DIOPHANTINE m-TUPLES FOR LINEAR POLYNOMIALS. II. EQUAL DEGREES

ANDREJ DUJELLA*, CLEMENS FUCHS‡, AND GARY WALSH

Abstract. In this paper we prove the best possible upper bounds for the number of elements in a set of polynomials with integer coefficients all having the same degree, such that the product of any two of them plus a linear polynomial is a square of a polynomial with integer coefficients. Moreover, we prove that there does not exist a set of more than 12 polynomials with integer coefficients and with the property from above. This significantly improves a recent result of the first two authors with R. F. Tichy [10].

2000 *Mathematics Subject Classification:* 11D09, 11C08.
Keywords: diophantine m-tuples, linear polynomials, Mason's inequality, function fields.

1. Introduction

Let n be a nonzero integer. A set of m positive integers $\{a_1, a_2, \ldots, a_m\}$ is called a Diophantine m-tuple with the property $D(n)$ or simply $D(n)$-m-tuple, if the product of any two of them increased by n is a perfect square.

Diophantus [2] found the first quadruple $\{1, 33, 68, 105\}$ with the property $D(256)$. The first $D(1)$-quadruple, the set $\{1, 3, 8, 120\}$, was found by Fermat. The folklore conjecture is that there does not exist a $D(1)$-quintuple. In 1969, Baker and Davenport [1] proved that the Fermat's set cannot be extended to a $D(1)$-quintuple. Recently, the first author proved that there does not exist a $D(1)$-sextuple and there are only finitely many $D(1)$-quintuples (see [5]). Moreover, the first and the second author proved that there does not exist a $D(-1)$-quintuple (see [9]).

The natural question is how large such sets can be. We define

$$M_n = \sup\{|S| : S \text{ has the property} D(n)\},$$

*The first author was supported by the Ministry of Science, Education and Sports, Republic of Croatia, grant 0037110.
‡The second author was supported by the Austrian Science Foundation FWF, grant S8307-MAT.
This paper was partly written during a visit of the first author at the Department of Mathematics, Graz University of Technology within a joint Austrian-Croatian project granted by the Croatian Ministry of Science, Education and Sport and the Austrian Exchange Service (Nr. 20/2004).

where $|S|$ denotes the number of elements in the set S. The first author proved that

$$M_n \leq 31 \quad \text{for } |n| \leq 400,$$
$$M_n < 15.476 \log |n| \quad \text{for } |n| > 400$$

(see [4, 6]).

A polynomial variant of the above problems was first studied by Jones [12], [13], and it was for the case $n = 1$.

Definition 1. *Let $n \in \mathbb{Z}[x]$ and let $\{a_1, a_2, \dots, a_m\}$ be a set of m nonzero polynomials with integer coefficients. We assume that there does not exist a polynomial $p \in \mathbb{Z}[x]$ such that $a_1/p, \dots, a_m/p$ and n/p^2 are integers. The set $\{a_1, a_2, \dots, a_m\}$ is called* a polynomial $D(n)$-m-tuple *if for all $1 \leq i < j \leq m$ the following holds: $a_i \cdot a_j + n = b_{ij}^2$, where $b_{ij} \in \mathbb{Z}[x]$.*

In analog to the above results, we are interested in the size of

$$P_n = \sup\{|S| : S \text{ is a polynomial } D(n)\text{-tuple}\}.$$

From [4, Theorem 1], it follows that $P_n \leq 22$ for all $n \in \mathbb{Z}$. The above mentioned result about the existence of only finitely many $D(1)$-quintuples implies that $P_1 = 4$. The first and the second author proved that $P_{-1} = 3$ (cf. [7]). Moreover, in [8] they proved that if $\{a, b, c, d\}$ is a polynomial $D(1)$-quadruple, then

$$(a + b - c - d)^2 = 4(ab + 1)(cd + 1),$$

which implies that every polynomial $D(1)$-triple can be extended to a polynomial $D(1)$-quadruple in an essentially unique way, which in turn gives $P_1 = 4$ once again.

Another polynomial variant of the problem was considered by the first author and Luca [11]. They considered sets of polynomials with the property that the product of any two elements plus 1 is a perfect kth power and they proved sharp upper bounds for the size of such sets.

The first and second author together with Tichy [10] considered the case of linear polynomials, i.e. $n = ax + b$, with integers $a \neq 0$ and b. Let us define

$$L = \sup\{|S| : S \text{ is a polynomial } D(ax + b)\text{-tuple for some } a \neq 0 \text{ and } b\},$$

and let us denote by L_k the number of polynomials of degree k in a polynomial $D(ax + b)$-m-tuple S. Trivially, $L_0 \leq 1$. We proved that

$$L_1 \leq 8, \quad L_2 \leq 5, \quad L_k \leq 3 \quad \text{for all } k \geq 3,$$

(see [10, Propositions 1,2 and 3]) and

$$L \leq 26$$

(see [10, Theorem 1]). Moreover, we proved that there are at most 15 polynomials of degree ≥ 4 in such a set S.

In this paper we will give sharp upper bounds for L_k for all $k \geq 1$. Moreover, we will significantly improve the upper bound for L.

Theorem 1. *There does not exist a set of five linear polynomials with integer coefficients and the property that the product of any two of then plus the linear polynomial $n = ax + b$ with integers $a \neq 0$ and b is a square in $\mathbb{Z}[x]$.*

This solves the problem for linear polynomials completely, in view of the following example:

$$\{x, 16x + 8, 25x + 14, 36x + 20\}$$

is a polynomial $D(16x + 9)$-quadruple (see [3]).

