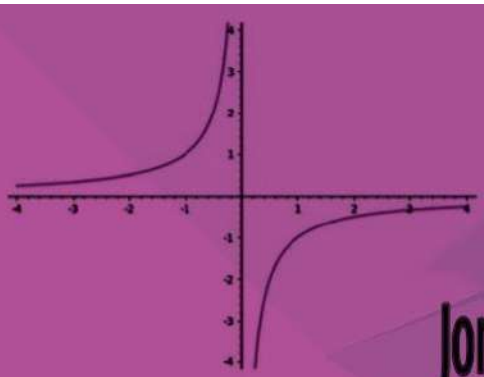
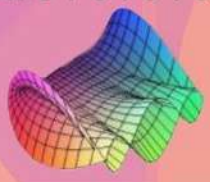


JEEPEMA

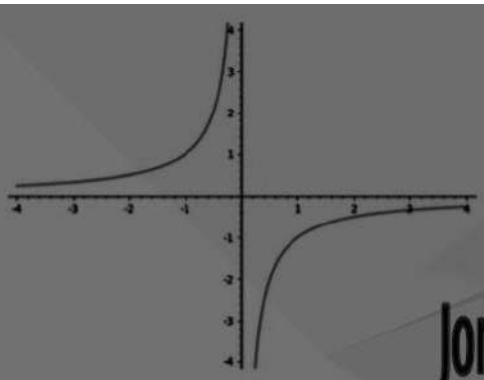
Jornal eletrônico de Ensino e Pesquisa de matemática

Cálculo Diferencial e Integral:

Exercícios • Apostilas • Resoluções • Vídeos Aulas •



um kit de sobrevivência!

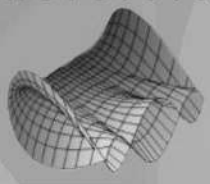


JEEPEMA

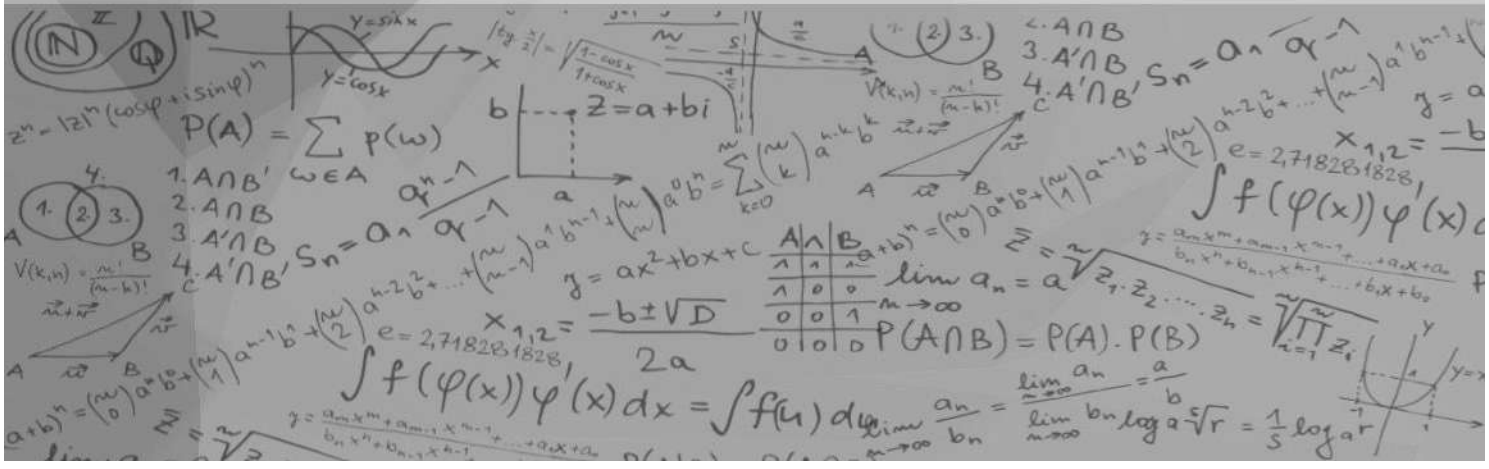
Jornal eletrônico de Ensino e Pesquisa de matemática

Cálculo Diferencial e INTEGRAL:

Exercícios • Apostilas • Resoluções • Vídeos Aulas •



um kit de sobrevivência!



Jornal Eletrônico de Ensino de Matemática - JEEPEMA
Universidade Estadual de Maringá, Maringá-PR - Brasil
ISSN: 2594-6323
DOI: 10.4025/jeepema

Vol. 2 N° 2 / 56 páginas - Dezembro/2018

Palavras-chave: Modelo Matemático, Seleção Natural, Teoria dos Números, Criptografia Teoria dos Jogos e Teorema de Nash.

Índice

Volume 2 - N° 2

Jornal Eletrônico de Ensino e Pesquisa de Matemática
(1s.) **v. 2** 2 (2018): 1–15. ©JEEPEMA–ISSN-2594-6323.
www.dma.uem.br/kit/jeepema

Notas sobre Modelagem Matemática na Genética de Populações com Seleção

Vinícius Freitas de Oliveira e Suzete Maria Silva Afonso

RESUMO: A genética de populações é a ciência que estuda o comportamento das frequências alélicas e genotípicas nas populações e quais os possíveis fenômenos que podem alterá-las ao longo do tempo. A fim de estabelecer uma interdisciplinaridade entre biologia e matemática, estas notas exibe a construção de um modelo matemático para populações com a presença de seleção natural de forma que contemple o comportamento de tais frequências no tempo. Para tanto, são utilizados conceitos de probabilidade, estatística e equações de diferença. O modelo final trata de uma equação de diferenças não linear e o estudo dos resultados conta com o auxílio do método teia de aranha para a análise qualitativa dos resultados. Estas notas foram inspiradas nas notas de aula de Ocone (2014), [7].

Sumário

1. Introdução

No final do século XIX, com a necessidade de estudar variações hereditárias nas populações, surgiu a ciência da genética de populações. Essa ciência analisa o comportamento das frequências gênicas nas populações, bem como os fenômenos capazes de alterá-las no decorrer do tempo. Esses fenômenos são compreendidos principalmente pela migração, seleção natural e mutação.

As variações gênicas dependem de características específicas dos indivíduos, o genótipo e o fenótipo, e para entendê-las advimos do sistema estrutural de funcionamento dos organismos vivos, a célula. É na célula que está contida toda a informação genética, passada de forma hereditária. Essa herança é chamada de gene e trata-se de um trecho da molécula de ácido desoxirribonucleico, o DNA (AMABIS e MARTHO, 1994).

Os genes são encontrados em um local dos cromossomos, denominado locus, no plural loci. As diferentes formas e variações dos genes são chamadas de alelos, que têm direta influência na determinação de uma característica (LEWIS, 2004). Os alelos são identificados por letras, podendo ser recessivos ou dominantes. Alelos dominantes, representados por letras maiúsculas, sempre se expressam. Já os alelos recessivos, representados por letras minúsculas, são inibidos na presença de alelos dominantes, ou seja, só possuem expressão quando sozinhos.

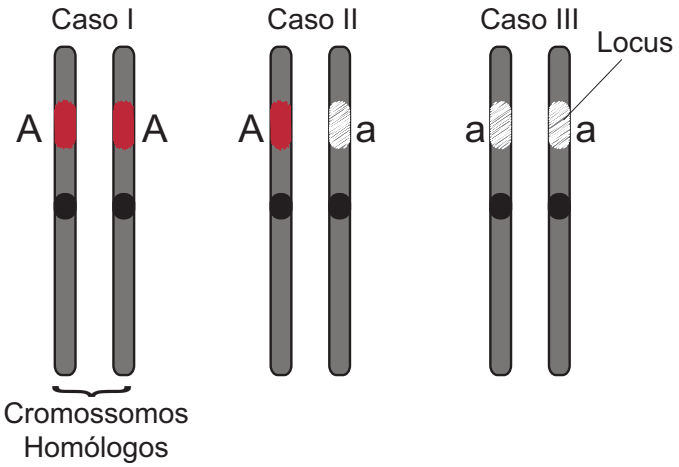
Os cromossomos podem ser subdivididos como autossômicos, que não se diferem entre os sexos, e sexuais, que determinam o sexo do indivíduo. Para as chamadas espécies diploides, os cromossomos autossômicos são agrupados em pares homólogos, que são iguais entre si. Esses cromossomos pareados são chamados de genótipos, que são uma estrutura gráfica dos alelos. São os genótipos que possuem o código para construir uma proteína e determinar uma característica. Essa característica é chamada de fenótipo (LEWIS, 2004).

A diferença entre genótipo e fenótipo é mais complexa, pois além do fenótipo ter dependência direta do genótipo, ele também depende da influência do meio em que se vive (HARTL e CLARK, 2007). Por exemplo, a cor da pele é uma característica, portanto, um fenótipo. O genótipo do indivíduo irá dizer a quantidade da proteína melanina que deverá ser produzida, porém, a exposição ao fator externo, o sol, também terá influência na cor da pele. A Figura 1 mostra cromossomos homólogos com seus diferentes genótipos.

Analisando a Figura 1, pelos casos I e III, observam-se os genótipos **AA** e **aa**, respectivamente, possuindo dois alelos iguais — homozigose; já no segundo caso, observa-se o genótipo **Aa**, com alelos diferentes — heterozigose.

O estudo dos genótipos e de suas frequências genotípicas é muito importante, pois nos permite prever as suas distribuições em proles provenientes de acasalamentos de um grupo de indivíduos da mesma espécie. As aplicações dessas previsões são numerosas e muito úteis na medicina, no direito, na biotecnologia, na sociologia, na antropologia, nas políticas sociais, dentre outras áreas. Por exemplo, a compreensão das distribuições genotípicas no decorrer do tempo pode ajudar na percepção de doenças hereditárias, levando a uma possível cura, ou no mapeamento genético da susceptibilidade de doenças, incluindo o câncer, ou na melhoria no desempenho de animais domésticos e plantas cultivadas, ou ainda na organização de programas de cruzamentos para a conservação de espécies ameaçadas de extinção (HARTL e CLARK, 2007).

Figura 1: Cromossomos Homólogos e Genótipos



FONTE: Os Autores (2018)

Aqui, temos como objetivo realizar aplicações matemáticas na genética de populações por meio da construção e análise de um modelo matemático para populações com seleção. Cabe mencionar que essa construção pode também ser verificada em Ocone (2014), [7]. A modelagem será promovida por meio de conceitos de probabilidade, estatística e equações de diferenças e o modelo será examinado mediante a análise de estabilidade e o método teia de aranha.

Para a elaboração da figura presente no texto foi utilizado o software Adobe Illustrator^{R} e para a construção dos gráficos o software AutoCAD^{R}.

2. Princípios de Genética de Populações

O grande propósito dos modelos de genética de populações é descobrir qual é a probabilidade que um indivíduo portador de um genótipo G tenha um descendente com esse mesmo genótipo. Essa probabilidade dependerá de diversas premissas sobre quão provável é que indivíduos de diferentes genótipos acasalem entre si. Os itens abordados nesta seção tratam de princípios por trás dessas premissas.

2.1. Frequências Alélicas e Frequências Genotípicas. Considere uma população qualquer e um dos possíveis genótipos, $G_1 \cdots G_k$. A frequência $f_{G_1 \cdots G_k}$ é definida pela seguinte fórmula:

$$f_{G_1 \cdots G_k} \triangleq \frac{\text{número de indivíduos com genótipo } G_1 \cdots G_k}{\text{tamanho da população}}. \tag{1}$$

Quando o tempo for considerado, $f_{G_1 \ldots G_k}(t)$ denotará a frequência genotípica no tempo t.

As frequências alélicas são calculadas contando somente alelos e ignorando como eles são organizadas em genótipos. Seja l um locus. Dada uma população, a coleção alélica para o locus l é a coleção de todos os alelos de genótipos de população que ocorrem no locus l. Lembramos que uma população é tratada como uma coleção de sequências de caracteres genotípicos. Considere um alelo particular A que pode ocorrer em l. A frequência f_A de A é definida como sua frequência relativa à coleção alélica correspondente a l da seguinte forma:

$$f_A \triangleq \frac{\text{número de } A\text{'s na coleção alélica de } l}{\text{tamanho da coleção alélica de } l}, \tag{2}$$

e, de forma similar à frequência genotípica, denotamos a frequência alélica no tempo t por $f_A(t)$.

Exemplo 2.1. *Considere o estudo de um locus com dois alelos, A e a, para uma população de espécies diploides. Uma coleta de 15 amostras dessa população obteve o seguinte resultado: $AA, AA, Aa, AA, aa, aa, aa, Aa, Aa, AA, AA, aa, Aa, Aa, AA$.*

Se essas amostras representam toda a população, então as frequências genotípicas valem: $f_{AA} = \frac{6}{15} = \frac{2}{5}$, $f_{Aa} = \frac{5}{15} = \frac{1}{3}$ e $f_{aa} = \frac{4}{15}$, valores obtidos com a fórmula (1). Com a fórmula (2), vemos que as frequências alélicas valem: $f_A = \frac{17}{30}$ e $f_a = \frac{13}{30}$.

Veja que para um locus com dois alelos, A e a, os possíveis genótipos são AA, Aa e aa, assim, é fácil notar que: $f_A + f_a = 1$ e $f_{AA} + f_{Aa} + f_{aa} = 1$. Além disso, existe uma relação entre as frequências genotípicas e alélicas. É o que veremos na próxima proposição.

Proposição 2.2. *Seja $\mathcal{P}$ uma população de uma espécie diploide com tamanho N e seja l um locus nessa população que admite dois alelos, A e a. Então,*

$$f_A = f_{AA} + \frac{f_{Aa}}{2} \quad e \quad f_a = f_{aa} + \frac{f_{Aa}}{2}.$$

Demonstração. Como N é o tamanho da população $\mathcal{P}$ e ela é diploide, segue que o tamanho da coleção de alelos no locus l, onde A ocorre, é $2N$. Contudo, para contarmos a quantidade de A's no grupo de alelos do locus l, usaremos as frequências genotípicas. Pela definição de f_{AA} (veja (1)), existem Nf_{AA} genótipos AA na população, e como cada um deles contribui com dois alelos A's, no total existem $2Nf_{AA}$ desses alelos na população $\mathcal{P}$. Do mesmo modo, existem Nf_{Aa} genótipos Aa que contribuem com um total de Nf_{Aa} alelos A. Como os indivíduos com genótipos aa não contribuem para a frequência f_A, por (2) segue que

$$f_A = \frac{2Nf_{AA} + Nf_{Aa}}{2N} = f_{AA} + \frac{f_{Aa}}{2}.$$

A frequência do alelo a, f_a, pode ser obtida de forma análoga. □

Embora as frequências alélicas possam ser encontradas através das frequências genotípicas, sem pormenorizar, a recíproca não é válida, pois as frequências genotípicas não dependem apenas da quantidade de alelos, mas de como os alelos estão distribuídos entre os indivíduos.

2.2. Acasalamento Aleatório. De acordo com Magalhães e Lima (2010), uma variável aleatória trata-se de um valor de interesse proveniente de um experimento aleatório e é exatamente esse conceito que arquiteta a definição de acasalamento aleatório.

