Publ. Math. Debrecen
82/1 (2013), 219–254
DOI: 10.5486/PMD.2013.5480

Combinatorial Diophantine equations and a refinement of a theorem on separated variables equations

By YURI F. BILU (Talence), CLEMENS FUCHS (Salzburg),
FLORIAN LUCA (Morelia) and ÁKOS PINTÉR (Debrecen)

Abstract. We look at Diophantine equations arising from equating classical counting functions such as perfect powers, binomial coefficients and Stirling numbers of the first and second kind. The proofs of the finiteness statements that we give use a variety of methods from modern number theory, such as effective and ineffective tools from Diophantine approximation. As a tool for one part of the statements we establish a theoretical result that gives a more precise description on the structure of the solution set in the theorem, due to Bilu and Tichy, on Diophantine equations with separate variables in the case when infinitely many solutions exist.

Mathematics Subject Classification: Primary 11D41, 11D61; Secondary 05A19, 11B65, 11B73, 14G05.
Key words and phrases: Diophantine equations, counting functions, Stirling numbers, effective and ineffective methods, Diophantine equations with separate variables.
Research of F. L. was supported in part by Grants SEP-CONACyT 79865, PAPIIT 104512. Research of Á. P. was supported in part by the Hungarian Academy of Sciences, OTKA grants T67580, K75566, K100339, NK101680, NK104208 and the Project TÁMOP 4.2.1./B-09/1/KONV-2010-0007 implemented through the New Hungary Development Plan co-financed by the European Social Fund and the European Regional Development Fund. Furthermore, Yu.F. B. and F. L. were supported in part by the joint project France–Mexico 25224/171999 "Linear recurrences, arithmetic functions and additive combinatorics", and F. L. and Á. P. were supported in part by the joint project Hungary-Mexico J.010.106 "Diophantine Equations and Applications in Cryptography". Part of this research was done while C. F. visited the Institute of Mathematics of the University of Debrecen in November 2009 and another part while F. L. visited the Department of Mathematics at ETH Zurich in March 2010. Research of C. F. was supported by Austrian Science Fund (FWF): P 24574-N26.

1. Introduction and results

Elementary counting functions appear in several areas of mathematics. The study of their arithmetical properties has a long history. In this paper, we are interested in studying the Diophantine equations which arise when two such counting functions are set to equal each other. The combinatorial background to this question is quite obvious. The counting functions that we are studying are the following:

n^k – Perfect powers: giving the number of maps from a set with k elements to a set of n elements, or the number of integer points in a k-dimensional cube with side length n and having one of its corners at the origin and the sides parallel to the coordinate axes;

$\binom{n}{k}$ – Binomial coefficients: giving the number of subsets with k elements of a set of n elements;

S_k^n – Stirling numbers of the second kind: giving the number of partitions in k nonempty disjoint subsets of a set of n elements;

s_k^n – Stirling numbers of the first kind: giving the number of permutations with k disjoint cycles of a set with n elements.

For the proofs of our main results, we will use a variety of methods from modern number theory, ranging from effective tools provided by Baker's theory of lower bounds for nonzero linear forms in logarithms in algebraic numbers, to ineffective methods such as the recent applications of the subspace theorem à la Corvaja and Zannier, as well as the finiteness theorem on separated variables equations from [8], see Theorem (BT) in Section 2.

We mention that in the course of applying Theorem (BT) the question arose whether one can get a more precise result on the structure of the solution set of such equations with separate variables in case that infinitely many solutions exist. This was the point when the first author joined in this project and contributed this general theoretical statement. A complete treatment, even in the more general case of rational solutions with bounded denominator, is given in Section 2 below. Using this new result, which is Theorem 4, one can rule out several cases immediately making the treatment of our equations via the Theorem (BT) much simpler. Clearly, this statement will be useful also for future concrete applications of this method.

Many arithmetical properties of the counting functions introduced above are well-known and we shall make use of some of these properties. All these numbers satisfy recurrence relations. For example, if we set $S_0^0 = 1$ and $S_0^n = 0$ for all

$n \geq 1$, then the recurrence $S_k^{n+1} = S_{k-1}^n + kS_k^n$ holds for all $n,\ k \geq 0$. Furthermore, if we set $s_0^0 = 1$ and $s_0^n = 0$ for all $n \geq 1$, then the recurrence $s_k^{n+1} = s_{k-1}^n - ns_k^n$ holds for all $n,\ k \geq 0$.

We also have

$$S_a^n = \frac{1}{a!}\left\{a^n - \binom{a}{1}(a-1)^n + \ldots + (-1)^{a-1}\binom{a}{a-1}1^n\right\}, \tag{1}$$

and

$$S_{n-a}^n = \binom{n}{a+1}\tilde{S}_1^{a+1} + \ldots + \binom{n}{2a}\tilde{S}_a^{2a}, \tag{2}$$

where $\tilde{S}_k^n$ are the associated Stirling numbers of the second kind. These associated Stirling numbers also have a combinatorial meaning, namely, $\tilde{S}_k^n$ counts the number of partitions of a set with n elements into k disjoint parts each having at least 2 elements. While we also have a similar representation as (2) for the analogous Stirling numbers of the first kind, namely

$$s_{n-a}^n = \binom{n}{a+1}\tilde{s}_1^{a+1} + \ldots + \binom{n}{2a}\tilde{s}_a^{2a}, \tag{3}$$

where $\tilde{s}_k^n$ are certain associated Stirling numbers of the first kind, there is no known formula analogous to (1) in the literature for Stirling numbers of the first kind. From the above identities, we see that for varying n and fixed a the function S_a^n is an exponential polynomial, or the nth term of a linearly recurrent sequence whose roots are all simple and given by $\{1, \ldots, a\}$, whereas the functions S_{n-a}^n, s_{n-a}^n are polynomials of degree $2a$ in n.

In this paper, we study the Diophantine equations resulting from when two such counting functions are set to equal each other. Some of the resulting Diophantine equations are easy, such as $x^a = y^b$ for given positive integers a and b where the unknowns are integers x and y. Other equations of this type have already been studied in the literature such as

$$\binom{x}{a} = y^b, \qquad \text{or} \qquad \binom{x}{a} = \binom{y}{b},$$

again for given integers $a > 1$ and $b > 1$ with integer solutions (x, y). For the first equation, the complete list of solutions, even with variable $a > 1$ and $b > 1$, appears in [21], which is based on results from [3] and [15]. Assuming that $x \geq 2a$, all solutions have $a = b = 2$ except for $(x, a, b, y) = (50, 3, 2, 140)$. For fixed $a > b > 1$, the second equation has only finitely many positive integer

solutions (x, y) (see [5]). For a list of solutions of the second equation for various small values of the parameters a and b, see [11], [30] and [31].

In a similar vein, effective upper bounds for the maximum of positive integers $x,\ y$ and $z > 1$ in the equations

$$S_{x-a}^x = by^z, \qquad \text{or} \qquad s_{x-a}^x = by^z,$$

where a and b are given positive integers, appear in [10]. All such equations have only finitely many solutions except when $z = 2$ and $a \in \{1, 3\}$; in these exceptional cases the equations lead to Pell equations which may have infinitely many solutions. In the same paper [10], it was shown that the equation

$$S_a^x = by^z$$

with fixed integers $a \geq 2$ and $b \geq 1$, where $x,\ y,\ z > 1$ are positive integer variables, implies that z is bounded by an effective constant depending only on a and b. The fact that there are only finitely many possibilities for x and y as well was shown in [22].

In [25], it was proved that if positive integers x and y are such that

$$S_a^x = S_b^y \tag{4}$$

for some fixed positive integers a and b, then the maximum of x and y is bounded by an effective constant depending on a and b. It is conjectured in [17] that all the non-trivial solutions of equation (4) (here, by non-trivial we mean $x \geq a > 1$ and $y \geq b > 1$) are

$$S_5^6 = S_2^5 = 15 \quad \text{and} \quad S_{90}^{91} = S_2^{15} = 4095.$$

This conjecture is known to be true for $\max\{a, b\} \leq 100$.

Here, we look at several of the remaining cases and we prove finiteness statements. For small values of the parameters, we give effective results. However, our general statements are ineffective. The case of s_{n-k}^n falls somewhat outside of our treatment because we could not deduce the desired finiteness result for this counting function out of the arithmetical information available to us on these numbers. The motivation for such equations is quite obvious. Observe, for example, that the equation $S_2^x = \binom{y}{2}$ can be rewritten as $2^{x+2} = (2y-1)^2+7$, which we recognize as the famous and well-studied Ramanujan-Nagell equation.

The first combinations of equations we are interested in are those in which S_a^n is involved. Our proof here uses a method introduced by Corvaja and Zannier in [13] which relies on the Schmidt subspace theorem [28]. This method was already used in [22].

Theorem 1. *Let $a \geq 2, b \geq 2$, $c \neq 0$ and $d \geq 1$ be integers. Then the Diophantine equations*

$$S_a^x = cy^b, \qquad S_a^x = \binom{y}{b}, \qquad S_a^x = S_{y-d}^y, \quad S_a^x = s_{y-d}^y \tag{5}$$

each have only finitely many positive integer solutions (x, y).

The next finiteness result deals with the remaining combinations of our classical counting functions. Here, the proofs rely on the already mentioned finiteness theorem from [8] (in the refined form stated as Theorem 4 below), whose proof in turn rests on results by Fried, Schinzel, and a classical result by Siegel.

Theorem 2. *Let a and b be positive integers. Then the Diophantine equations*

$$\begin{aligned}
S_{x-a}^x &= S_{y-b}^y, && (a > b > 1),\\
S_{x-a}^x &= s_{y-b}^y, && (a > 1, b > 1),\\
s_{x-a}^x &= s_{y-b}^y, && (a > b > 1),\\
S_{x-a}^x &= \binom{y}{b}, && (a > 1, b > 2),\\
s_{x-a}^x &= \binom{y}{b}, && (a > 1, b > 2)
\end{aligned}$$

each have only finitely positive integer solutions (x, y).

For small values of parameters, we present an effective result whose proof relies on an effective theorem due to Baker [2] based itself on linear forms in logarithms.

Theorem 3. *For fixed $a \geq 2$, the Diophantine equation*

$$S_{x-a}^x = S_{y-1}^y = s_{y-1}^y = \binom{y}{2}$$

has only finitely many integer solutions (x, y). Furthermore, they are all effectively computable.

We could not prove the same result as Theorem 3 for the similar equations involving s_{x-a}^x instead of S_{x-a}^x. We leave this as an open problem for the reader.

Remark. Using Runge's method (see, for example, [23], [26] and [33]), it is easy to solve the equations $S_{x-2}^x = \binom{y}{2}$ and $s_{x-2}^x = \binom{y}{2}$ in integers $x \geq 3$ and

$y \geq 2$. We detail this approach for the first equation only, because for the second equation the entire argument can be repeated. It is known that

$$S_{x-2}^{x} = \frac{1}{24}x(x-1)(x-2)(3x-5),$$

and by the transformation $u := 3x$ and $v := 9(2y-1)$, the first equation leads to the quartic Diophantine equation

$$u(u-3)(u-5)(u-6)+81 = u^4 - 14u^3 + 63a^2 - 90a + 81 = v^2.$$

The polynomial on the left-hand side of the last equation above is monic and of even degree, so Runge's method applies. In fact, some straightforward calculations yield that for $u \geq 24$ we have

$$(u^2 - 7u + 7)^2 < u^4 - 14u^3 + 63a^2 - 90a + 81 = v^2 < (u^2 - 7u + 8)^2.$$

From these inequalities, we deduce easily that all the solutions of the equation $S_{x-2}^{x} = \binom{y}{2}$ satisfy $x < 8$. Testing this small range reveals that the only solution is $(x, y) = (3, 2)$. In a forthcoming paper, we solve some further special cases of the above equations.

2. Separate variables equations with infinitely many solutions

In [8], the first author and Tichy proved Theorem (BT) below which basically says that if an equation of the type $f(x) = g(y)$ has infinitely many positive integer solutions x, y, then, up to certain transformations on the space of polynomials, the pair of polynomials $(f(X), g(X))$ must belong to one of five well-understood families of pairs of polynomials which they called *standard*. Therefore in concrete applications, as for example to treat the equations from Theorem 2, all one needs to do is to show that the polynomials under consideration are not related in the way the Theorem (BT) asserts to the pairs of polynomials belonging to the standard families.

