PROOF THAT P $\neq$ NP*

JAMELL IVAN SAMUELS†

Abstract. The question does P = NP has confounded mathematicians and computer scientists alike for over 50 years and although there is an almost unanimous agreement that it in fact does not, there still is no absolute proof. In this paper, I attempt to prove to that P does not equal NP.

Key words. NP, P, Computational Complexity

AMS subject classifications. 68Q12, 68Q17

1. Introduction.

In 1971 Stephen Cook [1] proposed a fundamental question to the theory of computer science. The question does NP = P has serious ramifications across a broad range of subjects from cryptography to DNA synthesis and a solution to this problem has been deemed worthy of a Millennium Prize. In this paper I establish the proof through the use of basic fundamentals.

2. Counting.

In mathematics the two basic operations are counting and totalling.

Definition 2.1.
Counting is the acting out of a method using a unit measure. Example there are a hive of bees, I count the bees using my unit measure | *as* ||||||.

Definition 2.2.
Totalling is the explicit use of number to sum a count, I sum my count |||||| *using my numerical system* $1, 2, 3, 4....$ *as* 6.

Counting and totalling inhabit a region named the Method Space M, which is an area used to categorise and derive operations.

Definition 2.3. *A Method M is any operation or process used to solve a problem. In the Method Space, methods are represented as M(current operation, next variable), where* $n \ \forall \ \mathbb{R}$ *and* $i \ \forall \ \mathbb{R}$.

Definition 2.4 (Limit of Counting to 0).
The limit of counting to 0 $M(n, i) \lim_{i\to 0} M(1, 0)$
The limit of totalling to 0 $M(n + i_i, i_{i+1}) \lim_{i\to 0} M(n, 0)$

Definition 2.5 (Limit of Counting to ∞).
The limit of counting to infinity $M(n, i) \lim_{i\to\infty} M(1, 1)$
The limit of totalling to infinity $M(n + i_i, i_{i+1}) \lim_{i\to\infty} M(\infty, \infty)$

Using the method of slopes to measure the difference between counting and totalling .

$$\frac{d\Delta T}{d\Delta C} = \frac{M(\infty,\infty) - M(n,0)}{M(1,1) - M(1,0)} = \frac{M(\infty,\infty)}{M(0,1)} \equiv \frac{(\infty,\infty)}{(0,1)} \tag{2.1}$$

Dividing to resolve this equation you obtain.

$$(1, \infty) \tag{2.2}$$

*Submitted to the editors 02/07/2020.

†Imperial College London, London, (jis13@ic.ac.uk, http://www.researchgate.com/~ddoe/).

Thereby establishing 0 as a non countable number.

3. Checking and Solving.

DEFINITION 3.1. *Checking is the process where you assure that the solution you have gained is valid.*

DEFINITION 3.2. *Solving is the method used to acquire a solution.*

LEMMA 3.3. *Your best solving method can not run faster than your best checking method. Solving* $\lim \xrightarrow{Method}$ *Checking*

4. Probability.

Probability can be stated as the likelihood that an event will occur. It is counted as the number of times an event will occur given the total number of possible events. Any probability outside the boundaries of [0,1] does not exist on the probability plane and therefore can only be interpreted for it's meaning rather than stated as an absolute definition of chance.

