The Complexity of Mathematics

Frank Vega

March 29, 2020

The Complexity of Mathematics

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

Abstract

The strong Goldbach's conjecture states that every even integer greater than 2 can be written as the sum of two primes. The conjecture that all odd numbers greater than 7 are the sum of three odd primes is known today as the weak Goldbach conjecture. A principal complexity class is NSPACE(S(n)) for some S(n). We show if the weak Goldbach's conjecture is true, then the problem PRIMES is not in NSPACE(S(n)) for all S(n) = o(log n). However, if this happens, then the strong Goldbach's conjecture is true or this has an infinite number of counterexamples. In addition, if this happens, then the Twin prime conjecture is true. Moreover, if this happens, then the Beal's conjecture is true. Furthermore, if this happens, then the Riemann hypothesis is true. Since the weak Goldbach's conjecture was proven, then this will certainly happen.

2012 ACM Subject Classification Theory of computation → Complexity classes; Theory of computation → Regular languages; Theory of computation → Problems, reductions and completeness; Mathematics of computing → Number-theoretic computations

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

1 Introduction

1.1 Goldbach's conjecture

Number theory is a branch of pure mathematics devoted primarily to the study of the integers and integer-valued functions [30]. Goldbach's conjecture is one of the most important and unsolved problems in number theory [14]. Nowadays, it is one of the open problems of Hilbert and Landau [14]. 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" [10]. 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 [33]. 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" [10]. This is known as the strong Goldbach conjecture.

Using Vinogradov's method [32], it has been showed that almost all even numbers can be written as the sum of two primes. In 1973, Chen showed that every sufficiently large even number can be written as the sum of some prime number and a semi-prime [6]. 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 [10]. 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 [16], [17]. In this work, we prove the strong Goldbach's conjecture is true or this has an infinite number of counterexamples.

1.2 Twin prime conjecture

On the other hand, the question of whether there exist infinitely many twin primes has been one of the great open questions in number theory for many years. This is the content of the

Twin prime conjecture, which states that there are infinitely many primes p such that $p+2$ is also prime [15]. In addition, the Dubner's conjecture is an as yet unsolved conjecture by American mathematician Harvey Dubner [11]. It states that every even number greater than 4208 is the sum of two t-primes, where a t-prime is a prime which has a twin [11]. We prove there are infinite even numbers that comply the Dubner's conjecture, where this also implies that the Twin prime conjecture is true [11].

1.3 Beal's conjecture

Fermat's Last Theorem was first conjectured by Pierre de Fermat in 1637, famously in the margin of a copy of Arithmetica where he claimed he had a proof that was too large to fit in the margin [33]. This theorem states that no three positive integers a, b, and c can satisfy the equation $a^n + b^n = c^n$ for any integer value of n greater than two [33]. It is not known whether Fermat found a valid proof or not [33]. His proof of one case ($n = 4$) by infinite descent has survived [33]. After many intents, the proof of Fermat's Last Theorem for every integer $n > 2$ was finally accomplished, after 358 years, by Andrew Wiles in 1995 [34]. However, the Andrew's proof seems to be quite different to the simple and unknown proof that Fermat claimed.

On the other hand, there is a similar and unsolved conjecture called the Beal's conjecture [20]. This conjecture states if $A^x + B^y = C^z$, where A, B, C, x, y and z are positive integers and x, y and z are all greater than 2, then A, B and C must have a common prime factor [33]. Fermat's Last Theorem can be seen as a special case of the Beal's conjecture restricted to $x = y = z$. Billionaire banker Andrew Beal claims to have discovered this conjecture in 1993 while investigating generalizations of Fermat's Last Theorem [20]. This conjecture has occasionally been referred to as a generalized Fermat equation [4] and the Mauldin or Tijdeman-Zagier conjecture [12].

Beal offered a prize of US $1,000,000 to the first person who tries to resolve it [33]. For example, the solution $3^3 + 6^3 = 3^5$ has bases with a common factor of 3, and the solution $7^6 + 7^7 = 98^3$ has bases with a common factor of 7. There are some particular cases which have been proved for this conjecture [8], [25], [29], [5]. There are considerable advances on this topic [22], [9]. We contribute on this subject showing the Beal's conjecture is true.

1.4 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 [27]. It is of great interest in number theory because it implies results about the distribution of prime numbers [27]. It was proposed by Bernhard Riemann (1859), after whom it is named [27]. 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 [19]. 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 [19]. Using this inequality, we prove that the Riemann hypothesis is true.

2 Background Theory

In 1936, Turing developed his theoretical computational model [31]. The deterministic and nondeterministic Turing machines have become in two of the most important definitions related to this theoretical model for computation [31]. A deterministic Turing machine has only one next action for each step defined in its program or transition function [31]. A nondeterministic Turing machine could contain more than one action defined for each step of its program, where this one is no longer a function, but a relation [31].

