The Complexity of Carry Propagation for Successor Functions

Jacques Sakarovitch[1]

[1]IRIF - UMR 8243 - CNRS/Paris Diderot University and Telecom ParisTech

Joint work with
Valérie Berthé[2], Christiane Frougny[2] and Michel Rigo[3]

[2] IRIF - UMR 8243 - CNRS/Paris Diderot University
[3] Université de Liège, Institut de Mathématiques

EXTENDED ABSTRACT

Carry propagation is the nightmare of school pupils and the headache of computer engineers: not only can the addition of two digits give rise to a carry, but this carry itself, when added to the next digits to the left[1] may give rise to another carry, and so on, and so forth, and this may happen for an arbitrarily long time. Since the beginnings of computer science, the evaluation of the carry propagation length has been the subject of many works and it is known that the average carry propagation length (or complexity) for addition of two uniformly distributed n-digits binary numbers is $\log_2(n) + \mathrm{O}(1)$ (see [5, 7, 10]).

We consider here the problem of carry propagation from a more theoretical perspective and in an apparently elementary case. We investigate the amortized carry propagation of the *successor function* in various numeration systems. The central case of integer base numeration system allows us to describe quickly what we mean. Let us take an integer p greater than 1 as a base. In the representations of the succession of the integers — which is exactly what the successor function does — the least digit changes at every step, the penultimate digit changes every p steps, the ante-penultimate digit changes every p^2 steps, and so on and so forth ... As a result, the average carry propagation of the successor function, computed over the first N integers, should tend to the quantity

$$1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots = \frac{p}{p-1} \quad ,$$

when N tends to infinity. It can be shown that it is indeed the case. Motivated by various works on non-standard numeration systems, we investigate the questions of evaluating and computing the amortized carry propagation in those systems. We thus consider several such numeration systems different from the classical integer base numeration systems: the greedy numeration systems and the beta-numeration systems, see [6], which are a particular case of the former, the rational base numeration systems [1] which are not greedy numeration systems, and

[1] We write numbers under MSDF (Most Significant Digit First) convention.

the abstract numeration systems [8] which are a generalization of the classical *positional numeration systems.*

The approach of *abstract numeration systems* of [8], namely the study of a numeration system via the properties of the set of expansions of the natural integers is well-fit to this problem. Such systems consist of a totally ordered alphabet A of the non-negative integers $\mathbb{N}$ and a language L of A^*, ordered by the *radix order* deduced from the ordering on A. The representation of an integer n is then the $(n+1)$-th word of L in the radix order. This definition is consistent with every classical standard and non-standard numeration system.

Given a system defined by a language L ordered by radix order, we denote by $\mathsf{cp}_L(i)$ the carry propagation in the computation from the representation of i in L to that of $i+1$. The *(amortized) carry propagation* of L, which we denote by CP_L, is the limit, *if it exists*, of the mean of the carry propagation at the first N words of L:

$$\mathsf{CP}_L = \lim_{N\to\infty} \frac{1}{N} \sum_{i=0}^{N-1} \mathsf{cp}_L(i) \ . \tag{1}$$

A further hypothesis is to consider *prefix-closed* and *right-extensible* languages, called 'PCE' languages in the sequel: every left-factor of a word of L is a word of L and every word of L is a left-factor of a longer word of L. Hence, L is the branch language of an infinite labelled tree $\mathcal{T}_L$ and, once again, every classical standard and non-standard numeration system meets that hypothesis.

We first prove two easy properties of the carry propagation of PCE languages. First, CP_L does not depend upon the labelling of $\mathcal{T}_L$, but only on its 'shape' which is completely defined by the infinite sequence of the degrees of the nodes visited in a breadth-first traversal $\mathcal{T}_L$, and which is called *signature* of $\mathcal{T}_L$ (or of L) in [9]. For instance, the signature of the representation language in base p is the constant sequence p^ω. Second, we call *local growth rate* of a language L, and we denote by γ_L, the limit, *if it exists*, of the ratio $\mathbf{u}_L(\ell+1)/\,\mathbf{u}_L(\ell)$, where $\mathbf{u}_L(\ell)$ is the number of words of L of length ℓ. *If* CP_L *exists, then* γ_L *exists* and it holds:

$$\mathsf{CP}_L = \frac{\gamma_L}{\gamma_L - 1} \ . \tag{2}$$

Examples show that γ_L may exist without CP_L exist. By virtue of this equality, the *computation* of CP_L is usually not an issue, the problem lies in proving its *existence*. We develop three different methods of existence proof, whose domains of application are pairwise incomparable: *combinatorial*, *algebraic*, and *ergodic.*, and which are built upon very different mathematical backgrounds.

