Dedicated to the memory of Lucian Bădescu

IDEALS GENERATED BY POWER SUMS

ALDO CONCA, ANURAG K. SINGH, and KANNAN SOUNDARARAJAN

Communicated by Marian Aprodu

We consider ideals in a polynomial ring generated by collections of power sum polynomials, and obtain conditions under which these define complete intersection rings, normal domains, and unique factorization domains. We also settle a key case of a conjecture of Conca, Krattenthaler, and Watanabe, and prove other results in that direction.

AMS 2020 Subject Classification: 13C40, 13C70, 05E05.

Key words: complete intersections, power sums.

1. INTRODUCTION

Let $S := K[x_1, \dots, x_n]$ be a polynomial ring over a field K. For a positive integer a, we use p_a to denote the power sum $x_1^a + \cdots + x_n^a$. If K has characteristic zero and $a_1, a_2, \dots, a_n$ are distinct positive integers, the Jacobian criterion shows that $p_{a_1}, \dots, p_{a_n}$ are algebraically independent polynomials over K; the problem of determining when $n+1$ power sums generate the field of symmetric rational functions in $x_1, \dots, x_n$ over K is settled in [5]. In a different direction, the following is studied in [4]:

PROBLEM 1.1. *Characterize the sets $A := \{a_1, a_2, \dots, a_n\}$ of positive integers such that the corresponding power sums $p_{a_1}, \dots, p_{a_n}$ form a regular sequence in the polynomial ring S.*

The base field is taken to be $\mathbb{C}$ in [4], but the problem makes sense more generally.

A.C. is supported by PRIN 2020355B8Y “Squarefree Gröbner degenerations, special varieties and related topics,” by MIUR Excellence Department Project awarded to the Dept. of Mathematics, Univ. of Genova, CUP D33C23001110001, and by INdAM-GNSAGA; A.K.S. is supported by NSF grants DMS 2101671 and DMS 2349623; K.S. is supported by a Simons Investigator award from the Simons Foundation, and by NSF grant DMS 2100933. A.C. and A.K.S. were also supported by NSF grant DMS 1928930 and by Alfred P. Sloan Foundation grant G-2021-16778, while in residence at SLMath/MSRI, Berkeley, during the Spring 2024 Commutative Algebra program.

doi: 10.59277/RRMPA.2025.49.71

Remark 1.2. We record some straightforward observations; some of these are proved in [4] in the case $K = \mathbb{C}$, but the proofs are readily adapted to the more general setting.

(1) Whether $p_{a_1}, \ldots, p_{a_n}$ is a regular sequence is unaffected by enlarging K, so one may assume that the base field K is algebraically closed.

(2) Set $d := \gcd(a_1, a_2, \ldots, a_n)$. It is readily seen that $p_{a_1}, \ldots, p_{a_n}$ is a regular sequence precisely if $p_{a_1/d}, \ldots, p_{a_n/d}$ is a regular sequence. Thus, in studying Problem 1.1, one may assume that $\gcd(a_1, a_2, \ldots, a_n) = 1$.

(3) A necessary condition for $p_{a_1}, \ldots, p_{a_n}$ to be a regular sequence is that $n!$ divides the product $a_1 a_2 \cdots a_n$.

(4) If the characteristic of K is 0 or strictly greater than n, and $a_1, \ldots, a_n$ are consecutive positive integers, then $p_{a_1}, \ldots, p_{a_n}$ is a regular sequence.

(5) If $p_{a_1}, \ldots, p_{a_n}$ form a regular sequence in $\mathbb{C}[x_1, \ldots, x_n]$, then they also form a regular sequence in $\mathbb{F}_p[x_1, \ldots, x_n]$ for sufficiently large prime integers p. However, finding optimal bounds for such primes appears hard; for example, p_1, p_6, p_{100} is a regular sequence in $\mathbb{C}[x_1, x_2, x_3]$, but is not a regular sequence in $\mathbb{F}_p[x_1, x_2, x_3]$ for the prime integer $p = 4594399$.

(6) Problem 1.1 is easily answered for $n = 2$: polynomials p_a, p_b form a regular sequence in $K[x_1, x_2]$ if and only if the characteristic of K differs from 2, and either $a/\gcd(a, b)$ or $b/\gcd(a, b)$ is even.

Problem 1.1 is open for $n = 3$; the following is [4, Conjecture 2.10]:

Conjecture 1.3. *Suppose $n = 3$, the characteristic of the field K is zero, and that a, b, c are integers with $0 < a < b < c$ and $\gcd(a, b, c) = 1$. Then p_a, p_b, p_c is a regular sequence if and only if 6 divides abc.*

One direction holds more generally, as recorded in Remark 1.2. The conjecture is proven for certain special values of a, b, c in [4]; the case $a = 1$ is completely settled in Section 4 of the present paper, while in Section 5, we prove that for each fixed positive integer a, there are at most finitely many triples (a, b, c) that possibly violate Conjecture 1.3.

In [10, Conjecture 12] the authors extend Conjecture 1.3 to a statement about the zero loci of p_a, p_b, p_c, under the assumption that $\gcd(a, b, c) = 1$, and verify their conjecture computationally for $a + b + c \leqslant 300$; we prove this stronger conjecture in the case $a = 1$.

In general, for distinct integers with $\gcd(a_1, a_2, \ldots, a_n) = 1$ and $n!$ dividing $a_1 a_2 \cdots a_n$, the elements $p_{a_1}, \ldots, p_{a_n}$ need not form a regular sequence.

Consider, for example, the case where $n = 4$, and take $p_{a_1}, \ldots, p_{a_4}$ in the polynomial ring $S := \mathbb{C}[x_1, x_2, x_3, x_4]$. Let ν_2 denote the 2-adic valuation on $\mathbb{Z} \smallsetminus \{0\}$. If each $\nu_2(a_i)$ is either 0 or k, for k a fixed positive integer, then

$$(p_{a_1}, \ldots, p_{a_4}) \subseteq (x_1 + x_2,\ x_3 + x_4,\ x_1^{2^k} + x_3^{2^k}),$$

which justifies condition (2) in the conjecture below. For condition (3), note that $p_5 \in (p_1, p_2)S$ by Remark 2.2, and consequently $p_{5d} \in (p_d, p_{2d})S$ for each positive integer d. A similar argument shows that $p_5 \in (p_1, p_3)S$, so the set A does not contain a subset of the form $\{d, 3d, 5d\}$; this condition, however, is implied by the others. The three conditions in the conjecture below are necessary and independent, see [4, Remark 2.16].

CONJECTURE 1.4 ([4, Conjecture 2.15]). *Suppose that $n = 4$ and K has characteristic zero. Let $A := \{a_1, a_2, a_3, a_4\}$ where* $\gcd(a_1, a_2, a_3, a_4) = 1$. *Then $p_{a_1}, p_{a_2}, p_{a_3}, p_{a_4}$ is a regular sequence if and only if A satisfies the following conditions:*

(1) *The product $a_1a_2a_3a_4$ is a multiple of* 24*;*

(2) *the set $\{\nu_2(a_i) \mid a_i \in A\}$ contains at least two distinct positive integers;*

(3) *the set A does not contain a subset of the form $\{d, 2d, 5d\}$ for any $d \in \mathbb{N}$.*

2. PRIMALITY, NORMALITY, AND FACTORIALITY

The discussion thus far concerned when power sums $p_{a_1}, \ldots, p_{a_n}$ form a regular sequence in $K[x_1, \ldots, x_n]$. It is also natural to ask:

Question 2.1. For a set of positive integers $A := \{a_1, \ldots, a_c\}$, let p_A denote the sequence of power sum polynomials $p_{a_1}, \ldots, p_{a_c}$ in $S := K[x_1, \ldots, x_n]$, and let $I_A := (p_A)$ denote the corresponding ideal of S.

(1) When is p_A a regular sequence, equivalently when is the ideal I_A a complete intersection of codimension c?

(2) When is S/I_A a normal domain?

(3) When is S/I_A a unique factorization domain?

(4) When is the ideal I_A radical?

(5) When is the ideal I_A prime?

Remark 2.2. The specification "of codimension c" in (1) is relevant; in general, the elements $p_{a_1}, \dots, p_{a_c}$ need not be minimal generators of I_A. For example, when $n \leqslant 4$, the polynomials p_1, p_2, p_3, p_4 generate the ring of symmetric polynomials; degree considerations then imply that p_5 is a K-linear combination of p_1^5, $p_1^3 p_2$, $p_1^2 p_3$, $p_1 p_2^2$, $p_1 p_4$, and $p_2 p_3$, so p_5 is an element of the ideal (p_1, p_2). Hence, $(p_1, p_2, p_5) = (p_1, p_2)$ is a complete intersection ideal, though not of codimension 3. The same argument shows as well that p_5 must be an element of the ideal (p_1, p_3).

