Evasividade de Propriedades de Grafos
Evasiveness of Graph Properties

Jair Donadelli
Departamento de Informática da UFPR, Centro Politécnico Jardim das Américas,
CP 19081, Curitiba - PR, CEP 81531-980
jair.donadelli@gmail.com

Resumo: Um problema bastante difícil em computação é determinar limitantes inferiores não-triviais para a complexidade de problemas computacionais. Um limitante desse tipo implica que qualquer algoritmo que resolve o problema tem no mínimo essa complexidade. Nesse texto, discorreu-se sobre complexidade de propriedades de grafos e sobre uma conjectura de 1973 e ainda não resolvida sobre a complexidade de propriedades monótonas de grafos. Também, expôs-se uma solução parcial para essa conjectura, um resultado de Kahn, Saks & Sturtevant, de 1984 [1], que até o momento é o único progresso relevante sobre o problema. O resultado de [1] é por meio de resultados de ponto fixo da ação de grupos sobre certos espaços topológicos.

Palavras-chave: complexidade de algoritmos, teoria dos grafos, métodos topológicos.

Abstract: Determine lower bounds for the complexity of computational problems is widely known to be a very difficult problem. Follows from a lower bound to the complexity of a specific problem that *any* algorithm that solve this problem has its complexity limited from below by that bound. In this manuscript we are concerned with lower bounds for the complexity of testing graph properties and we expose a conjecture posed in 1973 about the complexity of testing monotone properties of graphs. We also show a partial response to this conjecture given by Kahn, Saks e Sturtevant in 1984 [1] which make use of topological methods.

Keywords: complexity of algorithms, graph theory, topological methods.

---

1 INTRODUÇÃO

Considere-se o seguinte jogo entre dois jogadores, o *Ex Conde Dor* e o *Al Gor Itmo*: o Ex Conde conhece um grafo $G=(V,E)$ com n vértices, que o Al Gor desconhece. O Al Gor tem que descobrir se o grafo do Ex Conde satisfaz uma determinada propriedade P o mais cedo possível, por meio de sucessivas perguntas do tipo "$\{i,j\}\in E$?". A cada pergunta do Al Gor, o Ex Conde responde `sim` ou `não` com o objetivo de induzir o Al Gor a fazer o maior número possível de perguntas. Note-se que o Ex Conde pode decidir no momento se a resposta é `sim` ou `não`, como o grafo vai sendo revelado a cada pergunta não há motivo para o Ex Conde escolher um grafo antes do começo do jogo. As propriedades que interessam são as invariantes por isomorfismo.

A complexidade c(P) da propriedade P é o número de perguntas feitas por Al Gor quando ambos - o Ex Conde e o Al Gor - jogam com estratégias ótimas. Uma propriedade é dita *evasiva* se o Al Gor é forçado a fazer todas as $\binom{n}{2}$ perguntas.

Por exemplo, as seguintes propriedades são evasivas:

1. G tem no máximo k arestas ($0\leq k\leq\binom{n}{2}$);
2. G é uma árvore geradora;
3. G é uma floresta com k arestas ($k<n$);
4. G é acíclico ($n\leq 3$).

Nesses casos uma estratégia evasiva simples para o Ex Conde é a que segue: se em determinado momento o grafo construído é G_0 e a pergunta é "$\{i,j\}$ é uma aresta do grafo?", então a resposta é sim se e somente se algum supergrafo de $G_0 \cup \{\{i,j\}\}$ satisfaz *P*. É um exercício para o leitor provar que de fato com essa estratégia é preciso fazer todas as $\binom{n}{2}$ perguntas.

O seguinte exemplo [2, p. 409] mostra que existe uma propriedade *P* com $c(P) \neq \Omega(n^2)$: chame-se *G* de *grafo escorpião* se ele contém um vértice *b* de grau *n*-2, o único vértice não-adjacente a *b* tem grau 1 e é adjacente a um vértice de grau 2, as adjacências nos outros vértices são arbitrárias (veja-se Figura 1). A propriedade "*G* é um grafo escorpião" tem complexidade no máximo *6n*.

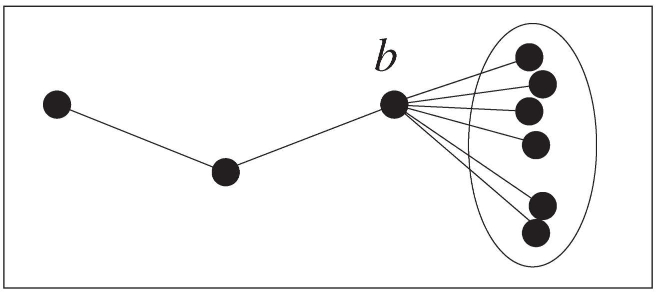

Figura 1: Grafo escorpião

Diz-se que uma propriedade *P é monótona* se é ela preservada por adição de arestas, e é *não-trivial* se vale para algum, mas não para todos os grafos sobre *V* (equivalentemente, podem ser consideradas como propriedade monótona aquelas preservadas por remoção de arestas).

Em 1973 Aanderaa & Rosenberg propuseram a seguinte conjectura:

existe uma constante $\varepsilon>0$ *tal que qualquer propriedade monótona não-trivial para grafos sobre n vértices tem complexidade pelo menos* εn^2.

Inicialmente a conjectura considerava grafos com laços, mas Lipton & Snyder (1974) deram contra-exemplos para essa conjectura, todos eles envolvendo laços. A conjectura foi mudada para a forma acima e provada por Rivest & Vuillemin [3] para $\varepsilon=1/16$ e depois melhorada por Kleitman & Kwiatkowski [4] para $\varepsilon=1/9$. A demonstração do resultado de Rivest e Vuillemin [3] pode ser encontrada em [2, Teorema 2.6, p. 414]. Na Seção 5.1 mostra-se que qualquer propriedade monótona não-trivial para grafos sobre *n* vértices tem complexidade pelo menos $n^2/4+o(n^2)$.

A seguinte conjectura foi atribuída a Karp (veja-se [1]) e a Best, van Emde Boas & Lenstra (veja-se [2]).

