[4] D. Hajela, *Some remarks on $B_h[g]$ sequences*, J. Number Theory 29 (1988), 311–323.
[5] H. Halberstam and K. F. Roth, *Sequences*, Oxford Univ. Press, 1966.
[6] F. Krückeberg, *B_2-Folgen und verwandte Zahlenfolgen*, J. Reine Angew. Math. 206 (1961), 53–60.

DEPARTMENT OF INFORMATICS
UNIVERSITY OF BERGEN
Thormøhlensgt. 55
N-5008 Bergen, Norway

Received on 25.7.1989 (1958)

ACTA ARITHMETICA
LVIII.1 (1991)

Polynomials whose powers are sparse

by

DON COPPERSMITH (Yorktown Heights, NY) and JAMES DAVENPORT (Bath)

Erdös [Erd] defines $Q(N)$ as the least possible number of nonzero coefficients ("the number of terms") in the square of a polynomial $f(x)$ with exactly N nonzero real coefficients. Erdös proves the existence of positive constants C_1, C_2 such that

$$Q(N) < C_1 N^{1-C_2}.$$

Verdenius [Ver] extends this result in two directions. He works with *complete* polynomials f, that is,

$$f(x) = \sum_{i=0}^{N-1} d_i x^i, \quad d_i \neq 0, \quad 0 \leqslant i \leqslant N-1.$$

He also establishes a similar inequality for cubes. Letting $Q_k(N)$ denote the least possible number of terms in the kth power of a complete real polynomial of degree $N-1$, Verdenius gives positive constants $C_{1,2}$, $C_{1,3}$ such that for any integer $N \geqslant 1$,

$$Q_2(N) < C_{1,2} N^{0.81071\ldots}, \quad Q_3(N) < C_{1,3} N^{0.99934\ldots}.$$

In the present note we extend this result to kth powers for each integer $k \geqslant 2$. Our main theorem is:

THEOREM 1. *Given an integer $k \geqslant 2$, there are positive constants $C_{1,k}$, $C_{2,k}$ such that for any integer $N \geqslant 1$,*

$$Q_k(N) < C_{1,k} N^{1-C_{2,k}}.$$

Remark. Schinzel [Sch] has studied a similar problem for fields of prime characteristic p. For any integer k not a power of p, he obtains polynomials with arbitrarily many terms, whose kth power has at most $2k$ terms. He also obtains lower bounds.

Two consequences of Theorem 1:

THEOREM 2. *Given an integer $k \geqslant 2$, there are positive constants $C_{1,j,k}$, $C_{2,j,k}$, $2 \leqslant j \leqslant k$, such that for any integer $N \geqslant 1$ there is a complete polynomial $f(x) \in \mathbf{R}[x]$ of degree $N-1$ such that the number of terms in each power $f^j(x)$, $2 \leqslant j \leqslant k$, is bounded by $C_{1,j,k} N^{1-C_{2,j,k}}$.*

THEOREM 3. *Given $F \in \mathbf{C}[y]$, $\deg(F) \geqslant 2$, there are positive constants $C_{1,F}$, $C_{2,F}$ such that for any integer $N \geqslant 1$ there is a complete polynomial $f \in \mathbf{C}[x]$ of degree $N-1$, such that the number of terms in the composition $F(f(x))$ is bounded by $C_{1,F}N^{1-C_{2,F}}$.*

We need some preliminary lemmas.

LEMMA 4. [Rén] $Q_k(tu) \leqslant Q_k(t)Q_k(u)$.

Proof. Let $f(x)$ be a polynomial exhibiting $Q_k(t)$ and $g(x)$ be a polynomial exhibiting $Q_k(u)$. Then $f(x)g(x^t)$ is a complete polynomial of degree $tu-1$ whose kth power has at most $Q_k(t)Q_k(u)$ terms. ∎

LEMMA 5 (see [Ver]). *If $c \geqslant 2$ and $(c-1)t < u \leqslant ct$ then $Q_k(u) \leqslant (k+1)kcQ_k(t)$.*

Proof. Let $f(x)$ be a polynomial exhibiting $Q_k(t)$. Select $\alpha \in \mathbf{R}$ such that

$$g(x) = f(x)h(x) = f(x)\Big(\sum_{i=0}^{c-2} x^{it} + \alpha x^{u-t}\Big)$$

is complete; we need only avoid finitely many selections of α. Each term of $h^k(x)$ has index $jt + l(u-t)$ where $0 \leqslant j < kc$ and $0 \leqslant l \leqslant k$, so that $h^k(x)$ has at most $(k+1)kc$ terms. Then $g(x)$ is a complete polynomial of degree $u-1$ whose kth power has at most $(k+1)kcQ_k(t)$ terms. ∎

The following technical lemmas form the basis of the proof for our main theorems. Their proofs will be delayed until the end of this section.

