On some arithmetic properties of polynomial expressions involving Stirling numbers of the second kind

Martin Klazar
Department of Applied Mathematics (KAM)
and Institute for Theoretical Computer Science (ITI)[1]
Charles University
Malostranské náměstí 25
118 00 Praha
Czech Republic
klazar@kam.ms.mff.cuni.cz

and

Florian Luca
Mathematical Institute, UNAM
Ap. Postal 61-3 (Xangari) CP 58 089
Morelia, Michoacán
Mexico
fluca@matmor.unam.mx

2000 MSC: Primary 11B73; Secondary 11D61.

Abstract

Let $S(n,k)$ be the clasical Stirling numbers of the second kind, $d>1$ be an integer, and $P,Q,R \in \mathbf{Q}[X_1,\ldots,X_m]$ be nonconstant polynomials such that P does not divide Q and R is not a dth power. We prove that if $k_1,\ldots,k_m$ are any sufficiently large distinct positive integers then, setting $S_i = S(n,k_i)$, $\frac{Q(S_1,\ldots,S_m)}{P(S_1,\ldots,S_m)} \in \mathbf{Z}$ for only finitely many $n \in \mathbf{N}$ and $R(S_1,\ldots,S_m) = x^d$ for only finitely many pairs $(n,x) \in \mathbf{N}^2$. We extend the latter finiteness result to all triples $(n,x,d) \in \mathbf{N}^3$, $d>1$. Our proofs are based on the results of Corvaja and Zanier. We give similar but more particular results on the more general Stirling-like numbers $T(n,k)$.

[1]Supported by the project LN00A056 of the Ministery of Education of the Czech Republic.

1 Introduction

Stirling numbers of the second kind $S(n,k)$, where $k,n \in \mathbf{N} = \{1,2,\ldots\}$, count partitions of the set $[n] = \{1,2,\ldots,n\}$ into k nonempty disjoint sets. For example, $S(n,1) = 1$ and $S(n,2) = 2^{n-1} - 1$ for every $n \in \mathbf{N}$. More generally,

$$S(n,k) = \sum_{i=1}^{k} \frac{(-1)^{k-i}}{(k-i)! \cdot i!} \cdot i^n. \tag{1}$$

The proof of this classical formula can be found, for example, in Stanley [21, p. 34]. For the sake of completeness we give a proof here. Let M be the set of all mappings from $[n]$ to $[k]$, N be the subset of all surjections among them, and N_i, $i = 1,\ldots,k$, be the subset of the mappings avoiding i in their image. On one hand, $|N| = k! \cdot S(n,k)$. On the other hand, $|N| = |M| - |N_1 \cup \ldots \cup N_k| = k^n - |N_1 \cup \ldots \cup N_k|$. Formula (1) follows by equating both expressions for $|N|$ and expanding $|N_1 \cup \ldots \cup N_k|$ by the inclusion-exclusion principle.

$S(n,k)$ belong to the most popular combinatorial numbers and as such are subject of many articles. A small sample is [3, 4, 6, 13, 14, 18, 22, 23]. Here we are inspired by the following questions. For a fixed $k \in \mathbf{N}$, are there infinitely many squares in the sequence $(S(n,k))_{n\geq 1}$? What about higher powers? And what about taking instead of $S(n,k)$ a polynomial expression in it or in several Stirling numbers $S(n,k_1), S(n,k_2),\ldots,S(n,k_m)$? The only results known to us dealing with these or related diophantine problems on $S(n,k)$ were obtained by Brindza and Pintér [5] and Pintér [16, 17]. We review them briefly and then summarize our theorems. The main tool that we use is the results of Corvaja and Zannier [7] which are described in section 2. New results follow in sections 3 and 4.

Pintér proved in [16] that for any fixed $a \in \mathbf{N}$, if $S(n, n-a)$ is an m-th power, $m \geq 3$, then $n < C$ where $C = C(a)$ is an effectively computable constant. He proved also an analogous result for the equation $S(n, n-a) \in S$ where S is the set of positive integers composed only of primes from a fixed finite set. In [17] he proved that for all fixed integers $1 < a < b$ the solutions of the equation $S(m,a) = S(n,b)$ satisfy $\max(m,n) < Cb(\log b)^3 \log(b!/a!) \log a$ where C is an efectively computable absolute constant. Brindza and Pintér [5] considered equations $S(x, x-a) = by^z$ and $S(x,a) = by^z$ with parameters $a,b \in \mathbf{N}$ and unknowns $x,y,z \in \mathbf{N}$. As for the first equation, they proved that if (x,y,z) is a solution with $x > 2b16^a a^{8a}$ and $y > 1$, then $z(7.5 + \log z)^{-2} < 11000(\log b + 8a \log a + 3a)$. (The same bound is proved also for Stirling numbers of the first kind $s(n,k)$ which count the permutations of $1,2,\ldots,n$ with k cycles.) Further, if $z \geq 3$ is fixed or $z = 2$ and $a \neq 1,3$, then $\max(x,y)$ can be effectively bounded in terms of a and b. As for the second equation, they proved that in all solutions (x,y,z) with $y>1$ (also $a>1$) z is bounded by a constant that is effectively computable in terms of a and b. The main tool used in all these results is the theory of linear forms in logarithms.

Our main results are four theorems in section 4. Theorem 4.4 and Corollary 4.5 state, roughly speaking, that if $P \in \mathbf{Q}[Y_1,\ldots,Y_m]$ is a nonconstant polynomial and $k_1,\ldots,k_m \in \mathbf{N}$ are distinct and sufficiently large, then $P(S(n,k_1),\ldots,S(n,k_m))$ is far from vanishing when n runs through $\mathbf{N}$. Theorem 4.6 says that if $P,Q \in \mathbf{Q}[Y_1,\ldots,Y_m]$ are two polynomials such that P does not divide Q and $k_1,\ldots,k_m \in \mathbf{N}$ are distinct and sufficiently large, then $\frac{Q(S(n,k_1),\ldots,S(n,k_m))}{P(S(n,k_1),\ldots,S(n,k_m))} \in \mathbf{Z}$ for only finitely many $n \in \mathbf{N}$. Theorem 4.8 says that for every integer $d>1$ and every polynomial $P \in \mathbf{Q}[Y_1,\ldots,Y_m]$ that is not a dth power in $\mathbf{Q}[Y_1,\ldots,Y_m]$, the diophantine equation $P(S(n,k_1),\ldots,S(n,k_m)) = y^d$ has only finitely many solutions $(n,y) \in \mathbf{N}^2$ (provided the fixed $k_1,\ldots,k_m \in \mathbf{N}$ are distinct and sufficiently large). Theorem 4.9 extends this finiteness result to all triples $(n,y,d) \in \mathbf{N}^3$, $d>1$.

The proofs of our theorems are based on two ingredients. The first one is the Corvaja–Zanier theory of formal exponentials explained in section 2 and the second one is our Propositions 4.1 and 4.3. (The proof of Theorem 4.9 uses also some bounds from the theory of linear forms in logarithms.) Proposition 4.1, the algebraic core of our argument, proves that certain polynomial systems $\{P_i \in \mathbf{C}[X_1,\ldots,X_m] :\ i=1,\ldots,m\}$ are invertible. Proposition 4.3 shows that systems $\{S(n,k_i) :\ i=1,\ldots,m\}$ can be reduced, restricting to appropriate sets of primes, to such polynomial systems. To obtain these sets we apply bounds on numbers of primes in short intervals.