Let $\alpha \in \mathbb{C}$ and β be nonzero, q, s and t be positive integers, r be a nonnegative integer, and $v(X) \in \mathbb{Q}[X]$ be a nonzero polynomial which may be constant. Define the nth *Dickson polynomial* $D_n(X, \alpha)$ of parameter α as

$$D_n(X, \alpha) := \sum_{i=0}^{[n/2]} \frac{n}{n-i}\binom{n-i}{i}(-\alpha)^i X^{n-2i}.$$

It follows that $D_n(z+\alpha/z) = z^n + (\alpha/z)^n$. Hence, the coefficients of $D_n(X,\alpha)$ are elements of the field $\mathbb{Q}(\alpha)$. Two polynomials $f(X)$ and $g(X)$ are said to form a *standard pair* if one of the ordered pairs $(f(X),g(X))$ or $(g(X),f(X))$ belongs to the list below. If this is the case, then the polynomials $f(X)$ and $g(X)$ are said to form a standard pair of the first kind, or second kind, etc., according to their location in the table below.

kind	explicit form of $\{f(X),g(X)\}$	parameter restrictions
first	$(X^q, \alpha X^r v(X)^q)$	$r<q, (r,q)=1, r+\deg v>0$
second	$(X^2, (\alpha X^2+\beta)v(X)^2)$	
third	$(D_s(X,\alpha^t), D_t(X,\alpha^s))$	$(s,t)=1$
fourth	$(\alpha^{-s/2}D_s(X,\alpha), -\beta^{-t/2}D_t(X,\beta))$	$(s,t)=2$
fifth	$((\alpha X^2-1)^3, 3X^4-4X^3)$	–

Theorem (BT)**.** *Let $f(X),g(X)\in\mathbb{Q}[X]$ be non-constant polynomials such that the equation $f(x)=g(y)$ has infinitely many solutions $x,y\in\mathbb{Q}$ with a bounded denominator. Then $f=\varphi\circ f_1\circ\lambda$ and $g=\varphi\circ g_1\circ\mu$ where $\lambda(X),\mu(X)\in\mathbb{Q}[X]$ are linear polynomials, $\varphi(X)\in\mathbb{Q}[X]$ and $(f_1(X),g_1(X))$ is a standard pair over $\mathbb{Q}$ such that the equation $f_1(x)=g_1(y)$ has infinitely many rational solutions with a bounded denominator.*

In concrete applications of Theorem (BT), it is useful to have a more precise structure of the set of solutions of $f(x)=g(y)$. In particular, one may wonder whether all but finitely many solutions of $f(x)=g(y)$ "originate" from the solutions of the simpler equation $f_1(x)=g_1(y)$. More precisely, one may ask the following question:

> *Given a non-zero integer Δ, is it true that all but finitely many rational solutions of $f(x)=g(y)$ with denominator Δ also satisfy the equation $f_1\circ\lambda(x)=g_1\circ\mu(y)$?*

Unfortunately, this is not true in general. More precisely, one may find a standard pair $(f_1(X),g_1(X))$ and a polynomial $\varphi(X)$ such that the equation $\varphi\circ f_1(x)=\varphi\circ g_1(y)$ has infinitely many solutions with a bounded denominator not satisfying the equation $f_1(x)=g_1(y)$. The simplest example is $f_1(X)=g_1(X)=X$ and $\varphi(X)=X^2$. After some reflection, one discovers three types of examples where the answer to the above question is negative:

1. Let $(f_1(X),g_1(X))$ be a standard pair of the first or of the third kind. Then each of the equations $f_1(x)=g_1(y)$ and $f_1(x)=-g_1(y)$ has infinitely many

solutions with a bounded denominator. Hence, if $\varphi(X)$ is a polynomial satisfying $\varphi(X) = \varphi(-X)$, then the equation $\varphi \circ f_1(x) = \varphi \circ g_1(y)$ has infinitely many solutions for which $f_1(x) \neq g_1(y)$.

2. Put $f_1(X) = X$. Then for any choice of the polynomial $g_1(X)$, the polynomials $f_1(X)$ and $g_1(X)$ form a standard pair of the first or of the third kind. Now if $\varphi(X)$ satisfies $\varphi(X) = \varphi(a - X)$ for some $a \in \mathbb{Q}$, then the equation $\varphi \circ f_1(x) = \varphi \circ g_1(y)$ has infinitely many solutions satisfying $f_1(x)+g_1(y)=a$.
3. Denote by $\Delta_n(X, \alpha)$ the polynomial defined in (7) below. Then, for odd n, we have $D_n(X, 1) \pm 2 = (X \pm 2)\,\Delta_n(X, \pm 1)^2$. Hence, each of the equations $x^2 = D_n(y, 1) \pm 2$ has infinitely many solutions in $\mathbb{Z}$. Now put $f_1(X) = X^2$ and $g_1(X) = D_n(X - 2, 1) + 2$. Then $(f_1(X), g_1(X))$ is a standard pair of the first kind, and for any polynomial $\varphi(X)$ satisfying $\varphi(4 - X) = \varphi(X)$, the equation $\varphi \circ f_1(x) = \varphi \circ g_1(y)$ has infinitely many solutions satisfying $f_1(x) + g_1(y) = 4$.

It turns out that these three examples exhaust all possible negative answers to the question raised above.

Theorem 4. *Let Δ be a non-zero integer and let $f(X), g(X) \in \mathbb{Q}[X]$ be non-constant polynomials such that the equation $f(x) = g(y)$ has infinitely many solutions $x, y \in \mathbb{Q}$ with denominator Δ; we denote the set of these solutions as S:*

$$S = \{(x, y) \in \mathbb{Q}^2 : f(x) = g(y), \quad \Delta x, \Delta y \in \mathbb{Z}\}.$$

Then $f = \varphi \circ f_1 \circ \lambda$, and $g = \varphi \circ g_1 \circ \mu$, where $\lambda(X), \mu(X) \in \mathbb{Q}[X]$ are linear polynomials, $\varphi(X) \in \mathbb{Q}[X]$ and $(f_1(X), g_1(X))$ is a standard pair over $\mathbb{Q}$ such that one of the following alternatives takes place:

1. *All but finitely many solutions from S satisfy the equation $f_1 \circ \lambda(x) = g_1 \circ \mu(y)$ as well.*
2. *The standard pair $(f_1(X), g_1(X))$ is of the first or of the third kind, we have $\varphi(X) = \varphi(-X)$, and all but finitely many solutions from S satisfy one of the equations $f_1 \circ \lambda(x) = \pm g_1 \circ \mu(y)$.*
3. *The standard pair $(f_1(X), g_1(X))$ is of the first kind, there exists $a \in \mathbb{Q}^\times$ such that $\varphi(X) = \varphi(a - X)$, and all but finitely many solutions from S satisfy one of the equations*

$$f_1 \circ \lambda(x) = g_1 \circ \mu(y), \qquad \text{or} \qquad f_1 \circ \lambda(x) + g_1 \circ \mu(y) = a. \tag{6}$$

Moreover, one of $f_1(X)$, $g_1(X)$ is X^2 and the other is $(a/4)D_n(X-2, 1)+a/2$, where n is odd.

The proof of this theorem is organized in four subsections. In the first subsection, we give some properties of Dickson polynomials. In the second subsection, we study the equation $f(x) = f(y)$. In the third subsection, we prove a technical property of standard pairs. Finally, in the fourth and last subsection, we give the proof of Theorem 4.

2.1. Some properties of Dickson polynomials. In this subsection, we recall some properties of the Dickson polynomials. A comprehensive account of the theory of Dickson polynomials can be found in [32, Section 1].

The simplest properties of Dickson polynomials that we need are collected in the following proposition (for the proofs, see, for instance, [6, Section 3]).

Proposition 1. *Put*

$$\Delta_n(X,\alpha) := \prod_{1\le k\le (n-1)/2} \big(X - \alpha\cdot 2\cos(2\pi k/n)\big). \tag{7}$$

Then for odd n

$$D_n(X,\alpha) \pm 2\alpha^{n/2} = \big(X \pm 2\alpha^{1/2}\big)\Delta_n(X,\pm\alpha^{1/2})^2,$$

while for even n

$$\begin{aligned} D_n(X,\alpha) - 2\alpha^{n/2} &= \big(X^2 - 4\alpha\big)\Delta_n\big(X,\alpha^{1/2}\big)^2,\\ D_n(X,\alpha) + 2\alpha^{n/2} &= D_{n/2}(X,\alpha)^2. \end{aligned}$$

For $\gamma \ne \pm\alpha^{n/2}$, the polynomial $D_n(X,\alpha) - \gamma$ has only simple roots. □

It is well-known that the Dickson polynomials are characterized by the orders of the roots of their translates. We shall need the following statement of this kind.

Proposition 2. *Let $\mathbb{K}$ be a field of characteristic 0 and let $f(X) \in \mathbb{K}[X]$ be a polynomial with the following property: there exist distinct $a, b \in \mathbb{K}$ such that both polynomials $f(X) - a$ and $f(X) - b$ have at most one root (in a fixed algebraic closure $\bar{\mathbb{K}}$) of odd order, and all the other roots are of even order. Then $n = \deg f$ is odd, and there exist $\eta \in \mathbb{K}^\times$ and $\beta \in \mathbb{K}$ such that*

$$f(X) = \frac{a-b}{4} D_n(\eta X + \beta, 1) + \frac{a+b}{2}.$$

Proof. Put

$$\Theta(f) = \deg \gcd(f, f');$$

in other words, $\Theta(f)$ is equal to $\deg f$ minus the number of distinct roots of f (in $\bar{\mathbb{K}}$). Clearly,

$$\sum_{c\in\bar{\mathbb{K}}} \Theta(f-c) = \deg f' = \deg f - 1. \tag{8}$$

The assumption implies that $\Theta(f-a), \Theta(f-b) \geq (\deg f - 1)/2$. Together with identity (8), this implies that $\Theta(f-a) = \Theta(f-b) = (\deg f - 1)/2$, and that $\Theta(f-c) = 0$ for all $c \in \bar{\mathbb{K}}$, $c \neq a, b$. It follows that each of the polynomials $f-a$ and $f-b$ has exactly one simple root, the other roots being of order exactly 2, and all the polynomials $f-c$ for $c \in \bar{\mathbb{K}}$, $c \neq a, b$ have only simple roots. Then clearly $n = \deg f$ is odd, and [32, Lemma 1.11] implies that $f(X) = \alpha D_n(X+\beta, \gamma) + \delta$ with some $\alpha, \beta, \gamma, \delta \in \mathbb{K}$, $\alpha\gamma \neq 0$.

Further, we have $\{a, b\} = \{\pm 2\alpha\gamma^{n/2} + \delta\}$, which implies that γ is a square in $\mathbb{K}$. Using the identity $D_n(X, \gamma) = \gamma^{n/2} D_n(\gamma^{-1/2}X, 1)$, and redefining α and β, we obtain $f(X) = \alpha D_n(\eta X + \beta, 1) + \delta$ with some $\eta \in \mathbb{K}^\times$. Further, since $\{a, b\} = \{\pm 2\alpha + \delta\}$, we have $\delta = (a+b)/2$, and either $\alpha = (a-b)/4$, or $\alpha = (b-a)/4$. In the first case we are done, and in the second case one has to replace η and β by $-\eta$ and $-\beta$, respectively. □

2.2. The equation $f(x) = f(y)$. Our principal tool is the following result about the equation $f(x) = f(y)$. It is very probable that this is well-known, but we did not find a suitable reference.

Proposition 3. *Let Δ be a non-zero integer and $f(X) \in \mathbb{Q}[X]$ be a non-constant polynomial such that the equation $f(x) = f(y)$ has infinitely many solutions $x, y \in \mathbb{Q}$ with denominator Δ. Then all but finitely many of these solutions satisfy either $x = y$ or $x + y = a$ for some fixed $a \in \mathbb{Q}$. The latter case is possible only if $f(X) = f(a - X)$.*

The proof relies on Siegel's theorem. Let us fix some terminology. Let $\mathbb{K}$ be a field of characteristic 0. By a *curve $\mathcal{X}$ over $\mathbb{K}$* we mean an absolutely irreducible projective algebraic curve defined over $\mathbb{K}$. By the *genus* of the curve we mean the *geometric genus*, that is, the genus of the function field $\bar{\mathbb{K}}(\mathcal{X})$. Similarly, by a *point* on a curve $\mathcal{X}$ we mean a *geometric $\bar{\mathbb{K}}$-point*, that is, a place of the field $\bar{\mathbb{K}}(\mathcal{X})$. The *field of definition* of a point is the residue field of the place it defines on $\mathbb{K}(\mathcal{X})$. A point P is *defined* over a field $\mathbb{L}$ (containing $\mathbb{K}$), or, shortly, is an *$\mathbb{L}$-point*, if the field of definition of P is contained in $\mathbb{L}$; as usual, we denote by $\mathcal{X}(\mathbb{L})$ the set of points defined over $\mathbb{L}$.

