

# Chapter 8

---

---

## *Some of My Favorite Problems (I)*

**Ron Graham**

*University of California at San Diego*

### CONTENTS

8.1	Introduction .....	127
8.2	Prologue .....	127
8.3	Universal Cycles .....	128
8.4	Combs .....	130
8.5	The Middle Binomial Coefficient $\binom{2n}{n}$ .....	131
8.6	The Steiner Ratio Problem .....	134
8.7	A Curious ‘Inversion’ in Complexity Theory .....	136
8.8	A Final Problem .....	138
	References .....	138

---

---

## 8.1 Introduction

In this paper I describe several problems I have worked on over the years which are still mostly unresolved. This paper is based on a talk on this subject which I presented at the 50<sup>th</sup> Southeastern Conference on Combinatorics, Graph Theory and Computing held in Boca Raton on March 4 - 8, 2019.

---

---

## 8.2 Prologue

The lights are dimmed and the performer produces a deck of ordinary cards, He casually removes the cards from the pack and gives them a few (Charlier) shuffles \*. He then wraps a rubber band around the shuffled deck and replaces them in the pack

\*Charlier shuffles, in spite of their appearance, just cyclically permute the deck.

and throws the pack into one of the first few rows of the audience. The performer then instructs the person holding the pack to remove the cards and the rubber band, give the deck a cut and then pass the deck to his right. The person to the right is instructed to do the same, and this continues until the deck has been cut 5 times. Now the person holding the deck is instructed to remove the top card and pass the deck to the person to his left. This person should then remove the top card and pass the deck to the person to his left and so on, until five cards have been removed. The performer now asks each card holder to concentrate on their selected card and he will attempt to read their minds! After (apparently) struggling to receive clear mental impressions of the selected cards, the performer suggests the the red cards (diamonds and hearts) are harder for him to detect, and asks the people with red cards to stand. Now, after a brief pause, the performer correctly names all the selected cards.

How is this possible? We explain in the next section.

### 8.3 Universal Cycles

At the 20<sup>th</sup> Southeastern Conference on Combinatorics, Graph Theory and Computing held in Boca Raton in 1989, the author presented a paper [9] (with Fan Chung and Persi Diaconis) on what we called *universal cycles for combinatorial structures*. Roughly speaking, these are ways of efficiently representing classes of combinatorial objects in the form of a cycle, with the various combinatorial objects appearing uniquely as a “window” of fixed width moves around the cycle. A classic example is that of the so-called de Bruijn cycle [10]. Here, the combinatorial objects are the binary sequences of length  $n$  and of course, in this case the cycle must have length  $2^n$ . For example, the cycle 00010111 is a de Bruijn cycle for binary triples and the cycle 0000111100110101 is a de Bruijn cycle for binary 4-tuples (where it is understood that we ‘go around the corner’ with our moving window). It is well-known [16] that the number of distinct de Bruijn cycles for binary  $n$ -tuples is  $2^{2^{n-1}-n}$ .

For our card trick, we use the following de Bruijn cycle for 5-tuples

00001001011001111100011011101010

In particular, our deck only has the 32 cards consisting of Ace through 8 of each of the four suits. The deck is arranged in a very special order. First of all, the positions with 1’s will correspond to the 16 red cards so that if you know the red-black arrangement of 5 consecutive cards, you know exactly where you are in the cycle. More specifically, each 5-tuple  $a_1a_2a_3a_4a_5$  will correspond to a specific card according to the following code. The first two digits  $a_1a_2$  will encode the *suit* of the card

using the following rules:

$$00 \longleftrightarrow \clubsuit$$

$$01 \longleftrightarrow \spadesuit$$

$$10 \longleftrightarrow \diamond$$

$$11 \longleftrightarrow \heartsuit$$

Similarly, the last three digits  $a_3a_4a_5$  will encode the *rank* of the card using the following rules:

$$001 \longleftrightarrow A$$

$$010 \longleftrightarrow 2$$

$$011 \longleftrightarrow 3$$

$$100 \longleftrightarrow 4$$

$$101 \longleftrightarrow 5$$

$$110 \longleftrightarrow 6$$

$$111 \longleftrightarrow 7$$

$$000 \longleftrightarrow 8$$

where ‘A’ stands for Ace. For example the sequence 10100 denotes the 4 of diamonds ( $=4\diamond$ ). Thus, our 32-card deck arranged according the above de Bruijn cycle is

$$A\clubsuit 2\clubsuit 4\clubsuit A\spadesuit 2\diamond \dots \dots 8\diamond 8\clubsuit$$

(going around the corner).

