $\varphi = as_1^2 + bs_2 + cs_1$, where $a, b, c \in \mathbb{Z}_p$, $a \neq 0$ and $b \neq 0$, as in Theorem 2.1 (iv). We note that the inequality $g(\varphi, \mathbb{Z}_p) \geq 2(p-1) + n(p)$ does not hold for $p = 3$. Indeed, a direct computation shows that $g(\varphi, \mathbb{Z}_3) = 5$ if $b = a$, and $g(\varphi, \mathbb{Z}_3) = 6$ if $b = -a$, while $2(p-1) + n(p) = 6$ if $p = 3$.

The problem of finding the value of $g(\varphi, \mathbb{Z}_p)$, where φ has the form above, for $p \geq 5$ is still open. A computer aided computation shows that $g(\varphi, \mathbb{Z}_5) = 11$ if $b = a$, and $g(\varphi, \mathbb{Z}_5) = 10$ if $b \neq a$; and $g(\varphi, \mathbb{Z}_7) = 17$ if $b = -2a$, and $g(\varphi, \mathbb{Z}_7) = 15$ if $b \neq -2a$. It can be seen that the lower bound for $g(\varphi, \mathbb{Z}_p)$ in Theorem 2.1 (iv) is sharp for $p = 5, 7$.

Acknowledgements. The authors would like to thank the anonymous referee for his valuable comments and suggestions.

References

[1] N. Alon and M. Dubiner, *Zero-sum sets of prescribed size*, Combinatorics, Paul Erdős is eighty, Vol. 1, Bolyai Soc. Math. Stud., János Bolyai Math. Soc., (Budapest, 1993), 33–50.

[2] A. Bialostocki, *Zero sum trees: a survey of results and open problems*, Finite and infinite combinatorics in sets and logic (Banff, AB, 1991), 19–29, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., 411, Kluwer Acad. Publ., Dordrecht, 1993.

[3] A. Bialostocki, *Some problems in view of recent developments of the Erdős-Ginzburg-Ziv theorem*, Combinatorial number theory, 111–120, de Gruyter, Berlin, 2007.

- [4] A. Bialostocki and P. Dierker, *Zero sum Ramsey theorems*, Proceedings of the Twentieth Southeastern Conference on Combinatorics, Graph Theory, and Computing (Boca Raton, FL, 1989). Congr. Numer. **70** (1990) 119–130.
- [5] A. Bialostocki and P. Dierker, *On the Erdős-Ginzburg-Ziv theorem and the Ramsey numbers for stars and matchings*, Discrete Math. **110** (1992), no. 1-3, 1–8.
- [6] A. Bialostocki, P. Dierker, D. Grynkiewicz, and M. Lotspeich, *On some developments of the Erdős-Ginzburg-Ziv theorem II*, Acta Arith. **110** (2003), no. 2, 173–184.
- [7] A. Bialostocki and M. Lotspeich, *Some developments of the Erdős-Ginzburg-Ziv theorem I*, Sets, graphs and numbers (Budapest, 1991), 97–117, Colloq. Math. Soc. János Bolyai 60, North-Holland, Amsterdam, 1992.
- [8] Y. Caro, *Zero-sum problems-a survey*, Discrete Math. **152** (1996), no. 1-3, 93–113.
- [9] P. Erdős, A. Ginzburg, and A. Ziv, *Theorem in additive number theory*, Bull. Res. Council Israel **10F** (1961), 41–43.
- [10] W. Gao and A. Geroldinger, *Zero-sum problems in finite abelian groups: a survey*, Expo. Math. **24** (2006) no. 4, 337–369.
- [11] A. Geroldinger, *Additive group theory and non-unique factorizations*, Combinatorial Number Theory and Additive Group Theory (A. Geroldinger and I. Ruzsa, eds.), Advanced Courses in Mathematics CRM Barcelona, Birkhäuser, 2009, pp. 1–86.
- [12] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics **278**, Chapman & Hall/CRC, 2006.
- [13] D. J. Grynkiewicz, *A weighted Erdős-Ginzburg-Ziv theorem*, Combinatorica **26** (2006), no. 4, 445–453.
- [14] C. Reiher, *On Kemnitz conjecture concerning lattice-points in the plane*, Ramanujan J. **13** (2007), no. 1-3, 333–337.
- [15] S. Savchev and F. Chen, *Long n -zero-free sequences in finite cyclic groups*, Discrete Math. **308** (2008), 1–8.
- [16] T. Yuster and B. Peterson, *A generalization of an addition theorem for solvable groups*, Canad. J. Math. **36** (1984) no. 3, 529–536.