Definição 2.3. *O acasalamento aleatório é a criação de um novo indivíduo pela união de dois gametas, um óvulo e um espermatozoide, escolhidos por experimentação aleatória na população. Em suma, cada gameta, seja masculino ou feminino, é cedido de maneira aleatória por seus pais.*

No caso de espécies monoicas, espécies que apresentam órgãos sexuais dos dois sexos, ambos gametas virão de um mesmo grupo de acasalamento, havendo possibilidade de reposição, ou seja, os dois gametas podem ser de um mesmo pai ou não. Quando os gametas vem de um mesmo pai, ocorre a chamada autofecundação. Para uma população com tamanho N, a probabilidade de ocorrer uma autofecundação é de $1/N$. Consequentemente, para uma população muito grande, essa probabilidade é extremamente pequena. O lema abaixo estabelece um princípio simples para calcular a probabilidade genotípica da prole através da frequência de ocorrência.

Lema 2.4. *Seja S uma população com reprodução por acasalamento aleatório e A um alelo. Se p_A^S é a probabilidade do gameta possuir o alelo A e f_A^S é a frequência desse alelo na população S, então:*

$$p_A^S = f_A^S \tag{3}$$

O Lema 2.4 traz um dos resultados mais importantes para modelos baseados em acasalamentos aleatórios e sua prova pode ser encontrada em Ocone (2014). A equação (3) é uma consequência da ideia de escolha aleatória do parceiro e da natureza da reprodução sexual.

Para finalizarmos as considerações a respeito do acasalamento aleatório, o exemplo abaixo traz uma aplicação importante do Lema 2.4.

Exemplo 2.5. *Considere um acasalamento aleatório ocorrendo em uma população de genótipos AA, Aa e aa em uma população monoica (com um locus e dois alelos A e a), com frequências alélicas f_A e f_a. Sejam p_A^1 e $p_a^1 = 1 - p_A^1$ as probabilidades dos progenitores masculinos passarem os alelos A e a, respectivamente, para a prole no acasalamento aleatório. E sejam p_A^2 e $p_a^2 = 1 - p_A^2$ as probabilidades dos progenitores femininos transmitirem os alelos A e a, respectivamente, para a prole no acasalamento aleatório. Uma vez que ambos os progenitores são escolhidos do mesmo grupo de acasalamento (estamos considerando uma espécie monoica), segue que:*

$$p_A^1 = p_A^2 = f_A \qquad e \qquad p_a^1 = p_a^2 = f_a.$$

A probabilidade da prole, de um acasalamento aleatório, possuir genótipo AA é equivalente à probabilidade dela receber o alelo A de cada progenitor (análogo para aa), já que os progenitores são escolhidos de forma independente. Sendo assim, tem-se

$$P(\textit{prole ser } AA) = p_A^1 \cdot p_A^2 = (f_A)^2 = \left(f_{AA} + \frac{f_{Aa}}{2}\right)^2 \tag{4}$$

e

$$P(\textit{prole ser } aa) = p_a^1 \cdot p_a^2 = (f_a)^2 = \left(f_{aa} + \frac{f_{Aa}}{2}\right)^2. \tag{5}$$

Por fim, para calcular a probabilidade da prole obter um genótipo Aa, leva-se em conta a contribuição de ambos os alelos, A e a. Desta forma, obtém-se

$$P(\textit{prole ser } Aa) = p_A^1 p_a^2 + p_a^1 p_A^2 = 2 f_A f_a = 2\left(f_{AA} + \frac{f_{Aa}}{2}\right)\left(f_{aa} + \frac{f_{Aa}}{2}\right). \tag{6}$$

2.3. Mutação, Seleção e Migração. A mutação é uma mudança aleatória na sequência do DNA de um único gene. Essa variação ocorre em um alelo de um gameta proveniente do grupo de acasalamentos por um erro no processo de reprodução ou por consequências da radiação (BEIGUELMAN, 2008).

A seleção natural, intitulada por Darwin, é um princípio em que indivíduos de uma população estão sujeitos, devido à luta pela vida, a probabilidades de sobrevivência antes de se tornarem possíveis reprodutores, por diversos fatores, incluindo a influência genotípica. Em outras palavras, a seleção natural acontece quando diferentes genótipos têm diferentes chances de sobrevivência ou sucesso reprodutivo (HARTL e CLARK, 2007).

Já a migração, segundo Hartl e Clark (2007), ocorre quando indivíduos entram e saem, em massa e de forma desorganizada, de uma população. As chamadas cidades universitárias dispõem dessa característica, pois muitos jovens chegam na cidade para estudar, fazem parte do grupo de reprodutores por um período de tempo muito curto, se formam e vão embora.

2.4. Gerações Não-sobrepostas. O conceito de gerações não-sobrepostas exprime que os indivíduos de uma geração qualquer t acasalam entre si para produzir a geração $t+1$ e a partir disso não acasalam mais. Da mesma forma, a geração $t+1$ acasala entre si e, analogamente, não acasalam mais, e assim por diante (OCONE, 2014). Esse princípio é muito útil para modelos de populações com acasalamentos sazonais, como é o caso de muitas espécies de pássaros.

2.5. Premissa da População Infinita. O próximo princípio é a suposição de uma população infinita, ou seja, a suposição de que o limite do tamanho da população tende ao infinito. Embora essa premissa seja extremamente simples, os seus resultados e a sua aplicação tem uma enorme relevância.

Considere uma população de filhos construída por acasalamento aleatório de uma determinada população de pais. Seja $f_{G_1 \cdots G_k}$ a frequência de um genótipo na população de descendentes e seja $p_{G_1 \cdots G_k}$ a probabilidade de que o genótipo é produzido em um único acasalamento aleatório.

A premissa da população infinita consiste em impor que, para todo genótipo, seja válida a seguinte identidade[1]:

$$f_{G_1 \cdots G_k} = p_{G_1 \cdots G_k}. \tag{7}$$

Na realidade prática, a utilização da premissa de população infinita é útil para uma população tão grande de tal forma que a identidade (7) represente o que ocorre quando a população tende ao infinito, tornando-se uma boa aproximação.

2.6. Equilíbrio de Hardy-Weinberg. Godfrey Harold Hardy e Wilhem Weinberg chegaram quase simultaneamente a conclusões sobre a genética de populações. Essas conclusões passaram a ser conhecidas como a lei do equilíbrio de Hardy-Weinberg.

Definição 2.6. *As frequências genotípicas f_{AA}, f_{Aa} e f_{aa}, com $f_{AA} + f_{Aa} + f_{aa} = 1$, estão no equilíbrio de Hardy-Weinberg se existir $p \in \mathbb{R}$, com $0 \leq p \leq 1$, de tal modo que:*

$$f_{AA} = p^2, \qquad f_{Aa} = 2p(1-p) \qquad e \qquad f_{aa} = (1-p)^2.$$

O equilíbrio de Hardy-Weinberg é muito importante pois sua ausência diz que a população pode sofrer mutação, migração ou seleção, adulterando os resultados das variações genéticas. Daí vem a importância prática de saber se a população está ou não nesse equilíbrio.

3. Construção do Modelo

Para a construção do modelo [2], consideremos as seguintes premissas:

1. Acasalamento aleatório;;
2. Gerações não-sobrepostas;
3. População infinita;
4. Espécies monoicas;
5. População sem migração e mutação;
6. População com seleção.

[1] OCONE (2014) traz detalhes técnicos para explicar a validade desta identidade.
[2] A construção desse modelo também é encontrada em Ocone (2014).

Também consideraremos que os acasalamentos ocorrem sazonalmente, ou seja, a geração t acasala para produzir a geração $t+1$ (depois não acasala mais por 2), assim, o próximo acasalamento só ocorrerá quando a geração $t+1$ for madura sexualmente para produzir a geração $t+2$, e assim por diante.

Para iniciarmos a modelagem, consideremos uma população com um locus e dois alelos, A e a. Definiremos dois tipos de frequências para uma mesma geração. Denotamos as frequências alélicas e genotípicas na geração t, no momento do nascimento, por $f_A(t)$ e $f_a(t)$ e $f_{AA}(t)$, $f_{Aa}(t)$ e $f_{aa}(t)$, respectivamente. Por exemplo, a frequência f_{AA} é a probabilidade de um indivíduo nascido na geração t possuir o genótipo AA.

O segundo grupo de frequências são aquelas que representam a geração t no momento da maturidade sexual, usaremos as notações $p_A(t)$ e $p_a(t)$ para as frequências alélicas e $p_{AA}(t)$, $p_{Aa}(t)$ e $p_{aa}(t)$ para as frequências genotípicas. Observemos que a frequência no momento da maturidade sexual depende da sobrevivência dos indivíduos. Assim, para o genótipo AA, por exemplo, segue que[3] $p_{AA}(t) = P(U_{AA}|S)$, onde U_{AA} é o evento do indivíduo nascido na geração t possuir genótipo AA, e S é o evento do indivíduo nascido na geração t sobreviver. A mesma derivação vale para $p_{Aa}(t)$ e $p_{aa}(t)$.

A premissa 6 diz que na população há presença de seleção e sabemos que ela ocorre quando os genótipos afetam a sobrevivência. Isso pode acontecer em duas situações: quando os genótipos possuem diferentes probabilidades de reprodução ou quando os genótipos possuem diferentes taxas de sobrevivência. Essas taxas de sobrevivência, ou coeficientes de seleção, serão denotadas por w_{AA}, w_{Aa} e w_{aa} e são iguais de geração em geração, ou seja, os coeficientes de seleção são independentes de indivíduo para indivíduo e independentes da geração. Para simplificarmos a compreensão, diremos que w_{AA} é a probabilidade de um indivíduo sobreviver visto que possui o genótipo AA, de forma análoga w_{Aa} para o genótipo Aa, e w_{aa} para o genótipo aa.

Nas próximas linhas aplicaremos o Teorema de Bayes, que será enunciado abaixo. Sua demonstração pode ser encontrada em Magalhães e Lima (2010).

Teorema 3.1 (Teorema de Bayes)**.** *Considere que os eventos A_1, A_2, ..., A_k formem uma partição do espaço amostral Ω e considere B um outro evento tal que $P(A_i)$ e $P(B|A_i)$, $i = 1, 2, \ldots, k$, sejam conhecidas. Para qualquer $j = 1, 2, \ldots, k$, tem-se*

$$P(A_j|B) = \frac{P(A_j \cap B)}{P(B)} = \frac{P(B|A_j) \cdot P(A_j)}{P(B)}$$

[3] $P(U_{AA}|S)$ equivale a probabilidade condicional do evento U_{AA} visto que o evento S ocorreu. Magalhães e Lima (2010) trazem uma abordagem mais completa sobre as probabilidade condicionais.

em que

$$P(B) = \sum_{i=1}^{k} P(A_i) \cdot P(B|A_i).$$

Por conseguinte, pelo Teorema de Bayes, tem-se:

$$p_{AA}(t) = \frac{P(S|U_{AA})P(U_{AA})}{P(S)}.$$

Além disso,

$$P(S) = P(S|U_{AA})P(U_{AA}) + P(S|U_{Aa})P(U_{Aa}) + P(S|U_{aa})P(U_{aa}) =$$

$$= w_{AA}f_{AA}(t) + w_{Aa}f_{Aa}(t) + w_{aa}f_{aa}(t),$$

de onde segue que

$$p_{AA}(t) = \frac{w_{AA}f_{AA}(t)}{w_{AA}f_{AA}(t) + w_{Aa}f_{Aa}(t) + w_{aa}f_{aa}(t)}. \tag{8}$$

O próximo objetivo é simplificar a equação (8) em função das frequências alélicas. Sabemos que a probabilidade de um pai da geração t, escolhido aleatoriamente, passar o alelo A para a prole é $p_A(t)$, e pela Proposição 2.2, segue que $p_A(t) = p_{AA}(t) + (1/2)p_{Aa}$. Consequentemente, pelas premissas 1 e 2, para todo $t \geq 0$, tem-se:

$$f_A(t+1) = p_A(t) \qquad \text{e} \qquad f_a(t+1) = (1 - p_A(t)), \tag{9}$$

e pelas equações (4), (5) e (6),

$$f_{AA}(t+1) = p_A^2(t), \quad f_{Aa}(t+1) = 2p_A(t)(1-p_A(t)) \quad \text{e } f_{aa}(t+1) = (1-p_A(t))^2. \tag{10}$$

Quando $t \geq 1$ as frequências acima estarão no equilíbrio de Hardy-Weinberg com

$$p = p_A(t-1) = f_A(t).$$

Portanto, substituindo (9) e (10) na Equação (8), temos:

$$p_{AA}(t) = \frac{w_{AA}f_A^2(t)}{w_{AA}f_A^2(t) + w_{Aa}2f_A(t)(1-f_A(t)) + w_{aa}(1-f_A(t))^2}, \tag{11}$$

similarmente,

$$p_{Aa}(t) = \frac{w_{Aa}2f_A(t)(1-f_A(t))}{w_{AA}f_A^2(t) + w_{Aa}2f_A(t)(1-f_A(t)) + w_{aa}(1-f_A(t))^2}. \tag{12}$$

Para completarmos o nosso objetivo usamos o fato de $f_A(t+1) = p_A(t) = p_{AA}(t) + (1/2)p_{Aa}(t)$ e somamos a Equação (11) com a metade da Equação (12) e finalmente obtemos:

$$f_A(t+1) = \frac{w_{AA}f_A^2(t) + w_{Aa}f_A(t)(1-f_A(t))}{w_{AA}f_A^2(t) + w_{Aa}2f_A(t)(1-f_A(t)) + w_{aa}(1-f_A(t))^2}. \tag{13}$$

Embora (13) seja válida apenas para todo $t \geq 1$, se assumirmos que a geração 0 está no equilíbrio de Hardy-Weinberg em sua infância, ou seja, que $f_{AA}(0) = f_A^2(0)$, $f_{Aa}(0) = 2f_A(0)(1-f_A(0))$ e $f_{aa}(0) = (1-f_A(0))^2$, então a Equação (13) também será válida para $t = 0$, e para prosseguirmos, assumiremos que isso ocorre, o que não afetará a análise qualitativa do limite de $f_A(t)$ quando t tende ao infinito.

Até então poderíamos considerar a Equação (13) como o modelo final, porém é conveniente simplificarmos a escrita com uma função chamada *função fitness*. Biologicamente, essa função avalia o quão adaptado está o indivíduo no ambiente em que vive e a tradução matemática é mostrada a seguir:

$$W(p) = p^2w_{AA} + 2p(1-p)w_{Aa} + (1-p)^2w_{aa}, \qquad \text{com } 0 \leq p \leq 1. \tag{14}$$

Portanto, para todo $t \geq 0$, aplicando (14) no modelo (13), obtemos a versão final, conforme segue abaixo.

$$f_A(t+1) = \frac{w_{AA}f_A^2(t) + w_{Aa}f_A(t)(1-f_A(t))}{W(f_A(t))}. \tag{15}$$

No início desta seção dissemos que a seleção ocorre em duas situações, porém o modelo foi construído tendo em vista que a seleção ocorre apenas quando genótipos possuem diferentes probabilidades de sobrevivência. Felizmente o modelo (15) pode ser generalizado para a outra situação, quando genótipos possuem diferentes probabilidades de reprodução. Para isso, é preciso apenas manter a premissa de acasalamentos aleatórios.

4. Análise do Modelo

Para a análise gráfica da equação (15) usaremos o método teia de aranha (*cobweb*), que pode ser analisado pelo leitor em Elaydi (2005).