The idea of the proof of Theorem 1 is the following: first we show that we may assume that one of the polynomials is a multiple of x, then we reduce the defining equations, which is a quadratic polynomial in x that is a square and therefore has vanishing discriminant, to a system of Diophantine equations for the coefficients. In the above example, the question of extendability reduces to finding all integer solutions of

$$n^2(3m - 8) + m^2(3n - 8)^2 - m^2n^2(36mn - 9(m + n) + 265) = 0,$$

which gives

$$(3mn - 8m - 8n + 8)(3mn - 8m - 8n - 8)(m - n + 1)(m - n - 1) = 0,$$

from which a contradiction can be derived.

The next theorem now deals with the case of quadratic polynomials.

Theorem 2. *There does not exist a set of four quadratic polynomials with integer coefficients and the property that the product of any two of them plus the linear polynomial $n = ax + b$ with integers $a \neq 0$ and b is a square in $\mathbb{Z}[x]$.*

Also this result is best possible since the set

$$\{9x^2 + 8x + 1, 9x^2 + 14x + 6, 36x^2 + 44x + 13\}$$

is a polynomial $D(4x+3)$-triple. Let us note that this triple can be extended to the $D(4x + 3)$-quadruple

$$\{1, 9x^2 + 8x + 1, 9x^2 + 14x + 6, 36x^2 + 44x + 13\}$$

(see [3]).

Corollary 1. *We have*

$$L_1 \leq 4, \quad L_k \leq 3 \quad \textit{for all } k \geq 2.$$

Moreover, all these bounds are sharp.

In order to show that the bound $L_k \leq 3$ for $k \geq 3$ is sharp, let us consider the following examples

$$\{x^{2k} - x, x^{2k} + 2x^k - x + 1, 4x^{2k} + 4x^k - 4x + 1\},$$
$$\{x^{2k-1} - 1, x^{2k-1} + 2x^k + x - 1, 4x^{2k-1} + 4x^k + x - 4\},$$

for $k = 1, 2, 3, \ldots$, which are polynomial $D(x)$-triples consisting of three polynomials with the same degree.

Using the new information from Theorems 1 and 2 together with a closer look at the case of polynomials with "large" degrees, we can prove the following result:

Theorem 3.

$$L \leq 12.$$

In analog to the classical integer case, we prove our result for "large" degree by using Mason inequality [14], which is the function field analog of Baker's method for linear forms in logarithms of algebraic numbers, to solve a certain elliptic equation over a function field in one variable, which is done by following the original ideas of Siegel [16].

In Section 2, we will consider the cases of equal degrees and give proofs of Theorems 1 and 2, which immediately imply Corollary 3. In Section 3 we prove an upper bound for the degree of the largest element in a $D(n)$-quadruple by considering the corresponding elliptic equation over a function field. In the last section (Section 4), by combining this upper bound with a gap principle and Theorems 1 and 2, we give a proof of Theorem 3.

2. Sets with polynomials of equal degree

First, we will handle the case of linear polynomials and therefore give a proof of Theorem 1. Afterwards, we consider the case of quadratic polynomials and therefore prove Theorem 2. Corollary 1 is then an immediate consequence of these two theorems together with the remark after [10, Proposition 2] in the first part to this paper.

2.1. Linear polynomials and proof of Theorem 1.

Let $\{ax+b, cx+d, ex+f\}$ be a polynomial $D(ux+v)$-triple. Then $\{a^2x+ab, acx+ad, aex+af\}$ is a polynomial $D(a^2ux+a^2v)$-triple. By substitution $ax = y$, it follows that $\{ay+ab, cy+ad, ey+af\}$ is a $D(auy+a^2v)$-triple, and finally by substitution $y+b=z$, we conclude that

$$\{az, cz+d', ez+f'\} \quad \text{is a polynomial } D(auz+v')\text{-triple},$$

where $d' = ad - cb, f' = af - eb, v' = a^2v - abu$.

We may assume that $\gcd(a,c,e)=1$, since otherwise we substitute $z' = z\gcd(a,c,e)$. This implies that a, c and e are perfect squares:

$$a = A^2, \quad c = C^2, \quad e = E^2,$$

where A, C, E are positive integers. Furthermore, by specializing $z = 0$, we see that v' is also a perfect square: $v' = V^2$. But we have

$$v' = a^2v - abu = A^4v - A^2bu = V^2.$$

Hence, $V = AW$ with $W^2 = A^2v - bu$.

Now from

$$A^2z \cdot (C^2z + d') + (A^2uz + A^2W^2) = (ACz \pm AW)^2,$$

we find by comparing the coefficients of z that $A^2d' + A^2u = \pm 2A^2CW$ and therefore $d' = \pm 2CW - u$. Analogously, $f' = \pm 2EW - u$. Hence, we obtained the set $\{A^2z, C^2z \pm 2CW - u, E^2z \pm 2EW - u\}$ which is a polynomial $D(A^2uz + A^2W^2)$-triple. It means that

$$(C^2z \pm 2CW - u) \cdot (E^2z \pm 2EW - u) + (A^2uz + A^2W^2)$$

is a square of a linear polynomial and this implies that the discriminant of this quadratic polynomial is equal to 0. The discriminant can be factored into 4 factors:

$$(C-E-A)(C-E+A)(\pm 2CEW - Cu - Eu + Au)(\pm 2CEW - Cu - Eu - Au),$$

which can be easily checked.