While we do not pursue it here, one may consider analogues of these questions for other families of symmetric polynomials such as complete symmetric polynomials or elementary symmetric polynomials; see for example [4, Conjecture 2.17].

THEOREM 2.3. *For distinct positive integers $a_1, \dots, a_c$ consider the ideal $I_A := (p_{a_1}, \dots, p_{a_c})$ in the polynomial ring $S := \mathbb{C}[x_1, \dots, x_n]$.*

(1) *If $n \geqslant 2c-1$, then the ideal I_A is a complete intersection of codimension c.*

(2) *If $n \geqslant 2c+1$, then S/I_A is a normal domain.*

(3) *If $n \geqslant 2c+3$, then S/I_A is a unique factorization domain.*

(4) *If $n \geqslant 2c$, then the ring S/I_A is reduced.*

Before proceeding with the proof, we note that the bounds in the theorem are optimal:

Example 2.4. (1) Suppose $n = 2c-2$, take $A := \{1, 3, 5, \dots, 2c-1\}$. Then $|A| = c$ but the ideal I_A has height at most $c-1$ since

$$I_A \subseteq (x_1 + x_2,\ x_3 + x_4, \dots, x_{2c-3} + x_{2c-2}).$$

Indeed, the height $c-1$ ideal displayed on the right contains p_a for each odd integer a.

(2) We show that I_A need not be prime in the case $n = 2c$. If $c = 1$, the ideal (p_2) is not prime; if $c \geqslant 2$, consider once again $A := \{1, 3, 5, \dots, 2c-1\}$ with $|A| = c$, in which case

$$I_A \subsetneq (x_1 + x_2,\ x_3 + x_4, \dots, x_{2c-1} + x_{2c}).$$

Since height $I_A = c$ by Theorem 2.3 (1), each ideal above has height c, so I_A is not prime.

(3) Suppose $n = 2c+2$, take $A := \{2, 6, 10, \dots, 4c-2\}$. Then $|A| = c$ and S/I_A is a normal domain of dimension $c+2$ by Theorem 2.3 (3). It is however, not a unique factorization domain: setting $i := \sqrt{-1}$ in $\mathbb{C}$, the image of

$$(x_1 - ix_2,\ x_3 - ix_4, \dots, x_{2c+1} - ix_{2c+2})$$

in S/I_A is a height one prime ideal that is not principal.

(4) Quite generally, one has $\mathbb{C}[e_1, \ldots, e_n] = \mathbb{C}[p_1, \ldots, p_n]$ where e_i is the i-th symmetric polynomial. Taking $n = 2c - 1$, it follows that

$$p_{2c} \in \mathbb{C}[p_1, \ldots, p_{2c-1}] =: R.$$

Degree considerations then imply that $p_{2c} = g_1 p_1 + \cdots + g_{c-1} p_{c-1} + g_c p_c^2$, where the g_i are homogeneous elements of R. It follows that

$$p_{2c} \in (p_1, \ldots, p_{c-1}, p_c^2)S$$

where, recall, $S = \mathbb{C}[x_1, \ldots, x_n]$. Since $p_1, \ldots, p_{c-1}, p_{2c}$ is a regular sequence in the ring S by Theorem 2.3 (1), one has $p_{2c} \notin (p_1, \ldots, p_{c-1})S$. Thus g_c, the coefficient of p_c^2 in the equation above, must be nonzero, hence a unit. It follows that

$$p_c^2 \in (p_1, \ldots, p_{c-1}, p_{2c})S.$$

If $p_c \in (p_1, \ldots, p_{c-1}, p_{2c})S$, then degree considerations would force

$$p_c \in (p_1, \ldots, p_{c-1})S,$$

which is not possible since $p_1, \ldots, p_c$ is a regular sequence in S by Theorem 2.3 (1). Hence, taking $A := \{1, \ldots, c-1, 2c\}$ one has $p_c^2 \in I_A$ and $p_c \notin I_A$, so the ideal I_A is not radical.

Proof. The proofs of (1) and (2) are intertwined, using induction on c. Suppose $c = 1$, then (1) is immediate, while (2) follows using the Jacobian criterion for the hypersurface S/I_A, bearing in mind that $n \geqslant 3$.

Next, suppose that $c > 1$ and $n \geqslant 2c - 1$. By the inductive hypothesis, $S/(p_{a_1}, \ldots, p_{a_{c-1}})$ is a normal domain using (2), so (1) follows. Let us suppose that $n \geqslant 2c + 1$ and that the elements of A are ordered as $a_1 < \cdots < a_c$. By induction, we know that p_A is a regular sequence; we determine the singular locus of S/I_A using the Jacobian criterion.

Up to scalar multiples of the rows, the Jacobian matrix takes the form

$$J := \begin{pmatrix} x_1^{a_1-1} & x_2^{a_1-1} & \ldots & x_n^{a_1-1} \\ x_1^{a_2-1} & x_2^{a_2-1} & \ldots & x_n^{a_2-1} \\ \vdots & \vdots & & \vdots \\ x_1^{a_c-1} & x_2^{a_c-1} & \ldots & x_n^{a_c-1} \end{pmatrix}.$$

Consider the size c minors of the Jacobian matrix J with respect to the lexicographic order induced by $x_n > x_{n-1} > \cdots > x_1$, e.g., the minor determined by the first c columns is

$$\det \begin{pmatrix} x_1^{a_1-1} & x_2^{a_1-1} & \dots & x_c^{a_1-1} \\ x_1^{a_2-1} & x_2^{a_2-1} & \dots & x_c^{a_2-1} \\ \vdots & \vdots & & \vdots \\ x_1^{a_c-1} & x_2^{a_c-1} & \dots & x_c^{a_c-1} \end{pmatrix} = x_1^{a_1-1}x_2^{a_2-1}\cdots x_c^{a_c-1} + \text{ lower order.}$$

Let $I_c(J)$ denote the ideal generated by the size c minors of J, and let H denote its initial ideal. Then $x_1^{a_1-1}x_2^{a_2-1}\cdots x_c^{a_c-1} \in H$, and similarly

$$x_{i_1}^{a_1-1}x_{i_2}^{a_2-1}\cdots x_{i_c}^{a_c-1} \in H \qquad \text{for all } 1 \leqslant i_1 < i_2 < \cdots < i_c \leqslant n.$$

Assume for the moment that $a_1 \geqslant 2$, in which case each exponent $a_i - 1$ above is positive. Then $\operatorname{rad} H$ contains each squarefree monomial of degree c in the variables $x_1, \dots, x_n$, so height $H \geqslant n-c+1$. On the other hand, if $a_1 = 1$, then $\operatorname{rad} H$ contains each squarefree monomial of degree $c-1$ in the $n-1$ variables $x_2, \dots, x_n$, so once again

$$\operatorname{height} H \;\geqslant\; (n-1)-(c-1)+1 \;=\; n-c+1.$$

In either case the ideal H, and hence $I_c(J)$, has height at least $n-c+1$ in the polynomial ring S. It follows that in the ring S/I_A, the defining ideal of the singular locus has height at least $n-2c+1$. Under our assumption that $n \geqslant 2c+1$, the ring S/I_A therefore satisfies the Serre condition (R_v) with $v = n-2c$, and is hence normal, completing the proof of (2).

In (3), one has $n \geqslant 2c+3$. If $c = 0$, there is little to be said, so assume $c \geqslant 1$. Then S/I_A is a complete intersection ring of dimension at least 4, satisfying the Serre condition (R_3) by the previous paragraph, and is hence, a UFD by [8, Corollaire XI.3.14].

For (4), note that $n \geqslant 2c$ implies that S/I_A is a complete intersection, so our computation of the singular locus still applies, and shows that S/I_A satisfies the Serre condition (R_0). □

Remark 2.5. Suppose $n \geqslant 2c-1$, so that I_A is a complete intersection of codimension c. Then, in the proof above, we saw that the ideal $I_c(J)$ has height at least $n-c+1$. As this is the upper bound for the height of the ideal of size c minors of a $c \times n$ matrix, it follows that height $I_c(J) = n-c+1$.

We mention that maximal minors of *generalized Vandermonde matrices*

$$\begin{pmatrix} x_1^{b_1} & x_2^{b_1} & \dots & x_n^{b_1} \\ x_1^{b_2} & x_2^{b_2} & \dots & x_n^{b_2} \\ \vdots & \vdots & & \vdots \\ x_1^{b_c} & x_2^{b_c} & \dots & x_n^{b_c} \end{pmatrix},$$

where $c \geqslant n$, are studied in [6]. Up to monomial and Vandermonde factors, these are the *Schur polynomials*.

