LETTERS TO PROGRESS IN PHYSICS

Dialogue Concerning the Two Chief World Views

Craig Alan Feinstein
2712 Willow Glen Drive, Baltimore, MD 21209, USA. E-mail: cafeinst@msn.com

In 1632, Galileo Galilei wrote a book called *Dialogue Concerning the Two Chief World Systems* which compared the new Copernican model of the universe with the old Ptolemaic model. His book took the form of a dialogue between three philosophers, Salviati, a proponent of the Copernican model, Simplicio, a proponent of the Ptolemaic model, and Sagredo, who was initially open-minded and neutral. In this paper, I am going to use Galileo's idea to present a dialogue between three modern philosophers, Mr. Spock, a proponent of the view that $\mathsf{P} \neq \mathsf{NP}$, Professor Simpson, a proponent of the view that $\mathsf{P} = \mathsf{NP}$, and Judge Wapner, who is initially open-minded and neutral.

Since 2006, I have published four proofs that $\mathsf{P} \neq \mathsf{NP}$ [5–8]. Yet at the present time, if one asks the average mathematician or computer scientist the status of the famous P versus NP problem, he or she will say that it is still open. In my opinion, the main reason for this is because most people, whether they realize it or not, believe in their hearts that $\mathsf{P} = \mathsf{NP}$, since this statement essentially means that problems which are easy to state and have solutions which are easy to verify must also be easy to solve. For instance, as a professional magician, I have observed that most laymen who are baffled by an illusion are usually convinced that the secret to the illusion either involves extraordinary dexterity or high technology, when in fact magicians are usually no more dexterous than the average layman and the secrets to illusions are almost always very simple and low-tech; as the famous designer of illusions, Jim Steinmeyer, said, "Magicians guard an empty safe" [13]. The thinking that extraordinary dexterity or high technology is involved in a magician's secret is, in my opinion, due to a subconscious belief that $\mathsf{P} = \mathsf{NP}$, that problems which are difficult to solve and easy to state, in this case "how did the magician do it?", must have complex solutions.

I have had many conversations in which I have tried to convince all types of people, from Usenet trolls to graduate students to professors to famous world-class mathematicians, that $\mathsf{P} \neq \mathsf{NP}$ with very little success; however, I predict that there will soon come a day when the mainstream mathematics and computer science community will consider people who believe that $\mathsf{P} = \mathsf{NP}$ to be in the same league as those who believe it is possible to trisect an angle with only a straightedge and compass (which has been proven to be impossible) [14].

I got the idea to write this paper after I learned of Galileo's book *Dialogue Concerning the Two Chief World Systems* [4], which presents a dialogue between three philosophers, Salviati, a proponent of the new Copernican model, Simplicio, a proponent of the old Ptolemaic model, and Sagredo, who was initially open-minded and neutral. The dialogue that follows is a dialogue between three modern philosophers, Mr. Spock, a proponent of the view that $\mathsf{P} \neq \mathsf{NP}$, Professor Simpson, a proponent of the view that $\mathsf{P} = \mathsf{NP}$, and Judge Wapner, who is initially open-minded and neutral. Professor Simpson, who is a fictitious anglicized straw man character like Simplicio, is a composite of many of the people whom I have had discussions with over the years about the P versus NP problem. He presents many challenges and questions, all of which have been raised before by real people, that Mr. Spock, the epitome of truth and logic, attempts to answer. And Judge Wapner, the epitome of open-mindedness and fairness, always listens to both sides of their arguments before drawing conclusions.

Spock: Yesterday we discussed the P versus NP problem [2, 3] and agreed that it is a problem of not only great philosophical importance, but also it has practical implications. We decided to look at a proof that $\mathsf{P} \neq \mathsf{NP}$ offered by Craig Alan Feinstein in a letter entitled "A more elegant argument that $\mathsf{P} \neq \mathsf{NP}$" [8]. The proof is surprisingly short and simple:

Proof: Consider the following problem: Let $\{s_1, \ldots, s_n\}$ be a set of n integers and t be another integer. Suppose we want to determine whether there exists a subset of $\{s_1, \ldots, s_n\}$ such that the sum of its elements equals t, where the sum of the elements of the empty set is considered to be zero. This famous problem is known as the SUBSET-SUM problem.