Let Σ be a finite alphabet with at least two elements, and let Σ^* be the set of finite strings over Σ [3]. A Turing machine M has an associated input alphabet Σ [3]. For each string w in Σ^* there is a computation associated with M on input w [3]. We say that M accepts w if this computation terminates in the accepting state, that is $M(w) = $ "*yes*" [3]. Note that M fails to accept w either if this computation ends in the rejecting state, that is $M(w) = $ "*no*", or if the computation fails to terminate, or the computation ends in the halting state with some output, that is $M(w) = y$ (when M outputs the string y on the input w) [3].

Another relevant advance in the last century has been the definition of a complexity class. A language over an alphabet is any set of strings made up of symbols from that alphabet [7]. A complexity class is a set of problems, which are represented as a language, grouped by measures such as the running time, memory, etc [7]. The language accepted by a Turing machine M, denoted $L(M)$, has an associated alphabet Σ and is defined by:

$$L(M) = \{w \in \Sigma^* : M(w) = \text{“}yes\text{”}\}.$$

Moreover, $L(M)$ is decided by M, when $w \notin L(M)$ if and only if $M(w) = $ "*no*" [7]. 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 $2 \times n^2 \neq o(n^2)$ [7].

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 complexity class *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 [21]. 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 [18]. The complexity class *1-NSPACE*$(f(n))$ 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 [21].

3 Results

3.1 Goldbach's conjecture

▶ **Definition 1.** *We define the weak Goldbach's language L_{WG} as follows:*

$$L_{WG} = \{1^{2\times n+1}0^p0^q0^r : n \in \mathbb{N} \wedge n \geq 4 \wedge p, q \textit{ and } r \textit{ are odd primes } \wedge 2\times n+1 = p+q+r\}.$$

We define the strong Goldbach's language L_G as follows:

$$L_G = \{1^{2\times n}0^p0^q : n \in \mathbb{N} \wedge n \geq 3 \wedge p \text{ and } q \text{ are odd primes } \wedge 2 \times n = p + q\}.$$

▶ **Theorem 2.** *If the weak Goldbach's conjecture is true, then the weak Goldbach's language L_{WG} is non-regular. Moreover, if the strong Goldbach's conjecture is true, then the strong Goldbach's language L_G is non-regular.*

Proof. If the weak Goldbach's conjecture is true, then the weak Goldbach's language L_{WG} is equal to the another language L' defined as follows:

$$L' = \{1^{2\times n+1}0^{2\times n+1} : n \in \mathbb{N} \wedge n \geq 4\}.$$

We can easily prove that L' is non-regular using the Pumping lemma for regular languages [26]. Moreover, if the strong Goldbach's conjecture is true, then the strong Goldbach's language L_G is equal to the another language L'' defined as follows:

$$L'' = \{1^{2\times n}0^{2\times n} : n \in \mathbb{N} \wedge n \geq 3\}.$$

We can easily prove that L'' is non-regular using the Pumping lemma for regular languages as well [26]. ◀

▶ **Definition 3.** *We define the weak verification Goldbach's language L_{WVG} as follows:*

$$L_{WVG} = \{(2 \times n + 1, p, q, r) : \text{ such that } 1^{2\times n+1}0^p0^q0^r \in L_{WG}\}.$$

We define the strong verification Goldbach's language L_{VG} as follows:

$$L_{VG} = \{(2 \times n, p, q) : \text{ such that } 1^{2\times n}0^p0^q \in L_G\}.$$

▶ **Definition 4.** *We define the weak Goldbach's language with separator L_{WSG} as follows:*

$$L_{WSG} = \{0^{2\times n+1}\#0^p\#0^q\#0^r : \text{ such that } 1^{2\times n+1}0^p0^q0^r \in L_{WG}\}$$

and we define the strong Goldbach's language with separator L_{SG} as follows:

$$L_{SG} = \{0^{2\times n}\#0^p\#0^q : \text{ such that } 1^{2\times n}0^p0^q \in L_G\}$$

where # is the blank symbol.

▶ **Lemma 5.** *The weak Goldbach's language with separator L_{WSG} is the unary representation of the weak verification Goldbach's language L_{WVG}. The strong Goldbach's language with separator L_{SG} is the unary representation of the strong verification Goldbach's language L_{VG}.*

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

▶ **Theorem 6.** *If $L_{WVG} \in NSPACE(S(n))$ for some $S(n) = o(\log n)$, then $L_{WG} \in REG$.*