However, given that we know the card corresponding to the 5-tuple  $x_kx_{k+1}x_{k+2}x_{k+3}x_{k+4}$ , how do we find the *next* card? Of course, this is the card corresponding to the sequence  $x_{k+1}x_{k+2}x_{k+3}x_{k+4}x_{k+5}$  (where indices are computed modulo 32). That is, how do we compute  $x_{k+5}$  from  $x_kx_{k+1}x_{k+2}x_{k+3}x_{k+4}$ ? Very simply! We just use the rule

$$x_{k+5} \equiv x_k + x_{k+2} \pmod{2}.$$

This generates a maximal length 31 shift-register sequence which will specify the exact arrangement of our deck. The missing 5-tuple 00000 is formed by just inserting a 0 next to the 0000.

Thus, if the red-card spectators form the 5-tuple 10100, then we know the first (left-most) card is  $4\diamond$ . Then the next digit must be  $1 + 0 \equiv 1 \pmod{2}$  so the next card is  $01001 = A\spadesuit$ , the card after that is  $10011 = 3\diamond$ , etc. With a little practice, this calculation can become routine.

Among the various universal cycles considered in [9] were those for the  $k$ -subsets of an  $n$ -set. Here, we are looking for a cycle  $(a_1a_2\dots a_N)$  of length  $N = \binom{n}{k}$  so that each of the  $k$ -element subsets of the set  $\{1, 2, \dots, n\}$  occurs exactly once (in some order) as  $\{a_{i+1}, a_{i+2}, \dots, a_{i+k}\}$  for some  $i$ .

For example, 1234513524 is a universal cycle for 2-sets of the 5-set  $\{12345\}$  and 82456145712361246783671345834681258135672568234723578147 is a universal cycle for the 3-sets of the 8-set  $\{1, 2, 3, 4, 5, 6, 7, 8\}$ .

We observe the following:

**Proposition 8.1** *A necessary condition for the existence of a universal cycle  $U$  for the  $k$ -subsets of an  $n$ -set is*

$$\binom{n-1}{k-1} \equiv 0 \pmod{k}. \quad (8.1)$$

**Proof** Consider the occurrence of some particular element  $x$  in the cycle  $U$ . It occurs in exactly  $k$  different  $k$ -sets as the window of width  $k$  moves by. On the other hand, there are just  $\binom{n-1}{k-1}$  different  $k$ -sets of the  $n$ -set which contain  $x$ . This proves (8.1).

In [9], the authors made the following conjecture:

**Conjecture 8.2** (\$100) *For each fixed  $k$ , (8.1) is also a sufficient condition for the existence for a universal cycle for  $k$ -sets of an  $n$ -set provided  $n > n_0(k)$  is sufficiently large.*

Partial progress has been made over the years by B. Jackson ( $n = 3$ ) [27], G. Hurlbert ( $n = 4, 5$ ) [23] and others. However, in a very recent brilliant stroke by Glock, Joos, Kühn and Osthus [17], Conjecture 8.2 has been fully proved. The proof, while short, uses sophisticated applications of the probabilistic method and quasirandom hypergraphs together with the recent breakthrough result of Keevash [28] (see also [18]) on the existence of  $t$ -designs. Their proof should in principle be able to produce universal cycles for  $k$ -sets of an  $n$ -set for any fixed value of  $k$ , e.g.,  $k = 10$ . However, I don't believe this has happened yet.

**Challenge 8.3** *Count (or obtain good estimates) for the number of universal cycles for  $k$ -sets of an  $n$ -set.*

Since it wasn't easy to show that there was at least *one*, this challenge will probably be rather difficult!

## 8.4 Combs

A variation on de Bruijn cycles considered in [1, 6] is to allow more general windows as we go around the cycle. For example, suppose for  $k = 3$ , instead of three consecutive positions we instead looked at positions 1, 2 and 5. We will call this the  $(1, 2, 5)$  comb with teeth at positions 1, 2 and 5. In this case, we can check that the cycle

11100100 is a universal cycle for this modified window or comb. In other words, as this window cycles around, we see all the binary triples 110, 111, 100, etc. In Table 8.1, we list the different combs with four teeth (up to rotational symmetry, reflections and 0/1 interchange) which have universal cycles. All other combs have no universal cycles.