In section 3, we give two simple and more particular applications of the Corvaja–Zanier theory. Let $T(n,k)=\sum_{i=1}^{k} t(k,i)i^n$ where $t(k,i) \in \mathbf{Q}$, $k,n \in \mathbf{N}$, are some constants which are always nonzero. Theorem 3.1 states that for every fixed $1<k_1<k_2$ one has $\frac{T(n,k_2)}{T(n,k_1)} \in \mathbf{Z}$ for only finitely many $n \in \mathbf{N}$. Theorem 3.2 states that if $d>1$ is an integer, $M \in \mathbf{Q}[Y_1,\ldots,Y_m]$ is a monic monomial that is not a dth power in $\mathbf{Q}[Y_1,\ldots,Y_m]$, and $k_1,\ldots,k_m \in \mathbf{N}$ are distinct numbers larger than 1, then the diophantine equation $M(S(n,k_1),\ldots,S(n,k_m)) = y^d$ has only finitely many solutions $(n,y) \in \mathbf{N}^2$. The proofs are straightforward applications of the results in section 2 and avoid the technicalities of section 4.

Some notation: $\mathbf{N}=\{1,2,\ldots\}$ are positive integers, $\mathbf{Z}$ is the set of all integers, $\mathbf{Q}$ are rational numbers, $\mathbf{C}$ are complex numbers, if $m \in \mathbf{N}$ then $[m]=\{1,2,\ldots,m\}$, and $\mathcal{P}=\{2,3,5,7,11,\ldots\}$ is the set of prime numbers.

2 The results of Corvaja and Zannier

We explain the results of Corvaja and Zannier [7] which we apply in sections 3 and 4. Let $\mathcal{E}$ be the set of all finite rational linear combinations

$$\alpha = \alpha(\nu) = \sum_{i=1}^{k} c_i a_i^\nu \tag{2}$$

where the $c_i \in \mathbf{Q}$ are all nonzero, $a_1 > a_2 > \ldots > a_k > 0$ are distinct positive integers, $k \geq 0$ (the empty sum being 0), and ν is a *formal* variable. The integers a_i are the *roots* of α, the rationals c_i are its *coefficients*, and k is its *rank*. $\mathcal{E}$ is, with the obvious addition and multiplication, a commutative integral domain with 1 which extends the field $\mathbf{Q}$. One more operation will be of importance. The substitutions $\nu := e + d\nu$, where $e, d, \in \mathbf{Z}$ and $d > 0$, act on $\mathcal{E}$ by transforming $c \cdot a^\nu$ to $ca^e \cdot (a^d)^\nu$. For example,

$$\text{if } \ \alpha(\nu) = \tfrac{1}{3}4^\nu - 3^\nu + \tfrac{7}{6}1^\nu \ \text{ then } \ \alpha(2\nu - 1) = \tfrac{1}{12}16^\nu - \tfrac{1}{3}9^\nu + \tfrac{7}{6}1^\nu.$$

One can turn α into a function $\alpha : \mathbf{N} \to \mathbf{Q}$ by substituting positive integers $n \in \mathbf{N}$ for ν. It is clear that two different $\alpha_1, \alpha_2 \in \mathcal{E}$ produce two different functions; one has even $\alpha_1(n) > \alpha_2(n)$ or vice versa for all $n > n_0$. Thus one can view $\mathcal{E}$ in two ways, as a ring of rational linear combinations of formal exponentials or as a ring of particular functions from $\mathbf{N}$ to $\mathbf{Q}$.

The following result is Theorem 1 of [7].

Proposition 2.1 *If $\alpha, \beta \in \mathcal{E}$ are such that $\alpha(n)/\beta(n) \in \mathbf{Z}$ for infinitely many $n \in \mathbf{N}$, then there is a $\gamma \in \mathcal{E}$ such that*

$$\alpha = \beta \cdot \gamma. \tag{3}$$

The following result is Corollary 1 of Theorem 2 in [7].

Proposition 2.2 *If $\alpha \in \mathcal{E}$, $d > 1$ is an integer, and $\alpha(n) = x^d$ has infinitely many solutions $(n, x) \in \mathbf{N}^2$, then there is an integer $e \in \{0, 1, \ldots, d-1\}$ and an element $\beta \in \mathcal{E}$ such that*

$$\alpha(e + d\nu) = \beta(\nu)^d. \tag{4}$$

The following result is a part of Corollary 2 of Theorem 3 in [7]; in [7] a stronger approximation result is given.

Proposition 2.3 *Suppose that $\alpha \in \mathcal{E}$ has rank at least 2 and its two leading roots $a_1 > a_2$ are coprime. Then, for every fixed integer $d > 1$, the equation $\alpha(n) = x^d$ has only finitely many solutions $(n, x) \in \mathbf{N}^2$.*

This is a consequence of Proposition 2.2. Indeed, suppose that there are infinitely many solutions. Then (4) holds. So $\beta(\nu)$ has rank at least 2 as well. If $b_1 > b_2$ are the two leading roots of $\beta(\nu)$, then $\beta(\nu)^d$ has two leading roots $b_1^d > b_1^{d-1}b_2$ with the gcd at least $b_1^{d-1} \geq b_1 \geq 2$. On the other hand, the two leading roots of $\alpha(e+d\nu)$ are $a_1^d > a_2^d$ and are coprime. Hence (4) cannot hold, which is a contradiction.

The simple criterion of Proposition 2.3 answers the question about perfect powers in $(S(n,k))_{n\geq 1}$. By (1), for $k \geq 2$ the two leading roots of $S(\nu,k)$ are the coprime numbers $k > k-1$. So, $S(n,k) = x^d$ has for fixed $k, d \geq 2$ only finitely many solutions $(n,x) \in \mathbf{N}^2$. Combining this with the result of Brindza and Pintér [5] (see the previous section) we obtain that for every fixed $k \geq 2$ the equation $S(n,k) = x^d$ has only finitely many solutions $(n,x,d) \in \mathbf{N}^3$ with $x, d > 1$.

There is yet the third way of looking at the ring $\mathcal{E}$, which was employed in Luca and Walsh [15]. $\mathcal{E}$ is isomorphic to the ring $\mathbf{Q}[X_p : p \in \mathcal{P}]$ of rational polynomials in countably many variables indexed by the prime numbers $p \in \mathcal{P}$. We define the isomorphism ψ first on p^ν, $p \in \mathcal{P}$, by $\psi(p^\nu) = X_p$ and on 1^ν by $\psi(1^\nu) = 1$. Then we extend ψ multiplicatively and additively. For example,

$$\psi(-\tfrac{7}{90}\cdot 24^\nu + 10^\nu + 5\cdot 9^\nu - 10\cdot 1^\nu) = -\tfrac{7}{90}X_2^3X_3 + X_2X_5 + 5X_3^2 - 10.$$

So, for $i \in \mathbf{N}$, $\psi(i^\nu) = \prod_{p\backslash i} X_p^{m_p(i)}$ where $m_p(i)$ is the exponent of p in the prime decomposition of i. Our main idea is to show that relations of type (3) or (4) are impossible by interpreting them via ψ as polynomial identities.