By an *affine embedding* of $\mathcal{X}$ over $\mathbb{K}$ we mean an n-tuple of rational function $x_1, \dots, x_n \in \mathbb{K}(\mathcal{X})$ (called *coordinate functions*, or simply *coordinates*) such that

$\mathbb{K}(\mathcal{X}) = \mathbb{K}(x_1, \ldots, x_n)$. An *affine curve* is a curve with a fixed affine embedding. A *point at infinity* of an affine curve is a point which is a pole of at least one of the coordinate functions. There are only finitely many points at infinity; all the other points are called *finite points*. Let R be a subring of $\bar{\mathbb{K}}$; an R-point is a finite point P defined over the quotient field of R such that $x_1(P), \ldots, x_n(P) \in R$. The set of R-points on an affine curve $\mathcal{X}$ will be denoted by $\mathcal{X}(R)$.

We now state the Theorem of Siegel in the form it is given in [1, Theorem 1.2].

Theorem (S)**.** *Let $\mathcal{X}$ be an affine curve over $\mathbb{Q}$ such that the set $\mathcal{X}(\mathbb{Z})$ of $\mathbb{Z}$-points is infinite. Then the curve $\mathcal{X}$ is of genus 0 and has at most 2 points at infinity. If there are exactly 2, then they are not defined over $\mathbb{Q}$, but are defined over $\mathbb{R}$.*

To continue, we need some lemmas. Let $\mathbb{K}$ be a field of characteristic 0 and $F(X, Y) \in \mathbb{K}[X, Y]$. We call the *principal part* of F the homogeneous polynomial $\widetilde{F}(X, Y)$ such that $\deg(F - \widetilde{F}) < \deg F$.

The following properties of the principal part are obvious.

Lemma 1.

1. *We have $\widetilde{F_1 F_2} = \widetilde{F}_1 \widetilde{F}_2$. In particular, if F divides G, then $\widetilde{F}$ divides $\widetilde{G}$.*
2. *Assume that $\widetilde{F}(x, y)$ is separable, that is, decomposes into pairwise non-proportional linear factors over $\bar{\mathbb{K}}$. Then the plane curve $F(x, y) = 0$ has exactly $\deg F$ non-singular points at infinity (defined over $\bar{\mathbb{K}}$). These points stay in one-to-one correspondence with the linear factors of $\widetilde{F}(X, Y)$, so that the field of definition of the point corresponding to the factor $\alpha X + \beta Y$ with (say) $\alpha \neq 0$ is $\mathbb{K}(\beta/\alpha)$.* □

Combining part 1 of this lemma with Theorem (S), we obtain the following.

Lemma 2. *Let $F(X, Y) \in \mathbb{Q}[X, Y]$ be an absolutely irreducible polynomial with the following properties:*

- *Its principal part $\widetilde{F}(X, Y)$ is separable.*
- *The equation $F(x, y) = 0$ has infinitely many solutions with bounded denominator.*

Then $\deg F \leq 2$ and, if $\deg F = 2$, then $\widetilde{F}$ is irreducible over $\mathbb{Q}$ but reducible over $\mathbb{R}$. □

Proof of Proposition 3. Let $F(X, Y)$ be a $\mathbb{Q}$-irreducible factor of $f(X) - f(Y)$ such that the equation $F(x, y) = 0$ has infinitely many rational solutions with denominator Δ. Then F is absolutely irreducible. Lemma 1.1 implies that $\widetilde{F}$

divides $X^n - Y^n$. In particular, $\widetilde{F}$ is separable. Lemma 2 implies that $\deg F \le 2$. Moreover, if $\deg F = 2$, then $\widetilde{F}$ is irreducible over $\mathbb{Q}$ but reducible over $\mathbb{R}$. However, $X^n - Y^n$ does not have factors with this property.

Thus, $\deg F = 1$ and, up to a constant multiple, $F(X,Y) = X \pm Y - a$ with $a \in \mathbb{Q}$. If $F(X,Y) = X - Y - a$, then, together with every root α, the polynomial f has the roots $\alpha \pm a$, $\alpha \pm 2a$, etc., which is impossible when $a \neq 0$. If $F(X,Y) = X + Y - a$, then the polynomial $f(X) - f(a - X)$ has infinitely many roots, and we have $f(X) = f(a - X)$. This proves the proposition. □

2.3. On standard pairs. We need the following technical property of standard pairs.

Proposition 4. *Let $(f(X), g(X))$ be a standard pair over $\mathbb{Q}$ such that the equation $f(x) = g(y)$ has infinitely many rational solutions with bounded denominator, and let a be a rational number. When $(f(X), g(X))$ is of the first or of the third kind, we assume in addition that $a \neq 0$ and that $\deg f, \deg g \ge 3$. Then the equation $f(x) + g(y) = a$ has at most finitely many rational solutions with bounded denominator.*

For the proof, we need a genus formula due to Fried. Let $f(X), g(X) \in \mathbb{K}[X]$ be polynomials over a field $\mathbb{K}$ of characteristic 0. We let $\lambda_1, \dots, \lambda_r$ be the orders of the distinct roots of f in the algebraic closure $\bar{\mathbb{K}}$ of $\mathbb{K}$:

$$f(X) = a(X - \alpha_1)^{\lambda_1} \cdots (X - \alpha_r)^{\lambda_r},$$

where $a \in \mathbb{K}^\times$ and $\alpha_1, \dots, \alpha_r \in \bar{\mathbb{K}}$ are pairwise distinct. Similarly, let $\mu_1, \dots, \mu_s$ be the orders of the distinct roots of g. We define

$$\omega(f,g) := \deg f \deg g - \sum_{\substack{1 \le i \le r \\ 1 \le j \le s}} \gcd(\lambda_i, \mu_j).$$

Clearly, $\omega(f,g) \ge 0$ and $\omega(f - c, g - c) = 0$ for all but finitely many $c \in \bar{\mathbb{K}}$.

Fried [18, Proposition 2 on page 240] proved the following genus formula for the curve $f(x) = g(y)$.

Proposition 5. *Let $\mathbb{K}$ be a field of characteristic 0 and $f(X), g(X) \in \mathbb{K}[X]$ be such that $f(x) = g(y)$ is an absolutely irreducible plane curve. Then the genus $\mathbf{g}$ of this curve satisfies*

$$2\mathbf{g} - 2 = \sum_{c \in \bar{K}} \omega(f - c, g - c) - \deg f \deg g - \gcd(\deg f, \deg g).$$

Proof of Proposition 4. Assume that $(f(X), g(X))$ is a standard pair of the second, fourth or fifth kind. Then both polynomials $f(X)$ and $g(X)$ are of even degree, and, since the equation $f(x) = g(y)$ has infinitely many rational solutions with a bounded denominator, their leading coefficients are of the same sign. It follows that $|f(x) + g(y)| \to \infty$ as $\max\{|x|, |y|\} \to \infty$, and the equation $f(x) + g(y) = a$ cannot have more than finitely many rational solutions with bounded denominator.

Now let $(f(X), g(X))$ be a standard pair of the first or of the third kind with $\deg f, \deg g \geq 3$, and $a \neq 0$. We shall prove that in this case the plane curve $f(x) + g(y) = a$ is absolutely irreducible and of genus at least 1, and complete the proof by Theorem (S).

Absolute irreducibility is immediate from the fact the degrees of f and g are coprime. The genus is given by

$$2\mathbf{g} - 2 = \sum_{c \in \bar{\mathbb{Q}}} \omega(f - c, g - a + c) - \deg f \deg g - 1. \tag{9}$$

Now assume that $(f(X), g(X))$ is of the first kind, and write $f(X) = X^m$ and $g(X) = \alpha X^r v(X)^m$, with $\gcd(r, m) = 1$, and a non-zero polynomial $v(X) \in \mathbb{Q}[X]$. Leaving in the sum from (9) only the terms corresponding to $c = 0$ and $c = a$ (here, we use that $a \neq 0$), we obtain

$$\begin{aligned} 2\mathbf{g} &\geq \omega(X^m, g(X) - a) + \omega(X^m - a, g(X)) - m \deg g + 1 \\ &\geq (m \deg g - \deg g) + \big(m \deg g - m(1 + \deg v)\big) - m \deg g + 1 \\ &= mr - (m + r) + (m^2 - 2m) \deg v + 1. \end{aligned} \tag{10}$$

Now recall that, by the assumption, $m \geq 3$ and $\deg g = r + m \deg v \geq 3$. In particular, either $r \geq 2$, or $r = 1$ and $\deg v \geq 1$. A simple inspection shows that in each case the right-hand side of (10) is strictly positive, proving that $\mathbf{g} > 0$.

Similarly, assume that $(f(X), g(X))$ is of the third kind, and write $f(X) = D_m(X, \alpha^n)$ and $g(X) = D_n(X, \alpha^m)$, with $\alpha \in \mathbb{Q}^\times$, $\gcd(m, n) = 1$, and $m, n \geq 3$ by the assumption. We have three cases: $a = \pm 4\alpha^{mn/2}$ and $a \neq \pm 4\alpha^{mn/2}$.

Case 1. $a = 4\alpha^{mn/2}$. Leaving in the sum from (9) only the terms with $c = \pm 2\alpha^{mn/2}$ and $c = 6\alpha^{mn/2}$, we obtain

$$\begin{aligned} 2\mathbf{g} \geq\ & \omega\big(D_m(X, \alpha^n) + 2\alpha^{mn/2}, D_n(X, \alpha^m) - 6\alpha^{mn/2}\big) \\ &+ \omega\big(D_m(X, \alpha^n) - 6\alpha^{mn/2}, D_n(X, \alpha^m) + 2\alpha^{mn/2}\big) \\ &+ \omega\big(D_m(X, \alpha^n) - 2\alpha^{mn/2}, D_n(X, \alpha^m) - 2\alpha^{mn/2}\big) - mn + 1. \end{aligned}$$

If both m and n are odd, then, using Proposition 1, we find

$$\omega\big(D_m(X,\alpha^n)+2\alpha^{mn/2}, D_n(X,\alpha^m)-6\alpha^{mn/2}\big)=\frac{(m-1)n}{2}, \tag{11}$$

$$\omega\big(D_m(X,\alpha^n)-6\alpha^{mn/2}, D_n(X,\alpha^m)+2\alpha^{mn/2}\big)=\frac{m(n-1)}{2},$$

$$\omega\big(D_m(X,\alpha^n)-2\alpha^{mn/2}, D_n(X,\alpha^m)-2\alpha^{mn/2}\big)=\frac{mn-1}{2}, \tag{12}$$

and we obtain

$$2\mathbf{g}\geq\frac{(m-1)(n-1)}{2}>0 \tag{13}$$

because $m,n\geq 3$.

If, say, m is even, then n is odd, and the right-hand sides of (11) and (12) become $mn/2$ and $(mn-2)/2$, respectively. We obtain $2\mathbf{g}\geq m(n-1)/2>0$.

Case 2. $a=-4\alpha^{mn/2}$. Now we leave in the sum the terms with $c=\pm 2\alpha^{mn/2}$ and $c=-6\alpha^{mn/2}$. Arguing as in the previous case, we obtain (13) when m and n are odd, and $2\mathbf{g}\geq(m-2)(n-1)/2>0$ when m is even.

Case 3. $a\neq\pm 4\alpha^{mn/2}$. In this case, we leave in the sum the terms with $c=\pm 2\alpha^{mn/2}$ and $c=a\pm 2\alpha^{mn/2}$. Arguing as above, we obtain the inequality $2\mathbf{g}\geq(m-1)(n-1)>0$ independently of the parity of m and n.

The proposition is proved. □

2.4. Proof of Theorem 4. Let $f(X)$, $g(X)$ and Δ satisfy the assumption of the theorem. Write $f=\varphi\circ f_1\circ\lambda$ and $g=\varphi\circ g_1\circ\mu$ as in Theorem (BT). Now we have three cases.

Case 1. There does not exist $a\in\mathbb{Q}$ such that $\varphi(X)=\varphi(a-X)$. In this case, Proposition 3 implies that we have option 1 of Theorem 4.