Inicialmente, observemos que os coeficientes de seleção são estritamente positivos, visto que são probabilidades, consequentemente a função fitness também assume valores positivos, $W(p) > 0$. Para simplificarmos a notação do modelo, denotaremos $f_A(t)$ por $f(t)$ e definiremos a função $\phi(p)$ por

$$\phi(p) = \frac{p^2w_{AA} + p(1-p)w_{Aa}}{W(p)}, \qquad 0 \leq p \leq 1.$$

Assim fica mais fácil enxergar a equação (15) como uma equação de diferenças autônoma de primeira ordem na seguinte forma $f(t+1) = \phi(f(t))$. O primeiro passo para a aplicação da teia de aranha é calcular os pontos fixos da função ϕ. Com efeito, os pontos $p \in [0,1]$ que satisfazem $\phi(p) = p$ são:

$$p_1^* = 0, \qquad p_2^* = 1 \qquad \text{e} \qquad p_3^* = \frac{w_{Aa} - w_{aa}}{-w_{AA} + 2w_{Aa} - w_{aa}}.$$

Os dois primeiros pontos fixos possuem uma análise preliminar muito importante. Note que quando $p = 0$ o alelo A entrará em extinção, pois se isso ocorrer em alguma geração, as próximas gerações continuarão em abstinência de A pois não há mutação para mudar esse quadro. De modo semelhante veja que quando $p = 1$ o alelo a entrará em extinção.

Além disso, como p pertence ao intervalo $[0,1]$, para que p_3^* esteja entre 0 e 1 é necessário que ou $w_{Aa} > w_{aa}$ e $w_{Aa} > w_{AA}$ ou $w_{Aa} < w_{aa}$ e $w_{Aa} < w_{AA}$. De fato, quando o numerador e o denominador de p_3^* são positivos, segue que:

$$0 < \frac{w_{Aa} - w_{aa}}{2w_{Aa} - w_{AA} - w_{aa}} < 1 \Rightarrow \begin{cases} w_{Aa} - w_{aa} > 0 \Rightarrow w_{Aa} > w_{aa} \\ w_{Aa} - w_{aa} < 2w_{Aa} - w_{AA} - w_{aa} \Rightarrow w_{Aa} > w_{AA}, \end{cases}$$

e caso o numerador e o denominador de p_3^* sejam negativos, segue que:

$$0 < \frac{w_{Aa} - w_{aa}}{2w_{Aa} - w_{AA} - w_{aa}} < 1 \Rightarrow \begin{cases} w_{Aa} - w_{aa} < 0 \Rightarrow w_{Aa} < w_{aa} \\ w_{Aa} - w_{aa} > 2w_{Aa} - w_{AA} - w_{aa} \Rightarrow w_{Aa} < w_{AA}. \end{cases}$$

O segundo passo para aplicarmos a teia de aranha é encontrarmos a derivada de ϕ no ponto p. Com efeito,

$$\phi'(p) = \frac{p^2 w_{AA} w_{Aa} + 2p(1-p) w_{AA} w_{aa} + (1-p)^2 w_{Aa} w_{aa}}{W^2(p)}.$$

Agora, dividiremos nosso estudo em quatro casos, que são eles: dominância do alelo a, dominância do alelo A, dominância dos heterozigotos e dominância dos homozigotos.

- **Caso I: Dominância do Alelo** a

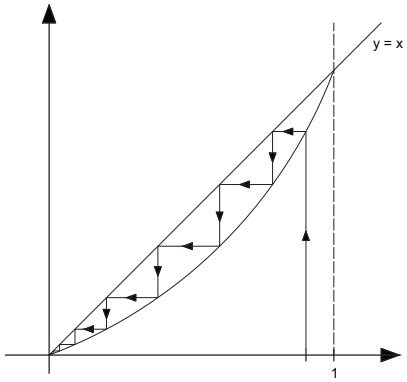
Para o primeiro caso consideremos que $w_{AA} < w_{Aa} < w_{aa}$. Veja que o ponto fixo p_3^* não está entre 0 e 1 e assim não faz parte do estudo, consequentemente teremos apenas dois pontos fixos de ϕ em $0 \leq p \leq 1$ que são $p_1^* = 0$ e $p_2^* = 1$. Podemos concluir que o gráfico da ϕ deve estar inteiramente acima ou inteiramente abaixo da reta diagonal $y = x$ no intervalo $0 < p < 1$.

A inclinação da reta tangente à função $y = \phi(p)$ em p_1^* é dada pela derivada da ϕ no ponto p_1^*, ou seja, $\phi'(0) = w_{Aa}/w_{aa}$. A hipótese inicial,

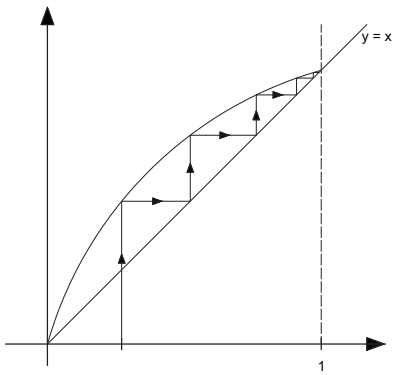
$w_{Aa} < w_{aa}$, implica que $\phi'(0) < 1$, consequentemente o gráfico da ϕ estará inteiramente abaixo da diagonal $y = x$, conforme mostra a Figura 2(a).

Aplicando o método da teia de aranha, conforme mostra a Figura 2(a), concluímos que $\lim_{t\to\infty} f(t) = 0$, o que significa que o alelo A entrará em extinção e o alelo a dominará o grupo de alelos.

Figura 2: Dominância dos alelos



[Dominância do alelo A]



[Dominância do alelo a]

FONTE: Os Autores (2018)

- **Caso II: Dominância do Alelo** A

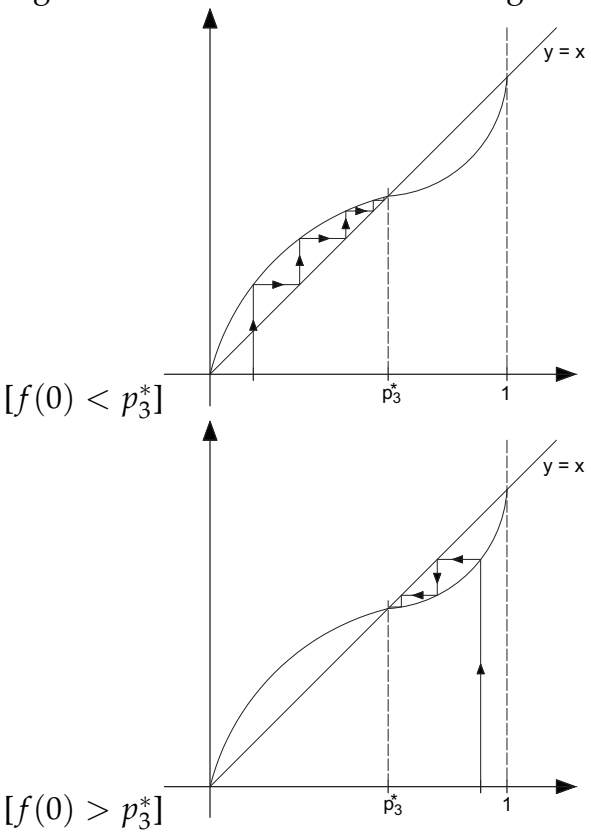
Para este caso consideremos que $w_{aa} < w_{Aa} < w_{AA}$. Novamente, o ponto fixo p_3^* não fará parte do estudo, então os pontos fixos da ϕ são p_1^* e p_2^*. Dessa vez, temos que $\phi'(0) > 1$, em virtude da hipótese. Consequentemente, o gráfico da ϕ estará inteiramente acima da diagonal $y = x$, conforme mostra a Figura 2(b).

Aplicando o método da teia de aranha para esse caso, conforme mostra a Figura 2(b), concluímos que $\lim_{t\to\infty} f(t) = 1$, o que significa que o alelo a entrará em extinção e o alelo A dominará o grupo de alelos.

- **Caso III: Dominância dos Heterozigotos**

Agora, consideremos $w_{Aa} > w_{AA}$ e $w_{Aa} > w_{aa}$. Veja que para esse caso os três pontos fixos da ϕ pertencem ao intervalo $[0,1]$. Porém, o gráfico da ϕ não estará inteiramente acima ou inteiramente abaixo da diagonal $y = x$, como foi garantido nos casos anteriores.

Figura 3: Dominância dos Heterozigotos



FONTE: Os Autores (2018)

Como $\phi'(0) > 1$, o gráfico da ϕ passará acima da diagonal $y = x$ no intervalo $0 < p < p_3^*$. Consequentemente, p_3^* será assintoticamente estável (Figura 3(a)) e pela análise de estabilidade (veja em ELAYDI (2005)) segue que $\phi'(p_3^*) < 1$, portanto o gráfico da ϕ manter-se-á abaixo da diagonal $y = x$ até chegar ao ponto fixo p_2^*. As Figuras 3(a) e 3(b) mostram essa ocorrência.

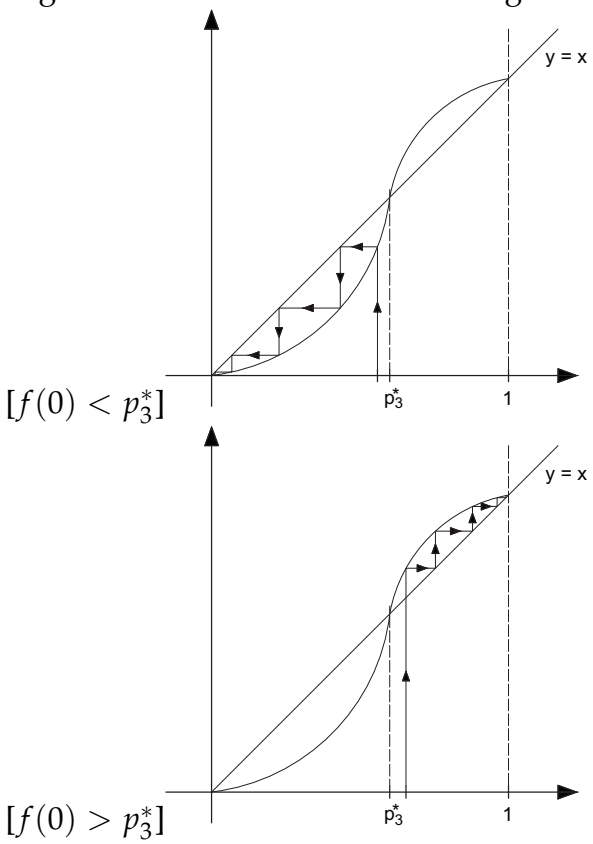
Aplicando a teia aranha, tanto para $f(0) < p_3^*$ (Figura 3(a)) ou para $f(0) > p_3^*$ (Figura 3(b)), segue que: $\lim_{t\to\infty} f(t) = p_3^*$, que implica a dominância dos heterozigotos, Aa.

- **Caso IV: Dominância dos Homozigotos**

Assumiremos para o último caso que $w_{Aa} < w_{AA}$ e $w_{Aa} < w_{aa}$ ocorrem, e como no Caso III, a função ϕ possui os três pontos fixos no intervalo $[0,1]$. Também de forma similar, veja que, como $\phi'(0) < 1$, o gráfico da ϕ estará abaixo da diagonal $y = x$ até o ponto fixo p_3^* e acima da diagonal $y = x$ a partir deste ponto.

Pela teia de aranha (Figura 4), segue que: $\lim_{t\to\infty} f(t) = 0$, quando $f(0) < p_3^*$ e $\lim_{t\to\infty} f(t) = 1$, quando $f(0) > p_3^*$.

Figura 4: Dominância dos Homozigotos



FONTE: Os Autores (2018)

Finalmente, este caso nos mostrou que $w_{Aa} < w_{Aa}$ e $w_{Aa} < w_{aa}$ acarretam a dominância dos homozigotos, AA e aa.

5. Considerações Finais

Levando em conta as numerosas aplicações da genética de populações e a relevância que elas exercem na sociedade, torna-se imprescindível a interdisciplinaridade entre as áreas da biologia e da matemática. Com este trabalho, através da construção do modelo matemático, foi possível perceber como essas ciências se relacionam harmonicamente.

Com o modelo construído vimos a grande utilidade da ferramenta teia de aranha. Mesmo nos deparando com uma equação de diferenças não linear, não foi necessário encontrar uma solução para obtermos conclusões a respeito das frequências no decorrer do tempo.

Embora os resultados obtidos nos quatro casos estudados pareçam óbvios, a análise do modelo fornece-nos também resultados quantitativos. No caso em que os heterozigotos dominaram foi possível observar qual é exatamente o valor do limite das frequências. Já no caso da dominância dos homozigotos pudemos encontrar a linha que divide as regiões de dominância dos alelos. Portanto, o modelo não nos promove apenas uma análise qualitativa dos seus resultados, por meio do método da teia de aranha, mas também nos direciona a valores exatos de dominância.

Por fim, observamos que este trabalho, embora não possua a análise de um modelo inédito, tem grande utilidade científica, principalmente por não existirem referências sobre o assunto no nosso idioma, podendo ser um agente fomentador para essa linha de pesquisa no país.

Referências

1. AMABIS, J. M; MARTHO, G. R. **Biologia das Populações**: Genética, Evolução e Ecologia. 1. ed. São Paulo: Editora Moderna, 1994.
2. BEIGUELMAN, B. **Genética de Populações Humanas**. Ribeirão Preto: SBG, 2008.
3. ELAYDI, S. **An Introduction to Difference Equations**. 3. ed. New York: Springer, 2005.
4. HARTL, D. L.; CLARK, A. G. **Principles of Population Genetics**. 4. ed. Sunderland: Sinauer Associates, 2007.
5. LEWIS, R. **Genética Humana**: Conceitos e Aplicações. 5. ed. Rio de Janeiro: Editora Guanabara Koogan S.A., 2004.
6. MAGALHÃES, M. N.; LIMA, A. C. P. **Noções de Probabilidade e Estatística**. 7. ed. São Paulo: Editora da Universidade de São Paulo, 2010.
7. OCONE, D. **Discrete and Probabilistic Models in Biology**. Apostila do Curso de Modelos Discretos e Probabilisticos na Biologia da Universidade de Rutgers, 2014.1, 3

Jornal Eletrônico de Ensino e Pesquisa de Matemática
(1s.) **v. 2** 2 (2018): 16–24. ©JEEPEMA–ISSN-2594-6323.
www.dma.uem.br/kit/jeepema

Algumas aplicações da aritmética à criptografia

D. Andrade (FEITEP)–Email:doherty200@hotmail.com

RESUMO: Neste trabalho apresentamos uma aplicação da teoria dos números à criptografia. Como veremos os números primos e a relação de congruência módulo inteiro desempenham um papel importante nesta área. Apresentaremos também alguns exemplos.

Sumário

1. Introdução

Atualmente os computadores com algoritmos sofisticados e processadores cada vez mais velozes criam rapidamente tabelas de números primos. Mas em passado recente tabelas eram elaboradas manualmente usando, por exemplo o crivo de Eratóstenes, como foi o caso da tabela publicada em 1914 por Derick Norman Lehemer que continha os números primos menores do que 10 milhões. Veja em [4].

Mesmo com esta facilidade computacional os números primos muito grandes resistem e a busca por eles e por um padrão em que aparecem (se existe) desafia os matemáticos. A utilização dos computadores nos trouxe a possibilidade de procurar números primos cada vez maiores, mas que utilidade tem o conhecimento de números primos cada vez maiores? A resposta é que

o conhecimento dos números primos muito grandes permite criptografar documentos e senhas. E isso não é pouco. Garantir a segurança e a integridade dos dados armazenados em um computador tornou-se atualmente vital para pessoas e companhias. Segurança e integridade de dados são coisas diferentes: segurança significa proteger os dados contra usuários não autorizadas e integridade significa proteger os dados contra usuários autorizados.

