PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 138, Number 5, May 2010, Pages 1549–1557
S 0002-9939(09)10259-9
Article electronically published on December 29, 2009

AN EXTENSION OF BÜCHI'S PROBLEM FOR POLYNOMIAL RINGS IN ZERO CHARACTERISTIC

HECTOR PASTEN

(Communicated by Julia Knight)

ABSTRACT. We prove a strong form of the "n Squares Problem" over polynomial rings with characteristic zero constant field. In particular we prove: for all $r \geq 2$ there exists an integer $M = M(r)$ depending only on r such that, if $z_1, z_2, ..., z_M$ are M distinct elements of F and we have polynomials $f, g, x_1, x_2, \ldots, x_M \in F[t]$, with some x_i non-constant, satisfiying the equations $x_i^r = (z_i + f)^r + g$ for each i, then g is the zero polynomial.

1. Introduction

Büchi's Problem, also known as the "n Squares Problem", asks whether there exists some positive integer M such that any sequence of M integer squares, whose second difference is constant and equal to 2, is of the form $(x+n)^2$, $n = 0, 1, \ldots, M$, for some integer x. This problem, still open, was proposed by R. Büchi in the 1970s (and publicized by L. Lipshitz in 1990 in [5]) as he realized that a positive answer to it would imply a strong improvement to the negative answer to Hilbert's Tenth Problem, recently obtained by Y. Matiyasevic, after the works of M. Davis, H. Putnam and J. Robinson. See [3] and [6].

Vojta proved in [12] that a positive answer to Büchi's Problem follows from a conjecture of Lang on rational points on projective varieties of general type. In [7], Pheidas and Vidaux proposed a problem $\mathbf{B_r}(A)$ extending Büchi's Problem by considering r-th differences of r-th powers constant and equal to $r!$, and where the variables range over any integral domain A, the point being that in most cases, a positive answer to $\mathbf{B_r}(A)$ will have logical consequences similar to the "integer and square case". If A is a ring of functions, then it is required also that not all the r powers are constant. Vojta [12] proved that the problem $\mathbf{B_2}(\mathcal{M})$, where $\mathcal{M}$ is the field of functions that are meromorphic over $\mathbb{C}$, has a positive answer (using Nevanlinna theory). Pheidas and Vidaux proved [8] that $\mathbf{B_2}(A)$ has a positive answer whenever A is a ring of polynomials or is a field of rational functions of zero characteristic, but if the characteristic is positive and large, there are more "trivial solutions" than those named in the original statement (see [9]). In [10], they proved that $\mathbf{B_3}(F[t])$ has a positive answer when F is any field of zero characteristic.

Received by the editors September 2, 2008, and, in revised form, March 12, 2009.
2010 *Mathematics Subject Classification.* Primary 11U05, 12L05; Secondary 11C08.
Key words and phrases. Büchi's problem, squares problem, polynomials, Hilbert's tenth problem.

As D. Hensley noticed in [4], $\mathbf{B_2}(\mathbb{Z})$ is equivalent to the following problem. $\mathbf{H_2}(\mathbb{Z})$: Does there exist a positive integer M such that, for any integers μ and ν, the following system of equations

$$x_n^2 = (n+\nu)^2 + \mu \ , \quad n = 0, \dots, M$$

has an integer solution if and only if $\mu = 0$?

It is not so difficult to see that this equivalence holds for many commutative rings (see Section 5).

So we may write $\mathbf{H_2}(A)$ for the analogue of Hensley's formulation over the ring A. Then we may consider the problem $\mathbf{H_r}(A)$ where the squares are simply replaced by r-th powers. Observe that a positive answer to $\mathbf{B_r}(A)$ would imply a positive answer to $\mathbf{H_r}(A)$, but the converse is true only if $r = 2$.

We sharpen techniques developed in [8] and [10] in order to prove that $\mathbf{H_r}(F[t])$, where F is a field of zero characteristic, has a positive answer (see Theorem 2.1 in Section 2). Other analogous forms of Büchi's Problem over the integers have been studied by Buell [2], then by Pinch [11] and eventually by Browkin and Brzeziński [1]. Our main result, Theorem 2.1, actually implies a quite stronger form of $\mathbf{H_r}(F[t])$ for any power r, so we may consider it as new evidence for $\mathbf{B_r}(F[t])$ to have a positive answer.