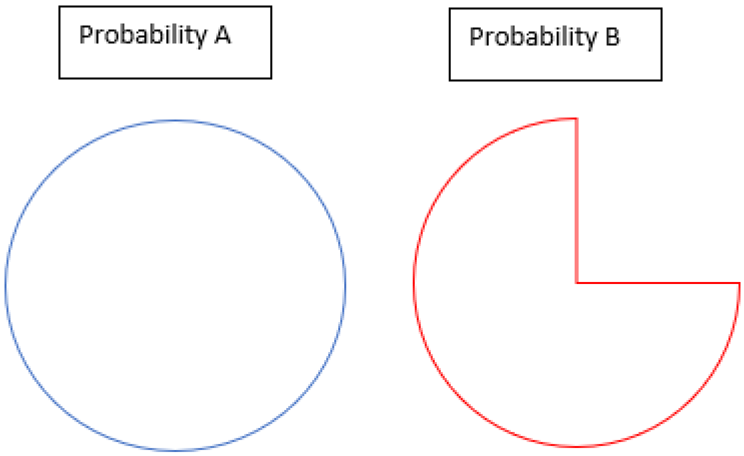

FIG. 1. *Planes of Probability*

4.1. Planes and Cylinders of Probability.

Probabilities must remain on the same plane and in truth they can only be added or subtracted. The use of multiplication can be considered the resolution of a stack of probabilities (and therefore multiple events) that exist on separate planes which you have resolved to one. Therefore we can define a probability plane or cylinder as.

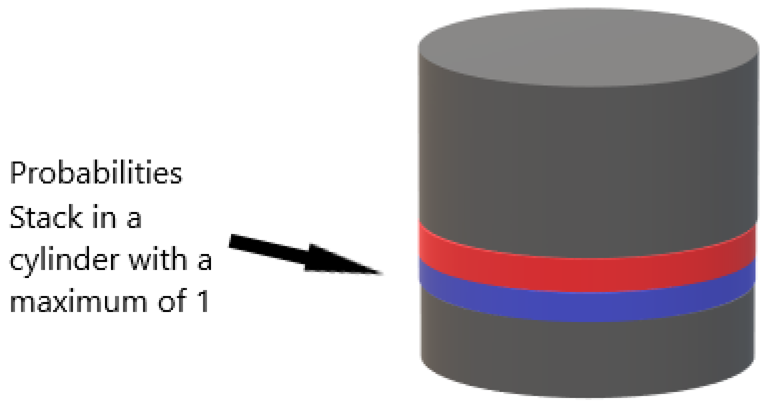

Fig. 2. *Probability Cylinder.*

- A probability plane is the area in which a probability exists or acts upon. Probabilities may exist on separate planes, but they must be resolved to act on one.
- A probability cylinder is a stack of multiple planes, a cylinder must be resolved to act on one plane to calculate the probability of the single event.

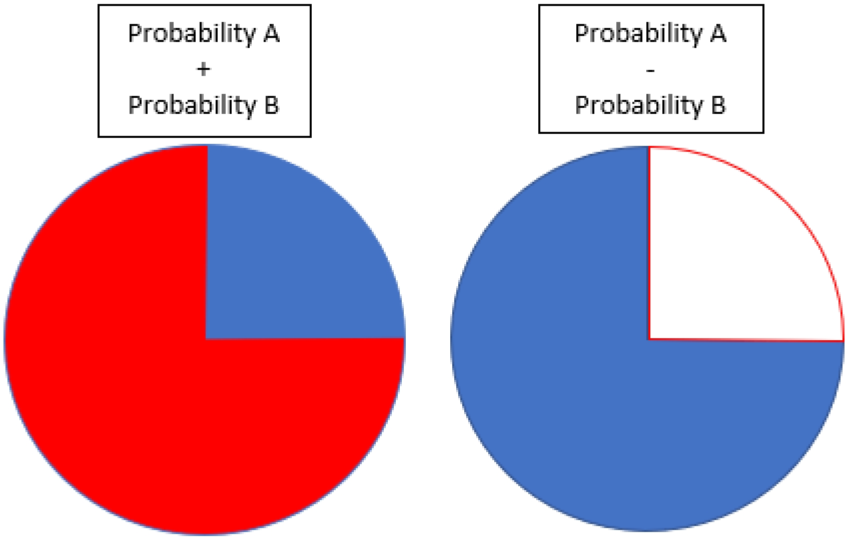

Fig. 3. *Example configurations of A and B.*

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 24 July 2020 doi:10.20944/preprints202007.0588.v1

4.2. The Fundamental Probability - Derivation of Given.

The most fundamental probability to calculate is the probability that event(B) is not going to happen given that event(A) has or is going to happen. All other probabilities that can be calculated, fundamentally rely on this and although can be calculated in other ways, risk losing the information contained within. Henceforth we are going to state the probabilities in the order that they are calculated.

