Annals of Mathematics and Artificial Intelligence 16(1996)89–152

Back and forth between continuous and discrete for the working computer scientist

Jean-Pierre Reveillès and Denis Richard
LLAIC1, Université d'Auvergne, IUT,
BP 86, 63172 Aubière Cedex, France
E-mail: {reveil, richard}@llaic.univ-bpclermont.fr

This paper gives a perfect, ideal, discretization of continuous notions. This is a very convenient frame to treat continuous problems or theories with the help of a computer. This is illustrated by the conversion of algorithms using real numbers into algorithms using integers only and the founding of discrete geometry.

0. Introduction

It is well known in computer science that using integers when possible, in place of reals in algorithms, leads to faster computations. The problem is that this *code optimization* is rather empirical, lacks precise justification, and is often connected to machine language. In this paper, we shed light on this important question of relations between integers and real numbers in a very unusual but efficient way, following the pioneering work of J. Harthong (see [7]). Our concern is not to give tricks to optimize code, but rather to present a mathematical theory thanks to which many difficult problems concerning conflicts between discrete and continuous encountered in computer science can be studied abstractly. Besides code optimization, which is a mere by-product of our approach, this theory is the first that is able to distinguish, among discrete notions, those which are the closest to their continuous analogue. We illustrate this by building a new *non-Euclidean* geometry, called ideal discrete geometry, which fits exactly the needs of discrete computer screens.

Here are the contents of this approach to finitization in computer science. Section 1 contains the foundations, using a little bit of nonstandard analysis and the

very first applications. To help the reader, we have placed, at strategic places, short texts summing up the essential facts. The first framed text (section 1.1.1) in the beginning sums up the essential properties of infinitely large or infinitely small numbers. Our method is based essentially on a correspondence between integers and reals, explained in 1.1.2 and 1.1.3, a short abstract being placed in 1.1.5. The first application in Euler's method with infinitesimal steps 1.2.2, 1.2.3 leading to the fast algorithm used to compute the exponential presented in the program CompExpo. As a second application, we look at Bresenham's algorithm in a straightforward way from the programs given for the exponential.

Section 2 gives a brief overview of both the main constructions used to build nonstandard models of arithmetic and of our discretization process allowing the use of integers as a tool for creating algorithms.

Section 3 briefly recalls the numerous conflicts that exist between discrete and continuous in computer science even if we restrict ourselves to geometry.

In section 4, we begin to solve these difficult questions by constructing a discrete geometry for computers. This is much more ambitious than the first applications of section 1, even if we mainly rely on the principles enunciated there. Contrary to former approaches to discrete geometry (cf. [1,3,23]), we first build, using infinitely large integers, an *ideal discrete geometry* which is infinitely close to classical Euclidean geometry. In this way, our theory inherits the most from its continuous cousin.

Ideal discrete geometry clearly shows the interest of *thickness* for ideal lines; we use this notion to define the main object of standard discrete geometry: discrete lines. This is done in section 5, where an arithmetical definition of computer discrete lines deriving naturally from ideal lines is given with numerous interesting consequences. More precisely, we connect our discrete lines with classical lines (Bresenham's notion); we show they are related to modular calculus, give formula describing their structure, connect them to quadratic residues, and finally give a non-vacuity condition for their intersecting.

1. A general discretization: Computing with integers

To create algorithms which solve a given problem, the first step consists of an investigation using ideal tools such as reals, real functions or numerical analysis notions. At first, using the floating point might seem an easy solution, but it is well known that this costs time and requires an arithmetical co-processor. Anyway, reals are both practical and common tools: every scientist knows enough about their properties to compute with them.

Alternatively, the working computer scientist knows that using integers can result in faster algorithms, if one can write programs developed in integers. Now, to formalize the scales between integers, it would be very convenient to have the possibilities of:

- expressing the notion that some integers are extremely large compared to others;
- expressing the notion that the real inverses of large integers are extremely small;
- keeping the good properties of positive integers (say the existence of a minimum for every non-empty set of positive integers, or all properties of addition, multiplication, division and order).

1.1. INFINITE INTEGERS FOR ARITHMETIZATION

1.1.1. If infinite large integers could exist

To be a little more precise but still from an informal point of view, we keep the set $\mathbb{N}$ of positive integers and we postulate the existence of a set *INFI* of positive infinite integers determined by the following condition: α is a positive infinite if and only if $\alpha > n$ for all $n \in \mathbb{N}$. From the very definition of the positive infinite integer α, the infinitesimal $1/\alpha$ satisfies

$$\forall n \in \mathbb{N} \setminus \{0\} \quad \left(\frac{1}{\alpha} < \frac{1}{n}\right).$$

Consequently, we can extend this definition by deciding that a real ε will be infinitesimal if and only if ε verifies

$$\forall n \in \mathbb{N} \setminus \{0\} \quad \left(\varepsilon < \frac{1}{n}\right).$$

The properties given in the frame below are intuitive and we shall make free use of them. For the moment, we are not concerned with the problem (investigated in section 2) of defining and introducing these objects within a theory. If x and y are reals such that $|x - y|$ is infinitesimal, then we write out $x \simeq y$.

Nevertheless, we can observe right now how to use these for writing out mathematical solutions to get programs in integers allowing a certain kind of curves, namely those which are solutions to differential equations, to be computed.

Suppose that we can reasonably define the union $M = \mathbb{N} \cup INFI$ of the usual integers with the above introduced set *INFI* consisting of elements $\alpha > n$ for all n of $\mathbb{N}$. Suppose also that we can structure $\mathbb{N} \cup INFI$ in such a way that all usual properties of $\mathbb{N}$ concerning the operations of addition, multiplication and division hold.

Verifying these usual properties together with the previous conditions provides a first and informal approach to conditions that will be imposed on M to develop the usefulness of infinite integers. As mathematicians construct $\mathbb{Z}$, the set of positive and negative integers, from $\mathbb{N}$, we admit that our set M of (old and new) integers

If α and β are *positive infinities*, if n, m and p are usual *positive integers* of $\mathbb{N}$, if ε and δ are real positive inverses of infinite integers – which we call *infinitesimal* –, then the following are *infinitesimals*:

$$-\varepsilon,\ \frac{1}{\alpha},\ \frac{\varepsilon}{n},\ \frac{\varepsilon}{\alpha},\ \frac{n}{\alpha},\ \varepsilon+\delta,\ \varepsilon-\delta,\ \varepsilon.\delta,\ n.\varepsilon,\ \sqrt[p]{\varepsilon}\,.$$

The following *are not infinitesimals and not infinite*:

$$-n,\ \frac{1}{n},\ \frac{n}{m},\ n+\varepsilon,\ m.n,\ \sqrt[p]{n},\ m+n.$$

(We shall freely use the word *finite* for such numbers in the first section, before coming to a more precise presentation of these objects.) The following can belong to the set of *infinitesimals*, or to the set of *finite* numbers which are not infinitesimals, or can be *infinite*:

$$\frac{\varepsilon}{\delta},\ \frac{\alpha}{\beta},\ \alpha.\beta,\ \alpha-\beta.$$

Frame 1.

can be embedded by symmetrization in a set $\mathbb{Z}(M)$ of (old and new) positive and negative integers containing $\mathbb{Z}$. Moreover, and in the same way as we construct the set $\mathbb{Q}$ of rationals from $\mathbb{Z}$ and the set $\mathbb{R}$ of reals from $\mathbb{Q}$, we admit the existence of a set of (old and new) rationals $\mathbb{Q}(M)$ containing $\mathbb{Q}$, constructed from $\mathbb{Z}(M)$ and the existence of a set of (old and new) reals $\mathbb{R}(M)$, which is the topological completion of $\mathbb{Q}(M)$ and contains the usual set of reals $\mathbb{R}$. This set $\mathbb{R}(M)$ verifies (in a certain sense to be explained later in section 2.2) most of the usual properties of the usual set $\mathbb{R}$ of reals.

1.1.2. Arithmetization of reals

Now, we want to code all (old and new) reals by (old and new) integers in such a way that the chosen correspondence mapping $\mathbb{R}(M)$ on $\mathbb{Z}(M)$ preserves the operations. We denote by $[\alpha]$ the integral part of the real α, namely the greatest integer of M smaller than α. In order to do this, we fix an infinite integer $\omega \in M \setminus \mathbb{N}$ and we define the function IC_ω (integer code on scale ω) as follows:

$$IC_\omega : \mathbb{R}(M) \to \mathbb{Z}(M)$$

$$x \to [\omega x].$$

Conversely, the decoding correspondence CR_ω (for coded real on scale ω) is the function determined as follows:

$$CR_\omega : \mathbb{Z}(M) \to \mathbb{R}(M)$$
$$x \to \frac{x}{\omega}.$$

In our situation, the kind of inversibility that we need is an extension of the normal one. In fact, it is only necessary for the inverse image of the range of an element x to be infinitesimally close to x. In that case, we shall say that a function has a *pseudo-inverse*. We see that IC_ω and CR_ω are mutually pseudo-inverse, since

$$IC_\omega \circ CR_\omega(x) = \left[\omega \frac{x}{\omega}\right] = x$$

and also

$$CR_\omega \circ IC_\omega(x) = \frac{[\omega x]}{\omega} = \frac{\omega x - d}{\omega} = x - \frac{d}{\omega}$$

for some d such that $0 \leq d < 1$.

We observe that $|CR_\omega \circ IC_\omega(x) - x| = d/\omega$ is infinitesimal so that $CR_\omega \circ IC_\omega(x)$ is infinitesimally close to x (denoted $CR_\omega \circ IC_\omega(x) \simeq x$) and so that IC_ω and CR_ω are pseudo-inverse mappings. They will be convenient tools for programming in integers.

Figure 1 shows the mutual situation of standard and nonstandard reals: near each standard real, we can find the reals that are infinitesimally close to it; one can see the infinite reals that are larger and smaller than a standard real; similarly, integers of the usual $\mathbb{Z}$ have smaller infinite integers below them and larger infinite integers above them. The coding devices that we use are based on a correspondence between reals and integers via homothety having as ratio a fixed infinite integer ω.

1.1.3. Arithmetization of operations

At this step, we would like the previous integer codes to preserve their usual operations. For this purpose, we first introduce a notion of indiscernibility within $\mathbb{Z}(M)$: we say that a and b are ω-indiscernible integers if and only if one has $\forall n \in \mathbb{N}$ $(n|a - b| < \omega)$. We denote ω-indiscernibility of a and b by $a \approx b$, a notation which is not to be confused with $x \simeq y$, for which the reader is reminded that $|x - y|$ is infinitesimal. It is important to note that

$$x \approx y \text{ if and only if } CR_\omega(x) \simeq CR_\omega(y).$$

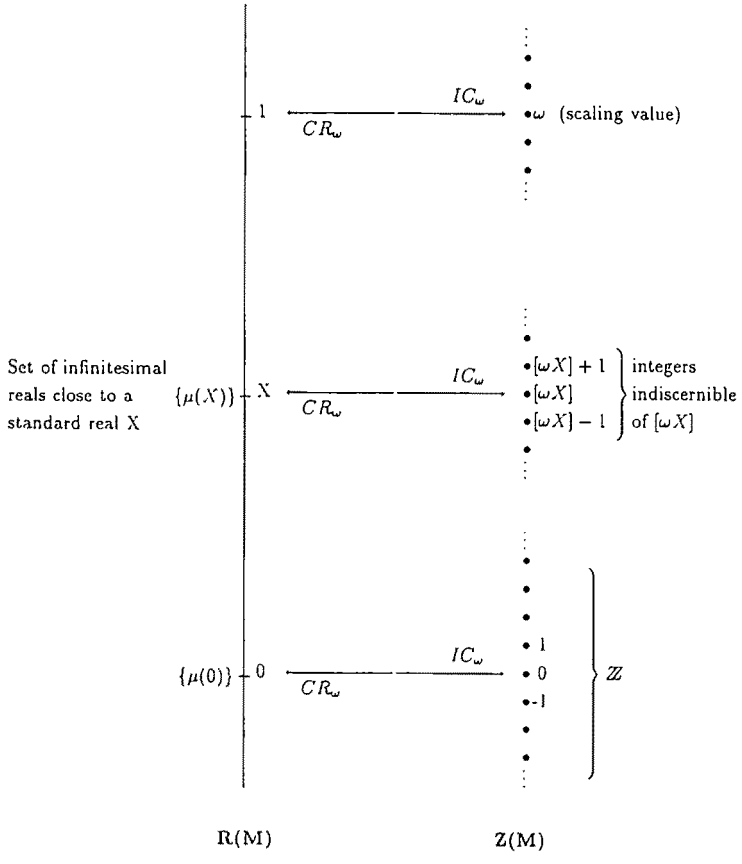


Fig. 1. The principle of arithmetization associates integer $[\omega x]$ to real number x; this is map IC_ω. Reciprocally, CR_ω maps integer n to the real number n/ω. Using the good properties of infinite integers, this mapping acts as if it were a *bijection*.

Since we have for all reals x and y of $\mathbb{R}(M)$ the usual inequalities

$$[\omega x] + [\omega y] < [\omega x + \omega y] < [\omega x] + [\omega y] + 2,$$

we get the following indiscernibilities:

$$IC_\omega(x) + IC_\omega(y) \approx IC_\omega(x + y),$$
$$IC_\omega(x) - IC_\omega(y) \approx IC_\omega(x - y).$$

In order to arithmetize, we need a multiplication on $\mathbb{Z}(M)$, say $\otimes$, such that for all reals x and y

$$IC_\omega(x) \otimes IC_\omega(y) \approx IC_\omega(xy).$$

The following map from $\mathbb{Z}(M) \otimes \mathbb{Z}(M)$ into $\mathbb{Z}(M)$ determined by $(x, y) \to [xy/\omega]$ is a natural and convenient candidate to take for the desired product $\otimes$.

As an exercise, we prove that for every pair $(x, y) \in \mathbb{Z}(M) \times \mathbb{Z}(M)$ and every pair $(x, y) \in \mathbb{R}(M) \times \mathbb{R}(M)$ the following relations of indiscernibility hold:

$$CR_\omega(x) \times CR_\omega(y) \simeq CR_\omega(x \otimes y), \tag{1}$$

$$IC_\omega(xy) \approx IC_\omega(x) \otimes IC_\omega(y). \tag{2}$$

For (1), we note that

$$CR_\omega(x) \times CR_\omega(y) = \frac{xy}{\omega^2}$$

and

$$CR_\omega(x \otimes y) = \frac{1}{\omega}\,\frac{xy}{\omega};$$

from the equality

$$\frac{xy}{\omega^2} - \frac{1}{\omega}\left[\frac{xy}{\omega}\right] = \frac{1}{\omega}\left(\frac{xy}{\omega} - \left[\frac{xy}{\omega}\right]\right) = \frac{\delta}{\omega} \quad \text{with } 0 \le d < 1,$$

it follows that δ/ω is infinitesimal. For (2), we have

$$IC_\omega(x) \otimes IC_\omega(y) = [\omega x] \otimes [\omega y] \approx \left[\frac{\omega x\, \omega y}{\omega}\right] = [\omega xy] = IC_\omega(xy),$$

proving the desired relation.

An adequate division, denoted //, providing a suitable arithmetization of reals must satisfy the following two conditions:

$$\frac{CR_\omega(x)}{CR_\omega(y)} \simeq CR_\omega(x//y), \tag{3}$$

$$IC_\omega\left(\frac{x}{y}\right) \approx IC_\omega(x)//IC_\omega(y), \tag{4}$$

the last one being true if y is not indiscernible with 0.

The following choice $x//y = [\omega x/y]$ is a convenient one. As a new exercise on infinite and infinitesimal, let us prove (3). We have

$$CR_\omega(x//y) = \frac{1}{\omega}\left[\frac{\omega x}{y}\right]$$

and

$$\frac{CR_\omega(x)}{CR_\omega(y)} = \frac{x}{\omega} \Big/ \frac{y}{\omega} = \frac{1}{\omega}\,\frac{\omega x}{y}$$

so that

$$CR_\omega(x//y) - \left[\frac{CR_\omega(x)}{CR_\omega(y)}\right] = \frac{1}{\omega}\left[\left[\frac{\omega x}{y}\right] - \frac{\omega x}{y}\right] = \frac{\delta}{\omega}$$

for some $\delta \in [0, 1]$, proving (3). The proof of (4) is analogous and left to the reader.

1.1.4. Usefulness of infinite integers as ideal objects

Our purpose is to program in integers to speed-up the implementation of algorithms by avoiding the floating point of real representations. First, we observe that the working computer scientist, looking for a solution to a given problem, begins by writing out the mathematical treatment usually connected to a numerical analysis. In so doing, he uses ideal objects such as reals. Of course, reals do not exist (the very name itself could be an historical ruse organized against computer scientists), since there is an infinite amount of information in most of them. Also, because of this infinity of elements defining a unique real, properties within real analysis are very sophisticated (for example, say the upper bound property). On the other hand, properties of integers often seem straightforward, and especially when we think about the possibility of using inductive methods. It is very convenient to possess a choice function giving the smallest integer satisfying a fixed property. Moreover, the possible inductive definitions in the framework of usual arithmetic are very close to recursivity, and to the process of incrementation and decrementations.

Retaining only the following two ideas out of many others:

(a) computing rapidly and being cost-efficient by saving time;

(b) helping the heuristic search for solutions having the simplest models of the lightest ideal objects, we want to develop in section 2 examples of such solutions in infography.

Before ending this section, we must make a few remarks.

Remark 1

We do think that a formal, in a certain sense, exhaustive axiomatization within any suitable set theory is intractable, of no use to non-logicians and unsuitable for popularizing among computer scientists the new method of finitization that we are developing in this work. Actually, while we have no desire to present our ideas on this, it is formally possible to consider definitions and results written

out in the first frame concerning the infinitesimal as axioms. This was done by J. Kiesler in [9], or in a more precise and sophisticated way by E. Nelson (cf. [11]). It seems that it is better for us to present informal properties leading to ideal objects which we have to set to work on immediately to create algorithms. In section 2, we prefer to take a semantical point of view consisting of describing sets of new objects (say infinite integers) in the usual mathematical structures which are taken as models for theories by logicians. Such a set is $\mathbb{N} \cup INFI$ that we defined above, and described from outside instead of giving a formal axion satisfied by this set (see [19,20]).

Remark 2

In section 3, we shall try to give some proofs of the existence of the new (so-called nonstandard) objects as a consequence of the ambiguity of formal languages. This ambiguity of first-order languages is well known within computer science. From both a semantical and syntactical approach, it is easy to give an external description of infinite integers and infinitesimal reals. To deal with regular curves, little knowledge of these new elements is required. Experience of working with them provides the best way of looking more deeply into the so-called nonstandard analysis.

