DIOPHANTINE m-TUPLES FOR LINEAR POLYNOMIALS

ANDREJ DUJELLA, CLEMENS FUCHS* AND ROBERT F. TICHY*

ABSTRACT. In this paper, we prove that there does not exist a set with more than 26 polynomials with integer coefficients, such that the product of any two of them plus a linear polynomial is a square of a polynomial with integer coefficients.

1991 *Mathematics Subject Classification:* 11D09.

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 [4] 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 [2] 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 [7]).

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

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

where $|S|$ denotes the number of elements in the set S. The first author proved that M_n is finite for all $n \in \mathbb{Z}\backslash\{0\}$. In his proof, he estimated the number of "large" (greater than $|n|^3$), "small" (between n^2 and $|n|^3$) and "very small" (less than n^2) elements of a set with the property $D(n)$, using a theorem of Bennett [3] on simultaneous approximations of algebraic numbers and a gap principle in the first, a weaker variant of the gap principle in the second and a large sieve method due to Gallagher [9] in the third case respectively (cf. [6]). Let us introduce the following notation:

$$A_n = \sup\{|S \cap [|n|^3, \infty\rangle| : S \text{ has the property} D(n)\},$$
$$B_n = \sup\{|S \cap [n^2, |n|^3\rangle| : S \text{ has the property} D(n)\},$$
$$C_n = \sup\{|S \cap [1, n^2\rangle| : S \text{ has the property} D(n)\}.$$

*This work was supported by the Austrian Science Foundation FWF, grant S8307-MAT.

His result was (cf. [6, Theorems 1, 2, 3 and 4])

$$\begin{aligned} A_n &\leq 21, \\ B_n &\leq 0.65 \log |n| + 2.24, \\ C_n &\leq \begin{cases} 265.55 \log |n| (\log\log |n|)^2 + 9.01 \log\log |n| & \text{for } |n| > 400, \\ 5 & \text{for } |n| \leq 400. \end{cases} \end{aligned}$$

Therefore

$$\begin{aligned} M_n &\leq 32 \quad \text{for } |n| \leq 400, \\ M_n &< 267.81 \log |n| (\log\log |n|)^2 \quad \text{for } |n| > 400. \end{aligned}$$

A polynomial variant of the above problems was first studied by Jones [10], [11], and it was for the case $n = 1$.

Definition 1. *Let $n \in \mathbb{Z}[x]$ and let $\{a_1, a_2, \ldots, a_m\}$ 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 $a_1/p, \ldots, a_m/p$ and n/p^2 are integers. The set $\{a_1, a_2, \ldots, a_m\}$ 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 $b_{ij} \in \mathbb{Z}[x]$.*

Let us mention that the assumption that there does not exist a polynomial p such that $a_1/p, \ldots, a_m/p$ and n/p^2 are integers means for constant n that not all elements $a_1, \ldots, a_m$ of a polynomial $D(n)$-m-tuple are allowed to be constant (compare with Definition 1 in [8]). For linear n the condition under consideration is trivially always satisfied.

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

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

From [6, 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 $P_1 = 4$. Recently, the first and the second author proved that $P_{-1} = 3$ (cf. [8]) by succesfully transferring the needed methods to the polynomial case.

The results of [6], by specialization, give a bound for P_n in terms of the degree and the maximum of the coefficients of n. We conjecture that there should exist a bound for P_n, which depends only on the degree of n. As we have seen, this is true for constant polynomials, and in the present paper we will prove this conjecture for linear polynomials.

We want to handle the case of linear polynomials, i.e. $n = ax + b$, with integers $a \neq 0$ and b. Let us define

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

It is easy to prove that $L \geq 4$. E.g. the set

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

is a polynomial $D(16x+9)$-quadruple and the set

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

is a polynomial $D(4x+3)$-quadruple (see [5]).

We intend to prove that $L < \infty$. More precisely, we want to find some good upper bound for L.

The idea is to estimate the number of polynomials in S with given degree and to consider separate cases whether the degree is "large" or "small".