Assume now that there exists a $D(ux+v)$-quintuple consisting of 5 linear polynomials. The above construction shows that in this case there exists a $D(A^2uz + A^2W^2)$-quintuple with one element equal to A^2z and with all other elements of the form

$$m_i^2z + 2m_iW - u \quad \text{for} \quad i = 1, 2, 3, 4.$$

Observe that the m_i can be positive or negative corresponding to the sign of W. Let

$$m_1 = \min\{m_1, m_2, m_3, m_4\}.$$

Then one of the remaining m_i's is equal to $m_1 + A$ and the other two come from the factors $\pm 2CEW - Cu - Eu + Au, \pm 2CEW - Cu - Eu - Au$. The condition $\pm 2ECW - Cu - Eu = Au$ or $-Au$ is equivalent to $(\pm 2CW - u)(\pm 2EW - u) = u^2 + 2AWu$ or $u^2 - 2AWu$. Therefore, let us denote

$$p_i := 2m_iW - u, \quad i = 1, 2, 3, 4; \quad P := u^2 - 2AWu, \quad Q := u^2 + 2AWu.$$

We may assume that $m_2 = m_1 + A$ and that

$$p_1p_3 = P, \quad p_1p_4 = Q.$$

We want to prove that $m_3 = m_2 + A$ or $m_4 = m_2 + A$. Suppose that this is not true, then $p_2p_3 = Q, p_2p_4 = P$. We have

$$\begin{aligned} AWu = Q - P &= p_3(p_2 - p_1) = 2p_3AW \\ &= p_4(p_1 - p_2) = -2p_4AW. \end{aligned}$$

Since p_3p_4 cannot be equal to P or Q, we have $|m_3 - m_4| = A$. But then

$$Q - P = p_2(p_3 - p_4) = \pm 2p_2WA,$$

which implies that $p_2 = p_3$ or $p_2 = p_4$, a contradiction. Hence, we may assume that $m_3 = m_2 + A$. Then, $p_2p_4 = P$. Moreover, from $|m_3 - m_4| = A$, we conclude that $m_4 = m_3 + A$.

Let us insert $m_2 = m_1 + A, m_3 = m_1 + 2A, m_4 = m_1 + 3A$ into the relation $p_1p_3 = p_2p_4$. We obtain

$$4W(m_2m_4 - m_1m_3) = 2(m_2 + m_4 - m_1 - m_3)u$$

or

$$4WA(2m_1 + 3A) = 4Au,$$

and finally

$$u = 2m_1W + 3AW.$$

From

$$4AWu = Q - P = 2p_1AW = -2p_4AW,$$

we find that $2u = p_1 = -p_4$. This implies that $2m_1W = 3u$ and $2m_4W = -u$ and we get

$$4u = 2(m_1 - m_4)W = -6AW. \tag{1}$$

Furthermore, since $p_1p_4 = Q$, we get $-4u^2 = u^2 + 2AWu$ and therefore

$$-5u = 2AW,$$

which is a contradiction to equation (1). This proves that there does not exist a polynomial $D(ux + v)$-quintuple consisting of linear polynomials. □

2.2. Quadratic polynomials and proof of Theorem 2.

Let $\mathbb{Z}^+[x]$ denote the set of all polynomials with integer coefficients with positive leading coefficient. For $a, b \in \mathbb{Z}[x]$, $a < b$ means that $b - a \in \mathbb{Z}^+[x]$.

Let $\{a, b, c\}$ be a polynomial $D(n)$-triple containing only quadratic polynomials and with linear $n \in \mathbb{Z}[x]$. Assume that $a < b < c$. In our previous paper ([10, Proof of Proposition 3]), we have shown that for fixed a and b such that $ab + n = r^2$, there are at most three possibilities for c, namely $c = a + b + 2r$ and two possible c's which come from

$$c_{1,2} = a + b + \frac{e}{n} + \frac{2}{n^2}(abe \pm ruv),$$

where $u, v \in \mathbb{Z}^+[x]$ and $e \in \mathbb{Z}$ satisfy $ae + n^2 = u^2, be + n^2 = v^2$.

Observe now that

$$c_1 \cdot c_2 \quad = \quad a^2 + b^2 + \frac{e^2}{n^2} - 2ab - \frac{2ae}{n} - \frac{2bc}{n} - 4n,$$

which implies that $c_2 < b$, a contradiction.

Now we assume that a polynomial $D(n)$-m-tuple S contains a, b, c, c_1. The same argument as above applied to the pair $\{b, c\}$ implies that $c_1 = d_0 = b + c + 2t$ or $c_1 = d_1$ or $c_1 = d_2$ with

$$d_{1,2} = b + c + \frac{f}{n} + \frac{2}{n^2}(abf \pm t\tilde{u}\tilde{v}),$$

where $bc + n = t^2$ and with certain $\tilde{u}, \tilde{v} \in \mathbb{Z}^+[x]$ and $f \in \mathbb{Z}$ satisfying $bf + n^2 = \tilde{u}^2, bf + n^2 = \tilde{v}^2$. As before we get $d_2 < c$ and therefore $c_1 \neq d_2$. Moreover, in the proof of [10, Proposition 3] it is shown that $be + n^2 = v^2$ and $bf + n^2 = \tilde{u}^2$ with $e, f \in \mathbb{Z}$ implies that $e = f$. Hence, $d_1 > c_1$. The only remaining case is

$$c_1 = d_0 = b + a + b + 2r + 2b + 2r = a + 4b + 4r,$$

which means that we have to deal with the only possible polynomial $D(n)$-quadruple of the form

$$\{a, b, a + b + 2r, a + 4b + 4r\}$$

with $ab + n = r^2$.

The only remaining condition for this set to be a polynomial $D(n)$-quadruple is $a \cdot (a + 4b + 4r) + n = z^2$, which implies

$$a^2 + 4(r^2 - n) + 4ar + n = z^2$$

or

$$(a + 2r - z)(a + 2r + z) = (a + 2r)^2 - z^2 = 3n. \tag{2}$$

This is a contradiction, since the left hand side of (2) has degree ≥ 2 and the right hand side has degree 1. Consequently, we have proved that there are at most 3 polynomials in the $D(n)$-m-tuple S all having degree two. $\square$

3. A certain elliptic equation

In this section we will reduce the problem of finding all extensions of $\{a, b, c\}$ to a polynomial $D(n)$-quadruple to finding all solutions in $\mathbb{Z}[x]$ of a certain elliptic equation in an algebraic function field in one variable over the algebraically closed field of constants $\mathbb{C}$.

