arXiv:1007.2239v1 [math.NT] 14 Jul 2010

INFINITE EASIER WARING CONSTANTS FOR COMMUTATIVE RINGS

TED CHINBURG

ABSTRACT. Suppose $n \geq 2$. We show that there is no integer $v \geq 1$ such that for all commutative rings R with identity, every element of the subring $J(2^n, R)$ of R generated by 2^n-th powers can be written in the form $\pm f_1^{2^n} \pm \cdots \pm f_v^{2^n}$ for some $f_1, \ldots, f_v \in R$ and some choice of signs.

1. INTRODUCTION

The object of this paper is to prove a result about easier Waring constants for commutative rings which was announced over thirty years ago in [3]. This result grew out of research of the author with Mel Henriksen in [4]. It is a pleasure to remember Mel's generosity and the excitement of working with him. This paper is dedicated to Mel.

Let R be a commutative ring with identity, and suppose k is a positive integer. Define $J(k, R)$ to be the subring of R generated by all k^{th} powers. If there is an integer v such that every element f of $J(k, R)$ is of the form

$$f = \sum_{i=1}^{v} \pm f_i^k$$

for some $f_1, \ldots, f_v \in R$ and some choice of signs, let $v(k, R)$ denote the smallest such v. If no such v exists, put $v(k, R) = \infty$. Let $V(k)$ be the sup, over all R, of $v(k, R)$. Our main result is:

Theorem 1.1. *For $n \geq 2$ one has*

$$V(2^n) = v(2^n, R_\infty) = \infty$$

when $R_\infty = \mathbb{Z}[\{x_i\}_{i=1}^\infty]$ is the ring of polynomials with integer coefficients in countably many indeterminates.

To our knowledge, this provides the first example of an integer k for which $V(k)$ is infinite.

Date: July 15, 2010.

The author was supported in part by NSF Grant DMS-0801030.

Concerning k for which $V(k)$ is finite, Joly proved in [7, Thm. 7.9] that $V(2) = 3$. In [3, Thm. 1] it was shown that if k is a prime which is not of the form $(p^{bc}-1)/(p^c-1)$ for some prime p and integers $b \geq 2$ and $c \geq 1$, then $V(k)$ is finite. This implies that $V(k)$ is finite for almost all primes k. As of this writing, we do not know of further integers k for which $V(k)$ has been shown to be finite. The smallest integer $k > 2$ for which the results of [3] show $V(k)$ to be finite is $k = 11$.

Striking quantitative results concerning upper bounds on $V(k)$ for various k, and on $v(k, R)$ for various R, have been proved by a number of authors including Car, Cherly, Gallardo, Heath-Brown, Newman, Slater, Vaserstein and others. See [1, 2, 6, 5, 8, 11, 12, 10, 9] and their references.

For $m \geq 1$ let $R_m = \mathbb{Z}[x_1, \ldots, x_m]$ be the ring of polynomials with integer coefficients in m commuting indeterminates. By [3, Theorems 3 and 4], $v(k, R_m)$ is finite for all k and m. By [7, Prop. 7.12],

$$V(k) = \sup_{m \geq 1} v(k, R_m) = v(k, R_\infty).$$

We show Theorem 1.1 by proving $\lim_{m\to\infty} v(k, R_m) = \infty$ when $k = 2^n > 2$. We now summarize the strategy to be used in §2 for bounding $v(k, R_m)$ from below in order to clarify how this approach might be applied for other values of k.

The strategy is to construct a surjection

$$\pi : J(k, R_m) \to A$$

to an abelian group A with the following property. For $v \geq 1$, let $J(k, R_m)_v$ be the subset of elements of $J(k, R_m)$ of the form $\sum_{i=1}^{v} \pm f_i^k$ for some $f_i \in R_m$ and some choice of signs. One would like to produce a π such that $\pi(J(k, R_m)_v)$ has order less than A unless v is at least some bound which goes to infinity with m.

For $k = 2^n > 2$, the π we construct in §2 results from combining congruence classes of the coefficients of high degree monomials which appear in the expansions of elements of $J(2^n, R_m)$. The group A is a vector space over $\mathbb{Z}/2$ of dimension $m(m-1)/2$. The π we consider has the property that for $f_i \in R_m$, the value of $\pi(f_i^{2^n})$ is 0 if f_i has odd constant term, and otherwise $\pi(f_i^{2^n})$ depends only on the coefficients mod 2 of the homogeneous degree 1 part of f_i. This means that the value of $\pi(\sum_{i=1}^{v} \pm f_i^{2^n})$ depends only on at most vm elements of $\mathbb{Z}/2$, so that

$$\#\pi(J(2^n, R_m)_v) \leq 2^{vm}.$$

If $v = v(2^n, R_m)$, so that $J(2^n, R_m)_v = J(2^n, R_m)$, we must therefore have

$$vm = v(2^n, R_m) \cdot m \geq \dim_{\mathbb{Z}/2}(A) = m(m-1)/2 \qquad (1.1)$$

since π is surjective. This produces the lower bound

$$v(2^n, R_m) \geq (m-1)/2 \tag{1.2}$$

and implies Theorem 1.1.

