Matemática Discreta

J. P. S. de Sousa

Contents

Chapter 1

Fundamentos

1.1 Introdução

1.1.1 O que é Matmética Discreta

A definição de Matmática Discreta é difícil de se obter, sendo comum dizer que é mais fácil a definir pelo que está fora dela do que de fato está incluso nela. Ela estuda uma coleção ampla e heterogênea de objetos, e que dialoga com diversas outras áreas, muito pelo fato dela lidar, entre outras coisas, com princípios fundamentais da matemática, como a contagem.

Numa tentiva de definir o conceito, podemos dizer que a Matemática Discreta não é um campo da matemática, mas sim a parte dela cujo foco está nas estruturas algébricas nas quais não há continuidade entre seus elementos. Seus objetos de estudo são estruturas, conjuntos e funções que lidam com elementos distintos e separados, tais como números inteiros, grafos e fórmulas lógicas.

1.1.2 Áreas da Matemática Discreta

Neste texto, iremos explorar alguns campos que são estudados, primariamente, sob luz da Matmética Discreta. Todos os campos compartilham a propriedade fundamental de estarem lidando com objetos como conjunto e funções discretas, implicando que eles podem ser distinguidos um dos outros, enumerados, ordenados e contados.

Combinatória

A combinatória, também chamada de Análise Combinatória em contextos mais elementares, estuda modos de contar, selecionar, combinar ou ordenar elementos de um conjunto finito sem necessariamente listar todas as possibilidades. Por sua vez, a combinatória pode ser dividida em alguns campos mais especializados, como:

- Enumerativa - busca contar o números de elementos de um conjunto que satisfazem uma determinada propriedade. É a área mais elementar da combinatória, sendo também chamada de contagem.
- Extremal - busca determinar o quão grande ou pequena uma coleção de elementos pode ser caso tenha que satisfazer determinadas restrições. Também estuda

como selecionar objetos que satisfaçam uma condição de extremalidade ou otimiladade. Surge em problemas combinatórios relacionados a otimização.

- Algébrica - um campo que visa empregar métodos da Álgebra Abstrata, especialmente da Teoria de Grupos e da Representação, em contextos combinatórios, enquanto que, ao mesmo tempo, emprega métodos combinatórios para manipular objetos de uma estrutura algébrica.
- Probabilística - um campo com maior grau de especialização introduzido por Paul Erdös que estuda o emprego de métodos probablísticos para demonstrar a existência de um determinado objeto combinatório. Em essência, busca-se provar que, ao selecionar aleatoriamente um objeto em dado universo, a probabilidade de que o objeto escolhido satisfaça uma propriedade desejada é estritamente maior do que zero.

Relações de Recorrência

As relações de recorrência são fórmulas que definem termos de uma sequência em função de termos anteriores. A relação de recorrência mais famosa é com certeza a Sequência de Fibonacci; nela, o termo base é $a_0 = 0$, e a fórmula de recorrência é dada por $a_n = a_{n-1} + a_{n-2}$, ou seja, um termos é definido como a soma dos outros dois imediatamente anteriores. Também é comum denotar recorrências como funções dos índices dos termos da sequeência, que no mesmo exemplo dado seria $f(0) = 0$ e $f(n) = f(n-1) + f(n-2)$.

As recorrências surgem naturalmente em diversos problemas que envolvem objetos discretos, de modo que a solução do problema torna-se resolver a recorrência, isto é, achar uma fórmula não recursiva – também chamada de fórmula fechada – em termos do próprio índice para obter qualquer termo da sequência, sem precisar computar os anteriores na ordem.

Teoria dos Grafos

A Teoria dos Grafos é um grande ramo da Matemática Discreta que lida com conjuntos de objetos que estão relacionados entre si. Os objetos de um grafo são representados por pontos, enquanto que as relações entre eles são denotados por setas ou segmentos de retas, a depender do tipo da relação sendo representada.

O estudo dos grafos gera ferramentas poderosas para a modelagem de diversos problemas, que passam a poder ser solucionados por algoritmos que resolvem questões como conectividade, caminhos mínimos, fluxos, emparelhamentos e colorações. Dessa forma, problemas oriundos de áreas como ciência da computação, engenharia, logística, biologia, redes sociais e economia podem ser formalizados de maneira precisa e analisados sistematicamente por meio dessas estruturas.

1.1.3 Notação

A seguir, serão apresentados, em grande parte, os símbolos e seus respectivos significados que virão ser usados no texto. Muitas delas terão seu significado melhor explicado quando for oportuno.

$\mathbb{N}$ – Conjunto dos Naturais, incluindo o 0.

$\mathbb{Z}$ – Conjunto dos Inteiros.

$\mathbb{R}$ – Conjunto dos Reais.

$\{x \in U \mid P(x)\}$ – Conjunto dos elementos em U que satisfazem a propriedade $P(x)$.

$[n]$ – conjunto dos naturais menores ou iguais a n.

$[n]^*$ – conjunto dos naturais não nulos menores ou iguais a n.

$\mathscr{P}(A)$ – conjunto das partes de A.

$[x]_R$ – classe de equivalência x na relação R.

$\vee$ – operador lógico de conjunção (ou).

$\wedge$ – operador lógico de disjunção (e).

$p \to q$ – se p, então q.

$p \implies q$ – p implica q.

$p \leftrightarrow q$ – p se, e somente se, q.

$p \iff q$ – p equivale a q.

$\forall$ – para todo.

$\exists$ – existe.

$!\exists$ – existe um único.

$(a_1, \ldots, a_n)$ – tupla ou sequência finita de n elementos.

$(a_1, a_2, \ldots)$ – sequência infinita.

1.2 Teoria de Conjuntos

Nesta seção, abordaremos alguns conceitos principais da Teoria de Conjuntos, mais precisamente da sua versão axiomática dada pela teoria de Zermelo-Fraenkel acrescido do Axioma da Escolha (ZFC). Não nos prenderemos muitos aos detalhes e demonstrações formais dos resultados da teoria, pois nossa intenção é apresentar as ideias que estarão permeando os capítulos futuros do texto.

Passaremos rapidamente pelos Axiomas de ZFC, apresentando-os conforme a necessidade de abordar uma forma especial de definir conjuntos, operações e outros objetos de interesse. Em seguida, apresentamos os conceitos de relação e função. Adiante, discutiremos o tópico dos números ordinais e cardinais, que formalizam os conceitos fundamentais de ordenação e quantidade tratados em Matemática Discreta. Por fim, daremos uma definição satisfatória para um dos principais objetos manipulados neste material: os conjuntos discretos.

1.2.1 Definindo Conjuntos

A ZFC é uma teoria de primeira ordem, o que significa que suas fórmulas [1] lógicas quantificam e afirmam a respeito de objetos individuais, chamados de conjuntos. Conjuntos é uma ideia primitiva que representa uma coleção de objetos que podem também ser partes de outras coleções.

Entre conjuntos, persiste uma relação binária fundamental chamada de pertinência, denotada por $\in$. Desse modo, se $a \in A$, então dizemos que a é elemento – ou membro – de A, ou que a pertence a A. A igualdade de conjuntos é definida pelo **Axioma da Extensão**, que determina que dois conjuntos são iguais quando possuem os mesmos elementos, não importando a ordem ou as multiplicidades deles.

$$A = B \iff \forall x \, (x \in A \leftrightarrow x \in B)$$

[1] Fórmulas são qualquer sequência de símbolos que possuem um significado em uma teoria

Por essa razão, diz-se que a identidade de um conjunto é definida inteiramente por seus elementos. Em especial, o conjunto x que satisfaz a fórmula

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

é chamado de conjunto vazio, sendo denotado por $\varnothing$. Do Axioma da Extensão, segue que esse conjunto é único.