Assume that the set $\{a, b, c, d\}$ is a polynomial $D(n)$-quadruple. Let $ab + n = r^2, ac + n = s^2, bc + n = t^2$ where $r, s, t \in \mathbb{Z}^+[x]$. Moreover, we have

$$ad + n = u^2, \quad bd + n = v^2, \quad cd + n = w^2,$$

with $u, v, w \in \mathbb{Z}[x]$. Multiplying these equations, we get the following elliptic equation

$$(uvw)^2 = (ad + n)(bd + n)(cd + n),$$

where we search for polynomial solutions $d \in \mathbb{Z}[x]$.

Let us denote $X = abcd$ and $Y = abcuvw$. Then by multiplying the above equation with $a^2b^2c^2$ we get

$$Y^2 = (X + nbc)(X + nac)(X + nab). \tag{3}$$

The polynomial on the right hand side becomes

$$\begin{aligned}(X + nbc)(X + nac)(X + nab) &= \\ &= X^3 + n(ab + bc + ac)X^2 + n^2abc(a + b + c)X + n^3a^2b^2c^2\end{aligned}$$

so this polynomial has coefficients and roots in $\mathbb{Z}[x]$. Instead of applying a general theorem for hyperelliptic equations in function fields due to Mason (cf. [15, Theorem 6]), as we did in our previous paper ([10, Lemma 2]), we will follow Siegel's original approach (cf. [16] and the method of proof of [15, Theorem 6]).

Therefore, let

$$F := \mathbb{C}(x, \sqrt{ab}, \sqrt{ac})$$

be a function field in one variable over the field of complex numbers. Let $\mathcal{O}$ denote the ring of elements of F integral over $\mathbb{C}[x]$. These elements have the property that $\nu(f) \geq 0$ for all finite valuations on F. Let us recall the definitions of the discrete valuations on the field $\mathbb{C}(x)$ where x is transcendental over $\mathbb{C}$. For $\xi \in \mathbb{C}$ define the valuation ν_ξ such that for $Q \in \mathbb{C}(x)$ we have $Q(x) = (x - \xi)^{\nu_\xi(Q)}A(x)/B(x)$ where A, B are polynomials with $A(\xi)B(\xi) \neq 0$. Further, for $Q = A/B$ with $A, B \in \mathbb{C}[x]$, we put $\deg Q := \deg A - \deg B$; thus $\nu_\infty := -\deg$ is a discrete valuation on $\mathbb{C}(x)$. These are all discrete valuations on $\mathbb{C}(x)$. Now let F as above be a finite extension of $\mathbb{C}(x)$. Each of the valuations ν_ξ, ν_∞ can be extended in at most $[F : \mathbb{C}(x)] =: d$ ways to a discrete valuation on F and in this way one obtains all discrete valuations on F. A valuation on F is called finite if it extends ν_ξ for some $\xi \in \mathbb{C}$ and infinite if it extends ν_∞.

All solutions of interest for us come from solutions of (3) in F, where $X + nbc, X + nac, X + nab$ are squares. Observe that this follows from the relations

$$\begin{aligned}X + nbc &= abcd + nbc = u^2bc,\\ X + nac &= abcd + nac = v^2ac,\\ X + nab &= abcd + nab = w^2ac\end{aligned}$$

and the fact that $\sqrt{ab}, \sqrt{ac}$ and therefore also

$$\sqrt{bc} = \frac{\sqrt{ab}\sqrt{ac}}{a}$$

are elements of F. We denote

$$\xi_1^2 = u^2bc = X + nbc, \quad \xi_2^2 = v^2ac = X + nac, \quad \xi_3^2 = w^2ac = X + nab$$

and we define $\beta_i, \hat{\beta}_i, i = 1, 2, 3$ by $\beta_1 = \xi_2 - \xi_3, \hat{\beta}_1 = \xi_2 + \xi_3$ with $\beta_2, \hat{\beta}_2, \beta_3, \hat{\beta}_3$ defined similarly by permutation of indices. All these elements are contained in the ring $\mathcal{O}$. Then $\beta_1\hat{\beta}_1 = na(b-c), \beta_2\hat{\beta}_2 = nb(c-a), \beta_3\hat{\beta}_3 = nc(a-b)$, and

$$\beta_1 + \beta_2 + \beta_3 = 0. \tag{4}$$

This is Siegel's classical identity. Moreover, we have

$$\beta_1 + \hat{\beta}_2 - \hat{\beta}_3 = -\hat{\beta}_1 + \beta_2 + \hat{\beta}_3 = \hat{\beta}_1 - \hat{\beta}_2 + \beta_3 = 0. \tag{5}$$

We note that each of β_1, β_2 and β_3 divide the fixed element

$$\mu = -n^3abc(b-a)(c-a)(c-b)$$

in $\mathcal{O}$. Hence, if ν is any finite valuation on F with $\nu(\mu) = 0$, then we have $\nu(\beta_i) = 0, i = 1, 2, 3$ and so $\nu(\hat{\beta}_i) = 0, i = 1, 2, 3$, also. Now we apply Mason's Inequality to Siegel's identity (4) to get an upper bound for the degree of the polynomials X and therefore also for the polynomials d.