Proof. In case of $L_{WVG} \in NSPACE(S(n))$ for some $S(n) = o(\log n)$, then there is a nondeterministic Turing machine which decides L_{WSG} that uses space that is smaller than $c \times \log \log n$ for all $c > 0$, because of L_{WSG} is the unary version of L_{WVG} due to Lemma 5 [13]. Certainly, the standard space translation between the unary and binary languages actually works for nondeterministic machines with small space [13]. This means that if some language belongs to $NSPACE(S(n))$, then the unary version of that language belongs to $\mathit{NSPACE}(S(\log n))$ [13]. In this way, we obtain that $L_{WSG} \in \mathit{REG}$ because of $\mathit{REG} = \mathit{NSPACE}(o(\log\log n))$ [21]. In addition, we can reduce in a nondeterministic constant space the language L_{WG} to L_{WSG} just nondeterministically inserting the blank symbol # within two arbitrary positions between the 0's on the input. Moreover, this nondeterminism reduction inserts the blank symbol # between the 1's and 0's and converts the 1's to 0's from the original input of L_{WG} just generating the final output to L_{WSG}. Consequently, we prove $L_{WG} \in \mathit{REG}$ under the assumption that $L_{WVG} \in \mathit{NSPACE}(S(n))$ for some $S(n) = o(\log n)$, since REG is also the complexity class of languages decided by nondeterministic Turing machines in constant space [28]. ◀

▶ **Theorem 7.** *$L_{WVG} \notin \mathit{NSPACE}(S(n))$ for all $S(n) = o(\log n)$.*

Proof. If the weak Goldbach's conjecture is true, then $L_{WG} \notin \mathit{REG}$ as a consequence of Theorem 2. However, if $L_{WVG} \in \mathit{NSPACE}(S(n))$ for some $S(n) = o(\log n)$, then $L_{WG} \in \mathit{REG}$ due to Theorem 6. In this way, the weak Goldbach's conjecture cannot be true under the assumption that $L_{WVG} \in \mathit{NSPACE}(S(n))$ for some $S(n) = o(\log n)$. Since the weak Goldbach's conjecture is true, then we obtain that $L_{WVG} \notin \mathit{NSPACE}(S(n))$ for all $S(n) = o(\log n)$ [16], [17]. ◀

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

Proof. From the Theorem 7, we obtain that $L_{WVG} \notin \mathit{NSPACE}(S(n))$ for all $S(n) = o(\log n)$. However, the checking of whether the four numbers on the input are odds and proving the equality of the sum's equation can be done in $\mathit{NSPACE}(o(\log n))$. Certainly, the verification of the odd property could be done in constant space. In addition, the verification of the equality of the sum's equation $2 \times n + 1 = p + q + r$ can be done in $\mathit{NSPACE}(o(\log n))$.

Indeed, given four natural numbers p, q, r and t in binary encoding, it is obviously possible to check in $\mathit{NSPACE}(\log n)$ whether $p + q + r = t$. We need to go through corresponding bits from p, q, r and t starting from least significant bits to most significant bits. So for each i from 1 to n, we check if p, q, r and t have compatible/matching bits at position i (i.e. p_i, q_i, r_i, and t_i are compatible). Then, we keep track of any carry bit in constant space and move to index $i + 1$. We just need to keep track of i written in binary. If n is the greatest bit length between p, q, r and t, then we need $\log n$ bits to keep track of i. However, we can keep track of i using $o(\log n)$ space.

The position i is stored using a triple (a, b, c) of binary strings that represent positive integers. In the least significant bit position we use $(1, 0, 0)$. For a current bit position i in a triple (a, b, c), we move for the new bit position $i + 1$ using the rules of the following steps:

1. If $0 < a < \lfloor \frac{n}{\log n} \rfloor$, then the next step $i + 1$ into the new bit position is $(a + 1, b, c)$,
2. else if $a = \lfloor \frac{n}{\log n} \rfloor$, then the next step $i + 1$ into the new bit position is $(0, 0, 1)$,
3. else if $a = 0$ then:
   a. if $c = \lfloor \log n \rfloor$, then the next step $i+1$ into the new bit position is $(a, b+1, 1)$ otherwise if $c \neq \lfloor \log n \rfloor$, then the next step $i + 1$ into the new bit position is $(a, b, c + 1)$.

Every triple (a, b, c) represents the bit position $a \leq \lfloor \frac{n}{\log n} \rfloor$ when $a > 0$ or $\lfloor \frac{n}{\log n} \rfloor + (\lfloor \log n \rfloor \times b) + c$ when $a = 0$. In this way, b and c always comply with $c \leq \lfloor \log n \rfloor$ and $b \leq \frac{n - \lfloor \frac{n}{\log n} \rfloor}{\lfloor \log n \rfloor}$. Certainly, this is based on the following equation

$$\lfloor \frac{n}{\log n} \rfloor + \lfloor \log n \rfloor \times \frac{n - \lfloor \frac{n}{\log n} \rfloor}{\lfloor \log n \rfloor} = n$$

However, the bit length of $\lfloor \log n \rfloor$ is bounded by $\log\lfloor \log n \rfloor$. In addition, the bit length of $\lfloor \frac{n}{\log n} \rfloor$ is bounded by $\log n - \log\log n$. Moreover, the bit length of the integer part of $\frac{n - \lfloor \frac{n}{\log n} \rfloor}{\lfloor \log n \rfloor}$ is bounded by $\log(n - \lfloor \frac{n}{\log n} \rfloor) - \log\lfloor \log n \rfloor$. Since we add the bit length of c in case of $a = 0$, then this will be $\log(n - \lfloor \frac{n}{\log n} \rfloor)$. In this way, the whole computation is bounded by $\log(n - \lfloor \frac{n}{\log n} \rfloor)$ or $\log n - \log\log n$ space. Furthermore, we use a single triple (a', b', c') to put the head into the bit positions of the binary numbers:

1. if we want to put the head of the tape into the bit position (a', b', c') inside of a binary string, then we just set the head in the least significant bit position and move to the left while we decrement in 1 the bit position using the same rules that we used for incrementing until we reach the value $(1, 0, 0)$
2. and after that, if we want to put the head of the tape into the bit position (a', b', c') inside of another binary string, then from the current position in the head tape, we move to the right while we just increment in 1 the bit position from the value $(1, 0, 0)$ using the same rules above until the head will stay in the least significant bit position of the current binary string reaching the previous value (a', b', c')
3. and while we doing that, we copy the bits p_i, q_i, r_i, and t_i to the work tapes from the bit position i that represents (a', b', c') and do the necessary verification
4. and finally, when we finish all that, then we erase the bits p_i, q_i, r_i, and t_i and create the next step $i + 1$ from the value (a', b', c') into the new bit position using the same rules above.

However, we know that $\log n - \log\log n = o(\log n)$ and $\log(n - \lfloor \frac{n}{\log n} \rfloor) = o(\log n)$ for $n \geq 3$ where the whole computation can be done in a nondeterministic way because of it is indeed deterministic [24]. In addition, the ultimate remaining verification that we need to analyze in L_{WVG} is whether p, q and r are primes. Since the other properties can be done in $\mathit{NSPACE}(o(\log n))$ excluding the primality test and $L_{WVG} \notin \mathit{NSPACE}(S(n))$ for all $S(n) = o(\log n)$, then we have as unique remaining possibility that $PRIMES \notin \mathit{NSPACE}(S(n))$ for all $S(n) = o(\log n)$. ◀

▶ **Theorem 9.** *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 $L_G \in \mathit{REG}$ or L_G is non-regular and its complement is infinite, since every finite set is regular and REG is also closed under complement [24]. Let's assume the possibility of $L_G \in \mathit{REG}$. However, this implies that the exponentially more succinct version of L_G, that is L_{VG}, 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 L_G within $\mathit{NSPACE}(o(\log\log n))$ could be easily transformed into a slightly modified algorithm that decides L_{VG} within $\mathit{NSPACE}(S(n))$ for some $S(n) = o(\log n)$ [21], [13]. Actually, L_G could be reduced to L_{SG} in a nondeterministic constant space following the idea of steps in Theorem 6 and L_{SG} is the unary version of L_{VG} due to Lemma 5. As we mentioned before, the standard space translation between the unary and binary languages actually works for nondeterministic machines with small space [13]. This means that if some unary language belongs to $\mathit{NSPACE}(S(\log n))$, then the binary version of that language belongs to $\mathit{NSPACE}(S(n))$ [13]. It is not possible that $L_{VG} \in \mathit{NSPACE}(S(n))$ for some $S(n) = o(\log n)$, because of $PRIMES \notin \mathit{NSPACE}(S(n))$ for all $S(n) = o(\log n)$. Certainly, the verification of whether p and q are primes need to be done in order to accept the elements of this language. Consequently, we obtain that $L_G \notin \mathit{REG}$, since it is not possible that $L_G \in \mathit{NSPACE}(o(\log\log n))$ under the result of $L_{VG} \notin \mathit{NSPACE}(S(n))$ for all $S(n) = o(\log n)$. In this way, we obtain a contradiction just assuming that the strong Goldbach's conjecture is false and $L_G \in \mathit{REG}$. In contraposition, we have the strong Goldbach's conjecture is true or this has an infinite number of counterexamples. ◀

3.2 Twin prime conjecture

▶ **Definition 10.** *We define the Dubner's language L_D as follows:*

$$L_D = \{1^{2\times n}0^p0^q : n \in \mathbb{N} \wedge n > 2104 \wedge p \textit{ and } q \textit{ are t-primes } \wedge 2 \times n = p + q\}.$$

▶ **Theorem 11.** *If the Dubner's conjecture is true, then the Dubner's language L_D is non-regular.*

Proof. If the Dubner's conjecture is true, then the Dubner's language L_D is equal to the another language L' defined as follows:

$$L' = \{1^{2\times n}0^{2\times n} : n \in \mathbb{N} \wedge n > 2104\}.$$

We can easily prove that L' is non-regular using the Pumping lemma for regular languages as well [26]. ◀

▶ **Definition 12.** *We define the verification Dubner's language L_{VD} as follows:*

$$L_{VD} = \{(2 \times n, p, q) : \textit{ such that } 1^{2\times n}0^p0^q \in L_D\}.$$

▶ **Definition 13.** *We define the Dubner's language with separator L_{SD} as follows:*

$$L_{SD} = \{0^{2\times n}\#0^p\#0^q : \textit{ such that } 1^{2\times n}0^p0^q \in L_D\}$$

where # is the blank symbol.

