Canad. Math. Bull. Vol. **62** (4), 2019 pp. 876–885
http://dx.doi.org/10.4153/S0008439519000225
© Canadian Mathematical Society 2019

Büchi's Problem in Modular Arithmetic for Arbitrary Quadratic Polynomials

Pablo Sáez, Xavier Vidaux, and Maxim Vsemirnov

Abstract. Given a prime $p \geqslant 5$ and an integer $s \geqslant 1$, we show that there exists an integer M such that for *any* quadratic polynomial f with coefficients in the ring of integers modulo p^s, such that f is not a square, if a sequence $(f(1),\dots,f(N))$ is a sequence of squares, then N is at most M. We also provide some explicit formulas for the optimal M.

1 Introduction

We are interested in the following question.

Question 1.1 Given an integer $m \geq 3$ and a quadratic polynomial $f(x) = f_2x^2 + f_1x + f_0$ over $\mathbb{Z}$, consider the sequence $B_f^N = (f(1),\dots,f(N))$ modulo m. How long can this sequence be if every element of it is a square modulo m, but f itself is not a square modulo m?

The same question can be considered for any commutative ring R with a unit, instead of a quotient of $\mathbb{Z}$. For $R = \mathbb{Z}$, it was first asked by R. Büchi in the early seventies, and was motivated by a decision problem in logic [Lip90, Maz94].

In the case of modular arithmetic, Question 1.1 was first addressed by D. Hensley (unpublished). He showed that in the particular case where m is an odd prime number and $f(x)$ is of the form $(x-v)^2 - a$, N is strictly less than m; nevertheless he does not give any explicit formula for the largest possible N as v and a vary. We dealt with the case where, for an odd given m, f_2 is invertible modulo m [SVV15]. (See Theorem 2.3 for the case of prime powers and [SVV15, §5] for general m.) In the present paper, we solve the problem for any given prime power and any f by reducing it to the case where f_2 is invertible; see Theorem 2.2.

To give a taste of our main result, without introducing too many technicalities, here we state a corollary.

Theorem 1.2 *Let p be a prime ≥ 3. Assume that g_2 is a non-zero square modulo p, s and $t_2 < s$ are positive even integers, and $f_2 = p^{t_2}g_2$. As f varies within the set of non-square quadratic polynomials with this restriction on f_2, the largest possible N such that*

Received by the editors September 23, 2017; revised April 22, 2019.

Published online on Cambridge Core August 30, 2019.

All three authors were partially supported by the grants "Fondecyt research projects 1130134 and 1170315, Chile" to author X. V., from Conicyt. Author M. V. was partially supported by the government of the Russian Federation (grant 14.Z50.31.0030).

AMS subject classification: **11B50,** 11B83.

Keywords: Büchi sequence, Hensley sequence.

each of $f(1),\dots,f(N)$ is a square modulo p^s is $p^{\frac{s-t_2}{2}}-1$, i.e., *there are sequences of this length, and no longer ones.*

Let us give a concrete example. For any odd prime p, modulo p^4, the polynomial $f(x)=p^2x^2+p^3$ is not the square of a polynomial, because p^3 is not a square; but by Hensel's lemma, it is easy to see that $f(k)$ is a square modulo p^4 for $k=1,\dots,p-1$, so the length $p^{\frac{4-2}{2}}-1=p-1$ is reached. Note that $f(0)$ and $f(p)$ are not squares modulo p^4.

Though many analogous results exist in the literature over different type of rings R, they always assume that the polynomial f is monic, with just one exception: Natalia Garcia-Fritz [Ga17, Theorem 1.6, Corollary 1.7 and the comments that follow] did not put restrictions on f_2 (unconditionally if R is a function field of a curve over $\mathbb{C}$, and assuming the Bombieri–Lang conjecture when $R=\mathbb{Q}$). There is some literature on sequences of squares whose second difference is an arbitrary element of R, which corresponds essentially to considering a quadratic f with an arbitrary dominant coefficient. Symmetric sequences of that kind were considered by Allison [All86], Bremner [Bre03], Browkin and Brzeziński [BB06], and Gonzalez-Jimenez and Xarles [GoX11].

Analogues of Question 1.1 have been considered for most classical rings (but in the case of number fields, under some well-known conjectures, like Bombieri–Lang for surfaces, or some version of ABC). Relevant results in positive characteristic can be found in [Pa11] (the analogue of Büchi's problem for any power over fields with a prime number of elements), and in [PaW15] (over rings of functions) that generalized previous results in [PhV06, PhV10, ShV10, AW11, AHW13]. For a general survey on Büchi's problem and its extensions to other structures and higher powers, see [PaPhV10].

2 Preliminaries and Main Result

If n is an integer, $[n]_m$ will denote its residue class modulo m (we use the bracket notation for polynomials and for sequences as well), and if p is a prime, $\operatorname{ord}_p n$ will stand for the usual order at p of n, with the convention $\operatorname{ord}_p(0)=\infty$, so that for every integer x we have $\operatorname{ord}_p x<\infty$ if and only if $x\neq 0$.

