A short state of the art of Büchi's problem

Xavier Vidaux
Universidad de Concepción
Séminaire de Structures Algébraiques Ordonnées n86 - 2010-2011

Abstract

Büchi's problem is a general problem of arithmetical flavor that can be asked in any ring with unit A, and that, if solved positively, can be used as a tool to obtain very strong undecidability results, as it (often) implies that the problem (or some slight modification of it) of representation of an arbitrary vector of elements of A by a system of diagonal forms (quadratic, or of any fixed order) over the prime subring of A is undecidable when the positive existential theory of the ring A is known to be undecidable. This was the original motivation of J. R. Büchi in the 70's, but since then Büchi's problem has been found to be relevant in various other contexts. Firstly, in 1999, P. Vojta found a connexion with Bombieri-Lang's conjecture on the locus of rational points on varieties of general type. Secondly, new applications to logic have been found recently, giving rise to quite general undecidability results, through existential definitions which are uniform among rings of different characteristics. Thirdly, H. Pasten recently found some connection with a special case of a conjecture by Vojta. We will make some of these statements a bit more precise in the text, but for an extensive discussion and bibliography on Büchi's problem, we refer to the survey [22], our objective being to make an updated and somewhat compact presentation of the state of the art on Büchi's problem and some problems in logic that are intrinsically linked to it. For that reason, we will try to concentrate on the qualitative aspects of the existing results.

1 Büchi's Problem

In any ring, define the k-th difference of a sequence $x = (x_n)_n$ (finite or infinite) by induction as

$$\Delta(x) = \Delta^{(1)}(x) = (x_{n+1} - x_n)_n, \qquad \text{and} \qquad \Delta^{(k)}(x) = \Delta(\Delta^{(k-1)}(x)).$$

If the sequence x has a finite length M, then the k-th difference is defined only for $k \leq M - 1$. We will assume from now on that all rings are commutative with unit. Since for any given x the k-th difference of the sequence $((x+n)^k)_n$ of consecutive powers is the constant sequence $(k!)_n$, it is natural to ask whether we can characterize somehow sequences of consecutive powers using k-th differences. We will call a *k-Büchi sequence* any sequence whose k-th difference of k-th powers is the constant sequence $(k!)$. Note that the sequence of squares (in the ring of integers $\mathbb{Z}$) of the sequence $(0, 7, 10)$ is $(0, 49, 100)$, hence is not of the form $(x^2, (x+1)^2, (x+2)^2)$, though it has second difference the one term sequence $(2) = (2!)$. Similarly, the sequence $(6, 23, 32, 39)$ has its second difference of squares constant equal to $(2, 2)$. Therefore, there are 2-Büchi sequences in $\mathbb{Z}$ of length 3 and 4 respectively which are not *trivial*, in the sense that their sequence of squares does not consist of consecutive squares. J.R. Büchi conjectured (see [13]) that there exist no non-trivial 2-Büchi sequence of length ≥ 5 over the integers (it is still a conjecture).

Key words and phrases: Büchi, Hensley, differences of powers, Hilbert's tenth problem.

Many thanks to M. Castillo, H. Pasten, T. Pheidas and P. Sáez for their comments and corrections on the first version of this survey.

We say that a sequence $(x_n)_n$ over a ring A of characteristic 0 is *a trivial k-Büchi sequence* if the sequence (x_n^k) consists of consecutive k-th powers, or more precisely, if there exists x in the ring such that $x_n^k = (x+n)^k$ for each n. In the case that A is a ring of functions, sequences of constants of the ring should also be considered as trivial. If A has positive characteristic p and $k = 2$, *trivial Büchi sequences* are those sequences $(x_n)_n$ for which there exist $x \in A$ and s a positive integer such that $x_n^2 = (x+n)^{p^s+1}$ for each n (with the same remark as in characteristic 0 when A is a ring of functions). The point here is that all trivial Büchi sequences are Büchi sequences that can be of infinite length, so that the following problem does not have trivially a negative answer:

Büchi's problem for k-th powers over a ring A, denoted $\mathbf{B^k}(A)$, is the problem to know whether or not there exists an integer M such that all k-Büchi sequences of length at least M are trivial.