In analog to the classical case, we prove our result for "large" degree by using a theorem due to Mason [12] on the polynomial solutions of hyperelliptic equations over function fields in one variable and a gap principle. Let S be a polynomial $D(ax+b)$-m-tuple with integers $a \neq 0$ and b. We prove

Proposition 1. *There are at most* 15 *polynomials in S with degree ≥ 4.*

We want to remark that a weaker result can be shown by applying the results from the classical integer case. From that, it is possible to show that there are at most 21 polynomials in S with degree ≥ 4.

We have to estimate the number of constant, linear, quadratic and cubic polynomials in S. We denote these numbers by L_0, L_1, L_2, L_3 respectively and we will consider them separately. First of all it is trivial to see that we have

$$L_0 \leq 1.$$

By using the mentioned gap principle once more, we get

Proposition 2. *There are at most three polynomials in S of degree* 3*. Therefore, we have*

$$L_3 \leq 3.$$

Let us remark that in fact the proof gives us the following result: There is no polynomial $D(ax+b)$-quadruple which consists of polynomials all having the same degree $\mu \geq 3$. For the case $n = 1$ this was already proved by Jones in [11].

By more detailed analysis we get

Proposition 3. *There are at most five polynomials in S of degree* 2*. Therefore, we have*

$$L_2 \leq 5.$$

Proposition 4. *There are at most eight linear polynomials in S. Therefore, we have*

$$L_1 \leq 8.$$

Altogether, we can prove the following bound for the size of polynomial $D(n)$-m-tuples for linear polynomials $n = ax+b$.

Theorem 1.

$$L \leq 26.$$

In Section 2, we will collect auxiliary results which are needed to prove our results. In Section 3, we handle Propositions 1 and 2 which are the cases of large degrees. In Section 4, we prove the results for the small degrees, i.e. Propositions 3 and 4 and therefore finally get Theorem 1.

2. Auxiliary results

Let K be an algebraically closed field with characteristic 0. Let us begin by recalling the definitions of the discrete valuations on the field $K(x)$ where x is transcendental over K. For $\xi \in K$ define the valuation ν_ξ such that for $Q \in K(x)$ 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 $A, B \in K[x]$, we put $\deg Q := \deg A - \deg B$; thus $\nu_\infty := -\deg$ is a discrete valuation on $K(x)$. These are all discrete valuations on $K(x)$. Now let L be a finite extension of $K(x)$. Each of the valuations ν_ξ, ν_∞ can be extended in at most $[L : K(x)] =: d$ ways to a discrete valuation on L and in this way one obtains all discrete valuations on L. A valuation on L is called finite if it extends ν_ξ for some $\xi \in K$ and infinite if it extends ν_∞.

We need the following generalization of the degree from $K[x]$ to L. We define the *height* of $f \in L$ by

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

where the sum is taken over all discrete valuations on L; thus for $f \in K(x)$ the height $\mathcal{H}(f)$ is just the number of poles of f counted according to multiplicity. We note that if f lies in $K[x]$ then $\mathcal{H}(f) = d \deg f$. We also want to define the height of a polynomial with coefficients in L. In order to do this let us denote for any finite set S of elements of L

$$\nu(S) = \min_{s \in S}\{\mathcal{H}(s)\} \quad \text{and} \quad \mathcal{H}(S) = -\sum_\nu \min\{0, \nu(S)\}$$

where the sum again runs over all valuations in L. If $P \in L[T]$ and S is the set of its coefficients, then the quantities $\nu(P)$ and $\mathcal{H}(P)$ are defined to be $\nu(S)$ and $\mathcal{H}(S)$ respectively.

Let $\mathcal{O}$ denote the ring of elements of L integral over $K[x]$. These elements have the property that $\nu(f) \geq 0$ for all finite valutations on L.

Now we are able to state the following theorem on the solutions of a hyperelliptic equation over an algebraic function field. A proof of this theorem can be found in the monograph of Mason (cf. [13, Theorem 6]).

