Elementary theory of ordinals with addition and left translation by ω

Christian Choffrut
LIAFA, Université Paris 7, 2, Pl. Jussieu
75 251 Paris Cedex 05, France
cc@liafa.jussieu.fr

1 Background

After Büchi it has become very natural to interprete formulae of certain logical theories as finite automata, i.e., as recognizing devices. This recognition aspect though, was neglected by the inventor of the concept and the study of the families of linear structures that could be accepted in the language theory sense of the term, was carried out by other authors. The most popular field of application of Büchi type automata is nowadays connected with model checking by considering a process as a possibly infinite sequence of events. For over a decade, the original model has been enriched by adding a time parameter in order to model reactive systems and their properties. Originally Büchi was interested in the monadic second order theory with the successor over ω but he later considered the theory of countable ordinals for which he was led to propose new notions of finite automata. Again these constructs can be viewed as recognizing devices of words over a finite alphabet whose length are countable ordinals. They were studied by other authors, mainly Choueka and Wojciechowski to who we owe two Theorems "à la Kleene" asserting the equivalence between expressions using suitable rational operators and subsets (languages) of transfinite words, [6] and [13].

Lately, there has been a renewed interest for strings of transfinite lengths as such by shifting the emphasis from logic to language theory. This is testified by various attempts to extend results from finite to transfinite strings. E.g., Eilenberg's famous varieties theorem suggested by Schützenberger's characterization of star-free languages, asserts that there exists a "natural" bijection between certain families of languages (i.e., subsets of finite length words) and certain families of finite semigroups. In both cases these families are defined by simple closure properties, [8]. In order to extend this result to words of transfinite length, Bedon and Carton extended Wilke's ω-semigroups to so-called ω_1-semigroups and were able that Eilenberg's theorem extends naturally, [1]. Also, the theory of rational relations which studies the rational subsets of pairs of words was extended to pairs of transfinite words in [4] where it is shown that the two traditional notions of rational relations still coincide when properly re-defined. Finally, we mention the beginning of a systematic study of the combinatorial properties of words of transfinte length by showing, for example, how equations in two unknowns can be "solved", [5].

2 Ordinals with addition and multiplication by constants

The first order theory of ordinal addition is long known to be decidable (Ehrenfeucht, 1957 [7], Büchi, 1964 [3]). Furthermore, its complexity is a linear tower of exponentials (Maurin, 1996 [10, 11]). There are two methods to obtain these results: one uses Fraïsse-Ehrenfeucht games ([7, 11]), the other relies on Büchi's theory [3] of sets of transfinite strings recognized by finite automata.

Here, we are concerned with the theory of ordinal addition enriched with the multiplication by a constant. Left and right ordinal multiplications have different properties. E.g., multiplication distributes over addition with a left multiplicand but not with a right one: $(\omega+1)\omega = \omega^2 \neq \omega^2 + \omega$. We shall state and briefly sketch the proofs of two results concerning the theory of the ordinals with the usual addition and the left multiplication by ω. Actullay, contrary to theory of ordinal addition, the Π^0_2-fragment of the first-order theory of $\langle \omega^\omega; =, +, x \mapsto \omega x\rangle$ is already undecidable while the existential fragment is decidable. Observe that enriching the language with the right multiplication by ω does not increase the power of expression.

Let us mention a recent paper though not directly connected to ours, which tackles the decidability issue of the theory of ordinal multiplication over the ordinal α and shows that it is decidable if and only if α is less than ω^ω, [2].

We refer the reader to the numerous standard handbooks such as [12] or [9] for a comprehensive exposition of the theory on ordinals. We recall that every ordinal α has a unique representation, known as Cantor's normal form, as a finite sum of non-increasing prime components. By grouping the equal prime components, all non-zero ordinals α can thus be written as

$$\alpha = \omega^{\lambda_n} a_n + \omega^{\lambda_{n-1}} a_{n-1} + \ldots + \omega^{\lambda_1} a_1 + \omega^{\lambda_0} a_0 \tag{1}$$

where $n \geq 0, 0 < a_n, \ldots, a_1, a_0 < \omega$ and $\lambda_n > \lambda_{n-1} > \ldots > \lambda_0 \geq 0$. The ordinal λ_n is the *degree* of α.

We consider the theory of the ordinals less than ω^ω with equality as unique predicate, the ordinal addition and the left ordinal multiplication by ω: $x \to \omega x$ as operations, in other words we consider the theory ThL $=$ Th$\langle \omega^\omega; +, x \to \omega x\rangle$ and we prove that it is undecidable by reducing the halting problem of Turing machines to it. We make the usual assumption that the formulas are in the prenex normal form

$$Q_1 y_1 \dots Q_p y_p : \ \phi(x_1, \dots, x_n) \tag{2}$$

where each Q_i is a universal or an existential quantifier, each x_i and each y_j is a variable and ϕ is a Boolean combination of formulas of the form

$$L(x_1, \dots, x_n) = R(x_1, \dots, x_n) \ \text{ or } L(x_1, \dots, x_n) \neq R(x_1, \dots, x_n) \tag{3}$$

with L and R linear combinations of terms such as ax and a where x is a variable and a is a constant.