Note that in positive characteristic p, we want an M that is at most p, as the condition for a sequence (x_n) to be a Büchi sequence implies that for each n we have $x_n = x_{n+p}$ (this can be seen immediately by writing each x_n as a function of x_1 and x_2).

Büchi's problem for $k \neq 2$ was proposed by Pheidas and the author in [24], and a first example of a ring where Büchi's problem has a positive answer for $k \neq 2$ was solved in [27] (Büchi's problem for cubes in polynomial rings of characteristic zero).

To end this section, we should mention that though Büchi's problem for squares was very little known to the mathematical community until it was publicized by L. Lipshitz in [13] and B. Mazur [14], and then conjecturally solved by P. Vojta in [36], a variant of it[1] had been studied since the early eighties by some mathematicians and computer scientists (see [3]).

2 The original motivation from Logic

Suppose that Büchi's problem for squares is solved over $\mathbb{Z}$ positively ("an M exists"). Büchi showed that the relation $y = x^2$ is positively existentially definable over the language $\mathcal{L}^2 = \{0, 1, +, P^2\}$, where P^2 is a symbol of unary relation interpreted by the set of squares in $\mathbb{Z}$. Indeed, the $\mathcal{L}^2$-formula $\varphi(r, s)$

$$\exists u_1 \cdots \exists u_M \left(\bigwedge_{i=1}^{M} P^2(u_i) \right) \wedge \left(\bigwedge_{i=1}^{M-2} u_{i+2} - 2u_{i+1} + u_i = 2 \right) \wedge s = u_1 \wedge 2r + 1 = u_2 - u_1$$

is satisfied in $\mathbb{Z}$ if and only if $s = r^2$, as easily verified. It is not too hard to generalize this idea to any power: if Büchi's problem for k-th powers is solved over $\mathbb{Z}$ positively, then the relation $y = x^k$ is positively existentially definable over the language $\mathcal{L}^k = \{0, 1, +, P^k\}$, where P^k is a symbol of unary relation interpreted by the set of k-th powers in $\mathbb{Z}$ (see [22] for a proof).

From that, it is standard to define existentially the multiplication. Since Hilbert's Tenth Problem is unsolvable (i. e. the positive existential theory of the ring $\mathbb{Z}$ is undecidable) as a consequence of DMPR Theorem (see for example [6]), we would then be able to deduce that the positive existential theory of $\mathbb{Z}$ as an $\mathcal{L}^k$-structure is undecidable as well (this is also a standard short argument). So, it would be proven that there is no algorithm to decide whether or not a system of equations of the form

$$\sum_{i=1}^{r} a_{i,j} x_i^k + \sum_{i=1}^{s} b_{i,j} y_i = c_j, \qquad j = 0, \ldots, n,$$

where $n, r, s \geq 0$ and the coefficients $a_{i,j}$, $b_{i,j}$ and c_j are arbitrary integers, has a solution over the integers. Since for any k there exists a natural number $v(k)$ such that every integer can be written as sums and differences of at most $v(k)$ k-th powers ("easier Waring's Problem"), we can get rid of the terms of the form $b_{i,j} y_j$ in the system above (the new system will have much more variables). Therefore, it would also follow that there is no algorithm to decide whether or not a system of equations of the

[1] asking for the difference of squares to be constant equal to (d), where d is not necessarily 2

form

$$\sum_{i=1}^{r} a_{i,j} x_i^k = c_j, \qquad j = 0, \dots, n,$$

where $n, r \geq 0$ and the coefficients $a_{i,j}$ and c are arbitrary integers, has a solution over the integers. The latter is referred to as the *problem of simultaneous representation by diagonal forms of order* k. For rings different from $\mathbb{Z}$, there are analogous logical consequences to solving positively Büchi's problem (as long as some analogue of Hilbert's Tenth Problem for that ring is unsolvable). We refer to [22] for a more detailed discussion on that subject.