Theorem 2. (R. C. Mason) *Let $\alpha_1, \ldots, \alpha_n \in \mathcal{O}$. All the solutions $X, Y \in \mathcal{O}$ of the hyperelliptic equation*

$$Y^2 = (X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n) \tag{1}$$

satisfy

$$\mathcal{H}(X) \leq 26H + 8g + 4(r-1);$$

here H denotes the height of the polynomial on the right hand side of (1), g denotes the genus of L/K and r denotes the number of infinite valuations on L.

Let us note that this bound varies only as a linear function of the height of the hyperelliptic equation, in contrast with the multiply exponential bounds for the classical case obtained by Baker [1]. This shows that the fundamental inequality due to Mason on which the proof of this theorem is based and which is the function field analog of Baker's method of linear forms in logarithms is very sharp.

Before we can go to the proofs of the results, we need the following useful construction with the elements of a polynomial $D(n)$-triple, where n is a polynomial with integer coefficients. The construction is a direct modification from the integer case (see [6, Lemma 3]). The analogous statement for polynomial $D(1)$-triples was proved by Jones in [11] and we did already use it in the case $n = -1$ (cf. [8]).

Lemma 1. *Let $\{a, b, c\}$ be a polynomial $D(n)$-triple and let $ab+n = r^2, ac+n = s^2, bc+n = t^2$. Then there exist polynomials $e, u, v, w \in \mathbb{Z}[x]$ such that*

$$ae + n^2 = u^2,\ be + n^2 = v^2,\ ce + n^2 = w^2.$$

More precisely,

$$e = n(a + b + c) + 2abc - 2rst.$$

Furthermore, it holds:

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

where $u = at - rs, v = bs - rt$.

Proof. We have

$$\begin{aligned}(ae + n^2) - (at - rs)^2 &= an(a + b + c) + 2a^2bc - 2arst + n^2 - \\ &\quad -a^2(bc + n) + 2arst - (ab + n)(ac + n) = 0.\end{aligned}$$

Hence, we may take $u = at - rs$, and analogously $y = bs - rt, z = cr - st$. We have

$$\begin{aligned}abe + ruv &= abn(a + b + c) + 2a^2b^2c - 2abrst + abrst - \\ &\quad -a(ab + n)(bc + n) - b(ab + n)(ac + n) + rst(ab + n) = \\ &= -abcn - n^2(a + b) + rstn,\end{aligned}$$

and finally

$$a+b+\frac{e}{n}+\frac{2}{n^2}(abe+ruv) = 2a+2b+c+\frac{2abc}{n}-\frac{2rst}{n}-\frac{2abc}{n}-2a-2b+\frac{2rst}{n} = c.$$

□

If we also define

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

then easy computation shows that

$$e \cdot \overline{e} = n^2(c-a-b-2r)(c-a-b+2r). \tag{3}$$

This relation will be very useful in the proof of Proposition 2, 3 and 4.

We conclude this section with the following definition: 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 $b-a \in \mathbb{Z}^+[x]$. The usual fundamental properties of inequality hold for this order. For $a \in \mathbb{Z}[x]$, we define $|a| = a$ if $a \geq 0$, and $|a| = -a$ if $a < 0$.

Observe that it is clear that all leading coefficients of the nonconstant polynomials in a polynomial $D(n)$-m-tuple have the same sign. This implies that there is no loss of generality in assuming that they are all positive, i.e. that all polynomials are in $\mathbb{Z}^+[x]$.

3. Elements with large degrees

Assume that the set $\{a, b, c, d\}$ is a polynomial $D(n)$-quadruple with $n \in \mathbb{Z}[x]$. Let $ab+n = r^2, ac+n = s^2, bc+n = t^2$ where $r, s, t \in \mathbb{Z}^+[x]$. In this paper, the symbols r, s, r will always have this meaning. 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 $d \in \mathbb{Z}[x]$. We will apply Mason's Theorem 2 to this equation.