We need the following generalization of the degree from $\mathbb{C}[x]$ to F. We define the *height* of $f \in F$ by

$$\mathcal{H}(f) = -\sum_{\nu} \min\{0, \nu(f)\}$$

where the sum is taken over all valuations on F; thus for $f \in \mathbb{C}(x)$ the height $\mathcal{H}(f)$ is just the number of poles of f counted according to multiplicity. We note that if f lies in $\mathbb{C}[x]$, then $\mathcal{H}(f) = d \deg f$. Moreover, we have

$$\max\{\mathcal{H}(f+h), \mathcal{H}(fh)\} \leq \mathcal{H}(f) + \mathcal{H}(h) \tag{6}$$

for any two elements f, h in F.

Now we state the following theorem on the solutions of two-dimensional unit equations over an algebraic function field, which is usually referred to as Mason's inequality and which can be seen as an analog of Baker's theorem in linear forms of logarithms of algebraic numbers. A proof of this theorem can be found in the monograph of Mason (cf. [15, Lemma 2]).

Theorem 4. (R. C. Mason) *Let γ_1, γ_2 and γ_3 be non-zero elements of F with $\gamma_1 + \gamma_2 + \gamma_3 = 0$, and such that $\nu(\gamma_1) = \nu(\gamma_2) = \nu(\gamma_3)$ for each valuation ν not in the finite set $\mathcal{V}$. Then either γ_1/γ_2 lies in $\mathbb{C}$, in which case $\mathcal{H}(\gamma_1/\gamma_2) = 0$, or*

$$\mathcal{H}(\gamma_1/\gamma_2) \leq |\mathcal{V}| + 2g - 2,$$

where $|\mathcal{V}|$ denotes the number of elements of $\mathcal{V}$ and g the genus of $F/\mathbb{C}(X)$.

Now we are ready to prove the following lemma:

Lemma 1. *Let $\{a, b, c, d\}$, $a < b < c < d$ be a polynomial $D(n)$-quadruple with $n \in \mathbb{Z}[x]$. Then*

$$\deg d \leq 7 \deg a + 11 \deg b + 15 \deg c + 14 \deg n - 4.$$

Proof. We denote by $\mathcal{W}$ the set of absolute values on F containing all infinite ones together with those finite absolute values ν for which $\nu(\mu) > 0$. For brevity we denote $M = 2g - 2 + |\mathcal{W}|$.

First, we need an upper bound for the genus g of $F/\mathbb{C}(x)$. We consider the two Kummer extensions $F_1 := \mathbb{C}(x, \sqrt{ab})$ and $F_2 := \mathbb{C}(x, \sqrt{ac})$ and calculate the genus g_1 of $F_1/\mathbb{C}(x)$ and g_2 of $F_2/\mathbb{C}(x)$, respectively. It follows from [17, Corollary III.7.4] (see also Example III.7.6 on page 113) that

$$g_1 = \frac{\deg a + \deg b - 2}{2}, \quad g_2 = \frac{\deg a + \deg c - 2}{2},$$

since neither ab nor ac can have odd degree ($ab + n$ and $ac + n$ are squares of polynomials and therefore have even degree). Observe that the degree of the extensions $F_1/\mathbb{C}(x)$ and $F_2/\mathbb{C}(x)$ is two in both cases. Now we can use Castelnuovo's inequality (cf. [17, Theorem III.10.3]) to get an upper bound for the genus g of $F = F_1 F_2$. We have

$$g \le 2\frac{\deg a + \deg b - 2}{2} + 2\frac{\deg a + \deg c - 2}{2} + 1 = 2\deg a + \deg b + \deg c - 3.$$

Next, we need an upper bound for the cardinality of the set $\mathcal{W}$. It can be obtained by considering the number of zeros and poles of $\mu = -n^3 abc(b - a)(c-a)(c-b)$. The number of zeros is bounded by the degree of the polynomial μ which is $3\deg n + \deg a + 2\deg b + 3\deg c$. Each zero can be extended to an absolute value of F in at most $[F : \mathbb{C}(x)] = 4$ ways. Moreover, there exist at most 4 infinite absolute values on F. Therefore,

$$|\mathcal{W}| \le 4(3\deg n + \deg a + 2\deg b + 3\deg c) + 4.$$

Now Mason's theorem (Theorem 4) applied to the equation $\beta_1 + \beta_2 + \beta_3 = 0$ yields that

$$\mathcal{H}(\beta_2/\beta_3) \le M.$$

Further, M also serves as an upper bound for each of $\mathcal{H}(\hat{\beta}_2/\beta_3), \mathcal{H}(\beta_2/\hat{\beta}_3)$ and $\mathcal{H}(\hat{\beta}_2/\hat{\beta}_3)$ because of equations (5). However, it is easy to check that

$$\frac{2(2X - nbc - nab)}{nc(a-b)} = \frac{\hat{\beta}_2}{\beta_3}\frac{\hat{\beta}_2}{\hat{\beta}_3} + \frac{\beta_2}{\beta_3}\frac{\beta_2}{\hat{\beta}_3}.$$

Hence, we have

$$\mathcal{H}\left(\frac{2X - nbc - nab}{nc(a-b)}\right) \le 4M$$

and therefore

$$\mathcal{H}(X) \le \mathcal{H}(nb(a+c)) + \mathcal{H}(nc(a-b)) + 4M,$$

where we have used that the height of a sum or a product is bounded by the sum of the heights (see (6)). Finally, since $X = abcd$, we get

$$\begin{aligned}
\mathcal{H}(X) &= 4(\deg a + \deg b + \deg c + \deg d),\\
\mathcal{H}(nb(a+c)) &= 4(\deg n + \deg b + \deg c),\\
\mathcal{H}(nc(a-b)) &\le 4(\deg n + \deg c + \deg b),
\end{aligned}$$

and therefore, by taking into account the bound for M which is

$$M \leq 4\deg a + 2\deg b + 2\deg c - 8 + 12\deg n + 4\deg a + 8\deg b + 12\deg c + 4,$$