While Theorem 2.3 addresses the case of c arbitrary power sums, we next record a result for consecutive power sums:

THEOREM 2.6. *Set $S := \mathbb{C}[x_1, \dots, x_n]$ be a polynomial ring, and let a and c be positive integers. Then the ring $S/(p_a, p_{a+1}, \dots, p_{a+c-1})$ has an isolated singular point.*

Proof. Set $R := S/(p_a, p_{a+1}, \dots, p_{a+c-1})$. If $c \geqslant n$, then R is an artinian local ring by [4, Proposition 2.9], so the assertion is immediate. Assume $c < n$, in which case R is a complete intersection ring by the same proposition; we examine the singular locus.

Up to scalar multiples of the rows, the Jacobian matrix takes the form

$$J := \begin{pmatrix} x_1^{a-1} & x_2^{a-1} & \dots & x_n^{a-1} \\ x_1^{a} & x_2^{a} & \dots & x_n^{a} \\ \vdots & \vdots & & \vdots \\ x_1^{a+c-2} & x_2^{a+c-2} & \dots & x_n^{a+c-2} \end{pmatrix}.$$

Using $I_c(J)$ for the ideal of minors as earlier, consider the ideal

$$\mathfrak{a} := I_c(J) + (p_a, p_{a+1}, \dots, p_{a+c-1})S$$

of S. It suffices to verify that the algebraic set $V(\mathfrak{a})$ contains no nonzero point of $\mathbb{C}^n$. Suppose $\boldsymbol{z} := (z_1, \dots, z_n) \in V(\mathfrak{a})$. If $\boldsymbol{z}$ has at least c distinct nonzero entries, without loss of generality $z_1, \dots, z_c$, evaluating the minor determined by the first c columns of J at $\boldsymbol{z}$ gives

$$\det \begin{pmatrix} z_1^{a-1} & z_2^{a-1} & \dots & z_c^{a-1} \\ z_1^{a} & z_2^{a} & \dots & z_c^{a} \\ \vdots & \vdots & & \vdots \\ z_1^{a+c-2} & z_2^{a+c-2} & \dots & z_c^{a+c-2} \end{pmatrix}$$

$$= (z_1 \cdots z_c)^{a-1} \det \begin{pmatrix} 1 & 1 & \dots & 1 \\ z_1 & z_2 & \dots & z_c \\ \vdots & \vdots & & \vdots \\ z_1^{c-1} & z_2^{c-1} & \dots & z_c^{c-1} \end{pmatrix}$$

which must be nonzero, a contradiction. It follows that the number k of distinct entries of $\boldsymbol{z}$ is at most c, allowing now for zero entries. Suppose $z_1, \dots, z_k$ are the distinct entries, and occur with multiplicity $m_1, \dots, m_k$, respectively, in the n-tuple $\boldsymbol{z}$. The fact that the power sums $p_a, p_{a+1}, \dots, p_{a+k-1}$ vanish at $\boldsymbol{z}$ gives us the matrix equation

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ z_1 & z_2 & \dots & z_k \\ \vdots & \vdots & & \vdots \\ z_1^{k-1} & z_2^{k-1} & \dots & z_k^{k-1} \end{pmatrix} \begin{pmatrix} m_1 z_1^a \\ m_2 z_2^a \\ \vdots \\ m_k z_k^a \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

This implies that the determinant of the Vandermonde matrix to the left must be zero, a contradiction. It follows that the only point in $V(\mathfrak{a})$ is $(0, \dots, 0)$. □

3. POWER SUMS IN FOUR VARIABLES

While each part of Theorem 2.3 is optimal in view of Example 2.4, the boundary cases can be subtle and interesting; for example, when $n = 4$ and $A = \{a, b\}$, the ideal I_A is radical by Theorem 2.3 (4), but it appears difficult to determine when I_A is prime, see Remark 3.3. First, however, we record precisely when the ring $\mathbb{C}[x_1, x_2, x_3, x_4]/(p_a, p_b)$ is a normal domain.

For p a prime integer, let ν_p denote the p-adic valuation on $\mathbb{Z} \smallsetminus \{0\}$, i.e., $\nu_p(n)$ is the largest integer e such that p^e divides n.

THEOREM 3.1. *Let $S := \mathbb{C}[x_1, \dots, x_4]$. For positive integers $a < b$, set*

$$p_a := x_1^a + \dots + x_4^a \qquad \text{and} \qquad p_b := x_1^b + \dots + x_4^b.$$

If $a = 1$, then $S/(p_a, p_b)$ is a normal domain if and only if b is even, whereas if $1 < a < b$, then $S/(p_a, p_b)$ is a normal domain if and only if

(1) *$\nu_2(a) \neq \nu_2(b)$, and*

(2) *either $\nu_3(a) \neq \nu_3(b)$, or $\nu_3(a) = \nu_3(b) = \nu_3(a - b)$.*

Proof. Since a and b are distinct, $S/(p_a, p_b)$ is a complete intersection ring of dimension 2, and is normal precisely if the singular locus consists of a point. Set $\mathfrak{m}$ to be the homogeneous maximal ideal of S.

Up to scalar multiples of the rows, the Jacobian matrix is

$$\begin{pmatrix} x_1^{a-1} & x_2^{a-1} & x_3^{a-1} & x_4^{a-1} \\ x_1^{b-1} & x_2^{b-1} & x_3^{b-1} & x_4^{b-1} \end{pmatrix},$$

with the ideal generated by its size two minors being

$$\mathfrak{a} := \big((x_i x_j)^{a-1}(x_j^{b-a} - x_i^{b-a}) : 1 \leqslant i < j \leqslant 4\big).$$

Consider first the case where $a = 1$. Then each minimal prime of $\mathfrak{a}$ has the form

$$\mathfrak{b} := (x_1 - \alpha x_4, x_2 - \beta x_4, x_3 - \gamma x_4),$$

where α, β, γ are complex numbers with $\alpha^{b-1} = \beta^{b-1} = \gamma^{b-1} = 1$. Since

$$p_a \equiv (\alpha + \beta + \gamma + 1)x_4 \bmod \mathfrak{b},$$

and

$$p_b \equiv (\alpha^b + \beta^b + \gamma^b + 1)x_4^b \equiv (\alpha + \beta + \gamma + 1)x_4^b \bmod \mathfrak{b},$$

it follows that $\mathfrak{m}$ is the unique minimal prime of $\mathfrak{a} + (p_a, p_b)$ unless there exist α, β, γ in $\mathbb{C}$ with $\alpha^{b-1} = \beta^{b-1} = \gamma^{b-1} = 1$ and $\alpha + \beta + \gamma + 1 = 0$. If b is even, no such (α, β, γ) exists by Lemma 3.2 (3), whereas if b is odd, one may take (α, β, γ) to be $(-1, 1, -1)$.

Next, suppose $a \geqslant 2$. Then, up to radical, the ideal $\mathfrak{a}$ contains

$$x_i x_j \big(x_j^{b-a} - x_i^{b-a}\big)$$

for each $1 \leqslant i < j \leqslant 4$. It follows that, up to permuting indices, a minimal prime of $\mathfrak{a}$ in S has one of the following forms

(a) (x_1, x_2, x_3),

(b) $(x_1, x_2, x_3 - \alpha x_4)$,

(c) $(x_1, x_2 - \alpha x_4, x_3 - \beta x_4)$, or

(d) $(x_1 - \alpha x_4, x_2 - \beta x_4, x_3 - \gamma x_4)$,

where $\alpha^{b-a} = \beta^{b-a} = \gamma^{b-a} = 1$. We examine these in turn:

Case (a) The only minimal prime of $(x_1, x_2, x_3) + (p_a, p_b)$ is $\mathfrak{m}$.

Case (b) The ideal $(x_1, x_2, x_3 - \alpha x_4) + (p_a, p_b)$ has radical

$$\big(x_1, x_2, x_3 - \alpha x_4, (\alpha^a + 1)x_4, (\alpha^b + 1)x_4\big) = \big(x_1, x_2, x_3 - \alpha x_4, (\alpha^a + 1)x_4\big),$$

where the equality above holds since $\alpha^{b-a} = 1$. There exists such an ideal other than $\mathfrak{m}$ precisely if $\nu_2(a) = \nu_2(b)$, see Lemma 3.2 (1).

Case (c) The ideal $(x_1, x_2 - \alpha x_4, x_3 - \beta x_4) + (p_a, p_b)$ has radical

$$\big(x_1, x_2 - \alpha x_4, x_3 - \beta x_4, (\alpha^a + \beta^a + 1)x_4\big).$$

Use Lemma 3.2 (2).

