ISSN 0027-1322, Moscow University Mathematics Bulletin, 2014, Vol. 69, No. 2, pp. 51–55. © Allerton Press, Inc., 2014.
Original Russian Text © S.B. Gashkov, E.T. Shavgulidze, 2014, published in Vestnik Moskovskogo Universiteta, Matematika. Mekhanika, 2014, Vol. 69, No. 2, pp. 9–14.

Representation of Monomials as a Sum of Powers of Linear Forms

S. B. Gashkov[a] **and E. T. Shavgulidze**[b]

[a] *Moscow State University, Faculty of Mechanics and Mathematics, Leninskie Gory, Moscow, 119991 Russia; e-mail: sbgashkov@gmail.com*

[b] *Moscow State University, Faculty of Mechanics and Mathematics, Leninskie Gory, Moscow, 119991 Russia; e-mail: shavgulidze@bk.ru*

Received October 1, 2012

Abstract—It is proved that the product of n complex variables can be represented as a sum of $m = 2^{n-1}$ n-powers of linear forms of n variables and for any $m < 2^{n-1}$ there is no such identity with m summands being nth powers of linear forms.

DOI: 10.3103/S0027132214020028

The identity $xy = ((x+y)^2-(x-y)^2)/4$ is widely known. It allows one to perform multiplication providing the table of squares is available. This technique was used centuries ago as an alternative to application of logarithms. It is less known that, given a table of cubes, one can multiply three numbers by the formula

$$xyz = \frac{1}{24}((x+y+z)^3 - (x+y-z)^3 - (x-y+z)^3 - (y+z-x)^3).$$

This formula can be generalized to the case of multiplication of n variables with the use of addition, subtraction, and raising to nth power. For any field whose characteristic is greater than n (or equals to zero), the following identity holds:

$$x_1 \dots x_n = \frac{1}{2^{n-1}n!} \sum_{\sigma_2=0,1,\dots\sigma_n=0,1} (-1)^{\sigma_2+\dots+\sigma_n}(x_1 + (-1)^{\sigma_2}x_2 + \dots + (-1)^{\sigma_n}x_n)^n.$$

To prove it, note that each of 2^{n-1} summands

$$(x_1 + (-1)^{\sigma_2}x_2 + \dots + (-1)^{\sigma_n}x_n)^n$$

contains the monomial $n!(-1)^{\sigma_2+\dots+\sigma_n}x_1 \dots x_n$ which being multiplied by $(-1)^{\sigma_2+\dots+\sigma_n}$ turns to the monomial $n!x_1 \dots x_n$, and after the calculation of the sum the monomial gets the coefficient $2^{n-1}n!$. It remains to verify that other monomials $x_{i_1}^{n_1} \dots x_{i_m}^{n_m}$, $m < n$, enter this sum with zero coefficients. In fact, for any such monomial there exists the variable x_i, $i > 1$, not entering it, or the variable x_i, $i > 1$, entering it squared. In both the cases the coefficient at this monomial in any summand $(x_1 + (-1)^{\sigma_2}x_2 + \dots + (-1)^{\sigma_n}x_n)^n$ does not depend on the index σ_i. Therefore, after multiplication by $(-1)^{\sigma_2+\dots+\sigma_n}$ the dependence of the index σ_i under fixed other indices σ_j, $j \neq i$, results in the change of sign under the change of the value of σ_i. Therefore, grouping together pairs of summands differing only in the values of the index σ_i, we obtain that the sum of each such pair is equal to zero and hence the total sum of 2^{n-1} summands is equal to zero, i.e., the coefficient at any monomial $x_{i_1}^{n_1} \dots x_{i_m}^{n_m}$, $m < n$, in the sum

$$\sum_{\sigma_2=0,1,\dots\sigma_n=0,1} (-1)^{\sigma_2+\dots+\sigma_n}(x_1 + (-1)^{\sigma_2}x_2 + \dots + (-1)^{\sigma_n}x_n)^n$$

is equal to zero, which proves the identity considered here.

