

THE POSSIBLE CONSISTENCY OF $P \neq NP$ WITH ZFC

S. GILL WILLIAMSON

ABSTRACT. Our main result, Theorem 3.3, is a restatement of Friedman's Jump Free Theorem which he has shown to be independent of ZFC, the usual axioms of set theory [Fri97]. We explore the consequences of Theorem 3.3, a straight forward translation of the statement of the Jump Free Theorem into sets and functions, also being independent. Corollary 3.4 follows trivially from Theorem 3.3. It is obvious that $P = NP$ also proves Corollary 3.4.

1. INTRODUCTION

Reference [Fri97] evolved from a seminar presented at UCSD (University of California San Diego) by Friedman and subsequent discussions. This latter work has inspired the studies of combinatorial structures cited in the references at the end of this paper. The paper in Journal of Combinatorics [Wil17c] describes connections between combinatorics, ZFC independence and the subset sum problem. An exposition of how this connection is made is given in [Wil17d]. An alternative approach which hints that $P \neq NP$ is consistent with ZFC is presented here. We describe an informal definition of statements that we designate as being in *ZFC Limbo*, a term introduced in the paper Combinatorics in ZFC Limbo [Wil17c]. We show that " $P=NP$ " is in ZFC Limbo in this framework, hinting that $P = NP$ cannot be proved in ZFC.

2. BASIC DEFINITIONS AND THEOREMS

Z denotes the integers and N the nonnegative integers. For $x = (n_1, \dots, n_k) \in N^k$, $\max\{n_i \mid i = 1, \dots, k\}$ is denoted by $\max(x)$. Define $\min(x)$ similarly.

Definition 2.1 (Cubes and Cartesian powers in N^k). The set $E_1 \times \dots \times E_k$, where $E_i \subset N$, $|E_i| = p$, $i = 1, \dots, k$, is called a k -cube of length p . If $E_i = E$, $i = 1, \dots, k$, then this cube is E^k , the k th Cartesian power of E .

Definition 2.2 (Order equivalent k -tuples). Two k -tuples, $x = (n_1, \dots, n_k)$ and $y = (m_1, \dots, m_k)$, are *order equivalent tuples* (x *ot* y) if the following holds: $\{(i, j) \mid n_i < n_j\} = \{(i, j) \mid m_i < m_j\}$ and $\{(i, j) \mid n_i = n_j\} = \{(i, j) \mid m_i = m_j\}$.

Professor Emeritus Computer Science and Engineering, University of California San Diego; <http://cseweb.ucsd.edu/~gill/> **Keywords:** Consistency, ZFC independence, P equals NP, ZFC Limbo regressive regularity, subset sum problem, Jump Free Theorem.

Note that ot is an equivalence relation on N^k . We use “ x ot y ” and “ x, y of order type ot ” to mean x and y belong to the same order type equivalence class. The number of equivalence classes is bounded by k^k .

We present some basic definitions due to Friedman.

Definition 2.3 (Field of a function and reflexive functions). For $A \subseteq N^k$ define $\text{field}(A)$ to be the set of all coordinates of elements of A . A function f is *reflexive* if $\text{domain}(f) \subseteq N^k$ and $\text{range}(f) \subseteq \text{field}(\text{domain}(f))$.

Definition 2.4 (The set of functions $T(k)$). $T(k)$ denotes all reflexive functions with finite domain. We denote a function with domain $D \subseteq N^k$ by f_D .

Definition 2.5 (Full and jump free families). Let $Q \subseteq T(k)$.

- (1) **full family:** We say that $Q \subseteq T(k)$ is a *full* family of functions if for every finite subset $D \subset N^k$ there is at least one function f in Q with domain D .
- (2) **jump free family:** For any finite $D \subset N^k$ and for any $x \in D$ we define $D_x = \{z \mid z \in D, \max(z) < \max(x)\}$. Suppose that for all functions f_A and f_B in Q , $x \in A \cap B$, $A_x \subseteq B_x$, and $f_A(y) = f_B(y)$ for all $y \in A_x$ imply that $f_A(x) \geq f_B(x)$. Then Q will be called a *jump free* family of functions in N^k .

The jump free property arises from numerous recursively constructed algorithms in combinatorics. See references at end. We use ZFC for the axioms of set theory: Zermelo-Frankel plus the axiom of choice. Friedman’s Jump Free Theorem, stated below, can be proved in $\text{ZFC} + (\forall n)(\exists n\text{-subtle cardinal})$ but not in $\text{ZFC} + (\exists n\text{-subtle cardinal})$ for any fixed n (assuming this theory is consistent).

Definition 2.6 (Function regressively regular over E^k). Let $k \geq 2$, $D \subset N^k$, D finite, $f : D \rightarrow N$. We say that f is *regressively regular* over E^k , $E^k \subseteq D$, if for each order type equivalence class ot of k -tuples of E^k either (1) or (2) occurs: (1) For all $x, y \in E^k$ of order type ot , $f(x) = f(y) < \min(E)$ or (2) For all $x \in E^k$ of order type ot , $f(x) \geq \min(x)$. (The third possibility $\min(E) \leq f(x) < \min(x)$ never occurs).

Theorem 2.7. Jump Free Theorem *Let $S \subseteq T(k)$ be a full and jump free family of functions. Let $p, k \geq 2$. Then some $f \in S$ is regressively regular over some E^k , cardinality $|E| = p$.*

A proof of the Jump Free Theorem is in Section 2 of [Fri97], “Applications of Large Cardinals to Graph Theory.” A discussion of a vector valued extension of the Jump Free Theorem and some of its applications is given in Section

3 of [RW99] as well as a short introduction to n -subtle cardinals (Appendix A).

