THIS FOUNDATIONALIST LOOKS AT P = NP

by
Harvey M. Friedman
Distinguished University Professor of Mathematics, Philosophy, Computer Science Emeritus
Ohio State University
Columbus, Ohio

2018 RESOLVE WORKSHOP
Ohio State University
May 29, 2018

My thanks to the RESOLVE community for inviting me to speak here.

Once upon a time I was actually relevant - I developed the decision procedure that led to Split Decision.

I strongly believe there is a huge future in strategic decision procedures of this kind in an essentially unlimited range of relevant contexts. I hope to one day come back to this adventure.

########################

Conventional Wisdom tells us that the possibility that the presently intractable theoretical computer science problems such as P = NP are so difficult because they are neither provable nor refutable in the usual ZFC axioms for mathematics, is too far fetched to deserve any serious consideration.

NOW AGAINST CW

Until recently, I completely agreed with this CW. However, there have been some major advances in discrete and even purely finitary examples of independence from ZFC that are so fundamentally transparent that the possibility of P = NP and related problems being independent of ZFC is at least worth some consideration.

We will discuss one of these new natural examples, Maximal Emulation Stability = MES, particularly slowly and carefully, in order to engage and hopefully interact with this audience of computer scientists and other scholars.

WHAT IS A FOUNDATIONALIST? (from title of talk)

The Foundationalist is continually formulating research projects heavily based on General Intellectual Interest. There is an emphasis on quality of knowledge and understanding rather than quantity or contemporary relevance.
***Blah Blah Blah*.**

Simplified version: I am a mathematical logician with relatively broad interests.

WHAT IS ZFC?

Some of you know and care, some of you care but don't know, and some of you don't know or care. Any know and don't care?

Rather than give any details, it suffices to say that ZFC is the usual foundations for mathematics. If something cannot be proved or refuted in ZFC then it is in a deep sense "mathematically transcendental". This is the beginnings of a much longer story, which will now be cut short.

WHAT IS ZFC INCOMPLETENESS?

Kurt Gödel essentially proved in the 1930's that there are statements in mathematics that are neither provable nor refutable in ZFC (assuming as is commonly believed, that ZFC is internally consistent).

However, the most commonly quoted examples of this "independence" from ZFC are not really part of "elemental combinatorial mathematics". This is the kind of basic mathematics that is the bread and butter of theoretical computer science, and in particular complexity theory.

GRADUAL MOVE TO EVERYBODY'S MATHEMATICS

Over many years, there has been a series of independence results from ZFC in elemental combinatorial mathematics, starting with rather artificial examples. They have gradually improved to recent ones that are unexpectedly simple and interesting. They have moved into the arena of what I call EVERYBODY'S MATHEMATICS.

EVERYBODY'S MATHEMATICS

I now want to present a very friendly slow discussion of one of these new examples, MES = Maximal Emulation Stability.

A good indication that I am indeed dealing with "Everybody's Mathematics" is if gifted high school students can *meaningfully engage* with MES. This will be documented through homework exercises and various forms of engagement.

I hope to be experimenting with this in 2019 and 2020.

WHAT IS MES?

Maximal Emulation Stability.

MES. EVERY FINITE SUBSET OF <u>*$Q[0,k]^k$*</u> HAS A <u>*STABLE MAXIMAL EMULATOR*</u>.

Now that didn't hurt much, did it?

Of course, I need to explain what I am talking about. Very very slowly... So slow that I want you to FEEL it - before you go to sleep.

Note that I have italicized and underlined those parts of MES that I have yet to define.

WHAT IS MES/2?

MES/2. EVERY FINITE SUBSET OF *$Q[0,2]^2$* HAS A *STABLE MAXIMAL EMULATOR*.

This is MES in dimension 2, which we expect to be even easier for many of you to FEEL. Note the continuing italicized underlining to flag notions that I have yet to define.

URGENT BULLETIN: Yesterday I came up with FINITE MES, using only finite initial segments of the natural numbers! This works miracles with people who are squeamish about infinite sets!! But I don't like giving talks on 12 hour old results or "results".

MES/2. EVERY FINITE SUBSET OF *Q[0,2]^2* HAS A *STABLE MAXIMAL EMULATOR*.