We observe that in contrast to the method developed in [8] and [10], we do not make use of the fact that elliptic curves do not admit rational parametrizations. Our proof is essentially combinatorial and therefore should be more easily adaptable, for example, to algebraic extensions of polynomial rings and rational function fields, both in positive and in zero characteristic.

This work was done during the undergraduate studies of the author at the Universidad de Concepción, Chile. I thank the professors of the math department (Departamento de Matemática) for their useful comments, especially Xavier Vidaux for many valuable discussions.

2. Main result and corollaries

Let F be a field of characteristic zero.

If S is a non-empty finite subset of F and $r \geq 2$ is an integer, we will write

$$\xi(S, r) = \max_{c,d \in \bar{F}} |S \cap \{x \in F : (x+c)^r = d\}|$$

where $\bar{F}$ denotes an algebraic closure of F. Observe that $1 \leq \xi(S, r)$ because $(s+0)^r = s^r$ for each s in S, and $\xi(S, r) \leq r$ since the polynomial $(X + c_1)^r - c_2$ has degree r.

For $x \in \mathbb{R}$ we denote by $\lceil x \rceil$ the least integer greater than or equal to x ($\lceil . \rceil$ is the ceiling function).

Theorem 2.1 (Main Result)**.** *Let F be a field of characteristic zero and $r \geq 2$ an integer. Suppose we have a sequence $(x_n)_{n=1}^M \subseteq F[t]$ of M polynomials such that:*

1. *Not all the x_n are constant.*
2. *There exist a set $S = \{z_n : n = 1, \dots, M\} \subseteq F$ with M elements and two polynomials f, g in $F[t]$ such that $\left\lceil \frac{r^3}{(r-1)^2} \xi(S, r) \right\rceil \leq M - 1$ and $x_n^r = (z_n + f)^r + g$ for each n.*

Then g is the zero polynomial.

If we know some information about r, F or S in the Main Result, then a constant M can be computed explicitly. To illustrate that, we may set $F = \mathbb{R}$ and $S \subseteq \mathbb{Z}$. At most 2 of the elements in S at the same time can be solutions of an equation of the form $(z + c_1)^r = c_2$ with c_1, c_2 in $\mathbb{C} = \bar{\mathbb{R}}$ (since the integers are collinear in $\mathbb{C}$); hence $\xi(S, r) = 2$. Another example is given by considering $F = \mathbb{C}$ and S a set of complex numbers such that no cyclic k-gon ($k \geq 3$) has vertices in S. Then $\xi(S, r) \leq \min\{r, k-1\}$, and we can compute an explicit value for M.

From Theorem 2.1, we can derive the following strong form of $\mathbf{H_r}(F[t])$.

Corollary 1. *For all $r \geq 2$ there exists an integer $M = M(r)$ depending only on r such that, if $z_1, z_2, ..., z_M$ are M distinct elements of F and we have polynomials $f, g, x_1, x_2, \ldots, x_M \in F[t]$, with some x_i non-constant, satisfiying the equations $x_i^r = (z_i + f)^r + g$ for each i, then g is the zero polynomial.*

Proof. Take $M = \lceil \frac{r^4}{(r-1)^2} \rceil + 1$ and $S = \{z_1, \ldots, z_M\}$. We have then

$$|S| = M = \left\lceil \frac{r^4}{(r-1)^2} \right\rceil + 1 \geq \left\lceil \frac{r^3}{(r-1)^2} \xi(S, r) \right\rceil + 1 \ . \qquad \square$$

In particular we have $\mathbf{H_r}(F[t])$:

Corollary 2. *Let $r \geq 2$ be an integer. There exists an integer $M = M(r)$ depending only on r such that, if the polynomials $f, g, x_1, x_2, ..., x_M \in F[t]$ (with some x_i non-constant) satisfy the equations $x_n^r = (n + f)^r + g$ for $n = 1, 2, \ldots, M$, then g is the zero polynomial.*

The n Squares Problem in $F[t]$ follows:

Corollary 3. *There exists an integer M such that any sequence $(x_n)_{n=1}^M$ of (not all constant) polynomials in $F[t]$ satisfying the system of equations*

$$\begin{aligned} x_1^2 - 2x_2^2 + x_3^2 &= 2 \\ x_2^2 - 2x_3^2 + x_4^2 &= 2 \\ &\cdots \\ x_{M-2}^2 - 2x_{M-1}^2 + x_M^2 &= 2 \end{aligned}$$

satisfies also the system of equations $x_n^2 = (n + f)^2$, $n = 1, \ldots, M$, for some $f \in F[t]$.

