ALGUNOS COMENTARIOS SOBRE LOS NÚMEROS REALES COMPUTABLES

ANDRÉS SICARD RAMÍREZ Y MARIO ELKIN VÉLEZ RUIZ

Resumen. Este artículo presenta un subconjunto propio de los números reales denominado *números reales computables* $\mathbb{R}_c$, donde el modelo de computación subyacente son las máquinas de Turing. Además, se establece que el conjunto $\mathbb{R}_c$, dotado de una operación de suma y multiplicación y de una relación, presenta una estructura algebraica de campo ordenado incompleto.

Abstract. This paper introduce a proper subset of real numbers called *computable real numbers* $\mathbb{R}_c$, where the *Turing machines* are the computation model used. In addition, we establish that the set $\mathbb{R}_c$, equipped with sum and multiplication operation and a relation has an algebraic structure of incomplete ordered field.

1. Introducción

Los modelos clásicos de computación, tales como las máquinas de Turing [9, 16], las funciones recursivas parciales [9, 10] o el λ-cálculo [2] son considerados usualmente como modelos *discretos* de computación. El carácter discreto de los modelos de computación está reflejado en el *espacio de computación* y la *dinámica de la computación*, es decir, los objetos sobre los cuales se computa son discretos y los pasos de computación son discretos.

Por otra parte, los modelos de computación que permiten la manipulación de objetos continuos pertenecen a una área de la computación teórica denominada *computación continua* o *computación analógica*; sin embargo, en la actualidad no existen ni la unicidad ni se han obtenido los resultados en esta área, que sí, se han obtenido en la *computación discreta* o *computación digital* [13, 17].

No obstante lo anterior, es posible realizar computación sobre objetos continuos a partir de los modelos de computación clásica. Este artículo presenta un subconjunto propio de los números reales denominado *números reales computables* $\mathbb{R}_c$, donde el modelo de computación subyacente son las máquinas de Turing. Además, se establece que el conjunto $\mathbb{R}_c$, dotado de una operación de suma y multiplicación y de una relación, presenta una estructura algebraica de campo ordenado incompleto.

El artículo procede de la siguiente manera: La sección 2 construye el campo ordenado de los números reales como clases de equivalencia de sucesiones de números racionales, la sección 3 define los números reales computables, la sección 4 construye el campo ordenado de los números reales computables y la sección 5 presenta algunas conclusiones.

Date: 20 de septiembre de 2000.

Se espera que el lector conozca la teoría de computablidad desde la perspectiva de las máquinas de Turing (Turing-computabilidad), en particular la definición de función Turing-computable (sobre los números naturales y sobre los números racionales), los teoremas básicos sobre las funciones totales Turing-computables, el resultado sobre la cardinalidad del conjunto de las máquinas de Turing, alguna codificación de las máquinas de Turing, los conceptos de conjunto recursivo y conjunto recursivamente enumerable y la indecibilidad del problema de la parada (*the halting problem*) (esta teoría es presentada en [8, 9]).

2. Sistema de los números reales

El sistema de los números reales se construye a partir del sistema de los números racionales, el cual se construye a partir del sistema de los números enteros, el cual se construye a partir del sistema de los números naturales, el cual se construye vía axiomática (axiomas de Peano). Se menciona el "sistema de números" en lugar del "conjunto de números" para resaltar el hecho de que la construcción del sistema de números X a partir del sistema de números Y, además de construir los elementos de X (conjunto de números) a partir de los elementos de Y (conjunto de números) construye operaciones y relaciones sobre los elementos del sistema de números X, a partir de operaciones y relaciones sobre los elementos del sistema de números Y.

La construcción del sistema de números reales será realizada a partir del sistema de los números racionales $\langle \mathbb{Q}, +, \cdot \rangle$, donde $\mathbb{Q}$ denota el conjunto de números racionales, $+$ denota la adición sobre números racionales y $\cdot$ denota la multiplicación sobre números racionales (una construcción del sistema de los números racionales a partir del sistema de los números enteros y una construcción de éstos a partir del sistema de los números naturales es presentada en [3]). La construcción del sistema de los números reales sólo hará referencia a aquellos aspectos relevantes para el sistema de los números reales computables (una construcción más completa es presentada en [3, 14, 15]). Existen varios procedimientos de construcción del sistema de números reales a partir del sistema de números racionales, entre ellos se destacan la construcción por *cortaduras de Dedekind* [3, 15] y la construcción por *sucesiones fundamentales de Cantor* o *sucesiones de Cauchy* [3, 14]. La construcción se hará con base en este último procedimiento porque es más adecuada para la definición del sistema de los números reales computables. Se seguirá la presentación realizada en [14].

Definición 2.1. Sea $\mathbb{Z}^+ = \{1, 2, \dots\}$ el conjunto de los números enteros positivos. Una *sucesión de números racionales*, denotada por $\{a_n\}$, es una función $s : \mathbb{Z}^+ \to \mathbb{Q}$, donde $s(n) = a_n$ denota el n-ésimo término de la sucesión $\{a_n\}$.