Remark 3

Some authors, such as J.H. Kiesler (see [9]) in the USA or M. Diener (see [5] and G. Reeb, make attempts to introduce nonstandard methods into the background of students in their first two years of university education. Physicists and other scientists seem interested in beginning the study of Nonstandard Analysis, which is the rigorous account of Leibnitz's *Analysis Infinitorum*. With the help of this theory, limits are computed algebraically (see 2.1.2 for a very simple example). This tool is both natural and cheap for computing, and close to the object phenomena observation that is to be modelized. Imagining solutions with simple concepts results in faster thought processes without artefacts due to complicated notions.

1.1.5. Abstracts of arithmetization of reals by finite and infinite integers

Our arithmetization principle is illustrated in fig. 2, where real numbers r and s are sent, by IC_ω, onto integers $[\omega r]$ and $[\omega s]$.

Algebraic remarks

- $(\mathbb{Z}(M)/\approx, +, .)$ is a ring
- The set of finite (usual or not, i.e. standard or nonstandard) reals $\mathbf{F} \subset \mathbb{R}(M)$ is determined by:

$$\mathbf{F} = \{r \in \mathbb{R}(M) \mid \exists \alpha \in \mathbb{R}^+(|r| \leq \alpha)\}.$$

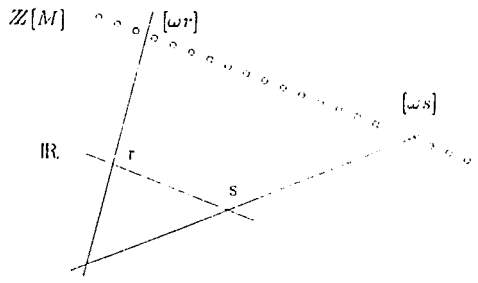


Fig. 2. ω-enlargement of the usual $\mathbb{R}$ in the set of infinite coding integers $\mathbb{Z}(M)$.

- By $\mu(0)$, we mean the set of infinitesimals.
- We can (easily) prove, but it is not at all used in this paper, the following statement:

$$\frac{\mathbb{Z}(M)}{\approx} \text{ is a ring isomorphic to } \mathbf{F}/\mu(0).$$

Our method is summarized in frame 2.

Coding devices of usual $\mathbb{R}$
Integer Code $IC_\omega(x) = [\omega x]$
Coded Real $CR_\omega(X) = X/\omega$
Formulas of pseudo-inversibility
$IC_\omega \circ CR_\omega(X) = X$
$CR_\omega \circ IC_\omega(x) \simeq x$
Addition $(X, Y) \mapsto X + Y$
Subtraction $(X, Y) \mapsto X - Y$
Product $(X, Y) \mapsto [XY/\omega]$
Division $(X, Y) \mapsto [\omega X/Y]$
ω-indiscernibility $X \approx Y \Leftrightarrow |X - Y|/\omega \approx 0$

Frame 2.

This principle will be very useful to obtain discretization for more complicated objects, functions, geometric objects, etc. The latter will be considered in sections 3, 4 and 5 with the aim of considering them as the pieces of a discrete geometry.

Let us consider, for example, the function $f : \mathbb{R} \to \mathbb{R}$; the former principle leads to function $F : \mathbb{Z} \to \mathbb{Z}$ given by $F(n) = [\omega f(n/\omega)]$, which is what we mean by $IC_\omega(f)$. This can, of course, be generalized to any number of variables.

1.2. FIRST ALGORITHMS

As we said before, algorithms are usually expressed within the framework of the floating point. In order to avoid such reals and to accelerate the running of programs, we are going to arithmetize computations using rudimentary tools described in section 1.1.

1.2.1. An example of arithmetization in analysis

(*This is not a necessary result for the rest of this paper.*) We add to our new objects the so-called nonstandard functions f from $\mathbb{R}(M)$ into itself and we ask the reader to accept the last natural property, namely the fact that the restrictions of f to the usual set $\mathbb{R}$ is continuous if and only if:

$$x \simeq y \Rightarrow f(x) \simeq f(y).$$

As an example, we prove the classical theorem of intermediate values.

THEOREM 1.1

If f is defined and continuous on a segment $[a, b]$ and if $f(a) < 0 < f(b)$, then there exists a real $c \in [a, b]$ such that $f(c) = 0$.

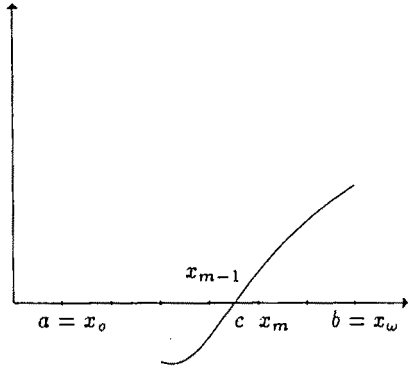


Fig. 3. The intermediate value theorem is easily proved with nonstandard analysis.

Proof

Let ω be an infinite integer. We consider points $x_i = a + (i/\omega)(b-a)$. Note that x_i and x_{i+1} are infinitesimally close. Let A be the set $\{i \in M \mid f(x-i) \geq 0\}$; since $b = x_\omega$, the set A is nonempty. *Here we can use methods of arithmetic – instead of the property of the upper bound of reals* – and take the minimum of A. Denote $\min(A)$ by m; from $f(x_0) = f(a) < 0$, we see that $m > 0$. Since $f(b) > 0$, we have $a < x_m < b$. Denote by c the unique usual (i.e. standard) real which is infinitesimally close to x. Because f is continuous, $f(x_m)$ and $f(c)$ are also infinitesimally close. Consequently, we have for infinitesimals ε and ε'

$$f(x_m) = f(c) + \varepsilon \quad \text{and} \quad f(x_{m-1}) = f(c) + \varepsilon'$$

so that, using the very definition of x_m which implies $f(x_{m-1}) < 0$, we have $-\varepsilon < f(c) < \varepsilon'$. We observe that $f(c)$ is a usual (standard) real bounded by two infinitesimals. Now all we have to do is to consider all possibilities of sign for ε and ε' and to use the property that infinitesimals are smaller than every number $1/n$ for all $n \in \mathbb{N}$ to deduce that $f(c)$ is 0, what we wanted to prove. □

Let us notice that each limited real number x is always infinitely close to a standard real number, called its standard part, denoted by $st(x)$ or ${}^o x$. We shall explain this operation in more detail in section 2.2.2. Moreover, we would encourage the reader to study also nonstandard analysis in the historical book of A. Robinson (see [22]) and also the books referenced in [2] and [5].

1.2.2. Euler's method with infinitesimal step

(*Fundamental result for the following algorithm.*) We shall make extended use of the following well-known device, which consists of confusing curve and its tangent. Figure 4 shows the situation with an infinitesimal step since the integer ω is chosen as infinite.

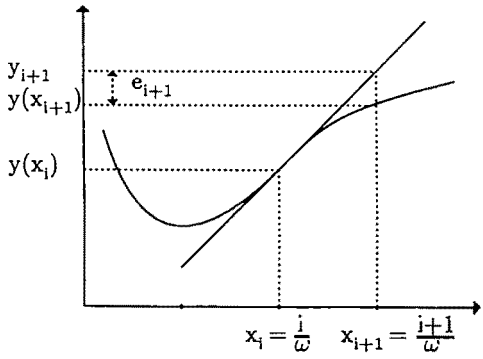


Fig. 4. Euler's integration of differential equations.

More precisely, we claim that the slope of the line passing through the points $(x_i, f(x_i))$ and $(x_{i+1}, f(x_{i+1}))$ is infinitesimally close to the slope of the tangent at $(x_i, f(x_i))$ which is $y'(x_i)$:

$$\frac{y(x_{i+1}) - y(x_i)}{1/\omega} = y'(x_i). \qquad (*)$$

With the notations in fig. 4, the error is $e_i = |y_i - y(x_i)|$ by definition.

Now suppose that the curve is determined by a differential equation $y'(x) = f(x, y(x))$ and some initial condition. For a fixed ω and using the relation (*), the previous differential equation *provides a finite difference equation, in integers,* which can be obtained by the following lines. By definition of the sequence $x_i = i/\omega$, we first have, using (*),

$$\frac{y(i + 1/\omega) - y(i/\omega)}{1/\omega} = f\left(\frac{i}{\omega}, y\left(\frac{i}{\omega}\right)\right)$$

or, multiplying by ω

$$\frac{\omega/(i + 1/\omega) - \omega y(i/\omega)}{1/\omega} = \omega f\left(\frac{i}{\omega}, y\left(\frac{i}{\omega}\right)\right).$$

Integer coding for functions leads us to introduce $Y(i) = IC_\omega(y(x))$ and $F(i, j) = IC_\omega(f(x, y))$; thus, the last equation finally gives the difference equation

$$Y(i + 1) - Y(i) = \frac{1}{\omega} F(i, Y). \qquad (1)$$

This is the key point of this arithmetization: to reach, from a differential equation (written out by Euler's method with an infinitesimal step), a recursive definition of the considered curve leading to straightforward program computing values. This program will be obtained using properties of integers such as ω-expansion, Euclidean division and the determination of remainders. In so doing and contrary to floating point programming, we shall "manage" remainders. The infinite character of ω has at least three virtues:

- it allows rigorous proofs in the frame of nonstandard analysis,
- it has heuristic advantages by letting the scientist imagine solutions in a discrete way (instead of using continuous notions),
- finally, it is sufficient to decree that ω is a usual large enough integer (128, 256, 2^n,...) to force our equation to produce the desired program.

Frame 3.

Then eq. (1) can be converted into a concrete recursive definition using *bounded integers*. We generally write integer sequence $Y(i)$ with two digits in radix

ω, giving $Y(i) = C_i\omega + D_i$ and function $F(i, Y(i))$ in the same way with two or more digits. Identifying corresponding digits in both members gives recursive definitions for all digits.

Let us explain this using a very simple example.

1.2.3. A first arithmetized algorithm of the exponential (G. Reeb [12])

The function $y = \exp x$ is the solution of $y'(x) = y(x)$ with $y(0) = 1$. We fix an infinite ω and so we have $\omega \in \mathbf{M} \setminus \mathbb{N}$. From the method just developed in section 2.2, it follows that

$$y\left(\frac{i+1}{\omega}\right) - y\left(\frac{i}{\omega}\right) \simeq \frac{1}{\omega} y'\left(\frac{i}{\omega}\right) = \frac{1}{\omega} y\left(\frac{i}{\omega}\right).$$

Putting $y(i/\omega) = y_i$, we obtain

$$\omega y_{i+1} - \omega y_i \simeq y_i. \tag{2}$$

From $\omega y_i = [\omega y_i] + r_i$ for $0 \leq r_i < 1$, it follows that $R_i = [\omega r_i] = IC_\omega(r_i)$ and by pseudo-inversibility on the one hand, $r_i \simeq R_i/\omega = CR_\omega(R_i)$ and, on the other hand, $y_i \simeq CR_\omega(Y_i) = Y_i/\omega$ from $Y_i = [\omega y_i] = IC_\omega(y_i)$. Formula (2) can be rewritten in integers as follows:

$$Y_{i+1} + \frac{R_{i+1}}{\omega} \simeq Y_i + \frac{R_i}{\omega} + \frac{1}{\omega}\left(Y_i + \frac{R_i}{\omega}\right). \tag{3}$$

Since $1/\omega^2$ is infinitesimally smaller than $1/\omega$, we can neglect R_i/ω^2 so that eq. (3) becomes

$$Y_{i+1} + \frac{R_{i+1}}{\omega} \simeq Y_i + \frac{R_i}{\omega} + \frac{Y_i}{\omega}. \tag{4}$$

From the inequality $0 \leq r_i < 1$, it follows that $R_i < \omega$ and

$$\begin{cases} Y_{i+1} = Y_i + \left[\dfrac{Y_i + R_i}{\omega}\right], \\ R_{i+1} = \left\{\dfrac{Y_i + R_i}{\omega}\right\}, \end{cases}$$

where, for an integer x, we denote the rest of Euclidean division of x by ω by $\{x/\omega\}$, the quotient being, as usual $[x/\omega]$.

Finally, to get the desired algorithm and to write out the corresponding program in PASCAL, we simply have to add Y_0 and R_0 initializations, for example, $Y_0 = R_0 = 0$.

Now, it is time for our *coup* and to decide that, in practical applications, the infinite character of ω is attributed to some integers or, for computing convenience, to some fixed power of 2, say $\omega = 2^7 = 128$ or $\omega = 2^{16}$ or other.

Table 1

	Y	Rest	DY
i	y_i	R_i	
$i+1$	$y_i + [R_i + y_i/128]$	$\{R_i + y_i/128\}$	Δy_i
0	128	0	1
1	129	0	1
2	130	1	1
3	131	3	1
4	132	6	1
5	133	10	1
6	134	15	1
7	135	21	1
8	136	28	1
9	137	36	1
10	138	45	1
11	139	55	1
12	140	66	1
13	141	78	1
14	142	91	1
15	143	105	1
16	144	120	2
17	146	8	1
18	147	25	1
19	148	43	1
20	149	62	1
21	150	82	1
22	151	103	1
23	152	125	2
24	154	20	1
25	155	44	1
26	156	69	1

In table 1, which gives a trace of this algorithm (where Δy_i is the difference $y_{i+1} - y_i$), we observe jumps in values for $i = 17$ and $i = 24$. The column entitled Rest (containing R_i values) shows that we have control over the remainders modulo 128. This is one difference, among many, between the two treatments (namely, floating point and computation in integer).

TEST 1

Reveillès used $\omega = 2^{16}$ on an INTEL 80286 microprocessor running at 10 Mhz; the computation provides 32000 values with 10 significant digits in 0.6 seconds.

TEST 2

Diener, on an INTEL 80386 with 10 Mhz and $\omega = 2^{16}$ obtained 8000 values of e^x in 0.25 seconds.

N.B. The previous results, and almost everything done in this area, are the work of researchers at IRMA in Strasbourg (see [13–17, 12, 24]).

Finally, we are in a position to write out the corresponding program in PASCAL.

```
Program CompExpo;
Const unit=128;
Var Y,i,rest:Integer;
begin
    Y := unit;
    Rest := 0;
    for i := 0 do unit do
        begin
            Y := Y + (Y + rest) div unit;
            rest := (Y + rest) mod unit;
        end;
    write(Y/unit:10:5)
end.
```

Program for computing exponentials.

Even if we use *div* and *mod* operations, these have been rewritten to coincide with Euclidean quotient and rest. We use these operations in this PASCAL program for pedagogical reasons, the main loop being only two lines long. But in actual programs we eliminate them, to increase speed, and replace them by tests followed by additions.

1.2.4. *Arithmetized algorithm of the exponential revisited by using ω-expansions of integers*

Integers R_i are bounded by ω; if we neglect R_{i+1}/ω and R_i/ω, eq. (4) is transformed into $Y_{i+1} \approx Y_i + Y_i/\omega$, which can also be expressed by

$$\omega Y_{i+1} \approx \omega Y_i + Y_i. \tag{5}$$

It must be emphasized that the great advantage of the last recursion equation resides in the actual fact that we use *the numeration of basis ω*. This is just a come back to the paradise of integers: the reader is reminded that reals are nothing else but sums of numerical infinite series. We note that using ω-expansions, we can write

$$\begin{cases} Y_i = C_1\omega + C_0, \\ Y_{i+1} = C_1'\omega + C_0', \end{cases} \tag{6}$$

where C_0, C_1, C_0' and $C_1' \in [0, \omega[$ are numerals of the basis ω. We observe that we can compute the ω-digits C_0' and C_1' from $\omega Y_{i+1} = C_1'\omega^2 + C_0'\omega$. Using the unicity of ω-expansions for ωY_{i+1} and (6), we obtain

$$C_0' = \left\{\frac{C_0 + C_1}{\omega}\right\},$$

$$C_1' = C_1 + \left[\frac{C_0 + C_1}{\omega}\right].$$

It is straightforward to write out a program computing exponentials from the two previous equations.

1.2.5. Retrieving Bresenham's algorithm

The straight line with equation $y(x) = \alpha x + \beta$ is the solution of the elementary differential equation $y'(x) = \alpha$ such that $y(0) = \beta$. The previous work done in section 1.2.3 for the general differential equation applies immediately to this case. We will nevertheless introduce a slight modification in our discretization process, introducing

$$Y_i = \left[\omega^2 y\left(\frac{i}{\omega}\right)\right] \quad \text{and} \quad A = [\omega\alpha] \quad \text{and} \quad B = [\beta\alpha],$$

leading to the relation

$$Y_{i+1} = Y_i + A.$$

Consequently, if we develop Y_i and Y_{i+1} in radix ω as

$$Y_{i+1} = C_1'\omega + C_0' \quad \text{and} \quad Y_i = C_1\omega + C_0,$$

we immediately obtain the following recursive equations in integers of this line:

$$\begin{cases} C_1 = C_1 + \left[\dfrac{C_0 + A}{\omega}\right], \\ C_0 = \left\{\dfrac{C_0 + A}{\omega}\right\}. \end{cases}$$

The initial value of sequence C_1 is taken to be equal to B. It is rather obvious to see that the values of sequence C_1 are also the same as those given by the sequence $[Ai/\omega] + B$. This sequence can be geometrically interpreted as the integer points immediately below the line with equation $y = (A/\omega)x + B/\omega$. This kind of point set, which we call discrete lines, will be studied in greater detail in sections 4 and 5 in

order to build a rigorous discrete geometry. Just to give an idea of the kind of problems we will develop in these sections, let us admit that if we change C_0''s initial condition by a value ε, then we just translate slightly the discrete line. And this parameter ε can be adjusted such that the sequence given by $C_i = [(Ai + \varepsilon)/\omega] + B$ satisfies other constraints. For example, if $\varepsilon = [\omega/2]$, this formula gives the integer points which are the closest to the former line; this is exactly Bresenham's line.

```
Program CompLine;
Var a, Y, i, rest, unit: Integer;
    begin
        write('a='); readln(a);
        write('b='); readln(b);
        write('unit='); readln(unit);
        rest := (unit div 2);
        Y := b;
        for i := 1 to unit do
            begin
                write(Y:5);
                Y := Y + (rest+a) div unit;
                rest := (rest+a) mod unit;
            end;
    end.
```

Program for drawing discrete lines.

Remarks

(1) It is easy to remove the DIV and MOD operations appearing in the loop by an inequality test followed by an IF...THEN...ELSE instruction (this is done in section 4.1.2).

(2) It is important to note that the program for computing exponentials provides in a straightforward manner a program that is equivalent (after execution) to Bresenham's for drawing lines.

(3) As an exercise, the reader may like to write out programs for computing *logarithms* (from the equation $Y_{i+1} - Y_i = \omega^2/i$), for computing *square roots* (from the equation $Y_{i+1} - Y_i = a/\omega Y_i$), *circles* from the differential system

$$\begin{cases} x'(t) = -y(t), \\ y'(t) = x(t), \end{cases}$$

which leads to the recursive integer equations

$$\begin{cases} X_{i+1} = X_i + Y_i/\omega, \\ Y_{i+1} = Y_i - X_i/\omega. \end{cases}$$

We must remark that this algorithm for drawing circles does not give the Bresenham circle built with the closest integer points to a real circle.