A partir da relação fundamental de pertinência, podemos definir outra chamada de "inclusão", denotada por $\subset$. Dizemos que A inclui um conjunto B caso todo elemento de B seja um elemento de A. Da mesma forma, podemos dizer que B é incluído por A, o que B é subconjunto de A.

$$B \subset A \iff \forall x\ (x \in B \to x \in A)$$

Se a relação vale nas duas direções, então A e B são iguais pelo Axioma da Extensão. A definição de inclusão implica também que o vazio e o próprio A são subconjuntos de A, de modo que subconjuntos diferentes desses últimos são chamados de subconjuntos próprios.

O **Axioma da Separação** nos oferece uma forma conveniente de definir subconjuntos de um conjunto por meio de uma propriedade. Se A é um conjunto, então podemos definir um subconjunto $S \subseteq A$ cujos elementos satisfazem uma propriedade $P(x)$. Denotaremos essa maneira de definir conjuntos como

$$S = \{x \in A \mid P(x)\}$$

Perceba que, na verdade, esse axioma trata-se de um esquema, pois ele é enunciado para cada uma das infinitas propriedades $P(x)$[2]

Para facilitar representação de conjuntos, muitas vezes iremos construir o conjunto S omitindo o superconjunto A. Logo, dada a propriedade $P(x)$, diremos simplesmente que S será o conjunto de todos os indivíduos que satisfazem ela.

$$S = \{x \mid P(x)\}$$

Esse modo de definição é chamado de "por abstração".

1.2.2 Operações com Conjuntos

Entre conjuntos, podemos definir algumas operações básicas usando os axiomas anteriores. Com o Axioma da Separação, definimos a interseção I de conjuntos A e B, que possui membros em comum desses dois últimos

$$I = \{x \in A \mid x \in A \land x \in B\}$$

Representaremos a interseção dos membros de um conjunto $\mathscr{F}$ como

$$\bigcap_{A \in \mathscr{F}} A$$

[2]Como mencionado, a ZFC é uma teoria de primeira ordem, não sendo capaz de enunciar fórmulas que quantifiquem outras fórmulas. Com isso, cada propriedade $P(x)$ necessita do seu próprio axioma.

Se a interseção de A e B for vazia, então dizemos que são disjuntos. Quando os elementos de um conjunto $\mathscr{F}$ forem todos disjuntos entre si, diremos que $\mathscr{F}$ é disjunto.

Com o Axioma da Separação também definimos a operação de diferença entre A e B, que resulta no conjunto de todos os membros do primeiro que não são membros do segundo.

$$D = A \setminus B \iff D = \{x \in A \mid x \notin B\}$$

Por fim, a operação de união entre A e B resulta no conjunto que possui tantos os membros de A quanto de B como elementos. No entanto, diferente das duas operações anteriores, o resultado não é subconjunto de um dos operandos, o que impede a utilização do Axioma da Separação e torna necessário a introdução de um novo axioma que garanta a existência da união. O **Axioma da União** enuncia que se $\mathscr{F}$ é um conjunto, então existe um conjunto U que reúne os membros dos membros de $\mathscr{F}$. Representaremos esse conjunto como

$$U = \bigcup_{A \in \mathscr{F}} A$$

Em particular, se $\mathscr{F} = A, B$, é comum escrever simplesmente que $U = A \cup B$.

$$U = A \cup B \iff \forall x,\ (x \in U \leftrightarrow x \in A \vee x \in B)$$

1.2.3 Conjuntos das Partes e Partições

O **Axioma da Potência** garante, para todo conjunto A, a existência do conjunto das partes de A, denotado por $\mathscr{P}(A)$, que reúne todos os subconjuntos de A como membros.

$$\forall A \exists \mathscr{P} \forall S,\ (S \subset A \to S \in \mathscr{P})$$

Usaremos a notação $\mathscr{P}^*(A)$ para denotar $\mathscr{P}(A) \setminus \varnothing$.

No conjunto das partes, há subconjuntos especiais que são chamados de partições. Se $P \subset \mathscr{P}^*(A)$ é um conjunto que satisfaz

$$\forall x, y \in P (x \cap y = \varnothing) \quad \text{e} \quad A = \bigcup_{x \in P} x$$

chamamos P de uma partição para o conjunto A.

1.2.4 Produto Cartesiano

O **Axioma do Par** enuncia que, dados conjuntos A e B, podemos construir um novo conjunto $C = \{A, B\}$. Esse axioma, em conjunto dos anteriores, torna a definição de Kuratowski para pares ordenados – uma coleção de dois objetos em que a ordem importa – satisfatória:

$$(a, b) = \{a, \{a, b\}\},$$

pois dela pode ser demonstrado que

$$(a, b) = (c, d) \iff a = c \wedge b = d$$

Exposto isso, definiremos a operação de produto cartesiano de dois conjuntos A e B, denotada por $A \times B$, como o conjunto de todos os pares ordenados (a, b) tal que que $a \in A$ e $b \in B$. É possível mostrar que esse conjunto existe agrumentando que

$$A \times B \subset \mathscr{P}(\mathscr{P}(A \cup B))$$

1.2.5 Outros Axiomas de ZFC

Dando sequência, aparesentaremos os demais axiomas da ZFC. O Axioma da Regularidade afirma que todo conjunto não vazio é disjunto com pelo menos um de seus elementos. Esse axioma impede a construção de uma série conjuntos que introduziriam paradoxos na Teoria de Conjuntos, a exemplos de

$$A = \{A\} \quad A = \{A, \varnothing\}$$

ou também situações como $A \in B$ e $B \in A$.

Chamamos de sucessor de um conjunto A aquele definido por $S(A) = A \cup \{A\}$. Com isso, definiremos o conjunto I que satisfaz

$$\varnothing \in I \wedge \forall A(A \in I \rightarrow S(A) \in I).$$

O conjunto I é chamado de indutivo, e a existência de pelo menos um conjunto indutivo é enunciada pelo Axioma do Infinito. A motivação para ele é garantir não só a existência de um conjunto infinito, mas também permitir a definição dos números naturais. Cada natural poderia, individualmente, ser definido como

$$\begin{aligned} 0 &= \varnothing \\ 1 = S(0) &= \{\varnothing\} \\ 2 = S(S(0)) &= \{\varnothing, \{\varnothing\}\} \\ &\vdots \end{aligned}$$

No entanto, ainda não teríamos garantido a existência de um conjunto que contenha todos os naturais definidos daquela maneira. Pela definição de conjunto indutivos, o vazio e seus sucessores precisam pertencer a qualquer conjunto deste tipo; em outras palavras, todos os conjuntos indutivos incluem os números naturais. Dessa forma, o conjunto dos naturais é definido como a interseção de todos os conjuntos indutivos.

$$\mathbb{N} = \{x \in I \mid \forall J,\ (J \text{ é indutivo} \rightarrow x \in J\}$$

O próximo é o Axioma da Substituição, o qual afirma que, em qualquer conjunto A, se para todo elemento $x \in A$ existe um único y, denominado imagem, que satisfaça uma relação ϕ, então existe um conjunto B que reúne todos os y para os quais existe $x \in A$ que satisfaça ϕ. Em resumo, o axioma garante a existência de um conjunto que reúne as imagens dos elementos de A sobre a relação ϕ. Esse axioma está intimamente ligado ao conceito de funções e o aplicaremos mais adiante.

Por fim, temos o Axioma da Escolha. Ele afirma que, dado um conjunto $\mathscr{F}$ com membros não vazios, existe um conjunto C tal que, para todo $A \in \mathscr{F}$, existe um único $(A, a) \in C$ com $a \in A$. O conjunto C é chamado de função de escolha, que toma um conjunto $A \in \mathscr{F}$ e retorna um elemento $a \in A$.

1.2.6 Relações

Chamaremos R uma relação entre A e B se R for um conjunto em $\mathscr{P}(A \times B)$, e se $(a, b) \in R$, então denotaremos esse fato por aRb. O conjunto $\mathrm{Dm}(R) \subset A$, chamado de domínio, é o conjunto de todos os elementos $a \in A$ tal que existe um $b \in B$ e $(a, b) \in R$. Já o conjunto B é chamado de contradomínio da relação, e o seu subconjunto Im que contém todos os b para os quais há um $a \in A$ e $(a, b) \in R$ é chamado de imagem da relação. Geralmente, definimos uma relação por meio de uma dada fórmula $\varphi(a, b)$ envolvendo símbolos para elementos daqueles conjuntos, possibilitando definir a relação tal como

$$R = \{(a, b) \in A \times B \mid a \in A \wedge b \in B \wedge \varphi(a, b)\}$$

A fórmula $\varphi(a, b)$ é chamada de lei de correspondência.