Um dos algoritmos atuais mais seguros de encriptação de informações, o algoritmo **RSA**, originou-se dos estudos de Ronald **R**ivest, Adi **S**hamir e Leonard **A**dleman, matemáticos que mudaram a história da Criptografia.

O princípio do algoritmo é construir, utilizando números primos, duas chaves: uma chave chamada de chave pública e outra chamada de chave privada. Uma chave é uma informação restrita que controla toda a operação dos algoritmos de criptografia. Inicialmente devem ser escolhidos dois números primos quaisquer e quanto maior os números escolhidos mais seguro será o algoritmo.

Antes de iniciar com os exemplos, vamos rever a relação de congruência módulo um inteiro $m > 1$. Seja $m > 1$ um inteiro fixado. Se x e y são inteiros, dizemos que x é congruente a y módulo m se $x - y$ é múltiplo de m. Isto é, se existe um inteiro k tal que $x - y = km$. Ou ainda, que m divide $x - y$. Representamos isso por $x \equiv y \mod m$ e lê-se: x é congruente a y módulo m. Observe que se x é congruente a y módulo m, então, quando divididos ambos por m, deixam o mesmo resto. De fato, suponha que $x = k_1m + r_1$ e $y = k_2m + r_2$, onde $0 \leq r_1, r_2 < m$. Calculando $x - y$ temos que:

$$x - y = (k_1 - k_2)m + (r_1 - r_2).$$

Como m divide $x - y$ e m divide $(k_1 - k_2)m$, então, m tem obrigatoriamente que dividir $(r_1 - r_2)$. Como $0 \leq r_1, r_2 < m$, então, $r_1 - r_2 = 0$ e, portanto, $r_1 = r_2$. Essa relação é uma relação de equivalência.

Usamos a notação $x \equiv y (\mod m)$ para representar que x e y são congruentes módulo m. Veja [1].

2. Algumas aplicações simples

2.1. **Código de César.** A aritmética módulo m é muito utilizada na criptografia. O exemplo mais simples (e muito antigo, remonta a Júlio César imperador romano). Veja [2]. Ele usava um método de escrita de mensagens secretas onde cada letra do alfabeto é associada a um número como na tabela abaixo e

depois transladava três casas mais à frente e tomava o módulo $m = 26$ (letras do alfabeto).

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Assim, no método de César define-se uma função $f(n) = (n + 3) \mod 26$ para encriptar uma mensagem, chamada de função encriptadora. Para desencriptar e recuperar a mensagem original utilizava a sua inversa $f^{-1}(n) = (n - 3) \mod 26$, chamada de função desencriptadora.

O método como apresentado acima é pouco seguro, já por volta de 1580 um sistema semelhante foi utilizado pela rainha Maria da Escócia, para conspirar junto com os espanhóis contra sua prima Isabel I. As mensagens de Maria foram facilmente decifradas culminando com a sua decapitação. Desde essa época os sistemas de codificação melhoraram muito. Veja [5].

Como vimos o método de César é pouco seguro e podemos melhorar definindo funções f mais gerais, como por exemplo, $f(n) = (an + b) \mod m$ com inteiros a e b de modo que f tenha inversa. Como por exemplo, a função $f(n) = (7n + 3) \mod 26$ como função encriptadora e, como função desencriptadora, $g(n) = (15n + 7) \mod 26$. Podemos criar um procedimento computacional para verificar o funcionamento desses funções. Veja abaixo um procedimento em Maple.

```
for k from 0 to 26 do
m[k] :=  mod(7*k+3, 26);
n[k] :=  mod (15*m[k]+7, 26);
od;
```

É bom registrar aqui que esta simplificação não leva em conta letras maiúsculas e minúsculas, acentos, espaços e outros caracteres. Há um método de conversão de caracteres ASCII, usado pela maioria dos computadores, está implementado no Maple^{R}. Vejamos um exemplo:

```
convert("Bom dia pessoal", bytes);
```

cujo resultado é

[66, 111, 109, 32, 100, 105, 97, 32, 112, 101, 115, 115, 111, 97, 108]

Para recuperar a expressão original:

```
convert([66, 111, 109, 32, 100, 105, 97, 32,
112, 101, 115, 115, 111, 97, 108], bytes);
```

2.2. **Geração de números aleatórios.** Muitas vezes a codificação de uma mensagem pode ser realizada por meio da geração aleatória de números. A geração de números aleatórios no computador não é de fato aleatório, por isso mesmo, são chamados muitas vezes de números pseudo-aleatórios. A variedade de métodos é grande, por exemplo, um dos métodos utiliza os movimentos do seu mouse armazenados nas últimas horas para gerar esses números. Mas o método mais comumente utilizado é o método das congruências lineares, descrito abaixo, que consiste em escolher 4 números inteiros positivos:

(i) um número m para a aritmética módulo m,

(ii) o multiplicador a,

(iii) o incremento c,

(iv) e a raiz x_0 satisfazendo $2 \leq a < m, 0 \leq c < m$ e $0 \leq x_0 < m$.

Em seguida, iniciando com x_0, gera-se uma sequência de números pseudo-aleatórios x_n com $0 \leq x_n < m$ para qualquer n, por meio da fórmula:

$$x_{n+1} = (ax_n + c) \pmod{m}, n \geq 0. \tag{1}$$

Como exemplo, escolhendo $m = 9, a = 7, c = 5, x_0 = 3$, obtemos de acordo com a equação 1 que:

$$\begin{aligned}
x_1 &= (7x_0 + 5) \mod 9 = 26 \pmod 9 = 8 \\
x_2 &= (7x_1 + 5) \mod 9 = 61 \pmod 9 = 7 \\
x_3 &= (7x_2 + 5) \mod 9 = 54 \pmod 9 = 0 \\
x_4 &= (7 \times 0 + 5) \mod 9 = 5 \pmod 9 = 5 \\
x_5 &= (7x_4 + 5) \mod 9 = 40 \pmod 9 = 4
\end{aligned}$$

Os valores obtidos acima e outros mais estão organizados na seguinte tabela:

n	0	1	2	3	4	5	6	8	8	9
x_n	3	8	7	0	5	4	6	2	1	3

Como $x_9 = x_0$, a sequência tem apenas 9 elementos diferentes, antes de começar a se repetir.

Novamente, podemos escrever facilmente um procedimento computacional para gerar números aleatórios como descrito acima. Apresentamos a seguir um procedimento em Maple que gera os números pseudo-aleatórios do exemplo acima.

```
m := 9; a := 7; c := 5; x[0] := 3;
for n from 0 to (m-1) do x[n+1] := modp(a*x[n]+c, m);od;
```

A maioria dos computadores utiliza este procedimento para gerar números aleatórios com o número de Mersenne $m = 2^{31} - 1$, com incremento $c = 0$ e multiplicador $a = 7^5$, o que permite gerar $2^{31} - 2$ números diferentes antes de iniciar a repetição. Veja [2].

3. Aplicação ao sistema de criptografia RSA

O sistema de criptografia **RSA**, iniciais de seus desenvolvedores **R**ivest, **S**hamir e **A**dleman surgiu em 1976. Atualmente o governo dos Estados Unidos da América detem a sua propriedade. Esse sistema é na verdade uma família de sistemas criptográficos diferentes se escolhermos os parâmetros diferentes, essa família é definida da seguinte forma:

(i) o espaço da mensagens: $\mathbb{Z}_n$, onde $n = p \times q$, com p, q números primos quaisquer.

(ii) $u(x) = x^a \pmod{n}$, para qualquer $x \in \mathbb{Z}_n$.

(iii) $v(y) = y^b \pmod{n}$, para qualquer $y \in \mathbb{Z}_n$,

onde a e b são tais que $a \times b \pmod{((p-1) \times (q-1))} = 1$.

As chaves u (pública) e a chave v (privada) devem satisfazer a duas propriedades para que o sistema seja seguro:

(i) $v(u(x)) = x$, para qualquer mensagem x.

(ii) Não deve ser possível obter x conhecendo-se $u(x)$ e não conhecendo $v(x)$. Note que resolver esta questão é um problema em aberto, com consequências importantes para a utilização da criptografia.

Consideremos ainda que $\text{MDC}(a, n) = 1$ e seja b a solução da congruência linear $ab \equiv 1 \pmod{n}$.

No sistema RSA, podemos começar por traduzir as mensagens (sequência de letras) em sequências de números inteiros. Por simplicidade e para ilustrar consideremos apenas as letras do alfabeto português:

A	B	C	D	E	F	G	H	I	J	L	M
00	01	02	03	04	05	06	07	08	09	10	11
N	O	P	Q	R	S	T	U	V	X	Z	
12	13	14	15	16	17	18	19	20	21	22	

O inteiro x resultante é então transformado, com a ajuda da chave pública, em um inteiro

$$u(x) \equiv x^a \pmod{n}.$$

Como exemplo tomemos $p = 43, q = 59$ e $a = 13$ e vamos codifique a palavra **GOLD**. Para as contas utilizamos o software Maple com o pacote numtheory.

Neste caso $n = 43 \times 59 = 2537$. Como $a = 13$ é primo, $\text{MDC}(3, 42 \times 58) = 1$. Codificando, obtemos

G	O	L	D
06	13	10	03

Logo, a mensagem corresponde é $x = 06131003$. Aplicando a chave pública u à mensagem x, obteremos uma mensagem codificada:

$$u(x) = (06131003)^{13} \pmod{2537} = 1868,$$

com apenas 4 dígitos. Para manter o mesmo número de dígitos, agrupamos em x os dígitos em blocos de 4 e depois aplicamos u a cada um dos blocos[1].

$$\begin{aligned} 0613 &\longrightarrow 0613^{13} \pmod{2537} = 1767 \\ 1003 &\longrightarrow 1003^{13} \pmod{2537} = 0885. \end{aligned}$$

[1] deve-se ter $x < n$.

A mensagem criptografada é 1767 0885.

Quando esta mensagem for recebida, o receptor a decodifica com a chave privada v que só ele conhece por meio de b:

$$x = v(u(x)) = u(x)^b \pmod{n}.$$

Assim, para determinar a chave privada b temos que resolver a congruência

$$13b \equiv 1 \pmod{2436}.$$

Resolvendo, obtemos $b = 937$.

Segue que $x_1 = 1767^{937} \pmod{2537} = 613 = 0613$ e $x_2 = 0885^{937} \pmod{2537} = 1003$, e, portanto, $x = x_1x_2 = 0613\ 1003$ que é a mensagem original **GOLD**.

Agora vamos ilustrar como resolver a congurência linear $13b \equiv 1 \pmod{2436}$ que utilizamos acima. É um exercício simples de máximo divisor comum entre dois inteiros positivos que recai nas equações Diofantinas.

Note que $13b \equiv 1 \pmod{2436} \Leftrightarrow 13b + 2436y = 1$, que é uma equação Diofantina. Como MDC(2436,13)=1, a congruência tem solução. Vamos determinar uma solução particular utilizando MDC(2436,13). Veja [1].

	187	2	1	1	2
2436	13	5	3	2	1
5	3	2	1	0	

Agora, reescrevendo o MDC, usando que

$$\begin{aligned} 2436 &= 13 \times 187 + 5 \\ 13 &= 5 \times 2 + 3 \\ 5 &= 3 \times 1 + 2 \\ 3 &= 2 \times 1 + 1. \end{aligned}$$

$$\begin{aligned} 1 &= 3 - 2 \times 1 \\ &= 3 - (5 - 3 \times 1) = 3 \times 2 - 5 \\ &= (13 - 5 \times 2) \times 2 - 5 = 13 \times 2 - 5 \times 5 \\ &= 13 \times 2 - (2436 - 13 \times 187) \times 5 = 13 \times 937 - 2436 \times 5. \end{aligned}$$

Segue que $b = 937$.

Resumindo, uma vez escolhidos os números primos P e Q, defina os números:

$$\begin{aligned} N &= P \times Q \\ Z &= (P-1) \times (Q-1). \end{aligned}$$

Agora escolha um número D que seja primo com relação ao número Z. De posse desses números começa o processo das chaves públicas e privadas. Para isto é necessário encontrar um número E que satisfaça à seguinte propriedade:

$$(E \times D) \pmod{Z} = 1.$$

Isto é, ED ao ser dividido por Z deixa resto igual a 1. Com esse processo definem-se as chaves de encriptação e desencriptação.

Para encriptar utilizamos E e N – esse par de números será utilizado como chave pública. Para desencriptar utilizamos D e N – esse par de números é utilizado como chave privada. As formas gerais são:

Texto Criptografado = ((Texto Original)^E) (mod N)
Texto Original = ((Texto Criptografado)^D) (mod N)

Mais um exemplo, tomemos $P = 17$e $Q = 13$ dois números primos. Assim, $N = PQ = 221$ e $Z = (P-1) \times (Q-1) = 192$. Em seguida, escolhemos o número $D = 7$ que é primo com relação a Z e o número $E = 55$ que é congruente a 1 módulo Z. Temos os seguintes resultados:

Encriptando	Desencriptando
Original =3	Criptografado = 198
Criptografado = (3^{55}) (mod 221)	Original = $((198)^7)$ (mod 221)
= (17444921100912017907117050 7) (mod 221)	= (11930436453209472) (mod 221)
Criptografado = 198	Original= 3

Como podemos ver, quanto maior os números escolhidos mais protegidos estarão os dados criptografados. A corrida por número primo muito grande já começou há algum tempo e não deve parar logo. Outros detalhes em [5].

Referências

1. MONTEIRO, L. H. Jacy, **Elementos de Álgebra**. LTC, 1978. 17, 22
2. ROSEN, Kenneth H., **Discrete Mathematics and its applications**. McGrill, 1995. 17, 20
3. ANDRADE, D. **Matemática Discreta: Notas de aula**. 2005.
4. Texto da internet. http://locomat.loria.fr/lehmer1914/lehmer1914doc.pdf. Acessado em julho/2016. 16
5. Texto da internet. http://www.dma.fi.upm.es/recursos/aplicaciones/matematica_discreta/web/aritmetica _modular/criptografia.html#1. Acessado em julho/2016. 18, 23

Jornal Eletrônico de Ensino e Pesquisa de Matemática
(1s.) **v. 2** 2 (2018): 25–51. ©JEEPEMA–ISSN-2594-6323.
www.dma.uem.br/kit/jeepema

Introdução à teoria dos Jogos

Doherty Andrade (FEITEP) & Thiago Zanko (UEM)

RESUMO: O presente texto tem por objetivo apresentar de forma sucinta os fundamentos elementares da teoria dos jogos e demonstrar o teorema de equilíbrio de Nash cuja demonstração utiliza o teorema do ponto fixo de Brouwer.

Sumário

1. Introdução

A teoria dos jogos é a teoria matemática que procura modelar fenômenos em que se pode observar conflito, isto é, quando dois ou mais agentes interagem com objetivos contrários. Assim, a teoria dos jogos pode ser definida como a teoria dos modelos matemáticos que estuda a escolha de decisões ótimas sob condições de conflito.

A origem da teoria do jogos pode ser situada no século XVIII, até onde se tem conhecimento, por meio de correspondências entre Nicolas Bernoulli e James Waldegrave, este último analisa um jogo e fornece uma solução no sentido que veremos mais adiante. No século XIX, Zermello e Borel, separadamente, publicaram diversos trabalhos sobre jogos. Borel achava que a guerra e a economia podiam ser estudadas por meio de jogos estratégicos.