Proof. This follows immediately from Corollary 2 (with $r = 2$) by solving the recurrence, see Section 5. $\square$

3. Intermediate results

In this section we shall prove some lemmas before proving Theorem 2.1.

Assumption 1. Without loss of generality, assume that F is algebraically closed.

Notation 1. Write $h = -g$ and $\xi = \xi(S, r)$. Set $I = \{1, 2, \ldots, M\}$, where $M = \left\lceil \frac{r^3}{(r-1)^2} \xi \right\rceil + 1$. Note that $M > 1$, since $\frac{r^3}{(r-1)^2} \xi > 0$. Label the elements of S as $z_n, n \in I$. So by hypothesis we have

$$x_n^r = (z_n + f)^r - h \ . \tag{3.1}$$

Set

$$d_f = \deg f \quad \text{and} \quad d_h = \deg h$$

and choose $\alpha \neq \omega \in I$ such that $d = \deg x_\alpha$ is maximum and $d_0 = \deg x_\omega$ is minimum (possibly $d = d_0$), among the degrees of the x_n's. Write

$$I' = I - \{\omega\} .$$

On the one hand, differentiating both sides of (3.1) we obtain

$$rx_n' x_n^{r-1} = rf'(z_n + f)^{r-1} - h';$$

hence

$$(rx_n' x_n^{r-1} + h')^r = r^r f'^r (z_n + f)^{r(r-1)}.$$

On the other hand, also from (3.1) we have

$$(x_n^r + h)^{r-1} = (z_n + f)^{r(r-1)} .$$

Substituting $(z_n + f)^{r(r-1)}$ into the previous equation, we obtain

$$(rx_n' x_n^{r-1} + h')^r = r^r f'^r (x_n^r + h)^{r-1} . \tag{3.2}$$

Let us denote

$$\Delta = h'^r - r^r f'^r h^{r-1} ,$$

namely, the part of (3.2) that does not depend on n.

Lemma 3.1. *We have*

(1) $0 < d = \deg x_n$, *for all* $n \in I'$;

(2) $\deg(\Delta) \leq \dfrac{r(dr^2 - (r-1))}{r-1}$.

Proof. For $j \neq k \in I$ we note that

$$\begin{aligned} x_j^r - x_k^r &= (z_j + f)^r - (z_k + f)^r \\ &= r(z_j - z_k) f^{r-1} + (\text{terms in lower powers of } f) . \end{aligned}$$

Therefore we have

$$\deg(x_j^r - x_k^r) = (r-1)d_f; \tag{3.3}$$

hence

$$d_f \leq \frac{r}{r-1} d. \tag{3.4}$$

From (3.1) and (3.4), it follows that

$$d_h \leq \max\{rd, rd_f\} \leq \frac{r^2}{r-1} d;$$

thus, after an easy computation,

$$\deg(\Delta) \leq \frac{r(dr^2 - r + 1)}{r-1} .$$

Note that from (3.3) we have

$$\deg(x_\alpha^r - x_\omega^r) = \deg(x_n^r - x_\omega^r)$$

as long as $n \in I'$. So, if $d > d_0$, then all x_n but possibly x_ω have degree d; otherwise all x_n have the same degree d, and from the hypothesis of some x_n being non-constant we have $d > 0$. □

Notation 2. We will be writing Λ for a least common multiple of $\{x_n | n \in I'\}$.

Note that Λ is not constant since, by Lemma 3.1 (1), none of the x_n's, for $n \in I'$, is constant.