Comb	# of universal cycles
(1,3,5,7)	16
(1,2,3,4)	8
(1,2,3,8)	5
(1,2,4,15)	4
(1,2,3,7)	3
(1,2,4,5)	2
(1,2,4,8)	1
(1,2,4,10)	1

**Table 8.1**

Binary combs with 4 teeth

What in the world is going on? (See [1] for more details.)

**Challenge 8.4** *Characterize those combs which have at least one universal cycle.*

**Challenge 8.5** *Count (or estimate) the number of universal cycles each comb has.*

Of course, the same questions can be asked for universal cycles for alphabets with more than two symbols.

In connection with our current topic, one can look for combs for  $k$ -subsets of an  $n$ -set. We still have the necessary condition (8.1). It turns out, for example that for the usual window for  $k = 3, n = 5$ , there are no universal cycles. However, with the comb (1, 2, 6), there is a universal cycle 1212343545 (courtesy of Steve Butler [4]). In fact, there are quite a few.

**Challenge 8.6** *Characterize those combs for  $k$ -subsets on an  $n$ -set which have universal cycles.*

**Challenge 8.7** *Count (or estimate) the number of universal cycles for  $k$ -subsets of an  $n$ -set each comb has.*

Given that it took 30 years to show that there was even *one* universal cycle for the (trivial) comb with  $k$  consecutive teeth, we suspect that these more general questions will be rather challenging!

## 8.5 The Middle Binomial Coefficient $\binom{2n}{n}$

Binomial coefficients have been the source of innumerable number-theoretic problems since they were first identified, which according to some accounts dates back to the second century B.C. The questions we address in this section arose from a paper by P. Erdős, I. Z. Ruzsa, E.G. Straus and myself [15] more than 40 years ago.

Let us begin by first looking at the first few middle binomial coefficients:

$n$	$\binom{2n}{n}$	factorization
1	2	2
2	6	$2 \cdot 3$
3	20	$2^2 \cdot 5$
4	70	$2 \cdot 5 \cdot 7$
5	252	$2^2 \cdot 3^2 \cdot 7$
6	924	$2^2 \cdot 3 \cdot 7 \cdot 11$
7	3432	$2^3 \cdot 3 \cdot 11 \cdot 13$
8	12870	$2 \cdot 3^2 \cdot 5 \cdot 11 \cdot 13$
9	48620	$2^2 \cdot 5 \cdot 11 \cdot 13 \cdot 17$
10	184756	$2^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19$

In general, the middle binomial coefficients tend to be highly composite. For example, it is not hard to show that these coefficients are all even, and though harder to show (but equally true!),  $\binom{8}{4} = 70$  is the last middle binomial coefficient which is squarefree [22]. However, it can be seen by observing the table that there are coefficients which are relatively prime to each of 3, 5 or 7. But how often can  $\binom{2n}{n}$  be relatively prime to *all three* of 3, 5 and 7, such as  $\binom{20}{10} = 2^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19$ , for example? Observing that  $3 \cdot 5 \cdot 7 = 105$ , we state:

**Conjecture 8.8** *There are infinitely many  $n$  such that  $\gcd\left(\binom{2n}{n}, 105\right) = 1$ .*

On the other hand, one could ask if the same behavior holds for the *four* primes 3, 5, 7 and 11? For example, it is not hard to see that the least odd prime factor of  $\binom{6320}{3160}$  is 13.

**Conjecture 8.9** *There are only finitely many  $n$  such that  $\gcd\left(\binom{2n}{n}, 3 \cdot 5 \cdot 7 \cdot 11\right) = 1$ . In particular, the largest such  $n$  is 3160.*

It is known [4] there are no such  $n$  with  $3161 \leq n < 10^{25000}$ .