Henceforth, we will only consider sequences B_f^N over $\mathbb{Z}$ that satisfy the two following conditions for some odd integer $m\geq 3$.

(C1) $f(1),\dots,f(N)$ are squares modulo m.
(C2) f is not the square of a polynomial modulo m.

Following [SVV15], sequences B_f^N satisfying (C1) are called *f-Büchi sequences modulo m*, and they are called *non-trivial* if (C2) is also satisfied (we can just say "Büchi" instead of "f-Büchi" when it is clear what f is). We should immediately point out that in [SVV15] we considered f-Büchi sequences as trivial when f is the square of a polynomial of degree at most 1. But indeed, when f_2 is invertible, this makes no difference with condition (C2), as shown by the following proposition, which will be proved at the beginning of the next section.

Proposition 2.1 *Let p be an odd prime and s be a positive integer. Let $f = f_2X^2 + f_1X + f_0 \in \mathbb{Z}[X]$. The following statements are equivalent.*

(i) *The polynomial f is the square of a polynomial modulo p^s.*

(ii) *Either $\operatorname{ord}_p f_0 < \min\{\operatorname{ord}_p f_1, \operatorname{ord}_p f_2\}$ and $[f_0]_{p^s}$ is a square, or f is the square of a polynomial modulo p^s whose degree is at most one.*

For odd $m \geq 3$, let us write $\mathrm{ml}(m, f_2, f_1)$ for

$$\max_{f_0}\left\{N : [B_f^N]_m \text{ is a non-trivial Büchi sequence, where } f = f_2X^2 + f_1X + f_0\right\},$$

(with the convention $\mathrm{ml}(m, f_2, f_1) = 0$ if all the sequences in the set are trivial), and $\mathrm{opt}(m, f_2, f_1) = \mathrm{ml}(m, f_2, f_1) + 1$. Also, we will write

$$\mathrm{ml}(m, f_2) = \max_{f_1} \mathrm{ml}(m, f_2, f_1) \quad \text{and} \quad \mathrm{opt}(m, f_2) = \mathrm{ml}(m, f_2) + 1.$$

Note that when $m = p$ is prime, we trivially have

$$\mathrm{ml}(p, 0) = \max_{f_1} \mathrm{ml}(p, 0, f_1) = \max\left\{\mathrm{ml}(p, 0, f_1) : [f_1]_p \neq [0]_p\right\}.$$

Here "ml" stands for "maximal length" and "opt" stands for "optimal bound". The reason to use both concepts is that the proofs are done in terms of maximal lengths but the formulas that we need from [SVV15] are nicer in terms of the optimal bound (the reader will see the point in Theorem 2.3).

We can now state our main theorem.

Theorem 2.2 *Let p be a prime ≥ 3 and s be a positive integer. Let $f_2 \in \mathbb{Z}$, with $f_2 \notin p^s\mathbb{Z}$ unless $f_2 = 0$. Write $t_2 = \operatorname{ord}_p f_2$ and let g_2 be such that $f_2 = p^{t_2} g_2$ when $f_2 \neq 0$, and $g_2 = 0$ otherwise. Assume $t_2 \neq 0$. We have*

$$\mathrm{opt}(p^s, f_2) = \begin{cases} \mathrm{opt}(p, 0) & \text{if } t_2 \text{ is odd or } t_2 = \infty, \\ \max\{\mathrm{opt}(p, 0), \mathrm{opt}(p^{s-t_2}, g_2)\} & \text{if } t_2 \text{ is even.} \end{cases}$$

In this paper, we deal only with the prime power modulus. The case of a general modulus m can be reduced to the case of powers of primes following the strategy described in [SVV15, §5.1]. Any Büchi sequence modulo $m = p_1^{s_1} \cdots p_k^{s_k}$ can be glued from Büchi sequences modulo the $p_i^{s_i}$ using the Chinese Remainder Theorem. The only subtle point to take care of is that one must check that the resulting sequence modulo m is non-trivial, so there are various cases to consider, which result in an elementary but cumbersome analysis; we leave the details to the reader.

While Theorem 2.2 is a natural extension of what we did in our previous work, it was not clear from the beginning what the right statement should be (for example, we were surprised when we discovered that the concept of *triviality* had to be kept unchanged). We have tried to write the proof in the most uniformly possible way, instead of doing the obvious case-by-case analysis.

In order to have a global picture of the situation, and for later references, we summarize in a single theorem what we knew in the case where f_2 is invertible. Given $\alpha \in \mathbb{Z}$ not divisible by p, we defined $\mathrm{ml}(m, \alpha)$ as

$$\max_{a,v}\left\{N : [B_f^N]_m \text{ is an } f\text{-Büchi sequence, where } f = \alpha(X + v)^2 + a \text{ and } a \neq 0\right\},$$

https://doi.org/10.4153/S0008439519000225 Published online by Cambridge University Press

and $\operatorname{opt}(m,\alpha) = \operatorname{ml}(m,\alpha) + 1$ [SVV15]. Note that when f_2 is invertible modulo an odd $m \geq 3$, then every polynomial $f(X) = f_2X^2 + f_1X + f_0$ can be written in a unique way in the form $\alpha(X+v)^2 + a$ modulo m, so the notation in [SVV15] is compatible with the present one.