Em 1928 o matemático John von Neumann demonstrou importantes resultados, em 1944, junto com o economista Oscar Morgenstern, publicou o livro "The theory of games and economic behaviour". O grande salto ocorreu em 1950 com John Forbes Nash Junior, em 1994, juntamente com outros receberam o prêmio Nobel por suas contribuições à teoria dos jogos.

Os primeiros registros de estudos de um jogo por estratégia mista datam de 1713 no estudo do jogo Le her (jogo de baralho com um deck de 52 cartas) realizado por James Waldegrave e descrito por ele em uma carta destinada a Pierre Rémond de Montmort. Em 1838, Augustin Cournot analisou um caso específico de duopólio e ele definiu conceito de equilíbrio de mercado como a situação em que ambas as empresas agem de forma ótima à decisão da empresa concorrente.

A Teoria dos Jogos só vai chamar a atenção das ciências sociais em 1944 (em plena Segunda Guerra Mundial) com o livro *Teoria dos Jogos e Comportamento econômico* de John Von Neumann e Oscar Morgenstern. Nessa obra, eles detalharam e especificaram a formulação de problemas econômicos e a aplicação da teoria dos jogos à economia

Para prosseguirmos com nossa explanação, voltemos a meados do século XVIII quando Adam Smith publica a obra *A Riqueza das Nações*. Considerado o pai do liberalismo e

um marco na economia, com uma burguesia emergente e à beira da revolução industrial, Adam Smith insere conceitos com *A Mão Invisível*, no qual ele afirma que existiria uma "mão invisível"que regula os mercados e seus agentes e estabelece uma determinada ordem originada da interação dos indivíduos. Independentemente de uma entidade coordenadora em comum. Ele afirmava ainda que se cada um fizesse o bem para si próprio, o estaria fazendo também para o coletivo. Em meados da década de 50, século XX, John Forbes Nash, prova a existência de um jogo cooperativo, ou seja, não há necessidade de sorte para jogá-lo, e afirma que você tem que fazer o bem para si próprio e para o coletivo simultaneamente. Por exemplo, o sonegador de impostos está se beneficiando com o valor que pagou a menos em tributos, mas prejudicou a construção de estradas, hospitais, ferrovias, ou seja, o seu coletivo. Ele prova então, que todo jogo possui um equilíbrio e ele é único, o que lhe renderia o Prêmio Nobel de economia de 1994. O trabalho de Nash foi um marco para a economia e para os conceitos matemáticos da Teoria dos Jogos da época, principalmente, porque era o período da Guerra Fria e buscava-se muito a compreensão da Teoria dos Jogos e como aplicá-la. Ele ainda formulou o problema da barganha e fez uma ampla contribuição para os jogos cooperativos e não cooperativos.

O tema de modelagem matemática em finanças é fascinante e possui aspectos interdisciplinares que relacionam algumas das principais contribuições científicas do século XX. Dentre elas, citamos como exemplo:

- A metodologia de Arrow-Debreu que está associada ao prêmio Nobel em Economia de Kenneth Arrow (1972) e o de Gerard Debreu (1983).

- A teoria de precificação por princípios de não-arbitragem e de cobertura de carteiras e que leva a equação de Black-Scholes. Esta última contribuição está associada ao prêmio Nobel de 1997 para Robert Merton e Myron Scholes também na área de Economia.

- A fórmula de Feynman-Kac que aqui novamente, temos uma referência ao célebre matemático aplicado Marc Kac em conexão com o físico Richard P. Feynman ganhador

do prêmio Nobel de Física de 1965.

Na próxima seção apresentamos a definição matemática de jogo e damos alguns exemplos.

2. Definição de jogo

Um jogo é uma terna (G, S, U), onde $G = \{g_1, g_2, \ldots, g_n\}$ denota um conjunto finito de jogadores g_i, S é o conjunto das estratégias de cada jogador $S = \{S_1, S_2, \ldots, S_n\}$ e $S_i = \{s_{i1}, s_{i2}, \ldots, s_{im_i}\}$ são opções de decisões do jogador g_i, denominadas de estratégias puras, e U é o conjunto das funções utilidades de cada jogador $U = \{u_1, u_2, \ldots, u_n\}$ em que cada u_i está definida por

$$\begin{aligned} u_i : \mathbf{S} &\to \mathbb{R} \\ \mathbf{s} &\mapsto u_i(\mathbf{s}) \end{aligned}$$

onde $\mathbf{S} = \prod_{i=1}^{n} S_i$ é o espaço das estratégias puras. Um elemento $\mathbf{s} \in \mathbf{S}$ é denominado um perfil de estratégias puras

$$\mathbf{s} = \{s_{1j_1}, s_{2j_2}, \ldots, s_{nj_n}\}.$$

Note que $u_i(\mathbf{s})$ associa a cada perfil de estratégias puras um ganho (*payoff*) do jogador g_i quando os jogadores utilizaram as suas estretégias puras apresentadas em $\mathbf{s}$.

3. Exemplos de jogos

Apresentamos a seguir alguns exemplos simples que ilustram os problemas tratados na teoria dos jogos.

• Exemplo 3.1 (Dilema do prisioneiro)

Este é um dos exemplos mais conhecidos, foi formulado por Albert W. Tucker em 1950.

Dois ladrões, Al e Bob, são capturados e acusados do mesmo crime. Presos em selas separadas e sem comunição entre si, o delegado faz a eles a seguinte proposta: cada um pode escolher entre confessar e negar o crime. Se nenhum deles confessar, então ambos

terão uma pena de um ano de prisão. Se os dois confessarem, então ambos terão pena de cinco anos. Mas se um confessar e o outro negar, então o que confessou será libertado e o outro será condenado a dez anos de prisão.

Neste exemplo, temos:

Jogadores	Estratégias
Al	S1={confessar, negar}
Bob	S2={confessar, negar}

O conjunto das estratégias **S** puras é o produto cartesiano $S1 \times S2$ das estratégias de cada um dos jogadores

$$\mathbf{S} = \{\text{(confessar, confessar), (confessar, negar), (negar, confessar), (negar, negar)}\}.$$

As duas funções utilidades são

$$\begin{array}{rccc} u_{Al}: & \mathbf{S} & \to & \mathbb{R}, \\ & (c,c) & \mapsto & -5 \\ & (c,n) & \mapsto & 0 \\ & (n,c) & \mapsto & -10 \\ & (n,n) & \mapsto & -1 \end{array} \qquad \begin{array}{rccc} u_{Bob}: & \mathbf{S} & \to & \mathbb{R} \\ & (c,c) & \mapsto & -5 \\ & (c,n) & \mapsto & -10 \\ & (n,c) & \mapsto & 0 \\ & (n,n) & \mapsto & -1 \end{array}$$

É usual representar os payoffs em uma tabela

		BOB: confessar	BOB: negar
AL	confessar	(-5,-5)	(0,-10)
	negar	(-10,0)	(-1,-1)

Vamos analisar este jogo do ponto de vista do Al. Duas situações podem ocorrer com relação ao Bob: confessa ou não confessa. Se Bob confessa, então é melhor Al confessar também. Se Bob não confessa, então Al ficará livre se confessar. Em qualquer caso, é melhor Al confessar.

Do mesmo modo, vamos alisar o jogo do ponto de vista de Bob. Duas situações podem ocorrer com relação ao Al: confessa ou não confessa. Se Al confessa, então é melhor Bob confessar também. Se Al não confessa, então Bob ficará livre se confessar. Em qualquer caso, é melhor Bob confessar.

Pensando assim, ambos ficarão presos por cinco anos.

• **Exemplo 3.2 (Guerra dos sexos)**

Um casal deseja sair para passear. O homem prefere assitir a um jogo de futebol enquanto a mulher prefere ir ao cinema. Ambos indo ao futebol ou ao cinema, apenas um deles terá maior satisfação; mas se sairem sozinhos então ambos ficarão igualmente insatisfeitos.

Esta situação se adequa ao um jogo estratégico em que o conjunto de jogadores é $G = \{\text{homem}, \text{mulher}\}$, as estratégias do homem $S_H = \{\text{futebol}, \text{cinema}\}$ e as estratégias da mulher $S_M = \{\text{futebol}, \text{cinema}\}$. Assim, o conjunto S das estratégias é

$$S = \{(\text{futebol}, \text{futebol}), (\text{futebol}, \text{cinema}), (\text{cinema}, \text{futebol}), (\text{cinema}, \text{cinema})\}.$$

As duas funções utilidade u_H e u_M estão descritas pela seguinte matriz dos payoffs

		Mulher	
		futebol	cinema
Homem	futebol	(10,5)	(0,0)
	cinema	(0,0)	(5,10)

• **Exemplo 3.3 (matching pennies)**

Neste jogo, dois jogadores exibem, ao mesmo tempo, a moeda que cada um esconde na sua mão. Se ambas apresentam cara ou coroa, o segundo jogador dá sua moeda ao primeiro jogador. Se ambos forem distintas, isto é, uma apresenta cara e o outro coroa, o primeiro jogador dá sua moeda ao segundo.

As duas funções utilidade estão descritas pela seguinte matriz dos payoffs

		g1	
		s_{21}	s_{22}
g2	s_{11}	(1,-1)	(-1,1)
	s_{12}	(-1,1)	(1,-1)

• **Exemplo 3.4 (Caso da perfuração dos poços de petróleo)**

As empresas XY e WZ ganham a licitação para a perfuração e exploração de um poço de petróleo P. Ambas devem iniciar suas atividades simultaneamente. Há duas opções de tubulação: a estreita, de custo de 1 (um) milhão de dólares e a larga ao custo de 5 (cinco) milhões de dólares. Ora, se XY e WZ acordarem em gastar menos, as duas instalam a tubulação estreita e extraem a mesma quantidade de petróleo. Mas se uma das duas decidirem colocar a tubulação larga para extrair mais petróleo e mais rápido, será beneficiada caso a outra mantenha a estreita. Mas se ambas tiverem o mesmo raciocínio, gastarão 5 (cinco) milhões e ao final vão extrair a mesma quantidade cada, mas com 4 (quatro) milhões de dólar a mais de custo.

As estratégias são:

$$S_{XY} \times S_{WZ} = \{\text{(estreita,estreita); (estrita,larga); (larga,estreita); (larga,larga)}\}.$$

A Matriz de payoffs é dada por:

		Perfuradora XY	
		larga	estreita
Perfuradora WZ	larga	(-5,-5)	(-5,-1)
	estreita	(-1,-5)	(-1,-1)

4. Dominância

Vamos denotar por $\mathbf{s}_{-i}$ um perfil de estratégia em que a estratégia do jogador g_i foi retirada, isto é,

$$\mathbf{s}_{-i} = \{s_{1j_1}, s_{2j_2}, \ldots, s_{(i-1)j_{i-1}}, s_{(i+1)j_{i+1}}, \ldots, s_{nj_n}\}\mathbf{S}_{-i}$$

e por $\mathbf{S}_{-i} = \mathbf{S}_1 \times \cdots \mathbf{S}_{i-1} \times \mathbf{S}_{i+1} \times \mathbf{S}_n$.

Deste modo, um perfil de estratégia pura pode ser convenientemente representado por $\mathbf{s} = (s_{ij}, \mathbf{s}_{-i})$.

Pelo par $(s_{ij_i}, \mathbf{s}_{-i})$ representamos

$$(s_{1j_1}, s_{2j_2}, \ldots, s_{(i-1)j_{i-1}}, s_{ij_i}, s_{(i+1)j_{i+1}}, \ldots, s_{nj_n}).$$

Dizemos que uma estratégia pura s_{ik} do jogador g_i é estritamente dominada pela estratégia $s_{ik'}$ se

$$u_i(s_{ik'}, \mathbf{s}_{-i}) > u_i(s_{ik}, \mathbf{s}_{-i}),$$

para todo $\mathbf{s}_{-i} \in \mathbf{S}_{-i}$.

A estratégia pura s_{ik} do jogador g_i é fracamente dominada pela estratégia $s_{ik'}$ se

$$u_i(s_{ik'}, \mathbf{s}_{-i}) \geq u_i(s_{ik}, \mathbf{s}_{-i}),$$

para todo $\mathbf{s}_{-i} \in \mathbf{S}_{-i}$.

Chamamos de dominância estrita iterada ao processo em que, sequencialmente, se eliminam as estratégias estritamente dominadas.

Uma solução estratégica ou equilíbrio de Nash de um jogo é um ponto onde cada jogador não tem incentivo de mudar sua estratégia se os demais jogadores não o fizerem. Em termos matemáticos, um perfil de estratégia pura

$$\mathbf{s}^* = (s_1^*, s_2^*, \ldots, s_{(i-1)}^*, s_i^*, s_{(i+1)}^*, \ldots, s_n^*) \in \mathbf{S}$$

é um equilíbrio de Nash se

$$u_i(s_i^*, \mathbf{s}_{-i}^*) \geq u_i(s_{ij_i}, \mathbf{s}_{-i}^*)$$

quando $i = 1, 2, \ldots, n$ e para todo $j_i = 1, 2, \ldots, m_i$, com $m_i \geq 2$.

No dilema dos prisioneiras, o perfil de estratégias (confessar, confessar) é um equilíbrio de Nash. Na batalha dos sexos, (futebol futebol) e(cinema, cinema) são únicos equilíbrios. No jogo de combinar moedas não há equilíbrio de Nash.

Uma alternativa para estes casos é considerar o jogo de ponto de vista probabilístico, isto é, ao invés de escolher um perfil de estratégia pura, o jogador deve escolher uma distribuição de probabilidades sobre suas estratégias puras.

Uma estratégia mista $\mathbf{p}_i$ para o jogador $g_i \in G$ é uma distribuição de probabilidades sobre o conjunto S_i de estratégias puras do jogador, isto é, $\mathbf{p}_i$ é um elemento do conjunto Δ_{m_i},

$$\Delta_{m_i} = \{(x_1, x_2, \ldots, x_{m_i}) \in \mathbb{R}^{m_i}; x_1, \geq 0, x_2, \geq 0, \ldots, x_{m_i} \geq 0 \text{ e } \sum_{k=1}^{m_i} x_k = 1\}.$$

Note que Δ_{m_i} é um conjunto compacto e convexo.

O espaço de todos os perfis de estratégia mista é o produto cartesiano

$$\Delta = \Delta_{m_1} \times \Delta_{m-2} \times \cdots \times \Delta_{m_n},$$

denominado de espaço de estratégia mista. Um vetor $\mathbf{p} \in \Delta$ é denominado de um perfil de estratégia mista.

Como no caso de estratégias puras, usamos a notação $\mathbf{p}_{-i}$ para representar as estratégias de todos os jogadores, com exceção do jogador g_i.

Note que Δ é compacto e convexo, pois é produto de compactos e convexos.

