COMPUTATIONAL CONFIRMATION OF CONSISTENCY

by
Harvey M. Friedman
Distinguished University Professor of Mathematics,
Philosophy, Computer Science Emeritus
Ohio State University
Columbus, Ohio
July 3, 2018

Abstract. In this entirely self contained paper, we focus on some practical nondeterministic constructions designed to actually confirm (or refute) the consistency of ZFC and fragments of SRP, or even HUGE. The carrying out of these constructions forever, which is equivalent to the carrying out of these constructions for any given finite number of steps, is equivalent to the consistency of SRP (or HUGE), thus providing algorithmically sensible explicitly Π^0_1 sentences independent of ZFC (and even SRP and HUGE). Here we do not fine tune the algorithms for mathematical simplicity, but rather for the facilitation of computer implementations which search for intense interaction with the essence of large cardinal combinatorics. This environment supports a virtually unlimited range of challenges, in which available computer resources and their optimal use seek their own level. Endless competitive challenges can be arranged representing a virtually unlimited range of difficulty.

1. INTRODUCTION

We recently announced the first tangible incompleteness from the usual ZFC axioms for mathematics, with these three statements:

MAXIMAL EMULATION STABILITY. MES. Every finite subset of $Q[0,k]^k$ has a stable maximal emulator.

MAXIMAL IMITATION STABILITY. MIS. Every finite subset of $Q[0,k]^k$ has a stable maximal imitator.

MAXIMAL CLIQUE STABILITY. MCS. Every order invariant graph on $Q[0,k]^k$ has a stable maximal clique.

See [Fr18b]. These statements are explicitly Σ^1_1 and implicitly Π^0_1 via Gödel's Completeness Theorem. As a spinoff of this development, we sought explicitly Π^0_1 forms which were also of such an elementary transparent character. We have been somewhat, though not yet unequivocally successful, in several directions. One direction involves emulation towers as presented in [Fr18b], section 6. However, we have also been pursuing several other directions, including a nondeterministic algorithms aimed at the construction of maximal cliques in order invariant graphs on Q_2^k. Here Q_2 is the set of dyadic rational numbers. The dyadic rationals are used to facilitate the computer implementations, suggesting the possible use of SAT technology.

The carrying out of these nondeterministic algorithms constructs maximal cliques on induced subgraphs with certain auxiliary properties, and require more than ZFC to prove. It also requires more than ZFC to prove that these nondeterministic algorithms can be carried out for any given finite number of steps. This results in explicitly Π^0_1 sentences that are independent of ZFC and beyond.

This is not the place for a systematic treatment of nondeterministic clique construction algorithms with strong metamathematical properties. We are preparing a separate manuscript with that purpose - see [Fr18c]. This current paper is self contained, and focuses on the nondeterministic algorithms designed for computer implementation that confirms (or refutes) the consistency of ZFC and beyond. Some simpler algorithms for different purposes appear in [Fr18c].

2. ORDER INVARIANT GRAPHS

DEFINITION 2.1. Q_2,Z,N is the set of all dyadic rationals, integers, nonnegative integers, respectively. We use

k,n,m,r,s,t,i,j, with or without subscripts, for positive integers, unless otherwise indicated. We use p,q, with or without subscripts, for dyadic rationals, unless otherwise indicated.

DEFINITION 2.2. A graph is a pair G = (V,E), where V is the set of vertices and $E \subseteq V \times V = V^2$ is the set of edges. It is required that E is irreflexive and symmetric. We say that G is a graph on V. v,w are adjacent if and only if v E w. w is a neighbor of v if and only if v,w are adjacent. A clique is an $S \subseteq V$ such that any two distinct elements of S are adjacent. We also consider a list to be a clique if and only if its set of terms is a clique.

DEFINITION 2.3. Let $x,y \in Q_2^k$. x,y are order equivalent if and only if for all $1 \leq i,j \leq k$, $x_i < x_j \leftrightarrow y_i < y_j$. The upper lift of $x \in Q_2^k$, ul(x), is the result of adding 1 to all nonnegative coordinates of x that are greater than all non integer coordinates of x. The upper shift of $x \in Q2k$, ush(x), is the result of adding 1 to all nonnegative coordinates of x. $x \leq_{lex} y$ if and only if x is lexicographically at most y.

DEFINITION 2.4. $S \subseteq Q_2^k$ is order invariant if and only if for all order equivalent $x,y \in S$, $x \in S \leftrightarrow y \in S$. An order invariant graph on Q_2^k is a graph on Q_2^k whose edge set is an order invariant subset of Q_2^{2k}.

3. NONDETERMINISTIC CONSTRUCTION

Here we present constructions $\alpha(k,G)$, where G is an order invariant graph on Q_2^k and $v \in Q_2^k$. This construction can always be carried out, but proving this requires roughly SRP.

DEFINITION 3.1. Let $v_1,...,v_t \in Q_2^k$. $w \in Q_2^k$ is generated by $v_1,...,v_t$ if and only if every coordinate w_i is
i. 0; or
ii. a coordinate of some v_j; or
iii. is sum of 1 and some nonnegative coordinate of some v_j.