Conjectura 1 (conjectura de Karp) - *Toda propriedade monótona não-trivial sobre grafos é evasiva.*

Em 1984, Kahn, Saks & Sturtevant [1**Erro! Fonte de referência não encontrada**.] recorreram a alguns teoremas sobre pontos fixos de ação de grupos em complexos simpliciais acíclicos e provaram a conjectura de Karp em grafos com potência de primos vértices (veja-se Seção 5) e grafos de seis vértices (veja-se Seção 7), além de uma intrigante conexão: *a realização geométrica de complexos simpliciais de propriedades não-evasivas contraíveis.* Note-se que uma propriedade monótona por remoção de arestas é, por definição, um complexo simplicial abstrato (veja [5] para noções de topologia algébrica). Usando as mesmas técnicas de [1], Yao [6] provou em 1988, que toda propriedade não-trivial monótona de grafos bipartidos é evasiva (veja-se Seção 6).

O objetivo desse texto é, além de apresentar um problema importante não completamente resolvido pela Teoria dos Grafos (conjectura de Karp), mostrar uma abordagem topológica do problema, em particular. Até hoje, essa é a única abordagem que resultou em um sucesso parcial para a resolução do problema;, mais ainda, quase todos os avanços recentes são baseados nessa técnica. Além disso, a prova topológica que se apresenta é a única conhecida até o momento, ou seja, não é conhecida uma prova combinatória desse resultado.

Finalmente, para alguns casos particulares de propriedades para as quais a conjectura foi respondida o leitor pode consultar [2, Cap. 8] e [7], por exemplo, as propriedades *G* é conexo, *G* é 2-conexo, *G* é planar (*n*>4), *G* para *n* primo é hamiltoniano foram provadas serem evasivas. O leitor interessado em saber mais sobre cotas inferiores obtidas por métodos topológicos pode consultar [8].

A seguir serão apresentadas algumas definições.

1.1 Grafos

Os grafos a que se referiu durante o texto são não-dirigidos, sem laços ou arestas múltiplas e sobre um conjunto fixo V de vértices. Pode-se identificar cada grafo G sobre V com um subconjunto do conjunto $V^{(2)}$ dos 2-subconjuntos de V, e pode-se identificar uma propriedade P dos grafos sobre V com uma família $\mathcal{P}$ de subconjuntos do conjunto das partes de $V^{(2)}$. Assim, diz-se $G \in \mathcal{P}$ se e somente se G tem a propriedade P.

As propriedades consideradas são invariantes por isomorfismo, isto é, se um determinado grafo G satisfaz $\mathcal{P}$, então todo grafo obtido por qualquer permutação nos rótulos dos vértices de G também satisfaz $\mathcal{P}$, sem perda de generalidade, pode-se supor que $V=[n]=\{1,2,\ldots,n\}$. Para simplificar, será usada, sempre que não for ambíguo a notação ij para a aresta $\{i,j\} \subseteq [n]$.

Uma propriedade $\mathcal{P}$ é *monótona decrescente* (resp., crescente) se $G \in \mathcal{P}$ e $H \subseteq G$ (resp., $G \subseteq H$) implicam $H \in \mathcal{P}$. Note-se que, se $\mathcal{P}$ é uma propriedade monótona crescente então a propriedade complementar $\mathcal{P}^c$ é monótona decrescente e $c(\mathcal{P}) = c(\mathcal{P}^c)$. Daqui em diante serão consideradas apenas propriedades monótonas decrescentes não-triviais, e será usado o termo *propriedade monótona.*

1.2 Árvores de decisão booleanas

Pode-se ver o problema de decisão acima de uma maneira mais genérica como o problema de computar uma função booleana de N variáveis $f\ \{0,1\}^N \to \{0,1\}$.

Um algoritmo para computar $f(x_1, \ldots, x_N)$ pode ser modelado como uma *árvore de decisão booleana,* que é uma árvore binária onde cada nó interno tem um rótulo x_i, para $1 \leq i \leq N$, o filho esquerdo de x_i corresponde à atribuição x_i=0 e o direito, a x_ii=1. As folhas também são rotuladas com 0 e 1 e nelas lê-se a resposta para o valor da função com as atribuições nas variáveis definidas pelo percurso da raiz até a folha (veja-se Figura 2).

Uma computação começa na raiz da árvore, segue pela ramificação definida pelos valores nas variáveis e termina numa folha onde se lê o valor da função.

Toda árvore de decisão booleana pode ser pensada como um jogo de perguntas entre os jogadores Ex Conde e Al Gor. O Ex Conde pensa em um elemento $x \in \{0,1\}^N$, e a tarefa do Al Gor é determinar $f(x)$, pondo perguntas a Ex Conde. Essas perguntas não podem ser arbitrárias: pode-se perguntar apenas o valor de alguma variável binária. A estratégia de Al Gor corresponde à árvore de decisão. Ex Conde joga de forma ótima se com suas respostas ele dirige Al Gor a um nó mais longe da raiz, enquanto que Al Gor tenta selecionar as questões que o capacitam a decidir tão rápido quanto possível o valor de $f(x)$.

Claramente qualquer árvore de decisão para uma função booleana tem altura no máximo, do número de variáveis da função. Um exemplo de função booleana que alcança esse limitante é a que segue:

$$\bigwedge_{i=1}^{N} \bigvee_{j=1}^{N} x_{ij}. \tag{1}$$

Não é difícil provar que com a seguinte estratégia Ex Conde força Al Gor a perguntar por todas as variáveis da função descrita na equação (1); Ex Conde responde que a variável x_{ij} é 0 sempre que existir uma variável indeterminada na linha i, caso contrário responde 1.

Note-se que, se f é simétrica, isto é, se o valor não altera se permutadas as variáveis e é não-constante, então f é evasiva. Isso porque deve existir um j tal que f=i ($i \in \{0,1\}$) para toda seqüência com j-1 posições 1 e f=1-i para toda seqüência com j posições 1.