Lemma 3.2. *The polynomial Λ^{r-1} divides Δ.*

Proof. From (3.2) we deduce that x_n^{r-1} divides Δ for each $n \in I'$ and the result follows. □

Lemma 3.3. *No $\xi+1$ polynomials in $\{x_n | n \in I'\}$ have a common non-constant factor.*

Proof. By Lemma 3.1 (1), the polynomials in $\{x_n | n \in I'\}$ are non-constant.

Suppose that for some distinct $\xi+1$ indices $i(1), i(2), ..., i(\xi+1) \in I'$, there exists $\rho \in F$ such that ρ is a common zero for all $x_{i(l)}$. Consider the following equations derived from (3.1):

$$\begin{aligned} x_{i(1)}^r - x_{i(2)}^r &= (z_{i(1)} + f)^r - (z_{i(2)} + f)^r \\ x_{i(2)}^r - x_{i(3)}^r &= (z_{i(2)} + f)^r - (z_{i(3)} + f)^r \\ &\cdots \\ x_{i(\xi)}^r - x_{i(\xi+1)}^r &= (z_{i(\xi)} + f)^r - (z_{i(\xi+1)} + f)^r. \end{aligned}$$

Evaluating at ρ we obtain

$$(z_{i(1)} + f(\rho))^r = (z_{i(2)} + f(\rho))^r = \cdots = (z_{i(\xi+1)} + f(\rho))^r = c$$

for some $c \in F$. It follows that the equation $(z + f(\rho))^r = c$ has at least $\xi + 1$ distinct roots, since by the hypothesis of Theorem 2.1, $i \neq j$ implies $z_i \neq z_j$. This contradicts the definition of ξ. □

Lemma 3.4. *We have $\Delta = 0$.*

Proof. Let $p \in F[t]$ be a prime polynomial. From Lemma 3.3, p divides at most ξ polynomials in $\{x_n | n \in I'\}$, so we have

$$\max\{\nu_p(x_n) | n \in I'\} \geq \frac{1}{\xi} \sum_{n \in I'} \nu_p(x_n) = \frac{1}{\xi} \nu_p \left(\prod_{n \in I'} x_n \right),$$

where ν_p denotes the function *"order at p"*.

Summing the left and right hand sides of this last inequality over the primes dividing $\prod_{n \in I'} x_n$, from Lemma 3.1 (1) we obtain

$$\deg\left(\operatorname{lcm}\{x_n | n \in I'\}\right) \geq \frac{1}{\xi} \deg\left(\prod_{n \in I'} x_n \right) = \frac{M-1}{\xi} d,$$

where "lcm" means *"least common multiple"*. Therefore we have

$$\deg(\Lambda) \geq \frac{M-1}{\xi} d.$$

Note that if Δ is not the zero polynomial, then from Lemma 3.2, we deduce

$$(r-1)\deg(\Lambda) \leq \deg(\Delta)\ .$$

Thus, by Lemma 3.1 (2), we have

$$\frac{M-1}{\xi} d \leq \deg(\Lambda) \leq \frac{1}{r-1} \deg(\Delta) \leq \frac{r(dr^2 - (r-1))}{(r-1)^2}.$$

As $0 < d$ (Lemma 3.1 (1)), this implies that

$$M \leq \frac{\xi}{d}\frac{r(dr^2-(r-1))}{(r-1)^2}+1 \leq \frac{r^3\xi}{(r-1)^2}-\frac{r\xi}{(r-1)d}+1$$
$$< \frac{r^3\xi}{(r-1)^2}+1 \leq \left\lceil \frac{r^3\xi}{(r-1)^2} \right\rceil + 1 = M,$$

hence gives us a contradiction. So we have $\Delta = 0$. □

4. Proof of Theorem 2.1

In order to prove the Main Result, we will suppose that

Assumption 2. h is not the zero polynomial.

We will obtain a contradiction.

The next four lemmas will be under Assumption 2.

From Lemma 3.4 we have

$$\Delta = h'^r - r^r f'^r h^{r-1} = 0 \Rightarrow h'^r = r^r f'^r h^{r-1}. \tag{4.1}$$

Since some of the x_n's are not constant, from (3.1) we note that f, g are not both constant. Therefore, from (4.1) and Assumption 2 we have that if h is a non-zero constant, then $f' = 0$, so f is constant; thus h is a non-constant polynomial. Moreover, if f is constant, then we have $h' = 0$ from (4.1); hence f is a non-constant polynomial. So, under Assumption 2, h and f are non-constant polynomials.

