José Acácio de Barros

CONJUNTOS GENÉRICOS SEGUNDO COHEN E SUAS APLICAÇÕES À FÍSICA

TESE DE

MESTRADO

CENTRO BRASILEIRO DE PESQUISA FÍSICAS

Rio de Janeiro

- 1989 -

Há um conceito que é o corruptor e o perturbador de todos os demais. Não me refiro ao Mal, cujo limitado império é a ética; falo sim do infinito.

Jorge Luis Borges

Esta tese é dedicada, pelo candidato e seu
orientador, à memória do Professor
Carlos Marcio do Amaral, mestre e amigo.

AGRADECIMENTOS:

Ao Doria, cujo estímulo, não só em física e matemática, mas também em outras tão avessas a essas, como aegiptologia, foi fundamental à minha formação.

Ao Teixeira, pelo seu apoio aqui no CBPF, sem o qual este trabalho não poderia ter sido realizado.

Aos amigos do CBPF, em especial aos amigos André, Emilia, Pardal (Fernando), Esquálidus (Ódivaldo), Welles (leia-se Vélis), Paschola (Ricardo), Ladaire, Marco Antônio, Tião e Sônia, Lula e Rosana, Gerson, Zé Luiz, Sérgio, Edson (estes últimos [RGZSE] formando, junto comigo, o 'grupo dos seis') e todos aqueles que de uma maneira ou de outra contribuiram para tornar mais agradável a minha estadia aqui.

Aos meus tios, pela "casa, comida e roupa lavada" durante mais de cinco anos, e aos meus pais, pelo mesmo motivo (a única diferença sendo o período, que passa agora para 22 [vinte e dois] anos)

RESUMO

Neste trabalho, demonstramos existir uma relação entre a razão de crescimento da cardinalidade das órbitas de um dado sistema simbólico e a sua entropia. Com a ajuda deste resultado, obtemos um teorema que nos mostra ter medida nula o conjunto de trajetórias cuja entropia é positiva. Mostramos também que a entropia não é um conceito absoluto (no sentido da teoria de conjuntos). Após isto damos um exemplo de proposição formalmente indecidível em eletromagnetismo clássico. Ainda seguindo a idéia dada pela teoria de conjuntos, mostramos as condições para a existência de espaços-tempo genéricos.

ABSTRACT

Here we show that exists a relation between the behavior of a symbolic system's orbit cardinality and its entropy. With the help of this relation, we show that a system with non-null entropy is a residual set. We also show that entropy is not a set-theoretically absolute concept (in the sense of Gödel). Then we find a formally undecidable statement on classical electromagnetic theory. Following this idea, we exhibit the conditions for the existence of generic space-times.

SUMÁRIO

INTRODUÇÃO

Num capítulo intitulado "Avatares da Tartaruga", do livro *Discussão*, Jorge Luis Borges nos lembra, ao falar do conhecido paradoxo de Zenon (no qual Aquiles, rápido corredor, não alcança uma tartaruga), quão fundamental e malicioso é o conceito de infinito. Ao lidarmos com o infinito, às vezes nos deparamos com resultados surpreendentes, como por exemplo o paradoxo de Banach-Tarski, que nos diz que uma esfera maciça pode ser decomposta em outras duas esferas maciças de mesmo volume (veja ref. [52']). Todos nós estamos acostumados a trabalhar com limites, a somar séries infinitas, a integrar, a derivar, mas raramente ao fazermos tais procedimentos "mecânicos", temos consciência das sutilezas que talvez venham a se esconder por trás deles. Nos seus infinitos avatares, o infinito gerou uma série de questões dentro de sua própria origem, que é a matemática (?). Estas questões criaram uma multiplicidade de correntes filosóficas, donde podemos destacar o *Platonismo*, o *Finitismo* e o *Formalismo*. Em vias gerais, podemos resumir os pontos de vista de cada linha da séguinte forma:

Platonismo: A matemática existe porquê a Natureza se comporta de forma matemática. Com isso, a matemática independe da vontade humana, sendo para nós imposta pela Natureza. Para um platonista, a geometria Riemanniana teria sentido somente se mergulhada dentro de uma geometria Euclidiana, se se provasse ser o espaço plano.

Finitismo: Para os Finitistas, é proibido o uso de processos que envolvam o conceito de infinito. Seguindo o exemplo da geometria, o conceito de reta seria absurdo, pois exigiria que um segmento se estendesse infinitamente tanto para um sentido quanto para o outro, tarefa irrealizável na prática. Para um finitista, um objeto só existe se ele pode ser "alcançado" (aspas necessárias); com isso, o conjunto dos naturais, por ser infinito, não pode existir.

Formalismo: O formalismo se baseia no sucesso do esquema axiomático, criado por Euclides, da geometria. Toda a matemática seria reduzida a um conjunto de axiomas, escritos numa linguagem formal, e manipulados conforme as regras dessa linguagem. A influência do matemático no processo seria nula, pois, uma vez sendo as regras de manipulação fixadas, a intuição não teria vez na solução dos problemas.

No fim do século passado, importantes pesquisadores aderiram ao ponto de vista formalista, e o seu sucesso foi tão grande que chegou a se acreditar ser a matemática uma teoria fechada, e que, por causa disso, o trabalho dos matemáticos se reduziria a marcar sequências de símbolos em papéis para se demonstrar a verdade ou a falsidade de um dado teorema. Dentro do espírito da escola formalista, David Hilbert fez, em 1900, a sua famosa lista dos 23 mais importantes problemas em aberto da matemática, que deveriam ter prioridade, em relação aos outros, de serem resolvidos.

Em 1931, um jovem logicista chamado Kurt Gödel, joga um balde de água fria sobre os ideais formalistas. Num artigo revolucionário ([16]), Gödel mostra que, dentro do esquema formalista, a consistência da aritmética não poderia ser demonstrada usando-se ferramentas da própria aritmética; Gödel mostra também que, se um dado sistema formal é consistente, então ele é obrigatoriamente incompleto, isto é, existem teoremas cuja veracidade ou falsidade não podem ser demonstrados (para maiores detalhes, veja-se o capítulo 1).

Um importante problema indecidível, face aos axiomas de Zermelo-Fränkel para a teoria dos conjuntos(pois não podemos decidir se é falso ou verdadeiro, usando esses axiomas) é a *Hipòtese do Contînuo*, que constava em 1º lugar na lista de Hilbert. A demonstração da independência da Hipótese do Contínuo face aos axiomas da teoria de conjuntos foi feita em 1963 por P. J. Cohen [05], que mostrou existirem modelos onde esta falhava (A prova da consistência havia sido dada por Gödel em 1938). Num artigo publicado na revista *Scientific American* [07], Cohen apontou a possibilidade de aplicarmos diferentes modelos para a teoria de conjuntos (modelos estes em que uma dada hipótese possa ser verdadeira ou falsa) na Física. Nesse artigo, Cohen faz um paralelo com o desenvolvimento das geometrias não-euclidianas e suas aplicações posteriores em física, como a Relatividade Geral.

Neste trabalho, tentamos obter algumas aplicações às quais Cohen se referia. Usamos aqui a técnica por ele inventada para a criação de modelos para diferentes teorias de conjuntos, conhecida como *forcing*. Por ser intuitivamente mais simples, usamos o *forcing* via modelos booleanos.

No primeiro capítulo, estudamos a linguagem formal sobre a qual se apoiará a nossa teoria, e, em seguida, vemos os axiomas do cálculo proposicional e da teoria de conjuntos; logo após fazemos uma breve introdução à teoria de modelos e então demonstramos o teorema de Löwenhein-Skolem; do estudo das funções recursivas esboçamos a prova do teorema de Gödel, mencionado acima; finalmente, completando o capítulo, apresentamos a teoria de modelos booleanos, colocando como exemplo de aplicação a prova da independência da hipótese do contínuo.

No capítulo dois é feita uma revisão da teoria ergódica; estudamos o caso do *shift* de Bernoulli e colocamos a demonstração do teorema ergódico; feito isso, definimos o que vem a ser entropia, seguida da prova do teorema de Kolmogorov-Sinai; obtemos, após a demonstração do teorema de Shannon-MacMillan-Breiman, a propriedade de equipartição da entropia; finalmente, obtemos uma relação entre o crecimento da cardinalidade das órbitas de um sistema simbólico com a sua entropia.

No terceiro capítulo, colocamos alguns exemplos de sentenças indecidíveis em física e em matemática. Mostramos uma sentençaindecidível em Eletromagnetismo Clássico. Em Relatividade Geral, mostramos que, em alguns casos, existem variedades genéricas (i. e. não-standard). Mostramos também que sistemas de entropia não nula podem ter entropia nula quando mudamos de modelo conjuntista; Usando a ferramenta criado no capítulo 2 mostramos o teorema de Rohlin.

A maior parte dos teoremas encontrados no texto estão sem as respectivas demonstrações, sendo estas facilmente encontradas nas referências lá citadas; estas provas não foram feitas para não tornarem este texto mais longo do que o razoável. Os teoremas mais importantes têm suas demonstrações feitas, ou ao menos esboçadas. A decisão de incluir praticamente duas seções de revisão se deve basicamente ou desconhecimente da maioria dos estudantes de física tanto da teoria ergódica quanto da teoria axiomática de conjuntos e a teoria de modelos; como referências para estas teorias podemos citar os livros de Billingslay [03], Friedman [15], Mañé [27] ou Petersen [32], para teoria ergódica; os livros de Bell [02], Jech [22], Manin [28], para a teoria de modelos booleanos,tendo os dois últimos material sobre teoria axiomática de conjuntos; Krivine [24], Kunen [25], Cohen [06], apresentam a teoria de modelos; Stoll [34], Suppes [36] são boas referências, apesar de antigas, para a axiomatização da teoria de conjuntos, apresentando o primeiro um capítulo sobre lógica.

Como pré-requisito, o leitor precisa de algum conhecimento de: Álgebras de Boole, que pode ser adquirido (até um pouco acima do que necessitamos) em Halmos [19]; Teoria Ingênua de

Conjuntos (Halmos [18]); Topologia Geral (um apanhado geral pode ser visto em Lipschutz [45']); Teoria da Medida ([14] ou [21]).

- CAPÍTULO 1 -

TEORIA AXIOMÁTICA DOS CONJUNTOS E MODELOS BOOLEANOS

1.1 INTRODUÇÃO:

Após o aparecimento da Teoria Ingênua dos Conjuntos (T.I.C.), inventada por Georg Cantor em fins do século XIX, surgiram nela métodos poderosos para o estudo de diferentes problemas em matemática, tornando esta teoria tão indispensável que, hoje em dia, não podemos nos imaginar aprendendo matemática sem usá-la.

Um dos mais importantes resultados desta teoria é que ela torna manipulável o conceito de infinito. Na verdade, Cantor criou a T.I.C. com o objetivo de estudar a convergência de determinadas séries infinitas, e as funções representáveis por Séries de Fourier.

Talvez a descoberta mais interessante de Cantor haja sido a existência de uma família ilimitada de infinitos diferentes. Intuitivamente, 'cardinalidade' é o número de elementos que um dado conjunto tem. Dizemos que dois conjuntos A e B têm a mesma cardinalidade se existe uma função biunívoca e sobrejetora entre A e B (veja [16] para uma revisão destes e de outros conceitos ligados à teoria ingênua de conjuntos). Com isto, podemos dizer que os conjuntos $\{a,b\}$ e $\{0,1\}$ têm a mesma cardinalidade (é simples definir uma função com as propriedades supra). Da mesma forma, podemos comparar a cardinalidade de dois conjuntos infinitos. O primeiro resultado que pode nos parecer estranho é que os números ímpares $\{1,3,5,\ldots\}$ têm a mesma cardinalidade dos inteiros positivos $\omega_o = \{0,1,2,3,\ldots\}$, ou seja, se temos um conjunto com infinitos elementos (os inteiros, no caso) e retiramos dele uma quantidade infinita de elementos (retiramos os pares para obtermos os ímpares, por exemplo) obtemos um conjunto diferente (no caso os ímpares) cujo número de elementos é o mesmo que o do conjunto inicial. Este aparente paradoxo, que remonta a Galileu, é a propriedade pela qual podemos definir um conjunto como sendo infinito: A é infinito se existe um seu subconjunto próprio $B \subsetneq A$, tal que a cardinalidade de B é igual à de A.

Cantor então comparou a cardinalidade dos naturais (um conjunto contável) com o número de elementos da reta real $\mathbb{R}$, demonstrando que $\mathbb{R}$ tem muito mais elementos que ω_o. Cantor deu mais de uma demonstração para isto, mas talvez a mais conhecida, possivelmente devido à sua simplicidade e beleza, seja a "prova diagonal", que mostraremos aqui.

Sabemos que todo o elemento de ω_o é obviamente também um elemento de $\mathbb{R}$, e que $|\mathbb{R}| = |\mathcal{P}(\omega_o)|$ onde $\mathcal{P}(X)$ denota o conjunto potência de X, isto é, o conjunto de todos os subconjuntos de X, e $|Y|$ a cardinalidade de Y.

Suponhamos que exista uma função $f : \omega_o \Rightarrow \mathcal{P}(\omega_o)$.

Mostraremos que qualquer função deste tipo não pode ser 1-1. Para isso formemos o conjunto

$$F = \{n \in \omega_0 : n \notin f(n)\}$$

Se existe um $n \in \omega_0$ tal que $F = f(n)$, obtemos uma contradição, pois pela definição de F temos:

$$n \in F \rightarrow n \in f(n) \rightarrow n \notin F$$

mas temos também que:

$$n \notin F \rightarrow n \notin f(n) \rightarrow n \in F$$

Com isto, a existência de uma função 1-1 entre ω_0 e $\mathcal{P}(\omega_0)$ implica em $n \notin F$ se e somente $n \in F$, que é uma contradição. Então existe um elemento F de $\mathcal{P}(\omega_0)$ que não está na imagem de f, o que implica que f não é 1-1. Disto obtemos $|\mathbb{R}| = |\mathcal{P}(\omega_0)| > |\omega_0|$.

Tais resultados não pareceram óbvios na época em que surgiram (e, quem sabe, talvez não o sejam ainda hoje). Além disso, começaram a surgir vários paradoxos oriundos da utilização indiscriminada do conceito de conjunto. Destes paradoxos provavelmente o mais conhecido é o de Russell ([28] ou [48]), que surge quando usamos a noção de que dada uma propriedade podemos formar um conjunto cujos elementos a obedecem. Consideremos o conjunto $S = \{ x : x \notin x \}$ sendo a propriedade definidora a de que os elementos de S não são elementos dele mesmo. Podemos fazer a seguinte pergunta: $S \in S$ ou $S \notin S$? Se $S \in S$, então obrigatoriamente (por definição), $S \notin S$. Se, por outro lado, $S \notin S$, satisfaz a propriedade definidora de S, isto é, $S \in S$. Temos aqui uma contradição, que é o chamado paradoxo de Russell. Vários outros paradoxos na teoria ingênua dos conjuntos foram encontrados posteriormente, levantando sérias questões sobre o problema da consistência daquela teoria, e consequentemente, da matemática.

A partir destes problemas criou-se a necessidade de se conhecer melhor os fundamentos da teoria de conjuntos, e várias linhas de filosofia da matemática surgiram para explicar-los. Uma delas é a abordagem formalista; dentro desta abordagem temos a Teoria Axiomática de Conjuntos (T.A.C.), em contraste à T.I.C., que será o objeto de estudo deste capítulo, junto com algumas outras consequências de caráter metamatemático.

1.2 CÁLCULO DE PREDICADOS DE PRIMEIRA ORDEM.

A Teoria Axiomática de Conjuntos é construida sobre uma linguagem formal, ou seja, uma coleção finita de símbolos (o alfabeto básico) e regras precisas para manipulá-los. O processo de manipulação, executado estritamente conforme estas regras, conduz ao que chamamos "teoremas". Com isto, demonstrações de teoremas reduzem-se explicitamente a um jogo de símbolos, como o jogo de xadrez ou o jogo da velha, com regras determinísticas bem definidas. Nosso objetivo é construir a teoria de conjuntos (e com isto toda a matemática usual) como um processo de manipulação explícita e verificável de símbolos; algo que pudesse ser, digamos, examinado com a ajuda de um macaco treinado - ou de um computador. Para entendermos melhor esse conceito precisamos formalizar o que entendemos por *computar*.

Sejam dois conjuntos X e Y. Uma função parcial de X em Y é um par <Dom(f), f> e uma função f : Dom(f) $\Rightarrow$ Y, onde Dom(f) $\subset$ X. As funções suc(x), cons(x) e $proj_i(x)$ são definidas por:

$$\begin{array}{ll} suc : \omega_0^+ \Rightarrow \omega_0^+ \quad , & suc(x) = x + 1; \\ cons : (\omega_0^+)^n \Rightarrow \omega_0^+ \quad , & cons(x_1, \ldots, x_n) = c \; , \quad n \geq 0; \\ proj_i : (\omega_0^+)^n \Rightarrow \omega_0^+ \quad , & proj_i(x_1, \ldots, x_n) = x_i, \; n \geq 1; \end{array}$$

onde $\omega_0^+ = \{1, 2, 3, 4, \ldots\}$ e $c \in \omega_0^+$ é uma constante. suc, cons, e $proj_i$ são também chamadas de funções básicas.

Com as funções supra, podemos definir uma série de operações, chamadas operações elementares, que são:

i) Composição. Sejam f : $(\omega_0^+)^m \Rightarrow (\omega_0^+)^n$ e g : $(\omega_0^+)^n \Rightarrow (\omega_0^+)^q$. A composição de f e g é uma função h = gof definida por:

$$Dom(gof) = \{ x \in (\omega_0^+)^m : x \in Dom(f),\ f(x) \in Dom(g) \}$$

$$(gof)(x) = g(f(x))$$

ii) Justaposição. Sejam $f_i: (\omega_0^+)^m \Rightarrow (\omega_0^+)^{n_i}$, $i = 1,\ldots,k$. Definimos a função $(f_1,\ldots,f_k)$ como:

$$(f_1,\ldots,f_k) : (\omega_0^+)^m \Rightarrow (\omega_0^+)^{n_1} \times\ldots\times (\omega_0^+)^{n_i}$$

$$Dom((f_1,\ldots,f_k)) = Dom(f_1) \cap\ldots\cap Dom(f_k)$$

$$(f_1,\ldots,f_k)(x_1,\ldots,x_m) = \langle f_1(x_1\ldots x_m),\ldots,f_k(x_1\ldots x_m)\rangle$$

iii) Recursão. Sejam $f : (\omega_0^+)^n \Rightarrow \omega_0^+$ e $g : (\omega_0^+)^{n+2} \Rightarrow \omega_0^+$. Definimos uma uma função $h : (\omega_0^+)^{n+1} \Rightarrow \omega_0^+$ por recursão como:

$$\begin{cases} h(x_1,\ldots,x_n,1) = f(x_1,\ldots,x_n) \\ h(x_1,\ldots,x_n,k+1) = g(x_1,\ldots,x_n,k,h(x_1,\ldots,x_n,k)), \quad k\geq 1 \end{cases}$$

e para Dom(h)

$$\begin{cases} \langle x_1,\ldots,x_n,1\rangle \in Dom(h) \leftrightarrow \langle x_1,\ldots,x_n\rangle \in Dom(f) \\ \langle x_1,\ldots,x_n,k+1\rangle \in Dom(h) \leftrightarrow \langle x_1,\ldots,x_n,k\rangle \in Dom(h) \\ \langle x_1,\ldots,x_n,k,h(x_1,\ldots,x_n,k)\rangle \in Dom(h) \text{ para } k\geq 1 \end{cases}$$

iv) Operador μ. Seja $f: (\omega_0^+)^{n+1} \Rightarrow \omega_0^+$, definimos $h = \mu f$ como $h : (\omega_0^+)^n \Rightarrow \omega_0^+$ tal que:

$$Dom(h) = \{\langle x_1,\ldots,x_n\rangle \;;\; \exists x_{n+1} \geq 1 \;(f(x_1,\ldots,x_n,x_{n+1})=1 \wedge \forall k \leq x_{n+1}(\langle x_1,\ldots,x_n,k\rangle \in Dom(f)))\}$$

$$h(x_1,\ldots,x_n) = \min\{x_{n+1} : f(x_1,\ldots,x_n,x_{n+1}) = 1\}$$

DEFINIÇÃO 1.1: Uma sequência de funções parciais $f_1, \ldots, f_N$ é dita ser uma descrição *recursiva primitiva* da função $f = f_N$ se

f_1 é uma função básica

f_i, $i \geq 2$ ou pertence à família das funções básicas ou é obtida aplicando-se as operações elementares *i)*-*iii)* a algumas das $f_1, \ldots, f_{i-1}$.

DEFINIÇÃO 1.2: Uma função f é dita *recursiva primitiva* se ela admite uma descrição recursiva primitiva.

As funções recursivas primitivas formalizam parte da intuição do que sejam funções calculáveis, ou seja, com a sua definição, com os inteiros $x_1, \ldots, x_n$ e usando as regras dadas para formar f_i a partir de $f_1, \ldots, f_{i-1}$ podemos obter $f(x_1, \ldots, x_n)$. As funções recursivas primitivas são a classe mais simples de funções calculáveis, mas não esgotam todas as funções efetivamente calculáveis (ou, como também são chamadas, computáveis).

DEFINIÇÃO 1.3: Uma sequência de funções parciais $f_1, \ldots, f_N$ é dita ser uma *descrição recursiva parcial* de $f = f_N$ se

f_1 é uma função básica

f_i, $i \geq 2$ ou pertence à família das funções básicas ou é obtido das funções $f_1, \ldots, f_{i-1}$ aplicando-se as operações elementares.

Uma função f é chamada de *recursiva parcial* se ela admite uma descrição recursiva parcial. f é *recursiva geral* se ela é recursiva parcial definida em todos os pontos.

DEFINIÇÃO 1.4: Seja S um conjunto de inteiros. Definimos $\chi_S(n) = 0$ se $n \notin S$ e $\chi_S(n) = 1$ se $n \in S$. χ_S é chamada de *função característica* de S.

As funções recursivas parciais esgotam todas as funções que podem ser efetivamente calculadas por um computador e por isso também são chamadas de funções computáveis. Este fato, que não pode ser demonstrado, é o conteúdo da Tese de Church: " Uma função f é computável se e somente se f e $\chi_{Dom(f)}$ são funções recursivas parciais". Funções computáveis são objetos extremamente singulares, no sentido de terem medida nula no conjunto de todas as funções em $\omega_o^{\omega_o}$ (veja [15]), apesar da definição, que aparenta não restingir muito.

Para maiores detalhes sobre as funções recursivas primitivas e recursivas sugerimos ao leitor a consulta de [08], [36] ou [44].

DEFINIÇÃO 1.5: Um conjunto S é *recursivo* se sua função característica é recursiva geral.

Dizer que S é recursivo é equivalente a dizer que existe um programa de computador* que nos diz se um dado objeto

---

*Para maiores detalhes veja [08]; para uma exposicao bem pertence ou não ao conjunto S.

DEFINIÇÃO 1.6: Um conjunto S é *recursivamente enumerável* se S é vazio ou se S é a imagem de uma função recursiva geral.

Destas definições resulta um importante teorema que é:

TEOREMA 1.1: Existe um conjunto recursivamente enumerável que não é recursivo.