This identity implies that in an arbitrary field of characteristic zero one can represent the monomial $x_1 \dots x_n$ as a linear combination of 2^{n-1} linear forms l_i of the same variables, i.e.,

$$x_1 \dots x_n = \sum_{i=1}^{2^{n'-1}} \alpha_i l_i^n.$$

Obviously, in the field $\mathbb{C}$ (or in any algebraically closed field) one can assume that $\alpha_i = 1$ in this identity, in the field $\mathbb{R}$ one can use only the coefficients $\alpha_i = \pm 1$, and for odd n only the coefficients $\alpha_i = 1$.

The following question arises: what is the least number m satisfying the identity

$$x_1 \dots x_n = \sum_{i=1}^{m} \alpha_i l_i^n,$$

where l_i are linear forms of the variables $x_1, \dots, x_n$? The first of the authors encountered this problem in the middle of 80s in the last century in connection with the following question: what is the least complexity of a formula constructed over the basis $B = \{x + y, x^2\} \cup \{ax : a \in \mathbb{R}\}$ consisting of the operations of addition, squaring, and multiplication by an arbitrary scalar, and calculating the function $x_1 \dots x_n$?

The notions of a formula over the basis B and its complexity are defined inductively in a standard manner (see, e.g., [1–3]). By definition, any variable is a formula; if Φ_i are formulas, then $\Phi_1 + \Phi_2$ is also a formula; if Φ is a formula, then Φ^2 and $a\Phi$ are also formulas for any $a \in \mathbb{R}$. The complexity of a formula is the number of all symbols of variables entering it (one can define the complexity of a formula as the number of basic operations in it, but this definition coincides in essence with this one). The complexity of a function is the minimal complexity of a formula realizing it.

One can inductively construct a formula in the basis B having the complexity $O(n^2)$ and realizing the product $x_1 \dots x_n$. To do that, represent $x_1 \dots x_n$ in the form of the product

$$y_1 y_2, \;\; y_1 = x_1 \dots x_{\lfloor n/2 \rfloor}, \;\; y_2 = x_{\lfloor n/2 \rfloor + 1} \dots x_n,$$

represent y_i by formulas Φ_i of complexity

$$O(n_i^2), \; n_1 = \lfloor n/2 \rfloor, \; n_2 = \lceil n/2 \rceil, \; n_1 + n_2 = n,$$

and represent $y_1 y_2$ by the formula

$$\frac{1}{4}((\Phi_1 + \Phi_1)^2 - (\Phi_1 - \Phi_1)^2).$$

The complexities of formulas considered here relate as $L(\Phi) \le 2(L(\Phi_1) + L(\Phi_2))$, which implies the inequality $L(n) \le 2(L(\lceil n/2 \rceil) + L(\lfloor n/2 \rfloor))$, where $L(n)$ is the complexity of realization of the product $x_1 \dots x_n$ by formulas in the given basis B. It is easy to show by induction that $L(n) = n^2$ for $n = 2^k$. In the general case, one can verify by induction that $L(n) \le \frac{9n^2-1}{8}$. The base of induction is obvious. In order to justify the inductive step, it is sufficient to check the inequalities

$$4\frac{9m^2-1}{8} \le \frac{9(2m)^2-1}{8}, \; 2\left(4\frac{9m^2-1}{8} + \frac{9(2m+1)^2-1}{8}\right) \le \frac{9(4m+1)^2-1}{8},$$

$$2\left(4\frac{9(m+1)^2-1}{8} + \frac{9(2m+1)^2-1}{8}\right) \le \frac{9(4m+3)^2-1}{8}.$$

Note that the proof of this estimate coincides in essence with the proof of the complexity estimate for realization of the linear Boolean function $x_1 \oplus \dots \oplus x_n$ by formulas in the basis $\{\&, \vee, \neg\}$ or by sequentially-parallel circuits (see [4]). The lower bound $L_{\&,\vee,\neg}(n) \ge n^2$ for the latter problem was proved in [5].

It is natural to suppose that such lower bound can be also proved for the case of realization of the product $x_1 \dots x_n$ by formulas in the basis $B = \{x + y, x^2\} \cup \{ax : a \in \mathbb{R}\}$.