It is not difficult to see that the case of roght multiplication is trivial. Indeed, for every $\xi < \omega^{\omega^\omega}$ the relations $y = \xi$ and $y = x\xi$ can be defined in every $\langle \lambda; =, +\rangle$ for $\lambda > 0$ and thus, in particular, the theory $\langle \lambda; +, x \to x\omega\rangle$ is decidable for all ordinals λ, [3].

2.1 Undecidability

Presburger arithmetics of the integers is cloesely related to the n-ary rational relations over ω and is therefore decidable. This connection no longer holds under our assumptions and ThL can be shown to be undecidable by reducing the halting problem of Turing machines to it.

Theorem 1. *The elementary theory* ThL $=$ Th$\langle \omega^\omega; +, x \to \omega x\rangle$ *is undecidable.*

Sketch of the proof. A computation of a Turing machine is a sequence of configurations $(c_i)_{0 \le i \le n}$ such that c_0 is the initial configuration, c_n is a final configuration and c_{i+1} is a next configuration of c_i for all $0 \le i \le n-1$. We view the set $\Sigma \cup Q$ as digits. To the sequence $(c_i)_{0 \le i \le n}$ we assign the ordinal

$$\sum_{0 \le i \le n} \omega^i ||c_i||$$

where $||c_i||$ is the integer whose representation is c_i in the appropriate base. The problem reduces to expressing the fact that there exists an ordinal α which encodes a valid computation by using no other operations than those of the logic. The first task is to decompose α into its Cantor normal form $\sum_{0\leq i\leq n}\omega^i a_i$ and to verify that the sequence of its coefficients a_i, once interpreted as strings c_i over $\Sigma\cup Q$, defines a computation. More precisely, α encodes a valid computation if a_0 can be interpreted as the initial configuration (with the input word on the tape and the initial state as current state), a_n as a final configuration and if for all $0\leq i\leq n-1$, a_i and a_{i+1} can be interpreted as two successive configurations.

Now we explain why this cannot work in such a simple way. Indeed, a configuration is traditionnaly a word of the form w_1qw_2 where $w_1w_2\in\Sigma^*$ is the content of the minimal initial segment of the tape comprising all cells containing a non-blank symbol along with the cell where the head is positionned, q is the current state and the reading head is at position $|w_1|$ from the left border (starting from position 0). Interpret a_i and a_{i+1} as the two successive configurations w_1qw_2 and y_1py_2. Since a_i and a_{i+1} are ordinary integers, the only operations at hand is the addition. It seems intuitively impossible to "extract" the values of the states q and p by a mere use of this operation. As a consequence, instead of encoding the configuration w_1qw_2 with an integer, we will encode it with the ordinal $\omega^2a_2+\omega a_1+a_0$ where $a_2=||w_1||$, $a_1=||q||$ and $a_0=||w_2||$.

2.2 Existential fragment of ThL

We mentioned earlier the connection between rational relations and Presburger formulae. For ThL this connection no longer holds even in the case of the existential fragment. In order to convince the reader we introduce some definitions inspired by the rational subsets of the free commutative monoids.

Define the ω-rational relations over ω^ω of arity n as the least family of relations containing the single n-tuples of ordinals and closed by set union, componentwise addition, Kleene and ω-closures wher by the Kleene closure of a subset X of ω we mean all possible finite (possibly empty) sums of elements in X and by the ω-closure of X we mean all ω-sums of elements in X.

A subset of $(\omega^\omega)^k$ is *linear* if it is of the form

$$\{\beta_0+\alpha_1x_1+\beta_1+\alpha_2x_2+\ldots+\alpha_rx_r+\beta_r\mid x_1,\ldots,x_r<\omega\}$$

where $\beta_0,\alpha_1,\beta_1,\ldots,\alpha_r,\beta_{r+1}$ are elements in $(\omega^\omega)^k$. It is *semilinear* if it is a finite union of linear subsets.

Proposition 1 *For an arbitrary subset $X \subseteq \omega^\omega \times \omega^\omega$ the following properties are equivalent*

1) *X is ω-rational*

2) *X is semilinear*

3) *X is a finite union of subsets of the form*

$$\alpha_1 R_1 + \alpha_2 R_2 + \ldots + \alpha_k R_k \tag{4}$$

where the α_i's are arbitrary k-tuples of ordinals in ω^ω and the R_i's are rational relations of $\mathbb{N}^k$.