Let $k \in \{1, \ldots, n\}$. Then the SUBSET-SUM problem is equivalent to the problem of determining whether there exist sets $I^+ \subseteq \{1, \ldots, k\}$ and $I^- \subseteq \{k+1, \ldots, n\}$ such that

$$\sum_{i \in I^+} s_i = t - \sum_{i \in I^-} s_i.$$

There is nothing that can be done to make this equation simpler. Then since there are 2^k possible expressions on the left-hand side of this equation and 2^{n-k} possible expressions on the right-hand side of this equation, we can find a lower-bound for the worst-case running-time of an algorithm that solves the SUBSET-SUM problem by minimizing $2^k + 2^{n-k}$ subject to $k \in \{1, \ldots, n\}$.

When we do this, we find that $2^k+2^{n-k} = 2^{\lfloor n/2\rfloor}+2^{n-\lfloor n/2\rfloor} = \Theta(\sqrt{2^n})$ is the solution, so it is impossible to solve the SUBSET-SUM problem in $o(\sqrt{2^n})$ time; thus, because the Meet-in-the-Middle algorithm [10,11,15] achieves a running-time of $\Theta(\sqrt{2^n})$, we can conclude that $\Theta(\sqrt{2^n})$ is a tight lower-bound for the worst-case running-time of any deterministic and exact algorithm which solves SUBSET-SUM. And this conclusion implies that $\mathsf{P} \neq \mathsf{NP}$. □

To me, Feinstein's proof is not only logical but elegant too. Also, his conclusion is confirmed by history; just as Feinstein's theorem retrodicts, no deterministic and exact algorithm that solves SUBSET-SUM has ever been found to run faster than the Meet-in-the-Middle algorithm, which was discovered in 1974 [10, 15].

Simpson: But there is an obvious flaw in Feinstein's "proof": Feinstein's "proof" only considers a very specialized type of algorithm that works in the same way as the Meet-in-the-Middle algorithm, except that instead of sorting two sets of size $\Theta(\sqrt{2^n})$, it sorts one 2^k-size set and one 2^{n-k}-size set. Under these restrictions, I would agree that the Meet-in-the-Middle algorithm is the fastest deterministic and exact algorithm that solves SUBSET-SUM, but there are still many possible algorithms which could solve the SUBSET-SUM problem that the "proof" does not even consider.

Wapner: Professor Simpson, where in Feinstein's proof does he say that he is restricting the algorithms to the class of algorithms that you mention?

Simpson: He does not say so explicitly, but it is obviously implied, since there could be algorithms that get around his assertion that the minimum number of possible expressions on both sides is $\Theta(\sqrt{2^n})$.

Spock: How do you know that there could be such algorithms?

Simpson: I do not know, but the burden of proof is not on me; it is on Feinstein. And he never considers these types of algorithms.

Wapner: It is true that Feinstein never explicitly considers algorithms which work differently than the Meet-in-the-Middle algorithm, and the burden of proof is on Feinstein to show that these types of algorithms cannot run any faster than $\Theta(\sqrt{2^n})$ time.

Spock: Professor Simpson, is the burden of proof on Feinstein to consider in his proof algorithms which work by magic?

Simpson: No, only algorithms that are realistic.

Spock: Then why would you think that algorithms that get around the assertion that the minimum total number of possible expressions on both sides is $\Theta(\sqrt{2^n})$ are realistic?

Simpson: I do not know, but the burden of proof is not on me; it is on Feinstein.

Spock: Have you considered the fact that an algorithm which determines in $o(\sqrt{2^n})$-time whether two sets of size $\Theta(\sqrt{2^n})$ have a nonempty intersection *must* work by magic, unless there is a way to mathematically reduce the two sets into something simpler?

Wapner: Yes, I see your point; the minimum total number of possible expressions on each side of the SUBSET-SUM equation puts a natural restriction on the time that an algorithm must take to solve the SUBSET-SUM problem.

Simpson: But how do you know it is impossible to reduce the SUBSET-SUM problem into something simpler, so that the number of possible expressions on both sides is $o(\sqrt{2^n})$?

Spock: Simple algebra. Try to simplify the SUBSET-SUM equation above. You cannot do it. The best you can do is manipulate the equation to get $\Theta(\sqrt{2^n})$ expressions on each side.

Simpson: I'll agree that you cannot do it algebraically, but what about reducing the SUBSET-SUM problem to the 3-SAT problem in polynomial-time? This can be done since 3-SAT is NP-complete. If there is an algorithm that can solve 3-SAT in polynomial-time, then it would also be able to solve SUBSET-SUM in polynomial-time, contradicting Feinstein's lower-bound claim of $\Theta(\sqrt{2^n})$.