Cada perfil de estratégia mista $\mathbf{p} = (\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_n) \in \Delta$ determina um payoff esperado, uma média dos payoffs ponderada pelas distribuições de probabilidades $\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_n$. Mais precisamente,

$$\mathbf{p} = (\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_n) = (p_{11}, p_{12}, \ldots, p_{1n}; p_{21}, p_{22}, \ldots, p_{2n}; \ldots; p_{n1}, p_{n2}, \ldots, p_{nm_n})$$

então

$$u_i(\mathbf{p}) = \sum_{j_1=1}^{m_1} \sum_{j_2=1}^{m_2} \cdots \sum_{j_n=1}^{m_n} \left(\prod_{k=1}^{n} p_{kj_k} u_i(s_{1j_1}, s_{2j_2}, \ldots, s_{nj_n} \right).$$

Sejam $S_i^{(0)} = S_i$ e $\Delta_{m_i}^{(0)} = \Delta_{m_i}$. Defina recursivamente,

$$S_i^{(n)} = \{s \in S_i^{(n-1)}; \nexists \mathbf{p} \in \Delta_{m_i}^{(n-1)} \text{ tal que } \forall s_{-i} \in S_{-i}^{(n-1)}, u_i(\mathbf{p}, s_{-i} > u_i(s, s_{-i})\}$$

e

$$\Delta_{m_i}^{(n)} = \{p = (p_1, p_2, \ldots, p_{m_i}) \in \Delta_{m_i}; \forall k = 1, 2, \ldots, m_i, p_k > 0 \text{ somente se } s_{ik} \in S_i^{(n)}\},$$

onde $u_i(\mathbf{p}, s_{-i})$, por abuso de notação, representa o payoff esperado quando o jogador g_i escolhe a estratégia mista $\mathbf{p}$ e os demais jogadores escolhem as estratégias mistas correspondentes as estratégias puras dadas por s_{-i}. A interseção

$$S_i^{(\infty)} = \bigcap_{n=0}^{\infty} S_i^{(n)}$$

é o conjunto das estratégias puras e

$$\Delta_{m_i}^{(\infty)} = \{p \in \Delta_{m_i};\ \nexists \mathbf{p}' \in \Delta_{m_i} \text{talque } \forall s_{-i} \in S_{-i}^{(\infty)} u_i(\mathbf{p}', s_{-i}) > u_i(\mathbf{p}, s_{-i})\},$$

é o conjunto de todas as estratégias mistas do jogador g_i que sobreviveram a técnica da dominância estrita iterada.

Definição 4.1 (Equilíbrio de Nash) *Dizemos que um perfil de estratégia mista*

$$\boldsymbol{p}^* = (\boldsymbol{p}_1^*, \boldsymbol{p}_1^*, \ldots, \boldsymbol{p}_n^*) \in \Delta = \Delta_{m_i} \times \Delta_{m_2} \times \cdots \times \Delta_{m_n}$$

é um equilíbrio de Nash se

$$u_i(\boldsymbol{p}_i^*, \boldsymbol{p}_{-i}^*) \geq u_i(\boldsymbol{p}_i, \boldsymbol{p}_{-i}^*)$$

para todo $p_i \in \Delta_{m_i}$, isto é, nenhum jogador se sente motivação de trocar sua estratégia mista se os demais jogadores são o fizerem.

• **Exemplo 4.2**

No dilema do prisioneiro, o perfil de estratégia mista $\mathbf{p}^* = (1, 0; 1, 0)$ é um equilíbrio de Nash, pois

$$u_1(\mathbf{p}, \mathbf{p}^*) = u_1(p, 1-p; 1, 0) = 5p - 10 \leq u_1(1, 0; 1, 0) = u_1(p_1^*, p_2^*),$$

para todo $\mathbf{p} = (1-p, p) \in \Delta_2$ e

$$u_2(\mathbf{p}_1^*, \mathbf{q}) = u_1(1,0;q,1-q) = 5q - 10 \leq u_2(1,0;1,0) = u_2(p_1^*, p_2^*),$$

para todo $\mathbf{q} = (1-q, q) \in \Delta_2$.

Note que este equilíbrio corresponde ao equilíbrio em estratégias puras $\mathbf{s}^* =$ (confessar, confessar).

5. O teorema minimax de von Neumann

5.1. Jogo com 2 jogadores e de soma constante. Um jogo com dois jogadores, g_l chamado jogador linha (com m estratégias) e g_c chamado jogador coluna (com n estratégias) e matriz de payoffs dado por

		g_c			
		1	2	$\cdots$	n
g_l	1	(a_{11}, b_{11})	(a_{12}, b_{12})		(a_{1n}, b_{1n})
	2	(a_{21}, b_{21})	(a_{22}, b_{22})		(a_{2n}, b_{2n})
	$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$
	m	(a_{m1}, b_{m1})	(a_{m2}, b_{m2})		(a_{mn}, b_{mn})

satisfazendo $a_{ij} + b_{ij} = c$, para todo $i = 1, 2, \ldots, m$ e todo $j = 1, 2, \ldots, n$ é dito um jogo de soma constante. No caso em que $c = 0$ o jogo é dito de soma zero.

Note que, nesse caso, conhecendo-se a matriz dos payoffs do jogador g_1 também se conhece a matriz dos payoffs do jogador g_2, pois $b_{ij} = c - a_{ij}$.

Se A é a matriz dos payoffs do jogador g_1 e B é a matriz dos payoffs do jogador g_2, então $A + B = C$, a matriz com todas as entradas iguais a c.

Se $p = (p_1, p_2, \ldots, p_m) \in \Delta_m$ é uma distribuição de probabilidade para as estratégias puras do jogador linha e se $q = (q_1, q_2, \ldots, q_n) \in \Delta_n$ é uma distribuição de probabilidade

para as estratégias puras do jogador coluna, então o payoff esperado para o jogador linha é

$$u_l(\mathbf{p},\mathbf{q}) = \sum_{i=1}^{m}\sum_{j=1}^{n} p_i q_j a_{ij} = \left[\begin{array}{cccc} p_1 & p_2 & \cdots & p_m \end{array}\right] \left[\begin{array}{cccc} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \vdots & a_{mn} \end{array}\right] \left[\begin{array}{c} q_1 \\ q_2 \\ \vdots \\ q_n \end{array}\right] = \mathbf{p}^T A \mathbf{q}.$$

De modo análogo,

$$u_c(\mathbf{p},\mathbf{q}) = \mathbf{p}^T B \mathbf{q}.$$

Como o jogo tem soma constante,

$$A + B = [a_{ij} + b_{ij}] = [c] = c[1],$$

onde $[1]$ denota a matriz $m \times n$ formada com 1 em todas as suas entradas.

Notando que $u_l(p,q) = \sum\sum p_i q_j a_{ij} = p^T A q$ obtemos $u_c(p,q) = \sum\sum p_i q_j b_{ij} = p^T B q = p^T(C-A)q = c - u_l(p,q)$. Assim, temos:

Lema 5.1 $u_c(p,q) = c - u_l(p,q)$.

Lema 5.2 *Vale a seguinte propriedade*

$$u_l(\mathbf{p}^*,\mathbf{q}^*) \geq u_l(\mathbf{p},\mathbf{q}^*) \Leftrightarrow u_c(\mathbf{p}^*,\mathbf{q}^*) \leq u_c(p,\mathbf{q}^*).$$

Demonstração: Note que $u_c(\mathbf{p}^*,\mathbf{q}^*) = c - u_l(\mathbf{p}^*,\mathbf{q}^*) \leq c - u_l(\mathbf{p},\mathbf{q}^*) = u_c(\mathbf{p},\mathbf{q}^*)$.

Para a recíproca, $u_l(\mathbf{p}^*,\mathbf{q}^*) = c - u_c(\mathbf{p}^*,\mathbf{q}^*) \geq c - u_c(\mathbf{p},\mathbf{q}^*) = u_l(\mathbf{p},\mathbf{q}^*)$.

Isto conclui a demonstração. □

5.2. EQUILÍBRIO DE NASH EM ESTRATÉGIAS PURAS. Dizemos que a_{ij} da matriz A é um ponto de sela se ele for simultaneamente um mínimo em sua linha e um máximo em sua coluna. Isto é,

$$\begin{aligned} a_{ij} &\geq a_{il}, \forall l = 1,2,\ldots,n \\ a_{ij} &\geq a_{kj}, \forall k = 1,2,\ldots,m. \end{aligned}$$

Teorema 5.3 *O elemento a_{ij} é um elemento de sela de A se, e somente se, o par (i, j) é um equilíbrio de Nash em estratégias puras para o jogo.*

Demonstração: Suponha que o ponto a_{ij} seja um ponto de sela de A. Como a_{ij} é um máximo na coluna, tem-se

$$u_l(i, j) = a_{ij} \geq a_{kj} = u_l(k, j), \forall k = 1, 2, \ldots, m.$$

Isto é, o jogador linha não pode aumentar o seu payoff se o jogador coluna mantiver a estratégia.

Por outro lado, como a_{ij} é mínimo em sua linha, vale que

$$u_c(i, j) = b_{ij} = c - a_{ij} \geq c - a_{il} = b_{il} = u_c(i, l)$$

para todo $l = 1, 2, \ldots, n$. Isto é, o jogador coluna não pode aumentar o seu payoff se o jogador linha mantiver a estratégia.

Se (i, j) é um equilíbrio de Nash para o jogo, é fácil ver que a_{ij} é uma máximo em sua coluna e um mínimo em sua linha e portanto, é um ponto de sela. □

Teorema 5.4 *Se a_{ij} e a_{rs} são pontos de sela de A, então a_{is} e a_{rj} também são pontos de sela e além disso,*

$$a_{ij} = a_{rs} = a_{is} = a_{rj}.$$

Demonstração: Considere a matriz dos payoffs $A = [a_{ij}]$. Como a_{ij} e a_{rs} são selas segue que

$$a_{ij} \leq a_{is} \leq a_{rs}$$

e

$$a_{ij} \geq a_{rj} \geq a_{rs}.$$

Donde segue a igualdade e a conclusão. □

Notação: $\underline{a_k} = \min\limits_{1 \leq l \leq n} a_{kl}$, mínimo na linha k e $\overline{a_l} = \max\limits_{1 \leq k \leq m} a_{kl}$, máximo na coluna k. Assim, o payoff mínimo do jogador coluna, se escolher a coluna l, é dado por $c - \overline{a_l}$.

Defina

$$\begin{aligned} v_l(A) &= \max_{1\leq k\leq m} \underline{a_k} = \max_{1\leq k\leq m} \min_{1\leq l\leq n} a_{kl} \\ v_c(A) &= \min_{1\leq l\leq n} \overline{a_l} = \min_{1\leq l\leq n} \max_{1\leq k\leq m} a_{kl}. \end{aligned}$$

Teorema 5.5 *Vale sempre a desigualdade* $v_c(A) \geq v_l(A)$.

Demonstração: É claro que $a_{kj} \geq \min_{1\leq l\leq n} a_{kl}, \forall k = 1, \ldots, m \ \forall l = 1, \ldots, n$. Tomando o máximo em k nessa expressão temos $\max_{1\leq k\leq m} a_{kj} \geq \max_{1\leq k\leq m} \min_{1\leq l\leq n} a_{kl} = v_l(A), \forall j$.

Agora tomando o mínimo em j, $\min_{1\leq j\leq n} \max_{1\leq k\leq m} a_{kj} \geq v_l(A), \forall j$, isto é, $v_c(A) \geq v_l(A)$. □

Teorema 5.6 *Uma matriz A tem ponto de sela, se e somente se,* $v_l(A) = v_c(A)$.

Demonstração: Suponha que a_{ij} seja ponto de sela da matriz A. Então, $a_{ij} = \min_{1\leq l\leq n} a_{il} = \underline{a_i}$. como $v_l(A) = \max_{1\leq k\leq m} \underline{a_k}$ segue que$v_l(a) \geq \underline{a_i} = a_{ij}$.

Po outro lado, $a_{ij} = \max_{a\leq k\leq m} a_{kj} = \overline{a_j}$ e como $v_c(A) = \min -1 \leq l \leq n\overline{a_l}$ segue que

$$v_c(A) \leq \overline{a_j} \leq a_{ij}.$$

Combinando, obtemos que $v_l(A) \geq v_c(A)$. Do teorema anterior, segue a igualdade.

Suponha que exista linha i tal que $v_l(A) = \underline{a_i}$. Mas como $\underline{a_i} = \min_{1\leq s\leq n} a_{is}$, existe coluna l tal que $\underline{a_i} = a_{il}$. Assim, $v_l(A) = \underline{a_i} = a_{il}$.

Do mesmo modo, $v_c(A) = a_{kj}$ para algum k e algum i.

Como $v_l(A) = v_c(A)$ temos que $a_{il} = a_{kj}$ donde segue que a_{ij} é ponto de sela. □

Assim, em um jogo de dois jogadores e com soma constante dado por uma matriz de payoffs A do jogador linha tem um equilíbrio de nash em estratégias puras se, e somente se, $v_l(A) = v_c(A)$.

6. Equilíbrio de Nash em estratégias mistas

Definimos as seguintes funções

$$v_l(A) = \max_{p\in\Delta_m}\min_{q\in\Delta_n} \mathbf{p}^T A\mathbf{q} \text{ e } v_c(A) = \min_{q\in\Delta_n}\max_{p\in\Delta_m} \mathbf{p}^T A\mathbf{q}.$$

Como no caso de estratégias puras, tem-se:

Teorema 6.1 *Vale sempre a desigualdade* $v_c(A) \geq v_l(A)$.

Demonstração: Temos que para todo $\mathbf{p} \in \Delta_m$,

$$\mathbf{p}^T A\mathbf{q} \geq \min_{\mathbf{y}\in\Delta_m} \mathbf{p}^T A\mathbf{y}.$$

Assim,

$$\max_{\mathbf{p}\in\Delta_m} \mathbf{p}^T A\mathbf{q} \geq \max_{\mathbf{p}\in\Delta_m}\min_{\mathbf{y}\in\Delta_m} \mathbf{p}^T A\mathbf{y} = v_l(A).$$

Consequentemente,

$$v_c(A) = \min_{\mathbf{q}\in\Delta_n}\max_{\mathbf{p}\in\Delta_m} \mathbf{p}^T A\mathbf{q} \geq \max_{\mathbf{p}\in\Delta_m}\min_{\mathbf{y}\in\Delta_m} \mathbf{p}^T A\mathbf{y} = v_l(A).$$

Isto completa a demonstração. □

O resultado a seguir, é um teorema que caracteriza a existência de equilíbrios de Nash em estratégias mistas em termos de v_l e v_c.

Teorema 6.2 *Um perfil de estratégias mistas* $(\mathbf{p}^*, \mathbf{q}^*)$ *é um equilíbrio de Nash de um jogo com dois jogadoes e com soma constante definido pela matriz de payoffs do jogador linha se, e somente se, tem-se* $v_l(A) = v_c(A) = \mathbf{p}^{*T} A\mathbf{q}^*$.

Demonstração: Se $(\mathbf{p}^*, \mathbf{q}^*)$ é um equilíbrio de Nash, então

$$\mathbf{p}^{*T} A\mathbf{q}^* = u_l(\mathbf{p}^*, \mathbf{q}^*) \geq u_l(\mathbf{p}, \mathbf{q}^*) = \mathbf{p}^T A\mathbf{q}^*,$$

para todo $\mathbf{p} \in \Delta_m$. Em particular,

$$\mathbf{p}^{*T} A\mathbf{q} = \max_{\mathbf{p}\in\Delta_m} \mathbf{p}^T A\mathbf{q}^* \geq \min_{y\in\Delta_n} \max_{p\in\Delta_m} \mathbf{p}^T A\mathbf{y} = v_c(A).$$

Vale também que

$$\mathbf{p}^{*T} A\mathbf{q} = c - u_c(\mathbf{p}^*, \mathbf{q}^*) \leq c - u_c(\mathbf{p}^*, \mathbf{q}) = \mathbf{p}^{*T} A\mathbf{q}$$

para todo $\mathbf{q} \in \Delta_n$. Em particular,

$$\mathbf{p}^{*T} A\mathbf{q}^* = \min_{\mathbf{q}\in\Delta_n} \mathbf{p}^{*T} A\mathbf{q} = v_l(A).$$

Assim, obtemos que $v_l(A) \geq v_c(A)$. Agora a igualdade segue do teorema.

