Polynomials whose powers are sparse

by

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

Erdős [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. Erdős proves the existence of positive constants \( C_1, C_2 \) such that

\[ Q(N) < C_1 N^{1 - C_1}. \]

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

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

He also establishes a similar inequality for cubes. Letting \( Q_k(N) \) denote the least possible number of terms in the \( k \)th 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 \( N \geq 1 \),

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

In the present note we extend this result to \( k \)th powers for each integer \( k \geq 2 \). Our main theorem is:

**Theorem 1.** Given an integer \( k \geq 2 \), there are positive constants \( C_{1,k}, C_{2,k} \) such that for any integer \( N \geq 1 \),

\[ Q_k(N) < C_{1,k} N^{1 - C_{2,k}}. \]

**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 \( k \)th power has at most \( 2k \) terms. He also obtains lower bounds.

Two consequences of Theorem 1:

**Theorem 2.** Given an integer \( k \geq 2 \), there are positive constants \( C_{1,k}, C_{2,k} \), \( 2 \leq j \leq k \), such that for any integer \( N \geq 1 \) there is a complete polynomial \( f(x) \in \mathbb{R}[x] \) of degree \( N - 1 \) such that the number of terms in each power \( f^j(x) \), \( 2 \leq j \leq k \), is bounded by \( C_{1,k} N^{1 - C_{2,k}} \).
THEOREM 3. Given $F \in \mathbb{C}[y]$, $\deg(F) \geq 2$, there are positive constants $C_1, F$, $C_2, F$ such that for any integer $N \geq 1$ there is a complete polynomial $f \in \mathbb{C}[x]$ 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] $Q_k(tu) \leq Q_k(t)Q_k(u)$.

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

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

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

$$g(x) = f(x)h(x) = f(x)(\sum_{i=0}^{c-2} x^i + x^{c-1})$$

is complete; we need only avoid finitely many selections of $\alpha$. Each term of $h^k(x)$ has index $jt + l(u - t)$ where $0 \leq j < kc$ and $0 \leq l \leq k$, so that $h^k(x)$ has at most $(k + 1)kc$ terms. Then $g(x)$ is a complete polynomial of degree $u - 1$ whose $k$th 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 $k \geq 2$, there is an integer $n = n_k > k + 1$ and a complete polynomial $R(x) \in \mathbb{R}[x]$ of degree $n - 1$, such that

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

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

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

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

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

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

**Proof of Theorem 1.** Set

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

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

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

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

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

In other words,

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

Also $1 < N/n^L \leq n$. Apply Lemma 5 with $c = \ceil{\log n^L}$ to obtain

$$Q_k(N) \leq (k+1)kcQ_k(n^L) < (k+1)kn^{1 - C_{2,k}} = C_{1,k}N^{1 - C_{2,k}}. ■$$

Remark. This part of the proof, and the proof of Lemma 7, are straightforward generalizations of the proofs in Verdenius [Ver]. Our theorem applies to all $k \geq 2$ 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 $k = 2, 3, 4$:

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

$$R_3(x) = 3 + 3x - 3x^2 + 5x^3 - 10x^4 - 239898713950134x^5 + 72842511443039x^6 + 5647801144270x^7 + 1378316906326019x^8 - 1.254037331018921x^9 + 4.22081543095043x^{10},$$

$$R_4(x) = 8 + 8x - 12x^2 + 28x^3 - 77x^4 + 231x^5 + 35.48749734170991x^6 + 3.90632136299001x^7 + 21.5035118849295x^8 + 81.9875727932204x^9 + 246.475594501046x^{10} + 117.61786628854x^{11} + 47.6016499619076x^{12} - 287.8978425147213x^{13} - 154.094066749553x^{14} + 75.7951862126009x^{15} + 335.797392244107x^{16} - 115.88929668943x^{17} + 192.78173536351x^{18}. ■$$

Remark. Verdenius [Ver] gives different polynomials for $R_3$ and $R_4$. Our polynomial $R_3$ gives $1 - C_{2,3} = \log_3 10 = 0.96025 ..., improving his result; also $1 - C_{2,4} = \log_4 18 = 0.98163 ..., while our value of $C_{2,4}$ 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 $R_4$. 

6. *Acta Arithmetica* LVIII.
Select integers 
\[ a > k^2 + k, \]
\[ b > (2k+1)a, \]
\[ c > (k^2 + k)b, \]
\[ n > (k^2 + k + 1)c. \]

Construct the disjoint sets 
\[ D = \{ b - c, c - a \} \cup \{ jn + l - (j-1)(n-b) - (j-k)c : 1 \leq j \leq k, 1 \leq l \leq k+1 \}, \]
\[ E = \{ jn + l - (j-1)(n-b) - (j-k)c : 1 \leq j \leq k-1, 1 \leq l \leq k+1 \}, \]
\[ F = \{ jn + l | 1 \leq j \leq k-1, 2 \leq l \leq k+1 \}. \]

Consider a polynomial \( S(x) = \sum_{i=0}^{n} s_i x^i \) 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 
\[ T(x) = S(x)^k = \sum_{i=0}^{n} t_i x^i. \]

Consider the values of \( t_h, h \in F \) as functions of \( s_i, i \in E. \) There is a one-one correspondence from \( F \) to \( E, \) mapping \( h = jn + l \in F \) to \( i_h = jn + l + a - (j-1)(n-b) - (j-k)c \in E, \) and there are positive integers \( y_h, z_h \) such that \( t_h = y_h + z_h s_h. \) 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 
\[ h = jn + l \]
\[ = 1 \cdot (jn + l - (j-1)(n-b) - (j-k)c + (j-1)(n-b) + (j-k)c) \]
(where all elements are from \( D \)) and 
\[ h = jn + l + a - (j-1)(n-b) - (j-k)c + (j-1)(n-b) + (j-k)c + 1 \cdot (c - a) \]
(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, \( y_h = k \cdot (k-1), \) \( z_h = k \cdot (k-2), \) and \( s_h = -y_h/z_h = -1/(k-j). \)