3 Two results for Stirling-like numbers

In the proofs of the next two theorems we need the well-known *Bertrand's postulate*. It asserts that for every $n \in \mathbf{N}$, $n \geq 2$, the interval $(n/2, n]$ contains at least one prime number. A simple proof was given by Erdős [8]. A nice presentation of this proof is in Aigner and Ziegler [1, pp. 7–12]. The "Stirling-like" numbers $T(n,k)$ are given by

$$T(n,k) = \sum_{i=1}^{k} t(k,i)i^n$$

where $t(k,i) \in \mathbf{Q}$ are fixed constants which for $i,k \in \mathbf{N}, 1 \leq i \leq k$, are never zero.

Theorem 3.1 *For every two fixed integers k_1 and k_2, $1 < k_1 < k_2$,*

$$\frac{T(n,k_2)}{T(n,k_1)} \in \mathbf{Z}$$

holds for only finitely many $n \in \mathbf{N}$.

Proof. Suppose, for the contradiction, that this holds for infinitely many $n \in \mathbf{N}$. By Proposition 2.1, we have in $\mathcal{E}$ the identity

$$T(\nu, k_2) = T(\nu, k_1) \cdot \gamma \tag{5}$$

for a nonzero $\gamma \in \mathcal{E}$. Hence $k_2 = ak_1$ where $a \in \mathbf{N}$ is the leading root of γ. Since $k_2 > k_1$, we have that $k_2 \geq 2k_1$. Then, by Bertrand's postulate, there is a prime number p such that $k_2 \geq p > k_1$. By (5),

$$A = B \cdot C$$

where $A = \psi(T(\nu, k_2))$, $B = \psi(T(\nu, k_1))$, and $C = \psi(\gamma)$ are polynomials from $\mathbf{Q}[X_p : \ p \in \mathcal{P}]$. The variable X_p does not appear in B but it appears exactly once in A, in the monomial $t(k_2, p)X_p$ (remember that all $t(k, i)$ are nonzero). Since $k_1 > 1$, B is a nonconstant polynomial. If X_p does not appear in C, the identity is patently impossible. If X_p appears in C, it is impossible also because then $B \cdot C$ has at least one monomial of the type DX_p, where D is a nonconstant monomial in the variables distinct from X_p, but A contains no such monomial. We have a contradiction. $\Box$

Theorem 3.2 *Suppose $d > 1$ is an integer, $a_1, \ldots, a_m \in \mathbf{N}$ are m positive integers, not all divisible by d, and $1 < k_1 < k_2 < \ldots < k_m$ are m distinct integers. Then the diophantine equation*

$$T(n, k_1)^{a_1} T(n, k_2)^{a_2} \ldots T(n, k_m)^{a_m} = x^d \tag{6}$$

has only finitely many solutions $(n, x) \in \mathbf{N}^2$.

Proof. Without loss of generality we can assume that no exponent a_i in (6) is divisible by d. We fix an m-tuple $1 < k_1 < \ldots < k_m$ of distinct integers and an m-tuple of positive integers $a_1, \ldots, a_m$ none of which is divisible by $d > 1$, and assume that

$$M(T(n, k_1), \ldots, T(n, k_m)) = T(n, k_1)^{a_1} \ldots T(n, k_m)^{a_m} = x^d$$

has infinitely many solutions $(n, x) \in \mathbf{N}^2$. We show that this leads to a contradiction.

By Proposition 2.2,

$$M(T(e + d\nu, k_1), \ldots, T(e + d\nu, k_m)) = \gamma^d$$

for some $e \in \{0, 1, \dots, d-1\}$ and $\gamma \in \mathcal{E}$. Applying ψ, we obtain the identity

$$\prod_{j=1}^{m}\Big(\sum_{i=1}^{k_j} t(k_j, i) i^e X(i)^d\Big)^{a_j} = Q^d \tag{7}$$

where $X(i) = \prod_{p \backslash i} X_p^{m_p(i)}$ and $Q = \psi(\gamma) \in \mathbf{Q}[X_p :\ p \in \mathcal{P}]$. Let q be the maximum prime number in the interval $(k_m/2, k_m]$. By Bertrand's postulate, q exists. The variable X_q appears in each of the m factors in the left hand side of (7) at most once, possibly in the summand $t(k_j, q)q^e X(q)^d = t(k_j, q)q^e X_q^d$, and it does appear in the last mth factor. Distinguishing X_q and denoting $R = \mathbf{Q}[X_p :\ p \in \mathcal{P}\ \&\ p \neq q]$, we write (7) in the form

$$\prod_{j=1}^{m}\Big(t(k_j, q)q^e X_q^d + B_j\Big)^{a_j} = Q^d. \tag{8}$$

Here $t(k_j, q) = 0$ if $q > k_j$ and $t(k_m, q) \neq 0$, $B_j \in R$, and $Q \in R[X_q]$. Clearly, every B_j is nonzero and except for the case $k_{j_0} = q$ and $k_{j_0-1} = q-1$ when $B_{j_0} = B_{j_0-1}$, we have that if $j_1 > j_2$ then B_{j_1} has a monomial not contained in B_{j_2} (since all $t(k, i)$ are nonzero). Hence each two of the B_js with $k_j \geq q$ differ by more than a constant multiple. So we write (8) as

$$B\prod_{j=1}^{s}\Big(X_q^d + C_j\Big)^{b_j} = Q^d$$

where $B, C_j \in R$ are nonzero, $s \geq 1$, b_j are positive integers not divisible by d, and C_j are mutually distinct. This identity is impossible. The left hand side, taken as a polynomial in X_q, has $ds \geq 2$ distinct roots none of which has multiplicity divisible by d. On the other hand, each root of the right hand side (if any) has multiplicity divisible by d. We have obtained a contradiction. $\square$

The proof of Theorem 3.1 would sound more naturally in $\mathcal{E}$ than in $\mathbf{Q}[X_p :\ p \in \mathcal{P}]$ but the second proof shows clearly the advantage and necessity of polynomial formulation. We will see more polynomial arguments in the next section. Theorems 3.1 and 3.2 are not subsumed in Theorems 4.6 and 4.8 because the latter theorems deal with the particular quantities $S(n, k)$ instead of the general $T(n, k)$. Theorem 3.1 cannot be generalized much more towards Theorem 4.6 because for $T_0(n, k) = k^n + (k-1)^n + \cdots + 1^n$, $Q(X_1, \dots, X_4) = X_1 - X_2$, and $P(X_1, \dots, X_4) = X_3 - X_4$ one has

$$\frac{Q(T_0(2k, n), T_0(2k-1, n), T_0(k, n), T_0(k-1, n))}{P(T_0(2k, n), T_0(2k-1, n), T_0(k, n), T_0(k-1, n))} = 2^n \in \mathbf{Z}$$

for every $k, n \in \mathbf{N}$ although P does not divide Q. Similarly, $T_0(n, k)$ and $P(X_1, X_2) = X_1 - X_2$ show that the monomial M in Theorem 3.2 cannot be in general replaced by a sum of two monomials because $P(T_0(k, n), T_0(k-1, n)) = k^n$ and this is a dth power infinitely often for any $d > 1$ and $k \in \mathbf{N}$ although P is linear. In the next section we show that for Stirling numbers $S(n, k)$ such heavy cancelations do not occur.