WHAT IS Q[0,2]^2?

Q is the set of all rational numbers. Q[0,2]^2 is the set of all ordered pairs from Q[0,2].

For MES/2, Q[0,2]^2 is our space of objects.

Think of Q[0,2]^2 as the 2 × 2 square [0,2] × [0,2]. Keep in the back of your mind that we are being much more explicit than using real numbers. We are only using the usual ordering of rational numbers. We will not even use ADDITION or MULTIPLICATION! Too advanced (smile).

MES/2. EVERY FINITE SUBSET OF $Q[0,2]^2$ HAS A *STABLE MAXIMAL EMULATOR*.

WHAT IS STABILITY IN MES/2?

A maximal emulator, when we slowly explain what it is later, is also going to be a subset of $Q[0,2]^2$ - this time often infinite.

$S \subseteq Q[0,2]^2$ is said to be STABLE if and only if for all $0 \leq p < 1$,

$$(p,1) \in S \leftrightarrow (p,2) \in S.$$

MES/2. EVERY FINITE SUBSET OF $Q[0,2]^2$ HAS A STABLE *MAXIMAL EMULATOR*.

WHAT IS STABILITY IN MES/2 GEOMETRICALLY?

an easy to visualize digression

Here we emphasize pure combinatorics. The geometry here is also important, and in MES/2, very easy to see.

What does stability say, geometrically, about $S \subseteq Q[0,2]^2$?

MES/2. EVERY FINITE SUBSET OF $Q[0,2]^2$ HAS A STABLE *MAXIMAL EMULATOR*.

WHAT IS STABILITY IN MES/2 GEOMETRICALLY?

Look at the line segment L_1 from (0,1) across to (1,1), and line L_2 from (0,2) across to (1,2). $S \subseteq Q[0,2]^2$ is stable means that

S on L_1 without right endpoint (1,1)
S on L_2 without right endpoint (1,2)

look the same. I.e., the second results from shifting the first up by 1.

MES/2. EVERY FINITE SUBSET OF $Q[0,2]^2$ HAS A STABLE *MAXIMAL EMULATOR*.

WHAT IS AN EMULATOR IN MES/2?

requires auxiliary definition

ORDER EQUIVALENCE OF ORDERED QUADRUPLES OF RATIONALS.

This means that they are in the same numerical order!

(0,0,0,0), (1/2,1/2,1/2,1/2) are order equivalent

(0,1/3,1/2,1), (0,1,3/2,2) are order equivalent

(0,1/3,1/2,0), (1,3/2,2,1) are order equivalent

(0,1/3,1/2,0), (1,3/2,2,1/2) are NOT order equivalent

MES/2. EVERY FINITE SUBSET OF $Q[0,2]^2$ HAS A STABLE *MAXIMAL EMULATOR*.

WHAT IS AN EMULATOR IN MES/2?

S is an emulator of $E \subseteq Q[0,2]^2$ if and only if

every element of $S^2 \subseteq Q[0,2]^4$ is order equivalent to some element of $E^2 \subseteq Q[0,2]^4$.

Informally, every pattern of a certain kind found in S can also be found in E.

MES/2. EVERY FINITE SUBSET OF $Q[0,2]^2$ HAS A STABLE *MAXIMAL* EMULATOR.

WHAT IS A MAXIMAL EMULATOR IN MES/2?

In particular, what is a maximal emulator S of E $\subseteq$ $Q[0,2]^2$?

S is a maximal emulator of E $\subseteq$ $Q[0,2]^2$ if and only if

S is an emulator of E $\subseteq$ $Q[0,2]^2$ which is not a proper subset of any emulator of E $\subseteq$ $Q[0,2]^2$.

MES/2. EVERY FINITE SUBSET OF $Q[0,2]^2$ HAS A STABLE MAXIMAL EMULATOR.

DOES EVERY FINITE E ⊆ $Q[0,2]^2$ HAVE A MAXIMAL EMULATOR?

not necessary stable

Yes! List $Q[0,2]^2$ sequentially without repetition.