3 Hensley's Problem

The following problem, denoted $\mathbf{H^k}(A)$, was proposed by D. Hensley [9] when $k = 2$ and for any power by Pasten in [17].[2] In any ring A, let us call a k-Hensley sequence any sequence of the form $((x+n)^k + a)_n$. The problem $\mathbf{H^k}(A)$ asks whether or not there exists an integer M such that all k-Hensley sequences of k-th powers of length $\geq M$ satisfy $a = 0$. Indeed, if $\mathbf{B^k}(A)$ has a positive answer then it is easy to see that $\mathbf{H^k}(A)$ also has a positive answer. The reciprocal should be false in general, but is true when $k = 2$ under slight conditions on the ring (for example, if $A/4A$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ or if 2 is invertible, see [17]). In practice, it sometimes turns out to be easier to solve Hensley's problem than Büchi's problem, but we need solving the latter one in order to obtain the consequence in Logic described in the previous section. As for Büchi's problem, we may add some natural hypothesis to the problem when A is a ring of functions (for example requiring that x is not a constant function) or if it has positive characteristic.

4 A *florilège* of results

For which rings A and which integers k do we know the answer to $\mathbf{B^k}(A)$ or $\mathbf{H^k}(A)$?

- For rings A that have *too many* k-th powers, $\mathbf{B^k}(A)$ has trivially a negative answer (e. g. the field $\mathbb{C}$ of complex numbers, or the ring of all real algebraic integers - consider for example $(\sqrt{n^2+1})_{n \geq 1}$).

- $\mathbf{B^k}(\mathbb{Z}_p)$ and $\mathbf{B^k}(\mathbb{Q}_p)$ have both a negative answer for any k (here $\mathbb{Z}_p$ and $\mathbb{Q}_p$ are respectively the ring of p-adic integers and the field of p-adic numbers). This was proved by J. Browkin for $k = 2$ in [2] and generalized to higher powers by M. Castillo in her Master thesis [5]. Indeed Browkin proves that, though there are arbitrarily long non trivial 2-Büchi sequences in $\mathbb{Z}_p$, there are no such sequences of infinite length (the situation being quite different in $\mathbb{Q}_p$, as there are non trivial 2-Büchi sequences of infinite length, see [2] for $k = 2$, and [5] for higher powers). Castillo also generalizes the latter in some cases to higher powers[3] (see [4]). No other example of this kind is known. Could this phenomenon have some interesting consequence in Logic? Note that we do no know any ring A such that $\mathbf{B^2}(A)$ has a positive answer and $\mathbf{B^2}(S^{-1}A)$ has a negative answer, where $S^{-1}A$ denotes here any localization of A: when we can solve Büchi's problem for a ring, the method always can be adapted to its total ring of fractions. The result of Browkin indicates that this phenomenon could be related to the methods used and the rings that we have considered so far.

- For every k, $\mathbf{B^k}(\mathbb{F}_p)$ has a positive answer for infinitely many primes p (Hensley [9] for $k = 2$ and Pasten [18] for higher powers). No consequence in Logic has been derived so far from these results.

[2] for most results by Pasten, see also [15] and [16] for a more extensive presentation and for some texts in Spanish language

[3] for infinitely many pairs (k, p).

- $\mathbf{B^2}(\mathcal{M})$ has a positive answer, where $\mathcal{M}$ is the field of meromorphic functions on the complex plane (Vojta [36]) or on the p-adic complex analogue $\mathbb{C}_p$ (Pasten [19]). Ta Thi Hoai An and Julie Tzu-Yueh Wang generalize these results by showing that $\mathbf{H^k}(\mathcal{M})$ has a positive answer for any k [1] (also in positive characteristic when $k \neq 2$). A strong version of Hensley's problem for any power in polynomial rings of characteristic zero had been previously solved by Pasten [17]. Except for Vojta's result, the general method used comes from the solution to Büchi's problem for squares for rings of rational functions over any field of characteristic 0 or high enough (at least 19), by Pheidas and the author, see [25] and [26]. Note that this is the only known method at the moment that gives results in positive characteristic. In particular, it could be generalized by Shlapentokh and the author to solve Hensley's problem for any power over an arbitrary algebraic function field of characteristic 0, or high enough (depending on the genus only), see [30]. [4]

- For any k, $\mathbf{B^k}(A)$ has a positive answer when A is a function field of a curve over an algebraically closed field of characteristic zero or the field of complex meromorphic functions. Vojta proved it in [36] for $k = 2$. The generalization to any power was obtained recently by Pasten with a new geometrical method, see [21]. He actually proves a much stronger result that we will not state here, see [20] for an earlier version of the work. [5]

In [36], Vojta proves also that $\mathbf{B^2}(\mathbb{Q})$ would have a positive answer if the following question by Bombieri would have a positive answer: Let X be a smooth projective algebraic variety of general type defined over a number field K. Does there exist a proper Zariski-closed subset of X which contains all its K-rational points?