Diz-seque f é fracamente simétrica se existe uma permutação que leva x_i em x_j sem mudar o valor de f; para todo $1 \leq i, j \leq N$, por exemplo, a

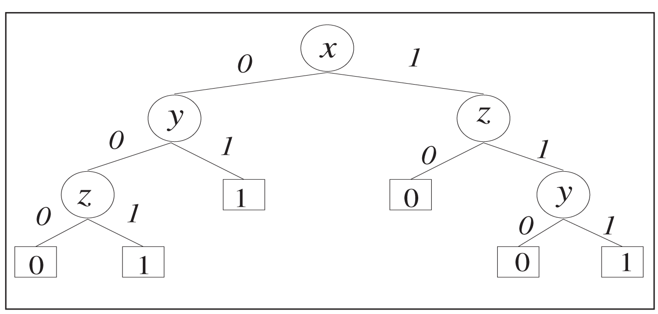

Figura 2: Exemplo de uma árvore de decisão booleana.

função $(x_1 \wedge x_2) \vee (x_2 \wedge x_3) \vee \cdots \vee (x_N \wedge x_1)$ é fracamente simétrica.

Conjectura 2 (conjectura de Karp generalizada para funções booleanas) *Se f é uma função booleana não-constante, fracamente simétrica e monótona, então f é evasiva.*

1.3 Complexos simpliciais

Para se saber mais sobre os conceitos de topologia algébrica que aparecem a seguir, indica-se [5].

Um *complexo simplicial abstrato* sobre um conjunto (finito) de *vértices* X é um par (X,Δ), onde Δ é uma coleção de subconjuntos de X satisfazendo as condições abaixo.

1. Se $x \in X$ então $\{x\} \in \Delta$, e
2. se $S \in \Delta$ e $T \subseteq S$, então $T \in \Delta$.

Um elemento $S \in \Delta$ é chamado uma *face* de Δ. Um *k-simplexo abstrato* é o complexo simplicial dado pelo conjunto das partes de um conjunto de $k+1$ vértices. Uma família de simplexos $\Delta = \{\sigma_1, \sigma_2, \ldots, \sigma_m\}$ é um *complexo simplicial* se (i) toda face de qualquer simplexo $\sigma \in \Delta$ é também um simplexo de Δ; (ii) se σ e σ' são simplexos de Δ, então a intersecção $\sigma \cap \sigma'$ é face de σ e σ'. Os σ_i são as faces maximais do complexo.

Uma realização geométrica de um complexo simplicial abstrato (X,Δ) pode ser obtida associando-se a cada vértice um vetor unitário do $\mathbb{R}^{|X|}$ e tomando-se o fecho convexo das faces de Δ. A união de todos os fechos das faces de Δ é denotada Δ. Cada complexo simplicial geométrico determina um complexo simplicial abstrato. Para um complexo simplicial abstrato existe associado um único (a menos de homeomorfismos) complexo simplicial geométrico. Δ.

Daqui em diante, será usado apenas Δ para um complexo simplicial e fica subentendido que $X = \bigcup_{S \in \Delta} S$.

2 COMPLEXIDADE DE PROPRIEDADES DE GRAFOS

Com $N=n^2$ variáveis booleanas x_{ij} que indicam se ij é ou não aresta, um grafo corresponde a uma valoração das variáveis e uma propriedade de grafo $\mathcal{P}$ corresponde a uma função booleana f definida nessas variáveis de modo que

$$f(x_{11}, \ldots, x_{ij}, \ldots, x_{nn}) = f(x_{\pi(1)\pi(1)}, \ldots, x_{\pi(i)\pi(j)}, \ldots, x_{\pi(n)\pi(n)}),$$

para toda permutação $\pi:[n]\rightarrow[n]$. Se $f(G)=1$ se e somente se $G \in \mathcal{P}$.

Se $\mathcal{P}$ é uma propriedade sobre as seqüências binárias de tamanho N, então denota-se por $c(\mathcal{P})$ a *complexidade da propriedade* $\mathcal{P}$, definida por

$$c(\mathcal{P})=\min\{h(T)\text{: T é uma árvore de decisão para } \mathcal{P}\},$$

onde $h(T)$ é a altura da árvore T. A propriedade é *evasiva* se tem complexidade N.

Uma vantagem de modelar algoritmos como árvores é poder usar técnicas combinatórias para limitar a altura das árvores: a árvore mais baixa que resolve o problema corresponde ao algoritmo ótimo. A seguir, apresentam-se dois exemplos dessas técnicas.

É um exercício interessante provar a seguinte cota inferior para a altura de uma tal árvore: se f é uma função booleana não-constante de N variáveis e t o número de entradas para as quais o valor da f é 1 e se 2^k é a maior potência de dois que divide t, então a altura de qualquer árvore de decisão que computa f é pelo menos N-t. Segue que se t é ímpar então a altura de qualquer árvore é t.

O *polinômio enumerador* para $\mathcal{P}$ é definido por $\phi_{\mathcal{P}}(z) = \sum z^{|G|}$, onde a soma é sobre todo $G \in \mathcal{P}$.

Proposição 3 Se $c(\mathcal{P})=d$ *então* $(z+1)^{N-d}$ divide $\phi_{\mathcal{P}}(z)$.

Proof: Sejam T uma árvore para $\mathcal{P}$ e w uma folha `sim` de T e profundidade p_w. Denote-se por S_w o conjunto de entradas que na árvore de decisão T terminam a computação na folha w.

Se S_w é o número de variáveis do raiz-w caminho em T rotuladas com 1, então tem-se que o número de entradas que pertencem a S_w e com quantidade de 1´s igual a $s_w + i$ $\binom{N-p_w}{i}$, para todo $0 \leq i \leq N - p_w$.

Portanto, a contribuição de cada folha w de T para o polinômio $\phi_{\mathcal{P}}(z)$ é a seguinte:

$$\sum_{i=0}^{N-p_w} \binom{N-p_w}{i} z^{s_w+i} =$$
$$z^{s_w} \sum_{i=0}^{N-p_w} \binom{N-p_w}{i} z^i =$$
$$z^{s_w}(1+z)^{N-p_w},$$

que é divisível por $(z+1)^{N-d}$, pois $p_w \leq d$. □

Corolário 4 (condição de balanceamento par-ímpar). *Se o número de elementos de $\mathcal{P}$ com cardinalidade par não é igual ao número de elementos de cardinalidade ímpar, então $\mathcal{P}$ é evasiva.* □

3 COMPLEXOS SIMPLICIAIS E EVASIVIDADADE

Nessa seção, será estabelecida a relação entre complexidade e topologia.