These applications of infinite integers used as tools for writing out integer programs conclude the present section. Of course, it is time to prove the existence of such objects that provide such efficient tools. This is done step-by-step below (see section 2). First, we show some situations where limitations of languages surprisingly provide a first notion of infinite integers. Then we try to show how our previous sets M and $\mathbb{Z}(M)$ and $\mathbb{Q}(M)$ and $\mathbb{R}(M)$ work. Avoiding presentation in the Nelson axiomatic way (within an extended and new set theory), we prefer to attempt a mathematical description of somehow familiar structures.

2. One possible arithmetization through model theory and nonstandard analysis

2.1. USING A BIT OF MODEL THEORY

2.1.1. Use of ambiguity of some formal "characterizations"

To give to a machine a precise definition of the *set of natural integers structured by its usual successor function*, it first seems convenient to note that the structure $\langle \mathbb{N}, 0, x \mapsto x+1 \rangle$ satisfies, with $S(x) = x+1$, the following conditions:

A1. $\forall x(S(x) \neq 0)$.

A2. $\forall x \exists y(y = S(x)) \wedge \forall x \forall y(x \neq y \Rightarrow S(x) \neq S(y))$.

A3. $\forall x(x \neq 0 \Rightarrow \exists y(x = S(y)))$.

We observe that these properties are expressed in a formal language including, in addition to usual logic symbols and identity, two specific symbols, namely a constant symbol (say 0) and a function symbol (say S). Since quantifications affect only one type of elements, this language will be called first-order language. Condition A1 means that 0 does not follow on from any element; from A2, we know that the successor is functional and one-to-one; finally, A3 means that every integer that is different from 0 is a successor of some integer. A more precise investigation of these necessary conditions is sufficient to see that they do not characterize (up to isomorphism) the structure $\langle \mathbb{N}, 0, x \mapsto x+1 \rangle$, as we can prove immediately. Let A be the set $(\mathbb{N} \times \{1\}) \cup (\mathbb{Z} \times \{2\})$ and let Σ be a (successor) function defined by

$$\Sigma(x,1) = (x+1,1) \quad \text{and} \quad \Sigma(x,2) = (x+1,2).$$

The set A can be drawn as follows:

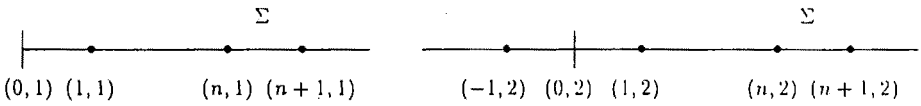


Fig. 5.

This set with successor function Σ and $(0, 1)$ as an interpretation of the symbol 0 satisfies the theory consisting of the three conditions {A1, A2, A3} when we replace S by Σ. Since A and $\mathbb{N}$ are obviously isomorphic, theory {A1, A2, A3} has non-isomorphic models (we say that this theory is not categorical) and, consequently, structure $\langle \mathbb{N}, 0, x \mapsto x + 1 \rangle$ is not characterized at all. Besides, it can be shown in mathematical logic that there is no possible characterization of natural integers equipped with the usual successor function in the frame of first-order logic. We shall say that $\langle A, (0, 1), \Sigma \rangle$ is a nonstandard model of {A1, A2, A3}, while $\langle \mathbb{N}, 0, x \mapsto x + 1 \rangle$ will be conveniently called the standard model. Considering the embedding $n \mapsto (n, 1)$, we see that, up to isomorphism, natural integers form an initial segment of A. To formalize this notion of an *initial segment*, we add to the language {0, S} a symbol for an order relation, say R, and we add to theory {A1, A2, A3} a new axiom, say A4, expressing that R is a linear order of which 0 is the first element and with no final element. Then both structures $\langle \mathbb{N}, 0, x \mapsto x + 1, \leq \rangle$ and $\langle A, (0, 1), \Sigma, \Delta \rangle$ satisfy theory {A1, A2, A3, A4} when $\leq$ is the natural order of $\mathbb{N}$ and when we put in A,

$$(x, i)\Delta(y, j) \Leftrightarrow [i < j \text{ or } (i = j \text{ and } x \leq y)].$$

It follows from this fact that every element of $\mathbb{Z} \times \{2\}$ (called nonstandard) is greater, in the sense of Δ, than any element of $\mathbb{N} \times \{1\}$ (which are said to be standard).

By identification between natural integers and these elements of A which lie in $\mathbb{N} \times \{1\}$, we see that the nonstandard elements of A are infinite since they are greater than any natural (hence finite) integer. These nonstandard elements will be called *infinitely large. The usual constructions allowing the mathematician to get rational and real numbers from integers work within A and provide infinitely large rationals or reals, infinitely small rationals and reals.* These new numbers give a new kind of approximation having the huge advantage of providing us with measures by means of integers (standard or not) and of their inverses. The new approximations are ideal since they are "infinitely" more precise than any classical approximation and also because they are just expressed by integers and their inverses.

If x and x' are usual reals (the numbers known by any pupil or undergraduate student) verifying $x < x'$, and if ω is an infinitely large integer, then $x < x + 1/\omega < x'$.

2.1.2. Leibnitz's dream: how to algebraize analysis

During their attempt at founding Infinitesimal Calculus, Newton, but especially Leibnitz, tried to add to the numbers they used (integers, rationals and reals) infinitely large and small ideal numbers. Unfortunately, the necessary formalism had not yet been invented (this was done by A. Robinson, who provided it for us in the sixties), so that the point of view of Leibnitz was abandoned in favour of

Weierstrass' formulations (and his $\varepsilon - \delta$ method) from which mathematics is taught nowadays. Now, *model theory* and particularly the discovery of nonstandard models of arithmetic by Skolem allows us to revise the ideas of Newton and Leibnitz. Without any justification, let us give the calculation from which a working mathematician and follower of nonstandard methods gets the derivative of the function $x \mapsto \sqrt{x}$ on $\mathbb{R}$:

$$\frac{d}{dx}\sqrt{x} = st\left(\frac{\sqrt{x+\Delta x}-\sqrt{x}}{\Delta x}\right)$$

$$= st\left(\frac{x+\Delta x-x}{\Delta x(\sqrt{x+\Delta x}+\sqrt{x})}\right) = st\left(\frac{1}{\sqrt{x+\Delta x}+\sqrt{x}}\right)$$

$$= \frac{1}{st(\sqrt{x+\Delta x})+\sqrt{x}} = \frac{1}{2\sqrt{x}}.$$

To intuitively understand this calculation, it is sufficient to consider Δx as an infinitely small real (which has an infinitely large inverse), and to know that the function denoted by *st* maps every *noninfinite nonstandard real onto an infinitely close standard real* (if any exist). It must be pointed out that in the previous calculation, *there seems to be no sort of limit.*

It is now time to briefly present the frame used in the second part for computing actual programs, namely the nonstandard methods of finitization.

2.2. FRAME OF NONSTANDARD ANALYSIS: THE UNIVERSES $\mathcal{U}$ AND $\mathcal{U}^*$ (*informal overview*)

We admit that *two universes* exist, denoted $\mathcal{U}$ and $\mathcal{U}^*$, such that $\mathcal{U} \subset \mathcal{U}^*$ and such that, in each of the two universes, a denumerable set of symbols of real analysis (namely, certain reals ($\sqrt{2}$, π,...), all integers and rationals, some sets of numbers like $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and some functions from $\mathbb{R}^m$ to $\mathbb{R}^n$) are realized (or interpreted) by elements of $\mathcal{U}$ and by elements of $\mathcal{U}^*$. Logicians would say that both universes $\mathcal{U}$ and $\mathcal{U}^*$ are structures of the language $L(RA)$ of the usual real analysis,[1] and *models* of the familiar real analysis considered as a first-order theory.[2]

For convenience (and also by abuse), we denote every symbol s of $L(RA)$ and its interpretation within $\mathcal{U}$ by the same symbol, but within $\mathcal{U}^*$, the same symbol s will be interpreted by an object denoted by s^*. For instance, the symbol $\mathbb{N}$ of $L(RA)$ will be interpreted by $\mathbb{N}$ in $\mathcal{U}$ and $\mathbb{N}^*$ in $\mathcal{U}^*$.

[1] All sentences that mathematicians can prove within the frame of a good set theory are considered as theorems of real analysis.

[2] $L(RA)$ does not seem to be a first-order language if we think that quantification over different kinds of objects (integers, functions, etc.) is allowed; actually, $L(RA)$ is a first-order language if we remind ourselves of the fact that all objects of analysis are of the same kind, namely sets.

In what follows (section 2.2.5) we shall see that $\mathcal{U}$ and $\mathcal{U}^*$ can be constructed so that the following conditions are satisfied:

AN1. We have $\mathbb{N} \underset{\neq}{\subset} \mathbb{N}^*, \mathbb{Z} \underset{\neq}{\subset} \mathbb{Z}^*, \mathbb{Q} \underset{\neq}{\subset} \mathbb{Q}^*, \mathbb{R} \underset{\neq}{\subset} \mathbb{R}^*$.

AN2. If f is a functional symbol of $L(RA)$, then the restriction $f^*|$ of f^* to $\mathbb{R}$ is f.

AN3. – transfer principle – a sentence T (a formula in $L(RA)$) for which all variables are quantified – in other words, a close formula – is satisfied in $\mathcal{U}$ if and only if it is satisfied in $\mathcal{U}^*$ (notation: $\mathcal{U} \models \mathrm{T} \Leftrightarrow \mathcal{U}^* \models \mathrm{T}$).

AN4. Both universes $\mathcal{U}$ and $\mathcal{U}^*$ are models of the theory of real analysis (in the sense that any theorem of real analysis is satisfied simultaneously within $\mathcal{U}$ and $\mathcal{U}^*$).

Example

Let us consider this theorem of analysis ensuring that $\mathbb{Q}$ is dense in $\mathbb{R}$, formalized as follows:

$$(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(x < y \Rightarrow (\exists z \in \mathbb{Q})(x < z < y)).$$

Consequently, we have simultaneously

$$\mathcal{U} \models (\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(x < y \Rightarrow (\exists z \in \mathbb{Q})(x < z < y)),$$

$$\mathcal{U}^* \models (\forall x \in \mathbb{R}^*)(\forall y \in \mathbb{R}^*)\ (x < y \Rightarrow (\exists z \in \mathbb{Q}^*)(x < z < y)).$$

2.2.1. Infinitely large integers

A major tool of the results developed in the second part are the so-called infinitely large integers. Their existence follows from the condition AN1, which ensures that $\mathbb{N} \underset{\neq}{\subset} \mathbb{N}^*$. So, we must specify what exactly these integers are.

PROPOSITION 2.1 (Conditions for defining infinite natural integers.)

Elements belonging to $\mathbb{N}^* \setminus \mathbb{N}$ are called infinitely large; $\alpha \in \mathbb{N}^* \setminus \mathbb{N}$ if and only if $\alpha \in \mathbb{N}^*$ and if, for all $n \in \mathbb{N}$, we have $\alpha > n$ (notation: $\alpha > \mathbb{N}$).

Proof

We know (condition AN1) that $\mathbb{N}^* \setminus \mathbb{N} \neq \emptyset$. Let α be a member of $\mathbb{N}^* \setminus \mathbb{N}$. Consider the following sentence T of $L(RA)$:

$$(\forall x)(x < n_0 \wedge x \in \mathbb{N} \Leftrightarrow (x = 0 \vee x = 1 \vee \ldots \vee x = n_0 - 1)),$$

where $0, 1, \ldots, n_0 - 1$, n_0 are symbols of natural integers within $L(RA)$. Of course, T is a sentence if and only if n_0 is a symbol that is always interpreted by a standard

(i.e. actual) natural integer. Moreover, as T is a theorem of real analysis, we have $\mathcal{U} \models T$ and $\mathcal{U}^* \models T$. Hence, $\alpha > n_0$ since, if not, $\alpha \leq n_0$, which implies from T that $\alpha \in \mathbb{N}$ and this is contrary to our assumption. Due to the fact that n_0 is arbitrary, it follows that $a > n$ for every n in $\mathbb{N}$. The converse is obvious. □

Remarks

- Since $(\forall n \in \mathbb{N})\exists p$ ((p is prime) $\wedge$ ($p > n$)) is a theorem, then that theorem is true within $\mathcal{U}^*$ so infinite natural integers exist which are prime.
- Let π be an infinite prime positive integer, then $\mathbb{N}^* \setminus \pi\mathbb{N}^* = \mathbb{R}^* \setminus \pi\mathbb{R}^*$ is a field. From $\mathbb{R} \subset \mathbb{R}^*$, all members of $\mathbb{R}^* \setminus \pi\mathbb{R}^*$ are inversible within $\mathbb{R}^* \setminus \pi\mathbb{R}^*$ and so, up to morphisms, $\mathbb{Q} \subset \mathbb{R}^* \setminus \pi\mathbb{R}^*$. This sort of reasoning is routine in nonstandard arithmetic.

2.2.2. *Infinitely small real numbers and some nonstandard notion of* $\mathbb{R}^*$

Because we have $\mathbb{N} \subset \mathbb{R}^*$ (due to the fact that both $\mathcal{U}$ and $\mathcal{U}^*$ satisfy $(\forall x \in \mathbb{N} \Rightarrow x \in \mathbb{R})$, in $\mathbb{R}^*$ there are reals which are infinitely large. Their inverses are *infinitely small* since when $\alpha \in \mathbb{N}^* \setminus \mathbb{N}$, we have $\alpha > n$ (for every n in $\mathbb{N}$) and $1/\alpha \in \mathbb{R}^*$ is such that $0 \neq 1/\alpha < 1/n$ (for every n in $\mathbb{N}$).

DEFINITION 2.1

A real number $r \in \mathbb{R}^*$ is said to be infinitely large if and only if $r > n$ for every $n \in \mathbb{N}$. A real $t \neq 0$ is said to be infinitely small or infinitesimal if and only if the inverse of its absolute value $1/|t|$ is infinitely large. A real $x \in \mathbb{R}^*$ is said to be finite if there exists $y \in \mathbb{R}^+$ such that $|x| < y$ (meaning $\mathcal{U}^* \models (|x| < y)$).

Remark

A real $r \in \mathbb{R}^*$ can be finite without belonging to $\mathbb{R}$ (for instance, $\sqrt{2} + 1/\alpha$ with $\alpha \in \mathbb{N}^* \setminus \mathbb{N}$). The monad of $0 \in \mathbb{R}^*$ (denoted by $\mu(0)$) is the set $\{x \in \mathbb{R}^* \mid |x|$ is infinitely small$\}$. The monad of $x \in \mathbb{R}^*$ is $\{y \in \mathbb{R}^* \mid x - y \in \mu(0)\}$ and is denoted by $\mu(x)$.

The following proposition shows that our intuition about the structure of infinitesimal reals, according to which we thought that a sum (or a product) of infinitely small reals is also of the same kind, is founded. More precisly, $\mu(0)$ is an actual ideal of the set of finite reals of $\mathbb{R}^*$.

PROPOSITION 2.2

Let F be the set $\{x \in \mathbb{R}^* \mid \exists y \in \mathbb{R}^+(|x| < y)\}$.

(i) The monad $\mu(0)$ is an ideal of F.

(ii) The quotient ring $F/\mu(0)$ is isomorphic to $\mathbb{R}$.

Proof

(i) Let α and β be members of $\mu(0)$. Then, for every $n \in \mathbb{N}\setminus\{0\}$, we have $\alpha < 1/2n$ and $\beta < 1/2n$, hence $\alpha + \beta < 1/n$ and $\alpha + \beta \in \mu(0)$. If $x \in F$, then is $a \in \mathrm{N}$ is such that $|x| < a$, and due to the fact that $\alpha < 1/na$ for every $n \in \mathbb{N}\setminus\{0\}$, we have $|xa| < 1/n$, so that $x\alpha \in \mu(0)$. Obviously, $\mu(0) \subset F$ and F is a subring of $\mathbb{R}^*$; moreover, the two previous remarks show that $\mu(0)$ is an ideal of the ring F.

(ii) To every $x \in \mathbb{R}$, we can associate $x + \mu(0) \in F/\mu(0)$. Conversely, every coset $\bar{a} \in F/\mu(0)$ determines a Dedekind's cut $A|B$ by putting

$$A = \{b \in \mathbb{R} \mid (b < a)\} \text{ and } B = \{b \in \mathbb{R} \mid (a < b)\}.$$

Such a cut defines a unique (standard) real, which we denote by ${}^*a$.

DEFINITION 2.2

Let $a \in F$; there exists a unique real denoted by ${}^*a$ or $st(a)$, called the standard part of a and such that ${}^*a \in \bar{a}$ and $\bar{a} \in F/\mu(0)$. If we call the members of $\mathbb{R}^*$ hyperreals, then the numbers of F are the finite (or bounded) hyperreals and the standard part ${}^*a \in \mathbb{R}$ of the finite hyperreal a is the unique (true) real of R infinitely close by a, since $a - {}^*a \in \mu(0)$. (Notation: $a - b \in \mu(0)$ is also denoted by $a \simeq b$, which is called a infinitely close by b).

The above proposition justifies the previous definition.

2.2.3. *How to prove in nonstandard analysis what $\mathcal{U}$ says, what $\mathcal{U}^*$ says, what the external observer says and the non-definable in L(RA)*

We must emphasize some difficulties, which are the key points of nonstandard analysis.

In fact, when we observe that both $\mathcal{U}$ and $\mathcal{U}^*$ realize the theorems of analysis, this means that they express the same result. Each of the universes $\mathcal{U}$ and $\mathcal{U}^*$ has its own notions of integer (respectively, members of $\mathbb{N}$ and members of $\mathbb{N}^*$). For $\mathcal{U}$ and $\mathcal{U}^*$, their respective integers have the usual arithmetical behaviour. What determines nonstandard analysis is the external observer simultaneously seeing $\mathcal{U}$ and $\mathcal{U}^*$, and who can say that $\mathbb{N} \subsetneq \mathbb{N}^*$. This is not expressible within the language $L(RA)$ of analysis because we do not know how to speak of infinitely large integers, we just know how to speak of integers. *Only a mathematician, in a first-order formalizable way situated in the framework of set theory, looking at $\mathcal{U}$ and $\mathcal{U}^*$, can compare them.* We can try to draw what our mathematician sees concerning $\mathbb{R}$ and $\mathbb{R}^*$ with the help of fig. 6; the left part represents $\mathbb{R}$ included in the whole $\mathbb{R}^*$.

Consequently, from the point of view of naive set theory, the main notions are summarized in the following framed text.

