The Complexity of Mathematics

Frank Vega
Joysonic, Uzun Mirkova 5, Belgrade, 11000, Serbia
vega.frank@gmail.com

Abstract

In mathematics, the Riemann hypothesis is a conjecture that the Riemann zeta function has its zeros only at the negative even integers and complex numbers with real part 1/2. Many consider it to be the most important unsolved problem in pure mathematics. It is one of the seven Millennium Prize Problems selected by the Clay Mathematics Institute to carry a US 1,000,000 prize for the first correct solution. We prove the Riemann hypothesis using the Complexity Theory. Number theory is a branch of pure mathematics devoted primarily to the study of the integers and integer-valued functions. The Goldbach's conjecture is one of the most important and unsolved problems in number theory. Nowadays, it is one of the open problems of Hilbert and Landau. We demonstrate the Goldbach's conjecture is true using the Complexity Theory as well. An important complexity class is NSPACE(S(n)) for some S(n). These mathematical proofs are based on if some unary language belongs to NSPACE(S(log n)), then the binary version of that language belongs to NSPACE(S(n)) and vice versa.

2012 ACM Subject Classification Theory of computation → Complexity classes; Theory of computation → Regular languages; Theory of computation → Problems, reductions and completeness

Keywords and phrases complexity classes, regular languages, reduction, complement, primes, number theory

1 Introduction

1.1 The Riemann hypothesis

In mathematics, the Riemann hypothesis is a conjecture that the Riemann zeta function has its zeros only at the negative even integers and complex numbers with real part $\frac{1}{2}$. Many consider it to be the most important unsolved problem in pure mathematics [15]. It is of great interest in number theory because it implies results about the distribution of prime numbers [15]. It was proposed by Bernhard Riemann (1859), after whom it is named [15]. In 1915, Ramanujan proved that under the assumption of the Riemann hypothesis, the inequality:

$$\sum_{d|n} d < e^{\gamma} \times n \times \log \log n$$

holds for all sufficiently large n, where $\gamma \approx 0.57721$ is the Euler's constant and $d|n$ means that the natural number d divides n [11]. The largest known value that violates the inequality is $n = 5040$. In 1984, Guy Robin proved that the inequality is true for all $n > 5040$ if and only if the Riemann hypothesis is true [11]. Using this inequality, we prove the Riemann hypothesis is true.

1.2 The Goldbach's conjecture

The Goldbach's original conjecture, written on 7 June 1742 in a letter to Leonhard Euler, states: "... at least it seems that every number that is greater than 2 is the sum of three primes" [5]. This is known as the ternary Goldbach conjecture. We call a prime as a natural number that is greater than 1 and has exactly two divisors, 1 and the number itself [17]. However, the mathematician Christian Goldbach considered 1 as a prime number. Euler replied in a letter dated 30 June 1742 the following statement: "Every even integer greater than 2 can be written as the sum of two primes" [5]. This is known as the strong Goldbach conjecture.

Using Vinogradov's method, Van der Corput and Estermann showed that almost all even numbers can be written as the sum of two primes (in the sense that the fraction of even numbers which can be so written tends towards 1) [16], [6]. In 1973, Chen showed that every sufficiently large even number can be written as the sum of some prime number and a semi-prime [3]. The strong Goldbach conjecture implies the conjecture that all odd numbers greater than 7 are the sum of three odd primes, which is known today as the weak Goldbach conjecture [5]. In 2012 and 2013, Peruvian mathematician Harald Helfgott published a pair of papers claiming to improve major and minor arc estimates sufficiently to unconditionally prove the weak Goldbach conjecture [9], [10]. In this work, we prove the strong Goldbach's conjecture is true.