In the case of realization by circuits this is not true because we obviously have $L_B(n) = O(n)$.

A similar problem can be considered for an arbitrary basis $B_k = \{x + y, x^k\} \cup \{ax : a \in \mathbb{R}\}$. For example, the estimate $L_{B_3}(n) = O(n^{\log_3 12})$ is valid for $k = 3$. One may also study similar problems for the basis $\{x + y, 1\} \cup \{ax : a \in \mathbb{R}\}$ consisting of an arbitrary nonlinear polynomial and the set of linear functions (it is proved that any polynomial can be represented in this basis).

The problem for the least number of linear forms l_i such that a certain linear combination of their nth powers is equal to $x_1 \dots x_n$ appeared in the attempt to solve the problem on the complexity of calculation of the product $x_1 \dots x_n$ by formulas in the basis $B = \{x + y, x^2\} \cup \{ax : a \in \mathbb{R}\}$. In modern terminology, the representation in the form of a sum of powers of linear forms is the realization by circuits (formulas) of depth two in the basis B.

The first author considered the problem of representation of products by sums of powers as a competition one and presented its particular cases for student and school mathematical contests, but had not proved the

lower bound in the general form. The second author proved it in the end of 1980s. The problem occurred to be too difficult for competitions and the authors had not seen any sense in its publication.

Recently, the first author have known that this (and a bit more general) problem was considered in [6] and, in particular, it was also proved that the number of summands in any identity

$$x_1 \dots x_n = l_1^d + \dots + l_s^d,$$

where l_i are affine forms, is not less than $2^n/(d+1)$, and it was proved in [7] that the number of summands in any identity

$$x_1 \dots x_n = Q_1^{e_1} + \dots + Q_s^{e_s},$$

where Q_i are polynomials of degree not exceeding d, satisfies the inequality $\ln s = \Omega(n/2^d) + O(d \ln n)$. In particular, the lower bound $s \geq 2^{\Omega(n)}$ was obtained for $d = 1$. Papers [6, 7] refer to [8] where the family of 2^{n-1} linear forms such that the sum of their nth powers with alternating signs is equal to the product of n variables was indicated (probably, this family coincides with that mentioned above in this paper).

Therefore, the first author decided to write this note. We had to restore the proof because it was not recorded at that time. Apparently, it is close to the proof found more than thirty years ago by the second author.

Theorem. *Given an arbitrary field whose characteristic is greater than n or equal to zero, the minimal number of linear forms l_i of the variables $x_1, \dots, x_n$ whose linear combination of nth powers coincides with the product $x_1 \dots x_n$ is equal to 2^{n-1}.*

Proof. The upper estimate was presented above. Prove the lower estimate. Let

$$x_1 \dots x_n = \sum_{i=1}^{s} \alpha_i l_i^n,\ l_i = a_{1,i}x_1 + \dots + a_{n,i}x_n,\ i = 1, \dots, s,$$

be a linear combination of nth powers of linear forms over an arbitrary field F and $\alpha_i \in F$. Prove that $s \geq 2^{n-1}$. Suppose $s < 2^{n-1}$ and get a contradiction. Consider the vectors $v_k = (a_{k,1}, \dots, a_{k,s}) \in F^s$, $k = 1, \dots, n$. Applying the operation of component-wise multiplication of vectors, introduce into consideration the 2^{n-1} vectors

$$v_1^n,\ v_1^{n-1}v_2, \dots, v_1^{n-1}v_n,\ v_1^{n-2}v_2v_3, \dots, v_1^{n-2}v_{n-1}v_n, \dots, v_1^2v_2 \dots v_{n-1}, \dots, v_1^2v_3 \dots v_n, v_1 \dots v_n,$$

where the cofactors $v_2, \dots, v_n$ enter every summand with the power not exceeding one, and all other vectors

$$v_{i_1}^{\mu_1} \dots v_{i_m}^{\mu_m},\ 1 \leq i_1 < \dots < i_m \leq n,\ \mu_1 + \dots + \mu_m = n,\ m < n.$$

For an arbitrary vector $w = (w_1, \dots, w_s) \in F^s$, denote $\sum_{i=1}^s \alpha_i w_i$ by $|w|$. Obviously,

$$\left| \sum_{j=1}^{m} \lambda_j e_j \right| = \sum_{j=1}^{m} \lambda_j |e_j|$$

for any vectors e_j and coefficients λ_j.