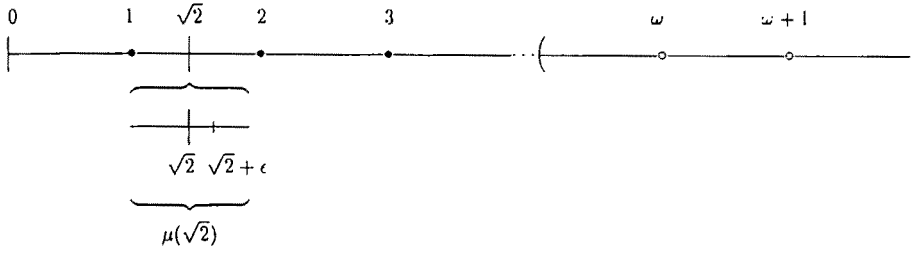


Fig. 6.

$\mathbb{R}$	True reals (also called standard reals)
$\mathbb{R}^* \supset \mathbb{R}$	Hyperreals (the whole collection, standard or nonstandard elements)
$\mu(0)$	Infinitely small reals, i.e. numbers whose absolute value is less than every positive standard
F	Finite hyperreals, those who are infinitely close to a true real
$\mathbb{R}^* \setminus F$	Infinite hyperreals, numbers whose absolute value is greater than every member of $\mathbb{R}$
$\mu(x)$	Hyperreals infinitely close to x. More precisely, $\mu(x) = \{y \mid x - y \in \mu(0)\}$

Frame 4.

2.2.4. Revisiting nonstandard proof of the intermediate value theorem given in 1.2.1

Below, we give a more precise version of the proof of the theorem presented in section 1.2.1. This new version is developed in the framework of nonstandard analysis by arithmetization.

INTERMEDIATE VALUE THEOREM 2.1

Let f be a continuous function from $[a, b]$ into $\mathbb{R}$. Let us assume $f(a) < 0 < f(b)$. Then there exists $c \in [a, b]$ such that $f(c) = 0$.

Proof

Let $\omega \in \mathbb{N}^* \setminus \mathbb{N}$, $x_i = a + (i/\omega)(b - a)$ for $0 < i < \omega$ and $A = \{i \in \mathbb{N}^* \mid f^*(x_i) > 0\}$. Since $\omega \in A$, the set A is nonempty and since $A \subset \mathbb{N}^*$, the set A has a minimum

denoted by m. From $f^*(x_0) = f(a) < 0$, it follows that $m > 0$. Consider x_m and note that $x_m \in F$, the set of finite hyperreals, because $a < x_m < b$. Let c be ${}^*x_m$. It is easy to show that the continuity of f implies that $f(c) \simeq f^*(x_m)$. But $x_{m-1} = x_m - (1/\omega)(b-a)$, so that $x_{m-1} \simeq x_m$ and it follows from the continuity of f that $f(c) \simeq f^*(x_{m-1})$.

Moreover, we have, by the very definition of m, the inequality $\alpha = f^*(x_{m-1}) < 0$ and $\beta = f^*(x_m) \geq 0$. So we have ${}^*\alpha = {}^*(f^*(x_{m-1})) = {}^*(f^*({}^*x_{m-1})) = f(c)$ and ${}^*\beta = {}^*(f^*(x_m)) = {}^*(f^*({}^*x_m)) = f(c)$. For every $x \in \mathbb{R}^*$, we can easily prove that the condition $x \leq 0$ (resp. $x > 0$) implies ${}^*x \leq 0$ (resp. ${}^*x > 0$) and consequently ${}^*\alpha \leq 0$ and ${}^*\beta \geq 0$, arriving at the proof of the desired equality $f(c) = 0$. □

Remark

The previous proof consists of *enumerating* some points of $[a, b]$ in $\mathbb{R}^*$ to find an *index* (m) of hyperreal x_m close to the desired standard point $c = {}^*x$. We have substituted for the notion of *greater lower bound* of a subset of reals the notion (not as complex) of a minimum of a nonempty subset of natural integers.

2.2.5. *Logic foundations of finitization and external description of the set of finite and infinite integers*

Here, we put emphasize on the fact that the finitization method is a positive by-product of a *failure* of logicians when they tried (and Gödel proved that any attempt could not succeed) to define natural integers at first order, i.e. with quantifications on only one sort of objects. Now we want to give some more details about that important question of defining integers.

(a) Second-order categorical definition of natural integers; uncategoricity of first-order Peano arithmetic.

It is very easy and well known that $\mathbb{N}$ can be *defined and characterized* within a logical language where it is possible to *quantify both on integers and on subsets of integers*. This is simply the usual presentation of $\mathbb{N}$ by the so-called (second-order) Peano's axioms which ensure that $\mathbb{N}$ is, up to isomorphism, the smallest set such that there exists a one-to-one mapping S (the successor function) from $\mathbb{N}$ into itself, almost to the extent that only the distinguished element 0 is not in the range of S, which is expressible by $S(\mathbb{N}) = \mathbb{N} \setminus \{0\}$ and verifying the second-order axiom of induction:

$$(\forall A \subseteq \mathbb{N})\,((0 \in A \wedge (x \in A \Rightarrow S(x) \in A)) \Rightarrow A = \mathbb{N}).$$

Unfortunately, the main results of mathematical logic (and especially the completeness theorem) only just hold in the framework of *first order*. Consequently, research *was done to find properties that were both expressible within a first-order*

language and able to characterize integers. In that direction appeared the first-order axioms of Peano. Then Gödel proved his famous theorems about the strong character of incompleteness of all theories containing a reasonable arithmetic. Finally, Skolem understood that Peano arithmetic **P** is not *categorical*: there exists at least a denumerable model (say **M**) of **P** which is not isomorphic to $\mathbb{N}$, but has $\mathbb{N}$ has a proper initial segment. So, the existence of infinitesimally large integers (members of $\mathbf{M} \setminus \mathbb{N}$) has been proved and also the existence of infinitesimal reals: nonstandard analysis was potentially there, but elaborating this theory and the connected methods of finitization had to wait for the work of Robinson.

It seems to us that understanding what a nonstandard model of **P** actually is cannot be done without giving a kind of external description (in the usual mathematical style within the framework of the usual naive set theory). Besides, in our opinion, the axiomatic presentation of nonstandard analysis via the IST system of Nelson (see [11]) is very interesting when one knows examples of nonstandard models.

(b) Nonstandard models of arithmetic: some of their properties considered from the outside.

Here, the use of the word *outside* refers to the character of nondefinability of the considered properties within our first-order language $L(RA)$. Now we restrict the used first-order language to $\mathcal{L}(\mathbf{P}) =< 0, S, <, +, . >$. We study the nonstandard models of Peano arithmetic **P**. Let $M \models \mathbf{P}$ be a denumerable model nonisomorphic to $\mathbb{N}$. We show that such a model is formed by an initial segment $\mathbb{N}$ followed by copies of $\mathbb{Z}$ structured as the chain $\mathbb{Q}$ of rationals.

PROPOSITION 2.3

The isomorphic order type of **M** is $(\omega + (\omega^* + \omega)\eta$, where ω, ω^* and η are, respectively, the order types of $\mathbb{N}$, of the set $\mathbb{Z}$ of rational integers and of the set $\mathbb{Q}$ of rational numbers.

Proof

Using the successor function S and the element 0 of **M**, we easily see that there exists an initial segment of $\mathbb{N}$, isomorphic to $\mathbb{N}$ and that we identify with $\mathbb{N}$. We use symbols 1 for $S(0)$ and n for $S \ldots S(0)$ with n letters S. Within **P**, it is formally provable that $[x < n \Leftrightarrow (x = 0 \vee x = 1 \vee \ldots \vee x = n - 1)]$ and consequently, as already mentioned, every nonstandard integer α (member of $\mathbf{M} \setminus \mathbf{N}$) is greater than any $n \in \mathbb{N}$ (hence α is infinitely large). Let $\alpha \in \mathbf{M} \setminus \mathbf{N}$ be such a fixed infinite integer. Then for all $n \in \mathbb{N}$, all integers $\alpha + n$ and $\alpha - n$ are also infinite. Let $\overline{\alpha}$ be the coset $\alpha + \mathbb{Z}$ in **M**. Note that $\overline{\alpha} = \overline{\beta}$ for $\beta \in \mathbf{M} \setminus \mathbf{N}$ iff there exists $z \in \mathbb{Z}$ such that $\alpha + z = \beta$, which defines an equivalence relation. Let $y = [x/2]$ be the integer which denotes the integral part of the rational number $x/2$; such an integral part is definable

in $\mathcal{L}(\mathbf{P})$ by the formula $[x = 2y \vee x = 2y + 1]$. From that, it follows that there are infinitely many cosets $\bar{\gamma}$ in $\mathbf{M}$, each one having $\omega^* + \omega$ as order type since $\bar{\gamma} = \{\gamma + z | z \in \mathbb{R}\}$. Now, we show that the set of all these cosets $\bar{\gamma}$, where $\gamma \in \mathbf{M} \setminus \mathbf{N}$, forms a denumerable dense linearly ordered set without first or last element, hence isomorphic to the chain $\mathbb{Q}$ of rationals; in other words, having η as order type. We put $\bar{\alpha} \ll \bar{\beta}$ if and only if $\alpha \in \mathbf{M} \setminus \mathbf{N}$ and $\beta \in \mathbf{M} \setminus \mathbf{N}$ and finally $\alpha < \beta$. This relation $\ll$ is clearly an order which is the quotient of $<$ by the previous relation, the coset of which is the $\bar{\gamma}$. Since $\bar{\alpha} \neq \bar{\beta}$ and $\bar{\alpha} \ll \bar{\beta}$ implies $\bar{\alpha} \underset{\neq}{\ll} [\frac{1}{2}\overline{\alpha + \beta}] \underset{\neq}{\ll} \bar{\beta}$, the required density is proved. Besides, inequalities like $[\alpha/2] \ll \bar{\alpha} \ll \overline{2\alpha}$ make the existence of a first and last element impossible. □

Remark

A nonstandard model of **P** can be drawn as in fig. 7. For some descriptions of the additive structure of certain particular nonstandard models of Peano, see the paper [19].

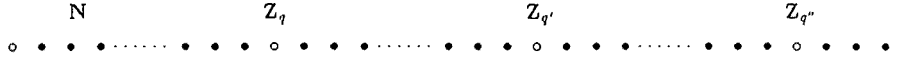


Fig. 7.

(c) Nonstandard models of $\mathbb{Z}$ and discretization of the real plane.

The external order structure of nonstandard models which we have just developed in the previous section provides a deep reason for the efficiency of the discretization obtained via a nonstandard method. Actually, the nonstandard part of a nonstandard model of arithmetic which is denumerable is arrived at exactly *by replacing every (standard) rational by a copy of* $\mathbb{Z}$*, the set of (standard) integers.* In a similar way, take nonstandard models which are of the same cardinality as the usual set of $\mathbb{R}$ (standard) reals. It can be proved that their order type is the following:

- first, a copy of the usual set $\mathbb{N}$ of (standard) integers,
- then the nonstandard part of the model obtained by replacing every (standard) real by a copy of $\mathbb{Z}$.

Now, if we look at the Cartesian product of the set $M = \mathbb{N} \cup INFI$ (of standard and nonstandard integers) and if we suppose that M has the same cardinality as the usual $\mathbb{R}$, then we get a discretization of the usual real plane. Actually, every usual real point (x, y) is the index of a net formed by a Cartesian product of the usual set $\mathbb{Z}$ (of standard positive or negative integers).

(d) Nondefinability of N within a nonstandard model of Peano and overspill.

Notions of internal set and of external set are central in logic as in nonstandard analysis. This is the reason why we now show that one cannot see (i.e. express by formulas of $\mathcal{L}(\mathbf{P})$ completed by a constant of $\mathbf{M}\setminus\mathbb{N}$), from the inside of a given nonstandard model of $\mathbf{P}$, the initial segment $\mathbf{I}$ isomorphic to $\mathbb{N}$. We can say that this set $\mathbf{I}$ is not definable within $\mathbf{M}$ by an $\mathcal{L}(\mathbf{P})$-formula, even accepting symbols for members of $\mathbf{M}\setminus\mathbb{N}$. Integers of $\mathbf{M}$ are finite (hence bounded) in the framework of $\mathbf{M}$. But (see next proposition) elements of $\mathbf{M}\setminus\mathbb{N}$ are infinite when seen from the outside (i.e. determined by the infinity of conditions $x > n$ with $n \in \mathbb{N}$). The set $\mathbb{N}$ is external in $\mathbf{M}$, but any actually finite $F \subseteq M$ (with cardinal in $\mathbb{N}$) is internal since it is definable by an obvious formula enumerating its members. Of course, many infinite (from the outside) subsets of $\mathbf{M}$ are definable within $\mathcal{L}(\mathcal{P})$ in $\mathbf{M}$: for instance the set of prime numbers, of Fermat numbers, and so on. This leads to the following

PROPOSITION 2.4

(i) In a nonstandard model $\mathbf{M} \models \mathbf{P}$, the initial segment $\mathbf{I}$ isomorphic to $\mathbb{N}$ is not definable by a formula of $\mathcal{L}(\mathcal{P})$, even with parameter symbols of $\mathbf{M}$.

(ii) (Overspill). Each definable subset of $\mathbf{M}$ including $\mathbf{I}$ contains at least an infinite integer, i.e. an element of $\mathbf{M}\setminus\mathbf{I}$.

(iii) (Second form of overspill). Each definable subset of $\mathbf{M}$ including $\mathbf{M}\setminus\mathbf{I}$ contains at least a finite integer, i.e. a member of $\mathbf{I}$.

Proof

(i) If $\mathbf{I}$ is definable, so is $\mathbf{M}\setminus\mathbf{N}$ (by negation) and, since in $\mathbf{M}$ every definable nonempty subset has a minimum, there is a smallest large integer, say α_0. From conditions $\mathbf{M} \models \alpha_0 > n + 1$ for every $n \in \mathbb{N}$, we have $\mathbf{M} \models \alpha_0 - 1 > n$ and hence the fact that $\alpha_0 - 1 \in \mathbf{M}\setminus\mathbb{N}$, which is contradictory to the very definition of α_0.

(ii) If a definable subset A is $\mathbf{I}$, then $\mathbf{I}$ is definable contrary to (i). So $A \subseteq \mathbb{N}$ and $A \neq \mathbb{N}$, and we have $A \cap (\mathbf{M}\setminus\mathbb{N}) \neq \emptyset$.

(iii) Analogous to (ii).

(e) Construction of universes $\mathcal{U}$ and $\mathcal{U}^*$.

This paper is certainly not the place to give an extended development of a construction of $\mathcal{U}$ and $\mathcal{U}^*$. Nevertheless, it is appropriate to convince the reader that nonstandard methods of finitization are in themselves included in the traditional

framework of a usual set theory to give[3] the main results concerning $\mathcal{U}$ and $\mathcal{U}^*$. The details of this construction can be found in the first chapter of the book by Martin Davis (see [4, pp. 5–41] and [21]).

Let us give

DEFINITION 2.3 (of the universe $\mathcal{U}$)

(a) Let S be an overset of $\mathbb{R}$; individuals of $\mathcal{U}$ are exactly the elements of S; by induction and if $\mathcal{P}(X)$ denotes the power set of a given set X, we define a sequence $(S_i)_{i\in\mathbb{N}}$ as follows: $S_0 = S, \ldots, S_{i+1} = S_i \cup \mathcal{P}(S_i)$. We put $\hat{S} = \bigcup_{i\in\mathbb{N}} S_i$.

(b) The universe $\mathcal{U}$ will be any subset of $\hat{S}$ simultaneously verifying the four conditions:

(i) $\emptyset \in \mathcal{U}$;

(ii) $S \subseteq \mathcal{U}$;

(iii) If $x \in \mathcal{U}$ and $y \in \mathcal{U}$, then $\{x, y\} \in \mathcal{U}$;

(iv) $\mathcal{U}$ is transitive (in other words: for all $x \in \mathcal{U}$, either $x \in S$ or $x \subseteq \mathcal{U}$).

Let UL be a proper ultrafilter on $\mathbb{N}$; the universe $\mathcal{U}^*$ is the ultrapower of $\mathcal{U}$ under UL. Then it can be shown that couple $(\mathcal{U}, \mathcal{U}^*)$ verifies all required properties AN1, AN2, AN3 and AN4. The proof is based on two logical results.

The first result is the theorem of Los, which admits the following consequence.

PROPOSITION 2.5

A sentence of $L(RA)$ is satisfied in $\mathcal{U}$ if and only if it is satisfied in $\mathcal{U}^*$.

The seond result ensures that $\mathcal{U}^*$ is richer than $\mathcal{U}$ because $\mathcal{U}^*$ is a $\aleph_1$-saturated model and this is written out in

PROPOSITION 2.6 (Robinson's principle)

A binary relation B of $\mathcal{U}$ is called concurrent if the condition (for every finite part $F = \{a_1, \ldots, a_n\}$ of $\mathcal{U}$ there exists an element $b(F)$ such that $(a_i, b(F)) \in B$ for every $i \in \{1, \ldots, n\}$) implies the existence of an element $b \in \mathcal{U}^*$ such that $(a, b) \in B$ for every element a of the domain $dom(B)$ of B.

[3] For the reader familiar with logic, elementary extensions and saturation, we would just like to say that we consider a transitive universe $\mathcal{U}$ containing $\mathbb{R}$ as a subset of individuals of $\mathcal{U}$ and we take an ultrapower modulo as a proper ultrafilter. By Los' theorem, sentences are preserved (this is *transfer*) in a richer universe $\mathcal{U}^*$ which is itself saturated. Hence, every denumerable family of existential conditions which is finitely realized is also realized in $\mathcal{U}^*$. This is *compacity* and this provides, for instance, infinitesimals and infinitely large reals.

Remark

Once more, we get a compacity result. In particular, if we take B as the natural order, then we obtain the existence of infinite integers because $dom(\leq) = \mathbb{N}$. This brings us back to the first AN1, which states the fact that $\mathbb{N} \subsetneq \mathbb{N}^*$.

2.2.6. To be or not to be finite: this is not expressible by machines

We remind the reader that it is possible to define the usual set $\mathbb{N}$ at the second order within a suitable set theory. Now let us recall the first-order Peano axioms, expressed in a usual first-order Peano language $\mathcal{L}(\mathcal{PA})$:

$$\forall x \forall y (Sx = Sy \Rightarrow x = y) \qquad (S1)$$

$$\forall x (x \neq 0 \Rightarrow \exists y (Sy = x)) \qquad (S2)$$

$$\forall x (x + 0 = x) \qquad (A1)$$

$$\forall x \forall y (x + Sy = S(x + y)) \qquad (A2)$$

$$\forall x (x \,.0 = 0) \qquad (M1)$$

$$\forall x \forall y (x.Sy = xy + x) \qquad (M2)$$

$$\forall x (\phi(x) \Rightarrow \phi(x + 1) \wedge \phi(0)) \Rightarrow \forall x \phi(x). \qquad (Rf)$$

It is clear that the usual $\mathbb{N}$ satisfies these axioms.