we obtain the following upper bound

$$\deg d \leq 14\deg n + 7\deg a + 11\deg b + 15\deg c - 4$$

as claimed in our lemma. □

4. Proof of Theorem 3

Let $S = \{a_1, a_2, \ldots, a_m\}$ be a polynomial $D(ux+v)$-m-tuple with some integers $u \neq 0$ and v. We already know that $m \leq 26$ from the main result in [10]. From the fact that the product of each two elements from S plus $ux+v$ is a square of a polynomial with integer coefficients, it follows that if the set S contains a polynomial with degree ≥ 2, then it contains either polynomials with even or polynomials with odd degree only. From Theorem 1 we get that there are at most 4 linear polynomials in S. Theorem 2 implies that there are at most 3 quadratic polynomials in S. The number of polynomials of degree $\mu \geq 3$ is also at most 3 and there is at most one constant in S.

We may assume that there is a polynomial of degree ≥ 2 in S. Therefore, we will consider separate cases depending on whether all degrees are even or all degrees are odd.

We use the following gap principle, which was already proved in our previous paper (cf. [10, Lemma 3]).

Lemma 2. *If $\{a, b, c, d\}$ is a polynomial $D(n)$-quadruple, where $n \in \mathbb{Z}[x]$, $a < b < c < d$ and $\deg a \geq 3$, then*

$$\deg d \geq \deg b + \deg c - 2.$$

Combining these gaps between the degrees of the elements in S with the upper bound proved in Lemma 1 we will get a much smaller upper bound for m.

First, we consider the case that all degrees of the a_i in S are odd. Let us assume the worst case, namely that there is the smallest possible gap between the degrees of the elements in S according to Lemma 2. In this case the following sequence of degrees is possible:

$$1, 1, 1, 1, 3, 3, 3, 5, 7, 11, 17, 27, 43, 69, 111, 179, \ldots. \tag{7}$$

More precisely, we get lower bounds for the degrees of the elements of S:

$\deg a_1 \geq 1,$	$\deg a_2 \geq 1,$	$\deg a_3 \geq 1,$	$\deg a_4 \geq 1,$
$\deg a_5 \geq 3,$	$\deg a_6, \geq 3,$	$\deg a_7 \geq 3,$	$\deg a_8 \geq 5,$
$\deg a_9 \geq 7,$	$\deg a_{10} \geq 11,$	$\deg a_{11} \geq 17,$	$\deg a_{12} \geq 27,$
$\deg a_{13} \geq 43,$	$\deg a_{14} \geq 69,$	$\deg a_{15} \geq 111,$	$\ldots$

We obtained this in the following way: there are at most 4 linear polynomials in S. The next possible (odd) degree is 3 and there are at most 3 polynomials of degree 3 in S. But having three polynomials of degree 3 enables us to use the above gap principle (Lemma 2) and we get that the next degree is

$$\deg a_8 \geq 3+3-2=4,$$

and since the smallest odd number ≥ 4 is 5 we get the lower bound as stated in the table, namely $\deg a_8 \geq 5$. Proceeding in this way, we produce the numbers in (7).

Since the linear polynomials in S play a special role here we will divide cases depending on how many linear polynomials our set S contains. If we assume that $\deg a_1 = \deg a_2 = \deg a_3 = \deg a_4 = 1$, then we have

$$\begin{array}{lll}
\deg a_1 = 1, & \deg a_2 = 1, & \deg a_3 = 1, \\
\deg a_4 = 1, & \deg a_5 = A, & \deg a_6 \geq A, \\
\deg a_7 \geq A, & \deg a_8 \geq 2A-1, & \deg a_9 \geq 3A-2, \\
\deg a_{10} \geq 5A-4, & \deg a_{11} \geq 8A-7, & \deg a_{12} \geq 13A-12, \\
\deg a_{13} \geq 21A-20, & \deg a_{14} \geq 34A-33, & \ldots
\end{array}$$

with $A \geq 3$.

Let us assume that $A > 3$ first. We get by Lemma 1 applied to $\{a_1, a_2, a_3, a_m\}$ that

$$\deg a_m \leq 7+11+15+14-4=43,$$

which gives a contradiction unless $m \leq 12$.

Now, we consider the case that $A=3$. We first show that the configuration of degrees $1,1,1,1,3,3,3$ is not possible. Assume that $\{a,b,c,d\} \subseteq S$ is a polynomial $D(ux+v)$-quadruple such that $\deg a = 1, \deg b = \deg c = \deg d = 3$. For the polynomials e and $\overline{e}$ defined by

$$e = n(a+b+c) + 2abc - 2rst, \tag{8}$$

$$\overline{e} = n(a+b+c) + 2abc + 2rst, \tag{9}$$

where $ab+n=r^2, ac+n=s^2, bc+n=t^2$, we have that $ae+n^2, be+n^2, ce+n^2$ are perfect squares (cf. [10, Lemma 1] applied to $\{a,b,c\}$) and

$$e \cdot \overline{e} = n^2(c-a-b-2r)(c-a-b+2r) \tag{10}$$

(see ([10, equation (2)]). It is plain that $\deg \overline{e} = 7, \deg(e\overline{e}) \leq 8$ and therefore $\deg e \leq 1$. Hence, $e=0$ or $\deg e = 1$. If $e=0$, then $c=a+b+2r$. Also the third polynomial of degree 3 has the form $d=b+c+2t$ by the proof of [10, Proposition 2]. Thus, $d=a+4b+4r$ and together with $ad+n=z^2$, we get