Theorem 2.3 ([SVV15, Theorems 1.7, 1.8, Lemma 2.13]) *Let p be an odd prime number, and let $s \geq 1$ and f_2 be integers. Assume that $[f_2]_{p^s}$ is invertible.*

(i) *If $[f_2]_{p^s}$ is a non-square and $p \geq 5$, then* $\operatorname{opt}(p^s, f_2) = \operatorname{opt}(p, n) < \infty$, *where n is any quadratic non-residue modulo p.*
(ii) *If $[f_2]_{p^s}$ is a non-zero square and $s = 2r$ is even, then* $\operatorname{opt}(p^s, f_2) = p^r$.
(iii) *If $[f_2]_{p^s}$ is a non-zero square and $s = 2r+1$ is odd, then* $\operatorname{opt}(p^s, f_2) = \operatorname{opt}(p,1)p^r < \infty$.
(iv) *We have* $\operatorname{opt}(p,0) \leq \frac{p+3}{2}$.
(v) *For any $k \in \mathbb{Z}$, we have* $\operatorname{opt}(3, 2+3k) = \infty$.
(vi) *For any $s \geq 2$ and $k \in \mathbb{Z}$, we have* $\operatorname{opt}(3^s, 2+3k) = 5$.

We get Theorem 1.2 by first applying Theorem 2.2 and then Theorem 2.3 items (ii) and (iv). For other cases, it is clear how similar corollaries can be obtained.

3 Reduction to the Case When $[f_2]_{p^s}$ Is Invertible or Is $[0]_{p^s}$

We will frequently use the following well-known fact.

Lemma 3.1 *Let p be an odd prime number. If $y \in \mathbb{Z}$ is a non-zero square modulo p^t for some $t \geq 1$, then y is a square modulo p^s for any $s \geq 1$.*

Proof of Proposition 2.1 We first prove that (ii) implies (i). Assume

$$\operatorname{ord}_p f_0 < \min\{\operatorname{ord}_p f_1, \operatorname{ord}_p f_2\}$$

and $[f_0]_{p^s}$ is a square. If f is identically 0 modulo p^s, then the claim is trivial, so we can assume that f_0 is not 0 modulo p^s. We have

$$f \equiv (p^r g_0)^2 + p^{2r+1}Xg \equiv (p^r g_0)^2(1 + pXh) \pmod{p^s}$$

for some $g \in \mathbb{Z}[X]$, $g_0 \in \mathbb{Z}$ not divisible by p, and $h \in \mathbb{Z}[X]$ such that $g_0^2 h \equiv g \pmod{p^s}$. The Taylor series modulo p^s of the square root of $1 + pXh$ is actually a polynomial, since denominators are powers of 2 and numerators have increasing order at p.

We now prove that (i) implies (ii). Assume $s \geq 2$ (indeed, for $s = 1$, the claim is trivial as $\mathbb{F}_p$ is an integral domain). Let $\varphi \in \mathbb{Z}[X]$ be such that $[f]_{p^s} = [\varphi^2]_{p^s}$. We can assume $[\varphi]_{p^s} \neq [0]_{p^s}$. Let u be the largest integer such that $\varphi = p^u g$ and $g \in \mathbb{Z}[X]$, so that $[g]_p \neq [0]_p$. We have $f \equiv \varphi^2 \equiv p^{2u}g^2 \pmod{p^s}$. If $2u \geq s$, there is nothing to prove, so we can assume $2u < s$, hence $2u + 1 \leq s$. Let $\widetilde{f} = \widetilde{f}_0 + \widetilde{f}_1 X + \widetilde{f}_2 X^2 \in \mathbb{Z}[X]$ be such that $p^{2u}\widetilde{f} = f$ and $[g^2]_p = [\widetilde{f}]_p$. So $[g^2]_p$ has degree at most 2, and since $[g]_p \neq [0]_p$, we deduce that $[g]_p$ has degree at most 1 (because we are now over the integral domain $\mathbb{F}_p$). So we have $g = g_0 + g_1X + p^v hX^2$, for some $v \geq 1$ and some $h \in \mathbb{Z}[X]$. If h is the zero polynomial, then we are done. Otherwise choose v as large

https://doi.org/10.4153/S0008439519000225 Published online by Cambridge University Press

as possible, so that h has at least one coefficient not divisible by p, namely, $[h]_p \neq [0]_p$. We then have $\varphi = p^u(g_0 + g_1X + p^\nu hX^2)$.

Case 1: Assume that p divides g_1, so that p does not divide g_0. We then have $\varphi = p^u g_0 + p^{u+1}k_0$ for some $k_0 \in \mathbb{Z}[X]$, hence $f \equiv \varphi^2 \equiv p^{2u}g_0^2 + p^{2u+1}k_1 \pmod{p^s}$ for some $k_1 \in \mathbb{Z}[X]$, so $2u = \operatorname{ord}_p f_0 < \min\{\operatorname{ord}_p f_1, \operatorname{ord}_p f_2\}$.

