

# 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 prove that Zermelo-Fraenkel set theory is inconsistent by proving, using Zermelo-Fraenkel set theory, the false statement that any algorithm that determines that an  $n \times n$  matrix over  $\mathbb{F}_2$ , the finite field of order 2, is nonsingular must run in exponential time.

**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.

Let  $M_n$  be the set of  $n \times n$  matrices over  $\mathbb{F}_2$ . 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  $f_j(B) = 1$ . We shall now prove, using Zermelo-Fraenkel set theory [1], the following theorem, that we shall afterwards show is false:

**Theorem:** Let  $A \in M_n$ . It is necessary for any algorithm that determines that  $f_i(A) = 1$  for each  $i = 1, \dots, m$  to compute  $f_i(A)$  for each  $i = 1, \dots, m$ , which takes at least  $m$  steps.

**Proof:** We use induction on  $m$ : For  $m = 0$ , the theorem is true vacuously.

Assume true for  $m = k$ . We shall prove true for  $m = k + 1$ : Let  $Q$  be an algorithm that determines that  $f_i(A) = 1$  for each  $i = 1, \dots, k + 1$ . Then  $Q$  determines that  $f_i(A) = 1$  for each  $i = 1, \dots, k$ , so by the induction hypothesis, it is necessary for  $Q$  to compute  $f_i(A)$  for each  $i = 1, \dots, k$ , which takes at least  $k$  steps. By the special property of the functions  $f_i$  given above,  $Q$  cannot determine that  $f_{k+1}(A) = 1$  from the fact that  $f_i(A) = 1$  for each  $i = 1, \dots, k$ ; thus, it is necessary for  $Q$  to also compute  $f_{k+1}(A)$  in order to determine that  $f_{k+1}(A) = 1$ , which takes at least another step. Hence, it is necessary for  $Q$  to 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 one-to-one and onto function  $g : \{1, \dots, m\} \rightarrow \mathbb{F}_2^n \setminus \{\mathbf{0}\}$ , 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 perform at least  $m = 2^n - 1$  steps in order to determine that  $f_i(A) = 1$  for each  $i = 1, \dots, m$ , since determining that  $f_i(A) = 1$  for each  $i = 1, \dots, m$  is equivalent to determining that  $A$  is nonsingular and it is possible to determine in polynomial-time that a 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.

## 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>