NOTAS DAS REUNIÕES DO PICME

COMBINATÓRIA E OTIMIZAÇÃO

Primeiro semestre de 2015

ANOTADO POR: Fabrício Caluza Machado

25 de junho de 2015

Sumário

1 Três Problemas Geométricos

17/03/2015 - Yoshiharu Kohayakawa

A seguir, veremos três problemas geométricos. Discutiremos o primeiro em maior detalhe e com o último, veremos um resultado surpreendente.

1.1 Separando ovelhas

Problema 1.1. Considere um pasto com ovelhas brancas e negras paradas. Suponha que para quaisquer quatro ovelhas, podemos separar as ovelhas de mesma cor com uma reta. Então podemos separar todas as ovelhas brancas e negras.

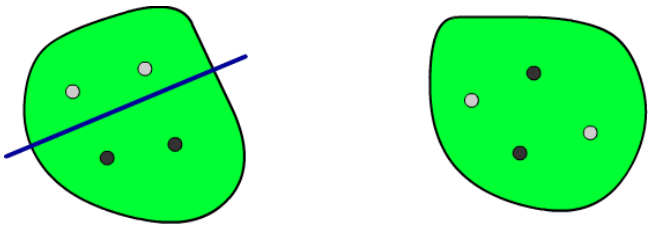

Figura 1: À esquerda, quatro ovelhas que podem ser separadas. À direita, quatro que não podem (uma configuração proibida).

Seja A o conjunto das ovelhas brancas e B o conjunto das ovelhas negras. Podemos tratá-los como subconjuntos finitos do plano, $A, B \subset \mathbb{R}^2$.

Afirmação 1.2. Separar as ovelhas é equivalente a separar o fecho convexo de A e B.

> **Definição 1.3.** Um ponto (vetor) x é dito *combinação convexa* de pontos x_1 e x_2 se existe $\lambda \in [0,1]$ tal que $x = \lambda x_1 + (1-\lambda)x_2$.
>
> O *segmento de reta* que une dois pontos é o conjunto de todos os pontos que são combinação convexa destes.
>
> Dizemos que um conjunto C é *convexo* se para quaisquer dois pontos $x_1, x_2 \in C$, C contém o segmento de reta que une estes pontos.
>
> O *fecho convexo* de um conjunto X, denotado $\operatorname{conv} X$, é a intersecção de todos os conjuntos convexos que contêm X. $\operatorname{conv} X := \bigcap_{C \text{ convexo, } C \supset X} C$.

Afirmação 1.4. Dois conjuntos convexos fechados (polígonos, no nosso caso) são separáveis se, e somente se, são disjuntos.

Demonstração. (esboço)

Sejam P, Q os dois polígonos. Definamos $d(P,Q) = \inf\{d(p,q) \ : \ p \in P, \ q \in Q\}$.

Como P e Q são polígonos (fechados), $\exists p \in P, q \in Q$ tais que $d(p,q) = d(P,Q)$.

Considere o segmento $\overline{pq}$ e uma reta perpendicular ao segmento passando pelo meio deste. Se ela não separasse P, Q poderíamos encontrar pontos em P e Q com distância menor. ■

Exercício 1.5. Se convença da última afirmação na demonstração anterior com um desenho e em seguida prove-a analiticamente.

Afirmação 1.6. Se dois polígonos se intersectam, existem 4 pontos (vértices) que violam a hipótese.

Demonstração.

Considere lados que se cruzam. ■

Agora vamos pensar no problema análogo em $\mathbb{R}^n$.

Queremos uma afirmação do tipo: "Sejam $A, B \subset \mathbb{R}^n$ finitos. Se podemos separar quaisquer s pontos com um hiperplano, então podemos separar todos". Mas qual deve ser o melhor valor para $s = s(n)$?

Se $s = 2(n+1)$, a prova é fácil. Particione cada poliedro em simplexos[1] e caso $\operatorname{conv} A \cap \operatorname{conv} B \neq \emptyset$, considere os vértices dos simplexos que se cruzam. Mas para $n = 2$, temos $s = 6$, e já sabemos que 4 basta...

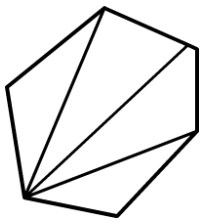

Figura 2: A partição de um poliedro bidimensional em triângulos.

A estimava correta é $s = n + 2$:

Teorema 1.7 (Kirchberger' 1903)
Sejam $A, B \subset \mathbb{R}^n$ conjuntos finitos com $|A| + |B| \geq n + 2$. Suponha que $\forall A' \subset A$ e $\forall B' \subset B$ com $|A'| + |B'| \leq n + 2$, há um hiperplano que separa A' de B' estritamente. Então existe um hiperplano que separa A de B estritamente.

Demonstração.

Sabemos que se $\operatorname{conv} A \cap \operatorname{conv} B = \emptyset$, a conclusão vale. Suponhamos portanto que $\operatorname{conv} A \cap \operatorname{conv} B \neq \emptyset$. Sem perda de generalidade, podemos supor que $0 \in \operatorname{conv} A \cap \operatorname{conv} B$.

Seja $A' \subset A$ e $B' \subset B$ com $|A'| + |B'|$ mínimo tal que $0 \in \operatorname{conv} A' \cap \operatorname{conv} B'$.

Pelo teorema de Carathéodory[2], temos $|A'| \leq n + 1$ e $|B'| \leq n + 1$.

Suponha $|A'| = r$ e $|B'| = s$. Temos que $r + s \geq n + 3$, caso contrário A' e B' poderiam ser

[1] Simplexos são triângulos quando $n = 2$, tetraedros quando $n = 3$ e o fecho convexo de $n + 1$ pontos afim independentes, em geral. Veja as notas de aula do PICME, primeiro semestre de 2014, dia 03/06/2014 para uma discussão mais detalhada.

[2] O teorema de Carathéodory diz que se $X \subset \mathbb{R}^n$ e $x \in \operatorname{conv} X$, x pode ser escrito como combinação convexa de $n+1$ pontos de X. Uma demonstração deste teorema também pode ser encontrada nas notas de aula do PICME, primeiro semestre de 2014, exercício resolvido 1.4.8.

separados pela hipótese. Seja U o espaço gerado por A', $U = \langle A' \rangle$ e W o espaço gerado por B', $W = \langle B' \rangle$.

Temos $\dim U = r-1$ e $\dim W = s-1$, mas $(r-1)+(s-1) \geq n+1$ e portanto $\dim(U \cap W) \geq 1$ e $U \cap W$ contém uma reta.

Seja $p \neq 0$ um ponto nesta reta (reta $= \{\alpha p \ , \ \alpha \in \mathbb{R}\}$).

Seja α o menor real não negativo com $\alpha p \in (\operatorname{conv} A') \cap (\operatorname{conv} B')$ e $\alpha p \in \operatorname{conv} A''$ para algum $A'' \subset A', A'' \neq A'$ (ou $\alpha p \in \operatorname{conv} B''$ para algum $B'' \subset B', B'' \neq B'$).

Então A'', B' (ou A', B'') contradizem a escolha de A', B'. ■

1.2 Simplexos vizinhentos (*Neighbourly simplices*)

Comecemos com o caso $n = 2$.

Consideramos dois triângulos, com interiores disjuntos, *vizinhos* se eles possuem um segmento de aresta em comum (intersecção de vértice com aresta não basta).

Pergunta 1.8. Qual a maior configuração de triângulos dois a dois vizinhos no plano?

Figura 3: À esquerda, três triângulos mutuamente vizinhos. À direita, quatro.

As figuras anteriores mostram que é possível 4 triângulos mutuamente vizinhos. Será possível mais?

Não. Se construirmos um grafo com um vértice em cada triângulo e uma aresta entre cada par de triângulos vizinhos, obtemos um grafo planar. Mas o K_5 (grafo completo com 5 vértices) não é planar.

Agora vejamos o caso $n \geq 3$:

Definição 1.9. Uma configuração C de n-simplexos no $\mathbb{R}^n$ é *vizinhenta* se $\forall c_1, c_2 \in C$, $c_1 \cap c_2$ tem dimensão $n-1$ e $(\operatorname{int} c_1) \cap (\operatorname{int} c_2) = \emptyset$.

Pergunta 1.10. Quanto vale $f(n) = \max\{|C| \ : \ C$ conjunto vizinhento de n-simplexos$\}$?

Bagemihl mostrou em 1956 que $8 \leq f(3) \leq 17$. O limitante inferior vem de uma construção derivada da exibida na figura 3 e a cota superior é obtida considerando um tetraedro e usando $f(2) = 4$ em cada face.

Bagemihl conjecturou ainda que $f(3) = 8$. Baston mostrou $f(3) \leq 9$ e Zak mostrou $f(3) = 8$ e ainda que $f(n) \geq 2^n$. Perles mostrou na década de 80, com um argumento simples, que $f(n) \leq 2^{n+1}$ e hoje em dia ainda é uma conjectura se $f(n) = 2^n$.

1.3 Politopos vizinhentos

Definição 1.11. Um *politopo* é o fecho convexo de um conjunto finito de pontos. [3]

Podemos definir o conceito de vizinhento e criar um problema semelhante ao anterior.

Definição 1.12. Uma configuração $\mathcal{P}$ de politopos no $\mathbb{R}^n$ é *vizinhenta* se $\forall P_1, P_2 \in \mathcal{P}$, $P_1 \cap P_2$ tem dimensão $n-1$ e $(\text{int } P_1) \cap (\text{int } P_2) = \emptyset$.

Pergunta 1.13. Quanto vale $g(n) = \max\{|\mathcal{P}| \ : \ \mathcal{P} \text{ conjunto vizinhento de politopos}\}$?

Aqui, podemos nos restringir ao caso $n = 3$. É claro que $g(3) \geq f(3) = 8$, mas na verdade:

Teorema 1.14 (Tietze / Besicovitch)

$$g(3) = \infty$$

24/03/2015 - Yoshiharu Kohayakawa

Agora, veremos em maior detalhe os dois últimos problemas abordados na aula passada.

1.4 Simplexos vizinhentos (II)

Comecemos relembrando alguns conceitos já vistos na seção 1.2:

Um *n-simplexo* é o fecho convexo de $n+1$ pontos afim independentes (ou, igualmente, em "posição geral", se estiverem contidos em um espaço de dimensão pelo menos n. Isto significa que não existe um hiperplano de dimensão k, $k < n$, que contenha $k+2$ destes pontos: não há 3 pontos colineares, nem 4 pontos coplanares, etc ...). Um 2-simplexo é um triângulo e um 3-simplexo é um tetraedro.

Dois n-simplexos são *vizinhos* se eles compartilham um pedaço de face $n-1$ dimensional e têm interiores disjuntos (figura 4).

Figura 4: À esquerda, dois triângulos vizinhos. À direita, triângulos que não são vizinhos.

[3] Esta definição corresponde ao que intuitivamente entendemos como poliedro. Entretanto, poliedros costumam ser definidos como a intersecção de um número finito de semiespaços, o que os permitem serem ilimitados. Nesse contexto, politopo pode ser entendido como um poliedro limitado.

Definimos $f(n) := \max |\mathcal{S}|$, onde $\mathcal{S}$ é uma família de n-simplexos em $\mathbb{R}^n$ dois-a-dois vizinhos.

No final da seção 1.2, vimos também uma revisão sobre o que se sabe sobre $f(n)$.

Proposição 1.15 (Bagemihl'56)**.** $f(3) \geq 8$

Demonstração.

Esta cota inferior vem de uma construção explícita, derivada da construção com 4 triângulos que mostra $f(2) \geq 4$. Podemos descrevê-la da seguinte maneira:

Fixe um plano e considere nele 4 triângulos mutuamente vizinhos, digamos, azuis. Ainda neste mesmo plano, sobreponha os 4 triângulos azuis com 4 triângulos amarelos, também mutuamente vizinhos, porém rotacione e reflita estes triângulos de modo que o interior de cada triângulo amarelo intersecte o interior de cada triângulo azul e vice-versa (figura 5). Considere um ponto azul fora do plano e crie 4 tetraedros, usando este ponto como pólo e os triângulos azuis como base. Considere um ponto amarelo do outro lado do plano e faça a mesma coisa com os triângulos amarelos. Obtemos, assim, 8 tetraedros vizinhentos (figura 6).

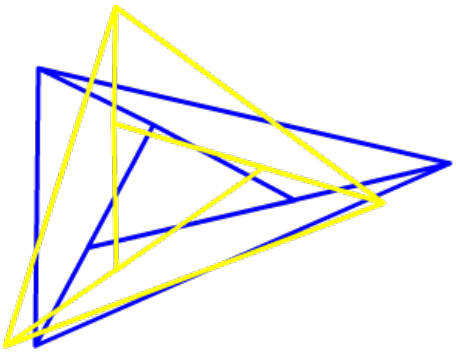

Figura 5: A configuração com 4 triângulos azuis e amarelos sobrepostos.

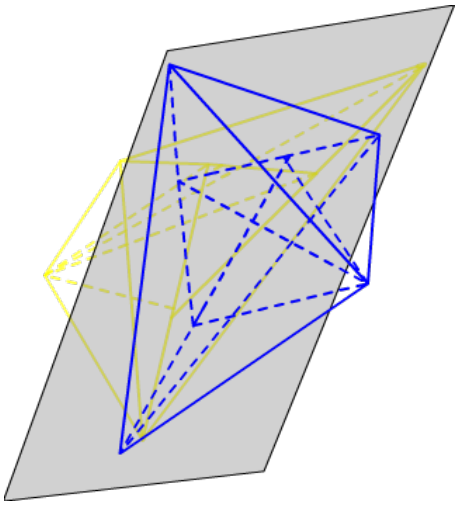

Figura 6: 8 tetraedros vizinhentos.

■

Proposição 1.16 (Perles'81)**.** $f(n) \leq 2^{n+1}$

Demonstração.

Fixado n, seja $\mathcal{S}$ uma configuração de n-simplexos vizinhentos. Queremos provar que $|\mathcal{S}| \leq 2^{n+1}$. Vamos descrever inicialmente a prova para o caso $n = 2$ e no fim concluímos que a prova é essencialmente a mesma para n em geral.

Para cada triângulo, trace suas 3 retas suporte e defina arbitrariamente um lado (semiplano) positivo e outro negativo.