$$P(!B|A) = P(A) - P(B) \tag{4.1}$$

$$P(B|A) = P(A) - P(!B|A) \tag{4.2}$$

4.3. A note on Circular Logic.

The statement $P(B|A) = P(A) - P(A|!B)$ is self refuting and is therefore contradictory. Probabilities as a matter of fact can not be self proving or self refuting as both are a form of circular logic. It is also not possible to circumvent this by stating $P(B|A) = P(A) - P(!B|A)$, because a 'not' case, not derived from an initial 'is' case, technically comes from a separate 'world' of probability. Example

$$P(A) = 1;\ P(B) = \frac{1}{2} \tag{4.3}$$

$$P(A) + P(B) = \frac{3}{2}$$

$$P(!A) + P(!B) = \frac{1}{2}$$

It can be seen that the two sums are distinctly different and therefore they can not be considered to come from the same case.

4.4. Simultaneous Occurrences.

Probabilities must exist on a single plane and as a single event. Any event with more than one possible outcome can be considered a simultaneous event. When resolving multiple events to a single plane or in a single plane, the probabilities must be fully counted to not lose or create inconsistencies in the information contained.

4.4.1. Probability of $\wedge$.

If you recall the standard probability definition of "and" is $P(A \wedge B) = P(A) \times P(B)$.

$$P(A) = 1;\ P(B) = \frac{1}{9}$$

$$1 \times \frac{1}{9} = \frac{1}{9}$$

Therefore.

$$P(A \wedge B) = P(B)$$

And you can henceforth state that the event $P(A \wedge B)$ is not dependent on $P(A)$. The same argument can also be made for $P(A|B)$. And ergo $P(A \wedge B)$ is fundamentally contradictory. This can be stated because the use of multiplication is the loss of information. For example. $[5 + 5 + 5 + 5 + 5]$ contains more information than 5×5. It is therefore better to state that $P(A \wedge B) = P(A|B) \times P(B|A)$. And to treat all "and" statements as a matrix containing the possible events.

 doi:10.20944/preprints202007.0588.v1

$$P(A \wedge B) = \begin{bmatrix} P(A|B) \\ P(B|A) \end{bmatrix} \tag{4.4}$$

4.4.2. Probability of ∨.

Although the probability of $(A \vee B)$ can be considered a fundamental probability as it can be calculated as $P(A) + P(B)$, it is actually one of the derived probabilities as it has more than one possible outcome and therefore must be resolved as a single event.

$$P(!A \vee !B) = \begin{bmatrix} P(!A|B) \\ P(!B|A) \end{bmatrix} \tag{4.5}$$

$$P(!A \vee !B) = P(A \wedge B) + P(!A \wedge !B) \tag{4.6}$$

$$P(A \vee B) = 1 - P(!A \vee !B) \tag{4.7}$$

5. Non-Polynomial Time Problems.

Any Non-Polynomial problem is the result of two distinct and independent variables. I shall refer to these as the value and the order.

- Value v is the property of a variable that makes it distinct.
- Order o is the particular arrangement of properties in manner that is transferable to a base 1 count.

An example of this is Sudoku, where the values are placed in a particular order to solve the problem. Any problem S which can be described in this manner is what we shall consider a Non-Polynomial problem for the sake of this argument.

Definition 5.1. *Polynomial Problems*

$$\begin{aligned} S &= f(v, o) \\ o &= f(v) \\ S &= f(v) \\ P(S) &= P(A) \end{aligned}$$

Definition 5.2. *Non-Polynomial Problems*

$$\begin{aligned} S &= f(v, o) \\ o &\neq f(v) \\ S &\neq f(v) \\ P(S) &= P(A|!B) \end{aligned}$$

5.1. Proof the Problem is exponential.

In the previous section, it was stated that non-polynomial problems are dependent on v and o. When solving a non-polynomial problem it is typical to say a solution is found when both events A and B occur, $P(A \wedge B)$. However in truth, a solution is found when given event A, B has occurred which can only be written as $P(B|A)$. However, when deriving a solution $P(A|!B)$ must be used as $P(A|B)$ as previously stated is contradictory and so therefore is wrong.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 24 July 2020 doi:10.20944/preprints202007.0588.v1