Case 2: Assume that p does not divide g_1. Write $\ell = g_0 + g_1X$, so that

$$f \equiv p^{2u}(\ell^2 + p^\nu hX^2(2\ell + p^\nu hX^2)) \pmod{p^s},$$

hence

$$f - p^{2u}\ell^2 \equiv p^{2u+\nu}hX^2(2\ell + p^\nu hX^2) \pmod{p^s}. \tag{3.1}$$

If $2u + \nu \geq s$, then we are done (since ℓ has degree 1). So it remains to consider the case where $2u + \nu < s$, which will turn out to be impossible. Multiplying both sides of (3.1) by

$$(2\ell)^{s-1} - (2\ell)^{s-2}p^\nu hX^2 + \cdots + (-1)^{s-1}(p^\nu hX^2)^{s-1}$$

we obtain

$$\begin{aligned}(f - p^{2u}\ell^2)\big[(2\ell)^{s-1} - (2\ell)^{s-2}p^\nu hX^2 + \cdots\big]&\\ &\equiv p^{2u+\nu}hX^2((2\ell)^s + (-1)^{s-1}(p^\nu hX^2)^s)\\ &\equiv p^{2u+\nu}hX^2(2\ell)^s \pmod{p^s},\end{aligned}$$

since $\nu \geq 1$. Hence we have

$$(\widetilde{f} - \ell^2)\big[(2\ell)^{s-1} - (2\ell)^{s-2}p^\nu hX^2 + \cdots\big] \equiv p^\nu hX^2(2\ell)^s \pmod{p^{\nu+1}}, \tag{3.2}$$

since $s - 2u \geq \nu + 1$. We now compare the coefficients of X^{2+d+s} on both sides, where d is the degree of $[h]_p$. Let $h_d \in \mathbb{Z}$ be the coefficient of h at X^d (so $[h_d]_p$ is the dominant coefficient of $[h]_p$), and let h_0 be the constant term of h. The coefficient of X^{2+d+s} modulo $p^{\nu+1}$ on the left-hand side is the coefficient of $(\widetilde{f} - \ell^2)(2\ell)^{s-2}p^\nu hX^2$ modulo $p^{\nu+1}$ (the terms that are not written in (3.2) will have order at least $2\nu \geq \nu + 1$, and in the term $(\widetilde{f} - \ell^2)(2\ell)^{s-1}$ all monomials have degree at most $s + 1 < 2 + d + s$), which is

$$2p^\nu h_0g_0 \cdot 2^{s-2}g_1^{s-2}p^\nu h_d,$$

(here the term $2p^\nu h_0g_0$ comes from (3.1)). On the other hand, the right-hand side of (3.2) gives $p^\nu h_d2^sg_1^s$, so we have

$$p^\nu \cdot 2h_0g_0 \cdot 2^{s-2}g_1^{s-2}h_d \equiv h_d2^sg_1^s \pmod{p},$$

which is a contradiction, since p divides neither g_1 nor h_d. ■

Note that if any of f_1 or f_2 is invertible modulo p, then the condition

$$\min\{\operatorname{ord}_p f_1, \operatorname{ord}_p f_2\} > \operatorname{ord}_p f_0$$

is never satisfied. We now prove a sequence of lemmas that will imply our main theorem.

Lemma 3.2 *Let p be an odd prime and $s \geq 1$. Let $f(X) = f_2X^2 + f_1X + f_0 \in \mathbb{Z}[X]$. Write $t_i = \operatorname{ord}_p f_i$ for each i. Assume that $\min\{t_1, t_2\} > t_0$ and $[f_0]_{p^s}$ is a non-square. If B_f^N is a Büchi sequence modulo p^s, then $N = 0$.*

https://doi.org/10.4153/S0008439519000225 Published online by Cambridge University Press

Proof Note that $t_0 \neq \infty$. Also note that $t_0 < s$ (because $[f_0]_{p^s}$ is a non-square, so in particular it is not $[0]_{p^s}$). Write $f(X) = p^{t_0} g(X)$, where $g(X) = p^{t_2-t_0} g_2 X^2 + p^{t_1-t_0} g_1 X + g_0$, so that g_0 is invertible modulo p. We assume $N \geq 1$ and will get a contradiction. Let $k, x \in \mathbb{Z}$ be such that $f(1) = x^2 + kp^s$. From the hypothesis of the lemma, we have

$$x^2 + kp^s = f(1) = p^{t_0} g(1) \equiv p^{t_0} g_0 = f_0 \pmod{p^{t_0+1}},$$

hence, recalling that $t_0+1 \leq s$, f_0 is a square modulo p^{t_0+1}. Since g_0 is non-zero modulo p, also f_0 is non-zero modulo p^{t_0+1}. So f_0 is a square modulo p^s by Lemma 3.1, which contradicts our hypothesis on f_0. ■

Lemma 3.3 *Let p be an odd prime and $s \geq 1$. Let $f_1, f_2 \in \mathbb{Z}$. If f_1 is invertible modulo p and f_2 is not invertible modulo p, then*

$$\operatorname{opt}(p^s, f_2, f_1) = \operatorname{opt}(p, 0, f_1).$$

Proof We first prove the "$\leq$" inequality. Let $N \geq 0$ and f_0 be integers. Write $f = f_2X^2 + f_1X + f_0$ and assume that B_f^N is a non-trivial Büchi sequence modulo p^s. Modulo p, since f_2 is not invertible, we have $f \equiv f_1X + f_0$. Write $g = f_1X + f_0$. Since $f(x)$ is a square modulo p^s for each $x = 1, \dots, N$, it is a square modulo p, so B_g^N is a Büchi sequence modulo p. Since f_1 is invertible, B_g^N is a non-trivial Büchi sequence modulo p, hence N is at most $\operatorname{ml}(p, 0, f_1)$.

