Evasiveness of Graph Properties and Topological Fixed-Point Theorems

Evasiveness of Graph Properties and Topological Fixed-Point Theorems

Carl A. Miller

University of Michigan
USA
carlmi@umich.edu

the essence of knowledge

Boston – Delft

Foundations and Trends® in Theoretical Computer Science

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
USA
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is C. A. Miller, Evasiveness of Graph Properties and Topological Fixed-Point Theorems, Foundation and Trends® in Theoretical Computer Science, vol 7, no 4, pp 337–415, 2011

ISBN: 978-1-60198-664-1

Foundations and Trends® in Theoretical Computer Science

Volume 7 Issue 4, 2011

Editorial Scope

Foundations and Trends® in Theoretical Computer Science will publish survey and tutorial articles in the following topics:

- Algorithmic game theory
- Computational algebra
- Computational aspects of combinatorics and graph theory
- Computational aspects of communication
- Computational biology
- Computational complexity
- Computational geometry
- Computational learning
- Computational Models and Complexity
- Computational Number Theory
- Cryptography and information security
- Data structures
- Database theory
- Design and analysis of algorithms
- Distributed computing
- Information retrieval
- Operations Research
- Parallel algorithms
- Quantum Computation
- Randomness in Computation

Information for Librarians

Foundations and Trends® in Theoretical Computer Science, 2011, Volume 7, 4 issues. ISSN paper version 1551-305X. ISSN online version 1551-3068. Also available as a combined paper and online subscription.

Preface

Beginning with the paper *A Topological Approach to Evasiveness* by Kahn, Saks, and Sturtevant [18], there have been a number of interesting research papers that use topological methods to prove lower bounds on the complexity of graph properties. This is a fascinating topic that lies at the interface between mathematics and theoretical computer science. The goal of this text is to offer an integrated version of the underlying proofs in this body of research. While there are a number of very good expositions available on topological methods in decision-tree complexity, all those that I have seen refer to other sources for the proofs of some topological results (including the key fixed-point theorem of R. Oliver [32]). In this text I have attempted to give a completely self-contained account.

I have not assumed that the reader has any prior background in algebraic topology—all constructions from that subject are developed from scratch. The only prerequisite is a high level of comfort with discrete mathematics and linear algebra. Indeed, though I will sometimes refer to subsets of $\mathbb{R}^n$ for intuition, all the results in this text finally rest on manipulations of finite sets.

While I was preparing this work for publication, I learned about the new book *A Course in Topological Combinatorics* by Mark de Longueville [27]. This book gives a similar treatment of topological methods for proofs of complexity of graph properties, including a proof of Oliver's theorem. Whereas my text is more economical and is intended to offer as direct a route as possible to [18] and its related results, de Longueville's book is broader in scope and encompasses topological methods for other combinatorial problems. I hope that the community will find both works beneficial.

The general flow of the text is to begin with foundational material and then to build up more complex results at a steady pace. The capstone results, which consist of three lower bounds on the complexity of graph properties, appear in the final part of the text. My undergraduate advisor Richard Hain once said that the final goal of mathematics is "to tell a good story." That is what I have attempted to do here, and I hope the reader will enjoy the result.

Foundations and Trends® in
Theoretical Computer Science
Vol. 7, No. 4 (2011) 337–415

DOI: 10.1561/0400000055

Evasiveness of Graph Properties and Topological Fixed-Point Theorems

Carl A. Miller

University of Michigan, Department of Electrical Engineering and Computer Science, 2260 Hayward St., Ann Arbor, MI 48109-2121, USA, carlmi@umich.edu

Abstract

Many graph properties (e.g., connectedness, containing a complete subgraph) are known to be difficult to check. In a decision-tree model, the cost of an algorithm is measured by the number of edges in the graph that it queries. R. Karp conjectured in the early 1970s that all monotone graph properties are evasive—that is, any algorithm which computes a monotone graph property must check all edges in the worst case. This conjecture is unproven, but a lot of progress has been made. Starting with the work of Kahn, Saks, and Sturtevant in 1984, topological methods have been applied to prove partial results on the Karp conjecture. This text is a tutorial on these topological methods. I give a fully self-contained account of the central proofs from the paper of Kahn, Saks, and Sturtevant, with no prior knowledge of topology assumed. I also briefly survey some of the more recent results on evasiveness.