LEMMA 6. *Given an integer $k \geqslant 2$, there is an integer $n = n_k > k+1$ and a complete polynomial $R(x) \in \mathbf{R}[x]$ of degree $n-1$, such that*

$$R(x)^k = \sum_{i=0}^{k(n-1)} a_i x^i, \quad a_{jn+l} = 0, \quad 0 \leqslant j \leqslant k-1,\ 2 \leqslant l \leqslant k+1.$$

LEMMA 7. *Given n, k, and $R(x)$ as in Lemma 6, and an integer $L \geqslant 1$, set*

$$f(x) = \prod_{q=0}^{L-1} R(x^{n^q})$$

and let b_m be the coefficients of $f(x)^k$:

$$f(x)^k = \sum_{m=0}^{kn^L-k} b_m x^m.$$

Then whenever the n-ary expansion of m contains the digit $k+1$, then $b_m = 0$.

Proof of Theorem 1. Set

$$C_{1,k} = (k+1)k^2 n \quad \text{and} \quad C_{2,k} = 1 - \log(n-1)/\log n,$$

where $n = n_k$ is obtained from Lemma 6. Given N, set $L = \lceil \log N/\log n \rceil - 1$, set

$$f(x) = \prod_{q=0}^{L-1} R(x^{n^q})$$

as in Lemma 7, and let b_m be the coefficients of $f(x)^k$. Evidently

$$\deg(f) = (n-1)\sum_{q=0}^{L-1} n^q = n^L - 1,$$

and f is complete. By Lemma 7, whenever the n-ary expansion of m contains the digit $k+1$, then $b_m = 0$. So the number of nonzero b_m is less than

$$k(n-1)^L = kn^{L\log(n-1)/\log n} < kN^{\log(n-1)/\log n} = kN^{1-C_{2,k}}.$$

In other words,

$$Q_k(n^L) < kN^{1-C_{2,k}}.$$

Also $1 < N/n^L \leqslant n$. Apply Lemma 5 with $c = \lceil N/n^L \rceil$ to obtain

$$Q_k(N) \leqslant (k+1)kcQ_k(n^L) < (k+1)knkN^{1-C_{2,k}} = C_{1,k}N^{C_{2,k}}. \ ∎$$

Remark. This part of the proof, and the proof of Lemma 7, are a straightforward generalization of the proofs in Verdenius [Ver]. Our theorem applies to all $k \geqslant 2$ because we have a stronger version of Lemma 6.

Proof of Lemma 6. It remains to construct the polynomial $R(x)$. We can solve the appropriate equations numerically, and find the following solutions for $k = 2,3,4$:

$$R_2(x) = 1 + 2x - 2x^2 + 4x^3 - 10x^4 + 50x^5 + 125x^6,$$

$$\begin{aligned} R_3(x) \simeq{} & 3 + 3x - 3x^2 + 5x^3 - 10x^4 - 2.398981739501343x^5 \\ & + 2.784251144343039x^6 + 5.64780114474305x^7 \\ & + 1.378316906326019x^8 - 1.254037331018921x^9 \\ & + 4.220815430395043x^{10}, \end{aligned}$$

$$\begin{aligned} R_4(x) \simeq{} & 8 + 8x - 12x^2 + 28x^3 - 77x^4 + 231x^5 + 35.48749734170991x^6 \\ & + 3.906321336259001x^7 + 21.50353118849295x^8 \\ & - 81.98757276932204x^9 - 246.4175594501046x^{10} \\ & - 117.6178681286485x^{11} + 47.60164949619076x^{12} \\ & - 287.8978425147213x^{13} - 154.0940676494553x^{14} \\ & + 75.79518623126009x^{15} + 335.7973392244107x^{16} \\ & - 115.8892966893413x^{17} + 192.7918735396351x^{18}. \end{aligned}$$

Remark. Verdenius [Ver] gives different polynomials for R_2 and R_3. Our polynomial R_3 gives $1 - C_{2,3} = \log_{11} 10 = 0.96025\ldots$, improving his result; also $1 - C_{2,4} = \log_{19} 18 = 0.98163\ldots$; while our value of $C_{2,2}$ is inferior to his.