▶ **Lemma 14.** *The Dubner's language with separator L_{SD} is the unary representation of the verification Dubner's language L_{VD}.*

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

▶ **Theorem 15.** *There are infinite even numbers that comply the Dubner's conjecture.*

Proof. If the Dubner's conjecture is false, then $L_D \in \mathit{REG}$ or L_D is non-regular and its complement is infinite, since every finite set is regular and REG is also closed under complement [24]. Let's assume the possibility of $L_D \in \mathit{REG}$. However, this implies that the exponentially more succinct version of L_D, that is L_{VD}, 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 L_D within $\mathit{NSPACE}(o(\log\log n))$ could be easily transformed into a slightly modified algorithm that decides L_{VD} within $\mathit{NSPACE}(S(n))$ for some $S(n) = o(\log n)$ [21], [13]. Actually, L_D could be reduced to L_{SD} in a nondeterministic constant space following the idea of steps in Theorem 6 and L_{SD} is the unary version of L_{VD} due to Lemma 14. As we mentioned before, the standard space translation between the unary and binary languages actually works for nondeterministic machines with small space [13]. This means that if some unary language belongs to $\mathit{NSPACE}(S(\log n))$, then the binary version of that language belongs to $\mathit{NSPACE}(S(n))$ [13]. It is not possible that $L_{VD} \in \mathit{NSPACE}(S(n))$ for some $S(n) = o(\log n)$, because of $PRIMES \notin \mathit{NSPACE}(S(n))$ for all $S(n) = o(\log n)$. Certainly, the verification of whether p and q are t-primes need to be done in order to accept the elements of this language. Consequently, we obtain that $L_D \notin \mathit{REG}$, since it is not possible that $L_D \in NSPACE(o(\log\log n))$ under the result of $L_{VD} \notin NSPACE(S(n))$ for all $S(n) = o(\log n)$. In this way, we obtain a contradiction just assuming that the Dubner's conjecture is false and $L_D \in REG$. In contraposition, we have there are infinite even numbers that comply with the Dubner's conjecture, since in case of L_D would be finite, then we obtain that the Dubner's conjecture is false and $L_D \in REG$ and we prove that is not possible. ◀

▶ **Lemma 16.** *The Twin prime conjecture is true.*

Proof. The Theorem 15 implies that there exists an infinite number of t-primes, and thus there will be an infinite number of twin prime pairs as well [11]. ◀

3.3 Beal's conjecture

▶ **Definition 17.** *For a specific choice of exponents (x, y, z) where $x, y, z \in \mathbb{N}$ and $x, y, z \geq 3$, we define the Beal's language L_B as follows:*

$$L_B = \{1^r 0^p 0^q : p, q, r \in \mathbb{N} \wedge p \leq q \wedge r = p + q\}$$

where when $p = 1$ then r has not a perfect z-root or r has a perfect z-root and there are no positive integers p and q such that $r = p + q$, p has a perfect x-root and q has a perfect y-root otherwise when $p > 1$ then $r = p + q$, r has a perfect z-root, p has a perfect x-root and q has a perfect y-root. Moreover, if $p > 1$ then for a fixed value of r, which is a perfect z-root, the greatest common divisor of p, q and r has the smallest possible value between all the possible numbers p and q with the following properties: $r = p + q$, p has a perfect x-root and q has a perfect y-root. In addition, if $p > 1$ then p, q and r are not co-primes.

▶ **Theorem 18.** *If the Beal's conjecture is true, then the Beal's language L_B is non-regular.*

Proof. If the Beal's conjecture is true, then the Beal's language L_B is equal to the another language L' defined as follows:

$$L' = \{1^n 0^n : n \in \mathbb{N} \wedge n \geq 2\}.$$

L' is a well-known non-regular language as a consequence of Pumping lemma [26]. ◀

▶ **Definition 19.** *We define the verification Beal's language L_{VB} as follows:*

$$L_{VB} = \{(r, p, q) : \text{ such that } 1^r 0^p 0^q \in L_B\}.$$

▶ **Definition 20.** *We define the Beal's language with separator L_{SB} as follows:*

$$L_{SB} = \{0^r \# 0^p \# 0^q : \text{ such that } 1^r 0^p 0^q \in L_B\}$$

where # is the blank symbol.

▶ **Lemma 21.** *The Beal's language with separator L_{SB} is the unary representation of the verification Beal's language L_{VB}.*

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

▶ **Theorem 22.** *$coL_{VB} \notin$ 1-NSPACE$(S(n))$ for all $S(n) = o(\log n)$.*

Proof. The complement coL_{VB} must check whether there is no a common prime factor between the three numbers in order to prove that these numbers are co-primes [15]. Certainly, coL_{VB} should contain the possible counterexamples of the Beal's conjecture for the chosen exponents (x, y, z) in coL_{VB}. The $COMPOSITE$ problem is the complement of $PRIMES$ language. Indeed, the computation of finding a common prime factor cannot be computed in *1-NSPACE*$(S(n))$ for some $S(n) = o(\log n)$, because of this would imply that the $COMPOSITE$ problem is in *1-NSPACE*$(S(n))$ for some $S(n) = o(\log n)$ as well.