Construa uma tabela com linhas indexadas pelos triângulos (p linhas) e colunas indexadas pelas retas (q colunas). Digamos que r seja uma reta suporte do triângulo Δ, a tabela terá valor 1 na entrada (Δ, r) se o triângulo Δ estiver no lado positivo da reta r e o valor da entrada será -1 caso contrário. Se r não for uma reta suporte de Δ, o valor será 0.

No exemplo da figura 7, a tabela será:

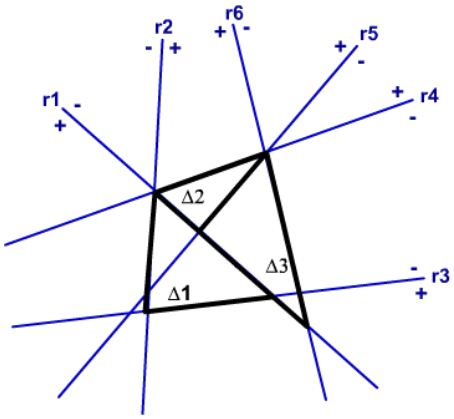

Figura 7: Um exemplo com 3 triângulos.

	r_1	r_2	r_3	r_4	r_5	r_6
Δ_1	1	1	-1	0	0	0
Δ_2	-1	0	0	-1	1	0
Δ_3	-1	0	0	0	-1	1

Observe que todas as linhas são distintas, pois do fato dos triângulos serem mutuamente vizinhos, segue que quaisquer dois triângulos possuem uma reta suporte em comum e um triângulo está do lado positivo e outro do lado negativo desta reta.

Agora, alteremos a tabela substituindo cada linha por 2^{q-3} linhas: trocando os 2^{q-3} zeros por todas as combinações possíveis de 1 ou -1. Obtemos uma tabela com $p.2^{q-3}$ linhas distintas, pois linhas provenientes de um mesmo triângulo receberam combinações distintas de 1 e -1 e já observamos que linhas de triângulos diferentes diferem na coluna da reta suporte em comum.

Como o número total de formas de preencher uma linha é 2^q, obtemos $p.2^{q-3} \leq 2^q \Rightarrow p \leq 2^3$.

Para n em geral, as retas se tornam hiperplanos, os semiplanos, semiespaços. Cada simplexo possui $n+1$ hiperplanos suporte, de modo que a tabela final possui $p.2^{q-n-1}$ linhas e no fim obtemos $p \leq 2^{n+1}$.

■

1.5 Politopos vizinhentos (II)

Na seção 1.3 definimos $g(n) := \max |\mathcal{S}|$, onde $\mathcal{S}$ é uma coleção de politopos no $\mathbb{R}^n$ tal que dois a dois: (a) possuem interiores disjuntos e (b) compartilham um pedaço de face $n-1$ dimensional.

Teorema
$g(3) = \infty$

Crum fez a pergunta sobre $g(n)$ em 1947 e Besicovich obteve a resposta do teorema no mesmo ano. Mas o problema já havia sido posto por Stöchel e resolvido por Tietze em 1905.

Demonstração.

Chamamos de *curva dos momentos* a curva $\Gamma(t) = (t, t^2, t^3),\ t \geq 0$.

Considere uma sequência de números $n_0, n_1, ...$ tal que $n_0 \geq 100$ e $n_i \geq n_{i-1}^2$, $i \geq 1$ (por exemplo, $n_i = 10^{2^{i+1}}$). Defina $P_i = \Gamma(n_i)$.

Seja C_i a *célula de Voronoi* do ponto P_i, definida pela coleção $\{P_i,\ i \geq 0\}$ de pontos, isto é, seja $C_i = \{Q \in \mathbb{R}^3\ :\ ||Q - P_i|| \leq ||Q - P_j||, \forall j \neq i\}$.

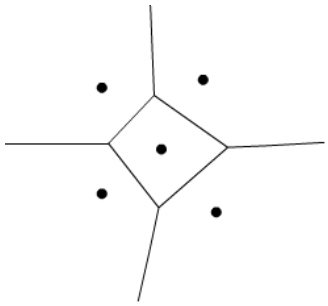

Figura 8: O diagrama de Voronoi de 5 pontos no plano.

Afirmação. Os C_i são dois a dois vizinhos e têm interiores disjuntos.

Demonstração. (esboço)

Considere três números da sequência: $a = n_\alpha, b = n_\beta, c = n_\gamma$, com $\alpha < \beta$ e os respectivos pontos na curva dos momentos: $P_\alpha = (a, a^2, a^3), P_\beta, P_\gamma$.

Seja $H_{\alpha\beta}$ o plano equidistante de P_α e P_β:

$$H_{\alpha\beta} = \{(x, y, z) \in \mathbb{R}^3\ :\ (a-b)x + (a^2 - b^2)y + (a^3 - b^3)z = K_{ab}\} \tag{1}$$

onde $K_{ab} = (a-b)\left(\frac{a+b}{2}\right) + (a^2 - b^2)\left(\frac{a^2+b^2}{2}\right) + (a^3 - b^3)\left(\frac{a^3+b^3}{2}\right)$.

Procuramos $P \in H_{\alpha\beta}$ tal que $d(P, P_\gamma) > d(P, P_\beta)$.

$$d(P, P_\gamma)^2 = (x-c)^2 + (y-c^2)^2 + (z-c^3)^2 > (x-a)^2 + (y-a^2)^2 + (z-a^3)^2 \tag{2}$$

De (1), obtemos $z = \frac{1}{a^3 - b^3}(K_{ab} - (a-b)x - (a^2 - b^2)y)$,

Substituindo em (2), temos que queremos:

$$\frac{(a-c)(b-c)}{a^2 + ab + b^2}((a+b+c)x + (ab + c(a+b))y + P_{ab}(c)/2) > 0 \tag{3}$$

onde $P_{ab}(c) = (a^2 + ab + b^2)c^4 + (a^3 + 2a^2b + 2ab^2 + b^3)c^3 + (a^4 + 2a^3b + 3a^2b^2 + 2ab^3 + b^4 + a^2 + ab + b^2)c^2 + (a+b)(ab(a^2 + ab + b^2) + ab - 1)c + ab(ab(a^2 + ab + b^2) + ab - 1)$

Analizando (3) em 3 casos: $c < a < b$, $a < b < c$ e $a < c < b$, podemos obter o resultado desejado.

■

Observamos que na construção dada, as células de Voronoi não são necessariamente politopos, pois podem ser ilimitadas. O que realmente queremos é mostrar que, para todo N, $g(3) > N$. Assim, basta considerarmos os N primeiros pontos $P_0, ..., P_{N-1}$ e intersectarmos a construção com um cubo de lado suficientemente grande, de modo a obter politopos.

■

2 Matróides

07/04/2015 - Lucas Praxedes

Para encontrar a melhor solução de um problema de combinatória, muitas vezes recorremos à buscas exaustivas. Outras vezes, usamos algoritmos gulosos, mas, para que estes funcionem bem, o problema deve ter uma certa estrutura. A teoria de matróides captura isso.

2.1 Definições e propriedades

Definição 2.1. Um *matróide* é um par ordenado $M = (S, I)$ tal que:

1. S é um conjunto finito não vazio.
2. I é uma família não vazia de subconjuntos de S, chamada de *subconjuntos independentes*[4] de S, tal que se $B \in I$ e $A \subset B$, então $A \in I$.

   Nós dizemos que I é *hereditário* se satisfaz esta propriedade.
3. Se $A, B \in I$, com $|A| < |B|$, então existe algum elemento $x \in B \backslash A$ tal que $A \cup \{x\} \in I$.

   Nós dizemos que M satisfaz a *propriedade de troca*.

Definição 2.2. Dado um grafo não-orientado $G = (V, E)$, definimos o *matróide gráfico* como sendo o par ordenado $M_G = (S_G, I_G)$, onde S_G é o conjunto E de arestas do grafo e I_G é a família de subconjuntos acíclicos de E.

Ou seja, um conjunto de arestas A é independente se, e somente se, o subgrafo $G_A = (V, A)$ é uma floresta.

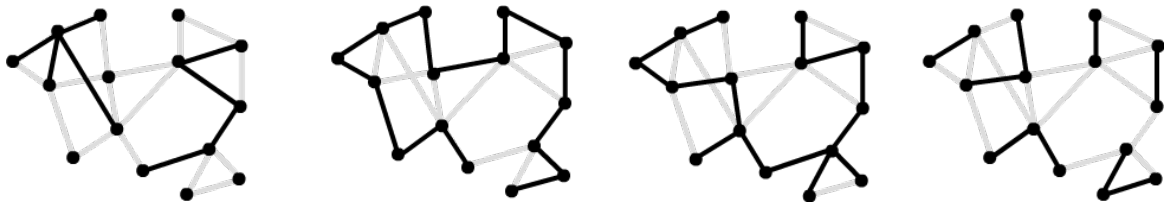

Figura 9: Exemplos de conjuntos independentes.

Na próxima aula, veremos que este matróide está muito relacionado ao problema da árvore geradora mínima.

Teorema 2.3
Se $G = (V, E)$ é um grafo não-orientado, o matróide gráfico $M_G = (S_G, I_G)$ é um matróide.

Demonstração.

Claramente, $S_G = E$ é um conjunto finito. Além disso, I_G é hereditário, uma vez que o subgrafo de uma floresta é uma floresta.

[4]Este nome vem de quando consideramos um conjunto finito de vetores em um espaço vetorial e seus subconjuntos linearmente independentes. Um exemplo de matróide.

Suponha que $G_A = (V, A)$ e $G_B = (V, B)$ sejam florestas de G e que $|B| > |A|$. Ou seja, A e B são conjuntos acíclicos de arestas e B contém mais arestas do que A.

Afirmação. Uma floresta $F = (V_F, E_F)$ contém exatamente $t = |V_F| - |E_F|$ árvores.

Demonstração.

Sejam e_i e v_i o número de arestas e vértices da i-ésima árvore. Então:

$$|E_F| = \sum_{i=1}^{t} e_i = \sum_{i=1}^{t} (v_i - 1) = \sum_{i=1}^{t} v_i - t = |V_F| - t$$

Onde usamos que o número de arestas de uma árvore com v vértices é $v - 1$.

Portanto $t = |V_F| - |E_F|$.

■

Assim, a floresta G_A possui $|V| - |A|$ árvores e a floresta G_B possui $|V| - |B|$ árvores. Como $|B| > |A|$, G_B tem menos árvores e deve possuir alguma árvore T cujos vértices estão em duas árvores diferentes na floresta G_A, sejam x e y estes vértices.

Como T é conexo, existe um caminho em T entre x e y e este caminho contém uma aresta que liga árvores diferentes em G_A, seja $\{u, v\}$ esta aresta.

Então, como a aresta $\{u, v\}$ conecta duas árvores diferentes na floresta G_A, nós podemos adicionar esta aresta à A sem criar um ciclo.

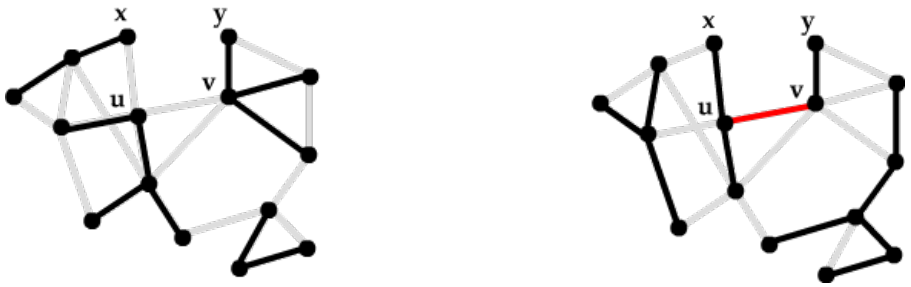

Figura 10: Exemplo com duas florestas, G_A à esquerda e G_B à direita.

Portanto, M_G satisfaz a propriedade de troca e é um matróide. ■

Definição 2.4. Dado um matróide $M = (S, I)$ e $A \in I$, chamamos um elemento $x \notin A$ de uma *extensão* de A se podemos adicionar x em A preservando sua independência, isto é, $A \cup \{x\} \in I$.

Se A não possui extensões, dizemos que A é *maximal*.

Teorema 2.5

Todos os subconjuntos independentes maximais possuem o mesmo tamanho.

Demonstração.

Suponha o contrário, que A seja um subconjunto independente maximal de M e haja outro subconjunto independente maior, B. Então a propriedade de troca implica que para algum $x \in B \backslash A$,

$A \cup \{x\} \in I$, o que contradiz que A seja maximal. ■

Definição 2.6. Dizemos que um matróide $M = (S, I)$ é *ponderado* se também temos uma função $w : S \to \mathbb{R}^+$ que assume valores estritamente positivos para cada elemento de S.

Dado $A \subset S$, definimos ainda $w(A) := \sum_{x \in A} w(x)$.

14/04/2015 - Lucas Praxedes

2.2 Algoritmos gulosos sobre um matróide ponderado

Muitos problemas para os quais uma aproximação gulosa produz soluções ótimas podem ser formulados em termos de encontrar um subconjunto independente de peso máximo em um matróide ponderado.

Definição 2.7. Dado um matróide ponderado, chamamos de *subconjunto ótimo* qualquer subconjunto independente que possua peso máximo possível.

A seguir, descreveremos um algoritmo guloso (*greedy algorithm*) simples que permite encontrar um subconjunto ótimo em qualquer matróide ponderado e provaremos sua corretude.

ALGORITMO
entrada: $M = (S, I)$, e $w : S \to \mathbb{R}^+$.
saída: A, um subconjunto ótimo do matróide.

1. $A = \emptyset$
2. ordene S em ordem decrescente relativa a w
3. para cada $x \in S$,
4. se $A \cup \{x\} \in I$,
5. então $A = A \cup \{x\}$
6. retorne A

Lema 2.8 (Propriedade gulosa)**.** Seja $M = (S, I)$ e $w : S \to \mathbb{R}^+$ um matróide ponderado e considere S ordenado em ordem decrescente. Seja x o primeiro elemento de S tal que $\{x\}$ é independente. Então existe um subconjunto ótimo que contém x.

Demonstração.

Seja B algum subconjunto ótimo tal que $x \notin B$. Nenhum elemento de B possui peso maior que $w(x)$, já que se $y \in B$, então $\{y\}$ é independente (pela hereditariedade) e S foi ordenado em ordem decrescente.