In the general case, we produce the following explicit construction, which however is quite inefficient, in that the resulting degree n is quite high, e.g. 11973 instead of 10 for R_3, or 31858 instead of 18 for R_4.

Select integers

$$a > k^2+k,$$
$$b > (2k+1)a,$$
$$c > (k^2+1)b,$$
$$n > (k^2+k+1)c.$$

Construct the disjoint sets

$$D = \{n-b, c, c-a\} \cup \{jn+l-(j-1)(n-b)-(k-j)c \mid 1 \leqslant j \leqslant k-1, 2 \leqslant l \leqslant k+1\},$$

$$E = \{jn+l+a-(j-1)(n-b)-(k-j)c \mid 1 \leqslant j \leqslant k-1, 2 \leqslant l \leqslant k+1\},$$

$$F = \{jn+l \mid 1 \leqslant j \leqslant k-1, 2 \leqslant l \leqslant k+1\}.$$

Consider a polynomial $S(x) = \sum_{i=0}^{n-1} s_i x^i$ such that

$$s_i = \begin{cases} 1 & \text{if } i \in D, \\ 0 & \text{if } i \notin D \cup E; \end{cases}$$

the values of s_i, $i \in E$, will be determined later. Set

$$T(x) = S(x)^k = \sum_{i \geqslant 0} t_h x^h.$$

Consider the values of $t_h, h \in F$ as functions of $s_i, i \in E$. There is a one-one onto correspondence from F to E, mapping $h = jn+l \in F$ to $i_h = jn+l+a-(j-1)(n-b)-(k-j)c \in E$, and there are positive integers y_h, z_h such that $t_h = y_h + z_h s_{i_h}$. This is because the size restrictions on a, b, c, n imply that there are only two ways to express h as the sum of exactly k elements of $D \cup E$, namely

$$h = jn+l$$
$$= 1 \cdot (jn+l-(j-1)(n-b)-(k-j)c) + (j-1) \cdot (n-b) + (k-j) \cdot (c)$$

(where all elements are from D) and

$$h = jn+l$$
$$= 1 \cdot (jn+l+a-(j-1)(n-b)-(k-j)c) + (j-1) \cdot (n-b) + (k-j-1) \cdot (c) + 1 \cdot (c-a)$$

(one element, i_h, is from E, and the rest are all from D). Thus nonzero values can be assigned to all s_i, $i \in E$, to satisfy $t_h = 0$, all $h \in F$. (Specifically, $y_h = k\binom{k-1}{j-1}$, $z_h = k(k-1)\binom{k-2}{j-1}$, and $s_{i_h} = -y_h/z_h = -1/(k-j)$.)

Further, the Jacobian matrix relating $\{s_i, i \in E\}$ (as independent variables) with $\{t_h, h \in F\}$ (as dependent variables) is nonsingular; it is a permutation of a nonzero diagonal matrix, with exactly one nonzero in each row and each column.

Now continuously perturb the values of $s_i, i \notin D \cup E$, in such a way that $s_i, 0 \leqslant i \leqslant k+1$, are the first terms of the Taylor expansion of $\delta \cdot (1+x)^{1/k}$ (all of which are nonzero reals), and the other values of s_i are also nonzero reals; here

δ is a small real which is being perturbed from 0. Choose the values of $s_i, i \in E$, so that $t_h = 0, h \in F$, remains satisfied; this is possible by the nonsingularity of the Jacobian, as long as the perturbations are small enough. Also, the values of $s_i, i \in E$, remain nonzero if the perturbations are small enough. Let R be the perturbed value of S, and r_i its coefficients. By construction, R is complete, and R^k has zeroes in positions $jn+l, 1 \leqslant j \leqslant k-1, 2 \leqslant l \leqslant k+1$. By selection of the initial values $r_0, r_1, \ldots, r_{k+1}$, we find that R^k also has zeroes in positions $0n+l, 2 \leqslant l \leqslant k+1$. This establishes the lemma. ∎