Spock: But this is magical thinking. If a problem is shown to be impossible to solve in polynomial time, then reducing the problem to another problem in polynomial-time will not change the fact that it is impossible to solve the first problem in polynomial time; it will only imply that the second problem cannot be solved in polynomial time.

Wapner: Spock is right about this. Do you have any other objections to Feinstein's argument?

Simpson: I have many objections. For instance, Feinstein's argument can be applied when the magnitudes of the integers in the set $\{s_1, \ldots, s_n\}$ and also t are assumed to be bounded by a polynomial to "prove" that it is impossible to solve this modified problem in polynomial-time. But it is well-known that one can solve this modified problem in polynomial-time.

Spock: But Feinstein's argument in fact *cannot* be applied in such a circumstance, because there would only be a polynomial number of possible values on each side of the equation, even though the total number of possible expressions on each side is exponential. Feinstein's argument implicitly uses the fact that the total number of possible values on each side of the SUBSET-SUM equation is usually of the same order as the total number of possible expressions on each side, when there is no restriction on the magnitude of the integers in the set $\{s_1, \ldots, s_n\}$ and also t.

Simpson: Then here is a better objection: Suppose the set $\{s_1, \ldots, s_n\}$ and also t consist of vectors in $\mathbb{Z}_2^m$ for some positive integer m, instead of integers. Then one could use the same argument that Feinstein uses to "prove" that it is impossible to determine in polynomial-time whether this modified SUBSET-SUM equation has a solution, when in fact one can use Gaussian elimination to determine this information in polynomial-time.

Spock: Feinstein's argument would not apply to this situation precisely because one can reduce the equation

$$\sum_{i \in I^+} s_i = t - \sum_{i \in I^-} s_i.$$

to a simpler set of equations through Gaussian elimination. But when the set $\{s_1, \ldots, s_n\}$ and also t consist of integers, nothing can be done to make the above equation simpler, so Feinstein's argument is applicable.

Simpson: OK, then how would you answer this? Consider the Diophantine equation:

$$s_1 x_1 + \ldots + s_n x_n = t,$$

where x_i is an unknown integer, for $i = 1, \ldots, n$. One could use the same argument that Feinstein uses to "prove" that it is impossible to determine in polynomial-time whether this equation has a solution, when in fact one can use the Euclidean algorithm to determine this information in polynomial-time.

Spock: But again Feinstein's argument would not apply to this Diophantine equation, precisely because this Diophantine equation can be reduced via the Euclidean algorithm to the equation,

$$\gcd(s_1, \ldots, s_n) \cdot z = t,$$

where z is an unknown integer. And it is easy to determine in polynomial-time whether this equation has an integer solution by simply testing whether t is divisible by $\gcd(s_1, \ldots, s_n)$. No such reduction is possible with the SUBSET-SUM equation.

Simpson: The Euclidean algorithm is a clever trick that has been known since ancient times. But how do I know that another clever trick cannot be found to reduce the SUBSET-SUM equation to something simpler? Like for instance, if I take the greatest common denominator of any subset of $\{s_1, \ldots, s_n\}$ and it does not divide t, then I can automatically rule out many solutions to SUBSET-SUM, all at once.

Spock: But such a clever trick does not always work; what if the gcd *does* divide t? The P versus NP problem is a problem about the *worst-case* running-time of an algorithm, not whether there are clever tricks that can be used to speed up the running-time of an algorithm in some instances. Feinstein's proof only considers the *worst-case* running-time of algorithms which solve SUBSET-SUM.

Wapner: Also, it is simple high school algebra that it is impossible to make the SUBSET-SUM equation simpler than it is: Whenever one decreases the number of possible expressions on one side of the equation, the number of possible expressions on the other side increases. Mathematicians can be clever, but they cannot be clever enough to get around this fact.

Simpson: OK, but what about the fact that Feinstein never mentions in his proof the model of computation that he is considering? To be an valid proof, this has to be mentioned.

Spock: Feinstein's proof is valid in any model of computation that is realistic enough so that the computer cannot solve an equation with an exponential number of possible expressions in polynomial-time, unless it is possible to reduce the equation to something simpler.