In the last part of this section, we would like to convince the reader that it is not possible to define at first order (in a usual logical language) the property, for a set, of being *finite*. In order to do this, consider a new constant symbol α and a new language $\mathcal{L}'$, defined as follows:

$$\mathcal{L}' = \mathcal{L}(P) \cup \{\alpha\} \cup \{\bar{n}\}_{n \in \mathbb{N}}.$$

Within this language $\mathcal{L}'$, we can express the infinite set of sentences

$$\sum(\alpha) = \{\alpha > \bar{n}\}.$$

Now suppose that $FINI(x)$ is a first-order $\mathcal{L}'$ formula such that its interpretation (in a model of the chosen set theory) is

$$x \text{ is finite.}$$

Considering any finite part, $\sum_f = \{\alpha > \overline{n_1}, \ldots, \alpha > \overline{n_k}\}$ of $\sum(\alpha)$ Then $m \in \mathbb{N}$ exists such that the structure $\langle \mathbb{N}, \tilde{\alpha} = m \rangle$ satisfies $P + \forall x\, FINI(x) + \sum_f(m)$. By the logical compactness theorem (see any introduction to mathematical logic), we know that if any finite part of an infinite set of sentences has a model, then the whole set of

sentences itself also has a model. Let $\mathcal{M}$ be such that there exists in $\mathcal{M}$ an element $\tilde{\alpha}$ (interpreting the symbol of $\mathcal{L}'$) such that the structure $\mathcal{M}$ verifies for all x in $\mathcal{M}$

$$P + \forall x\, FINI(x) + \sum(m).$$

Mézalor (R. Queneau):

- on one hand, $FINI(\tilde{\alpha})$ is true because for every element x of $\mathcal{M}$, the relation $FINI(x)$ is true;
- on the other hand, $\tilde{\alpha} > n$ for every $n \in \mathbb{N}$ so that $\tilde{\alpha}$ is *infinite*. This shows that structure $\mathcal{M}$ contains one element that does not satisfy the interpretation of *FINI*, while all elements satisfy the interpretation of *FINI*. This is a contradiction which makes it impossible to characterize at first order the notion of finiteness.

3. Computer science as a source of discrete problems

The conflicts between the continuum and the discrete

Computers being finite machines cannot manage directly nature's modelling obtained from continuous notions using real numbers. This is the main source of conflicts between two of our tools: modelling using continuous notions and computers. If we look a little bit closer, we see that the continuum usually requires the axiom of infinity which is out of the computer's range.

3.1. THE CLASSICAL THESIS AND ITS LIMITATIONS

By chance, using numerical analysis (error calculus), we can generally solve this conflict for functions whose range is contained in $\mathbb{R}$. This permits us, of course, to solve some geometrical or topological problems if a small error is accepted. Numerical processing of continuous objects defines discrete objects still greatly unknown. These are close to the continuous ones we want to study if the computation uses a high-precision floating-point or fix-point arithmetic, and this closeness is often sufficient. However, we can notice that this classical thesis in the way computers are used to manage continuous objects is far from perfect:

- This thesis is right for functions but is not very convenient when we want to study general continuous objects. For example, a discretized manifold will never be identical to its mother notion. It can be difficult to guess how some continuous properties we rely on for the end of an algorithm must be adapted in the discrete case (connected components, in particular, become practically unworkable).
- Floating of fix-point arithmetics are not the only way discrete objects appear; many devices (screens, scanners, printers, digital signal devices, etc.) also convert

continuous objects into discretized objects and often not very accurately. Consequently, discrete objects are, in these situations, unavoidable and cannot be hidden behind a high-precision computation. Once a line or a circle has been digitized in this way and transmitted, we have to make do with it.

- Even for functions, numerical analysis cannot answer all the questions. Geometrical transformations, for example plane rotations, which are relevant in this case, lose the property of being bijections after a discretization has occurred. Yet this property can be fundamental in certain situations such as image processing or desktop publishing.

The three former observations describe a very vast and almost virgin territory: defining and studying discrete objects which can be related to those appearing in the use of computers. Or to put it in another way, *what part of the continuous can be reached with a computer*? We intuitively feel that this domain is an unlimited source of questions and work.

3.2. THE EXAMPLE OF LINEAR APPLICATIONS

The main problem with the domain we have just outlines is its immensity. We would certainly first like to delimit some interesting areas where the job can be done effectively, but this is not so easy. To show an example of the type of difficulties, let us examine the discretization of a linear mapping. Many people already noticed in the past that quantization of linear mappings, even for the contracting ones, destroys their dynamical properties. Cycles may appear in the discretized function in place of the unique fixed-point, zero, of the linear map. But these cycles, which appear in fix-point computations for example, are really difficult to explain formally; we mean in such a way that we can, if we take into account the coefficients of a linear mapping, predict the cycles of its quantization. If we treat this problem along the lines of section 1, we can at least express formally these digitalizations, that is, give arithmetical formulas describing them exactly. These equations do in fact show that, among all discretizations, there exists a canonical one which, in a certain sense, is universal and is the first step in a theoretical study. Let f be a rational plane linear transform whose matrix (in canonical basis, for example) is

$$A = \frac{1}{\omega}\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

where all parameters are integers; this hypothesis is obviously not a restriction. Suppose we want to compute this transform using a finite precision device, say in fix-point arithmetic where precision is ε. If $(x, y) \in \mathbb{R}^2$ is a point in the Euclidean plane, the result of computation is exactly the point

$$\left(trunc\left(\frac{ax + by}{\omega}\right), trunc\left(\frac{cx + dy}{\omega}\right)\right),$$

where, for real number α, $trunc(\alpha)$ denotes the largest, among numbers of the form $k\varepsilon$, $k \in \mathbb{Z}$, and bounded by α. Moreover, if we are interested in f's iterations, we can also suppose that the starting point (x, y) is of the form $(m\varepsilon, n\varepsilon)$ for integers m and n. Function f's digitalization is then given by

$$\left(\left[\frac{am + bn}{\omega}\right]\varepsilon, \left[\frac{cm + dn}{\omega}\right]\varepsilon\right),$$

where brackets denote the integer part. Thus, we see that f's discretization is entirely defined by the function $\phi : \mathbb{Z}^2 \to \mathbb{Z}^2$, defined by

$$(\phi)\begin{cases} X' = \left[\frac{aX+bY}{\omega}\right], \\ Y' = \left[\frac{cX+dY}{\omega}\right]. \end{cases}$$

This integer function is a rescaling of f's digitalization. We observe that this rescaling is independent of precision ε; it is a normalized discretization. As far as fix-point arithmetic is concerned, any $\mathbb{R}^2$ linear rational mapping f is converted to such a $\mathbb{Z}^2$ transformation whatever the precision ε is; this shows that an increase in precision is useless if we want to know more about f's discretization. To do this, the best choice would be the study of ϕ. Of course, a perfect knowledge of ϕ may require errorless computations with large integers if x and y are large, otherwise its properties will *not be correctly detected.*

3.3. QUASI-AFFINE-TRANSFORMATIONS

We intend to call quasi-affine-transformation (QAT for short) $\mathbb{Z}^2$ mappings such as ϕ. This leads us immediately to the study of their numerous dynamical properties (cf. [10] and [8]). We must warn the reader that QATs possess many surprising properties. For example, this domain is very close to fractal geometry. Let us give a particular example, taking, in ϕ's definition, $a = 1$, $b = 1$, $c = -1$, $d = 1$ and $\omega = 2$. Figure 8 shows, for this mapping ϕ, the inverse image of the origin of order 7, that is, the set defined by $D_7 = \phi^{-7}(0)$.

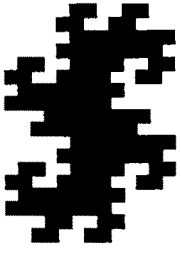


Fig. 8. The celebrated dragon curve obtained with a QAT.

We recognize the well-known dragon curves. A definition of D_k's through function ϕ leads to a new description of these fractal curves from which their properties can be developed (see ref. immediately above). This rather elementary example is nevertheless very instructive. It shows that a mere transcription of a discrete problem in our setting is a partial answer to some difficulties that come from quantization. Correctly converted, the problem reveals very quickly its deepest features, that it is a miscellany of arithmetics, dynamics and fractal geometry. At the same time, this example shows that the range of discrete notions is not organized in a simple manner: many domains, traditionally far apart in the classical point of view, interfere with each other as soon as quantization occurs.

3.4. THE EUCLIDEAN TRIANGLE'S PICTURE INDUCED ON $\mathbb{Z}^2$

It is rather easy to get examples of discretization that come from geometry. Let T be a usual triangle contained in an Euclidean plane. The very first question is: what is T's discretization? In the spirit of the truncation process explained before, this amounts to appyling the discretization process pointwise; this is the usual discretization giving the left lower corner of unit squares.

But this way of approximating T leads to numerous questions and difficulties. Here are some of them, illustrated by figs. 9 to 12 (the reader can produce as many as he or she wants to). We shall denote by P an Euclidean point and by $\overline{P}$ its canonical discretization ($\overline{P}$ is required to be an integer point).

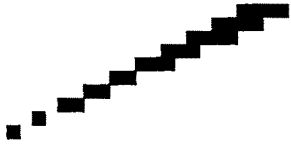


Fig. 9. A discretized triangle may be disconnected.

Another digitalization for T is simply given by the set of integer points it contains; this is closer to the principle of normalized discretization as being more invariant with respect to precision increasing. Higher precision digitalization amounts to considering integer points contained in homothetic magnifications of T. Nevertheless, this second discretization for T does not solve all former problems, though membership is clearer. It will not be surprising if we say that no intuitive solution exists; all the machinery of section 2 will be required to solve some of these questions. One can say the geometry which was, for a long time, the art of reasoning correctly from false patterns drawn on paper, nowadays has become, on computers, the art of reasoning from false numerical results giving false patterns when fortunately computations end. Let us observe that the first major difficulty is to find a convenient definition of discrete lines which makes their study possible.

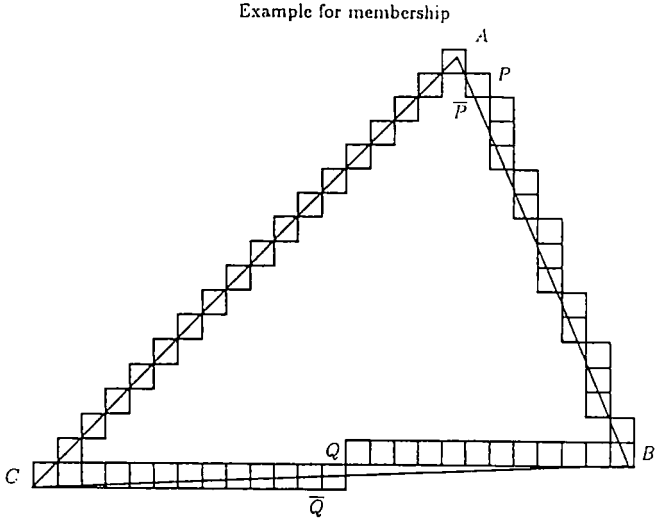


Fig. 10. If a rational triangle is given by the three vertices A, B and C, we can consider discrete sides (for example, in the sense of Bresenham) to convert it into a discrete triangle. But this leads to strange situations; for example, point P satisfies $P \notin T$ and $\overline{P} \in T$. On the other hand, point Q satisfies $Q \in T$ and $\overline{Q} \notin T$.

Fig. 11. A digitized triangle generally does not possess three vertices any longer.

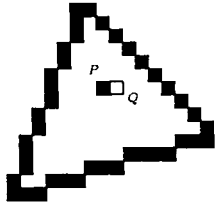


Fig. 12. The discretization of the three heights intersect at point P, while the discretization of the real orthocenter is point Q.

3.5. THE FUNDAMENTAL EXAMPLE OF DISCRETE LINES

When we look at and see how usual discrete objects are modified by digitalization (see, for example, the discretization of a real line in fig. 13), we may legitimately wonder if geometry is not completely lost through discretization.

Fig. 13. What occurs to Euclidean lines on a computer screen.

Figures 14 and 15 illustrate the puzzling problem of line intersection, which may also be void or infinite or contain any number of points. This gives an idea of the damages suffered by Euclidean geometry after digitalization.

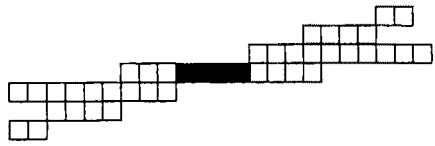


Fig. 14. Sometimes, line intersection is rather simple.

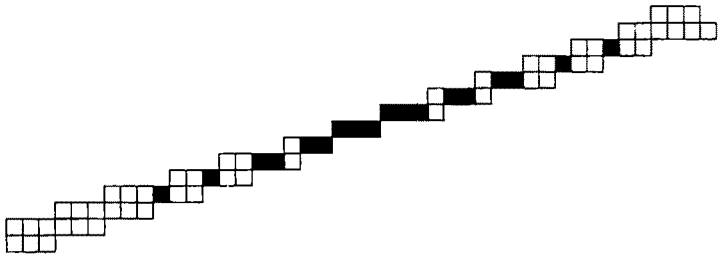


Fig. 15. Sometimes, line intersection can be complicated.

In Euclidean geometry, a false pattern is acceptable because its properties can still be obtained using simple axioms. In the discrete case, these axioms are lost; for example, there exist

- several discrete lines between two points,
- non-parallel lines with no common point,
- non-parallel lines with 18 common points (see fig. 15).

- subsegments whose slopes are different from the line including them. Hence, a lot of very important properties are lost when we go from continuous Euclidean geometry to discrete patterns of computer screens. Building discrete geometry is a difficult task.

For a long time, the only way to handle discrete lines was to use their definition as the set of the closest integer points from a given Euclidean line, or the set of points given by Bresenham's algorithm, which allows us to draw them (a short version of this algorithm is given below). Neither way, geometric or algorithmic is convenient to begin an actual study of these structures. The main reason comes from a simultaneous use of real and integer numbers (our arithmetization process is supposed to be able to solve this conflict).

```
y := 0
Error := b div 2;
drawpoint(0,0);
    for i := 1 to b do
        if error < b − a then
            begin
                error := error + a;
                drawpoint(i, y)
            end
        else
            begin
                error := error − b + a;
                y := y + 1;
                drawpoint(i, y)
            end;
```

A simplified version of Bresenham's algorithm.

We see, looking at Bresenham's algorithm, that it cannot answer the questions about discretization we presented above.

4. Ideal discrete geometry

In this section, we shall use the existence of infinite integers presented in section 1 to solve the difficult problem of constructing discrete geometry rigorously. We first build an ideal theory, as infinite integers are ideal integers possessing powerful properties, then we explain what this ideal discrete geometry says about standard discrete geometry.

4.1. BIG-POINTS ON THE HYPERFINITE SCREEN

To start our investigations, we can first try to keep a discrete screen which is supposed to be infinitely wide and measurable. This means that we can take an infinite integer ω for the width of the two edges of this square screen. We are indeed working within a hyperfinite square of $(\mathbb{Z}^*)^2$, denoted by $SQSC(\omega)$. Observing this screen, and thinking of proximity, it is clear that the vertices of the screen (seen as a square) are far from each other; and that neighbouring pixels are close. This closeness usually leads the Working Computer Scientist (WCS) to consider 4-connexity and 8-connexity. Unfortunately, the underlying topology is too far from the usual $\mathbb{R}$-topology needed by geometry. How can we make it more flexible in order to recover all Euclidean results? The answer already implicitly arises from the above.

Two points $A = (x_A, y_A)$ and $B = (x_B, y_B)$ of $(\mathbb{Z}^*)^2$ are *close* if and only if

$$\max(|x_A - x_B|, |y_A - y_B|) = \delta(A, B)$$

is infinitesimal in front of ω. Using ω-indiscernibility introduced in 1.1.3, this can also be written as

$$(x_A \approx x_B) \wedge (y_A \approx y_B).$$

We shall use the symbol $\delta \ll \omega$ to designate that integer δ is infinitely smaller than integer ω.

It must be emphasized that this integer $\delta(A, B)$ gives a notion of closeness. It has all the properties of a distance, but we save this denomination for the following:

$$d(A, B) = \frac{\max(|x_A - x_B|, |y_A, y_B|)}{\omega}.$$

Let A be an integer point, let us call it *big-point* associated to A, and denote $\overline{A}$ the collection (or coset) of all integer points M such that $d(A, M)$ is infinitesimal; ordinary integer points will still be called *points*. It is easy to see that the role of points within continuous geometry is held by these big-points. This can be done using a natural topology with the help of which we can recover the desired geometrical results. This topology is defined by the distance

$$\Delta(\overline{A}, \overline{B}) = [d(A, B)]^0.$$

The following result shows that big-points behave as usual Euclidean points; its proof follows immediately from definitions.

PROPOSITION 4.1

If big-points $\overline{A}$ and $\overline{B}$ have a common integer point, then $\overline{A} = \overline{B}$.

As usual for quotient spaces, the set of big-points associated with the ideal screen $SQSC(\omega)$ will be denoted by $SQSC(\omega)/\delta$.

The use of both notions of points allows us to solve the conflicts existing between Euclidean and discrete geometry. It is exactly here, for an easy management of these two notions at the same time, that the power of nonstandard analysis is required.

Remark

This paper is just a first introduction to ideal discrete geometry aiming to show how mathematics provides tools to solve many difficulties encountered in practice around discretization of continuous notions. We suppose implicitly some restrictions while constructing this geometry. First, we suppose our space of investigation is limited to our screen $SQSC(\omega)$, for example, point (ω^2, ω^2) is not considered; secondly, irrational numbers will be avoided.

Each of these limitations can be overcome using a little more of nonstandard analysis; for example, irrationals ξ can be replaced by infinitesimally close rational approximations $\xi \simeq \alpha/\beta$, with α and β infinitely large integers.

4.2. DISCRETE LINES ON THE HYPERFINITE SCREEN

Looking precisely at the way of thinking of Euclidean continuous geometry, we note that lines have both an ideal property of being without thickness and the physical property of having a thickness when drawn. To keep the physical thickness of lines, we introduce strips with a non-zero thickness, say $\tau \neq 0$, but to also keep the ideal property of thinness, we impose the fact that such a parameter τ must be infinitesimal in front of the width ω of edges of the screen. Let us note that it is the quotient τ/ω which is infinitesimal, so that it is consistent with the following assumptions:

- the parameters τ and ω are integers (condition of arithmetization);
- τ is hyperfinite (and so is ω).

To go into more detail, following the ideas contained in [15], a discrete line of rational direction (α, β) of width τ is the set of integer solutions (x, y) of the two inequalities

$$\gamma \leq \beta x - \alpha y < \gamma + \tau.$$

The meanings of parameters will become clearer and clearer as we go further into definitions and proofs; the width (or thickness) τ is not a metric notion, but rather an arithmetical one. If $x = 0$, this discrete line contains integer points whose ordinate satisfies $[(-\gamma - \tau)/\alpha] + 1 \leq y \leq [-\gamma/\alpha]$.