5.1.1. $P(!B|A)$**.** We are now going to derive the algorithm as given event A has occurred, event B will not happen. Where A is the probability that the order is correct B is the probability the value was correct and n is length of the problem i.e. the number of possible solutions .

$$P(A) = 1 \text{ The order is always assumed correct} \tag{5.1}$$
$$P(B) = \frac{1}{n} \text{ The value is assumed as typical to be } \frac{1}{n}$$
$$P(A|!B)_{Algorithm} = P(A) - P(B)$$

- For an algorithm to be correct the probability of finding a solution must equal 1.

$$P(A|!B)_{Algorithm} = 1. \tag{5.2}$$

- For n^2 required solutions the probability of finding the correct solution is.

$$P(A|!B)_{Algorithm} = (P(A) - P(B))^{n^2} = 1^{n^2} \tag{5.3}$$

Using the binomial identity

$$\sum_{k}^{n^2} \binom{n^2}{k} A^{n^2-k} B^k = 1. \tag{5.4}$$

- Where k represents a single step i and is equal to 1
- This can be expanded as

$$\binom{n^2}{0} A^{n^2} B^0 - \binom{n^2-k}{k} B^k + \binom{n^2-2k}{2k} B^{2k} ... + \binom{0}{n^2k} B^{2n^2k} \tag{5.5}$$

- As B is applied as a negative, every $(k+1)th$ step is impossible and therefore incalculable. We must therefore increase the total length of the algorithm to $2n^2$

$$\binom{2n^2}{0} A^{2n^2} B^0 + \binom{2n^2-2k}{2k} B^{2k} ... + \binom{0}{2n^2k} B^{2n^2k} \tag{5.6}$$

- Substituting $B^k = \frac{1}{n}^k$

$$\binom{2n^2}{0} A^{n^2} \left(\frac{1}{n}\right)^0 + \binom{2n^2-2k}{2k} \left(\frac{1}{n}\right)^{2k} ... + \binom{0}{2n^2k} \left(\frac{1}{n}\right)^{2n^2k} \tag{5.7}$$

- As previously stated, you can not count 0. And therefore the expression for the algorithm becomes

$$\binom{2n^2-2k}{2k} \left(\frac{1}{n}\right)^{2k} + \binom{2n^2-4k}{4k} \left(\frac{1}{n}\right)^{4k} ... + \binom{0}{2n^2k} \left(\frac{1}{n}\right)^{2n^2k} = 1. \tag{5.8}$$

5.1.2. Limit Of Probability.

If we are to assume that the solution we are checking is correct, the probability that the value and the order are correct are both 1.

$$P(A)_{Check} = 1 \tag{5.9}$$
$$P(B)_{Check} = 1 \tag{5.10}$$
$$P(A \wedge B)_{Check} = 1 \tag{5.11}$$
$$P(A|B)_{Check} = 1 \tag{5.12}$$

A property of a check is that it is self proving. So given the nature of the problem the probability of the check can be defined as $P(A|B)$. The probability of a check can also be stated to be $P(A \wedge B)$ as an efficient polynomial checking algorithm will only total. Removing the co-efficients from the previously stated algorithm and taking the pure calculation, synonymous to reducing the algorithm from a non-deterministic algorithm to a deterministic algorithm.

$$P(A|!B)_{Algorithm} = \left(\frac{1}{n}\right)^2 + \left(\frac{1}{n}\right)^4 + \left(\frac{1}{n}\right)^6 + ... \left(\frac{1}{n}\right)^{2n^2} = 1 \tag{5.13}$$

The limit of the sum is.

$$\Sigma P(A|!B)_{Algorithm} \to \lim 1. \tag{5.14}$$

And therefore, for non-polynomial problems, as the probability that any polynomial algorithm cam correctly solve the problem can never equal 1, there is no deterministic algorithm that can solve the problem in P time.