The construction proceeds in stages i = 1,2,3,... . Upon entering stage i, we have a nonempty finite clique $v_1,...,v_j$, $j \geq i$. At every stage, we will append one or more vertices, and never backtrack.

Upon entry to stage 1, which is initialization, we set $v_1 = (-1,...,-k)$.

Upon entry to stage $i \geq 2$, we have clique $v_1,...,v_j$, $j \geq i$. We find the least $1 \leq j' \leq j$ such that some vertex generated by $v_1,...,v_{j'}$ is adjacent to each of $v_1,...,v_j$, and choose one such vertex, y. (Under the unusual circumstance that j' does not exist, we update with $v_1,...,v_j,v_j$, and exit stage i.) Then we choose a non neighbor $z \leq_{lex} y$ of y, and update with $v_1,...,v_j,z,ul(z),ush(z)$, after verifying that this is a clique. We then exit stage i.

THEOREM 3.1. The following are equivalent over WKL_0.
i. Every $\alpha(k,G)$ can be carried out forever.
ii. Every $\alpha(k,G)$ can be carried out for any given finite number of steps.
iii. Con(SRP).
EFA proves ii $\leftrightarrow$ iii.

We now present construction $\beta(k,G)$, where G is an order invariant graph on $Q_2{}^k$ and $v \in Q_2{}^k$. This construction can always be carried out, but proving this requires roughly HUGE.

Upon entry to stage 1, which is initialization, we set $v_1 = (-1,...,-k)$.

Upon entry to stage $i \geq 2$, we have clique $v_1,...,v_j$, $j \geq i$. We find the least $1 \leq j' \leq j$ such that some vertex y with $y_1 \leq y_2$, generated by $v_1,...,v_{j'}$, is adjacent to each of $v_1,...,v_j$, and choose one such vertex, y. (Under the unusual circumstance that j' does not exist, we update with $v_1,...,v_j,v_j$, and exit stage i.) Then we choose a non neighbor $z \leq_{lex} y$ of y, and update with $v_1,...,v_j,z,ul(z),ush(z),(n+2^{-n},y_1,...,y_1,ush(y_1))$, where n is the least positive integer $\geq \max(ush(y_1))$. We then verify that every one of these j+4 terms u, with $u_1 \leq u_2$ is adjacent to every term $u' <_{lex} u$, and every term $(m+2^{-m},y_1,...,y_1,p)$, $m \geq p,1$, has $p = ush(y_1)$. We then exit stage i.

THEOREM 3.2. The following are equivalent over WKL_0.
i. Every $\beta(k,G)$ can be carried out forever.
ii. Every $\beta(k,G)$ can be carried out for any given finite number of steps.

iii. Con(HUGE).
EFA proves ii $\leftrightarrow$ iii.

The ii in both Theorems are obviously explicitly Π^0_2. However, using the well known decision procedure for the first order theory of (Q,<,+1) (or even (Q,Z,<,+)), we see that these ii is explicitly Π^0_1. We can also simply require the balancing discussed in section 4 in the construction, and this is obviously explicitly Π^0_1 without even invoking the decision procedure.

4. COMPUTER IMPLEMENTATIONS

The order invariant graph G can simply be given by a finite list from Q2k of edges up to order equivalence. It is natural to use a listing of elements of $\{1,...,2k\}^{2k}$, no two of which are order equivalent. We can also provide G by an algorithm, which would include simply listing the non edges. Experimentation with the number of edges in G (up to order equivalence) is recommended.

We first need to refine the Update procedure in $\alpha(k,G)$ in order to exert appropriate control over z (after y has been chosen). We add the following additional requirement on z. This will not affect Theorem 3.1. We can also use it for $\beta(k,G)$ and not affect Theorem 3.2.

$$*)\ -k \leq \min(z) \leq \max(z) \leq \max(y)+1$$

This appropriately controls the integer part of z. We also need to appropriately control the fractional parts of the coordinates of z. This is merely a routine bookkeeping issue. Since +1 on nonnegative dyadic rationals plays a role in the notions of internal and upper shift, as well as the nonnegative integers in the upper lift, the fractional parts are what is critical.

List the fractional parts of $v_1,...,v_j$, along with 0,1, as $0 = w_1 < ... < w_p = 1$, $p \geq 2$. We require that z be first provisionally adjusted so that the fractional parts of its coordinates of z lying strictly between two adjacent w's are equally spaced, and then perform round offs so that z remains a dyadic rational. It is imperative that this adjustments of the fractional parts of the coordinates of z be order preserving. In any case, this or some closely

related balancing process would normally be done in any normal computer implementation.

It is clear that $\alpha(k,G)$ as written in section 3 will rapidly get into unacceptable demands on computer resources. However, we can very conveniently adjust the demands that $\alpha(k,G)$ makes.