We now prove the other inequality. Let $h = f_1X + b$ be such that B_h^N is a Büchi sequence of length $N = \operatorname{ml}(p, 0, f_1)$ (note that this is always finite by Theorem 2.3(iv)). Consider

$$f = f_2X^2 + f_1X + b \equiv f_1X + b \pmod{p}.$$

If there is no $0 \pmod{p}$ in the sequence B_h^N, then $f(x)$ is a non-zero square modulo p for any $x \in \{1, \dots, N\}$, hence it is a square modulo p^s by Lemma 3.1. Assume that there is some $x_0 \in \{1, \dots, N\}$ such that $h(x_0)$ is congruent to 0 modulo p, so that b is congruent to $-f_1x_0$ modulo p (there can be at most one such x_0). In that case, consider

$$f = f_2X^2 + f_1X - f_1x_0 - f_2x_0^2 \equiv f_1X + b \pmod{p},$$

so that $f(x_0)$ is actually $0 \in \mathbb{Z}$, hence a square modulo p^s, and as before, when $x \neq x_0$, $f(x)$ is a non-zero square modulo p^s. In both cases, B_f^N is a Büchi sequence modulo p^s.

We now prove that B_f is a non-trivial Büchi sequence modulo p^s. It is enough to prove that $f(N+1)$ is not a square modulo p^s. Indeed, we have $f(N+1) \equiv h(N+1) \pmod{p}$, and the latter is not a square by definition of h, so $f(N+1)$ is not even a square modulo p. ■

Next comes the key lemma for having a uniform proof of Theorem 2.2.

Lemma 3.4 *Let p be an odd prime and $s \geq 1$. Let $f_1, f_2 \in \mathbb{Z}$, with $f_i \notin p^s\mathbb{Z}$ unless $f_i = 0$. Assume that not both f_1 and f_2 are 0. Write $t_1 = \operatorname{ord}_p f_1$ and $t_2 = \operatorname{ord}_p f_2$. For $i \in \{1, 2\}$, let g_i be such that $f_i = p^{t_i} g_i$ (if $f_i = 0$, take $g_i = 0$). Write $m = \min\{t_1, t_2\}$.*

https://doi.org/10.4153/S0008439519000225 Published online by Cambridge University Press

(i) *If m is even, then we have*

$$\operatorname{opt}(p^s, f_2, f_1) = \operatorname{opt}(p^{s-m}, p^{t_2-m}g_2, p^{t_1-m}g_1),$$

where $p^{t_i-m}g_i$ reads as 0 if $f_i = 0$.

(ii) *The sides of the equation in item (i) are infinite if and only if $p = 3$, $s = m + 1$, and $g_2 \in 2 + 3\mathbb{Z}$.*

(iii) *If m is odd, then we have* $\operatorname{opt}(p^s, f_2, f_1) \le 3$.

(iv) *If $t_2 = \infty$ and t_1 is odd, then* $\operatorname{opt}(p^s, 0, f_1) \le 2$.

Proof We first prove items (iii) and (iv), together with the "≤" inequality in item (i). Let $N \ge 0$ and f_0 be integers, and write $t_0 = \operatorname{ord}_p f_0$ and $f_0 = p^{t_0}g_0$ (with $g_0 = 0$ if $f_0 = 0$). Assume that B_f^N is a non-trivial Büchi sequence modulo p^s, where $f = f_2X^2 + f_1X + f_0$. In particular, by Proposition 2.1 the polynomial f is not the square of a linear polynomial modulo p^s, and we have $m \le t_0$, unless $[f_0]_{p^s}$ is a non-square. If $m > t_0$ and $[f_0]_{p^s}$ is a non-square, we have $N = 0$ by Lemma 3.2, so we can assume $m \le t_0$. Write $f = p^m g$, where

$$g = p^{t_2-m}g_2X^2 + p^{t_1-m}g_1X + p^{t_0-m}g_0.$$

We can now complete the proof of (iii). Assume m is odd. In that case, if $[f(n)]_{p^s}$ is a square, then $[g(n)]_p = [0]_p$. If $m = t_1 < t_2$, we have

$$g = p^{t_2-t_1}g_2X^2 + g_1X + p^{t_0-t_1}g_0 \equiv g_1X + p^{t_0-t_1}g_0 \pmod p,$$

hence $g(n)$ can be 0 modulo p for at most one value of n, hence $N \le 1$. If $m = t_2 \le t_1$, we have $g = g_2X^2 + p^{t_1-t_2}g_1X + p^{t_0-t_2}g_0$, so $g(n)$ can be 0 modulo p for at most two values of n, hence $N \le 2$.

