Invitation to Real Complexity Theory: Algorithmic Foundations to Reliable Numerics with Bit-Costs

Akitoshi Kawamura (The University of Tokyo) and Martin Ziegler (KAIST)

Abstract. While concepts and tools from Theoretical Computer Science are regularly applied to, and significantly support, software development for discrete problems, Numerical Engineering largely employs recipes and methods whose correctness and efficiency is demonstrated empirically. We advertise Real Complexity Theory: a resource-oriented foundation to rigorous computations over continuous universes such as real numbers, vectors, sequences, continuous functions, and Euclidean subsets: in the bit-model by approximation up to given absolute error. It offers sound semantics (e.g. of comparisons/tests), closure under composition, realistic runtime predictions, and proofs of algorithmic optimality by relating to known classes like $\text{NP}$, $\#\text{P}$, $\text{PSPACE}$.

Numerical methods permit digital computers, operating over sequences of bits, to solve problems involving a priori continuous objects such as real numbers, functions, or operators. Partial differential equations for instance are regularly treated by discretizing the domain, thus approximating the infinite-dimensional solution function space by a high but finite dimensional one. Other common (sub)problems include ordinary differential equations, numerical integration and differentiation, or maximizing some objective function subject to certain constraints. We thus record that numerical science has devised a variety of methods working impressively well in practice in terms of an intuitive conception of efficiency.

Formal notions of algorithmic efficiency, on the other hand, are at the core of Computer Science and have led to the well-established complexity theory with famous classes like $\text{P}$ and $\text{NP}$. They capture the computational difficulty inherent to a fully specified problem, rather than the cost of some method solving certain instances of it: thus providing a sound framework for comparing any specific algorithm against an (usually unknown) optimal one — in the discrete realm, that is, for problems over integers or graphs encoded as finite sequences of bits. Concerning real problems, we quote from [Linz88, p.412] and from [BCSS98, §1.4]:

*How do engineers deal with the problem of assigning some measure of reliability to the numbers that the computer produces? Over the years, I have sat on many Ph.D. qualifying examinations or dissertation defenses for engineering students whose work involved a significant amount of numerical computing. In one form or another, I invariably ask two questions: “Why did you choose that particular algorithm?” and “How do you know that your answers are as accurate as you claim?” The first question is usually answered confidently, using such terms as “second-order convergence” or “von Neumann stability criterion”. The next question, alas, tends to be embarrassing. After an initial blank or hostile stare, I usually get an answer like “I tested the method with some simple examples and it worked”, “I repeated the computation with several values of $n$ and the results agreed to three decimal places”, or more lamely, “the answers looked like what I expected”. So far, I have not faulted any student for the unsatisfactory nature of such a response. One reason for my reluctance to criticize is that I have really nothing better to offer. Rigorous analysis is out of the question.*

$\text{∗}$Partly supported by the Japan Society for the Promotion of Science (JSPS) Core-to-Core Program, by the JSPS Kakenhi project 26700001, by the German Research Foundation (DFG) project Zi 1009/4–1, and by the EU FP7 IRSES project 294962.
The developments described in the previous section (and the next) have given a firm foundation to computer science as a subject in its own right. Use of the Turing machines yields a unifying concept of the algorithm well formalized. [...] The situation in numerical analysis is quite the opposite. Algorithms are primarily a means to solve practical problems. There is not even a formal definition of algorithm in the subject. [...] Thus we view numerical analysis as an eclectic subject with weak foundations; this certainly in no way denies its great achievements through the centuries.