Case 2. We have $\varphi(X)=\varphi(-X)$. In this case, Propositions 3 and 4 imply that we have option 2 of Theorem 4.

Case 3. There exists a non-zero $a\in\mathbb{Q}$ such that $\varphi(X)=\varphi(a-X)$. In this case, Propositions 3 and 4 imply that $(f_1(X),g_1(X))$ is a standard pair of the first or of the third kind such that all but finitely many solutions of the original equation $f(x)=g(y)$ with any fixed denominator satisfy one of the equations (6), and one of the polynomials $f_1(X)$, $g_1(X)$ is of degree at most 2. We may assume that both equations in (6) have infinitely many solutions with a bounded denominator, otherwise we have option 1.

Assume first that one of the polynomials $f_1(X)$ and $g_1(X)$, say $f_1(X)$, is of degree 1. Replacing $\varphi(X)$ by $\varphi(X + a/2)$ and suitably modifying $\lambda(X)$, we obtain that $\varphi(X) = \varphi(-X)$ and $f_1(X) = X$, so that we again have option 2 of Theorem 4 with $(f_1(X), g_1(X))$ being a standard pair of the first kind.

We are left with the case when, say, $\deg f_1 = 2$. In this case, $n = \deg g_1$ is odd. Suitably modifying $\varphi(X)$ and $\lambda(X)$, we may assume that $f_1(X) = X^2$. Thus, each of the equations $x^2 = g_1(x)$ and $x^2 = a - g_1(x)$ has infinitely many solutions with a bounded denominator. It follows that each of the polynomials $g_1(X)$ and $g_1(X) - a$ has at most 2 roots of odd order in $\bar{\mathbb{Q}}$. Since $\deg g$ is odd, both have exactly one root of odd order.

Proposition 2 implies now that $g_1(X) = (a/4)D_n(\eta X + \beta, 1) + a/2$ with some $\eta \in \mathbb{Q}^\times$ and $\beta \in \mathbb{Q}$. Suitably modifying the linear polynomial $\mu(X)$, we complete the proof.

3. Proof of Theorem 1

For fixed $b \geq 2$ and $d \geq 1$, the polynomials appearing on the right-hand sides of equation (5) have degree at least two. For $a \geq 3$, the conclusion of Theorem 1 follows from the slightly more general result.

Theorem 5. *If $a \geq 3$ is fixed and $P(X) \in \mathbb{Q}[X]$ has degree $D \geq 2$, then the Diophantine equation $S_a^n = P(x)$ has only finitely many integer solutions (n, x).*

Proof. Let $\mathcal{E}$ denote the ring of all exponential polynomials with positive integer roots. That is, $\mathcal{E}$ is the set of all functions $f : \mathbb{N} \to \mathbb{Q}$ such that

$$f(n) = c_1 a_1^n + \cdots + c_k a_k^n$$

holds for all $n \geq 0$ with some fixed nonzero rational numbers $c_1, \ldots, c_k$ and integers $a_1 > a_2 > \cdots > a_k \geq 1$. The numbers $c_1, \ldots, c_k$ are called *coefficients* and the numbers $a_1, \ldots, a_k$ are called *roots*. We refer to a_1 as the *leading root*, to a_2 as the *second leading root*, etc. It is easy to see that $\mathcal{E}$ is a ring. The following important result is due to Corvaja and Zannier (see [13]). For extensions and generalizations of this result, see [14], [19] and [20].

Theorem (CZ)**.** *Assume that $f \in \mathcal{E}$ and $P(X) \in \mathbb{Q}[X]$ is such that the Diophantine equation $f(n) = P(x)$ has infinitely many solutions (n, x) in integers $n \geq 0$ and x. Then there exist integers $A > 0$ and $B \geq 0$, and $g \in \mathcal{E}$ such that the identity*

$$f(An + B) = P(g(n)) \quad \text{holds for all} \quad n. \tag{14}$$

More is known about the quantities appearing in formula (14). For example, one can choose $A := D$ to be the degree of $P(X)$ and $B \in \{0, 1, \ldots, A-1\}$. Furthermore, the roots of g are integers lying in the multiplicative group generated inside $\mathbb{Q}^\times$ by the roots of f. We shall not need such additional information.

We are now ready to prove Theorem 1. Assume that $a \geq 3$ and $S_a^n = P(x)$ has infinitely many integer solutions with n positive. By Theorem (CZ) above, we have an identity of the form

$$S_a^{An+B} = P(g(n)), \quad \text{which holds for all} \quad n \geq 0, \tag{15}$$

with some integers $A > 0$, $B \geq 0$, and some $g \in \mathcal{E}$. The first two leading roots of the exponential polynomial on the left are a^A and $(a-1)^A$ (see formula (1)). Let $b_1 > 1$ be the leading root of $g(n)$. If $g(n) = c_1 b_1^n$, or $g(n) = c_1 b_1^n + c_2$ for some nonzero coefficient(s) c_1 (and c_2 if it applies), then all roots of $P(g(n))$ are powers of b_1. In particular, any two of them are multiplicatively dependent, meaning that their logarithms are linearly dependent over $\mathbb{Q}$. However, since $a > 2$, the two leading roots a^A and $(a-1)^A$ of S_a^{An+B} are not multiplicatively independent; in fact, they are both > 1 and coprime. Thus, $g(n)$ must have a second leading root $b_2 > 1$. Write

$$g(n) = c_1 b_1^n + c_2 b_2^n + \text{linear combination of powers of smaller roots.}$$

Assume that

$$P(X) = C_0 X^D + C_1 X^{D-1} + \cdots + C_D$$

for some positive integer D and rational coefficients $C_0, \ldots, C_D$ with $C_0 \neq 0$. It is easy to see that the two leading roots of $C_0 g(n)^D$ are b_1^D and $b_1^{D-1} b_2$ with coefficients $C_0 c_1^D$ and $C_0 D c_1^{D-1} c_2$, respectively. Since the roots of $C_i g(n)^{D-i}$ are at most $b_1^{D-i} < b_1^{D-1} b_2$ for all $i \geq 1$, it follows that b_1^D and $b_1^{D-1} b_2$ are in fact the two leading roots of $P(g(n))$. Equating the two leading roots from identity (15), we get

$$a^A = b_1^D, \qquad \text{and} \qquad (a-1)^A = b_1^{D-1} b_2,$$

leading to $b_2/b_1 = ((a-1)/a))^A$. Since a and $a-1$ are coprime, it follows that there exists some positive integer λ such that $b_1 = \lambda a^A$ and $b_2 = \lambda (a-1)^A$. Hence,

$$a^A = b_1^D = \lambda^D a^{AD},$$

which is impossible because $a \geq 3$, $D \geq 2$ and $\lambda \geq 1$.

This shows that it is not possible for the equation $S_a^n = P(x)$ to have infinitely many integer solutions (n, x) with n positive. Note that this part of the argument was ineffective.

Assume on the other hand that it has infinitely many solutions (n, x) with n negative. This part of the argument is effective. Observe that S_a^n converges to a finite limit equal to $L := (-1)^{a-1}/(a-1)!$ when n tends to $-\infty$. Unless x is a root of the equation $P(x) = L$, it follows, since x is an integer, that $|P(x) - L| \geq 1/M$, where we can take M to be the least common multiple of the denominators of L and of all the coefficients of $P(X)$. Thus, if $n_0 < 0$ is sufficiently large in absolute value such that the inequality $|S_a^n - L| < 1/M$ holds for all $n \leq n_0$, we conclude that $S_a^n = P(x)$ can happen for such n with some integer x only when x is a root of $P(X) - L$. Since we have infinitely many possibilities and only finitely many roots for this last nonzero polynomial, it follows that we may assume that $x = x_0$ is fixed and that the relation $S_a^n = L$ holds for infinitely many negative integers n. However, this last claim is known to be false. In fact, the equation $S_a^x = K$ has, for any fixed constant K, at most $a - 1$ real solutions x.

This completes the proof of Theorem 5. □

To finish the proof of Theorem 1, we still need to address the case when $a = 2$. Then $S_a^n = 2^{n-1} - 1$. Then the equation $S_a^n = P(x)$ becomes $2^{n-1} = P(x) + 1$. It is well-known that if $Q(X) \in \mathbb{Q}[X]$ is a polynomial with at least two distinct roots, then the largest prime factor of $Q(x)$ tends to infinity with x in an effectively computable way when x is an integer with $|x|$ tending to infinity (see Notes to Chapter 7 in [29]). We apply this fact with the polynomials $P(X)$ appearing in the right-hand sides of equations (5). Observe that when $P(X) = cX^b$ and $b \geq 2$, then $Q(X) = P(X) + 1 = cX^b + 1$ has $b \geq 2$ distinct roots. For the remaining three polynomials, observe that when $P(X) = \binom{X}{b}$, then $P(X)$ has b real roots, namely the numbers $0, 1, \ldots, b - 1$, while when $P(X) = S_{X-d}^X$, or s_{X-d}^X, then $P(X)$ has at least $d + 1$ real roots, namely the numbers $0, 1, \ldots, d$. By Rolle's theorem, dP/dX has at least $b - 1$, or d, distinct real roots, respectively. But if $Q(X) = P(X) + 1$ has only one distinct root, that is, if it is a polynomial of the form $C_0(X - z_0)^D$, then its derivative dQ/dX will have only one repeated root also, and its derivative coincides with the derivative dP/dX of $P(X)$. Hence, we deduce that indeed $Q(X)+1$ must have at least two distinct roots whenever $b \geq 3$ and whenever $d \geq 2$. It remains to study the cases $b = 2$ and $d = 1$, for which $P(X) = \binom{X}{2} = S_{X-1}^X = s_{X-1}^X$ and for which $P(X)+1 = \binom{X}{2}+1 = (X^2-X+2)/2$ has two distinct roots anyway. Note that this part of the proof is effective.

This completes the proof of Theorem 1.

4. Proof of Theorem 2

All equations appearing in Theorem 2 are of the form $p(x) = q(y)$, where $p(X),\ q(X)$ are certain polynomials in $\mathbb{Q}[X]$, and thus we shall apply Theorem 4.

A quick look at the table on standard pairs in Section 2 reveals that the pairs of third and fourth kind consisting of Dickson polynomials have the property that all their monomials are concentrated either in even degrees, or in odd degrees. Namely, if D is the degree of such a polynomial, then monomials of degree $i \not\equiv D \pmod 2$ do not appear in such polynomials. Thus, we consider it useful to start with the following lemma.

Lemma 3. *When $a \geq 2$ is an integer, then there is no linear polynomial $\kappa(X) \in \mathbb{Q}[X]$ such that*

$$f \circ \kappa(X) = C_0 X^{2a} + C_2 X^{2a-2} + \sum_{0 \leq i \leq 2a-4} C_{2a-i} X^i,$$

whenever $f(X) \in \{S^X_{X-a},\ s^X_{X-a}\}$.