Proof of Lemma 7. We have

$$\sum_m b_m x^m = \prod_{q=0}^{L-1} \Big(\sum_{i=0}^{k(n-1)} a_i x^{in^q} \Big).$$

Suppose the digit $k+1$ occurs in the n-ary expansion of m. Then b_m is the sum of products of

$$a_{i_q}, \quad i_q = j_q n + l_q, \quad 0 \leqslant l_q \leqslant n-1,$$

where

$$\sum_q i_q n^q = m.$$

Let the n-ary expansion of m be

$$m = \sum_q r_q n^q, \quad 0 \leqslant r_q \leqslant n-1, \quad r_Q = k+1.$$

Looking at these equations modulo n^{Q+1}, we find either

$$(k+1)n^Q + \sum_{q=0}^{Q-1} r_q n^q = l_Q n^Q + \sum_{q=0}^{Q-1} i_q n^q \leqslant l_Q n^Q + kn^Q - k$$

or

$$(n+k+1)n^Q + \sum_{q=0}^{Q-1} r_q n^q = l_Q n^Q + \sum_{q=0}^{Q-1} i_q n^q \leqslant l_Q n^Q + kn^Q - k.$$

The latter case is clearly impossible. The former case implies that

$$2 \leqslant l_Q \leqslant k+1,$$

whence $a_{i_Q} = 0$ by our construction of R. Thus each summand contributing to b_m has a zero among its factors, so each summand is zero, and $b_m = 0$. ∎

Simultaneous sparseness of several powers. For each $k \geqslant 2$, we have found a polynomial whose kth power is sparse. In fact we can find a single polynomial all of whose jth powers, $2 \leqslant j \leqslant k$, are sparse simultaneously.

THEOREM 2. *Given an integer $k \geqslant 2$, there are positive constants $C_{1,j,k}$, $C_{2,j,k}$, $2 \leqslant j \leqslant k$, such that for any integer $N \geqslant 1$ there is a complete polynomial $f(x) \in \mathbf{R}[x]$ of degree $N-1$ such that the number of terms in each power $f^j(x)$, $2 \leqslant j \leqslant k$, is bounded by $C_{1,j,k} N^{1-C_{2,j,k}}$.*

Proof. Define

$$C_{1,j,k} = j^2(j+1)C_{1,j}, \quad C_{2,j,k} = C_{2,j}/(k-1),$$

where $C_{1,j}$, $C_{2,j}$ are defined in Theorem 1.

Assume given $N \geqslant 1$. Set

$$M = \lfloor N^{1/(k-1)} \rfloor .$$

For each j, $2 \leqslant j \leqslant k$, use Theorem 1 to construct a complete polynomial f_j of degree $M-1$, whose jth power has at most $C_{1,j}M^{1-C_{2,j}}$ nonzeroes. As in the proof of Lemma 4, construct

$$\tilde{f}(x) = f_2(x)f_3(x^M)f_4(x^{M^2})\dots f_k(x^{M^{k-2}}).$$

For each $j, 2 \leqslant j \leqslant k$, we can bound the number of terms in the jth power of $\tilde{f}$, as follows. We write $\tilde{f}$ as

$$\tilde{f}(x) = L_j(x)f_j(x^{M^{j-2}})R_j(x^{M^{j-1}})$$

where

$$L_j(x) = \prod_{i=2}^{j-1} f_i(x^{M^{i-2}}), \quad R_j(y) = \prod_{i=j+1}^{k} f_i(y^{M^{i-j-1}}).$$

The degree of L_j is given by

$$(M-1)+(M-1)M+(M-1)M^2+\dots+(M-1)M^{j-3} = M^{j-2}-1,$$

so the number of terms in its jth power is at most

$$1+j(M^{j-2}-1) < jM^{j-2}.$$

Similarly, the degree of $R_j(y)$ is

$$M^{k-j}-1.$$

The number of terms in $R_j^j(y)$, and hence the number of terms in $R_j^j(x^{M^{j-1}})$, is bounded by

$$1+j(M^{k-j}-1) < jM^{k-j}.$$

The number of terms in the jth power of $f_j(x^{M^{j-2}})$ is less than

$$C_{1,j}M^{1-C_{2,j}}.$$

So the number of terms in the jth power of $\tilde{f}(x)$ is less than

$$(jM^{j-2})(jM^{k-j})(C_{1,j}M^{1-C_{2,j}}) = (C_{1,j}j^2)M^{(k-2)+(1-C_{2,j})} \leqslant (C_{1,j}j^2)N^{1-(C_{2,j}/(k-1))}.$$