What is the motivation for our belief in these conjectures? Much of this rests on the following well-known result:

**Theorem 8.10** (E. Kummer (1852), [30]) *The power of the prime  $p$  which divides  $\binom{2n}{n}$  is equal to the number of carries which occur when  $n$  is added to itself when  $n$  is expressed in base  $p$ .*

In particular,  $\binom{2n}{n}$  will be relatively prime to  $p$  if and only if all the base  $p$  ‘digits’ of  $n$  are less than  $\frac{p}{2}$ . We call these the *small* digits base  $p$ . So we can state an equivalent conjecture to Conjecture 8.8

**Conjecture 8.11** *There are infinitely many  $n$  such that:*

*$n$  base 3 uses only the digits 0 and 1,*

*$n$  base 5 uses only the digits 0, 1 and 2,*

*$n$  base 7 uses only the digits 0, 1, 2 and 3.*

**Example 8.12** Expanding  $n = 3160$  to different bases, we find that  $3160_{(3)} = 10000111$ ,  $3160_{(5)} = 21001$ ,  $3160_{(7)} = 33121$  and  $3160_{(11)} = 3142$ . Thus,  $\binom{6320}{3160}$  is relatively prime to  $3 \cdot 5 \cdot 7 \cdot 11 = 1155$ , as claimed in Conjecture 8.9.

Here comes the heuristic. A large  $n$  has asymptotically  $\log_p n$  base  $p$  digits. Hence, the probability that all these digits are small, i.e., less than  $\frac{p}{2}$ , is roughly

$$\left(\frac{p+1}{2p}\right)^{\log_p n} = n^{\frac{\log\left(\frac{p+1}{2p}\right)}{\log p}} := n^{f(p)},$$

where this is used for the definition of  $f(p)$ . Therefore, assuming the expansions to different prime bases are *independent*, the expected number of numbers less than  $x$  which use only small digits in all the prime bases  $p_1, p_2, \dots, p_r$  is given by the expression

$$x^{1+\sum_i f(p_i)} = x^{1+\sum_i \frac{\log\left(\frac{p_i+1}{2p_i}\right)}{\log p_i}}. \quad (8.2)$$

For the set of primes  $\{3, 5, 7\}$  we have  $x^{1+f(3)+f(5)+f(7)} = x^{0.02595\dots}$ . This tells me that we should expect infinitely many  $n$  to have  $\gcd\left(\binom{2n}{n}, 3 \cdot 5 \cdot 7\right) = 1$ . On the other hand, for the primes  $\{3, 5, 7, 11\}$ , we have the exponent  $1 + f(3) + f(5) + f(7) + f(11) = -0.22682\dots$  I interpret this as indicating that there should be only finitely many  $n$  for which  $\gcd\left(\binom{2n}{n}, 1155\right) = 1$ . Computation seems to bear this out (although  $10^{25000}$  is still only 0 percent of the way to  $\infty!$ ). We can summarize these beliefs in the following conjecture.

**Conjecture 8.13** (\$1000) *Let  $P = \{p_1, p_2, \dots, p_r\}$  be a set of distinct odd primes and let  $F(P) = 1 + \sum_i f(p_i)$ .*

(a) *If  $F(P) > 0$  then there are infinitely  $n$  such that  $\gcd\left(\binom{2n}{n}, \prod_i p_i\right) = 1$ .*

(b) *If  $F(P) < 0$  then there are only finitely many  $n$  such that*

$$\gcd\left(\binom{2n}{n}, \prod_i p_i\right) = 1.$$

Actually, this is two conjectures so in fairness I should offer \$500 for each of them. However, I believe they are sufficiently difficult that I would gladly part

with the full reward for a resolution of either (a) or (b)! What are some more stringent tests of this conjecture? Well, for the set  $P = \{7, 11, 13, 17\}$  we have  $F(P) = -0.006185\dots$ . The largest known  $n$  having  $\gcd\left(\binom{2n}{n}, \prod_i p_i\right) = 1$  is 987237571886409516564612292787298523778234008606963100480478235918624119.

There are no others after this below  $10^{3500}$ . Presumably this is the last such  $n$ .

Even more delicate is the set  $P = \{31, 37, 59, 79, 89, 97\}$ . For this set we have  $F(P) = -0.00001139\dots$ . According to Conjecture 8.13(b), there should be only finitely many  $n$  satisfying  $\gcd\left(\binom{2n}{n}, \prod_i p_i\right) = 1$ . However, computation has produced such  $n > 10^{1200}$ ! †

What is known for this problem? In [15] it was shown that for any two primes  $p$  and  $q$ , there are infinitely many  $n$  such that  $\gcd\left(\binom{2n}{n}, pq\right) = 1$ . In fact much more is true.