4 Stirling numbers and general polynomials

A polynomial $P \in \mathbf{C}[X_1, \ldots, X_m]$ *depends* on X_i if $\frac{\partial P}{\partial X_i} \neq 0$. An *interval partition* $\mathcal{M}$ of $[m]$ is a partition $[m] = I_1 \cup I_2 \cup \ldots \cup I_s$ into disjoint nonempty intervals $I_1 < I_2 < \ldots < I_s$. A polynomial system $\{P_i \in \mathbf{C}[X_1, \ldots, X_m] : i = 1, \ldots, m\}$ is *$\mathcal{M}$-regular* if (i) for every k and $i \in I_k$ one has $P_i \in \mathbf{C}[X_j : j \in I_1 \cup \ldots \cup I_k]$, (ii) for every k and $i, j \in I_k$ the variable X_j appears in P_i only in the monomial $b_{i,j}X_j$ ($b_{i,j} \in \mathbf{C}$ is possibly zero), and (iii) the Jacobian $\det(\frac{\partial P_i}{\partial X_j})$ is a nonzero constant. We call the linear tail $\sum_{j \in I_k} b_{i,j}X_j$ of P_i, $i \in I_k$, the *linear part* of P_i.

Suppose $\{P_i : i = 1, \ldots, m\}$ is $\mathcal{M}$-regular. Then, by (i) and (ii), the Jacobi matrix $(\frac{\partial P_i}{\partial X_j})$ has a block lower triangular form with s blocks on the main diagonal (and zeros above the blocks) where the kth block is a square $|I_k| \times |I_k|$ matrix A_k of coefficients of the linear parts of the P_is, $i \in I_k$. The condition (iii) is equivalent to the fact that every A_k is regular because the Jacobian equals $\det(A_1) \cdot \ldots \cdot \det(A_s)$.

If the polynomials and their variables are indexed instead of $[m]$ by two arbitrary m-sets of integers M and N, we transfer the interval partition $\mathcal{M}$ of $[m]$ to M and N in the obvious way and work with $\mathcal{M}$-regular systems also in this more general situation.

Proposition 4.1 *Let $P \in \mathbf{C}[X_1, \ldots, X_m]$ be a nonconstant polynomial, $\mathcal{M}$ an interval partition of $[m]$ with parts $I_1 < \ldots < I_s$, and $\{P_i \in \mathbf{C}[X_1, \ldots, X_m] : i = 1, \ldots, m\}$ an $\mathcal{M}$-regular system of polynomials. Then the following holds.*

1. *There exist m polynomials $Q_1, \ldots, Q_m \in \mathbf{C}[X_1, \ldots, X_m]$ inverting the system $\{P_i : i = 1, \ldots, m\}$, that is, $P_i(Q_1, \ldots, Q_m) = X_i$ for every $i = 1, \ldots, m$.*

2. *The system $\{Q_i : i = 1, \ldots, m\}$ of 1 is $\mathcal{M}$-regular.*

3. *The polynomial $P(P_1, \ldots, P_m) \in \mathbf{C}[X_1, \ldots, X_m]$ is nonconstant.*

4. *If P depends on some variable X_j, $j \in I_s$, then $P(P_1, \ldots, P_m)$ depends also on some variable X_k, $k \in I_s$.*

Proof. Let P, $\mathcal{M}$, and $\{P_i : \; i = 1, \dots, m\}$ be as stated. For every $k = 1, \dots, s$ consider the linear system

$$\{\textstyle\sum_{j \in I_k} b_{i,j} X_j = Y_i - R_i : \; i \in I_k\}$$

in the unknowns X_j, $j \in I_k$, where the left hand sides are the linear parts of the P_is, $i \in I_k$, Y_i are new variables, and $R_i = P_i - \sum_{j \in I_k} b_{i,j} X_j \in \mathbf{C}[X_j : j \in I_1 \cup \ldots \cup I_{k-1}]$. The unique solution obtained by multiplying by A_k^{-1} is the polynomials $X_j = T_j(Y_j : \; j \in I_k; \; X_j : \; j \in I_1 \cup \ldots \cup I_{k-1})$, $j \in I_k$. The first $|I_1|$ polynomials T_j are linear and free of the X-variables. Substituting T_j for X_j, $j \in I_1$, in T_j with $j \in I_2$, we eliminate the X-variables in the next $|I_2|$ polynomials T_j. Continuing this way we eliminate from every T_j every X-variable and obtain some polynomials Q_j, $j = 1, \dots, m$, only in the Y-variables. It follows by elementary properties of matrix multiplication that $\{Q_j : \; j = 1, \dots, m\}$ indeed inverts $\{P_i : \; i = 1, \dots, m\}$.

The solution process in 1 gives the system $\{Q_i : \; i = 1, \dots, m\}$ the form prescribed in the conditions (i) and (ii) of regularity. The diagonal blocks of its Jacobi matrix are just the inverse matrices A_k^{-1}. Thus its Jacobian is nonzero and equals to the reciprocal of the Jacobian of $\{P_i : \; i = 1, \dots, m\}$. This proves 2.

The proof of 3 follows immediately from 1: If $P(P_1, \dots, P_m)$ were constant, then $P(P_1(Q_1, \dots, Q_m), \dots, P_m(Q_1, \dots, Q_m)) = P(X_1, \dots, X_m)$ would be constant as well.

As for 4, we show that for a specialization of the first $|I_1| + \cdots + |I_{s-1}|$ variables $P(P_1, \dots, P_m)$ becomes a nonconstant polynomial. We write P as a finite sum

$$P = \sum_M T_M \cdot M$$

where $M \in \mathbf{C}[X_j : \; j \in I_s]$ are distinct monic monomials and $T_M \in \mathbf{C}[X_j : j \in I_1 \cup \ldots \cup I_{s-1}]$. Since P depends on one of the last $|I_s|$ variables, there is a nonconstant M_0 with a nonzero T_{M_0}. By 3, $T^*_{M_0} = T_{M_0}(X_j := P_j : \; j \in I_1 \cup \ldots \cup I_{s-1})$ is a nonzero (but possibly constant) polynomial. We set $X_j := \alpha_j \in \mathbf{C}$, $j \in I_1 \cup \ldots \cup I_{s-1}$, so that $T^*_{M_0}$ becomes a nonzero constant. After this $P(X_j := P_j : \; j \in I_1 \cup \ldots \cup I_{s-1}; \; X_j : \; j \in I_s)$ becomes a nonconstant polynomial $P^* \in \mathbf{C}[X_j : \; j \in I_s]$ and $\{P_j : \; j \in I_s\}$ becomes an $\mathcal{N}$-regular system $\{P^*_j \in \mathbf{C}[X_j : \; j \in I_s] : \; j \in I_s\}$ where $\mathcal{N}$ consists of just one part I_s. Again by 3, $P(P_1, \dots, P_m)(X_j := \alpha_j : \; j \in I_1 \cup \ldots \cup I_{s-1}) = P^*(X_j := P^*_j : \; j \in I_s)$ is a nonconstant polynomial. $\square$

Claim 1 of the previous proposition is a particular (and rather trivial) case of the famous *Jacobian conjecture* which is still open. It states that for every system $\{P_i \in \mathbf{C}[X_1, \dots, X_m] : \; i = 1, \dots, m\}$ of polynomials whose Jacobian is a nonzero constant there exists the inverse system $\{Q_i \in \mathbf{C}[X_1, \ldots, X_m] : i = 1, \ldots, m\}$ such that $P_i(Q_1, \ldots, Q_m) = X_i$ for $i = 1, \ldots, m$. See, for example, [2, 9, 10, 11, 20].