Vojta's proof actually works for any number field, as noticed by Pasten, see [22]. Because it uses Falting's theorem, the method does not give any upper bound for M (in the case of $\mathbb{Q}$, it says that there would exist an $M \geq 8$ such that all 2-Büchi sequences over $\mathbb{Q}$ of length $\geq M$ are trivial).

By adapting his own new proof for meromorphic and algebraic functions, Pasten also shows in [21] that for any k and any number field K, a very strong version of $\mathbf{B^k}(K)$ would have a positive answer under the assumption of a conjecture by Vojta (a number field analogue of the second main theorem in value distribution theory). This result gives a new evidence for $\mathbf{B^k}(\mathbb{Z})$ to have a positive answer for any power.

5 Another approach to the Logic problem

Recall that P^k is interpreted in any ring as the set of k-th powers ($k \geq 2$). In the following, the symbol $|$ will be interpreted in $\mathbb{Z}$ as the divisibility (binary) relation.

In his master's thesis, J. Utreras studied the diophantine problem for $\mathbb{Z}$ over the language $\mathcal{L}^k = \{0, 1, +, P^k\}$. Since Büchi's problem is open over the integers for all k and seems to be out of reach at the moment, even for $k = 2$, one approach is to try to find/solve a problem somewhat weaker than Büchi's that still would imply undecidability over a language as close as possible to $\mathcal{L}_k$. He obtained in particular the following results, see [34], or [33] for a more extensive discussion. The positive existential theory of $\mathbb{Z}$ over $\mathcal{L}$ is undecidable when $\mathcal{L}$ is any of the following languages:

1. $\{0, 1, +, |, P^k\}$, for any $k \geq 2$;

2. $\{0, 1, +, |, P_k\}$, for any $k \geq 2$, where $P_k(x, y)$ is interpreted as $x = k^y$;

3. $\{0, 1, +, P2, R^k\}$, for any $k \geq 1$, where $R^k(x, y)$ is interpreted as "there exists t such that $y = tx$ and any prime p that divides t satisfies $p^k \leq x$".

[4] This seems to have been generalized recently by Julie Tzu-Yueh Wang, but I have not seen the paper yet. Also Julie Tzu-Yueh Wang and H. L. Huang have anounced a positive solution to Büchi's problem for cubes over function fields, and again as I have not seen the paper, I do not know whether their work includes some new feature.

[5] The last version of the work [21] is not yet publicly available.

Observe that the intersection of all relations R^k is just the equality. Results 1 and 2 should be seen in the light of L. Lipshitz's results on addition and divisibility. Their proof uses a theorem by Kosovskii [11]. Note that the positive existential theory of $\mathbb{N}$ over the following languages is decidable:

- $(0, 1, +, |)$ (Lipshitz [12]);
- $(0, 1, +, n \mapsto 2^n)$ (Semenov [31]);
- $(<, >, |, \nmid, \{c_n : n \in \mathbb{N}\}, \{f^k : k \in \mathbb{N}\})$, where c_n is interpreted by n and f^k by the map $n \mapsto n^k$ (Terrier [32]).

6 The language of *all powers*

In her master thesis, N. Garcia studied the Diophantine problem for rings of polynomials over the language $\mathcal{L}_P = \{0, 1, +, P\}$, where P is interpreted as the set of all powers in A (that is squares, cubes etc.). To that purpose, she proved, in particular, the following theorem: Let F be a field and b and c polynomials with coefficients in F. In the case of positive characteristic, assume moreover $b''c' - b'c'' \neq 0$. If b or c is non-constant then the expression $\lambda^2 + b\lambda + c$ is a cube or higher power for at most 12 values of $\lambda \in F$. [6]

In the case of characteristic zero, using the positive solution to a strong version of Büchi's problem for squares over polynomial rings by Pasten, and undecidability results by Denef [7] on one hand, and Pheidas and Zahidi [28] on the other hand, this allows her to prove the following. Let $F[t]$ be a polynomial ring over a field F of characteristic zero. The positive existential theory of $F[t]$ over the languages $\mathcal{L}_P \cup \{f_t\}$ and $\mathcal{L}_P \cup \{T\}$ is undecidable (here $f_t(x)$ is interpreted as tx, and T is Rubel's predicate, namely, $T(x)$ is interpreted as "x is non-constant"). If moreover the field F is algebraically closed, then the full theory of $F[t]$ is undecidable over $\mathcal{L}_P$.