2 Theory and Methods

We use o-notation to denote an upper bound that is not asymptotically tight. We formally define $o(g(n))$ as the set

$$o(g(n)) = \{f(n) : \textit{ for any positive constant } c > 0, \textit{ there exists a constant}$$

$$n_0 > 0 \textit{ such that } 0 \leq f(n) < c \times g(n) \textit{ for all } n \geq n_0\}.$$

For example, $2 \times n = o(n^2)$, but $2 \times n^2 \neq o(n^2)$ [4]. In theoretical computer science and formal language theory, a regular language is a formal language that can be expressed using a regular expression [2]. On the one hand, the complexity class $\mathit{DSPACE}(f(n))$ is the set of decision problems that can be solved by a deterministic Turing machine M, using space $f(n)$, where n is the length of the input [13]. On the other hand, the complexity class $\mathit{NSPACE}(f(n))$ is the set of decision problems that can be solved by a nondeterministic Turing machine M, using space $f(n)$, where n is the length of the input [13].

3 Results

3.1 The Complexity of PRIMES

The checking whether a number is prime can be decided in polynomial time by a deterministic Turing machine [1]. This problem is known as $PRIMES$ [1].

▶ **Theorem 1.** *$PRIMES \notin \mathit{NSPACE}(S(n))$ for all $S(n) = o(\log n)$.*

Proof. If we assume that $PRIMES \in \mathit{NSPACE}(o(\log n))$, then the unary version should be regular. Certainly, the standard space translation between the unary and binary languages actually works for nondeterministic machines with small space [7]. This means that if some language belongs to $\mathit{NSPACE}(S(n))$, then the unary version of that language belongs to $\mathit{NSPACE}(S(\log n))$ [7]. In this way, when $PRIMES \in \mathit{NSPACE}(o(\log n))$, then the unary version should be in $\mathit{NSPACE}(o(\log \log n))$ and we know that $\mathit{REG} = \mathit{NSPACE}(o(\log \log n))$ [13], [7]. Since we know that the unary version of $PRIMES$ is non-regular [12], then we obtain that $PRIMES \notin \mathit{NSPACE}(S(n))$ for all $S(n) = o(\log n)$. ◀

3.2 The Riemann hypothesis

▶ **Definition 2.** *We define the Robin's language* L_R *as follows:*

$$L_R = \{0^n\#0^{m_1}\#0^{m_2} : n \in \mathbb{N} \wedge n > 5040 \wedge m_1 = (\sigma(n) - n)$$

$$\wedge\ m_2 = \lceil e^{\gamma} \times n \times \log\log n \rceil \wedge m_1 + n < m_2\}$$

where $\#$ *is the blank symbol,* $\lceil \ldots \rceil$ *is the ceiling function,* γ *is the Euler's constant and* $\sigma(n) = \sum_{d|n} d$ *[11]. We define the language* coL_R *as*

$$coL_R = \{0^n\#0^{m_1}\#0^{m_2} : n \in \mathbb{N} \wedge n > 5040 \wedge m_1 = (\sigma(n) - n)$$

$$\wedge\ m_2 = \lceil e^{\gamma} \times n \times \log\log n \rceil \wedge m_1 + n \geq m_2\}$$

where coL_R *is the complement language of* L_R*.*

▶ **Definition 3.** *We define the verification Robin's language* L_{VR} *as follows:*

$$L_{VR} = \{(n, m_1, m_2) : \text{ such that } 0^n\#0^{m_1}\#0^{m_2} \in L_R\}.$$

Besides, we define the language coL_{VR} *as*

$$coL_{VR} = \{(n, m_1, m_2) : \text{ such that } 0^n\#0^{m_1}\#0^{m_2} \in coL_R\}$$