Contents

1

Introduction

Let V be a finite set of size n, and let $\mathbf{G}(V)$ denote the set of undirected graphs on V. For our purposes, a **graph property** is simply a function

$$f\colon \mathbf{G}(V) \to \{0,1\} \tag{1.1}$$

which is such that whenever two graphs Z and Z' are isomorphic, $f(Z) = f(Z')$. A graph Z "has property f" if $f(Z) = 1$.

We can measure the cost of an algorithm for computing f by counting the number of edge-queries that it makes. We assume that these edge-queries are adaptive (i.e., the choice of query may depend on the outcomes of previous queries). An algorithm for f can thus be represented by a binary decision-tree (see Figure 1.1). The **decision-tree complexity of** f, which we denote by $D(f)$, is the least possible depth for a decision-tree that computes f. In other words, $D(f)$ is the number of edge-queries that an optimal algorithm for f has to make in the worst case.

Some graph properties are difficult to compute. For example, let $h(Z) = 1$ if and only if Z contains a cycle. Suppose that an algorithm for h makes queries to an adversary whose goal is to maximize cost. The adversary can adaptively construct a graph Y to foil the algorithm: each

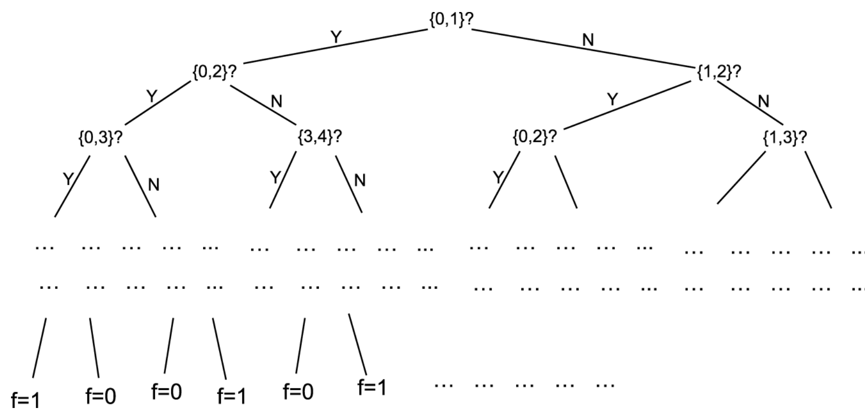

Fig. 1.1 A binary decision tree.

time a pair $(i,j) \in V \times V$ is queried, the adversary answers "yes," unless the inclusion of that edge would necessarily make the graph Y have a cycle, in which case he answers "no." After $\binom{n}{2} - 1$ edge-queries by the algorithm have been made, the known edges will form a tree on the elements of V. The algorithm at this point will have no choice but to query the last unknown edge to determine whether or not a cycle exists. We conclude from this argument that h is a graph property that has the maximal decision-tree complexity $\binom{n}{2}$. Such properties are called **evasive**.

A graph property is **monotone** if it is either always preserved by the addition of edges (monotone-increasing) or always preserved by the deletion of edges (monotone-decreasing). In 1973 the following conjecture was made [34].

Conjecture 1.1 (The Karp Conjecture). All nontrivial monotone graph properties are evasive.

To date, this conjecture is unproven and no counterexamples are known. However in 1984, a seminal paper was published by Kahn et al. [18] which proved the conjecture in some cases. This paper showed that evasiveness can be established through the use of topological fixed-point theorems. It has been followed by many more papers which exploited its method to prove better results.

This text is a tutorial on the topological method of [18]. My goal is to provide background on the problem and to take the reader through all of the necessary proofs. Let us begin with some history.

1.1 Background

Research on the decision-tree complexity of graph properties—including properties for both directed and undirected graphs—dates back at least to the early 1970s [4, 5, 15, 16, 21, 29, 34]. Proofs were given in early papers that certain specific graph properties are evasive (e.g., connectedness, containment of a complete subgraph of fixed size), and that other properties at least have decision-tree complexity $\Omega(n^2)$. Although it was known that there are graph properties whose decision-tree complexity is not $\Omega(n^2)$ (see Example 18 in [4]), Aanderaa and Rosenberg conjectured that all **monotone** graph properties have decision-tree complexity $\Omega(n^2)$ [34]. This conjecture was proved by Rivest and Vuillemin [33] who showed that all monotone graph properties satisfy $D(f) \geq n^2/16$. Kleitman and Kwiatkowski [22] improved this bound to $D(f) \geq n^2/9$.