**Theorem 8.14** [15] *Suppose  $A$  and  $B$  are integers satisfying*

$$\frac{A}{p-1} + \frac{B}{q-1} \geq 1.$$

*Then there are infinitely many integers whose base  $p$  expansion has all digits less than or equal to  $A$  and whose base  $q$  expansion has all digits less than or equal to  $B$ .*

Choosing  $A = \frac{p-1}{2}, B = \frac{q-1}{2}$  gives the preceding result for two primes  $p$  and  $q$ .

Of course, there is a rich literature on arithmetic properties of binomial coefficients and in particular, the middle binomial coefficient. For example, see [14] for an older reference, [2] for a fairly recent one and [32, 34] for very recent ones.

We close this section by mentioning one more problem from [15].

**Challenge 8.15** *Show that there are infinitely many pairs of middle binomial coefficients  $\binom{2m}{m}, \binom{2n}{n}$  which have the same set of prime divisors.*

*Examples of such pairs are  $\binom{174}{87}, \binom{176}{88}$  and  $\binom{1214}{607}, \binom{1216}{608}$ .*

As Paul Erdős like to say, every right-thinking mathematician knows this must be true but we are not yet at a stage where we can prove it.

## 8.6 The Steiner Ratio Problem

The Minimum Spanning Tree problem is a classic topic in combinatorial optimization. Given a set of points in the Euclidean plane (or more generally, in some metric

†the ! symbol does not denote factorial here!



space), it asks for the network connecting all these points together which has the shortest total length. The names of J. Kruskal [29] and R. Prim [33] (both at Bell Laboratories) are usually associated with the originators of efficient algorithms for this problem. However, research indicates that O. Boruvka should be given credit for this. (for a history of this problem, see [20]). In particular, it is an example in which a simple *greedy* algorithm succeeds in constructing such a network. Namely, just start adding edges in increasing order of length, except when a cycle is formed. In that case, skip that edge and go on to the next shortest edge. Stop when a tree (= acyclic connected graph) is formed. Since the shortest network will not contain a cycle, the optimal network will always be a tree (for graph-theoretic terminology, see [38]). The reason that this problem was of interest to researchers at Bell Labs was because of the way that tariffs at that time were written for billing long-distance customers. In particular, if a large company wanted to have a private long-distance network connecting many locations, the company would be billed on the basis of the length of the minimum spanning tree connecting these locations, not on the way that the telephone company actually constructed the network. It was soon realized that a company could create some imaginary locations so that the minimum spanning tree for the augmented set of locations could be shorter than that of the original set! As a simple example, if the original set of locations consisted of the three vertices of a unit equilateral triangle, the minimum spanning tree would consist of two of the sides of the triangle, and has total length 2. However, if we add the centroid of the triangle as an additional point, then the length of the minimum spanning tree for the enlarged set (joining the added point to each of the three vertices of the triangle) now has length only  $\sqrt{3}$ .

These additional points are now called “Steiner” points, and the optimal network obtained by adding (any number of) Steiner points is called the *Minimum Steiner Tree* for the original set of points. (For a history of this problem, which dates back to 1810, see [3]). For obvious reasons, it was of great interest to understand just how much shorter the length of the minimum Steiner tree could be compared to the length of the minimum spanning tree for any particular set of points. That is, if  $L_{St}(X)$  and  $L_M(X)$  denote the lengths of the minimum Steiner tree and the minimum spanning tree for a set  $X$ , respectively, then what is a lower bound for  $\frac{L_{St}(X)}{L_M(X)}$ ? The best bounds for pointsets  $X$  in the Euclidean plane evolved as follows:

- $\frac{L_{St}(X)}{L_M(X)} \geq \frac{1}{2}$  for  $X$  in any metric space (from antiquity);
- $\frac{L_{St}(X)}{L_M(X)} \geq \frac{1}{\sqrt{3}} = .5771\dots$  for  $X$  in any Euclidean space  
(1975) RLG / F. Hwang [20];
- $\frac{L_{St}(X)}{L_M(X)} \geq \frac{1}{3} \left( 2 + 2\sqrt{3} - \sqrt{7 + 2\sqrt{3}} \right) = .7431\dots$   
(1976) F. Chung / F. Hwang [8];
- $\frac{L_{St}(X)}{L_M(X)} \geq \frac{4}{5} = .8$

(1983) D. Z. Du/F. Hwang [12]