where coL_{VR} *is the complement language of* L_{VR}*.*

▶ **Lemma 4.** coL_R *is the unary representation of* coL_{VR}*.*

Proof. This is trivially true from the definition of these languages. ◀

▶ **Theorem 5.** $L_{VR} \notin NSPACE(S(n))$ *for all* $S(n) = o(\log n)$*.*

Proof. The language L_{VR} cannot be computed in $NSPACE(S(n))$ for some $S(n) = o(\log n)$, because of this would imply that the problem $PRIMES$ belongs to $NSPACE(S(n))$ for some $S(n) = o(\log n)$ as well. Certainly if this could be true, then we can find $m_2 = \lceil e^{\gamma} \times p \times \log\log p \rceil$ and check whether the triple $(p, 1, m_2)$ is an element of L_{VR} and thus, we could decide whether p is prime. Indeed, a number p is prime if and only if the sum of its divisors is $p + 1$ [8]. This could be nondeterministically done on input p just choosing arbitrarily another number m_2, but instead of putting in the work tapes, then this will put with p and 1 in the output tape just using constant space. We are able to do this, because of m_2 should be polynomially bounded by the input p. After that, we use the space composition reduction just using the previous output of p, 1 and some integer m_2 into a new nondeterministic Turing machine that would decide whether the instance belongs to L_{VR} in $NSPACE(S(n))$ for some $S(n) = o(\log n)$ using $(p, 1, m_2)$ as input [14]. Since $NSPACE(S(n))$ for some $S(n) = o(\log n)$ is closed under $NSPACE$-reductions with constant space, then the whole computation could be done in $NSPACE(S(n))$ for some $S(n) = o(\log n)$. Certainly, an $NSPACE$-reduction with constant space could be done in $DSPACE(o(\log\log n))$ [13]. This is possible, because the Robin inequality is always true on p for every prime number p. However, this would be a contradiction according to Theorem 1, since the language $PRIMES \notin NSPACE(S(n))$ for all $S(n) = o(\log n)$. Consequently, we obtain that $L_{VR} \notin NSPACE(S(n))$ for all $S(n) = o(\log n)$. ◀

▶ **Theorem 6.** $coL_{VR} \notin NSPACE(S(n))$ *for all* $S(n) = o(\log n)$*.*

Proof. The reason is because of $\mathit{NSPACE}(S(n))$ is closed under complement for $S(n) \geq \log n$ [13]. In this way, this is a direct consequence of Theorem 5. ◀

▶ **Theorem 7.** *The Riemann hypothesis is true.*

Proof. We may have only three options: coL_R is equal to the empty set or $coL_R \in \mathit{REG}$ and coL_R is not empty or coL_R is non-regular and coL_R is infinite, since every finite set is regular [14]. Let's assume the possibility of $coL_R \in \mathit{REG}$ and coL_R is not empty. Nevertheless, this implies that the exponentially more succinct version of coL_R, that is coL_{VR}, should be in $\mathit{NSPACE}(S(n))$ for some $S(n) = o(\log n)$, because of $\mathit{REG} = \mathit{NSPACE}(o(\log \log n))$ and the same algorithm that decides coL_R within $\mathit{NSPACE}(o(\log \log n))$ could be easily transformed into a slightly modified algorithm that decides coL_{VR} within $\mathit{NSPACE}(S(n))$ for some $S(n) = o(\log n)$ [13], [7]. Actually, coL_R is the unary version of coL_{VR} due to Lemma 4. As we mentioned before, the standard space translation between the unary and binary languages actually works for nondeterministic machines with small space [7]. This means that if some unary language belongs to $\mathit{NSPACE}(S(\log n))$, then the binary version of that language belongs to $\mathit{NSPACE}(S(n))$ [7]. In this way, we obtain that $coL_R \notin \mathit{REG}$, since it is not possible that $coL_R \in \mathit{NSPACE}(o(\log \log n))$ under the result of $coL_{VR} \notin \mathit{NSPACE}(S(n))$ for all $S(n) = o(\log n)$ as a consequence of Theorem 6. Consequently, we obtain a contradiction just assuming that $coL_R \in \mathit{REG}$ and coL_R is not empty. Therefore, coL_R is infinite or coL_R is equal to the empty set. Hence, we obtain that the Riemann hypothesis is true when coL_R is equal to the empty set or the Robin's inequality has an infinite number of counterexamples when coL_R is infinite. However, the asymptotic growth rate of the sigma function can be expressed by [11]:

$$\limsup_{n \to \infty} \frac{\sigma(n)}{n \times \log \log n} = e^{\gamma}$$

where lim sup is the limit superior and $\sigma(n) = \sum_{d|n} d$. In this way, if the Robin's inequality has an infinite number of counterexamples, then the previous limit superior should be false. Since this is a previous checked result, then we have the Riemann hypothesis is true as the remaining only option. ◀