Agora suponha que $v_l(A) = \max_{\mathbf{p}\in\Delta_m} \min_{\mathbf{q}\in\Delta_m} \mathbf{p}^T A\mathbf{q}$, então existe $\mathbf{p}^* \in \Delta_m$ tal que $v_l(A) = \min_{\mathbf{q}\in\Delta_n} \mathbf{p}^{*T} A\mathbf{q}$.

Analogamente, como $v_c(A) = \min_{\mathbf{q}\in\Delta_n} \max_{\mathbf{p}\in\Delta_m} \mathbf{p}^T A\mathbf{q}$, então existe $\mathbf{q}^* \in \Delta_n$ tal que $v_c(A) = \max_{\mathbf{p}\in\Delta_m} \mathbf{p}^T A\mathbf{q}^*$.

Como por hipótese, $v_c(A) = v_l(A)$, temos que

$$\min_{\mathbf{q}\in\Delta_m} \mathbf{p}^{*T} A\mathbf{q} = v_l(A) = v_c(A) = \max_{\mathbf{p}\in\Delta_m} \mathbf{p}^T A\mathbf{q}^*.$$

Afirmamos que $(\mathbf{p}^*, \mathbf{q}^*)$ é um equilíbrio de Nash do jogo. Com efeito,

$$u_l(\mathbf{p}^*, \mathbf{q}^*) = \mathbf{p}^{*T} A\mathbf{q}^* \geq \min_{\mathbf{q}\in\Delta_n} \mathbf{p}^{*T} A\mathbf{q} = \max_{\mathbf{p}\in\Delta_m} \mathbf{p}^T A\mathbf{q}^* \geq \mathbf{x}^T A\mathbf{q}^* = u_l(\mathbf{x}^T, \mathbf{q}^*)$$

para todo $\mathbf{x} \in \Delta_m$. Por outro lado,

$$u_c(\mathbf{p}^*, \mathbf{q}^*) = c - \mathbf{p}^{*T} A\mathbf{q}^* \geq c - \max_{\mathbf{p}\in\Delta_m} \mathbf{p}^T A\mathbf{q}^* = c - \min_{\mathbf{q}\in\Delta_n} \mathbf{p}^{*T} A\mathbf{q} \geq c - \mathbf{x}^{*T} A\mathbf{y} = u_c(\mathbf{p}^*, \mathbf{y})$$

para todo $\mathbf{y} \in \Delta_n$.

Deste modo,$(\mathbf{p}^*, \mathbf{q}^*)$ é um equilíbrio de Nash do jogo. □

7. O teorema minimax de von Neumann

O próximo teorema estabelece que, para jogos de dois jogadores e com soma zero, sempre $v_l(A) = v_c(A)$. Sendo assim, pelo teorema 6.2, para esta classe de jogos, existe sempre ao menos um equilíbrio de Nash em estratégias mistas. Além disso, o teorema a seguir dá um método para determinar o equilíbrio de Nash.

Teorema 7.1 (MiniMax de von Neumann) *Para todo jogo de soma zero com dois jogadores, representado pela matriz de payoffs de A do jogador linha, sempre existe um perfil de estratégia mista $(\mathbf{p}^*, \mathbf{q}^*) \in \Delta_m \times \Delta_n$ satisfazendo*

$$v_l(A) = \max_{\mathbf{p}\in\Delta_m} \min_{\mathbf{q}\in\Delta_n} \mathbf{p}^T A\mathbf{q} = \mathbf{p}^{*T} A\mathbf{q}^* = \min_{\mathbf{q}\in\Delta_n} \max_{\mathbf{p}\in\Delta_m} \mathbf{p}^T A\mathbf{q} = v_c(A).$$

Em particular, $(\mathbf{p}^*, \mathbf{q}^*)$ é um equilíbrio de Nash do jogo.

A demonstração deste resultado que apresentamos a seguir utiliza um importante resultado da programação linear, o teorema da dualidade.

Dado um problema de programação linear, chamado de primal,

$$\text{(primal)} \begin{cases} \text{Maximizar } b^T y \\ \text{sujeito a } Ay \leq c, \\ y \geq 0 \end{cases}$$

o seu dual é dado por

$$\text{(dual)} \begin{cases} \text{Minimizar } c^T x \\ \text{sujeito a } x^T A \geq b^T, . \\ x \geq 0 \end{cases}$$

Teorema 7.2 (dualidade) *O problema primal possui solução se, e somente se, o problema dual possui solução. Além disso, se y^* é solução do problema primal e x^* é solução do problema dual, então ambos os problemas possuem o mesmo valor ótimo, isto é, $c^T x^* = b^T y^*$.*

Demonstração: (Teorema 7.1)A demonstração consiste em introduzir os seguintes problemas de programação linear, onde $c = (1, 1, \ldots, 1)^T$ e $b = (1, 1, \ldots, 1)^T$ e

$$(\text{primal}) \begin{cases} \text{Maximizar } b^T y \\ \text{sujeito a } Ay \leq c, \\ y \geq 0 \end{cases}$$

o seu dual é dado por

$$(\text{dual}) \begin{cases} \text{Minimizar } c^T x \\ \text{sujeito a } x^T A \geq b^T, . \\ x \geq 0 \end{cases}$$

O problema dual tem solução $x^* \neq 0$ e o primal tem solução $y^* \neq 0$. Como $c^T x^* = b^T y^*$, definimos

$$\Theta = c^T x^* = b^T y^* > 0.$$

Note que $\Theta > 0$, pois $(0, 0, \ldots, 0)$ não é admissível.

Tome

$$\mathbf{p}^* = \frac{x^*}{\Theta} \text{ e } \mathbf{q}^* = \frac{y^*}{\Theta}.$$

Afirmamos que $\mathbf{p}^{*T} A \mathbf{q}^* = \Theta^{-1}$.

De fato,

$$\begin{aligned} \mathbf{x}^{*T} A &\geq b^T \Rightarrow \mathbf{x}^{*T} A y^* \geq b^T y^* = \Theta \\ A y^* &\leq c \Rightarrow \mathbf{x}^{*T} A y^* \leq c^T x^* = \Theta. \end{aligned}$$

Segue que $\mathbf{x}^{*T} A \mathbf{y}^* = \Theta$. Dividindo por Θ^2, obtemos

$$\left(\frac{\mathbf{x}^{*T}}{\Theta} \right) A \left(\frac{\mathbf{y}^*}{\Theta} \right) = \Theta^{-1}.$$

Isto é, $\mathbf{p}^{*T} A \mathbf{q}^* = \Theta^{-1}$.

Agora vamos provar que $(\mathbf{p}^*, \mathbf{q}^*)$ é um equilíbrio de Nash.

Notemos que $\mathbf{p}^* \in \Delta_m$ e que $\mathbf{q}^* \in \Delta_n$, pois são não negativos e

$$\sum p_i = \sum \frac{x_i^*}{\Theta} = \frac{c^T x^*}{\Theta} = \frac{\Theta}{\Theta} = 1$$

$$\sum q_j = \sum \frac{y_j^*}{\Theta} = \frac{b^T y^*}{\Theta} = \frac{\Theta}{\Theta} = 1.$$

Como ${\mathbf{x}^*}^T A \geq b^T$ (dual) obtemos ${\mathbf{x}^*}^T Aq \geq b^T q = 1$, para todo $q \in \Delta_n$. Logo,

$$\Theta {\mathbf{p}^*}^T Aq \geq 1 \Rightarrow {\mathbf{p}^*}^T Aq \geq \Theta^{-1} = {\mathbf{p}^*}^T A\mathbf{q}^*.$$

Como $A\mathbf{y}^* \leq c$ (primal) obtemos $\mathbf{p}^T A\mathbf{q}^* \geq \mathbf{p}^T c = 1$, para todo $\mathbf{p} \in \Delta_m$. Logo,

$$\Theta \mathbf{p}^T A\,(\mathbf{q}^*\Theta) \leq 1 \Rightarrow \mathbf{p}^T A\mathbf{q}^* \leq \Theta^{-1}.$$

Donde obtemos que

$$u_l(\mathbf{p}^*, \mathbf{q}^*) = {\mathbf{p}^*}^T A\mathbf{q}^* \geq \mathbf{p}^T A\mathbf{q}^* = u_l(p, \mathbf{q}^*),$$

assim, o jogador linha não pode aumentar o seu payoff esperado trocando $\mathbf{p}^*$ por $\mathbf{p}$ se o jogador coluna não mudar a sua estratégia.

Por outro lado, como o jogo é de soma zero

$$u_c(\mathbf{p}^*, \mathbf{q}^*) = -u_l(\mathbf{p}^*, \mathbf{q}^*) \geq -u_l(\mathbf{p}^*, \mathbf{q}) = u_c(\mathbf{p}^*, \mathbf{q}),$$

assim o jogador coluna não aumenta o seu payoff quando troca $\mathbf{q}^*$ por $\mathbf{q}$ se o jogador linha mantiver $\mathbf{p}^*$.

Logo,$(\mathbf{p}^*, \mathbf{q}^*)$ é um equilíbrio de Nash. □

• **Exemplo 7.3 (Vacinação)**

O governo deseja vacinar seus cidadãos contra um certo tipo de virus da gripe. Este virus possui dois sorotipos, sendo que é desconhecida a proporção na qual os dois sorotipos ocorrem na população di virus. Foram desenvolvidos duas vacinas em que a eficácia da

vacina 1 é 85% contra o sorotipo I e de 70% contra o sorotipo II. A eficácia da vacina 2 é de 60% contra o sorotipo I ede 90% contra o sorotipo II. Que política de vacinação deveria ser tomada pelo governo?

A situação pode ser modelada como um jogo de soma zero com dois jogadores, o nde o jogador linha, que é o governo, deseja fazer a compensação (a fração dos cidadãos resistentes ao virus) o maior possível e o jogador coluna (o virus) deseja fazer a compensação a menor possível. A matriz dos payoffs é a seguinte:

Virus

Governo		Sorotipo I	Sorotipo II
	Vacina I	$(0.85, -0.85)$	$(0.70, -0.70)$
	Vacina II	$(0.60, -0.60)$	$(0.90, -0.90)$

Para encontrar um equilíbrio de Nash, devemos resolver os seguintes problemas de programação linear (primal)

$$\begin{aligned} &\text{Maximizar } (y_1 + y_2) \\ \text{sujeito a } &\begin{bmatrix} 0.85 & 0.70 \\ 0.60 & 0.90 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \leq \begin{bmatrix} 1 \\ 1 \end{bmatrix} \\ &y_1 \geq 0 \\ &y_2 \geq 0 \end{aligned}$$

e o seguintes problema de programação linear (dual)

$$\begin{aligned} &\text{Minimizar } (x_1 + x_2) \\ \text{sujeito a } &\begin{bmatrix} x_1 & x_2 \end{bmatrix} \begin{bmatrix} 0.85 & 0.70 \\ 0.60 & 0.90 \end{bmatrix} \geq \begin{bmatrix} 1 & 1 \end{bmatrix} \end{aligned}$$

$$x_1 \geq 0$$
$$x_2 \geq 0$$

A solução do problema primal é dada por
$y^* = (\frac{40}{69}, \frac{50}{69})$
e a solução do problema dual é
$x^* = (\frac{20}{23}, \frac{10}{23})$.

Segue que $\theta = y_1^* + y_2^* = x_1^* + x_2^* = \frac{30}{23}$. Deste modo, o único equilíbrio de Nash para o problema é da pelo ponto (p^*, q^*), onde $p^* = \frac{x^*}{\theta} = (\frac{2}{3}, \frac{1}{3})$ e $q^* = \frac{y^*}{\theta} = (\frac{4}{9}, \frac{5}{9})$.

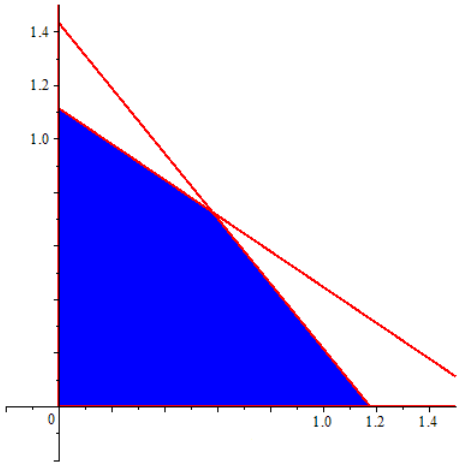


Figura 1: ppl- primal

8. O Teorema de Equilíbrio de Nash

Na seção anterior provamos o teorema minimax de von Neumann que dá a existência de um equilíbrio de Nash para jogos de soma zero com dois jogadores. Mas este resultado é geral: todo jogo definido por uma matriz de payoffs possui um equilíbrio de Nash em estratégias mistas.

A demonstração do Teorema de Equilíbrio de Nash utiliza o teorema do ponto fixo de Brouwer.

Teorema 8.1 (Brouwer) *Seja $\Delta \subset \mathbb{R}^n$ um compacto convexo e $F : \Delta \to \Delta$ contínua. Então, F possui um ponto fixo $\mathbf{p}^* \in \Delta$, isto é, $F(\mathbf{p}^*) = \mathbf{p}^*$.*

Definimos para cada $i = 1, ..., n$ e $j = 1, ..., m_i$ a função

$$\begin{aligned} z_{ij} : \Delta &\to \mathbb{R} \\ p &\mapsto z_{ij}(p) = u_i(s_{ij}, p_{-i}) - u_i(p_i, p_{-i}), \end{aligned}$$

que mede o ganho ou perda do jogador g_i quando ele troca a distribuição de probabilidade p_i pela estratégia pura s_{ij}.

Teorema 8.2 *Seja $p^* \in \Delta$. Temos que p^* é um equilíbrio de Nash se, e somente se, $z_{ij}(p) \leq 0$, para cada $i = 1, ..., n$ e $j = 1, ..., m_i$.*

Demonstração: Seja $p^* = (p_i^*, p_{-i}^*)$ um equilíbrio de Nash, então $u_i(p_i^*, p_{-i}^*) \geq u_i(s_{ij}, p_{-i}^*)$, para cada $i = 1, ..., n$ e $j = 1, ..., m_i$. Consequentemente,

$$z_{ij}(p^*) = u_i(s_{ij}, p_{-i}^*) - u_i(p_i^*, p_{-i}^*) \leq 0,$$

para cada $i = 1, ..., n$ e $j = 1, ..., m_i$.

Reciprocamente, se $z_{ij}(p^*) \geq 0$ para cada $i = 1, ..., n$ e $j = 1, ..., m_i$, então

$$u_i(e_j, p_{-i}^*) = u_i(s_{ij}, p_{-i}^*) \leq u_i(p_i^*, p_{-i}^*),$$

para cada $i = 1, ..., n$ e $j = 1, ..., m_i$.