These results are the first of that kind and they open the many questions about analogues for other structures.

7 Uniform undecidability results from solving Büchi's problem

Because the results mentioned in this section are quite technical if presented in all generality, I only present here some of the ideas and invite the reader to see [23] for more details.

It has already been mentioned that in positive characteristic p, any sequence $(x_n)_n$ satisfying $x_n^2 = (x + n)^{p^s+1}$ for each n is a 2-Büchi sequence of infinite length (here s is a non-negative integer). In [25] and [26], Pheidas and the author showed that over the rational function field $F(t)$, where F is a field of characteristic $p \geq 19$, any 2-Büchi sequence of length $M \geq 18$ has this form. This was generalized to function fields of curves in [30] by Shlapentokh and the author (the upper bound on M and the lower bound for p depend only on the genus of the curve).

Because the bound M involved does not really depend on the characteristic (the same M works for all large enough characteristics), it turns out that the binary relation

$$\text{“there exists a natural number } s \text{ such that } y = x^{p^s} \text{ or } x = y^{p^s}\text{”}$$

can be defined existentially in a uniform way in large classes of function fields over various natural languages (see [23]). The class essentially depends on the class of rings for which Büchi's problem has a positive answer. The languages involved are, for example, the language of rings $\mathcal{L}_A$ together with Rubel's predicate $\mathcal{L}_T = \mathcal{L}_A \cup \{T\}$, or $\mathcal{L}_z = \mathcal{L}_A \cup \{z\}$, where z is a symbol of constant which stands for a transcendental element, or $\mathcal{L}_{z,\mathrm{ord}} = \mathcal{L}_z \cup \{\mathrm{ord}\}$ where $\mathrm{ord}(x)$ is interpreted as "the order of x is non-negative at the prime z" (in the sense of valuation).

[6] The bounds are actually much better in characteristic zero, and in the case of positive characteristic the condition on b and c can be weakened - we present this simpler version of her theorem as it is enough to get the logic results.

In order to take the maximum benefit of this uniform definition and obtain uniform positive existential results, we then develop a concept of *uniform encodability* that does not seem to exist in the literature (related to interpretability). A direct corollary of our results is the following:

Theorem 7.1 If

1. $\mathcal{L}$ is any of $\mathcal{L}_z$ or $\mathcal{L}_T$ and Ω is a non-empty subclass of the class of all polynomial rings $\mathbb{F}_p[z]$, where p is an odd prime ≥ 17, or
2. $\mathcal{L}$ is $\mathcal{L}_{z,\mathrm{ord}}$ and Ω is a non-empty subclass of the class of all fields of rational functions of the variable z, over a field F of characteristic $p \geq 19$.

then

(a) there is no algorithm which determines whether or not an arbitrary positive-existential sentence of the language $\mathcal{L}$ is true or not in *some* member of Ω; and

(b) the conclusions of item (a) hold true if the class is assumed to be infinite and the (emphasized) word *some* is substituted by any of the following *all*, *all but possibly finitely many* or *infinitely many*.

8 Lower bounds

Assume that (some analogue of) Büchi's problem for k-th powers has a positive answer over some ring A. Write $\beta(k, A)$ for the lowest M such that all k-Büchi sequences over A of length M are trivial, and $\beta_f(k, A)$ for the lowest M such that all but finitely many k-Büchi sequences over A of length M are trivial.