- $\frac{L_{St}(X)}{L_M(X)} \geq \frac{4}{5} = \rho_0 = .8241\dots$   
 where  $\rho_0$  is a root of the irreducible polynomial  $x^{12} - 4x^{11} - 2x^{10} + 40x^9 - 31x^8 - 72x^7 + 116x^6 + 16x^5 - 151x^4 + 80x^3 + 56x^2 - 64x + 16$   
 (1985) F. Chung/RLG [7]

What is the best we could hope for here? A celebrated conjecture of E. N. Gilbert and H. O. Pollak (from Bell Labs, of course) from 1968 asserts:

$$\frac{L_{St}(X)}{L_M(X)} \geq \frac{\sqrt{3}}{2} = .8660\dots \tag{8.3}$$

This is what is achieved by the vertices of the equilateral mentioned earlier, so if true, this would be best possible. Finally, in (1992), a proof of (8.3) was announced by Du and Hwang [13]. However, several experts have now concluded [39, 25, 26] that the proof in [13] is incomplete so it seems that the Gilbert-Pollak conjecture (8.3) still stands, and that the best current bound is  $\rho_0 = .8241\dots$  mentioned above.

**Challenge 8.16** (\$1000) *Prove* (8.3).

One might wonder what the corresponding bound is for sets of points in Euclidean 3-space. This is given by the following conjecture of Warren Smith and J. MacGregor Smith [35]:

**Conjecture 8.17** (\$500) *For any finite pointset*  $X \in \mathbf{E}^3$  *we have:*

$$\frac{L_{St}(X)}{L_M(X)} > \sqrt{\frac{283 - 3\sqrt{21}}{700} + \frac{9\sqrt{11 - \sqrt{21}}\sqrt{2}}{140}} = .78419\dots$$

You must admit that isn't the first guess that comes to mind when thinking about the problem (at least, for me!). No finite set  $X$  is known which achieves this bound but there are sufficiently large sets which come arbitrarily close.

There is a substantial literature concerning the Steiner ratio for metric spaces with different norms, such as  $L_1$  [24], Minkowski normed planes [11], etc. The reader can consult [5] and the references therein for more sources.

## 8.7 A Curious ‘Inversion’ in Complexity Theory

It is known that the Euclidean minimum Steiner problem is **NP**-complete [19]. However, as we have seen, there are efficient (polynomial) algorithms for finding the minimum spanning tree for a set of points in the plane (and the same algorithm works in

any metric space). However, from the point of view of complexity theory, this should be phrased as a decision problem.

**Input:** A set  $X$  of points in the plane with integer coordinates, and a positive integer  $L$ .

**EMST:** Does  $X$  have a spanning tree with length  $\leq L$ ?

The purported algorithm should answer *YES* or *NO* in time polynomial in the size of the input. Amazingly, this problem is not even known to be in **NP**!

So how do you check if the sum of the lengths of the edges of a tree  $T$  is bounded by  $L$ ? The problem is that while the coordinates of  $T$  are integers, the lengths of the potential edges are *square roots* of integers. Thus, the problem comes down to deciding if a sum of  $n$  square roots of integers is bounded by some integer  $L$ . That is, we need to check in polynomial time if the following holds:

$$\sum_{k=1}^n \sqrt{m_k} \leq L$$

**Option 1.** By repeatedly ‘transposing terms and squaring’  $n$  times, we can get rid of all the square roots. The downside is that after  $n$  squarings, our integers can have exponential many digits!

**Option 2.** Approximate the square roots. The question then becomes one of knowing how closely to approximate them.

Consider the following related problem:

**Example 1.** Let

$$A = \{0, 11, 24, 65, 90, 129, 173, 212, 237, 278, 291, 302\},$$

$$B = \{3, 5, 30, 57, 104, 116, 186, 198, 245, 272, 297, 299\}.$$

Then

$$\sum_k \sqrt{1000000 + a_k} = 12000.9059482723022917534870728190449567268733681081168194090\dots,$$

$$\sum_k \sqrt{1000000 + b_k} = 12000.9059482723022917534870728190449567268733681081168194090\dots$$

Which sum is larger? (They are definitely not equal!) In principle, two sums of  $n$  square roots could agree for exponentially (in  $n$ ) many digits before diverging since they represent algebraic numbers of degree  $2^n$ . However, I don’t think this can actually happen.