Voltemos à nossa linguagem formal. Ela é construída da seguinte maneira: partimos de um conjunto finito de n símbolos, $n = \{0,1,2,\ldots,n-1\}$, que também (por conveniência) poderemos escrever $\{a_0, a_1, \ldots, a_{n-1}\}$. Formamos $L_n = n^{<\omega_0}$, conjunto de todas as sequências finitas (i.e., funções cujo domínio é um subconjunto finito de ω_0) de símbolos n. L_n é a linguagem livre sobre n. Definimos então uma regra f que nos permite construir um conjunto $L_n^f \subseteq L_n$:

i) f é uma função característica: $x \in L_n^f \leftrightarrow$ domínio $f = L_n$, e $f(x) = 1$; $x \notin L_n^f \leftrightarrow f(x) = 0$.

ii) f é computável.

L_n^f é o conjunto das fórmulas bem construídas (wff) na linguagem formal $\langle L_n, f\rangle$

---

acessível incluindo discussoes sobre funcoes recursivas e r.p. veja Doria em [33].

A linguagem sobre a qual construiremos a nossa teoria é composta do seguinte alfabeto inicial:

$\wedge$ (e);

$\neg$ (não);

$\exists$ (existe);

$=$ (igual);

(,) (parênteses);

R (símbolo para relação);

x (símbolo para variáveis);

c (símbolo para constantes);

' (índice);

As palavras entre parênteses ao lado de cada símbolo dão os seus significados correntes ou intuitivos. Lembremos que, na teoria, o significado dos símbolos não interessa; o que interessa é a maneira pela a qual são usados (ou seja, ao demonstrarmos um teorema, o significado dos símbolos guia, mas não influencia, nas regras usadas para sua manipulação).

Para simplificarmos a notação introduziremos novos símbolos como abreviações* de determinadas fórmulas. São estes:

1. x, y, z,... abreviam x, x', x'',... respectivamente;

2. a, b, c,... abreviam c, c', c'',... respectivamente;

---

*Abreviacoes sao comumente usadas em matemática para tornar mais fácil tanto a utilizacao quanto a interpretacao de determinados objetos. Usaremos aqui algumas abreviacoes com este mesmo intuito, podendo sempre o formalismo ser resgatado voltando-se ao alfabeto inicial.

3. R_1, R_2, R_3,... abreviam R, R', R'',... respectivamente;

4. $\forall x$ A abrevia $\neg(\exists x(\neg(A)))$;

5. (A) $\vee$ (B) abrevia $\neg((\neg(A)) \wedge (\neg(B)))$;

6. (A) $\rightarrow$ (B) abrevia $(\neg(A)) \wedge (B)$;

7. (A) $\leftrightarrow$ (B) abrevia $((A) \rightarrow (B)) \wedge ((B) \rightarrow (A))$;

8. $t_i \neq t_j$ abrevia $\neg(t_i = t_j)$, onde t_i, t_j podem ser variáveis ou constantes;

9. $\exists! x$ A(x) abrevia $\exists x \forall y$ (A(y) $\leftrightarrow$ x = y);

As interpretações intuitivas para os novos símbolos introduzidos são as usualmente empregadas em matemática, sendo $\forall$, $\vee$, $\rightarrow$, $\leftrightarrow$, $\neq$ e $\exists!$ traduzidas respectivamente como "para todo", "ou", "se ... então", "se e somente se", "diferente" e "existe um único".

R_1, R_2, R_3,... representam relações entre objetos, sendo R_i o i-ésimo elemento desta lista (abreviando o R com (i-1) linhas). R_i representa uma relação n_i-ária (entre n_i objetos) e podemos escrever $R_i(t_1, t_2, \ldots, t_{n_i})$ onde t_j pode ser tanto uma constante como uma variável. Como exemplo de relação binária temos a pertinência "$\in$"; $x \in y$ deve ser escrito numa linguagem formal como, por exemplo, $\in(x,y)$.

Conhecido o alfabeto da nossa linguagem, podemos agora ver as regras para a formação de uma frase gramaticalmente correta; Esta será chamada de fórmula bem formada e será abreviada por wff (do inglês "well formed formulae"). Estas regras são:

1. $x = x'$

$x = c$

$c = c'$

são wff;

2. Se R é uma relação n-ária e cada um dos $t_1, \ldots, t_n$ ou é uma constante ou é uma variável, então

$$R(t_1, \ldots, t_n)$$

é uma wff;

3. Se A e B são wff então também o são:

$$\neg(A); \ (A)\wedge(B); \ e \ \exists xA;$$

4. As únicas wff são as dadas por 1-3.

Na linguagem livre sobre o alfabeto $\{\wedge, \neg, \exists, =, (,), x, c, R, '\}$, é facil ver que o conjunto das wff é recursivo.

Neste momento, é útil introduzir os conceitos de "variáveis livres" e "variáveis ligadas". A ocorrência de uma variável numa fórmula é ligada se e somente se a sua ocorrência está dentro da abrangência de um quantificador (os quantificadores são $\exists$ e $\forall$). A ocorrência de uma variável é livre se e somente se ela não é ligada. Definimos uma variável como sendo livre numa fórmula se e somente se pelo menos uma ocorrência dela for livre; uma variável é ligada numa fórmula se e somente se pelo menos uma de suas ocorrências é ligada. Como exemplo podemos colocar a fórmula

$$\forall x \ R(x, y)$$

onde x é ligada e y é livre.

DEFINIÇÃO 1.7: Uma *sentença declarativa* é uma fórmula que não contém variáveis livres.

Tendo definido o que são sentenças declarativas, devemos lembrar que o nosso objetivo é construir uma teoria axiomática de conjuntos. Então, em última instância, o que queremos é: dado um conjunto de sentenças declarativas iniciais (axiomas), saber quais as sentenças declarativas que são consequência lógica destas (veremos adiante como formá-las) e quais as que não contradizem este sistema.

Dado um conjunto recursivo de sentenças bem construidas $L_n^f \subseteq L_n$, uma teoria sobre L_n^f é o par $T = \langle L_n^f, T_n^f \rangle$, onde $T_n^f \subseteq L_n^f$ é um subconjunto recursivamente enumerável de L_n^f. Em geral há um procedimento 'mecânico' θ que 'gera' T_n^f a partir de outro conjunto $A_n^f \subseteq L_n^f$, onde A_n^f são os 'axiomas' da teoria e θ são as 'regras de dedução'.

A teoria T é *trivial* se $L_n^f = T_n^f$; em caso contrário é não trivial.

Faltou-nos definir quais são as regras para, dado um conjunto de sentenças declarativas, obtermos outras sentenças declarativas válidas. Estas regras são conhecidas como *Cálculo de Predicados*. Antes de vermos esta regras definamos o que vem a ser uma *função proposicional*.

DEFINIÇÃO 1.8: Uma *função proposicional* é uma sucessão formal de simbolos definida da seguinte maneira:

1. Se A é uma variável então A é uma função proposicional;

2. Se P e Q são funções proposicionais então $\neg(P)$, $(P)\wedge(Q)$, $(P)\vee(Q)$, $(P)\rightarrow(Q)$ e $(P)\leftrightarrow(Q)$ são funções proposicionais;
3. As únicas funções proposicionais são as formadas como em 1 e 2.

Seja agora P uma função proposicional de $A_1,\dots,A_n$. Cada variável da função pode assumir o valor 1 (que é interpretado como "verdade") ou o valor 0 (interpretado como "falso"); formemos um conjunto D, chamado domínio, onde as variáveis $A_1,\dots,A_n$ variam em D. A função proposicional ou função lógica é um mapeamento de D em $2 = \{0,1\}$. De uma maneira mais precisa, uma função proposicional P será um mapeamento do tipo $P : 2^{<\omega_0} \Rightarrow 2$.

Se φ_1 é uma função que corresponde a P e φ_2 uma função correspodendo a Q ($\varphi_1 : D_1 \Rightarrow 2$ e $\varphi_2 : D_2 \Rightarrow 2$ onde D_1 e D_2 são elementos de 2^p e 2^q sendo p e q o número de variáveis livres de P e Q respectivamente) as funções que correspondem a $\neg(P)$, $(P)\wedge(Q)$, $(P)\vee(Q)$, $(P)\rightarrow(Q)$ e $(P)\leftrightarrow(Q)$ são respectivamente $\psi_1(\varphi_1)$, $\psi_2(\varphi_1, \varphi_2)$, $\psi_3(\varphi_1, \varphi_2)$, $\psi_4(\varphi_1, \varphi_2)$ e $\psi_5(\varphi_1, \varphi_2)$, dados pela tabela seguinte:

	$\psi_1(x)$	$\psi_2(x,y)$		$\psi_3(x,y)$		$\psi_4(x,y)$		$\psi_5(x,y)$	
y →		0	1	0	1	0	1	0	1
x ↓ 0	1	0	0	0	1	1	1	1	0
1	0	1	0	1	1	0	1	0	1

ou calculadas pelas fórmulas:

$$\| \neg P \| = 1 - \| P \|$$

$$\| P \wedge Q \| = \min (\| P \|, \| Q \|)$$

$$\| P \vee Q \| = \max (\| P \|, \| Q \|)$$

$$\| P \to Q \| = 1 - \| P \| + \| P \| . \| Q \|$$

$$\| P \leftrightarrow Q \| = \| P \| . \| Q \| + (1 - \| P \|)(1 - \| Q \|)$$

Com essas fórmulas podemos calcular a função proposicional de qualquer sentença. Como exemplo calcularemos a função proposicional da fórmula $P \to (Q \to P)$:

$$\| P \to (Q \to P) \| = 1 - \| P \| + \| P \| . \| Q \to P \| =$$

$$= 1 - \| P \| + \| P \| (1 - \| Q \| + \| Q \| . \| P \|) =$$

$$= 1 - \| P \| + \| P \| - \| P \| . \| Q \| + \| P \|^2 . \| Q \| = 1$$

$$\| P \to (Q \to P) \| = 1$$

Com isso concluimos que, independente de serem P ou Q falsos ou verdadeiros (0 ou 1), a fórmula $P \to (Q \to P)$ é sempre verdadeira (tem sempre valor verdade 1). A uma função proposicional que é identicamente verdadeira, isto é, assume somente o valor verdade 1, chamamos de tautologia.

Podemos agora enunciar as regras do cálculo proposicional. São elas:

1. Regra do Cálculo Proposicional

   Toda tautologia é uma frase declarativa válida.

2. "Modus Ponens" ou Regra de Inferência

   Se A e (A)→(B) são frases declarativas válidas então B também é uma frase declarativa válida.

3. Axiomas da Igualdade

   $x = x$

   $x = y \to (R(x,x) \to R(x,y))$

   são frases declarativas válidas.

Temos também os axiomas para a lógica dos quantificadores:

$$[\ \forall x\ A(x) \to A(c)\ ]$$

$$[\ A(c) \to \exists x\ A(x)\ ]$$

O primeiro desses axiomas é conhecido como "Regra da Especialização". Finalmente, temos as regras de introdução dos quantificadores $\forall$ e $\exists$ que estão esquematizadas abaixo:

$\forall$-introdução - Se $P \to Q(x)$ é verdade, então também é verdade que $P \to \forall x'\ Q(x')$, sendo x não livre em P.

$\exists$-introdução - Se $Q(x') \to P$ é verdade, então também é verdade que $\exists x\ Q(x) \to P$, onde x é não livre em P.

(Na verdade basta postularmos uma dessas regras supra, podendo a outra ser derivada via regras do cálculo proposicional)

Com essas regras dadas concluimos então a apresentação do alfabeto $\mathcal{A}$, com os símbolos dados no início, e da lingugem $L_1^=$, que será a linguagem sobre a qual poderemos construir a teoria de conjuntos. Apresentamos também o cálculo proposicional e o cálculo de predicados. Com isto estamos prontos para começarmos a discutir os axiomas para a T.A.C., que, pretendemos, formalize as intuições em T.I.C..

1.3 AXIOMAS DE ZERMELO-FRAENKEL

Na seção anterior apresentamos o alfabeto $\mathscr{A}$, demos as regras para a formação de frases gramaticalmente corretas e, posteriormente, as regras de dedução junto com os axiomas para o cálculo proposicional, que nos permitia derivar de uma coleção Γ de frases declarativas verdadeiras outras frases declarativas também verdadeiras.

Nessa seção apresentaremos um conjunto Γ de frases declarativas que axiomatizam a teoria de conjuntos. Isto significa que qualquer teorema sobre conjuntos terá que ser derivado de Γ..

Existem diferentes maneiras de axiomatizarmos a teoria de conjuntos; o sistema axiomático que adotaremos aqui será o de Zermelo-Fränkel, que chamaremos abreviadamente de ZF. Esta escolha foi feita por ser ZF o sistema mais intuitivo e, talvez por isso, o mais difundido.

Um axioma importante que é independente (isto é, não demonstrável a partir de) dos axiomas de ZF é o *Axioma da Escolha* (denotado por AC) que será apresentado ao fim da seção em separado de ZF. Ao sistema axiomático ZF mais AC chamaremos de ZFC.

Para não nos estendermos demasiadamente listaremos os axiomas de Zermelo-Fränkel e logo após colocaremos suas interpretações intuitivas.

Axiomas ZF:

(ZF1) - Axioma da Extensionalidade

$$\forall x\ \forall y\ (\forall z\ (z \in x \leftrightarrow z \in y) \rightarrow x = y)$$

Interpretando "$\in$" como a relação de pertinência em teoria de conjuntos, vemos que o axioma da extensionalidade nos diz intuitivamente que dois conjuntos são iguais se e somente se eles têm os mesmos elementos. Em outras palavras, um conjunto é determinado pelos seus elementos, donde vem o nome extensionalidade.

(ZF2) - Axioma do Conjunto Nulo

$$\exists x\ \forall y\ (\neg\ y \in x)$$

Este axioma nos garante a existência de um conjunto que não tem elementos, ou seja, o conjunto nulo ou vazio. De agora em diante representaremos o conjunto vazio por $\emptyset$ e abreviaremos $\neg(y \in x)$ por $y \notin x$. (ZF2) figura na lista dos nossos axiomas por motivo de simplicidade, mas pode-se mostrar que é derivável dos demais.

(ZF3) - Axioma dos Pares Não-Ordenados

$$\forall x, y\ \exists z\ \forall w\ (w \in z \leftrightarrow (w = x \vee w = y))$$

Por (ZF3) se x e y são dois conjuntos quaisquer então $z = \{x, y\}$ é também um conjuntos cujos elementos são x e y.

Já destes axiomas anteriores podemos definir alguns conceitos importantes. A partir, por exemplo, da existência do par não-ordenado podemos definir o par ordenado $\langle x, y\rangle$ como sendo o conjunto $\{x, \{x, y\}\}$. Pelo axioma da extensionalidade temos que $\langle x,y\rangle = \langle z,w\rangle$ se e somente se $x = z$ e $y = w$.

(ZF4) - Axioma da União

$$\forall x.\ \exists y\ \forall z\ (z \in y \leftrightarrow \exists w\ (z \in w \wedge w \in x))$$

Seja x um conjunto cujos elementos também são conjuntos. Este axioma garante a existência de um conjunto que é a união de todos os membros de x, ou seja, dados x e y existe um z denotado por $x \cup y$ tal que t pertence a z se e somente se t é um elemento de x ou um elemento de y.

(ZF5) - Axioma do Infinito ou da Indução

$$\exists x\ (\emptyset \in x \wedge \forall y\ (y \in x \rightarrow y \cup \{ y \} \in x))$$

Isto é, existe um conjunto que contém o conjunto vazio e que se y pertence a ele então $y \cup \{ y \}$ também lhe pertence.

(ZF5) nos garante a existência de um conjunto com infinitos elementos. Na realidade com (ZF5) temos um processo para construirmos os números naturais da seguinte maneira:

"0" $= \emptyset$ (que existe por (ZF2));

"1" $= \emptyset \cup \{ \emptyset \} = \{ \emptyset \}$;

"2" $= \{ \emptyset \} \cup \{\{ \emptyset \}\} = \{ \emptyset, \{ \emptyset \}\}$;

"3" $= \{ \emptyset, \{ \emptyset \}, \{ \emptyset, \{ \emptyset \}\}\}$;

$\vdots$

$(ZF6)_i$ - Esquema Axiomático da Substituição

Enumeremos as fórmulas em nosso sistema que têm pelo menos duas variáveis livres $R_i(x,y,z_1,\ldots,z_{n_i-2})$. O axioma da substituição é escrito como:

$$\forall z_1,\ldots,z_{n_i-2}\ \forall u\ (\forall x\ (x \in u \ \rightarrow\ \exists! y\ R_i(x,y,z_1,\ldots,z_{n_i-2}))$$
$$\rightarrow\ \exists w\ \forall y\ (y \in w\ \leftrightarrow\ \exists x\ (x \in u \wedge R_i(x,y,z_1,\ldots,z_{n_i-2}))))$$

Com isto temos uma maneira de obter, a partir de um conjunto previamente dado, um outro conjunto cujos elementos satisfazem a propriedade R_i, ou seja, a partir de uma propriedade dada podemos definir um conjunto (por exemplo, do conjunto dos inteiros podemos definir o conjunto cujos elementos têm a propriedade de não serem divisíveis por dois, ou seja, os números impares).

O fato de termos usado o índice i em (ZF6) vem de que este axioma é um esquema para formar axiomas (daí o nome), um para cada R_i.

(ZF7) - Existência do Conjunto Potência

$$\forall x\ \exists y\ \forall z\ (z \in y \leftrightarrow \forall z\ (w \in y \leftrightarrow w \in x))$$

Abreviaremos $\forall z\ (w \in y \leftrightarrow w \in x)$ por $z \subseteq x$.

(ZF7) é interpretado como dizendo que para cada conjunto x existe um outro conjunto y que contém todos os subconjuntos de x. O conjunto de todos os subconjuntos de x é chamado de conjunto potência de x e é denotado por $\mathcal{P}(x)$.

Apesar deste axioma definir um conjunto $y = \mathcal{P}(x)$ a partir de uma propriedade dada (que é a de y ter como elementos todos os subconjuntos de x), ele é independente de (ZF6); em certos modelos para teoria dos conjuntos, existem alguns subconjuntos de conjuntos infinitos que são, de alguma forma, objetos aleatórios, sem forma bem definida, e por isso não definíveis a partir de uma dada propriedade.

(ZF8) - Axioma da Regularidade ou da Fundação

$$\forall y\ \exists x\ (x = \emptyset \vee (y \in x \wedge \forall z\ (z \in x \rightarrow z \notin y)))$$

Este axioma nos garante a não existência de cadeias descendentes infinitas com respeito a $\in$, ou seja, não é permitido $\ldots \in x \in y \in z$. Como consequência para nenhum conjunto x temos $x \in x$. (ZF8) é introduzida na lista de axiomas para evitar problemas como o paradoxo de Russell.

(ZF1) - (ZF8) formam o sistema de axiomas de Zermelo-Fränkel para a teoria de conjuntos.

Daremos agora o axioma da escolha, mas antes precisamos de uma definição.

<u>DEFINIÇÃO</u> 1.9: Uma função é um conjunto f de pares ordenados tal que se $\langle x,y \rangle$ e $\langle x,z \rangle$ pertencem a f então $y = z$. Usaremos a notação Fun(f) para "f é uma função". Dom(f) é o conjunto dos x tal que $\langle x,y \rangle \in f$, e é chamado domínio da função f. Se $\langle y,z \rangle \in f$ escreveremos $f(y) = z$.

(AC) - Axioma da Escolha

$$\forall x\, \exists f\, (\mathrm{Fun}(f) \wedge \mathrm{Dom}(f) = x \wedge \forall y \in x (y \neq \emptyset \rightarrow f(y) \in y))$$

(AC) nos diz que se x é um conjunto cujos elementos são conjuntos, então existe uma função f, chamada função escolha, cujo domínio é x e que mapeia todos os elementos y de x nos elementos do próprio y. De uma maneira mais clara, seja x uma coleção de conjuntos, este axioma nos permite escolher de cada conjunto desta coleção um dado elemento (via função escolha) e então formar um outro conjunto.

Pela interpretação supra tem-se a impressão imediata de que (AC) é intuitivo, tal qual (ZF1) - (ZF8). Uma análise mais profunda nos mostra que é razoável supor a existência de uma função escolha quando x tem um número contável de elementos (pois em certos casos podemos até imaginar um programa de computador que execute essa tarefa), mas é difícil imaginar um processo que nos permita "pescar" elementos quando x tem um número incontável de elementos. Tal comentário torna-se pertinente quando lembramos que o (AC) é equivalente a uma série de afirmações nada triviais em matemática, como por exemplo o *Teorema de Tychonov* que nos diz que o produto cartesiano arbitrário de qualquer coleção de espaços compactos é também um espaço compacto. (AC) também é necessário na demonstração de que um espaço vetorial arbitrário tem uma base. É claro que possíveis resultados não intuitivos derivados deste axioma só aparecem em se tratando de problemas que manipulem com infinitos.

Vários outros axiomas podem se adicionados a ZF, como por exemplo a Hipótese do Contínuo (CH) ou o Axioma de Martin (MA). Podemos também substituir (AC) pelo axioma da escolha na forma fraca, que nos garante a existência da função escolha somente para coleções contáveis de conjuntos. Uma boa discussão destes e de vários outros axiomas, assim como a demonstração de suas independências face a ZF podem ser encontradas em Kunen [32] e referências lá citadas.

Com isto terminamos a nossa exposição sobre os axiomas de Zermelo-Fränkel. Como dissemos antes ZF não é a única maneira de axiomatizarmos a teoria de conjuntos. Um outro sistema de axiomas equivalente, mas que tem a vantagem, do ponto de vista filosófico, de ter um número finito de axiomas (lembremos do axioma da substituição), é o de Gödel-Bernays. Este sistema não foi estudado aqui por ser menos intuitivo que ZF, e por isso mais difícil de ser interpretado e comparado com a teoria de conjuntos de Cantor. Referências sobre o sistema de Gödel-Bernays podem ser encontradas em Stoll [44]. Uma apresentação deste sistema assim como a demonstração de sua equivalência em relação a ZF pode ser encontrada em Cohen [08].

1.4 NOTA SOBRE TEORIA DE MODELOS.

Neste momento podemos nos perguntar: como saber se um dado axioma é um teorema de ZF ou se é independente de ZF? O que são os conjuntos que obedecem a ZF? Estas perguntas ficam mais claras quando estudamos a chamada *Teoria de Modelos*, que começaremos a ver nessa seção. O que faremos aqui é apresentar rapidamente esta teoria, colocando o que não é essencial aqui para os capítulos seguintes. Uma apresentação mais abrangente e detalhada pode ser encontrada em Cohen [08], Jech [28], ou Manin [36].

Antes de estudarmos o que vem a ser um modelo para um dado conjunto de axiomas vejamos um exemplo. Uma *Álgebra de Boole* é uma estrutura $\langle B, \vee, \wedge, ^*, 0_B, 1_B \rangle$ onde B é um conjunto, $\vee$ e $\wedge$

são operações binárias* chamadas respectivamente de união e interseção, * é uma relação unária em B tendo B como domínio, 0_B e 1_B são dois elementos distintos de B, satisfazendo os seguintes axiomas (a, b, c ∈ B):

i) $a \vee (b \vee c) = (a \vee b) \vee c$ e $a \wedge (b \wedge c) = (a \wedge b) \wedge c$;

ii) $a \vee b = b \vee a$ e $a \wedge b = b \wedge a$;

iii) $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

e

$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$;

iv) Para todo a em B

$a \vee 0_B = a$ e $a \wedge 1_B = a$;

v) Para cada a em B existe um elemento * relacionado a^{*} tal que

$a \vee a^{*} = 1_B$ e $a \wedge a^{*} = 0_B$;

Se B é um conjunto cujos elementos obedecem às regras anteriores, então B é um modelo para os axiomas da álgebra de Boole (mais adiante definiremos de uma maneira mais rigorosa o que é um modelo para um conjunto dado de axiomas). Vemos que vários objetos, os mais variados possíveis, devem ser modelos para a álgebra booleana, o que mostra que o conceito de modelo é algo bem geral. Vejamos alguns exemplos de objetos que obedecem ao axiomas *i*) - *v*). São eles:

---

*Os símbolos para intersecao e uniao na álgebra de Boole coincidem com os conectivos lógicos 'e' e 'ou' respectivamente. Dentro do texto sempre ficará claro qual dos dois estaremos usando.