Ejemplo 2.2. Las siguientes son sucesiones de números racionales:

(1) La función $s : \mathbb{Z}^+ \to \mathbb{Q}$ definida por $s(n) = 3^n$. En este caso $\{a_n\} = \{3, 9, 27, \dots\}$.
(2) $\{a_n\} = \left\{\frac{1}{n}\right\} = \left\{1, \frac{1}{2}, \frac{1}{3}, \dots\right\}$.
(3) La sucesión cuyo n-ésimo término es $a_n = (1 + \frac{1}{n})^n$.
(4) $a_n = \sum_{k=0}^{n} \frac{1}{k!}$.

Definición 2.3. Sea $\{a_n\}$ una sucesión de números racionales. Se dice que la sucesión $\{a_n\}$ *converge al número racional* a, denotado por $\lim_{n\to\infty} a_n = a$, si para cualquier número racional $\epsilon > 0$ existe un número entero positivo $N(\epsilon)$ tal que si $n > N(\epsilon)$ entonces $|a - a_n| < \epsilon$.

Ejemplo 2.4. Para las sucesiones presentas en el ejemplo 2.2:

(1) La sucesión $\{3^n\}$ no converge a ningún racional puesto que $\lim_{n\to\infty} 3^n = \infty$.
(2) La sucesión $\left\{\frac{1}{n}\right\}$ converge a 0 puesto que $\lim_{n\to\infty} \frac{1}{n} = 0$.
(3) La sucesión $\left\{(1+\frac{1}{n})^n\right\}$ no converge a ningún racional puesto que $\lim_{n\to\infty}(1+\frac{1}{n})^n = e$ y $e \notin \mathbb{Q}$.
(4) $\lim_{n\to\infty} \sum_{k=0}^{n} \frac{1}{k!} = e$, entonces la sucesión $\left\{\sum_{k=0}^{n} \frac{1}{k!}\right\}$ no converge a ningún racional.

Definición 2.5. Sean $\{a_n\}$, una sucesión de números racionales. Se dice que la sucesión $\{a_n\}$ es una *sucesión de Cauchy* si para cualquier número racional $\epsilon > 0$ existe un número entero positivo $N(\epsilon)$ tal que si $n > N(\epsilon), m > N(\epsilon)$ entonces $|a_n - a_m| < \epsilon$.

Ejemplo 2.6. Para las sucesiones presentas en el ejemplo 2.2:

(1) La sucesión $\{3^n\}$ no es una sucesión de Cauchy.
(2) La sucesión $\left\{\frac{1}{n}\right\}$ es una sucesión de Cauchy.
(3) La sucesión $\left\{(1+\frac{1}{n})^n\right\}$ es una sucesión de Cauchy.
(4) La sucesión $\left\{\sum_{k=0}^{n} \frac{1}{k!}\right\}$ es una sucesión de Cauchy.

La relación entre las sucesiones de números racionales que convergen a un número racional y las sucesiones de números racionales que son sucesiones de Cauchy es presentada por el siguiente teorema.

Teorema 2.7. Sea $\{a_n\}$ una sucesión de números racionales. Si $\{a_n\}$ es una sucesión convergente a un número racional entonces $\{a_n\}$ es una sucesión de Cauchy.

Demostración.

(i) Sea $\{a_n\}$ una sucesión de números racionales y $a \in \mathbb{Q}$ tal que $\lim_{n\to\infty} a_n = a$.
(ii) Si $\lim_{n\to\infty} a_n = a$ entonces $\lim_{n\to\infty} |a_n - a| = 0$.
(iii) Sean $\epsilon > 0, N(\epsilon) = \frac{\epsilon}{2}$, entonces $|a_n - a| < \frac{\epsilon}{2}$ y $|a - a_m| < \frac{\epsilon}{2}$ para $n > \frac{\epsilon}{2}$ y $m > \frac{\epsilon}{2}$.
(iv) Sean $x, y \in \mathbb{Q}$ entonces $|x + y| \leq |x| + |y|$ (desigualdad triangular).
(v) Sean $x = a_n - a$ y $y = a - a_m$ entonces $|a_n - a_m| \leq a_n - a + |a - a_m| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon$. $\square$

La convergencia o la no convergencia a un número racional de toda sucesión de Cauchy juega un papel fundamental en la construcción del sistema de números reales a partir del sistema de números racionales, pues es uno de los aspectos que distingue estos dos sistemas de números desde la perspectiva de la estructura algebraica denominada campo ordenado.

Definición 2.8. Un *campo* es una estructura algebraica $\langle C, +, \cdot, 0, 1\rangle$ que satisface los siguientes axiomas [11], donde C es un conjunto no vacío; $+$ es una función $+ : C \times C \to C$ llamada *adición*; $\cdot$ es una función $\cdot : X \times X \to X$ llamada *multiplicación*; $0 \in C$ es una constante llamada *elemento neutro* del campo bajo la adición y $1 \in C$ es una constante llamada *elemento identidad* del campo bajo la multiplicación.