We now turn to (i). Assume m is even. Since f is not the square of a linear polynomial modulo p^s, g also is not the square of a linear polynomial modulo p^{s-m}. Moreover, since $t_0 \ge m = \min\{t_2, t_1\}$, we have

$$t_0 - m \ge \min\{t_2 - m, t_1 - m\},$$

hence B_g^N is a non-trivial Büchi sequence modulo p^{s-m} by Proposition 2.1, so we have $N \le \operatorname{ml}(p^{s-m}, p^{t_2-m}g_2, p^{t_1-m}g_1)$.

We now prove "≥" in (i) (so, in particular, we assume that m is even). First note that the claim is trivial when $t_2 = 0$ (which is the case in particular when $s = 1$). Let $g = p^{t_2-m}g_2X^2 + p^{t_1-m}g_1X + b$ be such that B_g^N is a non-trivial Büchi sequence of length $N = \operatorname{ml}(p^{s-m}, p^{t_2-m}g_2, p^{t_1-m}g_1)$ (N can be ∞).

Consider $f = p^m g = p^m(p^{t_2-m}g_2X^2 + p^{t_1-m}g_1X + b)$. For any $x \in \{1, \dots, N\}$, since $g(x)$ is a square modulo p^{s-m} and m is even, also $f(x)$ is a square modulo p^s, so B_f is a Büchi sequence modulo p^s.

We now prove that B_f^N is a non-trivial Büchi sequence modulo p^s. Since B_g^N is a non-trivial Büchi sequence modulo p^{s-m}, g is not the square of a linear polynomial modulo p^{s-m}, hence also, since m is even, $p^m g$ is not the square of a linear polynomial modulo p^s. Moreover, by Proposition 2.1, either $\min\{t_1 - m, t_2 - m\} \le \operatorname{ord}_p b$, in which case $\min\{t_1, t_2\} \le \operatorname{ord}_p p^m b$, or $[b]_{p^{s-m}}$ is not a square, in which case $[p^m b]_{p^s}$ is not a square. So B_f^N is a non-trivial Büchi sequence modulo p^s.

https://doi.org/10.4153/S0008439519000225 Published online by Cambridge University Press

We prove (ii). If $m = t_1 < t_2$, then the right-hand side is finite by Lemma 3.3. Otherwise it is an immediate consequence of Theorem 2.3 applied to modulus p^{s-m} (observe that in this theorem, (v) is the only case where opt is infinite). ■

Corollary 3.5 *Let p be an odd prime and $s \geq 1$. Let $f_1, f_2 \in \mathbb{Z}$, with $f_i \notin p^s\mathbb{Z}$, unless $f_i = 0$. Write $t_i = \operatorname{ord}_p f_i$ and let g_i be such that $f_i = p^{t_i} g_i$ (if $f_i = 0$, take $g_i = 0$). We have*

$$\operatorname{opt}(p^s, f_2, f_1) = \begin{cases} \operatorname{opt}(p^{s-t_2}, g_2, p^{t_1-t_2} g_1) & \text{if } t_2 \leq t_1 \text{ and } t_2 \text{ is even,} \\ \operatorname{opt}(p, 0, g_1) & \text{if } t_2 > t_1 \text{ and } t_1 \text{ is even.} \end{cases}$$

Proof First note that the claim is trivial when $t_2 = 0$. If $t_2 \leq t_1$ and t_2 is even, this is just Lemma 3.4. Assume that $t_2 > t_1$ and t_1 is even. In particular, since $t_2 > t_1$, f_1 cannot be 0. We have

$$\operatorname{opt}(p^s, f_2, f_1) = \operatorname{opt}(p^{s-t_1}, p^{t_2-t_1} g_2, g_1) = \operatorname{opt}(p, 0, g_1)$$

(recalling the convention that $p^{t_2-t_1} g_2 = 0$ if $f_2 = 0$), where the first equality comes from Lemma 3.4, and the second equality comes from Lemma 3.3 (which can be applied because $p^{t_2-t_1} g_2$ is not invertible modulo p, but g_1 is invertible modulo p since $f_1 \neq 0$). ■

Lemma 3.6 *Let p be a prime ≥ 3 and $s \geq 1$. Let $f_2 \in \mathbb{Z}$, with $f_2 \notin p^s\mathbb{Z}$ unless $f_2 = 0$. Write $t_2 = \operatorname{ord}_p f_2 \neq 0$. We have the following.*

(i) *If $t_2 = \infty$, then*

$$\max\{\operatorname{opt}(p^s, f_2, f_1) : \operatorname{ord}_p f_1 < \infty \text{ is even}\} \geq 2,$$

(ii) *If $t_2 < \infty$ is odd, then*

$$\max\{\operatorname{opt}(p^s, f_2, f_1) : \operatorname{ord}_p f_1 < t_2 \text{ and } \operatorname{ord}_p f_1 \text{ is even}\} \geq 3.$$