Further, for N sufficiently large, $M^{k-1} \leqslant N \leqslant 2M^{k-1}$, so that setting

$$f(x) = (1+\alpha x^{N-M^{k-1}})\tilde{f}(x)$$

as in the proof of Lemma 5, we find the required $f(x)$. ∎

From this it is easy to prove:

THEOREM 3. *Given $F \in \mathbf{C}[y]$, $\deg(F) \geqslant 2$, there are positive constants $C_{1,F}$, $C_{2,F}$ such that for any integer $N \geqslant 1$ there is a complete polynomial $f \in \mathbf{C}[x]$ of degree $N-1$, such that the number of terms in the composition $F(f(x))$ is bounded by $C_{1,F}N^{1-C_{2,F}}$.*

Proof. Let $\deg(F) = k \geqslant 2$. Use Theorem 2 to compute a complete polynomial $\hat{f}$ of degree $N-1$, whose jth powers, $2 \leqslant j \leqslant k$, are all sparse. Unfortunately, $F(\hat{f}(x))$ is not only a linear combination of these jth powers; rather, it is a linear combination of these jth powers, along with $\hat{f}$ itself (if F has a nonzero linear term), and an innocuous constant. So we must arrange to cancel the linear term in F.

Since $k \geqslant 2$, the derivative $F'(y)$ is a polynomial of degree at least 1. It has a root $\Delta \in \mathbf{C}$:

$$F'(\Delta) = 0.$$

Then set

$$f(x) = \Delta + \lambda\hat{f}(x),$$

where λ is a nonzero complex number such that $f(x)$ has a nonzero constant term. The Taylor expansion of F around the point Δ gives

$$F(f(x)) = F(\Delta+\lambda\hat{f}(x)) = \sum_{j=0}^{k} F^{(j)}(\Delta)\frac{(\lambda\hat{f}(x))^j}{j!}$$

where, by choice of Δ, we have

$$F^{(1)}(\Delta) = F'(\Delta) = 0.$$

Then $F(f(x))$ is a linear combination, over $\mathbf{C}$, of jth powers of $\hat{f}(x)$, $2 \leqslant j \leqslant k$, and 1. Thus the number of terms is bounded by the sum of the numbers of terms in the jth powers of $\hat{f}(x)$, plus 1 for the constant term $j = 0$. Selecting $\hat{f}(x)$ as prescribed by Theorem 2, we find that $f(x)$ satisfies the conclusion of the present theorem. ∎

Extensions and open question. We have seen (Theorem 2) that we can find a polynomial f with several powers sparse simultaneously, and (Theorem 3) that we can find a polynomial f such that $F(f(x))$ is sparse, if F is a given polynomial of degree at least 2. By the same techniques, if we have several polynomials $F_j(y)$ without linear terms, we can find $f(x)$ such that all the compositions $F_j(f(x))$ are simultaneously sparse. But we cannot achieve this for arbitrary $F_j(y)$. For example, if $F_1(y) = y^2$ and $F_2(y) = y^2+y$, then we cannot choose a complete $f(x)$ making $F_1(f(x))$ and $F_2(f(x))$ simultaneously sparse, since the linear combination $F_2(f(x)) - F_1(f(x))$ gives $f(x)$, which is complete.

Is this the only obstacle? If y cannot be expressed as a linear combination of $F_j(y)$ and 1, can we find $f(x)$ such that all $F_j(f(x))$ are sparse? In particular, can we find a family of complete polynomials $f(x)$ such that both $f(x)^2$ and $(f(x)+1)^3$ are sparse? The techniques of this paper seem to be insufficient to answer this question, and we leave it open.