O conceito de relações também podem ser extendido para além das binárias, que ocorrem entre dois conjuntos. Intuitivamente, o conceito de aridade duma relação está ligado a quantidade de conjuntos envolvidos nela, ou também com o tamanho das ordenações de elementos que pertencem a ela. Exemplo, uma relação ternária R entre conjuntos A, B e C terá como domínio $A \times B$ e contradomíno C, logo

$$R \subset (A \times B) \times C$$

Um exemplo de elemento em R seria $((a, b), c)$, mas iremos facilitar a notação impondo que

$$((a, b), c) = (a, b, c)$$

que é uma tripla ordenada. Em geral, uma relação de aridade n será um subconjunto no produto cartesiano de n conjuntos e cujos elementos serão tuplas ordenadas (ou tuplas somente).[3]

Há algumas relações que valem a pena serem destacadas para menções futuras. A primeira delas será a relação de ordem estrita linear, que, em essência, define uma maneira de comparar elementos num conjunto. Formalmente, uma relação R é uma ordem estrita linear para o conjunto A se satisfaz três propriedades[4]:

1. Assimetria - a relação não vale em duas direções.

$$\forall x, y \in A(xRy \rightarrow y \not R x)$$

2. Transitividade - numa cadeia de elementos relacionados, a relação vale para os elementos nas pontas da cadeia.

$$\forall x, y, z \in A(xRy \wedge yRz \rightarrow xRz)$$

3. Totalidade - todos os elementos estão relacionados entre si em ao menos uma direção.

$$\forall x, y \in A(x \neq y \rightarrow xRy \vee yRx)$$

[3] Fundamentalmente, nossas definições permitem apenas construírmos relações binárias, já que o produto cartesiano é uma operação binária por definição. Todavia, isso trata-se apenas de um detalhe de formalização, e, neste texto e em outros, adotaremos as tuplas para denotar elementos que estão relacionados entre si numa relação que envolve mais de dois conjuntos.

[4] O conjunto A é também o contradomíno da relação

A relação R será uma boa ordem para A se for uma ordem estrita linear, e todo subconjunto $B \subset A$ possui um menor elemento x, isto é,

$$\forall y \in B(xRy)$$

O conjunto A será bem ordenado se admite alguma boa ordem.

A segunda relação a ser mencionada é a de equivalência, que define um tipo especial de partição. Uma relação R é uma relação de equivalência num conjunto A se satisfaz:

1. Transitividade - já apresentada na relação de ordem.
2. Reflexividade - todo elemento está relacionado consigo mesmo.

$$\forall x \in A(xRx)$$

3. Simestria - a relação é bidirecional.

$$\forall x, y \in A(xRy \rightarrow yRx)$$

Pelo Axioma da Separação, podemos formar um conjunto $[x]_R \subset A$, com $x \in A$ e $\varphi(y) = xRy$ tal que

$$[x]_R = \{y \in A \mid \varphi(y)\}$$

Considere então os conjuntos $[x]_R$ e $[z]_R$. Se tivermos que xRz, segue que $[x]_R = [z]_R$, no contrário, $[x]_R \cap [z]_R = \varnothing$. O conjunto $[a]_R$ é chamado de classe de equivalência de A sobre R, e usando os axiomas do Par e da União, podemos construir o conjunto das classes de equivalência de A sobre R, denotado por A/R, que é uma partição de A.

1.2.7 Funções

Um tipo especial de relação são as famosas funções. Dados conjuntos A e B, a relação f é chamada de função de A em B se:

1. $A = \mathrm{Dm}(f)$
2. Se $(a, b) \in f$ e $(a, c) \in f$, então $b = c$, para todo a, b e c.

Em resumo, uma função relaciona todo elemento do domínio A a um único elemento do contradomínio B. Graças ao Axioma da Substituição, nem sempre é necessário explicitar o conjunto B, pois se temos o domínio A, uma fórmula $\varphi(x, y)$ e sabemos que, para todo $x \in A$, existe um único y, então já vimos que o axioma garantirá a existência de um conjunto imagem Im para a relação definida por $\varphi(x, y)$. Desse modo, a função f poderia ser definida com contradomínio no próprio Im ou qualquer conjunto que o contenha.

A notação para representar uma função f com domínio A no contradomínio B é

$$f : A \rightarrow B$$
$$x \mapsto f(x)$$

em que $f(x)$ é o elemento $y \in B$ que é imagem de $x \in A$. Denotaremos $\mathrm{Im}(f)$ como o conjunto imagem da função f.

Uma função pode ser classificada de três maneiras

- Injetiva - se um elemento no contradomínio é imagem de outro no domínio, então ele é imagem apenas desse último.

$$\forall y \in B,\ (y \in \mathrm{Im}(f) \rightarrow \exists! x \in A,\ (f(x) = y))$$

- Sobrejetiva - contradomínio e o cojunto imagem são iguais

$$B = \mathrm{Im}(f)$$

- Bijetiva - a função é injetiva e sobrejetiva, construindo uma correspondência de 1 para 1 entre os elementos no domínio e contradomínio da função.

1.2.8 Números Ordinais e Cardinais

Conjuntos transitivos são aqueles que possuem todos os elementos de seus elementos.

$$\forall x \forall y (x \in y \wedge y \in \alpha \rightarrow x \in \alpha)$$

Por sua vez, um ordinal α é um conjuntos que satisfaz

1. α e seus elementos são conjuntos transitivos
2. A relação $\in$ é uma boa ordem para α

Da definição segue que[5]:

I - $\varnothing$ é um ordinal por vacuidade, e os elementos de um ordinal são ordinais.

II - Todo ordinal é o conjunto de seus predecessores.

III - O suscessor de um ordinal é um ordinal.

Em especial, os elementos do conjunto dos naturais $\mathbb{N}$ são ordinais, ou seja, os números 1, 2, 3, ..., são ordinais (finitos). Além disso, o ordinal indentificado pelo próprio $\mathbb{N}$ é denotado por ω, sendo o primeiro ordinal transfinito.

Apresentados os ordinais, diremos que duas boas ordens (A, R) e (B, S) são isomorfas se existe uma bijeção $f : A \rightarrow B$ tal que

$$\forall x, y \in A (xRy \leftrightarrow f(x) S f(y))$$

Neste ponto é que a principal propriedade dos ordinais surge: todo conjunto bem ordenado é isomorfo a um, e somente um, ordinal. Isso implica que, se (A, R) é uma boa ordenação isomorfa a $(\alpha, \in)$, onde α é um ordinal, então podemos rotular cada elemento de A por um único elemento de α. Em outras palavras, os elementos de A podem ser indexados por ordinais, de acordo com sua posição na ordem. Ademais, como α é único para (A, R), então ele é uma representação canônica da estrutura daquela boa ordem.

Por fim, introduziremos a ideia dos cardinais, que, diferente dos ordinais, não indetifica a estrutura do conjunto, mas o seu tamanho.

[5] As afirmações listadas não são óbvias, mas as suas demonstrações em termos formais fugiria do escopo proposto para o texto

Antes de tudo, diremos que dois conjuntos são equipotentes se existe uma bijeção entre eles. Do Axioma da Escolha, segue o interessante Teorema da Boa Ordenação, o qual afirma que todo conjunto pode ser bem ordenado. Portanto, pelo que vimos dos ordinais, para todo conjunto A, existe um ordinal α equipotente a ele. Chamaremos de cardinal – ou cardinalidade – de um conjunto A, denotado por $|A|$, o menor ordinal equipotente a A.