Se for posto $X=V^{(2)}$, então um grafo sobre V é um subconjunto de X e uma propriedade de grafo $\mathcal{P}$ é um subconjunto do conjunto das partes de X. Ainda, se $\mathcal{P}$ é monótona então $\mathcal{P}$ é um complexo simplicial abstrato.

Daqui em diante, um complexo simplicial abstrato; e uma propriedade monótona serão confundidos e será usada a notação Δ ou $\mathcal{P}$, conforme houve interesse ou não nas propriedades topológicas dessa família de conjuntos.

Pode-se generalizar o problema da seguinte forma: dado um complexo simplicial Δ sobre um conjunto de vértices X, determinar se um subconjunto $\sigma \subseteq X$ é uma face de Δ fazendo perguntas do tipo "$x \in \sigma$?". O complexo Δ é *evasivo* se não existe estratégia que decida se σ é uma face de Δ em menos que $n=|X|$ perguntas, e é *não-trivial* se é diferente do vazio e de um n-simplexo.

Será vista agora uma interessante conexão entre topologia e evasividade, haverá necessidade de algumas definições.

Uma *face livre* de Δ é uma face não-maximal contida em uma única face maximal. Um *colapso elementar* em Δ é a operação de remoção de uma face livre de Δ junto com todas as faces que a contêm. Diz-se que Δ *colapsa* para Δ' se existe uma seqüência finita de colapsos elementares a partir de Δ resultando em Δ'. Um complexo é *colapsável* se ele colapsa para um 0-simplexo (vértice).

Para cada $x \in X$ existem associados dois complexos sobre $X \setminus \{x\}$: o complexo *ligação* e o complexo *co-estrela*

$$\begin{aligned} Lg(x) &= \{\sigma \subseteq X \setminus \{x\} : \sigma \cup \{x\} \in \Delta\} \text{ e} \\ Co(x) &= \{\sigma \subseteq X \setminus \{x\} : \sigma \in \Delta\}. \end{aligned}$$

Lema 5 (KAHN, SAKS & STURTEVANT 1984, 1). *Se existe $\{x\} \in \Delta$ tal que $Lg(x)$ e $Co(x)$ são colapsáveis então Δ é colapsável.*

Proof: Seja $\sigma_1, \sigma_2, \ldots, \sigma_k$ uma seqüência de faces livres usadas para o colapso do complexo $Lg(x)$. Para todo $i \in \{1......k\}$ tem-se que $\sigma_i \cup \{x\} \in \Delta$ e ainda $\sigma_i \cup \{x\}$ é livre no complexo resultante da seqüência de colapsos $\sigma_1, \sigma_2, \ldots, \sigma_{i-1}$.

Será mostrado que a seqüência de faces livres $\sigma_1 \cup \{x\}, \sigma_2 \cup \{x\}, \ldots, \sigma_k \cup \{x\}$ é um colapso de Δ para (x) e, portanto, Δ é colapsável.

Chame-se de Σ o resultado do colapso de Δ. Se $\alpha \in Co(x)$, então $x \notin \alpha$; suponha-se que $\alpha \notin \Sigma$, então $\sigma_i \cup \{x\} \subseteq \alpha$ para algum i, o que é uma contradição. Portanto, $Co\ (x) \subseteq \Sigma$.

Se $\alpha \in \Sigma$, então $\sigma_i \cup \{x\} \nsubseteq \alpha$, para todo i. Se $x \in \alpha$, então $\sigma_i \subseteq \alpha \setminus \{x\}$ para algum i, pois $\alpha \setminus \{x\} \in Lg(x)$ e $\sigma_1, \ldots, \sigma_k$ é uma seqüência que colapsa $Lg(x)$; portanto, $\sigma_i \cup \{x\} \subseteq \alpha$, o que é uma contradição. Logo, $x \notin \alpha$. Como $\alpha \in \Delta$, tem-se que $\alpha \in Co(x)$. Logo, $\Sigma = Co(x)$. □

A conexão com a topologia é dada pela seguinte proposição.

Teorema 6 (KAHN, SAKS & STURTEVANT 1984, 1). *Um complexo Δ não-evasivo é colapsável.*

Proof: Se Δ é um complexo não?evasivo sobre X então existe algum $x \in X$ tal que "$x \in \sigma$?" é uma primeira pergunta que decide pertinência em Δ em menos que $n = |X|$ perguntas para qualquer entrada $\sigma \subseteq X$.

Se a resposta para essa primeira pergunta é `sim` então $\sigma \in \Delta$ se e somente se $\sigma \setminus \{x\} \in Lg(x)$; caso contrário, $\sigma \in \Delta$ se e somente se $\sigma \in Co(x)$.

Note-se que não se pode decidir se $\sigma \setminus \{x\} \in Lg(x)$ se não se perguntar pelos vértices de $Lg(x) \setminus Co(x)$. Como *Co(x)* é um complexo sobre $n-1$ vértices tem-se que *Co(x)* é não?evasivo. Portanto, se *Lg(x)* ou *Co(x)* é evasivo então Δ é evasivo.

Assim, em ambos os casos existe uma estratégia não - evasiva que decide pertinência nos complexos *Lg(x)* e *Co(x)*. A prova agora segue por indução em $n = |X|$. □

4 AÇÕES DE GRUPOS

Do fato de propriedade *P* ser invariante por isomorfismo, o grupo simétrico S_n age transitivamente sobre os $\binom{n}{2}$ elementos de $V^{(2)}$ (o conjunto de todas as arestas sobre *V*) preservando o conjunto de grafos que satisfaz *P*. Isso leva à idéia de que se pode recorrer aos resultados sobre ações de grupos finitos em espaços topológicos.

A ação de um grupo *G* sobre um conjunto S é uma função *G*x*S* em *S* tal que *(i)* $1_G x = x$ e *(ii)* $(g_1 g_2)x = g_1(g_2 x)$, para todo $x \in S$.

Se Γ é um grupo de permutações, isto é, um subgrupo do grupo simétrico *Sm*, agindo de forma natural sobre [m] e $\{x_1, x_2, \ldots, x_\ell\} \subseteq [m]$ então a órbita pela ação de Γ é o conjunto abaixo:

$$orb_\Gamma(\{x_1, x_2, \ldots, x_\ell\}) = \{\{g(x_1), g(x_2), \ldots, g(x_\ell)\} : g \in \Gamma\},$$

e o *estabilizador* é o subgrupo $\Gamma_{\{x_1,\ldots,x_\ell\}}$ dado por

$$\{g \in \Gamma \ \{g(x_1), g(x_2), \ldots, g(x_\ell)\} = \{x_1, \ldots, x_\ell\}\}.$$

A ação de Γ é *transitiva* em *[m]* se para qualquer $q \in [m]$ tem-se $orb(q) = [m]$.