Iniciando com $A' = \{x\}$ e usando repetidamente a propriedade de troca com B, obtemos um conjunto A tal que $|A| = |B|$ e $A \backslash \{x\} \subset B$. Assim, $A = (B \backslash \{y\}) \cup \{x\}$ para algum $y \in B$ e $w(A) = w(B) - w(y) + w(x) \geq w(B)$, mas como supomos B ótimo, devemos ter $w(A) = w(B)$ e portanto A é um subconjunto ótimo que contém x. ■

Lema 2.9. Seja $M = (S, I)$ algum matróide. Se $x \in S$ e x é uma extensão de algum subconjunto independente $A \subset S$, então $\{x\}$ é também independente.

Demonstração.

Como $A \cup \{x\}$ é independente, $\{x\}$ é independente pela hereditariedade. ■

Definição 2.10. Dados um matróide $M = (S, I)$ e um elemento $x \in S$, definimos a *contração de* M *por* x como $M' = (S', I')$, onde $S' = S \backslash \{x\}$ e $I' = \{B \mid B \subset S',\ B \cup \{x\} \in I\}$. M' é um matróide desde que I' não seja vazio.

Lema 2.11 (Subestrutura ótima)**.** Seja x o primeiro elemento de S escolhido pelo algoritmo. O problema de encontrar um subconjunto independente de peso máximo contendo x se reduz a encontrar um subconjunto ótimo em M'.

Demonstração.

Se A é algum subconjunto ótimo contendo x, então $A' = A \backslash \{x\}$ é independente em M'. Se B' é ótimo em M', $w(B') \geq w(A')$, mas como $B = B' \cup \{x\}$ é independente em M, temos também $w(B) \leq w(A)$.

De $w(A) = w(A') + w(x)$ e $w(B) = w(B') + w(x)$, obtemos $w(B) \leq w(A) = w(A') + w(x) \leq w(B') + w(x) = w(B)$. Logo B é ótimo em M e A' é ótimo em M'. ■

Agora podemos provar a corretude do algoritmo.

Demonstração. (Corretude do algoritmo - esboço)

Uma vez que o algoritmo seleciona o primeiro elemento x, o lema 2.8 nos diz que o algoritmo não erra, já que existe um subconjunto ótimo contendo x. E o lema 2.11 implica que o problema remanescente é o de encontrar um subconjunto ótimo na contração de M por x, M'. Por indução em $|S|$, o algoritmo encontra um subconjunto ótimo em M', e portanto, em M. ■

2.3 Problema da árvore geradora mínima

Como exemplo de aplicação do algoritmo descrito na seção anterior, consideremos o problema da árvore geradora mínima:

Problema 2.12. Dado um grafo $G = (V, E)$ conexo, com pesos nas arestas dados por $w : E \to \mathbb{R}^+$, encontre uma árvore geradora de peso mínimo.

Já vimos que o matróide gráfico associado a G é um matróide e da teoria dos grafos, sabemos que os subconjuntos independentes maximais (subgrafos acíclicos maximais) são árvores geradoras de G. Resta adaptarmos o algoritmo, que resolve um problema de maximização, para este problema de minimização.

Fazendo $w_0 = 1 + \max\{w(e) \mid e \in E\}$, podemos definir $w' : E \to \mathbb{R}^+$ com $w'(e) = w_0 - w(e)$. Como, para qualquer $A \subset E$ que induza uma árvore geradora em G, temos:

$$w'(A) = \sum_{e \in A} w'(e) = \sum_{e \in A} (w_0 - w(e)) = (|V| - 1)w_0 - w(A)$$

Se maximizamos $w'(A)$, minimizamos $w(A)$ e podemos aplicar o algoritmo com a função w'.

Observação 2.13. A redução apresentada funciona entre diversos problemas de maximização e minimização. Uma característica fundamental que um problema deve ter para que este argumento

funcione é que o tamanho de todos os conjuntos ótimos seja igual. Matróides apresentam esta característica (teorema 2.5), mas outros problemas, como o do corte máximo/mínimo em um grafo e o do caminho mais longo/curto em um grafo, não (nestes dois casos, a versão de minimização pode ser resolvida de maneira eficiente, mas a de maximização não).

3 Um milhão de dígitos de π

28/04/2015 - Fernando Mário de Oliveira Filho

Aproximar[5] o número π é um problema considerado desde a antiguidade. Há muito sabe-se que $\sqrt{2}+\sqrt{3}$ é uma boa aproximação e é até mesmo possível inferir uma aproximação de um relato presente na bíblia. Mas o primeiro registro de um método para calcular aproximações e limitantes de π é devido ao matemático grego Arquimedes de Siracusa (287 - 212 AC).

Arquimedes calculou o perímetro de polígonos inscritos e circunscritos em um círculo de raio unitário, que fornecem limitantes inferiores e superiores para o π, respectivamente. Começando com um hexágono e considerando polígonos com cada vez mais lados, chegando a 96 lados, ele obteve:

$$3,1408 \simeq 3+\frac{10}{71} < \pi < 3+\frac{1}{7} \simeq 3,1428$$

Obtendo assim as duas primeiras casas decimais do π.

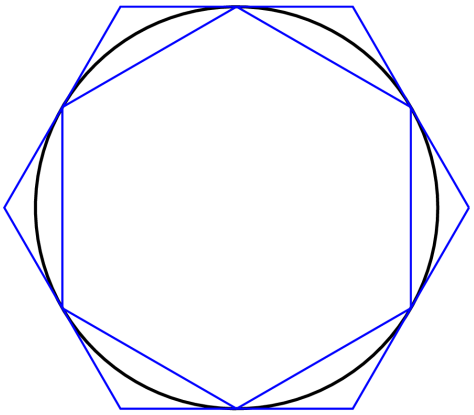

Figura 11: Círculo com hexágono inscrito e circunscrito.

Infelizmente, é difícil obter muitas casas decimais com essa técnica. Modernamente, com o advento do cálculo, passamos a considerar séries, como a expansão em Taylor da função $\arcsin$ em torno do 0:

$$\arcsin x = \sum_{k=0}^{\infty} \frac{(2k)!}{4^k (k!)^2 (2k+1)} x^{2k+1}$$

avaliada em $x=1$ ($\arcsin 1 = \frac{\pi}{2}$). Na prática, usamos outras séries que convergem mais rápido.

[5] O autor deste seminário disponibiliza um texto com mais detalhes sobre o assunto, em: `http://www.ime.usp.br/~fmario/divulg/pi.pdf`

3.1 Dificuldades Computacionais

Se programarmos em C, não podemos obter muita precisão numérica usando uma estrutura tipo ponto flutuante convencional. Para calcular a série diretamente, precisaríamos recorrer a uma biblioteca de precisão arbitrária (como a GMP) ou alguma implementação de aritmética racional, que costumam ser computacionalmente caras.

Veremos a seguir uma fórmula que nos permitirá calcular o n-ésimo dígito da representação hexadecimal de π sem termos que recorrer à aritmética de alta precisão, de forma que possamos usar os tipos comuns, *int, long* e *double*.

A fórmula a seguir é devida à Bailey, Borwein e Plouffe ('97):

Teorema 3.1 (Fórmula BBP)

$$\pi = \sum_{k=0}^{\infty} 16^{-k} \left(\frac{4}{8k+1} - \frac{2}{8k+4} - \frac{1}{8k+5} - \frac{1}{8k+6} \right)$$

Demonstração.

É um exercício de cálculo mostrar que

$$\pi = \int_0^{\frac{1}{\sqrt{2}}} \frac{4\sqrt{2} - 8x^3 - 4\sqrt{2}x^4 - 8x^5}{1 - x^8} dx$$

Usando a série de Taylor ao redor de 0 de $\frac{1}{1-x^8}$:

$$\frac{1}{1-x^8} = 1 + x^8 + x^{16} + ... = \sum_{k=0}^{\infty} x^{8k}$$

e usando que a série converge absolutamente, para trocarmos a soma com a integral, temos:

$$\begin{aligned}
\pi &= \int_0^{\frac{1}{\sqrt{2}}} 4\sqrt{2} \sum_{k=0}^{\infty} x^{8k} dx - \int_0^{\frac{1}{\sqrt{2}}} 8x^3 \sum_{k=0}^{\infty} x^{8k} dx - \int_0^{\frac{1}{\sqrt{2}}} 4\sqrt{2}x^4 \sum_{k=0}^{\infty} x^{8k} dx - \int_0^{\frac{1}{\sqrt{2}}} 8x^5 \sum_{k=0}^{\infty} x^{8k} dx \\
&= \sum_{k=0}^{\infty} 4\sqrt{2} \int_0^{\frac{1}{\sqrt{2}}} x^{8k} dx - \sum_{k=0}^{\infty} 8 \int_0^{\frac{1}{\sqrt{2}}} x^{8k+3} dx - \sum_{k=0}^{\infty} 4\sqrt{2} \int_0^{\frac{1}{\sqrt{2}}} x^{8k+4} dx - \sum_{k=0}^{\infty} 8 \int_0^{\frac{1}{\sqrt{2}}} x^{8k+5} dx \\
&= 4 \sum_{k=0}^{\infty} \frac{16^{-k}}{8k+1} - 2 \sum_{k=0}^{\infty} \frac{16^{-k}}{8k+4} - \sum_{k=0}^{\infty} \frac{16^{-k}}{8k+5} - \sum_{k=0}^{\infty} \frac{16^{-k}}{8k+6} \\
&= \sum_{k=0}^{\infty} 16^{-k} \left(\frac{4}{8k+1} - \frac{2}{8k+4} - \frac{1}{8k+5} - \frac{1}{8k+6} \right)
\end{aligned}$$

■

3.2 Cálculo do n-ésimo dígito hexadecimal

Na discussão a seguir, usaremos a seguinte notação:

- $\lfloor x \rfloor$, o piso de x, é o maior inteiro menor ou igual a x.

- $\text{frac}(x)$, a parte fracionária de x, $\text{frac}(x) = |x| - \lfloor |x| \rfloor$.
- $\text{int}(x)$, a parte inteira de x, $\text{int}(x) = |x| - \text{frac}(x)$.

Assim, se $x = -0,2$, temos $\lfloor x \rfloor = -1,\ \text{int}(x) = 0$ e $\text{frac}(x) = 0,2$. Também vamos convencionar contar a partir do 0, assim o primeiro dígito após a vírgula será associado a $n = 0$, o segundo dígito associado a $n = 1$, etc.

Temos as seguintes identidades:

- $x, y \geq 0,\ \text{frac}(x + y) = \text{frac}(\text{frac}(x) + \text{frac}(y))$
- $x \geq y \geq 0,\ \text{frac}(x - y) = \text{frac}(1 + \text{frac}(x) - \text{frac}(y))$

Pensando inicialmente em base 10, uma forma de obtermos o terceiro dígito decimal ($n = 2$) de $1,01234$ é fazendo a conta: $\text{int}(10.\,\text{frac}(10^2.1,01234)) = \text{int}(10.0,234) = \text{int}(2,34) = 2$. Assim, pensando da mesma forma em base 16, uma fórmula para o n-ésimo dígito hexadecimal de π é:

$$\text{int}(16.\,\text{frac}(16^n.\pi))$$

E uma fórmula para os k primeiros dígitos a partir do n-ésimo é:

$$\text{int}(16^k.\,\text{frac}(16^n.\pi))$$

Observação 3.2. Note que para obter o n-ésimo dígito, precisamos conhecer apenas a parte inteira de $16\,\text{frac}(16^n\pi)$. Logo, podemos fazer isso conhecendo poucos dígitos significativos de $16^n\pi$.

Definindo,

$$\sigma(n, c) = \sum_{k=0}^{\infty} \frac{16^{n-k}}{8k + c}$$

Temos:

$$16^n\pi = 4\sigma(n, 1) - 2\sigma(n, 4) - \sigma(n, 5) - \sigma(n, 6)$$

E portanto, podemos calcular uma boa aproximação para a parte fracionária de $16^n\pi$ se soubermos calcular uma boa aproximação para a parte fracionária de $\sigma(n, c)$.

Dividimos a soma em duas partes:

$$\sigma(n, c) = \sum_{k=0}^{n} \frac{16^{n-k}}{8k + c} + \sum_{k=n+1}^{\infty} \frac{16^{n-k}}{8k + c}$$

1. A primeira soma é uma soma finita que envolve números enormes, mas como estamos interessados apenas na parte fracionária, podemos fazer contas $\mod (8k + c)$, isto é, para calcular 16^{n-k}, usamos que $ab \mod d = (a \mod d)(b \mod d) \mod d$.[6]

[6] Aqui é necessário um cuidado adicional: o algoritmo ingênuo executaria $n - k$ operações, mas é possível gastar $\log(n - k)$ operações e isto tem um grande impacto no desempenho final do programa, quando escolhemos n grande.

2. A segunda soma é infinita, mas converge para 0 rapidamente, então podemos obter uma boa aproximação considerando poucos termos. De fato, $\sum_{k=n+l}^{\infty} \frac{16^{n-k}}{8k+c} \leq \sum_{k=n+l}^{\infty} 16^{n-k} = \frac{16^{-l}}{1-16^{-l}}$ e assim, se calcularmos apenas os primeiros 9 termos, cometeremos um erro menor que 10^{-10}, o que não deve afetar os dígitos mais significativos, nos quais estamos interessados[7].

3.3 Escrevendo π na base decimal

Com as informações descritas na última seção, podemos implementar um programa que calcula os dígitos hexadecimais de π. Mas... e os dígitos decimais? Curiosamente, não temos um método que calcula diretamente o m-ésimo dígito decimal do π. Precisamos calcular todos os n primeiros dígitos hexadecimais[8] e aí fazer uma conversão. Para isso, será necessário trabalhar com números grandes.

Com os n primeiros dígitos hexadecimais do π, temos o número inteiro $a = \operatorname{int}(16^n \operatorname{frac}(\pi))$ na base 16. Queremos expressar o número $\operatorname{int}(10^m a/16^n)$ na base 10.

Podemos expressar esses números no computador como vetores de inteiros e teremos que implementar funções para (i) multiplicar esses números por potências de 10; (ii) dividir esses números por potências de 10 e 16.

Mais detalhes sobre a implementação dessas funções encontram-se no texto indicado no início do capítulo.

4 Removendo arestas para tornar um grafo bipartido

12/05/2015 - Lucas Colucci

Nesta seção, nos preocuparemos com a seguinte pergunta:

Pergunta 4.1. Dado um grafo, qual o menor número de arestas que, se removidas, tornam o grafo bipartido?

4.1 Notação

Inicialmente, fixemos algumas notações que usaremos adiante.