1. We can set k to be very small. We recommend initially that we use only k = 2, with order invariant graphs G on Q_2^2, edges lying in Q_2^4.
2. Depending on the stage i, in the search for j', we can relax the requirement that j' be least. We do advise that in the search for j' there be some bias towards smallish j'.
3. Depending on the stage i, we can, at our own choosing, use only ul(z), or only ush(z), or neither.
4. We can set the goal to complete few or very few stages in the construction.

Under the various choices of G and 1-4, we obtain a well defined search space according to the nondeterministic choices. It is conceivable that one of these search spaces could be exhaustively searched, with no nondeterministic path found. This would establish the inconsistency of SRP. In fact, the trace of computation should be convertible to an actual inconsistency of SRP.

Similar considerations apply to $\beta(k,G)$, but we should first wait for implementations of $\alpha(k,G)$ to be well underway before addressing this.

5. CONFIRMING CONSISTENCY

Why do we believe that any specific $\alpha(k,G)$ can be carried out indefinitely, or even for any very small number of steps?

Except for really trivial cases, the only reason we have for believing this is the general theorem that it can always be carried out. And this general theorem is proved only with large cardinal hypotheses. That proof provides no information concerning how to actually carry out $\alpha(k,G)$ for even very small numbers of steps.

Furthermore, every time a computer is able to exhaust the full search space for a version of $\alpha(k,G)$, the very consistency of the relevant large cardinals is at stake. If the computer finds no path after exhaustive search, then this finding can be converted to an actual inconsistency (from the documentation of the negative computer search).

In this sense, when the computer is able to carry out various versions of the $\alpha(k,G)$, we are obtaining a kind of confirmation of the consistency of ZFC and even fragments of SRP.

The argument is strong but not air tight. For instance, we might figure out how to prove that under quite general, but not fully general, conditions, $\alpha(k,G)$ can be carried out, staying within a weak fragment of ZFC where the k,G that this finding applies to are not rare, and indeed include the kinds of k,G that one would naturally be investigating in the spirit of this discussion. I think this is very unlikely. But yes, this could deflate the claim that we are confirming consistency. But we could easily recover the initial enthusiasm by simply generating loads of k,G to which these finding does not apply, and successfully treating them.

6. FORMAL SYSTEMS USED

EFA Exponential function arithmetic. Based on 0, successor, addition, multiplication, exponentiation and bounded induction. Same as $I\Sigma_0(\exp)$, [HP93], p. 37, 405.

RCA_0 Recursive comprehension axiom naught. Our base theory for Reverse Mathematics. [Si99,09].

WKL_0 Weak Konig's Lemma naught. Our second level theory for Reverse Mathematics. [Si99,09].

ZF(C) Zermelo Frankel set theory (with the axiom of choice). ZFC is the official theoretical gold standard for mathematical proofs. [Ka94].

SRP ZFC + $(\exists\lambda)(\lambda$ has the k-SRP), as a scheme in k. [Fr01].

SRP^+ ZFC + $(\forall k)(\exists\lambda)(\lambda$ has the k-SRP). [Fr01].

HUGE ZFC + $\{(\exists\lambda)(\lambda$ is k-huge): $k \geq 1\}$.

$HUGE^+$ ZFC + $(\forall k)(\exists\lambda)(\lambda$ is k-huge).

λ is k-huge if and only if there exists an elementary embedding $j:V(\alpha) \to V(\beta)$ with critical point λ such that $\alpha = j^k(\lambda)$. (This hierarchy differs in inessential ways from the more standard hierarchies in terms of global elementary embeddings).

REFERENCES

[Fr01] H. Friedman, Subtle cardinals and linear orderings, Annals of Pure and Applied Logic, Volume 107, Issues 1-3, 15 January 2001, 1-34.

[Fr17] H. Friedman, Concrete Mathematical Incompleteness: Basic Emulation Theory, October 10, 2017, 78 pages. To appear in the Putnam Volume, ed. Cook, Hellman. https://u.osu.edu/friedman.8/foundational-adventures/downloadable-manuscripts/ #92.

[Fr18a] H. Friedman, This Foundationalist Looks At P = NP, May 29, 2018. Keynote Lecture, 2018 Resolve Workshop, Computer Science Department, Ohio State University. 32 pages (24 point). http://u.osu.edu/friedman.8/foundational-adventures/downloadable-lecture-notes-2/, #69.

[Fr18b] H. Friedman, Everybody's Mathematics – Maximal Emulation Stability, 18 pages, June 21, 2018. https://u.osu.edu/friedman.8/foundational-adventures/downloadable-manuscripts/ #106.

[Fr18c] H. Friedman, Clique Constructions and Large Cardinals, in preparation (abstract).

[Gr62] O. A. Gross, *The American Mathematical Monthly*, Vol. 69, No. 1 (Jan., 1962), pp. 4-8.

[HP93] P. Hajek, P. Pudlak, Metamathematics of First-Order Arithmetic, Perspectives in Mathematical Logic, Springer, 1993.

[Ka94] A. Kanamori, The Higher Infinite, Perspectives in Mathematical Logic, Springer, 1994.

[Si99,09] S. Simpson, Subsystems of Second Order Arithmetic, Springer Verlag, 1999. Second edition, ASL, 2009.