Se $\mathcal{P}$ é uma família de subconjuntos de *X* diz-se que a ação de Γ *preserva* $\mathcal{P}$ se dados $A \in \mathcal{P}$ e $g \in \Gamma$ tem-se $g(A) \in \mathcal{P}$, denota-ses por $Aut(\mathcal{P})$ o *grupo de permutações de X que preservam* $\mathcal{P}$.

O primeiro resultado sobre evasividade que leva em conta ações de grupo é de 1976.

Teorema 7 (Rivest & Vuillemin 1976, RV). *Se* $|X|$ *é uma potência do primo p,* $Aut(\mathcal{P})$ *é transitivo sobre X,* $\emptyset \in \mathcal{P}$ e $X \in \mathcal{P}$, *então* $\mathcal{P}$ *é evasiva.*

Proof: Tome-se $G \in \mathcal{P}$. Como $(\mathcal{P})$ é transitivo sobre *X*, cada elemento de *X* está contido em exatamente *c* conjuntos da órbita de *G*, para algum $c \geq 1$. Ademais, pondo-se $\Gamma = (\mathcal{P})$,

$$|orb_\Gamma(G)||G| = p^r c,$$

e, portanto, ou p divide $|orb_\Gamma(G)|$, ou p divide $|G|$. Se p não divide $|orb_\Gamma(G)|$, então $|G| = 0$. De fato, ou $|G| = 0$ ou $|G| = p^r$, mas esta última igualdade não vale pois $X \notin \mathcal{P}$.

Se $\mathcal{P}_i = \{G \in \mathcal{P}\ |G| \equiv i \mod 2\}$, $i = 0, 1$, então cada $\mathcal{P}_i$ consiste de órbitas inteiras. Logo a condição par - ímpar (corolário 4) não é balanceada pois, para algum *i*, a família $\mathcal{P}_i$ deve conter uma órbita de tamanho 1 (pois $\emptyset \in \mathcal{P}$), e as outras órbitas em ambas famílias têm tamanho divisível por p. Segue que $\mathcal{P}$ é evasiva. □

4.1 Ações de grupos em complexos simpliciais

Sejam Δ um complexo simplicial e Γ um grupo de permutações agindo nos vértices de Δ, define-se o complexo Δ_Γ da seguinte forma: os vértices de Δ_Γ são as faces de Δ não-vazias Γ-invariantes minimais e se $\sigma_1, \ldots, \sigma_k$ são vértices de Δ_Γ, então $\{\sigma_1, \ldots, \sigma_k\}$ é uma face de Δ_Γ se e somente se $\sigma_1 \cup \ldots \cup \sigma_k$ é uma face de Δ.

Por exemplo, considere-se o complexo Δ da Figura 3.

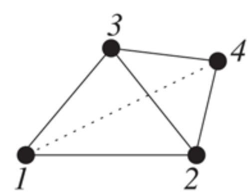

Figura 3: Exemplo: 3-simplexo

Suponha-se que $\Gamma = \langle(123)\rangle$. Então, {1,2,3} e {4} são as faces invariantes minimais pela ação de Γ. O complexo Δ_Γ tem vértices *X*={1,2,3} e *Y*={4}; como $X \cup Y$ é face de Δ, tem-se que {*X*,*Y*} é face de Δ_Γ. Note-se que Δ_Γ tem representação geométrica com *X* sendo o baricentro do fecho convexo de {1,2,3}, com *Y*=4, e {*X*,*Y*} o segmento que une esses pontos.

Representando-se um vértice de Δ_Γ pelo baricentro da face minimal invariante associada a ele tem-se:

$$\|\Delta_\Gamma\| = \|\Delta\|_\Gamma = \{x \in \|\Delta\| \colon g(x) = x \text{ para todo } g \in \Gamma\}.$$

Chama-se *Aut*(Δ) de *grupo de automorfismos* de Δ e esse grupo também age na realização geométrica $\|\Delta\|$ de Δ como um grupo de homeomorfismos lineares por partes da seguinte forma: dado $g \in Aut(\Delta)$ põe-se $\|g\|(\sum \lambda_i x_i) = \sum \lambda_i x_{g(i)}$.

A seguinte generalização da conjectura de Karp foi proposta por Kahn, Saks & Sturtevant [1].

Conjectura 8 (conjectura de Karp generalizada para complexos simpliciais). *Se Δ é um complexo simplicial sobre X, não-vazio e não-evasivo e Aut(Δ) é transitivo sobre X então Δ é um simplexo.*

5 PROPRIEDADES DE GRAFOS COM ORDEM POTÊNCIA DE PRIMO

Diz-se que um complexo Δ é *$\mathbb{Z}$-acíclico* se o *i*-ésimo grupo de homologia reduzido (veja [5]) é $\tilde{H}_i(\Delta;\mathbb{Z}) = 0$ para todo $i \geq 0$. Por exemplo, se Δ é um *k*-simplexo, então Δ é $\mathbb{Z}$-acíclico, em particular se Δ é colapsável, então Δ tem os mesmos grupos de homologia reduzido de um vértice (0-simplexo); portanto, Δ é $\mathbb{Z}$-acíclico.

Seja $\mathcal{M}$ a família de todos os grupos Γ contendo subgrupos Γ_1 e Γ_2 tais que

1. $\Gamma_1 \lhd \Gamma_2 \lhd \Gamma$, onde $\lhd$ é notação para subgrupo normal;
2. Γ_1 é um *p*-grupo, Γ_2/Γ_1 é cíclico e Γ/Γ_2 é um *q*-grupo, com *p* e *q* primos.

De acordo com essas definições, será assumido o seguinte resultado.

Proposição 9 (Oliver 1975, [10]). Se $\Gamma \in \mathcal{M}$ *age sobre o complexo $\mathbb{Z}$-acíclico Δ, então $\|\Delta\|_\Gamma \neq \emptyset$.* □

Com relação à conjectura 8, tem-se o seguinte resultado.

