Universidade Estadual de Campinas – UNICAMP

Algoritmos Abstratos e seu Significado para a Matemática

Ruben A. Pela

Algoritmos Abstratos e seu Significado para a Matemática

Este exemplar corresponde a redação final da tese devidamente corrigida e defendida pelo Sr. Ruben Alekxander Pela e aprovada pela Comissão Julgadora

Campinas, 17 de junho de 1996

Prof. Dr. Walter A. Carnielli – Orientador

Dissertação apresentada ao Instituto de Matemática, Estatística e Ciência da Computação, UNICAMP, como requisito parcial para obtenção do Título de Mestre em Matemática.

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP

Pela, Ruben Alekxander

P36a Algoritmos abstratos e seu significado para matemática / Ruben Alekxander Pela -- Campinas, [S.P. :s.n.], 1996.

Orientador : Walter Alexandre Carnielli

Dissertação (mestrado) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Ciência da Computação.

1. Teoria da computação. 2. Equações diferenciais. 3. Estabilidade. 4. Teoria de recursão. 5. Sistemas dinâmicos. I. Carnielli, Walter Alexandre. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Ciência da Computação. III. Título.

Tese defendida e aprovada em 17 de junho de 1996

Pela Banca Examinadora composta pelos Profs. Drs.

Prof (a). Dr (a). JAIRO JOSÉ DA SILVA

Prof (a). Dr (a). JOSÉ CARLOS CIFUENTES VÁSQUEZ

Prof (a). Dr (a). WALTER ALEXANDRE CARNIELLI

Resumo

O propósito deste trabalho é mostrar que o conceito de computabilidade sobre estruturas abstratas – apesar de não acrescentar nada genuinamente novo ao conceito clássico de computação, formalizado pela teoria da recursão –, pode ser útil do ponto de vista matemático se visto como um conceito genuíno de computação. Tomamos como motivação, de um lado, o problema proposto por Arnold de decidir algoritmicamente se um ponto fixo de uma equação diferencial é ou não estável, e de outro, uma solução negativa deste problema que utiliza o conceito clássico de função computável. A partir da discussão gerada em torno desta solução, tentamos mostrar que o conceito de Turing-computabilidade é inadequado, sob um certo ponto de vista, para tratar problemas deste tipo. Tentamos mostrar que os modelos de computabilidade sobre estruturas abstratas propostos por Moschovakis, Friedman e Blum *et al.* podem ser usados para tratar o problema de uma forma mais 'realista'. Também discutimos alguns aspectos da teoria de computabilidade sobre os reais e sua relação com sistemas dinâmicos com o objetivo de enfatizar nosso ponto de vista. Além disso, discutimos brevemente algumas implicações desta análise para a Tese de Church-Turing.

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP

Pela, Ruben Alekxander

P36a Algoritmos abstratos e seu significado para matemática / Ruben Alekxander Pela -- Campinas, [S.P. :s.n.], 1996.

Orientador : Walter Alexandre Carnielli

Dissertação (mestrado) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Ciência da Computação.

1. Teoria da computação. 2. Equações diferenciais. 3. Estabilidade. 4. Teoria de recursão. 5. Sistemas dinâmicos. I. Carnielli, Walter Alexandre. II. Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Ciência da Computação. III. Título.

Índice

Introdução

Vamos considerar a seguinte hipótese:

Hipótese da Computabilidade Abstrata. É possível formular uma teoria abstrata da computação de tal forma que:

(1) leve em conta processos matemáticos que aparentemente envolvem aspectos algorítmicos,

(2) possa servir de critério para expressar tais processos.

Este trabalho tem um duplo propósito:

- Mostrar em que termos a hipótese da computabilidade abstrata, `HCA`, deve ser entendida, ou seja, mostrar quais são os processos matemáticos que aparecem em (1) e em que tipo de questões se faz necessário uma tal teoria da computação.
- Mostrar porque acreditamos que `HCA` é verdadeira.

Os motivos que nos levaram a formular tal hipótese, e por consequência, em que termos `HCA` deve ser entendida envolvem alguns fatos que passaremos a considerar.

No Congresso Internacional de Matemática realizado em Paris em 1900, o então famoso matemático David Hilbert enunciou uma bem conhecida lista de problemas que direcionou grande parte da atividade matemática deste século. Desses, o décimo problema de Hilbert consistia em encontrar um procedimento geral capaz de decidir se uma equação diofantina sobre $\mathtt{Z}$ possui ou não soluções inteiras.

Com a formalização do conceito de *algoritmo* e o desenvolvimento da teoria da recursão, também chamada de teoria da computabilidade, parecia possível que um tal algoritmo poderia não existir. Trabalhando nesta direção, Davis, Matijasevich e Robinson [**DMR**] resolveram de forma notável o décimo problema de Hilbert, mostrando que de fato um tal algoritmo não existe.

Com o objetivo de avaliar a situação dos problemas de Hilbert, a *American Mathematical Society* realizou em 1974 uma conferência na qual, refletindo as principais tendências da pesquisa em matemática, uma nova lista de problemas foi proposta [1]. O matemático russo V. I. Arnold contribuiu com as seguintes questões relacionada a uma questão particularmente recalcitrante em quações diferenciais:

> *Is the stability problem for stationary points algorithmically decidable?* The well-known Lyapunov theorem solves the problem in the absence of eigenvalues with zero real parts. In more complicated cases, where the stability depends on higher order terms in the Taylor series, there exists no *algebraic* criterion.
>
> *Let be a vector field be given by polynomials of a fixed degree, with rational coefficients. Does an algorithm exist, allowing to decide, whether the stationary point is stable?*
>
> A similar problem: Does there exist an algorithm to decide, whether a plane polynomial vector field has a limit cycle?

Em [**dCD 4, 6, 7**] da Costa e Doria, utilizando basicamente as mesmas técnicas de Davis, Matijasevich e Robinson, e um resultado de Richardson [**Ri**], resolveram o problema acima de forma negativa, isto é, provando que não existe um algoritmo no sentido clássico capaz de decidir se um ponto singular de um sistema de equações diferenciais é ou não estável. Mais precisamente, eles construíram uma família $\Delta(m)$ enumerável de sistemas de equações diferenciais polinomiais parametrizadas por m, tal que o conjunto $\{m \in \mathbb{N} : \text{a origem é estável em } \Delta(m)\}$ não é recursivo.

Diante da solução de da Costa e Doria, em [**Ar4**] Arnold faz importantes observações sobre como o seu problema deve ser entendido:

> In my problem the coefficients of the polynomials of known degree and of a known number of variables are written on the tape of the standard Turing machine in the standard order and in the standard representation.
>
> The problem is whether there exists an algorithm (an additional text for the machine independent of the values of the coefficients) such that it solves the stability problem for the stationary point at the origin (i.e., always stops giving the answer"stable" or "unstable").
>
> I hope, this algorithm exists if the degree is one. It also exists when the dimension is one. My conjecture has always been that there is no algorithm for some sufficiently high degree and dimension, perhaps for dimension 3 and degree 3 or even 2. I am less certain about what happens in dimension 2.
>
> Of course the nonexistence of a general algorithm for a fixed dimension working for arbitrary degree or for a fixed degree working for an arbitrary dimen-

[1] *The mathematics arising from Hilbert's problem's*, **Proc. Symp. Pure Math.**, A.M.S., vol. 28, 1976.

sion, or working for all polynomials with arbitrary degree and dimension would also be interesting.

Integers were introduced in the formulation only to void the difficulty of explaining the way the data are written on the machine's tape. The more realistic formulation of the problem would require the definition of an analytic algorithm working with real numbers and functions (defined as symbols). The algorithm should permit arithmetical operations, modulus, differentiation, integration, solution of nondifferential equations (...), exponentiation, logarithms, evaluation of "computable" functions for "computable" arguments. The conjecture is that with all those tools one is still unable:

1. To solve the general stability problem starting from the right hand side functions as symbols with which one may perform the preceding operations.

2. To solve the above problem for polynomial vectorfields with real or complex coefficients.

3. To solve them with integer coefficients.

However as far as I know there are no words in logic to describe the above problem and I have thus preferred to stop at the level of algorithms in the usual sense rather than to try to explain to logicians the meaning of the impossibility of the solution of differential equations of a given type by quadratures (e.g., in the Liouville case in classical mechanics or in the theory of second order ordinary differential equations). The main difficulty here is that the solvability or unsolvability should be defined in a way that makes evident the invariance of this property under admissible changes of variables defined by functions that one can construct from the right hand side of the equations in a given corrdinate system. In other terms we should explicitly describe the structure of the manifold where the vector field is given, with respect to which the equation is nonintegrable.

In the usual approach this structure is a linear space structure, and I think it is too restrictive.

In any case I would like to known whether you think you have proved my conjectures on polynomial vectorfields with integer coefficients:

- For some pair (degree, dimension);
- For some dimension;
- For some degree, the polynonials being given on the tape of the machine in the standard form. If one of those undecidability conjectures is proved, it would be interesting to know for which pair (degree, dimension), or value of the dimension or value of the degree is the undecidability proven.

A partir deste comentário de Arnold podemos extrair as seguintes observações:

- Interpretar o sentido da palavra "algoritmo" que aparece na formulação original em termos de máquinas de Turing é apenas uma primeira aproximação, pois é o único conceito formal conhecido (por Arnold) que captura, segundo a Tese de Church, a noção de computabilidade intuitiva.
- Colocando o problema em termos da não existência de critérios algébricos, Arnold coloca em evidência o caráter algorítmico destes critérios, que estariam mais próximos de uma formulação "mais realista".

Cabe lembrar aqui que estas observações estão diretamente relacionadas a uma questão muito mais geral, a saber, sobre a existência de um conceito mais geral de computação, já tratada por Kreisel em [**Kr1**].

A partir destas observações optamos por abordar os seguintes ítens:

(1) Porque o conceito de Turing-computabilidade não é adequado frente a uma versão mais realista do problema, ou seja, em que sentido uma solução é esperada.

(2) A partir de (1), analisar a possibilidade de formalizar o conceito de computação que permeia os critérios algébricos de estabilidade e a noção intuitiva de algoritmo analítico. Mas isto pressupõe que estas noções carregam algum sentido computacional intuitivo. Qual seria então o sentido de 'computável' induzido por estas noções?

(3) Indicar que sentido uma solução poderia ser esperada em vista de (2) e (3).

Acreditamos que seria interessante responder, pelo menos de forma aproximada às questões acima.

Não há nenhuma intenção neste trabalho de responder a todas essas questões, embora obviamente, o sentido de se considerar uma tal discussão é obter como produto final uma resposta precisa, seja ela positiva ou não. Vamos apenas traçar um panorama geral de toda a problemática, esboçando os pressupostos e consequências.

Como subproduto desta análise, acreditamos obter argumentos que suportam a Hipótese da Computabilidade Abstrata, atigindo assim os propósitos iniciais.

A partir destas observações, optamos por estruturar este trabalho da seguinte maneira.

No Capítulo 1 vamos rever alguns dos resultados de da Costa e Doria relacionados a incompletude e indecidibilidade em Análise e a solução apresentada por estes autores do problema de Arnold.

A partir do material exposto neste capítulo podemos discutir com um pouco mais de embasamento a observação de Arnold diante da solução de da Costa e Doria e os motivos que levaram Arnold a formulação do seu problema. Isto é feito no Capítulo II onde, também com o objetivo de fundamentar os argumentos, há uma pequena apresentação sobre a insolubilidade algébrica do problema de classificação de pontos singulares com relação à estabilidade de LYAPUNOV. Por se tratar de um assunto bastante complexo, apresentamos apenas um esboço superficial das idéis envolvidas relevantes a esta discussão.

A partir deste ponto, acreditamos ter delineado de forma um pouco mais precisa, o sentido da não adequação do conceito clássico de algoritmo para tratar o problema de Arnold.

No capítulo III, somos levados a rever alguns trabalhos que têm por objetivo construir uma teoria de recursão generalizada como por exemplo [**Mos1, 2**] e [**Fr1**] e também um caso particular desta teoria, tratado por Blum, Shub e Smale em [**BSS**]. A motivação inicial é tentar capturar, pelo menos de forma aproximada, o conceito de algoritmo proposto por Arnold. Acreditamos que o material exposto neste capítulo fornece argumentos para sustentar o ponto central deste trabalho, ou seja, a hipótese HCA. Estaremos então, ao mesmo tempo, tentando estabelecer um ambiente para a discussão da possibilidade de uma solução satisfatória do problema de Arnold e, tentando mostrar como a teoria da computabilidade abstrata adquire um novo *status* diante de problemas, como os do tipo de Arnold.

No Capítulo IV exploramos um pouco mais computabilidade sobre anéis, em particular sobre os reais, na direção de resultados de indecidibilidade. Talvez este seja o capítulo mais técnico, onde estabelecemos algumas relações entre recursividade sobre os reais e dimensão de Hausdorff. Como consequência pode-se mostrar que o conjunto de Mandelbrot não é recursivo sobre os reais.

Apresentamos ainda no último capítulo, além de uma conclusão algumas questões que nos pareceram pertinentes.

Uma última observação: em todos os capítulos procuramos destacar os pontos que consideramos problemáticos. Talvez o aspecto mais interessante deste trabalho esteja justamente localizado nas questões não resolvidas que surgem durante a discussão e análise dos resultados.

1. Indecidibilidade e Incompletude em Análise

A. Algumas definições e resultados básicos.

Vamos rever alguns resultados clássicos envolvendo indecidibilidade e incompletude de sistemas formais. Assim, por exemplo, provaremos o primeiro teorema da incompletude de Gödel a partir da existência de conjuntos enumeráveis recursivamente não-recursivos e, juntamente com a caracterização algébrica dos conjuntos recursivamente enumeráveis obtida por Matijasevich, vamos obter uma versão do teorema de Gödel que será utilizada na seção C. Seguimos basicamente [**Od**], onde todas as demonstraçãos omitidas podem ser encontradas.

Definição. A classe `Prim` das **funções recursivas primitivas** é definida indutivamente por:

(1) as **funções iniciais** $\mathcal{Z}(x) = 0$, $\mathcal{S}(x) = x+1$ e $\mathcal{I}_i^n(x_1, \ldots, x_n) = x_i$ com $1 \leq i \leq n$, pertencem a `Prim`,

(2) **composição**: se $\psi, \phi_1, \ldots, \phi_m \in$ `Prim`, então $\psi(\phi_1, \ldots, \phi_m) \in$ `Prim`,

(3) **recursão**: se $\phi(\vec{x})$ e $\varphi(\vec{x}, y, z)$ pertencem a `Prim` então $\psi(\vec{x}, y)$ pertence a `Prim` onde,

$$\psi(\vec{x}, 0) =_{\text{def}} \phi(\vec{x})$$
$$\psi(\vec{x}, y+1) =_{\text{def}} \varphi(\vec{x}, y, \psi(\vec{x}, y))$$

(4) as únicas funções pertencentes a `Prim` são as funções definidas por aplicações sucessivas de (1), (2) e (3).

Um predicado $R(\vec{x})$ é **recursivo primitivo** se a função característica de R, denotada por $C_R \in$ `Prim`. Se $R(\vec{x}, y) \in$ `Prim`, então a operação de **μ-recursão limitada sobre** $R(\vec{x}, y)$ é definida por

$$\mu y_{\leq z} R(\vec{x}, y) =_{\text{def}} \begin{cases} \min_y R(\vec{x}, y) & \text{se } (\exists y \leq z) R(\vec{x}, y) \\ 0 & \text{caso contrário} \end{cases}$$

A função definida pela operação de μ-recursão limitada sobre um predicado recursivo primitivo é um exemplo de função recursiva primitiva (cf. [**EC**]). Outros exemplos que serão usados posteriormente são:

- $J(x, y) =_{\text{def}} \mu z_{\leq (x+y-2)(x+y-1)+2x} (2z = (x+y-2)(x+y-1)+2x)$

- $K(z) =_{\text{def}} \mu x_{\leq z}(\exists y \leq z)(z = J(x,y))$
- $L(z) =_{\text{def}} \mu y_{\leq z}(\exists x \leq z)(z = J(x,y))$

A função $J(x,y)$ é uma das possíveis funções que enumeram os racionais[2], que neste caso são vistos como pares de naturais. É claro, por construção, que $J : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ é uma bijeção e além disso, as funções K e J pertencem a `Prim` e satisfazem $K(J(x,y)) = x$, $L(J(x,y)) = y$ e $J(K(z), L(Z)) = Z$.

Se ϕ é uma função parcial então a notação $\psi \simeq_{\text{def}} \phi$ significa que ψ é indefinida se ϕ é indefinida e $\psi =_{\text{def}} \phi$ se ϕ é definida. Se ψ e ϕ são funções parciais já definidas, então $\psi(x) \simeq \phi(x)$ quando ou ambas são indefinidas ($\psi\uparrow$ e $\phi\uparrow$) para x ou, ambas são definidas ($\psi\downarrow$ e $\phi\downarrow$) em x e neste caso $\psi(x) = \phi(x)$;

Definição. A classe `Parc` das *funções recursivas parciais* é definida indutivamente por:

(1) as funções **iniciais** $\mathcal{Z}(x) = 0$, $\mathcal{S}(x) = x+1$ e $\mathcal{I}_i^n(x_1, \ldots, x_n) = x_i$ com $1 \leq i \leq n$, pertencem a `Parc`,

(2) **recursão**: se $\psi, \phi_1, \ldots, \phi_m \in$ `Parc`, então $\psi(\phi_1, \ldots, \phi_m) \in$ `Parc`,

(3) **composição**: se $\phi(\vec{x})$ e $\varphi(\vec{x}, y, z)$ pertencem a `Parc` então $\psi(\vec{x}, y)$ pertence a `Parc` onde,

$$\psi(\vec{x}, 0) \simeq_{\text{def}} \phi(\vec{x})$$
$$\psi(\vec{x}, y+1) \simeq_{\text{def}} \varphi(\vec{x}, y, \psi(\vec{x}, y))$$

(4) μ-**recursão**: se $\varphi \in$ `Parc` então $\psi \in$ `Parc` onde,

$$\psi(\vec{x}) \simeq_{\text{def}} \mu y[(\forall z \leq y)(\varphi(\vec{x}, z)\downarrow \wedge \varphi(\vec{x}, y) \simeq 0]$$

(5) as únicas funções pertencentes a `Parc` são as funções definidas por aplicações sucessivas de (1), (2), (3) e (4).

Uma função f é **recursiva** se $f \in$ `Parc` e f é **total**, i.e., f é sempre definida.

Teorema 1.1. (**Forma normal para funções recursivas parciais**) Existe uma função $\mathcal{U} \in$ `Prim` e, para cada $n \geq 1$, existem predicados recursivos primitivos T_n, tal que, para qualquer função $\varphi \in$ `Parc` de n variáveis, existe um número e (chamado **índice de** φ) tal que,

(1) $\varphi(x_1, \ldots, x_n)\downarrow \Leftrightarrow \exists y T_n(e, x_1, \ldots, x_n, y)$

(2) $\varphi(x_1, \ldots, x_n)\downarrow \simeq \mathcal{U}(\mu y T_n(e, x_1, \ldots, x_n, y))$.

[2] esta construção é análoga à de [**EC**, p. 40])

A partir deste resultado pode-se obter uma enumeração recursiva parcial das funções recursivas parciais, ou seja, se φ^n_e (ou $\{e\}^n$) é a e-ésima função recursiva parcial de n variáveis, i.e.,

$$\varphi^n_e(\vec{x}) \simeq \{e\}^n(\vec{x}) \simeq \mathcal{U}(\mu y T_n(e, \vec{x}, y)),$$

existe uma função recursiva parcial de $n+1$ variáveis tal que $\varphi(e, \vec{x}) \simeq \varphi^n_e(\vec{x})$. Para isto é suficiente definir $\varphi(e, \vec{x})$ por

$$\varphi(e, \vec{x}) \simeq_{\text{def}} \mathcal{U}(\mu y T_n(e, \vec{x}, y)).$$

Este resultado, conhecido como **teorema da enumeração**, admite uma formulação mais forte, devido basicamente a uniformidade do predicado T_n em relação à n, ou seja, se $\langle x_1, \ldots, x_n \rangle = p_0^n p_1^{x_1} \cdots p_n^{x_n}$, onde p_i é o $(i+1)$-ésimo primo, então,

Teorema 1.2. Existe uma função recursiva parcial $\varphi_{univ}(e, x)$, chamada de **função parcial universal** tal que se ψ é uma função recursiva parcial qualquer de n variáveis (n qualquer), então existe um índice e tal que

$$\psi(x_1, \ldots, x_n) \simeq \varphi_{univ}(e, \langle x_1, \ldots, x_n \rangle)$$

Pode-se obter resultados análogos aos anteriores para conjuntos e relações. Por definição, uma relação n-ária P é **recursivamente enumerável** quando o conjunto $\{\vec{x} : P(\vec{x})\}$ é o domínio de uma função n-ária recursiva parcial φ^n_e, i.e., $P(\vec{x}) \leftrightarrow \varphi_e(\vec{x})\downarrow$. O domínio de φ^n_e será denotado por $\mathcal{W}^n_e$. Um conjunto $\mathcal{A}$ é **recursivamente enumerável** se existe $\varphi_e \in \texttt{Parc}$ tal que $\varphi(\mathcal{A})\downarrow$. Um conjunto é **recursivo** se sua função característica $C_{\mathcal{A}}$ é recursiva.

Teorema 1.3. (**Forma normal para relações recursivamente enumeráveis**) Uma relação P n-ária é recursivamente enumerável se, e somente se, existe uma relação recursiva $n+1$-ária R tal que

$$P(\vec{x}) \Leftrightarrow \exists y R(\vec{x}, y),$$

i.e., se, e somente se existe um número e (chamado **índice de** P tal que,

$$P(\vec{x}) \Leftrightarrow \vec{x} \in \mathcal{W}^n_e \Leftrightarrow \exists y T_n(e, \vec{x}, y)$$

Demonstração. Se P é recursivamente enumerável, então existe um e tal que $P = \mathcal{W}_e$, e pelo teorema (1.1),

$$\begin{aligned} \vec{x} \in \mathcal{W}_e &\Leftrightarrow \varphi_e(\vec{x})\downarrow \\ &\Leftrightarrow \exists y T_n(e, \vec{x}, y). \end{aligned}$$

reciprocamente, se $P(\vec{x}) \Leftrightarrow \exists y R(\vec{x}, y)$ com R recursiva, então P é o domínio da função recursiva parcial $\varphi(\vec{x}) \ \simeq_{\text{def}} \ \mu y R(\vec{x}, y)$.□

Corolário 1.4. Um conjunto $\mathcal{A}$ é recursivo se, e somente se $\mathcal{A}$ e o complemento de $\mathcal{A}$, denotado por $\overline{\mathcal{A}}$, são ambos enumeráveis recursivamente

Demonstração. Se $\mathcal{A}$ é recursivo então $C_{\mathcal{A}}$ é recursiva e $\mathcal{A}$ e $\overline{\mathcal{A}}$ são respectivamente os domínios das funções parciais

$$\begin{aligned} \varphi(x) &\simeq \begin{cases} 1 & \text{se } C_{\mathcal{A}}(x) = 1 \\ \uparrow & \text{caso contrário} \end{cases} \\ \psi(x) &\simeq \begin{cases} 0 & \text{se } C_{\mathcal{A}}(x) = 0 \\ \uparrow & \text{caso contrário} \end{cases} \end{aligned}$$

Por outro lado, se $\mathcal{A}$ e $\overline{\mathcal{A}}$ são recursivamente enumeráveis então existem relações recursivas R e Q tais que

$$\begin{aligned} x \in A &\Leftrightarrow \exists y R(x, y) \\ x \in \overline{A} &\Leftrightarrow \exists y Q(x, y) \end{aligned},$$

e como $\forall x \exists y(R(x, y) \vee Q(x, y))$ vale, a função $f(x) = \mu y(R(x, y) \vee Q(x, y))$ é recursiva e, além disso, ou $Q(x, f(x))$ ou $R(x, f(x))$ é verdadeira. Isto mostra que o conjunto $\mathcal{A}$ é recursivo pois,

$$C_{\mathcal{A}}(x) = \begin{cases} 1 & \text{se } R(x, f(x)) \\ 0 & \text{caso contrário} \end{cases}$$

é recursiva.□

Combinando estes resultados podemos mostrar que *existe um conjunto $\mathcal{K}$ recursivamente enumerável e não recursivo*: basta definir $\mathcal{K}$ como

$$x \in \mathcal{K} \ \Leftrightarrow \ x \in \mathcal{W}_x \ \Leftrightarrow \ \varphi_x(x)\downarrow,$$

pois se $\varphi(e, x)$ é a função que enumera todas as funções recursivas parciais, então $\phi(x) \simeq_{def} \varphi(x, x)$ é recursiva parcial e $x \in \mathcal{K} \ \Leftrightarrow \ \phi(x)\downarrow$

Para mostrar que $\mathcal{K}$ não é recursivo, basta observar que se $\mathcal{K}$ fosse recursivo, $\overline{\mathcal{K}}$ seria recursivamente enumerável, mas $x \in \overline{\mathcal{K}} \ \Leftrightarrow \ x \notin \mathcal{W}_x$, i.e., $\exists u$ tal que $x \in \overline{K} \Leftrightarrow x \in \mathcal{W}_u$. Mas $u \in \overline{K} \Leftrightarrow u \in \mathcal{W}_u$ e $u \notin \mathcal{W}_u \Leftrightarrow u \in \overline{K}$. Uma contradição.□

Vamos agora embutir $\mathcal{K}$ num sistema formal através do conceito de **representabilidade** e mostrar como as propriedades de $\mathcal{K}$ interferem no poder de prova do sistema, gerando alguns fenômenos como incompletude e indecidibilidade.

Se L é uma linguagem formal enumerável fixada, então é fácil ver que o conjunto de fórmulas bem formadas e de sentenças de L podem ser identificados, através de um processo de aritmetização, a seus conjuntos de códigos, respectivamente, F e S, e além disso, estes conjuntos são conjuntos recursivos[3]

Definição. Seja L uma linguagem formal enumerável. Um **sistema formal** $\mathcal{F}$ em L é um par (T, R) de conjuntos enumeráveis recursivamente contidos em S e interpretados respectivamente, como os conjuntos dos (códigos de) teoremas e fórmulas refutáveis de $\mathcal{F}$. O sistema $\mathcal{F}$ é:

(1) **consistente** se $T \cap R = \emptyset$

(2) **completo** se $T \cup R = S$

(3) **decidível** se T e R são recursivos

(4) **indecidível** se T não é recursivo

Dizemos que $\mathcal{F}' = (T', R')$ é uma **extensão** de $F = (T, R)$ se $L_{\mathcal{F}} \subset L_{\mathcal{F}'}$, $T \subset T'$ e $R \subset R'$.

Se A e B são dois conjuntos, então A/B é definido usualmente como sendo o conjunto $\{x \in A : x \notin B\}$.

Um exemplo de sistema formal é a **Aritmética de Peano** $\mathtt{PA}$ que assumiremos como já definido axiomaticamente. Fazendo isso, estamos assumindo como fato que o conjunto das fórmulas bem formadas e sentenças de $\mathtt{PA}$ são recursivos.

Definição. Dado um sistema formal $\mathcal{F}$ e uma função f, dizemos que:

(1) f é **representável fracamente** em $\mathcal{F}$ se, para alguma fórmula φ da linguagem de $\mathcal{F}$,

$$f(x_1, \ldots, x_n) = y \ \Leftrightarrow \vdash_{\mathcal{F}} \varphi(\overline{x}_1, \ldots \overline{x}_n, \overline{y})$$

(2) f é **representável** em $\mathcal{F}$ se, para alguma fórmula φ,

$$f(x_1, \ldots, x_n) = y \ \Rightarrow \vdash_{\mathcal{F}} \varphi(\overline{x}_1, \ldots \overline{x}_n, \overline{y})$$
$$f(x_1, \ldots, x_n) \neq y \ \Rightarrow \vdash_{\mathcal{F}} \neg\varphi(\overline{x}_1, \ldots \overline{x}_n, \overline{y})$$

(3) f é **representável fortemente** em $\mathcal{F}$ se para alguma fórmula φ, f é representável por φ e,

$$\vdash_{\mathcal{F}} (\forall y)(\forall z)[\varphi(\overline{x}_1, \ldots, \overline{x}_n, y) \wedge \varphi(\overline{x}_1, \ldots, \overline{x}_n, z) \rightarrow y = z]$$

[3]cf. por exemplo [**Od**] ou [**EC**]

A idéia aqui é que $\varphi(x_1, \ldots, x_n, z)$ define uma função parcial de $x_1, \ldots, x_n$ pois z é determinado unicamente e, além disso, esta função coincide com f quando f é definida.

De maneira análoga, dado um sistema formal $\mathcal{F}$ e uma relação R, dizemos que,

(1) R é **representável fracamente** se, para alguma fórmula φ,

$$R(x_1, \ldots, x_n) \Leftrightarrow \vdash_{\mathcal{F}} \varphi(\overline{x}_1, \ldots, \overline{x}_n)$$

(2) R é **representável** se, para algum φ,

$$\begin{aligned} R(x_1, \ldots, x_n) &\Rightarrow \vdash_{\mathcal{F}} \varphi(\overline{x}_1, \ldots \overline{x}_n) \\ \neg R(x_1, \ldots, x_n) &\Rightarrow \vdash_{\mathcal{F}} \neg\varphi(\overline{x}_1, \ldots \overline{x}_n) \end{aligned}$$

Proposição 1.5. Em qualquer sistema formal consistente extendendo `PA`:

(1) uma relação é representável se, e somente se, é recursiva

(2) uma relação é representável fracamente se, e somente se, é recursivamente enumerável

Teorema 1.6. (**Gödel**) Se $\mathcal{F}$ é um sistema formal e é uma extensão consistente de `PA`, então $\mathcal{F}$ é indecidível e incompleto.