Lemma 2. *Let $\{a, b, c, d\}$, $0 < a < b < c < d$ be a polynomial $D(n)$-quadruple with $n \in \mathbb{Z}[x]$. Then*

$$\deg d \leq 51(\deg a + \deg b + \deg c) + 78 \deg n.$$

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

$$Y^2 = (X+nbc)(X+nac)(X+nab).$$

The polynomial on the left 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 $\mathbb{Z}[x]$. Let S be the set of coefficients of this polynomial, i.e.

$$S = \{1, n(ab+bc+ac), n^2abc(a+b+c), n^3a^2b^2c^2\}.$$

Since the elements of S are polynomials, we get for each $\xi \in \mathbb{C}$ that

$$\nu_\xi(S) = \min_{s \in S}\{0, \nu_\xi(s)\} = 0.$$

Moreover, we have

$$\nu_\infty(S) = \min_{s\in S}\{0, \nu_\infty(s)) = \min_{s\in S}\{-\deg s\} = -\max_{s\in S}\deg s,$$

and by comparing the degrees of the elements of S we get

$$\nu_\infty(S) = -2(\deg a + \deg b + \deg c) - 3\deg n.$$

Therefore,

$$\mathcal{H}(S) = -\sum_{\nu} \min\{0, \nu(S)\} = -\sum_{\xi\in\mathbb{C}} \min\{0, \nu_\xi(S)\} - \min\{0, \nu_\infty(S)\} =$$
$$= -\min\{0, \nu_\infty(S)\} = 2(\deg a + \deg b + \deg c) + 3\deg n.$$

Thus, we have for the height H of the polynomial on the right hand side of our elliptic equation

$$H = 2(\deg a + \deg b + \deg c) + 3\deg n.$$

By Mason's Theorem 2 with $L = \mathbb{C}(x)$ and $\mathcal{O} = \mathbb{C}[x]$ we therefore get

$$\deg X \leq 52(\deg a + \deg b + \deg c) + 78\deg n,$$

where we have used that the genus of the rational function field $\mathbb{C}(x)$ is zero (which can be found e.g. in [14], page 22) and that $\mathbb{C}(x)$ has only one infinite valuation, namely ν_∞. But now by the definition of $X = abcd$ we get

$$\deg d \leq 51(\deg a + \deg b + \deg c) + 78\deg n$$

as claimed in our lemma. □

Observe that due to the sharpness of the fundamental inequality this bound is very good. Especially, it does not depend on a gap which has to appear between the elements of the quadruple as in the classical case (cf. [6, Lemma 2]).

We use Lemma 1 to prove the following gap principle. It is very similar to [6, Lemma 4] in the classical case for integers.

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

$$n^2 d > 2bc.$$

Proof. We apply Lemma 1 to the triple $\{a, c, d\}$. Let e be defined as in Lemma 1. Since $ce+n^2$ is a perfect square, we have that $ce+n^2 \geq 0$. Assume that $e \leq -1$, then

$$ce + n^2 < -2n^2 + n^2 = -n^2 < 0,$$

a contradiction. Therefore, we have $e \geq 0$. Observe that, if $n > 0$ we have

$$a^2 < ac + r^2 = ac + ab + n \iff na^2 < na(b + c) + n^2 \iff$$
$$a^2t^2 = a^2(n + bc) = na^2 + a^2bc < a^2bc + na(b + c) + n^2 =$$
$$= (ab + n)(ac + n) = r^2s^2 \iff$$
$$at < rs \iff u < 0,$$

and

$$b^2 < bc + r^2 = bc + ab + n \iff nb^2 < nb(a+c) + n^2 \iff$$
$$b^2 s^2 = b^2(ac+n) = ab^2 c + b^2 n < ab^2 c + nb(a+c) + n^2 =$$
$$= (ab+n)(bc+n) = r^2 t^2 \iff$$
$$bs < rt \iff v < 0.$$

In the same way, one can show that $n < 0$ implies

$$u > 0 \quad \text{and} \quad v > 0.$$

If $e = 0$, then $d = a + c + 2s$. If $e \geq 1$, then

$$n^2 d = n^2(a+b) + en + 2(abe + ruv) > 2ab.$$

Note that we need here that $uv > 0$ which follows from the comments just made.