Underlying some of these proofs is the insight that if a graph property f has nonmaximal decision-tree complexity, then the collection of graphs that satisfy f have some special structure. For example, if f is not evasive, then in the set of graphs satisfying f there must be an equal number of graphs having an odd number of edges and an even number of edges. Rivest and Vuillemin [33] used the fact that if f has decision-tree complexity $\binom{n}{2} - k$, then the weight enumerator of f (i.e., the polynomial $\sum_j c_j t^j$, where c_j is the number of f-graphs containing j edges) must be divisible by $(1 + t)^k$.

A topological method for the evasiveness problem was introduced in [18]. Suppose that h is a monotone-increasing graph property on a vertex set $\{0, 1, \ldots, n-1\}$. Let T be the collection of all graphs that do *not* satisfy h. The set T has the property that if G is in T, then all of its subgraphs are in T. This is a close analogy to the property which defines simplicial complexes in topology. Let $\{x_{ab} \mid 0 \leq i < j < n\}$ be a labeled collection of linearly independent vectors in some vector space $\mathbb{R}^N$. Each graph in T determines a simplex in $\mathbb{R}^N$: one takes the convex

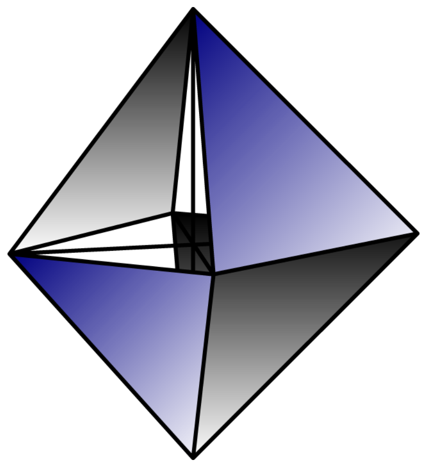

Fig. 1.2 The simplicial complex for "connectedness" on four vertices.

hull of the vectors x_{ab} corresponding to the edges $\{a, b\}$ that are in the graph. The union of these hulls forms a simplicial complex, Γ_h. The complex for "connectedness" on four vertices (represented in three dimensions) is shown in Figure 1.2.

A fundamental insight of [18] is that nonevasiveness can be translated to a topological condition. If h is not evasive, then Γ_h has a certain topological property called **collapsibility**. This property, which we will define formally later in this text, essentially means that Γ_h can be folded into itself and contracted to a single point. This property implies the even–odd weight-balance condition mentioned above, but it is stronger. In particular, it allows for the application of topological fixed-point theorems.

The following theorem is attributed to R. Oliver.

Theorem 1.2 (Oliver [32]). Let Γ be a collapsible simplicial complex. Let G be a finite group which satisfies the following condition:

(*) There is a normal subgroup $G' \subseteq G$, whose size is a power of a prime, such that G/G' is cyclic.

Then, any action of G on Γ has a fixed point.

When $\Gamma = \Gamma_h$, the fixed points of G correspond to graphs, and this theorem essentially forces the existence of certain graphs that do not satisfy h. This theorem is the basis for the following result of [18]:

Theorem 1.3 (Kahn et al. [18]). Let f be a monotone graph property on graphs of size p^k, where p is prime. If f is not evasive, then it must be trivial.

The proof of this theorem essentially proceeds by demonstrating an appropriate group action G on the set of graphs of order p^k such that the only G-invariant graphs are the empty graph and the complete graph.

Thus evasiveness is known for all values of n that are prime powers. What about other values of n? One could hope that if the decision-tree complexity is always $\binom{p}{2}$ when the vertex set is size p, then the quantity $\binom{p}{2}$ is a lower bound for the cases $p+1$, $p+2$, and so forth. Unfortunately there is no known way to show this. However, all is not lost. The following general theorem is also proved in [18].

Theorem 1.4 (Kahn et al. [18]). Let f be a nontrivial monotone graph property of order n. Then,

$$D(f) \geq \frac{n^2}{4} - o(n^2). \tag{1.2}$$

The paper [18] was then followed by several other papers on evasiveness by other authors who used the topological approach to prove new results on evasiveness [3, 8, 19, 23, 37, 38, 40]. Some of these papers found new group actions $G \circlearrowleft \Delta_h$ to exploit in the nonprime cases.