Um conjunto será finito se o menor ordinal equipotente a ele for finito, isto é, um elemento de ω. Dessa forma, a cardinalidade de um conjunto finito é igual a algum número natural. O cardinal $\aleph_0$ é representado pelo ordinal ω, sendo, pois, a cardinalidade dos naturais. Um conjunto A é infinito se possui cardinalidade maior ou igual a $\aleph_0$[6].

1.2.9 Estruturas Discretas

Um conjunto é contável, ou enumerável, se sua cardinalidade é menor ou igual aos dos números naturais. Isso significa que é possível listar todos os seus elementos e indexá-los utilizando somente os naturais. Uma condição necessária e suficiente para que dois conjuntos tenham a mesma cardinalidade é que exista alguma bijeção entre eles. Dado isso, ser enumerável equivale a ter uma bijeção com algum subconjunto dos naturais[7].

A ideia de estruturas discretas é intuitivamente simples, porém, formalmente, sua natureza é difícil de especificar. Intuitivamente, estruturas discretas são conjuntos finitos ou enumeráveis tais que todos os elementos distintos estão bem separados. A forma padrão de formalizar "separação" de elementos em um conjunto é por meio de topologias, que não iremos entrar em muitos detalhes por fugir do escopo do que a matemática discreta, especialmente a combinatória, necessitam.

A propriedade de discretude não é dada como uma característica de um conjunto, mas como parte de uma estrutura que, neste caso, consiga isolar os elementos um dos outros.

Uma topologia $\tau \subset \mathscr{P}(X)$ é uma coleção de partes de um conjunto X cujos elementos, denominados abertos, satisfazem:

1. $\varnothing$ e X são membros de τ.
2. A interseção de um número finito de abertos é um aberto
3. A união de um número potencialmente infinito de abertos é um aberto.

O par (X, τ) é chamado de espaço topológico. A ideia por detrás dos abertos é a de vizinhança de um ponto, composto por elementos que estão arbitrariamente próximos desse último. Uma vizinhança V de um ponto $x \in X$ é um subconjunto de X tal que exista um aberto A com $x \in A \subset V$.

[6] Existe outras definições alternativas para um conjunto infinito: (a) se existe uma injeção $f : A \to A$ não sobrejetiva, ou (b) se existe uma injeção $f : \mathbb{N} \to A$.

[7] Georg Cantor provou que os naturais, os inteiros e os racionais possuem a mesma cardinalidade, logo são todos enumeráveis. No caso de $\mathbb{R}$, ele mostrou que é impossível criar uma lista que contenha todos os números reais, provando que a cardinalidade desse último é maior do que de $\mathbb{N}$.

Para representar a ideia de separção de um ponto, usamos as suas vizinhanças, como se essas fossem as identidades do ponto na topologia especificada, como na famosa frase "digamas com quem tu andas que direi que tu és". Dessa forma, um ponto isolado seria aquele que não necessita de ninguém além dele mesmo para ser identificado. Seja (X, τ) um espaço topológico, dizemos que $x \in X$ é um ponto isolado no subconjunto $S \subset X$, com $x \in S$, se há vizinhança V para x tal que

$$V \cap S = \{x\}$$

Isso equivale a dizer que, no subespaço topológico (S, τ_S), tal que

$$\tau_S = \{U \cap S \mid U \in \tau\}$$

temos que $\{x\}$ é um aberto de τ_S. Se for satisfeito que

$$\tau = \mathscr{P}(X)$$

então o espaço topológico (X, τ) é discreto, pois

$$\forall x \in X, \{x\} \in \tau$$

e todo ponto é uma vizinhança de si mesmo, ou que todo ponto é isolado no próprio X.

1.3 Recursão e Indução

Nesta seção, discutiremos em alto nível uma das ferramentas mais úteis para solução de problemas matemáticos: o Princípio de Indução Finita. Este princípio permite demonstrar que, quando determinados estruturas podem ter seus elementos definidos a partir de outros mais simples, e provarmos que certa propriedade vale para esses últimos, então a propriedade vale também para elementos mais complexos. Antes disso, explicaremos a ideia de recursão e a usaremos para construir intuitivamente o Princípio de Indução.

1.3.1 Recursão

A recursão é uma forma de definição aplicada a objetos que podem ser descritos em termos de outros objetos do mesmo tipo, porém mais simples. Em geral, uma definição recursiva é composta por casos base, que correspondem aos objetos mais simples e não dependem de outras definições, e por casos recursivos, nos quais um objeto é definido a partir de instâncias menores ou mais simples de si mesmo.

Uma definição recursiva é dita bem definida quando todo objeto que não é um caso base pode ser decomposto, em um número finito de passos, até alcançar um dos casos base, garantindo assim que o processo de definição termine.

De modo mais formal, um conjunto admite uma definição recursiva quando seus elementos podem ser descritos a partir de casos bases e de regras de construção que utilizam objetos previamente definidos. Os casos base são constituem os elementos mínimos da definição, enquanto que as regras recursivas garantem que todo objeto, pode ser reduzido, num número finito de aplicações, a esses casos.

As definições recursivas são, sem dúvida, uma das ferramentas mais úteis para o estudo de objetos discretos pelo fato de muitos deles terem a propriedade de serem definidos a partir de objetos discretos menores. Com isso, nos aproveitaremos dessa forma de definição para criar descrições elegantes sobre muitas estruturas.

1.3.2 Princípio de Indução Finita

As definições recursivas permitem a demonstração de resultados a partir do poderoso Princípio de Indução Matemática. A demonstração por indução, geralmente aplicada em situações em que deseja-se provar que uma propriedade é satisfeita por todos os elementos de um conjunto, envolve dois passos principais: provar que a propriedade é verdadeira para os casos base e, supondo que a propriedade vale para um caso recursivo, provar que, ao obter um novo caso pelas regras de construção da definição recursiva, a propriedade valerá para esse novo caso.

Em resumo, a indução consiste em demonstrar que, se a propriedade vale para os casos base e que ela se mantém verdadeira sempre que aplicamos a regra de construção recursiva para um novo caso, então ela é verdadeira para todos os casos.

1.4 Funções Discretas

Nesta seção, iremos dissertar um pouco mais com o tipo de funções com as quais esteremos lidando ao longo do texto. Assim como na seção anterior, iremos dissecar a ideia do que seria a propriedade de discretude aplicada a funções, e, em seguida introduziremos alguns tipos de funções discretas que nos acompanharão. Pontua-se aqui que, nos exemplos, estará implícito que as funções manipulam objetos discretos.

1.4.1 Discretude de Funções

Como funções são um tipo de relação especial entre dois conjuntos, então é razoável pensar que se tivermos estruturas discretas envolvidas numa relação, então essa propriedade influenciará a própria estrutura da relação. Seja a função $f : A \to B$, f será uma função discreta caso A tenha uma estrutura discreta. Para defender que essa ideia faz sentido, podemos argumentar que:

1. O conjunto imagem sempre terá cardinalidade menor ou igual a do domínio. Dessa forma, a propriedade de enumerabilidade é preservada para imagem se ela vale para o domínio.

2. Se os objetos do domínio são separáveis, o fato de que cada elemento possui uma única imagem implicará que as imagens também poderão ser vistas a partir de uma estrutura que separa os seus pontos, sendo, pois, discreta.

No geral, a forma como se trata uma função discreta é a mesma como se trata uma contínua, com a diferença que a estrutura subjacente dos domínios envolvidos é que lhes dará comportamentos distintos. Nas partes as seguir, iremos observar alguns exemplos típicos de funções discretas.

1.4.2 Multiconjuntos

Multiconjuntos, apesar do nome, é um tipo de função que é utilizada como artifício para criar estruturas em que há repetição de elementos. Formalmente, chamaremos de multiconjuntos qualquer função na forma:

$$m : X \to \mathbb{N}$$

em que a imagem $m(x)$ de $x \in X$ é chamada de multiplicidade. Um multiconjunto trivial é aquele tal que

$$\forall x \in X,\ (m(x) = 0)$$

e chamaremos de binário aqueles que satisfazem

$$\forall x \in X,\ (m(x) = 0 \vee m(x) = 1)$$

que será usado para representar situações em que fazemos uma seleção sem repetição dos elementos de X.

