The Complexity of Mathematics

Frank Vega

June 7, 2020

The Complexity of Mathematics

Frank Vega[1[0000−0001−8210−4126]]

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 show the Goldbach's conjecture is true or this has an infinite number of counterexamples using the Complexity Theory as well. An important complexity class is 1NSPACE(S(n)) for some S(n). These mathematical proofs are based on if some unary language belongs to 1NSPACE(S(log n)), then the binary version of that language belongs to 1NSPACE(S(n)) and vice versa.

Keywords: complexity classes · regular languages · reduction · number theory · primes · one-way.

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 [16]. It is of great interest in number theory because it implies results about the distribution of prime numbers [16]. It was proposed by Bernhard Riemann (1859), after whom it is named [16]. 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 [12]. 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 [12]. 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" [6]. 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 [18]. 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" [6]. 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) [5], [7]. 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 [6]. 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 [10], [11]. In this work, we prove the strong Goldbach's conjecture is true or this has an infinite number of counterexamples.

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]. The complexity class that contains all the regular languages is REG. The two-way Turing machines may move their head on the input tape into two-way (left and right directions) while the one-way Turing machines are not allowed to move the head on the input tape to the left [14]. The complexity class *1NSPACE*$(f(n))$ is the set of decision problems that can be solved by a nondeterministic one-way Turing machine M, using space $f(n)$, where n is the length of the input [14].

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. *$PRIMES \notin$ 1NSPACE$(S(n))$ for all $S(n) = o(\log n)$.*

Proof. If we assume that $PRIMES \in$ *1NSPACE*$(o(\log n))$, 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 [8]. This means that if some language belongs to *1NSPACE*$(S(n))$, then the unary version of that language belongs to *1NSPACE*$(S(\log n))$ [8]. In this way, when $PRIMES \in$ *1NSPACE*$(o(\log n))$, then the unary version should be in *1NSPACE*$(o(\log \log n))$ and we know that $REG =$ *1NSPACE*$(o(\log \log n))$ [14], [8]. Since we know that the unary version of $PRIMES$ is non-regular [13], then we obtain that $PRIMES \notin$ *1NSPACE*$(S(n))$ for all $S(n) = o(\log n)$.

3.2 The Riemann hypothesis

Definition 1. *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 and $\sigma(n) = \sum_{d|n} d$ [12]. 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.

Theorem 2. *If the Riemann hypothesis is true, then the Robin's language L_R is non-regular.*

Proof. We can easily prove this using the Pumping lemma for regular languages [17].

Definition 2. *We define the verification Robin's language L_{VR} as follows:*

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

Lemma 1. *The Robin's language L_R is the unary representation of the verification Robin's language L_{VR}.*

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

Theorem 3. *$L_{VR} \notin$ 1NSPACE($S(n)$) for all $S(n) = o(\log n)$.*

Proof. The language L_{VR} cannot be computed in *1NSPACE*($S(n)$) for some $S(n) = o(\log n)$, because of this would imply that the problem $PRIMES$ belongs to *1NSPACE*($S(n)$) 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 $p + 1$ [9]. 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 in one-way. 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 *1NSPACE*($S(n)$) for some $S(n) = o(\log n)$ using $(p, 1, m_2)$ as input [15]. Since *1NSPACE*($S(n)$) for some $S(n) = o(\log n)$ is closed under *1NSPACE*-reductions with constant space, then the whole computation could be done in *1NSPACE*($S(n)$) for some $S(n) = o(\log n)$. However, this would be a contradiction according to Theorem 1, since the language $PRIMES \notin$ *1NSPACE*($S(n)$) for all $S(n) = o(\log n)$. Consequently, we obtain that $L_{VR} \notin$ *1NSPACE*($S(n)$) for all $S(n) = o(\log n)$.