Proof. Let us write down the first few coefficients of S^X_{X-a} and s^X_{X-a}, respectively. We have

$$\begin{aligned} S^X_{X-a} = {} & \frac{1}{2^a a!} X^{2a} - \frac{4a^2 - a}{2^a (3) a!} X^{2a-1} + \frac{a(a-1)(16a^2 - 2a + 3)}{2^a (18) a!} X^{2a-2} \\ & - \frac{a(a-1)(320a^4 - 520a^3 + 202a^2 - 185a - 48)}{2^a (810) a!} X^{2a-3} + \cdots \end{aligned} \tag{16}$$

and

$$\begin{aligned} s^X_{X-a} = {} & \frac{1}{2^a a!} X^{2a} - \frac{2a^2 + a}{2^a (3) a!} X^{2a-1} + \frac{a(a-1)(4a^2 + 4a + 3)}{2^a (18) a!} X^{2a-2} \\ & - \frac{a(a-1)(2a-1)(20a^3 - 11a - 48)}{2^a (810) a!} X^{2a-3} + \cdots, \end{aligned} \tag{17}$$

respectively. For simplicity of notation, put $F_a(X) := S^X_{X-a}$ and $f_a(X) := s^X_{X-a}$. Assume that $\kappa(X) := \gamma X + \delta$ for some rational numbers $\gamma \neq 0$ and δ. Then the coefficients of X^{2a-1} and X^{2a-3} in $F_a \circ \kappa(X)$ are

$$\frac{\gamma^{2a-1}}{2^a a!} U \qquad \text{and} \qquad \frac{\gamma^{2a-3}}{2^a a!} V, \tag{18}$$

with U and V being

$$U \ := \ 2a\delta - \frac{4a^2 - a}{3};$$

$$V := \delta^3\binom{2a}{3} - \delta^2\binom{2a-1}{2}\frac{4a^2-a}{3} + \delta\binom{2a-2}{1}\frac{a(a-1)(16a^2-2a+3)}{18} - \frac{a(a-1)(320a^4-520a^3+202a^2-185a-48)}{810},$$

respectively. Setting $U = 0$, we get $\delta = (4a-1)/6$, which substituted into the formula for V yields

$$V = \frac{4\gamma^{2a-3}a(a-1)(a^2+11)}{2^a(105)a!}. \tag{19}$$

The above expression is nonzero for $a > 1$. Similarly, the coefficients of X^{2a-1} and X^{2a-3} in $f_a \circ \kappa(X)$ are given by the expression (18) with the values for U and V being

$$U := 2a\delta - \frac{2a^2+a}{3};$$
$$V := \delta^3\binom{2a}{3} - \delta^2\binom{2a-1}{2}\frac{2a^2+a}{3} + \delta\binom{2a-2}{1}\frac{a(a-1)(4a^2+4a+3)}{18} - \frac{a(a-1)(2a-1)(20a^3-11a-48)}{810},$$

respectively. Setting $U = 0$, we get $\delta = (2a+1)/6$, which substituted into the formula for V yields the same nonzero expression for V as in (19). This completes the proof of the lemma. □

We are now ready to prove Theorem 2. Assume that

$$p_a(x) = q_b(y)$$

has infinitely many integer solutions (x, y) for some pair of polynomials $(p_a(X), q_b(X))$ as in the statement of Theorem 2. Here, $p_a(X)$ depends on a and $q_b(X)$ depends on b. First we ran a computation for all $a \leq 12$ and $b \leq 12$ subject to the inequalities from the statement of the theorem which confirmed that in all cases except for one of them, the polynomial $p_a(X) - q_b(Y) \in \mathbb{C}[X, Y]$ is irreducible and has genus ≥ 1. By Theorem (S), this implies that such Diophantine equations have only at most finitely many integer solutions (x, y) in this small range for the parameters a and b. The exceptional case was obtained when $a = b = 2$, which corresponds to the equation $S_{x-2}^x = s_{y-2}^y$, which is equivalent to the genus 0 equation

$$x(x-1)(x-2)(3x-4) = y(y-1)(y-2)(3y-1).$$

Both polynomials appearing above have even degree equal to 4 and equal leading terms. With Runge's method, we showed that the only integer solutions (x, y)

have both x and y in $\{0,1,2\}$. Thus, even in the exceptional case, we only got finitely many integer solutions (x,y).

From now on, assume that $\max\{a,b\} \geq 13$.

An application of Theorem 4 shows that $p_a \circ \kappa_1(X) = \phi \circ f(X)$ and $q_b \circ \kappa_2(X) = \phi \circ g(X)$ for some linear polynomials $\kappa_1(X)$ and $\kappa_2(X)$ in $\mathbb{Q}[X]$, some polynomial $\phi(X) \in \mathbb{Q}[X]$, and some standard pair $(f(X), g(X))$. Write $D := \deg \phi(X)$. Observe that in all cases $D \mid 2a$ and $D \mid 2b$, therefore $D \mid 2\gcd(a,b)$.

Assume first that $D > 2$. Then there exists some divisor $r > 1$ of both a and b such that $r \mid D$. The ratios of the leading terms of $p_a(X)$ and $q_b(X)$ must then be an rth perfect power. Since this ratio is $\Delta b!/a!$, where $\Delta \in \{2^{b-a}, 2^{-a}\}$, and both $b-a$ and a are multiples of r, we get that $b!/a!$ is an rth power. This is impossible by a famous result of Erdős and Selfridge [16] unless $|b-a| \leq 1$. But if $b - a = \pm 1$, then a and b are coprime, so $r = 1$.

Case 1. $D > 2$.

From the above discussion, we deduce that the case $D > 2$ is possible only if $a = b$ and $q_b(X) = \binom{X}{b}$. In this case, $\deg p_a(X) = 2a$ and $\deg q_b(X) = b = a$. We conclude that $\deg f(X) = 2 \deg g(X)$. Analyzing Table 2, it follows that the pair $(f(X), g(X))$ is one of the following:

(i) First kind with $v(X)$ constant, $q = 2$, $r = 1$. In this case, $p_a \circ \kappa_1(X) = \phi(X^2)$, so the coefficients of X^{2a-1} and X^{2a-3} in $p_a \circ \kappa_1(X)$ are zero. This is impossible by Lemma 3.

(ii) Second kind with $v(X)$ linear. In this case, $g(X) = X^2$ and $q_b \circ \kappa_2(X) = \phi(X^2)$ for some polynomial $\phi(X) \in \mathbb{Q}[X]$. Theorem 4.3 in [7] shows that $b = a$ is even and

$$\phi(Z) = \frac{1}{b!}\left(Z - \frac{1}{4}\right)\left(Z - \frac{9}{4}\right)\cdots\left(Z - \frac{(b-1)^2}{4}\right). \tag{20}$$

Furthermore, in this case we have $f(X) = (\alpha X^2 + \beta)v(X)^2$ for some nonzero rational numbers α and β, where $v(X)$ is linear and

$$p_a \circ \kappa_1(X) = \phi(f(X)) = \frac{1}{a!}\prod_{i=1}^{a/2}\left(f(X) - \frac{(2i-1)^2}{4}\right). \tag{21}$$

Observe that the above polynomial $\phi(X)$ is not of the form $\psi(X^2)$ for any $\psi(X) \in \mathbb{Q}[X]$. Thus, by the description of the integer solutions (x,y) from Theorem 4, we get that all but finitely many of them are of the form $x = \kappa_1(u)$ and $y = \kappa_2(w)$ for some rational numbers u and w such that $f(u) = g(w)$.

Observe that u and w are rational numbers with bounded denominators. In fact, letting Γ be the product of the numerators and denominators of all the nonzero coefficients of $\kappa_1(X)$ and $\kappa_2(X)$, we have that both Γu and Γw are integers. Now let us take a closer look at the relation $f(u) = g(w)$. It is

$$u^2 = (\alpha w^2 + \beta)v(w)^2. \tag{22}$$

If $v(w) = 0$, then $u = 0$, and w takes only finitely many values. Hence, at most finitely many integer solutions (x, y) can be obtained in this way.

Assume now that $v(w) \neq 0$. Let $\alpha := \alpha_1/\alpha_2$ and $\beta := \beta_1/\beta_2$, where $\alpha_1, \alpha_2, \beta_1, \beta_2$ are integers, with $\alpha_2 > 0$ and $\beta_2 > 0$, and $\gcd(\alpha_1, \alpha_2) = \gcd(\beta_1, \beta_2) = 1$. Dividing both sides of equation (22) by $v(w)$, and then multiplying both sides of the resulting equation by $\alpha_2^2\beta_2^2\Gamma^2$, we get

$$\left(\frac{\alpha_2\beta_2\Gamma u}{v(w)}\right)^2 = \alpha_1\alpha_2(\beta_2\Gamma u)^2 + (\alpha_2^2\beta_1\beta_2\Gamma^2).$$

Put $u_1 := \beta_2\Gamma u$, $w_1 := \alpha_2\beta_2\Gamma u/v(w)$, $\beta_3 := \alpha_2^2\beta_1\beta_2\Gamma^2$. We then have $u_1 \in \mathbb{Z}$, $\beta_3 \in \mathbb{Z}$, and

$$w_1^2 = \alpha_1\alpha_2 u_1^2 + \beta_3 \in \mathbb{Z}.$$

Hence, $w_1 \in \mathbb{Z}$. We have obtained the equation

$$w_1^2 - (\alpha_1\alpha_2)u_1^2 = \beta_3$$

in integers (u_1, w_1). If $\alpha_1\alpha_2 < 0$, then $\max\{|u_1|, |w_1|\} \leq \beta_3$, therefore there are only finitely many possibilities for the pair (u_1, w_1); hence, for the pair (x, y). Furthermore, if $\alpha_1\alpha_2$ is a square, then both $w_1 - \sqrt{\alpha_1\alpha_2}u_1$ and $w_1 + \sqrt{\alpha_1\alpha_2}u_1$ are integer divisors of β_3. This leads again to only finitely many possibilities for the pair (u_1, w_1); hence, for the pair (x, y). Both these scenarios are impossible. The conclusion therefore is that the parameter $\alpha = \alpha_1/\alpha_2$ must be positive and not a square of a rational number.

Now let us take a closer look at this parameter for our situation. Putting $\kappa_1(X) := \gamma X + \delta$ and $v(X) := \lambda X + \eta$, and identifying leading coefficients in formula (21), we get

$$\frac{\gamma^{2a}}{2^a a!} = \frac{(\alpha\lambda^2)^{a/2}}{a!},$$

therefore

$$\alpha = \pm\frac{\gamma^4}{4\lambda^2} = \pm\left(\frac{\gamma^2}{2\lambda}\right)^2.$$

Hence, either $\alpha < 0$, or α is a perfect square of a rational number, and we saw that none of these situations can happen in our instance.

(iii) Third kind with $s = 2$ and $t = 1$. In this case, $D_2(X, \alpha) = X^2 - \alpha$, therefore $p_a \circ \kappa_1(X) = \phi(D_2(X, \alpha))$ is a polynomial having no monomials of odd degree. In particular, the coefficients of X^{2a-1} and X^{2a-3} in $p_a \circ \kappa_1(X)$ are both 0, contradicting again Lemma 3.

(iv) Fourth kind with $s = 4,\ t = 2$. In this case, a is even, $D = a/2$, $D_4(X, \alpha) = X^4 - 4X^2\alpha + 2\alpha^2$, and

$$p_a \circ \kappa_1(X) = \phi(D_4(X, \alpha)) = C_0(X^4 - 4X^2\alpha + 2\alpha^2)^D + \sum_{1 \le i \le D} C_i(X^4 - 4X^2\alpha + 2\alpha^2)^{D-i}.$$

We see from the above representation, that the coefficients of X^{2a-1} and of X^{2a-3} in $p_a \circ \kappa_1(X)$ are both zero, contradicting again Lemma 3.

(v) Fifth kind: this is impossible since for pairs $(f(X), g(X))$ of this kind we have $\deg f / \deg g = 3/2$.

Hence, we need only to deal with the case when $D \le 2$. Observe that since $\max\{a, b\} > 12$, it follows that $f(X)$ and $g(X)$ cannot form a standard pair of the fifth kind.

Case 2. $D = 1$.

In this case, $\phi(X) \in \mathbb{Q}[X]$ is linear. If $(p_a(X), q_b(X))$ is related to a standard pair $(f(X), g(X))$ such that $f(X)$ is a Dickson polynomial, then $p_a \circ \kappa_1(X)$ has the property that the coefficients of X^{2a-1} and X^{2a-3} are zero, and this is impossible by Lemma 3. Thus, $(p_a(X), q_b(X))$ must be related to a standard pair of the first or second kind. In both such pairs, the polynomial X^q shows up for some $q \ge 2$. Suppose first that $p_a \circ \kappa_1(X) = \phi(X^q) = C_0X^q + C_q$. The number of real roots of such a polynomial is 1 or 2. However, since $p_a(X)$ is one of $F_a(X)$ or $f_a(X)$, it follows that it has at least $a + 1 > 2$ real roots, namely all the numbers of the form $0, 1, \dots, a$. This is a contradiction. Assume now that $q_b \circ \kappa_2(X) = \phi(X^q) = C_0X^q + C_q$ and (for $q_b(X)$ of the form $F_b(X)$ or $f_b(X)$ we get a contradiction as before) $q_b(X) = \binom{X}{b}$. However, again as above, the polynomial $C_0X^q + C_q$ can have at most 2 real roots, while since $b \ge 3$, we get that $q_b(X)$ has $b \ge 3$ real roots, namely all numbers $0, 1, \dots, b - 1$.

Case 3. $D = 2$.