One can surely improve (1.2), but we will not attempt to optimize the above method in this paper. A systematic approach would be to consider which combinations of congruence classes of higher degree monomial coefficients of elements f^k of $J(k, R_m)$ can be shown to depend only on the congruence classes of lower degree monomial coefficients of $f \in R_m$. These combinations should be chosen to be independent of one another, in the sense that they together produce a surjection from $J(k, R_m)$ to a large abelian group A.

2. Proof of Theorem 1.1

Let $m \geq 1$ be fixed. We will write polynomials in $R_m = \mathbb{Z}[x_1, \ldots, x_m]$ in the form

$$f = \sum_\alpha c_f(x^\alpha) x^\alpha \tag{2.3}$$

where

$$x^\alpha = \prod_{i=1}^m x_i^{\alpha_i}$$

is the monomial associated to a vector $\alpha = (\alpha_1, \ldots, \alpha_m)$ of non-negative integers and the integers $c_f(x^\alpha)$ are 0 for almost all α.

Lemma 2.1. *Suppose $n \geq 2$ and $1 \leq i < j \leq m$. Then $c_{f^{2^n}}(x_i x_j)/2^n$ and $c_{f^{2^n}}(x_i^{2^{n-1}} x_j^{2^{n-1}})/2$ are integers. One has*

$$\frac{c_{f^{2^n}}(x_i x_j)}{2^n} + \frac{c_{f^{2^n}}(x_i^{2^{n-1}} x_j^{2^{n-1}})}{2} \equiv (c_f(1)+1) c_f(x_i) c_f(x_j) \mod 2\mathbb{Z} \tag{2.4}$$

Proof. We first compute the coefficient $c_{f^{2^n}}(x_i x_j)$ of $x_i x_j$ in f^{2^n}. Write

$$f = c_f(1) + t$$

where t has constant term 0. Then

$$f^{2^n} = c_f(1)^{2^n} + 2^n c_f(1)^{2^n - 1} t + \frac{2^n(2^n-1)}{2} c_f(1)^{2^n-2} t^2 + z \tag{2.5}$$

where all the terms of $z \in R_m$ have degree larger than 2. Here

$$t \equiv \sum_{\ell=1}^m c_f(x_\ell) x_\ell \mod \text{terms of degree } \geq 2.$$

Because $i < j$, the coefficient of $x_i x_j$ in t^2 is $2c_f(x_i)c_f(x_j)$. Putting this into (2.5), and noting that the coefficient of $x_i x_j$ in t is $c_f(x_i x_j)$ by definition, we conclude that

$$c_{f^{2^n}}(x_i x_j) = 2^n c_f(1)^{2^n-1} c_f(x_i x_j) + 2^n(2^n-1) c_f(1)^{2^n-2} c_f(x_i) c_f(x_j). \tag{2.6}$$

Thus 2^n divides $c_{f^{2^n}}(x_i x_j)$. Because $n > 1$ and $a^s \equiv a \bmod 2$ for all $a \in \mathbb{Z}$ and $s \geq 1$, we find

$$\frac{c_{f^{2^n}}(x_i x_j)}{2^n} \equiv c_f(1)(c_f(x_i x_j) + c_f(x_i)c_f(x_j)) \mod 2\mathbb{Z}. \tag{2.7}$$

We now consider the coefficient $c_{f^{2^n}}(x_i^{2^{n-1}} x_j^{2^{n-1}})$ of $x_i^{2^{n-1}} x_j^{2^{n-1}}$ in f^{2^n}. Write

$$f^{2^{n-1}} = \left(\sum_\alpha c_f(\alpha)^{2^{n-1}} (x^\alpha)^{2^{n-1}} \right) + 2g \tag{2.8}$$

for some polynomial $g \in R_m$. Then

$$f^{2^n} = (f^{2^{n-1}})^2 \equiv \left(\sum_\alpha c_f(\alpha)^{2^{n-1}} (x^\alpha)^{2^{n-1}} \right)^2 \mod 4R_m. \tag{2.9}$$

When one expands the square on the right side of (2.9), the coefficient of $x_i^{2^{n-1}} x_j^{2^{n-1}}$ is

$$2c_f(1)^{2^{n-1}} c_f(x_i x_j)^{2^{n-1}} + 2c_f(x_i)^{2^{n-1}} c_f(x_j)^{2^{n-1}}.$$