Exemplo 1: A álgebra de 2 elementos do conjunto $B = \{0,1\}$ na qual $\vee$, $\wedge$, e * são definidos por $0 \vee 0 = 0, 0 \vee 1 = 1$, $1 \vee 1 = 1$, $0 \wedge 0 = 0$, $0 \wedge 1 = 0$, $1 \wedge 1 = 1$, $0^* = 1$ e $1^* = 0$.

Exemplo 2: A álgebra do conjunto potência $\mathcal{P}(X)$ de um dado conjunto X, na qual $\vee$, $\wedge$ e * são respectivamente a união, a interseção e a complementação com respeito a X; 0_B e 1_B são respectivamente $\emptyset$ e X.

Exemplo 3: Seja S_0 um conjunto de frases declarativas. Fechemos S_0 com respeito às operações lógicas $\vee$, $\wedge$ e $\neg$ formando assim um outro conjunto de frases declarativas S. Interpretando-se $\wedge$, $\vee$ e $\neg$ na lógica como $\wedge$, $\vee$, e * respectivamente temos que S forma uma álgebra de Boole, conhecida como álgebra de Lindenbaum.

Exemplo 4: A álgebra dos abertos regulares RO(X) de um espaço topológico X. Um subconjunto $\mathfrak{U}$ de X é um aberto regular se o interior do seu fechamento coincide com ele mesmo, isto é, $\mathfrak{U} = (\overline{\mathfrak{U}})^{\circ}$. Neste caso definimos para $u, v \in RO(X)$, $u \vee v$ como $(\overline{v \cup u})^{\circ}$, $u \wedge v$ como $u \cap v$ e u^* como $X - \overline{u}$. RO(X) forma com isto uma álgebra de Boole.

Todos os exemplos anteriores são modelos para os axiomas da álgebra de Boole segundo as interpretações dadas (para a demonstração disso veja as referências [25], [26] e [44]) para $\wedge$, $\vee$, e *. Observemos que o fato dos objetos mencionados nos exemplos 1 - 4 serem modelos para uma álgebra de Boole não implica nenhuma relação entre esses objetos (além, é claro, de obedecerem i) - v)), como homomorfismos ou isomorfismos.

Após esta apresentação da idéia intuitiva de modelo, definiremos este conceito de uma maneira formal.

Suponha que temos uma coleção de frases declarativas que envolvem constantes c_α, $\alpha \in I$ e símbolos relacionais R_β, $\beta \in J$. Seja $\underline{M}$ uma familia de objetos - não necessariamente um conjunto - não vazio e seja $c_\alpha \Rightarrow \bar{c}_\alpha$ uma aplicação dos símbolos de constantes sobre os elementos de $\underline{M}$ e $R_\beta \Rightarrow \bar{R}_\beta$ uma aplicação associando um símbolo relacional k-ário a um subfamília de $\underline{M}\times\underline{M}\times\ldots\times\underline{M}$ (k vezes). Tais mapeamentos nos dão uma interpretação dos c_α e dos R_β em $\underline{M}$.

Após termos definido como interpretar os c_α e os R_β, podemos induzir uma interpretação sobre outras fórmulas da maneira seguinte: Seja agora A uma fórmula com variáveis livres entre $x_1,\ldots,x_n$, $n \geq 0$ e $\bar{x}_1,\ldots,\bar{x}_n$ elementos de $\underline{M}$. Se A é da forma $x_i = x_j$, $x_i = c_j$ ou $c_i = c_j$ então A é verdadeira em $\underline{M}$ se $\bar{x}_i = \bar{x}_j$, $\bar{x}_i = \bar{c}_j$ ou $\bar{c}_i = \bar{c}_j$ respectivamente. Se A é $R(t_1,\ldots,t_m)$ onde em t_i temos $x_1,\ldots,x_n$ variáveis, então A é verdadeira em $\bar{x}_1,\ldots,\bar{x}_n$ se a m-upla $\langle\bar{t}_1,\ldots,\bar{t}_m\rangle$ está em $\bar{R}$. Dada uma função proposicional A, o seu valor verdade será calculado usando-se a dada interpretação via regras do cálculo proposicional, estabelecido nas seções anteriores. Se A é da forma $\forall y\; B(y,x_1,\ldots,x_n)$ então A é verdadeira em $\bar{x}_1,\ldots,\bar{x}_n$ se para todo o $\bar{y}$ em $\underline{M}$ temos $B(y,x_1,\ldots,x_n)$ verdadeira em $\bar{y},\bar{x}_1,\ldots,\bar{x}_n$. Do mesmo modo, $\exists y\; B(y,x_1,\ldots,x_n)$ é verdadeira em $\bar{x}_1,\ldots,\bar{x}_n$ se existe algum $\bar{y}$ em $\underline{M}$ tal que $B(y,x_1,\ldots,x_n)$ é verdadeira em $\bar{y},\bar{x}_1,\ldots,\bar{x}_n$.

Uma sentença é dita restrita se todo quantificador que nela ocorre seja da forma $\forall x \in y$ ou $\exists x \in y$. Seja $\varphi(x)$ restrita e com uma variável livre x. Se B é do tipo $\exists x\ \varphi(x)$ nós a chamaremos de Σ_1; se B for do tipo $\forall x\ \varphi(x)$ nós a chamaremos de Π_1.

<u>DEFINIÇÃO</u> 1.10: Se S é um conjunto de frases declarativas que contém c_α e R_β, $\underline{M}$ é uma família como acima, e $c_\alpha \Rightarrow \bar{c}_\alpha$ e $R_\beta \Rightarrow \bar{R}_\beta$ são aplicações definidas como acima, dizemos que $\underline{M}$ é um modelo para S (segundo uma interpretação dada) se todas as frases declarativas de S são verdadeiras em $\underline{M}$.

Esta definição obviamente concorda com a idéia intuitiva dada anteriormente para o caso das álgebras de Boole. Como dada uma álgebra booleana podemos definir uma sub-álgebra ou em teoria de grupos podemos definir sub-grupos, o mesmo podemos fazer para modelos. Seja $\underline{N} \subset \underline{M}$ duas famílias de objetos e sejam φ e ψ interpretações em $\underline{N}$ e $\underline{M}$ respectivamente que são compatíveis, no sentido que φ é uma restrição de ψ em $\underline{N}$. Se $\underline{M}$ e $\underline{N}$ são modelos para S, então $\underline{N}$ é um sub-modelo de $\underline{M}$.

<u>DEFINIÇÃO</u> 1.11: Uma função proposicional é $(\underline{M}, \underline{N})$-absoluta se o seu valor verdade é o mesmo em $\underline{M}$ e $\underline{N}$.

De cara vemos que existem fórmulas que não devem ser absolutas, como por exemplo as fórmulas Σ_1, pois se em $\underline{M}$ existe um elemento tal que $\varphi(x)$ seja verdadeira, em $\underline{N}$ este elemento pode não existir.

Um problema importante é saber se um dado conjunto de frases declarativas S é consistente, ou seja, se não podemos derivar de S (via cálculo proposicional) a frase declarativa $(A) \wedge (\neg(A))$ para algum A. Enunciaremos sem demonstrar um teorema que diz respeito à consistência de S:

TEOREMA 1.1: Se A é uma frase declarativa válida, é verdadeira em qualquer modelo. Se um conjunto de frases declarativas S tem um modelo então é consistente.

Outros dois teoremas importantes são devido a Gödel, e falam sobre a cardinalidade e a existência de determinados modelos. São eles:

TEOREMA 1.2 (de Gödel para o cálculo de predicados): Se S é um conjunto consistente de frases declarativas então existe um modelo para S cuja cardinalidade não excede a cardinalidade do número de frases declarativas em S se S for infinito e é no máximo contável se S for finito.

TEOREMA 1.3 (de Gödel sobre a completude do cálculo proposicional): Se S não contém quantificadores e é consistente então existe um modelo $\underline{M}$ em que todo elemento de $\underline{M}$ é da forma $\bar{c}_\alpha$ para algum c_α que apareça em S.

Uma consequência destes teoremas é o:

COROLÁRIO 1.4: Se A não é derivável de S então existe um modelo para S em que A é falsa.

Como dissemos no início dessa seção, um sistema de axiomas não precisa ter necessariamente um único modelo, nem diferentes modelos precisam ter algum tipo de isomorfismo entre si. Este fato é realçado pelo

COROLÁRIO 1.5: Se S admite um modelo infinito ou mesmo modelos finitos arbitariamente grandes, então S admite modelos de cardinalidades arbitrariamente grandes.

1.5 O TEOREMA DE LOEWENHEIN-SKOLEM.

Seja $\underline{M}$ um modelo para os axiomas de ZF, isto é, estes axiomas são verdadeiros, segundo uma interpretação dada, para os objetos de $\underline{M}$ e seja $\bar{A} \in \underline{M}$ um conjunto no nosso modelo. $\omega_o \in \underline{M}$ representa os inteiros no modelo (como dissemos antes os inteiros existem devido ao axioma da indução).

<u>DEFINIÇÃO</u> 1.12: $\bar{A}$ é enumerável em $\underline{M}$ se e somente se existe uma função $f \in \underline{M}$, $f : \omega_o \to \bar{A}$ tal que f seja 1-1 e bijetiva. $\bar{A}$ é incontável, ou não enumerável, se é infinito e se tal função f não existe.

Esta definição é semelhante à dada na introdução desse capítulo, com a diferença de que aqui, por estarmos trabalhando com um modelo $\underline{M}$, exigimos que $f \in \underline{M}$.

Definamos agora o que vêm a ser *Modelos Elementarmente Equivalentes*.

DEFINIÇÃO 1.13: Sejam $\underline{M}_1$ e $\underline{M}_2$ dois modelos para um dado sistema formal de axiomas. $\underline{M}_1$ e $\underline{M}_2$ são elementarmente equivalentes se as frases declarativas na linguagem formal que são verdadeiras em $\underline{M}_1$ são exatamente aquelas que são verdadeiras em $\underline{M}_2$. Se $\underline{M}_1 \subseteq \underline{M}_2$ diremos que $\underline{M}_1$ é um submodelo elementar de $\underline{M}_2$ se as constantes c_α são as mesmas em $\underline{M}_1$ e $\underline{M}_2$, as relações $\bar{R}_\beta$ em $\underline{M}_1$ são as restrições das relações R_β em $\underline{M}_2$ e para cada fórmula $A(x_1,...,x_n)$ se os $\bar{x}_i$ estão em $\underline{M}_1$ então $A(x_1,..,x_n)$ é verdadeira em $\underline{M}_1$ em $\bar{x}_1,..,\bar{x}_n$ se e somente se é verdadeira em $\underline{M}_2$ em $\bar{x}_1,...,\bar{x}_n$.

Em posse da definição de sistemas elementarmente equivalentes podemos enunciar o teorema de Löwenhein-Skolem.

TEOREMA 1.6 (Löwenhein-Skolem): Seja $\underline{M}$ um modelo para uma coleção T de símbolos de constantes e símbolos relacionais. Existe um submodelo elementar de $\underline{M}$ cuja cardinalidade não excede a de T se T é infinito e é no máximo contável se T é finito.

Prova: A nossa demonstração é idêntica à dada por Cohen [08]. Uma demonstração um pouco diferente, mas essencialmente a mesma, pode ser encontrada em Manin [36].

Seja N uma subfamília de $\underline{M}$ que contenha todas as constantes $\bar{c}_\alpha$. Criaremos um outro conjunto N^* da seguinte maneira: considere $A(y,x_1,\ldots,x_n)$ uma fórmula arbitrária de n + 1 variáveis. Para cada n-upla $\bar{x}_1,\ldots,\bar{x}_n$ em N onde houver um $\bar{y} \in \underline{M}$, tal que $A(y,x_1,\ldots,x_n)$ é verdadeiro em $\underline{M}$ em $\bar{y},\bar{x}_1,\ldots,\bar{x}_n$, escolhemos um destes e juntamos a N. Se fizermos isto para todas as fórmulas A e todos os x_i possíveis teremos um $N^* \supset N$. Se N é infinito o número de n-uplas de N tem cardinalidade igual a N e se N é finito tem cardinalidade contável. Com isto a cardinalidade de N^* deve obedecer a $| N^* | \leq | N | + | T | + \aleph_0$. Definamos agora um outro conjunto $\underline{N}' = \bigcup_k N_k$, tal que $N_0 = \{ \bar{c}_\alpha \}$ e $N_{k+1} = N_k^*$. Como $| N_0 | \leq | T |$, então $\underline{N}'$ obedece à restrição imposta à cardinalidade pelo enunciado do teorema. Temos que mostrar ser $\underline{N}'$ é um submodelo elementar de $\underline{M}$, o que completará a demonstração. Para tal mostraremos que $A(x_1,\ldots,x_n)$ é verdadeira em $\underline{N}'$ se e somente se ela é verdadeira em $\underline{M}$, sendo A uma fórmula arbitrária. A demosntração é feita por indução. Seja $A(x_1,\ldots,x_n)$ uma fórmula com r quantificadores. Pela própria construção de $\underline{N}'$, se r = 0 então A é verdadeira em $\underline{N}'$se e somente se é verdadeira em $\underline{M}$. A hipótese indutiva que usaremos é a seguinte: para qualquer fórmula $A(x_1,\ldots,x_m)$ com menos do que r quantificadores e qualquer $\bar{x}_1,\ldots,\bar{x}_n$ em $\underline{N}'$, A é verdadeira em $\underline{N}'$ em $\bar{x}_1,\ldots,\bar{x}_m$ se e somente se é verdadeira em $\underline{M}$ em $\bar{x}_1,\ldots,\bar{x}_m$. Podemos agora supor que A começa com um quantificador, sendo escrito da forma $\exists y\ B(y,x_1,\ldots,x_n)$, o que sempre pode ser feito pois mesmo A sendo do tipo $\forall y\ B(y,x_1,\ldots,x_n)$ podemos escreve-la como $\neg\exists y\ \neg B(y,x_1,\ldots,x_n)$. Sejam $\bar{x}_1,\ldots,\bar{x}_n$ elementos arbitrários de $\underline{N}'$. Por construção todos os x_i estão em N_k para algum k, e se existe um $\bar{y} \in \underline{M}$ tal que $B(y, x_1, \ldots, x_n)$ é verdadeira em $\underline{M}$ então $\bar{y}$ também está em $N_{k+1} = N_k^*$ e portanto $\bar{y} \in \underline{N}'$. B tem $r-1$ quantificadores e da hipótese de indução temos que B é verdadeira em $\bar{y}, \bar{x}_1, \ldots, \bar{x}_n$ em $\underline{N}'$, o que implica que A é verdadeira em $\underline{N}'$. Se por outro lado tal $\bar{y}$ não existe em $\underline{M}$ então não existe nenhum $\bar{y}$ em $\underline{N}'$ pela hipótese de indução, o que completa a demonstração.

$\therefore$

Uma importante consequência do teorema anterior é a existência de um modelo contável para os axiomas de Zermelo-Fränkel ((ZF1) - (ZF8)). Aqui surge uma aparente contradição, chamada paradoxo de Skolem: se usando ZF construimos toda a teoria de conjuntos, então destes axiomas podemos obter os números reais ($|\mathbb{R}| = |\mathcal{P}(\omega_0)|$). Ora, como pode existir um modelo contável para ZF se dentro de ZF temos um número incontável de objetos? A resposta a esse paradoxo é relativamente simples. Como dissemos anteriormente, o fato de um conjunto ser contável depende da existência de um mapeamento 1-1 entre esse conjunto e ω_0, conforme a definição 1.6, e se esse mapeamento não existe o conjunto é incontável. Com isto, $\underline{N}'$ tem um número contável de objetos quando visto de "fora", mas quando estamos dentro de $\underline{N}'$ existem conjuntos que são não-contáveis pois não existe um mapeamento 1-1 entre estes conjuntos e o ω_0 em $\underline{N}'$.

1.6 O PROBLEMA DA DECISÃO.

Vários outros sistemas formais podem ser obtidos na linguagem $L_1^=$ exposta na seção 1.2, além da teoria de conjuntos. Um destes sistemas que tem grande importância é a aritmética elementar, cujo estudo nos será útil para entendermos melhor o famoso teorema da indecidibilidade de Gödel.

Duas são as formalizações mais conhecidas para a aritmética, chamadas Z_1 e Z_2. São elas:

Axiomas de Z_1:

1. $\forall x, y\ \exists! z\ (x + y = z)$;
2. $\forall x, y\ \exists! z\ (x\ .\ y = z)$;
3. $\forall x\ ((x + 0 = x) \wedge (x\ .\ 1 = x))$ onde 0 e 1 são constantes;
4. $\forall x, y\ (x + (y + 1) = (x + y) + 1)$;
5. $\forall x, y\ ((x + 1 = y + 1) \rightarrow x = y)$;
6. $\forall x, y\ (x\ .\ (y + 1) = x\ .\ y + x)$;
7. $\forall x\ (\neg(x + 1 = 0))$;

8_m. $\forall t_1, \ldots, t_k\ [(A_m(0, t_1, \ldots, t_k) \wedge \forall y\ (A_m(y, t_1, \ldots, t_k) \rightarrow A_m(y + 1, t_1, \ldots, t_k))] \rightarrow \forall x\ A_m(x, t_1, \ldots, t_k)$;

Axiomas de Z_2:

1. $\forall x, y\ (x = y \leftrightarrow \forall z\ (z \in x \leftrightarrow z \in y))$;
2. $\forall x, y\ (x \notin \emptyset)$;
3. $\forall x, y\ \exists z\ \forall w\ (w \in z \leftrightarrow w = x \vee w = y)$;

4. $\forall x,y\ \exists z\ \forall w\ (w \in z \leftrightarrow w \in x \vee w \in y)$;

5_m. $\forall t_1,\ldots,t_k\ [A_m(0,t_1,\ldots,t_k) \wedge \forall y\ (Int(y) \wedge A(y,t_1,\ldots,t_k) \rightarrow A_m(y+1,t_1,\ldots,t_k))] \rightarrow \forall x\ (Int(x) \rightarrow A_m(x,t_1,\ldots,t_k))$;

Valem aqui alguns comentários sobre os axiomas Z_1 e Z_2. O índice m posto em 8 de Z_1 e em 5 de Z_2 é usado para indicar que na realidade esses axiomas não representam cada um único axioma mas sim uma infinidade de axiomas. 1, 2, 3 e 4 de Z_2 são respectivamente (ZF1), (ZF2), (ZF3) e (ZF4). Int(x) em Z_2 significa "x é um inteiro". 5_m e 8_m são chamados de axiomas da indução matemática.

Usando ZF podemos derivar toda a aritmética formal, mas Z_1 e Z_2 têm um papel importante no teorema de Gödel. Usando-se a teoria das funções recursivas primitivas obtemos o seguinte teorema:

TEOREMA 1.7: Se $f(x_1,\ldots,x_k)$ é uma função recursiva primitiva, existe uma fórmula $A(x_1,\ldots,x_k)$ em Z_2 tal que:

i) $\forall x_1,\ldots,x_k\ \exists!y\ A(x_1,\ldots,x_k,y)$ é uma frase declarativa verdadeira sobre os inteiros e é demonstrável em Z_2.

ii) Se $f(x_1,\ldots,x_n) = m$ então $A(x_1,\ldots,x_k,m)$ é demonstrável em Z_2.

Vale ressaltar algo que será importante no teorema de Gödel que é o fato de uma frase ser verdadeira num modelo não implicar que ela seja demonstrável em Z_1 ou Z_2. Uma maneira elegante de se mostrar isso é mapeando-se o cálculo proposicional numa álgebra de Boole (a álgebra de Lindenbaum) e provando que o conjunto das sentenças demonstráveis é um filtro na álgebra e que o conjunto das sentenças verdadeiras é um filtro maximal (ultrafiltro). Então, sendo $\mathcal{D}$ e $\mathcal{V}$ os conjuntos de sentenças demostráveis e verdadeiras teremos $\mathcal{D} \subseteq \mathcal{V}$. Se $\mathcal{D} = \mathcal{V}$ diremos que a teoria é completa; se $\mathcal{D} \subset \mathcal{V}$ a teoria é incompleta (para detalhes veja [26] ou [44]).

Um outro teorema análogo ao 1.7 existe para Z_1, como era de se esperar, pois tanto Z_1 quanto Z_2 são formalizações para a aritmética elementar.

COROLÁRIO 1.9: O problema da decisão para Z_2 (ou Z_1) é insolúvel, ou seja, dadas todas as frases declarativas de Z_2 (ou Z_1) (e deste modo todas as afirmações possíveis sobre a aritmética) não existe um processo mecânico (funções recursivas parciais, ou programa de computador) que nos diga se cada afirmação é verdadeira ou falsa.

Estamos agora em condições de apresentar um dos resultados mais importantes da matemática, o teorema da incompletude de Gödel para a aritmética formal.

TEOREMA 1.10 (da incompletude de Gödel): Existe uma frase declarativa A em Z_1 tal que nem A nem $\neg$A podem ser demostrados a partir dos axioma de Z_1.

Esboço da Prova*: Fazemos correspoder a cada fórmula em Z_1 um número, chamado número de Gödel, e enumeramos as sentenças em Z_1. Com isso, operações lógicas sobre dadas sentenças seriam equivalentes a uma determinada função recursiva primitiva sobre o seu número de Gödel. Se enumerarmos todas as demostrações possiveis concluimos que as sentenças demostráveis formam a imagem de uma função recursivas primitivas.

Pelo teorema 1.8 existe uma função cuja imagem não é recursiva. Com o auxílio de tal função mostra-se que se todas as sentenças forem demostráveis teremos uma inconsistência. Por outro lado se quisermos que a aritmética seja consistente então existirão sentenças que não são demostráveis.

Para detalhes da prova veja [22].

$\therefore$

1.7 MODELOS BOOLEANOS E FORCING.

Vejamos como obter a partir dos axiomas de ZF um universo $\underline{V}$, chamado de *Universo de Von Neumman*, que é um modelo para estes axiomas.

---

*A prova rigorosa desse teorema pode ser encontrada no artigo original de Goedel [22]; demostracoes menos detalhadas podem ser vistas em [08] e [36]; Uspenski [52] faz uma prova bem clara,mas detalhada, usando teoria da computacao e em [41] temos um esboco da prova original de Goedel duma maneira bastante acessível.

<u>DEFINIÇÃO</u> 1.14: O universo $\underline{V}$ é a classe de conjuntos $\bigcup_{\alpha \in Ord} V_\alpha$ definido por indução pelo seguinte:

$V_0 = \emptyset$;

$V_{\alpha+1} = \mathcal{P}(V_\alpha)$;

$V_\alpha = \bigcup_{\beta < \alpha} V_\beta$, se α é um ordinal limite.

Os modelos booleanos são construidos a partir desse universo para um outro $\underline{V}^B$, chamado de extensão booleana de $\underline{V}$, definido por recursão como:

$$V_\alpha^B = \{x : Fun(x) \wedge Ran(x) \subseteq B \wedge \exists \xi < \alpha \, (Dom(x) \subseteq V_\xi^B)\}$$

$$\underline{V}^B = \{x : \exists \alpha \, (x \in V_\alpha^B)\}$$

onde B é uma álgebra booleana completa (uma álgebra de Boole é completa se existe um Inf e um Sup para todo o subconjunto dessa álgebra). Pode-se ver das definições anteriores que se $B = 2 = \{0, 1\}$ o universo $\underline{V}^2$ é o conjunto de todas as funções características de $\underline{V}$, o que nos mostra que deve exister uma relação biunívoca entre os elementos de $\underline{V}^2$ e $\underline{V}$. Ainda desta definição vemos que os conjuntos em $\underline{V}^B$, também chamad--
conjuntos B-valorados, são funções que
cujo domínio é um conjunto B-valorado.