3.3 The Goldbach's conjecture

▶ **Definition 8.** *We define the Goldbach's language L_G as follows:*

$$L_G = \{0^{2\times n}\#0^p\#0^q : n \in \mathbb{N} \wedge n > 2 \wedge p \textit{ and } q \textit{ are odd primes } \wedge 2 \times n = p + q\}$$

where # is the blank symbol. We define the language coL_G as

$$coL_G = \{0^{2\times n}\#0^i\#0^j : n \in \mathbb{N} \wedge n > 2 \wedge 2 \times n = i + j$$

$$\wedge \textit{ there are not odd primes } p \textit{ and } q \textit{ such that } 2 \times n = p + q\}$$

where coL_G is the complement language of L_G.

▶ **Definition 9.** *We define the verification Goldbach's language L_{VG} as follows:*

$$L_{VG} = \{(2 \times n, p, q) : \textit{ such that } 0^{2\times n}\#0^p\#0^q \in L_G\}.$$

Besides, we define the language coL_{VG} as

$$coL_{VG} = \{(2 \times n, i, j) : \textit{ such that } 0^{2\times n}\#0^i\#0^j \in coL_G\}$$

where coL_{VG} is the complement language of L_{VG}.

▶ **Lemma 10.** *coL_G is the unary representation of coL_{VG}.*

Proof. This is trivially true from the definition of these languages. ◀

▶ **Theorem 11.** *$L_{VG} \notin NSPACE(S(n))$ for all $S(n) = o(\log n)$.*

Proof. The language L_{VG} cannot be computed in $NSPACE(S(n))$ for some $S(n) = o(\log n)$, because of this would imply that the problem $PRIMES$ belongs to $NSPACE(S(n))$ for some $S(n) = o(\log n)$ as well. Certainly, if this could be true, then we can take any number p and check whether p is prime. This could be nondeterministically done on input p just deterministically generating the numbers $p + 3$ and 3 and nondeterministically choosing an arbitrary number q, but instead of putting in the work tapes, then we will put them to the output tape just using constant space. After that, we use the space composition reduction just using the previous output of $(p + 3, 3, q)$ as input into a new nondeterministic Turing machine that would decide whether the instance belongs to L_{VG} in $NSPACE(S(n))$ for some $S(n) = o(\log n)$. Indeed, the nondeterministic computation will accept this input if and only if the nondeterministic generated number q is equal to p and p is prime. In this reduction, we assume the initial string p has a binary representation with the least significant bit in the first position within the input tape from left to right. In this way, it will be possible to deterministically generate $p + 3$ using constant space. Since $NSPACE(S(n))$ for some $S(n) = o(\log n)$ is closed under $NSPACE$-reductions with constant space, then the whole computation could be done in $NSPACE(S(n))$ for some $S(n) = o(\log n)$. Certainly, an $NSPACE$-reduction with constant space could be done in $DSPACE(o(\log \log n))$ [13]. This is possible, because the strong Goldbach's conjecture is always true on $p + 3$ for every prime number p. Nevertheless, this would be a contradiction according to Theorem 1, since the language $PRIMES \notin NSPACE(S(n))$ for all $S(n) = o(\log n)$. Consequently, we obtain that $L_{VG} \notin NSPACE(S(n))$ for all $S(n) = o(\log n)$. ◀

▶ **Theorem 12.** *$coL_{VG} \notin NSPACE(S(n))$ for all $S(n) = o(\log n)$.*

Proof. The reason is because of $NSPACE(S(n))$ is closed under complement for $S(n) \geq \log n$ [13]. In this way, this is a direct consequence of Theorem 11. ◀