Removing the parentheses in the formula for $x_1 \dots x_n$ and equating the coefficients, we get $|v_{i_1}^{\mu_1} \dots v_{i_m}^{\mu_m}| = 0$ for $m \leq n-1$. Assuming

$$w_{i_1,\dots,i_m} = v_1^{n-m} v_{i_1} \dots v_{i_m},$$

this fact, in particular, implies $|w_{i_1,\dots,i_m}| = 0$ for $m < n-1$, but $|w_{2,\dots,n}| = 1/n!$. In fact, the coefficient at $x_{i_1}^{\mu_1} \dots x_{i_m}^{\mu_m}$ in the summand $\alpha_i l_i^n$ is equal (up to a multiplier) to $\alpha_i v_{i_1}^{\mu_1} \dots v_{i_m}^{\mu_m}(i)$, where $v_{i_1}^{\mu_1} \dots v_{i_m}^{\mu_m}(i)$ is the ith component of the vector $v_{i_1}^{\mu_1} \dots v_{i_m}^{\mu_m}$. Summing, we get that the coefficient at $x_{i_1}^{\mu_1} \dots x_{i_m}^{\mu_m}$ in the sum $\sum_{i=1}^s \alpha_i l_i^n$ is equal to $|v_{i_1}^{\mu_1} \dots v_{i_m}^{\mu_m}|$. It equals zero in all the cases except for $m = n$, where it is distinct from zero.

Prove that the vector $w_{2,\dots,n}$ is a linear combination of the vectors

$$v_{i_1}^{\mu_1} \dots v_{i_m}^{\mu_m},\ 1 = i_1 < \dots < i_m \leq n,\ m < n.$$

In this case, according to the equalities indicated above and the linear property $\left| \sum_{j=1}^m \lambda_j e_j \right| = \sum_{j=1}^m \lambda_j |e_j|$, we obtain $|w_{2,\dots,n}| = 0$, which leads to contradiction and proves the theorem.

It remains to prove the existence of a linear combination possessing this property. To do that, consider two possible cases. Let all the vectors $w_{i_1,\dots,i_m} \in F^s$, where $m < n-1$, be linearly independent. In this case their number satisfies the inequality $2^{n-1} - 1 \geq s$, therefore, these vectors form a basis in the space F^s and we actually have $2^{n-1} - 1 = s$ and the vector $w_{2,\dots,n}$ is their linear combination, which was required.

We have to consider the second (more complicated) case where the set of vectors $w_{i_1,\dots,i_m}$, $m < n-1$, is linearly dependent. Take their nontrivial linear combination equal to the zero vector. We can consider only the vectors with nonzero factors λ_j in it. Select the vector $w_{j_1,\dots,j_m}$ with the maximal $m = M < n-1$ (or one of such vectors) from them. It can be represented as a linear combination of other vectors of the form $w_{i_1,\dots,i_m}$, $m \le M$. If the ith coordinate of the vector v_1 is equal to zero, $v_1(i) = 0$, then the ith coordinates of all considered vectors are also equal to zero. Remove such coordinates from those vectors. The vector $w'_{j_1,\dots,j_M}$ shortened this way can be represented through the shortened vectors $w'_{i_1,\dots,i_m}$, $m \le M$, as the linear combination with the same coefficients. Dividing each jth component in the considered vectors by $v_1^{n-M}(j) \ne 0$, we obtain the vectors $w''_{i_1,\dots,i_m}$, $m \le M$, whose components are expressed as