3. SUBSET SUM INSTANCES AND THE JUMP FREE THEOREM

Definition 3.1. (Partitions of N) Let $S \subseteq T(k)$ be a full and jump free family of functions. For a function $f \in S$ and $x \in E^k \subseteq \text{domain}(f)$, $f(x)$ is in one of three intervals that form a partition of N : $I_0^k = [0, \min(E))$, $I_1^k = [\min(E), \min(x))$, $I_2^k = [\min(x), \infty)$.

Note that for $x \in E^k$, $f(x) \notin [\min(E), \min(x))$ if f is *regressively regular* over E^k . In general, we define sets of integers in Z as follows.

Let $\Gamma = \{\gamma \mid \gamma : N \rightarrow Z\}$ denote bijections from N to Z . Let $\gamma X = \{\gamma(x) \mid x \in X\}$, $\gamma \emptyset = \emptyset$. Let $\hat{f} = f|E^k$ be f restricted to E^k . Note that

$$\text{image}(\hat{f}) \cap I_i^k = \{\hat{f}(x) \mid x \in I_i^k\}, i = 0, 1, 2.$$

We prefer the former notation for what follows.

Definition 3.2. Define subsets of Z as follows : For $\gamma_0, \gamma_1, \gamma_2$ in Γ , $f \in S$, $E^k \subseteq \text{domain}(f)$, $|E| = p$, $\hat{f} = f|E^k$. Define

$$F(\hat{f}) = \gamma_0(\text{image}(\hat{f}) \cap I_0^k) \cup \gamma_1(\text{image}(\hat{f}) \cap I_1^k) \cup \gamma_2(\text{image}(\hat{f}) \cap I_2^k)$$

and

$$H(\hat{f}) = \gamma_0(\text{image}(\hat{f}) \cap I_0^k) \cup \gamma_2(\text{image}(\hat{f}) \cap I_2^k).$$

Theorem 3.3. (Jump Free Theorem Set Version). *Let $S \subseteq T(k)$, $k \geq 2$, be a full and jump free family of functions. Consider sets $F(\hat{f})$ and $H(\hat{f})$ of integers. For each $p \geq 2$ there exists $f_p \in S \subseteq T(k)$ for which $F(\hat{f}_p) = H(\hat{f}_p)$.*

Proof. For each $p \geq 2$ use the Jump Free Theorem to choose $f_p \in S$ regressively regular over some $E^k \subseteq \text{domain}(f_p)$, $|E| = p$. By regressive regularity $\gamma_1(\text{image}(\hat{f}_p) \cap I_1^k)$ is the empty set. Thus, $F(\hat{f}_p) = H(\hat{f}_p)$ for this f_p . \square

Theorem 3.3 is a straight forward translation of the Jump Free Theorem into set theoretic terminology. It is very likely that it is itself independent. In any case it is in what we call ZFC Limbo in that its only known proof is the ZFC independent Jump Free Theorem.

Corollary 3.4. (Subset Sum) *Let $t \in N$. For $p \geq 2$ there exists $f_p \in S \subseteq T(k)$ for which the sequence $F(\hat{f}_p)$, $p \geq 2$ is subset sum target zero solvable in polynomial time $O(p^k)$ if and only if $H(\hat{f}_p)$, $p \geq 2$ is subset sum target zero solvable in polynomial time $O(p^k)$. Here the cardinalities of $F(\hat{f}_p)$ and $H(\hat{f}_p)$ are p^k as multisets.*

Proof. Follows directly from Theorem 3.3. It also follows from $P = NP$. \square

We use "ZFC Limbo" as a description of the current status of a statement with respect to the foundations of math. A statement is referred to as being in "ZFC Limbo" if its only known proof uses a statement independent of ZFC or if it has not been proved in ZFC but proves a statement in ZFC Limbo. For example, Theorem 3.3 is in ZFC Limbo because its only proof uses the Jump Free Theorem. Likewise Corollary 3.4 is in ZFC Limbo. " $P = NP$ " will be referred to as being in ZFC Limbo because it yet has no ZFC proof but proves Corollary 3.4. $P = NP$ being in ZFC Limbo in this sense hints at the difficulty of proving it in ZFC and thus at the possibility of $P \neq NP$ being consistent with ZFC.

Acknowledgment: The author thanks Professor Sam Buss (University of California San Diego, Department of Mathematics) for his help.

REFERENCES

- [Fri97] Harvey Friedman. Applications of large cardinals to graph theory. Technical report, Department of Mathematics, Ohio State University, 1997.
- [Fri98] Harvey Friedman. Finite functions and the necessary use of large cardinals. *Ann. of Math.*, 148:803–893, 1998.
- [RW99] Jeffrey B. Remmel and S. Gill Williamson. Large-scale regularities of lattice embeddings of posets. *Order*, 16:245–260, 1999.
- [Wil17a] S. Gill Williamson. ZFC Independence and Subset Sum *arXiv:1708.08186v1 [math.CO]*, 28 Aug 2017.
- [Wil17b] S. Gill Williamson. On the difficulty of proving $P=NP$ in ZFC. *arXiv:1708.08186 [math.CO]*, 2019.
- [Wil17c] S. Gill Williamson. Combinatorics in ZFC limbo. *JOC Vol. 10, Num. 3, 579-593* 2019.
- [Wil17d] S. Gill Williamson. Subset Sum Instances in ZFC Limbo *arXiv:2012.05385v2 [math.CO]*, 2021.