Sketch of the proof. In view of the previous discussion it suffices to prove that **3)** implies **1)**. But this is trivial since every pair of ordinals is a rational relation of $\omega^\omega \times \omega^\omega$ reduced to an element. ■

Now we return to the theory ThR and observe that the set of values of the free variables satisfying a given the formula is an ω-rational relation. This no longer holds for ThL as shown by the following formula

$$\phi \equiv (\omega^2 x + x = y) \wedge (z = x + z = \omega^2)$$

where the set of pairs of ordinals satisfying ϕ is equal to $\{(\omega^3 n + \omega^2 p + \omega n + p,\ \omega n + p) \mid n, p < \omega\}$.

We prove that the existential fragment of ThL is decidable. After possible introduction of new individual variables and equalities for transforming all disequalities, the general form of such an existential formula is a disjunction of conjunctions of equalities

$$L(x_1, \ldots, x_n) = R(x_1, \ldots, x_n) \tag{5}$$

prefixed by a collection of existential quantifiers. Actually each handside is a linear combination

$$\alpha_1 y_1 + \beta_1 + \alpha_2 y_2 + \beta_2 + \ldots \alpha_p y_p + \beta_p$$

where the α_i's and the β_i's are ordinals and the y_i's are (possibly repeated) unknowns. We consider a system of equations

$$L_j(x_1, x_2 \ldots, x_n) = R_j(x_1, x_2 \ldots, x_n) \ j = 1, \ldots t \tag{6}$$

where each left- and right-handside is a linear combination. A *monomial* of the above system is an expression of the form $\alpha_i y_i$ which occurs in a left- or right-handside of some equation of the system.

Theorem 2. *The existential fragment of* ThL *is decidable*

Sketch of the proof. It suffices to show that the existence of a solution for the system (6) is decidable. Consider Cantor's normal form of the value of an arbitrary unkown

$$x = \omega^m a_m + \omega^{m-1} a_{m-1} + \ldots + \omega a_1 + a_0 \tag{7}$$

If we can effectively bound the degree m of each of these variables then we can also effectively bound the degrees of each handside of each equation the system say these degrees are less than N. By equating the coefficients of degree less than N, each equation of the system splits into up to $N+1$ linear equations where the unknowns are the coefficients a_i of the variables as in (7). Denote by δ the maximum degree of the coefficients α_i in (6) and by K the least common multiple of all integers less than or equal to δ. Let $d_1 \leq d_2 \leq \ldots\ldots d_p$ be the sequence, in non-decreasing order, of the degrees of the monomials occurring in an equation of the system. We can show that if the sytem has a solution, then it has one that satisfies for all $1 \leq i \leq p$

$$\delta \leq d_i < d_{i+1} \Rightarrow d_{i+1} \leq d_i + 3K$$

which proves the claim. ■

References

1. N. Bedon and O. Carton. An Eilenberg theorem for words on countable ordinals. In *Proceedings of Latin'98 Theoretical Informatics*, number 1380 in LNCS, pages 53–64. Springer-Verlag, 1998.
2. Alexis Bès. Decision problems related to the elementary theory of oordinal multiplication. *Fund. Math.*, xxx(xxx):xxx. to appear.
3. J. Büchi. Transfinite automata recursions and weak second ordre theory of ordinals. In *International Congress in Logic, Methodology and Philosophy of Sciences*, pages 3–23. North-Holland, 1964.
4. C. Choffrut and S. Grigorieff. Uniformization of rational relations. In G. Paun J. Karhumäki, H. Maurer and G. Rozenberg, editors, *Jewels are Forever*, pages 59–71. Springer Verlag, 1999.
5. C. Choffrut and S. Horváth. Transfinite euqations in transfinite strings. *Internat. J. Algebra Comput.*, 10(5):625–649, 2000.
6. S. C. Choueka. Finite automata, definable sets and regular expressions over ω^n-tapes. *J. Comput. System Sci.*, 17:81–97, 1978.
7. A. Ehrenfeucht. Applications of games to some problems of mathematical logic. *Bull. Académie Polonaise des Sciences*, 5:35–37, 1957.
8. S. Eilenberg. *Automata, Languages and Machines*, volume B. Academic Press, 1976.

9. D. Klaua. *Allgemeine Mengenlehre*. Akademie Verlag, 1969.
10. F. Maurin. Exact complexity bounds for ordinal addition. *Theoret. Comput. Sci.*, 165(2):247–273, 1996.
11. F. Maurin. Ehrenfeucht games and ordinal addition. *Annals of Pure and Applied Logic*, 89(1):53–73, 1997.
12. W. Sierpiński. *Cardinal and Ordinal Numbers.* Warsaw: PWN, 1958.
13. J. Wojciechowski. Finite automata on transfinite sequences and regular expressions. *Fundamenta Informaticae*, 8(3–4):379–396, 1985.