$G = (V, E)$ sempre será um grafo com conjunto de vértices V e arestas E, quando necessário distinguir o grafo, usaremos $V(G)$ e $E(G)$ para o conjunto de vértices e arestas de G, respectivamente. De forma análoga, $v(G) := |V(G)|$ e $e(G) := |E(G)|$ são o número de vértices e arestas do grafo G. Muitas vezes, usaremos as letras $n = v(G)$ e $m = e(G)$ para denotar estes parâmetros.

Dado um vértice $x \in V$, denotamos por $\Gamma(x)$ a vizinhança de x, isto é, o conjunto de vértices adjacentes à x (note que $x \notin \Gamma(x)$!). Já $\bar{\Gamma}(x)$ são os vértices diferentes e não adjacentes à x, isto é, $\bar{\Gamma}(x) = V \backslash (\{x\} \cup \Gamma(x))$.

Ainda com $x \in V$, $\deg(x) := |\Gamma(x)|$ é o grau de x. Se $A \subset V$, $\deg_A(x) := |\Gamma(x) \cap A|$ é o número de vizinhos de x no conjunto A.

Se $A \subset V(G)$, $G[A]$ é o subgrafo induzido por A, isto é, o grafo com conjunto de vertices A e apenas as arestas de G que são entre vértices de A.

[7] Aqui também devemos ser cautelosos: por exemplo, se somarmos 10^{-10} ao número $0,0999999999$, obtemos $0,1$. Então também devemos verificar se algo assim não ocorre.

[8] Um inteiro a precisa de $1 + \lfloor \log_b a \rfloor$ dígitos para ser representado na base b. Assim, se quisermos m dígitos de π na base 10, precisamos dos $n = 1 + m \log_{16} 10 \leq 1 + 0,84m$ dígitos na base hexadecimal.

A seguinte figura será útil:

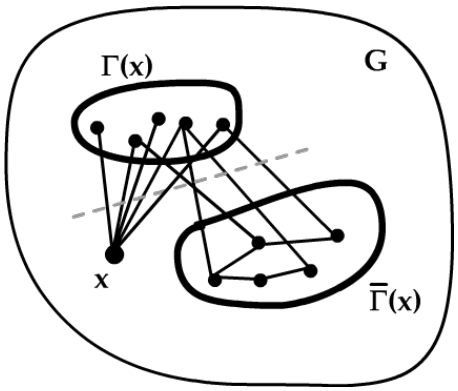

Figura 12: Um exemplo com x, $\Gamma(x)$ e $\bar{\Gamma}(x)$. Note o subgrafo bipartido induzido pelo corte $(\Gamma(x), \{x\} \cup \bar{\Gamma}(x))$.

4.2 Tornando grafos bipartidos

Fato 4.2. Um grafo G pode ser feito bipartido removendo-se no máximo metade de suas arestas. Formalmente, existe $G_0 \subset G$ bipartido, tal que $V(G_0) = V(G)$ e $e(G_0) \geq e(G)/2$.

Demonstração.

Comece com uma partição arbitrária dos vértices, (A, B). Se $x \in A$ tem mais vizinhos em A do que em B, altere a partição transferindo x para o conjunto B. Faça o análogo para vértices em B, isto é, se $x \in B$ tem mais vizinhos em B do que em A, mova-o para o conjunto A.

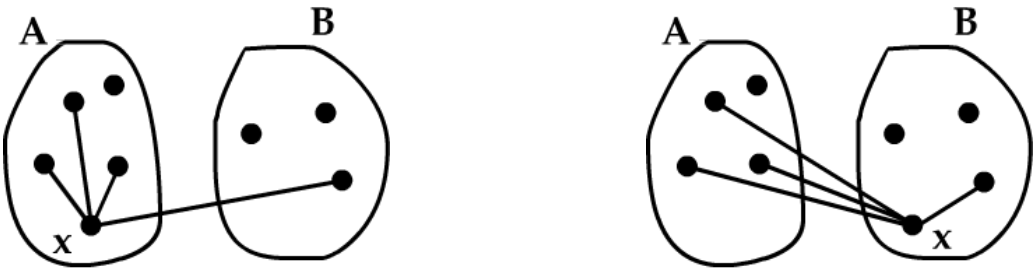

Figura 13: A transferência de um vértice.

Cada vez que essa operação é realizada, o número de arestas entre as partes A e B cresce, portanto após um número finito de operações, este processo não poderá ser repetido.

Se não podemos mais repetir a operação, vale que $\forall a \in A$, $\deg_A(a) \leq \deg_B(a)$ e $\forall b \in$

B, $\deg_B(b) \leq \deg_A(b)$. E então:

$$\begin{aligned}\text{\# arestas entre } A \text{ e } B =& \frac{1}{2}\left(\sum_{a\in A}\deg_B(a) + \sum_{b\in B}\deg_A(b)\right)\\ \geq& \frac{1}{2}\left(\frac{1}{2}\sum_{a\in A}(\deg_A(a)+\deg_B(a)) + \frac{1}{2}\sum_{b\in B}(\deg_B(b)+\deg_A(b))\right)\\ =& \frac{1}{4}\sum_{v\in V}\deg(v) = \frac{e(G)}{2}\end{aligned}$$

Portanto o número de arestas internas em A e B é menor ou igual à $e(G)/2$ e removendo-as obtemos um grafo bipartido. ■

O fator $\frac{1}{2}$ é ótimo, pois o grafo completo K_n tem $\binom{n}{2}$ arestas e seu maior subgrafo bipartido é o grafo bipartido completo $K_{\frac{n}{2},\frac{n}{2}}$ com $\frac{n^2}{4} \simeq \frac{1}{2}\binom{n}{2}$ arestas.

A seguir, uma conjectura de Erdös que motivará os próximos resultados desta seção. Lembremos o resultado de teoria dos grafos de que os grafos bipartidos são exatamente aqueles que não possuem ciclos ímpares. Assim, não possuir triângulos é um "primeiro passo" para ser bipartido.

Conjectura 4.3 (Erdös)**.** Um grafo G com n vértices e livre de triângulos pode ser feito bipartido removendo-se no máximo $\frac{n^2}{25}$ arestas.

Observação 4.4. A conjectura é motivada pelo seguinte exemplo (que mostra que a conjectura não pode ser melhorada): considere o grafo formado por 5 partes: A_1, A_2, A_3, A_4 e A_5, cada uma com $n/5$ vértices e arestas apenas entre vértices de partes consecutivas: A_i, A_{i+1}, $i = 1$ a 4 e A_5, A_1. É necessário remover pelo menos $\frac{n^2}{25}$ arestas deste grafo para torná-lo bipartido. (Exercício: mostre isso![9])

Observação 4.5. Segue diretamente do Fato 4.2 que se $e(G) \leq \frac{n^2}{12,5}$, a conjectura vale .

Teorema 4.6 (Erdös, Gijon, Simonovits)
A conjectura é verdadeira se $e(G) \geq \frac{n^2}{5}$.

Demonstração.

Para cada $x \in V(G)$, considere o grafo bipartido induzido por $(\Gamma(x), V\backslash\Gamma(x))$ (reveja a figura 12). Como G é livre de triângulos, não existem arestas entre vértices de $\Gamma(x)$ e assim o número de arestas deste subgrafo bipartido é igual à soma dos graus dos vértices em $\Gamma(x)$. Variando x, podemos calcular a média de arestas neste subgrafo bipartido:

$$\frac{1}{n}\sum_{x\in V(G)}\sum_{u\in\Gamma(x)}\deg(u) = \frac{1}{n}\sum_{u\in V(G)}\deg(u)^2 \geq \left(\frac{\sum_{u\in V(G)}\deg(u)}{n}\right)^2 = \frac{4e(G)^2}{n^2} \tag{4}$$

Sendo que na primeira igualdade trocamos a ordem das somatórias e notamos que cada vértice u é contado exatamente $\deg(u)$ vezes e a desigualdade é devida à convexidade da função $f(t) = t^2$.

[9]DICA: conte quantos C_5 há no grafo e quantos incidem em cada aresta.

Concluímos que existe um vértice $x \in V(G)$ tal que $\sum_{u\in\Gamma(x)} \deg(u) \geq \frac{4e(G)^2}{n^2}$ e portanto é possível obter um grafo bipartido removendo-se $e(G) - \frac{4e(G)^2}{n^2}$ arestas. Disto resulta a tese, já que $e(G) - \frac{4e(G)^2}{n^2} \leq \frac{n^2}{25}$ quando $e(G) \geq \frac{n^2}{5}$. ■

Enunciamos a seguir o principal resultado desta seção (e o mais perto que chega-se da conjectura de Erdös).

Teorema 4.7 (Erdös, Faudree, Pach, Spencer '86)
Um grafo G com n vértices e livre de triângulos pode ser feito bipartido removendo-se no máximo $\frac{n^2}{18} + \frac{n}{2}$ arestas.

Para provar este teorema, consideraremos dois casos. Se o número de arestas for grande, o grafo bipartido induzido pelo partição $(\Gamma(x), \{x\} \cup \bar{\Gamma}(x))$ para um certo $x \in V$ resolverá. Caso contrário, olharemos para os ciclos de tamanho 4 (C_4), incidentes em uma certa aresta xy e o grafo bipartido induzido pela partição $(\Gamma(x)\backslash\{y\}, \Gamma(y)\backslash\{x\})$. Veja a figura 14.

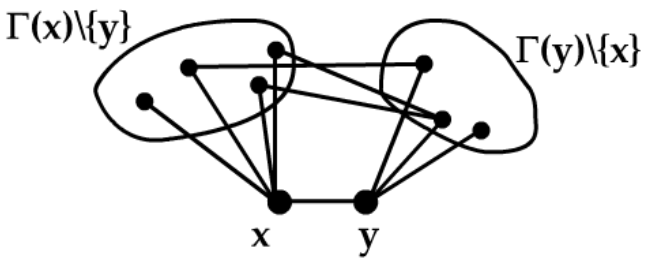

Figura 14: As arestas no grafo bipartido induzido por $(\Gamma(x)\backslash\{y\}, \Gamma(y)\backslash\{x\})$ são exatamente o número de C_4's incidentes em xy.

Provemos alguns lemas antes de procedermos à demonstração do teorema.

Lema 4.8. Todo grafo livre de triângulos tem um vértice x tal que $e(G[\bar{\Gamma}(x)]) \leq e(G) - \frac{4e(G)^2}{n^2}$

Demonstração.
Segue diretamente da equação (4) e do argumento usado na prova do Teorema 4.6 de que para algum vértice $x \in V(G)$, $\sum_{u\in\Gamma(x)} \deg(u) \geq \frac{4e(G)^2}{n^2}$. ■

Lema 4.9. Seja G um grafo com n vértices e m arestas, então:

(i) G tem uma aresta contida em pelo menos $\left(\frac{8m^2}{n^4} - \frac{6m}{n}\right) C_4$'s.

(ii) Se G é livre de triângulos, então existe uma aresta contida em pelo menos $\frac{4m(2m^2-n^3)}{n^2(n^2-2m)} C_4$'s.

Demonstração.
Dados $x, y \in V$, seja $t(\{x, y\}) := |\Gamma(x) \cap \Gamma(y)|$ o número de vizinhos comuns a x e y.

Temos:

$$\sum_{\{x,y\}} t(\{x,y\}) = \sum_{u \in V} \binom{\deg(u)}{2} \geq n\binom{2m/n}{2} \tag{5}$$

onde a primeira soma é sobre todos os pares de vértices no grafo, a igualdade é justificada por um argumento de contagem dupla e a desigualdade se deve à convexidade da função $f(x) = \binom{x}{2} = \frac{x(x-1)}{2}$.

Usando isto, podemos contar o número de C_4's contidos em G:

$$\begin{aligned}
\#\, C_4\text{'s em } G &= \frac{1}{2} \sum_{\{x,y\}} \binom{t(\{x,y\})}{2} \\
&\geq \frac{1}{2}\binom{n}{2}\binom{\sum_{\{x,y\}} t(\{x,y\})/\binom{n}{2}}{2} \\
&\geq \frac{1}{2}\binom{n}{2}\binom{n\binom{2m/n}{2}/\binom{n}{2}}{2} \\
&\geq \frac{2m^4}{n^4} - \frac{3m^2}{2n}
\end{aligned}$$

onde contamos cada C_4 a partir de seus pares de vértices opostos (somando sobre todos os pares de vértices do grafo) e em seguida usamos novamente a convexidade de $\binom{x}{2}$ e a equação (5).

Contando o número de elementos do conjunto $X = \{(e, C) \,:\, e \in E, C \simeq C_4 \subset G,\ e \in C\}$ de duas formas, a partir das arestas e a partir dos C_4's, obtemos:

$$\sum_{e \in E} [\#\, C_4\text{'s que contêm } e] = |X| \geq \frac{8m^4}{n^4} - \frac{6m^2}{n}$$

Dividindo tudo por m, temos a média do número de C_4's que contêm cada aresta, e portanto existe uma aresta contida em pelo menos $\frac{8m^3}{n^4} - \frac{6m}{n}$ C_4's.

A prova de (ii) é semelhante, apenas restringimos a soma sobre os $\{x, y\}$ não adjacentes. ■

Lema 4.10. Seja $W \subset V(G)$ tal que $G[W]$ pode ser feito bipartido removendo-se δ arestas. Então G pode ser feito bipartido removendo-se no máximo $\frac{1}{2}e(G) - \frac{1}{2}e(G[W]) + \delta$ arestas.

Demonstração.

Seja (W_1, W_2) uma partição de W com $e(G[W_1]) + e(G[W_2]) \leq \delta$ e seja (U_1, U_2) uma partição de $U = V \backslash W$ tal que $e(G[U_1]) + e(G[U_2]) \leq e(G[U])/2$ (que existe pelo Fato 4.2).

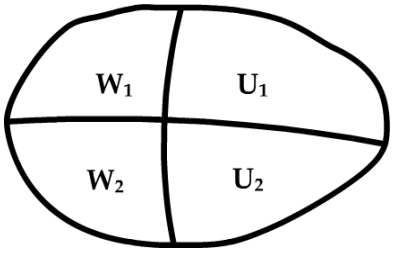

Figura 15: $V(G)$ divido em 4 partes.