Axiomas para la adición: Sean $x, y \in C$

(1a) $(x + y \in C)$ (clausurativa $+$)

(1b) $(x + y = y + x)$ (conmutativa $+$)

(1c) $(x + (y + z) = (x + y) + z)$ (asociativa $+$)

(1d) $(x + 0 = 0 + x = x)$ (elemento neutro para $+$)

(1e) Existe $-x \in C$ tal que $(x + (-x) = 0)$ (existencia elementos inversos bajo $+$)

Axiomas para la multiplicación: Sean $x, y \in C$

(1f) $(x \cdot y \in C)$ (clausurativa $\cdot$)

(1g) $(x \cdot y = y \cdot x)$ (conmutativa $\cdot$)

(1h) $(x \cdot (y \cdot z) = (x \cdot y) \cdot z)$ (asociativa $\cdot$)

(1i) $(x \cdot 1 = 1 \cdot x = x)$ (elemento neutro para $\cdot$)

(1j) Existe $x' \in C$ tal que $(x \neq 0 \rightarrow x \cdot x' = 1)$ (existencia elementos inversos para $\cdot$)

Axiomas que relacionan la adición y la multiplicación: Sean $x, y, z \in C$

(1k) $(x \cdot (y + z) = x \cdot y + x \cdot z)$ (distributiva derecha)

(1l) $((y + z) \cdot x = y \cdot x + z \cdot x)$ (distributiva izquierda)

Teorema 2.9. La estructura algebraica $\langle \mathbb{Q}, +, \cdot, 0, 1 \rangle$ es un campo, denominado el campo de los números racionales.

Definición 2.10. Un *campo ordenado* es una estructura algebraica $\langle C, \prec \rangle$ que satisface los siguientes axiomas [11], donde C es un campo y $\prec$ es una relación binaria sobre C.

(2a) Sea $x \in C$ entonces $(x \prec 0 \vee x = 0 \vee 0 \prec x)$ (tricotomía)

(2b) Sean $0 \prec x, 0 \prec y \in C$ entonces $(0 \prec x + y)$ ($+$ de números positivos)

(2c) Sean $0 \prec x, 0 \prec y \in C$ entonces $(0 \prec x \cdot y)$ ($\cdot$ de números positivos)

Teorema 2.11. La estructura algebraica $\langle \mathbb{Q}, < \rangle$ es un campo ordenado, donde $\mathbb{Q}$ denota el campo de los números racionales y $<$ denota la relación de orden usual en $\mathbb{Q}$.

Definición 2.12. Un campo ordenado $\langle C, \prec \rangle$ se denomina completo si cada sucesión de Cauchy $\{a_n\}$ de elementos del campo converge a un elemento del campo.

Los literales (3) y (4) de los ejemplos 2.2, 2.4 y 2.6 indican que el campo ordenado de los números racionales no es un campo ordenado completo. La idea de construir el sistema de los números reales a partir del sistema de los números racionales, es la idea de "completar" el campo de los números racionales para obtener el campo ordenado completo de los números reales. Intuitivamente un campo ordenado incompleto se completa adicionando los elementos necesarios para que toda sucesión de Cauchy converja a un elemento del campo. Debido a que diferentes sucesiones de Cauchy pueden converger al mismo elemento, la completación de un campo ordenado incompleto se realiza por medio de límites de clases de equivalencias de sucesiones de Cauchy.

Definición 2.13. Sean $\{a_n\}$ y $\{b_n\}$ dos sucesiones de Cauchy de números racionales. Se dice que las dos sucesiones son *equivalentes*, denotado por $\{a_n\} \sim \{b_n\}$, si $\lim_{n\to\infty}(a_n - b_n) = 0$.

Ejemplo 2.14. Las sucesiones $\left\{(1+\frac{1}{n})^n\right\}$ y $\left\{\sum_{k=0}^{n} \frac{1}{k!}\right\}$ presentadas en los literales (3) y (4) del ejemplo 2.2 son equivalentes puesto que $\lim_{n\to\infty}(1+\frac{1}{n})^n = \lim_{n\to\infty} \sum_{k=0}^{n} \frac{1}{k!} = e$.

Teorema 2.15. Sea QC el conjunto de sucesiones de Cauchy de números racionales. La relación $\sim$ es una relación de equivalencia sobre QC.

Demostración.

(i) Reflexividad
  (a) Sea $\{a_n\} \in$ QC.
  (b) $\lim_{n\to\infty}(a_n - a_n) = 0$.
  (c) Luego, $\{a_n\} \sim \{a_n\}$.

(ii) Simetría
  (a) Sean $\{a_n\}, \{b_n\} \in$ QC tal que $\{a_n\} \sim \{b_n\}$.
  (b) $\lim_{n\to\infty}(a_n - b_n) = 0$.
  (c) $\lim_{n\to\infty}(b_n - a_n) = 0$.
  (d) Luego, $\{b_n\} \sim \{a_n\}$.

(iii) Transitividad
  (a) Sean $\{a_n\}, \{b_n\}, \{c_n\} \in$ QC tal que $\{a_n\} \sim \{b_n\}$ y $\{b_n\} \sim \{c_n\}$.
  (b) $\lim_{n\to\infty}(a_n - b_n) = \lim_{n\to\infty}(b_n - c_n) = 0$.
  (c) $\lim_{n\to\infty}(a_n - b_n) + \lim_{n\to\infty}(b_n - c_n) = \lim_{n\to\infty}(a_n - c_n) = 0$.
  (d) Luego, $\{a_n\} \sim \{c_n\}$.

$\square$

Teorema 2.16. Sean $\{a_n\}, \{b_n\} \in$ QC y $a \in \mathbb{Q}$. Las sucesiones $\{a_n\}$ y $\{b_n\}$ son equivalentes, si y sólo si, $\lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n = a$.