The target results of this exposition are Theorems 1.3 and 1.4, and a theorem by Yao on evasiveness of bipartite graphs [40]. Now let us summarize what we need to do in order to get there.

1.2 Outline of Text

My goal in this exposition is to give a reader who does not know algebraic topology a complete tutorial on topological proofs of evasiveness. Therefore, a fair amount of space will be devoted to building up concepts from algebraic topology. I have tended be economical in my discussions and to develop concepts only on an as-needed basis. Readers who wish to learn more algebraic topology after this exposition may want to consult good references such as [14, 30].

We begin, in *Basic Concepts*, by formalizing the class of simplicial complexes and its relation to the class of graph properties. While we have presented a simplicial complex in this introduction as a subset of $\mathbb{R}^n$, it can also be defined simply as a collection of finite sets. (This is the notion of an **abstract simplicial complex**.) Although the definition in terms of subsets of $\mathbb{R}^n$ is helpful for intuition, the definition in terms of finite sets is the one we will use in all proofs.

A critical construction in this monograph is the set of **homology groups** of a simplicial complex. These groups are algebraic objects which measure the shape of the complex, and also — crucially for our purposes — help us understand the behavior of the complex under automorphisms. *Chain Complexes* defines homology groups and provides some of the standard theory for them.

In *Fixed-Point Theorems* we prove some topological results. The first is the Lefschetz fixed-point theorem. One way to state this theorem is to say that any automorphism of a collapsible simplicial complex has a fixed point. However we instead prove a theorem which applies to the more general class of $\mathbb{F}_p$**-acyclic** complexes. A simplicial complex is $\mathbb{F}_p$-acyclic if its homology groups (over $\mathbb{F}_p$) are trivial. When a simplicial complex is $\mathbb{F}_p$-acyclic it behaves much like a collapsible complex (and in particular, any automorphism has a fixed point). Finally, we prove a version of Theorem 1.2. The proof of the theorem depends on finding a tower of subgroups

$$\{0\} = G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_n = G, \tag{1.3}$$

where each quotient G_i/G_{i-1} is cyclic, and performing an inductive argument.

Results on Decision-Tree Complexity proves Theorem 1.3, a bipartite result of Yao [40], and Theorem 1.4. We conclude with an informal discussion of a few of the more recent results on decision-tree complexity of graph properties [3, 8, 19, 23, 37, 38].

My primary sources for this exposition were [10, 18, 30, 35, 40]. A particular debt is owed to Du and Ko [10], which was my first introduction to the subject.

1.3 Related Topics

I will briefly mention two alternative lines of research that are related to the one I cover here. One can change the measure of complexity that one is using to measure graph properties, and this leads to new problems requiring different methods. A natural variant is the **randomized decision-tree complexity.** Suppose that in our decision-tree model, our algorithm is permitted to make random choices at each step about which edges to check. We define the cost of the algorithm on a particular input graph to be the *expected* number of edge queries, and the cost of the algorithm as a whole to be the maximum of this quantity over all input graphs. The minimum of this quantity over all algorithms is the randomized decision-tree complexity, $R(f)$.

There is a line of research studying the randomized decision tree complexity of monotone graph properties [7, 11, 12, 13, 20, 31, 41]. While it is easy to see that $R(f)$ can be less than $\binom{n}{2}$, there are graph properties for which $R(f)$ is provably $\Omega(n^2)$ (such as the "emptiness property"—the property that the graph contains no edges). It is conjectured that $R(f)$ is always $\Omega(n^2)$ for monotone graph properties, just as in the deterministic model. The best proved lower bound [7, 13] is $\Omega(n^{4/3}(\log n)^{1/3})$.

Another variant of decision-tree complexity is **bounded-error quantum query complexity**. A quantum query algorithm for a graph property uses a quantum "oracle" in its computation. The oracle accepts a quantum state which is a superposition of edge-queries to a graph, and it returns a quantum state which encodes the answers to those queries. The algorithm is permitted to use this oracle along with arbitrary quantum operations to determine its result. The algorithm is permitted to make errors, but the likelihood of an error must be below a fixed bound on all inputs. (See [6].)