Inductively put the terms in when and only when you still have an emulator of the given E ⊆ $Q[0,2]^2$. This is greedy and resulting greedy emulator is low level computable.

STABILITY? Well that's the crucial issue!

Greedy emulators are maximal, but may not be stable!

MES/2. EVERY FINITE SUBSET OF $Q[0,2]^2$ HAS A STABLE MAXIMAL EMULATOR.

MAXIMAL EMULATORS OF CERTAIN $E \subseteq Q[0,2]^2$

Emulators and maximal emulators of $\emptyset \subseteq Q[0,2]^2$ are $\emptyset$. Stable.

Emulators of $\{x\} \subseteq Q[0,2]^2$ are $\emptyset$, $\{y\}$, y order equivalent to x. Maximal ones are these $\{y\}$. Stable if 1,2 do not appear in y, easily arranged.

Emulators of $\{(0,0),(1,1),(2,2)\} \subseteq Q[0,2]^2$ are the $S \subseteq Q[0,2]^2$ where all $(p,q) \in S$ has $p = q$. The maximal one is $\{(p,p): 0 \le p \le 2\}$, which is stable.

MES/2. EVERY FINITE SUBSET OF $Q[0,2]^2$ HAS A STABLE MAXIMAL EMULATOR.

MAXIMAL EMULATORS OF CERTAIN $E \subseteq Q[0,2]^2$

Emulators of $\{(0,1),(0,2)\} \subseteq Q[0,2]^2$ are the $S \subseteq Q[0,2]^2$ where all $(p,q),(r,s) \in S$ have $p < q \wedge p = r < s$. The maximal ones are $\{(p,q): p < q\}$, $0 \le p < 2$ fixed. With $p = 0$, is stable.

Emulators of $\{(0,1),(1,2)\} \subseteq Q[0,2]^2$ are $\emptyset$, $\{(p,q)\}$, $p < q$, and the $\{(r,s),(s,t)\} \subseteq Q[0,2]^2$, $r < s < t$. Maximal ones are $\{(0,2)\}$ and these $\{(r,s),(s,t)\}$. Latter are stable if 1,2 do not appear. Easily arranged.

MES/2. EVERY FINITE SUBSET OF $Q[0,2]^2$ HAS A STABLE MAXIMAL EMULATOR.

MAXIMAL EMULATORS OF CERTAIN $E \subseteq Q[0,2]^2$

Emulators of $\{(0,1),(3/2,2)\} \subseteq Q[0,2]^2$ are the $S \subseteq Q[0,2]^2$ where all distinct $(p,q),(r,s) \in S$ have $p < q < r < s \vee r < s < p < q$. The maximal ones are the S with no gaps. Some of these S are stable and some are not. It is easy to arrange for 1,2 to not appear in these S, in which case these S are stable.

MES/2. EVERY FINITE SUBSET OF $Q[0,2]^2$ HAS A STABLE MAXIMAL EMULATOR.

CAN WE PROVE MES/2 IN ZFC?

YES! With difficulty. But I do use a bit more than recursion on the first uncountable ordinal ω_1. Exotic for something in everybody's math!

I envision avoiding ω_1 by analyzing maximal emulators of finite $E \subseteq Q[0,2]^2$, and finitistically constructing stable maximal emulators.

Using a bit more than ω_1 I also prove some sharp forms of MES/2, some of which call for a more powerful form of emulator:

MES/2*. EVERY FINITE SUBSET OF $Q[0,2]^2$ HAS A STABLE MAXIMAL *r-EMULATOR*.

WHAT IS AN r-EMULATOR?

S is an r-emulator of $E \subseteq Q[0,2]^2$ if and only if every element of $S^r \subseteq Q[0,2]^{2r}$ is order equivalent to some element of $E^r \subseteq Q[0,2]^{2r}$.

So an emulator is simply a 2-emulator.

1-emulators are lame. All maximal 1-emulators are easily seen to be stable, and everything is immediate.

MES/2*. EVERY FINITE SUBSET OF $Q[0,2]^2$ HAS A STABLE MAXIMAL r-EMULATOR.

It seems likely that MES/2* will require the same bit more than transfinite recursion on ω_1 to prove. I am hoping to establish this.