Consideremos as partições $(W_1 \cup U_1, W_2 \cup U_2)$ e $(W_1 \cup U_2, W_2 \cup U_1)$ de $V(G)$. Em média, o

número de arestas que precisam ser removidas para tornar G bipartido com estas partições é:

$$\begin{aligned}
&\frac{1}{2}\left[(e(W_1 \cup U_1) + e(W_2 \cup U_2)) + (e(W_1 \cup U_2) + e(W_2 \cup U_1))\right] \\
&= \frac{1}{2}\left(e(G) + 2e(U_1)_2 e(U_2) - e(U) + 2e(W_1) + 2e(W_2) - e(W)\right) \\
&\leq \frac{1}{2}e(G) + \delta - \frac{e(W)}{2}
\end{aligned}$$

E portanto uma destas partições nos dá o resultado desejado. ■

Demonstração. (Teorema 4.7)

Pelo Lema 4.8, sabemos que G pode ser feito bipartido com a remoção de no máximo $m - \frac{4m^2}{n^2}$ arestas. Se $m \geq \frac{n^2}{6}$, segue que $m - \frac{4m^2}{n^2} \leq \frac{n^2}{18}$ e obtemos o resultado.

Consideremos então, $m < \frac{n^2}{6}$.

Pelo item (ii) do Lema 4.9, existe uma aresta $xy \in E$ contida em pelo menos $\frac{4m(2m^2-n^3)}{n^2(n^2-2m)}C_4$'s.

Isto significa que $W = (\Gamma(x)\backslash\{y\}) \cup (\Gamma(y)\backslash\{x\})$ induz um grafo bipartido (ja que G é livre de triângulos) com pelo menos $\frac{4m(2m^2-n^3)}{n^2(n^2-2m)}$ arestas (reveja a figura 14).

Então, pelo Lema 4.10, usando este W e $\delta = 0$, G pode ser feito bipartido com a remoção de no máximo $\frac{m}{2} - \frac{2m(m^2-n^3)}{n^2(n^2-2m)}$ arestas.

Como $m < n^2/6$, pode-se mostrar que $\frac{2m(m^2-n^3)}{n^2(n^2-2m)} \leq \frac{n^2}{18} + \frac{n}{2}$ e concluímos a demonstração.

■

5 Grupos, Números e a Conjectura de Artin

19/05/2015 - Bruno Pasqualotto Cavalar

Toda fração possui uma representação decimal, eventualmente uma dízima periódica. Por exemplo:

$$\frac{1}{11} = 0,\overline{09} \qquad \frac{1}{7} = 0,\overline{142857}$$

Mais geralmente, se p é primo e diferente de 2 ou 5, $\frac{1}{p}$ é uma dízima periódica da forma $\frac{1}{p} = 0,\overline{a_1...a_k}$.

Manipulando a dízima, podemos escrever:

$$\begin{aligned}
&\frac{1}{p} = 0,\overline{a_1...a_k} = \left(\frac{a_1}{10} + ... + \frac{a_k}{10^k}\right).\left(1 + \frac{1}{10^k} + \frac{1}{10^{2k}} + ...\right) = M.\frac{1}{1-\frac{1}{10^k}} = \frac{M10^k}{10^k - 1} \\
&\Rightarrow 10^k - 1 = c.p \\
&\Rightarrow 10^k \equiv 1 \pmod{p}
\end{aligned}$$

Com mais cuidado, podemos ver que k, o período da dízima, é o menor inteiro tal que 10^k é congruente a 1, módulo p. Pelo pequeno teorema de Fermat, sabemos que $p-1$ possui essa propriedade. Se $k = p - 1$, então dizemos que 10 é uma raiz primitiva módulo p (portanto 10 é raiz primitiva módulo 7, mas não módulo 11).

A conjectura de Artin diz (em particular) que 10 é raiz primitiva de infinitos números primos e mais: que isto ocorre com aproximadamente $3/8$ dos números primos.

Explicaremos melhor todos estes conceitos adiante. Comecemos revisando algumas definições e conceitos básicos de Teoria dos Números.

5.1 Revisão de Teoria dos Números

Definição 5.1. Dados inteiros d e a, dizemos que d *divide* a e denotamos $d|a$ se existir $q \in \mathbb{Z}$ tal que $a = d.q$.

Definição 5.2. Dados inteiros a e b, definimos o *máximo divisor comum* de a e b como $\mathrm{mdc}(a,b) := \max\{d \in \mathbb{Z} \ : \ d|a, \ d|b\}$.

Definição 5.3. Se a e b são inteiros tais que $\mathrm{mdc}(a,b) = 1$, dizemos que a e b são *primos entre si*.

O seguinte lema é muito usado:

Lema 5.4 (Bézout)**.** Dados $a, b \in \mathbb{Z}$, $d = \mathrm{mdc}(a,b)$ se, e somente se, existem $x, y \in \mathbb{Z}$ tais que $xa + yb = d$ e d é o menor inteiro positivo com essa propriedade.

Lema 5.5. Se $d|ab$ e $\mathrm{mdc}(d,a) = 1$, então $d|b$.

Lema 5.6. Se $\mathrm{mdc}(a,b) = 1$, $a|c$ e $b|c$, então $ab|c$.

Proposição 5.7 (Algoritmo da divisão)**.** Dados $a, b \in \mathbb{Z}$, existem únicos $q, r \in \mathbb{Z}$ tais que $a = qb + r$, com $0 \leq r < b$.

Definição 5.8. Dados $a, b, n \in \mathbb{Z}$, dizemos que a é *congruente* à b *módulo* n e denotamos $a \equiv b \pmod{n}$ se $n|(b-a)$, ou de maneira equivalente, se a tem o mesmo resto que b, quando divididos por n.

Teorema 5.9 (Teorema Fundamental da Aritmética)
Se $n \in \mathbb{Z}$, existem $p_1, ..., p_k$ primos distintos e $r_1, ..., r_n \in \mathbb{Z}_+$ tais que $n = p_1^{r_1}...p_k^{r_k}$. Essa representação é única a menos de permutações entre os fatores.

5.2 Introdução à Teoria dos Grupos

Definição 5.10. Um *grupo* $(G, \cdot)$ é formado por um conjunto G munido de uma operação $\cdot$ com as seguintes propriedades:

- *(Associatividade)* $\forall a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- *(Identidade)* $\exists e \in G$ tal que $\forall a \in G, \ e \cdot a = a \cdot e = a$.
- *(Inverso)* $\forall a \in G, \ \exists a^{-1} \in G$ tal que $a^{-1} \cdot a = a \cdot a^{-1} = e$.

Muitas vezes denotamos o grupo simplesmente pelo seu conjunto de elementos G.

Alguns exemplos de grupos:

1. $(S_n, \circ)$ Chamado grupo simétrico, composto pelas permutações de n elementos, com a operação de composição.

2. $(\mathbb{Z}, +)$ O grupo dos números inteiros, com a operação de soma.

3. $(\mathbb{Z}/n\mathbb{Z}, +)$ O grupo dos inteiros módulo n, com a operação de soma.

4. $((\mathbb{Z}/n\mathbb{Z})^*, .)$ O grupo dos inteiros primos com n, módulo n, com a operação de multiplicação.

Este último exemplo será importante no resto desta seção. Vejamos em detalhes que $(\mathbb{Z}/n\mathbb{Z})^*$ é de fato um grupo com a operação de multiplicação:

Proposição 5.11. O conjunto $(\mathbb{Z}/n\mathbb{Z})^* := \{a \pmod n \mid \mathrm{mdc}(a, n) = 1\}$ com a operação de multiplicação é um grupo e $(\mathbb{Z}/n\mathbb{Z})^* = \{a \pmod n \mid \exists x \in \mathbb{Z}, ax \equiv 1 \pmod n\}$.

Demonstração.

A operação está bem definida, pois se $a, b \in (\mathbb{Z}/n\mathbb{Z})^*$, temos que existem $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ tais que $1 = x_1a + y_1n = x_2b + y_2n$. Multiplicando, obtemos $1 = (x_1x_2)ab + (x_1y_2a + y_1x_2b + y_1y_2n)n$ e portanto $\mathrm{mdc}(ab, n) = 1$ e $ab \in (\mathbb{Z}/n\mathbb{Z})^*$.

As propriedades de associatividade e identidade são de fácil verificação, vejamos a existência de inverso: se $a \in (\mathbb{Z}/n\mathbb{Z})^*$, então existem $x, y \in \mathbb{Z}$ tais que $xa + yn = 1$ e logo $a^{-1} = x$ e $ax \equiv 1 \pmod n$, o que também prova a última afirmação da proposição. ■

O lema a seguir segue facilmente das propriedades que definem um grupo:

Lema 5.12. Se $(G, \cdot)$ é um grupo e $a, b, u \in G$, então:

1. $ua = ub \Rightarrow a = b$

2. $au = bu \Rightarrow a = b$

3. $(ab)^{-1} = b^{-1}a^{-1}$

Definição 5.13. Se G é um grupo e $H \subset G$, dizemos que H é um *subgrupo* de G e denotamos $H \leq G$ se H for um grupo com relação à mesma operação de G.

Lema 5.14. $H \leq G \Leftrightarrow \forall a, b \in H$ temos $ab \in H$ e $a^{-1} \in H$.

Proposição 5.15. Se G é finito, $H \subset G$ e $\forall a, b \in H$, $ab \in H$, então H é um subgrupo de G.

Demonstração.

Se $H = \{e\}$, a afirmação é verdadeira. Caso contrário, seja $a \in H$, $a \neq e$. Considere $A = \{a, a^2, a^3, ...\}$. Como G é finito, A também é e $\exists i, j \in \mathbb{Z}$, $i < j$ tais que $a^i = a^j \Rightarrow e = a^{j-i} \Rightarrow a.a^{j-i-1} = e \Rightarrow a^{-1} = a^{j-i-1} \in H$, pois $j - i > 1$ ($a \neq e$) e $j - i - 1 \geq 1$.

■

Definição 5.16. Dado $a \in G$, o conjunto $\langle a \rangle := \{a^k \ : \ k \in \mathbb{Z}\}$ é o *subgrupo cíclico gerado* por a. Dizemos que um grupo H é *cíclico* se existe $a \in H$ tal que $H = \langle a \rangle$. Neste caso, chamamos a de *gerador* do grupo H.

Definição 5.17. Se G for um grupo finito, definimos a *ordem* de G como $o(G) := |G|$.

Definição 5.18. Se $a \in G$, definimos a ordem de a, $o(a) := \min\{m \in \mathbb{Z}_+ \ : \ a^m = e\}$.

Lema 5.19. Se G é um grupo finito e $a \in G$, $o(a) = o(\langle a \rangle)$.

Definição 5.20. Se $H \leq G$, escrevemos $a \equiv b \pmod H \Leftrightarrow ab^{-1} \in H$.

Observação 5.21. Note que a definição anterior é uma extensão da definição 5.8, de congruência. G é o grupo $(\mathbb{Z}, +)$ e H o subgrupo $(n\mathbb{Z}, +)$, dos inteiros múltiplos de n.

Lema 5.22. A relação $\equiv$ é uma relação de equivalência.

Definição 5.23. Dado $a \in G$, $H \leq G$, definimos a *coclasse* (ou *classe lateral*) de a com relação à H como $Ha := \{ha \mid h \in H\}$.

Lema 5.24. Ha é a classe de equivalência de a, com respeito à relação $\equiv$.

Demonstração.

Denotemos por $[a]$ a classe de a.

$Ha \subset [a]$. Para todo $h \in H$, $a(ha)^{-1} = aa^{-1}h^{-1} = h^{-1} \in H \Rightarrow a \equiv ha \pmod H \Rightarrow ha \in [a] \forall h \in H$.

$[a] \subset Ha$. Se $x \in [a]$, $ax^{-}1 \in H \Rightarrow (ax^{-1})^{-1} \in H \Rightarrow xa^{-1} \in H \Rightarrow \exists h = xa^{-1} \in H$ tal que $ha = x \Rightarrow x \in Ha$. ■

Lema 5.25. Existe uma bijeção entre quaisquer coclasses de H em G e portanto elas têm o mesmo número de elementos. Como $|He| = |H|$, $|Ha| = |H|$, $\forall a \in G$.

Demonstração.

Sejam $a, b \in G$ e considere $\varphi : Ha \to Hb$, $\varphi(ha) = hb$. φ é claramente sobrejetora. Como $h_1 b = h_2 b \Rightarrow h_1 = h_2 \Rightarrow h_1 a = h_2 a$, φ é injetora. ■

O próximo teorema exerce um papel fundamental na teoria dos grupos finitos e possui diversas consequências importantes.

Teorema 5.26 (Teorema de Lagrange)
Se G é um grupo finito e $H \leq G$, então $o(H)|o(G)$.

Demonstração.

Seja k o número de coclasses de H, como todas têm tamanho igual a $o(H)$, $o(G) = k.o(H)$ e o teorema segue. ■

Corolário 5.27. Se G é um grupo finito e $a \in G$, então $o(a)|o(G)$.

Corolário 5.28. Se G é um grupo finito e $a \in G$, então $a^{o(G)} = e$.

Demonstração.

Como $o(a)|o(G)$, existe $m \in \mathbb{Z}$ tal que $o(G) = m.o(a) \Rightarrow a^{o(G)} = (a^{o(a)})^m = e^m = e$. ■

Corolário 5.29. Se G é um grupo finito, $a \in G$ e $a^m = e$, então $o(a)|m$.

Demonstração.

Pelo algoritmo da divisão (proposição 5.7), existem $q, r \in \mathbb{Z},\ 0 \leq r < o(a)$ tais que $m = o(a).q + r$. Como $e = a^m = a^{o(a)q+r} = a^r$, pela definição de $o(a)$, temos que $r = 0$ ou $r \geq o(a)$. Pela forma como r foi escolhido, $r = 0$. ■

5.3 A função ϕ de Euler

Definição 5.30. Dado $n \in \mathbb{Z}_+$, definimos a *função ϕ de Euler* como o número de inteiros primos com n e menores que n:

$$\phi(n) = o((\mathbb{Z}/n\mathbb{Z})^*)$$

Essa função é muito usada em teoria dos números e possui diversas propriedades, vejamos algumas:

Proposição 5.31 (Fatos sobre $\phi(n)$)**.**

1. Se p é primo e $n \in \mathbb{Z}_+$, $\phi(p^n) = p^n - p^{n-1}$.
2. Se $m, n \in \mathbb{Z}_+$ e $\mathrm{mdc}(m, n) = 1$, então $\phi(mn) = \phi(m)\phi(n)$.
3. $\forall n \in \mathbb{Z}_+,\ \sum_{\substack{d>0 \\ d|n}} \phi(d) = n$.

Demonstração.