Here, the links between discrete and continuous geometry are given by the notion of the shadow line $\overline{D}$ of any discrete line D canonically determined by

$$\overline{D} = \{\overline{A} \in SQSC(\omega)/\delta \mid A \in D\}.$$

Within such a frame, it is time to list and prove some main results of continuous geometry in this altogether heuristically finite in one sense (because τ and ω are hyperfinite integers), infinite in another (because $\tau > n$ and $\omega > n$ for all standard n) and in any case discrete geometry (as one can see by the very definition of our screen).

4.3. HOW EUCLIDEAN GEOMETRY LIFTS TO IDEAL DISCRETE GEOMETRY

Our discrete version of the classical Euclidean theorems concerning lines (usually taken as axioms), providing a first step in a discrete axiomatization of geometry, is the following.

THEOREM 4.1 (bipoint determination)

Let A and B be two integer points of the screen $SQSC(\omega)$ such that $\Delta(\overline{A}, \overline{B})$ is appreciable, and let τ be a given integer such that $\mathbb{N} << \tau << \omega$. Then all discrete lines D with width τ passing through A and B have a unique shadow line $\overline{D}$.

Proof

Let $A = (x_A, y_A)$, $B = (x_B, y_B)$ be the given points. The hypothesis on A and B says that at least one of the two numbers $x_B - x_A$ and $y_B - y_A$ is not infinitely small with respect to ω. Eventually exchanging x and y, we can suppose that it is $x_B - x_A$. Let D's inequations be

$$\gamma \leq ax - by < \gamma + \tau,$$

where a, b and γ are integers, and τ is an arithmetic width satisfying the above conditions. Also, let $M = (x_M, y_M)$ be a point in discrete line D. We will suppose that M is ω-limited, which means that a standard integer s exists such that $\Delta(\overline{O}, \overline{M})$ is bounded by $s\omega$; this allows us to treat points off the screen $SQSC(\omega)$ but not too far. Let us recall the meaning of the hypothesis $\Delta(A, B)$ *is appreciable* imposed on big-points $\overline{A}$ and $\overline{B}$; this condition means that this (real) value must be non-infinitely small and ω-limited. This amounts to saying that $\Delta(\overline{A}, \overline{B})$ is infinitely close to a non-zero standard real number. Translated into ordinary points A and B, this means that there exists a standard integer s such that

$$\frac{\omega}{s} \leq \delta(A, B) \leq s\omega.$$

From the hypothesis on A, B and M, we can immediately deduce that the rational number

$$\frac{x_M - x_A}{x_B - x_A}$$

is limited (i.e. bounded by a standard real number). Let us consider point $R = (x_M, y_R)$, with the same abscissa x_M as M, belonging to the real line passing through A and B. We point out that although point M is an integer, R is generally rational. We must show that, for all authorized y_M values, the difference $|y_M - y_R|$ is bounded by an integer which is infinitely small with respect to ω. The equation of line AB is

$$(y_B - y_A)(x - x_A) - (x_B - x_A)(y - y_A) = 0,$$

from which we get

$$y_R = y_A + (x_M - x_A)\frac{(y_B - y_A)}{(x_B - x_A)}.$$

From the definition of A and M, there exist integers τ_A and τ_M in interval $[\gamma, \gamma + \tau[$ such that we have equalities

$$ax_A - by_A = \gamma + \tau_A$$

$$ax_M - by_M = \gamma + \tau_M,$$

leading to

$$y_R = \frac{1}{b}x_A - \frac{(\gamma + \tau_A)}{b} + (x_M - x_A)\frac{(y_B - y_A)}{(x_B - x_A)}$$

and

$$y_M = \frac{a}{b}x_M - \frac{(\gamma + \tau_M)}{b}.$$

Forming the difference of ordinates $y_M - y_R$, we obtain

$$|y_M - y_R| = \left|(x_M - x_A)\left(\frac{a}{b} - \frac{y_B - y_a}{x_B - x_A}\right) + \frac{\tau_A - \tau_M}{b}\right|,$$

which can be written as

$$|y_M - y_R| = \left|\frac{1}{b}\left(\frac{x_M - x_A}{x_B - x_A}\right)(a(x_B - x_A) - b(y_B - y_A)) + \frac{\tau_A - \tau_M}{b}\right|.$$

The definition of B gives, as for A, the existence of an integer $\tau_B \in [\gamma, \gamma + \tau[$ such that we have

$$ax_B - by_B = \gamma + \tau_B;$$

from this, it is easily deduced that $|a(x_B - x_A) - b(y_B - y_A)| \leq \tau$. As we also have $|\tau_A - \tau_M| \leq \tau$, we obtain

$$|y_M - y_R| \leq \left|\frac{\tau}{b}\right| \left|\frac{x_M - x_A}{x_B - x_A}\right| + 1.$$

But $\Delta(\overline{A}, \overline{B})$ being appreciable, we have seen above that $(x_M - x_A)/(x_B - x_A)$ is bounded by a standard number whence $|y_M - y_R|$ is bounded by τ times a standard integer and is effectively *small* with respect to ω. □

THEOREM 4.2 (crossing lines)

Two given lines D and D' with respective different standard rational slopes have a nonempty intersection contained in the unique coset $\overline{A}$ of any point A of that intersection. Moreover, the big-point $\overline{A}$ satisfies $\{\overline{A}\} = \overline{D} \cap \overline{D}'$.

Proof

The theorem first asserts that there is a point $M \in D \cap D'$. Let us suppose these discrete lines respectively defined by inequations

$$\gamma \leq ax - by < \gamma + \tau, \qquad (D)$$

$$\gamma' \leq a'x - b'y < \gamma' + \tau', \qquad (D')$$

where a, b, a' and b' are standard and their arithmetic width τ and τ' are infinitely large integers which are infinitesimal with respect to ω; we also suppose $gcd(a, b) = gcd(a', b') = 1$; let $\delta = a'b - ab'$ be the determinant, which can be supposed positive. Any solution to inequations (D) and (D') is of the form

$$ax - by = \varepsilon,$$

$$a'x - b'y = \varepsilon',$$

where $\varepsilon \in [\gamma, \gamma + \tau[$ and $\varepsilon' \in [\gamma', \gamma' + \tau'[$. To solve this system we use Bezout's theorem, which gives two standard integers u and v such that $au - bv = 1$. Solutions of the first equation are $(x, y) = (kb + \varepsilon u, ka + \varepsilon v)$. Carrying back in the second equation, we obtain one integer k satisfying the equation

$$\delta k = (a'u - b'v)\varepsilon - \varepsilon',$$

which implies that the system associated with intersection $D \cap D'$ has integer solutions if and only if there are two integers ε and ε' in their respective intervals such that

$$\varepsilon' \equiv (a'u - b'v)\varepsilon \mod \delta.$$

If a solution exists, there is an integer m such that

$$\varepsilon' = (a'u - b'v)\varepsilon + m\delta,$$

from which we immediately deduce that the (x, y) solution is

$$(x, y) = (u\varepsilon + bm, v\varepsilon + am).$$

A solution to the system $(D) \cap (D')$ does exist because, for any ε, δ being standard and τ' infinitely large, there are values of m such that

$$(a'u - b'v)\varepsilon + m\delta \in [\gamma', \gamma' + \tau'[.$$

We now consider the constraints on ε', say $\gamma' \leq \varepsilon' < \gamma' + \tau'$; from the above expression for ε' and the bounds on ε, we can deduce the bounds on integer m. First we have

$$\gamma' \leq m\delta + (a'u - b'v)\varepsilon < \gamma' + \tau',$$

then

$$\gamma' - (a'u - b'v)\varepsilon \leq m\delta < \gamma' + \tau' - (a'u - b'v)\varepsilon.$$

Using ε's bounds, we have (if $a'u - b'v \geq 0$),

$$\gamma' - (a'u - b'v)(\gamma + \tau) \leq m\delta < \gamma' + \tau' - (a'u - b'v)\gamma.$$

But the difference between these last bounds is exactly

$$\tau' + |a'u - b'v|\tau,$$

from which we can deduce that m belongs to an interval of length

$$\left[\frac{\tau' + |a'u - b'v|\tau}{\delta}\right] = \tau''.$$

A similar conclusion can be made if $a'u - b'v < 0$. This last bound τ'' is, as required, infinitely large but small with respect to ω; moreover, this length is bounded by $\tau + \tau'$ because $|a'u - b'v| < \delta$ and $\delta > 1$. An easy consequence of this bound for m is that for two different solutions (x_1, y_1) and (x_2, y_2) of system $D \cap D'$ we have, with obvious notations,

$$|x_1 - x_2| \leq |u(\varepsilon_1 - \varepsilon_2)| + |b(m_1 - m_2)| \leq |u|\tau + |b|\tau'',$$
$$|y_1 - y_2| \leq |v(\varepsilon_1 - \varepsilon_2)| + |a(m_1 - m_2)| \leq |v|\tau + |a|\tau''.$$

The last assertion of this theorem is then obvious. □

Let us point out that a, b, a', b' being all standard from the hypothesis, then *the slopes are different standard rationals*. If that were not the case we could have, for example, a, b standards and a', b' infinitely large, such that both rationals a/b and a'/b' would have been infinitely close. But then the length of the interval

containing m values could have been ω-appreciable and thus not negligible in front of ω. This theorem can be generalized to nonstandard slopes $a/b \neq a'/b'$, where a, b, a' and b' are infinitely large integers.

THEOREM 4.3 (Euclid postulate)

Let D be a discrete line with given slope α and given width τ such that $\mathbb{N} << \tau << \omega$ and A be an integer point such that the big-point $\overline{A}$ does not belong to $\overline{D}$. Let τ' be a given integer such that $\mathbb{N} << \tau' << w$; then any discrete line D' with width τ' and slope infinitely close to α has the same shadow $\overline{D'}$ (the parallel to $\overline{D}$ passing through $\overline{A}$).

Proof

The proof results immediately from the following lemma, which says that close enough lines have the same macroscopic trace. □

LEMMA

Let D and D' be two discrete lines, whose slopes are infinitely close, containing an integer point A; then $\overline{D} = \overline{D'}$.

Proof

With now usual notations, both lines are defined as

$$\gamma \leq ax - by < \gamma + \tau, \tag{D}$$

$$\gamma' \leq a'x - b'y < \gamma' + \tau', \tag{D'}$$

with $\mathbb{N} << \tau, \tau' << w$. We also suppose that $b > 0$, $b' > 0$ and determinant $\delta = ab' - a'b > 0$, which implies $a'/b' < a/b$. This is not a restriction. The hypothesis on the slopes says that the difference $a/b - a'/b'$ is infinitesimal. We also use integers u and v which, by Bezout's theorem, satisfy the relation: $au - bv = 1$. Point $A = (x_A, y_A)$ belonging to $D \cap D'$ and two integers $\varepsilon \in [\gamma, \gamma + \tau[$ and $\varepsilon' \in [\gamma', \gamma' + \tau'[$ exist such that

$$ax_A - by_A = \varepsilon,$$

$$a'x_A - b'y_A = \varepsilon'.$$

The proof of the previous theorem showed us that this system accepts a solution (x_A, y_A), thus values $\gamma + \varepsilon$ and $\gamma' + \varepsilon'$ are necessarily tied by the congruence

$$\varepsilon' \equiv (a'u - b'v)\varepsilon \mod \delta,$$

which says that integer $m = vx - uy$ is such that

$$\gamma' = -\varepsilon' + (a'u - b'v)(\gamma + \varepsilon) + m\delta.$$

We must now consider two points in D and D' having the same abscissa x and different respective ordinates y and y', and show that the value $(y-y')/\omega$ is infinitesimal; for the same reasons as those mentioned in the preceding theorems we can suppose x is ω-limited. We can draw y and y' from Ds and D's above inequations; this gives

$$\frac{1}{b}(ax-\gamma-\tau+1) \le y < \frac{1}{b}(ax-\gamma+1), \tag{1}$$

and

$$\frac{1}{b'}(a'x-\gamma'-\tau'+1) \le y' < \frac{1}{b'}(a'x-\gamma'+1). \tag{2}$$

Subtracting eqs. (1) and (2), we obtain the inequalities

$$\left(\frac{a}{b}-\frac{a'}{b'}\right)x+\frac{\gamma'}{b'}-\frac{\gamma}{b}+\frac{1-\tau}{b}+\frac{1}{b'} \le y-y'$$

$$\le \left(\frac{a}{b}-\frac{a'}{b'}\right)x+\frac{\gamma'}{b'}-\frac{\gamma}{b}+\frac{\tau'-1}{b}+\frac{1}{b}.$$

Dividing this equation by ω gives

$$\left(\frac{a}{b}-\frac{a'}{b'}\right)\frac{x}{\omega}+\frac{1}{\omega}\left(\frac{\gamma'}{b'}-\frac{\gamma}{b}\right)+\frac{1-\tau}{\omega b} \le \frac{y-y'}{\omega}$$

$$\le \left(\frac{a}{b}-\frac{a'}{b'}\right)\frac{x}{\omega}+\frac{1}{\omega}\left(\frac{\gamma'}{b'}-\frac{\gamma}{b}\right)+\frac{\tau'-1}{\omega b}+\frac{1}{\omega b}.$$

To conclude the proof, it is sufficient to show that left and right members are infinitesimal. This amounts to proving that each term occurring in these sums is infinitesimal:

- The term $(a/b-a'/b')x/\omega$ is infinitesimal because $(a/b-a'/b')$ is infinitesimal and x/ω is bounded by a standard integer.
- For $1/\omega(\gamma'/b'-\gamma/b)$, we first observe that $\gamma'/b'-\gamma/b = \varepsilon/b-\varepsilon'/b' + x_A(a'/b'-a/b)$ (multiply relations defining x_A and y_A respectively by b' and b, form their difference and use $\delta = ab'-a'b$. Then we get $1/\omega(\gamma'/b'-\gamma/b) = 1/\omega(\varepsilon/b-\varepsilon'/b') + x_A/\omega(a'/b'-a/b)$ but $\varepsilon < \tau$ and $\varepsilon' < \tau'$, arithmetical widths τ and τ' being infinitesimal with respect to ω, and x_A/ω is bounded by a standard integer. We can then deduce from these bounds that $1/\omega(\gamma'/b'-\gamma/b)$ is infinitesimal.
- The final terms $(1-\tau/\omega b'$, $(\tau'-1)/\omega b$ and $1/\omega b$ are obviously infinitesimal. □

The introduced ideal lines are somehow regular because we supposed their slope is *rational* and *standard*, a and b being standard integers. This is not a real

limitation; we can introduce *nonstandard* discrete lines with a and b infinitely large integers, arithmetical width τ being restricted by $\max(|a|, |b|) << \tau << \max(|a|, |b|)\omega$. Nonstandard lines can be seen as discretization of Euclidean lines with irrational slope; previous theorems can be generalized, with slight modifications, to these lines.

4.4. THE STATUS OF IDEAL DISCRETE GEOMETRY. THE WAY TO STANDARD DISCRETE GEOMETRY

The previous theorems are examples of properties of discrete lines we introduced. They should convince the reader that all Euclidean notions and theorems can be adapted, in the same fashion, for conveniently defined discrete objects; their totality will form ideal discrete geometry (IDG for short). This geometry is then a perfect discretization of Euclidean geometry (abbreviated to EG) because any classical result has an IDG version and every IDG result gives in return a macroscopic, Euclidean, similar property. Nothing is lost going from EG to IDG. In other words, the last theory is an infinitesimal deformation of the first; we also say that ideal discrete geometry is potentially equivalent to Euclidean geometry. But this does not mean that EG and IDG have the *same* properties; an infinitesimal drift is indeed present. Let us consider how line intersection depends on their angle. In EG, this intersection is a point if the angle is non-zero and a line if it is zero. This dependence is *non-continuous*. Besides, for two discrete lines their intersection increases regularly from a small number of integer points when the angle is standard to a very large number when this angle decreases toward infinitesimal values. It is not difficult to generalize theorem 4.2 and prove that discrete line intersection depends *continuously* on their angle. The remarkable fact is that these different behaviours do not prevent an exact conversion of properties from one theory to the other; this equivalence relies on the strength of standard part function.

What occurs if we decrease the size of our screen $SQSC(\omega)$? As long as ω remains an infinitely large integer, we can show that all discrete models $SQSC(\omega)$ of the continuous plane are equivalent. But when ω lands in standard territory, the situation is completely different: $SQSC(\omega)$'s topology is a discrete topology (in the classical sense: every set is open) and its geometry is now *very far* from Euclidean. We are now in the usual domain of discrete geometry (DG for short), that of computer science. Hence, we can travel from continuum to discrete through a hyperfinite number of steps.

Two main remarks have to be made at this point. We have a whole family of *geometries*, those of all screens $SQSC(\nu)$ for $\nu = \omega, \omega - 1, \omega - 2, \ldots, 1024, 1023, \ldots, 512, \ldots$, the last ones being usual computer screens. From our point of view, this is a one-parameter family of geometries and this family is heuristically continuous. This explains how objects or properties can travel along this route from EG to DG through the intermediate state given by IDG. This allows us to predict

that EG can leave impressions on DG. More precisely, if we are trying to define or study new DG objects, let us say a notion $\mathcal{N}$, it is very helpful to do it for the whole chain of notions $\mathcal{N}(v)$ at once. That is, we try to work for all screen resolutions at the same time and especially for those with infinitely large values where continuous geometry is potentially true. Moreover, good discrete notions $\mathcal{N}(v)$ will have a corresponding notion in IDG, which is of invaluable help to decide if $\mathcal{N}(v)$ has some interest in DG. For example, IDG says that arithmetical width τ of discrete lines is a good notion. The last section of this paper is simply a by-product of this observation.

5. Standard discrete geometry

5.1. STANDARD DISCRETE LINES

At the beginning of section 4, we reminded the reader how lines are digitalized on computer screens with the help of Bresenham's algorithm. It is well known that, if a Euclidean line D is given, this discretization $\mathcal{D}$ is made up of the set of integer points which are the closest to D. Consequently, this discrete line has a *functional* property: for all integer values of the variable, there is one and only one point of $\mathcal{D}$ having this abscissa (in other words, these lines are 8-connected and not 4-connected). But we can ask if this notion of a discrete line is convenient for building up a discrete geometry. The answer is no. We can already understand the main reason for this: if a good theory is obtained with these lines on standard screens, i.e. $SQSC(v)$ with v standard, then we can follow the way to the continuum and we should, for infinitely large values of v, obtain geometries equivalent to IDG. But our study of IDG's axiomatics shows that arithmetical thickness has often to be infinitely large if we want to obtain general and easy theorems. Thus is it very natural, and in fact *unavoidable*, to introduce a notion of discrete lines where arithmetical thickness is a new parameter independent of slope and ordinate at the origin. This leads us to the following definition, which first appeared in [15].

DEFINITION 5.1

A discrete rational line $\mathcal{D}$ is the set of integer solutions (x, y) of inequalities

$$\gamma \leq ax + by < \gamma + \omega,$$

where a, b, γ, ω are integers and $\omega > 0$; we denote it $\mathcal{D}(a, b, \gamma, \omega)$.