Demonstração. O conjunto $\mathcal{K}$ é recursivamente enumerável e assim, pela proposição (1.5) existe uma fórmula φ que representa fracamente $\mathcal{K}$, i.e.,

$$x \in \mathcal{K} \Leftrightarrow \vdash_{\mathcal{F}} \varphi(\overline{x}).$$

Se $\mathcal{F}$ fosse decidível, então $\mathcal{K}$ seria recursivo, contradizendo as propriedades de $\mathcal{K}$. Além disso, $\mathcal{K}$ não pode ser representável por φ pois neste caso "$x \in \mathcal{K}$" seria, pela proposição (1.5), recursiva e consequentemente $\mathcal{K}$ seria recursivo. Então existe pelo menos um x tal que

$$x \in \overline{\mathcal{K}} \wedge \nvdash_{\mathcal{F}} \neg\varphi(\overline{x})$$

Como $\overline{\mathcal{K}}$ não é recursivamente enumerável, novamente pelo teorema (1.10), pela representabilidade fraca de $\mathcal{K}$, se $x \in \overline{\mathcal{K}}$ então $x \notin \mathcal{K}$, i.e., $\nvdash_{\mathcal{F}} \varphi(\overline{x})$. Então $\mathcal{F}$ é incompleto, pois $\varphi(\overline{x})$ e $\neg\varphi(\overline{x})$ não são prováveis em $\mathcal{F}$.□

Podemos caracterizar algebricamente os conjuntos enumeráveis recursivamente e obter uma expressão em termos de polinômios para a sentença $\varphi \in S/(T \cup R)$ obtida na demonstração do teorema (1.6).

Teorema 1.7. (**Matijasevich**) Um conjunto $\mathcal{W}$ é recursivamente enumerável se, e somente se, existe um polinômio $p_{\mathcal{W}}(\vec{x}, y)$ com coeficientes inteiros tal que

$$y \in \mathcal{W} \;\Leftrightarrow\; (\exists x_1, \ldots, x_n \in \mathbb{N})(p_{\mathcal{W}}(\vec{x}, y) = 0)$$

Se $\mathcal{W}_u$ é definido por

$$z \in \mathcal{W}_u \Leftrightarrow \varphi_{univ}(L(z), K(z))\downarrow$$

então como consequência deste resultado, existe um polinômio P_u tal que $z \in \mathcal{W}_u$ se, e somente se $P_u(z, \vec{x}) = 0$ para algum $\vec{x}$. Assim para todo $\mathcal{W}$ existe um índice e tal que

$$\begin{aligned} z \in \mathcal{W} \Leftrightarrow \varphi_{univ}(e, z)\downarrow &\Leftrightarrow J(e, z) \in \mathcal{W}_u \\ &\Leftrightarrow (\exists \vec{x}) P_u(J(e, z), \vec{x}) = 0 \end{aligned}$$

O polinômio P_u é chamado de **polinômio universal** e será denotado por P_{univ}.

Se $\mathcal{F}$ é um sistema formal e $L_{\text{PA}} \subset L_{\mathcal{F}}$, então $\mathcal{F}$ é **aritmeticamente consistente** se o modelo standard dos naturais $\mathbb{N}$ é um modelo para todas as sentenças de L_{PA} que são prováveis em $\mathcal{F}$.

Proposição 1.8. Se $\mathcal{F}$ é um sistema formal que contém PA e é aritmeticamente consistente, então existe um polinômio $p(x_1, \ldots, x_n)$ com coeficientes inteiros tal que

$$\begin{aligned} &\nvdash_{\mathcal{F}} (\forall x_1 \ldots x_n \in \mathbb{N})(p(x_1, \ldots, x_n) > 0) \;\; e, \\ &\nvdash_{\mathcal{F}} (\exists x_1 \ldots x_n \in \mathbb{N})(p(x_1, \ldots, x_n) = 0) \end{aligned}$$

Demonstração. Seja $A =_{\text{def}} \{a \in \mathbb{N} : \vdash_{\mathcal{F}} \neg(\exists \vec{x}) P_{univ}(J(a, a), \vec{x}) = 0\}$. Como os teoremas de $\mathcal{F}$ são enumeráveis recursivamente, existe um índice k tal que A é $\mathcal{W}_k$. Temos a seguinte situação:

(1) $k \in \mathcal{W}_k \leftrightarrow$ existe $\vec{x}$ tal que $P_{univ}(J(k, k), \vec{x}) = 0$, e

(2) $k \in \mathcal{W}_k \leftrightarrow \vdash_{\mathcal{F}} \neg(\exists \vec{x}) P_{univ}(J(k, k), \vec{x}) = 0$.

Se $k \in \mathcal{W}_k$ então por (2), $\vdash_{\mathcal{F}} \neg(\exists \vec{x}) P_{univ}(J(k, k), \vec{x}) = 0$. Como $\mathcal{F}$ é aritmeticamente consistente, pelo ítem (1) temos que $\nvdash_{\mathcal{F}} \neg(\exists \vec{x}) P_{univ}(J(k, k), \vec{x}) = 0$, ou seja, novamente por (2), $k \notin \mathcal{W}_k$. Uma contradição. Logo $k \notin \mathcal{W}_k$. Isto significa que

$$\nvdash_{\mathcal{F}} \neg(\exists \vec{x}) P_{univ}(J(k, k), \vec{x}) = 0$$

Por outro lado, como $\mathcal{F}$ é aritmeticamente consistente e $k \notin \mathcal{W}_k$, temos

$$\nvdash_{\mathcal{F}} (\exists \vec{x}) P_{univ}(J(k, k), \vec{x}) = 0 \qquad \square$$

Definição. Uma **função parcial** f **de** $\mathbb{N}^n$ **em** $\mathbb{N}$ é qualquer função definida (parcialmente) sobre $\mathbb{N}^n \to \mathbb{N}$. Vamos denotar por $\mathcal{PF}_n$ o conjunto de todas as funções parciais de $\mathbb{N}^n$ em $\mathbb{N}$. Um **funcional** F é uma função (parcial)

$$F : \mathcal{PF}_{k_1} \times \ldots \times \mathcal{PF}_{k_m} \times \mathbb{N}^n \to \mathbb{N}$$

O funcional $F(\alpha_1, \ldots, \alpha_n, \vec{x})$ é um **funcional recursivo parcial** se ele pode ser obtido de $\alpha_1, \ldots, \alpha_n$ e das funções iniciais por composição, recursão primitiva e μ-recursão. Dizemos que $F(\alpha_1, \ldots, \alpha_n, \vec{x})$ é **restrito** se $\alpha_1, \ldots, \alpha_n$ são funções totais.

Se f é uma função de $\mathbb{N}$ em $\mathbb{N}$ então $\langle f \rangle(y) =_{\text{def}} \langle f(0), f(1), \ldots, f(y) \rangle$

Teorema 1.9. (**Forma normal para funcionais recursivos parciais restritos**) Existe uma função $\mathcal{U} \in$ `Prim` e (para cada m, $n \geq 1$) predicados recursivos primitivos $T_{m,n}$ tal que, para qualquer funcional recursivo parcial restrito F de (m, n)-ário, existe um número e (chamado **índice de** F) tais que:

(1) $F(g_1, \ldots, g_m, \vec{x})\downarrow \Leftrightarrow \exists y T_{m,n}(e, \vec{x}, \langle g_1 \rangle(y), \ldots \langle g_n \rangle(y), y)$

(2) $F(g_1, \ldots, g_m, \vec{x}) \simeq \mathcal{U}(\mu y T_{m,n}(e, \vec{x}, \langle g_1 \rangle(y), \ldots, \langle g_n \rangle(y), y))$.

De forma análoga ao caso de funções recursivas parciais, definimos φ_e^A como a e-ésima função de n variáveis **recursiva parcial em** A, i.e.,

$$\varphi_e^A \simeq \mathcal{U}(\mu y T_{n,1}(e, \vec{x}, \langle c_A \rangle(y), y))$$

Definição. Um conjunto A é **Turing-redutível** a um conjunto B, denotado por $A \leq_T B$, se existe um índice e tal que $C_A \simeq \varphi_e^B$. $A \equiv_T B$ se $A \leq_T B$ e $B \leq_T A$. A relação $\equiv_T$ é uma relação de equivalência e as classes de equivalência definas por $\equiv_T$ são chamadas de T-**graus**.

É fácil ver que se A é recursivamente enumerável então $A \leq_T K$ e quaisquer dois conjuntos recursivamente enumeráveis são equivalentes por $\equiv_T$.

Seja $(x)_n =_{\text{def}}$ " o expoente do n-ésimo primo na decomposição de x". Então não é difícil ver que $(x)_n$ é uma função recursiva primitiva (cf. [**EC**]). Se $\mathcal{U}$ e $T_{m,n}$ são a função e o predicado definidos pelo teorema (1.6), então a função

$$\psi(e, w) \simeq_{\text{def}} \mathcal{U}(\mu y T_{1,1}(e, (w)_1, (w)_2, y))$$

é recursiva parcial. Sendo assim, $\phi(x) \simeq_{\text{def}} \psi(K(x), L(x))$ também é recursiva parcial e, $\phi(J(e, w)) \simeq \psi(e, w)$. Seja u tal que $\phi(x) \simeq \varphi_{univ}(u, x)$. Agora, se $A \subset \mathbb{N}$ é um conjunto qualquer e e é um índice qualquer e além disso sabemos o valor de $C_A(y)$

para todo $y \in \mathtt{N}$, então, utilizando este fato,

$$\begin{aligned} x \in \mathcal{W}_e^A &\Leftrightarrow \varphi_e^A(x)\downarrow \Leftrightarrow \mathcal{U}(\mu y T_{1,1}(e, x, \langle c_A\rangle(y), y)\downarrow \\ &\Leftrightarrow \psi(e, p_0^x p_1^{\langle c_A\rangle(y_0)})\downarrow \\ &\Leftrightarrow \phi(J(e, p_0^x p_1^{\langle c_A\rangle(y_0)}))\downarrow \\ &\Leftrightarrow \varphi_u(J(e, p_0^x p_1^{\langle c_A\rangle(y_0)}))\downarrow \\ &\Leftrightarrow J(e, p_0^x p_1^{\langle c_A\rangle(y_0)}) \in \mathcal{W}_u \end{aligned} \tag{1.10}$$

onde $y_0 = \mu y T_{1,1}(e, x, \langle c_A\rangle(y), y)$. Finalmente, usando o polinômio P_{univ}

$$x \in \mathcal{W}_e^A \Leftrightarrow (\exists y_1, \ldots, y_n \in \mathtt{N})[P_{univ}(J(u, J(e, p_0^x p_1^{\langle c_A\rangle(y_0)})), y_1, \ldots, y_n) = 0] \tag{1.11}$$

B. As traduções de Richardson.

Certas generalizações de resultados da teoria de números, como por exemplo, uma versão do décimo problema de Hilbert para corpos em geral tratada em [**Ph**] , que em sua forma original foi resolvido por Matijasevich graças aos resultados desenvolvidos por Davis, Putnam e Robinson, colocam novamente em evidência problemas envolvendo questões de decidibilidade (veja por exemplo [**Mz**]).

Basicamente, a principal técnica utilizada para mostrar a indecidibilidade de um corpo K, é mostrar que os inteiros são definíveis na teoria de K e, então, aplicar de forma adequada o resultado de Matijasevich, ou o fato de que existem subconjuntos de $\mathtt{N}$ não recursivos (em [**Ph**] há vários exemplos que utilizam esta construção). É interessante observar que esta mesma técnica foi usada por Richardson em 1968 [**Ri**] para mostrar que certos predicados existenciais sobre os *reais* são indecidíveis. Em linhas gerais, a idéia é construir, para cada polinômio $f(x, y)$ com coeficientes inteiros definido sobre $\mathtt{R}^n \times \mathtt{R}$, uma certa função $F(x, y) : \mathtt{R}^n \times \mathtt{R} \to \mathtt{R}$, de tal forma que o conjunto $A = \{y \in \mathtt{Z} : (\exists x \in \mathtt{R}^n)(F(x, y) = 0)\}$ coincide com o conjunto $B = \{y \in \mathtt{Z} : (\exists x \in \mathtt{N}^n)(f(x, y) = 0)\}$. Como existem polinômios para os quais B não é recursivo, o conjunto A correspondente também não será recursivo. Através desta construção é possível *traduzir* na linguagem da aritmética de segunda ordem $\mathtt{PA}^2$, i.e., na linguagem da *Análise*, predicados não recursivos sobre os naturais, obtendo predicados não recursivos sobre *os reais*.

O teorema (1.6), que em essência é o primeiro teorema da incompletude de Gödel, garante que $\mathtt{PA}^2$ também é um sistema formal indecidível e incompleto. Além disso a fórmula $\varphi \in S_{\mathtt{PA}^2}/(T_{\mathtt{PA}^2} \cup R_{\mathtt{PA}^2})$ é na verdade uma sentença expressável em $L_{\mathtt{PA}}$. Através deste processo de tradução, formalizado pelas chamadas **traduções de Richardson** (abaixo definidas), podemos construir sentenças indecidíveis envolvendo quantificação sobre os reais e, além disso, as expressões destas sentenças envolvem apenas funções elementares, como por exemplo, senos, somas e produtos.

Vamos rever alguns dos resultados obtidos por Richardson em [**Ri**].

Seja $X = \{x_i \mid i \in \mathbb{N}\}$ um conjunto de variáveis e $\mathcal{P}$ uma classe de expressões definida indutivamente por,

$$\mathcal{P}_0 = \{X\} \cup \{-1, 1\}$$
$$\mathcal{P}_i = \{e_k + e_l : e_k, e_l \in \mathcal{P}_{i-1}\} \cup \{e_k \cdot e_l : e_k, e_l \in \mathcal{P}_{i-1}\}$$
$$\mathcal{P} = \bigcup_{i \in \mathbb{N}} \mathcal{P}_i$$

Se $\overline{p} \in \mathcal{P}$ e n é o maior índice tal que x_n ocorre em $\overline{p}$ então, $\overline{p}$ define de maneira natural (interpretando $+$ e $\cdot$ como as operações usuais sobre um anel R) uma função polinomial com coeficientes inteiros $p(x_1, \ldots, x_n)$ definida sobre R^n, onde $R^n = \bigoplus_{i=1}^n R$.

Definimos de maneira análoga a classe $\mathcal{E}$ por,

$$\mathcal{E}_0 = \mathcal{P}_0$$
$$\mathcal{E}_i = \mathcal{P}_i \cup \{\operatorname{sen} e_k : e_k \in \mathcal{E}_{i-1}\} \cup \{|e_k| : e_k \in \mathcal{E}_{i-1}\}$$
$$\mathcal{E} = \bigcup_{i \in \mathbb{N}} \mathcal{E}_i$$

Dado as interpretações usuais de $+$, sen, $\cdot$ e $|\cdot|$ no corpo dos reais $\mathbb{R}$, cada $\overline{f} \in \mathcal{E}$ define uma função $f(x_1, \ldots, x_n)$ sobre $\mathbb{R}^n$ para algum n adequado. A fim de facilitar a exposição não vamos nos deter em questões de formalismo e usaremos as abreviações usuais das expressões acima. Assim, por exemplo, nem sempre será feita a distinção entre $\overline{f} \in \mathcal{E}$ e a função f definida por $\overline{f}$.

Para cada $f \in \mathcal{P}$ vamos definir por indução nas classes $\mathcal{P}_i$ uma expressão $\alpha f \in \mathcal{E}$ de tal forma que:

(1) para qualquer $x \in \mathbb{R}^n, \alpha f(x) > 1$,

(2) para quaisquer $x, \delta \in \mathbb{R}^n$, com $|\, \delta \,| \leq 1$, $\alpha f(x) > \| \, f(x+\delta) \, \|$

A definição pode ser feita da seguinte maneirra: se $f(x_1, \ldots, x_n) \in \mathcal{P}_0$ então ou $f = c$, onde c é uma constante, e neste caso $\alpha f =_{\text{def}} |\, c \,| + 2$; ou $f(x_1, \ldots, x_n) = x_i$ e então tomamos $\alpha f =_{\text{def}} x_i^2 + 2$. Se $f \in \mathcal{P}_i$ então ou $f = s + t$, com $s, t \in \mathcal{P}_{i-1}$ e $\alpha f = \alpha s + \alpha t$, ou $f = s \cdot t$, e neste caso tomamos $\alpha f = \alpha s \cdot \alpha t$.

Definição. A função β, chamada de **primeira tradução de Richardson**, que leva as funções definidas pelas expressões de $\mathcal{P}$ na classe de funções definidas pelas expressões de $\mathcal{E}$, é definida [4] por:

$$\beta(f(z_1,\ldots,z_n,w))(x_1,\ldots,x_n,y) =$$
$$= (n+1)^2(f^2(x_1,\ldots,x_n,y)+\sum_{i=1}^{n}(\sin^2\pi x_i)g_i^2(x_1,\ldots,x_n,y)),$$

onde $g_i = \alpha(\dfrac{\partial}{\partial x_i}f^2)$

Dado $f(z_1,\ldots,z_n,w) \in \mathcal{P}$, a função $\beta(f(z_1,\ldots,z_n,w))(x_1,\ldots,x_n,y)$ será denotada por $\beta f(x_1,\ldots,x_n,y)$.

Proposição 1.12. ([**Ri**], [**W**]) Para cada $f \in \mathcal{P}$ e $y \in \mathrm{Z}$ os seguintes ítens são equivalentes:

(1) existe $\vec{x} \in \mathrm{Z}^n$ tal que $f(\vec{x},y) = 0$,

(2) existe $\vec{x} \in \mathrm{R}^n$ tal que $\beta f(\vec{x},y) = 0$,

(3) existe $\vec{x} \in \mathrm{R}^n$ tal que $\beta f(\vec{x},y) < 1$.

Demonstração. Se y é um número natural fixado, basta mostrar que, se $a_1,\ldots,a_n \in \mathrm{R}$, $\beta f(a_1,\ldots,a_n,y) < 1$, então $f(b_1,\ldots,b_n,y) < 1$, onde b_i é o menor inteiro tal que $|b_i - a_i| \leq 1/2$. Isto implica que $f(b_1,\ldots,b_n,y) = 0$ pois f leva inteiros em inteiros. As outras equivalências são imediatas.

Vamos supor então que $\beta f(a,y) < 1$ para algum $a \in \mathrm{R}^n$. Então $f(a,y) < 1/(n+1)$ e $(\mathrm{sen}\pi a_i)g_i(a,y) < 1/(n+1)$. Pelo teorema do valor médio n-dimensional, existem c_i entre a_i e b_i tal que

$$\begin{aligned} f^2(b,y) &\leq f^2(a,y) + \sum_{i=1}^{n}|b_i - a_i|(\partial/\partial x_i)f^2(c,y) \\ &\leq f^2(a,y) + \sum_{i=1}^{n}|b_i - a_i|\, g_i(a,y), \qquad (\text{ pois } |c_i - a_i| \leq 1) \end{aligned}$$

Se mostarmos que $|b_i - a_i| \leq |\mathrm{sen}\pi a_i|$, então,

$$f^2(b,y) \leq f^2(a,y) + \sum_{i=1}^{n}|\mathrm{sen}\pi a_i| g_i(a,y)$$

Como cada um dos termos dessa desigualdade é menor do que $1/(n+1)$, teremos $f^2(b,y) < 1$ e consequentemente $f(b,y) = 0$.

[4] Pode-se tomar, na definição de βf, $|g_i|$ em vez de g_i^2. Fazendo isso, a proposição (1.12) continua válida. Mas na seção C, a função βf deverá ser polinomial, o que justifica nossa escolha.

Vamos supor então que $x \in \mathbb{R}$. Então, existe $x_0 \in [0, 1/2]$ e um inteiro k tal que $x = x_0 + k$ ou $x = 1 - x_0 + k$. Como $|\text{sen}\pi x| = |\text{sen}\pi(x+k)|$ para qualquer inteiro k, se $x \leq |\text{sen}\pi x|$ para $x \in [0, 1/2]$, então $|b_i - a_i| \leq |\text{sen}\pi a_i|$.

Agora é fácil ver (pelo menos graficamente) que $x \leq |\text{sen}\, \pi x|$ para $x \in [0, 1/2]$. Formalmente, tomando $g(x) = \text{sen}\, \pi x - x$, $g''(x) < 0$ em $(0, 1/2)$, $g'(0) = 0$ e $g'(1/2) < 0$. Portanto $g(x)$ assume um mínimo em 0, mas $0 \leq \text{sen}\, \pi 0 = 0$.□

Consequentemente, $\forall \vec{x} \in \mathbb{Z}^n f(\vec{x}, y) \neq 0 \Leftrightarrow (\forall \vec{x} \in \mathbb{R})\beta f(\vec{x}, y) > 0$.

Definição. Seja $\zeta(x) =_{\text{def}} x\text{sen}\, x$ e $\xi(x) =_{\text{def}} x\text{sen}\, x^3$. Considere as funções $\psi_i(x)$ definidas indutivamente por

$$\begin{aligned} &\psi_1(x) = \zeta(x) \\ &\psi_2(x) = \xi(\zeta(x)) \\ &\psi_i(x) = \xi(\psi_{i-1}(x)) \qquad 2 \leq i \leq n-1 \\ \text{e} \quad &\psi_n(x) = \xi^{on}(x) \end{aligned}$$

A função γ que leva as funções definidas por expressões da classe $\mathcal{P}$ em funções definidas pelas expressões da classe $\mathcal{E}$, é definida por,

$$\begin{aligned} &\gamma(f(z_1, \ldots, z_n, w))(x, y) \\ &\qquad = \beta(f(z_1, \ldots, z_n, w))(\psi_1(x), \psi_2(x), \ldots, \psi_n(x), y) \end{aligned}$$

e é chamada de **segunda tradução de Richardson.**

Proposição 1.13. [**Ri**], [**W**]) Para cada $y \in \mathbb{Z}$ e $f \in \mathcal{P}$, os seguintes ítens são equivalentes:

(1) existe $\vec{x} \in \mathbb{Z}^n$ tal que $f(\vec{x}, y) = 0$,

(2) existe $x \in \mathbb{R}$ tal que $\gamma f(x, y) < 1$.

A demonstração dessa proposição envolve basicamente a continuidade de βf e o fato de que para quaisquer reais $x_1, \ldots, x_n$ e $\delta > 0$, existe $z \in \mathbb{R}$ tal que

$$|\psi_i(z) - x_i| < \delta, \; 1 \leq i \leq n-1 \qquad e \qquad \psi_n(z) = x_n \tag{1.13.1}$$

Demonstração. Vamos mostrar inicialmente (1.13.1) por indução em n. Dados x_1, x_2 e $\delta > 0$ é sempre possível obter z_1 e z_2 tais que

$$\begin{aligned} &z_2 > z_1 > |x_2|, \\ &\zeta(z_2) = x_1, \\ &z_2^3 - z_1^3 > 2\pi, \\ &(z_2 - z_1)(z_2 + 1) < \delta \end{aligned} \tag{1.13.2}$$

Basta tomar $z_2 = (z_1 + \delta/2)^{1/2}$ e $z_1 > \max(4\pi/\delta, |x_2| + 1)$ tal que $z_2 \mathrm{sen} z_2 = x_1$.

Pelo Teorema do Valor médio e (1.13.2), para qualquer z entre z_1 e z_2 tem-se,

$$\begin{aligned}
|\psi_1(z) - x_1| &= |\zeta(z) - \zeta(z_2)| \\
&\leq (z_2 - z)|(\mathrm{sen} x + x\cos x)|, \qquad z < x < z_2 \\
&< (z_2 - z_1)(z_2 + 1) \\
&< \delta
\end{aligned}$$

Por outro lado, novamente por (1.13.2) existe z entre z_1 e z_2 tal que $\xi(z) = x_2$. Isto mostra que (1.13.1) é válido para $n = 2$.

Suponha por hipótese de indução que temos o resultado para $n = k$, i.e., existe $z^* \in \mathbb{R}$ tal que,

$$\begin{aligned}
&|\psi_1(z^*) - x_2| < \delta \\
&|\psi_2(z^*) - x_3| < \delta \\
&\qquad \vdots \\
&|\psi_{k-1}(z^*) - x_k| < \delta \\
&\xi^{ok}(z^*) = x_{k+1}
\end{aligned} \tag{1.13.3}$$

Novamente, pelo mesmo argumento para o caso $n = 2$, existe um número real z tal que $|\zeta(z) - x_1| < \delta$ e $\xi(z) = z^*$. Fazendo então as substituições em (1.13.1) obtemos (1.13.3).

Finalmente, dado uma função $f \in \mathcal{P}$ definida sobre $\mathbb{R}^n$, se o ítem (1) é válido, então, pela proposição (1.12) existem reais $a_1, \ldots, a_n$ tal que $\beta f(a_1, \ldots, a_n, y) < 1$, e por continuidade, existe $\delta > 0$ tal que se $|y_i - a_i| < \delta$, então $\beta f(y_1, \ldots, y_n, y) < 1$. Por (1.13.1), tomando $x_i = a_i$, existe um z tal que $|\psi_i(z) - a_i| < 0$. Tomando $y_i = \psi_i(z)$, teremos $\gamma f(z, y) < 1$. Reciprocamente, se existe um z tal que $\gamma f(x, y) < 1$, por continuidade, existe $\delta > 0$ tal que, se $a_1, \ldots a_n$ são tais que

$$\begin{aligned}
&|\psi_1(z) - a_1| < \delta \\
&|\psi_2(z) - a_2| < \delta \\
&\qquad \vdots \\
&|\psi_{n-1}(z) - a_{n-1}| < \delta \\
&\psi_n(z) = a_n,
\end{aligned}$$

então $\beta f(a_1, \ldots, a_n, y) < 1$ e assim, aplicando a proposição (1.12), os ítens (1) e (2) são equivalentes. □

C. Os resultados de da Costa e Doria.

Seja $\phi_m(n)$ a m-ésima função recursiva parcial aplicada em n.

Definição. A função

$$\theta(m,n) = \begin{cases} 1 & \text{se } \varphi_m(n)\downarrow \\ 0 & \text{caso contrário} \end{cases}$$

é chamada de **função de parada**

Esta função não é recursiva pois, caso contrário, $\theta(n,n)$ também seria recursiva e assim K seria recursivo. Consequentemente θ não é representável em PA.

Em [
smallbf dCD1], da Costa e Doria conseguiram obter, utilizando as traduções de Richardson, uma expressão para θ na linguagem da Análise. Vamos rever aqui este resultado e algumas de suas principais consequências.

Seja W um conjunto enumerável recursivamente e $p_{\mathcal{W}}(x_1,\ldots,x_u,y)$ o polinômio de Matijasevich definido pelo teorema (1.7) a partir de W. Seja

$$B(W,x,y) =_{\text{def}} |\gamma p_W(x,y) - 1| - \gamma p_W(x,y) + 1$$

Pelo teorema da enumeração a função $\varphi(x,y) \simeq_{\text{def}} \varphi_x(y)$ é recursiva parcial e portanto existe um índice e tal que

$$\varphi(x,y) \simeq \varphi_e(J(x,y))$$

Lembrando que $\mathcal{W}_e$ denota o domínio de φ_e,

$$\begin{aligned} \theta(m,n) = 1 &\Leftrightarrow J(m,n) \in \mathcal{W}_e \\ &\Leftrightarrow (\exists x_1,\ldots,x_v \in \mathtt{N}) p_{\mathcal{W}_e}(x_1,\ldots,x_v,J(m,n)) = 0 \qquad \text{(teorema (1.7))} \end{aligned}$$

Por um teorema de Lagrange, para qualquer natural $a > 0$ existem inteiros a_1, a_2 , a_3 e a_4 tal que $a = 1 + \sum_{i=1}^{4}(a_i)^2$. Então, dado um conjunto enumerável recursivamente $\mathcal{W}$, podemos definir um polinômio $L_{\mathcal{W}}$ a partir do polinômio $p_{\mathcal{W}}$ definido pelo teorema (1.7) da seguinte maneira:

$$\begin{aligned} L_{\mathcal{W}}(x_{1,1},\ldots,x_{1,4},\ldots,x_{i,1},x_{i,2},x_{i,3},x_{i,4},\ldots,x_{v,4},y) &=_{\text{def}} \\ &= p_{\mathcal{W}}(y, 1+\sum_{i=1}^{4}(x_{1,i})^2,\ldots,1+\sum_{i=1}^{4}(a_{j,i})^2,\ldots,1+\sum_{i=1}^{4}(a_{v,i})^2) \end{aligned}$$

Sendo assim, o teorema (1.7) continua válido para polinômios definidos sobre os inteiros, i.e.,

$$y \in \mathcal{W} \Leftrightarrow (\exists x_{1,1},x_{1,2},\ldots,x_{v,4} \in \mathtt{Z})(L_{\mathcal{W}}(\vec{x},y) = 0)$$

Aplicando as traduções de Richardson a $L_{\mathcal{W}_e}$ obtemos as seguintes equivalências:

$$\begin{aligned}\theta(m,n)=1 &\Leftrightarrow (\exists x_1,\ldots,x_{4v}\in \mathrm{Z})L_{\mathcal{W}_e}(x_1,\ldots,x_{4v},J(m,n))=0\\ &\Leftrightarrow (\exists \vec{x}\in \mathrm{R}^{4v})[\beta L_{\mathcal{W}_e}(\vec{x},J(m,n))=0] \qquad \text{(proposição (1.12))}\\ &\Leftrightarrow (\exists x\in \mathrm{R})[\gamma L_{\mathcal{W}_e}(x,J(m,n))<1]\\ &\Leftrightarrow (\exists x\in \mathrm{R})[B(\mathcal{W}_e,x,J(m,n))>0]\end{aligned}$$

Se $\sigma(x)=_{\text{def}} 0$ se $x=0$ e $\sigma(x)=_{\text{def}} 1$ caso contrário, então,

Teorema 1.14. (**da Costa-Doria, [dCD1]**)

$$\theta(m,n)=\sigma(C(m,n)) \;\; e$$
$$C(m,n)=_{\text{def}}\int_{-\infty}^{\infty}\frac{B(\mathcal{W}_e,x,J(m,n))}{1+B(\mathcal{W}_e,x,J(m,n))}e^{-x^2}dx$$

Se K e L são tais que $J(K(n),L(n))=n$, $L(J(m,n))=n$ e $K(J(m,n))=m$, então $\theta(n)=_{\text{def}}\theta(L(n),K(n))$.