(iii) *If $t_2 < \infty$ is even, then*

$$\max\{\operatorname{opt}(p^s, f_2, f_1) : \operatorname{ord}_p f_1 \geq t_2, \text{ or } \operatorname{ord}_p f_1 < t_2 \text{ and } \operatorname{ord}_p f_1 \text{ is even}\} \geq 3.$$

Proof For (i), just note that for any non-zero $b \in \mathbb{Z}$ that is coprime with p, the function $f = b^2 X$ defines a non-trivial Büchi sequence of length ≥ 1. Indeed, if $f \equiv (g_1 X + g_2)^2 \pmod{p^s}$, then $g_1^2 \equiv g_2^2 \equiv 0 \pmod{p^s}$, hence $[g_1]_p = [g_2]_p = 0$, but $2g_1 g_2 \equiv b^2 \pmod{p^s}$, which contradicts the fact that b is coprime with p, and the constant term is 0, hence has order greater than or equal to the order of the other coefficients. We conclude by Proposition 2.1 that it is a non-trivial sequence.

For (ii) and (iii), choose $f = f_2 X^2 + f_1 X + f_0$ with $f_1 = 1 - 3f_2$ and $f_0 = 2f_2 - 1$, so that $f(1) = 0$ and $f(2) = 1$ (so they are squares modulo any p^s). Since $t_2 \neq 0$, f_2 is divisible by p, hence $\operatorname{ord}_p(f_1) = 0$ is even and $< t_2$. Moreover, B_f^2 is a non-trivial sequence because, on the one hand, we have $\operatorname{ord}_p(f_0) = 0 \geq \min\{\operatorname{ord}_p f_1, \operatorname{ord}_p f_2\}$, and on the other hand, it is not the square of a linear polynomial modulo p^s. If it were, then we would have

$$f = f_2 X^2 + (1 - 3f_2)X + 2f_2 - 1 \equiv g_1^2 X^2 + 2g_1 g_2 X + g_2^2 \pmod{p^s},$$

https://doi.org/10.4153/S0008439519000225 Published online by Cambridge University Press

which is impossible, since modulo p the right-hand side is a constant polynomial (because p divides f_2, hence also g_1), while the left-hand side is a non-constant polynomial, since $1-3f_2$ is not divisible by p. ∎

We conclude this work with the proof of our main theorem.

Proof of Theorem 2.2 If $f_2 = 0$, then we have (recalling the convention $\operatorname{opt}(p^s,0,0)=1$; see the introduction)

$$\begin{aligned}\operatorname{opt}(p^s,f_2) &= \max\{\operatorname{opt}(p^s,0,f_1) : f_1\in\mathbb{Z}\}\\ &= \max\big(\{\operatorname{opt}(p^s,0,f_1) : \operatorname{ord}_p f_1<\infty \text{ is even}\}\\ &\qquad\qquad \cup\{\operatorname{opt}(p^s,0,f_1) : \operatorname{ord}_p f_1<\infty \text{ is odd}\}\big)\\ &= \max\{\operatorname{opt}(p^s,0,f_1) : \operatorname{ord}_p f_1<\infty \text{ is even}\}\\ &= \max\{\operatorname{opt}(p,0,g_1) : g_1 \text{ is invertible modulo } p\}\\ &= \operatorname{opt}(p,0),\end{aligned}$$

where the second and third equalities come from Lemma 3.6(i) and Lemma 3.4, and the fourth equality comes from Corollary 3.5.

If $t_2<\infty$ is odd, then we have (using again Lemmas 3.6, 3.4, and Corollary 3.5)

$$\begin{aligned}\operatorname{opt}(p^s,f_2) &= \max\{\operatorname{opt}(p^s,f_2,f_1) : f_1\in\mathbb{Z}\}\\ &= \max\big(\{\operatorname{opt}(p^s,f_2,f_1) : \operatorname{ord}_p f_1<t_2 \text{ and } \operatorname{ord}_p f_1 \text{ is even}\}\\ &\qquad\qquad \cup\{\operatorname{opt}(p^s,f_2,f_1) : \operatorname{ord}_p f_1\geq t_2 \text{ or } \operatorname{ord}_p f_1 \text{ is odd}\}\big)\\ &= \max\{\operatorname{opt}(p^s,f_2,f_1) : \operatorname{ord}_p f_1<t_2 \text{ and } \operatorname{ord}_p f_1 \text{ is even}\}\\ &= \max\{\operatorname{opt}(p,0,g_1) : g_1 \text{ is invertible modulo } p\}\\ &= \operatorname{opt}(p,0).\end{aligned}$$

If $0\neq t_2<\infty$ is even, then we have

$$\begin{aligned}\operatorname{opt}(p^s,f_2) &= \max\{\operatorname{opt}(p^s,f_2,f_1) : f_1\in\mathbb{Z}\}\\ &= \max\Big\{\operatorname{opt}(p^s,f_2,f_1) : \operatorname{ord}_p f_1\geq t_2,\\ &\qquad\qquad \text{or } \operatorname{ord}_p f_1<t_2 \text{ and } \operatorname{ord}_p f_1 \text{ is even},\\ &\qquad\qquad \text{or } \operatorname{ord}_p f_1<t_2 \text{ and } \operatorname{ord}_p f_1 \text{ is odd}\Big\}\\ &= \max\big(\{\operatorname{opt}(p^{s-t_2},g_2,p^{t_1-t_2}g_1) : [g_1]_p\neq[0]_p\}\\ &\qquad\qquad \cup\{\operatorname{opt}(p,0,g_1) : [g_1]_p\neq[0]_p\}\big)\\ &= \max\{\operatorname{opt}(p^{s-t_2},g_2),\operatorname{opt}(p,0)\}.\end{aligned}$$ ∎

https://doi.org/10.4153/S0008439519000225 Published online by Cambridge University Press