Lemma 4.2 *Let $1 \leq k_1 < k_2 < \ldots < k_m$ be m distinct integers and*

$$D_m = D_m(X_1, X_2, \ldots, X_m) = \det\left(\prod_{k=1}^{k_m - k_i} (k_i + k - X_j) \right)_{i,j=1}^{m}$$

where for $i = m$ the product is defined as 1. Then for every $t \in \mathbf{N}$ and $A \subset \mathbf{C}$ with $|A| \geq m(k_m - k_1 + t)$ there exist t mutually disjoint m-tuples $(\alpha_{i,1}, \ldots, \alpha_{i,m}) \in A^m$ of elements of A, the elements in each m-uple being mutually distinct, such that $D_m(\alpha_{i,1}, \ldots, \alpha_{i,m}) \neq 0$ for every $i = 1, \ldots, t$,

Proof. D_m is a polynomial which has degree at most $d = k_m - k_1$ in every variable X_i. We show that D_m is not identically zero by proving by induction on m that actually $\deg_{X_1}(D_m) = d$ (by the symmetry, this holds for every variable). For $m = 1$ it is true because $D_1 = 1$. For $m > 1$ we expand D_m by the first row:

$$D_m = \prod_{k=1}^{k_m - k_1} (k_1 + k - X_1) \cdot E + \sum_{j=2}^{m} (-1)^{j+1} a_{1,j} M_{1,j}$$

where $E = D_{m-1}(X_2, \ldots, X_m)$ corresponds to the $(m-1)$-tuple $k_2, \ldots, k_m$, $a_{i,j}$ is the entry of the matrix defining D_m, and $M_{i,j}$ is the minor of $a_{i,j}$. The first term is of degree d in X_1 (by induction, E is a nonzero polynomial), $a_{1,j}$ are X_1-free, and $\deg_{X_1}(M_{1,j}) \leq k_m - k_2 < d$. Hence $\deg_{X_1}(D_m) = d$.

Now it suffices to prove that for every $A \subset \mathbf{C}$ with $|A| \geq m(d+1)$ we can select m distinct elements $\alpha_1, \ldots, \alpha_m \in A$ such that $D_m(\alpha_1, \ldots, \alpha_m) \neq 0$. Since D_m is a nonzero polynomial in m variables and of degree at most d in each, this follows by an easy induction on m using the basic fact that every nonzero $P \in \mathbf{C}[X]$, $\deg(P) \leq d$, has at most d roots. $\Box$

In the next proof we need a bound on the number of primes in the interval $(x - \Delta, x)$ stronger than Bertrand's postulate. We use the fact that there exists a real number θ, $0 < \theta < 1$, and constants $\kappa, x_0 > 0$ such that

$$\pi(x) - \pi(x - \Delta) > \frac{\kappa \Delta}{\log x} \tag{9}$$

whenever $x > x_0$ and $x^\theta < \Delta < x$. By the result of Iwaniecz and Pintz [12], this is true for every $\theta > \frac{23}{42}$. We can certainly fix θ to be $\frac{2}{3}$.

Proposition 4.3 *For every $m, t \in \mathbf{N}$ there is a constant $C = C(m,t) > 0$ such that the following holds. For every m distinct positive integers $C < k_1 < k_2 < \ldots < k_m$ there is an interval partition $\mathcal{M}$ of $[m]$ and t mutually disjoint m-sets of prime numbers $\mathcal{P}_1, \ldots, \mathcal{P}_t$ such that for every $k = 1, \ldots, t$ and every specialization $\{\alpha_p \in \mathbf{C} : \ p \in \mathcal{P}\}$ the system of m polynomials from $\mathbf{Q}[X_p : \ p \in \mathcal{P}_k]$*

$$\{\psi(S(\nu, k_i))(X_p := \alpha_p : \ p \notin \mathcal{P}_k) : \ i = 1, \ldots, m\}$$

is $\mathcal{M}$-regular.

Proof. First we fix an arbitrary decreasing sequence $\theta_1 > \theta_2 > \ldots$ of numbers in the interval $(\frac{2}{3}, 1)$. To be specific, we set

$$\theta_i = \frac{5}{3} - \frac{i+2}{i+3}.$$

So $(\theta_i)_{i \geq 1} = (\frac{11}{12}, \frac{13}{15}, \frac{5}{6}, \ldots)$. Let $m, t \in \mathbf{N}$ be given. We fix a sufficiently large constant $C = C(m,t) > 0$ meeting the following conditions, in which x_0 and κ are the constants of bound (9) corresponding to $\theta = \frac{2}{3}$.

$$\begin{aligned} C &> x_0, && (10) \\ k > C &\Rightarrow mk^{\theta_1} < \tfrac{1}{2}k, && (11) \\ k > C &\Rightarrow \frac{\kappa k^{\theta_i}}{\log k} > m(m(2k)^{\theta_{i+1}} + t) \text{ for every } i = 1, \ldots, m. && (12) \end{aligned}$$

Let $C < k_1 < k_2 < \ldots < k_m$ be m fixed integers. We take the set A, $1 \in A \subset [m]$, defined by

$$A = \{1\} \cup \{i \in [m] : \ i \geq 2 \ \& \ k_i - k_i^{\theta_i} \geq k_{i-1}\}.$$

A has $s \geq 1$ elements $1 = a_1 < a_2 < \ldots < a_s \leq m$. We define the interval partition $\mathcal{M}$ of $[m]$ by

$$\mathcal{M} = \{I_1, \ldots, I_s\} = \{[1, a_2 - 1], [a_2, a_3 - 1], \ldots, [a_{s-1}, a_s - 1], [a_s, m]\}$$

and set $a_{s+1} = m + 1$. For $j = 1, \ldots, s$ we define the interval

$$J_j = (k_{a_j} - k_{a_j}^{\theta_{a_j}}, k_{a_j}].$$

Clearly,

$$k_{a_j - 1} < J_j \leq k_{a_j}. \tag{13}$$

Let $K = k_{a_{j+1}-1} = \max\{k_i : \ i \in I_j\}$. By the definition of A,

$$k_{a_{j+1}-2} > K - K^{\theta_{a_{j+1}-1}} \geq K - K^{\theta_{a_j}}.$$

From this,

$$k_{a_{j+1}-3} > k_{a_{j+1}-2} - k_{a_{j+1}-2}^{\theta_{a_{j+1}-2}} \geq K - 2K^{\theta_{a_j}}$$

and so on. In the end,

$$k_{a_j} > K - (|I_j| - 1)K^{\theta_{a_j}} \geq K - (m-1)K^{\theta_{a_j}}.$$

From this and by (11),

$$K = k_{a_{j+1}-1} < 2k_{a_j} \tag{14}$$

and

$$k_{a_j} - k_{a_j}^{\theta_{a_j}} > K - mK^{\theta_{a_j}} > \tfrac{1}{2}K = \tfrac{1}{2}k_{a_{j+1}-1}.$$