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

Now continuously perturb the values of \( s_i, i \notin D \cup E, \) in such a way that \( s_i, 0 \leq i \leq k + 1, \) are the first terms of the Taylor expansion of \( \delta \cdot (1 + x)^{k+1} \) (all of which are nonzero reals), and the other values of \( s_i \) are also nonzero reals; here \( \delta \) 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 zeros in positions \( jn + l, 1 \leq j \leq k-1, 2 \leq l \leq k+1. \) By selection of the initial values \( r_0, r_1, \ldots, r_{k+1}, \) we find that \( R^k \) also has zeros in positions \( 0n + l, 2 \leq l \leq k+1. \) This establishes the lemma. \( \square \)

**Proof of Lemma 7.** We have
\[ \sum_{m} b_m x^m = \prod_{q=0}^{l-1} \left( \sum_{i=0}^{m(n-1)} a_q x^{i q^r} \right). \]

Suppose the digit \( k+1 \) occurs in the \( n \)-ary expansion of \( m. \) Then \( b_m \) is the sum of products of
\[ a_{l q}, \quad i_q = jn + l q, \quad 0 \leq l q \leq n - 1, \]
where
\[ \sum_{q} i_q n^q = m. \]

Let the \( n \)-ary expansion of \( m \) be
\[ m = \sum_{q} r_q n^q, \quad 0 \leq r_q \leq n - 1, \quad r_{k+1} = 1. \]

Looking at these equations modulo \( p^{k+1}, \) we find either
\[ (k+1)n^q + \sum_{q=0}^{k-1} r_q n^q = l_0 n^q + \sum_{q=0}^{k-1} i_q n^q \leq l_0 n^q + kn^q - k \]
or
\[ (n+k+1)n^q + \sum_{q=0}^{k-1} r_q n^q = l_0 n^q + \sum_{q=0}^{k-1} i_q n^q \leq l_0 n^q + kn^q - k. \]

The latter case is clearly impossible. The former case implies that
\[ 2 \leq l_0 \leq k + 1, \]
whence \( a_{l_0} = 0 \) by our construction of \( R. \) Thus each summand contributing to \( b_m \) has a zero among its factors, so each summand is zero, and \( b_m = 0. \) \( \square \)

**Simultaneous sparseness of several powers.** For each \( k \geq 2, \) we have found a polynomial whose \( k \)th power is sparse. In fact we can find a single polynomial of whose \( j \)th powers, \( 2 \leq j \leq k, \) are sparse simultaneously.

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

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

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

\[ f_j(x) = f_2(x)f_3(x^M)f_4(x^{M^2}) \ldots f_k(x^{M^{k-2}}). \]

For each \( j, 2 \leq j \leq k \), we can bound the number of terms in the \( j \)th power of \( f_j \), as follows. We write \( f_j \) as

\[ f_j(x) = L_j(x)f_j(x^{M^{j-2}})R_j(x^{M^{j-1}}), \]

where

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

The degree of \( L_j \) is given by

\[ (M-1)+(M-1)M+(M-1)M^2 + \ldots + (M-1)M^{j-2} = M^{j-2} - 1, \]

so the number of terms in its \( j \)th power is at most

\[ 1+j(M^{j-2} - 1) < jM^{j-2}. \]

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

\[ M^{j-1} - 1. \]

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

\[ 1+j(M^{j-2} - 1) < jM^{j-1}. \]

The number of terms in the \( j \)th 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 \( j \)th power of \( f_j(x) \) is less than

\[ (jM^{j-2} - 1)(jM^{j-2} - 1)(C_{1,j}M^{1-C_{2,j}}) = (C_{1,j}j^2)M^{1-C_{2,j}} < C_{1,j}j^2M^{1-C_{2,j}}. \]

Further, for \( N \) sufficiently large, \( M^k - 1 \leq N \leq 2M^k - 1 \), so that setting

\[ f(x) = (1 + 2x^{N-M^k})f(x) \]

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

From this it is easy to prove:

**Theorem 3.** Given \( F \in \mathbb{C}[y], \deg(F) \geq 2 \), there are positive constants \( C_{1,F}, C_{2,F} \) such that for any integer \( N \geq 1 \) there is a complete polynomial \( f \in \mathbb{C}[x] \) 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 \( \deg(F) = k \geq 2 \). Use Theorem 2 to compute a complete polynomial \( f \) of degree \( N-1 \), whose \( j \)th powers, \( 2 \leq j \leq k \), are all sparse. Unfortunately, \( f(x) \) is not only a linear combination of these \( j \)th powers; rather, it is a linear combination of these \( j \)th powers, along with itself (if \( F \) has a nonzero linear term), and an innocuous constant. So we must arrange to cancel the linear term in \( F \).

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

\[ F'(A) = 0. \]

Then set

\[ f(x) = A + \lambda f(x), \]

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

\[ F(f(x)) = F(A + \lambda f(x)) = \sum_{j=0}^{k} F^{(j)}(A) \frac{(\lambda f(x))^j}{j!}, \]

where, by choice of \( A \), we have

\[ F^{(j)}(A) = F(0) = 0. \]

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

**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.
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 $d+1$ zeros 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