Lema 10 (Kahn, Saks & Sturtevant 1984, [1]). *Se Δ é um complexo não-vazio $\mathbb{Z}$-acíclico e Aut(Δ) contém um subgrupo vértice-transitivo $\Gamma \in \mathcal{M}$, então Δ é um simplexo.*

Proof: Suponha-se que $\Gamma \in \mathcal{M}$ age transitivamente no conjunto *X* de vértices de Δ. Pela Proposição 9 existe $x \in \|\Delta\|_\Gamma$. Considere-se $A \in \Delta$ a face minimal de Δ com $x \in \|A\|$. Então $g(A) = A$ para todo $g \in \Gamma$ e pela transitividade da ação de Γ em *X* segue que $A = X$. Portanto, Δ é um simplexo. □

Com essa conexão em mãos pode-se provar o principal resultado dessa seção.

Teorema 11 (Kahn, Saks & Sturtevant 1984, [1]). *Se n é uma potência de primo então toda propriedade não-trivial monótona de grafos com n vértices é evasiva.*

Proof: Seja $\mathcal{P}$ uma propriedade monótona não-trivial sobre grafos de ordem $|V| = p^r$, onde p é um primo.

Suponha-se que $\mathcal{P}$ é não-evasiva; pelo Teorema 6 tem-se que mostrar que existe $\Gamma \in \mathcal{M}$ subgrupo de $(\mathcal{P})$ pois, nesse caso, $\mathcal{P}$ é colapsável, portanto $\mathbb{Z}$-acíclico e pelo Lema 10 conclui-se que $\mathcal{P}$ é trivial, um absurdo que prova o teorema.

Para mostrar que existe $\Gamma \in \mathcal{M}$ subgrupo de $(\mathcal{P})$, identifica-se *V* com o corpo finito com p^r elementos $\mathrm{GF}(p^r)$ e consideram-se o grupo de transformações lineares e subgrupo das translações, respectivamente

$$\begin{aligned} \Gamma &= \{x \mapsto ax + b \colon a, b \in \mathrm{GF}(p^r),\ a \neq 0\} \quad \text{e} \\ \Gamma_1 &= \{x \mapsto x + b \colon b \in \mathrm{GF}(p^r)\}. \end{aligned}$$

A ação de Γ sobre *V* é duplamente transitiva sobre os elementos de $\mathrm{GF}(p^r)$ e transitiva nos vértices de $\mathcal{P} \subseteq V^{(2)}$ pois

$$x \mapsto \frac{z_2 - w_2}{z_1 - w_1} x + \frac{z_1 w_2 - w_1 z_2}{z_1 - w_1}$$

leva $z_1 w_1$ em $z_2 w_2$. Γ_1 é um p-subgrupo normal de Γ pois para todos $a, b, b' \in \mathrm{GF}(p^r)$, com $a \neq 0$,

$$x \xrightarrow{g^{-1}} a^{-1}x - b \xrightarrow{g_1} a^{-1}x + b' - b \xrightarrow{g} x - ab + ab' + b,$$

onde $g\ x \mapsto ax + b$ e $g_1\ x \mapsto x + b'$. Portanto, $g\Gamma_1 g^{-1} \subseteq \Gamma_1$.

Agora, se $g(x) = x + b$ $(x \in \mathrm{GF}(p^r))$ é um elemento de Γ_1 então $g^p = id$. Ainda, Γ/Γ_1 é isomorfo ao grupo multiplicativo do corpo $\mathrm{GF}(p^r)$:

$$\Gamma/\Gamma_1 \to \mathrm{GF}(p^r)^*$$
$$\Gamma_1 g \mapsto a,$$

onde $g : x \mapsto ax + b$, é um isomorfismo. Portanto, Γ/Γ_1 é cíclico.

Tomando $\Gamma_2 = \Gamma$ tem-se que $\Gamma \in \mathcal{M}$. □

5.1 Uma implicação na conjectura de Aanderaa-Rosenberg

Nesta seção será vista uma implicação do resultado de Kahn, Saks & Sturtevant na conjectura de Aanderaa-Rosenberg.

Denota-se por K_i o grafo completo sobre o conjunto de vértices $V=[i]$ e por $K_i \cup K_i$ a união disjunta dos grafos completos K_i e K_i. Denota-se por E_m o grafo (V,E), com $V=[m]$ e $E=\emptyset$, e por K_1+G o grafo com conjunto de vértices $\{1\} \cup V(G)$ (união disjunta) e conjunto de arestas $\{(1,i): i \in V(G)\} \cup E(G)$. Ainda, $c(n)$ denota o mínimo entre as complexidades de todas as propriedades monótonas não-triviais de grafos de ordem n.

Lema 12 *Qualquer propriedade monótona não-trivial de grafos de ordem n tem complexidade* $c(n) \geq \min\{c(n-1), \lfloor n^2/4 \rfloor\}$.

Proof: Seja $\mathcal{P}$ uma propriedade monótona não - trivial de grafos de ordem n. Se $K_1 + E_{n-1} \in \mathcal{P}$, então $\mathcal{P}' = \{G' \ K_1 + G' \in \mathcal{P}\}$ é uma propriedade monótona não - trivial de grafos de ordem $n - 1$ de complexidade pelo menos $c(n - 1)$. Da mesma forma, se $K_1 \cup K_{n-1} \notin \mathcal{P}$ constrói $\mathcal{P}'$ de complexidade pelo menos $c(n - 1)$. Em ambos casos, $c(\mathcal{P}') \leq c(\mathcal{P})$. Então, é possível supor que $K_1 \cup K_{n-1} \in \mathcal{P}$ e $K_1 + E_{n-1} \notin \mathcal{P}$.

Considere-se o grafo $K_{V_2} \cup E_{V_1}$ consistindo de um grafo completo sobre um subconjunto V_2 de $[n]$ com cardinalidade $[n/2]$ e nenhuma aresta incidindo nos $[n/2]$ vértices restantes, que se denota por V_1. Se Γ é o grupo que deixa esse grafo invariante então Γ pode ser escrito como o produto direto do grupo simétrico sobre os vértices de V_1 com o grupo simétrico sobre os vértices de V_2. Denote-se por L o conjunto de arestas com um extremo em V_1 e o outro em V_2. Represente-se uma aresta de L por (i, j)com $i \in V_1$ e $j \in V_2$.