$$v_1^{M-m}(j)v_{i_1}(j)\dots v_{i_m}(j).$$

The vector $w''_{j_1,\dots,j_M}$ is expressed through the vectors $w''_{i_1,\dots,i_m}$, $m \le M$, as the linear combination with the same coefficients. Restore removed zero components in each of these vectors. Denote the vectors of dimension s obtained this way by $w''_{i_1,\dots,i_m}, m \le M$, as before. The vector $w''_{j_1,\dots,j_M}$ is expressed through the vectors $w''_{i_1,\dots,i_m}$, $m \le M$, as the linear combination with the same coefficients. Consider the set of numbers $1 = k_1 < \dots < k_{n-M}$ not equal to any number $j_1, \dots, j_M$. Multiply all the vectors $w''_{i_1,\dots,i_m}$, $m \le M$, by the vector $v_{k_1}\dots v_{k_{n-M}}$. We get the vector

$$v_{k_1}\dots v_{k_{n-M}}w''_{j_1,\dots,j_M} = v_1\dots v_n = w_{2,\dots,n}$$

and the vectors (distinct from it)

$$v_{k_1}\dots v_{k_{n-M}}w''_{i_1,\dots,i_m} = v_{i_1}^{\mu_1}\dots v_{i_t}^{\mu_t},\ i_1 = 1,\ t < n.$$

This vector $w_{2,\dots,n}$ is expressed through the vectors indicated here as the linear combination with the same coefficients. Therefore, we have also constructed the required linear combination in the second case considered here. As above, its existence implies a contradiction. The theorem is proved.

I. S. Sergeev noted that we have actually proved that the number of occurrences of symbols of a given variable in the formula

$$x_1\dots x_n = l_1^n + \dots + l_m^n, \quad l_i = l_i(x_1,\dots,x_n) = \sum_{j=1}^{n} a_{i,j}x_j$$

is not less than 2^{n-1}, which implies that the complexity of a formula of such form is not less than $2^{n-1}n$ and all these bounds are attainable. The assertion formulated above is in some sense an analogue of the theorem that the complexity of realization of the linear Boolean function $x_1 \oplus \dots \oplus x_n$ by disjunctive normal forms (DNF) is equal to $2^{n-1}n$, and the number of conjunctions in the shortest DNF for this linear function is equal to 2^{n-1}. The analogy becomes more explicit if we notice that for $x_i = \pm 1$ one can represent x_i in the form $(-1)^{y_i}$, $y_i \in \{0,1\}$, and then

$$x_1\dots x_n = (-1)^{y_1\oplus\dots\oplus y_n}.$$

Give some further remarks. In the case of fields with the characteristic comparatively small with respect to n, the identity $x_1\dots x_n = l_1^n + \dots + l_s^n$, where l_i are linear polynomials, may not exist (for example, for n equal to the order of field).

It is interesting to solve a similar problem for an arbitrary monomial, arbitrary homogeneous polynomial, and an arbitrary polynomial in general, for example, over a field of characteristic zero. It is obvious that any monomial of degree n of m variables can be represented for any $d \ge n$ as a sum of linear combinations of not more than 2^{d-1} affine forms raised to the power d. This implies that any homogeneous polynomial of degree n of m variables is representable in the form of linear combination of not more than $2^{n-1}\binom{n+m-1}{n}$ linear forms raised to the power n. The estimate for the number of linear forms can be improved if we notice, for example, that $x_1^2\dots x_{n/2}^2$ can be represented as a linear combination of $(3^{n/2-1}-1)/2$ linear forms $x_1 \pm x_1 \pm x_2 \pm x_2 \pm \dots \pm x_{n/2} \pm x_{n/2}$ raised to the power n. For example,

$$(x_1x_2)^2 = (1/12)((x_1+x_2)^4 + (x_1-x_2)^4 - 2x_1^4 - 2x_2^4).$$

It was shown in [9] (see also [10]) that such representation consisting of $(n+1)^m$ linear forms exists. In [11], another proof of the same estimate was given (the problem was presented in a student mathematical contest without a requirement to obtain the bound for the number of summands).

For $m = \Omega(n)$ the bound $2^{n-1}\binom{n+m-1}{n}$ is better, and for small m the bound $(n+1)^m$ is better.