MES/3. EVERY FINITE SUBSET OF $Q[0,3]^3$ HAS A STABLE MAXIMAL EMULATOR.

MES/3*. EVERY FINITE SUBSET OF $Q[0,3]^3$ HAS A STABLE MAXIMAL r-EMULATOR.

Stable here means: $0 \leq p < 1 \rightarrow ((p,1,2) \in S \leftrightarrow (p,2,3) \in S)$. r-emulator here means: every element of $S^r \subseteq Q[0,3]^{3r}$ is order equivalent to some element of $E^r \subseteq Q[0,3]^{3r}$.

My proof of MES/3 goes way way beyond ZFC. I doubt if MES/3 can be proved in ZFC, and I strongly doubt that MES/3* can be proved in ZFC.

MES. EVERY FINITE SUBSET OF $Q[0,k]^k$ HAS A STABLE MAXIMAL EMULATOR.

MES*. EVERY FINITE SUBSET OF $Q[0,k]^k$ HAS A STABLE MAXIMAL r-EMULATOR.

Stable here means: $0 \leq p < 1 \rightarrow ((p,1,...,k-1) \in S \leftrightarrow (p,2,...,k) \in S)$. r-emulator means: every $x \in S^r$ is order equivalent to some $y \in E^r$.

We claim MES,MES* are independent of ZFC. See my site, ms. #92, proving MES,MES*. going way way beyond ZFC.
In prep: MES not provable in ZFC. Expect unprovability of MES/k, tiny k, will fall out.

WHAT DOES THIS HAVE TO DO WITH P = NP?

Nothing directly, but:

We believe that the independence from ZFC of statements of this level of fundamentally transparent elementary combinatorial mathematics - "everybody's mathematics" - at least raises the possibility that ZFC does not support a considerable array of combinatorial methods some of which are of just the right kind to be applicable to currently intractable fundamentally combinatorial problems such as P = NP.

ACTION!!!!

We now need to identify mathematical contexts where one or more of the basic elements of MES are present or approximately present.

1. Where have you seen order equivalence? This is all through a lot of math logic, and also the kind of Ramsey theory related to Ramsey's 1930 paper. Where else?

2. Where have you seen our stability, or symmetry suggestive of stability? It is a kind of invariance. It is all through set theory. Where else?

MORE ACTION !!!!

3. Where have you seen things like emulation? What I mean is that we have a given mathematical object, and we look for other mathematical objects that don't introduce any new patterns.

4. Maximality is all over the place in many forms. Can you modify an existing maximality context so that it incorporates elements of 1-3 above?

GILL WILLIAMSON'S IDEAS

Gill Williamson (UCSD CS) has optimistically suggested that some of my *earlier independent combinatorial statements* should lead to the independence of P = NP from ZFC! And he thinks that I may be just the right person to prove this!! This is going to be quite a challenge!!!

I have been concentrating on pushing ZFC Incompleteness squarely into "everybody's mathematics" and will only now start to give Gill's ideas some of the attention they deserve.

GILL WILLIAMSON LINKS

He offers three manuscripts.

Lattice Exit Models

ZFC Limbo

ZFC Independence and Subset Sum

cseweb.ucsd.edu/~gill

http://cseweb.ucsd.edu/~gill/MultUnivSite/

FINITE MAXIMAL EMULATION STABILITY ALSO INDEPENDENT OF ZFC!

Let $n > (8k)!$. Every subset of $\{0,...,kn\}^k$ has a *stable weakly maximal* emulator.

Emulators same except space is $\{0,...,kn\}^k$ - not $Q[0,k]^k$.

$S \subseteq \{0,...,kn\}^k$ is stable if and only if for all $0 \leq p < n$, $(p,n,2n,...,(k-1)n) \in S \leftrightarrow (p,2n,3n,...,kn) \in S$.

S is a weakly maximal emulator of $E \subseteq \{0,...,kn\}^k$ iff S is an emulator of $E \subseteq \{0,..., kn\}^k$ where for all emulators $S \cup \{x,ny\}$ of $E \subseteq \{0,...,kn\}^k$, (x,ny) is order equivalent to some $(x',ny) \in S^2$.