Ponha-se $\mathcal{P}' = \{H \subseteq L \ H \cup K_{V_2} \in \mathcal{P}\}$. Então, $\mathcal{P}'$ é monótona, e não - trivial ($L \notin \mathcal{P}'$, caso contrário $K_1 + E_{n-1} \in \mathcal{P}$). Pelo Teorema 15 tem-se que $\mathcal{P}'$ é evasiva, isto é, $c(\mathcal{P}') = \lfloor n/2 \rfloor \lceil n/2 \rceil = \lfloor n^2/4 \rfloor$; também, $c(\mathcal{P}') \leq c(\mathcal{P})$. Portanto, $c(\mathcal{P}) \geq \lfloor n^2/4 \rfloor$.
□

O Teorema dos Números Primos diz que se $\pi(x)$ é a quantidade de números primos menores ou iguais a x, então $\pi(x)(\log x/x)$ tende a 1 quando x cresce indefinidamente. Segue daí que existe uma função real $f(x)=o(x)$ tal que existe um primo entre x e $x+f(x)$, para todo x.

Teorema 13 (Kahn, Saks & Sturtevant 1984, [1]) *Qualquer propriedade monótona não-trivial de grafos de ordem n tem complexidade pelo menos* $n^2/4+o(n^2)$.

Proof: Tem-se do lema acima que $c(n) \geq \min\{c(p), (p+1)^2/4\}$, onde p é a maior potência de primo menor que n. Portanto tem-se do Teorema 11 que $c(n) \geq \min\{\binom{p}{2}, (p+1)^2/4\} \geq (p+1)^2/4$. Como $p = n - o(n)$ tem-se que:

$$c(n) \geq \frac{(n^2 + o(n)^2 - 2o(n)n)}{4} = n^2/4 + o(n^2). \qquad \square$$

6 PROPRIEDADES DE GRAFOS BIPARTIDOS

Tomem-se V e W os conjuntos de naturais positivos $[m]$ e $[n]$, respectivamente. Por toda esta seção, consideram-se grafos bipartidos $G=(V \cup W,A)$ com bipartição $V \cup W$ e propriedades monótonas não-triviais de grafos bipartidos, invariantes por isomorfismos, isto é, invariante sob a ação natural do grupo $S_m \oplus S_n$ sobre $V \cup W$.

Denota-se por B_D, onde $D \subseteq V$, o grafo bipartido $(V \cup W,A)$ com $A=\{(v,w): v \in D, w \in W\}$=DxW. Note que se $\mathcal{P}$ é uma propriedade monótona não-trivial, então existe um inteiro $r(\mathcal{P}) \in \{0,\dots ,m-1\}$ tal que $B_D \in \mathcal{P}$ se $|D| \leq r(\mathcal{P})$ e $B_D \in \mathcal{P}$ caso contrário.

De fato, tem-se que se $B_D \in \mathcal{P}$ e $D' \subseteq V$ com $|D|=|D'|$ então $B_{D'} \in \mathcal{P}$ pois $\mathcal{P}$ é invariante sob ação do $S_m \oplus S_n$. Como $\mathcal{P}$ é monótona não-trivial para algum inteiro $0 \leq r < m$ temos que $B_D \in \mathcal{P}$ se e somente se $|D| \leq r$.

Será assumido o seguinte resultado.

Proposição 14 (Oliver 1975, [10]). *Se Δ é um complexo simplicial $\mathbb{Z}$-acíclico e Γ é um grupo cíclico, então $\chi(\Delta_\Gamma)=1$.* □

Assim, coloca-se o resultado principal desta seção.

Teorema 15 (Yao, 1988, [6]) *Toda propriedade monótona não-trivial de grafos bipartidos é evasiva.*

Proof: Assuma-se que $\mathcal{P}$ é uma propriedade monótona não - trivial e não - evasiva de grafos bipartidos. Então $\Delta = \mathcal{P}$ é acíclico.

Tome-se $\Gamma = \{A_0, A_1, \ldots, A_{n-1}\}$, onde $A_i(r,s) = (r, s+i \mod n)$. Então $\Gamma = 1 \oplus_n < S_m \oplus S_n$ e, portanto, Δ é invariante sob a ação de Γ. Assim, pela Proposição 14 tem-se que $\chi(\Delta_\Gamma) = 1$.

Agora, vai olhar para Δ_Γ. Se $r(\mathcal{P}) = 0$ então Δ_Γ é vazio e $\chi(\Delta_\Gamma) = 0 \neq 1$, o que é uma contradição. Se $r(\mathcal{P}) \geq 1$, tem-se que $A_1, \ldots, A_m$, onde $A_i = \{(i,w)\, w \in W\}$, são as faces não - vazias de Δ minimalmente invariantes sob a ação de Γ. Ademais,

$$\Delta_\Gamma = \{\{A_i\, i \in D\}\, D \subseteq V \text{ e } B_D \in \Delta\}.$$

Se $B_D \in \Delta$, então $B_D \in \mathcal{P}$ e viu-se que isso acontece se e somente se $|D| \leq r(\mathcal{P})$. Como uma face de dimensão *j* tem cardinalidade *j+1* e elas são em número $\binom{m}{j+1}$, tem-se que:

$$\begin{aligned}
\chi(\Delta_\Gamma) &= \sum_{j=0}^{r(\mathcal{P})-1} (-1)^j \binom{m}{j+1} \\
&= \sum_{j=0}^{r(\mathcal{P})-1} (-1)^j \left(\binom{m-1}{j+1} + \binom{m-1}{j} \right) \\
&= 1 + (-1)^{r(\mathcal{P})-1} \binom{m-1}{r(\mathcal{P})} \\
&\neq 1,
\end{aligned}$$

e tem-se uma contradição da Proposição 14. Portanto, $\mathcal{P}$ é evasiva. □

7 PROPRIEDADES DE GRAFOS DE ORDEM 6

O caso de seis vértices é o menor caso não coberto pelo Teorema 11 e também foi resolvido em [1].