However nowadays we do have a sound, realistic, and applicable theory of computations over continuous universes in the bit-cost model approximations up to guaranteed absolute error $2^{-n}$: Initiated by Alan Turing in the very same work [Turi37] that introduced the machine now named after him — and before he ‘invented’ matrix condition numbers in 1948 — Recursive Analysis has developed into a sound algorithmic foundation to verified/reliable/rigorous (not necessarily interval) numerics and to computer-assisted proofs [Rump04,PWNT14] in unbounded precision; cmp. [BLWW04,BrCo06,Brav13]. Traditionally focused on the computational contents of existence claims from classical analysis (see Items a,b,e,g,k,m in the below Example), incomputability results often encode the Halting Problem in a clever way; while positive ones usually devise algorithms and establish their correctness. Starting with [KoFr82], however, the more refined view of complexity has received increasing attention and in the last few years accumulated a striking momentum [Ko91,Weih03,Schr04,KaCo10] with quantitative notions of efficiency and optimality of actual numerical computations! Here are some of its main features:

- Including transcendental calculations such as the exponential function: no restriction to algebraic numbers
- Guaranteed output approximations suitable (among others) for testing inner-mathematical conjectures
- up to absolute error $2^{-n}$ roughly corresponding to $n$ valid binary digits after the radix point: renders addition of real numbers computable in time linear in $n$.
- Adaptive precision for intermediate calculations beyond the paradigmatic chains of hardware floats.
- Fully specified algorithms of guaranteed behavior on explicit classes of admissible inputs.
- Parameterized analyses asymptotically for $n \to \infty$
- quantitatively with respect to resources like running time, memory (often the harder constraint), or #processors/cores
- Relating to standard complexity classes from Theoretical Computer Science such as $L \subseteq \text{NC} \subseteq \text{P} \subseteq \text{NP} \subseteq \text{P}^{\text{NP}} \subseteq \text{PSPACE} \subseteq \text{EXP}$ etc.
- Proving optimality of an algorithm: for instance using adversary arguments in a bounded-precision adaptation of IBC or relative to complexity-theoretic conjectures like $\text{P} \neq \text{NP}$.
- Based on Turing machines for a formal foundation of numerical calculations in the bit-cost model that yield
- both practical predictions of the behaviour of actual implementations
- and closure under composition, both of computable and polynomial-time computable functions: a prerequisite to modular software development relying crucially on both real number outputs and inputs being given by approximations!
- Actual programming in imperative object-oriented higher-level languages such as C++ using libraries that implement a new data type REAL which through overloading support ‘exact’ operations, thus facilitating
Definition 1. a) Computing a real number $x$ means printing some infinite sequence $a_n$ of integers (in binary without leading zeros) as mantissa/numerators to dyadic rationals $a_n/2^n$ that approximate $x$ up to absolute error $1/2^n$.

b) More generally, a real sequence $(x_j)$ means producing an integer double sequence $a_{j,m}$ with $|x_j - a_{j,m}|/2^m \leq 1/2^m$. Formally, the elements of said sequence occur in order according to the Cantor pairing function

$$\mathbb{N} \times \mathbb{N} \ni (j, m) \mapsto \langle j, m \rangle := j + (j + m) \cdot (j + m + 1)/2 \in \mathbb{N} := \{0, 1, 2, \ldots\} \quad (1)$$

that is, the output consists of the single integer sequence $(a_n)$ with $n = \langle j, m \rangle$.

c) Computing a univariate and possibly partial real function $f : \mathbb{R} \to \mathbb{R}$ amounts to converting every given sequence $(a_m) \subseteq \mathbb{Z}$ with $|x - a_m/2^m| \leq 1/2^m$ for any $x \in \text{dom}(f)$ into a sequence $(b_n) \subseteq \mathbb{Z}$ with $|f(x) - b_n/2^n| \leq 1/2^n$.

d) For some mapping $t : \mathbb{N} \to \mathbb{N}_+ := \{1, 2, \ldots\}$, the above computations are said to run in time $t(n)$ if the $n$-th integer output appears within at most $t(n)$ steps. Polynomial time (or polytime for short) means running time bounded by some polynomial $t \in \mathbb{N}[X]$. Similarly for exponential time and polynomial space.