5.1.3. Proof of Exponential Nature.

Proof. Recalling that the relationship between $P(A)$,$P(B)$ and n is

$$\Pi_{k=1}^{n^2} P(A)^{n^2-k} P(B)^k = \tfrac{1}{n}^{\sum 2k} \text{ where } k = \begin{bmatrix} n^2 \\ 1 \end{bmatrix}$$

As the left side is checking, let it be said that $P(A) = P(B) = 1$

$$1 = \left(\tfrac{1}{n}\right)^{\sum_1^{n^2} 2k}$$
$$ln|1| = -\sum_1^{n^2} 2kln|n|$$
$$0 = -\sum_1^{n^2} 2kln|n|$$
$$0 = \frac{-\sum_1^{n^2} 2k}{n} \quad \text{derivative}$$
$$e^0 = e^{\frac{-\sum_1^{n^2} 2k}{n}}$$
$$1 = e^{\frac{-\sum_1^{n^2} 2k}{n}}$$

Thereby proving that the problem is naturally exponential. This expression can be calculated as,
$1 = -1$.
And as the modulus of $1 = |-1|$ we can conclude the problem is correctly solved, however, as $-1 \neq 1$ we can also conclude that $NP \neq P$.

5.2. The Argument of Intent.

$P(!B|A)$ represents an algorithm with the intention of getting it wrong/'can be said to be not knowing'. However, by some miracle it manages to get it right, if only once, as it's limit approaches 1. However, $P(B|A)$ which is equal to $(1-\frac{8}{9})$ can never get it right. As the algorithm that intends to get it right, can not get it right, and the algorithm that intends to get it wrong can, we can therefore state that there is no single intentional method that can solve this problem and we can therefore conclude that no efficient polynomial solution exists.

5.3. Upper Bound.

As previously stated in *Lemma* 3.3, the limit for solving is checking.

$$\text{Solving } \lim \xrightarrow{Method} \text{Checking} \tag{5.15}$$

$$e^{\frac{-\sum_1^{n^2} 2k}{n}} lim \xrightarrow{Method} 1$$

$$2n^2 e^{\frac{-\sum_1^{n^2} 2k}{n}} lim \xrightarrow{Method} 2n^2$$

And therefore we can state that the Upper Bound is equal to

$$2n^2 e^{\frac{-\sum_1^{n^2} 2k}{n}}.$$

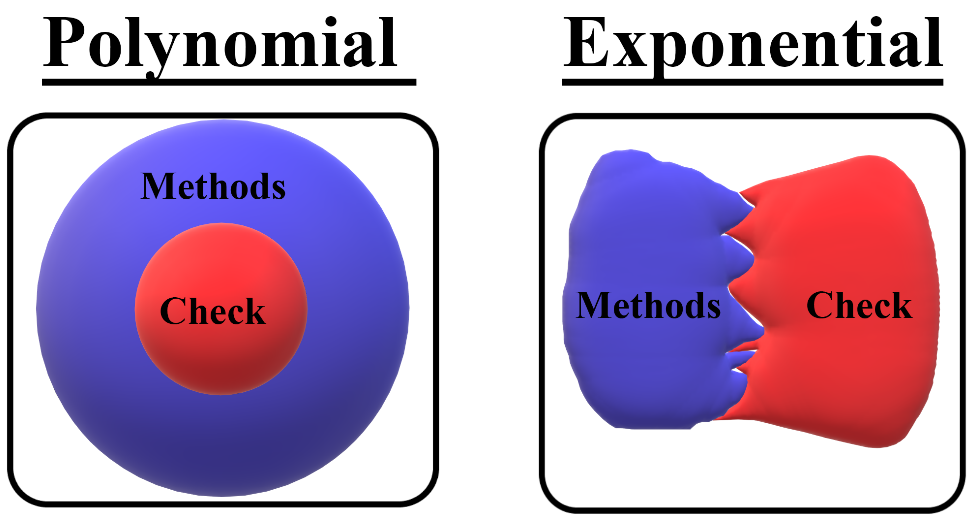

FIG. 4. *'Method Space' for polynomial and non-polynomial problems.*

Acknowledgements. Thank you to Sergei Chernyshenko for dissecting an earlier copy of my work.

REFERENCES

[1] Cook. A.S, "The P versus NP Problem" *Clay Mathematics*,