Case (d) Lastly, the ideal $(x_1 - \alpha x_4, x_2 - \beta x_4, x_3 - \gamma x_4) + (p_a, p_b)$ has radical

$$\big(x_1 - \alpha x_4, x_2 - \beta x_4, x_3 - \gamma x_4, (\alpha^a + \beta^a + \gamma^a + 1)x_4\big),$$

in which case we use Lemma 3.2 (3). □

Lemma 3.2. *Let a and b be distinct positive integers.*

(1) *There exists α in $\mathbb{C}$ with $\alpha^{b-a} = 1$ and with $\alpha^a + 1 = 0$ if and only if $\nu_2(a) = \nu_2(b)$.*

(2) *There exists α and β in $\mathbb{C}$ with $\alpha^{b-a} = 1 = \beta^{b-a}$ and $\alpha^a + \beta^a + 1 = 0$ if and only if $\nu_3(a) = \nu_3(b) < \nu_3(b-a)$.*

(3) *There exists α, β, and γ in $\mathbb{C}$ with $\alpha^{b-a} = \beta^{b-a} = \gamma^{b-a} = 1$ and with $\alpha^a + \beta^a + \gamma^a + 1 = 0$ if and only if $\nu_2(a) = \nu_2(b)$.*

Proof. The conditions are symmetric with respect to a and b, e.g., the condition $\alpha^{b-a} = 1$ gives $\alpha^b = \alpha^a$.

(1) If $e := \nu_2(a) = \nu_2(b)$, choose $\alpha \in \mathbb{C}$ with $\alpha^{2^e} = -1$, in which case $\alpha^a = -1 = \alpha^b$. For the converse, let $a = 2^e c$ and $b = 2^f d$, where c and d are odd. If $\alpha^a = -1 = \alpha^b$, then

$$(\alpha^{cd})^{2^e} = -1 = (\alpha^{cd})^{2^f},$$

so $e = f$.

(2) Let ω be a primitive cube root of unity. If

$$e := \nu_3(a) = \nu_3(b) < \nu_3(b-a),$$

choose α with $\alpha^{3^e} = \omega$. Then $\alpha^{3^{e+1}} = 1$, so $\alpha^{b-a} = 1$. Setting $\beta := \alpha^2$, one has $\beta^{b-a} = 1$ as well. Moreover, $\{\alpha^a, \beta^a\} = \{\omega, \omega^2\}$, so that

$$\alpha^a + \beta^a + 1 = 0.$$

For the converse, if α^a and β^a are roots of unity with $\alpha^a + \beta^a + 1 = 0$, then α^a and β^a must be complex conjugates with real part $-1/2$. It follows that $\{\alpha^a, \beta^a\} = \{\omega, \omega^2\}$. Assume, without loss of generality, that $\alpha^a = \omega$. Let $a = 3^e c$ and $b = 3^f d$, where c and d are relatively prime to 3. Suppose now that $\alpha^{b-a} = 1$. Then

$$(\alpha^{cd})^{3^e} = \omega^d \quad \text{and} \quad (\alpha^{cd})^{3^f} = \omega^c$$

are primitive cube roots of unity, so $e = f$. Also, $\alpha^{b-a} = 1$ implies that $\alpha^{3^e(d-c)} = 1$, so

$$\omega^{d-c} = \alpha^{a(d-c)} = \alpha^{3^e c(d-c)} = 1,$$

implying that 3 divides $d - c$.

(3) If $e := \nu_2(a) = \nu_2(b)$, choose α with $\alpha^{2^e} = -1$. Then $\alpha^{2^{e+1}} = 1$ so $\alpha^{b-a} = 1$. Setting $\beta := \alpha^2$ and $\gamma := \alpha$, one has $\beta^{b-a} = \gamma^{b-a} = 1$, and also

$$\alpha^a + \beta^a + \gamma^a + 1 = (-1) + 1 + (-1) + 1 = 0.$$

The converse. Suppose 4 distinct roots of unity sum to 0, then the corresponding vectors in the complex plane have length 1 and form a rhombus; pairing the parallel sides, each pair has sum 0. It follows that one of α^a, β^a, or γ^a equals -1. If the roots of unity are repeated, then $\{\alpha^a, \beta^a, \gamma^a, 1\} = \{\pm 1\}$. Assume, without loss of generality, that $\alpha^a = -1$. Then, if $\alpha^{b-a} = 1$, part (1) of the lemma implies that $\nu_2(a) = \nu_2(b)$. $\square$

Remark 3.3. Set $S := \mathbb{C}[x_1, x_2, x_3, x_4]$. It does not appear easy to determine precisely when the ring $S/(p_a, p_b)$ is a domain; we record some observations in this regard:

(1) If $a < b$ are odd integers, then (p_a, p_b) is not prime since the ideal (p_a, p_b) is strictly contained in $(x_1 + x_2, x_3 + x_4)$.

(2) If (p_a, p_b) is not prime, then neither is (p_{ak}, p_{bk}) for any positive integer k; one has an embedding of $\mathbb{C}$-algebras $S/(p_a, p_b) \hookrightarrow S/(p_{ak}, p_{bk})$ induced by $x_i \longmapsto x_i^k$.

(3) If $b = 4k + 2$, then $S/(p_2, p_b)$ is not normal in view of Theorem 3.1. Moreover,
$$(p_2, p_b) \subsetneq (x_1 - ix_2,\ x_3 - ix_4)$$
shows that (p_2, p_b) is not prime in this case.

(4) When $a = 2$, we conjecture that $S/(p_2, p_b)$ is a domain that is not normal precisely when $b = 6k + 5$ or $b = 12k + 8$, and k is an integer with $k \geqslant 1$. The case $k = 0$ of these appears below:

(5) The ideal (p_2, p_5) is not prime: one has $p_5 \in (p_1, p_2)$, see Remark 2.2, and it follows that $(p_2, p_5) \subsetneq (p_1, p_2)$.

(6) The ideal (p_2, p_8) is not prime: in the ring $S/(p_2, p_8)$ one has
$$\left(x_2^2x_3^2 + x_2^2x_4^2 + x_3^2x_4^2 - x_1^4\right)^2 - 2(x_1x_2x_3x_4)^2 = 0,$$
so the image of $x_2^2x_3^2 + x_2^2x_4^2 + x_3^2x_4^2 - x_1^4 - \sqrt{2} \cdot x_1x_2x_3x_4$ in $S/(p_2, p_8)$ is a zerodivisor; one may verify readily that this image is nonzero.

In contrast, one may verify that $\mathbb{Q}[x_1, x_2, x_3, x_4]/(p_2, p_8)$ is an integral domain using [3] or [7].

(7) When $a = 3$, we conjecture that $S/(p_3, p_b)$ is a domain that is not normal precisely when $b = 18k + 12$ and $k \geqslant 0$ is an integer.

(8) We arrived at our conjectures in the cases $a = 2$ and $a = 3$ as follows: first, one verifies using [3] or [7] that when $\mathbb{C}$ is replaced by $\mathbb{Q}$, the corresponding ring
$$R := \mathbb{Q}[x_1, x_2, x_3, x_4]/(p_a, p_b)$$
is an integral domain. Then, we use the computational algebra programs to determine the integral closure R' of R. Note that $R' \otimes_{\mathbb{Q}} \mathbb{C}$ is also normal, hence a product of normal domains. If $[R']_0 = \mathbb{Q}$, then $R' \otimes_{\mathbb{Q}} \mathbb{C}$ must be a normal domain, and it follows that its subring $R \otimes_{\mathbb{Q}} \mathbb{C} = S/(p_a, p_b)$ is a domain.

4. POWER SUMS IN THREE VARIABLES: A SPECIAL CASE OF THE CONJECTURE

We work over the complex numbers $\mathbb{C}$ throughout this section. Given positive integers $a < b < c$ with $\gcd(a, b, c) = 1$, Conjecture 1.3 as generalized in [10, Conjecture 12] may be rephrased as saying that the equations
$$1 + x^a + y^a = 1 + x^b + y^b = 1 + x^c + y^c = 0$$
only have trivial solutions, i.e., with either x and y being cube roots of unity, or one of them being 0 and the other being -1. We settle the conjecture when $a = 1$. In this case, $y = -1 - x$, so we are interested in solutions to the pair of polynomial equations

$$1 + x^b + (-1 - x)^b = 0 = 1 + x^c + (-1 - x)^c. \tag{4.0.1}$$

Indeed, we prove:

THEOREM 4.1. *For integers b and c with $1 < b < c$, the only possible common zeros of the polynomials $1 + x^b + (-1 - x)^b$ and $1 + x^c + (-1 - x)^c$ are 0, -1, ω, ω^2, where $\omega := e^{2\pi i/3}$. The common zeros at 0, -1 occur when $2 \nmid bc$, while the common zeros at ω, ω^2 occur when $3 \nmid bc$. Consequently, when $6 \mid bc$, there are no common zeros to the two polynomials.*

Closely related problems were considered previously in [1, 11]. In particular, Beukers [1, Theorem 4.1] established the following result:

THEOREM 4.2. *If $\theta \in \mathbb{C}$ differs from 0, -1, ω, ω^2, where $\omega := e^{2\pi i/3}$, then there is at most one integer $n > 1$ such that $1 + \theta^n - (1 + \theta)^n = 0$.*

If both b and c are odd, then Beukers's result shows that there are no solutions to (4.0.1) apart from 0, -1, ω, or ω^2. We now treat the cases when at least one of b or c is even. Our proof has some points in common with Beukers's approach, but is also different in some details. When $b \leqslant 5$, there are no roots of $1 + x^b + (-1 - x)^b$ apart from 0, -1, ω, ω^2, and so we may assume in what follows that $b \geqslant 6$.