Dado um conjunto odenado $X = \{x_1, \ldots, x_n\}$ e um multiconjunto m, denotaremos por $m(X)$ o conjunto ordenado $\{m_1, \ldots, m_n\}$ tal que $m(x_i) = m_i$, para $i \in [n]$.

1.4.3 Funções de Contagem

Um dos problemas fundamentais da matemática combinatória é a contagem de objetos membros de uma dado universo que satisfazem certas restrições. Muitas vezes, é possível detectar um padrão nessas estruturas de forma a possibilitar a abstração da contagem por meio de uma função que relaciona uma tupla de parâmetros característicos da estrutura ao número de objetos que satisfazem as restrições impostas. Chamaremos essas relações de funções de contagem, que assumem a forma

$$f : \mathbb{N}^k \to \mathbb{N}$$

onde k é o número de parâmetros envolvidos na contagem.

As funções de contagem possuem um forte aspecto computacional embutido, pois muitas vezes a sua lei de relação é uma especificação de um método que permite, por meio de uma sequência finita de passos, determinar a contagem dos objetos. Em outras palavras, essas funções especificam algoritmos.

1.4.4 Fatoriais

Um caso particular de função discreta que surge naturalmente em problemas combinatórios são os fatoriais. Essas funções computam o produto de todos os inteiros não negativos até um $n \in \mathbb{N}$. Visto isso, o fatorial de um número n, denotado por $n!$, é recursivamente definindo como

$$n! = \begin{cases} 1, & \text{se } n = 0 \\ n(n-1)!, & \text{se } n > 0 \end{cases}$$

Os fatoriais tem uma propriedade interessante de que os valores se tornam absurdamente grandes mesmo com variações graduais na entrada da função. A calculadora do meu celular, por exemplo, só é capaz de computar o fatorial de até 170, cujo resultado supera – com grande folga – o número de partículas no universo.

1.4.5 Sequências

As sequências discretas são uma forma de representar uma sucessão de valores, que pode ser finita ou infinita, que possuem um primeiro elemento. Formalmente, diremos que S é uma sequência se for uma função injetora na forma $S : D \to A$ tal que D satisfaz uma das opções a seguir:

1. $D = [n]^*$, tal que $n \in \mathbb{N}$, caso em que a sequência é dita finita.
2. $D = \mathbb{N}$, caso onde a sequência é dita infinita.

Diremos que S é uma sequência para um conjunto A se ele for o contradomínio da sequência. Se $S : D \to A$, representaremos essa sequência enquanto uma tupla ordenada $(a_1, \ldots, a_n)$ de A^n, com $n = |D|$ de modo que

$$a_i = a \iff S(i) = a.$$

Quando a sequência for infinita, usaremos as reticências, como em $(1, 2, \ldots)$. Dessa maneira, conseguiremos tratar sequências e tuplas de maneira intercambiável. Rotineiramente, iremos dizer que uma sequência é igual a sua tupla correspondente.

Usaremos as sequências também para representar conjuntos cujos elementos estão ordenados por idexados por naturais. Resumidamente, se A é enumerável e bem ordenado pela relação estrita linear R, com menor elemento a_1, i.e.,

$$\forall a \in A,\ (a \not R a_1)$$

e S for uma sequência para A com $S(1) = a_1$, então representaremos A como:

1. A é finito, então seja a_n aquele que statisfaz

   $$\forall a \in A,\ (a R a_n),$$

   com $|A| = n$ e

   $$A = [a_1, \ldots, a_n] \iff \forall i, j \in [n],\ (i < j \leftrightarrow S(i)\ R\ S(j))$$

2. Se A for infinito enumerável, então

   $$A = [a_1, \ldots] \iff \forall i, j \in \mathbb{N},\ (i < j \leftrightarrow S(i)\ R\ S(j))$$

Omitindo a relação R e a sequência S, iremos usar a representação de um conjunto enquanto sequência para denotar uma situação em que queremos tratar os elementos do conjunto em uma determinada ordem[8].

Ainda sobre notações, tomemos a sequência $S : D \to A$ e a função $f : A \to B$. Construiremos a sequência $S_f : D \to \mathrm{Im}(f)$ como aquela que satisfaz

$$\forall k \in D\, \forall a \in A,\ (S(k) = a \leftrightarrow S_f(k) = f(x))$$

[8] Em outros textos é comum denotar os elementos de conjuntos ordenados estando entre parênteses, mas preferiremos os colchetes pela opinião de que os primeiros já estão semanticamente sobrecarregados.

Com essa formalização, iremos admitir que, quando houver uma sequência S para A, e f for uma função com domínio em A, então podemos tomar a tupla da sequência

$$(a_1, a_2, \ldots)$$

e substituir os termos pelas suas respectivas imagens em f, obtendo a representação em tupla da sequência S_f:

$$(f(a_1), f(a_2), \ldots).$$

Também usaremos essa forma para representar uma função f qualquer, intercalando com as formas já mostradas em seções anteriores..

Existem três formas principais de definir uma sequência discreta:

Relações de Recorrência

Aplicando as definições recursivas vistas na 1.3, as relações de recorrência, ou funções recursivamente definidas, definem sequências em que os termos dependem seus anteriores na sequência. Um exemplo clássico é a sequência de Fibonacci, em que cada termo é a soma dos outros dois anteriores.

$$S(n) = \begin{cases} 1, & \text{se } n = 1 \\ 1, & \text{se } n = 2 \\ f(n-1) + f(n-2), & \text{se } n > 2 \end{cases}$$

Funções de Índice

Ao contrário das definições recursivas, as sequências com função do índice são aquelas em que cada termo pode ser dado por uma fórmula fechada apenas em termos do índice da posição dele na sequência. Em outras palavras, a lei de formação de S é expressa numa fórmula apenas em termos de n.

Propriedade dos Termos

Alguns tipos de sequência, em vez de uma lei algébrica – como nos casos anteriores – utilizam uma determinada propriedade para definir os seus termos. Exemplos desse casos incluem: a sequência dos números primos ou a sequência do número de divisores de cada natural.

1.4.6 Princípio da Casa dos Pombos

O princípio da casas dos pombos é um interessante, e ao mesmo tempo simples, resultado sobre funções entre dois conjuntos finitos. Esse princípio carrega aquele nome devido ao forma como ele é geralmente explicado; admita que tenhamos n pombos e queiramos construir casas para eles, porém somente dispomos de material o suficiente para construir m casas, tal que $n > m$. Consequentemente, conclui-se que pelo menos dois pombos terão de compartilhar a mesma casa.

Na sua forma formal, o princípio estabelece que, se A e B são conjuntos finitos, de modo que $|A| > |B|$, então toda função $f : A \to B$ não poderá ser uma injeção. É verdade que, presumindo que f seja uma injeção, então dois casos podem ocorrer:

1. Se f for sobrejetiva, então ela é uma bijeção, e como vimos na seção de conjunto, A e B teriam de ter a mesma cardinalidade.

2. Se f não é sobrejetiva, então há pelo menos um elemento de B que não se relaciona com nenhum de A. Como $|A| = |\text{Im}(f)|$ pela injetividade, e $|\text{Im}(f)| \leq B$, então $|A| \leq |B|$.

O princípio, apesar de simples, é suficiente poderoso para demonstrar alguns teoremas interessantes, como o resultado de que num grupo qualquer de pessoas, em que alguém pode ou não ser amigo de outros, sempre haverá duas pessoas com o mesmo número de amigos.

1.5 Argumentos Combinatórios

Para alguns problemas, uma abordagem simplesmente algébrica, que consistiria na manipulação de termos em uma fórmula, pode ser difícil, cansativo e até mesmo deselagante. Essa situação ocorre frequentemente na matemática discreta, em que, muitas vezes, daremos prioridade aos argumentos combinatórios, que tentam atacar um problema dando mais atenção a estrutura dos objetos envolvidos, como sua quantidade, ordenação e formas de combiná-los para obter outros elementos, do que a fórmulas algébricas.