Finally, let us suppose that $D = 2$. Writing γ and λ for the leading terms of $\kappa_1(X)$ and $\kappa_2(X)$, we get, by setting the leading coefficients of $p_a \circ \kappa_1(X)$ and $q_b \circ \kappa_2(X)$ to equal each other, that

$$\frac{\gamma^{2a}}{2^a a!} = \frac{\Delta\lambda^{\delta b}}{b!},$$

where $(\Delta, \delta) := (1, 1)$ if $q_b(X) = \binom{X}{b}$, and $(\Delta, \delta) := (2^{-b}, 2)$ if $q_b(X)$ is one of $F_b(X)$ and $f_b(X)$. In the first case, since D divides the degree of $q_b(X)$, it follows that b is even, while in the second case δb is even. Thus, in all instances we get that $a!/b!$ is a square or twice times a square. Hence, $|b-a| \leq 2$, by a result from [16] (see also [4]).

Assume now that $(p_a(X), q_b(X))$ is related to a standard pair involving Dickson polynomials. Then

$$p_a \circ \kappa_1(X) = C_0 D_a(X, \alpha)^2 + C_1 D_a(X, \alpha) + C_2.$$

Observe that $D_a(X, \alpha)^2$ has no monomials of odd order in it. Thus, if $a > 3$, then $2a - 3 > a = \deg(D_a(X, \alpha))$, so that X^{2a-1} and X^{2a-3} do not appear in $p_a \circ \kappa_1(X)$, which is in contradiction with Lemma 3. But if $a \leq 3$, then $b \leq 5$, and this is impossible since $\max\{a, b\} \geq 13$.

Assume now that $(p_a(X), q_b(X))$ is related to one of the standard pairs of first or second kind. Say $p_a(X) = C_0 x^{2q} + C_1 X^q + C_2$. The derivative of such a polynomial, which is $qX^{q-1}(2C_0 X^q + C_1)$, has at most three distinct real roots. But $p_a(X)$ has $a + 1$ distinct real roots, so the derivative of $p_a \circ \kappa_1(X)$ has at least a distinct real roots by Rolle's theorem. We get a contradiction for $a \geq 4$. But if $a \leq 3$, then $b \leq 5$, which is not allowed. A similar argument applies when $q_b(X) = C_0 X^{2q} + C_1 X^q + C_2$ and $q_b(X)$ is one of $F_b(X)$ or $f_b(X)$ (with $b \geq 4$), or $q_b(X) = \binom{X}{b}$ (with $b \geq 5$). But if $b \leq 4$, then $a \leq 6$, which again is not allowed.

This completes the proof of Theorem 2.

5. Proof of Theorem 3

Our equation can be rewritten as $8S^x_{x-a} + 1 = (2y - 1)^2$. In order to prove that it has only finitely many integer solutions (x, y), it suffices, via Baker's theorem on integral solutions of hyperelliptic equations (cf. [2]), to prove that the polynomial $8F_a(X) + 1 = 8S^X_{X-a} + 1$ has at least three roots of odd multiplicities. We shall assume that this is not so and arrive at a contradiction. We start with a lemma concerning the size of the roots of $8S^X_{X-a} + 1$.

Lemma 4. *If $a \geq 2$ and $z \in \mathbb{C}$ is a zero of $8S^X_{X-a}+1$, then we have $|z| < 10a^2$.*

Proof. We know that the sequence $\{\tilde{S}^{a+k}_k\}_{k=1,\ldots,a}$ is log-concave (see page 81 in [9]). In particular, the sequence

$$\frac{\tilde{S}^{a+k}_k}{\tilde{S}^{a+k+1}_{k+1}} \qquad \text{for} \quad k = 1, 2, \ldots, a-1$$

is increasing with the maximal value being

$$\frac{\tilde{S}_{a-1}^{2a-1}}{\tilde{S}_a^{2a}} = \frac{a-1}{3}.$$

Suppose now that $|z| \geq 10a^2$ is a root of this polynomial. In particular, $|z| > 2a$, so that $(z)_{2a} = z(z-1)\cdots(z-(2a-1)) \neq 0$. Rewrite the fact that $S_{z-a}^z = -1/8$ as

$$\sum_{k=1}^{a-1} \frac{(2a)!}{(a+k)!} \frac{(z)_{a+k}}{(z)_{2a}} \frac{\tilde{S}_k^{a+k}}{\tilde{S}_a^{2a}} = -\frac{1}{8} - \frac{(2a)!}{\tilde{S}_a^{2a}(z)_{2a}}. \tag{23}$$

We take absolute values in equation (23) above and apply the absolute value inequality. Since $\tilde{S}_a^{2a}$ is an integer, $|(z)_{2a}| > (10a^2 - 2a)^{2a} > (8a)^{2a}$ and $(2a)! < (2a)^{2a}$, it follows that

$$\left| \frac{(2a)!}{\tilde{S}_a^{2a}(z)_{2a}} \right| \leq \frac{(2a)^{2a}}{(8a)^{2a}} = \frac{1}{4^{2a}},$$

therefore the absolute value of the right-hand side of relation (23) above is

$$\geq \frac{1}{8} - \frac{1}{4^{2a}} > \frac{1}{9}$$

for $a \geq 2$. In the left-hand side of relation (23), we apply the absolute value inequality getting

$$\sum_{k=1}^{a-1} \frac{(a+k+1)\cdots(2a)}{(|z|-(a+k))\cdots(|z|-(2a-1))} \frac{\tilde{S}_k^{a+k}}{\tilde{S}_a^{2a}} > \frac{1}{9}. \tag{24}$$

Clearly,

$$\begin{aligned}
(a+k+1)\cdots(2a) &< (2a)^{a-k}; \\
\frac{1}{(|z|-(a+k))\cdots(|z|-(2a-1))} &< \left(\frac{1}{10a^2-2a}\right)^{a-k} \leq \frac{1}{5}\left(\frac{1}{2a(a-1)}\right)^{a-k}; \\
\frac{\tilde{S}_k^{a+k}}{\tilde{S}_a^{2a}} &= \frac{\tilde{S}_k^{a+k}}{\tilde{S}_{k+1}^{a+k+1}} \cdots \frac{\tilde{S}_{a-1}^{2a-1}}{\tilde{S}_a^{2a}} \\
&\leq \left(\frac{a-1}{3}\right)^{a-k}
\end{aligned}$$

for all $k = 1, 2, \ldots, a-1$. Multiplying the above inequalities, we get that the general term in the sum appearing in the left-hand side of (24) is

$$\frac{(a+k+1)\cdots(2a)}{(|z|-(a+k))\cdots(|z|-(2a-1))} \frac{\tilde{S}_k^{a+k}}{\tilde{S}_a^{2a}} < \frac{1}{5}\left(\frac{1}{3}\right)^{a-k}.$$

Hence, inequality (24) leads to

$$\frac{1}{9} < \frac{1}{5}\sum_{k=1}^{a-1}\left(\frac{1}{3}\right)^{a-k} < \frac{1}{5}\sum_{m\geq 1}\left(\frac{1}{3}\right)^{m} = \frac{1}{10},$$

which is a contradiction. □

A quick computation of some of the values of its coefficients (see equations (16), for example) gives us that

$$\begin{aligned} 8S_{X-a}^{X} + 1 =& \frac{X^{2a}}{2^{a-3}a!} - \frac{(4a^2-a)X^{2a-1}}{2^{a-3}\cdot 3\cdot a!} + \frac{a(a-1)(16a^2-2a+3)X^{2a-2}}{2^{a-3}\cdot 18\cdot a!} \\ & - \frac{a(a-1)(320a^4-520a^3+202a^2-185a-48)x^{2a-3}}{2^{a-3}\cdot 810\cdot a!} + \cdots + 1 \end{aligned}$$

for $a \geq 2$. Since it has even degree $2a$, it follows that it has an even number of roots of odd multiplicity. If this even number is 0, we then get that the relation

$$8S_{X-a}^{X} + 1 = a_0 f(X)^2$$

holds with some monic polynomial $f(X)$ with rational coefficients, where $a_0 := 1/(2^{a-3}a!)$ is the leading coefficient of $8S_{X-a}^{X} + 1$. Putting $x := 0$, we get

$$f(0)^2 = \frac{1}{a_0} = 2^{a-3}a!,$$

but this is impossible for any $a \geq 3$, since by Bertrand's postulate, the interval $(a/2, a]$ always contains a prime $p \geq 3$ for $a \geq 3$. Such a prime p has the property that $p \| 2^{a-3}a!$, so $2^{a-3}a!$ cannot be the square of a rational number when $a \geq 3$.

It remains to deal with the case when $8S_{X-a}^{X} + 1$ has two roots of odd multiplicity. In this case, we write

$$8S_{X-a}^{X} + 1 = a_0 f(X) g(X)^2, \tag{25}$$

where $f(X) := (X - x_1)(X - x_2)$. Clearly, $f(X) \in \mathbb{Q}[X]$, so either x_1 and x_2 are both rational, or the quadratic polynomial $f(X)$ is irreducible over $\mathbb{Q}$ and then x_1 and x_2 are quadratic and conjugate. Now let us make some remarks about the polynomial

$$a_0^{-1}(8S_{X-a}^{X} + 1).$$

It is a monic polynomial. Using formula (2), we get that this polynomial is

$$(X)_{2a} + \sum_{k=1}^{a-1}(X)_{a+k}\frac{2^a a!}{(a+k)!}\tilde{S}_k^{a+k} + 2^{a-3}a!. \tag{26}$$

We write the above polynomial (26) as

$$\begin{aligned} X^{2a} &- \frac{(4a^2-n)}{3}X^{2a-1} + \frac{a(a-1)(16a^2-2a+3)X^{2a-2}}{18} \\ &- \frac{a(a-1)(320a^4-520a^3+202a^2-185a-48)X^{2a-3}}{810} + \cdots + 2^{a-3}a! \\ &=: \sum_{k=0}^{2a} c_k X^{2a-k}. \end{aligned}$$

Let us get a handle on the denominators of the coefficients c_k for $k = 0, \ldots, 2a$. Write

$$\frac{2^a a!}{(a+k)!}\tilde{S}_k^{a+k} =: \frac{a_{a,k}}{b_{a,k}},$$

where $a_{a,k}$ and $b_{a,k}$ are coprime integers. We need to understand the numbers $b_{a,k}$ and their least common multiple, which we denote by D, as k varies in $\{1, \ldots, a-1\}$.

Now a formula from page 222 in [12], tells us that $\tilde{S}_k^{a+k}$ is a multiple of $1 \cdot 3 \cdots (2k-1)$. Thus, $a_{a,k}/b_{a,k}$ is an integer multiple of the rational number

$$\frac{2^a a! \cdot 1 \cdot 3 \cdots (2k-1)}{(a+k)!} = \frac{2^a a!(2k)!}{2^k k!(a+k)!} = \frac{2^{a-k}a!(2k)!}{k!(a+k)!}.$$

Let p be an arbitrary prime with $2 \le p < 2a$. Let us find an upper bound for its exponent in $b_{a,k}$. Writing $\nu_p(r)$ for the exponent of p in the factorization of r and using the fact that the formula

$$\nu_p(m!) = \sum_{s \ge 1} \left\lfloor \frac{m}{p^s} \right\rfloor$$

holds for all positive integers m, it follows that the exponent of p in $b_{a,k}$ satisfies

$$\nu_p(b_{a,k}) \le \sum_{s \ge 1} \left(\left\lfloor \frac{a+k}{p^s} \right\rfloor - \left\lfloor \frac{a}{p^s} \right\rfloor \right) + \left(\left\lfloor \frac{k}{p^s} \right\rfloor - \left\lfloor \frac{2k}{p^s} \right\rfloor \right). \tag{27}$$

Clearly,

$$\left\lfloor \frac{a+k}{p^s} \right\rfloor - \left\lfloor \frac{a}{p^s} \right\rfloor \in \left\{ \left\lfloor \frac{k}{p^s} \right\rfloor, \ \left\lfloor \frac{k}{p^s} \right\rfloor + 1 \right\},$$

and

$$\left\lfloor \frac{k}{p^s} \right\rfloor - \left\lfloor \frac{2k}{p^s} \right\rfloor \in \left\{ -\left\lfloor \frac{k}{p^s} \right\rfloor, \ -\left\lfloor \frac{k}{p^s} \right\rfloor - 1 \right\},$$

together implying that for a fixed $s \geq 1$, we have

$$\left(\left\lfloor \frac{a+k}{p^s} \right\rfloor - \left\lfloor \frac{a}{p^s} \right\rfloor \right) + \left(\left\lfloor \frac{k}{p^s} \right\rfloor - \left\lfloor \frac{2k}{p^s} \right\rfloor \right) \in \{0, \pm 1\}.$$