We know the numbers $\beta(k, A)$ and $\beta_f(k, A)$ only in very few cases. Even for rings of the form $\frac{\mathbb{Z}}{n\mathbb{Z}}$ the value of $\beta(k, A)$ is not known in general. If Büchi's problem has a positive answer for rings A and B then it has a positive answer for the ring $A \times B$, and the optimal M for $A \times B$ is the maximum of the optimal M for ring A and the optimal M for ring B (see [22]). So in order to know $\beta(k, \frac{\mathbb{Z}}{n\mathbb{Z}})$ for each $n > 2$ not of the form $2m$ for some odd m (because Büchi's problem has trivially a negative answer if $n = 2$), it is enough to know it for each n of the form p^m, where p is a prime number. One can easily verify (by direct computation) that $\beta(2, \frac{\mathbb{Z}}{4\mathbb{Z}}) = \beta(2, \frac{\mathbb{Z}}{8\mathbb{Z}}) = 3$, $\beta(2, \frac{\mathbb{Z}}{5\mathbb{Z}}) = 4$, and using the remark above, $\beta(2, \frac{\mathbb{Z}}{60\mathbb{Z}}) = 4$.

In [17], Pasten shows that $\beta(2, \mathbb{F}_p) \leq \frac{p+3}{2}$, and more generally, under some condition on the prime p, $\beta(k, \mathbb{F}_p) = O(p^{\frac{1}{2}} \log p)$. Note that in the field $\mathbb{F}_{p^r}$, with $r \geq 2$, Büchi's problem is open in general (if we consider sequences $(x_n)_n$ such that $x_n^2 = (x + n)^{p^s+1}$ as trivial sequences).

If A is the field of meromorphic functions, the ring of analytic functions, the field of rational functions, or the ring of polynomials over $\mathbb{C}$, the best result is by Vojta: $\beta(2, A) \leq 8$. In the same paper [36], Vojta shows that $\beta_f(2, K) \leq 8$ for any number field K if Bombieri's question has a positive answer (see [22] for a quite precise sketch of the proof). On the other hand, Büchi conjectured that $\beta(2, \mathbb{Z})$ is finite and is equal to 5, and still no 2-Büchi sequence of length 5 is known to exist. However, $\beta(2, \mathbb{Z}) \geq 5$ (if it exists).[7]

Next, and finally, we will mention an approach *from below* to Büchi's problem for squares over $\mathbb{Z}$: can we characterize all solutions of length 3 and/or 4 in a nice enough way so that it could solve Büchi's problem?

[7] Browkin and Breziński proved a few years ago that $\beta_f(2, \mathbb{Q}) \geq 7$ (unpublished as far as I know). Indeed, they show that there exist infinitely many non-trivial 2-Büchi sequences of length 5 and 6 over $\mathbb{Q}$. They conjecture that the sequences of length 6 are all symmetric (namely, of the form $(x_1, x_2, x_3, x_3, x_2, x_1)$) and notice that there are no symmetric 2-Büchi sequences of length 6 over the integers (hence, if their conjecture is true, then $\beta(2, \mathbb{Z}) \leq 6$). Very recently, M. Artebani, A. Laface and D. Testa showed more generally that the set of 2-Büchi sequences of length 5 over $\mathbb{Q}$ is Zariski-dense in the variety defined by the Büchi equations $x_5^2 - 2x_4^2 + x_3^2 = x_4^2 - 2x_3^2 + x_2^2 = x_3^2 - 2x_2^2 + x_1^2 = 2$.

From now on Büchi sequences will refer to 2-Büchi sequences.

In [9] and [10], D. Hensley characterizes all Büchi sequences of length 3 over the rationals, and through some smart conditions of divisibility, he deduces from it a nice characterization of the integer sequences of length 3 (see [22] for more details). This allows him in particular to show that there exist infinitely many non-trivial sequences of length 4.

In [29], P. Sáez and the author find a more direct characterization of sequences of length 3 (without passing through the rational numbers). Indeed, we consider the subgroup H of $\mathrm{GL}(3,\mathbb{Z})$ generated by the matrices

$$B = \begin{pmatrix} 3 & 4 & 0 \\ 2 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad \text{and} \qquad J = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

and prove that it is isomorphic to the free product $\mathbb{Z} * \mathbb{Z}_2$. This group acts naturally on the set of Büchi sequences of length 3. Let