Because of the congruence (2.9) and the fact that $n > 1$, we conclude that $c_{f^{2^n}}(x_i^{2^{n-1}} x_j^{2^{n-1}})$ is divisible by 2, and

$$\begin{aligned} \frac{c_{f^{2^n}}(x_i^{2^{n-1}} x_j^{2^{n-1}})}{2} &\equiv c_f(1)^{2^{n-1}} c_f(x_i x_j)^{2^{n-1}} + c_f(x_i)^{2^{n-1}} c_f(x_j)^{2^{n-1}} \mod 2\mathbb{Z} \\ &\equiv c_f(1) c_f(x_i x_j) + c_f(x_i) c_f(x_j) \mod 2\mathbb{Z} \qquad (2.10) \end{aligned}$$

Adding (2.7) and (2.10) gives (2.4) and completes the proof. □

Proof of Theorem 1.1

Fix $n > 1$ and $m \geq 2$ and suppose $1 \leq i < j \leq m$. By Lemma 2.1, there is a unique homomorphism

$$\pi_{i,j} : J(2^n, R_m) \to \mathbb{Z}/2 \tag{2.11}$$

which for $f \in R_m$ has the property that

$$\pi_{i,j}(f^{2^n}) = \left(\frac{c_{f^{2^n}}(x_i x_j)}{2^n} + \frac{c_{f^{2^n}}(x_i^{2^{n-1}} x_j^{2^{n-1}})}{2} \right) \mod 2$$

with the notation of Lemma 2.1. The product of these homomorphisms over all pairs (i, j) of integers such that $1 \le i < j \le m$ gives a homomorphism

$$\pi : J(2^n, R_m) \to (\mathbb{Z}/2)^{\binom{m}{2}} = A \tag{2.12}$$

Suppose we fix a pair (i', j') of integers such that $1 \le i' < j' \le m$ and we let $f = x_{i'} + x_{j'}$. Formula (2.4) shows that $\pi_{i,j}(f^{2^n}) = 0$ if $(i, j) \neq (i', j')$ while $\pi_{i',j'}(f^{2^n}) = 1$. It follows that π in (2.12) is surjective. On the other hand, formula (2.4) shows that $\pi_{i,j}(f^{2^n}) = 0$ if f has odd constant term $c_f(1)$, and that otherwise $\pi_{i,j}(f^{2^n})$ depends only on the congruence classes mod 2 of the linear terms in f. Therefore the same is true of $\pi(f^{2^n})$. As explained in the second to last paragraph of the introduction, this leads to the lower bounds (1.1) and (1.2), which completes the proof.

References

[1] M. Car, New bounds on some parameters in the Waring problem for polynomials over a finite field. Finite fields and applications, 59–77, Contemp. Math., 461, Amer. Math. Soc., Providence, RI, 2008.

[2] J. Cherly, Sommes d'exponentielles cubiques dans l'anneau des polynômes en une variable sur le corps à 2 éléments, et application au problème de Waring. Astérisque No. 198-200 (1991), 83–96 (1992).

[3] T. Chinburg, "Easier" Waring problems for commutative rings. Acta Arith. 35 (1979), no. 4, 303–331.

[4] T. Chinburg and M. Henriksen, Sums of k-th powers in the ring of polynomials with integer coefficients. Acta Arith. 29 (1976), no. 3, 227–250.

[5] L. Gallardo and D. R. Heath-Brown. Every sum of cubes in $\mathbb{F}_2[t]$ is a strict sum of 6 cubes. Finite Fields Appl. 13 (2007), no. 4, 981–987.

[6] L. Gallardo and L. Vaserstein, The strict Waring problem for polynomial rings. J. Number Theory 128 (2008), no. 12, 29632972.

[7] J. R. Joly, Sommes de pusissances d-ièmes dans un anneau commutatif, Acta Arith. 17 (1970), 37-114.

[8] D. J. Newman and M. Slater, Waring's problem for the ring of polynomials. J. Number Theory 11 (1979), no. 4, 477–487.

[9] L. Vaserstein, Ramsey's theorem and Waring's problem for algebras over fields. The arithmetic of function fields (Columbus, OH, 1991), 435–441, Ohio State Univ. Math. Res. Inst. Publ., 2, de Gruyter, Berlin, 1992.

[10] L. Vaserstein, Sums of cubes in polynomial rings. Math. Comp. 56 (1991), no. 193, 349–357.

[11] L. Vaserstein, Waring's problem for algebras over fields. J. Number Theory 26 (1987), no. 3, 286–298.

[12] L. Vaserstein, Waring's problem for commutative rings. J. Number Theory 26 (1987), no. 3, 299–307.

T.C.: Department of Mathematics, University of Pennsylvania, Philadelphia, PA 19104-6395
E-mail address: ted@math.upenn.edu