$$3n=(a+2r-z)(a+2r+z),$$

a contradiction. Therefore, we may assume that $\deg e = 1$. From $be+n^2=y^2$, we have $y \pm n = e \cdot f$ with $\deg f = 1$. This gives $b = ef^2 \mp 2fn$. Hence, $f|b$. We want to prove that there are at most 3 such f's corresponding to the possible linear factors of b. Assume that we have two such f's (say f and f') which correspond to the same linear factor of b, i.e. $f' = \alpha \cdot f, \alpha \neq 1$. From

$$b = ef^2 \mp 2fn = e'f'^2 \mp 2f'n,$$

we find

$$f(e' \cdot \alpha^2 - e) = \pm 2n(\alpha \pm 1).$$

Thus, $n|f$ and $n|b$. From $be+n^2=y^2$ we find that $n|y$ and $n^2|be$. Hence, $n|e$. Now $ce+n^2$ being a perfect square, implies that $n|c$ and $n^2|bc$ contradicting the relation $bc+n=t^2$. Therefore, there are at most 3 polynomials f with the above property and consequently, there are at most 3 possibilities for the polynomial e. Altogether, this means that for fixed polynomials b and c of degree 3, there are at most 3 possibilities for the linear polynomial a (each e induce two possible a's, but as we have shown above only one of them is indeed a polynomial). Hence, we proved that the configuration $1,1,1,1,3,3,3$ is not possible. The remaining case to consider is

$$\begin{array}{lll}
\deg a_1 = 1, & \deg a_2 = 1, & \deg a_3 = 1, \\
\deg a_4 = 1, & \deg a_5 = A, & \deg a_6 \geq A, \\
\deg a_7 \geq 2A-1, & \deg a_8 \geq 3A-2, & \deg a_9 \geq 5A-4, \\
\deg a_{10} \geq 8A-7, & \deg a_{11} \geq 13A-12, & \deg a_{12} \geq 21A-20, \\
\deg a_{13} \geq 34A-33, & \dots &
\end{array}$$

with $A=3$. But as above we get $\deg a_{13} \leq 43$, and therefore

$$34A - 33 \leq \deg a_{13} \leq 43,$$

which is a contradiction to $A=3$.

Similarly, we get upper bounds for m in the case that we have

$$\begin{aligned}
&\deg a_1 = \deg a_2 = \deg a_3 = 1 \quad \text{and} \\
&\deg a_4 = A \geq 3, \deg a_5 \geq A, \deg a_6 \geq A, \deg a_7 \geq 2A-1, \dots, \\
&\deg a_{13} \geq 34A - 33,
\end{aligned}$$

where we get $\deg a_{13} \leq 43$ as before and therefore $m \leq 12$. In the case

$$\begin{aligned}
&\deg a_1 = \deg a_2 = 1, \deg a_3 = A \geq 3, \\
&\deg a_4 \geq A, \deg a_5 \geq A, \deg a_6 \geq 2A-1, \dots, \deg a_{13} \geq 55A - 54,
\end{aligned}$$

we get

$$\deg a_{13} \leq 7 + 11 + 15A + 14 - 4 = 15A + 28$$

and therefore $m \leq 12$. Next, we consider the case

$$\begin{aligned}
&\deg a_1 = 1, \deg a_2 = A, \deg a_3 = B, \\
&\deg a_4 \geq B, \deg a_5 \geq 2B-1, \dots, \deg a_{12} \geq 55B - 54
\end{aligned}$$

with $3 \leq A \leq B$, where we get

$$\deg a_{12} \leq 7 + 11A + 15B + 14 - 4 \leq 26B + 17$$

and therefore $m \leq 11$. Observe that we can apply the gap principle already to get a lower bound for $\deg a_4$, since we have three elements with degree ≥ 3. Finally, we consider the case

$$\begin{aligned}
&\deg a_1 = A, \deg a_2 = B, \deg a_3 = C, \\
&\deg a_4 \geq C, \deg a_5 \geq 2C-1, \dots, \deg a_{12} \geq 55C - 54
\end{aligned}$$

with $3 \leq A \leq B \leq C$, where we get

$$\deg a_{12} \leq 7A + 11B + 15C + 14 - 4 \leq 33C + 10$$

and therefore $m \leq 11$. Altogether, we see that there are at most 12 polynomials in S all of them having odd degrees.

The case where all polynomials in S have even degree can be handled in essentially the same way. Here the degrees 0 (which appears at most once) and 2 play a special role.

Let us start by showing that it is not possible to have polynomials $\{a, b, c, d\} \subseteq S$ with $\deg a = A, \deg b = \deg c = \deg d = B$ and $a < b < c < d, 2 \leq A < B$. By the proof of [10, Proposition 2] we have $d = b + c + 2t$, where $bc + n = t^2$. Consider the triple $\{a, b, c\}$ and let e and $\overline{e}$ be the polynomials defined by (8) and (9), which exist by [10, Lemma 1]. Since $\deg \overline{e} = A + 2B, \deg(e\overline{e}) \leq 2B + 2$ (by (10)), it follows that $\deg e \leq 2 - A \leq 0$. Hence, e is a constant. But by the proof of [10, Proposition 3] (we used these arguments already above), there is at most one nonzero constant e such that $ae + n^2$ is a perfect square. Therefore, one of the polynomials c and d corresponds to $e = 0$. We may assume that $c = a + b + 2r$. Then $d = a + 4b + 4r$, and the condition $ad + n = z^2$ leads again to

$$3n = (a + 2r - z)(a + 2r + z),$$

a contradiction.