1.5.1 Contagem Duplas

A contagem dupla é dos argumentos combinatórios mais simples e comuns de serem observados em demonstrações. Ela é geralmente usada para provar a validade de uma identidade algébrica sobre alguma estrutura discreta, mostrando a igualdade dos dois membros ao argumentar que eles contam as mesmas coisas naquela estrutura.

1.5.2 Argumento da Bijeção

Já apresentado na seção de conjuntos, o Argumento da Bijeção visa construir uma bijeção entre dois conjuntos a fim de mostrar que ambos possuem a mesma quantidade de elementos. Dessa forma, se formos capazes de mostrar a equivalência entre pares de objetos de dois conjuntos, então teremos mostrado que eles possuem a mesma cardinalidade.

1.5.3 Argumento Extremal

Esse argumento usa a estratégia da prova por contradição para demonstrar um critério de extremalidade para objetos de uma estrutura. Em essência, ele se baseia na intuição trivial de que: se um objeto é maximiza uma propriedade, então não pode existir outro mais extremo. Para tanto, admite-se que haja um objeto que atenda a condição de extremalidade e de um objeto que seja mais extremo que o anterior, mostrado, em sequência, que isso leva a uma contradição.

1.5.4 Argumento Probabilístico

Os argumentos probabilísticos, popularizados pelo matemático Paul Erdös, é uma classe de argumentos não construtivos que visam mostrar a existência de um objeto numa estrutura que satisfaça uma dada propriedade. Eles fazem isso mostrando que, se selecionássemos objetos aleatoriamente da estrutura, então a probabilidade de eventualmente um objeto com a propriedade desejada ser escolhido é maior do que zero.

Chapter 2

Contagem e Combinatória Enumerativa

2.1 Princípios Fundamentais de Contagem

A grande maioria dos exercícios de contagem se baseiam no uso de dois princípios básicos: o aditivo e o multiplicativo. A seguir, iremos enunciar o problema fundamental de cada princípio e demonstrar o seu funcionamento.

2.1.1 Princípio Aditivo

O nosso primeiro problema de contagem será o de determinar a quantidade de elementos na união de uma família finita de conjuntos finitos e disjuntos. A seguir, enunciaremos o Princípio Aditivo para resolver esse problema.

Teorema 2.1. *Se $\mathscr{F} = \{A_1, A_2, \ldots, A_n\}$ é uma família de conjuntos finitos disjuntos dois a dois, então cardinalidade da união U desses conjuntos é a soma de suas cardinalidades.*

Demonstração. Considere o conjunto

$$D = \bigcup_{A \in \mathscr{F}} (A \times \{A\}).$$

Como os conjuntos de $\mathscr{F}$ são disjuntos dois a dois, para todo elemento $a \in U$ existe um único conjunto $A \in \mathscr{F}$ tal que $a \in A$. Definimos então a função

$$f : U \to D, \qquad f(a) = (a, A).$$

A função f é bem definida e bijetiva. De fato, se $f(a) = f(b)$, então $(a, A) = (b, A)$, o que implica $a = b$, mostrando que f é injetiva. Além disso, dado $(a, A) \in D$, temos $a \in U$ e $f(a) = (a, A)$, logo f é sobrejetiva.

Assim, $|U| = |D|$. Como D é uma união disjunta e

$$|D| = \sum_{A \in \mathscr{F}} |A|,$$

concluímos que

$$|U| = \sum_{A \in \mathscr{F}} |A|.$$

■

2.1.2 Princípio Multiplicativo

Outro problema básico de contagem é determinar a cardinalidade do produto cartesiano de dois ou mais conjuntos. Esse problema também pode ser enunciado como o número de tuplas ordenas podem ser geradas de forma que cada posição seja preenchida por um elemento de um conjunto finito. A solução desse problema encontra-se no Princípio Multiplicativo, também chamado de Princípio Fundamental da Contagem (PFC) por ser a base das soluções de vários outros problemas de contagem. O PFC é enunciado e demonstrado a seguir.

Teorema 2.2. *Seja $\mathscr{F} = \{A_1, \ldots, A_n\}$ uma família de dois ou mais conjuntos finitos. A cardinalidade do produto cartesiano desses conjuntos é igual ao produto das cardinalides deles.*

$$|A_1 \times A_2 \times \ldots \times A_n| = \prod_{A \in \mathscr{F}} |A|$$

Demonstração. A prova será por indução no número de conjuntos n em $\mathscr{F}$.

Base: Se $n = 2$, então suponha que $\mathscr{F}$ seja formada pelos conjuntos A e B, tal que

$$A = [a_1, \ldots, a_m].$$

Admita também uma partição de $R = A \times B$ dada por $\Psi \subset \mathscr{P}(R)$ tal que

$$\Psi = \{P_1, \ldots, P_m\},$$

em que, para $k \in [m]$, tem-se

$$P_k = \{(a, b) \in A \times B \mid a = a_k\}$$

Considere agora uma família de funções indexadas por $[m]$ tal que

$$\begin{aligned} f_k : B &\to P_k \\ b &\mapsto (a_k, b) \end{aligned}$$

É verdade que, para todo $k \in [m]$, f_k está bem definida e é bijetiva. Primeiramente, a sobrejetividade é garantida, pois se $(a_k, b) \in P_k$, então $\exists b \in B$ tal que $f_k(b) = (a_k, b)$. Também é verdade que f_k é injetiva, uma vez que se $f_k(b_i) = f_k(b_j)$, para $i, j \in [|B|]$, então $(a_k, b_i) = (a_k, b_j)$, implicando que $b_i = b_j$. Isso mostra que $|B| = |P_k|$.

Por outro lado, é fácil perceber que, se g é a função definida por

$$\begin{aligned} g : A &\to \mathscr{P} \\ a_k &\mapsto P_k \end{aligned}$$

então g também é uma bijeção e $|A| = |\mathscr{P}| = m$. Além disso, pelo fato de R ser a união da família de conjuntos disjuntos Ψ, temos que a cardinalidade de R é igual a

$$\sum_{P \in \Psi} |P|$$

pelo Principio Aditivo, donde segue que

$$|R| = \sum_{P \in \mathscr{P}} |P| = m \cdot |B| = |A| \cdot |B|$$

o que prova o teorema para o caso base.

Hipótese de Indução: Suponha que o teorema vale para uma família de n conjuntos. É verdade que, se $\mathscr{F} = \{A_1, \ldots, A_{n+1}\}$ e que

$$R = A_1 \times \ldots \times A_{n+1}$$

então o teorema vale para os primeiros n conjuntos de $\mathscr{F}$ pela Hipótese de Indução. Por conseguinte, se $R' = A_1 \times \ldots \times A_n$, então $R = R' \times A_{n+1}$, que consiste no caso base de dois conjuntos, para qual o princípio de indução vale. Temos então

$$|R| = |R'| \cdot |A_{n+1}| = \prod_{A \in R} |A|$$

provando o teorema. ■

Corolário 2.1. *Seja $\mathscr{F} = \{A_1, \ldots, A_n\}$ uma família de conjuntos finitos não vazios. O número de funções de escolhas para $\mathscr{F}$ é igual a*

$$\prod_{A \in \mathscr{F}} |A|$$

Demonstração. Toda função de escolha f equivale a uma única tupla no produto cartesiano dos conjuntos de $\mathscr{F}$, o qual será equipotente ao conjunto das funções de escolha. ■

Esse resultado irá facilitar bastante nosso trabalho, pois ele pode ser interpretado como: se uma escolha final é obtida por escolhas menores tomadas individualmente de universos finitos, então o total de escolhas é igual ao produto das quantidades de escolhas individuais em cada universo. Em demonstrações de resultados futuros, usaremos essa abordagem para aplicar o PFC.