A partir da expressão de θ é trivial construirmos exemplos de problemas indecidíveis em análise. Considere por exemplo a família de números reais $n+r\theta(n)$, onde r é um irracional qualquer. Então não podemos decidir se um membro da família é um inteiro ou um irracional.

Aplicando esta mesma idéia, para cada $m\in\mathrm{N}$ seja $\Delta(m)$ o seguinte sistema de equações diferenciais definido sobre $\mathrm{R}\times\mathrm{R}$:

$$\dot{x}=\mu_m x-y,$$
$$\dot{y}=x+\mu_m y,$$

com $\mu_m=_{\text{def}}\theta(m)-1/2$, cujas soluções são da forma

$$\begin{pmatrix}x(t)\\ y(t)\end{pmatrix}=e^{\mu_m t}\begin{pmatrix}\cos t & -\mathrm{sen} t\\ \mathrm{sen} t & \cos t\end{pmatrix}\begin{pmatrix}x_0\\ y_0\end{pmatrix}$$

É imediato que para qualquer m a origem de R^2 é um ponto fixo de $\Delta(m)$ e, pela forma das soluções, se $\theta(m)=0$ então a origem é assintoticamente estável. Por outro lado, como θ só assume os valores 1 ou 0, a origem é assintoticamente estável se, e somente se, $\theta(m)=0$. Se

$$E=_{\text{def}}\{m\in\mathrm{N}: 0 \text{ é um ponto assintoticamente estável de } \Delta(m)\}$$

então E *não é recursivo*. De uma forma um pouco mais geral, mas igualmente trivial, para qualquer $n\in\mathrm{N}$, podemos construir uma família $\Delta(m)$ sobre R^n tal que a origem de R^n é um ponto singular de $\Delta(m)$ e o conjunto E associado a família $\Delta(m)$ não é recursivo: para $n = 1$, basta considerar o sistema $\dot{x} = (\theta(m) - 1/2)x$ cujas soluções são da forma $x(t) = e^{(\theta(m)-1/2)t}x_0$. Para $n \geq 2$, basta definir $\Delta(m)$ por

$$\begin{aligned} \dot{x}_1 &= \mu_m x_1, \\ \dot{x}_i &= -x_i, \qquad 2 \leq i \leq n. \end{aligned}$$

onde $\mu_m = \theta(m) - 1/2$

Um elemento arbitrário da família $\Delta(m)$ definida em ambos os exemplos possui uma expressão bastante complicada envolvendo polinômios, integrais impróprias, etc.. Não é trivial, e inclusive algoritmicamente indecidível, saber quando $\theta(m) = 0$ ou $\theta(m) = 1$. Mas, uma vez determinado, de alguma forma, o valor de $\theta(m)$, o tipo de estabilidade da origem também é imediatamente determinado, pois os sistemas considerados são extremamente simples. O ponto crucial, usando as palavras de da Costa e Doria, é que nós não somos capazes de dizer a partir da expressão de $\Delta(m)$ em qual caso estamos.

No caso do problema de Arnold, no caso onde os campos vetoriais são dados por polinômios com coeficientes inteiros, a situação não é trivial como nos casos acima, pois a estabilidade é determinada em geral pelos coeficientes do polinômio que define o campo vetorial. Como os coeficientes são *números inteiros dados*, não podemos aplicar o mesmo argumento acima, que se utilizaria da indecidibilidade algorítmica do valor de algum dos coeficientes. Em outras palavras, não nos parece possível reunir estabilidade e instabilidade de um ponto num mesmo sistema $\Delta(m)$, como é feito nestes exemplos, com a condição adicional de que $\Delta(m)$ seja polinomial, pois a função $\theta(m)$ não-recursiva que distinguiria estes dois casos não é polinomial.

Os sistemas definidos pelos teoremas acima não são polinomiais da mesma forma que a função

$$f(m,n) = \begin{cases} 1 & \text{se } TM_m(n) \downarrow \\ 0 & \text{se } TM_m(n) \uparrow \end{cases}$$

não é recursiva, embora para cada m_0, n_0 dados, $f(m_0, n_0)$ seja constante e portanto recursiva.

Talvez tenha sido Kreisel em [**Kr2**] o primeiro a observar que os trabalhos de Scarpellini e Richardson poderiam ser aplicados a problemas de estabilidade em equações diferenciais, embora existam, neste mesmo trabalho, algumas observações com relação a problema de Arnold, não há nenhuma referência explícita em utilizar os métodos de Richardson para atacar esse problema.

Por outro lado parece claro a partir dos exemplos acima que podemos extrair um resultado geral de incompletude e indecidibilidade. Levando em conta uma observação de Suppes neste sentido, em [**dCD 5, 6, 7**] da Costa e Doria conseguiram obter uma solução negativa do problema de Arnold além de outros resultados sobre indecidibilidade e incompletude que, apesar da simplicidade da técnica geral das demonstrações, possuem importantes consequências e serão usados como referências nos capítulos II e III. Basicamente o material exposto aqui é uma coleção de parte de [**dCD5**] e [**dCD7**].

Definição. Seja L_T a linguagem formal de alguma teoria T. um predicado $P(x)$ de L_T é **não trivial** se existem termos ξ e ζ de L_T tal que $T \vdash P(\xi)$ e $T \vdash \neg P(\zeta)$. Um predicado de T é **decidível** se o conjunto

$$\{n \in \mathbb{N} : \text{ existe um termo fechado } v \text{ de } T \text{ com } \{v\} = n \text{ e } t \vdash T(v)\}$$

é recursivo ($\{v\}$ denota o número de Gödel de v).

Proposição 1.15. Seja T uma teoria aritmeticamente consistente e $L_{\mathrm{PA}^2} \subset L_T$. Se $P \in L_{\mathrm{PA}^2}$ é um predicado não trivial, então existe um termo $\varsigma \in L_{\mathrm{PA}^2}$ que, se N é o modelo standard dos naturais, $N \models P(\varsigma)$ enquanto que $T \not\vdash P(\varsigma)$ e $T \not\vdash \neg P(\varsigma)$.

Em outras palavras, qualquer propriedade não trivial expressável na linguagem de T é indecidível.

Demonstração. Basta definir $\varsigma =_{\text{def}} \sigma(p)\xi + (1 - \sigma(p))\zeta$, onde $\vdash P(\xi)$, $\vdash \neg P(\zeta)$ e p é o polinômio definido pela proposição (1.8) . Assim, se $p > 0$, $N \models \forall \vec{x} p(\vec{x}) > 0$ e portanto $N \models P(\varsigma)$. Mas se $T \vdash P(\varsigma)$, como $T \vdash P(\xi)$ temos $T \vdash \forall \vec{x} p(\vec{x}) > 0$, uma contradição. Se $T \vdash \neg P(\varsigma)$, então $T \vdash P(\zeta)$ i.e., $T \vdash \exists \vec{x} p(\vec{x}) = 0$, novamente uma contradição. □

Uma consequência imediata da proposição (1.15) é a ***indecidibilidade*** de qualquer propriedade P não trivial expressável na linguagem de T, pois neste caso, existe um termo ς que satisfaz P, mas $T \not\vdash P(\varsigma)$ e $T \not\vdash \neg P(\varsigma)$. No caso do problema de Arnold para campos vetoriais polinomiais, este resultado não se aplica, pois o termo ς foi construído em termos de θ, que não é polinomial. Este obstáculo pode ser superado, conforme [**dCD 4, 6, 7**], da seguinte maneira.

A idéia básica de da Costa e Doria é construir uma família $\Delta(m)$ enumerável de equações diferenciais polinomiais parametrizadas por μ_m, i.e.,

$$\dot{x} = f_{\mu_m}(x)$$

$m \in \mathbb{N}$, definidas sobre um $\mathbb{R}^k$ adequado, que satisfaça as seguintes propriedades:

(1) Para todo m, a origem é um ponto de equilíbrio de $\Delta(m)$.

(2) Se $\mu_m < 0$ a origem é um ponto fixo estável enquanto que para $\mu_m > 0$ ela é instável.

(3) O conjunto $\{m \in \mathbb{N} | \ \mu_m > 0\}$ não é recursivo.

Esta construção está reapresentada aqui de tal forma que os pontos considerados obscuros – para nós –, estão isolados.

Vamos considerar então, a seguinte família de sistemas de equações diferenciais parametrizadas por $\mu \in \mathbb{R}$:

$$\begin{aligned} \dot{x} &= -y + x(\mu - (x^2 + y^2)) \\ \dot{y} &= x + y(\mu - (x^2 + y^2)) \end{aligned} \tag{1.21}$$

Obviamente, para qualquer μ, a origem é um ponto fixo de (1.21) e além disso o sistema (1.21) satisfaz a condição (2) acima (cf. [**HK**])

Seja $p_{univ}(y, x_1, \ldots, x_v)$ o polinômio universal (que é definido sobre $\mathbb{N}$ com coeficientes em $\mathbb{Z}$). Pelo teorema de Lagrange, para qualquer natural a existem inteiros a_1, a_2 , a_3 e a_4 tal que $a = 1 + \sum_{i=1}^{4}(a_i)^2$. Seja então p o seguinte polinômio,

$$\begin{aligned} &p(x_{1,1}, \ldots, x_{1,4}, \ldots, x_{i,1}, x_{i,2}, x_{i,3}, x_{i,4}, \ldots, x_{v,4}, y) =_{\text{def}} \\ &\qquad = p_{univ}(y, 1 + \sum_{i=1}^{4}(x_{1,i})^2, \ldots, 1 + \sum_{i=1}^{4}(a_{j,i})^2, \ldots, 1 + \sum_{i=1}^{4}(a_{v,i})^2) \end{aligned}$$

Vamos considerar agora a função $\mu_m(x_1, \ldots, x_{4v}, y_1, \ldots, y_{4v})$ definida por

$$\begin{aligned} \mu_m(x_1, \ldots, x_{4v}, y_1, \ldots, y_{4v}) = -\{(n+1)^2(p^2(x_1, ..., x_{4v}, m) + \\ \sum_{i=1}^{4v}(y_i^2)(g_i^2(x_1, ..., x_{4v}, m)) - 1/2\} \end{aligned}$$

onde $g_i = \alpha(\dfrac{\partial}{\partial x_i}p^2)$. Observe que, se $y_i = \operatorname{sen} \pi x_i$, temos, para cada m natural, usando a proposição (1.12),

$$\begin{aligned} (\forall \vec{x} \in \mathbb{R}^{4v})[\mu_m(\vec{x}, \vec{y}) < 0] &\Leftrightarrow ((\forall \vec{x} \in \mathbb{R}^{4v})[\beta p(\vec{x}, m) > 1/2] \\ &\Leftrightarrow ((\forall \vec{x} \in \mathbb{R}^{4v})[\beta p(\vec{x}, m) > 0] \\ &\Leftrightarrow (\forall \vec{x} \in \mathbb{Z}^{4v})[p(\vec{x}, m) \neq 0] \end{aligned} \tag{1.22}$$

Portanto o conjunto $A = \{m \in \mathbb{N} : (\forall \vec{x} \in \mathbb{R}^{4v})[\mu_m(\vec{x}, \vec{y}) < 0]\}$ não é recursivo, pois A não é enumerável recursivamente.

Vamos considerar agora o seguinte sistema, definido em $\mathbb{R}^{16v+1}$,

$$\begin{aligned} \dot{y}_i &= cw_i z_i, \\ \dot{z}_i &= -cw_i z_i \\ \dot{c} &= 0 \\ \dot{x}_i &= w_i \\ \dot{w}_i &= -x_i \end{aligned} \tag{1.23}$$

com $i = 1, \ldots, 4v$. Sobre condições iniciais adequadas, as funções,

$$\begin{aligned}
x_i(t) &= \operatorname{sen} t \\
w_i(t) &= \cos t \\
y_i(t) &= \operatorname{sen} \pi x_i(t) \\
z_i(t) &= \cos \pi x_i(t) \\
c(t) &= \pi
\end{aligned}$$

são soluções de (1.23) e então, conforme da Costa e Doria [**dCD7**, p. 1895], o conjunto

$$B = \{m \in \mathbb{N} : (\forall t \in \mathbb{R})[\mu_m(x_i(t), \ldots, x_{4v}(t), y_1(t), \ldots, y_{4v}(t)) > 0]\}$$

não é recursivo, pois pela primeira tradução de Richardson $m \in B \Leftrightarrow (\forall \vec{x} \in \mathbb{Z}^{(4v)})[p(\vec{x}, m) \neq 0]$. Isto parece ser uma consequência de (1.22), mas como x_i é uma função periódica do tempo t, então $B = \{m \in \mathbb{N} : (\forall t \in \mathbb{R})[\mu_m(\vec{x}(t), \vec{y}(t)) < 0]\}$ pode ser enumerável recursivamente, pois como cada $x_i(t)$ é limitada, temos

$$(\forall t \in \mathbb{R})[\mu_m(\vec{x}(t), y(t)) < 0] \not\Rightarrow (\forall \vec{x} \in \mathbb{R}^{4v})[\mu_m(\vec{x}, \vec{y}) < 0]$$

Como não sabemos como contornar este problema preferimos isolá-lo como uma hipótese:

Hipótese. O conjunto $B = \{m \in \mathbb{N} : (\forall t \in \mathbb{R})[\mu_m(\vec{x}(t), \vec{y}(t)) < 0]\}$ não é recursivo.

Considere agora a seguinte família enumerável definida sobre $\mathbb{R}^{16v+3}$ e $i = 1, \ldots, 4v$:

$$\begin{aligned}
\dot{\xi} &= -\eta + \xi(\mu_m(x_1, \ldots, x_{4v}, y_1, \ldots, y_{4v}) - \xi^2 - \eta^2), \\
\dot{\eta} &= \xi + \eta(\mu_m(x_1, \ldots, x_{4v}, y_1, \ldots, y_{4v}) - \xi^2 - \eta^2), \\
\dot{y}_i &= c w_i z_i, \\
\dot{z}_i &= -c w_i y_i, \\
\dot{c} &= 0 \\
\dot{x}_i &= w_i \\
\dot{w}_i &= -x_i
\end{aligned} \tag{1.24}$$

Então a origem é um ponto estacionário deste sistema, que é polinomial e além disso, dado m,

- *se para todo t, $\mu_m(t) < 0$, então a origem é estável*[5]. Basta notar que a função

[5]Em [**dCD7**], da Costa e Doria apresentam uma demonstração na qual a origem neste caso é assintoticamente estável. Isto não é possível pois as coordenadas x_i, y_i, z_i e w_i que aparecem nas curvas que são soluções de $\Delta(m)$ são todas funções periódicas e portanto não satisfazem a condição de estabilidade assintótica. Mas a demonstração ainda funciona se repassarmos estabilidade assintótica por estabilidade, como fazemos aqui.

$V : \mathbb{R}^{(4v+3)} \to \mathbb{R}$ definida por

$$V(\xi, \eta, y_1, \ldots, y_v, z_1, \ldots, z_v, x_1, \ldots, x_v, w_1, \ldots, w_v, c) = (1/2)[\xi^2 + \eta^2 + c^2 + \\ + \sum_i (y_i^2 + z_i^2 + x_i^2 + w_i^2)]$$

é uma *função de Lyapunov* com $\dot{V} \leq 0$ em $U - 0$, onde U é qualquer vizinhança da origem, pois

$$\dot{V} = (\xi^2 + \eta^2)(\mu_m - \xi^2 - \eta^2)$$

- *se existe t tal que $\mu_m(t) > 0$ então a origem é instável.* Isto é equivalente ao Lema (3.6) de [**dCD7**].

A partir destas observações associadas à hipótese acima, podemos concluir que existem condições iniciais de $\Delta(m)$ tal que o conjunto $\{m \in \mathbb{N} :$ a origem de $\Delta(m)$ é estável$\}$ não é recursivo. Portanto não existe um algoritmo, ou seja, uma máquina de Turing que decida quando a origem de um sistema de equações diferenciais polinomiais é ou não estável.

A solução negativa do problema de Arnold depende da não recursividade de K, i.e., da não recursividade de θ. Em outras palavras, se T é uma teoria aritmeticamente consistente e $L_{PA^2} \subseteq L_T$, então para algum m, $T \nvdash \theta(m) = 0$ e $T \nvdash \theta(m) = 1$.

Mesmo que não possamos demonstrar com T se $\theta(m) = 0$ ou não, pode-se considerar uma extensão T' de T acrescentando os axiomas "$\theta(m_0) = 0$", $\theta(m_1) = 0$", ..., ou seja, θ pode ser visto como um oráculo no sentido usual. Da mesma forma que no caso clássico, o fenômeno de incompletude, e por consequência o de indecidibilidade, é um fenômeno persistente pois podemos definir uma nova função θ' tal que $T' \nvdash \theta'(m) = 0$ e $T' \nvdash \theta'(m) = 1$. Como a linguagem da análise é muito rica, podemos continuar este processo indefinidamente sempre encontrando uma expressão para as novas funções que se comportam como θ em cada nova extensão de T. Este fenômeno de persistência da incompletude e indecidibilidade será retomado no capítulo III.

Definição. O **jump** de um conjunto A, denotado por A' é a relativização de K à A, i.e,

$$x \in A' \Leftrightarrow x \in \mathcal{W}_x^A \Leftrightarrow \varphi_x^A(x)\downarrow$$

Pela definição de T-grau pode-se mostrar que $A \leq_T B$ se, e somente se, $A' \leq_T B'$. Podemos então estender a definição de jump para graus, i.e., se $\boldsymbol{a}$ é um T-grau o *jump* de $\boldsymbol{a}$, denotado por $\boldsymbol{a}'$ é o grau de A'. De uma forma mais geral, o n-**jump** $A^{(n)}$ de A é definido indutivamente por

$$A^{(0)} = A \qquad A^{(n+1)} = (A^{(n)})'$$

e o *n-jump* $\boldsymbol{a}^{(n)}$ de $\boldsymbol{a}$ é o grau de $A^{(n)}$ para qualquer conjunto $A \in \boldsymbol{a}$, i.e.,

$$\boldsymbol{a}^{(0)} = \boldsymbol{a} \qquad \boldsymbol{a}^{(n+1)} = (\boldsymbol{a}^{(n)})'$$

Vamos denotar por $\emptyset^{(n)}$ como sendo o representante para $\mathbf{o}^{(n)}$ (note que $\emptyset \in \mathbf{o}$ e K é o jump de $\emptyset$).

Pela equivalência (1.11) podemos, através da função θ definida pelo teorema (1.14) *obter uma expressão para a função característica $C_{\emptyset^{(n)}}$ em* $\mathtt{PA}^2$ que pode ser definida indutivamente da seguinte maneira: para $n = 0$, $C_{\emptyset^{(0)}}(m) =_{\text{def}} \theta(m, m)$; e para $n > 0$ e algum m_0 adequado,

$$\begin{aligned} & C_{\emptyset^{(n+1)}}(m) = 1 \ \Leftrightarrow \ m \in \mathcal{W}_m^{\emptyset^{(n)}} \\ \Leftrightarrow \ & (\exists y_1, \ldots, y_v \in \mathbb{N})[p_u(J(m, p_0^m p_1^{(c_{\emptyset^{(n)}})(m_0)}), y_1, \ldots, y_v) = 0] \\ \Leftrightarrow \ & \theta(u, J(m, p_0^m p_1^{(c_{\emptyset^{(n)}})(m_0)})) = 1 \end{aligned} \tag{1.27}$$

logo $C_{\emptyset^{(n+1)}}(m) =_{\text{def}} \theta(u, J(m, p_0^m p_1^{(c_{\emptyset^{(n)}})(m_0)}))$

Se T é uma teoria e $L_{\mathtt{PA}^2} \subset L_T$, vamos denotar por $T^{(m+1)}$ a teoria formada pelos axiomas e regras de T mais os axiomas "$n_0 \in \emptyset^{(m)}$", "$n_1 \in \emptyset^{(m)}$", ..., que descrevem o conjunto $\emptyset^{(m)}$.

Lema 1.16. Se $T^{(m+1)}$ é aritmeticamente consistente, então $\varphi_x^{\emptyset^{(m)}}(x)\downarrow$ se, e somente se, para algum m_0,

$$\begin{aligned} T^{(m+1)} \vdash & (\exists y_1, \ldots, y_n \in \mathbb{N}) \\ & [p_{univ}(J(\rho(m), J(m, p_0^m p_1^{(c_{\emptyset^{(m)}})(m_0)})), y_1, \ldots, y_v) = 0] \end{aligned}$$

A demonstração do lema utiliza o mesmo argumento da demonstração do caso não relativizado. Como o complemento do conjunto $\emptyset^{(m+1)}$ não é enumerável recursivamente em $\emptyset^{(m)}$, existe um índice $e(\emptyset^{(m)}) = J(\rho(m), J(m, p_0^m p_1^{(c_{\emptyset^{(m)}})(m_0)}))$ tal que $(\forall \vec{x})[P_{univ}^2(e(\emptyset^{(m)}), \vec{x}) > 0]$ e, utilizando o mesmo argumento da proposição (1.8), este fato não pode ser demonstrado por $T^{(m+1)}$.

Corolário 1.17. Se T é aritmeticamente consistente e $L_{\mathcal{PA}^2} \subset L_T$, então para:

$$\begin{aligned} \beta^{(m+1)} &= \sigma(G(e(\emptyset^{(m)}))), \\ G(e(\emptyset^{(m)})) &= \int_{-\infty}^{\infty} \frac{B(\gamma P_{univ}(x, e(\emptyset^{(m)})))e^{-x^2}}{1 + B(\gamma P_{univ}(x, e(\emptyset^{(m)}))} dx \\ B(\gamma p) &=_{\text{def}} |\gamma p - 1| - \gamma p + 1 \end{aligned}$$

existe um modelo $\mathbf{M}$ tal que $\mathbf{M} \models \beta^{(m+1)} = 0$ mas para todo $n \leq m+1$, $T^{(n)} \not\vdash \beta^{(m+1)} = 0$ e $T^{(n)} \not\vdash \neg(\beta^{(m+1)} = 0)$

Corolário 1.18. Seja T como na proposição (1.17), então existe $\varsigma \in L_T$ e um modelo $\mathbf{M}$ tal que $\mathbf{M} \models P(\varsigma)$, $T^{(n)} \not\vdash P(\varsigma)$ e $T^{(n)} \not\vdash \neg P(\varsigma)$.

Demonstração. Se ξ e ζ são tais que $T^{(n)} \vdash P(\xi)$ e $T^{(n)} \vdash \neg P(\zeta)$ então por um argumento análogo ao da proposição (1.15), basta definir $\varsigma = \xi\sigma(\beta^{(m+1)}) + \zeta\sigma(1 - \beta^{(m+1)})$. □

Diante desses resultados é natural perguntarmos o que acontece se acrescentarmos a T todos os axiomas que caracterizam os conjuntos $\mathcal{K}^{(n)}$. Isto pode ser feito da seguinte maneira.

Definição.

$$\emptyset^{(\omega)} =_{\text{def}} \{\langle x, y\rangle : x \in \emptyset^{(y)}\}$$
$$\emptyset^{(\omega+1)} =_{\text{def}} (\emptyset^{(\omega)})'$$

Consequentemente a função característica de $\emptyset^{(\omega)}$ é dada por

$$C_{\emptyset^{(\omega)}} = C_{\emptyset^{L(m)}}(K(m))$$

e se o T-grau de $\emptyset^{(\omega)}$ é denotado por $\mathbf{0}^{(\omega)}$, então se $\mathbf{0}^{(\omega+1)} = (\mathbf{0}^{(\omega)})'$ então $\mathbf{0}^{(\omega+1)}$ é o grau de $\emptyset^{(\omega+1)}$, pois $A \in \mathbf{0}^{(\omega)}$ se, e somente se, $A' \in \mathbf{0}^{(\omega+1)}$.

Por um argumento similar ao do corolário (1.17), pode-se obter o seguinte:

Proposição 1.19. Se T é aritmeticamente consistente e $L_{\mathcal{PA}^2} \subset L_T$, então para:

$$\beta^{(m+1)} = \sigma(G(e(\emptyset^{(m)}))),$$
$$G(e(\emptyset^{(\omega)})) = \int_{-\infty}^{\infty} \frac{B(\gamma P_{univ}(x, e(\emptyset^{(\omega)})))e^{-x^2}}{1 + B(\gamma P_{univ}(x, e(\emptyset^{(\omega)})))}dx$$
$$B(\gamma p) =_{\text{def}} |\gamma p| - \gamma p + 1$$

existe um modelo $\mathbf{M}$ tal que $\mathbf{M} \models \beta^{(\omega+1)} = 0$ mas $T^{(\omega)} \not\vdash \beta^{(\omega+1)} = 0$ e $T^{(\omega)} \not\vdash \neg(\beta^{(\omega+1)} = 0)$

Se ξ e ζ são sentenças de L_T, então ξ e ζ são **demonstravelmente equivalentes** se $T \vdash \xi \leftrightarrow \zeta$. Se $L_{\mathbf{PA}} \subset L_T$ então a sentença $\xi \in L_T$ é **aritmeticamente expressável em** T se ξ é demostravelmente equivalente em T a alguma sentença de $L_{\mathcal{PA}}$.

Proposição 1.20. (**Incompletude não aritmética**) Seja T como na proposição (1.19). Então dado qualquer propriedade não trivial P em L_T:

(1) Existe uma família de expressões $\varsigma_m \in L_T$ tal que o conjunto $\{m : P(\varsigma_m)\}$ não é recursivo.

(2) Existe uma expressão $\varsigma \in L_T$ e um modelo $\mathbf{M}$ de T tal que $\mathbf{M} \models P(\varsigma)$ enquanto que $T \nvdash P(\varsigma)$ e $T \nvdash \neg P(\varsigma)$.

(3) ς_m e ς não são expressáveis aritmeticamente.

Demonstração. Sejam ξ e ζ termos de L_T tais que $T \vdash P(\xi)$ e $T \vdash \neg P(\zeta)$. Para (1) basta tomar

$$\varsigma_m =_{\text{def}} \xi C_{\emptyset(\omega+1)}(m) + (1 - C_{\emptyset(\omega+1)}(m))\zeta$$

Para o ítem (2) tomamos $\varsigma_m = \xi\sigma(\beta^{(\omega+1)}) + \zeta(\sigma(1 - \beta^{(\omega+1)}))$. Além disso, como já foi observado, nem $\beta^{(\omega+1)}$ nem $C_{\emptyset(\omega+1)}$ são expressáveis aritmeticamente. $\square$

Em vista destes resultados, em [**dCD5**] da Costa e Doria observam que,

> (...) in general nothing interesting can be decided and very little can be proved (...) At the same time we received notice that our results were at first met with disbelief by researchers in dynamical systems precisely due to that very general incompleteness statement; it was then argued that those results were correct but 'strange' due to some undetected conceptual flaw in the current view on the foundations of mathematics.
>
> [...]
>
> Yet our assertions have a very clear, let us say, *pratical* meaning: if what we mean by 'proof' in mathematics is *algoritmic* proof, that is to say, something that can be simulated by a Turing machine, then very difficult problems are to be expected everywhere at the very heart of everyday mathematical activity.
>
> [. . .]
>
> What can we make out of that? We do not think that there is any essencial flaw in the present-day view about foundational concepts; however we think that our incompleteness theorems point out very clearly where the problem lies. Nothing will be gained by adding 'stronger'and 'stronger' axioms to our current axiomatizations. But we certainly must strenghten our current concept of mathematical proof. Turing-computable proofs are not enough, for Church-Turing computation is not enough. We must look beyond.

Vamos preferir interpretar estes resultados como *evidência da inadequação do conceito de algoritmo clássico para questões abstratas de indecidibilidade*, como por exemplo, as questões propostas por Arnold. Discutiremos este ponto de vista nos próximos capítulos.

2. Revendo as Idéias de Arnold

Este capítulo deve ser visto como o gatilho temático deste trabalho. Vamos rever a crítica de Arnold à solução proposta por da Costa e Doria a seu problema e analisar brevemente os motivos que levaram Arnold a formulá-lo.

Tendo em vista estes objetivos, vamos rever num primeiro momento, um resultado do próprio Arnold sobre insolubilidade algébrica do problema da estabilidade para pontos singulares de equações diferenciais. O que realmente importa aqui é a interpretação deste resultado e sua relação com a crítica de Arnold.

Com isso pode-se precisar em que sentido o conceito de algoritmo clássico não é adequado, pois neste caso, já se pressupõe em que termos uma solução deve ser esperada. Isto nos remete a uma observação de Kreisel [**Kr1**]:

> Mathematicians understand problems which leave open in what terms they are to be answered, and recognize their solutions when they see them! for example, Higman's solution, by use of classical recursion theory, of the question: Which finitely generated groups are subgroups of some finitely presented group? Nobody told him just how the word 'which' was to be narrowed down.

Como subproduto desta análise discutiremos brevemente o significado dos resultados de da Costa e Doria sobre indecidibilidade e incompletude frente a uma interpretação "mais realista" do problema de Arnold. Fazendo isto esperamos enfatizar, por contraste o que estamos tentando fazer.