e) Generalizing (c) and (d), consider a partial real multivalued function $f : \mathbb{R}^d \times \mathbb{N} \Rightarrow \mathbb{R}^e \times \mathbb{N}$. Computing $f$ amounts to converting, for every $(\vec{x}, k) \in \text{dom}(f)$, given $k \in \mathbb{N}$ and any sequence $(\vec{a}_m) \subseteq \mathbb{Z}^d$ with $\|\vec{x} - \vec{a}_m/2^m\| \leq 1/2^m$, into $\ell \in \mathbb{N}$ and some sequence $(\vec{b}_n) \subseteq \mathbb{Z}^e$ with $\|\vec{y} - \vec{b}_n/2^n\| \leq 1/2^n$ for some $(\vec{y}, \ell) \in f(\vec{x}, k)$.

Such a computation is said to run in fully polynomial time if $\vec{b}_n$ appears within a number of steps at most polynomial in $n + k$, and $\ell$ is bounded by some polynomial in $k$ only.

Parameterized complexity theory as in (e) relaxes Condition (d) requiring the running time to be bounded in terms of the output precision only; see Example 2(f) and (s) below. Fully polynomial-time computable functions are closed under composition.

Example 2 a) Monotone Convergence Theorem: There exists a computable, monotonically increasing sequence $(x_j) \subseteq [0; 1]$ with incomputable limit $\sup_j x_j$, that is, $(x_j)$ admits no recursively bounded rate of convergence [Spec49].

b) Bolzano–Weierstraß: There exists a computable sequence $(x_j) \subseteq [0; 1]$ such that no accumulation point can be computed even relative to the Halting Problem as oracle [LRZ08 Theorem 3.6].

c) Real-Closed Fields: Sum, product, and inverse of (polynomial-time) computable reals are again (polynomial-time) computable. For every complex polynomial with computable coefficients, all its real roots are again computable [Spec69]. In fact, if the polynomial’s coefficients are polynomial-time computable, then so are its real roots [Scho82].
d) Matrix Diagonalization: Every real symmetric $d \times d$-matrix $M$ with computable entries admits a computable basis of eigenvectors. However such a basis cannot in general be computed from approximations to $M$ only; whereas restricted to non-degenerate $M$ and, more generally, when providing in addition to approximations to $M$ the integer Card $\sigma(M) \in \{1, \ldots, d\}$ of distinct eigenvalues, it can [ZiBr04, §3.5] – and this amount of so-called discrete enrichment is optimal [Zieg12].

e) Power Series: There exists a computable real sequence $\{c_j\}$ whose radius of convergence $R(\mathcal{c}) := 1/\limsup_j |c_j|^{1/j}$ is not computable even relative to the Halting Problem as oracle [ZhWe01, Theorem 6.2]. Moreover power series evaluation $x \mapsto \sum_j c_j x^j$ is in general not computable on $(-R, R)$ [Weih00, Example 6.5.1]; whereas, for every fixed $0 < r < R$, it is computable on $[-r; r]$ [Weih00, Theorem 4.3.12].

f) Some Polynomial-Time Computable Functions: Addition $(x, y) \mapsto x+y$ and multiplication $(x, y) \mapsto x\cdot y$ on the real interval $[-2^k; 2^k]$ are computable in time polynomial in $k+n$, where $n$ denotes the output precision in the sense of guaranteed approximation up to absolute error $1/2^n$. The exponential function (family) on $[-2^k; 2^k]$ is computable in time polynomial in $2^k+n$ but not in time depending only on $n$. Reciprocals $[2^{-k}; \infty) \ni x \mapsto 1/x$ are computable in time polynomial in $k+n$. The square root is computable on $[0; 2^k]$ in time polynomial in $k+n$. The following explicit function is computable in exponential time, but not in polynomial time — even relative to any oracle:

$$h_{\exp} : [0; 1] \to \mathbb{R}, \quad h_{\exp}(0) := 0, \quad 0 < x \mapsto h_{\exp}(x) := 1/\ln(e/x) \quad (2)$$

g) Maxima: For every computable $f : [0; 1] \to \mathbb{R}$, the parametric maximum function $\text{MAX}(f) : [0; 1] \ni c \mapsto \max \{f(t) : 0 \leq t \leq c\}$ is again computable. However there exists a computable smooth $f$ which attains its maximum at (many, but) no computable $x$ [Spec59].