Certainly if this could be true, then we can go from the numbers 2 to $n - 1$ and check whether these have a common prime factor with n and thus, we could decide whether n is composite. This could be nondeterministically done on input n just choosing arbitrarily another number lesser than n and greater than 1, but instead of putting in the work tapes, then this will put with n in the output tape just using constant space in one-way. After that, we use the space composition reduction just using the previous output of n and some integer $2 \leq i \leq n - 1$ into a new nondeterministic Turing machine that would compute the finding of a common prime factor in *1-NSPACE*$(S(n))$ for some $S(n) = o(\log n)$ using (n, i) as input [24]. Since *1-NSPACE*$(S(n))$ for some $S(n) = o(\log n)$ is closed under *1-NSPACE*-reductions with constant space, then the whole computation could be done in *1-NSPACE*$(S(n))$ for some $S(n) = o(\log n)$.

Nevertheless, this would be a contradiction according to Theorem 8, since the language $PRIMES \notin$ *NSPACE*$(S(n))$ for all $S(n) = o(\log n)$. The reason is because of *NSPACE*$(S(n))$ is closed under complement for $S(n) \geq \log n$ [21]. Hence, if $PRIMES \notin$ *NSPACE*$(S(n))$ for all $S(n) = o(\log n)$, then $COMPOSITE \notin$ *NSPACE*$(S(n))$ for all $S(n) = o(\log n)$ [21]. Furthermore, if $COMPOSITE \notin$ *NSPACE*$(S(n))$ for all $S(n) = o(\log n)$, then $COMPOSITE \notin$ *1-NSPACE*$(S(n))$ for all $S(n) = o(\log n)$ [21]. Since coL_{VB} depends mostly on checking whether there is no a common prime factor between the three numbers in order to accept its elements, then $coL_{VB} \notin$ *1-NSPACE*$(S(n))$ for all $S(n) = o(\log n)$. ◀

▶ **Theorem 23.** *The Beal's conjecture is true.*

Proof. If the Beal's conjecture is false, then $coL_B \in REG$ and coL_B is not empty or coL_B is non-regular and is infinite, since every finite set is regular [24]. Let's assume that $coL_B \in REG$ and coL_B is not empty. Hence, this implies that the exponentially more succinct version of coL_B, that is coL_{VB}, should be in *1-NSPACE*$(S(n))$ for some $S(n) = o(\log n)$, because of $REG =$ *1-NSPACE*$(o(\log \log n))$ and the same algorithm that decides coL_B within *1-NSPACE*$(o(\log \log n))$ could be easily transformed into a slightly modified algorithm that decides coL_{VB} within *1-NSPACE*$(S(n))$ for some $S(n) = o(\log n)$ [21], [13]. Actually, coL_B could be reduced to coL_{SB} in a nondeterministic constant space following the idea of steps in Theorem 6 and coL_{SB} is the unary version of coL_{VB} due to Lemma 21. As we mentioned before, the standard space translation between the unary and binary languages actually works for nondeterministic machines with small space [13]. This means that if some unary language belongs to *1-NSPACE*$(S(\log n))$, then the binary version of that language belongs to *1-NSPACE*$(S(n))$ [13]. In this way, we obtain that $coL_B \notin REG$ when coL_B is not empty, since it is not possible that $coL_B \in$ *1-NSPACE*$(o(\log \log n))$ under the result of $coL_{VB} \notin$ *1-NSPACE*$(S(n))$ for all $S(n) = o(\log n)$ as a consequence of Theorem 22. Consequently, we obtain a contradiction just assuming that $coL_B \in REG$ and coL_B is not empty. In contraposition, for a specific choice of exponents (x, y, z), we obtain that the Beal's conjecture is true, that is when coL_B is empty (we know the empty language is regular), or this has an infinite number of counterexamples (co-prime solutions), that is when coL_B is non-regular and is infinite, since coL_B uses a specific choice of exponents

(x, y, z). The Darmon-Granville theorem uses Faltings's theorem to show that for every specific choice of exponents (x, y, z), there are at most finitely many co-prime solutions for (A, B, C) [9]. In conclusion, we obtain that necessarily the Beal's conjecture is true for this specific choice of exponents (x, y, z) as the remaining only option. Since we took arbitrarily the exponents (x, y, z), then the Beal's conjecture will be true for every specific choice of exponents (x, y, z). ◀

3.4 Riemann hypothesis

▶ **Definition 24.** *We define the Robin's language L_R as follows:*

$$L_R = \{a^n b^{m_1} c^{m_2} : n \in \mathbb{N} \wedge n > 5040 \wedge m_1 = (\sigma(n) - n) \wedge m_2 = \lceil e^{\gamma} \times n \times \log\log n \rceil\}$$

where $\sigma(n) = \sum_{d|n} d$ [19].