1. Queremos contar $|\{a \ :\ 0 \leq a \leq p^n - 1,\ \mathrm{mdc}(a, p^n) = 1\}|$. Para isso, podemos contar quantos números não são primos com p^n e subtrair de p^n. Mas se $\mathrm{mdc}(a, p^n) \neq 1$, $a = k.p$ com $0 \leq k \leq (p^{n-1} - 1)$. Portanto, $\phi(p^n) = p^n - p^{n-1}$.
2. Sejam $m, n \in \mathbb{Z}_+,\ \mathrm{mdc}(m, n) = 1$.

   Considere $T : (\mathbb{Z}/mn\mathbb{Z}) \to (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$, $T(a \pmod{mn}) = (a \pmod{m}, a \pmod{n})$.

   T está bem definida, pois se $a \equiv b \pmod{mn} \Rightarrow mn|(a-b) \Rightarrow m|(a-b)$ e $n|(a-b) \Rightarrow a \equiv b \pmod{m}$ e $a \equiv b \pmod{n}$.

   T é injetora, pois se $T(a \pmod{mn}) = T(b \pmod{mn}) \Rightarrow a \equiv b \pmod{m}$ e $a \equiv b \pmod{n} \Rightarrow m|(b-a)$ e $n|(b-a) \overset{\text{Lema } 5.6}{\Rightarrow} mn|(b-a) \Rightarrow a \equiv b \pmod{mn}$.

   Como o domínio e o contra-domínio de T possuem a mesma cardinalidade, concluímos que T é bijetora.

   Agora, a é primo com mn se, e somente se, a é primo com m e a é primo com n. Para vermos a ida, basta usar o fato de que existem $x, y \in \mathbb{Z}$ tais que $xa + ymn = 1$. Para a volta, temos que existem $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ tais que $x_1a + y_1m = 1$ e $x_2a + y_2n = 1$ e multiplicando, obtemos $(y_1y_2)mn + (ax_1x_2 + x_1y_2n + y_1x_2m)a = 1$.

   Concluímos, então, que existe uma bijeção entre $(\mathbb{Z}/mn\mathbb{Z})^*$ e $(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$, logo estes conjuntos têm a mesma cardinalidade e $\phi(mn) = \phi(m)\phi(n)$.

3. Pelo teorema fundamental da aritmética, existem primos $p_1, ..., p_k$ distintos e $r_1, ..., r_k \in \mathbb{Z}_+$ tais que $n = p_1^{r_1}...p_k^{r_k}$. Provaremos a afirmação por indução em k.

   Se $k = 1$, temos $n = p^r$ e $d|n \Leftrightarrow d = p^s$, com $0 \leq s \leq r$. Mas $\sum_{\substack{d>0 \\ d|n}} \phi(d) = 1 + \sum_{\substack{d>1 \\ d|n}} \phi(d) = 1 + \sum_{s=1}^{r}(p^s - p^{s-1}) = 1 + p^r - 1 = p^r = n$.

   Se $k > 1$, temos $n = p_1^{r_1}...p_k^{r_k}$ e $d|n \Leftrightarrow d = p_1^{s_1}...p_k^{s_k}$, com $s_i \in \mathbb{Z},\ 0 \leq s_i \leq r_i$ e $1 \leq i \leq k$. Mas $\sum_{\substack{d>0 \\ d|n}} \phi(d) = \sum_{s_1=0}^{r_1} ... \sum_{s_k=0}^{r_k} \phi(p_1^{s_1}...p_k^{s_k}) = \sum_{s_1=0}^{r_1} ... \sum_{s_k=0}^{r_k} \phi(p_1^{s_1}...p_{k-1}^{s_{k-1}})\phi(p_k^{s_k}) = \left(\sum_{s_k=0}^{r_k} \phi(p_k^{s_k})\right) \cdot \left(\sum_{s_1=0}^{r_1} ... \sum_{s_{k-1}=0}^{r_{k-1}} \phi(p_1^{s_1}...p_{k-1}^{s_{k-1}})\right) \overset{HI}{=} (p_k^{r_k}).(p_1^{r_1}...p_{k-1}^{r_{k-1}}) = n$.

■

A seguir, mais um corolário do Teorema de Lagrange (5.26), muito usado em teoria dos números.

Teorema 5.32 (Pequeno Teorema de Fermat)
Se $n \in \mathbb{Z}_+$ e $\text{mdc}(a, n) = 1$, então $a^{\phi(n)} \equiv 1 \pmod{n}$. Em particular, se $n = p$ primo e $p \nmid a$, $a^{p-1} \equiv 1 \pmod{p}$.

Demonstração.
Segue diretamente do corolário 5.28 aplicado ao grupo $(\mathbb{Z}/n\mathbb{Z})^*$. ■

5.4 Raízes primitivas e a Conjectura de Artin

Finalmente, estamos em condições de definir o que é uma raiz primitiva e apresentar a conjectura de Artin.

Definição 5.33. Se $(\mathbb{Z}/n\mathbb{Z})^*$ é cíclico e $(\mathbb{Z}/n\mathbb{Z})^* = \langle g \rangle$, então g é *raiz primitiva* módulo n.

Conjectura 5.34 (Artin)**.** Todo $a \in \mathbb{Z}$, $a \neq -1$ e que não é um quadrado perfeito, isto é, $a \neq n^2, n \in \mathbb{Z}$ é raiz primitiva de $A \simeq 0,379...$ dos primos.

Sendo que essa proporção é formalizada com o conceito de densidade assimtótica, isto é:

$$\lim_{n\to\infty} \frac{|\{p \ : \ 1 < p \leq n, p \text{ é primo e } a \text{ é raiz primitiva de } p\}|}{|\{p \ : \ 1 < p \leq n \text{ e } p \text{ é primo}\}|}$$

e $A = \prod_{p \text{ primo}} \left(1 - \frac{1}{p(p-1)}\right)$.

26/05/2015 - Bruno Pasqualotto Cavalar

Observação 5.35. É necessário excluir os quadrados perfeitos da conjectura de Artin porque se $a = h^2,\ h \in \mathbb{Z}$ e $a \not\equiv 0 \pmod{p}$, temos $a^{\frac{p-1}{2}} \equiv h^{p-1} \equiv 1 \pmod{p}$ (pelo pequeno teorema de Fermat, 5.32) $\Rightarrow o(a) \leq \frac{p-1}{2}$ e $\langle a \rangle \neq (\mathbb{Z}/p\mathbb{Z})^*$.

Definição 5.36. Sejam G e $\bar{G}$ grupos. Se $\varphi : G \to \bar{G}$ é tal que $\varphi(ab) = \varphi(a)\varphi(b) \forall a, b \in G$ dizemos que φ é um *homeomorfismo*. Se φ for bijetora, dizemos que φ é um *isomorfismo*, que os grupos G e $\bar{G}$ são *isomorfos* e denotamos $G \simeq \bar{G}$.

Lema 5.37. Se G é finito, cíclico e $o(G) = d$, então $G \simeq (\mathbb{Z}/d\mathbb{Z})$.

Demonstração.

Como G é cíclico, existe $g \in G$ tal que $\langle g \rangle = G$. Considere $T : G \to \mathbb{Z}/d\mathbb{Z},\ T(g^n) = n \pmod{d}$.

T está bem definida, pois se $g^a = g^b$ e $a < b \Rightarrow e = g^{b-a} \Rightarrow o(g)|b-a \Rightarrow d|b-a \Rightarrow a \equiv b \pmod{d}$.

T é injetora, pois se $a \equiv b \pmod{d}$, então $d|b-a \Rightarrow b-a = kd,\ k \in \mathbb{Z} \Rightarrow g^{b-a} = g^{kd} = e \Rightarrow g^b = g^a$.

Como o domínio e a imagem são finitos e possuem mesma cardinalidade, T é bijetora.

T é um isomorfimo, pois $T(g^a g^b) = T(g^{a+b}) = (a+b) \pmod{d} = (a \pmod{d}) + (b \pmod{d})$. ■

Lema 5.38. Se $G \simeq U$, o número de elementos de ordem d em G e U são iguais.

Demonstração.

Seja $\varphi : G \to U$ o isomorfismo e seja $x \in G$ com $o(x) = d$.

Temos $x^d = e_G \Rightarrow \varphi(x^d) = e_U \Rightarrow (\varphi(x))^d = e_u$.

Como φ^{-1} é injetiva, se $o(\varphi(x)) \neq d$, obteríamos $o(x) \neq d$, contradição. Logo, φ é uma bijeção entre $\{x \in G\ :\ o(x) = d\}$ e $\{y \in U\ :\ o(y) = d\}$ e estes conjuntos possuem a mesma cardinalidade. ■

Lema 5.39. O grupo $(\mathbb{Z}/d\mathbb{Z}, +)$ tem $\phi(d)$ elementos de ordem d.

Demonstração.

Seja $a \in \mathbb{Z},\ 0 < a < d$ tal que $\mathrm{mdc}(a,d) = 1$. Afirmamos que $o(a) = d$, pois caso contrário, existira $k \in \mathbb{Z}, 0 < k < d$ tal que $ka \equiv 0 \pmod{d} \Rightarrow d|ka \Rightarrow d|k$, o que não é possível. Portanto, $\mathbb{Z}/d\mathbb{Z}$ possui pelo menos $\phi(d)$ elementos de ordem d.

Se $\mathrm{mdc}(a,d) > 1$, temos que $a\frac{d}{\mathrm{mdc}(a,d)} = \frac{a}{\mathrm{mdc}(a.d)}d \equiv 0 \pmod{d} \Rightarrow o(a) < d$.

Portanto $\mathbb{Z}/d\mathbb{Z}$ possui exatamente $\phi(d)$ elementos. ■

Corolário 5.40. Se G é finito, cíclico e $o(G) = d$, então G tem $\phi(d)$ elementos de ordem d.

A seguir, algumas definições que precisaremos para enunciar um lema usado na prova do teorema 5.46.

Definição 5.41. Um *corpo* é uma estrutura algébrica constituída pela tripla $(\mathbb{K}, +, .)$, onde $\mathbb{K}$ é um conjunto e $+, .$ são duas operações (chamadas de soma e multiplicação) que satisfazem as propriedades:

1. ($+$ associativa) $a + (b + c) = (a + b) + c\ \forall a, b, c \in \mathbb{K}$.
2. ($+$ comutativa) $a + b = b + a\ \forall a, b \in \mathbb{K}$.
3. (elemento neutro aditivo) $\exists 0 \in \mathbb{K}$ tal que $0 + a = a\ \forall a \in \mathbb{K}$.
4. (inverso aditivo) $\forall a \in \mathbb{K},\ \exists -a \in \mathbb{K}$ tal que $a + (-a) = 0$.
5. ($.$ associativo) $a(bc) = (ab)c\ \forall a, b, c \in \mathbb{K}$.
6. ($.$ comutativo) $ab = ba\ \forall a, b \in \mathbb{K}$.

7. (elemento neutro multiplicativo) $\exists 1 \in \mathbb{K}$ tal que $1a = a\ \forall a \in \mathbb{K}$.

8. (inverso multiplicativo) $\forall a \in \mathbb{K}, a \neq 0,\ \exists a^{-1} \in \mathbb{K}$ tal que $aa^{-1} = 1$.

9. (distributiva) $a(b + c) = ab + ac\ \forall a, b, c \in \mathbb{K}$.

Certamente $\mathbb{R}$ e $\mathbb{C}$ são exemplos de corpos, mas também $(\mathbb{Z}/p\mathbb{Z}, +, .)$ é um corpo se p for primo.

Definição 5.42. Se $\mathbb{K}$ é um corpo, denotamos por $\mathbb{K}[x]$ seu *anel de polinômios*[10] na variável x.

Definição 5.43. Se $p \in \mathbb{K}[x]$, defimos seu *grau*, $\mathrm{gr}(p)$, como o maior expoente da variável x em p.

Definição 5.44. Dizemos que $a \in \mathbb{K}$ é uma *raiz* de $p \in \mathbb{K}[x]$, se $p(a) = 0$.

Enunciaremos o próximo lema sem demonstração, porém observamos que esta está ligada à um algoritmo de divisão entre polinômios, semelhante à divisão entre inteiros (5.7).

Lema 5.45. Se $\mathbb{K}$ é um corpo, $p \in \mathbb{K}[x]$ e $\mathrm{gr}(p) = d$, então p tem no máximo d raízes em $\mathbb{K}$.

Teorema 5.46
O grupo $((\mathbb{Z}/p\mathbb{Z})^*, .)$ é cíclico para todo primo p.

Demonstração.

Considere $\psi(d) = \#\{a \in (\mathbb{Z}/d\mathbb{Z})^* \ :\ o(a) = d\}$. Queremos mostrar que $\psi(p-1) \neq 0$.

Considere um $d|p-1$ tal que $\psi(d) \neq 0$. Logo $\exists x \in (\mathbb{Z}/p\mathbb{Z})^*$ com $o(x) = d$. Para todo $y \in \langle x \rangle$, $y^d \equiv 1 \pmod{p}$. Como $T^d \equiv 1 \pmod{p}$ tem no máximo d soluções em $\mathbb{Z}/p\mathbb{Z}$, todo elemento de ordem d está em $\langle x \rangle$.

Portanto $\psi(d) = \phi(d)$, se $\psi(d) \neq 0$. Como $p - 1 = \sum_{\substack{d|p-1 \\ d>0}} \psi(d) \leq \sum_{\substack{d|p-1 \\ d>0}} \phi(d) = p - 1$, $\psi(d) = \phi(d)\ \forall d|p-1$. Em particular, $\psi(p-1) = \phi(p-1) > 0$. ■

Vejamos agora um "argumento heurístico" a favor da conjectura de Artin.

Fixe $a \in \mathbb{Z}$. Para cada primo p, seja $g_p \in (\mathbb{Z}/p\mathbb{Z})^*$ uma raiz primitiva módulo p e seja $m \in \mathbb{N}$ tal que $g_p^m \equiv a \pmod{p}$. Considere $G_p := \mathrm{mdc}(m, p-1)$.

Afirmação 5.47. $\langle a \rangle = (\mathbb{Z}/p\mathbb{Z})^* \Leftrightarrow G_p = 1$.

Demonstração.

($\Rightarrow$) Suponha $G_p > 1$, então $a^{\frac{p-1}{G_p}} \equiv (g^m)^{\frac{p-1}{G_p}} \equiv (g^{\frac{m}{G_p}})^{p-1} \equiv 1 \pmod{p}$. Portanto $o(a) < p-1$ e $\langle a \rangle \neq (\mathbb{Z}/p\mathbb{Z})^*$.