In the quantum case it is clear that a lower bound of $\Omega(n^2)$ does not hold: Grover's algorithm [1] can search a space of size N in time

$\Theta(\sqrt{N})$ using an oracle model. With a modified version of Grover's algorithm, one can compute the emptiness property in time $\Theta(n)$. There are a number of other monotone properties for which the quantum query complexity is known to be $o(n^2)$ (see [9] for a good summary on this topic). It is conjectured that all monotone graph properties have quantum query complexity $\Omega(n)$. The best proved lower bound is $\Omega(n^{2/3})$, from an unpublished result attributed to Santha and Yao (see [36]).

1.4 Further Reading

Other expositions about topological proofs of evasiveness can be found in [10] (in the context of computational complexity theory) and [24] (in the context of algebraic topology), and also in Lovasz's lecture notes [26]. A reader who wishes to learn more about algebraic topology can consult [30], or, for a more advanced treatment, [14]. For the particular subject of the topology of complexes arising from graphs, there is an extensive treatment [17], which builds further on many of the concepts that I will discuss here. And finally, for readers who generally enjoy reading about applications of topology to problems in discrete mathematics, the excellent book [28] contains more material of the same flavor. It involves applications of a different topological result (the Borsuk–Ulam theorem) to some problems in elementary mathematics.

References

[1] A. Ambainis, "Quantum query complexity and lower bounds," in *Classical and New Paradigms of Computation and their Complexity Hierarchies*, vol. 23 of *Trends in Logic*, pp. 15–32, 2004.

[2] R. Ash, *Basic Abstract Algebra.* Dover Publications, 2007.

[3] L. Babai, A. Banerjee, R. Kulkarni, and V. Naik, "Evasiveness and the distribution of prime numbers," in *Symposium on Theoretical Aspects of Computer Science*, pp. 71–82, 2010.

[4] M. Best, P. Emde Boas, and H. Lenstra, "A sharpened version of the Aanderaa-Rosenberg conjecture," *Stichting Mathematisch Centrum. Zuivere Wiskunde*, vol. ZW 30/74, pp. 1–20, 1974.

[5] B. Bollobas, "Complete subgraphs are elusive," *Journal of Combinatorial Theory, Series B*, vol. 21, no. 1, pp. 1–7, August 1976.

[6] H. Buhrman, R. Cleve, R. de Wolf, and C. Zalka, "Bounds for small-error and zero-error quantum algorithms," in *Proceedings of the 40th Annual Symposium on Foundations of Computer Science*, pp. 358–368, 1999.

[7] A. Chakrabati and S. Khot, "Improved lower bounds on the randomized complexity of graph properties," *Random Structures and Algorithms*, vol. 30, no. 3, pp. 427–440, 2007.

[8] A. Chakrabati, S. Khot, and Y. Shi, "Evasiveness of subgraph containment and related properties," *SIAM Journal on Computing*, vol. 31, no. 3, pp. 866–875, 2002.

[9] A. Childs and R. Kothari, "Quantum query complexity of minor-closed graph properties," in *Proceedings of the 28th International Symposium on Theoretical Aspects of Computer Science*, pp. 661–672, 2011.

[10] D. Du and K. Ko, *Theory of Computational Complexity.* Wiley, 2000.

[11] E. Friedgut, J. Kahn, and A. Wigderson, "Computing graph properties by randomized subcube partitions," in *Randomization and Approximation Techniques in Computer Science*, vol. 2483 of *Lecture Notes in Computer Science*, pp. 105–113, 2002.

[12] H. Groger, "On the randomized complexity of monotone graph properties," *Acta Cybernetica*, vol. 10, no. 3, pp. 119–127, 1992.

[13] P. Hajnal, "An $\omega(n^{\frac{4}{3}})$ lower bound on the randomized complexity of graph properties," *Combinatorica*, vol. 11, no. 2, pp. 131–143, 1991.

[14] A. Hatcher, *Algebraic Topology*. Cambridge University Press, 2002.

[15] R. Holt and E. Reingold, "On the time required to detect cycles and connectivity in graphs," *Mathematical Systems Theory*, vol. 6, no. 1–2, pp. 103–106, 1972.