A. Insolubilidade algébrica do problema da estabilidade.

O estudo topológico de pontos singulares de campos vetorias, que inclui estabilidade das órbitas próximas a estes pontos, assim como o estudo de bifurcações de famílias de campos vetorias é em essência o estudo do espaço de funções dividido em várias partes correspondendo aos vários tipos de degenerações (cf. [**Ar3**]). A fim de contornar o problema da dimensionalidade infinita do espaço de funções, foi introduzido um aparato de aproximações finito-dimensionais do espaço de funções chamado de variedades de k-jatos que vamos passar a definir.

Definição. Sejam M e N variedades diferenciáveis e f, $g : M \to N$ funções diferenciáveis. Vamos supor que $f(p) = g(p) = q$ para algum $p \in M$. Então f e g são 1-**tangentes** em p se as diferenciais $(df)_p$ e $(dg)_p$ coincidem enquanto funções ($(df)_p, (dg)_p : T_pM \to T_qM$, onde T_xM denota o espaço tangente de M em x). Dizemos que f e g são k-**tangentes** em p se $(df) : TM \to TN$ é $(k-1)$-tangente a dg em qualquer ponto de T_pM. A relação de k-tangência num ponto p entre duas funções é na verdade uma relação de equivalência e será denotada por $\sim_{k,p}$. Vamos denotar por $J^k(M,N)_{p,q}$ o conjunto das classes de equivalência sobre $\sim_{k,p}$ das funções $f : M \to N$, onde $f(p) = q$. O **espaço de k-jatos de M em N** é definido[6] por

$$J^k(M,N) =_{\text{def}} \cup_{(p,q)\in M\times N} J^k(M,N)_{p,q}$$

Dado uma função diferenciável $f : M \to N$ o k-**jato** de f, denotado por j^kf, é uma função definida de M em $J^k(M,N)$ da seguinte maneira:

$$j^kf(p) =_{\text{def}} \text{ a classe de equivalência de } f \text{ em } J^k(M,N)_{p,f(p)}$$

Seja $\alpha = (\alpha_1, \ldots, \alpha_n)$ uma n-upla de inteiros não negativos. Então

$$\frac{\partial^{|\alpha|}}{\partial x^\alpha} =_{\text{def}} \frac{\partial^{|\alpha|}}{\partial x_1^{\alpha_1}\partial x_2^{\alpha_2}\cdots\partial x_n^{\alpha_n}} f \qquad \text{onde} \qquad |\alpha| = \alpha_1 + \cdots \alpha_n$$

Proposição 2.1. Seja U um aberto de $\mathbb{R}^n$, p um ponto em U e $f, g : U \to \mathbb{R}^m$ funções diferenciáveis. Então,

$$f \sim_{p,q} g \;\Leftrightarrow\; \frac{\partial^{|\alpha|} f_i}{\partial x^\alpha}(p) = \frac{\partial^{|\alpha|} g_i}{\partial x^\alpha}(p)$$

para qualquer α com $|\alpha| \leq k$ e $1 \leq i \leq m$ onde f_i e g_i são as funções coordenadas determinadas por f e g respectivamente e x_i são coordenadas sobre U.

A prova desta proposição pode ser encontrada em [**GG**]. Como corolário deste resultado temos que $f \sim_{k,p} g$ se, e somente se, as expansões de Taylor de f e g em p até ordem k coincidem. Na verdade $j^kf(p)$ é apenas uma forma invariante de descrever a expansão de Taylor de f em p até ordem k. No caso em que M e N são os espaços $\mathbb{R}^n$ e $\mathbb{R}^m$, respectivamente, podemos identificar $j^kf(p)$ com a matriz dos coeficientes da expansão de Taylor de f em torno de p. Assim $j^kf(p)$ é o conjunto de todas as funções cujas expansões de Taylor em torno de p coincidem até a ordem k. Se $g \in j^kf(p)$ dizemos que g é um **representante** de $j^kf(p)$.

[6] É possível mostrar que $J^k(M,N)$ possui uma estrutura natural de variedade diferenciável (cf. [**GG**]).

Definição. Seja $f : \mathbb{R}^n \to \mathbb{R}^m$ uma função diferenciável e p um ponto singular de f, i.e., $f(p) = 0$. Um jato $j^k f(p)$ é **positivo** em relação à estabilidade de Lyapunov se todos os seus representantes são estáveis, no sentido de Lyapunov, em p. Dizemos que $j^k f(p)$ é **negativo** se todos os seus representantes são instáveis em p, e $j^k f(p)$ é **neutro** com relação à estabilidade de Lyapunov se $j^k f(p)$ não é positivo nem negativo.

Exemplo. Se $f : \mathbb{R}^n \to \mathbb{R}^n$ é uma função diferenciável, p um ponto singular de f e $Df(p)$ é a matrix do Jacobiano de f em p, então é possível mostrar que, se todos os autovalores de $Df(p)$ têm parte real negativa, p é um ponto de equilíbrio assintoticamente estável da equação diferencial $\dot{x} = f(x)$ (cf. [**HK**]). Por outro lado se pelo menos um autovalor tem parte real estritamente positiva, então p é um ponto de equilíbrio instável. Assim, dado um ponto p e qualquer função diferenciável $f : \mathbb{R}^n \to \mathbb{R}^n$ singular em p, é possível caracterizar, através de um número finito de igualdades e desigualdades envolvendo as derivadas parciais de f em p, os conjuntos de 1-jatos positivos, negativos e neutros com relação à estabilidade de Lyapunov.

Definição. Seja $p \in \mathbb{R}^n$ e $\mathcal{V}$ a classe dos campos vetoriais para os quais p é um ponto singular. O problema de determinar para quais campos vetoriais de $\mathcal{V}$, p é um ponto de equilíbrio estável ou instável é **algebricamente solúvel** se as seguintes condições são satisfeitas:

(1) **Semialgebricidade:** Os conjuntos de N-jatos positivo, negativo e neutro em relação à estabilidade de Lyapunov são subconjuntos de $J^N(\mathbb{R}^n, \mathbb{R}^n)$ semialgébricos para cada N,

(2) **Quase determinação finita**: A codimensão da subvariedade dos N-jatos neutros na variedade $J^N(\mathbb{R}^n, \mathbb{R}^n)$ tende a ∞ quando $N \to \infty$.

Isto significa que o conjunto das funções para as quais não é possível mostrar, a partir de qualquer número de termos na série de Taylor, se uma dada função deste conjunto satisfaz ou não uma certa propriedade A, que neste caso é a propriedade da estabilidade de Lyapunov é muito "magro", i.e., ele tem codimensão infinita no espaço de funções.

R. Thom mostrou que o problema da classificação topológica de campos de vetores é algebricamente solúvel (cf. [**Ar3**]), mas no caso do problema da estabilidade, Arnold mostrou o seguinte resultado, que implica que o problema da estabilidade de Lyapunov é algebricamente insolúvel:

Teorema 2.2. (**Arnold**, [**Ar1**]) Existe uma família de jatos de codimensão 100 no no espaço $J^5(\mathbb{R}^3, \mathbb{R}^3)$ cuja intersecção com o conjunto de jatos neutro não é um conjunto semialgébrico.

Em vista desta impossibilidade,

> There remains some hope for the existence of a nonalgebraic algorithm, nevertheless, i.e., that the property of almost finite determinacy holds[7]: the set of germs whose topological type (or stability) is not determined by any finite segment of the Taylor series may have infinite codimension.[**Ar3**]

B. Discussão.

A partir destas observações podemos inferir que,

(a) é bastante claro que o problema de Arnold como formulado originalmente em [**Ar2**], foi colocado em função da não existência de critérios algébricos:

> *Is the stability problem for stationary points algorithmically decidable?* The well-known Lyapounov Theorem solves tha problem in the absence of eigenvalues with zero real parts. In more complicated cases, where the stability depends on higher order terms in the Taylor series, there exists no *algebraic* criterion.

(b) O ponto central é que, fazendo isso, Arnold *coloca em evidência o caráter algorítmico dos critérios de classificação* , como é confirmado pelo seguinte comentário em [**Ar3**] (já citado):

> There remains some hope for the existence of a nonalgebraic algorithm, nevertheless, i.e., that the property of almost finite determinacy holds (...)

O ponto crucial é que a simples existência das condições $(p(x) = 0) \bigvee_i (p_i(x) > 0)$ que caracterizam os coinjunto de jatos positivos, negativos e neutros, juntamente com a condição de quase-determinação finita, seria uma solução do problema, não importando se alguma destas desigualdades é decidível ou não.

É claro que o algoritmo algébrico em questão não é equivalente a Turing-computabilidade, pois considerando o sistema $\Delta(m)$ definido no capítulo I, usado para mostrar que o problema de Arnold é indecidível, as próprias condições sobre μ_m determinam se a origem é estável ou não. Temos então, neste caso, um critério algébrico.

Mas como vimos, o problema de Arnold tem uma solução negativa. Para isto foi necessário precisar o sentido de "ser decidível algoritmicamente". Em vista da solução de da Costa e Doria, Arnold observa que (cf. [**Ar4**]),

[7] Como um resultado relacionado ao princípio de quase determinação finita podemos citar [**To**]

Integers were introduced in the formulation only to avoid the difficulty of explaining the way the data are written on the machine's tape.The more realistic formulation of the problem would require the definition of an analytic algorithm working with real numbers and functions (defined as symbols). The algorithm should permit arithmetical operations, modulus, differentiation, integration, solution of nondifferential equations (also for implicit functions in situations where conditions for the implicit function theorem are violated), exponentiation, logarithms, evaluation of "computable" functions for "computable" arguments.

The conjecture is that with all those tools one is still unable:

1- To solve the general stability problem starting from the right hand side functions as symbols with which one may perform the preceding operations.

2- To solve the above problem for polynomial vectorfields with real or complex coefficients.

3- To solve them with integer coefficients.

However as far as I know there are no words in logic to describe the above problem and I have thus preferred to stop at the level of algorithms in the usual sense (...)

Assim, admitindo a hipótese do conteúdo algorítmico dos critérios de classificação, a formulação do problema em termos de algoritmos clássicos seria uma *primeira aproximação* a uma solução, mas *inadequada* se interpretarmos o problema original em função da não existência de critérios algébricos, que corresponde a formulação "mais realista".

É evidente neste ponto o contraste entre a forma de tratamento esperada ao problema de Arnold, expressa pela possibilidade de que o critério de quase determinação finita seja satisfeito, e os resultados de da Costa e Doria expostos no capítulo anterior.

Como já foi observado no capítulo I, podemos interpretar os resultados de da Costa e Doria sobre indecidibilidade e incompletude geral (corolários (1.17), (1.18) e proposições (1.19) e (1.20)), como uma evidência da inadequação do

conceito de algoritmo clássico para tratar problemas do tipo acima. Pois através da identificação de algoritmos e provas, incompletude e indecidibilidade se confundem, e o que importa aparentemente neste caso é a existência ou não de algoritmos ideais que não levam em consideração se as operações envolvidas nestes critérios são decidíveis ou não.

Podemos extrair dessas considerações as seguintes problemas (já citados na introdução):

Problema 1. Existe um "conteúdo algorítmico" permeando os critérios de classificação de pontos singulares. Como formalizar a noção de algoritmo por traz desses critérios?

Problema 2. Qual o sentido de "computável" induzido por estes novos conceitos?

Na verdade estas questões são casos particulares de uma questão muito mais geral considerada por Kreisel em [**Kr1**]:

> *Is there such a thing as a general concept of computation? or the related question:*
>
> *Is there such a thing as an extension of Church's Thesis to general (abstract) strutures?*

Se a resposta para estas questões forem negativas, talvez seja matematicamente proveitoso ver os procedimentos algorítmicos implícitos por exemplo na estrutura da teoria de classificação de singularidades, ou no caso do problema de Arnold, como computáveis. Isto também é explicitado por Kreisel:

> (i) if the answer is positive, we have to do with the analysis of a concept, apecifically a phenomenological analysis of the kind given by Turing for mechanical computations of number theoretic functions. The mathematics has here much the same role as in the natural sciences: to state rival hypotheses and to help one to deduce from them a consequence, an experimentum crucis which distinguishes between them; one will try to avoid artefacts and systematic error. Equivalence results do not play a special role, simply because one good reason is better than 20 bad ones, which may be all equivalent because of systematic error.
>
> (ii) If the aswer is negative, (...) it may still possible to use some idea of 'general computation' in a metaphorical way for applications (which do not in turn refer to the metaphor). What one has to guard against is to imitate mechanically the basic development of classical recursion theory. specifically, at least many of the basic theorems were used in connection with Turing's (genuine) analysis, not for their pure mathematical interest. It would be quite unreasonable to suppose that generalizations of these same theorems will be useful for applications of generalized recursion theory.

Esta posição de Kreisel já adverte contra a inutilidade de uma generalização apenas formal da teoria da recursão, que não traria realmente nenhum novo aparte a um conceito genuinamente novo de computação generalizada. Mas como veremos, apesar de o conceito de computabilidade sobre estruturas abstratas não trazer de fato nada novo, do ponto de vista conceitual, ao conceito de computação, ele pode ser útil do ponto de vista matemático e ganhar um novo *status* conceitual.

3. Novos Rumos para a Computabilidade

Neste capítulo serão discutidos, sem nenhuma pretensão de completude, algumas das idéias de dois dos principais trabalhos clássicos em teoria de recursão sobre estruturas abstratas, que são [**Mos 1, 2**] e [**Fr1**], além do trabalho de Blum, Shub e Smale [**BSS**] que tem por mérito fornecer exemplos de aplicação desta teoria sobre algums estruturas particulares como por exemplo, anéis e em particular o corpo dos reais.

Acreditamos que os resultados deste capítulo, juntamente com o material exposto nos capítulos precedentes, suportam as seguintes teses (já colocadas na introdução):

T1 A teoria da computabilidade sobre os reais, no sentido de [**BSS**], constitui uma primeira aproximação à noção de algoritmo analítico proposta informalmente por Arnold (*apud* [**dCD6**]).

T2 Embora o conceito formal de computabilidade sobre estruturas abstratas não acrescente nada genuinamente novo ao conceito de computação, ele pode ser útil do ponto de vista matemático.

A tese **T2** deve ser vista com cuidado: não se pode falar *no conceito de computabililidade sobre estruturas abstratas*, pois dada uma estrutura A, é possível definir várias classes distintas de "funções computáveis sobre A" dependendo das capacidades dos processos algorítmicos escolhidos que definem estas classes . Sendo assim, a relação de inclusão entre estas classes depende da estrutura em questão.

Por outro lado o conceito de **esquema de definição efetivo**, denotado por EDE, introduzido por Friedman em [**Fr1**], parece ser tão geral que captura qualquer outra noção de computação gerada por um algoritmo. Isto se deve ao fato de que um EDE captura a "topologia" de qualquer algoritmo, i.e., um EDE descreve todos os caminhos possíveis de sequências de instruções de um algoritmo. Assim em **T2**, o conceito formal de computabilidade sobre estruturas abstratas deve ser entendido como o conceito de EDE.

A essência das diversas noções de computabilidade sobre estruturas abstratas é declarar como computável as funções geradas por *algoritmos abstratos*[8]. Com isso,

[8]Em [**Mos 4, 5, 6**] Moschovakis desenvolve uma teoria de algoritmos, chamada de teoria da recursão abstrata que vai de encontro a nossa análise. Esperamos num futuro trabalho, incorporar estes resultados aos nossos propósitos.

não é levado em conta os possíveis conteúdos computacionais das operações de cada estrutura particular – onde, eventualmente, pode estar embutido algo novo do ponto de vista conceitual, como veremos. O teorema (3.2) mostra que um EDE é equivalente a uma **máquina de Turing generalizada**, e assim o conteúdo computacional de um EDE, i.e., o processo de computação envolvido, é análogo ao de uma máquina de Turing usual. Apesar disso, a generalidade de um EDE, e portanto a permissividade do conceito de função EDE-computável – que anula qualquer extensão do conceito de computação que possa estar embutido nas funções iniciais – pode adquirir um novo *status* conceitual:

- esta permissividade adquire uma certa funcionalidade em alguns processos matemáticos que aparentemente envolvem aspectos algorítmicos,
- sendo assim, a teoria abstrata da computação pode servir de critério para expressar tais processos.

É neste sentido que a tese **T2** deve ser entendida.

Cabe ainda enfatizar aqui que vamos nos concentrar muito mais nas idéias do que nas demonstrações.

A. Computabilidade sobre estruturas abstratas.

Seja A um conjunto qualquer, $A^0 = A \cup \{0\}$ e A^* o fecho de A^0 sobre a operação

$$(x, y) =_{\text{def}} \{\{x, y\}, y\}$$

Desta forma, os números naturais $0, 1, 2, \ldots$ são identificados respectivamente com $0, (0, 0), ((0, 0), 0), \ldots$, e assim $\mathtt{N} \subset A^*$.

A sequência $\langle x_1, \ldots, x_n \rangle$ de elementos de A^* é identificada com o elemento $(n, (x_1, \ldots, (x_n, 0) \ldots))$ de A^*. Se $x = \langle x_1, \ldots, x_n \rangle$ então $lh(x) =_{\text{def}} n$ e $(x)_i =_{\text{def}} x_i$. Além disso, para $s, t \in A^*$, $\pi(s, t) = s$ e $\delta(s, t) = t$; para $x \in A$, $\pi x = \delta x = (0, 0)$ e $\pi 0 = \delta 0 = 0$.

Definição. O conjunto PRI^0 é definido indutivamente por:

(1) Para todo $z \in A^*$ e todo $n \in \mathtt{N}$, $\langle 1, n, z \rangle \in PRI$.

(2) Para todo n e i tal que $1 \leq i \leq l$, $\langle 0, n_i + n, i \rangle$, $\langle 2, n + 1 \rangle$, $\langle 3, n + 2i \rangle$, $\langle 4, n + 1, 0 \rangle$ e $\langle 4, n + 1, 1 \rangle$ estão em PRI.

(3) Se g e h estão em PRI, $(g)_2 = n + 1$ e $(h)_2 = n$, então $\langle 5, n, g, h \rangle \in PRI$.

(4) Se g e h estão em PRI, $(g)_2 = n + 1$ e $(h)_2 = n + 4$, então $\langle 6, n + 1, g, h \rangle \in PRI$.

Seja $\boldsymbol{\varphi} = \varphi_1, \ldots, \varphi_k$ uma lista de funções $\varphi : A^* \to \mathcal{P}(A^*)$ que pode inclusive ser vazia.

Definição. Dado A, $\boldsymbol{\varphi}= \varphi_1, \dots, \varphi_l$ onde cada φ_i é uma função n_i-ária, e $n \in \mathbb{N}$, então o predicado '$\{f\}\mathrm{pr}(\boldsymbol{u}) = z$ é definido indutivamente sobre A, $\boldsymbol{\varphi}$ e n da seguinte maneira.

(C0$_i$) ($i = 1, \dots, l$). Se $f = \langle 0, n_i + n, i \rangle$ para algum $n_i \in \mathbb{N}$ e, se $\{\boldsymbol{t}_i, \boldsymbol{x}\} \subset A^*$ e $\varphi_i(\boldsymbol{t}_i) = z$ então $\{f\}\mathrm{pr}(\boldsymbol{t}_i, \boldsymbol{x}) = z$. ($\boldsymbol{x} = x_1, \dots, x_n$).

(C1) Se $f = \langle 1, n, y \rangle$ e $\boldsymbol{x} \in A^*$, então $\{f\}\mathrm{pr}(\boldsymbol{x}) = z$.

(C2) Se $f = \langle 2, n+1 \rangle$ e $\{\boldsymbol{x}, z\} \subset A^*$, então $\{f\}\mathrm{pr}(z, \boldsymbol{x}) = z$.

(C3) Se $f = \langle 3, n+2 \rangle$ e $\{s, t, \boldsymbol{x}, (s,t)\} \subset A^*$, então $\{f\}\mathrm{pr}(s, t, \boldsymbol{x}) = (s, t)$.

(C4$_0$) Se $f = \langle 4, n+1, 0 \rangle$ e $\{y, \pi y, \boldsymbol{x}\} \subset A^*$, então $\{f\}\mathrm{pr}(y, \boldsymbol{x}) = \pi y$.

(C4$_1$) Se $f = \langle 4, n+1, 1 \rangle$ e $\{y, \delta y, \boldsymbol{x}\} \subset A^*$, então $\{f\}\mathrm{pr}(y, \boldsymbol{x}) = \delta y$.

(C5) Se $f = \langle 5, n, g, h \rangle$, $\{g\}\mathrm{pr}(y, \boldsymbol{x}) = z$ e $\{h\}\mathrm{pr}(\boldsymbol{x}) = y$, então $\{f\}\mathrm{pr}(\boldsymbol{x}) = z$.

(C6) Se $f = \langle 6, n+1, g, h \rangle$ e,

(a) $h \in PRI$, $(h)_2 = n + 4$, $y \in A^0$ e $\{g\}\mathrm{pr}(y, \boldsymbol{x}) = z$, então $\{f\}\mathrm{pr}(y, \boldsymbol{x}) = z$.

(b) $y = (s, t)$, $\{f\}\mathrm{pr}(s, \boldsymbol{x}) = u$, $\{f\}\mathrm{pr}(t, \boldsymbol{x}) = v$ e $\{h\}\mathrm{pr}(u, v, s, t, \boldsymbol{x}) = z$, então $\{f\}\mathrm{pr}(y, \boldsymbol{x}) = z$.

(C7) Se $f = \langle 7, n, j, g \rangle$, $j < n$ e

$$\{g\}\mathrm{pr}(x_{j+1}, x_1, \dots, x_j, x_{j+2}, \dots, x_n) = z$$

então $\{f\}\mathrm{pr}(\boldsymbol{x}) = z$.

Esta definição é análoga aos esquemas de Kleene [**Kl1**] para funções recursivas primitivas, acrescentando $\boldsymbol{\varphi}$ como funções iniciais.

Definição. Uma função $\psi : A^* \to \mathcal{P}(A^*)$ é **computável primitiva em $\boldsymbol{\varphi}$ sobre** A^* se existe $f \in PRI$ tal que para todo $\boldsymbol{u} \in A^*$,

$$\{f\}\mathrm{pr}(\boldsymbol{u}) = \psi(\boldsymbol{u})$$

Em outros termos, cada $f \in PRI$ define um funcional $\{f\}\mathrm{pr}(\varphi_1, \dots, \varphi_k, \boldsymbol{u})$ sobre A^*.

Se $A = \emptyset$ na definição acima, então dizemos que ψ é *absolutamente computável primitiva em* $\boldsymbol{\varphi}$.

É possível mostrar (cf. [**Mos1**]) que se $\boldsymbol{\varphi}$ é vazia e $f(\boldsymbol{u})$ é computável primitiva sobre $\boldsymbol{\varphi}$ e leva $\mathbb{N}$ em $\mathbb{N}$, então a restrição de f a $\mathbb{N}$ é recursiva primitiva no sentido usual.

Seguindo Kleene [**Kl1**], o propósito de uma definição indutiva usando índices, como a definição do predicado $\{f\}_{\mathrm{pr}}(\boldsymbol{u}) = z$, é dar um sentido computacional a $\{f\}(\boldsymbol{u})$. Da mesma forma que no caso clássico, se $\{f\} \in PRI$, então a própria definição de $\{f\}(\boldsymbol{u})$ fornece um procedimento para computar $\{f\}$ 'módulo' as funções iniciais de $\boldsymbol{\varphi}$, que podem inclusive não ser classicamente computáveis. O que importa é que é razoável postular, como faz Kleene no caso clássico, que a função que enumera a classe das funções computáveis primitivas sobre $\boldsymbol{\varphi}$ também é computável neste sentido. O mesmo procedimento, quando aplicado neste caso mais geral, conduz à classe das funções *prime*-computáveis sobre A^* definida por Moschovakis em [**Mos1**].

Mais precisamente, se $f : A^* \to \mathcal{P}(A^*)$ e $f(x) \to z \Leftrightarrow_{\mathrm{def}} z \in f(x)$, então, uma função $\psi : A^* \to \mathcal{P}(A^*)$ é **prime-computável em $\boldsymbol{\varphi}$ sobre** A^* se existe $f \in PRI_p$ tal que para todo $\boldsymbol{u} \in A^*$,

$$\{f\}_{\mathrm{pr}}(\boldsymbol{u}) \to z \Leftrightarrow \psi(\boldsymbol{u}) \to z$$

onde PRI_p é definido indutivamente pelas mesmas cláusulas de PRI acrescentando a cláusula

$$\langle 8, n+m+1, n\rangle \in PRI_p \text{ para todo } m, n$$

O predicado $\{f\}_{\mathrm{pr}}(\boldsymbol{u}) \to z$ é definido indutivamente pelas mesmas cláusulas que definem o predicado $\{f\}_{\mathrm{pr}}(\boldsymbol{u}) = z$ com as seguintes modificações: $=$ é repassado por $\to$ e a cláusula (C8) é acrescentada, onde

(C8) Se $f = \langle 8, n+m+1, n\rangle$, $e \in PRI_p$ e $\{\boldsymbol{x}, \boldsymbol{y}\} \subset A^*$ então $\{f\}_{\mathrm{pr}}(e, \boldsymbol{x}, \boldsymbol{y}) = \{e\}(\boldsymbol{x})$

Um resultado de [**Mos1**] mostra que se $g(i, \boldsymbol{x})$ é *prime*-computável, definida e $g(i, \boldsymbol{x}) : A^* \to A^*$, então a função $f(\boldsymbol{x}) = \mu_{i \in \mathbb{N}}[g(i, \boldsymbol{x}) = 0]$ também é *prime*-computável. Mas sobre um conjunto arbitrário A não existe em geral uma boa ordem natural sobre a qual podemos realizar uma operação de busca, como é necessário para a definição do operador μ. Pode-se porém definir um **operador de busca não ordenado** v de forma análoga ao operador μ:

$$vy[g(y, \boldsymbol{x}) \to 0] \to z \Leftrightarrow_{\mathrm{def}} g(z, \boldsymbol{x}) \to 0$$

Note que $vy[g(y, \boldsymbol{x}) \to 0]$ pode tomar valores em $P(A^*)$.

Este operador pode ser entendido da seguinte forma: a busca é realizada por um oráculo que, embora não possa percorrer todos os elementos de A^* num tempo finito, pode procurar através de partes arbitrariamente grandes de A^*, ou melhor, este oráculo realiza uma busca sobre uma boa-ordem em A^* que sempre existe (pelo axioma da escolha), e o oráculo sabe qual é, embora "esta boa-ordem pode não ser definível em termos de quaisquer conceitos que um 'computador humano' entenderá" (cf. [**Mos1**]).

A classe de funções **search-computáveis** é obtida a partir da classe de funções *prime*-computáveis como sendo o fecho desta classe com a operação de busca não ordenada. Como observa Moschovakis [**Mos1**],

> It appears to us that Church's thesis cannot be stated for abstract domains with the precision with which it is stated for the natural numbers. By this we mean that in the absence of more specific information about A and φ, one cannot define a class of functions on A^* which is so intrinsic that one can assert without reservation that it is the class of all functions on A^* intuitively computable from φ. Instead we would suggest that the classes of prime computable and search computable functions form natural bounds for effective computability. We state this precisely as our (weak) abstract version of Church's thesis, for single-valued absolutely computable functions; people who believe in the computability of arbitrary constants on an arbitrary set would wish to omit the word "absolutely", but we have our reservations on this.
>
> *Let C, E be subsets of A^*. every single-valued, totally defined function on C to E which is the restriction to C of an absolutely prime computable function is intuitively effectively computable (from φ). Every single-valued totally defined function on C to E which is intuitively effectively computable (from φ) is the restriction to C of an absolutely search computable function.*

Isto sugere que o conteúdo computacional embutido na definição de função *prime*-computável pode ser capturado pela noção formal de recursão, assumindo a Tese de Church. Em outras palavras, a noção de *prime*-computabilidade sobre estruturas abstratas não acrescenta nada genuinamente novo ao conceito de computação usual, pois o processo computacional envolvido não leva em conta se as funções iniciais são ou não computáveis em algum sentido, mas simplesmente assume como computáveis todas as funções iniciais, que passam a desempenhar um papel análogo ao de oráculos, como na teoria clássica. De fato parece ser possível mostrar, como veremos, que uma função *prime*-computável em φ sobre um conjunto A^* é computável por uma *máquina de Turing generalizada* sobre a estrutura (A,φ). E assim a análise de Turing pode ser aplicada.

Por outro lado, aceitar que a definição de *search*-computabilidade possui um conteúdo computacional implica em aceitar que *o axioma da escolha envolve um processo computacional*. Deve-se notar que o operador de busca foi introduzido no processo de computação e não declarado como operação inicial. Apesar disto, parece claro, embora não demonstramos, que *search*-computabilidade pode ser capturada por *prime*-computabilidade: basta considerar uma estrutura mais complexa onde o operador de busca pode ser declarado como uma função inicial. Isto aniquila o conteúdo computacional do operador de busca, pois quando considerado como função inicial, perde seu *status* inicial.

Vamos nos deter um pouco mais na afirmação de que o processo de computação envolvido em *prime*-computabilidade não traz nada genuinamente novo ao conceito de computação.

Em [**Fr1**], Friedmam observa que,

> Turing's analysis (as improved by Kleene and others) gives a mathematical analysis of configurational computations: one operates only on a fixed finite set of symbols which at each stage are arranged in a finite configuration in which the same symbol may occur in many different positions.

Baseado nesta observação pode-se dizer que uma máquina de Turing descreve um **procedimento algorítmico** que avalia uma função parcial sobre o conjunto $\{a_1, \ldots, a_n\}^*$ de todas as sequências finitas formadas sobre o conjunto finito de símbolos $\{a_1, \ldots, a_n\}$. Este procedimento algorítmico é exatamente a sequência de instruções realizadas por uma máquina de Turing a cada passo, i.e., comparar configurações linerares e modificá-las de acordo com o resultado da comparação[9].