We conclude that

$$J_j \subset (\tfrac{1}{2}k_i, k_i] \text{ for every } i \in I_j. \tag{15}$$

Let $j \in \mathbf{N}$, $1 \leq j \leq s$, be again arbitrary and fixed. Let $\mathcal{Q} \subset J_j$ be an $|I_j| = (a_{j+1} - a_j)$-element set of primes. By (15), for every $i \in I_j$ and $p \in \mathcal{Q}$ the variable X_p appears in $\psi(S(\nu, k_i))$ only in the linear term $\alpha_{i,p}X_p$. By (1), the matrix of coefficients A_j is

$$A_j = (\alpha_{i,p})_{i\in I_j,\, p\in\mathcal{Q}} = \left(\frac{(-1)^{k_i-p}}{(k_i-p)!\cdot p!}\right)_{i\in I_j,\, p\in\mathcal{Q}}.$$

Let again $K = k_{a_{j+1}-1}$. The determinant $\det A_j$ is nonzero if and only if $\det B_j$ is nonzero where the matrix B_j arises by multiplying every column p of A_j by $(-1)^p(K-p)!\cdot p!$ and every row k_i by $(-1)^{k_i}$. We have

$$B_j = \left(\prod_{k=1}^{K-k_i}(k_i + k - p)\right)_{i\in I_j,\, p\in\mathcal{Q}}.$$

Hence $\det A_j \neq 0$ if and only if the polynomial $D_{|I_j|}$ of the previous lemma, corresponding to the parameters $\{k_i : \ i \in I_j\}$, does not vanish on the ordered $|I_j|$-tuple of the elements of $\mathcal{Q}$. $D_{|I_j|}$ has in every variable degree $K - k_{a_j}$. By the definition of A and by (14),

$$\begin{aligned} K - k_{a_j} &= \sum_{r=1}^{a_{j+1}-a_j-1} k_{a_j+r} - k_{a_j+r-1} < \sum_{r=1}^{a_{j+1}-a_j-1} k_{a_j+r}^{\theta_{a_j+r}} \leq mK^{\theta_{a_j+1}} \\ &< m(2k_{a_j})^{\theta_{a_j+1}}. \end{aligned} \tag{16}$$

By (9) and (10),

$$|J_j \cap \mathcal{P}| > \frac{\kappa k_{a_j}^{\theta_{a_j}}}{\log(k_{a_j})}. \tag{17}$$

By (12), (16), and (17),

$$|J_j \cap \mathcal{P}| > m(K - k_{a_j} + t) \geq |I_j|(K - k_{a_j} + t).$$

Using the previous lemma, we select t mutually disjoint $|I_j|$-sets of primes $\mathcal{Q}_{1,j} \subset J_j, \ldots, \mathcal{Q}_{t,j} \subset J_j$ such that for every $\mathcal{Q}_{i,j}$, $1 \leq i \leq t$, the corresponding matrix of coefficients A_j is regular. We define, for $i = 1, \ldots, t$, the desired m-element sets of primes as

$$\mathcal{P}_i = \bigcup_{j=1}^{s} \mathcal{Q}_{i,j}.$$

By the selection of the $\mathcal{Q}_{i,j}$s and by (13), these sets are disjoint. Let $\{\alpha_p \in \mathbf{C} : \ p \in \mathcal{P}\}$ be any fixed specialization. By (13) and (15), for every $k = 1, \ldots, t$ the Jacobi matrix of $\{\psi(S(\nu, k_i))(X_p := \alpha_p : \ p \notin \mathcal{P}_k) : \ i = 1, \ldots, m\}$ satisfies conditions (i) and (ii) of $\mathcal{M}$-regularity. It has nonzero Jacobian because of the selection of the $\mathcal{Q}_{i,j}$s. The proposition is proved. $\square$

Note that we prove more than it is stated (and we will need this): By (15), if $p \in \mathcal{P}_k$ belongs to the last part of $\mathcal{M}$, that is $p \in \mathcal{Q}_{k,s}$, then X_p appears in every $\psi(S(\nu, k_i))$ (in all variables $\{X_p : \ p \in \mathcal{P}\}$) only in the linear term bX_p.

Theorem 4.4 *Let $P \in \mathbf{Q}[Y_1, \ldots, Y_m]$ be a nonconstant polynomial and $t \in \mathbf{N}$ a number. There exists a constant $C = C(m, t) > 0$ such that if $C < k_1 < k_2 < \ldots < k_m$ are m distinct integers, then the polynomial*

$$P(\psi(S(\nu, k_1)), \ldots, \psi(S(\nu, k_m)))$$

depends on at least t variables.

Proof. This follows immediately by combining 3 of Proposition 4.1 and Proposition 4.3. $\square$

We have the following corollary in terms of numbers.

Corollary 4.5 *Let $\theta > \frac{23}{42}$ and $P \in \mathbf{Q}[Y_1, \ldots, Y_m]$ be a nonconstant polynomial. There exists a constant $C = C(m, \theta) > 0$ such that if $C < k_1 < k_2 < \ldots < k_m$ are m distinct integers, then*

$$|P(S(n, k_1), \ldots, S(n, k_m))| > (k_1 - k_1^{\theta})^n$$

for every $n \geq n_0$.

Proof. We can use in the proof of Proposition 4.3 a decreasing sequence $(\theta_i)_{i\geq 1}$ in the interval $(\frac{23}{42}, 1)$ such that $\theta_1 = \theta$. Then we set C to be $C(m, 1)$ of the previous theorem. By this theorem and by the proof of Proposition 4.3, the polynomial

$$Q = P(\psi(S(\nu, k_1)), \dots, \psi(S(\nu, k_m)))$$

has a monomial (with nonzero coefficient) containing a power X_p^s such that $s \geq 1$ and $p > k_1 - k_1^\theta$. Thus the leading root $a \in \mathbf{N}$ of $\psi^{-1}(Q) = ca^\nu + \cdots$, $c \in \mathbf{Q}$ is nonzero, satisfies $a \geq p > k_1 - k_1^\theta$ and the corollary follows. $\square$

Theorem 4.6 *Let $P, Q \in \mathbf{Q}[Y_1, \dots, Y_m]$ be two polynomials such that P does not divide Q. There exists a constant $C = C(m) > 0$ depending only on m such that if $C < k_1 < \ldots < k_m$ are m distinct integers, then*

$$\frac{Q(S(n, k_1), \dots, S(n, k_m))}{P(S(n, k_1), \dots, S(n, k_m))} \in \mathbf{Z}$$

for only finitely many $n \in \mathbf{N}$.