**Challenge 8.18** (\$10) *Show that two sums of square roots of integers cannot agree for exponentially many digits (measured by the size of the input).*

**Option 3.** Something else. Consider the following example.

**Example 8.19** Let

$$P = \sqrt{5} + \sqrt{22 + 2\sqrt{5}} = 7.3811759408956797266875465\dots,$$

$$Q = \sqrt{11 + 2\sqrt{29}} + \sqrt{16 - 2\sqrt{29} + 2\sqrt{55 - 10\sqrt{29}}} = 7.3811759408956797266875465\dots$$

Computation shows that  $P$  and  $Q$  agree in more than 500 digits. In fact, they agree in more than 50000 digits! The reason: Because they are equal! This is not so obvious (to me) at first glance. In fact, there are serious logical difficulties in proving that a given mathematical expression is zero [36]. For example, is it true that

$$\sum_{n=1}^{\infty} (-1)^{n-1} \frac{H(2n) + 4H(n)}{n^3 \binom{2n}{n}} - \frac{2}{75} \pi^4 = 0$$

where  $H(n) = \sum_{k=1}^n \frac{1}{k}$  is the well-known harmonic series? Nobody knows! (see [37]).

**Option 4.** Quantum computing and AI? We'll have to wait and see!

## 8.8 A Final Problem

Speaking of the harmonic series  $H(n)$ , we close with one more problem. Let  $\sum_{d|n} d$  denote the sum of the divisors of  $n$ .

**Conjecture 8.20** (\$1,000,000)

$$\sum_{d|n} d \leq H(n) + e^{H(n)} \log H(n) \tag{8.4}$$

for all  $n \geq 1$  (where  $\log$  is the natural logarithm).

Why is this reward so outrageous? Because this conjecture is equivalent to the Riemann Hypothesis! A single  $n$  violating (8.4) would imply there are infinitely many zeroes of the Riemann zeta function off the critical line  $\Re(z) = \frac{1}{2}$  (see [31]). Of course, the \$1,000,000 prize is not from me but rather is offered by the Clay Mathematics Institute since the Riemann Hypothesis is one of their six remaining Millennium Prize Problems [40].

We hope to live to see progress in the Challenges and Conjectures mentioned in this note, especially the last one!

---

---

## References

- [1] A. Alhakim, S. Butler and R. L. Graham, de Bruijn sequences with varying combs, *INTEGERS: The Electronic Journal of Number Theory* **14A** (2014) #A1. 23pp.
- [2] D. Berend and J. E. Harmse, On some arithmetic properties of middle binomial coefficients, *Acta Arithmetica* **84** (1998), 31–41.
- [3] M. Brazil, R. L. Graham, D. A. Thomas and M. Zachariasen, On the history of the Euclidean Steiner tree problem, *Archive for History of Exact Sciences* **68**, (2014), 327–354.
- [4] S. Butler (personal communication, March 2019)
- [5] D. Cieslik, *The Steiner Ratio*, Kluwer, Dordrecht, (2001).
- [6] J. N. Cooper and R. L. Graham, Generalized de Bruijn cycles, *Ann. Comb.* **8** (2004), no.1, 13–25.
- [7] F. R. K. Chung and R. L. Graham, A new bound for Euclidean Steiner minimal trees, *Discrete Geometry and Convexity, Annals N. Y. Acad. Sci.* **440** (1985), 328–346.
- [8] F. R. K. Chung and F. K. Hwang, A lower bound for the Steiner tree problem, *SIAM J. Appl. Math.*, **34** (1978), 27–36.
- [9] F. Chung, P. Diaconis and R. L. Graham, Universal cycles for combinatorial structures, *Discrete Math* **110** (1992), 43–59.
- [10] P. Diaconis and R. L. Graham, *Magical Mathematics: The Mathematical Ideas that Animate Great Magic Tricks*, Princeton Univ. Press, (2011), 244 pp.
- [11] D. Z. Du, B. Gao and R. L. Graham, a tight lower bound for the Steiner ratio in Minkowski Planes, *Disc. Math.* **142** (1995), 49–63.
- [12] D. Z. Du and F. K. Hwang, A new bound for the Steiner ratio, *Trans. Amer. Math. Soc.* **278** (1983), 137–148.
- [13] D. Z. Du and F. K. Hwang, A proof of Gilbert-Pollak’s conjecture on the Steiner ratio, *Algorithmica* **7**, (1992), 121–135.
- [14] P. Erdős On some divisibility properties of  $\binom{2n}{n}$ , *Canad. Math. Bull.* **7** (1964), 513–518.
- [15] P. Erdős, R. L. Graham, I.Z. Ruzsa and E. G. Straus,, On the prime factors of  $\binom{2n}{n}$ , *Math. Comp.*, **29** (1975), 83–92.
- [16] C. Flye Sainte-Marie, Solution to question nr. 48, *L’Intermédiaire des Mathématiciens*, **1** (1894), 107–110.