Definición 2.17. La relación $\sim$ induce una partición del conjunto QC en *clases de equivalencia*, denotadas por $[\{a_n\}]$, están definidas por $[\{a_n\}] = \{\, \{b_n\} \in \text{QC} \mid \{a_n\} \sim \{b_n\}\,\}$.

El conjunto de los números reales se identifica con el conjunto de las clases de equivalencia de la relación $\sim$ sobre el conjunto QC.

Definición 2.18. El conjunto cociente QC$/\sim$, es decir, el conjunto de las clases de equivalencia de QC inducidas por la relación $\sim$, es el *conjunto de los números reales*, denotado por $\mathbb{R}$.

Es necesario dotar al conjunto $\mathbb{R}$ de una operación de adición y de una operación de multiplicación que satisfagan los axiomas (1) y de una relación binaria que satisfaga los axiomas (2) para obtener el campo ordenado completo de los números reales.

Definición 2.19. Sean $[\{a_n\}], [\{b_n\}] \in \mathbb{R}$. La *adición* de $[\{a_n\}]$ y $[\{b_n\}]$, denotada $[\{a_n\}] \oplus [\{b_n\}]$, está definida por $[\{a_n\}] \oplus [\{b_n\}] = [\{a_n + b_n\}]$.

Definición 2.20. Sean $[\{a_n\}], [\{b_n\}] \in \mathbb{R}$. La *multiplicación* de $[\{a_n\}]$ por $[\{b_n\}]$, denotada $[\{a_n\}] \otimes [\{b_n\}]$, está definida por $[\{a_n\}] \otimes [\{b_n\}] = [\{a_n \cdot b_n\}]$.

Teorema 2.21. La estructura algebraica $\langle \mathbb{R}, \oplus, \otimes, [\{0\}], [\{1\}] \rangle$ es un campo, denominado el campo de los números reales.

Definición 2.22. Sean $[\{a_n\}], [\{b_n\}] \in \mathbb{R}$. El número $[\{b_n\}]$ es *menor* que el número $[\{a_n\}]$, denotado $[\{b_n\}] \triangleright [\{a_n\}]$, si existe un número racional positivo ϵ y un número entero positivo $N(\epsilon)$ tal que para cualquier par de sucesiones $\{a_n\} \in [\{a_n\}]$, $\{b_n\} \in [\{b_n\}]$ se tiene que $a_n > b_n + \epsilon$ para todo $n > N(\epsilon)$.

Teorema 2.23. La estructura algebraica $\langle \mathbb{R}, \triangleright \rangle$ es un campo ordenado, donde $\mathbb{R}$ denota el campo de los números reales.

Teorema 2.24. Cada sucesión de Cauchy de números reales converge a un número real.

Como resultado del teorema 2.24 se obtiene que el campo ordenado $\langle \mathbb{R}, \triangleright \rangle$ es un campo ordenado completo. Una vez establecida la definición del conjunto de los números reales como clases de equivalencia de sucesiones de Cauchy de números racionales, se identifican los números reales como los límites de sucesiones de números racionales y se opera con el campo ordenado completo de los números reales usual $\langle \mathbb{R}, +, \cdot, 0, 1, < \rangle$.

3. Números reales computables

El ampliar el espacio discreto de la computación de números naturales y funciones sobre los números naturales a números reales y funciones sobre los números reales, exige trasladar y expandir los conceptos y métodos propios de la computación discreta a un dominio continuo. Para realizar esta expansión es posible seguir tres alternativas: (i) Algebraica: El modelo propuesto por Lenore Blum, Mike Shub y Steve Smale [4, 5] es un modelo de computación sobre un anillo ordenado arbitrario $\mathfrak{A}$; cuando $\mathfrak{A} = \mathbb{Z}_2$, el modelo es equivalente a una máquina de Turing, pero cuando $\mathfrak{A} = \mathbb{R}$, el modelo computa funciones sobre los números reales, (ii) Funcional: Vasco Brattka [7] y Cristopher Moore [12] presentan independientemente una definición de las funciones recursivas reales con base en un conjunto de funciones iniciales sobre los números reales y algunos esquemas de creación de funciones sobre los números reales y (iii) Analítica: Alan Turing [16], Douglas S. Bridges [8] y Klaus Weihrauch [17] a partir de las funciones computables por una máquina de Turing (funciones Turing-computables) y a partir de la construcción de los números reales como límites de sucesiones de números racionales definen los números reales computables. Se ha seleccionado el enfoque analítico para la presentación de los números reales computables, pues surge naturalmente del modelo de computación de las máquinas de Turing. Se seguirá la presentación realizada en [8].

Definición 3.1. Como se indicó en la sección 2 cada $x \in \mathbb{R}$ es el límite de una sucesión de números racionales, es decir, $\lim_{n\to\infty} s(n) = x$ ó $\lim_{n\to\infty} |x - s(n)| = 0$, donde $s : \mathbb{Z}^+ \to \mathbb{Q}$ es una sucesión de números racionales. La sucesión $s(n)$ es denominada *un generador* del número real x.

Definición 3.2. Sea $s : \mathbb{Z}^+ \to \mathbb{Q}$ un generador del número real x. La sucesión $s(n)$ es denominada un *generador Turing-computable* si $s(n)$ es una función total Turing-computable [8, 9].