▶ **Theorem 25.** *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 [26]. ◀

▶ **Definition 26.** *We define the verification Robin's language L_{VR} as follows:*

$$L_{VR} = \{(n, m_1, m_2) : \textit{ such that } a^n b^{m_1} c^{m_2} \in L_R\}.$$

▶ **Definition 27.** *We define the Robin's language with separator L_{SR} as follows:*

$$L_{SR} = \{0^n \# 0^{m_1} \# 0^{m_2} : \textit{ such that } a^n b^{m_1} c^{m_2} \in L_R\}$$

where $\#$ is the blank symbol.

▶ **Lemma 28.** *The Robin's language with separator L_{SR} is the unary representation of the verification Robin's language L_{VR}.*

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

▶ **Theorem 29.** *$L_{VR} \notin$ 1-NSPACE$(S(n))$ for all $S(n) = o(\log n)$.*

Proof. The language L_{VR} cannot be computed in *1-NSPACE*$(S(n))$ for some $S(n) = o(\log n)$, because of this would imply that the $PRIMES$ problem belongs to *1-NSPACE*$(S(n))$ for some $S(n) = o(\log n)$ as well. Certainly if this could be true, then we can find $m_2 = \lceil e^{\gamma} \times n \times \log\log n \rceil$ and check whether the triple $(n, 1, m_2)$ is an element of L_{VR} and thus, we could decide whether n is prime. Indeed, a number n is prime if and only if the sum of its divisors is $n + 1$ [15]. This could be nondeterministically done on input n just choosing arbitrarily another number m_2, but instead of putting in the work tapes, then this will put with n 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 n. After that, we use the space composition reduction just using the previous output of n, 1 and some integer m_2 into a new nondeterministic Turing machine that would decide whether the instance belongs to L_{VR} in *1-NSPACE*$(S(n))$ for some $S(n) = o(\log n)$ using $(n, 1, m_2)$ as input [24]. Since *1-NSPACE*$(S(n))$ for some $S(n) = o(\log n)$ is closed under *1-NSPACE*-reductions with constant space, then the whole computation could be done in *1-NSPACE*$(S(n))$ for some $S(n) = o(\log n)$. However, this would be a contradiction according to Theorem 8, since the language $PRIMES \notin$ *NSPACE*$(S(n))$ for all $S(n) = o(\log n)$. Certainly, if $PRIMES \notin$ *NSPACE*$(S(n))$ for all $S(n) = o(\log n)$, then $PRIMES \notin$ *1-NSPACE*$(S(n))$ for all $S(n) = o(\log n)$ [21]. Consequently, we obtain that $L_{VR} \notin$ *1-NSPACE*$(S(n))$ for all $S(n) = o(\log n)$. ◀

▶ **Theorem 30.** *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 is infinite, since every finite set is regular and REG is also closed under complement [24]. Let's assume the possibility of $L_R \in REG$. Hence, this implies that the exponentially more succinct version of L_R, that is L_{VR}, should be in *1-NSPACE*$(S(n))$ for some $S(n) = o(\log n)$, because of $REG =$ *1-NSPACE*$(o(\log \log n))$ and the same algorithm that decides L_R within *1-NSPACE*$(o(\log \log n))$ could be easily transformed into a slightly modified algorithm that decides L_{VR} within *1-NSPACE*$(S(n))$ for some $S(n) = o(\log n)$ [21], [13]. Actually, L_R could be reduced to L_{SR} in a nondeterministic constant space following the idea of steps in Theorem 6 and L_{SR} is the unary version of L_{VR} due to Lemma 28. As we mentioned before, the standard space translation between the unary and binary languages actually works for nondeterministic machines with small space [13]. This means that if some unary language belongs to *1-NSPACE*$(S(\log n))$, then the binary version of that language belongs to *1-NSPACE*$(S(n))$ [13]. In this way, we obtain that $L_R \notin REG$, since it is not possible that $L_R \in$ *1-NSPACE*$(o(\log \log n))$ under the result of $L_{VR} \notin$ *1-NSPACE*$(S(n))$ for all $S(n) = o(\log n)$ as a consequence of Theorem 29. 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 [19]:

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

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. ◀

4 Conclusions

4.1 Goldbach's conjecture

Statistical considerations that focus on the probabilistic distribution of prime numbers present informal evidence in pos of the strong conjecture for sufficiently large integers: The greater the integer, the more ways there are available for that number to be represented as the sum of two other numbers, and the more "likely" it becomes that at least one of these representations consists entirely of primes. In this way, the statement that the strong Goldbach's conjecture has an infinite number of counterexamples is certainly "unlikely". To sum up, this work represents a big step forward in showing the strong Goldbach's conjecture should be really true.