Analogously, we apply Lemma 1 to the triple $\{b, c, d\}$ and obtain either $d = b + c + 2t$ or $n^2 d > 2bc$. However, $d = b + c + 2t$ is impossible since $s^2 = ac + n < bc + n = t^2$ and therefore $s < t$ which implies $a + c + 2s < b + c + 2t$ and

$$n^2(b + c + 2t) < n^2 \cdot 4c < 2ac,$$

which follows from

$$t^2 = bc + n \leq (c-1)c + n = c^2 + n - c < c^2 + n - n^2 < c^2$$

since $c > 2n^2$ and consequently $t < c$.

Hence, we proved

$$n^2 d > 2bc,$$

as claimed in our lemma. □

Proof of Proposition 1.

Assume that $\{a, b, c, a_4, a_5, \ldots, a_{16}\}$ is a polynomial $D(n)$-16-tuple and $|n|^3 \leq a < b < c < a_4 < a_5 < \ldots < a_{16}$. We apply Lemma 2 to the quadruple $\{a, b, c, a_{16}\}$ and obtain

$$a_{16} < (abc)^{52} n^{78} < c^{156} n^{78} < c^{182}, \tag{4}$$

since $|n|^3 < c$.

Lemma 3 implies $n^2 a_4 > bc > |n|^3 c$ and $a_4 > c|n|$. Furthermore, $n^2 a_5 > a_4 c > c^2 |n|$ and $|n| a_5 > c^2$. In the same manner, Lemma 3 gives

$$\begin{array}{lll} n^2 a_6 > a_5 a_4 > c^3, & |n|^5 a_7 > |n|^3 a_6 a_5 > c^5, & |n|^9 a_8 > c^8, \\ n^{16} a_9 > c^{13}, & |n|^{27} a_{10} > c^{21}, & |n|^{45} a_{11} > c^{34}, \\ n^{74} a_{12} > c^{55}, & |n|^{121} a_{13} > c^{89}, & |n|^{197} a_{14} > c^{144}, \\ |n|^{320} a_{15} > c^{233}, & |n|^{519} a_{16} > c^{377}, & \end{array}$$

which implies (since $|n|^3 < c$) that

$$c^{173} a_{16} > c^{377}$$

and therefore

$$a_{16} > c^{204},$$

a contradiction to (4). □

Proof of Proposition 2.

Let $S = \{a, b, c\}$ with $a < b < c$ be a polynomial $D(n)$-triple with linear $n \in \mathbb{Z}[x]$ and let $\deg a = \deg b = \deg c = 3$. Then by (2) we get $\deg \overline{e} = 9$. But from (3) it follows that $\deg e\overline{e} \leq 8$. Thus we have a contradiction unless $e = 0$, i.e. $c = a + b + 2r$. Consequently, if we fix a and b, then c is unique, which implies that S cannot be extended to a polynomial $D(n)$-quadruple. Therefore,

$$L_3 \leq 3,$$

as claimed in our proposition. □

Observe that Proposition 2 follows directly from Lemma 3, but the above proof gives more information on triples of cubic polynomials.

4. Elements with small degrees

First we prove Proposition 3. Here the argument from the proof of Proposition 2 does not longer work. The polynomials e which are induced by a polynomial $D(ax+b)$-triple in Lemma 1 are constants. The proof uses the fact that $u^2 - n^2 = (u - n)(u + n)$ is a complete factorization of the polynomial a up to the constant factor.

Proof of Proposition 3.

Let $\{a, b, c\}$ with $a < b < c$ be a polynomial $D(n)$-triple with linear $n \in \mathbb{Z}[x]$ and let $\deg a = \deg b = \deg c = 2$. Then by (2) we get $\deg \overline{e} = 6$. Now (3) implies that e is a constant. Assume that two distinct e's exist. We call them e and f. From $ae + n^2 = u^2$ we see that a is a product of two linear polynomials:

$$a = \alpha(x - a_0)(x - a_1).$$

Let us assume that we have

$$u - n = \varepsilon_1(x - a_0), \quad u + n = \varepsilon_2(x - a_1),$$

where $\varepsilon_1\varepsilon_2 = \alpha\varepsilon$. It implies

$$2n = x(\varepsilon_2 - \varepsilon_1) + \varepsilon_1 a_0 - \varepsilon_2 a_1.$$