h) Integration: For every computable $f : [0; 1] \to \mathbb{R}$, the indefinite Riemann integral $\int f : [0; 1] \ni x \mapsto \int_0^x f(t) \, dt$ is again computable.

i) Derivatives: There exists a computable $f \in C^1[0; 1]$ with $f'$ non-computable [Myhi71]. Every computable $f \in C^2[0; 1]$ has a computable derivative [Weih00, Corollary 6.4.8].

k) Ordinary Differential Equations: There exists a computable (and thus continuous) $f : [0; 1] \times [-1; 1] \to [-1; 1]$ such that the initial value problem

$$\dot{y}(t) = f(t, y(t)), \quad y(0) = 0 \quad (3)$$

has (many, but) no computable solution $y : [0; 1] \to [-1; 1]$ [PER79]. However if $f$ is computable and Lipschitz, then the (now unique) solution $y$ is again computable.

m) Partial Differential Equations: There exists a computable $f \in C^1(\mathbb{R}^3)$ such that the strong solution $u = u(t, x, y, z)$ to the linear Wave Equation in 3D

$$\frac{\partial^2}{\partial t^2} u = \frac{\partial^2}{\partial x^2} u + \frac{\partial^2}{\partial y^2} u + \frac{\partial^2}{\partial z^2} u, \quad u(0, \cdot) = f, \quad \frac{\partial}{\partial t} u(0, \cdot) = 0 \quad (4)$$

is incomputable at $(1, 0, 0, 0)$ [PER81]. Its Sobolev solution however is computable [WeZi02].

n) Euclidean subsets: There exist compact subsets $A, B \subseteq \mathbb{R}$ with computable distance function whose intersection $A \cap B \neq \emptyset$ has a non-computable distance function [Weih00, Exercise 5.1.15]. There exists a regular compact subset of the plane whose weak membership oracle [GLS93] is polynomial-time computable, while its distance function is so if and only if $P = \text{NP}$ holds [Brav04]. For any convex compact Euclidean subset on the other hand, the computational complexity of its distance function and its weak membership oracle are parameterized polynomially related [Roes15].
o) Maximum values, again: Whenever \( f : [0; 1] \rightarrow \mathbb{R} \) is polynomial-time computable, \( \text{MAX}(f) \) is computable in exponential time and polynomial space. In case \( P = NP \), \( \text{MAX}(f) \) is even polynomial-time computable. Conversely, there exists a polynomial-time computable \( f \in C^\infty [0; 1] \) such that polynomial-time computability of \( \text{MAX}(f) \) implies \( P = NP \) \([Ko91, \text{Theorem 3.7}]\). For analytic functions \( f \), however, \( \text{MAX}(f) \) is polynomial-time computable whenever \( f \) is \([M"ull87]\).

p) Integration, again: Whenever \( f : [0; 1] \rightarrow \mathbb{R} \) is polynomial-time computable, \( \int f \) is computable in exponential time and polynomial space. In case \( \text{FP} = \#P \), \( \int f \) is even polynomial-time computable in polynomial time. Conversely, there exists a polynomial-time computable \( f \in C^\infty [0; 1] \) such that polynomial-time computability of \( \int f \) implies \( \text{FP} = \#P \) \([Ko91, \text{Theorem 5.33}]\). For analytic functions \( f \), however, \( \int f \) is polynomial-time computable whenever \( f \) is \([M"ull87]\).