Assim temos um procedimento algorítmico que descreve como a máquina opera, i.e., um conjunto finito de instruções aplicado a uma estrutura particular cujo universo é o conjunto $\{a_1, \ldots, a_n\}^*$ e as funções e relações básicas são exatamente as operações e comparações na definição de uma máquina de Turing.

A idéia crucial de Friedman é abstrair esta noção de procedimento algorítmico desvinculando-a de qualquer estrutura particular, não especificando as operações e testes básicos, e nem o domínio de aplicação.

Assim cada procedimento algorítmico, quando aplicado a uma estrutura particular, define uma função parcial sobre o domínio da estrutura *dada a abilidade de realizar as operações e testes básicos da estrutura.*

Mais precisamente, seja L uma linguagem de tipo finito σ e $\mathcal{A}$ uma interpretação de L, i.e, um universo não vazio U com constantes, relações e funções sobre U correspondentes ao tipo σ. Um **procedimento algorítmico finito**, denotado por `PAF`, é uma sequência finita $I_1, \ldots, I_q$ onde cada I_i instrução de uma das seguintes formas[10]:

$y := f(x_1, \ldots x_n)$

`se` $R(x_1, \ldots, x_m)$ `então` i `caso contrário` j

`pare`

Se estas instruções são interpretadas sobre uma certa estrutura relacional $\mathcal{A}$ com domínio D, i.e., interpretando todos os f e R como funções e predicados sobre D, e x_i,

[9] Cabe lembrar aqui que em [**SB**], Sieg e Byrnes generalizam o conceito de máquina de Turing a outras configurações e também os argumentos de Turing, que suportam a tese de Church-Turing, a estas novas máquinas, chamadas de *K-graph machines*.

[10] A definição de Friedman é mais cuidadosa, mas é em essência a mesma.

y como variáveis tomando valores em D, então um PAF se tranforma num programa (usual) que computa uma função parcial sobre D assumindo que o valor das funções iniciais aplicadas a um elemento qualquer de D e relações são sempre fornecidos quando necessário (por exemplo por um oráculo). Neste caso vamos dizer que as funções e relações iniciais são 'computáveis *a priori*'.

Podemos adicionar à lista de instruções, variáveis e operações sobre os números naturais do tipo

$c = 0$

$c = n + 1$

se $c_1 = c_2$ então i caso contrário j

Um PAF que também utiliza estas intruções será denotado por $\mathtt{PAF}_c$. Se os números naturais e as operações acima podem ser simulados pelos elementos e operações da estrutura então é intuitivo que PAF e $\mathtt{PAF}_c$ coincidem (cf. [**Fr1**]).

Observe que estamos assumindo que todas as operações de um PAF são computáveis *a priori*, i.e., as operações de armazenar quaisquer elementos do universo de $\mathcal{A}$, calcular as funções básicas de $\mathcal{A}$ e decidir as relações básicas de $\mathcal{A}$. Dependendo da interpretação, a função definida por um PAF pode não ser computável no sentido usual pois a definição acima permite, por exemplo, operações não computáveis classicamente como, por exemplo, a capacidade de armazenar um número irracional ou comparar quaisquer dois números reais.

Vamos supor agora que, dado uma estrutura $\mathcal{A}$, assumimos como computável (mesmo num sentido metafórico) as funções e relações básicas de $\mathcal{A}$. A partir deste pressuposto, uma questão natural é saber se toda função "intuitivamente computável" sobre $\mathcal{A}$ é $\mathtt{PAF}_c$-computável (sobre $\mathcal{A}$).

Uma primeira tentativa de responder esta questão é aplicar a mesma análise de Turing, levada a cabo em [**T**], no contexto de estruturas abstratas. Isto pode ser feito adicionando a uma máquina de Turing usual a capacidade de, armazenar quaisquer elementos do domínio de $\mathcal{A}$, testar quando uma relação básica é válida e, se f é uma função básica, substituir o conteúdo de qualquer célula observada na fita por $f(x_1, \ldots, x_n)$. Então espera-se que esta **máquina de Turing generalizada**, denotada por MTg, produza funções "computáveis" assumindo que as operações e relações da estrutura são "computáveis". Isto foi desenvolvido por Shepherdson em [**Sh1**] e é uma aplicação do mesmo argumento usado por Turing [**T**].

Portanto, a partir desta **Tese de Church-Turing relativizada** obtida por Shepherdson, uma MTg não traz nenhum refinamento ao conceito de computação, pois o processo de computação que está envolvido nos passos de uma MTg é exatamente o mesmo do que em uma máquina de Turing usual. Mais precisamente, uma máquina de Turing opera sobre um número finito de símbolos ordenados linearmente e a análise de Turing é uma análise matemática do conceito intuitivo de computabilidade linear.

Assumindo *a priori* que as operações e relações da estrutura são computáveis, o conceito de computabilidade capturado formalmente – assumindo que a análise de Turing é correta – pelas operações de uma máquina de Turing usual é exatamente o mesmo envolvido numa MTg *assumindo a hipótese inicial*.

Concluindo a relação entre *prime* e *search* computabilidade e uma Tese de Church-Turing relativizada, se $C_{\mathcal{A}}(\mathtt{MTg})$ e $C_{\mathcal{A}}(\mathtt{PAF}_c)$ são as classes de funções computáveis respectivamente por uma MTg e $\mathtt{PAF}_c$, então (cf. [**Fr1**]),

Teorema 3.1.

(1) Para qualquer estrutura $\mathcal{A}$, $C_{\mathcal{A}}(\mathtt{PAF}_c) \subseteq C_{\mathcal{A}}(\mathtt{MTg})$.

(2) Existe uma estrutura $\mathcal{B}^*$ tal que $C_{\mathcal{B}^*}(\mathtt{MTg}) \not\subseteq C_{\mathcal{B}^*}(\mathtt{PAF}_c)$.

Parece claro que uma função $\mathtt{PAF}_c$-computável sobre uma estrutura $\langle A,\varphi\rangle$ pode ser simulada por uma função *prime*-computável em φ sobre A, pois pela proposição (3.3) abaixo, as funções recursivas parciais são $\mathtt{PAF}_c$-computáveis e além disso, o processo de recursão utilizado na definição da classe de funções *prime*-computáveis é exatamente análogo ao caso das funções recursivas parcias. O que não é o caso de *search*-computabilidade.

Problema 3. Como comparar a classe das funções *serach*-computáveis em φ sobre A^* com a classe das funções MTg-computáveis sobre $\langle A,\varphi\rangle$?

Voltando ao trabalho de Friedman, num segundo momento ele mostra que alguns dos principais resultados básicos da teoria da recursão clássica não são mais válidos quando considerados sobre estruturas em geral. Isto pode ser interpretado da seguinte maneira: em termos conceituais, o sentido do conceito de computação envolvido no processo de computabilidade sobre estruturas abstratas é no máximo equivalente ao conceito de computação clássico, embora as classes de funções computáveis sobre outras estruturas é eventualmente bem mais ampla.

Estas observações parecem ir na direção oposta de nosso objetivo, que é o de formalizar um conceito aparentemente mais geral de computação embutido nas observações de Arnold. O ponto crucial na argumentação a favor da tese **T2**, é que computabilidade sobre estruturas abstratas, embora não seja uma *extensão conceitual* de "ser computável no sentido usual", é mais *permissível* do que computabilidade clássica, e isto parece ser suficiente para os propósitos de um algoritmo analítico como proposto por Arnold.

Seja L uma linguagem de tipo finito σ. Uma L-fórmula ϕ é chamada de **semi-algébrica básica** se ϕ pode ser definida como uma conjunção finita de fórmulas atômicas e suas negações de tal forma que se ϕ é $A_1 \wedge \ldots \wedge A_n$, então se $i \neq j$ não ocorre $A_i = B$ e $A_j = \neg B$. Como L possui um número enumerável de símbolos, é possível identificar as L-fórmulas semialgébricas básicas φ com seus respectivos números de Gödel $\langle\varphi\rangle$.

Definição. Um EDE de tipo (n, m, σ) é um conjunto enumerável de sentenças (strings) da forma

$$\phi_i \to t_i$$

onde ϕ_i e t_i são L-fórmulas e L-termos respectivamente, construídos a partir de um conjunto finito fixado de variáveis $\{x_1, \ldots, x_n, v_1, \ldots, v_m\}$ que satisfaz as seguintes propriedades:

(1) Quaisquer duas sentenças $\phi \to t$ e $\psi \to t'$ têm antecedentes incompatíveis, i.e., se ϕ é $A_1 \wedge \ldots \wedge A_n$ e ψ é $B_1 \wedge \ldots \wedge B_m$, então $A_i = \neg B_j$ para algum i, j.

(2) O conjunto $\{(\phi_i, t_i) | i \in \omega\}$ é enumerável recursivamente.

Um EDE de tipo (n, m, σ) define uma função parcial $f : D^n \to D$, onde D é o domínio de qualquer estrutura de tipo σ interpretando $\varphi \to t$ por "se ϕ é verdadeira então o valor da função definida por este EDE é t". Mais precisamente, uma função $f(x_1, \ldots, x_n)$ é **EDE-definível** se existe um EDE $\{\phi_i(u_1, \ldots, u_n, v_1, \ldots, v_m) \to t_i(u_1, \ldots, u_n, v_1, \ldots, v_m) | i \in \omega\}$, onde os u's e v's são variáveis formais, cada ϕ_i é uma L-fórmula semialgébrica básica, cada t_i é um L-termo e existem elementos $a_1, \ldots, a_m$ de D tal que f é definida pela disjunção de todas as condições da forma

$$f(x_1, \ldots, x_n) = t_i(x_1, \ldots, x_n, a_1, \ldots, a_m) \qquad \text{se} \qquad \phi_i(x_1, \ldots, x_n, a_1, \ldots, a_m).$$

A condição (1) da definição de EDE garante que f está bem definida; os elementos $a_1, \ldots, a_n$ são chamados de **parâmetros da definição** [11]. Na verdade EDE é uma generalização da definição de funções recursivas por casos.

Teorema 3.2. Para qualquer $\mathcal{A}$ de tipo σ, $C_{\mathcal{A}}(\mathtt{FAP}_c) \subseteq C_{\mathcal{A}}(\mathtt{EDE})$ e $C_{\mathcal{A}}(\mathtt{MTg}) \equiv C_{\mathcal{A}}(\mathtt{EDE})$.

A demonstração detalhada se encontra em **[Fr1]** e os detalhes são bastante técnicos, mas segundo Shepherdson **[Sh2]**,

[11] A definição de função EDE-definível em **[FM]** é um pouco diferente da definição em [Fr1] que pode ser vista como uma definição local, onde os parâmetros da definição são as constantes da estrutura. Isto altera a classe de funções EDE-definíveis sobre cada estrutura. Apesar disto, como os outros conceitos também são locais neste sentido, e os resultados de comparação envolvendo estes conceitos valem localmente, então é fácil ver que também valem globalmente. i.e., permitindo que os parâmetros das definições sejam quaisquer elementos do universo das estruturas. A definição dada acima é compatível com [FM] que é mais geral e adequada para os nossos propósitos.

> The argument applies not only to FAP or MTg but to any conceivable kind of computation and convince us that in the EDE's he [Friedman] really has captured the most general notion of computability over abstract structures.

Apesar de existirem estruturas para as quais a classe das funções EDE computáveis não coincide com a classe das funções $\mathtt{PAF}_c$ computáveis (cf. [**Fr1**]), se a estrutura for suficientemente "rica", então as classes coincidem. Este é o caso por exemplo de corpos e anéis.

Uma estrutura $\mathcal{A}$ é *ω-rica* se existe uma função injetora $\psi : \mathtt{N} \to A$ e funções $\overline{pred}$ e $\overline{suc}$ PAF-computáveis sobre A tal que $\psi(pred(n)) = \overline{pred}(\psi(n), \ldots, \psi(n))$, $\psi(suc(n)) = \overline{suc}(\psi(n), \ldots, \psi(n))$ e, $\psi(zero(n)) = \overline{zero}(\psi(n), \ldots, \psi(n))$, onde $\overline{zero}$ é a restrição de uma fórmula atômica aplicada a termos PAF-computáveis.

Seguindo a notação usual, se x é o número de Gödel de um L-termo formal t , então $\{x\}$ denota a função definida por t.

Uma estrutura é **estrutural** se é ω-rica e para cada n existe uma função PAF-computável $val_n(y, x_1, \ldots, x_n)$ tal que se x é o número de Gödel de um termo $t(v_1, \ldots, v_n)$, então,

$$val_n(\psi(x), x_1, \ldots, x_n) = \{x\}(x_1, \ldots, x_n)$$

Proposição 3.3. Suponha que $\mathcal{A}$ é ω-rica. Se $f(x_1, \ldots, x_n)$ é recursiva parcial, então existe uma função $F(y_1, \ldots, y_n)$, PAF computável sobre $\mathcal{A}$ tal que $\psi(f(x_1, \ldots, x_n)) = F(\psi(x_1), \ldots, \psi(x_n))$.

Demonstração (esboço). A classe das funções recursivas parciais é a menor classe de funções sobre os naturais que contém os polinômios, o predicado $zero(x)$, e é fechada por composição, recursão primitiva e μ-recursão. No caso dos polinômios, como $\mathcal{A}$ é ω-rica a proposição claramente é verdadeira. Não é difícil mostrar que as operações que definem a classe Parc podem ser simuladas por um PAF (como por exemplo em [**Od**]). □

Como estamos assumindo que L é uma linguagem finita, é fácil ver que a função $truth_n(x)$ definida como sendo o valor verdade da fórmula atômica de número de Gödel x, é PAF-computável, pois para estruturas ω-ricas vale a proposição (3.3) e $truth_n(x)$ é classicamente recursiva.

Proposição 3.4. Se uma estrutura $\mathcal{A}$ é ω-rica e estrutural então $C_{\mathcal{A}}(\mathtt{EDE}) = C_{\mathcal{A}}(\mathtt{PAF})$.

Demonstração: Suponha que $f(x_1, \ldots, x_n)$ é EDE-computável. Isto significa que existem funções recursivas primitivas p e q tal que $f(x_1, \ldots, x_n)$ é definida pela conjunção de cláusulas da forma:

$$f(x_1, \ldots, x_n) = t_i(x-1, \ldots, x_n, a_1, \ldots, a_k) \text{ se } \phi_i(x_1, \ldots, x_n, a_1, \ldots, a_k)$$

onde t_i é o termo com número de Gödel $p(i)$ e ϕ_i é a fórmula com número de Gödel $q(i)$. Observe que, como $\mathcal{A}$ é ω-rica, as funções recursivas parciais são PAF-definíveis sobre $\mathcal{A}$, i.e., se $f(x)$ é recursiva parcial então existe, pela proposição (3.3), uma função F, PAF-computável, definida sobre $\mathcal{A}$ tal que $\psi(f(x)) = F(\psi(x))$.

Como p e q são recursivas primitivas sejam P e Q tais que $\psi(p(i)) = P(\psi(i))$ e $\psi(q(i)) = Q(\psi(i))$. Então f é definida pelo PAF que procura um $\psi(i)$ tal que *truth* $_{n+k}(Q(\psi(i)), x_1, \ldots, x_n, a_1, \ldots, a_k)$ é verdadeira, e então fornece o valor *val* $_{n+k}(P(\psi(i)), x_1, \ldots, x_n, a_1, \ldots, a_k)$. $\square$

Consequentemente para corpos e anéis de característica zero as funções PAF-computáveis coincidem com as funções EDE-computáveis.

B. Máquinas sobre anéis.

Preocupado com problemas de complexidade de alguns algoritmos em análise, principalmente relacionados com a questão de como encontrar zeros de polinômios de forma eficiente, S. Smale [**Sm 1, 2, 3, 4**]observou que a noção de algoritmo , concebido como uma *máquina de Turing*, é inadequada para tratar tais tipos de problemas, pois uma máquina de Turing não é capaz de capturar a matemática envolvida.

Baseados em alguns exemplos de sistemas dinâmicos, L. Blum, M. Shub e S. Smale [**BSS**] começaram a desenvolver uma teoria de computabilidade baseada em um modelo de *máquinas sobre anéis*. Neste novo modelo, os elementos de um anel R são tratados como objetos definidos axiomaticamente, ou seja, considerando-se suas propriedades básicas.

No caso do corpo R dos números reais, esta forma de concepção difere de algumas das outras abordagens propostas para uma teoria de computabilidade sobre R, como por exemplo em [**PR**]. Nesses trabalhos os números reais são tratados como sequências de números naturais, o que conduz ao conceito de *número real computável*, isto é, a sequência de formação é definida por uma função recurssiva primitiva. Assim, o conceito de computabilidade sobre os reais computáveis se reduz ao conceito clássico, e os resultados de indecidibilidade clássica, por exemplo se aplicam de forma natural.

Seja R um anel ordenado, comutativo com unidade. Vamos denotar por R^n a soma direta $\bigoplus_1^n R$.

Seja $G = (X, U)$ um grafo orientado e conexo de grau N, onde X é o conjunto dos

nós de G e, U é uma família de elementos do produto $X \times X$, a família dos **arcos** de G. Suponha que G satisfaz as seguintes propriedades:

(1) G possui exatamente um nó x_1, (*input node*), tal que, para todo $y \in X$, $(y, x_1) \notin U$,

(2) G possui exatamente um nó x_N, (*output node*), tal que, para todo $y \in X$, $(x_N, y) \notin U$,

(3) o conjunto dos sucessores de um nó x em G, denotado por $\Gamma_G^+(x)$ tem no máximo dois elementos. Assim, $\Gamma_G^+(x) = \{\gamma(x)\}$, (*computational node*), ou $\Gamma_G^+(x) = \{\gamma_-(x), \gamma_+(x)\}$, (*branch node*).

Uma **máquina** M **sobre** R é uma dupla (G, Φ), onde G é um grafo orientado e conexo de grau N satisfazendo as condições (1)-(3) acima, e Φ é um conjunto de funções $\{\phi_1, \ldots, \phi_N\}$ definidas por,

(1) $\phi_1 : R^l \to R^m$, $l \leq m$, é a inclusão,

(2) se $|\Gamma_G^+(x_i)| = 1$, $\phi_i : R^m \to R^m$ é uma função polinomial,

(3) se $|\Gamma_G^+(x_i)| = 2$, $\phi_i : R^m \to R$ é um polinômio e,

(4) $\phi_N : R^m \to R^n$, $n \leq m$, é a projeção usual.

Os anéis R^l, R^n e R^m são chamados, respectivamente, de *input*, *output* e *state spaces* e serão denotados por $\overline{I}$, $\overline{O}$ e $\overline{S}$.

Vamos supor que M seja uma máquina sobre R com $X = \{1, \ldots, N\}$ o conjunto dos nós e $\overline{S}$ o seu espaço de estados. A função $H : X \times \overline{S} \to X \times \overline{S}$, chamada de **endomorfismo computacional**, é definida por $H(n, x) = (\beta(n, x), \chi(n, x))$, onde $\beta(n, x) = n$ se $n = N$ e, caso contrário,

$$\beta(n,x) = \begin{cases} n & \text{se } |\Gamma_G^+(n)| = \emptyset \\ \gamma(n) & \text{se } |\Gamma_G^+(n)| = 1 \\ \gamma(n)_+ & \text{se } |\Gamma_G^+(n)| = 2 \text{ e } \phi_n(x) < 0 \\ \gamma(n)_- & \text{se } |\Gamma_G^+(n)| = 2 \text{ e } \phi_n(x) \geq 0 \\ n & \text{se } |\Gamma_G^+(n)| = 0 \end{cases}$$

e além disso,

$$\chi(n,x) = \begin{cases} x & \text{se } n = 1 \text{ ou } |\Gamma_G^+(n) = 2| \text{ ou } |\Gamma_G^+(n)| = 0 \\ \phi_n(x) & \text{caso contrário} \end{cases}$$

Assim, a **computação** de uma máquina M sobre um anel R com *input* $y \in \overline{I}$ é representada por uma sequência $z_0, z_1, \ldots, z_k, \ldots$, $z_k \in X \times \overline{S}$, $z_0 = (1, \phi_1(y))$ e $z_k = H(z_{k-1})$, $k = 1, \ldots$. Usando a terminologia de sistemas dinâmicos, esta sequência é chamada de **órbita** de y.

Uma condição necessária e suficiente para que uma sequência $z_0, z_1, \ldots$ seja uma computação de M é que

$$z_0 = (1, \phi_1(y)), \qquad \text{para algum } y \in \overline{I}$$

$$z_k = H(z_{k-1}), \qquad k = 1, 2, \ldots \tag{3.5}$$

Dada uma máquina M, podemos definir naturalmente,a partir de H, a função parcial "computada por M", $\varphi_M : \overline{I} \to \overline{O}$. Se π_1 e π_2 são as projeções usuais, então,

$$\varphi_M(x) = \begin{cases} \pi_2(z_{k+1}) & \text{se } \pi_1(z_k) = N, \\ \text{indefinida} & \text{caso contrário.} \end{cases}$$

Observe que φ_M está bem definida, pois se $\pi_1(z_{k_1}) = \pi_1(z_{k_2}) = N$, então $\pi_2(z_{k_1}) = \pi_2(z_{k_2})$.

Vamos considerar, inicialmente, somente as sequências $z_k = (n_k, x_k)$ satisfazendo as equações (3.5) com a condição adicional $n_T = N$ para algum $T < \infty$. Se existe um tal T para algum $y \in \overline{I}$, então $T = T(y)$ é chamado de **tempo de parada** de M para computar $\varphi_M(y)$. O **conjunto de parada de** M, denotado por Ω_M é definido por

$$\Omega_M = \cup_{T \in \mathbf{N}} \{y \in \overline{I} | T(y) < T\}$$

Se R é um anel e $\varphi : R^l \to R^n$ é uma função parcial, então φ é uma **função computável sobre** R se existe uma máquina M sobre R tal que, o domínio Ω_φ de φ coincide com Ω_M e $\varphi_M(x) = \varphi_M(x)$ para $x \in \Omega_\varphi$. Um conjunto $Y \subset R^n$ é **decidível sobre** R se existem máquinas M e M' sobre R tais que $Y = \Omega_M$ e $R^n - Y = \Omega_{M'}$.

Vamos denotar por $C_M(R)$ a classe de funções computáveis sobre R.

Podemos caracterizar indutivamente $C_M(R)$ da seguinte maneira. Seja P_R a menor classe de funções parciais $f : R^l \to R^m$, $(l, m, < \infty)$, contendo as funções iniciais:

(1) funções polinomiais (sobre R) $f : R^l \to R$,

(2) a função característica $\chi : \Omega_\chi = R \to \{0, 1\}$, onde

$$\chi = \begin{cases} -1 & \text{se } x < 0 \\ 0 & \text{se } x = 0 \\ 1 & \text{se } x > 0 \end{cases}$$

e fechada sobre as seguintes operações:

- `Composição`. Se $f : R^l \to R^m$ e $g : R^m \to R^n$ estão em P_R, então a **composição** $g \circ f : R^l \to R^n$ é definida por $g(f(x))$ e $\Omega_{g \cdot f} = f^{-1}\Omega_g$.
- `Concatenação`. Se $f_i : R^l \to R^{m_i}$, $(i = 1, \ldots, k)$ estão em P_R e ψ é o isomorfismo natural de $R^{m_1} \times \cdots \times R^{M_k}$ em $R^{m_1 + \cdots m_k}$, então a **concatenação** $F = (f_1, \ldots, f_k) : R^l \to R^{m_1 + \cdots m_k}$ é dada por $F(x) = \psi(f_1(x), \ldots, f_k(x))$ para $x \in \Omega_F = \bigcap_{i=1}^{k} \Omega_{f_i}$.
- `Iteração`. Se $g : R^l \to R^l$ está em P_R, então $G : \mathrm{Z}^{\geq 0} \times R^l \to R^l$ definida por $G(0, x) = x$ e $G(t + 1, x) = g(G(t, x))$ está em P_R e

$$\Omega_G = \{(n, x) \in \mathrm{Z}^{\geq 0} \times R^l | n = 0 \text{ ou } n = t + 1 \text{ e } (t, x) \in \Omega_G, G(t, x) \in \Omega_g\}$$

- `Minimalização`. Dado $F : \Omega_F \supseteq \mathrm{Z}^{\geq 0} \times R^l \to R$, a operação de minimalização define uma função parcial $L : R^l \to \mathrm{Z}^{\geq 0}$ onde $L(x) = \min_t(F(t,x) = 0) = \min\{t \in \mathrm{Z}^{\geq 0} : F(t,x) = 0\}$.

Utilizando algumas propriedades do endomorfismo computacional H associado a uma máquina M, é possível mostrar os seguintes resultados (cf. [**BSS**]).

Proposição 3.6. $C_M(R)$ coincide com a classe P_R.

Proposição 3.7. A classe das funções recursivas parciais clássicas sobre Z coincide com $C_M(\mathrm{Z})$.

Como R é uma anel ordenado comutativo com unidade, sempre existe um homomorfismo (preservando a ordem e injetor) $\varphi : \mathrm{Z} \to R$ e portanto, para cada n, uma extensão $\overline{\varphi} : \mathrm{Z}[x_1, \ldots, x_n] \to R[x_1, \ldots, x_n]$ tal que, se f é um polinômio sobre Z, então, se $f(x_1, \ldots, x_n) = y$, $\varphi(f)(\varphi(x_1), \ldots, \varphi(x_n)) = \varphi(y)$. Sendo assim, se $\phi \in C_M(\mathrm{Z})$ podemos definir indutivamente uma função $\overline{\phi} \in C_M(R)$, (a partir da definição de ϕ), tal que, $\overline{\phi}(\varphi(\mathrm{Z}^l)) \subset \varphi(\mathrm{Z}^l)$, e

$$\varphi^{-1} \circ \overline{\phi}(x) = \phi(\varphi^{-1}(x)), \qquad x \in \varphi(\overline{I}),\ \overline{I} = \mathrm{Z}^l$$

Em outras palavras, todas as funções recursivas parciais clássicas sobre Z são *simuladas* por funções computáveis sobre R restritas a $\varphi(\mathrm{Z}^l)$.

Seja R um anel e L a linguagem formal usual associada. Vamos denotar por $C_E(R)$ a classe das funções EDE-definíveis sobre L.

Proposição 3.8. $C_M(R) \equiv C_E(R)$, i.e., se $f \in C_M(R)$ e $g \in C_E(R)$, então $f \simeq g$.

Demonstração. Vamos usar dois resultados ainda não demonstrados (proposição (3.12) e teorema (4.3)).

Vimos que classe $C_E(R)$ coincide com a classe das funções FAP-computáveis sobre o reais. É fácil transformar um PAF numa máquina sobre R.

Reciprocamente, se $f \in C_M(R)$, então existe M tal que $f = \varphi_M$ e $\Omega_f = \Omega_M$. Como $\Omega_M = \cup_{T \in \mathrm{N}} \Omega_{M,T}$ e pelo teorema (4.3), cada $\Omega_{M,T}$ é um conjunto semialgébrico básico de R com parâmetros no fecho algébrico de $a_1, \ldots, a_n$ ($a_1, \ldots, a_n$ são todos os coeficientes dos polinômios que ocorrem na definição de M), uma aplicação da proposição (3.12) conclui a demonstração. $\square$

Consequentemente para anéis ordenados de característica zero as classes de funções PAF-computáveis, PAF_c-computáveis, EDE-computáveis, e C_M coincidem.

Exemplo 3.9. A função $f(x) = \sqrt{x}$ não é computável sobre os reais.

Demonstração. Suponha que $x^{1/2}$ é definível por um conjunto enumerável de cláusulas da forma '$x^{1/2} = t_i(x)$ se $\varphi_i(x)$', onde cada t_i é uma função racional com coeficientes reais. Então pelo menos um dos φ_i deve ser satisfeito para um número não enumerável de elementos, e portanto existem polinômios P_i e Q_i tal que $P_i^2(x) = xQ_i^2(x)$ para um número não enumerável de x's, mas isto é impossível pois o grau de $P_i^2(x)$ é par enquanto que o grau de $xQ_i^2(x)$ é ímpar. □

Exemplo 3.10. ([**Ck**]) Toda função $f : \mathbb{N} \to \mathbb{N}$ é computável sobre os reais.

Demonstração. Dado um subconjunto S qualquer de $\mathbb{N}$ então S é recursivo, pois a seguinte sequência ordenada de instruções computa a função característica $C_S(n)$ de S ($I(x)$ é a parte inteira de x que é computável sobre os reais e $s =_{def} s_1 s_2 \dots$ é o número real definido por: $s_i = 1$ se $s \in S$, e $s_i = 0$ se $s_i \notin S$):

(1) $y = n$

(2) $(x_1, x_2) = (I(2^n x_1), 2I(2^{n-1}s))$

(3) `se` $x_1 - x_2 = 1$ `então` (4) `caso contrário (6)`

(4) $C_S(y) = 1$

(5) `pare`

(6) $C_S(y) = 0$

(7) `pare`

Agora considere o polinômio

$$P(n, m) = \frac{1 + n + m}{2}(n + m) + (m + 1)$$

e o conjunto $S = \{P(x, f(x)) : x \in \mathbb{N}\}$. Então o seguinte algoritmo computa $f(n)$:

(1) $y = n$

(2) $m = 0$

(3) `se` $C_S(P(n, m)) = 0$ `então (4) caso contrário (6)`

(4) $m = m + 1$

(5) `vá para (3)`

(6) $f(y) = m$

(7) `pare` □

A partir deste resultado, qualquer subconjunto de $\mathbb{N}$ é recursivo sobre os reais, inclusive $\mathcal{K}$. Isto trivializa qualquer problema de decisão envolvendo subconjuntos de naturais.

Vimos no capítulo I que indecidibilidade é um fenômeno persistente, mesmo se acrescentarmos todos os oráculos que decidem $\mathcal{K}^{(n)}$ para todo n. Note que existe um salto conceitual aqui, pois todos os subconjuntos de $\mathbb{N}$ são recursivos sobre os reais, i.e., todas as funções $C_{\emptyset(n)}$ e $C_{\emptyset(\omega+n)}$ são computáveis sobre os reais.