Corolário 2.2. *Sejam A e B conjuntos finitos tal que*

$$n = |A| \qquad m = |B|.$$

O número de funções de $f : A \to B$ é igual a

$$m^n.$$

Demonstração. Contar quantas funções de A para B existem equivale a contar de quantas formas podemos escolher um elemento de B para ser imagem A. Dado que A tem n elementos, cada um para o qual há m escolhas, então o número total de funções é dado por:

$$\underbrace{m \cdot \ldots \cdot m}_{n} = m^n$$

■

2.1.3 Arranjos e Permutações

Arranjar os elementos de um conjunto finito significa criar sequência de elementos desse conjunto. A repetição de cada elemento e a ordem da sequência distinguem um arranjo um do outro. Com isso, os arranjos são equivalentes a sequências

Definição 2.1. *Seja A um conjunto de n elementos. Diremos que uma sequência S é um arranjo de r elementos de A se*

$$S : [r] \to A$$

Quando S for injetora, o arranjo é dito sem repetição. Se for bijetora, o arranjo é chamado de permutação.

Do corolário 2.2 segue que o número de arranjos de tamanho r com de um conjunto com n elementos é n^r. Para o caso sem repetição, precisamos contar quantas funções injetivas existem entre dois conjuntos.

Corolário 2.3. *Se A e B são conjuntos finitos com cardinalidades n e m respectivamente, então existem*

$$\frac{n!}{(n-m)!}$$

funções injetivas entre A e B.

Demonstração. O diferencial das injetivas para uma função qualquer é que, a cada escolha feita para imagem de um elemento de A, o universo de escolhas é reduzido em 1. Com efeito, o total de injeções será igual a

$$n \cdot (n-1) \cdot \ldots \cdot (n-m+1)$$
$$n \cdot (n-1) \cdot \ldots \cdot (n-m+1) \cdot \frac{(n-m)!}{(n-m)!}$$

que equivale a

$$\frac{n!}{(n-m)!}$$

■

Desta forma, se o arranjo é de r elementos, então a função de contagem de arranjos dos elementos de um conjunto finito de n elementos é

$$\mathrm{Arr}(n,r) = \frac{n!}{(n-r)!}.$$

As permutações correspondem ao caso em que $n = r$, e o número de permutações de tamanho n será dado simplesmnte por:

$$\mathrm{P}(n) = n!$$

2.2 Número Binomiais

Os números binomiais são objetos combinatórios simples e que representam o conceito de seleção de elementos de um conjunto finito. A seguir, apresentaremos sua definição formal, identidades básicas e algumas propriedades interessantes.

2.2.1 Definição e Interpretação

Definição 2.2. *Sejam n e k inteiros não negativos. Um número binomial, ou coeficiente binomial, de numerador n e classe k, denotado por*

$$\binom{n}{k}$$

é igual ao número de subconjuntos de k elementos presentes em $[n]$.

Conjuntos não admitem repetição de elementos, o que torna razoável a interpretação combinatória de que um subconjunto S dum conjunto A é uma seleção de membros desse último. Se chamarmos os subconjuntos de A, com $|A| = n$, que possuem exatamente $k \leq n$ elementos de subconjuntos de classe k, então o número binomial $\binom{n}{k}$ representa quantos subconjuntos de classe k o conjunto A possui. Essa representação está de acordo com a definição dos binomiais, uma vez que $|A| = |[n]|$, e ambos os conjuntos possuirão a mesma quantidade de subconjuntos.

2.2.2 Identidades Básicas

Demonstraremos agora duas propriedades fundamentais sobre números binomiais.

Definição 2.3. *Seja o número binomial* $\binom{n}{k}$, *o seu complementar é aquele dado por*

$$\binom{n}{n-k}$$

Se um subconjunto $S \subset A$ é uma seleção, então seu complementar S^c é a seleção complementar. Uma vez que para todo subconjunto há um único complementar, então a contagem de seleção realizadas por um binomial deve ser igual àquela feita pelo seu complementar, resultado esse formalizado a seguir:

Teorema 2.3. *Números binomiais complementares são iguais*

$$\binom{n}{k} = \binom{n}{n-k}$$

Demonstração. Suponha que C seja o conjunto dos subconjuntos de $[n]$ de classe k

$$C = \{S \in \mathscr{P}([n]) \mid |S| = k\},$$

e o conjunto C' aquele cujos subconjuntos são de classe $n-k$

$$C' = \{S \in \mathscr{P}([n]) \mid |S| = n-k\},$$

Para todo $S \in C$, vale que $[n] \setminus S \in C'$, pois $|[n] \setminus S| = n-k$. Com efeito, C' será o conjunto imagem da relação de complementar dos subconjuntos de classe k e $n-k$. Em outras palavras, existe uma função f sobrejetora tal que

$$\begin{aligned} f : C &\to C' \\ S &\mapsto S^c \end{aligned}$$

A função f é injetora, pois vale que se $f(S_1) = f(S_2)$, então

$$S_1^c = S_2^c$$
$$S_1 = S_2$$

Sendo f uma bijeção, então $|C| = |C'|$, implicando, finalmente, que

$$\binom{n}{k} = \binom{n}{n-k}$$

■

Introduzemos agora a relação de consecutividade entre binomiais.

Definição 2.4. *Dois números binomiais são consecutivos se possuem o mesmo numerador e o módulo da diferença de suas classes é 1.*

Uma propriedade fundamental dos números binomiais consecutivos é chamada de Relação de Stifel, e é ela é a base da construção do famoso triângulo de Pascal, que veremos mais adiante.

Teorema 2.4 (Relação de Stifel)**.** *Sejam n e k inteiros não negativos com $n-1 > k$, então*

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$$

Demonstração. Seja $S \subset [n]$ subconjunto de classe k. Com efeito, o complementar de S em relação a $[n]$ terá $n-k$ elementos, e para todo subconjunto de classe k de $[n]$, haverá $n-k$ formas de criar um novo subconjunto de classe $k+1$. Pelo PFC, temos que

$$\binom{n}{k+1} = (n-k)\binom{n}{k},$$

e somando $\binom{n}{k}$ a ambos os membros, obtemos

$$\binom{n}{k} + \binom{n}{k+1} = (n-k+1)\binom{n}{k}$$

Usaremos agora um argumento combinatório para demonstrar o resultado desejado. Visto que $[n+1] = [n] \cup \{n+1\}$, o complementar de S em relação a $[n+1]$ terá $n-k+1$ elementos. Desse modo, para todo subconjunto de classe k de $[n]$, existem $n-k+1$ maneiras de obter um subconjunto de classe $k+1$ de $[n+1]$, e, pelo PFC,

$$(n-k+1)\binom{n}{k} = \binom{n+1}{k+1},$$

o que prova o teorema. ■

Por fim, iremos demonstrar como computar o valor de um número binomial.

Teorema 2.5.

$$\binom{n}{k} = \frac{n!}{(n-k)!r!}$$

Demonstração. Suponhamos que

$$x = \binom{n}{k}$$

e seja $C = \{C_1, C_2, \ldots, C_x\}$ os subconjuntos de classe k de $[n]$. Iremos utilizar agora o argumento de contagem dupla sobre o número de arrajos de tamnaho k de $[n]$. Com efeito, para cada $i \in [x]$, podemos obter $k!$ arranjos de k elementos de C_i, totalizando

$$x \cdot k!$$

arranjos de k elementos de $[n]$. Mas sabemos que

$$\text{Arr}(n,k) = \frac{n!}{(n-r)!},$$

donde segue

$$x \cdot k! = \frac{n!}{(n-r)!}$$
$$x = \frac{n!}{(n-r)!r!}$$

■

2.2.3 Combinações

Combinações são seleções de objetos de um conjunto finito, estando intimamente conectadas com os binomiais vistos anteriormente. A definição a seguir formalizará a intuição de seleção que estávamos usando até então, representando-as como multiconjuntos.

Definição 2.5. *Seja A um conjunto de n elementos. Uma combinação s de A é um multiconjunto não trivial na forma*

$$s : A \to \mathbb{N}$$

Se s é uma combinação binária, então ela é dita sem repetição.