Notation 3. Let φ, η be the leading coefficients of f, h respectively.

Lemma 4.1. *We have $d < d_f$.*

Proof. From Assumption 2 we have f non-constant; thus from (4.1) we deduce

$$r(d_h - 1) = r(d_f - 1) + d_h(r-1) \Rightarrow d_h = rd_f \neq 0$$

and

$$(d_h\eta)^r = r^r(d_f\varphi)^r\eta^{r-1} \Rightarrow \eta = \left(\frac{rd_f}{d_h}\right)^r \varphi^r = \varphi^r \ .$$

It follows that $(z_n + f)^r$ and h must have the same degree and leading coefficient for each $n \in I$. Hence, by (3.1), we have $rd < rd_f$; hence $d < d_f$. □

Lemma 4.2. *We have*

$$r\deg(x_n) = rd = (r-1)d_f$$

for each $n \in I'$.

Proof. By (3.1), for each $n \in I'$ we have $h = (z_n+f)^r - x_n^r$. Plugging this expression for h into (4.1), we obtain

$$(rf'(z_n+f)^{r-1} - rx_n'x_n^{r-1})^r = r^r f'^r((z_n+f)^r - x_n^r)^{r-1};$$

hence

$$(f'(z_n+f)^{r-1} - x_n'x_n^{r-1})^r = f'^r((z_n+f)^r - x_n^r)^{r-1}. \tag{4.2}$$

Expanding each side of this equation we get

$$\sum_{i=0}^{r}(-1)^i\binom{r}{i}(f'(z_n+f)^{r-1})^{r-i}(x_n'x_n^{r-1})^i \\ = \sum_{j=0}^{r-1}(-1)^j\binom{r-1}{j}f'^r(z_n+f)^{r(r-1-j)}x_n^{rj},$$

and cancelling terms for $i=0=j$ we have

$$\sum_{i=1}^{r}(-1)^i\binom{r}{i}(f'(z_n+f)^{r-1})^{r-i}(x_n'x_n^{r-1})^i \\ = \sum_{j=1}^{r-1}(-1)^j\binom{r-1}{j}f'^r(z_n+f)^{r(r-1-j)}x_n^{rj}\ .$$

Since $d<d_f$ (by Lemma 4.1) and $0<d=\deg x_n, \forall n\in I'$ (by Lemma 3.1 (1)), the sequence of polynomials in each sum of the last equation has decreasing positive degree. Therefore, by observing the leading coefficients at $i=1=j$, we have

$$r(d_f\varphi)^{r-1}\varphi^{(r-1)^2}d_nX_n^r=(r-1)(d_f\varphi)^r\varphi^{r(r-2)}X_n^r,$$

where $d_n=d$ and X_n are the degree and the leading coefficient of x_n for each $n\in I'$, respectively. Hence we have

$$rd_n=(r-1)d_f\ . \qquad \square$$

Notation 4. Write $\Gamma=\gcd\{x_n'x_n^{r-1}|n\in I'\}$, where gcd means "greatest common divisor".

Note that Γ is well defined since $0<d=\deg x_n, \forall n\in I'$, and is not the zero polynomial.

Lemma 4.3. *We have* $\deg\Gamma\geq d_f-1$.

Proof. From (4.2),

$$(f'(z_n+f)^{r-1}-x_n'x_n^{r-1})^r=f'^r((z_n+f)^r-x_n^r)^{r-1},$$

we see that f' divides $x_n'x_n^{r-1}$ for all $n\in I'$. $\square$

Recall that we have $d_f\geq 1$ and $r\geq 2$. So Lemma 4.2 implies that r divides d_f; hence the degree of f' is $d_f-1\geq 1$. We conclude that Γ is not constant by Lemma 4.3.

Lemma 4.4. *The following inequality holds:*

$$d-1\geq\frac{M-1-\xi}{M-1}\deg\Gamma.$$

Proof. Write $\prod_{p_i|\Gamma}p_i^{a_i}$ for the prime factorisation of Γ (up to factors in F). Since Γ is not constant this product is not empty, and since F is assumed to be algebraically closed we have $\deg p_i=1$ for each i.