LEMMA 4.3. *For integers $n \geqslant 2$, the polynomial $P_n(z) := 1+z^n+(-1-z)^n$ has degree n if n is even, and degree $n-1$ if n is odd; it factors as $C_n(z)Q_n(z)$ where $C_n(z)$ equals*

$$\begin{aligned} 1 \quad & \text{for } n \equiv 0 \bmod 6; \\ z(z+1)(z^2+z+1)^2 \quad & \text{for } n \equiv 1 \bmod 6; \\ (z^2+z+1) \quad & \text{for } n \equiv 2 \bmod 6; \\ z(z+1) \quad & \text{for } n \equiv 3 \bmod 6; \\ (z^2+z+1)^2 \quad & \text{for } n \equiv 4 \bmod 6; \\ z(z+1)(z^2+z+1) \quad & \text{for } n \equiv 5 \bmod 6. \end{aligned}$$

In particular, the degree of $Q_n(z)$ is a multiple of six; the zeros of $Q_n(z)$ differ from 0, -1, ω, ω^2 and occur in groups of six, with equal numbers of zeros on:

(1) *the open line segments $\mathrm{Re}(z) = -1/2$ going from ω to $-1/2 + i\infty$, and its conjugate segment going from ω^2 to $-1/2 - i\infty$;*

(2) *the open arc of the unit circle going counterclockwise from ω to ω^2;*

(3) *the open arc of the circle $|z+1| = 1$ going counterclockwise from ω^2 to ω.*

Specifically, suppose $\alpha := -1/2 + it$ is a zero with $t > \sqrt{3}/2$. Then:

(i) *α and $\overline{\alpha} = -1 - \alpha$ are zeros on the conjugate line segments as above;*

(ii) *$\overline{\alpha}/\alpha = (-1 - \alpha)/\alpha$ and $\alpha/\overline{\alpha} = -\alpha/(1 + \alpha)$ are zeros lying on the arc of $|z| = 1$;*

(iii) *$1/\alpha$ and $1/\overline{\alpha}$ are zeros lying on the arc of $|z + 1| = 1$.*

Proof. The first assertion on identifying the possible zeros at 0, -1, ω, ω^2 is readily checked. We now produce the right number of zeros on the line segment $-1/2 + it$ with $t > \sqrt{3}/2$ by counting sign changes; the remaining zeros stem from these zeros α by taking $\overline{\alpha}$, $(-1 - \alpha)/\alpha$, $-\alpha/(1 + \alpha)$, $1/\alpha$ and $1/\overline{\alpha}$.

Write $z = -1/2 + it$ as $z = -1/2(1 + i\tan\theta) = -e^{i\theta}/(2\cos\theta)$, where θ decreases from $2\pi/3$ (when $z = -1/2 + i\sqrt{3}/2$) to $\pi/2$ (when $z = -1/2 + i\infty$). Note that $2\cos\theta$ goes from -1 to 0 as θ decreases from $2\pi/3$ to $\pi/2$. Then

$$P_n(z) = 1 + 2\cos(n\theta)/(-2\cos\theta)^n = \frac{2\cos(n\theta) + (2|\cos\theta|)^n}{(2|\cos\theta|)^n}.$$

Clearly, this is real valued, and has the same sign as the numerator, which is positive for values $\theta \in (\pi/2, 2\pi/3)$ with $n\theta \equiv 0 \bmod 2\pi$, and negative for values $\theta \in (\pi/2, 2\pi/3)$ with $n\theta \equiv \pi \bmod 2\pi$. Upon splitting n into progressions mod 6, and counting the sign changes produced in this way, we find that all the zeros of $P_n(z)$ are accounted for. $\square$

Let $\mathcal{Z}(b,c)$ denote the set of common zeros of the polynomials in (4.0.1), excluding possible zeros at 0, -1 or cube roots of unity. In other words, $\mathcal{Z}(b,c)$ is the set of complex roots of $\gcd(Q_b(z),\ Q_c(z))$. We wish to show that this set is empty, and assume for the sake of contradiction that this is not the case. Naturally, if α is a common zero, then so are all its Galois conjugates, as well as $1/\alpha$ (and its Galois conjugates), and $(-1-\alpha)/\alpha$ together with its Galois conjugates. Let ζ denote an element of $\mathcal{Z}(b,c)$ of largest absolute value, and let r denote this absolute value.

Lemma 4.4. *Suppose that one of b or c is even. If $\mathcal{Z}(b,c)$ is nonempty, then it contains an element with absolute value $r > 14/9$.*

Proof. Suppose to the contrary that bc is even, and that all the elements in $\mathcal{Z}(b,c)$ have absolute value bounded above by $14/9$. Consider the polynomial

$$f(x) := \prod_{\alpha \in \mathcal{Z}(b,c)} (x-\alpha).$$

Note that $f(x) = \gcd(Q_b(x),\ Q_c(x))$ is a monic polynomial in $\mathbb{Q}[x]$, and that it divides both $1+x^b+(-1-x)^b$ and $1+x^c+(-1-x)^c$. Since b or c is even, at least one of the polynomials $1+x^b+(-1-x)^b$ or $1+x^c+(-1-x)^c$, that lie in $\mathbb{Z}[x]$, has leading coefficient 2. By unique factorization in $\mathbb{Z}[x]$, we conclude that $2f(x)$ must have integer coefficients. Therefore, $2f(\omega)$ is an element of $\mathbb{Z}[\omega]$, and by the definition of $\mathcal{Z}(b,c)$ we have $f(\omega) \neq 0$. It follows that

$$2\prod_{\alpha \in \mathcal{Z}(b,c)} |\omega - \alpha| = 2|f(\omega)| \geqslant 1.$$

Note that, as in Lemma 4.3, the zeros in $\mathcal{Z}(b,c)$ occur in groups of 6: if $\alpha = -\frac{1}{2} + it$ lies in $\mathcal{Z}(b,c)$, where $t > \sqrt{3}/2$, then so do $\overline{\alpha}$, $1/\alpha$, $1/\overline{\alpha}$, $-1-1/\alpha$, and $-1-1/\overline{\alpha}$. The contribution of such a group of 6 to the product above is

$$\begin{aligned} &\big|(\alpha-\omega)(\overline{\alpha}-\omega)(1/\alpha-\omega)(1/\overline{\alpha}-\omega)(\omega^2-1/\alpha)(\omega^2-1/\overline{\alpha})\big| \\ &\qquad\qquad = \frac{|\alpha^2+\alpha+1|^3}{|\alpha|^4} = \frac{(t^2-3/4)^3}{(1/4+t^2)^2}. \end{aligned}$$

If $|\alpha| = (1/4+t^2)^{1/2} \leqslant 14/9$, then the above is no greater than $0.4888 < 1/2$, which gives a contradiction. $\square$

Our next lemma treats the case when c is small.

LEMMA 4.5. *Suppose that one of b or c is even and that $\mathcal{Z}(b,c) \neq \emptyset$. Let r be largest absolute value of an elements in $\mathcal{Z}(b,c)$. Then c must be larger than $\pi r^b/2$.*

Proof. Let $\zeta \in \mathcal{Z}(b,c)$ have maximal absolute value r. Since $1/\zeta$ must also be in $\mathcal{Z}(b,c)$, we have

$$\Big(-1-\frac{1}{\zeta^b}\Big)^c = \Big[\Big(-1-\frac{1}{\zeta}\Big)^b\Big]^c = \Big[\Big(-1-\frac{1}{\zeta}\Big)^c\Big]^b = \Big(-1-\frac{1}{\zeta^c}\Big)^b.$$

Taking logarithms, we see that

$$\sum_{\ell=1}^{\infty}\frac{(-1)^{\ell-1}}{\ell}\Big(\frac{c}{\zeta^{b\ell}}-\frac{b}{\zeta^{c\ell}}\Big) \in \pi i\mathbb{Z}. \tag{4.5.1}$$

However, by the triangle inequality, the quantity in (4.5.1) is bounded in absolute value by

$$\sum_{\ell=1}^{\infty}\frac{1}{\ell}\Big(\frac{c}{r^{b\ell}}+\frac{b}{r^{c\ell}}\Big) \leqslant \sum_{\ell=1}^{\infty}\frac{c+b/r}{r^{b\ell}} \leqslant \frac{c(1+1/r)}{r^b-1} < \frac{2c}{r^b},$$

since $r > 14/9$ by Lemma 4.4. Thus, if $c \leqslant \pi r^b/2$, then the quantity to the left in (4.5.1) is less than π in absolute value, so it must be zero.