The values a, b define $\mathcal{D}$'s slope, γ and $\gamma + \omega$ are $\mathcal{D}$'s bounds, and ω is $\mathcal{D}$'s arithmetical thickness.

In addition to the theoretical vindication of arithmetical thickness, many other reasons to introduce this notion can be found afterwards; they all support this

way of defining discrete lines. Even if we do not study them in what follows, let us give some of these motivations.

- If we consider different discretizations of a continuous line, all are particular cases of our discrete line notion for well-chosen τ values. Consider, for example, the set of pixels across a given Euclidean line; this discretization is in fact *thicker* than Bresenham's line, but this is exactly what we obtain using our notion if we take $\tau = |a| + |b|$. Other cases also fit perfectly.
- The thickness of lines allows a discrete version of stretching and folding which is inaccessible to usual discrete notions. This possibility is valuable in the study of metric properties of discrete lines or discrete transformations.
- Definitions of higher dimensional lines, planes, hyperplanes, etc. are obvious from our point of view. Moreover, the consideration of discrete planes immediately shows that their plane sections are general discrete lines such as we have just introduced.

5.2. ARITHMETICS OF DISCRETE LINES. MODULAR CALCULUS AND ALGORITHMICS

A former definition of discrete lines requires the study of their algorithmic properties. Up to now, we have not been able to decide if the general notion is, from an algorithmical point of view, as simple as Bresenham's lines or more complicated. In other words, is the the interest in these new lines only theoretical or also practical? In what follows, we will show that general discrete lines contain Bresenham's lines and that they are, algorithmically, as simple. To obtain this answer, we will follow a simple idea, which goes back very far in the history of science, but has been rather overlooked. Prior to 1750, the astronomer Jean Bernoulli introduced *Une Nouvelle Méthode de Calcul*, which was an arithmetical treatment of linear rational interpolation. He observed that if we want to interpolate a linear rational function

$$y = \frac{a}{b}x$$

for rational values of abscissa x, it is very convenient to work with *radix* b. Jean Bernoulli observed that the knowledge of the sequence

$$ax \text{ modulo } b, \text{ for } x = 0, 1, \ldots, b-1$$

is sufficient to compute the values of the function y for all abscissa

$$x = x_2 x_1 x_0 \cdot x_{-1} x_{-2} x_{-3} x_{-4} \cdots$$

written in radix b; this means x_i's are digits, i.e. $x_i \in [0, b[$. With proper shifting of digits, it is sufficient to compute the values for abscissa equal to $x = x_n x_{n-1} \cdots x_1 x_0$, the result being given by $y = y_{n+1} y_{n-1} \cdots y_1 y_0$, $y_i \in [0, b-1[$. Introducing sequence

r_i for carries defined by $r_0 = 0$, and for $0 \leq i \leq n$ $r_{i+1} = [(ax_i + r_i)/b]$, y_i values are given by

$$y_i = \left\{\frac{ax_i + r_i}{b}\right\}, \quad 0 \leq i \leq n,$$

and $y_{n+1} = r_{n+1}$.

This computation uses modular evaluation and integer parts, but an occurring integer part function has a limited domain, interval $[0, b-1[$, and can also be studied with modular evaluation; it is indeed a discrete line. J. Bernoulli, who was the first to be interested in this structure, developed algorithms allowing fast modular evaluation if values $ax \bmod b$ are already computed: only easy carry reports have to be done. Here is what he said about the computing method he derived from this:

> "*... Et cette méthode est d'une telle facilité dans l'application, qu'on est souvent en état d'écrire, sans autre calcul, les produits de plus de 1000 règles de trois, en deux heures de tems.*" [4]

His concern with computing time (besides that of numeration basis) seems very modern. His position as an astronomer explains that he certainly needed to compute extensively and was already interested in fast algorithms. Let us restrict this study to the, so-called, naive lines which, by definition, satisfy condition $\tau = \max(|a|, |b|)$. It is easy to prove tht naive lines are 8-connected. For convenience, we also suppose $\mathcal{D}$'s inequations are $\gamma \leq ax - by < \gamma + \tau$, and that parameters a and b satisfy both of the following conditions: $-\ 0 \leq a < b$ – greatest common divisor of a and b is equal to 1, we can express $\mathcal{D}(a, b, \gamma, \tau)$'s y values as a function of x. We obtain, using $\tau = b$, that

$$y = \left\lceil \frac{ax - \gamma}{b} \right\rceil \quad \text{for } x \in \mathbb{Z}.$$

Denoting, respectively, by $[m/n]$ and $\{m/n\}$ the quotient and the rest of the Euclidean division of m by n, we can write the identity

$$ax - \gamma = \left\lceil \frac{ax - \gamma}{b} \right\rceil b + \left\{\frac{ax - \gamma}{b}\right\},$$

where $\{(ax - g)/b\} \in [0, b[$, or alternatively

$$\frac{ax - \gamma}{b} = \left\lceil \frac{ax - \gamma}{b} \right\rceil + \frac{\{(ax - \gamma)/b\}}{b}.$$

[4] *... and this method is so easy to apply that we can write, without computation, the result of more than a thousand rules of three, within two hours.*

This proves that the discrete naive line $D(a, -b, \gamma, b)$ is formed by all the integer points situated immediately below the Euclidean line whose equation is

$$y = \frac{ax - \gamma}{b},$$

and that errors made in replacing exact rational values by the integer part $[(ax-\gamma)/b]$ are all proportional to the values of the modular sequence $\{(ax-\gamma)/b\}$, $x \in \mathbb{Z}$. Let us observe now that this modular sequence is nothing but the repetitive addition of the constant value a, this evaluation being made modulo b. The immediate consequence of this is that if for a certain integer value x we have

$$\left\{\frac{ax - \gamma}{b}\right\} < \left\{\frac{a(x+1) - \gamma}{b}\right\},$$

then we also have equality $\{[a(x + 1) - \gamma]/b\} = \{(ax - \gamma)/b\} + a$. Adding a to both sides of the former Euclidean division equation, we get

$$ax - \gamma + a = \left[\frac{ax - \gamma}{b}\right] b + \left\{\frac{ax - \gamma}{b}\right\} + a,$$

hence

$$a(x+1) - \gamma = \left[\frac{ax - \gamma}{b}\right] b + \left\{\frac{a(x+1) - \gamma}{b}\right\},$$

which is a Euclidean division equality; unicity says that for such x we have

$$\left[\frac{ax - \gamma}{b}\right] b = \left[\frac{a(x+1) - \gamma}{b}\right].$$

We have proved the main part of the following proposition.

PROPOSITION 5.1

The horizontal steps of the discrete naive line $\mathcal{D}(a, -b, \gamma, b)$, a, b satisfying the previous hypothesis, are in a one-to-one correspondence with ascending parts of the modular sequence $\{(ax - \gamma)/b\}$.

The last part of this result says that the jumps between horizontal steps correspond exactly to descending parts of this modular sequence; the proof follows by similar arguments. This proposition has two fundamental consequences. First, it says that:

All geometric information contained in a discrete naive line is contained in a modular sequence $\{ax/b\}$.

This general principle can be pursued much further. The proposition is the key result to obtain many fast algorithms to draw generalized lines (see [15]). Let us give the first of these algorithms.

Let us denote by $y_0(x) = [ax/b]$ and $y_1(x) = \{ax/b\}$ the two sequences associated with the particular naive line $0 \leq ax - by < b$ (former hypothesis $0 \leq a < b$ and $gcd(a, b) = 1$ are still valuable). The second sequence is periodical with period b; consequently, the first one is pseudo-periodical and its periodicity vector is (b, a). We immediately obtain the simple algorithm:

Starting with a **zero** *value, then*

- *if the current value is strictly lower than* $b - a$, *then* **add** a
- *otherwise* **subtract** $b - a$.

For example, let us take $a/b = 5/17$, and collect values of the first period of both sequences in table 2.

Table 2

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
y_0	0	0	0	0	1	1	1	2	2	2	2	3	3	3	4	4	4
y_1	0	5	10	15	3	8	13	1	6	11	16	4	9	14	2	7	12

In the second period, $x \in [17, 33]$, y_0 values are the same as the preceding ones increased by 5; those of the y_1 sequence are the same. For a general naive line, with $\gamma \neq 0$, the algorithm is the same except we start with a value equal to $\{\gamma/b\}$ and $y_0 = [\gamma/b]$.

5.3. THE RELATION BETWEEN DISCRETE LINES AND BRESENHAM'S LINES

Let D be the rational *Euclidean* line whose equation is

$$ax - by + c = 0.$$

By definition, Bresenham's line associated to D is the set of integer points which are the closest to D. Let us prove it is precisely the discrete and naive line:

$$\mathcal{D}\left(a, -b, -c - \left[\frac{b}{2}\right], b\right).$$

We will prove this in the particular case $c = 0$, the general case following easily. If $x \in \mathbb{Z}$, then if b is odd ot if b is even and $\{ax/b\} \neq [b/2]$, the integer point which is closest to $(x, ax/b)$ is given by

$$\begin{cases} \left[\frac{ax}{b}\right] & \text{if } \left\{\frac{ax}{b}\right\} \leq \left[\frac{b}{2}\right], \\ \left[\frac{ax}{b}\right] + 1 & \text{if } \left\{\frac{ax}{b}\right\} > \left[\frac{b}{2}\right]. \end{cases}$$

Otherwise (b even and $\{ax/b\} = [b/2]$) there are two closest integer points, $[ax/b]$ and $[ax/b] + 1$. The preceding formula gives the first one, that is, $[ax/b]$. This sequence, which at first sight needs two formulas for its generation, is identical with the sequence $(x, [(ax + [b/2])/b]$. To see this, we just have to consider both Euclidean division identities

$$ax + \left[\frac{b}{2}\right] = \left[\frac{ax - \left[\frac{b}{2}\right]}{b}\right] b + \left\{\frac{ax - \left[\frac{b}{2}\right]}{b}\right\}$$

and

$$ax + \left[\frac{b}{2}\right] + \left[\frac{b}{2}\right] = \left[\frac{ax}{b}\right] b + \left\{\frac{ax}{b}\right\} + \left[\frac{b}{2}\right],$$

and the equality

$$\left\{\frac{ax + \left[\frac{b}{2}\right]}{b}\right\} = \left\{\frac{\left\{\frac{ax}{b}\right\} + \left[\frac{b}{2}\right]}{b}\right\}.$$

They show that if $\{ax/b\} \leq [b/2]$, we have inequality $\{ax/b\} + [b/2] \leq b$, otherwise we have inequalities $b \leq \{ax/b\} + [b/2] < 2b$. In the first case, we can deduce that both Euclidean division equalities are identical and consequently we have: $[(ax + [b/2]/b] = [ax/b]$. In the second case, we get the relation $[(ax + [b/2]/b] = [ax/b] + 1$. In all cases, we have verified that $(x, [(ax + [b/2]/b])$ is the integer point which is the closest to the rational point $(x, ax/b)$, from which is follows that Bresenham's line associated with Euclidean line D is indeed $\mathcal{D}(a, -b, -c - [b/2], b)$. Other computations in the same vein lead us to the following:

PROPOSITION 5.2

All discrete lines with the same parameters a, b and τ are equal within a plane integer translation.

Consequently we see, as an example, that Bresenham's line associated with D and the discrete line of rounded points, that is, $\mathcal{D}(a, b, -c, b)$, are equal within translation. Any property true for Bresenham's notion is also true for our naive discrete lines and reciprocally. Since our definition is more manageable, this equivalence is interesting.

5.4. SYMMETRIES OF DISCRETE LINES

Here is one example of the advantage of our lines: their symmetries can be pulled much more directly than using Bresenham's definition. In fact, they follow directly from our definition.

Let $\mathcal{D}(a, b, \gamma, \tau)$ be a discrete line, then its transform by symmetry with respect to

- Ox is $\mathcal{D}(a, -b, \gamma, \tau)$,
- Oy is $\mathcal{D}(-a, b, \gamma, \tau)$,
- O is $\mathcal{D}(-a, -b, \gamma, \tau)$ or $\mathcal{D}(a, b, -\gamma - \tau + 1, \tau)$,
- line $X = x_0$, $x_0 \in \mathbb{Z}$, is $\mathcal{D}(-a, b, \gamma - 2ax_0, \tau)$,
- line $Y = y_0$, $y_0 \in \mathbb{Z}$, is $\mathcal{D}(a, -b, \gamma - 2by_0, \tau)$,
- point (x_0, y_0) is $\mathcal{D}(-a, -b, \gamma - 2(ax_0 + by_0), \tau) = \mathcal{D}(a, b, -\gamma + 2(ax_0 + by_0) - \tau + 1, \tau)$.

Moreover, line $\mathcal{D}(a, b, \gamma, \tau)$ contains symmetry points if and only if its thickness τ is odd; in this case, its symmetry points are the solutions of the diophantine equation $ax + by = \gamma + [\tau/2]$.

These properties of discrete lines explain why we can restrict our study, in accordance with our recurring hypothesis: $0 \leq a < b$ and $gcd(a, b) = 1$, to lines contained in the first octant.

5.5. ARITHMETICS AGAIN: LINEAR RECIPROCITY AND STEP END FORMULAS

The nice thing about generalized discrete lines is that they are pure arithmetical objects (more precisely, they belong to the geometry of numbers). Considering them as such is by far the most fruitful point of view, the best way to translate and solve real-life probems when they occur. It is very surprising to consider theoretical questions obtained by translating actual questions. They may be elementary or deeper arithmetic results or entirely new queries. Once again, using a computer initiates new abstract matters. In the last pages of this paper, we will somehow argue this point without being able to exhaust it. Discrete lines, as we have seen, are made of horizontal steps; we would like to know a little more about this structure: is there, for example, a law which will give the successive lengths of these steps? This question will be tackled using elementary arithmetic tools. Under the standing hypothesis on parameters a and b, we will now prove a formula, well known to mathematicians, which expresses how the *reciprocal* function of a discrete naive line works. Here, this formula has a geometric flavour which explains it nicely and which can, once understood, answer our question. We know that the application $\lambda : \mathbb{Z} \to \mathbb{Z}$, such that $\lambda(x) = [ax/b]$, is not *linear* at all; nonetheless, this discretization of a linear function reminds us of a little of continuum life (another example of continuous mark) and satisfies the following formula, which says that function λ is a kind of *reciprocal* of funtion $\kappa(x) = [bx/a]$; the composition $\lambda \circ \kappa$ is *close to identity*. But we warn the working computer scientist that the other composition, $\kappa \circ \lambda$, is not the identity.

PROPOSITION 5.3

If $0 \leq a < b$ and $gcd(a, b) = 1$, then we have

$$\left\lfloor \frac{a\left\lfloor \frac{bx}{a} \right\rfloor}{b} \right\rfloor = \begin{cases} x-1 & \text{if } x \not\equiv 0 \bmod a, \\ x & \text{if } x \equiv 0 \bmod a. \end{cases}$$

Proof

Let $\phi(x) = [a[bx/a]/b]$ denote the composition $\lambda \circ \kappa$. If x is an integer multiple of a, we have

$$\phi(x) = \left\lfloor \frac{a\frac{bx}{a}}{b} \right\rfloor = [x] = x.$$

If x is not an integer multiple of a, the rational bx/a is not integer (we supposed $gcd(a, b) = 1$). Thus, $[bx/a] < bx/a$. We easily deduce the following upper bounds:

$$\frac{a}{b}\left\lfloor \frac{bx}{a} \right\rfloor < x$$

and

$$\phi(x) < x.$$

The next lower bounds are clear:

$$\left\lfloor \frac{bx}{a} \right\rfloor > \frac{bx}{a} - 1,$$

$$\frac{a}{b}\left\lfloor \frac{bx}{a} \right\rfloor > x - \frac{a}{b},$$

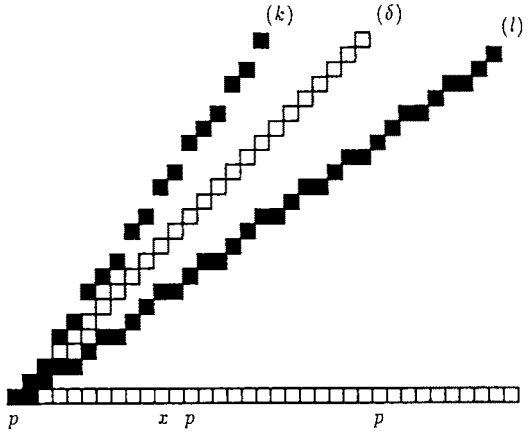
$$\left\lfloor \frac{a}{b}\left\lfloor \frac{bx}{a} \right\rfloor \right\rfloor > \frac{a}{b}\left\lfloor \frac{bx}{a} \right\rfloor - 1 > x - \frac{1}{b} - 1.$$

Reminding the reader that a/b is lower than 1, we obtain

$$\phi(x) > x - 2,$$

whence the result. □

The geometrical interpretation is as follows. The graph of function κ is a discrete line of slope greater than 1, it is *injective*, so that is loses no information; function λ recovers that information. If we compose the other side, the story is not the same: function λ begins to lose information. Within horizontal steps, integer values are mapped onto the same point; if these are coloured pixels, for example, the last in wipes former ones out, nothing can be done to recover them.



Linear reciprocity formula
a=12, b=17

Fig. 16. Start with an abscissa x, then go to up to curve (k) of slope 17/12, then reflect on diagonal (δ) and go down to line (l) of slope 12/17 and go back horizontally to diagonal (δ). We always reach abscissa $x = 1$ except for periodically spaced points $p = 12k$, where we reach p again.

COROLLARY (linear reciprocity formula)

If $0 \leq a < b$ and $gcd(a, b) = 1$, then we have for integers x the identity

$$\left[\frac{a\left[\frac{bx-1}{a}\right]}{b}\right] + 1 = x.$$

The corollary follows immediately from the former identity and we would like to make one remark which is the content of the next forthcoming lemma.

This formula says that function $[ax/b] + 1$ is the *left inverse* of function $[(bx - 1)/a]$; they are, respectively, slight perturbations of the functions λ and κ we considered above. The linear reciprocity formula will be used in one or another form: as in proposition or corollary. This reciprocity formula has nice consequences for discrete lines. Let us give two of them.

First, it implies that the lengths of horizontal steps forming the discrete line given by function $\lambda(x) = [ax/b]$ are always the integers $[b/a]$ and $[b/a] + 1$. Of course, both lengths are equal to b if $a = 1$.

Secondly, it gives a formula for the abscissa X_n of the last point of the nth horizontal step. This formula is given by the following proposition.

PROPOSITION 5.4 (step end formula)

We have

$$X_n = \left\lceil \frac{bn-1}{a} \right\rceil, \quad n \in \mathbb{Z},$$

and, by convention, we give index $n = 1$ to the horizontal step beginning with 0.

Proof

We begin by showing two lemmas.