Now assume that $\deg a_1 = 0, \deg a_2 = 2, \deg a_3 = 2$. Then $\deg a_4 \geq 2, \deg a_5 \geq 4$ (since there are at most 3 elements of degree 2 in the set S by Theorem 2), $\deg a_6 \geq 4$, (since by the arguments from above with one polynomial of degree ≥ 2 there are at most two polynomials with the same degree $B > 2$) $\deg a_7 \geq 6, \deg a_8 \geq 8, \deg a_9 \geq 12, \deg a_{10} \geq 18, \deg a_{11} \geq 28, \deg a_{12} \geq 44, \deg a_{13} \geq 70$. On the other hand, we get the upper bound

$$\deg a_{13} \leq 0 + 22 + 30 + 14 - 4 = 62,$$

which is a contradiction. Therefore, we get $m \leq 12$ in this case.

Assume now that

$$\begin{array}{lll} \deg a_1 = 0, & \deg a_2 = A, & \deg a_3 = B, \\ \deg a_4 \geq B, & \deg a_5 \geq 2B - 2, & \deg a_6 \geq 3B - 4, \\ \deg a_7 \geq 5B - 8, & \deg a_8 \geq 8B - 14, & \deg a_9 \geq 13B - 24, \\ \deg a_{10} \geq 21B - 30, & \deg a_{11} \geq 34B - 54, & \deg a_{12} \geq 55B - 84 \end{array}$$

with $2 \leq A < B$ and where we have again used the gap principle (Lemma 2) several times. Applying Lemma 1 to the quadruple $\{a_1, a_2, a_3, a_{12}\}$ we get

$$\deg a_{12} \leq 11A + 15B + 14 - 4 \leq 26B + 10,$$

a contradiction. Hence, $m \leq 11$ in this case.

Finally, we consider the case that

$$\deg a_1 = A, \deg a_2 = B, \deg a_3 = C,$$

where $2 \leq A \leq B \leq C$. If $C \geq 4$, then we have

$$\deg a_4 \geq C, \deg a_5 \geq 2C-2, \ldots, \deg a_{13} \geq 89C-140.$$

By Lemma 1 we obtain

$$\deg a_{13} \leq 7A+11B+15C+14-4 \leq 33C+10,$$

which gives a contradiction. If $A = B = C = 2$, then we have $\deg a_1 = 2, \deg a_2 = 2, \deg a_3 = 2, \deg a_4 \geq 4, \deg a_5 \geq 4, \deg a_6 \geq 6, \deg a_7 \geq 8, \deg a_8 \geq 12, \deg a_9 \geq 18, \deg a_{10} \geq 28, \deg a_{11} \geq 44, \deg a_{12} \geq 70, \deg a_{13} \geq 112$ and

$$\deg a_{13} \leq 14+22+30+14-4 = 76,$$

which gives a contradiction, showing that $m \leq 12$. Altogether, we have at most 12 polynomials in S all having even degrees. □

References

[1] A. Baker and H. Davenport, The equations $3x^2-2=y^2$ and $8x^2-7=z^2$, *Quart. J. Math. Oxford Ser.* (2) **20** (1969), 129–137.

[2] Diophantus of Alexandria, Arithmetics and the Book of Polygonal Numbers, (I. G. Bashmakova, Ed.) (Nauka, 1974) (in Russian), 85–86, 215–217.

[3] A. Dujella, Generalization of a problem of Diophantus, *Acta Arith.* **65** (1993), 15–27.

[4] A. Dujella, On the size of Diophantine m-tuples, *Math. Proc. Cambridge Philos. Soc.* **132** (2002), 23–33.

[5] A. Dujella, There are only finitely many Diophantine quintuples, *J. Reine Angew. Math.* **566** (2004), 183-214.

[6] A. Dujella, Bounds for the size of sets with the property $D(n)$, *Glas. Mat. Ser. III* **39** (2004), 199-205.

[7] A. Dujella and C. Fuchs, A polynomial variant of a problem of Diophantus and Euler, *Rocky Mountain J. Math.* **33** (2003), 797-811.

[8] A. Dujella and C. Fuchs, Complete solution of the polynomial version of a problem of Diophantus, *J. Number Theory* **106** (2004), 326-344.

[9] A. Dujella and C. Fuchs, Complete solution of a problem of Diophantus and Euler, *J. London Math. Soc. (2)* **71** (2005), 33-52.

[10] A. Dujella, C. Fuchs and R. F. Tichy, Diophantine m-tuples for linear polynomials, *Period. Math. Hungar.* **45** (2002), 21-33.

[11] A. Dujella and F. Luca, On a problem of Diophantus with polynomials, *Rocky Mountain J. Math.*, to appear (Preprint: http://www.math.hr/~duje/dvi/dluca.dvi).

[12] B. W. Jones, A variation of a problem of Davenport and Diophantus, *Quart. J. Math. Oxford* Ser.(2) **27** (1976), 349–353.

[13] B. W. Jones, A second variation of a problem of Davenport and Diophantus, *Fibonacci Quart.* **15** (1977), 323–330.

[14] R. C. Mason, The hyperelliptic equation over function fields, *Proc. Camb. Philos. Soc.* **93** (1983), 219–230.

[15] R. C. Mason, *Diophantine equations over function fields*, London Mathematical Society Lecture Notes Series, vol. 96, Cambridge University Press, Cambridge, 1984.

[16] C. L. Siegel, The integer solutions of the equation $y^2 = ax^n + bx^{n-1} + \ldots + k$, *J. London Math. Soc. (1)* (1926), 66-68 (under the pseudonym X).

[17] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin, 1993.

Andrej Dujella
Department of Mathematics
University of Zagreb
Bijenička cesta 30
10000 Zagreb, Croatia.
e-mail: duje@math.hr

Clemens Fuchs
Institut für Mathematik
TU Graz
Steyrergasse 30
A-8010 Graz, Austria.
e-mail: clemens.fuchs@tugraz.at

Gary Walsh
Department of Mathematics
University of Ottawa
585 King Edward St.
Ottawa, Ontario, K1N 6N5, Canada.
e-mail: gwalsh@mathstat.uottawa.ca