Suppose now that $a \geq 1000$. Suppose also that $p \geq a/22$. Then $p^2 \geq a^2/22^2 > 2a$. Thus, in formula (27) we have that

$$\nu_p(b_{a,k}) \leq 1 \quad \text{for} \quad p \geq a/22 \quad \text{assuming that} \quad a \geq 1000.$$

For the remaining primes $p < a/22$, we have that

$$\nu_p(b_{a,k}) \leq \sum_{\substack{s \geq 1 \\ p^s \leq 2a}} 1 \leq \frac{\log(2a)}{\log p}.$$

Hence, we have that

$$B := \prod_{\substack{p^{a_p} \| \mathrm{lcm}[b_{a,k} : 1 \leq k \leq a-1] \\ p < a/22}} p^{a_p} \leq \prod_{p < a/22} p^{\log(2a)/\log p} \leq (2a)^{\pi(a/22)}.$$

We conclude that

$$D := \mathrm{lcm}[b_{a,k} : 1 \leq k \leq a-1] = BC,$$

where

$$B = \prod_{\substack{p^{a_p} \\ p < a/22}} p^{a_p} < \exp\left(\pi\left(\frac{a}{22} \right) \log(2a) \right), \qquad \text{and} \qquad C := \prod_{\substack{a/22 \leq p \leq 2a \\ b_p \in \{0,1\}}} p^{b_p}. \quad (28)$$

Now let $z \in \{x_1, x_2\}$ be some root of $f(x)$. We first deal with the case when z is rational. It is clear that the denominator of z divides D but we can do better. Namely, we show that the denominator of z divides B. Indeed, to see why, assume that $p \geq a/22$ divides the denominator of z. Since C is squarefree, it follows that pz is a rational number having both numerator and denominator coprime to p. Multiplying relation

$$z^{2a} - \frac{(4a^2 - a) z^{2a-1}}{3} + \cdots + 2^{a-3} a! = 0$$

with p^{2a} and regrouping, we get

$$(pz)^{2a} = \frac{p(4a^2 - a)}{3} (pz)^{2a-1} - \sum_{k=2}^{2a} p^k c_k (pz)^{2a-k}. \quad (29)$$

Since $p > 3$ (because $a/22 > 3$ for $a \geq 1000$), and the denominator of c_k is not a multiple of p^2 for any $k = 2, \ldots, 2a$, it follows easily that the right-hand side of the above formula is a rational number whose numerator in reduced form is a multiple of p, while the left-hand side is a rational number which in reduced form has numerator coprime to p. This contradiction shows that the denominator of z is a divisor of B. We now write $x_1 := u_1/v_1,\ x_2 := u_2/v_2$ with $u_1,\ u_2,\ v_1 > 0,\ v_2 > 0$ integers such that $\gcd(u_1, v_1) = \gcd(u_2, v_2) = 1$, and evaluate relation (25) in $x := 0$ getting

$$2^{a-3} n! = x_1 x_2 g(0)^2,$$

In particular, it follows that $u_1 u_2$ is a multiple of all primes $p \in (a/2, a]$. Hence,

$$|u_1 u_2| \geq \prod_{a/2 < p \leq a} p > \left(\frac{a}{2}\right)^{\pi(a)-\pi(a/2)}. \tag{30}$$

Thus,

$$|u_1 u_2| \geq \left(\frac{a}{2}\right)^{\pi(a)-\pi(a/2)}. \tag{31}$$

Assuming say that $|u_1| \geq |u_2|$, we conclude that

$$|u_1| \geq (|u_1 u_2|)^{1/2} \geq \exp\left(\frac{1}{2}\left(\pi(a) - \pi\left(\frac{a}{2}\right)\right)\log\left(\frac{a}{2}\right)\right).$$

Hence, using the fact that $v_1 \mid B$ and estimate (28), we get that

$$\begin{aligned} |x_1| &= |u_1| v_1^{-1} \geq |u_1| B^{-1} \\ &\geq \exp\left(\frac{1}{2}\left(\pi(a) - \pi\left(\frac{a}{2}\right)\right)\log\left(\frac{a}{2}\right) - \pi\left(\frac{a}{22}\right)\log(2a)\right). \end{aligned}$$

However, Lemma 4 implies that $|x_1| \leq 10a^2$. We thus get the inequality

$$\log(10a^2) \geq \frac{1}{2}\left(\pi(a) - \pi\left(\frac{a}{2}\right)\right)\log\left(\frac{a}{2}\right) - \pi\left(\frac{a}{22}\right)\log(2a). \tag{32}$$

Using the inequalities

$$\frac{x}{\log x - 0.5} < \pi(x) < \frac{x}{\log x - 1.5} \qquad \text{for all} \quad x \geq 67,$$

(see Theorem 2 in [27]) with $x = a,\ a/2$, and $a/22$ respectively, we get that

$$\log(10a^2) \geq \frac{1}{2}\left(\frac{a}{\log a - 0.5} - \frac{a}{2(\log(a/2) - 1.5)}\right)\log\left(\frac{a}{2}\right) - \frac{a\log(2a)}{22(\log(a/22) - 1.5)} \tag{33}$$

for $a \geq 1474$. The condition $a \geq 1474$ arises from the condition $a/22 \geq 67$, which is necessary for Theorem 2 in [27] to apply. On the other hand, the inequality (33) above yields $a < 1200$. This shows that in fact the inequality $a < 1474$ must hold. Then we also checked that the inequality (32) holds for no $a \in [1000, 1474]$. Thus, we must in fact have $a < 1000$, assuming that one of (hence, both) x_1 or x_2 is rational.

From now on, we treat the slightly more complicated case of the quadratic roots x_1 and x_2. As in the previous case, we assume that $a \geq 1000$ for this case also.

Let us write

$$x_{1,2} = \frac{u \pm v\sqrt{d}}{c},$$

where $u,\ v,\ w > 0$ and $d \neq 1$ are integers, with d squarefree. We may also assume that there is no common prime factor number dividing all three of $u,\ v$ and c. Since $Dx_{1,2}$ are algebraic integers, it follows easily that $c/\gcd(c, D) = 1,\ 2$. The plan is to show that c and C are coprime. This will show that $c \leq 2B$. Well, let's do it. Assume that there is some prime $p \geq a/22$ dividing c. We distinguish three possibilities:

(i) $p \nmid u^2 - dv^2$;

(ii) $p \mid u^2 - dv^2$, and $p \mid u$;

(iii) $p \mid u^2 - dv^2$, but $p \nmid u$.

The first instance is similar to the case in which one of (hence, both) x_1 or x_2 are rational whose denominator is a multiple of p. Indeed, assuming that we are in Case (i) above, relation (29) with $z = x_1$ has the property that the number appearing in its left-hand side is a quadratic algebraic number whose norm is a rational number having both numerator and denominator coprime to p. The right-hand side of the same relation however, is the product between p and a linear combination (with rational coefficients, the denominators of which are not multiples of p) of quadratic algebraic numbers the denominators of which are also coprime to p. Hence, upon taking norms in (29) relative to the quadratic field $\mathbb{K} := \mathbb{Q}[x_1]$, the left-hand side evaluates to a rational number having both numerator and denominator coprime to p, while the right-hand side evaluates to a rational number which in reduced form has its numerator a multiple of p. This is a contradiction.

A somewhat similar argument works for Case (ii). Here, one notices that

with $z := x_1$ we have

$$(pz)^k = \left(\frac{u+v\sqrt{d}}{c/p}\right)^k = p^{k/2}\left(\frac{u/\sqrt{p}+v\sqrt{d/p}}{c/p}\right)^k =: p^{k/2}\lambda^k,$$

where $\lambda := (u/\sqrt{p}+v\sqrt{d/p})/(c/p)$ is a quadratic or bi-quadratic (depending on whether $d = p$, or not) algebraic number, which is the ratio of two algebraic integers $u/\sqrt{p}+v\sqrt{d/p}$ and c/p, having norms powers of $(u^2-dv^2)/p$ and $(c/p)^2$, which are both integers coprime to p. Thus, relation (29) becomes

$$\begin{aligned} p^n\lambda^{2a} = p^a\Bigg(&\frac{(4a^2-a)}{3}p^{1/2}\lambda^{2a-1} - \frac{a(a-1)(16a^2-2a+3)^{2a-2}p}{18}\lambda^{2a-2} \\ &- \sum_{k=3}^{2a} p^{k/2}c_k\lambda^{2a-k}\Bigg) =: p^a\gamma. \end{aligned} \tag{34}$$

Observe that if $k \geq 3$, then $p^{k/2}c_k\lambda^{2a-k}$ is the product between $p^{1/2}$ and some algebraic number the norm of which has denominator coprime to p. The same is true for $k = 2$ since $p \geq a/22 > 3$ (because $a \geq 1000$). Thus, simplifying both sides of relation (34) by p^a, putting $\beta := \gamma/p^{1/2}$, and then taking norms in $\mathbb{L} := \mathbb{Q}[p^{1/2}, \lambda]$ of both sides of the resulting identity, we end up with an equality between $N_{\mathbb{L}}(\lambda^{2a})$, which is a rational number having numerator and denominator coprime to p, and $N_{\mathbb{L}}(p^{1/2}\beta) = p^\ell N_{\mathbb{L}}(\beta)$, with $\ell = 1$ or 2, according to whether the degree of $\mathbb{L}$ over $\mathbb{Q}$ is 2 or 4, where $N_{\mathbb{L}}(\beta)$ is a rational number whose denominator is coprime to p. This is a contradiction.

Finally, let us look at the possible primes occurring in Case (iii). In this case, $x_1 + x_2 = u/c = d_1/p$, where d_1 is some rational number having both numerator and denominator coprime to p. Observe also that $x_1x_2 = (u^2 - dv^2)/c^2$. We distinguish two cases.

Case (iii.1) $p \| u^2 - dv^2$.

In this case,

$$f(x) = x^2 + \frac{d_1x}{p} + \frac{d_2}{p},$$

where d_2 is a rational number having numerator and denominator coprime to p. We write

$$g(x)^2 = x^{2a-2} + e_1x^{2a-3} + e_2x^{2a-4} + \cdots + e_{2a-2}, \tag{35}$$

and prove by induction on $m \geq 1$ that $e_m = f_m/p^m$, where f_m is a rational number having numerator and denominator coprime to p. Indeed, multiplying

$f(x)$ with $g(x)^2$ and identifying coefficients, we get

$$\begin{aligned} f(x)g(x)^2 &= x^{2a} - \frac{(4a^2-a)}{3}x^{2a-1} + \frac{a(a-1)(16a^2-2a+3)}{18}x^{2a-2} + \cdots \\ &= x^{2a} + \left(\frac{d_1}{p} + e_1\right)x^{2a-1} + \left(\frac{d_2}{p} + \frac{d_1e_1}{p} + e_2\right)x^{2a-2} + \cdots . \end{aligned}$$

Since the denominator of $(4a^2-a)/3$ is not a multiple of p, we get that $e_1 = f_1/p$ with f_1 a rational number whose numerator and denominator is coprime to p. Thus, indeed e_1 has the desired shape. Now

$$c_2 = \frac{d_2}{p} + \frac{d_1e_1}{p} + e_2 = \frac{d_2}{p} + \frac{d_1f_1}{p^2} + e_2,$$

and the denominator of c_2 is not a multiple of p, showing that $e_2 = f_2/p^2$, where the numerator and denominator of f_2 are coprime to p. Assuming that e_i has the desired shape f_i/p for $i = 1, \ldots, m$ and some $1 < m < 2a-2$, and computing the coefficient of $x^{2a-(m-1)}$, we get

$$c_{m+1} = \frac{d_2e_{m-1}}{p} + \frac{d_1e_m}{p} + e_{m+1} = \frac{d_2f_{m-1}}{p^m} + \frac{d_1f_m}{p^{m+1}} + e_{m+1}.$$

Since the denominator of c_{m+1} is not divisible by p^2, we get that indeed $e_{m+1} = f_{m+1}/p^{m+1}$ for some rational number f_{m+1} having numerator and denominator both coprime to p. Thus, the last coefficient of $f(x)g(x)^2$ is $d_2e_{2a-2}/p = d_2f_{2a-2}/p^{2a-1}$, which is impossible since this coefficient must be the integer $2^{a-3}a!$. Hence, this case is impossible.

Case (iii.2) $p^2 \mid u^2 - dv^2$.