- [17] S. Glock, F. Joos, D. Kühn and D. Osthus, Euler tours in hypergraphs, arXiv:1808.07720 (2017)
- [18] S. Glock, F. Joos, D. Kühn and D. Osthus, Hypergraph  $F$ -designs for arbitrary  $F$ , arXiv:1706.01800 (2017)
- [19] M. R. Garey, R. L. Graham and D. S. Johnson, The complexity of computing Steiner minimal trees, *SIAM J. Appl. Math.* **32** (1977), 835–859.
- [20] R. L. Graham and P. Hell, On the history of the Minimum Spanning Tree problem, *Annals Hist. of Comp.* **7** (1985), 43–57.
- [21] A. Granville, Arithmetic properties of binomial coefficients, I. Binomial coefficients modulo prime powers, in *Organic mathematics (Burnaby, B.C., 1995)*, pp. 253–276, CMS conf. Proc., **20**, Amer. Math. Soc., Providence RI, 1997.
- [22] A. Granville and O. Ramaré, Explicit bounds on exponential sums and the scarcity of squarefree binomial coefficients, *Mathematica*, **43**, (1995), 73–107.
- [23] G. Hurlbert, On universal cycles for  $k$ -subsets of an  $n$ -set, *SIAM J. Discrete Math.* **7** (1994), 598–604.
- [24] F. K. Hwang, On Steiner minimal trees with rectilinear distance, *SIAM J. Comput.* **30**, (1976), 104–114.
- [25] N. Innami, B. H. Kim, Y. Mashiko and K. Shiohama, The Steiner ratio conjecture of Gilbert-Pollak may still be open, *Algorithmica* **77**:4 (2010), 869–872.
- [26] A. O. Ivanov and A. A. Tuzhilin, The Steiner ratio Gilbert-Pollak conjecture is still open, *Algorithmica* **62** (2012), 630–632.
- [27] B. Jackson, Universal cycles of  $k$ -subsets and  $k$ -permutations, *Discrete Math.* **117** (1993), 141–150.
- [28] P. Keevash, The existence of designs II, arXiv:1802.05900 (2018)
- [29] J. B. Kruskal, On the shortest spanning tree of a graph and the traveling salesman problem, *Proc. Amer. Math. Soc.* **7** (1956), 48–50.
- [30] E. Kummer, Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen, *J. Reine Angew. Math.* **44** (1852), 93–146.
- [31] J. C. Lagarias, An elementary problem equivalent to the Riemann hypothesis, *Amer. Math. Monthly* **109**, (2002), 534–543.
- [32] C. Pomerance, Divisors of the middle binomial coefficient, *Amer. Math. Monthly* **122** (2015), 636–644.
- [33] R. C. Prim, Shortest connection networks and some generalizations, *Bell Syst. Tech. J.* **36** (1957), 1389–1401.
- [34] C. Sanna, Central binomial coefficients divisible by or coprime to their indices, *Int. J. of Number Theory* (in press) (2018)

- [35] W. D. Smith and J. MacGregor Smith, On the Steiner ratio in 3-space, *J. Comb. Th., Series A*, (1995), 301–332.
- [36] D. T. Stallworth and F. W. Roush, An undecidable property of definite integrals, *Proc. Amer. Math. Soc.* **125** (1997), 2147–2148.
- [37] Z. W. Sun, List of conjectural series for powers of  $\pi$  and other constants, arXiv:1102.5649
- [38] D. B. West, *Introduction to Graph Theory*, (second edition) Prentice-Hall, Upper Saddle river, NJ, (2001).
- [39] P. O. De Wet, *Geometric Steiner minimal trees*, Ph. D. thesis, Univ. of South Africa, Pretoria (2008)
- [40] Wikipedia entry for Millennium Prize Problems.