We claim that each $p_i^{a_i}$ in the factorisation of Γ divides at least $M-1-\xi$ elements in $\{x_n' \mid n\in I'\}$. Indeed, recall that $|I'|=M-1$ and notice that each $p_i^{a_i}$ must divide $x_n'x_n^{r-1}$ for each $n\in I'$ by definition of Γ. But from Lemma 3.3 we know

that each p_i can divide at most ξ polynomials in $\{x_n^{r-1} \mid n \in I'\}$; hence each $p_i^{a_i}$ must divide at least $M-1-\xi$ polynomials in $\{x'_n \mid n \in I'\}$.

Therefore we have that for each p_i, $p_i^{a_i(M-1-\xi)}$ divides $\prod_{n\in I'} x'_n$. Hence $\Gamma^{M-1-\xi}$ divides $\prod_{n\in I'} x'_n$ and we have

$$(M-1)(d-1) = \deg\left(\prod_{n\in I'} x'_n\right) \geq (M-1-\xi)\deg\Gamma,$$

which proves the lemma, since $M > 1$. □

Proof of Main Result. Suppose that Assumption 2 is true. By Lemma 4.3 and Lemma 4.4 we have

$$d-1 \geq \frac{M-1-\xi}{M-1}\deg\Gamma \geq \frac{M-1-\xi}{M-1}(d_f-1)\ .$$

Thus, by Lemma 4.2 and the definition of M we have

$$\begin{aligned} d-1 &\geq \frac{M-1-\xi}{M-1}\left(\frac{rd}{r-1}-1\right) = \frac{\left\lceil \frac{r^3}{(r-1)^2}\xi\right\rceil + 1 - 1 - \xi}{\left\lceil \frac{r^3}{(r-1)^2}\xi\right\rceil + 1 - 1}\left(\frac{r}{r-1}d-1\right) \\ &= \frac{\left\lceil \frac{r^3}{(r-1)^2}\xi\right\rceil - \xi}{\left\lceil \frac{r^3}{(r-1)^2}\xi\right\rceil}\left(\frac{r}{r-1}d-1\right)\ . \end{aligned}$$

Since $\lceil y\rceil \geq y$ by definition, and $y \mapsto (y-\xi)/y = 1-\frac{\xi}{y}$ is an increasing positive function for $y > \xi$, we have

$$d-1 \geq \frac{\frac{r^3}{(r-1)^2}\xi - \xi}{\frac{r^3}{(r-1)^2}\xi}\left(\frac{r}{r-1}d-1\right);$$

hence

$$\begin{aligned} d-1 &\geq \frac{\frac{r^3}{(r-1)^2}-1}{\frac{r^3}{(r-1)^2}}\left(\frac{r}{r-1}d-1\right) = \left(1-\frac{1}{\frac{r^3}{(r-1)^2}}\right)\left(\frac{r}{r-1}d-1\right) \\ &= \frac{r}{r-1}d - 1 - \frac{(r-1)^2}{r^3}\left(\frac{r}{r-1}d-1\right); \end{aligned}$$

hence

$$\frac{(r-1)^2}{r^3}\left(\frac{r}{r-1}d-1\right) \geq \frac{r}{r-1}d - d = \frac{d}{r-1};$$

hence

$$\frac{(r-1)^2}{r^3}(rd-r+1) \geq d\ .$$

Therefore, as $r \geq 2$ we have

$$d \leq \frac{(r-1)^2}{r^3}(rd-r+1) < \frac{(r-1)^2}{r^3}(rd-1+1) = \frac{(r-1)^2}{r^3}rd < d,$$

which gives us a contradiction. Hence Assumption 2 is false and g is the zero polynomial. □

5. Equivalence of Büchi's problem and Hensley's formulation

Proposition 1. *Let A be a commutative ring with unit, of characteristic different from 2.*

(1) *If $\mathbf{B_2}(A)$ has a positive answer, then $\mathbf{H_2}(\mathbf{A})$ has a positive answer.*
(2) *Suppose that $2 \in A$ is invertible or $A/4A \simeq \mathbb{Z}/4\mathbb{Z}$. If $\mathbf{H_2}(A)$ has a positive answer, then $\mathbf{H_2}(\mathbf{A})$ has a positive answer.*

Proof. For (1), it is easy to check that a sequence $(x_k)_{k=1}^N$ in A with terms of the form $x_k^2 = (k+f)^2 + g$ for fixed $f, g \in A$ is also a sequence with constant second difference equal to 2.