Proof. We set the constant C to be $C(m, 1)$ of Proposition 4.3. We prove the contraposition of the implication. Suppose that $C < k_1 < \ldots < k_m$ are fixed and $\frac{Q(S(n,k_1),\dots,S(n,k_m))}{P(S(n,k_1),\dots,S(n,k_m))} \in \mathbf{Z}$ for infinitely many $n \in \mathbf{N}$. By Proposition 2.1, we have in $\mathbf{Q}[X_p : \ p \in \mathcal{P}]$ the identity

$$\psi(Q(S(\nu, k_1), \dots, S(\nu, k_m))) = \psi(P(S(\nu, k_1), \dots, S(\nu, k_m))) \cdot T$$

for some polynomial T. Let $\mathcal{P}_1$ be the m-set of primes ensured by Proposition 4.3, with elements $p_1 < \ldots < p_m$. Setting all X_p, $p \notin \mathcal{P}_1$, equal to zero we obtain the identity

$$Q(S_1^*, \dots, S_m^*) = P(S_1^*, \dots, S_m^*) \cdot T^*$$

where $S_i^* = \psi(S(\nu, k_i))(X_p = 0 : \ p \notin \mathcal{P}_1)$, $i = 1, \dots, m$, and T^* are polynomials from $\mathbf{Q}[X_p : \ p \in \mathcal{P}_1]$. Substituting for X_p, $p \in \mathcal{P}_1$, the polynomial $Q_p(Y_p : \ p \in \mathcal{P}_1)$ ensured by 1 of Proposition 4.1 and Proposition 4.3, we obtain the identity

$$Q(Y_{p_1}, \dots, Y_{p_m}) = P(Y_{p_1}, \dots, Y_{p_m}) \cdot T^{**}.$$

Hence P divides Q. $\square$

To prove the next theorem we need a simple lemma.

Lemma 4.7 *Let K be an integral domain of characteristic 0, $g, d \in \mathbf{N}$ be two numbers, and let $P \in K[X]$ satisfy*

$$P^g \in K[X^d].$$

Then $P = X^s Q(X^d)$ for some integer $s \geq 0$ and a polynomial $Q \in K[X]$.

Proof. We write $P = X^s Q$ where $c = Q(0) \neq 0$. From $P^g \in K[X^d]$ it follows that d divides gs and $Q^g \in K[X^d]$. Suppose, for the contradiction, that $Q \notin K[X^d]$. Let $m > 0$ be the smallest integer not divisible by d for which X^m has in Q a nonzero coefficient f. It is easy to see that the coefficient of X^m in Q^g is

$$gc^{g-1} f \neq 0.$$

This contradicts the assumption $Q^g \in K[X^d]$. $\square$

Theorem 4.8 *Let $d \in \mathbf{N}$, $d > 1$, and $P \in \mathbf{Q}[Y_1, \ldots, Y_m]$ be a polynomial which is not a dth power in $\mathbf{Q}[Y_1, \ldots, Y_m]$. There is a constant $C = C(m, \deg(P))$ depending only on m and the degree of P such that if $C < k_1 < \ldots < k_m$ are m distinct numbers, then the diophantine equation*

$$P(S(n, k_1), \ldots, S(n, k_m)) = y^d$$

admits only finitely many solutions $(n, y) \in \mathbf{N}^2$.

Proof. We can assume that P depends on all variables $Y_1, \ldots, Y_m$ and that if Q^d divides P for some $Q \in \mathbf{Q}[Y_1, \ldots, Y_m]$ then Q is constant. We set $t = \deg(P) + 1$ and C to be $C(m, \deg(P) + 1)$ of Proposition 4.3. Suppose that $C < k_1 < \ldots < k_m$ are fixed and $P(S(n, k_1), \ldots, S(n, k_m))$ is a dth power of a positive integer infinitely often. By Proposition 2.2, there is an integer e, $0 \leq e < d$, and an element τ of $\mathcal{E}$ so that

$$P(S(e + d\nu, k_1), \ldots, S(e + d\nu, k_m)) = \tau^d.$$

Thus

$$P(S_1, \ldots, S_m) = T^d$$

where $T = \psi(\tau)$ and $S_i = \psi(S(e + d\nu, k_i))$ are polynomials from $\mathbf{Q}[X_p : p \in \mathcal{P}]$. Let $\mathcal{M} = \{I_1, \ldots, I_s\}$ be the interval partition of $[m]$ and $\mathcal{P}_1, \ldots, \mathcal{P}_t$ be the t disjoint m-sets of primes guaranteed by Proposition 4.3. Let $\mathcal{A} = \{\alpha_p \in \mathbf{C} : p \in \mathcal{P}\}$ be any fixed specialization. We take any of the sets, say $\mathcal{P}_1$ with the elements $p_1 < \ldots < p_m$, and set every X_p for $p \notin \mathcal{P}_1$ equal to α_p. We get the identity

$$P(S_1^*, \ldots, S_m^*) = (T^*)^d \tag{18}$$

where T^* and $S_i^* = S_i(X_p := \alpha_p :\ p \notin \mathcal{P}_1)$ are polynomials from $\mathbf{Q}[X_p :\ p \in \mathcal{P}_1]$.

Due to the substitution $\nu := e + d\nu$, actually the polynomials S_i and hence $P(S_1^*, \ldots, S_m^*)$ lie in $\mathbf{Q}[X_p^d :\ p \in \mathcal{P}_1]$. Applying the previous lemma (with $g = d$) for each of the m variables, we see that

$$T^* = M \cdot U(X_p^d :\ p \in \mathcal{P}_1) \tag{19}$$

where $M = \prod_{p \in \mathcal{P}_1} X_p^{s_p}$, $s_p \geq 0$. From (18) and (19) we obtain, by replacing X_p^d with the variable Z_p, that

$$P(U_1, \ldots, U_m) = \prod_{p \in \mathcal{P}_1} Z_p^{s_p} \cdot U^d$$

where $U_i, U \in \mathbf{Q}[Z_p :\ p \in \mathcal{P}_1]$. It follows that $\{U_i :\ i = 1, \ldots, m\}$ is an $\mathcal{M}$-regular system. Indeed, $\mathcal{S} = \{\psi(S(\nu, k_i))(X_p := \alpha_p :\ p \notin \mathcal{P}_1) :\ i = 1, \ldots, m\}$ is $\mathcal{M}$-regular by Proposition 4.3 and $U_i = \psi(S(e + d\nu, k_i))(X_p := \alpha_p :\ p \notin \mathcal{P}_1;\ X_p^d := Z_p :\ p \in \mathcal{P}_1)$. That the system $\{U_i :\ i = 1, \ldots, m\}$ satisfies the conditions (i) and (ii) of regularity is clear. Its Jacobian is nonzero because the substitution $\nu := e + d\nu$ results only in multiplying the column of X_p in the diagonal block in the Jacobi matrix of $\mathcal{S}$ by the nonzero constant p^e. Inverting $\{U_i :\ i = 1, \ldots, m\}$ by 1 of Proposition 4.1, we get the identity

$$P(Z_{p_1}, \ldots, Z_{p_m}) = \prod_{p \in \mathcal{P}_1} Q_p^{s_p} \cdot U(Z_p := Q_p :\ p \in \mathcal{P}_1)^d$$

for some polynomials $Q_p \in \mathbf{Q}[Z_p :\ p \in \mathcal{P}_1]$. If U were nonconstant, then $U(Z_p := Q_p :\ p \in \mathcal{P}_1)$ would be nonconstant as well, by 2 and 3 of Proposition 4.1, which is impossible because P is free of all nonconstant dth powers. Hence the polynomial U is a constant different from 0. Using (18) and (19) we conclude from this that

$$P(S_1^*, \ldots, S_m^*) = c \prod_{p \in \mathcal{P}_1} X_p^{ds_p}$$

where $c \in \mathbf{C}$ is nonzero and s_p are nonnegative integers. Not all s_p may be zero. Even more is true: By 4 of Proposition 4.1, there exists a $k \in I_s$ so that $s_{p_k} > 0$. Returning to all the variables before the specialization, we conclude that

$$P(S_1, \ldots, S_m) = A \cdot \prod_{p \in \mathcal{P}_1} X_p^{ds_p} + B \tag{20}$$

where $s_{p_k} > 0$, $A, B \in \mathbf{Q}[X_p :\ p \in \mathcal{P} \backslash \mathcal{P}_1]$, and

$$B(X_p := \alpha_p :\ p \in \mathcal{P} \backslash \mathcal{P}_1) = 0. \tag{21}$$

Since the expression of $P(S_1, \ldots, S_m)$ in the form (20) is unique, the polynomials A and B are independent of the choice of the specialization $\mathcal{A}$. Since (21) holds for every specialization, B must be a zero polynomial.