Toda combinação s sem repetição de A equivale a um subconjunto desse conjunto. A intuição é simples: o multiconjunto é função booleana que indica se o elemento pertence ou não ao subconjunto. Se $S \subset A$, então S equivale a combinação s que satisfaz:

$$\forall x \in A\,(x \in S \leftrightarrow s(x) = 1)$$

Dessa maneira, toda combinação de r elementos de A equivale a um subconjunto de classe r de A, e o número de combinações de um conjunto finito de n elementos será, portanto, igual ao binomial

$$\binom{n}{r} = \frac{n!}{(n-r)!r!}.$$

2.3 Anagramas

Nesta seção iremos introduzir os anagramas de um multiconjunto, também chamados de permutações com repetição. Depois, iremos aplicar o conceito para contar as soluções não negativas de uma equação, e, no fim, iremos demonstrar a função de contagem das combinações com repetição.

2.3.1 Contagem de Anagramas

A ideia de anagramas é análoga àquela para strings[1]: diferentes sequências de elementos em que trocar elementos repetidos em posições distintas não altera a sequência.

Definição 2.6. *Seja A um conjunto, e $s : A \to \mathbb{N}$ um multiconjunto. Chamamos $g : [n] \to A$ de anagrama de s se*

$$n = \sum_{a \in A} s(a)$$

e se $I(a)$ é o conjunto dos índices em $[n]$ que tem a como imagem em g, i.e.,

$$I(a) = \{k \in A \mid s(k) = a \wedge a \in A\}$$

então $|I(a)| = s(a)$.

O que vai nos interressar é a contagem dos anagramas de um multiconjunto s.

Teorema 2.6. *Seja $s : A \to \mathbb{N}$ um multiconjunto com $|A| = m$. Se*

$$n = \sum_{a \in A} s(a),$$

então o número de anagramas de s é dado por

$$\frac{n!}{\prod_{a \in A} s(a)!}$$

Demonstração. Com $A = [a_1, \ldots, a_m]$, denotemos $s_i = s(a_i)$ para $i \in [m]$. A prova usará contagem dupla para enumerar permutações de n elementos. A primeira contagem é dada por simplesmente $Pm(n) = n!$. Para segunda, presumindo que o número de anagramas seja x, seja $g : [n] \to A$ representado pela tupla

$$(a_{ij})_{i \in [m] \wedge j \in [n]},$$

em que o i-ésimo elemento de A ocupa a j-ésima posição. Com efeito, para toda sequência g teremos que

$$x \cdot s_i!$$

é equivalente ao número permutações de $m + s_i - 1$ elementos considerando que permutar os termos iguais a a_i geram sequências diferentes. Isso vale pelo PFC, pois para cada anagrama, podemos obter $s_i!$ ordenações em que considera-se a repetições de a_i. Generalizando, termos então que

$$x \cdot \prod_{i \in [m]} s_i!$$

conta o número de permutações em que se considera a repetição de todos os elementos de A, equivalendo ao número de permutações de

$$m + \sum_{i \in [m]} s_i - 1 = m + n - m = n$$

[1] sequência de símbolos

elementos. Ora, temos então que

$$x \cdot \prod_{i \in [m]} s_i! = n!$$
$$x = \frac{n!}{\prod_{i \in [m]} s_i!}$$

■

2.3.2 Soluções Não Negativas de Equações

Aqui demonstraremos bravemente uma aplicação do que vimos até aqui para resolver um problema interessante. Equações são entidades algébricas que representam a igualdade entre dois membros, e nosso foco será naquelas que assumem a forma:

$$\sum_{i=1}^{n} x_i = r. \tag{2.1}$$

O problema combinatório em questão é enumerar as soluções não negativas desse tipo de equação, ou melhor, quantas tuplas $(a_1, \ldots, a_n)$, tal que $a_i \in \mathbb{N}$, $i \in [n]$, são solução para aquela equação.

Para chegar à solução, iremos utilizar um argumento de bijeção, determinando uma associação entre uma tupla solução e uma forma única de a codificar. Introduzamos o seguinte algoritmo:

Algoritmo 1: Codificação de uma solução inteira não negativa de uma equação

Entrada: Uma tupla $s = (a_1, \ldots, a_n)$ solução de uma equação na forma de 2.1
Saída: Uma string que codifica a tupla s

```
1  início
2      str ← "";
3      para cada i ∈ [n] faça
4          p ← string com a_i símbolos iguais a ".";
5          str ← concatena(str, p);
6          se i ≠ n então
7              str ← concatena(str, "+");
8          fim
9      fim
10     retorna str
11 fim
```

Agora devemos provar a terminação e a corretude do algoritmo. A terminação é trivial, pois a tupla é finita. A demonstração da corretude consiste em provar que duas soluções distintas nunca terão a mesma codificação. Para isso, basta argumentar que, se $(a_i)_{i \in [n]}$ e $(b_j)_{j \in [n]}$ são soluções de uma equação na forma de 2.1 que tem a mesma codificação dada pelo algoritmo 1, então elas são a mesma solução. Isso é verdade, pois, para cada iteração no loop iniciado na linha 3, a string p da linha 4 será a mesma para duas entrada se, e somente, se $a_i = b_i$. Com isso, se a codificação produzida for a

mesma, então é verdade que, para todo $i \in [n]$, temos $a_i = b_i$, provando que o algoritmo produz uma única representação para cada solução.

Mas por que a representação dada pelo 1 é razoável? Se $(a_i)_{i\in[n]}$ é uma solução, então

$$\sum_{i=1}^{n} a_i = r,$$

e o total de símbolos iguais a "." na representação é igual ao próprio r. Por exemplo: a equação $x_1 + x_2 = 3$ tem como algumas de suas soluções as tuplas $(1, 2)$ e $(3, 0)$, cujas representações seriam, respectivamente: ".+.." e "...+". Em ambas, temos 3 símbolos iguais a 3. Outra invariante das representações é que haverão $n - 1$ símbolos iguais a "+", em que n é o número de variáveis, já que o algoritmo adiciona o simbolo citado para cada iteração exceto a última.

Como toda solução admite uma representação dada pelo algoritmo 1, e essa representação é única, então contar o número de soluções inteiras não negativas de uma equação como em 2.1 equivale a contar quantos anagramas existem com r símbolos iguais a "." e $n - 1$ símbolos iguais a "+". Pelo teorema 2.6, teremos que essa quantidade é exatamente

$$\frac{(r + n - 1)!}{r!(n - 1)!}$$

2.3.3 Combinações com Repetição

Quando abordamos combinações de um conjunto finito, apenas consideramos aquelas sem repetição, isto é, aos subconuntos do conjunto de escolhas. No entanto, neste momento, estamos aptos a prover um argumento combinatório para demonstrar a função de contagem de uma combinação $s : A \to \mathbb{N}$ qualquer, isto é, com repetição de elementos.

Teorema 2.7. *Seja A um conjunto de n elementos. A função de contagem das combinações $s : A \to \mathbb{N}$ de r elementos de A é dada por*

$$\mathrm{CR}(r, n) = \frac{(r + n - 1)!}{r!(n - 1)!}$$

Demonstração. Admitindo que $A = [a_1, \ldots, a_n]$, toda combinação com repetição de r elementos pode ser representada por uma sequência $(s_1, \ldots, s_n)$ tal que

$$s_i = s(a_i)$$

para $i \in [n]$. Como essas combinações são ditas com r elementos, então todas elas devem satisfazer que

$$\sum_{i=1}^{n} s_i = r.$$

Dessa forma, toda representação de tupla $(s_i)_{i\in[n]}$ para uma combinação de r elementos equivale a uma solução da equação anterior, e, pelo visto na seção anterior, temos que há

$$\frac{(r + n - 1)!}{r!(n - 1)!}$$

combinações com repetição de r elementos de A. ■

Chapter 3

Teoria dos Grafos

Chapter 4

Combinatória Extremal e Probabilística