$$\Delta = \{(2,1,0), (-2,1,0), (1,0,1), (-1,0,1), (-1,0,-1)\}.$$

We then prove that, given a 3-terms Büchi sequence $x = (x_1, x_2, x_3)$ of integers there exists a matrix $M \in H$ and a unique $\delta \in \Delta$ such that $x = M\delta$. Moreover, the matrix M is unique with this property if $\delta \notin \{(1,0,1), (-1,0,-1)\}$, and it is unique up to right-multiplication by J otherwise. From this theorem, one can build up a strategy to solve Büchi's problem, following more or less the following idea. Suppose that $x = (x_1, \ldots, x_5)$ is a Büchi sequence. By changing the signs appropriately, on can assume that both (x_1, x_2, x_3) and (x_3, x_4, x_5) are in the orbit of $(2,1,0)$, or that both are in the orbit of $(-1,0,1)$. Therefore, there exists a matrix M_x that sends (x_1, x_2, x_3) to (x_3, x_4, x_5). One can then prove that if $M_x = B$ or B^{-1} then the sequence x is trivial. Since we know the presentation of H, is it possible to prove by induction that for all matrices M_x, the sequence x is trivial?[8] That would show that there are no non-trivial Büchi sequences of length 5. By similar arguments, we propose a problem P such that: if P has a positive answer then there are no non-trivial Büchi sequences of length 8, and if there are no non-trivial Büchi sequences of length 5 then P has a positive answer.

In [35], the author tries to characterize all Büchi sequences of length 4 over the integers (methods from algebraic geometry allow a complete characterization over the rationals, as the variety involved is a Segre surface - see [35] for a rational parametrization of all Büchi sequences of length 4 whose computation is due to O. Wittenberg). In [35], we give an explicit infinite family of polynomial parametrizations of non-trivial 4-terms Büchi sequences of integers: by a polynomial parametrization, we mean a sequence (P_1, P_2, P_3, P_4) of elements of the ring of polynomials $\mathbb{Z}[t]$ such that for each t the sequence $(P_1(t), P_2(t), P_3(t), P_4(t))$ is a Büchi sequence. Unfortunately, we do not know whether we characterize all but finitely many Büchi sequences. Still, these parametrizations give rise to an explicit infinite family of curves with the following property: any (non-trivial) integral point on one of these curves would give a length 5 non-trivial Büchi sequence of integers. Finally, we prove that infinitely many 4 terms non-trivial Büchi sequences do not extend to a 5-terms Büchi sequence (we show that various of the curves involved are hyperelliptic and do not have any non-trivial integer point). Because of the way these parametrizations are defined, induction is also available here, but we were not able to use it in an effective enough way in order to show that none of the curves involved has a non-trivial integer point.

References

[1] Ta Thi Hoai An and J. Tzu-Yueh Wang, *Hensley's problem for complex and non-Archimedean meromorphic functions*, Journal of Mathematical Analysis and Applications, **381-2**, 661-677 (2011).

[8] this strategy cannot work without considering that (x_2, x_3, x_4) is also a Büchi sequence

[2] J. Browkin, *Büchi sequences in local fields and local rings*, Bull. Polish Acad. Sci. Math. **58**, 109-115 (2010).

[3] J. Browkin and J. Brzeziński, *On sequences of squares with constant second differences*, Canad. Math. Bull. **49-4**, 481-491 (2006).

[4] M. Castillo, *El Problema de Büchi para números p-ádicos*, Tesis de Magíster (Master thesis), Universidad of Concepción, Chile (2011).
http://dmat.cfm.cl/colloquium/2011-03-31-17:00.pdf

[5] M. Castillo, *A note on Büchi's problem for p-adic numbers*, Proyecciones **30-3**, 295-302 (2011).

[6] M. Davis, *Hilbert's tenth problem is unsolvable*, American Mathematical Monthly **80**, 233-269 (1973).

[7] J. Denef, *The Diophantine Problem for polynomial rings and fields of rational functions*, Transactions of the American Mathematical Society **242**, 391-399 (1978).

[8] N. Garcia, *Potencias en subsucesiones de progresiones aritméticas en anillos de funciones y un problema de indecidibilidad*, Tesis de Magíster (Master thesis), Universidad of Concepción, Chile (2011).
http://dmat.cfm.cl/colloquium/2011-04-15-12:00.pdf

[9] D. Hensley, *Sequences of squares with second difference of two and a problem of logic*, unpublished (1980-1983).

[10] —– *Sequences of squares with second difference of two and a conjecture of Büchi*, unpublished (1980-1983).

[11] N. K. Kosovskii, *On solutions of systems consisting of both word equations and word length inequalities*, Zap. Naucn. Sem. Leningrad. Otdel. Mat. Inst. Steklov **40**, 24-29, (1974).