4.2 Beal's conjecture

Peter Norvig, Director of Research at Google, have conducted a series of numerical searches for counterexamples to Beal's conjecture. Among his results, he excluded all possible solutions having each of $x, y, z = 7$ and each of $A, B, C = 250,000$, as well as possible solutions having each of $x, y, z = 100$ and each of $A, B, C = 10,000$ [23]. We conclude announcing the failure in the prolonged search of counterexamples since the Beal's conjecture is true.

Fermat's Last Theorem established that $A^n + B^n = C^n$ has no solutions for $n > 2$ for positive integers A, B, and C. If any solutions had existed to Fermat's Last Theorem, then by dividing out every common factor, there would also exist solutions with A, B, and C co-prime which would mean they do not have a common prime factor [15]. Hence, Fermat's Last Theorem can be seen as a special case of the Beal's conjecture restricted to $x = y = z$ [4].

The Fermat-Catalan conjecture is that $A^x + B^y = C^z$ has only finitely many solutions with A, B, and C being positive integers with no common prime factor and x, y, and z being positive integers satisfying $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} < 1$ [33]. Beal's conjecture can be restated as "All Fermat-Catalan conjecture solutions will use 2 as an exponent".

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 Sanjeev Arora and Boaz Barak. *Computational complexity: a modern approach*. Cambridge University Press, 2009.

4 Michael A. Bennett, Imin Chen, Sander R. Dahmen, and Soroosh Yazdani. Generalized Fermat Equations: A Miscellany, June 2014. Available at `http://people.math.sfu.ca/~ichen/pub/BeChDaYa.pdf`. Retrieved 21 February 2020.

5 Frits Beukers. The generalized fermat equation, January 2006. Available at `http://www.staff.science.uu.nl/~beuke106/Fermatlectures.pdf`. Retrieved 21 February 2020.

6 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.

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

8 Richard Crandall and Carl Pomerance. *Prime Numbers: A Computational Perspective*. Springer, 2000.

9 Henri Darmon and Andrew Granville. On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$. *Bulletin of the London Mathematical Society*, 27:513–543, 1995.

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

11 Harvey Dubner. Twin prime conjectures. *JOURNAL OF RECREATIONAL MATHEMATICS*, 30(3):199–205, 2000.

12 Noam D. Elkies. The ABC's of Number Theory. *The Harvard College Mathematics Review*, 1(1), 2007.

13 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`.

14 Richard K. Guy. *Unsolved Problems in Number Theory*. New York, Springer-Verlag, 3 edition, 2004.

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

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

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

18 Martin Kutrib, Julien Provillard, György Vaszil, and Matthias Wendlandt. Deterministic One-Way Turing Machines with Sublinear Space. *Fundamenta Informaticae*, 136(1-2):139–155, 2015. `doi:10.3233/FI-2015-1147`.

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

20 R. Daniel Mauldin. A Generalization of Fermat's Last Theorem: The Beal Conjecture and Prize Problem. *Notices of the AMS*, 44(11):1436–1439, 1997.

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

22 Abderrahmane Nitaj. On A Conjecture of Erdos on 3-Powerful Numbers. *Bulletin of the London Mathematical Society*, 27(4):317–318, 1995.

23 Peter Norvig. Beal's Conjecture: A Search for Counterexamples, October 2015. Available at http://norvig.com/beal.html. Retrieved 21 February 2020.

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

25 Bjorn Poonen, Edward F. Schaefer, and Michael Stoll. Twists of $x(7)$ and primitive solutions to $x^2 + y^3 = z^7$. *Duke Mathematical Journal*, 137:103–158, 2005.

26 Michael O. Rabin and Dana Scott. Finite automata and their decision problems. *IBM journal of research and development*, 3(2):114–125, 1959. doi:10.1147/rd.32.0114.

27 Peter Sarnak. Problems of the millennium: The riemann hypothesis (2004), April 2005. Available at http://www.claymath.org/library/annual_report/ar2004/04report_prizeproblem.pdf. Retrieved 1 March 2020.

28 John C. Shepherdson. The Reduction of Two-Way Automata to One-Way Automata. *IBM Journal of Research and Development*, 3(2):198–200, 1959. doi:10.1147/rd.32.0198.

29 Samir Siksek and Michael Stoll. The generalised fermat equation $x^2 + y^3 = z^{15}$. *Archiv der Mathematik*, 102:411–421, 2013.

30 Joseph H. Silverman. *A Friendly Introduction to Number Theory.* Pearson Education, Inc., 4 edition, 2012.

31 Michael Sipser. *Introduction to the Theory of Computation*, volume 2. Thomson Course Technology Boston, 2006.

32 Ivan M. Vinogradov. Representation of an Odd Number as a Sum of Three Primes. *Comptes Rendus (Doklady) de l'Académie des Sciences de l'USSR*, 15:169–172, 1937.

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

34 Andrew Wiles. Modular elliptic curves and Fermat's Last Theorem. *Annals of Mathematics*, 141(3):443–551, 1995. doi:0.2307/2118559.