In the same manner, we can conclude from $af + n^2 = u^2$ that

$$u - n = \varphi_1(x - a_0), \quad u + n = \varphi_2(x - a_1),$$

or

$$u - n = \varphi_1(x - a_1), \quad u + n = \varphi_2(x - a_0)$$

holds. Let us first consider that the first of this equations holds. Then we get

$$2n = x(\varphi_2 - \varphi_1) + \varphi_1 a_0 - \varphi_2 a_1,$$

where $\varphi_1\varphi_2 = \alpha f$. Hence, $\varepsilon_2 - \varepsilon_1 = \varphi_2 - \varphi_1, \varepsilon_1 a_0 - \varepsilon_2 a_1 = \varphi_1 a_0 - \varphi_2 a_1$. Consequently, we have $a_0(\varepsilon_1 - \varphi_1) = a_1(\varepsilon_2 - \varphi_2) = a_1(\varepsilon_1 - \varphi_1)$. We have two possibilities: $\varepsilon_1 = \varphi_1$ or $a_0 = a_1$.

Let first assume $\varepsilon_1 = \varphi_1$. This implies also $\varepsilon_2 = \varphi_2$ and therefore $e = f$, a contradiction. Now we assume that $a_0 = a_1$ holds. Then $x - a_0 | n$ and together with $ab + n = r^2$ this implies $x - a_0 | r$. Therefore $(x - a_0)^2 | n$, and we obtained a contradiction since n is a linear polynomial.

Now let us consider the second case. So assume that we have

$$u - n = \varphi_1(x - a_1), \quad u + n = \varphi_2(x - a_0),$$

where φ_1, φ_2 are as above. It implies

$$2n = x(\varphi_2 - \varphi_1) + \varphi_1 a_1 - \varphi_2 a_0.$$

Hence, $\varepsilon_2 - \varepsilon_1 = \varphi_2 - \varphi_1, \varepsilon_1 a_0 - \varepsilon_2 a_1 = \varphi_1 a_1 - \varphi_2 a_0$. This yields, $a_0(\varepsilon_1 + \varphi_2) = a_1(\varphi_1 + \varepsilon_2) = a_0(\varepsilon_1 + \varphi_2)$. We have again two possibilities: $\varepsilon_1 = -\varphi_2$ which implies $\varepsilon_2 = -\varphi_1$ and therefore $e = f$, a contradiction, or $a_0 = a_1$. But as above this yields a contradiction with the assumption that n is a linear polynomial.

Therefore, there is at most one such constant e. It follows that for fixed a and b, there are at most three c, namely $c = a + b + 2r$ and two possible $c(e)$ which come from

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

where u, v satisfy $ae + n^2 = u^2, be + n^2 = v^2$. This last equations fix u and v only up to the sign and therefore we get two possible c's in this case. Consequently we get

$$L_2 \leq 5,$$

which was claimed in the proposition. □

As in the proof of Proposition 3, we will see that also the proof of Proposition 4 heavily depends on the fact that we are considering linear polynomials. Especially, we will use that (3) is the complete factorization of the product $e\overline{e}$.

Proof of Proposition 4.

Let $S = \{a, b, c\}$ with $a < b < c$ be polynomial $D(n)$-triple with linear $n \in \mathbb{Z}[x]$ and let $\deg a = \deg b = \deg c = 1$. Then by (2) we get $\deg \overline{e} = 3$. Now (3) implies that

$$\deg e \leq 1.$$

From $ab + n = r^2$ it follows that at most one of the elements in S is divisible by n. Indeed, assume that a and b are divisible by n. Then $n | r$ and $n^2 | n$, a

contradiction. Thus we may assume that a, b, c are not divisible by n. We have

$$e + \overline{e} = 2n(a + b + c) + 4abc. \tag{5}$$

$$\overline{e} - e = 4rst. \tag{6}$$

If $n|e$, then (3) implies that $n|\overline{e}$ and therefore, by (5), we get $n|abc$, a contradiction.