Definición 3.3. Sea $x \in \mathbb{R}$. El número x es denominado un *número real computable* si existe un generador $s(n)$ para x tal que

$$s(n) \text{ sea un generador Turing-computable y} \tag{3}$$

$$|x - s(n)| \leq 2^{-n}, \quad \text{para todo } n \in \mathbb{Z}^+. \tag{4}$$

El conjunto de los números reales computables es denotado por $\mathbb{R}_c$.

La ecuación (3) señala que el número real x es el límite de una sucesión de números racionales $s(n)$ tal que cada término de la sucesión puede ser generado por una máquina de Turing. La ecuación (4) señala por su parte que la convergencia de la sucesión de números racionales es "rápida" [7]. Sea $x_b \equiv 0.x_1x_2\ldots$ donde $x_i \in \{0, 1\}$ la representación en binario de un número real $x \in (0, 1)$. El término 2^{-n} indica que la sucesión $s(n)_b$ tiene las primeras n-ésimas cifras binarias iguales a las primeras n-ésimas cifras binarias del número x_b.

Definición 3.4. Sea $x \in \mathbb{R}$. Si x no es un número real computable x es denominado un *número real no computable.*

Ejemplo 3.5. Los números racionales son números reales computables. Sea $q \in \mathbb{Q}$ un número racional y sea $s : \mathbb{Z}^+ \to \mathbb{Q}$ la sucesión de números racionales definida por $s(n) = q$. La función $s(n)$ es un generador para q que satisface la propiedad (i) de la definición 3.3, es decir, $s(n)$ es un generador Turing-computable de q, puesto que la función $s(n) = q$ es una función total Turing-computable, además $s(n)$ satisface $|q - s(n)| \leq 2^{-n}$, ya que $|q - s(n)| = 0$, para todo $n \in \mathbb{Z}^+$.

Ejemplo 3.6. El número e es un número real computable. La sucesión $\{s_n\}$ presentada en la parte (3) del ejemplo 2.2 es un generador para el número e, es decir $\lim_{n\to\infty}(1+\frac{1}{n})^n = e$. El comportarmiento de $\left|e - (1 + \frac{1}{n})^n\right|$ y 2^{-n} para $n = 1, \ldots, 5$ es presentado en la tabla 1. De acuerdo a la tabla 1, $s(n) = (1 + \frac{1}{n})^n$ no satisface que $\left|e - (1 + \frac{1}{n})^n\right| \leq 2^{-n}$ para $n = 1, \ldots, 5$; por lo tanto es necesario seleccionar otro generador para el número e.

n	$\left\lvert e - (1 + \frac{1}{n})^n\right\rvert$	$\left\lvert e - \sum_{k=0}^{n} \frac{1}{k!}\right\rvert$	$\left\lvert e - \sum_{k=0}^{n+1} \frac{1}{k!}\right\rvert$	2^{-n}
1	0,718282	0,718282	0,218282	0,5
2	0,468282	0,218282	0,0516152	0,25
3	0,347911	0,0516152	0,0099485	0,125
4	0,276876	0,0099485	0,00161516	0,0625
5	0,229962	0,00161516	0,000226273	0,03125

TABLA 1. Valores para $\left|e - (1 + \frac{1}{n})^n\right|$, $\left|e - \sum_{k=0}^{n} \frac{1}{k!}\right|$, $\left|e - \sum_{k=0}^{n+1} \frac{1}{k!}\right|$ y 2^{-n}.

La función $s(n)$ presentada en la parte (4) del ejemplo 2.2 es un generador para el número e. El comportamiento de $\left|e - \sum_{k=0}^{n} \frac{1}{k!}\right|$ y 2^{-n} para $n = 1, \ldots 5$ es presentado en la tabla 1. De acuerdo a la tabla 1, $s(n) = \sum_{k=0}^{n} \frac{1}{k!}$ no satisface la propiedad $\left|e - \sum_{k=0}^{n} \frac{1}{k!}\right| \leq 2^{-n}$ para $n = 1$, pero si la satisface para $n = 2, \ldots, 5$. Un nuevo generador para e es la función $s(n) = \sum_{k=0}^{n+1} \frac{1}{k!}$. El comportarmiento de $\left|e - \sum_{k=0}^{n+1} \frac{1}{k!}\right|$ y 2^{-n} para $n = 1, \ldots, 5$ es presentado en la tabla 1. Es necesario demostrar que

$$\left|e - \sum_{k=0}^{n+1} \frac{1}{k!}\right| \leq 2^{-n}, \quad \text{para todo } n \in \mathbb{Z}^+. \tag{5}$$

Inicialmente se demuestra que

$$e \leq \sum_{k=0}^{n+1} \frac{1}{k!} + 2^{-n}, \quad \text{para todo } n \in \mathbb{Z}^+. \tag{6}$$

Con base en la fórmula de Maclaurin [1] para la función e^x cuando $x = 1$ se obtiene

$$e = \sum_{k=0}^{n+1} \frac{1}{k!} + R_{n+1}, \quad \text{donde} \quad R_{n+1} = \frac{e^z}{(n+2)!}, \quad z \in (0,1). \tag{7}$$

De las ecuaciones (6) y (7) es necesario demostrar que

$$e^z \leq \frac{(n+2)!}{2^n}, \quad \text{para todo } n \in \mathbb{Z}^+, \text{ con } z \in (0,1). \tag{8}$$

Como las funciones e^z y $\frac{(n+2)!}{2^n}$ son crecientes entonces basta demostrar que

$$e^1 = e \leq \frac{(1+2)!}{2^1} = 3. \tag{9}$$

De forma similar se demuestra que

$$\sum_{k=0}^{n+1} \frac{1}{k!} - 2^{-n} \leq e, \quad \text{para todo } n \in \mathbb{Z}^+. \tag{10}$$

Además como la función $s(n) = \sum_{k=0}^{n+1} \frac{1}{k!}$ es un generador Turing-computable para e, se concluye que el número $e \in \mathbb{R}_c$.