But the triangle inequality also shows that the quantity in (4.5.1) is bounded below in absolute value by

$$\begin{aligned}\frac{c}{r^b}-\frac{b}{r^c}-\sum_{\ell=2}^{\infty}\frac{1}{\ell}\Big(\frac{c}{r^{b\ell}}+\frac{b}{r^{c\ell}}\Big) &> \frac{c}{r^b}-\frac{c}{r^c}-\sum_{\ell=2}^{\infty}\frac{c}{r^{b\ell}}\\ &= \frac{c}{r^b}-\frac{c}{r^c}-\frac{c}{r^b(r^b-1)} > \frac{c}{r^b}\Big(1-\frac{1}{r}-\frac{1}{r^b-1}\Big).\end{aligned}$$

Since $r > 14/9$ and $b \geqslant 6$, the quantity above is strictly positive, and we have arrived at a contradiction. This proves the lemma. □

It remains to deal with the case when c is large, specifically, $c > \pi r^b/2$. To handle this, we require a result on diophantine approximation due to Laurent, Mignotte, and Nesterenko [9]; the formulation that we record below follows from [2, Theorem 2.6] with a little cleaning up. By the *primitive minimal polynomial* of an algebraic number α, we mean the primitive polynomial $a_0x^d + a_1x^{d-1} + \cdots + a_d \in \mathbb{Z}[x]$ of least degree with α as a root, and a_0 a positive integer. In this case, the *absolute height* of α is

$$h(\alpha) := \frac{1}{d}\Big(\log a_0 + \sum_{\sigma}\log\max\{1, |\sigma(\alpha)|\}\Big),$$

where the elements $\sigma(\alpha)$ are the Galois conjugates of α.

Lemma 4.6. *Let α be an algebraic number of absolute value 1 that is not a root of unity, and let d be its degree. Let $h(\alpha)$ denote the absolute height of α as above. Then, for any positive integer k, we have*

$$|\alpha^k - 1| \geqslant \exp\Big(-\frac{9}{8}\big(22\pi + dh(\alpha)\big)\big(\max\{34,\ d\log(k/2)+10\}\big)^2\Big).$$

Proof of Theorem 4.1. Let ζ be an element of the set $\mathcal{Z}(b,c)$ with maximal absolute value $r := |\zeta|$, and take $\alpha = -1 - 1/\zeta$, so that α is an element of $\mathcal{Z}(b,c)$ with $|\alpha| = 1$. Note that α cannot be a root of unity, else some conjugate of α will not lie on the arc from ω to ω^2. Since α is a root of $1+x^b+(-1-x)^b$, the degree d of α is at most b. Since one of b or c is even, α satisfies a polynomial in $\mathbb{Z}[x]$ with leading coefficient 2, so that the primitive minimal polynomial of α in $\mathbb{Z}[x]$ has leading coefficient 1 or 2. Since only one third of the elements of $\mathcal{Z}(b,c)$ have absolute value exceeding 1, and these absolute values are bounded above by r, we conclude that

$$dh(\alpha) \leqslant \log 2 + \frac{b}{3}\log r.$$

Appealing to Lemma 4.6, we conclude that for any positive integer k one has

$$\text{(4.6.1)}\qquad |\alpha^k - 1| \geqslant \exp\Big(-\frac{9}{8}\Big(70 + \frac{b}{3}\log r\Big)\big(\max\{34,\ b\log(k/2)+10\}\big)^2\Big).$$

Since α is a root of $1+x^c+(-1-x)^c$, and $|-1-\alpha| = 1/r$, we have $|1+\alpha^c| \leqslant 1/r^c$ so

$$\text{(4.6.2)}\qquad |\alpha^{2c} - 1| \leqslant \frac{2}{r^c}.$$

On the other hand, assuming that $c \geqslant e^5$ and using that $b \geqslant 6$, we may simplify the bound in (4.6.1) to yield

$$\begin{aligned} |\alpha^{2c} - 1| &\geqslant \exp\Big(-\frac{9}{8}\Big(70 + \frac{b}{3}\log r\Big)(b\log c + 10)^2\Big) \\ &\geqslant \exp\Big(-2b^2(\log c)^2\Big(70 + \frac{b}{3}\log r\Big)\Big). \end{aligned}$$

Comparing this with (4.6.2), we obtain a contradiction unless

$$c\log r \leqslant \log 2 + 2b^2(\log c)^2\Big(70 + \frac{b}{3}\log r\Big).$$

Since $r > 14/9$ by Lemma 4.4, the above bound, under the assumption $c \geqslant e^5$, implies that

$$\text{(4.6.3)}\qquad \frac{c}{(\log c)^2} \leqslant \frac{\log 2}{\log(14/9)(\log c)^2} + 2b^2\Big(\frac{70}{\log(14/9)} + \frac{b}{3}\Big) \leqslant 320b^2 + 2b^3/3.$$

If $b \geqslant 43$, then by Lemmas 4.4 and 4.5, we see that $\mathcal{Z}(b,c) = \emptyset$ unless $c \geqslant (\pi/2)(14/9)^b$. But a small calculation shows that this lower bound for c, which is much bigger than e^5, contradicts the upper bound imposed in (4.6.3). Thus, we conclude that $\mathcal{Z}(b,c) = \emptyset$ whenever $c > b \geqslant 43$.

For $6 \leqslant b \leqslant 42$, it is easy to check that after accounting for the zeros at $0, -1, \omega, \omega^2$, the remaining part of the polynomial $1 + x^b + (-1-x)^b$, denoted earlier by $Q_b(x)$, is irreducible. This allows us to obtain improved estimates for the size of r in Lemma 4.4, thereby obtaining a larger lower bound for c in Lemma 4.5. For all $17 \leqslant b \leqslant 42$, the polynomial $1 + x^b + (-1-x)^b$ has a root of size at least 2.72, so that in these cases, we may use $r \geqslant 2.72$, and $c \geqslant (\pi/2)(2.72)^b$; this bound can be checked to contradict (4.6.3). Thus $\mathcal{Z}(b,c) = \emptyset$ for $c > b \geqslant 17$. When b equals 12, 14, or 16, there is a root of size $r \geqslant 3.83$, and our argument applies in these cases as well.

The case $b = 6$ is covered by [4, Theorem 2.11], while the case $b = 7$ does not arise, since $1 + x^7 + (-1-x)^7$ only has roots at $0, -1, \omega, \omega^2$. When $b = 9$, the nontrivial factor of $1 + x^9 + (-1-x)^9$ is a primitive irreducible polynomial of degree 6, with leading coefficient 3, and therefore cannot divide $1 + x^c + (-1-x)^c$ for c even, since this polynomial has leading coefficient 2. Similarly, when $b = 15$, the nontrivial factor of $1+x^{15}+(-1-x)^{15}$ is a primitive irreducible polynomial of degree 12, with leading coefficient 15, and once again this cannot divide $1 + x^c + (-1-x)^c$ for c even.

We are left with four remaining cases, $b = 8$, 10, 11, and 13, where an additional small computation is needed to check the theorem. We illustrate this calculation in the case $b = 8$, the other cases being similar. The nontrivial factor of $1+x^8+(-1-x)^8$ has degree 6, with a root of largest absolute value at

$$\zeta \approx -\frac{1}{2} + 2.513228157188i.$$

It follows from Lemma 4.5 that $\mathcal{Z}(8,c) = \emptyset$ for $8 < c \leqslant 2500$, while from (4.6.3) it follows that $\mathcal{Z}(8,c) = \emptyset$ for $c > 5 \times 10^6$. To handle the remaining range for c, write $(1 + 1/\zeta^8)$ as $e^{i\theta}$ with $\theta = -0.0005379141\ldots$, so that by (4.5.1) we have, for some integer m,

$$|c\theta + m\pi| \leqslant 8 \sum_{\ell=1}^{\infty} \frac{1}{\ell|\zeta|^{c\ell}} \leqslant 9 \times (2.5)^{-c} < (2.5)^{-2400}.$$

Thus, $m\pi/|\theta|$ must be extremely close to the integer c. Now

$$\pi/|\theta| = 5840.32375784959\ldots,$$

and since $2500 < c \leqslant 5 \times 10^6$, we may restrict attention to integers m that lie in the range $1 \leqslant m \leqslant 1000$. A rapid calculation (for instance, by examining the continued fraction expansion of $\pi/|\theta|$) shows that there are no m in this range with $m\pi/|\theta|$ being extremely close to an integer, which completes our treatment of the case $b = 8$. □

5. POWER SUMS IN THREE VARIABLES: THE GENERAL CASE

Adapting the argument from the previous section, we establish the following more general result.