Simpson: Or what about the fact that Feinstein never mentions in his paper the important results that one cannot prove that $\mathsf{P} \neq \mathsf{NP}$ through an argument that relativizes [1] or through a natural proof [12]?

Spock: Feinstein's proof does not relativize, because it implicitly assumes that the algorithms that it considers do not have access to oracles, and Feinstein's proof is not a natural proof, since it never even deals with the circuit complexity of boolean functions.

Simpson: What about the 2010 breakthrough by Howgrave-Graham and Joux [9] which gives a probabilistic algorithm that solves SUBSET-SUM in $o(\sqrt{2^n})$ time? I realize that the P versus NP problem is not about probabilistic algorithms, but what if their algorithm can be derandomized and solved in $o(\sqrt{2^n})$ time?

Spock: The algorithm by Howgrave-Graham and Joux does not in fact solve SUBSET-SUM, because it cannot determine for certain when there is no solution to a given instance of SUBSET-SUM; it can only output a solution to SUBSET-SUM in $o(\sqrt{2^n})$ time with high probability when a solution exists. Furthermore, even if their algorithm can be derandomized, this does not guarantee that it will run in $o(\sqrt{2^n})$ time. And Feinstein has already proven that such a deterministic and exact algorithm is impossible.

Wapner: Are there any more objections to Feinstein's argument?

Simpson: I have no more specific objections. But the fact that the P versus NP problem has been universally acknowledged as a problem that is very difficult to solve and Feinstein's "proof" is so short and simple makes it almost certain that it is flawed. The fact that I could not give satisfactory responses to Spock's arguments does not mean that Feinstein is correct; Feinstein's proof has been out on the internet for a few years now, and still the math and computer science community as a whole does not accept it as valid. Hence, I believe that they are right and that Feinstein is wrong.

Wapner: Professor Simpson, isn't your reason for not believing Feinstein's proof the same reason Feinstein suggested for why most people do not believe his proof? Because most people believe in their hearts that P=NP, that problems which are difficult to solve and easy to state, in this case the P versus NP problem, cannot have short and simple solutions?

Spock: Indeed it is.

Wapner: And yes indeed, I am convinced that Feinstein's proof is valid and that P ≠ NP.

Submitted on May 22, 2016 / Accepted on May 24, 2016

References

1. Baker T.P., Gill J., and Solovay R. Relativizations of the P ≠ NP Question. *SIAM Journal on Computing*, 1975, v. 4(4), 431–442.
2. Bovet P.B. and Crescenzi P. Introduction to the Theory of Complexity. Prentice Hall, 1994.
3. Cormen T.H., Leiserson C.E., and Rivest R.L. Introduction to Algorithms. McGraw-Hill, 1990.
4. Galilei G. Dialogue Concerning the Two Chief World Systems. University of California Press, 1953.
5. Feinstein C.A. Complexity science for simpletons. *Progress in Physics*, 2006, v. 2, issue 3, 35–42.
6. Feinstein C.A. An elegant argument that $P \neq NP$. *Progress in Physics*, 2011, v. 7, issue 2, 30–31.
7. Feinstein C.A. The computational complexity of the traveling Salesman Problem. *Global Journal of Computer Science and Technology*, 2011, v. 11, issue 23, 1–2.
8. Feinstein C.A. A more elegant argument that $P \neq NP$. *Progress in Physics*, 2012, v. 8, issue 1, L10.
9. Howgrave-Graham N., and Joux A. New generic algorithms for hard knapsacks. *IACR Cryptology ePrint Archive*, 2010, 189.
10. Horowitz E. and Sahni S. Computing partitions with applications to the Knapsack Problem. *Journal of the ACM*, 1974, v. 2l, no. 2, 277–292.
11. Menezes A., van Oorschot P., and Vanstone S. Handbook of Applied Cryptography. CRC Press, 1996.
12. Razborov A. and Rudich S. Natural proofs. *Journal of Computer and System Sciences*, 1997, v. 55, issue 1, 24–35.
13. Steinmeyer J. Hiding the Elephant: How Magicians Invented the Impossible and Learned to Disappear. Da Capo Press, 2004.
14. Angle Trisection. From MathWorld — A Wolfram Web Resource. http://mathworld.wolfram.com/AngleTrisection.html
15. Woeginger G.J. Exact algorithms for NP-hard problems. In: *Lecture Notes in Computer Science*, Springer-Verlag Heidelberg, 2003, v. 2570, 185–207.