Todas as sentenças construidas e
construidas em $\underline{V}^B$. O que fazemos é
B-valorado a estas sentenças em $\underline{V}^B$. O q

agora é que os valores verdade poderão assumir qualquer valor sobre B, isto é, $\|.\|$ será um mapa de sentenças em $\underline{V}^{B}$ para B. Intuitivamente isso significa que estamos modificando o conceito de verdade permitindo a existência de sentenças que podem ser nem verdadeiras nem falsas, tendo seus valores verdade situados em algo como "quase verdadeiro", "quase falso", " igual probabilidade de se verdadeiro e falso" etc.

Definiremos agora como se relacionam os valores booleanos $\|.\|$ de duas sentenças σ e τ:

$$\| \sigma \wedge \tau \| = \| \sigma \| \wedge \| \tau \|$$

$$\| \neg \sigma \| = \| \sigma \|^{*}$$

Se $\phi(x)$ é uma fórmula tal que $\| \phi(x) \|$ tenha sido definida para todo $u \in \underline{V}^{B}$, definimos

$$\| \exists x \; \phi(x) \| = \bigvee_{u \in \underline{V}^{B}} \| \phi(u) \|$$

onde $\vee$ representa o supremo.

Lembrando das definições de $\sigma \vee \tau$, $\sigma \to \tau$, $\tau \leftrightarrow \sigma$ e $\forall x \; \phi(x)$ em função de $\exists$, $\wedge$ e $\neg$ obtemos:

$$\| \sigma \vee \tau \| = \| \sigma \| \vee$$

$$\| \sigma \to \tau \| = \| \sigma \| \Rightarrow |$$

$$\| \sigma \leftrightarrow \tau \| = \| \sigma \| \Leftrightarrow$$

$$\| \forall x \; \phi(x) \| = \bigwedge_{u \in V^{B}} \| \phi$$

onde $a, b \in B$, $a \Rightarrow b$ e $a \Leftrightarrow b$ abreviam respectivamente $a^* \vee b$ e $(a \Rightarrow b) \wedge (b \Rightarrow a)$ e $\bigwedge$ representa o ínfimo no álgebra.

Para "=" e "∈" temos as regras

$$\| a = a \| = 1$$

$$\| a = b \| = \| b = a \|$$

$$\| \phi(a) \| \wedge \| a = b \| \leq \| \phi(b) \|$$

Em colocando valores booleanos para as relações "∈" e "=" somos guiados pela idéia de função característica, e damos o valor verdade de $x \in y$ com uma função $y(x)$ que assume valores sobre a álgebra B. Com isso não dizemos mais se x é com certeza um elemento de y e sim qual é a probabilidade dele ser. Temos as seguintes definições para $\| x \in y \|$:

$$\| x \in y \| = \bigvee_{w \in Dom(y)} [y(w) \wedge \| x = w \|]$$

$$\| x = y \| = \bigwedge_{w \in Dom(x)} [x(w) \Rightarrow \| w \in y \|] \wedge \bigwedge_{w \in Dom(y)} [y(u) \Rightarrow \| u \in x \|]$$

Nesta interpretação dos valores verdade dizemos que σ é verdadeira se o seu valor booleano é 1. A uma sentença σ verdadeira em $\underline{V}^{B}$ escrevemos "$\underline{V}^{B} \models \sigma$" que é lida como "
verdadeira em $\underline{V}^{B}$.

TEOREMA 1.11: Todos os axiomas do cá
1° ordem juntamente com as regra
verdadeiras em $\underline{V}^{B}$.

TEOREMA 1.12: Todos os axiomas de ZFC são verdadeiros em $\underline{V}^{B}$.

As provas desses teoremas é feita calculando-se o valor verdade de cada axioma em $\underline{V}^{B}$. Tais demostrações podem ser encontradas em [03], [16], [32] ou [36].

Diferentes álgebras booleanas são usadas para construirmos os modelos; esses serão usados para demonstrar a independência de determinadas sentenças face a ZFC. Isto é feito da maneira seguinte: digamos que A seja a sentença que queremos mostrar ser indenpedente; construimos dois modelos $\underline{V}^{B}$ e $\underline{V}^{B'}$ tal que em um A é vedade e no outro ¬A é verdade.

Uma técnica muito usada para se fazer tal tipo de demonstração é o *forcing* introduzido por Paul Cohen em 1963. O fim dessa seção será dedicado ao estudo do *forcing* via modelos booleanos e também ao estudo de algumas propriedades de determinados conjuntos em $\underline{V}^{B}$ (para maiores detalhes veja [03], [16] ou [32]). Como uma aplicação do *forcing* mostraremos a clássica prova da independência da Hipótese do Contínuo.

Nos parágrafos anteriores mencionamos existir uma relação biunívoca entre os elementos de $\underline{V}$ e $\underline{V}^{2}$. Um mapa podia ser definido entre esses dois modelos relacionando os seus elementos. Pode-se mostrar a existência de um mapa similar (que em geral não é 1-1) dos elementos de $\underline{V}$ sobre $\underline{V}^{B}$. Este mapa é definido por recursão como:

<u>DEFINIÇÃO</u> 1.15: Para cada $x \in \underline{V}$

$$\hat{x} = \{\langle \hat{y}, 1\rangle : y \in x\}$$

Temos associado a cada $x \in \underline{V}$ um $\hat{x}$; $\hat{x} \in \underline{V}^2$ e como consequência $\hat{x} \in \underline{V}^B$ pois $\underline{V}^2 \subseteq \underline{V}^B$. Os objetos de $\underline{V}^B$ da forma $\hat{x}$ são chamados de objetos *standard*.

Com o que temos podemos estabelecr uma série de resultados que nos serão úteis na demonstração da hipótese do contínuo (para isto seguiremos o texto de Doria [16]).

Sejam $\underline{M}$ e $\underline{N}$ dois modelos booleanos para um dado conjunto de axiomas; "$\underline{L} \models \varphi$" é a afirmação '$\varphi$ é verdadeira no modelo $\underline{L}$'.

PROPOSIÇÃO 1.13: Se ψ é Σ_1 então $\underline{M} \models \psi$ implica $\underline{N} \models \psi$. Se φ é Π_1 então $\underline{N} \models \varphi$ implica $\underline{M} \models \varphi$.

<u>DEFINIÇÃO</u> 1.16: To(x) abrevia $\forall y \in x\ \forall z \in x\ (y \in z \vee y = z \vee z \in y)$; Trans(x) abrevia $\forall v \in x\ \forall z \in v\ (z \in x)$; Ord(x) abrevia (Tans(x) $\wedge$ To(x)).

To(x), Tans(x) e Ord(x) se lêm respectivamente como "x é totalmente ordenado", "x é transitivo" e "x é um ordinal". Note que as definições anteriores formalizam o que vem a ser um ordinal.

PROPOSIÇÃO 1.14: Ord(x) se e somente se $\underline{V}^B \models \mathrm{Ord}(\hat{x})$.

PROPOSIÇÃO 1.15: $|\ x\ | = |\ y\ |$ é uma fórmula Σ_1.

<u>DEFINIÇÃO</u> 1.17: Lord(x) abrevia $[\forall y \in x\ \exists z \in x\ (y \in z) \wedge$

Ord(x)].

DEFINIÇÃO 1.18: $x = \omega_0 \leftrightarrow \mathrm{Lord}(x) \wedge \forall y \in x\, (\neg \mathrm{Lord}(y))$.

Seguindo as definições anteriores para Ord(x) temos que Lord(x) significa intuitivamente "x é um ordinal limite" sendo ω_0 o primeiro ordinal limite. Estas definições nos dão:

PROPOSIÇÃO 1.16: $x = \omega_0$ se e somente se $\underline{V}^{B} \models \hat{x} = \hat{\omega}_0 = \omega_{\hat{0}}$.

PROPOSIÇÃO 1.17: Para todos os ordinais α, $\underline{V}^{B} \models \hat{\aleph}_{\alpha} \leq \aleph_{\hat{\alpha}}$.

DEFINIÇÃO 1.19: Uma álgebra booleana satisfaz a ccc (condição da cadeia contável) se e somente se toda a anticadeia ($A \subseteq B$ é uma anticadeia em B se $a \wedge b = 0$ para quaisquer dois elementos distintos de A) nela é contável.

Com isto, uma álgebra B satisfaz a ccc se todo o conjunto disjunto de elementos não nulos de B é contável.

PROPOSIÇÃO 1.18: Se B satisfaz a ccc então, para qualquer $\alpha, x, y \in \underline{V}$,

i) $\mathrm{Card}(\alpha) \rightarrow \underline{V}^{B} \models \mathrm{Card}(\hat{\alpha})$;

ii) $\underline{V}^{B} \models \hat{\aleph}_{\alpha} = \aleph_{\hat{\alpha}}$;

iii) $|x| = |y| \rightarrow \underline{V}^{B} \models |\hat{x}| = |\hat{y}|$;

onde Card(x) significa "x é um cardinal".

As demonstrações das proposições anteriores podem ser encontradas em [16] ou em [03].

Seja agora $P \subset B$ um conjunto fixo parcialmente ordenado.

DEFINIÇÃO 1.20: Dois elementos $p, q \in P$ são ditos compatíveis, abreviadamente Com(p, q), se existe um $r \in P$ tal que $r \leq p$ e $r \leq q$.

DEFINIÇÃO 1.21: P é dito ser refinado se $\forall p, q \in P\ (\neg q \leq p \rightarrow \exists p' \leq q\ (\neg Com(p, q')))$.

DEFINIÇÃO 1.22: Um subconjunto X de uma álgebra de Boole B é denso se $0 \notin X$ e para cada $0 \neq b \in B$ existe um $x \in X$ tal que $x \leq b$.

DEFINIÇÃO 1.23: O par $\langle B, e\rangle$ é um fecho booleano de P se:

i) B é uma álgebra booleana completa;

ii) "e" é um isomorfismo ordenado de P sobre um subconjunto denso de B.

DEFINIÇÃO 1.24: P é uma base para B se é refinado e se $\langle B, e\rangle$ é um fecho booleano para P.

Sejam x, y conjuntos não vazios e C(x,y) o conjunto de todos os mapeamentos com domínio finito em x e contradominio em y. Colocamos como relação de ordem parcial em C(x,y) a inclusão inversa $\supseteq$, isto é, $x \leq y$ se e somente se $x \supseteq y$. Para $p \in C(x,y)$ (onde y^x é o conjunto de todos os mapas de x em y)

$$N(p) = \{f \in y^x : p \subseteq f\}$$

Com isto temos que $\langle RO(y^x), N\rangle$ é um fecho booleano e $C(x,y)$ uma base para $RO(y^x)$.

Estamos aptos a definir o que vem a ser forçar uma sentença em um modelo booleano. Para uma sentença σ em B, dizemos que $p \in P$, onde P é uma base para B, *força* σ, escrito como $p \Vdash \sigma$, se e somente se $p \leq \| \sigma \|$. As principais propriedades do *forcing* são expressas no teorema seguinte:

TEOREMA 1.19: Sejam σ e τ sentenças em $\underline{V}^B$ e seja $\phi(x)$ uma fórmula em $\underline{V}^B$. Então:

i) $p \Vdash \neg\sigma$ se e somente se $\neg\exists q \leq p(q \Vdash \sigma)$;

ii) $p \Vdash \sigma \wedge \tau$ se e somente se $p \Vdash \sigma$ e $p \Vdash \tau$;

iii) $p \Vdash \sigma \vee \tau$ se e somente se $\forall q \leq p\ \exists r \leq q(r \Vdash \sigma$ ou $r \Vdash \tau)$;

iv) $p \Vdash \sigma \rightarrow \tau$ se e somente se $\forall q \leq p(q \Vdash \sigma \rightarrow \exists r \leq q(r \Vdash \tau))$;

v) $p \Vdash \forall x\ \phi(x)$ se e somente se $\forall u \in \underline{V}^B(p \Vdash \phi(u))$;

vi) $p \Vdash \exists x\ \phi(x)$ se e somente se $\forall q \leq p\ \exists r \leq q\ \exists u \in \underline{V}^B$ $(r \Vdash \phi(u))$;

vii) para $a \in \underline{V}$, $p \Vdash \forall x \in \hat{a}\ \phi(x)$ se e somente se $\forall x \in a(p \Vdash \phi(\hat{x}))$;

viii) para $a \in \underline{V}$, $p \Vdash \exists x \in \hat{a}\ \phi(x)$ se e somente se $\forall q \leq p\ \exists r \leq q \exists x \in a(r \Vdash \phi(\hat{x}))$;

ix) $\| \sigma \| = 0$ se e somente se $\neg \exists p(p \Vdash \sigma)$;

x) $\| \sigma \| = 1$ se e somente se $\forall p(p \Vdash \sigma)$;

xi) $\forall p\ \exists q \leq p(q \Vdash \sigma$ ou $q \Vdash \neg\sigma)$;

xii) $p \Vdash \sigma$ implica $\neg(p \Vdash \neg\sigma)$;

xiii) $(q \leq p$ e $p \Vdash \sigma)$ implica $q \Vdash \sigma$;

Vamos provar agora a independência da Hipótese do Contínuo (CH) via modelos booleanos. A CH é a seguinte afirmação (para uma discussão detalhada veja [23]): $2^{\aleph_0} = \aleph_1$, ou seja, o primeiro cardinal depois de $\aleph_0$ é o contínuo. A Hipótese Generalizada do Contínuo (GCH) nos diz que para todo o cardinal K vale $2^k = k^+$ onde k^+ representa o cardinal imediatamente maior que k. Para demontrarmos a independência apresentaremos um modelo no qual a CH é violada e outro no qual ela é válida. A nossa prova será idêntica à dada por Bell [03], que por sua vez em pouco modifica a de Cohen [07].

TEOREMA 1.20: Suponha que $\aleph_\alpha^{\aleph_0} = \aleph_\alpha$ e seja $B = RO(2^{\omega_0 \times \omega_\alpha})$. Então

$$\underline{V}^B \models 2^{\aleph_0} = \aleph_\alpha$$

Prova: Antes precisamos de um lema.

Lema 1.21: Para cada conjunto I, seja 2^I o espaço produto onde a 2 é dado uma topologia discreta. Se $|\ I\ | = \aleph_\alpha$ então

$$\aleph_\alpha \leq |\ RO(2^I)\ | \leq \aleph_\alpha^{\aleph_0}$$

Prova do Lema 1.21: Veja Bell [002] pag. 59.

Com esse lema temos

$$\aleph_\alpha \leq | B | \leq \aleph_\alpha^{\aleph_0}$$

mas pelo enunciado do teorema $\aleph_\alpha^{\aleph_0} = \aleph_\alpha$, o que aplicando na desigualdade anterior resulta em $| B | = \aleph_0$.

Com isto, lembrando que os objetos de $\underline{V}^{\mathbf{B}}$ são funções B-valoradas, obtemos

$$| \operatorname{Dom} \mathcal{P}^{\mathbf{B}}(\hat{\omega}) | = | B^{\operatorname{Dom}(\omega)} | = \aleph_\alpha^{\aleph_0} = \aleph_\alpha$$

Lema 1.22: Para qualquer $u \in \underline{V}^{\mathbf{B}}$ podemos encontrar um $f \in \underline{V}^{\mathbf{B}}$ tal que

$$\underline{V}^{\mathbf{B}} \models \operatorname{Fun}(f) \wedge \operatorname{Dom}(f) = \operatorname{Dom}(u)^\wedge \wedge u \subseteq \operatorname{Ran}(f)$$

e

$$\underline{V}^{\mathbf{B}} \models | u | \leq | \operatorname{Dom}(u)^\wedge |$$

Prova do Lema 1.22: Veja Bell [02] pag. 45.

Aplicando esse lema ao resultado anterior temos

$$\underline{V}^{\mathbf{B}} \models | \mathcal{P}^{\mathbf{B}}(\hat{\omega}) | \leq | \aleph_\alpha |$$

Como B satisfaz a ccc temos $\underline{V}^{\mathbf{B}} \models | \aleph_\alpha | = \hat{\aleph}_\alpha$ pela proposição 1.18, o que nos dá

$$\underline{V}^{B} \models |\mathcal{P}(\omega)| = 2^{\aleph_0} \leq \aleph_{\alpha}^{\wedge}$$

Definamos para cada $\nu \in \omega_{\alpha}$ um $u_{\nu} \in \underline{V}^{B}$ por $\mathrm{Dom}(u_{\nu}) = \mathrm{Dom}(\hat{\omega}_0)$ e

$$u_{\nu}(\hat{n}) = \{f \in 2^{\omega_0 \times \omega_{\alpha}} : f(n,\nu) = 1\}$$

$$\| u_{\nu} \subseteq \hat{\omega}_0 \| = \bigwedge_{n \in \omega_0} [u_{\nu}(\hat{n}) \Rightarrow \| \hat{n} \in \hat{\omega}_0 \| = 1$$

Seja $P = C(\omega_0 \times \omega_{\alpha}, 2)$ uma base para B. Para $p \in P$

$$p \Vdash \hat{n} \in u_{\nu} \text{ se e somente se } p(n,\nu) = 1$$

$$p \Vdash \hat{n} \notin u_{\nu} \text{ se e somente se } p(n,\nu) = 0$$

Lema 1.23: Se $\mu, \nu < \omega_{\alpha}$ e $\mu \neq \nu$, então $\| u_{\nu} = u_{\mu} \| = 0$.

Prova do lema 1.23: Suponha que seja falso. Então existe um $\mu, \nu < \omega_{\alpha}$, $\mu \neq \nu$ tal que $p \in P$ e $p \Vdash u_{\nu} = u_{\mu}$. Seja $n \in \omega_0$ e $\langle \eta, \xi \rangle \notin \mathrm{Dom}(p)$, $\xi < \omega_{\alpha}$

$$p' = p \cup \{\langle\langle \eta, \xi \rangle, 1\rangle\} \cup \{\langle\langle \eta, \nu \rangle, 0\rangle\}$$

$p' \Vdash \hat{n} \in u_{\mu} \wedge \hat{n} \notin u_{\nu}$, então $p' \Vdash u_{\mu} \neq u_{\nu}$. Desde que $p' \leq p$ e $p \Vdash u_{\mu} = u_{\nu}$ obtemos $p' \Vdash u_{\mu} = u_{\nu}$ o que pelo teorema 1.19 não é possível, resultando numa contradição. $\therefore$

Definamos $f \in \underline{V}^{B}$ como

$$f = \{\langle \hat{\nu}, u_{\nu} \rangle^{B} : \nu < \omega_{\alpha}\} \times \{ 1 \}$$

Como $\| u_{\nu} = u_{\mu} \| = 0$ para $\mu \neq \nu$ então

$$\underline{V}^{B} \models f \text{ é } 1\text{-}1$$

mas como B satisfaz a ccc

$$\underline{V}^{B} \models \hat{\omega}_{\alpha} = \omega_{\hat{\alpha}}$$

e temos

$$\underline{V}^{B} \models f \text{ é um mapa } 1\text{-}1 \text{ de } \omega_{\hat{\alpha}} \text{ em } \mathcal{P}(\hat{\omega})$$

o que resulta em $\underline{V}^{B} \models \aleph_{\hat{\alpha}} \leq 2^{\aleph_0}$.

Como temos $\underline{V}^{B} \models 2^{\aleph_0} \leq \aleph_{\hat{\alpha}}$ isto completa a demonstração do teorema 1.20.

$\therefore$

- CAPÍTULO 2 -

TEORIA ERGÓDICA; ENTROPIA E FUNÇÕES EXPONENCIAIS

2.1 INTRODUÇÃO:

É comum, em Física, tentarmos aproximar determinadas equações de movimento por outras que sejam mais facilmente tratáveis pela análise padrão. Assim, se temos uma determinada lei dinâmica, experimentamos aproximá-la por outra bem comportada. Infelizmente este tipo de procedimento nem sempre funciona, pois, na Natureza, podemos encontrar algumas situações em que, com uma pequena mudança na dinâmica, modificamos em muito o comportamento do sistema.

Nos últimos anos o papel que os sistemas turbulentos ou caóticos tinham aumentou consideravelmente na Física, crescendo em particular o interesse naqueles cujo movimento fosse regido pelo azar, isto é, por probabilidades.

Imaginemos uma experiência em que medimos a temperatura de uma amostra a cada cinco minutos. Um possível resultado para esta experiência é mostrado na tabela abaixo:

Temperatura (^oK)	/ Tempo (x 5 min.)
⋮	⋮
4.20	-1
4.21	0
4.20	1
4.19	2
4.22	3
⋮	⋮

Podemos representar este resultado por uma sequência (...,4.20,4.21,4.20,4.19,4.22,...), onde a cada número corresponde uma temperatura num dado instante; por exemplo, se 4.20 é a temperatura em t = -5 min., 4.21 é a temperatura em t = 0 min. e assim por diante.

Do mesmo modo, podemos imaginar experiências similares em que controlamos um determinado parâmetro (medida) em função do tempo. Suponhamos, de uma maneira mais geral, que esse parâmetro assuma valores sobre um conjunto pré-estabelecido $\rho = \{\rho_0, \rho_1, \rho_2, \ldots, \rho_{r-1}\}$. Uma experiência poderá ser representada por uma sequência bi-infinita de elementos de ρ do do tipo $\omega = (\ldots, \omega_{-1}, \omega_0, \omega_1, \omega_2, \ldots)$, onde $\omega_i \in \rho$ é o resultado da experiência no instante t_i (o uso de uma sequência desse tipo implica num tempo de experiência que se prolonga infinitamente tanto para o futuro quanto para o passado; fisicamente isso é impossível de ser realizado,* mas matematicamente esta hipótese

---

*Uma possível alternativa seria o uso de números hiperfinitos, tomados num modelo nao-standard para a aritmética.

é crucial). Às sequências desta forma chamaremos de *Trajetórias Simbólicas*.

O objetivo da Teoria Ergódica (T.E.) é o estudo de trajetórias simbólicas cujos ω_i evoluem segundo leis probabilísticas e, por isso, centralizaremos nossa atenção sobre os Espaços de Medida.

Seja $(X,\mathcal{B},\mu)$ um espaço de probabilidades (para uma revisão da teoria de medidas veja [19] ou [27]; o que necessitamos pode ser encontrado no Cap. 0 do livro de Mañé [35]), onde X é o conjunto de todas as trajetórias simbólicas admissíveis e $\mathcal{B}$ é uma σ-álgebra sobre X, usualmente gerada pelos boreleanos. Seja $T : X \Rightarrow X$ uma transformação que leva objetos de X sobre ele mesmo. T é mensurável se $A \in \mathcal{B}$ implica que $T^{-1}A = \{\omega: T\omega \in A\} \in \mathcal{B}$. T preserva a medida se $\mu(T^{-1}A) = \mu(A)$ para todo o A pertencente à σ-álgebra $\mathcal{B}$.

Na Teoria Ergódica estudamos as tranformações T que preservam a medida. A motivação para isto é dada pelo Teorema de Liouville em Mecânica Estatística* mas podemos ver a sua necessidade se queremos estudar processos cuja passagem do tempo, representada pela aplicação de T, não altera as probabilidades para que determinado valor seja medido.

Definiremos um conjunto A como sendo como sendo invariante se $T^{-1}A = A$.