THEOREM 5.1. *Let $2 \leqslant a < b < c$ be integers such that $2 \mid abc$, and $\gcd(a, b, c) = 1$. Suppose that the system of equations*

$$1 + x^a + y^a = 1 + x^b + y^b = 1 + x^c + y^c = 0$$

has a solution where x and y are not cube roots of unity. Then:

(1) *We have $b < 600a^2 2^a$.*

(2) *If exactly one of a, b, c is even, then $b < 600a^2$.*

(3) *For each b in the range $a < b < 600a^2 2^a$, there are at most finitely many possible choices for c.*

Let $\mathcal{Z}(a, b, c)$ denote the set of all $\alpha \in \mathbb{C}$, excluding cube roots of unity, for which there exists some $\beta \in \mathbb{C}$ with

$$1 + \alpha^a + \beta^a = 1 + \alpha^b + \beta^b = 1 + \alpha^c + \beta^c = 0.$$

LEMMA 5.2. *Suppose that $\gcd(a, b, c) = 1$ and that at least one of a, b, or c is even. If $\alpha \in \mathcal{Z}(a, b, c)$, then the primitive minimal polynomial of α in $\mathbb{Z}[x]$ has degree at most ab, and leading coefficient 1 or 2. If exactly one of a, b, or c is even, then the leading coefficient must be 1, i.e., α is an algebraic integer.*

Proof. Note that

$$(1 + \alpha^a)^b = (-\beta^a)^b = (-1)^b(\beta^b)^a = (-1)^{b+a}(1 + \alpha^b)^a,$$

and similarly $(1 + \alpha^a)^c = (-1)^{a+c}(1 + \alpha^c)^a$, and $(1 + \alpha^b)^c = (-1)^{b+c}(1 + \alpha^c)^b$. Thus, α is a root of the three polynomials

$$\text{(5.2.1)} \qquad \begin{gathered}(1 + x^a)^b - (-1)^{a+b}(1 + x^b)^a, \quad (1 + x^a)^c - (-1)^{a+c}(1 + x^c)^a, \\ \text{and } (1 + x^b)^c - (-1)^{b+c}(1 + x^c)^b.\end{gathered}$$

It follows that α is an algebraic number of degree at most ab. Furthermore, since two of the integers a, b, c must have opposite parity, one of the displayed polynomials must have leading coefficient 2, so the primitive minimal polynomial for α must have leading coefficient 1 or 2. Finally, if exactly one of a,

b, c is even, then two of the three polynomials have leading coefficient 2, and the third has an odd leading coefficient. Therefore, in this case, the primitive minimal polynomial of α, which divides all three of the polynomials (5.2.1), has leading coefficient 1. $\square$

LEMMA 5.3. *Suppose w is a complex number with $e^{-\delta} \leqslant |w| \leqslant e^{\delta}$ and $e^{-\delta} \leqslant |1+w| \leqslant e^{\delta}$, where $0 \leqslant \delta \leqslant 1/10$. Then*

$$|w^2 + w + 1| \leqslant 10\delta.$$

Proof. By assumption,

$$|1+w|^2 = 1 + w + \overline{w} + |w|^2$$

lies in the interval $[e^{-2\delta}, e^{2\delta}]$, so that

$$|1 + w + \overline{w}| \leqslant \max\{e^{2\delta} - |w|^2,\ |w|^2 - e^{-2\delta}\} \leqslant e^{2\delta} - e^{-2\delta}.$$

Therefore,

$$\begin{aligned} |w^2 + w + 1| &= |w|\left|w + \frac{1}{w} + 1\right| \leqslant |w|\left(|w + \overline{w} + 1| + \left|\frac{1}{w} - \overline{w}\right|\right) \\ &\leqslant |w|(e^{2\delta} - e^{-2\delta}) + \left|1 - |w|^2\right| \leqslant e^{\delta}(e^{2\delta} - e^{-2\delta}) + (e^{2\delta} - 1), \end{aligned}$$

and the lemma follows. $\square$

LEMMA 5.4. *Suppose* $\gcd(a,b,c) = 1$ *and* $2 \mid abc$. *Suppose $\mathcal{Z}(a,b,c) \neq \emptyset$, let r denote the largest absolute value of an element of $\mathcal{Z}(a,b,c)$. Then*

$$r \geqslant \exp\Big(\frac{1}{10a2^a}\Big).$$

If exactly one of a, b, c is even, then this may be improved to

$$r \geqslant \exp\Big(\frac{1}{10a}\Big).$$

Proof. Note that if α belongs to $\mathcal{Z}(a,b,c)$, then so does $1/\alpha$. Thus, all elements of $\mathcal{Z}(a,b,c)$ have absolute value between $1/r$ and r.

For $\alpha \in \mathcal{Z}(a,b,c)$, let β be such that $1 + \alpha^a + \beta^a = 1 + \alpha^b + \beta^b = 1 + \alpha^c + \beta^c = 0$. We know that α^a and β^a both have absolute value in the interval $[r^{-a},\ r^a]$. But $\beta^a = -(1+\alpha^a)$, so by Lemma 5.3 we conclude that

$$|\alpha^{2a} + \alpha^a + 1| \leqslant 10\log(r^a). \tag{5.4.1}$$

Next, we claim that $\alpha^{2a} + \alpha^a + 1$ cannot equal zero. If it did, then α^a would be a primitive cube root of unity, i.e., ω or ω^2, and therefore, so would β^a. Now, α^b and $\beta^b = -(1+\alpha^b)$ both have absolute value 1, so that by Lemma 5.3 α^b must be ω or ω^2. The same conclusion holds for α^c. But since

$\gcd(a, b, c) = 1$, we conclude that α itself must be a cube root of unity, which is not permitted given the definition of $\mathcal{Z}(a, b, c)$.

Summarizing the argument thus far, if $\alpha \in \mathcal{Z}(a, b, c)$ then α and all its Galois conjugates satisfy the bound from equation (5.4.1), and furthermore, $\alpha^{2a} + \alpha^a + 1 \neq 0$. Let $f(x)$ denote the primitive minimal polynomial for α in $\mathbb{Z}[x]$, and set $g(x) := x^{2a} + x^a + 1$. By Lemma 5.2, the degree d of $f(x)$ is at most ab, and its leading coefficient is 1 or 2. The resultant of $f(x)$ and $g(x)$ is a nonzero integer, and therefore

$$1 \leqslant |\operatorname{Res}(f, g)| \leqslant 2^{2a} \prod_{\sigma} \left|\sigma(\alpha)^{2a} + \sigma(\alpha)^a + 1\right| \leqslant 2^{2a}(10a \log r)^d,$$

where $\sigma(\alpha)$ are the Galois conjugates of α, and we have used (5.4.1) for the upper bound. Since d must be at least 2, the first bound of the lemma follows. If exactly one of a, b, c is even, then $f(x)$ is monic, and the improved bound holds. □

Lemma 5.5. *Suppose* $\gcd(a, b, c) = 1$ *and* $2 \mid abc$. *Suppose* $\mathcal{Z}(a, b, c) \neq \emptyset$, *let* r *be the largest absolute value of an element of* $\mathcal{Z}(a, b, c)$. *Then* c *must be larger than* $\pi r^b/2$.

Proof. The argument is identical to the proof of Lemma 4.5. □

Lemma 5.6. *Suppose* $\gcd(a, b, c) = 1$ *and* $2 \mid abc$. *Let* α *denote an element of* $\mathcal{Z}(a, b, c)$ *with smallest absolute value, which is* $1/r$. *Let* β *be such that*

$$1 + \alpha^a + \beta^a = 1 + \alpha^b + \beta^b = 1 + \alpha^c + \beta^c = 0.$$

Then $\zeta := \beta/\overline{\beta}$ *is an algebraic number of degree at most* $(ab)^2$, *with absolute height*

$$h(\zeta) \leqslant 2 \log(2r).$$

If $2b^8 \leqslant r^b$, *then* ζ *is not a root of unity. If* ζ *is a root of unity, then either* $r^c < 2b^8$, *or* α^c *and* β^c *are both real numbers.*

Proof. Since β is an algebraic number with degree at most ab (from Lemma 5.2), it follows that $\zeta = \beta/\overline{\beta}$ has degree at most $(ab)^2$. As β has a primitive minimal polynomial with leading coefficient at most 2, and since all its Galois conjugates have absolute value at most r, we see that $h(\beta) \leqslant \log(2r)$. Now

$$h(\zeta) \;=\; h(\beta/\overline{\beta}) \leqslant h(\beta) + h(\overline{\beta}) \leqslant 2 \log(2r).$$

It remains to justify the assertions about when ζ can be a root of unity. Suppose that it is, write $\beta = |\beta| e^{\pi i \ell/k}$ where ℓ/k is a reduced fraction. Then $\zeta = e^{2\pi i \ell/k}$ is a primitive k-th root of unity.