Rényi's polynomial. Our investigation began when we saw the following beautiful example of Rényi [Rén], and some of our techniques came from reverse engineering his example:

$$P(x) = (1+2x-2x^2+4x^3+4x^4)(1+2x^4-2x^8+4x^{12}-10x^{16}+28x^{20}-84x^{24}).$$

$P(x)$ has degree 28; all its 29 coefficients are nonzero integers. Its square has only 28 nonzero coefficients. Indeed, the second factor is the first seven terms in the Taylor expansion of $(1+4x^4)^{1/2}$, and if we take instead the first n terms, the resulting P will have degree $4n$, with $4n+1$ nonzero integer coefficients, while P^2 has only $3n+7$ nonzero coefficients. As soon as $n \geqslant 7$, we have $4n+1 > 3n+7$.

Professor Schinzel has kindly made us aware of two polynomials with eighteen terms each, whose squares are also sparse. One construction of a polynomial with 18 terms whose square has only 17 terms is due to R. Freud [Fre]. An unpublished example by Mr. Ajai Choudhry [Cho]:

$$f(x) = (x^2+2x-2)(x^{15}+4x^{12}-8x^9+32x^6-160x^3+896),$$

gives the same polynomial as [Fre], up to reflection, but derived independently and by different methods.

A smaller example for squares. One product of our investigation was a smaller example for squares. Define

$$P_{12}(x) = (1+2x-2x^2+4x^3-10x^4+50x^5+125x^6)(1-110x^6)$$

and remark that P_{12} is a smaller polynomial with the same properties: complete, degree 12, thus 13 nonzero coefficients, and its square has only 12 nonzero coefficients. Notice that the first factor,

$$(1+2x-2x^2+4x^3-10x^4+50x^5+125x^6),$$

when squared, yields a polynomial of degree twelve, with zeroes in positions 2, 3, 4, 8, 9, 10, and nonzeroes in positions 0, 1, 5, 6, 7, 11, 12. The second factor could be chosen as $(1+\alpha x^6)$ for arbitrary α, and the resulting square would have at most 13 nonzeroes, at positions 0, 1, 5, 6, 7, 11, 12, 13, 17, 18, 19, 23, 24. By our choice $\alpha = -110$, we arrange to cancel one of the coefficients (number 13), bringing the count down to twelve. As in Rényi's example, if we selected the second factor to be some polynomial in x^6 whose square had a lot of consecutive zeroes (e.g. the first several terms of the expansion of $(1+\alpha x^6)^{1/2}$) we would have about $(0.5N+\text{constant})$ nonzero coefficients in the square of a complete polynomial of degree N.

Smaller yet? The existence of smaller examples can be determined by a finite algebraic computation. For each degree $d < 12$, and each possible pattern of $d+1$ zeroes among the $2d+1$ coefficients of $P(x)^2$, we can write down the $d+1$ equations that must be satisfied by the coefficients of $P(x)$. Then a Groebner basis constructor can be invoked to decide whether these equations have a solution with P complete. In this way we have discovered that no example of degree $d \in \{6, 7\}$ exists. Smaller degree examples are easily ruled out. The cases 8, 9, 10 and 11 remain open.

Acknowledgment. It is a pleasure to acknowledge Prof. Andrzej Schinzel for encouragement and several helpful pointers to the literature.

References

[Cho] A. Choudhry, unpublished, communicated to us by A. Schinzel, 1988.

[Erd] P. Erdös, *On the number of terms of the square of a polynomial*, Nieuw Arch. Wisk. (2) 23 (1949), 63–65.

[Fre] R. Freud, *On the minimum number of terms in the square of a polynomial* (Hungarian), Mat. Lapok 24 (1973), 95–98.

[Rén] *Selected Papers of Alfred Rényi*, vol. 1, Budapest 1976, pp. 44 and 47. See also *On the minimal number of terms in the square of a polynomial*, Acta Math. Hungar. 1 (1947), 30–34.

[Sch] A. Schinzel, *On the number of terms of a power of a polynomial*, Acta Arith. 49 (1987), 55–70.

[Ver] W. Verdenius, *On the number of terms of the square and the cube of polynomials*, Indag. Math. 11 (1949), 546–565.

IBM RESEARCH
T. J. WATSON RESEARCH CENTER
Yorktown Heights, NY 10598, USA

SCHOOL OF MATHEMATICAL SCIENCES
UNIVERSITY OF BATH
Bath, England

Received on 5.9.1989
and in revised form on 16.2.1990 (1962)