Devemos mostrar que para todo $p_i \in \Delta_{m_i}$, tem-se

$$u_i(p_i, p_{-i}^*) \leq u_i(p_i^*, p_{-i}^*).$$

Como $x \mapsto u_i(x, p_i^*)$ é um funcional linear, temos que

$$\begin{aligned} u_i(p_i, p^*_{-i}) &= u_i\left(\sum_{k=1}^{m_i} p_{ik} \cdot e_k, p^*_{-i}\right) = \sum_{k=1}^{m_i} p_{ik} \cdot u_i(e_k, p^*_{-i}) \\ &\leq \sum_{k=1}^{m_i} p_{ik} \cdot u_i(p^*_i, p^*_{-i}) = u_i(p^*_i, p^*_{-i}) \cdot \sum_{k=1}^{m_i} p_{ik}, \end{aligned}$$

onde, na última igualdade, usamos o fato de que $\sum_{k=1}^{m_i} p_{ik} = 1$, dado que $p_i \in \Delta_{m_i}$. □

Para cada $i = 1, ..., n$ e $j = 1, ..., m_i$, definimos a função

$$\begin{aligned} g_{ij} : \Delta &\to \mathbb{R} \\ p &\mapsto g_{ij}(p) = \max\{0, z_{ij}(p)\} \end{aligned}$$

Corolário 8.3 *Seja $p^* \in \Delta$. Temos que p^* é um equilíbrio de Nash se, e somente se, $g_{ij}(p*) = 0$, para cada $i = 1, ..., n$ e $j = 1, ..., m_i$.*

Definimos a aplicação

$$\begin{aligned} F : \Delta = \Delta_{m_1} \times ... \times \Delta_{m_n} &\to \Delta = \Delta_{m_1} \times ... \times \Delta_{m_n} \\ p = (p_1, ..., p_n) &\mapsto F(p) = (y_1(p), ..., y_n(p)), \end{aligned}$$

onde $p_i = (p_{i1}, ..., p_{im_i})$, $y_i(p) = (y_{i1}(p), ..., y_{im_i}(p))$ e

$$y_{ij}(p) = \frac{p_{ij} + g_{ij}(p)}{1 + \sum_{k=1}^{m_i} g_{ik}(p)}.$$

8.1. A demonstração.

Teorema 8.4 *Seja $p^* \in \Delta$. Temos que p^* é um equilíbrio de Nash se, e somente se, $F(p^*) = p^*$.*

Demonstração: Observemos que $y_i(p) \in \Delta_{m_i}$, para todo $i = 1, ..., n$. De fato, claramente $y_{ij} \geq 0$ para todo $i = 1, ..., n$ e $j = 1, ..., m_i$. Para todo $p \in \Delta$, tem-se

$$\begin{aligned}\sum_{k=1}^{m_i} y_{ik}(p) &= \sum_{k=1}^{m_i}\left(\frac{p_{ik}+g_{ik}(p)}{1+\sum_{k=1}^{m_i} g_{ik}(p)}\right) = \frac{\sum_{k=1}^{m_i} p_{ik}+\sum_{k=1}^{m_i} g_{ik}(p)}{1+\sum_{k=1}^{m_i} g_{ik}(p)} \\ &= \frac{1+\sum_{k=1}^{m_i} g_{ik}(p)}{1+\sum_{k=1}^{m_i} g_{ik}(p)} = 1,\end{aligned}$$

ou seja, mostramos que $F(\Delta) \subset \Delta$.

Seja p^* um equilíbrio de Nash, então $g_{ij}(p^*) = 0$ para cada $i = 1, ..., n$ e $j = 1, ..., m_i$. Deste modo, $y_{ij}(p^*) = p^*$ para cada $i = 1, ..., n$ e $j = 1, ..., m_i$, isto é, $y_i(p^*) = p_i^*$ para cada $i = 1, ..., n$, ou ainda, $F(p^*) = p^*$.

Reciprocamente, se $p^* \in \Delta$ é um ponto fixo do operador $F : \Delta \to \Delta$, isto é,

$$p_{ij}^* = \frac{p_{ij}^* + g_{ij}(p^*)}{1+\sum_{k=1}^{m_i} g_{ik}(p^*)},$$

para todo $i = 1, ..., n$ e $j = 1, ..., m_i$. Segue que

$$g_{ij}(p^*) = p_{ij}^* \sum_{k=1}^{m_i} g_{ik}(p^*). \tag{1}$$

Definimos $\alpha = \sum_{k=1}^{m_i} g_{ik}(p^*)$ para cada $i = 1, ..., n$ e $j = 1, ..., m_i$. Queremos mostrar que $\alpha = 0$, de modo que $g_{ik}(p^*) = 0$ para todo $i = 1, ..., n$ e $k = 1, ..., m_i$. Suponhamos, por absurdo, que $\alpha > 0$, vemos por (1) que

$$g_{ij}(p^*) > 0 \quad \Leftrightarrow \quad p_{ij}^* > 0.$$

Sem perda de generalidade suponhamos que para algum $0 < l < m_i$, tem-se $p_{i1}^* > 0, ...p_{il}^* > 0$ e $p_{i(l+1)}^* = ... = p_{im_i}^* = 0$. Observemos que

$$p_i^* = \sum_{k=1}^{m_i} p_{ik}^* e_k,$$

onde e_i é o i-ésimo vetor da base canônica de $\mathbb{R}^{m_i}$. Como $g_{ik}(p^*) > 0$ para $k = 1, ..., l$, temos $0 < g_{ik}(p^*) = z_{ik}(p^*)$, ou seja

$$u_i(p_i^*, p_{-i}^*) < u_i(e_i, p_{-i}^*),$$

para todo $k = 1, ..., l$. Desta maneira, temos

$$\begin{aligned} u_i(p_i^*, p_{-i}^*) &= u_i\left(\sum_{k=1}^{m_i} p_{ik}^*, p_{-i}^*\right) = \sum_{k=1}^{m_i} p_{ik}^* \cdot u_i(e_i, p_{-i}^*) > \sum_{k=1}^{m_i} p_{ik}^* \cdot u_i(p_i^*, p_{-i}^*) \\ &= u_i(p_i^*, p_{-i}^*) \cdot \sum_{k=1}^{m_i} p_{ik}^* = u_i(p_i^*, p_{-i}^*), \end{aligned}$$

um absurdo. Isto demonstra que $g_{ij}(p^*) = 0$, para todo $i = 1, ..., n$ e $j = 1, ..., m_i$ e, assim pelo corolário 8.3, p^* é um equilíbrio de Nash em estratégias mistas. □

Teorema 8.5 (equilíbrio de Nash) *Todo jogo definido por matrizes de payoffs possui um equilíbrio de Nash.*

Demonstração: A aplicação $F : \Delta \to \Delta$ é contínua e Δ é um conjunto compacto e convexo. Pelo teorema do ponto fixo de Brouwer, F possui um ponto fixo p^*. Pelo Teorema 8.4, p^* é um equilíbrio de Nash. □

O corolário 8.3 acima apresenta também um método para calacular os equilíbrios de Nash de um jogo. Eles são as soluções do seguinte problema de otimização não-linear:

$$\begin{aligned} \text{minimizar} \quad & \sum_{i=1}^{n} \sum_{j=1}^{m_i} \left(g_{ij}(p)\right)^2 \\ \text{sujeito a} \quad & p \in \Delta. \end{aligned}$$

De fato, a soma dos quadrados é zero se, e somente se, cada parcela é nula.

No caso do dilema do prisioneiro $(\mathbf{p}, \mathbf{q}) = (p, 1-p; q, 1-q) \in \Delta_2 \times \Delta_2$ é um equilíbrio de Nash se, e somente se, (p, q) é solução do seguinte problema

$$\text{Minimizar } G(p,q) = (\max\{0, -(-1+p)(4q+1)\})^2 + (\max\{0, -p(4q+1)\})^2 +$$

$$+(\max\{0, -(4p+1)(-1+q)\})^2 + (\max\{0, -q(4p+1)\})^2$$

sujeito a $0 \leq p \leq 1, \quad 0 \leq q \leq 1$.

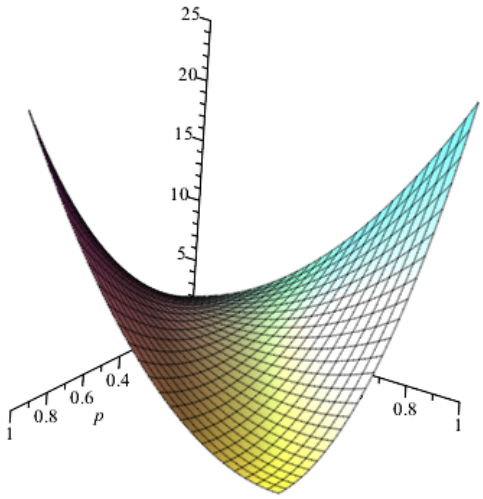


Figura 2: superfície para o dilema dos prisioneiros

Sabemos que $(\mathbf{p},\mathbf{q}) = (1,0;1,0)$ é o único equilíbrio de Nash para o dilema dos prisioneiros . A figura 2 mostra a superfície.

No caso do jogo a batalha dos sexos, devemos maximizar a função

$$(\max\{0,5\ (-1+p)\,(3\,q-1)\})^2+(\max\{0,-5\,p\,(3\,q-1)\})^2+(\max\{0,-5\ (3\,p-2)\,(-1+q)\})^2+$$

$$+(\max\{0,-5\,q\,(3\,p-2)\})^2$$

Sabemos que $(\mathbf{p},\mathbf{q}) = (1,0;1,0)$ ou $(0,1;0,1)$ ou $(\frac{2}{3},\frac{1}{3};\frac{1}{3};\frac{2}{3})$ são os únicos equilíbrios de Nash para a batalha dos sexos. A figura 3 mostra a superfície.

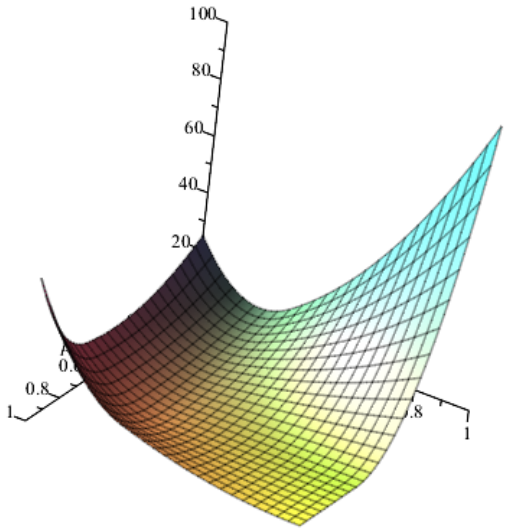


Figura 3: superfície para a batalha dos sexos

Referências

1. Max Oliveira de Souza e Jorge Zubelli .Modelagem matemática em finanças quantitativas em tempo discreto. Notas de Matemática aplicada, 2007.

2. D. Andrade et.al. Introdução à teoria dos Jogos. Notas de Minicurso na XXII semana de Matemática da UEM. 2011.

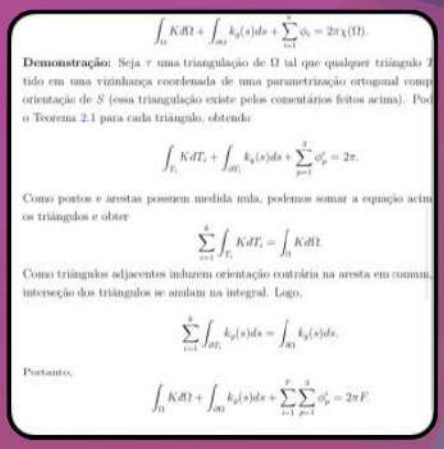
3. H. Bortolossi, G. Garbugio, Brigida Sartini. Uma introdução à teoria do jogos. 26^0 colóquio Brasileiro de Matemática, 2007.

4. Avner Friedman, Foundations of Modern Analysis. Holt, Reinehart and Winston, Inc., 1970.

5. S. Kesavan, Topics in Functional Analysis and Applications. Bangalores, John Wiley and Sons, 1988.

UEM Universidade Estadual de Maringá

Cálculo Diferencial e Integral:
um kit de sobrevivência



$$\int_\Omega K d\Omega + \int_{\partial\Omega} k_g(s)ds + \sum_{i=1}^{k} \phi_i = 2\pi\chi(\Omega).$$

Demonstração: Seja τ uma triangulação de Ω tal que qualquer triângulo T tido em uma vizinhança coordenada de uma parametrização ortogonal comp orientação de S (essa triangulação existe pelos comentários feitos acima). Poc o Teorema 2.1 para cada triângulo, obtendo

$$\int_{T_i} K dT_i + \int_{\partial T_i} k_g(s)ds + \sum_{p=1}^{3} \phi_p^i = 2\pi.$$

Como pontos e arestas possuem medida nula, podemos somar a equação acim os triângulos e obter

$$\sum_{i=1}^{k} \int_{T_i} K dT_i = \int_\Omega K d\Omega.$$

Como triângulos adjacentes induzem orientação contrária na aresta em comum, interseção dos triângulos se anulam na integral. Logo,

$$\sum_{i=1}^{k} \int_{\partial T_i} k_g(s)ds = \int_{\partial\Omega} k_g(s)ds.$$

Portanto,

$$\int_\Omega K d\Omega + \int_{\partial\Omega} k_g(s)ds + \sum_{i=1}^{k}\sum_{p=1}^{3} \phi_p^i = 2\pi F.$$

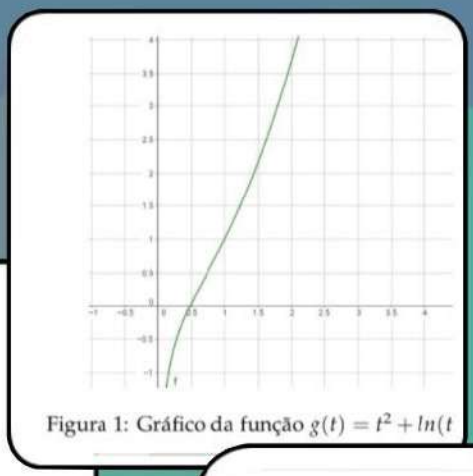
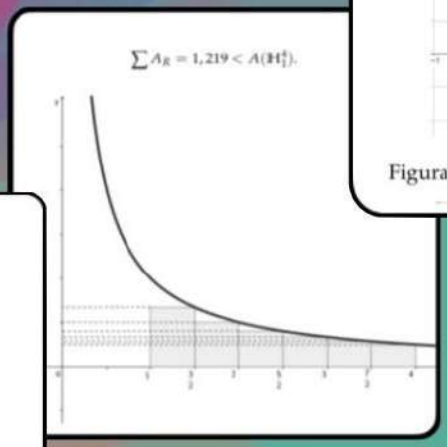


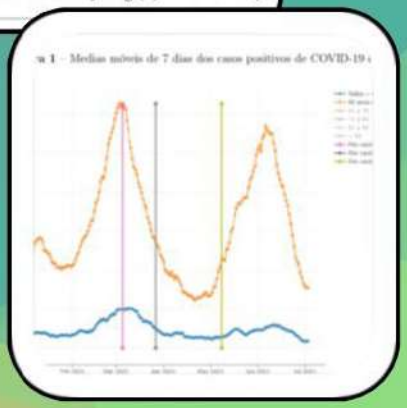
Figura 1: Gráfico da função $g(t) = t^2 + ln(t$



$$\sum A_R = 1,219 < A(\mathbb{H}^4_1).$$

O volume da esfera

Figura 8: Cone com área da base igual a πr^2 e altura $4r$.



Esta revista é responsável pela formulação de textos autorais desenvolvido pelo projeto de extensão "Kit". Neste projeto, contamos com alunos graduandos e demais interessados em matemática aplicada.
Entre seus textos, podemos encontrar, curiosidades, resoluções, demonstrações , fatos relevantes , ideais para IC, entre outros!