q) ODEs, again: Whenever \( f : [0; 1] \times [-1; 1] \rightarrow [-1; 1] \) is polynomial-time computable and Lipschitz continuous, then the unique solution \( y \) to Equation (3) is computable in exponential time and polynomial space. In case \( P = \text{PSPACE} \), \( y \) is even computable in polynomial time. Conversely, there exists a polynomial-time computable \( f \in C^1 \) such that polynomial-time computability of solution \( y \) implies \( P = \text{PSPACE} \) \([Kawa10, KORZ12]\). If analytic \( f \) is polynomial-time computable, then so is \( y \) \([M"ull95]\).

r) PDEs, again: Recall the Dirichlet Problem for Poisson’s linear partial differential equation:

\[
    f = \Delta u \quad \text{on } \Omega, \quad u = g \quad \text{on } \partial \Omega.
\]  

(5)

On the Euclidean unit ball \( \Omega \subseteq \mathbb{R}^d \) for polynomial-time computable \( f : \Omega \rightarrow \mathbb{R} \) and \( g : \partial \Omega \rightarrow \mathbb{R} \), the strong solution \( u \) exists and is computable in exponential time and polynomial space. In case \( \text{FP} = \#P \), it is even computable in polynomial time. Conversely, there exist polynomial-time computable smooth \( f, g \) such that polynomial-time computability of \( u \) implies \( \text{FP} = \#P \) \([KSZ15]\).

s) Analytic and Gevrey Functions: For \( \gamma, B, \ell \in \mathbb{N} \) let \( G^{\gamma}_{B,\ell}[0; 1] \) denote the class of all infinitely differentiable functions \( f : [0; 1] \rightarrow \mathbb{R} \) satisfying \( |f^{(j)}(x)| \leq B \cdot \ell^j \cdot j!^\gamma \). Then \( \bigcup_{\ell} G^{\gamma}_{B,\ell}[0; 1] \) coincides with the class of real analytic functions. Moreover (i) evaluation, (ii) addition, (iii) multiplication, (iv) differentiation, (v) integration, and (vi) maximization on \( G^{\gamma}_{B,\ell}[0; 1] \) is uniformly computable in time polynomial in \( (n + \ell + \log B)^\gamma \); and this is asymptotically best possible \([KMRZ15]\).

Items (o) to (r) suggest numerical approaches to famous open problems in discrete complexity theory. From a different perspective, they demonstrate exponential-time behaviour of algorithms for several numerical problems to be optimal subject to said conjectures \([KaOt14]\).

Item (s) ‘explains’ for the phase transition between analytic to smooth functions indicated in Items (o) and (p). It also exhibits parameterized reductions to the actual behaviour of fully-specified algorithms — as opposed to ‘methods’ or ‘recipes’ for a vaguely-defined task such as in the following quote from the NAG library’s documentation:

\[
\text{nag_opt_one_var_deriv(e04bbc) normally computes a sequence of } x \text{ values which tend in the limit to a minimum of } F(x) \text{ subject to the given bounds.}
\]

We particularly promote three concepts from logic that have turned out essential in Real Complexity Theory with consequences for computational practice:
Nonextensional/multivalued Functions: A (total) relation \( f \subseteq X \times Y \) can alternatively be regarded as a partial set-valued mapping \( f : \text{dom}(f) \subseteq X \rightarrow 2^Y \setminus \{\emptyset\} \), sometimes also written as \( f : \text{dom}(f) \subseteq X \Rightarrow Y \) with \( \text{dom}(f) := \{ x \in X : \exists y \in Y : (x,y) \in f \} \), via \( x \mapsto \{ y \in Y : (x,y) \in f \} \). It corresponds to a computational semantics where an algorithm is permitted, given \( x \) encoded in one way, to output some \( y \in f(x) \) but some possibly different \( y' \in f(x) \) when given the same \( x \) encoded in another way. Such non-extensionality models computational search problems well-known in the discrete case. However in the real setting this effect emerges naturally also in subproblems even when computing only single-valued functions; see [Brat96, §2.3.6], [Weih00, Exercise 5.1.13], or [Luck77].

