

Puzzle: Zermelo-Fraenkel set theory is inconsistent

Craig Alan Feinstein

2712 Willow Glen Drive, Baltimore, Maryland 21209

E-mail: cafeinst@msn.com, BS"D

Abstract: In this note, we present a puzzle. We prove that Zermelo-Fraenkel set theory is inconsistent by proving, using Zermelo-Fraenkel set theory, the false statement that any algorithm that determines whether any $n \times n$ matrix over \mathbb{F}_2 , the finite field of order 2, is nonsingular must run in exponential time in the worst-case scenario.

Disclaimer: This article was authored by Craig Alan Feinstein in his private capacity. No official support or endorsement by the U.S. Government is intended or should be inferred.

In this note, we present a puzzle. Let M_n be the set of $n \times n$ matrices over \mathbb{F}_2 , the finite field of order 2. And let $f_i : M_n \rightarrow \{0, 1\}$, for $i = 1, \dots, m$, be m functions with the following special property: For any $j \in \{1, \dots, m\}$, there exist at least two $n \times n$ matrices, A and B , such that $f_i(A) = f_i(B) = 1$ for each $i = 1, \dots, j-1, j+1, \dots, m$, but $f_j(A) = 0$ and $f_j(B) = 1$. And let $f : M_n \rightarrow \{0, 1\}$ be defined as $f(A) = \prod_{i=1}^m f_i(A)$ for each $A \in M_n$. We shall now prove, using Zermelo-Fraenkel set theory [1], the following theorem, that we shall afterwards show is false:

Theorem: For any algorithm that computes $f(A)$ given any matrix $A \in M_n$, the algorithm must compute $f_i(A)$ for each $i = 1, \dots, m$ whenever $f_i(A) = 1$ for each $i = 1, \dots, m$, which takes at least m steps.

Proof: We use induction on m : For $m = 1$, the theorem is a tautology.

Assume true for $m = k$. We shall prove true for $m = k + 1$: Let Q be an algorithm that computes $f(A)$ given any matrix $A \in M_n$. Suppose that $f_{k+1}(A) = 1$. Then $f(A) = \prod_{i=1}^k f_i(A)$, so by the induction hypothesis, Q must compute $f_i(A)$ for each $i = 1, \dots, k$ if $f_i(A) = 1$ for each $i = 1, \dots, k$, which takes k steps. Suppose that $f_i(A) = 1$ for each $i = 1, \dots, k$. Then $f(A) = f_{k+1}(A)$, so by the special property of the functions f_i given above, Q must compute $f_{k+1}(A)$, which takes at least one step. Hence, whenever $f_i(A) = 1$ for each $i = 1, \dots, k + 1$, Q must compute $f_i(A)$ for each $i = 1, \dots, k + 1$, which takes at least $k + 1$ steps. \square

We can easily see that the above theorem is false when we let $m = 2^n - 1$ and we define functions $f_i : M_n \rightarrow \{0, 1\}$, where each $i \in \{1, \dots, m\}$ corresponds to

a vector $\mathbf{x} \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}$ via a bijection $g : \{1, \dots, m\} \rightarrow \mathbb{F}_2^n \setminus \{\mathbf{0}\}$, such that $f_{g^{-1}(\mathbf{x})}(A) = 0$ if and only if $A\mathbf{x} = \mathbf{0}$. In this situation, it is not necessary for an algorithm to take at least $m = 2^n - 1$ steps in the worst-case scenario to compute $f(A) = \prod_{i=1}^m f_i(A)$, since computing $f(A)$ is equivalent to determining whether A is nonsingular and it is possible to determine in polynomial-time whether any matrix A is nonsingular via Gaussian elimination [2]. Hence, since we have proven, using Zermelo-Fraenkel set theory, a statement that is known to be false, we can conclude that Zermelo-Fraenkel set theory is inconsistent. Puzzle: Where is the error? (There is an error.)

References

- [1] Weisstein, Eric W. "Zermelo-Fraenkel Set Theory." From MathWorld—A Wolfram Web Resource. <http://mathworld.wolfram.com/Zermelo-FraenkelSetTheory.html>
- [2] Weisstein, Eric W. "Gaussian Elimination." From MathWorld—A Wolfram Web Resource. <http://mathworld.wolfram.com/GaussianElimination.html>