LEMMA 1

For any integer value x, we have the identity

$$\left\lceil \frac{bx-1}{a} \right\rceil = \begin{cases} \left\lceil \frac{bx}{a} \right\rceil & \text{if } x \not\equiv 0 \bmod a, \\ \left\lceil \frac{bx}{a} \right\rceil - 1 & \text{if } x \equiv 0 \bmod a. \end{cases}$$

The second case is clear; the first one follows, as always, from Euclidean division equality $bx = [bx/a]a + \{bx/a\}$ from whose members we subtract 1; this gives: $bx - 1 = [bx/a]a + \{bx/a\} - 1$. But the hypothesis implies that $\{bx/a\} > 0$, thus the final equality is another Euclidean division equality; the equation follows.

The following lemma characterizes the points which are located at the right end of each horizontal step of a naive discrete line. It is given, always for $0 \leq a < b$ and $gcd(a, b) = 1$, in the particular case of lines $\mathcal{D}(a, -b, 0, b)$ which, as we have seen, allow a parametrization $y = [ax/b]$. But the invariance of structure with respect to discrete lines' third parameter, i.e. bound γ, permits us to generalize this lemma easily to all naive lines. Its proof follows directly from the general principle relating the behaviour of modular sequences, here $\{ax/b\}$, to discrete lines' geometrical properties. Let us recall a particular point of our preceding algorithm: each jump between two consecutive $\mathcal{D}$'s steps correspond to values where the modular sequence is greater than or equal to $b - a$. Hence, we have

LEMMA 2

Let $\mathcal{D}$ be the discrete line given by $y = [ax/b]$; x is located at the end of a $\mathcal{D}$'s step if and only if $\{ax/b\} \geq b - a$.

Now we are close to the step end formula; let us consider the horizontal step of line $\mathcal{D}$ where the ordinate value is n and the point whose abscissa is $[(bn - 1)/a]$; its ordinate is $[(a[bn - 1/a])/b]$. But the conjunction of the first lemma and the linear reciprocity law shows that this function takes, for any n, the value $n - 1$. Moreover, for the point considered, the value of the modular function is

$\{(a[bn - 1/a])/b\}$. This integer can be shown to be equal to $b - \{bx/a\}$ if $x \not\equiv 0 \bmod a$, and to $b - a$ if $x \equiv 0 \bmod a$. But both values are $\geq b - a$; hence, after our second lemma, this is an end point of a horizontal step.

We advise the reader that, because of the shift between n and $n - 1$ which appeared in the computation, we must give index one to the horizontal step containing 0; so the end of the first step occurs with abscissa $[(b - 1)/a]$ and the index of the step containing 0 is equal to -1.

Let us use our former example $a/b - 5/17$ again to illustrate this step end formula. If $n = 1, 2, \ldots, 5$, the abscissa are given by $[(17n - 1)/5]$ and we obtain, respectively, 3, 6, 10, 13 and 16.

The study of the lines' steps can be pushed much further (see [15]), but we cannot go on here.

5.6. ARITHMETICAL THICKNESS AND QUADRATIC RECIPROCITY LAW

We now present one example of a rather surprising mixture of a practical problem and deep arithmetics. It has to do with Bresenham's lines, naive lines and quadratic reciprocity law. Let is briefly recall the definition of Legendre's symbol. Let p be a prime number and a any integer. The symbol takes three values:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue of } p, \\ -1 & \text{if } a \text{ is a non-residue of } p, \\ 0 & \text{if } p \text{ divides } a. \end{cases}$$

The following *Gauss lemma* (one of them!) which expresses Legendre's symbol $\left(\frac{a}{p}\right)$ as a quantity $(-1)^{\mu}$, with a convenient integer μ, is the main part of his celebrated *quadratic reciprocity formula* (cf. [6] for a proof).

LEMMA 3

Let p be a prime number greater than 2, a any integer and μ be the number among elements

$$a, 2a, \ldots, \left(\frac{p-1}{2}\right)a,$$

whose smallest Euclidean rest modulo p are *negative*. Then Legendre's symbol is equal to $(-1)^{\mu}$.

The smallest rest refers to the alternative Euclidean division defined, for two integers a and p, by

$$a = pq + r \quad \text{and} \quad -\left[\frac{p}{2}\right] \leq r < \left[\frac{p}{2}\right].$$

It results from the definition of discrete lines that

- Bresenham's line associated with the usual line $y = ax/p$ is given by $y = [ax/p]^*$, where $[\ ]^*$ denotes the smallest rest quotient.
- Bresenham's line is also equal to $\mathcal{D}(a, -p, -[p/2], p)$, from which we immediately deduce that integer μ is equal to the number of points in the interval $[0, [p/2]]$ where functions $[ax/p]$ and $[(ax + [p/2])/p]$ differ by 1. In fig. 17, we represent the second function with white pixels, then the first function with black pixels which hide some white pixels. But abscissa where the two functions differ by 1 are unambiguously identified by the presence of a black pixel above a white one. As the first half of one period is needed, we directly interpret μ as the number of such twin pixels on the left of the vertical line.

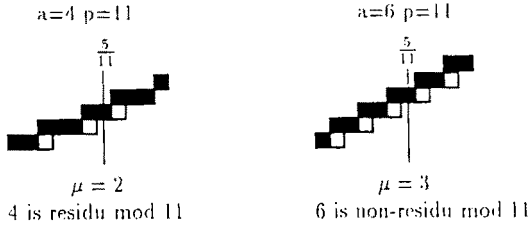


Fig. 17.

This number μ can be interpreted in a slightly different way. It is also

- either the number of *intersection points* of the naive lines $\mathcal{D}(a, -p, 0, p)$ and $\mathcal{D}(a, -p, -[p/2] + p, p)$ whose abscissa is bounded by 1 and $[p/2]$,
- or the number of points of the *non-connected* line $\mathcal{D}(a, -p, -[p/2], [p/2])$ whose abscissa is bounded by 0 and $[p/2]$.

5.7. NON-VACUITY OF THE INTERSECTION OF TWO LINES

As a further nontrivial example of our approach to discrete lines, we give here some simple conditions on the parameters defining two discrete lines so that their intersection in non-void. Such conditions will undoubtedly interest computer graphists, for they seem to be completely new. This certainly shows the advantage of science over tricks – even the most ingenious ones.

Let $\mathcal{A}$ and C be two discrete lines defined by their inequations

$$\begin{cases} \gamma \le ax + by < \gamma + \omega & (\mathcal{A}), \\ \eta \le cx + dy < \eta + \rho & (C), \end{cases} \tag{1}$$

where $(a, b) = (b, d) = (c, d) = 1$, $ad - bc = d > 0$, $\omega > 0$ and $\rho > 0$. Determining their intersection is equivalent to solving diophatine system (1). Using matricial notation, it becomes simply

$$\begin{pmatrix} \gamma \\ \eta \end{pmatrix} \leq \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} < \begin{pmatrix} \gamma + \omega \\ \eta + \rho \end{pmatrix}. \tag{2}$$

If $\delta = 1$, the lattice generated by vectors (a, b) and (c, d) is all $\mathbb{Z}^2$. In this case, the number of intersection points of $\mathcal{A} \cap \mathcal{B}$ being exactly $\omega\rho$, this intersection is always non-void because we supposed $\omega > 0$ and $\rho > 0$. The main work concerns the case $\delta > 1$, treated below. Let us consider the vector (v, u) of line $\mathcal{A}$, defined by $au + bv = 1$, and the unimodular matrix

$$M = \begin{pmatrix} a & b \\ -v & u \end{pmatrix}.$$

Then we have equality

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} M^{-1} = \begin{pmatrix} 1 & 0 \\ cu + dv & \delta \end{pmatrix}.$$

Consequently, (2) is equivalent to

$$\begin{pmatrix} \gamma \\ \eta \end{pmatrix} \leq \begin{pmatrix} a & b \\ c & d \end{pmatrix} M^{-1} M \begin{pmatrix} x \\ y \end{pmatrix} < \begin{pmatrix} \gamma + \omega \\ \eta + \rho \end{pmatrix}, \tag{3}$$

or, still denoting $M\binom{x}{y}$ by $\binom{X}{Y}$ (this is well defined because M is unimodular),

$$\begin{pmatrix} \gamma \\ \eta \end{pmatrix} \leq \begin{pmatrix} 1 & 0 \\ cu + dv & \delta \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} < \begin{pmatrix} \gamma + \omega \\ \eta + \rho \end{pmatrix}. \tag{4}$$

Let us introduce the vertical transvection matrix

$$N = \begin{pmatrix} 1 & 0 \\ -(cu + dv) & 1 \end{pmatrix};$$

then the lattice generated by vectors $\binom{1}{cu + dv}$ and $\binom{0}{\delta}$ is transformed in the lattice $\mathcal{R}$ generated by vectors $\binom{1}{0}$ and $\binom{0}{\delta}$. This means that the system matrix $\binom{a\ b}{c\ d}$ has been reduced to Smith normal form. Solving system (4) is thus equivalent to determining which points of the lattice $\mathcal{R}$ are contained in the parallelogram $\Pi = ABCD$, the image by transvection N of the rectangle $[\gamma, \gamma + \omega[\eta, \eta + \rho[$. Of course, the solutions lying on the union of segments AD and CD are omitted. We denote, to ease notation, $cu + dv$ by θ; an easy proof shows there is a right vector (u, v) such that inequations $0 \leq \theta < \delta$ are satisfied. Let us then determine the coordinates of the vertices of Π, which are

$$A = \begin{pmatrix} \gamma \\ \eta + \rho - \theta\gamma \end{pmatrix}, \quad B = \begin{pmatrix} \gamma \\ \eta - \theta\gamma \end{pmatrix},$$

$$C = \begin{pmatrix} \gamma + \omega \\ \eta - \theta(\gamma + \omega) \end{pmatrix}, \quad D = \begin{pmatrix} \gamma + \omega \\ \eta + \rho - \theta(\gamma + \omega) \end{pmatrix}.$$

To obtained the simplest possible non-vacuity condition, we first recall a necessary and sufficient condition such that the interval $[m, n] \subset \mathbb{Z}$ contains an integer multiple of $\delta > 0$ (obviously, condition $n - m \geq \delta$ is sufficient but not necessary). We have

LEMMA 5

If $n - m < \delta$, then the $]m, n]$ contains a multiple of δ if and only if we have

$$\left\{ \frac{m}{\delta} \right\} \geq \delta + m - n.$$

Proof

If there is an integer k such that $k\delta \in]m, n]$, we have $n = k\delta + u$, $u \geq 0$ and $m = kd - v$, $v > 0$. As $n - m < \delta$, we have $u + v < \delta$, hence $u < \delta$ and $v < \delta$, from which equalities $\{\frac{m}{\delta}\} = \delta - v$ and $\delta + m - n = \delta - v - u$ and the conclusion follows.

Reciprocally, let us denote $r = \{\frac{m}{\delta}\}$, $q = [\frac{m}{\delta}]$, $m = q\delta + r$. Hypothesis $r \geq \delta + m - n$ gives $n \geq \delta + m - r = (q + 1)\delta$. Thus, we have $(q + 1)\delta \in]m, n]$, ending the proof. □

Let us return to system (4) and consider parallelogram Π' obtained from Π omitting sides AD and CD. As A', C', D' are integer points, their coordinates are $A' = A + (0, -1)$, $C' = C + (-1, \theta)$ and $D' = D + (-1, \theta - 1)$. The question is to know if Π' contains a point of lattice $\mathcal{R}$.

We first ask if there is a line with equation $y = k\delta$ intersecting Π'? The former lemma applied to the interval defined by C' and A' ordinates gives the answer. Such a line exists if and only if we have

$$\left\{ \frac{\eta - \theta\gamma - \theta(\omega - 1) - 1}{\delta} \right\} \geq \delta - \rho - \theta(\omega - 1).$$

Then, does such a line contain an integer point in Π'? We remark that if Π'' is the parallelogram $A'B''C'D''$ where $B'' = (\gamma - (\rho - 1)/\theta,\ \eta + \rho - \theta\gamma - 1)$ and $D'' = (\gamma + \omega - 1 + (\rho - 1)/\theta, \eta - \theta(\gamma + \omega - 1))$, then if a line $y = k\delta$ has an integer point in Π'' it has one in Π'. This is due to the fact that segments $A'B$ and $C'D'$ are parallel to the second coordinate axis and have integer abscissa. If D_k denotes the line with equation $y = k\delta$, then D_k cuts Π' (or Π'') if and only if

$$k\delta \in [\eta - \theta(\gamma - 1) - \theta\omega, \eta - 1 - \theta\gamma + \rho].$$

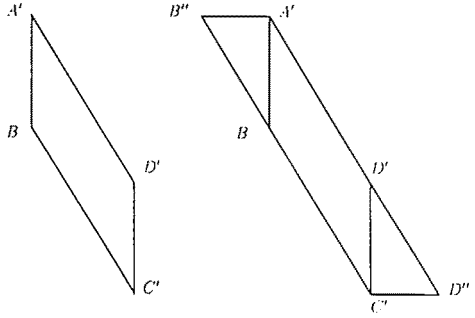


Fig. 18. Parallelograms Π' and Π''.

In this case, a short computation gives abscissa of intersection points $D_k \cap B''C'$ and $D_k \cap A'D''$:

$$\frac{\eta - k\delta}{\theta} \quad \text{and} \quad \frac{\eta - k\delta + \rho - 1}{\theta}.$$

Then line D_k contains an integer point within Π'' if and only if the interval

$$\left[\frac{\eta - k\delta}{\theta}, \frac{\eta - k\delta + \rho - 1}{\theta}\right]$$

contains an integer number or, equivalently, if and only if the interval

$$[\eta - k\delta, \ \eta - k\delta + \rho - 1]$$

contains an integer multiple of θ, whence, using the above lemma,

$$\left\{\frac{\eta - k\delta - 1}{\theta}\right\} \geq \theta - \rho.$$

Finally, the two discrete lines $(\mathcal{A})$ and (C) have a non-empty intersection if and only if both conditions are satisfied:

$$\begin{cases} \left\{\dfrac{\eta - 1 - \theta(\gamma + \omega - 1)}{\delta}\right\} \geq \delta - \rho - \theta(\omega - 1) \ \ (1) \\ \quad \text{and if (1) is satisfied} \\ \exists k \in \left[\dfrac{\eta - 1 - \theta(\gamma + \omega)}{\delta}, \dfrac{\eta - 1 + \rho - \theta\gamma}{\delta}\right] \\ \qquad \text{such that } \left\{\dfrac{\eta - 1 - k\delta}{\theta}\right\} \geq \theta - \rho. \end{cases}$$

Remarks

- These conditions, mainly the second one, are certainly difficult to *guess* or *circumvent* if we want to solve such an intersection problem without a theoretical approach.
- This way of studying line intersection requires, for the second case $\theta\omega > \rho$, a walk within a part of a discrete line. Here, the non-vacuity condition is not given by a *formula* in the sense we are accustomed to in Euclidean geometry. This drawback, which is rather unavoidable in discrete geometry, results from the fact that many arithmatical functions, for instance the length of the Euclidean algorithm, are not describable by formulae.
- In order to obtain an actual and fast computer implementation, the computation of the modular sequence $\{(\eta - 1 - k\delta)/\theta\}$, for authorized k values, can be done in the same way as the algorithm given in the paragraph concerning modular calculus and algorithms.
- The walk is efficient because we use multiples of δ, the largest invariant factor of the system matrix. Moreover, this method can be generalized to any dimension or to any number of lines or discrete spaces after the system matrix has been reduced to its Smith normal form and by then using invariant factors in decreasing order. Nevertheless, we do not know if this algorithm is optimal.

Acknowledgement

We thank E. Benoit for his numerous comments during the preparation of this paper.

References

[1] J. Bresenham, Algorithm for computer control of a digital plotter, IBM Syst. J. 4(1965)25–30.
[2] C.C. Chang and H.J. Keisler, *Model Theory*, 2nd ed. (North-Holland, Amsterdam, 1977).
[3] J.M. Chassery and A. Montanvert, *Géométrie Discrète* (Editions Hermès, 1991).
[4] M. Davis, *Applied Non-Standard Analysis* (Wiley-Interscience, 1977).
[5] M. Diener, Application du calcul de Harthong-Reeb aux routines graphiques, *Séminaire Non-Standard*, Université Paris 7 (1988).
[6] G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers*, 5th ed. (Oxford University Press, 1989).
[7] J. Harthong, Eléments pour une théorie du continu, Astérisque 235(1983)109–110.
[8] M.A. Jacob, Applications quasi-affines, Thèse, Université Louis Pasteur, Strasbourg (1993).
[9] J. Keisler, *Elementary Calculus* (Prindle–Weber & Schmidt, Boston, MA).
[10] P. Nehlig, Applications quasi-affines discrètes et antialiassage, Thèse, Université Louis Pasteur, Strasbourg (1992).
[11] E. Nelson, Internal set theory, BAMS 83(1977)1165–1198.
[12] G. Reeb, J.P. Reveillès, A. Troesch and E. Urlacher, Equations différentielles et nombres entiers, Preprint, IRMA Université Louis Pasteur, Strasbourg (1987).

[13] J.P. Reveillès, Simulation arithmétique du continu, Preprint, IRMA, Université Louis Pasteur, Strabourg (1987).
[14] J.P. Reveillès, Les paliers des droites de Bresenham, in: *PIXIM 88* (Hermès Ed, Paris, 1988) pp. 81–101.
[15] J.P. Reveillès, Géométrie Discrète, Calcul en nombres entiers et algorithmique, Thèse, Université Louis Pasteur, Strasbourg (1991).
[16] J.P. Reveillès, Libérez les chiffres – Continuité et microprocesseur, Preprint, IRMA, Université Louis Pasteur, Stransbourg (1987).
[17] J.P. Reveillès, Structure arithmétique du continu, Preprint, IRMA, Université Louis Pasteur, Stransbourg (1987).
[18] J.P. Reveillès, Les droites discrètes – Une définition générale, leurs intersections, Preprint, INRIA, Sohpia-Antipolis (1990).
[19] D. Richard, De la structure additive la saturation des modèles de Peano et à une classification des sous-langages de l'arithmétique, *Lecture Notes in Mathematics 890*, eds. C. Berline, K. McAloon and J.P. Ressayre (Springer, 1981) pp. 270–296.
[20] D. Richard, On extremal properties of non standard models of arithmetics, Preprint, Dépt. Math., Université de Lyon (1977) t. 14–4, pp. 57–75.
[21] P. Dehornoy, S. Grigorieff, D. Richard, R. Sami and J. Stern, CIMPA – L'Analyse non-standard, in Cours de logique du CIMPA (1984).
[22] A. Robinson, *Non-Standard Analysis* (North-Holland, Amsterdam, 1966).
[23] A. Rosenfeld and R.A. Melter, Digital geometry, Math. Intell. 11(3)(1989)69–72.
[24] R. Seroul, Equations différentielles et nombres entiers ou la méthode TRRU, *L'ouvert No. 48* (1987).