Exemplo 3.11. Considere a seguinte família de sistemas planares parametrizadas por $\mu_m \in \mathbb{R}$:

$$\begin{aligned} \dot{x} &= -y + x(\mu_m - (x^2 + y^2)) \\ \dot{y} &= x + y(\mu_m - (x^2 + y^2)) \end{aligned} \tag{$*$}$$

Sabemos que,

(1) para todo $m \in \mathbb{N}$, a origem é um ponto de equilíbrio de $(*)$,

(2) se $\mu_m < 0$ a origem é um ponto fixo assintoticamente estável de $(*)$, enquanto que para $\mu_m > 0$ ela é instável. Se $\mu_m = 0$ então a origem é estável.

Considerando computabilidade sobre os naturais (i.e., o conceito clássico), o conjunto $\{m \in \mathbb{N} - \{0\}$: a origem é assintoticamente estável $\}$ em geral, não é recursivo no sentido usual – basta tomar $\mu_m = \theta(m) - 1/2$ – mas é obviamente recursivo sobre os reais.

O ponto crucial aqui é que não importa se não é possível decidir classicamente, ou mesmo demonstrar, para todo $\mu \in \mathbb{R}$, se $\mu > 0$, ou $\mu < 0$, ou $\mu = 0$. O que conta aqui é que *temos um critério de estabilidade que se aplica a todos os casos*, i.e.,

(1) se $\mu < 0$ a origem é assintoticamente estável,

(2) se $\mu > 0$ origem é instável,

(3) se $\mu = 0$ a origem é estável, e que *não leva em consideração se é possível ou não decidir, dado μ, quando μ satisfaz (1), (2), ou (3).*

Neste caso, o conceito de computabilidade sobre os reais captura esta idéia, pois as condições que determinam a estabilidade da origem definem diretamente um EDE.
□

De uma forma mais geral, suponha que f é EDE-computável com

$$f(x_1, \ldots, x_n) = t_i(x_1, \ldots, x_n, a_1, \ldots, a_k) \text{ se } \phi_i(x_1, \ldots, x_n, a_1, \ldots, a_k)$$

e φ_i é semialgébrica básica, ou seja φ_i é uma interseção finita de fórmulas da forma $p_j(x_1, \ldots, x_n) < 0$ ou $p_j(x_1, \ldots, x_n) = 0$ onde cada p_j é um polinômio sobre um certo corpo fixo que depende dos parâmetros $a_1, \ldots, a_k$. Em outras palavras cada conjunto

$A_i = \{\vec{x} \in \mathbb{R}^n : \varphi_i(\vec{x})\}$ é um conjunto semialgébrico básico de R. [12] Portanto o domínio de f é uma união enumerável de subconjuntos semialébricos básicos de R. [13]

Reciprocamente, suponha que $\mathbb{Q}(a_1, \ldots, a_n)$ é um corpo com grau de transcendência finito, então,

Proposição 3.12. Seja $\Omega = \cup_{i=1}^{\infty} \Omega_i$ onde cada Ω_i é um conjunto semialgébrico básico de R tal que o conjunto dos parâmetros que ocorrem nos polinômios de cada Ω_i está no fecho algébrico de $a_1, \ldots, a_n$. Então Ω é um conjunto enumerável recursivamente sobre R.

Demonstração ([**Fr2**]). Suponha que temos uma relação em $x_1, \ldots, x_m$ definida como uma união enumerável de fórmulas $\varphi_i(b_{i,1}, \ldots, b_{i,k(i)}, x_1, \ldots, x_m)$ livres de quantificadores onde todos os $b_{i,j}$ estão no fecho algébrico de $a_1, \ldots, a_m$. Assim, cada $b_{i,j}$ é a solução de um polinômio sobre $\mathbb{Q}(a_1, \ldots, a_n)$, e portanto existe um polinômio $\varphi_{i,j}(a_1, \ldots, a_m, y)$ tal que $b_{i,j}$ é a única raíz. Então a nossa relação original é uma união de relações definidas pelas fórmulas

$$\exists y_1, \ldots, y_{k(i)} (\varphi_i(y_1, \ldots, y_{k(i)}, x_1, \ldots, x_n) \bigwedge_{j=1}^{k(i)} \varphi_{i,j}(a_1, \ldots, a_m, y_{k(i)})$$

Pelo teorema de eliminação de quantificadores de Tarski para corpos fechados reais (cf. [**vdD**]), cada uma destas fórmulas é equivalente a uma fórmula livre de quantificadores com as mesmas variáveis livres. É fácial construir uma função $d(n, x)$ computável sobre os reais tal que $d(n, x)$ é o n-ésimo dígito na decomposição binária de x. Assim, se a é o número real definido por $d(n, a) = 1$ se, e somente se, n é o número de Gödel de uma dessas fórmulas livres de quantificadores, considere o PAF que, dado $x_1, \ldots, x_n$, procura por um n tal que $d(n, a) = 1$ e a fórmula com número de Gödel n é verdadeira em $x_1, \ldots, x_n$. □

A idéia por detrás dos critérios algébricos de Arnold é bastante parecida com o que ocorre nos exemplos acima. Se interpretarmos o problema de Arnold como sendo formulado em função da não existência de critérios algébricos, e portanto, o sentido do processo algorítmico envolvido no problema não é equivalente a uma máquina de Turing, então, de acordo com o que foi discutido no capítulo II, o conceito de EDE parece ser *suficiente* para os propósitos de um algorítmo analítico.

Problema 4. No caso do problema de Arnold não importa se as funções iniciais sejam

[12] veja por exemplo o capítulo IV, seção A.

[13] No capítulo IV este resultado é demonstrado diretamente a partir da definição de máquinas sobre anéis.

computáveis, pois o problema seria solúvel se existisse um algoritmo algébrico. Mas, existe um processo sobre o qual pode-se argumentar do ponto de vista fenomenológico – como faz Turing ao analisar a noção intuitiva de computabilidade – que ainda pode ser chamado de computável e ao mesmo tempo ser pelo menos equivalente a computabilidade sobre os reais, por exemplo?

Não nos parece trivial estabelecer uma relação entre o fato de um problema ser algebricamente solúvel e ser EDE-decidível, pois a formulação dos critérios algébricos envolve uma aproximação infinita e além disso, não é claro o sentido de codimensão infinita. Como observa Arnold [**Ar3**],

> There remains some hope for the existence of a nonalgebraic algorithm, nevertheless, i.e., that the property of almost finite determinacy holds: the set of germs whose topological type (or stability) is not determined by any finite segment of the Taylor series may have infinite codimension. The question of whether this is so presents serious difficulties; its formulation has to be made precise, by indicating the exact sense of the word codimension[14]. The sets in the space of k-jets whose codimension has to be defined are not algebraic and set-theoretical difficulties may arise. Thom conjectured that the answer to this question is negative.
>
> We also mention the problem of algorithmical decidability of the stability of a stationary point for a vector field with polynomial components over the ring of integers.

Problema 5. Em vista dessas observações, é possível estabelecer uma relação entre critérios algébricos e EDE's?

A partir do que foi exposto acima, acreditamos que, mesmo que o conceito de computabilidade que aparece na teoria de computabilidade sobre estruturas abstratas seja uma metáfora (cf. [**Kr1**]), aqui ele adquire um novo *status* conceitual, pois tem uma funcionalidade se visto de fato como "computável".

[14] Talvez os resultados de [**To**] ofereçam alguma idéia.

4. Recursividade e sistemas dinâmicos.

Um dos resultados mais interessantes da teoria de recursão clássica é a existência de conjuntos recursivamente enumeráveis cujo complemento não é recursivamente enumerável. Este resultado além de implicar importantes consequências matemáticas, como por exemplo a insolubilidade do problema da parada e todas as suas consequências, (inclusive a solução de da Costa e Doria do problema de Arnold), tornou-se objeto básico de estudo de grande parte do trabalho que vem sendo desenvolvido em teoria da recursão, como por exemplo a teoria dos graus de redutibilidade.

Usualmente, a construção de conjuntos enumeráveis recursivamente não recursivos é baseada, na teoria clássica, na existência de funções universais. Este método, conforme [**Ma**],

> (...) produces sets so far from the realm of ordinary mathematics that at first they might appear to be irrelevant. (...) the situation is very different for recursion theory over abstract models.

O objetivo deste capítulo é rever alguns destes exemplos. A idéia geral é a seguinte. É evidente que sistemas dinâmicos discretos e as máquinas sobre anéis de [**BSS**], ou de forma equivalente, EDE's sobre anéis, estão intimamente relacionados como já foi observado no capítulo anterior. Na verdade, a partir de uma caracterização algébrico-topológica dos conjunto Ω_M, podemos estabelecer uma relação entre estes conjuntos e dimensão de Hausdorff, um conceito bastante utilizado na teoria de sistemas dinâmicos. Estabelecer esta relação é basicamente o propósito da primeira seção . A partir deste fato, e este é o conteúdo da seção B, pode-se mostrar que alguns objetos amplamente estudados nesta teoria não são recursivos sobre os reais, como por exemplo alguns atratores, o conjunto de Mandelbrot e certos conjuntos de Julia.

A. Conjuntos recursivamente enumeráveis sobre anéis.

A existência de conjuntos recursivamente enumeráveis cujo complemento não é recursivamente enumerável constitui um ingrediente básico para gerar incompletude numa teoria na qual estes conjuntos são representáveis, como revela a demonstração do teorema (1.12). Além disso, indecidibilidade também é definida nestes termos. Por outro lado, o conjunto $\mathcal{K}$ foi definido a partir da existência da função universal

$\varphi_{univ}(e, x)$ (Capítulo I). Uma questão imediata: se M é uma estrutura qualquer e existe uma função universal M-computável, i.e., EDE-computável sobre M, então M possui conjuntos recursivamente enumeráveis não recursivos?

Uma análise da definição de $\mathcal{K}$ mostra que sempre é possível a partir de uma função universal computável, construir um conjunto recursivamente enumerável não recursivo. Mas esta técnica não funciona no caso de computabilidade sobre os reais, pois,

Teorema 4.1 O corpo dos números reais R não possui uma função universal R-computável.

A demonstração deste resultado utiliza o fato, ainda não demonstrado de que, se M é uma máquina sobre um anel R então Ω_M é uma união enumerável de *subconjuntos semialgébricos básicos* de R. Cabe lembrar aqui que se $X \subset R^n$, onde R é um anel ordenado de característica zero, então X é **semialgébrico básico sobre** R se existem polinômios $p, q_1, \ldots, q_m$ sobre R tal que

$$X = \{(x_1, \ldots, x_n) \in R^n : p(x_1, \ldots, x_2) = 0, q_i(x_1, \ldots, x_n) > 0, i = 1, \ldots, n\}$$

Apesar deste resultado podemos mostrar que existem subconjuntos dos reais recursivamente enumeráveis não-recursivos sobre R. Basta observar por exemplo, e isto é um fato bem conhecido (cf. [**vdD**]), que conjuntos semialgébricos possuem um número finito de componentes conexas. Esta simples propriedade topológica nos permite concluir, por exemplo, que o conjunto de Cantor não é recursivamente enumerável sobre R. Mas conectividade não é suficiente para caracterizar topologicamente recursão sobre os reais, pois, como veremos, o conjunto de Mandelbrot não é recursivo sobre os reais e é conexo (cf. [**DH**]). Mesmo no caso algébrico a situação geral não é tão simples: se R é um corpo fechado real, então um conjunto é recursivamente enumerável sobre R, se, e somente se, é uma união enumerável de conjuntos semialgébricos com parâmetros do mesmo corpo com grau de transcendência finito (proposição (3.12)). No caso de subanéis de R o problema foi resolvido por [**By**] e [**Mi**], mas o caso geral ainda é um problema em aberto. No caso topológico pode-se estabelecer uma outra condição necessária, mais fina que conectividade, para que um subconjunto de R seja recursivamente enumerável sobre R. Antes porém, vamos demonstrar o resultado acima enunciado de que um conjunto recursivamente enumerável sobre um anel R é uma união enumerável de subconjuntos semialgébricos de R. Vamos utilizar o formalismo de máquinas sobre anéis de [**BSS**], mas evidentemente, este mesmo resultado pode ser obtido utilizando EDE's (cf. [**FM**, teorema 21]).

Dado uma máquina M sobre um anel R, vamos denotar por $\Omega_{M,T}$ o conjunto $\{y \in \overline{I} | T(y) < T\}$. Seja $\Gamma_{M,T}$ o conjunto das sequências $(n_0, \ldots, n_T) \in X^{T+1}$ que satisfazem,para algum $y \in \overline{I}$, as seguintes condições,

$$\begin{aligned} n_0 &= 1 \\ n_i &= \pi_1(H^{\circ i}(1, \phi_1(y))), \qquad 1 \leq i \leq T-1, \text{ e} \\ N_T &= N \end{aligned}$$

É fácil ver que, se $B_M = \sum_{i=1}^{N-1}(|\Gamma_G^+(i)| - 1)$, então $|\Gamma_{M,T}| \leq 2^{\max(B_M, T-2)}$. Para cada $\gamma \in \Gamma_{M,T}$, seja

$$\Omega_{M,\gamma} = \{y \in \overline{I} | \pi_1(H^{\circ i}(1, \phi_1(y))) = \pi_{i+1}(\gamma), 1 \leq i \leq T\}$$

Então, $\Omega_{M,T} = \cup_{\gamma \in \Gamma_{M,T}} \Omega_{M,\gamma}$.

Proposição 4.2. Se M é uma máquina sobre R com input space $\overline{I}$, então $\Omega_{M,T}$ é um subconjunto semialgébrico básico de $\overline{I}$.

Demonstração. Seja $b(\gamma, i)$ o i-ésimo *branch node* de γ e $B_\gamma = \sum_{i=1}^{T}(|\Gamma_G^+(\pi_i(\gamma))| - 1)$. Se $y \in \Omega_{M,\gamma}$, então, para $1 \leq i \leq B_\gamma$

$$\begin{aligned} &\phi_{b(\gamma,i)} \circ \pi_2(H^{\circ b(\gamma,i)}(1, \phi(y))) < 0 \qquad \text{se } \pi_{b(\gamma,i)+1}(\gamma) = \beta_+(b(\gamma, i)) \text{ ou} \\ &\phi_{b(\gamma,i)} \circ \pi_2(H^{\circ b(\gamma,i)}(1, \phi(y))) \geq 0 \qquad \text{se } \pi_{b(\gamma,i)+1}(\gamma) = \beta_-(b(\gamma, i)) \end{aligned} \tag{4.1.1}$$

ou seja,

$$\Omega_{M,\gamma} \subset \bigcap_{1 \leq i \leq B_\gamma} \{y \in \overline{I} | C(i, y)\},$$

onde $C(i, y)$ é uma das desigualdades de (4.1.1). Por outro lado, é fácil ver, por indução em B_γ, que $\gamma_1 = \gamma_2$ se, e somente se, $B_{\gamma_1} = B_{\gamma_2}$ e $n_{b(\gamma_1,i)+1} = n_{b(\gamma_2,i)+1}$, $1 \leq i \leq B_{\gamma_1}$. Assim, se $y \in \bigcap_{1 \leq i \leq B_\gamma} \{y \in \overline{I} | C(i, y)\}$, então, existe uma única $\gamma' \in \Gamma_{M,T}$ tal que

$$\pi_{b(\gamma',i)+1}(\gamma') = \pi_1(H^{\circ b(\gamma',i)}(1, \phi_1(y)))$$

Mas γ também satisfaz esta condição, logo $\gamma' = \gamma$ e $y \in \Omega_{T,\gamma}$. Agora, basta mostrar que $\phi_{b(\gamma,i)} \circ \pi_2(H^{\circ b(\gamma,i)}(1, \phi(y)))$, entendido como uma função de y, é um polinômio sobre R. Mas isto é óbvio por indução em B_γ e pela definição de H. □

Teorema 4.3. Ω_M é uma união enumerável de subconjuntos semialgébricos básicos de $\overline{I}$.

Demonstração. $\Omega_M = \cup_{T \in \mathbb{N}} \Omega_{M,T}$ □

A partir deste resultado podemos mostrar, por exemplo, que *o conjunto I dos irracionais não é recursivamente enumerável sobre os reais.* A demonstração é bastante simples: vamos supor por hipótese que I é recursivamente enumerável. Então existe uma máquina M tal que $\Omega_M = I$. É claro que M tem pelo menos um *branch node*. A partir da demonstração da proposição (4.2), existe um número finito de elementos $a_1, \ldots, a_n \in \mathbb{R}$ tal que os coeficientes dos polinômios que aparecem em M são todos elementos do corpo $\mathbb{Q}[a_1, \ldots, a_n]$. Então todos os polinômios que aparecem em todas as órbitas possíveis finitas são polinômios sobre $\mathbb{Q}[a_1, \ldots, a_n]$. Como o corpo dos reais tem grau de transcendência infinito sobre os racionais, existe $i \in I$ que não é algébrico em $\mathbb{Q}[a_1, \ldots, a_n]$. Como I é recursivamente enumerável, por hipótese, I é uma união enumerável de conjuntos semialgébricos e portanto $i \in I$ satisfaz um número finito de igualdades e desigualdades ($i \in \Omega_{M,T}$). Mas i não satisfaz nenhuma igualdade, pois não é algébrico sobre $\mathbb{Q}[a_1, \ldots, a_n]$. Portanto, se $z_0 = (1, \phi_1(i)), z_1 = H(z_0), \ldots, z_N = H(z_{N-1})$ é a órbita de i e γ é a sequência $(1, \pi_1(H(1, \phi(i)), \pi_1(H \circ H(1, \phi(i))), \ldots, N)$, utilizando a mesma notação da demonstração da proposição (4.1), existe um T tal que o irracional i satisfaz as seguintes desigualdades, para $1 \leq j \leq B_\gamma$,

$$\begin{aligned} &\phi_{b(\gamma,j)} \circ \pi_2(H^{\circ b(\gamma,j)}(1, \phi(i))) < 0 \qquad \text{se } \pi_{b(\gamma,j)+1}(\gamma) = \beta_+(b(\gamma, j)) \text{ ou} \\ &\phi_{b(\gamma,j)} \circ \pi_2(H^{\circ b(\gamma,j)}(1, \phi(i))) > 0 \qquad \text{se } \pi_{b(\gamma,i)+1}(\gamma) = \beta_-(b(\gamma, i)) \end{aligned}$$

Como $\phi_{b(\gamma,j)} \circ \pi_2(H^{\circ b(\gamma,j)}(1, \phi(y)))$ é um polinômio, para cada j, os conjuntos

$$\begin{aligned} &\{y \in \mathbb{R} : \phi_{b(\gamma,j)} \circ \pi_2(H^{\circ b(\gamma,j)}(1, \phi(i))) < 0\}, \\ &\{y \in \mathbb{R} : \phi_{b(\gamma,j)} \circ \pi_2(H^{\circ b(\gamma,j)}(1, \phi(i))) > 0\}, \end{aligned}$$

são abertos, e portanto $\Omega_{M,\gamma}$ é uma intersecção finita de abertos, i.e, $\Omega_{M,\gamma}$ é um subconjunto aberto de $\mathbb{R}$. Mas então $\Omega_{M,\gamma} \subset \Omega_M$ contém racionais, isto é $I = \Omega_M$ contém racionais, o que é um absurdo.

De certa forma esta mesma estratégia pode ser usada para demonstrar o teorema (4.1):

Demonstração do teorema (4.1). Seja $U_n(e, x_1, \ldots, x_n)$ uma função universal sobre $\mathbb{R}$, i.e., se $f : \mathbb{R}^n \to \mathbb{R}$ é uma função computável sobre $\mathbb{R}$, então existe um índice e tal que $f(x_1, \ldots, x_n) = U_n(e, x_1, \ldots x_n)$. Dado um índice e, $\Omega_{U_n(e,-)}$ denota o domínio de $U_n(e, -)$.

A idéia geral da demonstração é definir $f : \mathbb{R} \to \mathbb{R}^{n+1}$ de tal forma que , dado uma $n+1$-upla $\alpha = (\alpha_1, \ldots, \alpha_{n+1}) \in \mathbb{R}^{n+1}$, exista um $e \in \mathbb{R}$ tal que $f(e) = \alpha$ e além disso, $U_1(e, \pi_i \circ \alpha)\downarrow$ e $|\Omega_{U_1(e,-)}| < \infty$. Se $a_1, \ldots, a_k \in \mathbb{R}$ são tais que, todos os polinômios que ocorrem na máquina que define $U_1(e, -)$ são polinômios sobre $\mathbb{Q}(e, a_1, \ldots, a_k)$, como

$|\Omega_{U_1(e,-)}| < \infty$ e $\Omega_{U_1(e,-)}$ é uma união enumerável de subconjuntos semialgébricos básicos de R, então as coordenadas de $f(x)$ são números algébricos sobre $\mathbb{Q}(x, a_1, \ldots, a_k)$ (se $x \in \Omega_{U_1(e,-)}$ então x é raíz de pelo menos algum polinômio que ocorre na órbita de x). Mas isto não é possível pois se $\phi_1(x,y), \phi_2(x,y)\ldots$ é uma enumeração dos polinômios de duas variáveis sobre $\mathbb{Q}(a_1, \ldots, a_k)$ e para cada $(i,j) = i_1, \ldots, i_{n+1}, j_1, \ldots, j_{n+1} \in \mathbb{N}$

$$\psi_{(i,j)}(x) =_{\text{def}} \langle i_1\text{-ésima raíz de } \phi_{j_1}(x,-), \ldots, i_{n+1}\text{-ésima raíz de } \phi_{j_{n+1}}(x,-)\rangle$$

então, conforme [**FM**], a imagem de $\psi_{(i,j)}$ não é densa em $\mathbb{R}^{n+1}$, mas

$$\mathbb{R}^{n+1} = \mathrm{Im} f \subset \bigcup_{(i,j)\in\mathbb{N}^{2n+2}} \mathrm{Im}\ \psi_{(i,j)}$$

o que é um absurdo. □

No caso $n = 1$, uma primeira aproximação para a definição de f seria, a partir do par $\langle a,b\rangle \in$ R, definir uma função $\xi_{\langle a,b\rangle}(x)$ como sendo: $\xi_{\langle a,b\rangle}(x) = 1$ se $x = a$ ou $x = b$ e, caso contrário, $\xi_{\langle a,b\rangle}(x)$ é indefinida. É claro que ξ é computável sobre R e portanto existe um e tal que $|U_1,(e,-)| \leq 2$, $U_1(e,a)\downarrow$ e $U_1(e,b)\downarrow$, e além disso $f(e) =_{\text{def}} \langle a,b\rangle$. Mas, evidentemente, f não está bem definida como função. A forma correta, neste caso, é a seguinte:

$$f(x) =_{\text{def}} \begin{cases} \langle 0,0\rangle & \text{se } |\Omega_{U_1(x,-)}| > 3 \text{ ou } |\Omega_{U_1(x,-)}| = 0, \\ \langle y,y\rangle & \text{se } |\Omega_{U_1(x,-)}| = 1 \text{ e } U_1(x,y)\downarrow, \\ \langle y,z\rangle & \text{se } |\Omega_{U_1(x,-)}| = 2 \text{ e } U_1(x,y)\downarrow,\ U_1,(x,z)\downarrow \text{ e } y < z, \\ \langle y,z\rangle & \text{se } |\Omega_{U_1(x,-)}| = 3 \text{ e } U_1(x,y)\downarrow,\ U_1,(x,z)\downarrow \text{ e } z < y \end{cases}$$

É claro que f é sobrejetora, pois dado $\langle a,b\rangle \in \mathbb{R}^2$, se

$$\xi_{\langle a,b\rangle}(x) \simeq_{\text{def}} \begin{cases} 0 & \text{se } a = b = 0 \\ 1 & \text{se } (x \neq 0 \wedge x = a = b)\vee \\ & \quad \vee(x = a \vee x = b \wedge a < b) \vee (x = a \vee x = b \vee x = a+1 \wedge b < a) \\ \uparrow & \text{caso contrário} \end{cases}$$

então $\xi_{\langle a,b\rangle}$ é computável sobre R e portanto existe $e_{\langle a,b\rangle}$ tal que $\xi_{\langle a,b\rangle}(x) \simeq U_1(e_{\langle a,b\rangle}, x)$ e pela definição de f, $f(e_{\langle a,b\rangle}) = \langle a,b\rangle$. Para $n \geq 2$ a construção é análoga, embora as definições de f e ξ sejam muito mais complexas devido a quantidade de casos a se considerar.

Vamos passar agora à relação entre conjuntos recursivamente enumeráveis sobre R e dimensão.

Se U é um subconjunto não vazio de $\mathbb{R}^n$ o **diâmetro** de U é definido como $|U| = \sup\{|x-y| : x,y \in U\}$. Se $\{U_i\}$ é uma família enumerável de subconjuntos de $\mathbb{R}^n$, então $\{U_i\}$ é uma **δ-cobertura de U** se $U \subset \bigcup_{i=1}^{\infty} U_i$ e $0 < |U_i| < \delta$.

Se F é um subconjunto de Borel de $\mathbb{R}^n$, s um número não-negativo e $\delta > 0$, então

$$\mathcal{H}^s_\delta(F) =_{\text{def}} \inf\Big\{\sum_{i=1}^{\infty} |U_i|^s : \{U_i\} \text{ é uma } \delta\text{-cobertura de } F\Big\}$$

Definição. Se F é um subconjunto de $\mathbb{R}^n$ e s é um número não negativo, então a **medida de Hausdorff s-dimensional de F** é definida como

$$\mathcal{H}^s =_{\text{def}} \lim_{\delta \to 0} \mathcal{H}^s_\delta(F)$$

Pode-se mostrar que $\mathcal{H}^s(F)$ é fato uma **medida**, i.e: $\mathcal{H}^s(\emptyset) = 0$, se $F \subset E$ então $\mathcal{H}^s(F) \leq \mathcal{H}^s(E)$ e se $\{F_i\}$ é uma coleção enumerável de conjuntos de Borel disjuntos, então $\mathcal{H}^s\Big(\cup_{i=1}^{\infty} F_i\Big) = \sum_{i=1}^{\infty} \mathcal{H}^s(F_i)$

Conforme observa [**Fa**], a medida de Hausdorff generaliza as idéias de comprimento, área, volume, etc. Pode-se mostrar, por exemplo, que se $F \subset \mathbb{R}^n$ é um subconjunto de Borel, então $\mathcal{H}^n(F) = c_n \text{vol}^n(F)$, onde c_n é o volume n-dimensional de uma bola de raio $1/2$ em $\mathbb{R}^n$ (veja por exemplo [**Ed**]).

Se $t > s$ e $\{U_i\}$ é uma δ-cobertura de F, então

$$\sum_i |U_i|^t \leq \delta^{t-s} \sum_i |U_i|^s$$

e sendo assim, $\mathcal{H}^t_\delta(F) \leq \delta^{t-s}\mathcal{H}^s_\delta(F)$. Se $\mathcal{H}^s(F) < \infty$ tomando o limite $\delta \to 0$ temos que $\mathcal{H}^t(F) = 0$ para $t > s$. Portanto existe um valor s_0 tal que $\mathcal{H}^{s_0}(F)$ salta de ∞ para 0.

Definição. Seja $F \subset \mathbb{R}^n$ um conjunto de Borel. A **dimensão de Hausdorff** de F é definida como sendo

$$\dim_H F = \inf\{s : \mathcal{H}^s(F) = 0\} = \sup\{s : \mathcal{H}^s(F) = \infty\}$$

Se $E \subset F$ então, para cada s, é imediato que $\mathcal{H}^s(E) \leq \mathcal{H}^s(F)$ e assim $\dim_H E \leq \dim_H F$. Além disso se $F_1, F_2, \ldots$ é uma sequência de conjuntos é claro que $\dim_H \cup_{i=1}^{\infty} F_i \geq \dim_H F_j$ para cada j. Por outro lado, se $s > \dim_H F_i$ para todo i, então $\mathcal{H}^s(F_i) = 0$, ou seja, $\mathcal{H}^s(\cup_{i=1}^{\infty} F_i) = 0$. Por consequência, $\dim_H \cup_{i=1}^{\infty} F_i = \sup_{1 \leq i < \infty}\{\dim_H F_i\}$.

Um exemplo clássico. O conjunto de Cantor tem dimensão de Hausdorff $\log_2 3$ (cf. [**Fa**]).

Se X é um conjunto, uma **medida exterior** sobre X é uma função $\mu : \mathcal{P}(X) \to [0, \infty]$ satisfazendo:

(1) $\mu(\emptyset) = 0$,

(2) se $A \subseteq B$, então $\mu(A) \leq \mu(B)$,

(3) $\mu(\bigcup_{n\in\mathbb{N}} A_n) \leq \sum_{i=1}^{\infty} \mu(A_n)$.

Seja X um conjunto e $\mathcal{V}$ uma família de subconjuntos de X com $X \subset \bigcup_{A\in\mathcal{V}} A$ e $\varphi : \mathcal{V} \to [0, \infty]$ uma função qualquer,

$$\mu(B) =_{\text{def}} \inf\{\sum_{A\in\mathcal{U}} \varphi(A) : \mathcal{U} \text{ é uma cobertura enumerável de } B \text{ e } \mathcal{U} \subset \mathcal{V}\}$$

Lema 4.4. A função μ acima definida é a única medida exterior sobre X tal que

(1) $\mu(A) \leq \varphi(A)$ para todo $A \in \mathcal{V}$,

(2) se η é uma outra medida exterior sobre X com $\eta(A) \leq c\varphi(A)$ para alguma constante c e todo $A \in \mathcal{V}$, então $\eta(B) \leq c\,\mu(B)$ para todo $B \subseteq X$.