For (2), let $(x_k)_{k=1}^N$ be a sequence in A with constant second difference equal to 2. Then we have $x_{k-2}^2 - 2x_{k-1}^2 + x_k^2 = 2$ for $k = 3, ..., N$. The sequence of second partial sums of this last expression gives $(x_1^2 - x_2^2)(k-2) - x_2^2 + x_k^2 = (k-2)(k-1)$; hence $x_k^2 = k^2 + (x_2^2 - x_1^2 - 3)k + (2 + 2x_1^2 - x_2^2)$.

If 2 is invertible we take $f = (x_2^2 - x_1^2 - 3)/2, g = (2 + 2x_1^2 - x_2^2) - f^2$ and the result follows. Otherwise, if $A/4A \simeq \mathbb{Z}/4\mathbb{Z}$, then $A/2A \simeq \mathbb{Z}/2\mathbb{Z}$ and the equation $(x_1^2 - x_2^2) - (x_2^2 - x_3^2) = 2$ seen modulo $4A$ easily gives $x_1^2 - x_2^2 = 1$ or $3 \mod 4A$; hence $x_1^2 - x_2^2 \notin 2A$. Therefore $(x_2^2 - x_1^2 - 3) \in 2A$ and we can take f, g as before. □

References

1. J. Browkin and J. Brzeziński, *On sequences of squares with constant second differences*, Canad. Math. Bull. **49-4**, 481-491 (2006). MR2269761 (2007h:11136)
2. D. A. Buell, *Integer squares with constant second difference*, Mathematics of Computation **49**, no. 180, 635-644 (1987). MR906196 (88j:11090)
3. M. Davis, *Hilbert's tenth problem is unsolvable*, American Mathematical Monthly **80**, 233-269 (1973). MR0317916 (47:6465)
4. D. Hensley, *Sequences of squares with second difference of two and a problem of logic*, unpublished.
5. L. Lipshitz, *Quadratic forms, the five squares problem, and diophantine equations*, The collected works of J. Richard Büchi (S. Mac Lane and Dirk Siefkes, eds.), Springer, 677-680, 1990. MR1030043 (92b:01080)
6. Y. Matiyasevic, *Enumerable sets are diophantine*, Dokladii Akademii Nauk SSSR **191** (1970), 279-282; English translation, Soviet Mathematics Doklady **11**, 354-358 (1970).
7. T. Pheidas and X. Vidaux, *Extensions of Büchi's problem: Questions of decidability for addition and n-th powers*, Fundamenta Mathmaticae **185**, 171-194 (2005). MR2163109 (2006f:03064)
8. T. Pheidas and X. Vidaux, *The analogue of Büchi's problem for rational functions*, Journal of the London Mathematical Society **74-3**, 545-565 (2006). MR2286432 (2007k:03097)
9. T. Pheidas and X. Vidaux, *Errata: The analogue of Büchi's problem for rational functions*, submitted to the Journal of the London Mathematical Society.
10. T. Pheidas and X. Vidaux, *The analogue of Büchi's problem for cubes in rings of polynomials*, Pacific Journal of Mathematics **238-2**, 349-366 (2008). MR2442997 (2009g:03059)
11. R. G. E. Pinch, *Squares in quadratic progression*, Mathematics of Computation **60-202**, 841-845 (1993). MR1181330 (93h:11029)
12. P. Vojta, *Diagonal quadratic forms and Hilbert's tenth problem*, Contemporary Mathematics, 270, 261-274, Amer. Math. Soc., Providence, RI, 2000. MR1802018 (2001k:11260)

Departamento de Matemática, Facultad de Ciencias Físicas y Matemáticas, Universidad de Concepción, Concepción, Chile

E-mail address: hpasten@gmail.com