Theorem 4. *The Riemann hypothesis is true.*

Proof. If the Riemann hypothesis is false, then $L_R \in REG$ or L_R is non-regular and its complement coL_R is infinite, since every finite set is regular and REG is also closed under complement [15]. Let's assume the possibility of $L_R \in REG$. Nevertheless, this implies that the exponentially more succinct version of L_R, that is L_{VR}, should be in *1NSPACE*($S(n)$) for some $S(n) = o(\log n)$, because of $REG =$ *1NSPACE*($o(\log \log n)$) and the same algorithm that decides L_R within *1NSPACE*($o(\log \log n)$) could be easily transformed into a slightly modified algorithm that decides L_{VR} within *1NSPACE*($S(n)$) for some $S(n) = o(\log n)$ [14], [8]. Actually, L_R is the unary version of L_{VR} due to Lemma 1. As we mentioned before, the standard space translation between the unary and binary languages actually works for nondeterministic machines with small space [8]. This means that if some unary language belongs to *1NSPACE*($S(\log n)$), then the binary version of that language belongs to *1NSPACE*($S(n)$) [8]. In this way, we obtain that $L_R \notin REG$, since it is not possible that $L_R \in$ *1NSPACE*($o(\log \log n)$) under the result of $L_{VR} \notin$ *1NSPACE*($S(n)$) for all $S(n) = o(\log n)$ as a consequence of Theorem 3. Consequently, we obtain a contradiction just assuming that the Riemann hypothesis is false and $L_R \in REG$. Hence, we obtain that the Riemann hypothesis is true or the Robin's inequality has an infinite number of counterexamples. However, the asymptotic growth rate of the sigma function can be expressed by [12]:

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

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 3. *We define the Goldbach's language L_G as follows:*

$$L_G = \{0^{2\times n}\#0^p0^q : n \in \mathbb{N} \wedge n > 2 \wedge p \textit{ and } q \textit{ are odd primes } \wedge 2\times n = p+q\}$$

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

$$coL_G = \{0^{2\times n}\#0^{2\times n} : n \in \mathbb{N} \wedge n > 2 \wedge$$
$$\textit{there are not odd primes } p \textit{ and } q \textit{ such that } 2\times n = p+q\}$$

where coL_G is the complement language of L_G.

Theorem 5. *If the strong Goldbach's conjecture is true, then the Goldbach's language L_G is non-regular.*

Proof. We can easily prove this using the Pumping lemma for regular languages [17].

Definition 4. *We define the verification Goldbach's language L_{VG} as follows:*

$$L_{VG} = \{(2\times n, p, q) : \textit{ such that } 0^{2\times n}\#0^p0^q \in L_G\}.$$

Lemma 2. *The Goldbach's language L_G is the unary representation of the verification Goldbach's language L_{VG}.*

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

Theorem 6. *$L_{VG} \notin$ 1NSPACE$(S(n))$ for all $S(n) = o(\log n)$.*

Proof. The language L_{VG} cannot be computed in *1NSPACE*$(S(n))$ for some $S(n) = o(\log n)$, because of this would imply that the problem $PRIMES$ belongs to *1NSPACE*$(S(n))$ 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 in one-way. 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 *1NSPACE*$(S(n))$ for some $S(n) = o(\log n)$. Indeed, the nondeterministic one-way 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 $p+3$ in one-way using constant space. Since *1NSPACE*$(S(n))$ for some $S(n) = o(\log n)$ is closed under *1NSPACE*-reductions with constant space, then the whole computation could be done in *1NSPACE*$(S(n))$ for some $S(n) = o(\log n)$. Nevertheless, this would be a contradiction according to Theorem 1, since the language $PRIMES \notin$ *1NSPACE*$(S(n))$ for all $S(n) = o(\log n)$. Consequently, we obtain that $L_{VG} \notin$ *1NSPACE*$(S(n))$ for all $S(n) = o(\log n)$.