[12] L. Lipshitz, *The Diophantine problem for addition and divisibility*, Transactions of the American Mathematical Society **235**, 271-283, (1978).

[13] —–, *Quadratic forms, the five square problem, and diophantine equations*, The collected works of J. Richard Büchi (S. MacLane and Dirk Siefkes, eds.) Springer, 677-680, (1990).

[14] B. Mazur, *Questions of decidability and undecidability in number theory*, The Journal of Symbolic Logic **59-2**, 353-371 (1994).

[15] H. Pasten, *Extensiones del problema de Büchi a distintas estructuras y potencias más altas*, Master thesis (2010).
http://dmat.cfm.cl/colloquium/2010-04-19-11:00.pdf

[16] —–, *Problemas de definibilidad e indecidibilidad en algunos anillos de funciones*, PhD thesis (2010).
http://dmat.cfm.cl/colloquium/2010-09-13-10:00.pdf

[17] —–, *An extension of Büchi's Problem for polynomial rings in zero characteristic*, Proceedings of the American Mathematical Society **138**, 1549-1557 (2010).

[18] —– *Büchi's problem in any power for finite fields*, Acta Arithmetica **149-1**, 57-63 (2011).

[19] —– *Representation of squares by monic second degree polynomials in the field of p-adic meromorphic functions*, Transactions of the American Mathematical Society, **364**, 417–446 (2012).

[20] —— *Representation of powers by polynomials over function fields and a problem of logic*, arXiv:1107.4019.

[21] —— *Powerful values of polynomials and a conjecture of Vojta*, preprint.

[22] H. Pasten, T. Pheidas, X. Vidaux, *A survey on Büchi's problem: new presentations and open problems*, Proceedings of the Hausdorff Institute of Mathematics, Zapiski POMI **377**, 111-140, Steklov Institute of Mathematics. Published online http://www.pdmi.ras.ru/znsl/2010/v377.html (2010).

[23] —— *Uniform Definability and Undecidability in Classes of Structures*, arXiv:1012.0960v1 (2011).

[24] T. Pheidas and X. Vidaux, *Extensions of Büchi's problem: Questions of decidability for addition and n-th powers*, Fundamenta Mathematicae **185**, 171-194 (2005).

[25] —— *The analogue of Büchi's problem for rational functions*, The Journal of The London Mathematical Society **74-3**, 545-565 (2006).

[26] —— *Corrigendum: The analogue of Büchi's problem for rational functions*, The Journal of the London Mathematical Society **82-1**, 273-278 (2010).

[27] —— *The analogue of Büchi's problem for cubes in rings of polynomials*, Pacific Journal of Mathematics **238** (2), 349-366 (2008).

[28] T. Pheidas and K. Zahidi, *Undecidable existential theories of polynomial rings and function fields*, Communications in Algebra **27(10)**, 4993-5010 (1999).

[29] P. Sáez and X. Vidaux, *A characterization of Büchi's integer sequences of length 3*, Acta Arithmetica **149-1**, 37-56 (2011).

[30] A. Shlapentokh and X. Vidaux, *The analogue of Büchi's problem for function fields*, Journal of Algebra **330-1**, 482-506 (2010).

[31] A. L. Semenov, *Logical theories of one-place functions on the set of natural numbers*, Math. USSR Izvestiya **22-3**, 587-618 (1984).

[32] V. Terrier, *Decidability of the existential theory of the set of natural numbers with order, divisibility, power functions, power predicates, and constants*, Proceedings of the American Mathematical Society **114-3**, 809-816 (1992).

[33] J. Utreras, *Análogos del Décimo Problema de Hilbert*, Master thesis, Universidad de Concepción, Chile (2010).
http://dmat.cfm.cl/colloquium/2010-07-02-17:00.pdf

[34] J. Utreras, *A logical approach to the problem of representation of integers by systems of diagonal forms*, Bulletin of the London Mathematical Society **43-2**, 299-310 (2011).

[35] X. Vidaux, *Polynomial parametrizations of length 4 Büchi sequences*, Acta Arithmetica **150-3**, 209-226 (2011).

[36] P. Vojta, *Diagonal quadratic forms and Hilbert's Tenth Problem*, Contemporary Mathematics **270**, 261-274 (2000).