A demonstração deste resultado pode ser encontrada em [**Ed**] por exemplo. Este resultado é uma forma de construir medidas sobre X a partir de uma função φ e de uma família de subconjuntos de X que cobrem X. O problema é que se μ é uma medida construída desta forma então é possível que nem todos os subconjuntos de Borel de X sejam **mensuráveis** sobre μ, ou seja, é possível (cf. [**Ed**]) existir $A \in X$ tal que $\mu(E) \neq \mu(E \cap A) + \mu(E/A)$ para todo $E \subseteq X$, uma propriedade quase sempre indesejável. O fato é que isto pode ser superado através de uma construção que também fornece um outro método para a construção de medidas. A idéia é a seguinte.

Sejam $\mathcal{U} \subseteq \mathcal{V}$ duas coberturas de X por subconjuntos de X, e $\varphi : \mathcal{V} \to [0, \infty]$ uma função. Se μ é definida por φ e $\mathcal{U}$ pelo lema (4.4), e se η é definida por φ e $\mathcal{V}$, então $\mu(A) \geq \eta(A)$ para todo $A \subseteq X$, pois $\eta(A) \leq \varphi(A)$ para todo $A \in \mathcal{V}$ e em particular para todo $A \in \mathcal{U}$.

Assim, seja $\mathcal{V}$ uma família de subconjuntos de um *espaço métrico* X tal que, dado ε e $x \in X$, existe $A \in \mathcal{V}$ com $x \in A$ e $|A| \leq \varepsilon$ e $\varphi : \mathcal{V} \to [0, \infty]$ uma função qualquer. Se $\mathcal{A}_\varepsilon \subset \mathcal{V}$ é uma ε-cobertura de X, e μ_ε é a medida exterior definda pelo lema (4.4) sobre $\mathcal{A}_\varepsilon$ e φ, então a função $\mu : \mathcal{P}(X) \to [0, \infty]$ definida por

$$\mu(E) =_{\text{def}} \lim_{\varepsilon\to 0} \mu_\varepsilon(E) = \sup_{\varepsilon>0} \mu_\varepsilon(E)$$

também é uma medida exterior e além disso, os conjuntos de Borel são conjuntos mensuráveis sobre medidas construídas desta forma (cf. [**Ed**]).

É imediato que a medida de Hausdorff s-dimensional é uma medida deste tipo, onde $\varphi(E) = |E|^s$. Se $\mathcal{A}_\varepsilon$ é a coleção de todos os **hipercubos** A_ε **n-dimensionais de lado $\leq \varepsilon$ de** R^n, onde

$$A_\varepsilon =_{\text{def}} \{(x_1, \ldots, x_n) \in \mathrm{R}^n : a_i \leq x_i \leq b_i,\ b_i - a_i \leq \varepsilon\}$$

para algum $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in \mathrm{R}^n$, então, dado $E \subset \mathrm{R}^n$ a **medida de Lebesgue n-dimensional** de E é definida como

$$\mathcal{L}^n(E) =_{\text{def}} \lim_{\varepsilon \to 0} \mathcal{L}^n(E)_\varepsilon = \sup_{\varepsilon > 0} \mathcal{L}^n_\varepsilon(E),$$

onde $\mathcal{L}^n_\varepsilon$ é a medida exterior definida pelo lema (4.4) sobre $\mathcal{A}_\varepsilon$ e $\varphi(A) = \mathrm{vol}_n A$ para todo $A \in \mathcal{A}_\varepsilon$

Lema 4.5. Se $B \subseteq \mathrm{R}^n$ é um conjunto de Borel, então existem constantes c_n e d_n tal que

$$c_n \mathcal{L}^n(B) \leq \mathcal{H}^n(B) \leq d_n \mathcal{L}^n(B)$$

Demonstração. Vamos mostrar inicialmente uma propriedade simples sobre medidas de Hausdorff. Dado um conjunto $B \subseteq \mathrm{R}^n$, λB denota o conjunto $\{\lambda x \in \mathrm{R}^n : x \in B\}$. Agora, se $\{U_i\}$ é uma δ-cobertura de B, então $\{\lambda U_i\}$ é uma $\lambda\delta$ cobertura de λB e

$$\mathcal{H}^s_{\lambda\delta}(\lambda B) \leq \lambda^s \sum |U_i|^s \leq \lambda^s \mathcal{H}^s_\delta(B)$$

ou seja, $\mathcal{H}^s(\lambda B) \leq \lambda^s \mathcal{H}^s(B)$. Pelo mesmo argumento, fazendo as substituições adequadas, temos $\lambda^s \mathcal{H}^s(B) \leq \mathcal{H}^s(\lambda B)$, i.e., $\mathcal{H}^s(\lambda B) = \lambda^s \mathcal{H}^s(B)$.

Se A_1 é um hiper-cubo n-dimensional de lado igual a 1 é claro que $\mathcal{H}^n(A_1)$ é finito e portanto, para cada ε, $\mathcal{H}^n_\varepsilon(\lambda A_1) = \lambda^n \mathcal{H}^n_\varepsilon(A_1) \leq \mathcal{L}^n_\varepsilon(A_\lambda)\mathcal{H}^n(A_1)$.

Como $\mathcal{L}^n_\varepsilon$ foi definida pelo lema (4.4) com $\varphi = \mathrm{vol}_n$ e $\mathcal{V}$ como sendo a coleção de todos os hiper-cubos A_ε n-dimensionais de R^n de lado $\leq \varepsilon$, então, como $\mathcal{H}^n_\varepsilon(\lambda A_1) \leq \mathcal{H}^n(A_1)\mathcal{L}^n_\varepsilon(A_\lambda)$, pelo lema (4.4) $\mathcal{H}^n_\varepsilon(B) \leq \mathcal{H}^n(A_1)\mathcal{L}^n_\varepsilon(B)$ para todo subconjunto de R^n, ou seja, $\mathcal{H}^n(B) \leq \mathcal{H}^n(A_1)\mathcal{L}^n(B)$.

Por outro lado, dado $\varepsilon > 0$ e $\lambda \leq \varepsilon$, se $B \subset \mathrm{R}^n$ com $|B| = \varepsilon$, então existe um hiper-cubo A_1 de lado 1 tal que $B \subseteq \lambda A_1$ e uma bola $B_{\lambda/2}$ de raio $\lambda/2$ que contém B. Assim, $\mathcal{L}^n_\varepsilon(B) \leq c_n \lambda^n = c_n |B|^n$, e novamente pelo lema (4.4), $\mathcal{L}^n_\varepsilon(B) \leq c_n \mathcal{H}^n_\varepsilon(B)$ para todo $B \subset \mathrm{R}^n$. $\square$

Teorema 4.6. Se $F \subset \mathrm{R}^n$, e F é um conjunto recursivamente enumerável sobre R, então $\dim_H F = m$ onde $0 \leq m \leq n$.

Demonstração. Como F é recursivamente enumerável, existe uma máquina M sobre $\mathbb{R}$ tal que $F = \Omega_M = \cup_{T \in \mathbb{N}} \Omega_{M,T}$ e cada $\Omega_{M,T}$ é um subconjunto semialgébrico de $\overline{I}$.

Vamos considerar o caso $n = 1$. Como os polinômios são funções contínuas, para cada T, ou $\Omega_{M,T}$ é finito ou contém um aberto. Se para todo T, $\Omega_{M,T}$ é finito temos

$$\dim_H F = \sup_{1 \leq T < \infty} \{\dim_H \Omega_{M,T}\} = 0$$

Por outro lado se existe T tal que $\Omega_{M,T}$ contém um aberto, e assim, um intervalo aberto B de $\mathbb{R}$. Então, se $m > 1$, $\mathcal{L}^m(B) = 0$ e para $m < 1$, $\mathcal{H}^m(B) = \infty$. Logo, pelo lema (4.5) $\dim_H \Omega_M = 1$. O caso $n > 1$ é análogo, pois se existe T tal que $\Omega_{M,T}$ não é finito, então $\Omega_{M,T}$ contém uma bola aberta B de $\mathbb{R}^m$ para algum $m \leq n$, m maximal. Neste caso, $\mathcal{L}^s(B) = 0$ se $s > m$ e $\mathcal{L}^s(B) = \infty$ se $s < m$, ou seja, pelo lema (4.5) $\dim_H \Omega_{M,T} = m$. Mas como

$$\begin{aligned} \dim_H \Omega_M &= \sup_{0 \leq i < \infty} \{\dim_H \Omega_{M,T}\} \\ &= \max\{m \in \mathbb{N} : \exists\, T \in \mathbb{R}\ \Omega_{M,T} \text{ contém uma bola de } \mathbb{R}^m\} \end{aligned}$$

Problema. Como completar a demonstração para os casos $n > 1$? □

B. Recursividade e dinâmica

Uma consequência imediata da relação entre recursividade e dimensão expressa pelo teorema (4.6) é a grande variedade de exemplos de conjuntos não recursivos que podem ser encontrados na teoria de sistemas dinâmicos. Alguns dos exemplos mais notáveis, além dos atratores com dimensão de Hausdorff não inteira, são o conjuntos que aparecem com frequência em fenômenos dinâmicos envolvendo iterações de funções complexas, como conjuntos Julia e o conjunto de Mandelbrot.

Esta seção não é uma exposição sobre a teoria de sistemas dinâmicos discretos, nem um levantamento dos principais resultados sobre o assunto. Vamos apenas rever um pouco da teoria básica dos conjuntos de Julia e Mandelbrot com o objetivo de fornecer os ingredientes necessários para mostrar que o conjunto de Mandelbrot é não-recursivo sobre os reais (cf. [**Ma**]), assim como alguns conjuntos de Julia. Este último fato pode ser estabelecido mostrando alguns exemplos de conjuntos de Julia com dimensão de Hausdorff não inteira. Este mesmo resultado também pode ser obtido como corolário da solução de um outro problema tratado em [**BSS**] que é o de caracterizar topologicamente quais conjuntos de Julia são recursivamente enumeráveis sobre os reais.

As referências básicas para os resultados sobre conjuntos de Julia e Mandelbrot esboçados aqui são [**Bl**], [**Br**] e principalmente [**Fa**].

Seguindo [**FA**] vamos considerar os caso de sistemas dinâmicos gerados por polinômios $f : \mathbb{C} \to \mathbb{C}$ de grau $n \geq 2$ com coeficientes complexos[15], ou seja, sistemas dinâmicos gerados pela aplicação repetida (iteração) de funções $f(z)$. Assim, dado um ponto $w \in \mathbb{C}$, a **órbita** de w é a sequência $(z_n)_n$ definida indutivamente por $z_{n+1} = h(z_n)$. Se $z_1 = h(w)$, vamos denotar z_{k+1} por $h^{\circ(k+1)}(w)$.

Um ponto z_0 é **periódico de período** k se $z_k = z_0$ e $z_j \neq z_0$ para $0 < j < k$. Neste caso a órbita de z_0 é chamada **ciclo**.

Para um ponto periódico z_0 de perído k definimos o *autovalor* ρ *de* z_0 como a derivada de $h^{\circ k}$ em z_0. Usando a regra da cadeia temos

$$\rho = (f^{\circ k})'(z_0) = \prod_{j=0}^{k-1} f'(z_j),$$

o que mostra que a derivada de $f^{\circ k}$ é a mesma em todos os pontos do ciclo.

O comportamento das órbitas dos pontos próximos de um ponto periódico z_0, analisados através da série de Taylor de f em torno de z_0, sugere a seguinte definição. O ponto w (ou o ciclo) é chamado de:

(1) **atrator** se $|\rho| < 1$,

(2) **superatrator** se $\rho = 0$,

(3) **repulsor** se $|\rho| > 1$,

(4) **neutro** se $|\rho| = 1$.

A principal questão relacionada ao estudo de sistemas dinâmicos gerados pela iteração de polinômios complexos é a de determinar o comportamento da órbita de um ponto w qualquer, ou em outras palavras, determinar a estrutura das órbitas. De maneira análoga, para uma família de polinômios, o principal problema é determinar como o comportamento da órbita de um determinado ponto varia conforme os parâmetros (cf. [**Br**], [**Bl**]).

Dado um polinômio f o **conjunto de Julia** $J(f)$ de f pode ser definido como sendo o fecho do conjunto dos pontos periódicos repulsores de f. O complemento de $J(f)$ é chamado **conjunto de Fatou**, ou **conjunto estável** e denotado por $F(f)$.

Se $f(z) = z^2$, então $f^{\circ k}(z) = 2^{2^k}$ e os pontos satisfazendo $f^{\circ k}(z) = z$ são os pontos de $\{\exp(2\pi i p/(2^k - 1)) : 0 \leq p \leq 2^k - 2\}$, que são repulsores, pois $|(f(z)^{\circ k})'(z)| = 2$ nestes pontos. Então $J(f)$ é o círculo unitário $|z| = 1$. Além disso $J(f) = f(J(f)) = f^{-1}(J(f))$ e, se $|z| < 1$, $f^{\circ K}(z) \to 0$ quando $K \to \infty$, e se $|z| > 1$, $f^{\circ K}(z) \to \infty$ quando $K \to \infty$. Assim o conjunto de Julia de f é a fronteira entre o conjunto de pontos cujas órbitas tendem a 0 e para ∞. Neste caso $J(f)$ é bastante simples, mas

[15] Deve-se observar que a teoria permanece válida se f é uma função racional sobre o plano complexo extendido $\mathbb{C} \cup \{\infty\}$ ou se f é uma função meromórfica sobre $\mathbb{C} \cup \{\infty\}$. Nestes casos, poucos resultados não são mais válidos, mas os principais continuam válidos (cf. [**Bl**]).

em geral o conjunto de Julia é extremamente complicado, com dimensão de Hausdorff não inteira.

Para estabelecer algumas propriedades dos conjuntos de Julia é inevitável falar sobre famílias normais e um teorema devido a Montel (teorema 4.8).

Se U é um aberto em $\mathbb{C}$ e $g_k : U \to \mathbb{C}$ é uma família de funções analíticas complexas, então g_k é **normal sobre U** se qualquer sequência de funções de $\{g_k\}$ possui uma subsequência de funções que converge uniformemente, ou a uma função analítica limitada ou para ∞, sobre qualquer subconjunto compacto de U, . A família $\{g_k\}$ é **normal em** $w \in U$ se existe uma vizinhança V de U que contém w e $\{g_k\}$ é normal em V.

Se considerarmos a esfera de Riemann, i.e. o plano compactificado $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$, então uma família de funções meromórficas $\{f_k\} : U \subset \hat{\mathbb{C}} \to \hat{\mathbb{C}}$ é normal se, e somente se, é **eqüicontínua** sobre qualquer subconjunto compacto de U (cf. [**Ah**]). Isto significa que se $\{f^{\circ k}\}$ é normal então pontos suficientemente próximos não divergem sobre iteração.

Dado um polinômio $f : \mathbb{C} \to \mathbb{C}$ seja $J_0(f)$ definido por

$$J_0(f) = \{z \in \mathbb{C} : \text{ a família } \{f^{\circ k}(z)\} \text{ não é normal em } z\}$$

É imediato que o complemento

$$\begin{aligned} F_0(f) \equiv & \mathbb{C}/J_0(f) \\ = & \{z \in \mathbb{C} : \text{ existe um aberto } V \text{ com} \\ & z \in V \text{ e } \{f^{\circ k}\} \text{ é normal em } V\} \end{aligned}$$

é aberto, e portanto $J_0(f)$ é fechado.

Proposição 4.7. $J_0(f) = f(J_0(f)) = f^{-1}(J_0(f))$.

Demonstração. Vamos mostrar que o complemento $F_0(f)$ é invariante. Seja V um aberto com $\{f^{\circ k}\}$ normal em V e $\{f^{\circ k_i}\}$ uma subsequência de $\{f^{\circ k}\}$. Então $\{f^{\circ(k_i+1)}\}$ possui uma subsequência $\{f^{\circ(k_i'+1)}\}$ que é uniformemente convergente sobre subconjuntos compactos de V. Como f é contínua, $f^{-1}(V)$ é aberto. Então se D é um subconjunto compacto de $f^{-1}(V)$, $\{f^{\circ(k_i'+1)}\}$ é uniformemente convergente sobre o compacto $f(D)$, e assim $\{f^{\circ(k_i')}\}$ é uniformemente convergente sobre D. Então $\{f^{\circ k}\}$ é normal sobre $f^{-1}(V)$, i.e., $F_0(f) \subset f^{-1}(F_0(f))$. As outras inclusões são similares lembrando que se V é aberto, $f(V)$ é aberto pelo teorema da função aberta. □

O seguinte teorema é essencial para derivar propriedades sobre J_0.

Teorema 4.8. (**Montel**) Seja $\{g_k\}$ uma família de funções analíticas complexas sobre um domínio aberto U. Se $\{g_k\}$ não é uma família normal, então para todo $w \in \mathbb{C}$ com no máximo uma exceção, temos $g_k(z) = w$ para algum $z \in U$ e algum k.

Uma consequência deste resultado é que vizinhanças de pontos em J_0 são espalhadas pelas iterações preenchendo o plano complexo todo, com exceção possivelmente de um ponto.

Proposição 4.9. Seja f um polinômio, $w \in J_0(f)$ e U uma vizinhançqualquer de w. Então $W \equiv \cup_{k=1}^{\infty} f^{\circ k}(U)$ é o plano complexo todo com exceção possivelmente de um único ponto v. Além disso $v \notin J_0(f)$ e v é independente de w e U.

Demonstração. Pela definição de J_0, a família $\{f^{\circ k}\}$ não é normal em w e, pelo teorema de Montel, a primeira afirmação é imediata.

Vamos supor $v \notin W$. Se $f(z) = v$, como $f(W) \subset W$, $z \notin W$. Como $\mathbb{C}/W$ consiste de no máximo um ponto, $z = v$. Então f é um polinômio de grau n tal que a única solução de $f(z) - v = 0$ é v, ou seja, $f(z) - v = c(z - v)^n$ para alguma constante c.

Se z é suficientemente próximo de v, então $f^{\circ k}(z) - v \to 0$ quando $k \to \infty$, e a convergência é uniforme sobre $\{z \in \mathbb{C} : (z - v) < (2c)^{-1/(n-1)}\}$. Então $\{f^{\circ k}\}$ é normal em v, ou seja, $v \notin J_0(f)$ e claramente v depende apenas de f. $\square$

Uma consequência imediata deste resultado é que se $\mathrm{int}(J_0) \neq \emptyset$ então $J_0 = \mathbb{C}$, pois se $w \in \mathrm{int}(J_0)$ existe U aberto em $\mathrm{int}(J_0)$ e pela invariância de J_0, $J_0 \supset \cup_{n \in \mathbb{N}} f^{\circ n}(U) \supset \mathbb{C} - \{E\}$, onde E contém no máximo um ponto. Como J_0é fechado, $J_0 = \mathbb{C}$. Pode-se derivar, a partir da caracterização de famílias normais dada pelo teorema de Montel, algumas outras propriedades de J_0, como por exemplo,

- $J_0(f)$ é não vazio
- $J_0(f) = J_0(f^{\circ p})$ para qualquer inteiro positivo p.
- $J_0(f)$ é um conjunto perfeito, i.e, $J_o(f)$ é fechado e sem pontos isolados.

A partir disto pode-se provar o seguinte teorema (clássico).

Teorema 4.10. Se f é um polinômio[16], $J_0(f) = J(f)$.

[16]Este resultado também vale no caso de funções racionais cf. [**Bl**].

Corolário 4.11. Seja A um subconjunto fechado de $\hat{\mathbb{C}}$ tal que $A \cup \hat{\mathbb{C}}/W = \emptyset$, onde W é o conjunto definido pela proposiç ao (4.9). Dado uma vizinhança U de um ponto $p \in J$, existe um inteiro N tal que $A \subset g^{\circ N}(U)$. Portanto se D é um conjunto aberto conexo e $D \cap J \neq \emptyset$, então exist N tal que $f^N(D \cap J) = J$.

Demonstração. Seja $w \in U$ um ponto repulsor de período n e V uma vizinhança de w tal que $V \subset U$ e $V \subset g^{\circ n}(V)$. Como $A \cap \hat{\mathbb{C}}/W = \emptyset$ e $w \in J(g)$,

$$A \subset \bigcup_{k=1}^{\infty} g^{\circ kn}(V)$$

Por construção $g^{\circ n}(V) \subset g^{\circ 2n}(V) \subset g^{\circ 3n}(V) \subset \ldots$, e como A é compacto, $A \subset g^{\circ N}(V) \subset g^{\circ N}(U)$ para algum $N = kn$. □

Como consequência deste teorema, dado um polinômio f, existe um $\delta > 0$ tal que para qualquer $x \in J(f)$ existem pontos $y \in J(f)$ arbitrariamente próximos de x tal que $|f^{\circ k}(x) - f^{\circ k}(y)| \geq \delta$ para algum k. Neste caso dizemos que f **sensivelmente dependente das condições iniciais.** Além disso, por definiç ao, os pontos periódicos de f são densos em $J(f)$. Também é possível mostrar (Proposição (4.11)) que $J(f)$ contém pontos z cuja órbita é densa em $J(f)$. Estas três condições caracterizam **o comportamento caótico da ação de f sobre** $J(f)$. Assim, dado um polinômio f, podemos decompor o **plano dinâmico de** f, i.e., $\mathbb{C}$, em dois conjuntos disjuntos, o conjunto de Julia de f, no qual a dinâmica é caótica, e o conjunto de Fatou, no qual a dinâmica é bem comportada.

Dado um polinômio f, pode-se decompor o plano dinâmico em três outros subconjuntos disjuntos: o conjunto dos pontos com órbitas limitadas $K_f =_{\text{def}} \{z \in \mathbb{C} : \lim_{k\to\infty} f^{\circ k}(z) \neq \infty\}$, o conjunto dos pontos com órbitas não limitadas $A_f(\infty) =_{\text{def}} \mathbb{C}/K_f = \{z \in \mathbb{C} : \lim_{k\to\infty} f^{\circ k}(z) = \infty\}$, e a fronteira $\partial A_f = \partial K_f$.

Se $w \in K_f$ ou $w \in A_f$ então como w é atrator, existe um aberto V contendo w em K_f ou em A_f (no caso $w = \infty$ tomamos $\{z : |z| > r\}$ para r suficientemente grande). Isto implica que K_f e A_f são abertos, pois $f^{\circ k}(z) \in V$ para algum k, i.e., $zinf^{-1}(V)$, que é aberto.

Proposição 4.12. $J(f) = \partial K_f = \partial A_f$.

Demonstração. Se $z \in J(f)$ então existe uma vizinhança aberta U de z em $J(f)$, e pela proposição (4.9) o conjunto $f^{\circ k}(U)$ contém pontos de A_f para algum k (A_f é aberto e portanto contém obviamente mais de um ponto). Então existem pontos de A_f arbitrariamente próximos a z, ou seja $z \in \partial A_f$.

Vamos supor que $z \in \partial A_f$ mas $z \notin J(j) = J_0(f)$. Então z possui uma vizinhança U sobre a qual $\{f^{\circ k}\}$ é normal em U. Isto significa que z possui uma vizinhança aberta conexa V sobre a qual $\{f^{\circ k}\}$ tem uma subsequência convergente ou a uma função analítica, ou a ∞. A subsequência converge para um ponto em $V \cap (K_f \cup A_f)$, que é aberta e não-vazia, e portanto sobre V, pois uma função analítica é constante sobre um conjunto conexo se é constante sobre qualquer subconjunto aberto. Como $\cup_k f^{\circ k}(V) \subset A_f \cup K_f$, temos $V \subset A_f \cup K_f$, contradizendo que $z \in \partial K_f$. □

Seja w um ponto fixo de f, i.e., $f(w) = w$. A **bacia de atração de** w é o conjunto

$$A(w, f) =_{\text{def}} \{z \in \mathbf{C} : f^{\circ k}(z) \to w \text{ quando } k \to \infty\}$$

De maneira análoga definimos $A(\infty, f)$. A **bacia de atração imediata de** w, denotada por $A^*(w, f)$ é o conjunto aberto conexo maximal que contém w tal que $\{f^{\circ k}\}$ é normal sobre $A^*(w, f)$. É claro que $A^*(w) \subset A(w)$ (vamos omitir f quando possível).

No caso em que o conjunto de Julia de um polinômio possui pelo menos dois pontos fixos atratores é possível mostrar (cf. [**Br**]) sobre algumas condições, que J consiste de curvas de Jordan, i.e., curvas simples e fechadas. Mais precisamente, se w e v são pontos fixos atratores de $J(f)$ com $A^*(w) = A(w)$ e $A^*(v) = A(v)$, então $J(f)$ é uma curva de Jordan. Além disso, se $A^*(w) = A(w)$ para um único ponto fixo atrator w, e $J(f) \cap \overline{C} = \emptyset$, onde $\overline{C}$ é o fecho do conjunto dos pontos críticos das funções $\{(f^{-1})^{\circ n}\}$, então $J(f)$ contém um número infinito de curvas de Jordan. Em [**Br**], Brolin obtém mais informações sobre estas curvas:

Proposição 4.13 Se w é um ponto fixo atrator de f e,

(1) $A^*(w)$ é simplesmente conexo,

(2) $\partial A^*(w)$ é uma curva de Jordan analítica ou um arco analítico, então $\partial A^*(w)$ é um círculo ou um arco de um círculo.

Proposição 4.14. Se w é um ponto fixo atrator de f e

(1) $A^*(w)$ é simplesmente conexo,

(2) $\partial A^*(w) \cap \overline{C} = \emptyset$, então, se $\partial A^*(w)$ não é um círculo nem uma reta, $\partial A^*(w)$ não tem tangente em nenhum ponto.

As provas destas proposições não são fáceis e dependem de uma série de outros resultados sobre conjuntos de Julia. O que nos interessa aqui é que podemos combinar os resultados obtidos sobre os conjuntos de Julia e caracterizar topologicamente os conjunros de julia que são recursivamente enumeráveis sobre os reais (teorema (4.17)).

Um conjunto D é **completamente invariante** se $F(D) = D$ e $f^{-1}(D) = D$

É possível mostrar (cf. [**Bl**]) que o conjunto de Fatou não pode ter mais do que duas componentes simplesmente conexas diferentes e totalmente invariantes. Consequentemente, como a fronteira é um subconjunto de J não vazio, fechado e completamente invariante, ela deve ser J.

Usando técnicas bastante sofisticadas (cf. [**Bl**]), Sullivan completou a classificação das possibilidades dinâmicas do conjunto de Fatou de uma função meromórfica. Vamos apenas enunciar os resultados que caracterizam as possibilidades dinâmicas do conjunto de Fatou.

Uma componente conexa D é **periódica**[17] se existe um m tal que $f^{\circ m}(D)$ é periódica, ou seja, existe n tal que $f^{\circ n}(f^{\circ m}(D)) = f^{\circ m}(D)$.

Teorema 4.15. (**Sullivan**) Qualquer componente do conjunto de Fatou é eventualmente periódica

Um **domínio de Sullivan** de uma função racional $g : \hat{\mathbb{C}} \to \hat{\mathbb{C}}$ é uma componente conexa periódica do conjunto $F(g)$.

Assim para entender a dinâmica do conjunto de Fatou basta considerar domínios de Sullivan, e o segundo teorema de Sullivan classifica os domínios de Sullivan em cinco comportamentos possíveis.

Definição. Seja D um domínio de Sullivan de período n e $S = g^{\circ n}$. Então,

(1) D é um **domínio atrator** se D contém um ponto periódico p tal que $0 < |S'(p)| < 1$ e $D = A^*(p, S)$

(2) D é um **domínio superatrator** se D contém um ponto periódico p tal que p é um ponto crítico de S e $D = A^*(p, S)$.

(3) D é um **domínio parabólico** se existe um ponto periódico p em ∂D cujo período divide n e $S^{\circ k}(z) \to p$ quando $k \to \infty$ para todo $z \in D$.

(4) D é um **disco de Siegel** se D é simplesmente conexo e D é analiticamente conjugado a uma rotação.

(5) D é um **anel de Herman** se D é conformalmente equivalente a um **annulus** $A = \{z \in \mathbb{C} : 0 \leq r_1 < |z| < r_2, r_1, r_2 \in \mathbb{R}\}$ e a função $S|_D$ é analiticamente conjugada a uma rotação rígida de A.

Teorema 4.16. (**Sullivan**) Qualquer domínio de Sullivan é de um dos conco tipos acima. Além disso,

(1) qualquer conjunto de Fatou possui um número finito desses domínios,

(2) no caso parabólico $S'(p) = 1$,

(3) os domínios parabólicos e atratores contém infinitas órbitas positivas de pontos críticos,

[17] *eventualy periodic.*

(4) as fronteiras dos domínios de rotação estão contidas no fecho das órbitas positivas dos pontos críticos.

Teorema 4.17. ([**BSS**]) Seja $g : \hat{\mathbb{C}} \to \hat{\mathbb{C}}$ uma função racional. Se $J(g)$ é recursivamente enumerável sobre o corpo dos reais, então $J(g)$ satisfaz um dos seguintes ítens,

(1) $J(g) = \emptyset$ e neste caso g é uma rotação ou uma constante,

(2) $J(g)$ consiste de um único ponto e g é uma transformação linear fracionária mas não uma rotação,

(3) $J(g)$ é um arco analítico real, e neste caso, se os pontos fixos de g são hiperbólicos, o arco é o arco de um círculo,

(4) $J(g)$ é uma curva de Jordan analítica real, e no caso hiperbólico $J(g)$ é um círculo,

(5) $J(g) = \hat{\mathbb{C}}$.