Suppose that b is not a multiple of k. Then

$$r^{-2b} = |1+\beta^b|^2 = 1 + |\beta|^{2b} + 2|\beta|^b\cos(\pi\ell b/k) \geqslant \big(1+|\beta|^{2b}\big)\big(1-|\cos(\pi\ell b/k)|\big) \geqslant \big(1-\cos(\pi/k)\big) > k^{-2},$$

so that $k > r^b$. However, the degree of ζ is $\varphi(k)$, which is at most $(ab)^2$. Now $\varphi(k) \geqslant \sqrt{k/2}$ for all integers k, so

$$r^b < k \leqslant 2\varphi(k)^2 \leqslant 2(ab)^4 < 2b^8.$$

In other words, if $r^b \geqslant 2b^8$ then b must be a multiple of k. The same argument shows that if $r^c \geqslant 2b^8$ then c is a multiple of k.

If b is a multiple of k, then β^b is real, which forces α^b to also be real. Similarly, if c is a multiple of k, then β^c and α^c are once again real numbers. The last assertion of the lemma is immediate.

Finally, if $r^b \geqslant 2b^8$, then our argument so far shows that b and c are multiples of k. Now, we must have $|\beta|^b = 1+\alpha^b$, and $|\beta|^c = 1+\alpha^c$, so that α^b and α^c must be real numbers (of absolute value r^{-b} and r^{-c}, respectively). If $|\beta| \geqslant 1$, then $\alpha^b = r^{-b}$ and $\alpha^c = r^{-c}$. However,

$$|\beta|^c \geqslant |\beta|^b = 1 + r^{-b} > 1 + r^{-c} = |\beta|^c$$

yields a contradiction. Similarly, if $|\beta| < 1$, then $\alpha^b = -r^{-b}$ and $\alpha^c = -r^{-c}$, and

$$|\beta|^b > |\beta|^c = 1 - r^{-c} > 1 - r^{-b} = |\beta|^b$$

gives a contradiction. Thus, in this situation ζ cannot be a root of unity, and this completes the proof of the lemma. □

Proof of Theorem 5.1. We begin by proving the first two parts of the theorem. We assume that $\mathcal{Z}(a,b,c) \neq \emptyset$, and note that Lemma 5.4 gives a lower bound for the largest absolute value r of an element of $\mathcal{Z}(a,b,c)$. We assume that b is at least $600a^2 2^a$ or $600a^2$, depending on whether we seek to establish (1) or (2), and work towards a contradiction. Using the lower bounds for r from Lemma 5.4 in the respective cases, we see that $r^b \geqslant 2b^8$. Hence, taking α, β, ζ as in Lemma 5.6, we see that ζ is not a root of unity. Since $\beta^c = -(1+\alpha^c)$, we have

$$\zeta^c = \frac{\beta^c}{\overline{\beta}^c} = \frac{1+\alpha^c}{1+\overline{\alpha}^c},$$

and so

$$|\zeta^c - 1| \leqslant \frac{2r^{-c}}{1-r^{-c}} \leqslant 3r^{-c} \tag{5.6.1}$$

since $r^c > r^b > 3$. On the other hand, from Lemma 4.6 and Lemma 5.6, we know that

$$|\zeta^c - 1| \geqslant \exp\Big(-\frac{9}{8}\big(70 + (ab)^2 2\log(2r)\big)(ab)^4(\log c)^2\Big).$$

Since $ab \geqslant 100$, we may simplify the above to

$$|\zeta^c - 1| \geqslant \exp\bigl(-(ab)^6(2+3\log r)(\log c)^2\bigr).$$

Combining this with (5.6.1), we conclude that

$$\frac{c}{(\log c)^2} \leqslant 3(ab)^6\Bigl(1+\frac{1}{\log r}\Bigr). \tag{5.6.2}$$

On the other hand, $c \geqslant \pi r^b/2$ by Lemma 5.5. Since $r^b \geqslant 10$, we have $c/(\log c)^2 \geqslant r^b/(b\log r)^2$, which along with (5.6.2) gives

$$r^b \leqslant 3a^6b^8 \log r(1+\log r).$$

Since $b \geqslant 600a^2$, we find

$$r^{b/2} \geqslant \frac{(b\log r)^{11}}{2^{11}\cdot 11!} \geqslant \frac{b^8(\log r)^{11}}{2^{11}\cdot 11!}(600a^2)^3 > a^6b^8\frac{(\log r)^{11}}{380},$$

and combining this with our upper bound on r^b, we conclude that

$$r^{b/2} < 1140(\log r)^{-10}(1+\log r).$$

In other words,

$$b < \frac{2}{\log r}\log\bigl(1140(\log r)^{-10}(1+\log r)\bigr).$$

Inserting here the bounds from Lemma 5.4 which give $\log r \geqslant (10a2^a)^{-1}$ in case (1) and $\log r \geqslant (10a)^{-1}$ in case (2), we obtain the desired contradiction.

It remains lastly to establish (3). Fix a and b with $2 \leqslant a < b < 600a^2 2^a$. We wish to show that if c is sufficiently large, with $2 \mid abc$ and $\gcd(a,b,c) = 1$, then $\mathcal{Z}(a,b,c) = \emptyset$. First, note that any $\alpha \in \mathcal{Z}(a,b,c)$ is a root of the polynomial

$$(1+x^a)^b - (-1)^{a+b}(1+x^b)^a$$

by (5.2.1), and thus lies in a set of size at most ab. Let α, β, ζ, and r be as in Lemma 5.6, and assume that $c \geqslant 600a^2 2^a$ so that $r^c \geqslant 2c^8 \geqslant 2b^8$. If ζ is not a root of unity, then our earlier argument invoking Lemma 4.6 applies, and yields the upper bound (5.6.2), which shows that there are at most finitely many possibilities for c. Finally, if ζ is a root of unity, then the last assertion of Lemma 5.6 yields that α^c and β^c are real with $1+\alpha^c+\beta^c = 0$. Since $|\alpha| = r^{-1} < 1$, this equation may be written as $|\beta|^c = 1+r^{-c}$ if $|\beta| > 1$, and as $|\beta|^c = 1-r^{-c}$ if $|\beta| < 1$. Given α and β, there can be at most one solution c to these equations. Finally, since α and β are elements of the finite set of roots of the polynomial $(1+x^a)^b - (-1)^{a+b}(1+x^b)^a$, there are only finitely many possibilities for c. $\square$

Acknowledgments. The use of the computer algebra systems `Macaulay2` [7] and `Magma` [3] is gratefully acknowledged.

REFERENCES

[1] F. Beukers, *On a sequence of polynomials*. J. Pure Appl. Algebra **117/118** (1997), 97–103.

[2] Y. Bugeaud, *Linear Forms in Logarithms and Applications*. IRMA Lect. Math. Theor. Phys. 28. European Mathematical Society (EMS), Zürich, 2018.

[3] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*. J. Symbolic Comput. **24** (1997), *3-4*, 235–265.

[4] A. Conca, C. Krattenthaler, and J. Watanabe, *Regular sequences of symmetric polynomials*, Rend. Semin. Mat. Univ. Padova **121** (2009), 179–199.

[5] R. Dvornicich and U. Zannier, *Newton functions generating symmetric fields and irreducibility of Schur polynomials*. Adv. Math. **222** (2009), *6*, 1982–2003.

[6] R. Fröberg and B. Shapiro, *On Vandermonde varieties*. Math. Scand. **119** (2016), *1*, 73–91.

[7] D.R. Grayson and M.E. Stillman, *Macaulay2, a software system for research in algebraic geometry*. Available at https://macaulay2.com/.

[8] A. Grothendieck, *Cohomologie locale des faisceaux cohérents et théorèmes de Lefschetz locaux et globaux* (*SGA* 2). Advanced Studies in Pure Mathematics, Vol. 2. North-Holland Publishing Co., Amsterdam; Masson & Cie, Editeur, Paris, 1968.

[9] M. Laurent, M. Mignotte, and Y. Nesterenko, *Formes linéaires en deux logarithmes et déterminants d'interpolation*. J. Number Theory **55** (1995), *2*, 285–321.

[10] H. Melánová, B. Sturmfels, and R. Winter, *Recovery from power sums*. Exp. Math. **33** (2024), *2*, 225–234.

[11] P.M. Nanninga, *Cauchy-Mirimanoff and related polynomials*. J. Aust. Math. Soc. **92** (2012), *2*, 269–280.

Received 10 July 2024

Aldo Conca
Dipartimento di Matematica,
Dipartimento di Eccellenza 2023-2027,
Universitá di Genova,
Via Dodecaneso 35,
I-16146 Genova, Italy
aldo.conca@unige.it

Anurag K. Singh
Department of Mathematics,
University of Utah,
155 South 1400 East,
Salt Lake City, UT 84112, USA
singh@math.utah.edu

Kannan Soundararajan
Department of Mathematics,
Stanford University,
450 Serra Mall,
Stanford CA 94305, USA
ksound@stanford.edu