Seja Δ uma propriedade não-evasiva monótona decrescente de grafos de ordem seis e defina-se a propriedade dual $\Delta^*=\{A \subseteq V^{(2)}: A^c = V^{(2)} A \in \Delta\}$. Se *H* é um grafo de ordem seis diz-se que Δ *contém H ou H pertence* a Δ se qualquer (equivalentemente, algum) grafo sobre $V=\{1,2,\ldots,6\}$ isomorfo a *H* é face de Δ.

Assuma-se que Δ é diferente do vazio e de um simplexo. Essas hipóteses sobre Δ também são válidas para Δ^*. A demonstração prossegue considerando ações de subgrupos Γ do grupo S_6 e aplicando as Proposições 16 e 17 dadas abaixo ao complexo Δ.

Proposição 16 (Smith, 1941, [11]). *Se Γ é um p-grupo agindo sobre um complexo simplicial $\mathbb{Z}$-acíclico Δ, então Δ_Γ é $\mathbb{Z}$-acíclico.* □

Proposição 17 (Oliver, 1975, [10]). *Se o grupo Γ age sobre o complexo $\mathbb{Z}$-acíclico Δ, e se Γ contém um p-subgrupo normal Γ_1 tal que Γ/Γ_1 é cíclico, então $\chi(\Delta_\Gamma) = 1$.*

Lema 18 *Emparelhamentos perfeitos pertencem a Δ.*

Proof: Seja Γ o estabilizador de $M = \{\{1,2\},\{3,4\},\{5,6\}\}$. Então, $\Gamma S_3 \times C_2 \times C_2 \times C_2$ e, portanto, $\Gamma \in \mathcal{M}$ pois é possível tomar $\Gamma_1 C_2^4$ e $\Gamma/\Gamma_1 C_3$ e $\Gamma_2 = \Gamma$. Pela Proposição 17 (Δ é acíclico pois está-se assumindo não - evasividade) Δ_Γ é não - vazio. As possíveis faces de Δ fixas pela ação de Γ são as órbitas da ação de Γ, assim, pelo menos uma órbita está em Δ.

Mas se $M^c \in \Delta$, então $M \in \Delta$ pois *M* é isomorfo ao subgrafo $M' = \{\{1,6\},\{2,3\},\{5,4\}\}$ de M^c. □

Lema 19 *Exatamente um de $2K_3$ e $K_{3,3}$ pertence a Δ.*

Proof: Tome-se $\Gamma = \langle(123), (456), (14)(25)(36)\rangle$. Então $\Gamma C_3 \times C_3 \times C_2$ e segue que $\Gamma \in \mathcal{M}$. Pela Proposição 9 pelo menos uma órbita da ação de Γ está em Δ. Pela Proposição 17, se as duas órbitas estão em Δ então a união delas também está (Caso contrário, Δ_Γ é formado por dois vértices o que contraria a Proposição 17), e assim ter-se-ia que Δ é um simplexo, pois a união das órbitas é o K_6. $\square$

Suponha-se que $2K_3$ pertença a Δ (e, portanto, a Δ^*) e tome o grupo de permutações $\Gamma= \langle(153624)\rangle$. Então, Γ_6 e, portanto, pertence à família $\mathcal{M}$. Sejam A, B e C as órbitas da ação de Γ.

A órbita A pertence a Δ, pois emparelhamentos perfeitos pertencem a Δ, e C pertence a Δ por hipótese. Portanto, a órbita B pertence a Δ, pois, caso contrário a Proposição 17 força $A\cup C$ estar em Δ e B é isomorfo a um subgrafo de $A\cup C$. Logo, $B\in\Delta$.

Dessa forma tem-se uma contradição, pois tudo o que se fez vale para Δ^*, isto é, A, B e C pertencem a Δ^* e, então, $A^c=B\cup C$, $B^c=A\cup C$ e $C^c=A\cup B$ não pertencem a Δ, o que contradiz a Proposição 17, pois, neste caso, ter-se-ia $\chi(\Delta_\Gamma)=3$. Assim, $2K_3\in\Delta$ e, portanto, $K_{3,3}\in\Delta$ e $K_{3,3}\in\Delta^*$.

Lema 20 *K_3 não pode pertencer a ambos Δ e Δ^*.*

Proof: Tome-se $\Gamma = \langle(123), (456)\rangle$. Neste caso, ΓC_3 x C_3 e, então, Γ pertence à família $\mathcal{M}$. Se $K_3 \in \Delta$, tem-se que D, E e F, pertencem a Δ. Pela Proposição 16 tem-se que $D\cup E$ (que é isomorfo a $D\cup F$) pertence a Δ. Mas então, $(D\cup E)^c = F = K_3$ não pode pertencer a Δ. $\square$

Assim, pode-se assumir que K_3 não pertence a Δ. Agora, tomando o grupo $\Gamma= \langle(12), (3456), (35)\rangle$, tem-se $\Gamma\cong C_4 x C_2 x C_2$ e, portanto, Γ pertence a $\mathcal{M}$.

Lema 21 *As faces de Δ_Γ são $\{\emptyset\}$, $\{A\}$, $\{B\}$, $\{C\}$, $\{A,B\}$, $\{A,C\}$.*

Proof: Cada um dos grafos listados são subgrafos do $K_{3,3}$ e, portanto, faces de Δ_Γ. Por outro lado, $A \cup D$, $B \cup D$, $C \cup D$ e $B \cup C$ contêm o K_3 e, portanto, não pertencem a Δ. Se $D \in \Delta_\Gamma$ então $\chi(\Delta_\Gamma) = 2$ e a Proposição 17 implica que um de $A \cup D$, $B \cup D$ ou $C \cup D$ pertence a Δ. Logo $D \notin \Delta$. $\square$

O vértice A é fixo pela ação de Γ de modo que Γ age sobre $Lg(A,\Delta)$ e os pontos fixos dessa ação são dados por

$$((A, \Delta))_\Gamma = (A, \Delta_\Gamma) = \{C, B\}.$$

Por outro lado, $Lg(A,\Delta)$ é não-evasivo (em princípio isso é verdade para algum vértice, mas então, é verdade para todos pois $Aut(\Delta)$ é transitivo). Então, pela Proposição 17 $(Lg(A,\Delta))_\Gamma$ deve ter característica de Euler igual a 1, uma contradição que completa a prova.