---

*Esta ligacao vem de equiprobabilizarmos o espaco de fase, em Mecanica Estatistica Classica, ou o espaco de Hilbert, em Mecanica Estatistica Quantica, quando usamos o Ensemble Microcanonico. Para esta canexao veja por exemplo [02], [29] ou [51].

<u>DEFINIÇÃO</u> 2.1 (Lei Zero-Um): Uma transformação T é dita *ergódica* se cada conjunto invariante em $\mathcal{B}$ tem ou medida nula ou um.

De posse de todas estas definições preliminares, vejamos um exemplo conhecido como *shifts* ou deslocamentos de Bernoulli.

2.2 SHIFTS DE BERNOULLI.

Seja ρ um conjunto definido como na seção anterior. Atribuimos a cada elemento ρ_i de ρ um peso p_i tal que $p_i \geq 0$ e $\sum_{i=0}^{r-1} p_i = 1$. O espaço $\rho^{\mathbb{Z}}$, onde $\mathbb{Z} = \{\ldots,-2,-1,0,1,2,\ldots\}$ é o conjunto dos inteiros, é o espaço de todas as sequências bi-infinitas de símbolos de ρ possíveis. Seja ainda $x_n: X \Rightarrow \rho$, onde aqui consideramos $X = \rho^{\mathbb{Z}}$, uma função que nos dá o valor da n-ésima coordenada de uma sequência $\omega \in X$, ou seja, $x_n(\omega) = \omega_n \in \rho$. A σ-álgebra $\mathcal{B}$ é gerada pela álgebra consistida dos conjuntos cilíndricos (ou simplesmente cilindros)

$$\{ \omega : x_l(\omega)=i_l, \ n \leq l < n+k \}$$

onde $i_l \in \rho$. A medida μ, definida sobre os elementos da σ-álgebra $\mathcal{B}$, é dada em função dos pesos (ou probabilidades) p_i dos elementos de ρ como:

$$\mu(\{\omega : x_l(\omega)=i_l, \ n \leq l < n+k \})=$$

$$p_{i_n} \cdot p_{i_{n+1}} \cdot \ \cdots \ \cdot p_{n_{n+k-1}} =$$

$$= \prod_{l=n}^{n+k-1} p_{i_l}$$

Seja agora T: $\rho^{\mathbb{Z}} \Rightarrow \rho^{\mathbb{Z}}$ uma tranformação do tipo *shift** determinada pela equação:

$$x_n(T(\omega)) = x_{n+1}(\omega)$$

Esta tranformação obviamente preserva a medida μ determinada anteriormente. T, definida como acima, é conhecida como *Shift de Bernoulli*; se temos n elementos em ρ com probabilidade p_i, $0 \le i \le n-1$, o *shift* de Bernoulli correspondente é denotado por $\mathcal{B}(p_0,...,p_{n-1})$. Com isto $\mathcal{B}(1/2,1/2)$ modela, por exemplo, uma experiência tipo cara-coroa.

2.3 O TEOREMA ERGÓDICO.

Apresentaremos nessa seção uma das muitas maneiras ([04], [21], [35] ou [42]) de demonstrarmos o Teorema Ergódico (T.E.). Devido a sua grande importância tanto na Física quanto na Matemática (veja Mackey [29] ou Tolman [49]), resolvemos dedicar toda essa seção ao T.E..

Existem vários enunciados diferentes para o Teorema

*shift em portugues significa deslocamento e seguindo a tradicao da literatura especializada brasileira manteremos esta palavra em ingles no texto.

Ergódico, e a forma que apresentaremos aqui é conhecida como Teorema Ergódico de Birkhoff ([05]); a nossa demonstração segue as provas dadas por Mañé [35] e Petersen [42].

TEOREMA 2.1 (Teorema Ergódico de Birkhoff): Seja $(X, \mathcal{B}, \mu)$ um espaço de probabilidade, T: $X \to X$ uma transformação que preserva a medida e $f \in L^1(X, \mathcal{B}, \mu)$. Então

1) $\lim_{n\to\infty} (1/n) \sum_{k=0}^{n-1} f(T^k x) = \bar{f}(x)$ existe em q.t.p.;

2) $\bar{f}(Tx) = \bar{f}(x)$ em q.t.p.;

3) $\bar{f} \in L^1$, e de fato $\|\bar{f}\|_1 \le \|f\|_1$;

4) Se $A \in \mathcal{B}$ com $T^{-1}A = A$, então

$$\int_A f.d\mu = \int_A \bar{f}.d\mu \ ;$$

5) $(1/n) \sum_{n=0}^{n-1} f \ T^k \to \bar{f}$ em L^1 .

(q.t.p é a abreviatura de "quase todos os pontos", isto é, a menos de um conjunto de medida nula.)

Prova do Teorema 2.1: Antes, precisamos de um Lema,

Lema 2.2 (Teorema Ergódico Maximal): Seja $f \in L^1(X)$ e definamos

$$E(f) = \{ x : \sup_{n\ge 0} \sum_{j=0}^{n} f(T^j(x)) > 0 \}$$

Então:

$$\int_{E(f)} f.d\mu \ge 0$$

Prova do Lema 2.2: Veja Mañé [35] pag. 120.

Desse Lema obtemos o

Corolário 2.3: Se $A \subset E(f)$ pertença à σ-álgebra e $T^{-1}(A) = A$, então

$$\int_A f \, d\mu \geq 0$$

Prova do Corolário: Veja Mañé [35] pag. 118.

Voltemos à prova do Teorema.

1) Como $f \in L^1(X)$ podemos definir

$$E^+_\alpha(f) = \left\{x : \lim_{n\to\infty} \sup\, (1/n+1) \sum_{j=0}^{n} f(T^j(x)) > \alpha\right\}$$

e

$$E^-_\alpha(f) = \left\{x : \lim_{n\to\infty} \inf\, (1/n+1) \sum_{j=0}^{n} f(T^j(x)) < \alpha\right\}$$

Das definições obtemos

$$E^+_\alpha(f) = E^+_0(f - \alpha)$$
$$E^-_\alpha(f) = E^+_{-\alpha}(-f)$$

Temos que

$$\int_{E^+_\alpha(f)} f \, d\mu = \int_{E^+_\alpha(f)} (f - \alpha) \, d\mu + \alpha.\mu(E^+_\alpha(f)) =$$

$$= \int_{E^+_0(f-\alpha)} (f - \alpha) \, d\mu + \alpha.\mu(E^+_\alpha(f))$$

que resulta em

$$\int_{E_0^+(f-\alpha)} (f - \alpha)\, d\mu \geq 0$$

pelo corolário anterior e pelo fato de que $T^{-1}(E_0^+(f - \alpha)) \subset E_0^+(f - \alpha)$ e $E_0^+(f - \alpha) \subset E(f - \alpha)$. Usando estes resultados podemos ver que

$$\int_{E_\alpha^+(f)} f\, d\mu \geq \alpha.\, \mu(E_\alpha^+(f))$$

Se $A \in \mathscr{B}$ está contido em $E_\alpha^+(f)$ e $T^{-1}(A) = A$ então

$$\int_A f\, d\mu \geq \alpha.\, \mu(A) \qquad (*)$$

pois $\int_A f\, d\mu = \int_A f.\chi_A\, d\mu = \int_{E_\alpha^+(f.\chi_A)} f.\chi_A\, d\mu \geq \alpha.\, \mu(E_\alpha^+) = \alpha.\, \mu(A)$.

Como $E_\alpha^-(f) = E_\alpha^+(-f)$, temos de $(*)$ que se $f \in L^1(X)$, $A \in \mathscr{B}$ está contido em $E_\beta^-(f)$ e satisfaz $T^{-1}(A) = A$ então

$$\int_A \chi_A\, d\mu \leq \beta.\, \mu(A)$$

Dessa equação e de $(*)$, se $\alpha > \beta$ temos

$$\mu(E_\alpha^+(f) \cap E_\beta^-(f)) = 0$$

fazendo-se $A = E_\alpha^+(f) \cap E_\beta^-(f)$.

Se pegamos uma sequência α_n, $n \geq 1$ densa em $\mathbb{R}$ resulta que

$$\left\{x : \lim_{n\to\infty} \inf \frac{\sum_{j=0}^{n} f(T^j(x))}{n+1} > \lim_{n\to\infty} \inf \frac{\sum_{j=0}^{n} f(T^j(x))}{n+1}\right\} =$$

$$= \bigcup_{\alpha_n > \alpha_m} E^+_{\alpha_n}(f) \cap E^-_{\alpha_m}(f)$$

Como vimos $\mu\left[\bigcup_{\alpha_n > \alpha_m} E^+_{\alpha_n}(f) \cap E^-_{\alpha_m}(f)\right] = 0$; então o limite

$$\lim_{n\to\infty} \frac{1}{n} \sum_{j=0}^{n-1} f(T^j(x))$$

converge em q.t.p.;

2)

$$\bar{f}(T(x)) = \lim_{n\to\infty} \frac{1}{n} \sum_{j=0}^{n-1} f(T^j(x)) =$$

$$= \lim_{n\to\infty} \left[\frac{1}{n} \sum_{j=0}^{n} f(T^j(x)) - \frac{1}{n} f(x)\right] =$$

$$= \lim_{n\to\infty} \frac{n+1}{n} \frac{1}{n+1} \sum_{j=0}^{n} f(T^j(x)) - \lim_{n\to\infty} \frac{1}{n} f(x) =$$

$$= \lim_{n\to\infty} \frac{1}{n+1} \sum_{j=0}^{n} f(T^j(x)) = \bar{f}(x) \qquad \text{q.t.p.}$$

3)

$$\left| \frac{1}{n} \sum_{k=0}^{n-1} f\ T^k \right| \leq \frac{1}{n} \sum_{k=0}^{n-1} |\ f\ | T^k$$

e temos

$$\int_X |\ \bar{f}\ |\ d\mu \leq \lim_{n\to\infty} \inf \int_X \frac{1}{n} \sum_{k=0}^{n-1} |\ f(T^k(x))\ |\ d\mu =$$

$$= \int |\ f\ |\ d\mu < \infty$$

x

então

$$\| \bar{f} \|_1 \leq \| f \|_1$$

5) Provaremos antes a parte 5) do teorema para depois tirarmos 4) como um corolário.

Temos que mostrar que

$$\lim_{n \to \infty} \| \bar{f} - \frac{1}{n} \sum_{j=0}^{n-1} f \circ T^j \|_1 = 0$$

Se g é uma função limitada $0 \leq g \leq f$, então

$$\| \frac{1}{n} \sum_{k=0}^{n-1} f \circ T^k - \bar{f} \|_1 \leq \| \frac{1}{n} \sum_{k=0}^{n-1} (f \circ T^k - g \circ T^k) \|_1 +$$

$$+ \| \frac{1}{n} \sum_{k=0}^{n-1} g \circ T^k - \bar{g} \|_1 + \| \bar{g} - \bar{f} \|_1$$

Pelo ítem 3) $\| g - f \|_1 \geq \| \bar{g} - \bar{f} \|_1$ e pode ser arbitrariamente aproximada escolhendo-se um g apropriado. Da mesma maneira, o primeiro termo também é menor ou igual a $\| f - g \|_1$. Uma vez sendo g fixo o segundo termo se aproxima de zero quando $n \to \infty$ o que prova o item 5).

4) Para provar 4) temos

$$\left| \int_A f \, d\mu - \int_A \bar{f} \, d\mu \right| = \left| \int_A \left(\frac{1}{n} \sum_{k=0}^{n-1} f \circ T^k - \bar{f} \right) d\mu \right| \leq$$

$$\leq \int_A \left| \frac{1}{n} \sum_{k=0}^{n-1} f \circ T^k - \bar{f} \right| d\mu = \| \frac{1}{n} \sum_{k=0}^{n-1} f \circ T^k - \bar{f} \|_1 \to 0$$

o último limite vindo do ítem 5).

∴

2.4 ENTROPIA.

Um dos conceitos mais interessantes é o de *Entropia*, aparecendo com destaque em diferentes áreas da Física e da Matemática, introduzida na teoria ergódica em 1958 por Kolmogorov, a partir de idéias de Nyguest e Shannon em teoria da informação. Usando-a, Kolmogorov e Sinai mostraram que os *shifts* de Bernoulli $\mathcal{B}(1/2,1/2)$ e $\mathcal{B}(1/3,1/3,1/3)$ não eram equivalentes, i. e., não modelavam o mesmo experimento.

A pergunta que eles fizeram foi: dada uma tranformação T que preserva a medida em $(X, \mathcal{B}, \mu)$ e $\tilde{T}$ uma t.p.m. em $(\tilde{X}, \tilde{\mathcal{B}}, \tilde{\mu})$, são T e $\tilde{T}$ isomorfas, no sentido de representarem a mesma experiência?

Para respondermos a essa questão, precisamos antes definir, de uma maneira precisa, o que é um isomorfismo entre dois sistema.

<u>DEFINIÇÃO</u> 2.2: Seja $X_o \in \mathcal{B}$ e $\tilde{X}_o \in \mathcal{B}$, conjuntos de medida 1. Se existe um mapeamento ϕ de X_o sobre $\tilde{X}_o$ com as propriedades:

1) ϕ é 1-1;

2) Se $A \subset X_o$ e $\tilde{A} = \phi A$, então $A \in \mathcal{B}$ se e somente se $\tilde{A} \in \tilde{\mathcal{F}}$; nesse caso $\mu(A) = \tilde{\mu}(\tilde{A})$;

3) Se temos $X_o \subset T^{-1}X_o$ e $\tilde{\Omega}_o \subset \tilde{T}^{-1}\tilde{\Omega}_o$ então

$$\phi T\omega = \tilde{T}\phi\omega$$

vale para qualquer ω em X_o;

então dizemos que $(X_o, \mathcal{B}, \mu, T)$ e $(\tilde{\Omega}_o, \tilde{\mathcal{F}}, \tilde{\mu}, \tilde{T})$ são isomorfos.

Para provarmos que duas tranformações não são isomorfas, teríamos que construir todos os mapeamentos possíveis entre um espaço e o outro, e depois mostrar que esses mapas não satisfazem às condições da definição anterior. Obviamente este é um trabalho penoso, algumas vezes impossível de ser realizado.

Este problema pode ser contornado usando-se o conceito de invariante. Suponhamos que T seja isomorfa a $\tilde{T}$ segundo $(X_o, \tilde{\Omega}_o, \phi)$. Se T tem uma determinada propriedade e, por isso, $\tilde{T}$ também a tem obrigatoriamente, então esta propriedade é um invariante. Como um exemplo temos o *mixing* (uma t.p.m. é *mixing* se $\lim_{n\to\infty} \mu(A \cap T^{-n}B) = \mu(A)\mu(B)$). Se T e $\tilde{T}$ são isomorfas e se T é *mixing* então $\tilde{T}$ também é. A recíproca não é verdadeira, ou seja, T e $\tilde{T}$ serem *mixing* não implica que também sejam isomorfas. Um outro exemplo de invariante é a ergodicidade.

Dentre os invariantes os mais interessantes estão aqueles ditos completos. Um invariante é completo se dois sistemas que têm esse mesmo invariante forem obrigatoriamente isomorfos. Foi com o intuito de procurar invariantes completos que Kolmogorov introduziu a entropia, mostrando que $\mathcal{B}(1/2,1/2)$ e $\mathcal{B}(1/3,1/3,1/3)$ não são isomorfos.

Antes de definirmos entropia vejamos algumas definições preliminares.

<u>DEFINIÇÃO</u> 2.3: Uma *subálgebra σ-finita* (ou simplesmente *σ-finita*) de $\mathcal{B}$ é um conjunto X, tal que X pode ser escrito como uma união enumerável $X = \bigcup_{n\geq 1} A_n$ e tal que $\mu(A_n) < \infty$

para todo o n e $A_n \in \mathscr{B}$.

DEFINIÇÃO 2.4: $\{A_1, \ldots, A_n\}$ é uma *$\mathscr{B}$-decomposição* de X se é uma coleção finita e disjunta de elementos de $\mathscr{B}$ cuja união é X. Os elementos A_i são chamados de *átomos*.

Qualquer σ-finito vem de uma $\mathscr{B}$-decomposição. Seja $\mathscr{A}$ uma subálgebra σ-finitas de $\mathscr{B}$. A entropia de $\mathscr{A}$ é definida por

$$H(\mathscr{A}) = -\sum_{A \in \mathscr{A}} \mu(A) \log \mu(A)$$

onde os elementos $A \in \mathscr{A}$ são os átomos de uma $\mathscr{A}$-decomposição.

A entropia de um σ-finito $\mathscr{A}$ relativa à transformação T é

$$h(\mathscr{A}, T) = \lim_{n \to \infty} \sup \frac{1}{n} H\left(\bigvee_{k=0}^{n-1} T^{-k} \mathscr{A} \right)$$

onde $\bigvee_{k=0}^{n-1}$. denota a σ-álgebra gerada por $\bigcup_{k=0}^{n-1} T^{-K}\mathscr{A}$, $T^{-n}\mathscr{A} = \{T^{-n}A : A \in \mathscr{A}\}$. Com isto podemos definir a entropia de T como

$$h(T) = \sup_{\mathscr{A}} h(\mathscr{A}, T)$$

onde o supremo é tomado em relação a todos os σ-finitos $\mathscr{A}$ de $\mathscr{B}$.

Listaremos algumas das principais propriedades de $H(\mathscr{A})$ e $h(\mathscr{A}, T)$ (as demonstrações podem ser encontradas em Billingsley [04] pags. 77 - 84) mas antes definamos um conceito auxiliar chamado *entropia condicional* de $\mathscr{A}$ dado $\mathscr{B}$, sendo $\mathscr{A}$ e $\mathscr{B}$

subálgebras σ-finitas de $\mathscr{B}$, como:

$$H(\mathscr{A}|\mathscr{B}) = \sum_{B} \mu(B) \sum_{A} (-\mu(A|B) \log (\mu(A|B))) =$$
$$= - \sum_{A,B} \mu(A \cap B) \log \mu(A|B)$$

onde $\mu(A|B) = \mu(A \cap B)/\mu(B)$, a soma é feita sobre os átomos de $\mathscr{A}$ e $\mathscr{B}$ e onde suprimimos qualquer termo envolvendo um átomo de medida nula.

Propriedades de $H(\mathscr{A})$ e $H(\mathscr{A}|\mathscr{B})$

H1) $H(\mathscr{A} \vee \mathscr{B}|\mathscr{C}) = H(\mathscr{A}|\mathscr{B}) + H(\mathscr{B}|\mathscr{A} \vee \mathscr{C})$

$H(\mathscr{A} \vee \mathscr{B}) = H(\mathscr{A}) + H(\mathscr{B}|\mathscr{A})$

H2) $H(\mathscr{A}|\mathscr{C}) \leq H(\mathscr{B}|\mathscr{C})$ se $\mathscr{A} \subset \mathscr{B}$

$H(\mathscr{A}) \leq H(\mathscr{B})$ se $\mathscr{A} \subset \mathscr{B}$

H3) $H(\mathscr{A}|\mathscr{C}) \leq H(\mathscr{A}|\mathscr{B})$ se $\mathscr{C} \supset \mathscr{B}$

$H(\mathscr{A}|\mathscr{C}) \leq H(\mathscr{A})$

H4) $H(\mathscr{A} \vee \mathscr{B}|\mathscr{C}) \leq H(\mathscr{A}|\mathscr{C}) + H(\mathscr{B}|\mathscr{C})$

$H(\mathscr{A} \vee \mathscr{B}) \leq H(\mathscr{A}) + H(\mathscr{B})$

H5) $H(T^{-1}\mathscr{A}|T^{-1}\mathscr{B}) = H(\mathscr{A}|\mathscr{B})$

$H(T^{-1}\mathscr{A}) = H(\mathscr{A})$

Propriedades de $h(\mathscr{A}, T)$

h1) $h(\mathscr{A}, T) = \lim_{n\to\infty} H(\mathscr{A}| \bigvee_{i=1}^{n-1} T^{-i}\mathscr{A})$

h2) $h(\mathscr{A}, T) \leq h(\mathscr{B}, T)$ se $\mathscr{A} \subset \mathscr{B}$

h3) $h(\bigvee_{j=u}^{v} T^{-j}\mathcal{A},\ T) = h(\mathcal{A},\ T)$

h4) $h(\bigvee_{j=0}^{k-1} T^{-j}\mathcal{A},\ T^{k}) = k.h(\mathcal{A},\ T)\ ,\ k \geq 1$

h5) $h(\mathcal{A},\ T) \leq h(\mathcal{B},\ T) + H(\mathcal{A}|\mathcal{B})$

Demonstraremos um importante teorema que relaciona $h(T)$ com $h(\mathcal{A},\ T)$.

TEOREMA 2.4 (de Kolmogorov-Sinai): Se T é inversivel e $\bigvee_{n=-\infty}^{+\infty} T^{n}\mathcal{A} = \mathcal{B}$, então $h(T) = h(\mathcal{A},\ T)$.

Prova: Temos que mostrar que para qualquer subálgebra $\mathcal{B}$ de $\mathcal{B}$ vale $h(\mathcal{B},\ T) \leq h(\mathcal{A},\ T)$ pois então $h(\mathcal{A},\ T) = \sup_{\mathcal{B}} h(\mathcal{B},\ T) = h(T)$.

Seja $\mathcal{A}_n = \bigvee_{k=-n}^{n} T^{k}\mathcal{A}$; resulta de h3) que

$$h(\mathcal{A}_n,\ T) = h(\mathcal{A},\ T)$$

e por h5)

$$h(\mathcal{B},\ T) \leq h(\mathcal{A}_n,\ T) + H(\mathcal{B}|\mathcal{A}_n) = h(\mathcal{A},\ T) + H(\mathcal{B}|\mathcal{A}_n)$$

É suficiente mostrar que $\lim_{n\to\infty} H(\mathcal{B}|\mathcal{A}_n) = 0$. Para isso precisamos de um lema.

Lema 2.5: Suponha que a álgebra finita $\mathcal{A}$ é contida na σ-álgebra gerada por $\mathcal{B}_0$. Então, para qualquer $\varepsilon > 0$

existe uma subálgebra finita $\mathcal{B}$ de $\mathcal{B}_0$ tal que $H(\mathcal{A}|\mathcal{B}) < \varepsilon$.

Prova do Lema: Veja Billingsley [04] pag. 80.

Se $\mathcal{B}_0 = \bigcup_n \mathcal{A}_n$ então $\mathcal{B}_0$ gera $\mathcal{B}$. Pelo Lema 2.5, para qualquer $\varepsilon > 0$, existe uma subálgebra finita $\mathcal{C}$ de $\mathcal{B}_0$ tal que $H(\mathcal{B}|\mathcal{C}) < \varepsilon$. $\mathcal{C}$ fica em algum $\mathcal{A}_{n_0}$; se $n \geq n_0$

$$H(\mathcal{B}|\mathcal{A}_n) \leq H(\mathcal{B}|\mathcal{A}_{n_0}) \leq H(\mathcal{B}|\mathcal{C}) < \varepsilon$$

o que termina a demonstração.

$\therefore$

Vejamos como essas definições podem, ser usadas num *shift* de Bernoulli $\mathcal{B}(p_0, p_1, \ldots, p_{n-1})$. Suponhamos que nossa trajetória simbólica ω assuma valores em $\rho^{\mathbb{Z}}$ e ainda que nossa transformação de *shift* seja $\sigma : \rho^{\mathbb{Z}} \to \rho^{\mathbb{Z}}$. É fácil ver que a entropia é dada por

$$H = - \sum_{i=0}^{n-1} p_i \log p_i$$

que é justamente a calculada por Shannon via Teoria da Informação [45]. Isto justifica a interpretação de que a entropia é a medida da informação ou da aleatoriedade com que os pontos de X são movidos por T.