Demonstração (esboço). Pelo corolário (4.11) é possível mostrar que ou J é conexo ou possui um número não enumerável de componentes conexas. Como J é uma união enumerável de conjuntos semialgébricos básicos, e cada um possui um número finito de componentes conexas, J deve ser conexo. Se $\mathrm{int}(J) \neq \emptyset$, então $J = \hat{\mathbb{C}}$. Se J é vazio ou consiste de um único ponto segue-se que o grau de g é 1 ou 0 e os casos (a) e (b) são triviais. Então vamos considerar o caso onde J é uma união enumerável de conjuntos semialgébricos básicos que podemos assumir que são fechados. Como corolário do teorema de Baire, existe pelo menos um desses conjuntos fechados que possui interior não vazio. Então podemos encontrar um arco analítico real I neste conjunto e, novamente pelo corolário (4.11), um $n_0 \geq 0$ tal que $g^{\circ n_0}(I) = J$. Mas se I tem ramos ou se cruza, então I possui um número finito de ramos e de pontos de cruzamento. Mas pelo corolário (4.11) os ramos e os pontos de cruzamento devem ser densos, um absurdo. Logo I é ou um arco analítico ou uma curva de Jordan analítica.

Faltam os casos (c) e (d) no caso de pontos fixos hiperbólicos. Sabemos que o complemento de J possui no máximo duas componentes simplesmente conexas totalmente invariantes. Pelo teorema (4.16) estas componentes são bacias de atração de um ponto hiperbólico e pelas proposições (4.13) e (4.14) concluímos a demonstração. □

Vamos passar a definição do conjunto de Mandelbrot.

Se $\Omega(f)$ é o conjunto dos pontos críticos de um polinômio f, então é possível mostrar que $\Omega(f) \subset K_f$ se, e somente se, $J(f)$ é conexo e, se $\Omega(f) \cap K_f = \emptyset$, então $J(f)$ é um conjunto totalmente desconexo, compacto e perfeito, i.e., homeomorfo ao conjunto de Cantor. No caso de polinômios quadráticos existe apenas um ponto crítico, logo, J é conexo ou homeomorfo ao conjunto de Cantor. esta dicotomia determina uma decomposição natural do plano de parâmetros.

Seja $f_c(z) = z^2 + c$. É fácil ver que qualquer polinômio quadrático pode ser conjugado analiticamente a um polinômio da forma $p(z) = z^2 + c$ (cf. [**Fa**]). Como consequência, para estudar o conjunto de Julia de polinômios quadráticos é suficiente estudar a classe dos polinômios da forma $p(z) = z^2 + c$.

Definição. O **conjunto de Mandelbrot** M é definido por:

$$M =_{def} \{c \in \mathbb{C} : J(f_c) \text{ é conexo}\}$$

Um resultado clássico é que

$$\begin{aligned} M &= \{c \in \mathbb{C} : \lim_{n\to\infty} P_c^{\circ n}(0) \not\to \infty\} \\ &= \{c \in \mathbb{C} : c, c^2 + c, (c^2 + c)^2 + c, \ldots \not\to \infty\} \end{aligned}$$

O conjunto de Mandelbrot possui uma quantidade enorme de informação acerca dos conjuntos de Julia $J(f_c)$, mas como observa Branner [**Br**], não é trivial a partir desta definição, que as componentes de $\mathbb{C} - \partial M$ determinam de fato a decomposição do plano de parâmetros em regiões com comportamentos dinâmicos qualitativamente diferentes, e que a fronteira de M é o conjunto de bifurcação, i.e., o conjunto dos pontos para os quais o comportamento dinâmico muda qualitativamente. Mas preferimos não nos deter nesta discussão e sugerimos [**Br**] ou [**Fa**] onde outras referências a esta questão podem ser encontradas. Vamos caminhar num outro sentido.

Cabe observar aqui que, devido a um resultado de Ruelle (cf. [**Fa**]),

$$\dim_H J(f_c) = 1 + |c|^2/4 \log 2 + \text{ termos em } |c|^3 \text{ e potências maiores}$$

e $\dim_H J(f_c)$ é uma função analítica real de c. Isto mostra que muitos conjuntos de Julia não são recursivamente enumeráveis sobre os reais.

Um ponto c é chamado de **ponto de Misiurewicz** se a órbita de 0 sobre f_c é estritamente préperiódica, i.e., se $z_0 = f_c(0)$, então $z_{k+l} = z_l$ para algum $K \geq l$ e $l > 0$. Por exemplo, se $c = i$ então c é um ponto de Misiurewicz. É possível mostrar que se c é um ponto de Misiurewicz $J(f_c)) = K_{f_c}$.

Seja $f_n : \mathbb{C} \to \mathbb{C}$ uma família de funções definida indutivamente por

$$f_1(c) = c, \qquad f_n(c) = (f_{n-1}(c))^2 + c$$

Então, dado c a sequência $0, f_1(c), f_2(c), \ldots$ é aórbita de 0 sobre f_c. Se $r = \max(2, |c|)$ então para $|z| > r$, $|P_c(z)|/|z| > 1$. Se $|c| > 2$, então $|f_1(c)| > 2$ e então $f_n(c) \to \infty$ quando $n \to \infty$. Assim, para $c \in \mathbb{C} - M$ temos $f_n(c) \to \infty$, e para $c \in M$ temos $|f_n(c)| \leq 2$. Então para qualquer vizinhança U família $f_n|_U : U \to \mathbb{C}$ não é normal.

Proposição 4.18. Os pontos de Misiurewicz são densos na fronteira de M.

Demonstração. Seja $c_0 \in \partial M$ e $c_0 \neq 1/4$. Supondo que a afirmação é falsa, é possível escolher uma vizinhança U simplesmente conexa de c_0 tal que U não contém $1/4$ e nenhum ponto de Misiurewicz c tal que a órbita de 0 sobre f_c contém um ponto fixo. Como U é simplesmente conexo e $1/4 \notin U$, podemos escolher $g_1, g_2 : U \to \mathbb{C}$ como sendo dois ramos da raíz $\sqrt{1-4c}$. Então $f_n(c)$ omite três pontos:

$$h_1(c) = 1/2 + g_1(c), \qquad h_2(c) = 1/2 + g_2(c) \qquad \text{e} \qquad \infty$$

Os dois pontos h_1 e h_2 são pontos fixos distintos de f_n que coincidem somente se $c = 1/4$. Por uma construção usual obtemos uma família $F_n : U \to \hat{\mathbb{C}}$ que omite 0, 1 e ∞, ou seja

$$F_n = \frac{f_n - h_1}{h_2 - h_1}$$

A família $\{F_n\}$ é normal e portanto $\{f_n\}$ é normal, o que é um absurdo. □

Teorema 4.19. O conjunto de Mandelbrot não é recursivamente numerável sobre os reais.

Demonstração (esboço). Existem pelo menos duas demonstrações parciais deste resultado. Uma devida a Blum e a Smale [**BS**], e outra devida a Mansfield [**Ma**]. Mas ambas dependem de hipóteses não demonstradas que são, segundo estes autores, certamente verdadeiras[18]:

- *Hipótese de* [**BS**]: $\dim_H(\partial M) > 1$.

Com base nesta hipótese, se M é enumerável recursivamente sobre $\mathbb{R}$ então M é uma união enumerável de conjuntos semialgébricos básicos de $\mathbb{R}$. Como M é fechado e o fecho de conjuntos semialgébricos básicos é um conjunto semialgébrico básico, podemos supor

$$M = \bigcup_{i=1}^{\infty} S_i$$

onde cada $S_i \subset \mathbb{C} \equiv \mathbb{R}^2$ é semialgébrico básico e fechado. Se $\dim_H S_i \leq 1$ então $\dim_H(\partial M \cap S_i) \leq 1$. Por outro lado, se $\dim_H S_i > 1$, então $\dim_H S_i = 2$, e assim $\dim_H(\partial M \cap S_i) \leq 1$. Como S_i é fechado, $\dim_H \partial S_i \leq 1$. Além disso como $\text{int}(S_i) \subset \text{int}(M)$, temos

$$\dim_H(\partial M \cap S_i) \leq \dim_H(\partial M \cap \partial S_i) \leq 1$$

[18]Foi demonstrado recentemente por Shishimura que a dimensão de Hausdorff de ∂M é igual a 2.

ou seja,

$$\dim_H \partial M = \sup_{1\leq i \leq \infty} \{\dim_H(\partial M \cap S_i)\} \leq 1$$

contradizendo a hipótese inicial.

- *Hipótese de* [**Ma**]: $\dim_H(\partial M \cap U)$ não é inteira para qualquer aberto U.

Observe que se M é enumerável recursivamente sobre $\mathtt{R}$ e $w \in \partial M$ e w satisfaz somente inequações estritas, então existe um aberto U que contém w e U também satisfaz estas inequações, ou seja, existem pontos $z \in \mathtt{C}-M$ que pertencem ao conjunto de parada da máquina que define M, que é um absurdo. Assim, para mostrar que M não é enumerável recursivamente sobre $\mathtt{R}$, basta mostrar que, para qualquer lista $a_1, \ldots, a_n \in \mathtt{R}$ de parâmetros existe um ponto (x_0, y_0) na fronteira de M (e portanto em M) tal que (x_0, y_0) não satisfaz nenhuma equação polinomial da forma $p(x,y) = 0$, onde p é um polinômio sobre $\mathtt{Q}(a_1, \ldots, a_n)$. Suponha o contrário, i.e., existe uma lista de parâmetros tal que qualquer ponto da fronteira satisfaz alguma equação algébrica sobre esta lista. Então ∂M está contida numa união enumerável de curvas algébricas. Mas pelo teorema de Baire, como M é fechado e portanto completo, alguma destas curvas algébricas tem interior em M não vazio, digamos C_n. Isto significa que existe um aberto $U \subset \mathtt{R}^2$ tal que $U \cap \partial M = U \cap C_n$. Mas $\dim_H(U \cap \partial M)$ não é inteira pela hipótese assumida, enquanto que curvas algébricas tem dimensão de Hausdorff igual a 1. □

Acreditamos que a evidência para ambas as afirmações acima provém de um resultado de Tan Lei (cf. [**Br**]) de que em torno de um ponto de Misiurewicz c os conjuntos $J(f_c)$ e ∂M são "similares". Como a dimensão de Hausdorff de $J(f_c)$ é não-inteira então, como os pontos de Misiurewicz são densos na fronteira de M (proposição (4.18)), $\dim_H(\partial M \cap U)$ também não é inteira para qualquer U.

Em [**dCD8**], da Costa e Doria observam que alguns teoremas intuitivamente óbvios, como por exemplo o Teorema da Curva de Jordan, possuem demonstrações bastante complicadas. Segundo estes autores,

> How comes that the strict mathematical proof for those "intuitively obvious" facts is so involved? To answer it in a nutshell: mathematics restricts its proof tools to *digital*, discrete, stepwise techniques, while we have used here some kind of *analog-like* arguments.

A partir destas observações pode-se formular uma teoria de computação, chamada de H-computação, que assume como computável o seguinte processo geométrico:

Princípio geométrico. Sempre podemos decidir quando duas curvas diferenciáveis [*smooth*] têm um ponto em comum numa região limitada por um retângulo.

É fácil ver, usando as traduções de Richardson que a função de parada θ é H-computável.

Por outro lado, os teoremas (4.17) e (4.18) sugerem que conjuntos topologicamente muito complicados, como por exemplo os conjuntos de Julia que não satisfazem as condições do teorema (4.17), não são recursivos sobre os reais. É difícil não notar uma certa semelhança entre a simplicidade dos conjunto recursivos sobre os reais, pelo menos nestes exemplos, e o princípio geométrico acima.

Problema 7. H-computação e computabilidade sobre os reais são equivalentes?

Note que o princípio geométrico é muito mais justificável como um processo computável do que computabilidade sobre os reais.

5. Conclusão e Algumas Observações Inconclusas

Como vimos no capítulo II, a observação de Arnold à solução negativa, proposta por da Costa e Doria, do seu problema sobre estabilidade de Lyapunov, pressupõe a possibilidade de um *processo* que ainda pode ser chamado de *computável*, e além disso, este 'algoritmo analítico', como é denominado por Arnold, não é equivalente a uma máquina de Turing, e seria mais adequado para tratar esse problema.

A idéia de 'ser mais adequado' já pressupõe, como foi observado no capítulo II, em que sentido uma solução é esperada. Combinando então estas observações, pode-se induzir que existe uma noção intuitiva de um processo que ainda pode ser chamado de computável e que não é Turing-computável.

Na verdade isto não contradiz a Tese de Church, de que o que pode ser efetivamente computável é computável por uma máquina de Turing, pois como observa Gandy [**Ga**], num trabalho excepcional, (e também Kreisel [**Kr 1**]), 'efetivamente computável' significa 'o que pode ser calculado por um ser humano abstrato', e além disso, a análise de Turing em [**T**], fornece argumentos para o seguinte 'Teorema': *o que pode ser efetivamente calculado por um 'ser humano abstrato' é computável*. Mas não para a tese de que *o que pode ser calculado por um mecanismo é Turing-computável*.

A palavra 'abstrato' usada aqui, indica, conforme Gandy, que o argumento não faz nenhum apelo a limitações físicas de tempo ou espaço. A palavra 'efetiva' significa que o processo é determinista e que deve terminar em um tempo finito. Deixando um pouco a parte as objeções de Gödel à análise de Turing[19], que podem ser justificadas apenas através de uma 'teoria da inteligência' (discutidas por exemplo em [**We**], [**Kr 3**] ou [**Wa**]), pode-se mostrar, como faz Gandy, que alguns passos cruciais da análise de Turing não se sustentam com a hipótese de que o cálculo está sendo feito por um mecanismo. Portanto, como já foi observado, a análise Turing não fornece argumentos para o seguinte:

Tese M. O que pode ser computável por um mecanismo é computável por uma máquina de Turing.

[19] Mas não esquecendo que talvez tenha sido Gödel o primeiro a chamar a atenção para a possibilidade de que o conceito formal de computabilidade, obtido através da análise de Turing, seja insuficiente para capturar todos os processos mentais que poderiam ser chamados de computáveis.

O que Gandy faz é limitar o significado de mecanismo[20], que é muito geral, definindo quatro *princípios para mecanismos* que têm por objetivo capturar formalmente a noção geral de um dispositivo mecânico determinista no qual o processo de cálculo pode ser descrito em termos discretos. A partir disso, pode-se enunciar uma versão mais definida da Tese M,

Tese P. Qualquer dispositivo mecânico determinista discreto satisfaz os quatro princípios para mecanismos.

e demonstrar o seguinte teorema:

Teorema P. O que pode ser calculável por um dispositivo satisfazendo os princípios I-IV é Turing-computável.

Não nos parece muito difícil intuir que o conceito de computabilidade sobre estruturas abstratas constitui um mecanismo, pois, como vimos no capítulo III, a análise de Friedman dos conceitos de FAP, MTg mostra que a ação simbólica destes dispositivos a cada *input*, visto como um termo formal, pode ser simulada por uma máquina de Turing usual (cf. a prova do teorema (3.2)). E o conjunto de todas as ações, ou 'órbitas' possíveis constitui um EDE, que é em essência uma relativização da definição de função recursiva parcial por casos. No caso de *prime* e *search* computabilidade, isto pode ser visto diretamente a partir da própria definição dessas classes de funções, pois nestes casos, basta notar que a análise de Kleene [**Kl1**] se aplica.

De fato, em [**Sh2**], Shepherdson modificou alguns dos princípios de Gandy e delimitou, através de quatro princípios $I' - IV'$, uma classe de mecanismos mais geral (incluindo por exemplo dispositivos que operam em paralelo e sobre estruturas abstratas totais e parciais) obtendo um resultado semelhante ao teorema P, reforçando o caráter mecanicista de uma MTg[21],

Teorema S. z/ Qualquer mecanismo que satisfaça os princípios I'-IV' é equivalente a uma MTg ou a uma MTg que opera em paralelo sobre todas as interpretações nas quais

[20] Mecanismo é um termo bastante impreciso, mas está sendo usado aqui para significar por exemplo, máquinas que operam um número arbitrário de símbolos simultâneamente, máquinas analógicas, teorias físicas mecanicistas no sentido de [**Kr2**], ou mesmo teorias físicas num sentido mais amplo (cf. [**Ga**]).

[21] Neste caso é necessário incluir operações em paralelo que não podem ser simuladas por um procedimento serial se as estruturas consideraradas forem estruturas parciais (cf. [**Sh1**]). Sendo assim, como uma MTg é um procedimento serial, ela não é mais universal e deve ser repassada por dispositivo que opera em paralelo.

ele é determinado.

Diante destes resultados acreditamos não ser totalmente discrepante afirmar que os critérios algébricos de Arnold constituem um mecanismo.Em vista disso, podemos formular a seguinte questão,

Problema 8. Os critérios algébricos de Arnold satisfazem os princípios de Shepherdson?

As dificuldades apontadas no capítulo III de se estabelecer de fato uma relação entre EDE's e as condições de *semialgebricidade* e *quase determinação finita* que definem estes critérios, constituem, em vista do teorema S, um obstáculo a uma possível solução positiva do problema acima.

Por outro lado, parece claro que se uma relação, ou propriedade P, definida sobre um conjunto U, é EDE-decidível, então existe uma lista enumerável (possivelmente finita) de condições φ_i tal que $x \in U \Leftrightarrow x$ satisfaz alguma φ_i. Se permitirmos quantificadores, como faz por exemplo [**Mos2**], então dependendo da uniformidade da fórmula φ_i em relação a i, a lista pode ser finita e então temos um resultado do tipo

$$P(x) \Leftrightarrow \varphi_i(x), \qquad (i = 1, \ldots, n) \tag{$*$}$$

Em outras palavras, $(*)$ é um *teorema* que determina condições necessárias e suficientes para que um dado $x \in U$ satisfaça P. Mas como P é genérica, *qualquer teorema desta forma possui um conteúdo algorítmico.* Se temos apenas condições necessárias, então P é pelo menos 'recursivamente enumerável', i.e., equivalente a algum EDE finito sobre alguma estrutura adequada.

Talvez, resolver o problema de Arnold signifique, em última análise, estabelecer um número finito condições necessárias e suficientes sobre os campos vetorias que determinam os sistemas considerados, que por sua vez caracterizam os sistemas onde temos estabilidade ou não[22]

Esta interpretação, relacionando teoremas que estabeçam condições necessárias e suficientes (i.e., teoremas de classificação completa) com algoritmos, pode parecer simplista, mas o próprio Arnold parece confirmar isto nos seguintes momentos,

- em resposta à solução negativa proposta por da Costa e Doria [**Ar4**], logo após a formulação de seu problema e termos de algoritmos analíticos:

[22] De acordo com esta interpretação, uma solução negativa envolvendo EDE's sobre uma certa estrutura, significa a impossibilidade de se estabelecer $(*)$ (mesmo no caso $i = 1, \ldots, \infty$) usando fórmulas semialgébricas básicas na linguagem desta estrutura. É claro que, para cada propriedade P, existe uma estrutura na qual P é EDE-decidível: basta declarar P como relação básica. Logo EDE-indecidibilidade geral nunca é possível. O problema então é qual estrutura escolher.

However as far as I know there are no words in logic to describe the above problem and I have thus preferred to stop at the level of algorithms in the usual sense rather than to try to explain to logicians the meaning of the impossibility of the solution of differential equations of a given type by quadratures[23] (e.g., in the Liouville case in classical mechanics or in the theory of second order ordinary differential equations). The main difficulty here is that the solvability or unsolvability should be defined in a way that makes evident the invariance of this property under admissible changes of variables defined by functions that one can construct from the right hand side of the equations in a given coordinate system. In other terms we should explicitly describe the structure of the manifold where the vectorfield is given, with respect to wich the equation is nonintegrable.

- num comentário a respeito do significado da solução negativa de Smale para o problema de classificação topológica de equações diferenciais [Ar3, p. 89]:

He [Smale] showed that for phase spaces of large dimension, systems exist in the neighborhood of which there is no structurally stable system. For the qualitative theory of differential equations this result has approximately the same significance as Liouville's theorem on the impossibility of solving differential equations by quadrature for the integration theory of differential equations. It shows that the problem of the complete topological classification of differential equations with high-dimensional phase space is hopeless even if restricted to generic equations and nondegenerate cases.

Diante destas observações, os teoremas sobre incompletude e indecidibilidade em teorias que extendem a Análise (corolários (1.17), (1.18) e proposições (1.19) e (1.20)) mostram uma vez mais que, computabilidade no sentido de Turing-computabilidade, num certo sentido, não é adequado para resolver um problema do tipo do de Arnold, por exemplo, pois não exclui a possibilidade de existência de um teorema do tipo (*) que é o tipo de solução esperada. Uma solução negativa, usando Turing-computabilidade, mostra apenas que alguma φ_i é indecidível. Isto é o que acontece, por exemplo, em (3.11).

Mesmo que nossas interpretações estejam corretas e a teoria de computabilidade sobre estruturas abstratas seja suficiente para os propósitos matemáticos, como os do tipo levantados por Arnold, é possível concebermos uma extensão genuína do conceito de computação, onde estes problemas possam ser resolvidos de forma satisfatória.

[23] Este é um resultado garantido pelo teorema de Liouville, ou seja, equações lineares de segunda ordem em geral, possuem soluções que não podem ser expressas em termos dos coeficientes por meio de operações aritméticas, soluções de equações algébricas (inclusive as não solúveis por radicais) exponenciação e integração.

Referências bibliográficas

[Ar1] V. I. Arnold, *Algebraic unsolvability of the problem of Lyapunov stability and the problem of topological classification of singular points of an analytic system of differential equations*, traduzido de Funk. Anal. i Ego Pril.**4**, (1970), 173-180.

[Ar2] V. I. Arnold, in *The Mathematics Arising from Hilbert's Problems*, Proc. Symp. Pure Math. **28**, (1976).

[Ar3] V. I. Arnold, *Geometrical Methods in the Theory of Ordinary Differential Equations*, segunda edição, Springer-Verlag, 1988.

[Ar4] V. I. Arnold, *e-mail message to FAD in* [**dCD7**].

[Ba] N. P. Bamber, *Computation with access to the reals but using only classical machines*, Lecture Notes in Comp. Science **713**, (1993), 97-107.

[BSS] L. Blum, M. Shub e S. Smale, *On a theory of computation and complexity over the real numbers: NP-completness, recursive functions and universal machines*, Bull. Amer. Math. Soc. **21**, (1989), 1-120.

[dCD1] N. C. A. da Costa e F. A. Doria, *Undecidability and Incompletness in Classical Mechanics*, Int. J. Theor. Phys. **30**, (1991), 1041-1073.

[dCD2] N. C. A. da Costa e F. A. Doria, *Classical Physics and Penrose thesis*, Found. Phys. Lettes **4**, (1991), 363-373.

[dCD3] N. C. A. da Costa e F. A. Doria, *Mathematics is dramatically incomplete*, (1992), preprint.

[dCD4] N. C. A. da Costa e F. A. Doria, *On Arnol'd's Hilbert Synposium problems*, Lecture Notes in Comp. Science **713**, (1993), 152-158.

[dCD5] N. C. A. da Costa e F. A. Doria, *Suppes predicades and the construction of unsolvable problems in the axiomatized sciences*, in *Patrick Suppes: Scientific Philosopher*, (P. Humphreys ed.), **2**, (1994), 151-193.

[dCD6] N. C. A. da Costa e F. A. Doria, *Undecidability, Incompleteness and the Arnol'd's problems*, Studia Logica **55**, (1995), 23-32.

[dCD7] N. C. A. da Costa e F. A. Doria, *Undecidable Hopf bifurcation with undecidable fixed point*, Int. Jour. Theor. Phys. **33**, (1994), 1885-1903.

[dCD8] N. C. A. da Costa e F. A. Doria, *Variations on an original theme*, apresentado no encontro sobre os "Limites do Conhecimento Científico" em Abisko, (1995).

[DMR] M. Davis, Y. Matijasevich e J. Robinson, *Hilbert's tenth problem. Doiphantine equations: positive aspects of a negative solution*, Proc. Symp. in Pure Math. **28**, (1976), 323-378.

[FM] H. Friedman e R. Mansfield, *Algorithmic procedures*, Trans. Am. Math. Soc. **332**, (1992), 297-312.

[Fr1] H. Friedman, *Algorithmic procedures, generalized Turing algorithms and elementary recursion theory*, in *Logic Colloquium 1969*, (R.O. Gandy and Yates eds.), North-Holland, (1971), 361-389.

[Fr2] H Friedman, *Algorithmic Procedures* , Trans. Am. Math. Soc.**332**, (1992), 297-312.

[Ga] R. Gandy, *Church's Thesis and principles of mechanism*, in *The Kleene Symposium*, (J. Barwise *et al.*, eds.), North Holland, 1980, 123-148.

[GG] M. Golubitsky e V. Guillemin, *Stable Mappings and their Singularities*, Graduate Texts in Math. **14**, Springer-Verlag, (1973).

[GH] J. Guckenheimer e P. Holmes, *Nonlinear Oscillations, Dynamical Systems, and Bifurcations of Vector Fields*, Springer-Verlag, 1983.

[Go] C. E. Gordon, *Comparisons between some generalizations of recursion theory*, Compositio Math. **22**, (1970), 333-346.

[HK] J. K. Hale e H. Koçak, *Dynamics and Bifurcations*, Springer-Verlag, 1991.

[Kl1] S. C. Kleene, *Recursive functionals and quantifiers of finite types. I*, Trans. Amer. Math. Soc. **91**, (1959), 1-52.

[Kl2] S. C. Kleene, *The theory of recursive functions aprroaching its centennial*, Bull. Amer. math. Soc. **1**, (1981), 43-61.

[Kr1] G. Kreisel, *Some reasons for generalizing recursion theory* , in *Logic Colloquium 1969*, (R. O. Gandy and Yates eds.), North Holland, (1971), 139-198.

[Kr2] G. Kreisel, *A notion of mechanistic theory*, Synthese **29**, (1974), 11-26.

[Kr3] G. Kreisel, *review of Gödel's Collected Works, Vol. II*, Notre Dame J. Formal Logic **31**, (1990), 602-641.

[KS] L. G. Khazin e E.E. Shnol, *On the stability of the equilibrium position in critical and near critical cases*, Prikl. Matem. Mekhan. **45**, (1981), 437-444.

[Ma] R. Mansfield, *The irracional are not recursively enumerable* , Proc. Amer. Math. Soc. **110**, (1990), 495-497.

[Mos1] Y. Moschovakis, *Abstract first order computability I*, Trans. Am. math. Soc **138**, (1969), 427-464.

[Mos2] Y. Moschovakis, *Abstract first order computability II*, Trans. Am. math. Soc **138**, (1969), 465-504.

[Mos3] Y. Moschovakis, *Abstract computability and invariant definability*, J. Symb. Logic **34**, (1969), 605-633.

[Mos4] Y. Moschovakis, *Abstract Recursion theory* , Lecture Notes in Mathematics **1104**, 289-364.

[Mos5] Y. Moschovakis, *The formal language of recursion* , J. Symb. Logic **54**, (1989), 1216-1252.

[Mos6] Y. Moschovakis, *A mathematical modeling of pure, recursive algorithms* , Lecture Notes in Computer Science **363**, 208-229.

[Mz] B. Mazur, *Questions of decidability and undecidability in number theory*, J. Symb. Logic **59**, (1994), 353-371.

[Od] P. Odifreddi, *Classical Recursion Theory*, North Holland, 1989.

[Ph] T. Pheidas, *Extensions of Hilbert's tenth problem*, J. Symb. Logic **59**, (1994), 372-397.

[PR] M. B. Pour-El I. Richards, *Computability and noncomputability in classical analysis*, Trans. Am. Math. Soc. **275**, (1983), 539-560.

[Ri] D. Richardson, *Some undecidable problems involving elementary functions of a real variable*, J. Symb. Logic **33**, (1968), 514-520.

[Sa] G. Sacks, *Higher Recursion theory*, Springer-Verlag, 1987.

[SB] W. Sieg e J. Byrnes, *K-Graph Machines: generalizing Turing's Machines and arguments*, Report Carnegie Mellon Univ. **55**, (1994).

[Sh1] J. C. Shepherdson, *Computation over abstract structures: serial and parallel procedures and Friedman's effetive definitional schemes*, (?)

[Sh2] J. C. Shepherdson, *Algorithmic Procedures, generalized Turing algorithms and elementary recursion theory*, in *Harvey Friedman's Research on the Foundations of Mathematics*, (L. Harrington *et al.* eds.), North-Holland, (1985), 285-309.

[Sh3] J. C. Shepherdson, *Mechanisms for computing over arbitrary structures*,

(?)

[Sm1] S. Smale, *On the efficiency of algorithms of analysis*, Bull. Amer. Mat. Soc. **13**, (1985),87-121.

[Sm2] S. Smale, *On the topology of algorithms I*, J. Complexity **3**, (1987), 81-89.

[Sm3] S. Smale, *Algorithms for solving equations*, in *Procedings of the International Congress of Mathematicians*, Berkeley, U.S.A., (1986), 172-195.

[Sm4] S. Smale, *Some remarks on the foundations of numerical analysis*, SIAM review **32**, (1990), 211-220.

[Sm5] S. Smale, *Theory of computation*, Lect. Notes in Math. **1525**, (1991), 59-69.

[St] I. Stewart, *The dynamics of impossible devices*, Nonlinear Science Today **1**, (1991), 8-9.

[T] A. Turing, *On computable numbers, with an aplication to the Entscheidungsproblem*, Proc. London. Math. Soc. **42**, (1936-7), 230-265.

[To] J. C. Tougeron, *Idéaux des fonctions différentiables I*, Ann. Inst. fourier **18**, 91968), 177-240.

[vdD] van den Dries, *Alfred Tarski's elimination theory for real closed fields*, J. Symb. Logic **53**, (1988), 7-19.

[W] P. S. Wang, *The undecidability of the existence of zeros of real elementary functions*, J. Assoc. Comp. Mach., **21**, (1974), 586-589.

[Wa] H. Wang, *On phisicalism and algorithmism: can machines think?*, Philosophia Math. **3**, (1983), 97-138.

[We] J. C. Webb, *Introductory note to 1972a, in 'The Complete Works of Kurt Gödel* I, 292-304.