Ejemplo 3.7. El número π es un número real computable. De la serie para π dada por Leibniz [6], $\pi = 4(1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \ldots)$ se obtiene un generador para π definido por $s(n) = \sum_{k=0}^{n+1} (-1)^k \frac{1}{2k+1}$, tal que $s(n)$ es una función total Turing-computable y $|\pi - s(n)| \leq 2^{-n}$, para todo $n \in \mathbb{Z}^+$.

La rapidez de la aproximación en base binaria de un número real computable puede ser modificada por la aproximación rápida en cual otra base $d \geq 2$.

Teorema 3.8. Sea $s(n)$ un generador Turing-computable para x tal que $|x - s(n)| \leq d^{-n}$, para todo $n \in \mathbb{Z}^+$, donde $d \geq 2$, entonces x es un número real computable.

Demostración.

(i) $s(n)$ es un generador Turing-computable para x.
(ii) $|x - s(n)| \leq d^{-n}$, para todo $n \in \mathbb{Z}^+$.
(iii) $d^{-n} \leq 2^{-n}$, para todo $d \geq 2$.
(iv) Luego, $|x - s(n)| \leq 2^{-n}$, para todo $n \in \mathbb{Z}^+$. □

Una vez establecido que los números racionales son números reales computables (ejemplo 3.5) y la existencia de algunos números reales no racionales computables (ejemplos 3.6 y 3.7), es necesario demostrar la existencia de números reales no computables. Inicialmente se presenta un teorema que señala la existencia de estos números.

Teorema 3.9. Existen números reales no computables.

Demostración. (versión no constructiva)

(i) El conjunto de las máquinas de Turing es enumerable [9].
(ii) El conjunto de las funciones Turing-computables es enumerable.
(iii) El conjunto de los generadores $s : \mathbb{Z}^+ \to \mathbb{Q}$ Turing-computables es enumerable.
(iv) El conjunto de los números reales es no enumerable [10].
(v) Por lo tanto deben existir números reales para los cuales no exista un generador $s(n)$ total Turing-computable. □

Demostración. (versión constructiva)

(i) Sea $A \subseteq \mathbb{N}$. El número $x_A = \sum_{k \in A} 2^{-k}$ es un número real computable, si y sólo si, A es un conjunto recursivo [17].
(ii) Entonces, si $A \subseteq \mathbb{N}$ es un conjunto recursivamente enumerable pero no recursivo el número $x_A = \sum_{k \in A} 2^{-k}$ es un número real no computable.
(iii) Desde la teoría de la Turing-computabilidad si $A \subseteq \mathbb{N}$ es un conjunto recursivamente enumerable pero no recursivo, existe una función total Turing-computable inyectiva $f : \mathbb{N} \to A$. Sea $x_A = \sum_{k \in \mathbb{N}} 2^{-f(k)}$ y sea la sucesión de números racionales $x_n = \sum_{i \leq n} 2^{-f(i)}$.
(iv) La sucesión de números racionales $\{x_n\}$ es una sucesión acotada y creciente.
(v) El límite de la sucesión $\{x_n\}$ es un número real no computable. La sucesión $\{x_n\}$ es denominada *sucesión de Specker* [17]. □

Ejemplo 3.10. Con base en el contrarrecíproco del teorema 3.9 si $A \subseteq \mathbb{N}$ es un conjunto no recursivo entonces $x_A = \sum_{k \in A} 2^{-k}$ es un número real no computable. Sea $\mathrm{MTP} \subseteq \mathbb{N}$ el conjunto formado por los códigos (números) de las máquinas de Turing que se detienen. Debido a la indecidibilidad del problema de la parada [8, 9, 16] el conjunto MTP es no recursivo, por lo tanto el número $x_{\mathrm{MTP}} = \sum_{k \in \mathrm{MTP}} 2^{-k}$ es un número real no computable.

4. Campo ordenado de los números reales computables

Para demostrar que el sistema de los números reales computables es un campo es necesario definir operaciones de suma y multiplicación sobre el conjunto $\mathbb{R}_c$ que satisfagan los axiomas (1), además es necesario señalar la existencia de los inversos aditivos y de los inversos multiplicativos en $\mathbb{R}_c$. Inicialmente se demuestra que la adición y la multiplicación de numeros reales computables es un número real computable.

Teorema 4.1. Si x y y son números reales computables entonces (i) $x+y$, (ii) $x-y$ y (iii) $x \cdot y$ es un número real computable.

Demostración.