Como dissemos anteriormente, a entropia é um invariante, mas não é completa. Ela é na verdade um invariante para o que se chama de isomorfismo fraco, sendo duas transformações com a mesma entropia fracamente isomorfas (para um exemplo de tais sistemas veja [43]), ou seja, homeomorfas módulo zero.

2.5 O TEOREMA DE SHANNON-MCMILLAN-BREIMAN.

Nessa seção demonstraremos um resultado fundamental em teoria ergódica, obtido em diferentes graus de generalização por C. Shannon 1948, B. McMillan 1953 e L. Breiman 1957, conhecido como Teorema de Shannon-McMillan-Breiman, que nos diz que, se temos um tempo suficientemente longo, a quantidade média de informação por símbolo converge para a entropia da fonte.

A demonstração resulta do teorema ergódico mais o da convergência para probabilidades condicionais, enunciado abaixo.

TEOREMA 2.6 (da convergência para probabilidades condicionais): Suponha que $\mathscr{G}_1 \subset \mathscr{G}_2 \subset \ldots$ e que $\mathscr{G} = \bigvee_{n=1}^{\infty} \mathscr{G}_n$. Então, para qualquer x integrável nós temos (com $E\{x\|\mathscr{G}\}$ denotando o valor esperado de x com respeito a $\mathscr{G}$ e $\mu\{M,\mathscr{G}\}$ a probabilidade condicional de M com relação a $\mathscr{G}$)

$$\lim_{n\to\infty} E\{x\|\mathscr{G}_n\} = E\{x\|\mathscr{G}\} \qquad \text{q. t. p.}$$

e para qualquer $M \in \mathscr{B}$ temos

$$\lim_{n\to\infty} \mu\{M\|\mathcal{G}_n\} = \mu\{M\|\mathcal{G}\} \qquad \text{q.t.p.}$$

Prova: Veja Billingsley [04] pag. 116.

TEOREMA 2.7 (Shannon-McMillan-Breiman): Se T é um *shift* ergódico então

$$\lim_{n\to\infty} \left\{ -\frac{1}{n} \log \mu(x_0(\omega),\ldots,x_{n-1}(\omega)) \right\} = h(T) \qquad \text{q.t.p.}$$

Prova: Seguiremos estritamente a demonstração dada por Billingsley [04] pag. 129.

Consideremos as funções

$$g_0(\omega) = -\log \mu(x_0(\omega))$$

$$g_k(\omega) = -\log \left\{ \frac{\mu(x_{-\alpha}(\omega),\ldots,x_{-1}(\omega),x_0(\omega))}{\mu(x_{-k}(\omega),\ldots,x_{-1}(\omega))} \right\}$$

$$f_k^{(i)} = -\log \left\{ \frac{\mu(x_{-\alpha}(\omega),\ldots,x_{-1}(\omega),i)}{\mu(x_{-k}(\omega),\ldots,x_{-1}(\omega))} \right\}$$

note que, sendo $\mu\{x\|\mathcal{G}\}_\omega$ o valor de $\mu\{x\|\mathcal{G}\}$ no ponto ω, $f_k^{(i)} = -\log \mu\{x_0 = i \,\| x_{-k},\ldots,x_{-1}\}_\omega$.

Temos que

$$\frac{1}{n}\sum_{k=0}^{n-1} g_k(T^k\omega) = \frac{1}{n}\left\{g_0(\omega) + g_1(T\omega) + \ldots + g_{n-1}(T^{n-1}\omega)\right\} =$$

$$= \frac{1}{n}\left\{ -\log \mu(x_0(\omega)) - \log \frac{\mu(x_{-1}(T\omega),x_0(T\omega))}{\mu(x_{-1}(T\omega))} - \right.$$

$$- \log \frac{\mu(x_{-2}(T^2\omega),x_{-1}(T^2\omega),x_0(T^2\omega))}{\mu(x_{-2}(T^2\omega),x_{-1}(T^2\omega))} -$$

$$- \cdots - \log \frac{\mu(x_{1-n}(T^{n-1}\omega), \ldots, x_0(T^{n-1}\omega))}{\mu(x_{1-n}(T^{n-1}\omega), \ldots, x_1(T^{n-1}\omega))} \Bigg\} =$$

$$= -\frac{1}{n}\left\{ \log \left[\mu(x_0(\omega)) \, . \, \frac{\mu(x_{-1}(T\omega), x_0(T\omega))}{\mu(x_{-1}(T\omega))} \, . \, \cdots \right.\right.$$

$$\left.\left. \cdots \, . \, \frac{\mu(x_{1-n}(T^{n-1}\omega), \ldots, x_0(T^{n-1}\omega))}{\mu(x_{1-n}(T^{n-1}\omega), \ldots, x_1(T^{n-1}\omega))} \right] \right\}$$

Como T é um *shift* ergódico temos que

$$\frac{1}{n}\sum_{k=0}^{n-1} g_k(T^k\omega) = -\frac{1}{n}\left\{ \log \left[\mu(x_0(\omega)) \, . \, \frac{\mu(x_0(\omega), x_1(\omega))}{\mu(x_0(\omega))} \, . \, \cdots \right.\right.$$

$$\left.\left. \cdots \, . \, \frac{\mu(x_0(\omega), \ldots, x_{n-1}(\omega))}{\mu(x_0(\omega), \ldots, x_{n-2}(\omega))} \right] \right\}$$

então

$$\frac{1}{n}\sum_{k=0}^{n-1} g_k(T^k\omega) = -\frac{1}{n} \log(x_0(\omega), \ldots, x_{n-1}(\omega))$$

Pelo teorema 2.6, $\mu\{x_0 = i \parallel x_{-k}, \ldots, x_{-1}\}$ converge q.t.p. para $\mu\{x_0 = i \parallel \ldots, x_{-2}, x_{-1}\}$. Mas $f_k^{(i)} = -\log \mu\{x_0 = i \parallel x_{-k}, \ldots, x_{-1}\}_\omega$, então, pela continuidade da função log, $f_k^{(i)}$ converge q.t.p.; desde que $g_k(\omega)$ coincide com $f_k^{(i)}(\omega)$ no cilindro $\{\omega : x_0(\omega) = i\}$, o limite

$$g(\omega) = \lim_{k\to\infty} g_k(\omega)$$

existe q.t.p..

Mostraremos que (usando a notação $E(f) = \int f(\omega)\mu(d\omega) = \int f d\mu$, c.f. Billingsley)

$$E\{\sup_k g_k(\omega)\} < +\infty$$

que resulta em $g(\omega)$ ser integrável e finita em quase todos os pontos. Se

$$E_k = \{\omega : \max_{1\leq j<k} g_j(\omega) \leq \lambda < g_k(\omega)\}$$

então

$$\mu(E_k) = \sum_i \mu(\{x_o = i\} \cap E_k) = \sum_i \mu(\{x_o = i\} \cap F_k^{(i)}\}$$

onde $F_k^{(i)} = \{\omega : \max_{1\leq j<k} f_j^{(i)}(\omega) \leq \lambda < f_k^{(i)}(\omega)\}$. Mas $F_k^{(i)}$ é a σ-álgebra gerada por $x_{-k},\dots,x_{-1}$, então

$$\mu(\{x_o = i\} \cap F_k^{(i)}\}) = \int_{F_k^{(i)}} \mu\{x_o = i \parallel x_{-k},\dots,x_{-1}\}\, d\mu(\omega) =$$

$$= \int_{F_k^{(i)}} e^{-f_k^{(i)}(\omega)} \mu(d\omega) \leq e^{-\lambda}.\,\mu(F_k^{(i)})$$

$F_k^{(i)}$ sendo disjunto para diferentes k,

$$\sum_k \mu(E_k) \leq \sum_i e^{-\lambda} \sum_k \mu(F_k^{(i)}) \leq re^{-\lambda}$$

onde r é o tamanho de ρ. Então

$$\mu\{\omega : \sup_k g_k(\omega) > \lambda\} \leq re^{-\lambda}$$

onde resulta que

$$E\{\sup_k g_k(\omega)\} < +\infty$$

Com isto g é integrável e podemos integrar o limite $E\{g\} = \lim_{k\to\infty} E\{g_k\}$. Como $\frac{1}{n}(x_0(\omega),\ldots,x_{n-1}(\omega)) = \frac{1}{n}\sum_{k=0}^{n-1} g_k(T^k\omega)$ e $\int_{T^{-1}} f(T\omega)\,\mu(d\omega) = \int_A f(\omega)\,\mu(d\omega)$ temos

$$E\{g\} = \lim_{n\to\infty} E\left\{\frac{1}{n}\sum_{k=0}^{n-1} g_k(T^k\omega)\right\} = h(T)$$

Obtemos

$$\frac{1}{n}\sum^{n-1} g_k(T^k\omega) = \frac{1}{n}\sum_{k=0}^{n-1} g(T^k\omega) + \frac{1}{n}\sum_{k=0}^{n-1} (g_k(T^k\omega) - g(T^k\omega)) \qquad (*)$$

O teorema 2.1 implica que

$$\lim_{n\to\infty} \frac{1}{n}\sum_{k=0}^{n-1} g(T^k\omega) = E\{g\} = h(T) \quad \text{q.t.p.} \qquad (**)$$

Se $G_N(\omega) = \sup_{k\geq N} |g_k(\omega) - g(\omega)|$, então

$$\lim_{n\to\infty} \sup \left| \frac{1}{n} \sum_{k=0}^{n-1} (g_k(T^k\omega) - g(T^k\omega)) \right| \leq$$

$$\lim_{n\to\infty} \sup \frac{1}{n} \sum_{k=0}^{n-1} \left| g_k(T^k\omega) - g(T^k\omega) \right| \leq$$

$$\lim_{n\to\infty} \sup \frac{1}{n} \sum_{k=0}^{n-1} G_N(T^k\omega) = E\{G_N\} \qquad \text{q.t.p.}$$

Mas $G_N(\omega)$ converge a zero em q.t.p. e é domonada pela função $g(\omega) + \sup_k g_k(\omega)$, e temos $\lim_N E\{G_N\} = 0$. Então combinando (*) com (**) implica

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=0}^{n-1} g_k(T^k\omega) = h(T) \qquad \text{q.t.p.}$$

Mas como vimos antes, $\frac{1}{n} \sum_{k=0}^{n-1} g_k(T^k\omega) = -\frac{1}{n} \log(x_0(\omega),\ldots,x_{n-1}(\omega))$ o que resulta em

$$\lim_{n\to\infty} \left\{ -\frac{1}{n} \log \mu(x_0(\omega),\ldots,x_{n-1}(\omega)) \right\} = h(T) \qquad \text{q.t.p.}$$

que era o que queriamos demonstrar.

$\therefore$

Como uma consequência do Teorema anterior temos a propriedade de Equipartição da Entropia.

Corolário 2.8 (Propriedade de Equipartição da Entropia): Seja T um *shift* ergódico com entropia h. Então para qualquer $\varepsilon > 0$ existe um inteiro positivo $b_0(\varepsilon)$ tal que se $b \geq b_0(\varepsilon)$ então ρ^b se decompõe em dois conjuntos $\mathscr{H}$ e $\mathscr{L}$ tal que

$$\sum_{u \in \mathscr{L}} \mu(u) = \mu\{(x_1,\ldots,x_b) \in \mathscr{L}\} < \varepsilon$$

e tal que

$$e^{-b(h+\varepsilon)} < \mu(u) = \mu\{(x_1,\ldots,x_0) = u\} < e^{-b(h-\varepsilon)}$$

para qualquer b-upla u em $\mathscr{H}$.

Prova: Desde que $\lim\limits_{n\to\infty} \left\{ -\frac{1}{n}\, \mu(x_0(\omega),\ldots,x_{n-1}(\omega)) \right\} = h$, a convergência deste limite também ocorre na medida, ou seja, para cada $\varepsilon > 0$ existe um b_0 tal que $b \geq b_0$ implica que

$$\mu\{x : \left| \frac{1}{b}\, \mu(x_0,\ldots,x_{n-1}) - h \right| \geq \varepsilon\} < \varepsilon$$

Seja $\mathscr{H}$ as b-uplas u para qual

$$\left| -\frac{1}{b} \log \mu(u) - h \right| < \varepsilon$$

e seja $\mathscr{L}$ o complemento de H em ρ^b. Daí vemos que $\mathscr{H}$ e $\mathscr{L}$ satisfazem as condições dadas no corolário, o que completa a prova.

$\therefore$

2.6 ENTROPIA E FUNÇÕES EXPONENCIAIS.

Nessa seção obteremos, como uma consequência do corolário 2.8, uma relação entre a entropia de um sistema e o crescimento do seu número de órbitas.

Aqui tudo acontecerá dentro de uma classe de objetos que servem como um modelo para ZFC. Seja o conjunto $s = \{0,1,2,...,s-1\} \subset \omega_0$; Consideraremos as trajetórias simbólicas ω pertencentes a $s^{\mathbb{Z}}$. O conjunto de todos os mapas totais de y em x será $[x^y]$ e, o de todos os mapas com domínio finito $C(y,x)$. Uma órbita será um elemento $\alpha_G \in [s^{\mathbb{Z}}]$ tal que se $G \subset C(\mathbb{Z},s)$ é um filtro e $\bigcup G$ é um mapa total então $\alpha_G = \bigcup G$; note que os cilindros são elementos de $C(x,y)$.

Dado um mergulho

$$N : C(\mathbb{Z},s) \Rightarrow s^{\mathbb{Z}}$$

$$p \in C(\mathbb{Z},s) \to N(p) = \{\alpha \in [s^{\mathbb{Z}}] : p \subset \alpha\}$$

nós tomaremos $N(p)$ como uma base para a topologia de $[s^{\mathbb{Z}}]$. O que temos que fazer agora é definir uma medida sobre os elementos de $[s^{\mathbb{Z}}]$ que são as nossas trajetórias simbólicas. Denotemos por a o conjunto seguinte:

$$a = \{\alpha \in [s^{\mathbb{Z}}] : \alpha(0) = s_a \in s\}$$

onde $\alpha(0) = \alpha_0$ como definido na seção 2.1. Impomos para μ as seguinte restrições:

$$\mu(N(p)) \geq 0$$

$$\sum_{s_\alpha \in s} \mu(\alpha) = 1$$

que caracterizam μ como uma probabilidade. Temos ainda que para uma coleção contável $p_i \leq p$ (onde a ordenação é feita segundo a inclusão inversa), tal que $p_i \perp p_j$ (para $i \neq j$, p_i e p_j são incompatíveis), que implica $N(p_i) \cap N(p_j) = \emptyset$, e também que $\bigcup_i N(p_i) = N(p)$, teremos:

$$\mu(N(p)) = \sum_{\text{todos } i} \mu(N(p_i))$$

Finalmente, seja $p + (k)$, com $p \in C(\mathbb{Z},s)$ e $k \in \mathbb{Z}$, denotando o elemento de $C(\mathbb{Z},s)$ cujo domínio foi deslocado por k, ou seja, $Dom(p + (k)) = \{n + k : n \in Dom(p)\}$ e $(p + (k))(i + k) = p(i)$. Temos como consequência que

$$\mu(N(p + (k))) = \mu(N(p))$$

e o que temos é um *shift* estacionário, como o de Bernoulli. Nos limitaremos a *shifts* como esses, com a propriedade extra de serem ergódicos.

Consideremos uma trajetória $\alpha \in [s^{\omega_0}]$ e seja $B \subset [s^{\omega_0}]$ tal que $\mu(B) = 1$; seja também α_n o segmento inicial, com n símbolos, de α (ou seja, se $\alpha = (0,1,1,0,0,1,0,\ldots)$, $\alpha_3 = (0,1,1))$ e B_n o conjunto de todos os α_n. $F_B(n)$ é a função $F_B : \omega_0 \Rightarrow \omega_0$ definida por $F_B(n) = |\, B_n \,|$. Uma propriedade imediata dessa função é $F_B(n) \leq F_B(n+1)$. Com isso podemos definir a entropia de B_n, c.f. seção 2.4, como:

$$H(B_n) = -\sum_{\alpha_n \in B_n} \mu(N(\alpha_n)) \log \mu(N(\alpha_n))$$

onde $\alpha_n \in C(\omega_o, s)$. Disto temos a entropia de Shannon-Kolmogorov-Sinai, dada por:

$$h(B) = \lim_{n<\omega_o} \left(\frac{1}{n} \right) H(B_n)$$

O resultado que anunciamos anteriormente é o seguinte: Seja $\langle B,\mu\rangle$ um processo ergódico estacionário definido como anteriormente. Seja $\varepsilon > 0$ um número real positivo; denotaremos por $f <^* g$, dadas funções f e g definidas de ω_o em ω_o ou $\mathbb{R}$, se e somente se existe um $n_o \in \omega_o$ tal que para todo $n_o < n$, $f(n) < g(n)$. Então,

PROPOSIÇÃO 2.9: $h(\langle B,\mu\rangle) = 0$ se e somente se para todo $\varepsilon > 0$, $| B_n | <^* 2^{\varepsilon n}$.

Prova: Provemos primeiro que a condição é suficiente ($\rightarrow$).

Se $h(\langle B,\mu\rangle) = 0$ então, para todo o $\varepsilon_n > 0$, dado um n, $-\frac{1}{n} \sum_{\text{todos } \alpha_n} \mu(\alpha_n) \log \mu(\alpha_n) < \varepsilon_n$, $\alpha_n \in B_n$ (α_n é o segmento inicial com n simbolos das trajetórias de B).

Como sabemos, a medida equiprovável maximiza a entropia, e para todas as medidas sobre B_n vale

$$-\frac{1}{n}\sum_{\text{todos } \alpha_n} \mu(\alpha_n) \log \mu(\alpha_n) \le \frac{1}{n} \log F_B(n)$$

Consideremos o caso da medida equiprovável, posto que esse caso implica nas outras situações. Com isto temos

$$\frac{1}{n} \log F_B(n) < \varepsilon_n$$

ou seja

$$\log (F_B(n))^{1/n} < \varepsilon_n$$

o que implica em

$$F_B(n) < 2^{(\varepsilon_n)n} \qquad \text{(com log na base 2)}$$

para todo o n.

(⇐)

Peguemos $F_B(n) < 2^{\varepsilon_n}$, $n > n_0$; nós temos

$$\frac{1}{n} \log f(n) < \varepsilon_n , \quad \text{para todo o } n$$

na qual, como a medida equiprovável μ_0 majora todas as entropias, significa que

$$0 = h(B,\mu) \le h(B,\mu_0) = 0$$

Seja (B,μ) um *shift* ergódico. Pelo corolário 2.8, para $h = 0$ temos que

$$\sum_{\alpha_n \in \mathscr{L}_n} \mu(\alpha_n) < \varepsilon$$

$$0 \le \mu(\alpha_n) \le 2^{-\varepsilon h}$$

$$\alpha_n \in \mathscr{H}_n$$

Com isso

$$\mu(\mathscr{L}_n) < \varepsilon$$

$$\mu(\mathscr{H}_n) \le |\mathscr{H}_n|\, 2^{-\varepsilon n} \le f(n)\, 2^{-\varepsilon n}$$

Como $f(n)$ é subexponencial para $h = 0$, temos como resultado que $\mu(B_n) < \varepsilon + f(n)\, 2^{-\varepsilon n} \to 0$.

$\therefore$

Para generalizarmos o resultado anterior precisamos de alguns lemas.

Lema 2.10: A entropia relativa $H(\mathscr{P}|Q)$ se anula se e somente se $\mathscr{P} \le Q$ ($\mathscr{P} \le Q$: todo o átomo de $\mathscr{P}$ é uma união de átomos de Q).

Prova: veja Mañé [35] pag. 276.

Lema 2.11: $h(T,\mathscr{P}) = \lim_{n\to\infty} H(\mathscr{P}|T^{-1}\mathscr{P}\vee\ldots\vee T^{-n}\mathscr{P})$.

Prova: veja Mañé [35] pag. 278.

Pelos dois lemas anteriores (2.10 e 2.11) a antropia $h(T,\mathcal{P})$ se anula se e somente se $\lim_{n\to\infty} H(\mathcal{P}|T^{-1}\mathcal{P}\vee\ldots\vee T^{-n}\mathcal{P}) = 0$. Então $h(T,\mathcal{P}) = 0 \leftrightarrow \forall n > n_0 \ \exists\varepsilon_n (\lim_{n\to\infty} H(\mathcal{P}|T^{-1}\mathcal{P}\vee\ldots\vee T^{-n}\mathcal{P})) < \varepsilon_n$, o que resulta em,

$$h(T,\mathcal{P}) = 0 \leftrightarrow \frac{1}{n} H(\mathcal{P}|\bar{T}^{-1}\mathcal{P}\vee\ldots\vee\bar{T}^{-(n-1)}\mathcal{P}) < \varepsilon_n,$$

É fácil ver que $|\mathcal{B}_n| = f(n) =$ í de átomos $(\mathcal{P}|\bar{T}^{-1}\mathcal{P}\vee\ldots\vee\bar{T}^{-(n-1)}\mathcal{P})$, e temos que a entropia anterior pode ser posta como $\frac{1}{n}(-\sum_{\text{átomos}} \mu(\alpha_i)\log\mu(\alpha_i)) < \varepsilon_n$.

Pelo teorema de Shannon-MacMillan-Breiman, as trajetórias se dividem em duas partes tais que:

1° parte: $\mu(\alpha_i) \sim 1/f(n)$;

2° parte: entropia tende a zero.

onde na primeira parte estimamos uma medida equiprovável, o que não afeta nosso resultado pois torna a entropia máxima. Com isso temos $\frac{1}{n}\log f(n) < \varepsilon_n$, ou $f(n) < 2^{\varepsilon_n n}$, para todo o ε_n.

- CAPÍTULO 3 -

OBJETOS GENÉRICOS E SUAS APLICAÇÕES À FÍSICA

3.1 INTRODUÇÃO.

Nesse capítulo, apresentaremos alguns exemplos de proposições formalmente indecidíveis, tanto em física como em matemática. Faremos isto exibindo predicados conjuntistas e, posteriormente, mostrando que esses predicados podem ser verdadeiros num modelo e falsos noutro. Antes de apresentarmos essas proposições, precisamos de alguns conceitos preliminares.

Começemos examinando o que vem a ser o *Universo Construtível de Goedel*, denotado usualmente por $\underline{L}$. $\underline{L}$ é uma classe própria do Universo de Von Neumman $\underline{V}$ (também conhecido como *Universo Bem Fundado*) e, intuitivamente, é o modelo no qual todos os subconjuntos de um dado conjunto A são definíveis por meio de um predicado. Podemos definir o universo construtível como:

<u>DEFINIÇÃO</u> 3.1: $\underline{L}$ é a menor classe própria de $\underline{V}$ que é transitiva e que contém todos os cardinais.

Da definição 3.1 não é claro o motivo de $\underline{L}$ ser chamado *Universo Construtível*. Uma definição mais direta é dada, conforme Krivine [31], da seguinte maneira:

DEFINIÇÃO 3.2: Sejam dois conjuntos x e y tal que $y \subseteq x$. y é uma parte definível de x, com parâmetros, se existir uma sentença $\phi(w, a_1, \ldots, a_k)$ com uma variável livre w e com parâmetros $a_1, \ldots, a_k \in x$, cujo valor em x é y. Definimos $k = \Pi(x)$ como "k é o conjunto das partes de x definíveis por parâmetros".

Formamos a coleção de conjuntos construtíveis a partir de ϕ de maneira análoga a $\underline{V}$.