Therefore, $e = \delta \cdot (c - a - b \pm 2r)$, $\delta \in \mathbb{Q}$. Assume that $\delta \neq 0$. We have

$$\overline{e} = n^2(c - a - b \mp 2r)\frac{1}{\delta}.$$

This implies

$$\frac{e}{\delta} - \frac{\overline{e}\delta}{n^2} = \pm 4r$$

or

$$\frac{n^2 e}{\delta} - \overline{e}\delta = \pm 4n^2 r$$

or

$$\frac{n^2 e}{\delta} - e\delta = 4r(\delta st \pm n^2).$$

This can be written as

$$\frac{e}{\delta}(n^2 - \delta^2) = 4r(\delta st \pm n^2).$$

Hence, there are two possibilities: $r|e$ or $r|n \pm \delta$.

If $r|e$, then by (6) we have $r|\overline{e}$ which yields

$$r^2 | n^2(c - a - b - 2r)(c - a - b + 2r).$$

If $r|n$, then from $ab + n = r^2$ we conclude $r|a$ or $r|b$. Both cases lead to a contradictions since this would imply $n|a$ or $n|b$. Observe that r and n only differ by a constant factor since they are both linear. Thus, $r|c - a - b$, say $c = a + b + r \cdot \rho$, $\rho \in \mathbb{Q}$. But from this we get

$$ac + n = a^2 + ab + ar\rho + n = a^2 + r^2 + \rho ar = s^2$$

or

$$(2r + \rho a)^2 - (\rho^2 - 4)a^2 = (2s)^2.$$

Now, if $\rho = \pm 2$ then $c = a + b \pm 2r$. Observe that by considering leading coefficients it is clear that $a + b - 2r < b$ so this case is impossible and it remains the possible case $c = a + b + 2r$. Otherwise, if $\rho \neq \pm 2$, we have

$$(\rho^2 - 4)a^2 = (2r + \rho a - 2s)(2r + \rho a + 2s)$$

which implies $a|r$ and $a|s$, and moreover, using $ab + n = r^2$, we get $a|n$ or equivalently $n|a$, a contradiction.

Therefore, it remains the case $r|n \pm \delta$. It means that δ is unique. It is defined by $n \equiv \mp\delta \pmod{r}$. Let $n \equiv \delta_0 \pmod{r}$. We have the following five possibilities for c, namely $c = a + b + 2r$ and $c(e)$, where $e = (c - a - b +$

$2r)(-\delta_0)$ or $e = (c-a-b-2r)\cdot\delta_0$. Each of this two e's induce at most two c's as we have seen at the end of the proof of Proposition 3. Therefore, we have at most seven linear polynomials in S which are not divisible by n. We get

$$L_1 \leq 8,$$

and so the proof is finished. □

Now we are ready to prove our bound for L.

Proof of Theorem 1.

Let S be a polynomial $D(ax+b)$-m-tuple with some integers $a \neq 0$ and b. From the fact that the product of each two elements from S plus $ax+b$ 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. Together with the upper bound for the number of polynomials in S with degree ≥ 4, this implies that we have

$$|S| \leq 11 + 15 = 26.$$

This proves our theorem. □

References

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

[2] 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.

[3] M. A. Bennett, On the number of solutions of simultaneous Pell equations, *J. Reine Angew. Math.* **498** (1998), 129–137.

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

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

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

[7] A. Dujella, There are only finitely many Diophantine quintuples, preprint.

[8] A. Dujella and C. Fuchs, A polynomial variant of a problem of Diophantus and Euler, *Rocky Mountain J. Math.*, to appear.

[9] P. X. Gallagher, A large sieve, *Acta Arith.* **18** (1971), 77–81.

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

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

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

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

[14] 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

Robert F. Tichy
Institut für Mathematik
TU Graz
Steyrergasse 30
A-8010 Graz, Austria.
e-mail: tichy@tugraz.at