Discrete Enrichment: Many incomputable (single or multivalued) problems \( f : X \Rightarrow Y \) do become computable when providing, in addition to approximations to the arguments \( x \in X \) certain additional information, a concept well-known as enrichment in logic [KrMa82, p.238/239]. In many practical cases it suffices to enrich the given \( x \) with some suitable integer \( k = k(x) \), usually even from a bounded range. For instance according to Example 2(d), only the second line in the following C++ fragment can lead code correctly returning some eigenvector to a given real symmetric \( 2 \times 2 \)-matrix:

```c++
void EV(REAL A11, REAL A12, REAL A22, REAL &EVx, REAL &EVy)
void EV(REAL A11, REAL A12, REAL A22, int degenerate, REAL &EVx, REAL &EVy)
```

Parameterized Complexity: Theoretical Computer Science traditionally considers the worst-case resource consumption in dependence on the binary input length parameter \( n \). In the real realm inputs are infinite, and \( n \) instead denotes the output precision. However in both disciplines additional parameters \( k \) allow for a finer-grained analysis and more realistic predictions; recall Definition 1(e) with Example 2(f) and (s). In the discrete case this leads to the field of Parameterized Complexity. In the real case, condition numbers are (but) one example of a secondary parameter; the complexity analyses of addition and exponential function from the above examples demonstrate also other natural choices. Discrete enrichment often simultaneously serves as a secondary complexity parameter; cmp. Example 2(s).

To conclude, Real Complexity Theory provides a computer-scientific foundation to Numerics bridging from Recursive Analysis to practice. It asserts in a sound setting that common problems with guaranteed precision are surprisingly hard in the worst case, even restricted to smooth functions. On the other hand recipes and methods do work surprisingly well in practice. This gives raise to one among many questions and challenges for future research:

**Challenge 3**

a) Formally capture the class of ‘practical’ functions that renders standard operations (i) to (vi) from Example 2(s) polynomial-time computable.
b) Devise, similarly to Example 2(s), a parameterized complexity theory and reliable implementation of ODE solutions.
c) Identify a suitable notion of resource-bounded computation on Sobolev spaces, and characterizes the complexity inherent to the last line of Example 2(m).
d) Develop a sound computability and complexity-theoretic foundation of recent approaches in numerical engineering to shape and topology optimization.

We close with some programming examples evolving around iterating the Logistic Map:

\[
[0; 1] \ni x \mapsto r \cdot x \cdot (1 - x) \in [0; 1], \quad 1 < r < 4 .
\] (6)
It is well-known to exhibit chaotic behaviour for many values of the parameter $r$ beyond $3.56995$, with the exception of isolated so-called islands of stability for example at $r = 1 + \sqrt{8} \approx 3.82843$. For $r := 15/4 = 3.75$ and $x_0 := 1/2$ and $m = 30, 40, 85, 100, 200, 500, 1000, 10000$, the reader is encouraged to actually run the code fragments below, and to compare the results they produce: in Matlab (left box), Maple (middle), and in C++ (right box) with first line alternatingly replaced by `#define REAL double`, by `#define REAL long double`, and by `#include "iRRAM.h"`. The latter refers to the iRRAM library freely available from http://www.informatik.uni-trier.de/iRRAM/.

```
function y=logistic(m)
    x=1/2; r=vpa(15/4);
    for j=1:m x=r*x*(1-x);
    end; y=x; end
logistic:=proc(m)
    local j,x,r;
    x:=1/2; r:=15/4;
    for j from 1 to m
        do x:=r*x*(1-x)
    end do end proc;
#define REAL float
REAL logistic(int m) {
    REAL x = REAL(1)/REAL(2),
    r = REAL(15)/REAL(4);
    while (m--) x = r*x*(1-x);
    return(x); }
```

References