DEFINIÇÃO 3.3: A coleção $\underline{L}$ de conjuntos construtíveis é definida por indução como:

$$L_0 = \emptyset$$

$$\vdots$$

$$L_\alpha = \bigcup_{\beta < \alpha} \Pi(L_\beta) \quad , \ \mathrm{Ord}(\alpha)$$

e $\quad \underline{L} = \{x : \exists\alpha \ (\mathrm{Ord}(\alpha) \wedge x \in L_\alpha)\}$

DEFINIÇÃO 3.4: x é construtível, denotado por $L(x)$, se $x \in \underline{L}$.

Aos axiomas ZF podemos acrecentar o chamado *Axioma da Construtibilidade*, denotado $\underline{V} = \underline{L}$, que é a sentença: $\forall x \ L(x)$.

TEOREMA 3.1: $\underline{L} \models ZFC + GCH$

Prova: Veja Kunen [32], Manin [36] ou Krivine [31].

Outro axioma que pode ser adicionado à ZF é o de Martin (veja [03], [32] ou [28]), e pode ser definido como afirmação: Nenhum espaço compacto de Hausdorff que obedece à c.c.c. é a união de $< 2^{\omega_0}$ conjuntos fechados nunca densos (Kunen [32], pag. 52).

O axioma de Martin (MA) pode ser visto como uma sentença reguladora. Se MA é verdadeiro, pode-se mostrar que, se $\omega_0 < k < 2^{\omega_0}$, então $2^k = 2^{\omega_0}$.

Para exibirmos uma sentença indecidível numa teoria, precisamos, antes de mais nada, passar esta teoria para uma linguagem formal, que no nosso caso será a $L_1^=$. Tal formalização pode ser feita usando-se o conceito de *estruturas matemáticas* de Boubarki ou os *predicados conjuntistas* de Suppes (como em da Costa e Doria [12]). Da Costa e Chuaqui [10] mostraram que ambas as formalizações são, de cerrto modo, equivalentes.

Uma estrutura matemática E é uma coleção finita e ordenada de conjuntos de nível finito (um conjunto x é de nível finito se existe um α, tal que $x \in L_\alpha$ e α é finito) sobre a união dos domínios de duas sequências finitas de conjuntos $X_1, \ldots, X_m$ e $Y_1, \ldots, Y_n$, tal que $m > 0$ e $n \geq 0$. Estes conjuntos X_i e Y_i são conhecidos como conjuntos de base, sendo X_i a base principal e Y_i a base auxiliar. O predicado de Suppes é uma fórmula da teoria de conjuntos da forma:

$$P(E, X_1, \ldots, X_m, Y_1, \ldots, Y_n)$$

na qual as únicas variáveis livres em P são E, $X_1, \ldots, X_m$, $Y_1, \ldots, Y_n$. Esta fórmula especifica a construção na T.A.C. de E, a partir de dois tipos de conjuntos base, e também os axiomas para as espécies de estruturas no qual estamos interessados. Os conjuntos de base principais podem variar, enquanto que os conjuntos de base auxiliares são fixos. Com a variação dos $X_1, \ldots, X_m$ temos as espécies de estruturas. Isto pode ser posto de uma maneira mais explícita escrevendo-se o predicado de Suppes de E da maneira seguinte:

$$Q(E) \leftrightarrow \exists X_1, \ldots, X_m \; P(E, X_1, \ldots, X_m, Y_1, \ldots, Y_n)$$

Vejamos um exemplo:

Seja x um conjunto e τ uma coleção de subconjuntos de x, tal que possuam as propriedades seguintes:

AI) $\emptyset$, $x \in \tau$;

AII) A união de qualquer coleção de conjuntos de τ pertence a τ;

AIII) A interseção de qualquer número finito de conjuntos de τ pertence a τ.

A coleção τ de conjuntos é chamada *topologia em* x; x é um *espaço topológico*.

Um espaço topológico pode então ser formalizado como o par $H = \langle x, \tau \rangle$ cujo predicado de Suppes é:

$$P(H,x) \leftrightarrow \exists \tau \ (H = \langle x,\tau \rangle \wedge \tau \subseteq \mathcal{P}(x) \wedge AI \wedge AII \wedge AIII)$$

ou

$$Q(H) \leftrightarrow \exists x \ P(H,x)$$

3.2 A ENTROPIA COMO UM CONCEITO NÃO-ABSOLUTO

Dissemos no capítulo 2 que os *shifts* ergódicos aparecem em várias situações relevantes em Física. Nessa seção obteremos que um *shift* de Bernouilli fica com entropia nula quando mudamos nosso modelo para os axiomas de ZFC (veja [11]).

Como no capítulo 2, seja p um número inteiro, e $[p^{\omega_o}] \subset p^{\omega_o}$ o conjunto de todas as funções totais de $\aleph_o$ em p. Dizemos que $[p^{\omega_o}]$ é o espaço dos *shifts*. Seguindo a caracterização de Chaitin, dizemos que um mapa $\sigma \in [p^{\omega_o}]$ é determinístico se ele pode ser gerado por um algorítmo (programa de computador), aplicado sobre uma entrada de dados finita, ou seja, se a sequência total pode ser comprimida numa sequência finita. A cardinalidade de $[p^{\omega_o}]$ é $2^{\aleph_o}$, e a cardinalidade do conjunto de todos os mapas determinísticos, chamado Σ, é o infinito contável. Σ é denso na topologia usual de $[p^{\omega_o}]$. Se tiramos Σ de $[p^{\omega_o}]$ obtemos o conjunto $p \cdot lr$, ou seja, o conjunto de todas as p-sequências irracionais (não determinísticas). Se pegarmos $Ir \subset [0,1]$, os irracioanis contidos no intervalo $[0,1]$, pode-se mostrar que existe um homomorfismo entre este conjunto e $p \cdot Ir$, isto é, $p \cdot Ir \cong Ir$. Como Σ será o nosso espaço de *shifts*, dotamos p de uma medida equiprovável.

Seja $B \in \underline{V}$ uma álgebra booleana completa, que obedece à condição da cadeia contável, tal que, ao tomarmos a extensão booleana $\underline{V}^B$ de $\underline{V}$, $\underline{V}^B \models$ ZFC + Axioma de Martin + $2^{\aleph_0} = \varkappa > \aleph_1$.

Proposição 3.2: $\underline{V}^B \models |(p \cdot Ir)^{\wedge}| = \hat{\aleph}_1 < 2^{\aleph_0}$.

Prova: $\underline{V}^B \models |(p \cdot Ir)^{\wedge}| = |\mathcal{P}(\hat{\omega}_0)^{\wedge}| = \hat{\aleph}_1$. ∴

Como a cardinalidade de $(p \cdot Ir)^{\wedge}$ é $\hat{\aleph}_1$, então este conjunto é obrigatoriamente diferente de $(p \cdot Ir)^B$, cuja cardinalidade é $2^{\aleph_0}$.

Proposição 3.3: Se $\underline{V}^B \models$ "$(p \cdot Ir)^{\wedge} \subset (p \cdot Ir)^B$, junto com uma medida induzida", então $\underline{V}^B \models$ "A entropia por símbolo do *shift* cujo espaço de fase é $(p \cdot Ir)^{\wedge}$ é zero".

Prova: Resulta do lema seguinte,

Lema 3.4: Suponha que o axioma de Martin seja verdadeiro. Seja $X_\alpha \subset \mathbb{R}$, $\alpha < \varkappa$ e $\aleph_0 \leq \varkappa \leq 2^{\aleph_0}$ sejam conjuntos de medida nula. Então $\bigcup_{\alpha < \varkappa} X_\alpha$ tem medida nula.

Prova do Lema 3.4: Veja Kunen [32] pag. 59 ou da Costa e Doria [11]. $\therefore$

Como $\underline{V}^{B} \models |(p\cdot Ir)^{\wedge}| < 2^{\aleph_0}$ (pois B obedece à c.c.c.), então, pelo axioma de Martin, $\underline{V}^{B} \models \mu[(p\cdot Ir)^{\wedge}] = 0$. Com isto temos $\underline{V}^{B} \models h[(p\cdot Ir)^{\wedge}] = 0$. Então, como resultado imediato temos $\underline{V}^{B} \models \mu[p\cdot Ir - (p\cdot Ir)^{\wedge}] = p$ e a nossa proposição.

$\therefore$

Com isto vimos que processos cuja entropia é positiva num modelo podem ter entropia nula noutro.

Um outro resultado que podemos obter, para que possamos entender melhor o conceito de entropia é a proposição seguinte:

Proposição 3.5: O conjunto das trajetórias cuja entropia é zero é um conjuno residual.

Prova: Seja $B\cdot Ir \subset [0,1]$ os irracionais binários. Seja $f: \omega_0 \Rightarrow \omega_0$ uam função monotonamente não-decrescente tal que $f(0) = 1$.

Lema 3.6': Existe uma aplicação 1-1 entre funções monotonamente não-decrescentes, representadas por $\mathcal{CE}$ (de crescentes eventualmente), e os irracionai binários.

Prova do Lema 3.6': Seja $\alpha \in B\cdot Ir$ uma sequência de zeros e uns. Construimos a partir desta sequência uma função $f \in \mathscr{C}\mathscr{S}$ da maneira seguinte: f(n) = (número de zeros entre o n-ésimo um e o início de α); como exemplo imaginemos a sequência α = 00111001..., e temos, para esta sequência, f(0) = 0, f(1) = 2, f(2) = 2, f(3) = 2, f(4) = 4 e assim por diante. Usando-se a mesma aplicação anterior, é fácil ver que a cada f(n) corresponderá uma sequência $\alpha \in B\cdot Ir$. ∴

Como vimos no fim do capítulo dois, temos uma aplicação (que não é obrigatoriamente 1-1) entre algumas partições $(\mathscr{P}\vee T^{-1}\mathscr{P}\vee\ldots\vee T^{-(n-1)}\mathscr{P})$ sobre o número de átomos dessa partição. Via Lema 3.6', temos então uma aplicação dos espaços de partição nos binários irracionais. Como o teorema de Shannon-MacMillan-Breiman trata de comportamentos assintóticos, podemos ignorar os segmentos iniciais das sequências α e obter o lema.

Lema 3.7': O conjunto das sequências binárias que coincidem sempre, a menos de um segmento inicial, é um ultrafiltro $\mathcal{U}$ em $B\cdot Ir$.

Prova do Lema 3.7': Que $\mathcal{U}$ é um filtro é imediato. Como as sequências coincidem a menos de um segmento inicial então $\mathcal{U}$ é um filtro maximal, portanto um ultrafiltro. ∴

Contruimos agora o conjunto $B\cdot Ir/\mathcal{U}$ dotado da topologia quociente. Pelos lemas anteriores sabemos que existe uma aplicação do espaço das partições sobre B·Ir/$\mathcal{U}$. Mas, funções que crescem exponencialmente estão relacionadas a binários não-normais (um binário é normal se a razão entre o número de zeros e uns tende para 1/2). Então estas funções são de medida nula em B·Ir e são um conjunto magro, o que completa a demonstração, pois pela Proposição 2.9 estas funções são as responsáveis pela parte não-nula da entropia.

∴

3.3 UM EXEMPLO NO ELETROMAGNETISMO CLÁSSICO.

Como vimos na seção anterior, podemos formalizar várias teorias matemáticas via o conceito de estruturas. Isto pode ser feito, em particular, para as teorias físicas, como a mecânica clássica, a mecânica quântica, a Relatividade Geral ou o eletromagnetismo (cf. ref. [11], [12], [14]).

Nessa seção examinaremos o caso do eletromagnetismo clássico e, a partir de sua formalização, construiremos uma proposição indecidível nessa teoria (veja [13]). Trabalharemos sempre com o sistema de axiomas ZFC e, quando for necessária a inclusão de algum outro axioma, isto será dito explicitamente.

Um campo eletromagnético será, para nós, um conjunto cuja estrutura pode ser deduzida do par ordenado $\langle M, U(1)\rangle$, onde M é a variedade espaço-temporal e U(1) é o grupo do círculo, i. e., U(1) é o grupo das transformações unitárias com um único parâmetro (para uma revisão dos conceitos de geometria diferencial veja [17] ou [20]). O nosso espaço-tempo M é uma variedade quadridimensional, Hausdorff e de classe C^∞, dotada de uma métrica lorentziana ([17]). Sabemos que um campo eletromagnético F tem que obedecer à equação de Maxwell:

$$dF = 0$$

Seja $\Lambda^2 T^*M$ o espaço fibrado das 2-formas sobre M, e seja $\mathcal{D}(M)$ o grupo de todos os difeomorfismos de classe C^∞ sobre M. Peguemos agora $C^\infty(\Lambda^2 T^*M)$ como sendo o conjunto de todas as seções de corte C^∞ de $\Lambda^2 T^*M$. Se $Z^2(M) \subset C^\infty(\Lambda^2 T^*M)$ é o espaço de todos os 2-cociclos em M, isto é, de todas as 2-formas cuja derivada exterior é nula, podemos fazer a seguinte definição:

<u>DEFINIÇÃO</u> 3.5: $EM = Z^2(M)/\mathcal{D}(M)$ é o espaço de todos os campo eletromagnéticos sobre M.

Uma rápida olhada nos mostra que a definição supra está de acordo com a dada usualmente para um campo eletromagnético (uma outra maneira de formalizarmos o eletromagnetismo pode ser encontrada em [12]), e que se F é um tal campo, então $F \in EM$ (veja [20] e [18]). A divisão feita entre $Z^2(M)$ e $\mathcal{D}(M)$ é necessária se quisermos que dois campos sejam iguais a menos de uma transformação de coordenadas.

Como $Z^2(M)$ tem uma base contável, EM também tem. Com isto, e acrecentando o fato de que EM é um espaço completo e métrico, concluimos que o espaço de todos os campos eletromagnéticos é um espaço polonês (cf. [11]; sobre as propriedades de um espaço polonês veja [50]).

Proposição 3.5: Consideremos o sistema ZFC + $2^{\aleph_0} = \aleph_\lambda >$ $\aleph_1$ + MA. Então, se $(\ldots)^{\underline{L}}$ denota os conjuntos construtiveis, no sentido de Gödel, na nossa teoria,

i) $(EM)^{\underline{L}}$ é magro em EM;

Se $(\ldots)^{B}$ denota a restrição a uma subclasse de conjuntos que ainda obedecem ao MA junto com o menor valor de cardinal para o contínuo, temos:

ii) $(EM)^{B}$ é magro em EM.

Prova: Ver em da Costa e Doria [11].

<u>DEFINIÇÃO</u> 3.6: Seja x um conjunto e $\underline{L}(x)$ a classe de todos os conjuhtos que podem ser construídos, no sentido de Gödel, de x. Dizemos que y pode ser obtido de x se e somente se $y \in \underline{L}(x)$.

Desde já, podemos ver que a definição anterior pode ser pensada como um processo qualquer que, usando o objeto x, obtemos, a partir de uma série de cálculos, o objeto y. Esta é uma caracterização bem liberal, que pode abranger vários conceitos em eletromagnetismo, como, por exemplo, a aproximação de um dado campo por outro, posto que ela exige que um dado y seja derivado de x por uma série de construções predicativas.

Com essa definições em punho, podemos estabelecer o nosso principal resultado nessa seção.

Proposição 3.6: A sentença:

"Todo o campo eletromagnético pode ser obtido de qualquer conjunto de campos que seja denso e que tenha a cardinalidade do contínuo, no espaço EM."

é indecidível em ZFC.

Prova: Chamemos a sentença entre aspas, da proposição anterior, de φ.

Lema 3.7: Em ZFC + $\underline{V} = \underline{L}$, $(\mathbb{R})^{\underline{\mathbf{L}}}$ é denso em $\mathbb{R}$.

Prova do Lema 3.7: Numa teoria em que vale o axioma $\underline{V} = \underline{L}$, todos os elementos são construtíveis. Como $(\mathbb{R})^{\underline{\mathbf{L}}}$ é o conjunto dos reais construtíveis no modelo, e $\mathbb{R}$ representa os reais nesse modelo, sabendo que $\mathbb{R}$ é contrutivo (pois $\underline{V} = \underline{L}$), temos que $(\mathbb{R})^{\underline{\mathbf{L}}}$ é denso em $\mathbb{R}$. $\therefore$

Lema 3.8: ZFC + $\underline{V} = \underline{L} \models \varphi$.

Prova do Lema 3.8: Dos axiomas ZFC, pode-se obter, como um teorema de ZFC, que, dados os irracionais, $Ir \subset [0, 1]$, existe uma função que é contínua, aberta e sobrejetora, da forma $f\colon Ir \Rightarrow Z^2(M)/\mathcal{D}(M)$. Então, no universo construtível de

Gödel, temos uma função $f^{\bar{L}}: (Ir)^{\bar{L}} \Rightarrow (EM)^{\bar{L}}$ que tem as propriedades supracitadas. Mas, todo $x \in (Ir)^{\bar{L}}$ pode ser construído (no sentido de Gödel) de um subconjunto denso, via cortes de Dedekind. Usando então a função $f^{\bar{L}}$ (que existe em consequência de ZFC), todos os $(EM)^{\bar{L}}$ podem ser obtidos a partir de um subconjunto denso e contável. ∴

Lema 3.9: ZFC + $\underline{V} \neq \underline{L}$ + GCH $\models \neg \varphi$.

Prova do Lema 3.9: Neste sistema de axiomas $|(Ir)^{\bar{L}}| = 2^{\aleph_0}$, e então, como a função f descrita na demonstração do lema anterior também existe aqui, $|(EM)^{\bar{L}}| = 2^{\aleph_0}$. Pelo lema 3.4, $(EM)^{\bar{L}}$ é denso em EM. Contudo, EM - $(EM)^{\bar{L}}$ não pode ser obtido de um subconjunto de campos que é construtível, incontável e que tem a cardinalidade do contínuo. ∴

Dos lemas 3.8 e 3.9, concluimos que existe um modelo em que φ é verdadeira e outro em que φ é falsa, ambos sendo modelos para ZFC. Com isto completa-se a demonstração.

∴

3.4 SOBRE A EXISTÊNCIA DE ESPAÇOS-TEMPO GENÉRICOS.

Estamos interessados aqui na existência de variedades genéricas na Relatividade Geral. Para tal, usando as ferramentas esboçadas na seção 3.1, por da Costa e Chuaqui ([10]), descrevemos intuitivamente como é feita a formalização da Relatividade Geral ([12] ou [14]). Nosso ponto de partida são os números reais, contruidos a partir dos inteiros via cortes de Dedekind obtidos com o uso dos axiomas de Zermelo-Frënkel. Via Predicados de Suppes construimos as estrutursas algébricas necessárias (para detalhes veja os exemplos dados em [12]) tais como grupos, aneis, corpos, etc...

Uma variedade diferenciável (que será o nosso espaço-tempo) é construida com dois conjuntos: Um espaço métrico separável e completo X, que será o conjunto de base principal, mais o conjunto dos reais, que servirá como base auxiliar. De $X \cup \mathbb{R}$ podemos obter $\mathbb{R}$ e $\mathbb{R}^n$, e aplicando-se o axioma do conjunto potência construimos os conjuntos $\mathbb{R}^X$ e $(\mathbb{R}^n)^X$. Se k denota um critério de diferenciabilidade, podemos obter, a partir do axioma da separação, os subconjuntos

$$k(X,\mathbb{R}) \subset \mathbb{R}^X$$

$$k(X,\mathbb{R}^n) \subset (\mathbb{R}^n)^X$$

$$k(\mathbb{R}^n,\mathbb{R}^n) \subset (\mathbb{R}^n)^{\mathbb{R}^n}$$

$$k(X,X) \subset X^X$$

necessários à construção do predicado de Suppes. Este predicado será uma união dos axiomas que caracterizam uma variedade diferencial real de dimensão finita.

Dada uma variedade diferenciável M, que é definida relacionando-se em ZFC domínios locais de M em $\mathbb{R}^n$, formemos o fibrado tangente $T^{\cdot}M$ e o fibrado cotangente $T^{-1}.M$. Do produto tensorial, para n=4, que é a dimensão do espaço-tempo, obtemos um co-tensor de segunda ordem g, a métrica, que será não degenerada e de assinatura +2.

Da maneira precedente podemos formalizar todos os pricipais objetos usados na Relatividade Geral e, com isto, mostra-se a existência destes objetos em ZFC.

Seja agora $\mathscr{E}$ uma 4-variedade cilíndrica, isto é, da forma $C\times\mathbb{R}$, onde C é uma 3-variedade compacta, real, lisa e tipo Hausdorff. Dotamos $\mathscr{E}$ de um tensor métrico lorentziano tal que para $x \in \mathbb{R}$, $C\times\{x\}$ é uma superfície tipo espaço.

Mostraremos que, se o espaço-tempo é uma variedade cilíndrica, então não existem espaços-tempo genéricos. Este resultado é obtido a partir de uma série de proposições, que serão postas a seguir.

Proposição 3.10: ZFC $\vdash$ "O conjunto de todas as classes de difeomorfismos dos espaço-tempo cilíndricos é contável".

Prova: Primeiro mostraremos que existem $\aleph_0$ espaços-tempo cilíndricos, para depois mostrarmos que existem no máximo $\aleph_0$.

Para que existam pelo menos $\aleph_0$ 4-variedades cilíndricas, temos que mostrar existirem pelo menos $\aleph_0$ 3-variedades compactas. Existem $\aleph_0$ 2-variedades compactas, como consequência do teorema da classificação (veja [30]). Se N é uma variedade dois-dimensional e compacta, então $N\times S^1$ é uma 3-variedade compacta, pois o círculo S^1 é compacto. Com isto temos que existem pelo menos $\aleph_0$ 3-variedades compactas e, como consequência, pelo menos $\aleph_0$ espaços-tempo compactos.

Existem no máximo $\aleph_0$ 3-variedades compactas, pois todas as 3-variedades são trianguláveis (veja [39]). Podemos com isso dividir a variedade num número finito de 3-simplices. Cada decomposição pode ser codificada por uma sequência finita de símbolos, e o número total de sequências deste tipo é no máximo $\aleph_0$.

$\therefore$

Seja $\mathcal{M}$ o conjunto de todos os espaçosa-tempo cilíndricos. Pela definiçãode cardinalidade, obtemos o seguinte corolário da proposição anterior:

Corolário 3.11:

i) ZFC $\vdash$ "Existe uma função $f : \omega_0 \Rightarrow \mathcal{M}$ que é sobrejetora e 1-1".

ii) ZFC $\vdash$ "Para todo n, $n \in \omega_0$ se e somente se $M_n = f(n) \in \mathcal{M}$".

Prova: Imediata.

Seja agora B uma álgebra booleana completa. Temos:

Proposição 3.12: $\|M_n \in \mathcal{M}\| = \bigvee_{m \in \omega_0} \|\hat{m} = n\|$.

Prova: Pelo corolário anterior temos que ZFC $\vdash$ " $\forall n$ [$(n \in \omega_0)$ $\leftrightarrow$ $M_n \in \mathcal{M}$]". Desta expressão obtemos

$$\|n \in \omega_o\| = \|M_n \in \mathcal{M}\| = \bigvee_{m \in \omega_o} \|\hat{m} = n\|.$$

$\therefore$

Corolário 3.13: $\underline{V}^{B} \models \mathcal{M} = \hat{\mathcal{M}}$.

Prova: Imediata.

O corolário 3.13 nos diz que o conjunto de todos os espaços-tempo cilíndricos é um conjunto *standard* numa extensão booleana $\underline{V}^{B}$.

Vejamos agora se existem espaços-tempo genéricos se a variedade é não compacta. Começaremos com a proposição seguinte:

Proposição 3.14: Seja M uma variedade quadridimensional real, lisa e não compacta. Então ZFC $\vdash$ "M admite um tensor métrico não degenerado e lorentziano".

Prova: veja Steenrod [47].