($\Leftarrow$) Se $G_p = 1$, suponha que exista $k \in \mathbb{Z},\ 0 < k < p-1$ tal que $a^k \equiv 1 \pmod{p}$. Então $g^{mk} \equiv 1 \pmod{p} \Rightarrow p-1|mk \Rightarrow p-1|k$, contradição. ■

[10] *Anel* é uma outra estrutura algébrica, muito estudada, semelhante a um corpo, porém sem a exigência do inverso multiplicativo. $\mathbb{Z}$ é um exemplo de anel e é claro que todo corpo $\mathbb{K}$ também é um anel. Os polinômios de $\mathbb{K}$ na variável x, com as operações usuais, são outro exemplo de anel.

Portanto, a é raiz primitiva módulo p se, e somente se, não existir l primo tal que $l|G_p$.

Agora, fixado um p e um l, qual a probabilidade de l dividir G_p? Isso ocorre se l dividir m e $p-1$. Assumindo que m pode ser qualquer número módulo l e $p-1$ qualquer coisa diferente de $l-1$ módulo l (pois $l \neq p \Rightarrow p \not\equiv 0 \pmod{l}$), a probabilidade disso acontecer é $\frac{1}{l(l-1)}$.

Portanto, a probabilidade de $l \nmid G_p$ para nenhum l primo (assumindo que essa probabilidade seja independente entre diferentes l - o que não deve ser verdade) é:

$$A = \prod_{l \text{ primo}} \left(1 - \frac{1}{l(l-1)}\right)$$

6 Conexões entre Topologia e Combinatória

26/05/2015 - Gabriel Bonuccelli Heringer Lisboa

Nesta seção, tentaremos relacionar objetos combinatoriais com espaços topológicos usando diversos teoremas que possibilitam conexões entre essas áreas.

Comecemos com algumas definições básicas de topologia.

6.1 Introdução à Topologia

Definição 6.1. Um *espaço topológico* é um conjunto X com um sistema $\tau \subseteq 2^X = \mathcal{P}(X)$ que satisfaz:

- $\emptyset, X \in \tau$.
- A intersecção de qualquer família finita de elementos de τ pertence à τ.
- A união de qualquer família arbitrária de elementos de τ pertence à τ.

Os conjuntos de τ são chamados *abertos*.

Um conjunto é dito *fechado* se seu complementar é aberto.

Uma *vizinhança* de um elemento $x \in X$ é um conjunto aberto que contém x.

Como exemplos de espaços topológicos, temos:

1. $\mathbb{R}$ com o sistema usual de abertos ($A \subset \mathbb{R}$ é aberto se $\forall a \in A,\ \exists \epsilon > 0$ tal que $(a-\epsilon, a+\epsilon) \subset A$).
2. $\mathbb{R}^n$, também com o sistema usual de abertos ($A \subset \mathbb{R}^n$ é aberto se $\forall a \in A,\ \exists \epsilon > 0$ tal que $\{x \in \mathbb{R}^n \ :\ \|x-a\| < \epsilon\} \subset A$).
3. X e $\tau = \{\emptyset, X\}$. (topologia trivial)
4. X e $\tau = \mathcal{P}(X)$. (topologia discreta)
5. $X = \{1,2,3,4\}$ e $\tau = \{\emptyset, \{2\}, \{3\}, \{2,3\}, \{1,2,3\}, \{1,2,3,4\}\}$.

Por outro lado, não é um espaço topológico $X = \mathbb{Z}$ e τ a família de todos os subconjuntos finitos de $\mathbb{Z}$, além do próprio $\mathbb{Z}$. Pois se fosse, pelos axiomas de espaço topológico, $A = \bigcup_{a \neq 0}\{a\} = \mathbb{Z}\backslash\{0\} \in \tau$, mas A é infinito, contradição.

Definição 6.2. Uma família $\tau' \subset \tau$ é uma *base* de um espaço topológico se qualquer elemento de τ pode ser escrito como uma união de elementos de τ'.

Definição 6.3. Seja (X, τ) um espaço topológico e $Y \subset X$. A *topologia induzida* por Y é $(Y, \{Y \cap U \ : \ U \in \tau\})$. Pode-se verificar que isto de fato é uma topologia.

Definição 6.4. Sejam (X_1, τ_1) e (X_2, τ_2) dois espaços topológicos. Uma função $f : X_1 \to X_2$ é dita *contínua* se a pré-imagem de qualquer conjunto aberto é aberto. Em símbolos, $\forall U \in \tau_2, \ f^{-1}(U) \in \tau_1$.

Observação 6.5. É interessante observar que esta definição generaliza a definição de função contínua entre $\mathbb{R}$ e $\mathbb{R}$ vista no curso de cálculo. De fato, dado um aberto $U \subset \mathbb{R}$ e $x \in \mathbb{R}$ tal que $f(x) \in U$, pela definição de aberto de $\mathbb{R}$ (exemplo 1), existe $\epsilon > 0$ tal que $(f(x) - \epsilon, f(x) + \epsilon) \subset U$ e pela definição de continuidade do cálculo, existe $\delta > 0$ tal que $f((x - \delta, x + \delta)) \subset (f(x) - \epsilon, f(x) + \epsilon) \subset U$. Isto é, provamos que para todo $x \in f^{-1}(U)$, existe $\delta > 0$ tal que $(x - \delta, x + \delta) \subset f^{-1}(U)$ e portanto $f^{-1}(U)$ é aberto.

02/06/2015 - Gabriel Bonuccelli Heringer Lisboa

Proposição 6.6. Uma função entre dois espaços topológicos é contínua se, e somente se, a pré-imagem de qualquer conjunto fechado é fechada.

Teorema 6.7

Sejam X e Y dois espaços topológicos e suponha que $X = X_1 \cup ... \cup X_n$, com X_i fechado para todo $i \in \{1, ..., n\}$.

Seja $f : X \to Y$. f é contínua em $X \Leftrightarrow f_i := f|_{X_i}$ é contínua em X_i para todo $i \in \{1, ..., n\}$.

Demonstração.

($\Rightarrow$) Fixe $i \in \{1, ..., n\}$, vamos provar que $f_i : X_i \to Y$ é contínua. Tome um aberto $U \subset Y$ e note que $f_i^{-1}(U) = \{x \in X_i \ : \ f_i(x) \in U\} = \{x \in X_i \ : \ f(x) \in U\} = X_i \cap f^{-1}(U)$ é aberto na topologia induzida por X_i, pois estamos supondo f contínua e logo $f^{-1}(U)$ é aberto em X.

($\Leftarrow$) Tome $U \subset Y$ fechado. Para cada $i \in \{1, ..., n\}$, temos que f_i é contínua e pela proposição 6.6, $f_i^{-1}(U) = f^{-1}(U) \cap X_i =: C_i$ é fechado em X_i. Logo, existe um subconjunto C_i' fechado em X tal que $C_i = C_i' \cap X_i$ (pela definição de topologia induzida adaptada à fechados). Como C_i' e X_i são fechados em X, C_i também o é. Como $f^{-1}(U) = C_1 \cup ... \cup C_n$, concluímos que $f^{-1}(U)$ é fechado e portanto f é contínua (novamente pela proposição 6.6). ■

Definição 6.8. Uma função $\varphi : A \to B$ é um *homeomorfismo* se é uma bijeção e tanto φ quanto φ^{-1} são contínuas.

Dizemos que dois espaços A e B são *homeomorfos* se existir um homeomorfismo entre eles e escrevemos $A \sim B$.

Como exemplo, temos que $\mathbb{R} \sim (0, 1)$. Um homeomorfismo é $f : \mathbb{R} \to (0, 1)$, definida por $f(x) = \frac{1}{\pi} \tan^{-1}(x) + \frac{1}{2}$ e sua inversa $f^{-1}(x) = \tan(\pi(x - \frac{1}{2}))$ (veja a figura 16).

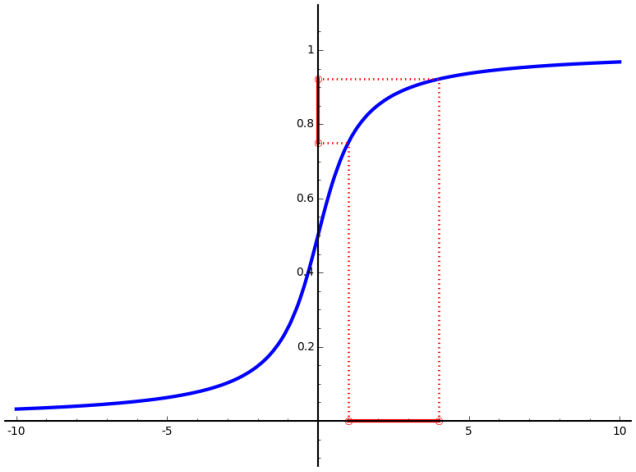

Figura 16: O gráfico do homeomorfismo. Observe como a função mapeia os abertos de $\mathbb{R}$ em abertos de $(0, 1)$.

Definição 6.9. Sejam X, Y espaços topológicos e $Y \subset X$. Uma *retração* de X em Y é uma função $F : X \times [0, 1] \to X$ contínua[11], tal que $F(x, 0) = x$ para todo $x \in X$, $F(y, t) = y$ para todo $y \in Y$ e todo $t \in [0, 1]$ e $F(X, 1) = Y$.

Observação 6.10. Podemos interpretar o segundo parâmetro de F como tempo e escrevendo $F(x, t) = f_t(x)$, F representa uma família de funções $f_t : X \to X$ que "deformam continuamente"o espaço X, transformando-o no Y.

Observação 6.11. Segue da definição de topologia produto (veja a nota 11) que se escolhemos $x \in X$ e $t \in (0, 1)$ e uma vizinhança V aberta de $F(x, t)$, existem $\delta > 0$ e U_x vizinhança de x em X tal que $F(x', t') \in V$ para todo $x' \in U_x$ e $t' \in (t - \delta, t + \delta)$.

Definição 6.12. Duas funções contínuas $f, g : X \to Y$ são *homotópicas* (denotamos $f \sim g$) se existe $F : X \times [0, 1] \to Y$ contínua, com $F(x, 0) = f(x)$ e $F(x, 1) = g(x)$ para todo $x \in X$.

Dizemos que $f : X \to Y$ é 0-*homotópica* se for homotópica à função constante.

Observação 6.13. Tal como na última definição, podemos interpretar a segunda coordenada de F como tempo e F como uma "interpolação contínua"entre as funções f e g.

Proposição 6.14. A relação de homotopia é uma relação de equivalência.

Funções contínuas na reta sempre são homotópicas (se $f, g : \mathbb{R} \to \mathbb{R}$ são contínuas, considere $F(x, t) = f(x) + t(g(x) - f(x))$). Portanto, para exibirmos contra-exemplos e mostrarmos funções que não sejam homotópicas, precisamos considerar espaços topológicos mais complicados.

O *toro* ou *círculo* (denotado por $\mathbb{T}$) é definido como $\mathbb{T} = \mathbb{R}/\mathbb{Z}$, isto é, o conjunto das classes de equivalência da relação sobre $\mathbb{R}$ definida como $x \sim y \Leftrightarrow x - y \in \mathbb{Z}$. $\mathbb{T}$ é um espaço topológico com base de abertos formada pelos arcos do círculo, ou igualmente, intervalos do tipo $(a, b) \subset [0, 1)$ (com $0 \leq a < b \leq 1$) e $(a, 1) \cup [0, b)$ (com $0 < b < a < 1$).

[11] Se A e B são dois espaços topológicos, definimos uma topologia em seu produto $A \times B$ com base de abertos da forma $U \times V$, com U aberto em A e V aberto em B (também devem ser considerados uniões de conjuntos dessa forma). F deve ser contínua nessa topologia.

Considere as funções $f, g : \mathbb{T} \to \mathbb{T}$ definidas como $f(x) = x\ \forall x \in \mathbb{T}$ e $g(x) = x$ se $x \in [0, 1/2]$, $g(x) = 1 - x$, se $x \in (1/2, 1)$. Afirmamos, sem demonstrar, que g é 0-homotópica, mas f não e portanto f e g não são homotópicas. Observe que $F(x, t) = (1 - t)f(x)$ não é contínua para $t \neq 0, 1$ em $(0, t) \in \mathbb{T} \times [0, 1]$.

Definição 6.15. Se X e Y são espaços topológicos, dizemos que X e Y tem o mesmo *tipo homotópico* e escrevemos $X \approx Y$ se existirem funções contínuas $f : X \to Y$ e $g : Y \to X$ tais que $f \circ g : Y \to Y \sim \mathrm{id}_Y$ e $g \circ f : X \to X \sim \mathrm{id}_X$.

Como exemplo, temos que $[0, 1] \approx \{0\}$. Considere $f : [0, 1] \to \{0\}, f(x) = 0\ \forall x \in [0, 1]$ e $g : \{0\} \to [0, 1], g(0) = 0$. $f \circ g = \mathrm{id}_{\{0\}}$ e $g \circ f \equiv 0 \sim \mathrm{id}_{[0,1]}$.

09/06/2015 - Gabriel Bonuccelli Heringer Lisboa

Na próxima seção definiremos um novo conceito, da matemática discreta, que nos auxiliará a estabelecer a relação entra esta e a topologia. Mas antes, falaremos sobre combinações afim e simplexos.

6.2 Complexos Simpliciais

Definição 6.16. Os vetores $v_1, ..., v_k \in \mathbb{R}^d$ são *afim dependentes* se existirem escalares $\alpha_1, ..., \alpha_k$ não todos nulos tais que $\sum_{i=0}^{k} \alpha_i v_i = 0$ e $\sum_{i=0}^{k} \alpha_i = 0$. Caso contrário, dizemos que os vetores são *afim independentes*.

Se $k = 1$ e $v_0 = v_1$, tomando $\alpha_0 = 1$ e $\alpha_1 = -1$, notamos que v_0, v_1 são afim dependentes. Se $v_0 \neq v_1$, suponha que existam α_0 e α_1 não ambos nulos tais que $\alpha_0 v_0 + \alpha_1 v_1 = 0$ e $\alpha_0 + \alpha_1 = 0$. Segue que $\alpha_0 = -\alpha_1$ e $\alpha_0 v_0 = \alpha_0 v_1$. Como $\alpha_0 \neq 0$, obtemos $v_0 = v_1$, contradição. Portanto, dois pontos distintos são afim independentes.

Proposição 6.17. Os vetores $v_0, v_1, ..., v_k \in \mathbb{R}^d$ são afim independentes se, e somente se, os k vetores $v_1 - v_0, v_2 - v_0, ..., v_k - v_0$ são linearmente independentes.