(1) Sea $s : \mathbb{Z}^+ \to \mathbb{Q}$ un generador Turing-computable para x tal que $|x - s(n)| \leq 2^{-n}$, para todo $n \in \mathbb{Z}^+$.
(2) Sea $t : \mathbb{Z}^+ \to \mathbb{Q}$ un generador Turing-computable para y tal que $|y - t(n)| \leq 2^{-n}$, para todo $n \in \mathbb{Z}^+$.
(3) Parte (i)
  (a) Sea $u(n) = s(n+1) + t(n+1)$.
  (b) Para todo $n \in \mathbb{Z}^+$

$$\begin{aligned} |(x+y) - u(n)| &\leq |x - s(n+1)| + |y - t(n+1)| \quad \text{(desigualdad triangular)} \\ &\leq 2^{-n-1} + 2^{-n-1} \\ &= 2^{-n}. \end{aligned}$$

  (c) Luego, $u(n)$ es un generador Turing-computable para $x+y$ tal que $|(x+y) - u(n)| \leq 2^{-n}$, para todo $n \in \mathbb{Z}^+$.
(4) Parte (ii)
  (a) Sea $v(n) = s(n+1) - t(n+1)$.
  (b) Para todo $n \in \mathbb{Z}^+$

$$\begin{aligned} |(x-y) - v(n)| &\leq |x - s(n+1)| + |y - t(n+1)| \quad \text{(desigualdad triangular)} \\ &\leq 2^{-n-1} + 2^{-n-1} \\ &= 2^{-n}. \end{aligned}$$

  (c) Luego, $v(n)$ es un generador Turing-computable para $x-y$ tal que $|(x-y) - v(n)| \leq 2^{-n}$, para todo $n \in \mathbb{Z}^+$.
(5) Parte (iii)
  (a) Sea $m \in \mathbb{Z}^+$ tal que si $|x - z| \leq 1$ o $|y - z| \leq 1$ entonces $|z| \leq 2^{-m}$.
  (b) Sea $w(n) = s(m+n+1) \cdot t(m+n+1)$.

(c) Para todo $n \in \mathbb{Z}^+$,

$$\begin{aligned}|(x \cdot y) - w(n)| \leq\ & |x \cdot y - y \cdot s(m+n+1)| \\ & + |y \cdot s(m+n+1) - s(m+n+1) \cdot t(m+n+1)| \\ & \text{(desigualdad triangular)} \\ \leq\ & |x - s(m+n+1)| \cdot |y| + |y - t(n+1)| \cdot |s(m+n+1| \\ \leq\ & 2^{-(m+n+1)} \cdot 2^m + 2^{-(m+n+1)} \cdot 2^m \\ =\ & 2^{-n}.\end{aligned}$$

(d) Luego, $w(n)$ es un generador Turing-computable para $x \cdot y$ tal que $|(x \cdot y) - w(n)| \leq 2^{-n}$, para todo $n \in \mathbb{Z}^+$.

□

Una vez definidas la adición y la multiplicación sobre $\mathbb{R}_C$ se demuestra la existencia de inversos para estas operaciones.

Teorema 4.2. Si $x > 0$ es un número real computable entonces $-x$ es un número real computable.

Demostración. Por el ejemplo 3.5 sólo es necesario considerar el caso de que $x \in (\mathbb{R} - \mathbb{Q}^+)$.

(1) Sea $x \in (\mathbb{R} - \mathbb{Q}^+)$ un número real computable.

(2) Por la parte (ii) del teorema 4.2 $-x = 0 - x$ es un número real computable. □

Teorema 4.3. Si $x \neq 0$ es un número real computable entonces $\frac{1}{x}$ es un número real computable.

Demostración.

(i) Sea $s : \mathbb{Z}^+ \to \mathbb{Q}$ un generador total Turing-computable para x tal que $|x - s(n)| \leq 2^{-n}$, para todo $n \in \mathbb{Z}^+$.

(ii) Sea $m \in \mathbb{Z}^+$ tal que $|x| > 2^{-m}$ entonces $|s(n)| > 2^{-(m+1)}$ para $n > m$.

(iii) Sea $u(n) = \frac{1}{s(2m+n+1)}$.

(iv) Para todo $n \in \mathbb{Z}^+$,

$$\begin{aligned}\left|\frac{1}{x} - u(n)\right| &= \left|\frac{1}{x} - \frac{1}{s(2m+n+1)}\right| \\ &= |x - s(2m+n+1)| \cdot |x|^{-1} \cdot |s(2m+n+1)|^{-1} \\ &\leq 2^{-(2m+n+1)} \cdot 2^m \cdot 2^{m+1} \\ &= 2^{-n}.\end{aligned}$$

(v) Luego, $u(n)$ es un generador Turing-computable para $\frac{1}{x}$ tal que $\left|\frac{1}{x} - u(n)\right| \leq 2^{-n}$, para todo $n \in \mathbb{Z}^+$. □

Una vez definidas las operaciones de adición y multiplicación de números reales y sus correspondientes inversos de forma tal que satisfacen los axiomas (1) se obtiene que el sistema de los números reales computables es un campo.

Teorema 4.4. La estructura algebraica $\langle \mathbb{R}_c, +, \cdot, 0, 1\rangle$ es un campo, denominado el campo de los números reales computables.