For $n = 2$ this problem coincides with the problem of representation of a quadratic form of m variables as a sum of squares. As is known, the number of summands in such representation is not greater than m and this bound is attainable.

For $m = 1$ it is easy to prove that any polynomial of degree n of a single variable x can be represented as a linear combination of binomials $(x + k)^n$, $k = 0, 1, \ldots, n$. It is sufficient to notice that the difference of kth order for the monomial x^n equal to

$$x^n - \binom{k}{1}(x+1)^n + \ldots + (-1)^k(x+k)^n$$

is a polynomial of degree $n - k$, in particular, the constant $n!$ (and any constant) is representable as a linear combination of binomials $(x + k)^n$, $k = 0, 1, \ldots, n$, therefore, any polynomial of the first degree is representable in the form of a linear combination of those binomials, any polynomial of the second degree is also representable, etc., i.e., the linear space of polynomials of degree n has the basis $(x+k)^n$, $k = 0, 1, \ldots, n$.

Since the representation

$$f(x) = \sum_{i=1}^{s}(a_i x + b_i)^n$$

contains $2s$ parameters a_i, b_i and the polynomial $f(x)$ is determined by $n+1$ coefficients, then for $2s < n+1$ the representation in the form indicated above exists only for polynomials with coefficients from $\mathbb{R}$ forming a set of zero measure in the space of all polynomials of degree n over $\mathbb{R}$. Therefore, the lower bound for s is $(n+1)/2$ in this case. For odd n Sylvester proved in XIXth century (see [10]) that for almost all polynomials $f(x)$ of degree n there exists a representation in the form of a linear combination

$$f(x) = \sum_{i=1}^{(n+1)/2} a_i(x + b_i)^n,$$

and there exist polynomials having the minimal number of summands $s > (n + 1)/2$ in such representation.

All the problems considered here are of certain interest in the case of finite fields.

Note in conclusion that the classic problem of the number theory on representation of a natural number as a sum of minimal number of powers of natural numbers and its variants (Waring's problem) has a similar formulation.

ACKNOWLEDGMENTS

The work was supported by the Russian Foundation for Basic Research (projects no. 11–01–00508, 11–01–00792a).

REFERENCES

1. S. B. Gashkov, "A Method for Calculation of Lower Bounds for the Complexity of Monotone Calculation of Polynomials," Vestn. Mosk. Univ., Matem. Mekhan., No. 5, 7 (1987).
2. S. B. Gashkov, "Complexity of Calculation of Certain Classes of Polynomials of Several Variables," Vestn. Mosk. Univ., Matem. Mekhan., No. 1, 89 (1988).
3. S. B. Gashkov, "Parallel Calculation of Certain Classes of Polynomials with the Growing Number of Variables," Vestn. Mosk. Univ., Matem. Mekhan., No. 2, 88 (1990).
4. S. V. Yablonskii, "Realization of a Linear Function in the Class of Π-Circuits," Doklady Akad. Nauk SSSR **94** (5), 805 (1954).
5. V. M. Khrapchenko. "Complexity of Realization of a Linear Function in the Class of Π-Circuits," Matem. Zametki **10** (1), 83 (1971).
6. X. Chen, N. Kayal, and A. Wigderson, "Partial Derivatives in Arithmetic Complexity," Foundations and Trends in Theoretical Computer Science **6** (1, 2), 2010.
7. N Kayal, "An Exponential Lower Bound for the Sum of Powers of Bounded Degree Polynomials," in *Electronic Colloquium on Computational Complexity*, Report 81, 2012.
8. I. Fisher, "Sums of Like Powers of Multivariant Linear Forms," Math. Mag. **67** (1), 59 (1994).
9. H. Sonnenschein, "A Representation for Polynomials in Several Variables," Amer. Math. Monthly **78** (1), 45 (1971).
10. V. V. Prasolov, *Polynomials* (MCCME, Moscow, 2000) [in Russian].
11. *Student's Mathematical Competitions in Algebra in Mathematical and Mechanical Department of MSU in 2006–2011* (MCCME, Moscow, 2012) [in Russian].

Translated by V. Valedinskii