Theorem 7. *The strong Goldbach's conjecture is true or this has an infinite number of counterexamples.*

Proof. If the strong Goldbach's conjecture is false, then $L_G \in REG$ or L_G is non-regular and its complement coL_G is infinite, since every finite set is regular and REG is also closed under complement [15]. Let's assume the possibility of $L_G \in REG$. However, this implies that the exponentially more succinct version of L_G, that is L_{VG}, should be in *1NSPACE*$(S(n))$ for some $S(n) = o(\log n)$, because we would have $REG =$ *1NSPACE*$(o(\log\log n))$ and the same algorithm that decides L_G within the complexity *1NSPACE*$(o(\log\log n))$ could be easily transformed into a slightly modified algorithm that decides L_{VG} within *1NSPACE*$(S(n))$ for some $S(n) = o(\log n)$ [14], [8]. Actually, L_G is the unary version of L_{VG} due to Lemma 2. As we mentioned before, the standard space translation between the unary and binary languages actually works for non-deterministic machines with small space [8]. This means that if some unary language belongs to *1NSPACE*$(S(\log n))$, then the binary version of that language belongs to *1NSPACE*$(S(n))$ [8]. Consequently, we obtain that $L_G \notin REG$, since it is not possible that $L_G \in$ *1NSPACE*$(o(\log\log n))$ under the result of $L_{VG} \notin$ *1NSPACE*$(S(n))$ for all $S(n) = o(\log n)$ as result of Theorem 6. In this way, we obtain a contradiction just assuming that the strong Goldbach's conjecture is false and $L_G \in REG$. In contraposition, we have the strong Goldbach's conjecture is true or this has an infinite number of counterexamples.

References

1. Agrawal, M., Kayal, N., Saxena, N.: PRIMES is in P. Annals of Mathematics **160**(2), 781–793 (2004). https://doi.org/10.4007/annals.2004.160.781
2. Aho, A.V., Hopcroft, J.E.: The Design and Analysis of Computer Algorithms. Pearson Education India (1974)
3. Chen, J.: 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. Cormen, T.H., Leiserson, C.E., Rivest, R.L., Stein, C.: Introduction to Algorithms. The MIT Press, 3 edn. (2009)
5. Van der Corput, J.G.: Sur l'hypothèse de Goldbach pour presque tous les nombres pairs. Acta Arithmetica **2**(2), 266–290 (1936)
6. Dickson, L.E.: History of the Theory of Numbers: Divisibility and Primality, vol. 1. New York, Dover (2005)

7. Estermann, T.: 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)
8. Geffert, V., Pardubská, D.: Unary Coded NP-Complete Languages in ASPACE (log log n). International Journal of Foundations of Computer Science **24**(07), 1167–1182 (2013). https://doi.org/10.1007/978-3-642-31653-1_16
9. Hardy, G.H., Wright, E.M.: An Introduction to the Theory of Numbers. Oxford University Press (1979)
10. Helfgott, H.A.: Minor arcs for Goldbach's problem. arXiv preprint arXiv:1205.5252 (2012)
11. Helfgott, H.A.: Major arcs for Goldbach's theorem. arXiv preprint arXiv:1305.2897 (2013)
12. Lagarias, J.C.: An elementary problem equivalent to the riemann hypothesis. The American Mathematical Monthly **109**(6), 534–543 (2002)
13. Matuszek, D.: Pumping Lemma Example 3 (February 1996), in The Pumping Lemma Lecture at https://www.seas.upenn.edu/~cit596/notes/dave/pumping6.html. Retrieved 26 April 2020
14. Michel, P.: A survey of space complexity. Theoretical computer science **101**(1), 99–132 (1992). https://doi.org/10.1016/0304-3975(92)90151-5
15. Papadimitriou, C.H.: Computational complexity. Addison-Wesley (1994)
16. Sarnak, P.: 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 26 April 2020
17. Sipser, M.: Introduction to the Theory of Computation, vol. 2. Thomson Course Technology Boston (2006)
18. Wells, D.G.: Prime Numbers, The Most Mysterious Figures in Math. John Wiley & Sons, Inc. (2005)