Demonstração.

($\Rightarrow$) Se $\lambda_1, ..., \lambda_k$ são escalares tais que $\lambda_1(v_1 - v_0) + ... + \lambda_k(v_k - v_0) = 0$, temos $(-\lambda_1 - ... - \lambda_k)v_0 + \lambda_1 v_1 + ... + \lambda_k v_k = 0$. Fazendo $\alpha_0 = -\lambda_1 - ... - \lambda_k, \alpha_1 = \lambda_1, ..., \alpha_k = \lambda_k$, observamos que $\sum_{i=0}^{k} \alpha_i = 0$ e $\sum_{i=0}^{k} \alpha_i v_i = 0$. Como, por hipótese, $v_0, v_1, ..., v_k$ são afim independentes, temos que $\alpha_i = 0$ para todo i de 0 a k. Então $\lambda_i = 0$ para todo i de 1 a k e $v_1 - v_0, ..., v_k - v_0$ são linearmente independentes.

($\Leftarrow$) Se $\alpha_0, ..., \alpha_k$ são escalares tais que $\alpha_0 v_0 + ... + \alpha_k v_k = 0$ e $\sum_{i=0}^{k} \alpha_i = 0$, queremos provar que $\alpha_0 = \alpha_1 = ... = \alpha_k = 0$. De $\sum_{i=0}^{k} \alpha_i = 0$, vem que $\alpha_0 = -\sum_{i=1}^{k} \alpha_i$. Substituindo em $\sum_{i=0}^{k} \alpha_i v_i = 0$, vem que $-(\alpha_0 + ... + \alpha_k)v_0 + \alpha_1 v_1 + ... + \alpha_k v_k = 0 \Rightarrow \alpha_1(v_1 - v_0) + ... + \alpha_k(v_k - v_0) = 0 \Rightarrow \alpha_1 = ... = \alpha_k = 0$, pois por hipótese, $v_1 - v_0, ..., v_k - v_0$ são linearmente independentes. ■

Desta proposição, vemos que três vetores são afim independentes se, e somente se, são não colineares e quatro vetores são afim independentes se, e somente se, são não coplanares.

Definição 6.18. O *fecho convexo* de um conjunto $A \subset \mathbb{R}^d$, denotado por $\mathrm{conv}(A)$, é a intersecção de todos os conjuntos convexos que contêm A.

Definição 6.19. Um n-*simplexo* σ é o fecho convexo de um conjunto $A \subset \mathbb{R}^d$ de $n+1$ pontos afim independentes.

Os pontos de A são os *vértices* de σ e a *dimensão* de σ é n.

O fecho convexo de um subconjunto dos vértices de um simplexo σ é uma *face* de σ.

O *interior relativo* de um simplexo é obtido removendo-se todas as faces com dimensão menor que a do simplexo

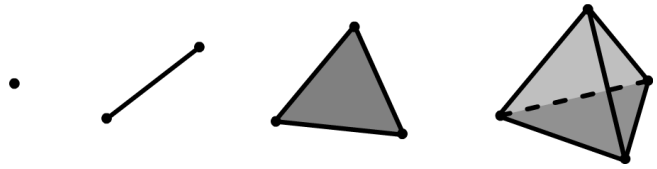

Figura 17: Exemplos de simplexos de dimensões $0, 1, 2$ e 3.

Proposição 6.20. Cada ponto $x \in \mathrm{conv}(A)$ pode ser escrito como uma combinação convexa de pontos de A, isto é, existem $x_1, ..., x_n \in A$ e escalares $\alpha_1, ..., \alpha_n \geq 0$ tais que $\sum_{i=1}^{n} \alpha_i = 1$ e $x = \sum_{i=1}^{n} \alpha_i x_i$.

Definição 6.21. Uma família não vazia Δ de simplexos é um *complexo simplicial* se:

1. Toda face de qualquer simplexo $\sigma \in \Delta$ também é um simplexo de Δ.
2. A intersecção $\sigma_1 \cap \sigma_2$ de simplexos $\sigma_1, \sigma_2 \in \Delta$ é uma face de ambos σ_1 e σ_2.

A *dimensão* de um complexo simplicial é $\dim \Delta := \max\{\dim \sigma : \sigma \in \Delta\}$.

Um *subcomplexo* de Δ é um subconjunto de Δ que também é um complexo simplicial.

Figura 18: À esquerda, um exemplo de um complexo simplicial. Os triângulos cinzas são 2-simplexos pertencentes ao complexo, já no triângulo não preenchido, apenas suas arestas são 1-simplexos pertencentes ao complexo. À direita, contra-exemplos.

Definição 6.22. O *conjunto de vértices* do complexo simplicial Δ, denotado por $V(\Delta)$, é a união dos conjuntos dos vértices de todos os simplexos de Δ. Alternativamente, são todos os simplexos de dimensão 0 em Δ.

Definição 6.23. A união de todos os simplexos do complexo simplicial Δ é o *poliedro* de Δ, denotado por $\|\Delta\|$.

Definição 6.24. Seja X um espaço topológico. Um complexo simplicial Δ cujo poliedro é homeomorfo[12] à X ($X \sim \|\Delta\|$) é uma *triangulação* de X.

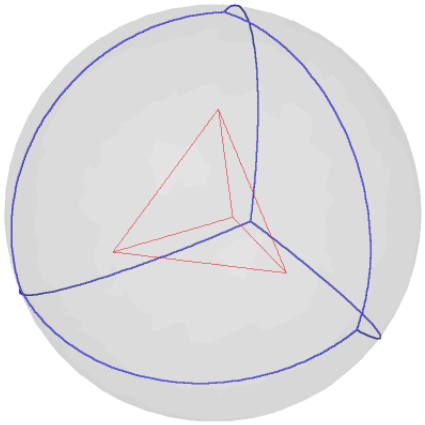

Figura 19: Como exemplo de triangulação, vemos um complexo simplicial formado por um único tetraedro e todas as suas faces e seu poliedro projetado na superfície da esfera S_2.

09/24/2015 - Gabriel Bonuccelli Heringer Lisboa

Agora veremos o teorema de Borsuk-Ulam, um famoso teorema da topologia e seu correspondente combinatorial, o lema de Tucker.

6.3 O Teorema de Borsuk-Ulam

Definição 6.25. Denotamos $S^{n-1} = \{x \in \mathbb{R}^n \mid \|x\| = 1\}$ a esfera de dimensão $n-1$, contida em $\mathbb{R}^n$. E denotamos $B^n = \{x \in \mathbb{R}^n \mid \|x\| \leq 1\}$ a bola de dimensão n, também contida em $\mathbb{R}^n$.

Apresentamos a seguir quatro enunciados equivalentes, todos conhecidos como "teorema de Borsuk-Ulam". Provaremos sua equivalência, porém omitiremos sua demonstração.

Proposição 6.26. São equivalentes as afirmações:

(1) Toda função contínua $f : S^n \to \mathbb{R}^n$ admite um ponto $x \in S^n$ tal que $f(x) = f(-x)$.

(2) Toda função contínua $f : S^n \to \mathbb{R}^n$ que preserva pares de pontos antípodas[13] (ímpar) possui um ponto $x \in S^n$ satisfazendo $f(x) = 0$.

(3) Não existe função contínua $f : S^n \to S^{n-1}$ que preserva pares de pontos antípodas (ímpar).

(4) Não existe função contínua $f : B^n \to S^{n-1}$ que preserva pares de pontos antípodas na fronteira $\partial B^n = S^{n-1}$.

Demonstração.

[12] Devemos ver $\|\Delta\|$ como subconjunto de $\mathbb{R}^d$ e considerar sua topologia induzida.

[13] Dizemos que uma função definida em S^n *preserva pares de pontos antípodas* ou é *ímpar* se $f(-x) = -f(x)$ para todo $x \in S^n$. Observe que se $x, -x \in S^n$, então $f(x)$ e $f(-x)$ também são pontos opostos na imagem de f.

$(1) \Rightarrow (2)$ Seja $f : S^n \to \mathbb{R}^n$ uma função contínua que preserva pares de pontos antípodas. Por (1), existe $x \in S^n$ tal que $f(x) = f(-x)$. Pela propriedade da função, vem que $f(x) = -f(x) \Rightarrow 2f(x) = 0 \Rightarrow f(x) = 0$.

$(2) \Rightarrow (1)$ Dada $f : S^n \to \mathbb{R}^n$ contínua, considere $g(x) = f(x) - f(-x)$. Podemos ver que g é ímpar e por (2), existe $x \in S^n$ tal que $g(x) = 0 \Rightarrow f(x) = f(-x)$.

$(2) \Rightarrow (3)$ Suponha que exista $f : S^n \to S^{n-1}$ contínua e que preserva pares de pontos antípodas. Podemos considerar $f' : S^n \to R^n, f'(x) = f(x)$ para todo $x \in S^n$ e provar que f' também é contínua. Por (2), $0 \in \mathrm{Im}(f')$, mas $\mathrm{Im}(f') = \mathrm{Im}(f) \subset S^{n-1}$, absurdo. Portanto tal f não existe.

$(3) \Rightarrow (2)$ Suponha que exista $f : S^n \to \mathbb{R}^n$ contínua e que preserva pares de pontos antípodas e tal que $f(x) \neq 0$ para todo $x \in S^n$. Podemos, então, definir a função $g : S^n \to S^{n-1}$ dada por $g(x) = \frac{f(x)}{\|x\|}$. Esta função é contínua e também preserva pares de pontos antípodas, o que entra em contradição com (3).

$(4) \Rightarrow (3)$ Consideremos o conjunto $U = \{x = (x_1, ..., x_{n+1}) \in S^n \mid x_{n+1} \geq 0\}$ e a projeção $\pi : U \to B^n, \pi((x_1, ..., x_{n+1})) = (x_1, ..., x_n)$. Observe que π é uma bijeção.

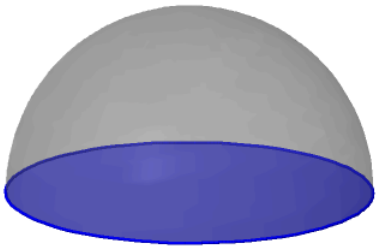

Figura 20: Para $n = 2$, ilustramos o conjunto U em cinza e B^2 em azul. Observe que a projeção π fixa a borda de $B^2 = S^1$.

Suponha que exista uma função contínua que preserva pares de pontos antípodas $f : S^n \to S^{n-1}$. Podemos, então, definir a função $g : B^n \to S^{n-1}$ dada por $g(x) = f(\pi^{-1}(x))$. Esta função é contínua e preserva pares de pontos antípodas em $\partial B^n = S^{n-1}$, pois nessa borda π é a identidade e f preserva pares de ponto antípodas. Chegamos em uma contradição com (4).

$(3) \Rightarrow (4)$ Suponha que exista $g : B^n \to S^{n-1}$ que preserva pares de pontos antípodas em $\partial B^n = S^{n-1}$. Definimos a função $f : S^n \to S^{n-1}$ por $f(x) = g(\pi(x))$, se $x \in U$ e $f(x) = -g(\pi(-x))$, se $-x \in U$.

Observamos que f está bem definida, pois se $x, -x \in U$, então $x, -x \in \partial B^n, \pi(x) = x, \pi(-x) = -x$ e como g preserva pares de pontos antípodas em ∂B^n, temos $-g(\pi(-x)) = -g(-x) = g(x) = g(\pi(x))$ e as duas definições coincidem. Ademais, f é contínua, pois é contínua em U e em $-U$ e ambos formam uma cobertura de S^n por fechados (Teorema 6.7).

Obtemos uma contradição com (3), pois da forma como foi definida, f preserva pares de pontos antípodas. ■

Teorema 6.27 (Borsuk-Ulam)
As afirmações da proposição anterior são verdadeiras.

Com o teorema de Borsuk-Ulam podemos provar o chamado Teorema do Ponto Fixo de Brower.

Teorema 6.28 (Teorema do Ponto Fixo de Brower)

Se $f : B^n \to B^n$ é contínua, então existe $x \in B^n$ tal que $f(x) = x$.

Demonstração.

Suponha que exista $f : B^n \to B^n$ contínua e que não admite um ponto fixo, isto é, $f(x) \neq x$ para todo $x \in B^n$. Vamos obter uma contradição com o item (4) do teorema de Borsuk-Ulam.

Construímos a função $F : B^n \to S^{n-1}$ tal que para $x \in B^n$, consideramos o segmento entre $f(x)$ e x e o alongamos, na direção de x, até S^{n-1}. Isto é, $F(x) = x + \lambda(f(x) - x)$, com $\lambda > 0$ tal que $\|F(x)\| = 1$.

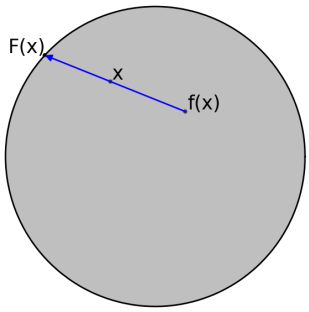

Figura 21: A função F no caso $n = 2$.

Observamos que $F(x) = x$ para todo $x \in \partial B^n = S^{n-1}$. Portanto, F preserva pares de pontos antípodas e obtemos uma contradição com o item (4) do teorema anterior. ■

Terminamos a seção enunciando o Lema de Tucker, que também pode ser mostrado equivalente ao Teorema de Borsuk-Ulam e usado na demonstração deste. Precisamos de uma definição antes de enunciar o lema:

Definição 6.29. Uma triangulação T da bola B^n é *antipodal e simétrica na fronteira* se para todo simplexo $\sigma \in T$ que é mapeado na fronteira $\partial B^n = S^{n-1}$, $-\sigma$ também pertence à triangulação.

Observação 6.30. Conforme descrito na definição 6.24, triangulação é um homeomorfismo entre um complexo simplicial e um espaço topológico (no caso, B^n). Assim, notamos que o $-\sigma$ presente na definição anterior é um pequeno abuso de notação, pois estamos realmente nos referindo à imagem de σ sob o homeomorfismo.

Teorema 6.31 (Lema de Tucker)

Sejam T uma triangulação de B^n que é antipodal e simétrica na fronteira e $\lambda : V(T) \to \{\pm 1, \pm 2, ..., \pm n\}$ uma indexação de T que satisfaz $\lambda(-v) = -\lambda(v)$ para todo $v \in S^{n-1}$. Então existe um 1-simplexo que é complementar, isto é, seus vértices têm índices opostos.