Com isto, em oposição aos espaços-tempo cilíndricos (Proposição 3.6), obtemos:

Proposição 3.15: ZFC $\vdash$ "Existem $2^{\aleph_o}$ classes de difeomorfismo das 4-variedades reais e não-compactas".

Prova: A demonstração segue a da proposição 3.6, ou seja, primeiro provamos ser no máximo $2^{\aleph_0}$ e depois provamos ser no mínimo $2^{\aleph_0}$.

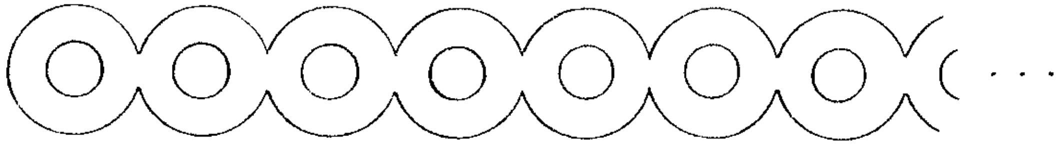
Para tal, seja uma aplicação $\varphi : \omega_0 \Rightarrow T^2$ de ω_0 em um 2-torus, isto é, a cada inteiro n associamos um torus $T^2 = S^1 x S^1$ representado por $T^2(n)$. Formemos com isto a soma conexa $\# \sum_{i \in \omega_0} T^2(i)$, que representa uma cadeia linear com vários tori, da forma $\ldots \# T^2(n-1) \# T^2(n) \# T^2(n+1) \# \ldots$. Obviamente se $T^2(n)$ é lisa, então $\# \sum_{i \in \omega_0} T^2(i)$ também é.

Para estabelecermos uma relação entre as 2-variedades e o contínuo, faremos o seguinte: Seja uma sequência binária $\alpha \in B\cdot Ir \subset 2^{\omega_0}$, onde $B\cdot Ir$ são os irracionais binários, cuja cardinalidade é $2^{\aleph_0}$; formamos de α a partir de $\# \sum_{i \in \omega_0} T^2(i)$ uma nova variedade, obtida de acordo com as regras:

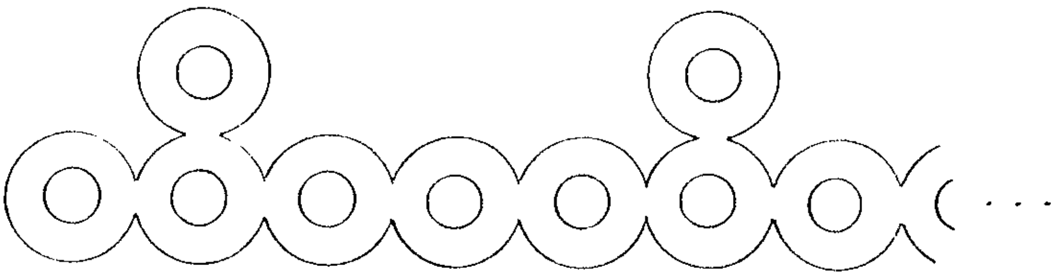
Se $\alpha(n) \neq 0$, não fazemos nada;

Se $\alpha(n) = 1$, somamos conexamente à $\# T^2(i) \subset \# \sum_{i \in \omega_0} T^2(i)$ um outro torus T^2;

Para exemplificarmos o procedimento, considermos a cadeia original $\# \sum_{i \in \omega_0} T^2(i)$ esquematizada abaixo:



Se a sequência α for da forma 0100010..., pelas regras anteriores obteremos a cadeia seguinte:



Se denotamos por M_α a nova variedade construida a partir do irracional α, é facil ver que se $\alpha, \beta \in B\cdot Ir$, $\alpha \neq \beta$ se e somente se $M_\alpha \not\cong M_\beta$, onde $\not\cong$ significa "não homeomorfo a".

Com isto, vimos que o conjunto $\{M_\alpha : \alpha \in B\cdot Ir\}$ tem a cardinalidade do contínuo, e então as variedades da forma $\{\mathbb{R}^{n-2}\times M_\alpha : \alpha \in B\cdot Ir\}$ formam um conjunto de variedades não-compactas e não-difeomorfas cuja cardinalidade é $2^{\aleph_0}$.

Falta-nos mostrar que existem no máximo $2^{\aleph_0}$ variedades não-compactas. Para tal, lembremos que toda a variedade diferenciável é paracompacta, o que implica existir um refinamento local finito para a cobertura contável, pois as variedades que estamos lidando são não-compactas (para tais definições veja Borisovich et al. [06]). Então, toda variedade não-compacta e diferenciável pode ser representada por uma cobertura localmente finita mais um conjunto contável de funções de transição. O conjunto de todos estes objetos devidamente codificados tem uma cardinalidade no máximo igual à do contínuo.

$\therefore$

Corolário 3.16: ZFC $\vdash$ "Existe uma função 1-1 e sobrejetora $f : 2^{\omega_0} \Rightarrow \mathcal{N}$, onde $\mathcal{N}$ é o conjunto de todas as variedades não compactas que admitem espaço-tempo".

Prova: Imediata.

Seja agora $\underline{V}$ um modelo para ZFC mais a hipótese generalizada do contínuo e o axioma da contrutibilidade, isto é, $\underline{V} \models$ ZFC + GCH + $\underline{V} = \underline{L}$. Em $\underline{V}$ temos a álgebra de Boole $B = RO(2^{\omega_o \times \omega_1})$, e podemos com isto construir a extensão booleana $\underline{V}^B$. Como vimos no Capítulo 1, $\underline{V}^B \models$ ZFC + CH.

Lema 3.17: $\underline{V}^B \models$ "Existem $2^{\hat{\aleph}_o}$ subconjuntos genéricos de $\hat{\omega}_o$.

Prova: veja Bell [03].

Corolário 3.18: $\underline{V}^B \models$ "Existem $2^{\aleph_o}$ variedades genéricas que admitem espaços-tempo".

Prova: Pelo Lema anterior, temos $2^{\hat{\aleph}_o}$ subconjuntos genéricos de $\hat{\omega}_o$. Mas, pela Proposição 3.16, concluimos que existem $2^{\hat{\aleph}_o}$ variedades genéricas. ∴

Examinemos com mais detalhe estas variedades genéricas.

Um espaço-tempo é um par ordenado $\langle M, g\rangle$, onde g é uma métrica lorentziana e M uma 4-variedade separável e tipo Hausdorff. Seja X uma cobertura contável para M,

$X = \{U_i : i \in \omega_o\}$ tal que:

i) $\bigcup_{i \in \omega_o} U_i = M$;

ii) Para $i \neq j$, é falso que $U_i \subseteq U_j$ ou $U_j \subseteq U_i$.

Proposição 3.18: ZFC $\vdash$ "Seja $f \in 2^{\omega_o}$, e associemos a cada f um subconjunto $X_f \subset X = \{U_i : i \in \omega_o\}$, dado da maneira seguinte:

$U_i \in X_f$ se e somente se $f(i) = 1$;

$U_i \not\in X_f$ se e somente se $f(i) = 0$.

Então:

a) $\bigcup V_j$, para todo $V_j \in X_f$, é um aberto;

b) Para $f \neq f'$, $\bigcup_{V_j \in X_f} V_j \neq \bigcup_{W_k \in X_{f'}} W_k$, f e $f' \in 2^{\omega_o}$"

Prova: Imediata.

Seaj agora $\underline{V}$ o universo bem fundado, e seja $B = RO(2^{\aleph_o})$ uma álgebra de Boole em $\underline{V}$, isto é, $B \in \underline{V}$. Então:

Proposição 3.19: $\underline{V}^{B} \vdash$ "Existe um conjunto aberto $U \subset \hat{M}$ tal que para todo o conjunto aberto standard $\hat{V} \subset \hat{M}$, temos $U \neq \hat{V}$".

Prova: Em $\underline{V}^{B} \vdash (2^{\hat{\omega}_o})^{\wedge} \subsetneq 2^{\hat{\omega}_o}$. Peguemos um f tal que $\underline{V}^{B} \vdash f \in 2^{\hat{\omega}_o}$ e tal que para, todo o elemento $\hat{g}$ que seja standard, temos $f \neq \hat{g}$. Então, $\underline{V}^{\mathbf{B}} \models$ "Para todo o $\hat{g} \in 2^{\hat{\omega}_o}$,

$$\bigcup_{v_{\hat{j}} \in x_f} V_{\hat{j}} \neq \bigcup_{w_{\hat{k}} \in x_{\hat{g}}} W_{\hat{k}} . \quad \therefore$$

Então, quando vamos para a extensão booleana $\underline{V}^{\mathbf{B}}$ de $\underline{V}$, concluimos que $\underline{V}^{\mathbf{B}}$ tem mais conjuntos abertos, que são os abertos genéricos. Podemos, a partir disto, colocar a seguinte pergunta: Trazem estes abertos alguma informação adicional, do ponto de vista da física? De outra maneira, existe alguma experiência que possa detectar esses novos abertos?

Tentemos clarear estas questões através de algunsa resultados e exemplos envolvendo os conjunto abertos genéricos.

Proposição 3.20: $\underline{V}^{\mathbf{B}} \models$ "Todo a bola aberta $U \subset M$ é difeomorfa a uma bola aberta standard $\hat{W} \subset M$".

Prova: Imediata, pois todas as bolas abertas são difeomorfas entre si na variedade M. $\therefore$

Proposição 3.21: $\underline{V}^{\mathbf{B}} \models$ "Se $K \subset M$ é compacta, então K é standard".

Prova: Se K é compacta, então só existem $\aleph_0$ subvariedades com esta propriedade (mostra-se de m aneira similar à proposição 3.10). Com isto todas as subvariedades K que são compactas são também standard. $\therefore$

Daremos agora alguns exemplos que explicitam mais como os conjuntos abertos genéricos em M podem ser difeomorfos a abertos standard. Nossos exemplos serão dados em uma extensão por forcing $\underline{V}(B)$ do universo booleano $\underline{V}^{B}$.

Exemplo 1: Seja $\mathbb{R}$, a reta real, coberta com uma coleção contável de intervalos abertos centrados em cada $x \in \mathbb{Z}$, e com diâmetro igual a $1 + \varepsilon$, $0 < \varepsilon << 1$. Se X é tal cobertura, qualquer $\bigcup_{V_i \in Y} V_i$, $Y \subsetneq X$ será aberta e desconexa. Dado $\underline{V}^{B}$, seja $\underline{M}[G]$ o modelo por forcing associado a $\underline{V}^{B}$ (veja Kunen [32]). Seja ainda u um objeto não standarrd em $\underline{M}[G]$. Então, o aberto (em $\underline{M}[G]$) $X_u = \bigcup_{i \in u} V_i$ tem $\aleph_0$ pedaços. Mas X_u é difeomorfo (em $\underline{M}[G]$) a $Z = \bigcup_{i \text{ par}} V_i$, que é claramente um conjunto standard.

Exemplo 2: Em $\underline{M}[G]$, cubramos $\mathbb{R}^2$ com um conjunto contável de quadrados abertos centrados em cada $x \in \mathbb{Z}^2$ e com lados iguais a $1 + \varepsilon$, $0 < \varepsilon << 1$, paralelos aos eixos coordenados. Restringiremos a nossa atenção ao primeiro quadrante. Como a cobertura é contável, podemos associar a cada quadrado aberto um número inteiro. Com isto, podemos conectar cada centro de quadrado por uma linha contínua. Dada tal enumeração, e para um u genérico (como no exemplo anterior), tiramos os quadrdos abertos cujos índices caiam sobre u. Temos então um plano com $\aleph_0$ buracos nos x em u. Desde que podemos traçar uma linha contínua através de todos os pares positivos com coordenadas integrais em $\mathbb{R}^2$, podemos "esticar" esta linha, tal que os buracos que formamos em $\mathbb{R}^2$ irão cair, digamos, na primeira coluna do quadrante positivo. Temos novamente um conjunto aberto genérico (o plano sem os buracos nos lugares codificados por u) que é difeomorfo a um conjunto standard aberto em $\mathbb{R}^2$.

Pela construção do exemplo anterior, vemos que ele pode facilmente ser generalizado para dimensões superiores a dois, sendo válido para qualquer $\mathbb{R}^n$, $n \in \omega_o$.

Exemplo 3: Seja dada uma cadeia infinita de tori $\#\sum_{i \in \omega_o} T^2(i)$, como a vista anteriormente, em $\underline{M}[G]$. Esta variedade é claramente standard. Seja agora dada uma função característica $f_u \in \underline{M}[G]$ para um subconjunto genérico $u \subset \hat{\omega}_o$, e corte um disco de cada torus $T^2(i) \subset \#\sum_{i \in \omega_o} T^2(i)$ se e somente se $f_u(n) = 1$ e não faça mais nada se e somente se $f_u(n) = 0$. Este procedimento resultará numa variedade $\xi_u \subsetneq \#\sum_{i \in \omega_o} T^2(i)$ que é obviamente genérica e não-compacta, porque ele não pode ser difeomorfa a uma variedade standard.

Com o exemplo 3 vimos que, dada uma variedade standard $\hat{M} \in \underline{M}[G]$, podemos ter subvariedades abertas genéricas $X \subsetneq \hat{M}$, tal qual ξ_u.

CONCLUSÕES

Utilizando as ferramentas dadas pela teoria axiomática de conjuntos e a teoria de modelos, mostramos em que isto influi na semântica de uma teoria axiomatizada em física matemática. Após termos estudado alguns conceitos relacionados à teoria ergódica, demonstramos a existência de uma ligação entre a velocidade de crescimento da cardinalidade do conjunto de órbitas simbólicas de um dado sistema e sua entropia. Este resultado nos levou a uma versão diferente do teorema de Rohlin ([46]). Junto com este teorema, mostramos que a entropia não é um conceito absoluto (do ponto de vista da teoria de modelos).

Como sabemos, a entropia é uma medida da quantidade de informação de um dado sistema ([45]). Se um sistema se comporta de maneira aleatória, a quantidade de informação contida nesse sistema é maior, implicando ser a sua entropia positiva. Mas vimos que, se um dado sistema tem entropia positiva num dado modelo, ele pode ter entropia nula noutro. Resta-nos então a pergunta: este sistema é ou não determinístico?

Todos estes resultados nos levam a pensar melhor sobre a caracterização, via entropia, de fenômenos caóticos ou aleatórios.

Na seção 3.3, obtivemos uma sentença formalmente indecidível no eletromagnetismo clássico. Esta sentença nos dizia que, numa dada extensão booleana, podiam existir campos eletromagnéticos que não seriam alcançáveis, via processos contrutíveis (no sentido de Gödel), de um conjunto denso de campos, que poderiam ser escolhidos (fisicamente e matematicamente) como sendo os campos "bem comportados". Tais processos construtivos quaisquer poderiam bem ser interpretados como sendo uma aproximação (no sentido amplo da palavra).

Ainda dentro da idéia original, verificamos algumas consequências da teoria de modelos booleanos em espaços-tempo da Relatividade Geral ([14]). Mostramos que, se o espaço-tempo for cilíndrico, não teremos espaços-tempo genéricos; por outro lado, se o espaço-tempo for não compacto, teremos uma infinidade de espaços-tempo genéricos. Pela Proposição 3.20 e pelos exemplos na seção 3.4, vimos que, só podemos diferenciar variedades genéricas de variedades *standard* via propriedades globais, posto que abertos locais serão sempre difeomorfos entre si e, pelo princípio da relatividade, com isto, não existem experiências (locais) que diferenciem abertos genéricos de abertos *standard*. Uma pergunta, ainda não respondida, nos resta ([14]): Como podemos detectar se o nosso universo é ou não genérico? Como vimos, somente experiências globais poderiam nos trazer uma resposta a esta pergunta.

Vimos, com todos estes exemplos, que uma determinada teoria pode nos levar a uma multiplicidade de conclusões, o que nos mostra que existe bem mais trabalho para o físico matemático fazer do que se supõe. O que temos aqui, como Cohen sugeriu ([09]), é algo parecido com a situação da divisão da geometria no século XIX, quando Gauss, Lobatchevskii e Riemann mostraram existir outras geometrias, além da euclidiana, onde o quinto postulado de Euclides não era mais válido.

REFERÊNCIAS:

[01] - B. W. Augerstein, *Hadron Physics and Transfinite Set Theory*, Inter. J. Theoretical Phys. 23(1984) 1197;

[02] - Roger Balian, *Du Microscopique au Macroscopique* - Tome 1, École Polytechnique 1982;

[03] - J. L. Bell, *Boolean-Valued Models and Independence Proofs in Set Theory* - 2nd edition, Clarendon Press 1985;

[04] - Patrick Billingslay, *Ergodic Theory and Information*, John Wiley ú Sons, Inc. 1965;

[05] - G. D. Birkhoff, *Proof of the Ergodic Theorem*, Proc. Nat. Acad. Sci. USA 17(1931) 656;

[06] - Yu. Borisovich, N. Blizniakov, Ya. Izrailevich, T. Fomenko, *Introduction to Topology*, Mir Publishers 1985;

[07] - P. J. Cohen, *The Independence of the Continuum Hypothesis*, Proc. Nat. Acad. Sci. USA 50(1963), 1143 - 1148; *The Independence of the Continuum Hypothesis II*, Proc. Nat. Acad. Sci. 51(1964) 1143;

[08] - P. J. Cohen, *Set Theory and the Continuum Hypothesis*, W. A. Benjamin Inc. 1966;

[09] - P. J. Cohen e R. Hersh, *Non-Cantorian Set-Theory*, Sci. Amer., 217(Dec. 1967) 104;

[10] - N. C. A. da Costa e R. Chuaqui, *On Suppes Set Theoretical Predicates*, Erkenntnis, 29(1988) 95;

[11] - N. C. A. da Costa e F. A. Doria, *Structures, Suppes Predicates and Boolean-Valued Models in Physics*, a aparecer em Papers in Honour of V. Smyslov, Moscou 19XX;

[12] - N. C. A. da Costa e F. A. Doria, *Suppes Predicates for First-Quantized Physics*, preprint 1989;

[13] - N. C. A. da Costa, F. A. Doria e J. A. de Barros, *On a Formally Undecidable Statement in Classical Electromagnetic Theory*, a aparecer em S. de Barros, ed. Essays in Honor of Prof. C. M. do Amaral.

[14] - N. C. A. da Costa, F. A. Doria e J. A. de Barros, *A Suppes Predicate for General Relativity and Set-theoretically Generic Space-times*, preprint 1989;

[15] - F. A. Doria, J. A. de Barros e M. Ribeiro da Silva, *Non-Computable Functions, Generic Functions and Random Sequences*, Boletim da SPM 8(2) (1987) 197;

[16] - F. A. Doria, *Boolean-Valued Models in Set Theory*, Notas de Curso, Forum de Ciência e Cultura/UFRJ, 1988;

[17] - T. Eguchi, P. B. Gilkey e A. J. Hanson, *Gravitation, Gauge Theory and Differential Geometry*, Phys. Rep. 66(6) (1980) 213;

[18] - G. G. Emch, *Mathematical and Conceptual Foundations of the 20th Century Physics*, North Holland 1984;

[19] - P. Fernandez, *Medida e Integração*, Projeto Euclides, IMPA 1976;

[20] - H. Flanders, *Differential Forms*, Academic Press 1963;

[21] - Nathaniel A. Friedman, *Introduction to Ergodic Theory*, Van Nostrand Reinhold Company 1970;

[22] - Kurt Gödel, *Ueber Formal Unentscheidbare Saetz der Principia Matematica und Verwandter Systeme I*, Monastch. Math. Phys. 38(1931) 173; Uma tradução ao português pode ser encontrada em: K. Gödel, *O Teorema de Goedel e a Hipòtese de Contìnuo*, Ed. Calouste Gulbenkian 1979;

[23] - Kurt Gödel, *What is Cantor's Continuum Problem?*, The Amer. Math. Monthly 54(1947) 515;

[24] - Paul R. Halmos, *Naive Set Theory*, Van Nostrand 1960;

[25] - Paul R. Halmos, *Lectures on Boolean Algebras*, Van Nostrand Reinhold 1963;

[26] - Paul R. Halmos, *The Basic Concepts of Algebraic Logic*, Amer. Math. Monthly 63(1956) 363;

[27] - Paul R. Halmos, *Measure Theory*, D. Van Nostrand Company Inc. 1950;

[28] - Thomas Jech, *Set Theory*, Academic Press 1978;

[29] - Amnon Katz, *Principles of Statistical Mechanics*, W. H. Freeman and Company 1967;

[30] - Czes Kosniowski, *A First Course in Algebraic Topology*, Cambridge University Press 1980;

[31] - J. L. Krivine, *Thèorie Axiomatique des Ensembles*, NRF 1969;

[32] - Kenneth Kunen, *Set Theory*, North Holland 1983;

[33] - Emanuel Carneiro Leão, Marcio Tavares D'Amaral, Muniz Sodré e F. A. Doria, *A Màquina e seu Avesso*, Francisco Alves 1987;

[34] - Seymour Lipschutz, *General Topology*, Schaum Publishing Company 1965;

[35] - Ricardo Mañé, *Teoria Ergòdica*, Projeto Euclides, IMPA 1983;

[36] - Yuri Ivanovich Manin, *A Course in Mathematical Logic*, Springer Verlag 1977;

[37] - G. W. Mackey, *Ergodic Theory and its Significance for Statistical Mechanics and Probability Theory*, Adv. in Math. 12(1974) 178;

[38] - Richard Mansfield e John Dawson, *Boolean-Valued Set Theory and Forcing*, Synthèse 33(1976) 223 - 252;

[39] - Edwin E. Moise, *Affine Structures in 3-Manifolds, V. The Triangulation theorem and Hauptvermutung*, Annals of Math. 56(1952) 96;

[40] - James R. Munkres, *Elements of Algebraic Topology*, The Benjamin/Cummings Publishing Company, Inc. 1984;

[41] - Ernest Nagel e James R. Newman, *Prova de Goedel*, Editora Perspectiva 1973;

[42] - Karl Petersen, *Ergodic Theory*, Cambridge University Press 1983;

[43] - Daniel J. Rudolph, *An Example of a Measure Preserving Map with Minimal Self-joining, and Applications*, Journal d'Analyse Math. 35(1979) 97;

[44] - Robert R. Stoll, *Set Theory and Logic*, Dover Pub. 1979;

[45] - Claude Shannon, *A Mathematical Theory of Communication*, Bell System Technical Journal 27(1948) 379;

[46] - Karl Sigmund, *On the prevalence of Zero Entropy*, Israel J. Math. 10(1971) 281;

[47] - N. Steenrod, *The Topology of Fiber Bundles*, Princeton University Press 1951;

[48] - P. Suppes, *Axiomatic Set Theory*, Van Nostrand 1960;

[49] - Richard C. Tolman, *Principles of Statistical Mechanics*, Dover Pub. Inc. 1979;

[50] - François Treves, *Topological Vector Spaces, Distributions and Kernels*, Academic Press 1967;

[51] - Constantino Tsallis, *Notas do Curso de Mecânica Estatística*, CBPF 1978;

[52] - Y. Uspenski, *Goedel's Undecidability Theorem*, Mir Publishers 1987;

"CONJUNTOS GÊNERICOS SEGUNDO COHEN E SUAS APLICAÇÕES À FÍSICA"

JOSÉ ACÁCIO DE BARROS

Tese de Mestrado apresentada no Centro Brasileiro de Pesquisas Físicas do Conselho Nacional de Desenvolvimento Científico e Tecnológico, fazendo parte da Banca Examinadora os seguintes Professores:

Francisco Antonio de Moraes Accioli Dória
(Orientador)

Antonio Fernandes da Fonseca Teixeira
(Co-orientador)

Marcelo Dutra Fragoso

Newton Carneiro Affonso da Costa

Rio de Janeiro, 06 de outubro de 1989