A combinatorial method shows that languages with *eventually periodic signature* have a carry propagation. These languages are essentially the rational base numeration systems (including the integer base numeration systems), possibly with non-canonical alphabets of digits ([9]).

We next consider the *rational abstract numeration systems*, that is, those systems which are defined by languages accepted by *finite automata*. Examples of such systems are the Fibonacci numeration system, more generally, beta-numeration systems where beta is a *Parry number* ([6]), and other systems different from beta-numeration. By means of a property of rational power series with positive coefficients which is reminiscent of Perron-Frobenius Theorem, we prove that *the carry propagation of a rational* PCE *language* L *exists if* L *has a local growth rate and all its quotients also have a local growth rate.*

The definition of carry propagation (Equation (1)) inevitably reminds of Ergodic Theorem. We then consider the *greedy numeration systems*. The language of greedy expansions in such a system is embedded into a compact set, and the successor function is extended as an action, called *odometer*, on that compactification. This gives a dynamical system, but Ergodic Theorem does not directy apply as the odometer is not continuous in general. Recently tools in ergodic theory ([2]) allow us to prove the existence of the carry propagation for greedy systems with exponential growth, and thus for beta-numeration in general.

This work was indeed motivated by a paper where the *amortized (algorithmic) complexity* of the successor function for some beta-numeration systems was studied ([3]). Whatever the chosen computation model, the (amortized) complexity is greater than the (amortized) carry propagation, hence can be seen as the sum of two quantities: the carry propagation itself and an *overload*. The study of carry propagation lead to quite unexpected and winding developments that form a subject on its own, leaving the evaluation of the overload to future works. A complete version of this present work ([4]) will appear soon.

References

1. Akiyama, S., Frougny, C., Sakarovitch, J.: Powers of rationals modulo 1 and rational base number systems. Israel J. Math. **168**, 53–91 (2008)
2. Barat, G., Grabner, P.: Combinatorial and probabilistic properties of systems of numeration. Ergod. Th. & Dynam. Sys. **36**, 422–457 (2016)
3. Barcucci, E., Pinzani, R., Poneti, M.: Exhaustive generation of some regular languages by using numeration systems. In: Proc. Words 2005. pp. 119–127. No. 36 in Monographies du LaCIM, UQaM (2005)
4. Berthé, V., Frougny, C., Rigo, M., Sakarovitch, J.: On the concrete complexity of the successor function. Part I: The carry propagation, in preparation.
5. Burks, A.W., Goldstine, H.H., von Neumann, J.: Preliminary discussion of the logical design of an electronic computing instrument. In: Taub, A.H. (ed.) Collected Works of John von Neumann, vol. 5, pp. 34–79. Macmillan (1963)
6. Frougny, C., Sakarovitch, J.: Number representation and finite automata, in Combinatorics, Automata and Number Theory, V. Berthé, M. Rigo (eds), Cambridge Univ. P., 34–107 (2010)
7. Knuth, D.E.: The average time for carry propagation. Nederl. Akad. Wettensch. Indag. Math. **40**, 238–242 (1978)
8. Lecomte, P., Rigo, M.: Abstract numeration systems, in Combinatorics, Automata and Number Theory, V. Berthé, M. Rigo (eds), Cambridge Univ. Press, 34–107 (2010)
9. Marsault, V., Sakarovitch, J.: Trees and languages with periodic signature. Indagationes Mathematicae **28**, 221–246 (2017)
10. Pippenger, N.: Analysis of carry propagation in addition: An elementary approach. J. Algorithms **42**(2), 317–333 (2002)