References

[All86] D. Allison, *On square values of quadratics*. Math. Proc. Cambridge Philos. Soc. 99(1986), no. 3, 381–383. https://doi.org/10.1017/S030500410006432X

[AHW13] T. T. H. An, H.-L. Huang, and J. T.-Z. Wang, *Generalized Büchi's problem for algebraic functions and meromorphic functions*. Math. Z. 273(2013), no. 1–2, 95–122. https://doi.org/10.1007/s00209-012-0997-9

[AW11] T. T. H. An and J. T. Y. Wang, *Hensley's problem for complex and non-Archimedean meromorphic functions*. J. Math. Anal. Appl. 381(2011), no. 2, 661–677. https://doi.org/10.1016/j.jmaa.2011.03.025

[Bre03] A. Bremner, *On square values of quadratics*. Acta Arith. 108(2003), 95–111. https://doi.org/10.4064/aa108-2-1

[BB06] J. Browkin and J. Brzeziński, *On sequences of squares with constant second differences*. Canad. Math. Bull. 49-4(2006), 481–491. https://doi.org/10.4153/CMB-2006-047-9

[Ga17] N. Garcia-Fritz, *Quadratic sequences of powers and Mohanty's conjecture*. Int. J. Number Theory 14(2018), no. 2, 479–507. https://doi.org/10.1142/S1793042118500306

[GoX11] E. González-Jiménez and X. Xarles, *On symmetric square values of quadratic polynomials*. Acta Arith. 149(2011), no. 2, 145–159. https://doi.org/10.4064/aa149-2-4

[Lip90] L. Lipshitz, *Quadratic forms, the five square problem, and diophantine equations*, The collected works of J. Richard Büchi, eds. MacLane S. and Siefkes Dirk, Springer, 1990, pp. 677–680.

[Maz94] B. Mazur, *Questions of decidability and undecidability in number theory*. J. Symbolic Logic 59-2(1994), 353–371. https://doi.org/10.2307/2275395

[Pa11] H. Pasten, *Büchi's problem in any power for finite fields*. Acta Arith. 149-1(2011), 57–63. https://doi.org/10.4064/aa149-1-4

[PaPhV10] H. Pasten, T. Pheidas, and X. Vidaux, *A survey on Büchi's problem: new presentations and open problems*. Zapiski POMI 377(2010), 111–140. https://doi.org/10.1007/s10958-010-0181-x

[PaW15] H. Pasten and J. T.-Y. Wang, *Extensions of Büchi's higher powers problem to positive characteristic*. Int. Math. Res. Not. IMRN 2015 no. 11, 3263–3297.

[PhV06] T. Pheidas and X. Vidaux, *The analogue of Büchi's problem for rational functions*. J. London Math. Soc. 74(2006), no. 3, 545–565. https://doi.org/10.1112/S0024610706023283

[PhV10] T. Pheidas and X. Vidaux, *Corrigendum: The analogue of Büchi's problem for rational functions*. J. London Math. Soc. 82(2010), 273–278. https://doi.org/10.1112/jlms/jdq002

[SVV15] P. Sáez, X. Vidaux, and M. Vsemirnov, *Optimal bounds for Büchi's problem in modular arithmetic*. J. Number Theory 149(2015), 368–403. https://doi.org/10.1016/j.jnt.2014.10.008

[ShV10] A. Shlapentokh and X. Vidaux, *The analogue of Büchi's problem for function fields*. J. Algebra 330(2010), 482–506. https://doi.org/10.1016/j.jalgebra.2011.01.008

[Vo00] P. Vojta, *Diagonal quadratic forms and Hilbert's Tenth Problem*. In: *Hilbert's tenth problem: relations with arithmetic and algebraic geometry*, Contemp. Math., 270, American Mathematical Society, Providence, RI, 2000, pp. 261–274. https://doi.org/10.1090/conm/270/04378

Concepción, Chile
e-mail: pablosaezphd@gmail.com

Universidad de Concepción, Facultad de Ciencias Físicas y Matemáticas, Departamento de Matemática, Casilla 160 C, Concepción, Chile
e-mail: xvidaux@udec.cl

St. Petersburg Department of V.A.Steklov Institute of Mathematics, 27 Fontanka, St. Petersburg, 191023, Russia and St. Petersburg State University, Department of Mathematics and Mechanics, 28 University prospekt, St. Petersburg, 198504, Russia
e-mail: vsemir@pdmi.ras.ru

https://doi.org/10.4153/S0008439519000225 Published online by Cambridge University Press