Part of this case is similar to the previous one. Here, we have

$$f(x) = x^2 + \frac{d_1x}{p} + d_2,$$

where d_2 is a rational number whose denominator is coprime to p. In the notation (35), one gets that

$$f(x)g(x)^2 = x^{2a} + \left(\frac{d_1}{p} + e_1\right)x^{2a-1} + \left(d_2 + \frac{d_1e_1}{p} + e_2\right)x^{2a-2} + \cdots .$$

From the above, we see right away that $e_1 = f_1/p$, where f_1 is a rational number whose numerator and denominator are coprime to p, and then that

$$c_2 = d_2 + \frac{d_1e_1}{p} + e_2 = d_2 + \frac{d_1f_1}{p^2} + e_2.$$

Since the denominator of c_2 is not a multiple of p, we get that $e_2 = f_2/p^2$, where f_2 is a rational number whose numerator and denominator are coprime to p. By induction over $m \geq 1$, we get as in the previous case that $e_m = f_m/p^m$, where f_m is a rational number whose numerator and denominator are coprime to p. For the induction step, we use the formula

$$c_{m+1} = d_2 e_{m-1} + \frac{d_1 e_m}{p} + e_{m+1} = \frac{d_2 f_{m-1}}{p^{m-1}} + \frac{d_1 f_m}{p^{m+1}} + e_{m+1}.$$

By looking at the last coefficients, we have $d_2 e_{2a-2} = d_2 f_{2a-2}/p^{2a-2}$. Since this last coefficient is in fact an integer, it follows that $\nu_p(d_2) \geq 2a-2$, which in turn implies that $\nu_p(u^2 - dv^2) \geq 2a$.

Hence, so far, we conclude that if c has prime factors p in $[a/22, 2a]$, then $\nu_p(u^2 - dv^2) \geq 2a$. Now write

$$c = c_1 C_1,$$

where $C_1 = \gcd(c, C)$ and $c_1 \mid 2B$. It then follows that

$$|u^2 - dv^2| \geq C_1^{2a},$$

so that

$$|x_1 x_2| = \left| \frac{u^2 - dv^2}{c^2} \right| = \left| \frac{u^2 - dv^2}{c_1^2 C_1^2} \right| \geq C_1^{2a-2} (2B)^{-2}.$$

Using Lemma 4 and inequality (28) we arrive at

$$400 a^4 (2a)^{2\pi(a/22)} > C_1^{2a-2}.$$

Assuming that $C_1 > 1$, and using the trivial fact that $\pi(x) < x$, we are led to the inequality

$$400 a^4 (2a)^{a/11} > \left(\frac{a}{22}\right)^{2a-2},$$

which is false for any $a \geq 40$. So, this case cannot occur either.

Hence, we have just shown that c divides $2B$. Thus, $4B^2 |x_1 x_2|$ is an integer which, by Lemma 4, is at most as large as

$$(10a^2)^2 (4B^2).$$

However, since $4B^2 x_1 x_2 = 4B^2 f(0) = 4B^2 2^{a-3} a! g(0)^{-2}$, it follows easily, that this integer is a multiple of

$$\prod_{a/2 < p \leq a} p > \left(\frac{a}{2}\right)^{\pi(a) - \pi(a/2)}.$$

So, we get that

$$400a^4B^2 > \left(\frac{a}{2}\right)^{\pi(a)-\pi(a/2)},$$

which via inequality (28) leads to

$$400a^4 > \exp\left(\left(\pi(a) - \pi\left(\frac{a}{2}\right)\right)\log\left(\frac{a}{2}\right) - 2\pi\left(\frac{a}{22}\right)\log(2a)\right).$$

Taking square-roots and then logarithms, we get

$$\log(20a^2) > \frac{1}{2}\left(\pi(a) - \pi\left(\frac{a}{2}\right)\right)\log\left(\frac{a}{2}\right) - \pi\left(\frac{a}{22}\right)\log(2a).$$

This last inequality is only slightly worse than (33) and in fact, assuming again that $a \geq 1474$ so that the inequalities from [27] hold, it yields to the contradiction $a < 1200$. Again we checked with Mathematica that in fact the inequality does not hold for any $a \in [1000, 1474]$ either.

This argument shows that indeed $8S^X_{X-a} + 1$ has at least four simple roots for all $a \geq 1000$. It remains to check it when $a < 1000$.

Here is how we checked it. We first used the Principle of Inclusion and Exclusion to get that

$$\tilde{S}^{a+k}_k = \sum_{i=0}^{k-1}(-1)^i\binom{a+k}{i}S^{a+k-i}_{k-i}.$$

Thus,

$$\begin{aligned} S^X_{X-a} &= \sum_{k=1}^{a}\binom{X}{a+k}\sum_{i=0}^{k-1}(-1)^i\binom{a+k}{i}S^{a+k-i}_{k-i} \\ &= \sum_{\ell=1}^{a}S^{a+\ell}_{\ell}\sum_{k=\ell}^{a}(-1)^{k-\ell}\binom{a+k}{k-\ell}\binom{X}{a+k}. \end{aligned}$$

MAPLE simplified the inner sum to

$$\binom{X}{2a+1}(-1)^{a-\ell+1}\frac{a-\ell+1}{a+\ell-X}\binom{2a+1}{a+\ell}.$$

Hence,

$$1 + 8S^X_{X-a} = 1 + 8\binom{X}{2a+1}\sum_{k=1}^{a}(-1)^{a-k+1}\frac{a-k+1}{a+k-X}\binom{2a+1}{a+k}S^{a+k}_k.$$

Using this representation, we checked with Mathematica that the values of the above polynomials assume signs

x	$-\infty$	$1/2$	1	$5/2$	$+\infty$
$\operatorname{sign}(1+8S^x_{x-a})$	$+$	$-$	$+$	$-$	$+$

for all $a \in [10, 1000]$. But a polynomial having such sign changes cannot be of the form $a_0 f(X) g(X)^2$ with $a_0 > 0$, $f(X)$ and $g(X)$ both monic, and $f(X)$ of degree 2. Thus, it remains to study the values of $a \leq 9$. A quick check with Mathematica shows that except for the case $a = 1$ when

$$8S^X_{X-1} + 1 = (2X-1)^2,$$

for all other values $a \in [2, 9]$ the polynomial $8S^X_{X-a} + 1$ has only simple roots.

We conjecture that $8S^X_{X-a} + 1$ is irreducible for all $a \geq 2$, and we leave this as an another open problem for the reader.

References

[1] P. Alvanos, Yu. F. Bilu and D. Poulakis, Characterizing algebraic curves with infinitely many integral points, *Int. J. Number Th.* **5** (2009), 585–590.

[2] A. Baker, Bounds for the solutions of the hyperelliptic equation, *Proc. Camb. Phil. Soc.* **65** (1969), 439–444.

[3] M. A. Bennett, Rational approximation to algebraic numbers of small height: the Diophantine equation $|ax^n - by^n| = 1$, *J. Reine Angew. Math.* **535** (2001), 1–49.

[4] M. A. Bennett, Products of consecutive integers, *Bull. London Math. Soc.* **36** (2004), 683–694.

[5] F. Beukers, T. N. Shorey and R. Tijdeman, Irreducibility of polynomials and arithmetic progressions with equal products of terms, Number theory in progress, Vol. 1 (Zakopane-Kościelisko, 1997), *de Gruyter*, *Berlin*, 1999, 11–26.

[6] Yu. F. Bilu, Quadratic factors of $f(x) - g(y)$, *Acta Arith.* **90** (1999), 341-355.

[7] Yu. F. Bilu, B. Brindza, P. Kirschenhofer, Á. Pintér and R. F. Tichy, Diophantine equations and Bernoulli polynomials. With an appendix by A. Schinzel, *Compositio Math.* **131** (2002), 173–188.

[8] Yu. F. Bilu and R. F. Tichy, The Diophantine equation $f(x) = g(y)$, *Acta Arith.* **95** (2000), 261–288.

[9] F. Brenti, Unimodal, log-concave and Pólya frequency sequences in combinatorics, *Memoirs Amer. Math. Soc.* **81** (1989).

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

[11] Y. Bugeaud, M. Mignotte, S. Siksek, M. Stoll and Sz. Tengely, Integral points on hyperelliptic curves, *Algebra Number Theory* **2** (2008), 859–885.

[12] L. Comtet, Advanced Combinatorics, *D. Reidel Publishing Company*, 1974.

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

[14] P. Corvaja and U. Zannier, Some new applications of the subspace theorem, *Compositio Math.* **131 no. 3** (2002), 319–340.

[15] P. Erdős, On a Diophantine equation, *J. London Math. Soc.* **26** (1951), 176–178.

[16] P. Erdős and J. L. Selfridge, The product of consecutive integers is never a power, *Illinois J. Math.* **19** (1975), 292–301.

[17] J. Ferenczik, Á. Pintér and B. Porvázsnyik, On equal values of Stirling numbers of the second kind, *Appl. Math. Comput.* **218** (2011), 980–984.

[18] M. Fried, Arithmetical properties of function fields. II. The generalized Schur problem, *Acta Arith.* **25** (1973/74), 225–258.

[19] C. Fuchs, Polynomial-exponential equations involving multi-recurrences, *Studia Sci. Math. Hungar.* **46** (2009), 377–398.

[20] C. Fuchs and A. Scremin, Polynomial-exponential equations involving several linear recurrences, *Publ. Math. Debrecen* **65** (2004), 149–172.

[21] K. Győry, On the Diophantine equation $\binom{n}{k} = x^l$, *Acta Arith.* **80** (1997), 289–295.

[22] M. Klazar and F. Luca, On some arithmetic properties of polynomial expressions involving Stirling numbers of the second kind, *Acta Arith.* **107** (2003), 357–372.

[23] D. W. Masser, Polynomial bounds for diophantine equations, *Amer. Math. Monthly* **93** (1986), 486–488.

[24] M. Mignotte, A note on the equation $ax^n - by^n = c$, *Acta Arith.* **75** (1996), 287–295.

[25] Á. Pintér, On a Diophantine problem concerning Stirling numbers, *Acta Math. Hungar.* **65** (1994), 361–364.

[26] D. Poulakis, A simple method for solving the diophantine equation $Y^2 = X^4 + aX^3 + bX^2 + cX + d$, *Elem. Math.* **54** (1999), 32–36.

[27] J. B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. Math.* **6** (1962), 64–94.

[28] W. M. Schmidt, Diophantine approximations and Diophantine equations, Lecture Notes in Mathematics, Vol. 1467, *Springer-Verlag*, *Berlin*, 1991.

[29] T. N. Shorey and R. Tijdeman, Exponential diophantine equations, Cambridge Tracts in Mathematics, Vol. 87, *Cambridge University Press*, *Cambridge*, 1986.

[30] Th. Stoll, R. F. Tichy, The Diophantine equation $\alpha\binom{x}{m} + \beta\binom{y}{n} = \gamma$, *Publ. Math. Debrecen* **64** (2004), 155–165.

[31] R. J. Stroeker and B. M. M. de Weger, Elliptic binomial Diophantine equations, *Math. Comp.* **68** (1999), 1257–1281.

[32] G. Turnwald, On Schur's conjecture, *J. Austral. Math. Soc.* **58** (1995), 312–357.

[33] P. G. Walsh, A quantitative version of Runge's theorem on Diophantine equations, *Acta Arith.* **62** (1992), 157–172; Correction to: A quantitative version of Runge's theorem on Diophantine equations, *Acta Arith.* **73** (1995), 397–398.

YURI F. BILU
IMB
UNIVERSITÉ BORDEAUX 1
351 COURS DE LA LIBRATION
33405 TALENCE
FRANCE

E-mail: yuri.bilu@math.u-bordeaux1.fr

CLEMENS FUCHS
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF SALZBURG
HELLBRUNNERSTR. 34/I
5020 SALZBURG
AUSTRIA

E-mail: clemens.fuchs@math.ethz.ch

FLORIAN LUCA
MATHEMATICS CENTRE
UNAM
AP. POSTAL 61-3 (XANGARI)
CP 58 089 MORELIA, MICHOACÁN
MEXICO

E-mail: fluca@matmor.unam.mx

ÁKOS PINTÉR
INSTITUTE OF MATHEMATICS, MTA-DE RESEARCH GROUP "EQUATIONS, FUNCTIONS AND CURVES"
HUNGARIAN ACADEMY OF SCIENCES AND UNIVERSITY OF DEBRECEN
P. O. BOX 12, H-4010 DEBRECEN
HUNGARY

E-mail: apinter@science.unideb.hu

(Received March 7, 2012)