[16] J. Hopcroft and R. Tarjan, "Efficient planarity testing," *Journal of the ACM*, vol. 21, no. 4, pp. 549–568, October 1974.

[17] J. Jonsson, *Simplicial Complexes of Graphs*. Springer-Verlag, 2008.

[18] J. Kahn, M. Saks, and D. Sturtevant, "A topological approach to evasiveness," *Combinatorica*, vol. 4, no. 4, pp. 297–306, 1984.

[19] V. King, "A lower bound for the recognition of digraph properties," *Combinatorica*, vol. 10, no. 1, pp. 53–59, 1990.

[20] V. King, "An $\omega(n^{5/4})$ lower bound on the randomized complexity of graph properties," *Combinatorica*, vol. 11, no. 1, pp. 23–32, 1991.

[21] D. Kirkpatrick, "Determining graph properties from matrix representations," in *Proceedings of Sixth Annual ACM Symposium on Theory of Computing*, pp. 84–90, 1974.

[22] D. Kleitman and D. Kwiatowksi, "Further results on the Aanderaa-Rosenberg conjecture," *Journal of Combinatorial Theory, Series B*, vol. 28, pp. 85–95, 1980.

[23] T. Korneffel and E. Triesch, "An asymptotic bound for the complexity of monotone graph properties," *Combinatorica*, vol. 30, no. 6, pp. 735–743, 2010.

[24] D. Kozlov, *Combinatorial Algebraic Topology*. Berlin Heidelberg: Springer, 2008.

[25] S. Lang, *Algebra*. Number 211 in Graduate Texts in Mathematics. Springer-Verlag, rev. 3rd Edition, 2002.

[26] L. Lovasz and N. Young, "Lecture notes on evasiveness of graph properties," arXiv:cs/0205031v1, May 2002.

[27] Mark de Longueville, *A Course in Topological Combinatorics*. Springer, 2013.

[28] J. Matousek, *Using the Borsuk-Ulam Theorem*. Springer-Verlag, corrected 2nd printing Edition, 2008.

[29] E. Milner and D. Welsh, "On the computational complexity of graph theoretical properties," in *Proceedings of the Fifth British Combinatorial Conference*, pp. 471–487, 1975.

[30] J. Munkres, *Elements of Algebraic Topology*. Addison-Wesley, 1984.

[31] R. O'Donnell, M. Saks, O. Schramm, and R. Serveido, "Every decision tree has an influential variable," in *Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science*, pp. 31–39, 2005.

[32] R. Oliver, "Fixed-point sets of group actions on finite acyclic complexes," *Commentarii mathematici Helvetici*, vol. 50, pp. 155–177, 1975.

[33] R. Rivest and J. Vuillemin, "On recognizing graph properties from adjacency matrices," *Theoretical Computer Science*, vol. 3, pp. 371–384, 1976.

[34] A. Rosenberg, "On the time required to recognize properties of graps: A problem," *SIGACT News*, vol. 5, no. 4, pp. 15–16, October 1973.

[35] P. Smith, "Fixed-point theorems for periodic transformations," *American Journal of Mathematics*, vol. 63, no. 1, pp. 1–8, 1941.

[36] X. Sun, A. Yao, and S. Zhang, "Graph properties and circular functions: How low can quantum query complexity go?," in *Proceedings of the IEEE Annual Conference on Computation Complexity*, pp. 286–293, 2004.

[37] E. Triesch, "Some results on elusive graph properties," *SIAM Journal on Computing*, vol. 23, no. 2, pp. 247–254, 1994.

[38] E. Triesch, "On the recognition complexity of some graph properties," *Combinatorica*, vol. 16, no. 2, pp. 259–268, 1996.

[39] V. Welker, "Constructions preserving evasiveness and collapsibility," *Discrete Mathematics*, vol. 207, no. 1–3, pp. 243–255, 1999.

[40] A. Yao, "Monotone bipartite graph properties are evasive," *SIAM Journal on Computing*, vol. 17, no. 3, pp. 517–520, June 1988.

[41] A. Yao, "Lower bounds to randomized algorithms for graph properties," *Journal of Computer and System Sciences*, vol. 42, no. 3, pp. 267–287, June 1991.

[42] D. Zagier, "Newman's short proof of the prime number theorem," *American Mathematical Monthly*, vol. 104, no. 8, pp. 705–708, October 1997.