▶ **Theorem 13.** *The strong Goldbach's conjecture is true.*

Proof. We may have only three options: coL_G is equal to the empty set or $coL_G \in REG$ and coL_G is not empty or coL_G is non-regular and coL_G is infinite, since every finite set is regular [14]. Let's assume the possibility of $coL_G \in REG$ and coL_G is not empty. However, this implies that the exponentially more succinct version of coL_G, that is coL_{VG}, should be in $NSPACE(S(n))$ for some $S(n) = o(\log n)$, because we would have $REG = NSPACE(o(\log \log n))$ and the same algorithm that decides coL_G within the complexity $NSPACE(o(\log \log n))$ could be easily transformed into a slightly modified algorithm that decides coL_{VG} within $NSPACE(S(n))$ for some $S(n) = o(\log n)$ [13], [7]. Actually, coL_G is the unary version of coL_{VG} due to Lemma 10. As we mentioned before, the standard space translation between the unary and binary languages actually works for nondeterministic machines with small space [7]. This means that if some unary language belongs to $NSPACE(S(\log n))$, then the binary version of that language belongs to $NSPACE(S(n))$ [7]. Consequently, we obtain that $coL_G \notin REG$, since it is not possible that $coL_G \in NSPACE(o(\log \log n))$ under the result of $coL_{VG} \notin NSPACE(S(n))$ for all $S(n) = o(\log n)$ as result of Theorem 12. In this way, we obtain a contradiction just assuming that $coL_G \in REG$ and coL_G is not empty. Therefore, coL_G is infinite or coL_G is equal to the empty set. Hence, we have the strong Goldbach's conjecture is true when coL_G is equal to the empty set or this has an infinite number of counterexamples when coL_G is infinite. However, if the strong Goldbach's conjecture has an infinite number of counterexamples, then this violates the known fact that almost all even numbers are sum of odd primes [16], [6]. As result, we obtain the strong Goldbach's conjecture is true as the remaining only option. ◀

References

1 Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. PRIMES is in P. *Annals of Mathematics*, 160(2):781–793, 2004. doi:10.4007/annals.2004.160.781.

2 Alfred V. Aho and John E. Hopcroft. *The Design and Analysis of Computer Algorithms*. Pearson Education India, 1974.

3 Jing-run Chen. On the Representation of a Large Even Integer as the Sum of a Prime and the Product of Two Primes at Most. *Sci. Sinica*, 16:157–176, 1973.

4 Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. *Introduction to Algorithms*. The MIT Press, 3 edition, 2009.

5 Leonard Eugene Dickson. *History of the Theory of Numbers: Divisibility and Primality*, volume 1. New York, Dover, 2005.

6 Theodor Estermann. On Goldbach's problem: Proof that almost all even positive integers are sums of two primes. *Proceedings of the London Mathematical Society*, 2(1):307–314, 1938.

7 Viliam Geffert and Dana Pardubská. Unary Coded NP-Complete Languages in ASPACE (log log n). *International Journal of Foundations of Computer Science*, 24(07):1167–1182, 2013. doi:10.1007/978-3-642-31653-1_16.

8 Godfrey Harold Hardy and Edward Maitland Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, 1979.

9 Harald A. Helfgott. Minor arcs for Goldbach's problem. *arXiv preprint arXiv:1205.5252*, 2012.

10 Harald A. Helfgott. Major arcs for Goldbach's theorem. *arXiv preprint arXiv:1305.2897*, 2013.

11 Jeffrey C. Lagarias. An elementary problem equivalent to the riemann hypothesis. *The American Mathematical Monthly*, 109(6):534–543, 2002.

12 David Matuszek. Pumping Lemma Example 3, February 1996. In The Pumping Lemma Lecture at https://www.seas.upenn.edu/~cit596/notes/dave/pumping6.html. Retrieved 10 June 2020.

13 Pascal Michel. A survey of space complexity. *Theoretical computer science*, 101(1):99–132, 1992. doi:10.1016/0304-3975(92)90151-5.

14 Christos H. Papadimitriou. *Computational complexity*. Addison-Wesley, 1994.

15 Peter Sarnak. Problems of the millennium: The riemann hypothesis (2004), April 2005. In Clay Mathematics Institute at http://www.claymath.org/library/annual_report/ar2004/04report_prizeproblem.pdf. Retrieved 10 June 2020.

16 Johannes Gualtherus Van der Corput. Sur l'hypothèse de Goldbach pour presque tous les nombres pairs. *Acta Arithmetica*, 2(2):266–290, 1936.

17 David G. Wells. *Prime Numbers, The Most Mysterious Figures in Math*. John Wiley & Sons, Inc., 2005.