La relación $\rhd$ de $\mathbb{R}$ es heredada por el sistema de los números reales computables, por lo tanto, este sistema adquiere la estructura de campo ordenado.

Teorema 4.5. La estructura algebraica $\langle \mathbb{R}_c, \rhd\rangle$ es un campo ordenado, donde $\mathbb{R}_c$ denota el campo de los números reales computables.

Teorema 4.6. La estructura algebraica $\langle \mathbb{R}_c, \rhd\rangle$ es un campo ordenado incompleto.

Demostración.

(i) El campo ordenado completo de los números reales $\langle \mathbb{R}, \rhd\rangle$ es el menor campo ordenado completo (excepto isomorfismos) que contiene al campo de los ordenado incompleto de los números racionales [14].

(ii) El campo ordenado de los números reales computables $\langle \mathbb{R}_c, \rhd\rangle$ contiene al campo ordenado de las números racionales.

(iii) Los campos ordenados $\langle \mathbb{R}, \rhd\rangle$, $\langle \mathbb{R}_c, \rhd\rangle$ no son isomorfos.

(iv) El campo ordenado $\langle \mathbb{R}_c, \rhd\rangle$ es un campo ordenado incompleto. □

5. Conclusiones

La teoría (clásica) de la computabilidad ha sido considerada usualmente como una teoría discreta (en cuanto al espacio y a la evolución de la computación), sin embargo desde el mismo trabajo fundacional de Alan Turing relacionado con las (hoy denominadas) máquinas de Turing [16], es presentado el concepto de número real computable. La existencia del campo de los números reales computables indica como es posible pensar en computación sobre objetos continuos a partir de modelos de computación discreta.

En la actualidad, el trenzado de grandes áreas de las matemáticas (tales como el álgebra, la topología y el análisis) y la computabilidad posibilita por una parte, la construcción de teorías más sólidas relacionadas con la computación de objetos continuos y por otra parte, posibilita una mejor comprensión (y porque no, una posible extensión) de los objetos computables y las relaciones entre ellos.

6. Agradecimientos

Este artículo fue financiado por la universidad EAFIT, bajo el proyecto de investigación nro. 817424.

Referencias

[1] Apostol, Tom M. Calculus. 2.ª ed. Vol. 1. John Wiley & Sons, 1967.

[2] Barendregt, Henk. Functional Programming and Lambda Calculus. En: Handbook of Theoretical Computer Science. Volume B. Formal Models and Semantics. Ed. por van Leeuwen, J. Second impression. MIT Press, 1992. Cap. 7. DOI: 10.1016/B978-0-444-88074-1.50012-3.

[3] Behnke, H., Bachmann, F., Fladt, K. y Süs, W., eds. Fundamentals of Mathematics, Volume 1: Foundations of Mathematics, the Real Number System and Algebra. Third printing. Translated by S. H. Gould. MIT Press, 1986.

[4] Blum, Lenore, Cucker, Felipe, Shub, Michael y Smale, Steve. Complexity and Real Computation. Springer-Verlag, 1998.

[5] Blum, Lenore, Shub, Michael y Smale, Steve. On a Theory of Computation and Complexity over the Real Numbers: NP-Completeness Recursive Functions and Universal Machines. Bulletin of the American Mathematical Society 21.1 (1989), págs. 1-46. DOI: 10.1090/S0273-0979-1989-15750-9.

[6] Boyer, Carl B. A History of Mathematics. John Wiley & Sons, 1968.

[7] Brattka, Vasco. Recursive Characterization of Computable Real-Valued Function and Relations. Theoretical Computer Science 162.1 (1996), págs. 45-77. DOI: 10.1016/0304-3975(95)00249-9.

[8] Bridges, Douglas S. Computability: A Mathematical Sketchbook. Vol. 146. Graduate Texts in Mathematics. Springer-Verlag, 1994.

[9] Davis, Martin. Computability and Unsolvability. Dover Publications, 1982.

[10] Kleene, Stephen C. Introducción a la Metamatemática. Trad. por Garrido, Manuel. Vol. 42. Estructura y Función. Editorial Tecnos, 1974.

[11] Mac Lane, Saunders y Birkhoff, Garrett. Algebra. 3.ª ed. AMS Chelsea Publishing, 1999.

[12] Moore, Cristopher. Recursion Theory on the Reals and Continuous-Time Computation. Santa Fe, Institute. 1997.

[13] Penrose, Roger. La Nueva Mente del Emperador. Colección: Libro de mano No. 38. Grijalbo Mondadori, 1991.

[14] Phillips, Esther R. An Introduction to Analysis and Integration Theory. Dover Publications, 1984.

[15] Rudin, Walter. Principios de Análisis Matemático. 3.ª ed. McGraw-Hill, 1980.

[16] Turing, Alan M. On Computable Numbers, with an Application to the Entscheidungsproblem. Proceeding of the London Mathematical Society s2-42 (1936-1937), págs. 230-265. DOI: 10.1112/plms/s2-42.1.230.

[17] Weihrauch, Klaus. Computable Analysis: An Introduction. Springer-Verlag, 2000.

Email address: asr@eafit.edu.co
Email address: mvelez@eafit.edu.co
URL: www1.eafit.edu.co/asr

Grupo Lógica y Computación

Escuela de Ciencias y Humanidades

Universidad EAFIT