Thus there is a $k \in I_s$ such that the polynomial $P(S_1, \ldots, S_m)$ is divisible by $X_{p_k}^d$. Since I_s is the last part of $\mathcal{M}$, by the remark after Proposition 4.1 the variable X_{p_k} appears in every S_i only in the linear term $bX_{p_k}^d$. Taking any of the sets of primes $\mathcal{P}_i$, $i = 1, \ldots, t$, in the place of $\mathcal{P}_1$, we obtain a set $\mathcal{Q}$ of t primes such that (i) the monomial $\left(\prod_{p \in \mathcal{Q}} X_p\right)^d$ divides $P(S_1, \ldots, S_m)$ and (ii) every X_p, $p \in \mathcal{Q}$, appears in every S_i only in the linear term bX_p^d. By (i), the degree of $P(S_1, \ldots, S_m)$ in the variables $\{X_p : \ p \in \mathcal{Q}\}$ is at least $dt = d(\deg(P) + 1)$. By (ii), this degree is at most $d \deg(P)$. We have a contradiction. $\square$

Theorem 4.9 *If $P \in \mathbf{Q}[Y_1, \ldots, Y_m]$ is not a perfect power in $\mathbf{Q}[Y_1, \ldots, Y_m]$, then there exists a constant $C_1 = C_1(P)$ depending only on P such that if $C_1 < k_1 < \ldots < k_m$ are m distinct integers, then the diophantine equation*

$$P(S(n, k_1), \ldots, S(n, k_m)) = y^d$$

has only finitely many solutions $(n, y, d) \in \mathbf{N}^3$, $y, d > 1$.

Proof. In view of the previous theorem it suffices to show that if $C_1 < k_1 < \ldots < k_m$ are distinct then the equality $P(S(n, k_1), \ldots, S(n, k_m)) = y^d$ for $n, y \in \mathbf{N}$, $y > 1$, implies that d is bounded by a constant. We assume that P depends on all m variables and set $C_1 = C_1(P)$ to be equal to the constant $C(m, \deg(P))$ of the previous theorem. Suppose that $Q = P(\psi(S(\nu, k_1)), \ldots, \psi(S(\nu, k_m)))$ is a monomial. We know, by the previous proof, that Q depends on $t = \deg(P) + 1$ variables X_p such that each of them appears in every $\psi(S(\nu, k_i))$ only in the linear term. But then we have the same contradiction for the degree of Q in these variables as before. So Q is not a monomial and $P(S(\nu, k_1), \ldots, S(\nu, k_m)) \in \mathcal{E}$ has rank at least two. Thus $(P(S(n, k_1), \ldots, S(n, k_m)))_{n \geq 1}$ is a non-degenerate linearly recurrent sequence having a leading root. By a result from Shorey and Stewart [19], it follows that there exists a constant C_2 which is effectively computable and depends on P and $k_1, k_2, \ldots, k_m$, such that the equality $P(S(n, k_1), \ldots, S(n, k_m)) = y^d$, $n, y \in \mathbf{N}$, $y > 1$, implies $d < C_2$. $\square$

References

[1] M. Aigner and G. Ziegler, *Proofs from the Book*, Springer, Berlin, 2001.

[2] H. Bass, E. H. Conell and D. Wright, The Jacobian conjecture: reduction of degree and formal expansion of the inverse, *Bull. Amer. Math. Soc.* **7 (2)** (1982), 287–330.

[3] S. Berg, On snowball sampling, random mappings and related problems, *J. Appl. Probab.* **18** (1981), 283–290.

[4] D. Branson, Stirling numbers and Bell numbers: Their role in combinatorics and probability, *Math. Sci.* **25** (2000), 1–31.

[5] B. Brindza and Á. Pintér, On the power values of Stirling numbers, *Acta Arith.* **60** (1991), 169–175.

[6] E. R. Canfield and C. Pomerance, On the problem of uniqueness for the maximum Stirling number(s) of the second kind, *Integers* **2** (2002), A1.

[7] P. Corvaja and U. Zannier, Diophantine equations with power sums and universal Hilbert sets, *Indag. Mathem., N. S.* **9** (1998), 317–332.

[8] P. Erdős, Beweis eines Satzes von Tschebyschef, *Acta Sci. Math. (Szeged)* **5** (1930-32), 194–198.

[9] A. van den Essen, Polynomial automorphisms and the Jacobian conjecture. In: J. Alev and G. Cauchon (editors), *Algèbre non commutative, groupes quantiques et invariants. Septième contact Franco-Belge, Reims, France, June 26–30, 1995.*, Société Mathématique de France, Paris, 1995. ; pp. 55–81.

[10] A. van den Essen, To believe or not to believe: The Jacobian conjecture, *Rend. Semin. Mat., Torino* **55** (1997), 283–290.

[11] A. van den Essen, The sixtieth anniversary of the Jacobian Conjecture: a new approach, *Ann. Pol. Math.* **76** (2001), 77–87.

[12] H. Iwaniec and J. Pintz, Primes in short intervals, *Monatsh. Math.* **98** (1984), 115–143.

[13] M. Klazar, Counting pattern-free set partitions. I: A generalization of Stirling numbers of the second kind, *Eur. J. Comb.* **21** (2000), 367–378.

[14] J. W. Layman and C. L. Prather, Generalized Bell numbers and zeros of successive derivatives of an entire function., *J. Math. Anal. Appl.* **96** (1983), 42–51.

[15] F. Luca and P. G. Walsh, The product of like-indexed terms in binary recurrences, to appear in *J. Number Theory.*

[16] Á. Pintér, On some arithmetical properties of Stirling numbers, *Publ. Math.* **40** (1992), 91–95.

[17] Á. Pintér, On a diophantine problem concerning Stirling numbers, *Acta Math. Hung.* **65** (1994), 361–364.

[18] R. Sánchez-Peregrino, The Lucas congruence for Stirling numbers of the second kind, *Acta Arith.* **94** (2000), 41–52.

[19] T. N. Shorey and C. L. Stewart, Pure powers in recurrence sequences and some related diophantine equations, *J. Number Theory* **27** (1987), 324–352.

[20] D. Singer, On Catalan trees and the Jacobian conjecture, *Electr. J. Combin.* **8** (2001), R2, 35 pages.

[21] R. P. Stanley, *Enumerative Combinatorics, Volume 1*, Wadsworth & Brooks/Cole, Monterey, Ca, 1986.

[22] L. A. Székely, The analytic behavior of the holiday numbers, *Acta Sci. Math.* **51** (1987), 365–369.

[23] P. T. Young, Congruences for Bernoulli, Euler, and Stirling numbers, *J. Number Theory* **78** (1999), 204–227.