Greatly improved thematically and conceptually from 4/20/18, though 4/20/18 is worth keeping.

UPPER IMAGE STABILITY

by
Harvey M. Friedman
Distinguished University Professor of Mathematics, Philosophy, Computer Science Emeritus
Ohio State University
Columbus, Ohio
April 22, 2018

ABSTRACT. We begin with the Upper Image Equation $R_<[A] = A'$, where $R \subseteq [t]^k \times [t]^k$ is the known and $A \subseteq [t]^k$ is the unknown. This Upper Image Equation is easily seen to have a unique solution. For order invariant R, these unique solutions exhibit computational completeness. We seek "stable" $A \subseteq [kn]^k$, $n >> k$, in the sense that for all $p \in [n-1]$, $(p,n,2n,...,kn-n) \in A \leftrightarrow (p,2n,3n,...,kn) \in A$. This requires that we use an approximate form of the Upper Image Equation $R_<[A] = A'$. Upper Image Stability is proved only by going well beyond the usual ZFC axioms for mathematics. In fact, Upper Image Stability is provably equivalent to Con(SRP) over EFA, and is explicitly Π^0_1 (using $n \geq (8k)!!$).

1. DEFINITIONS

DEFINITION 1.1. N is the set of all nonnegative integers. We use n,m,r,s,t for positive integers unless otherwise indicated. $[t] = \{0,...,t\}$. For $x \in N^k$, max(x) is the largest coordinate of x. Let $R \subseteq [t]^k \times [t]^k$ and $A \subseteq [t]^k$. $R_<[A]$ is the Upper Image of R on A, $\{y: (\exists x \in A)(x\ R\ y \wedge \max(x) < \max(y))\}$. $A' = [t]^k \setminus A$. The Upper Image Equation is the equation $R_<[A] = A'$, with known $R \subseteq [t]^k \times [t]^k$ and unknown $A \subseteq [t]^k$.

DEFINITION 1.2. $x,y \in [t]^k$ are order equivalent if and only if for all $1 \leq i,j \leq k$, $x_i < x_j \leftrightarrow y_i < y_j$. $A \subseteq [t]^r$ is order invariant if and only if for all order equivalent $x,y \in$

$[t]^r$, $x \in A \leftrightarrow y \in A$. $R \subseteq [t]^k \times [t]^k$ is order invariant if and only if R is order invariant as a subset of $[t]^{2k}$.

After section 2, we work with t = kn, n >> k, signaling the distinguished numbers n,2n,...,kn. We again work with known order invariant $R \subseteq [kn]^k \times [kn]^k$ and unknown $A \subseteq [kn]^k$.

DEFINITION 1.3. $A \subseteq [kn]^k$ is stable if and only if for all p $\in$ [n-1], (p,n,2n,...,(k-1)n) $\in$ A $\leftrightarrow$ (p,2n,3n,...,kn) $\in$ A.

We seek stable solutions to the Upper Image Equation. Unfortunately, this is not possible. However, we can recover using order equivalence of sets relative to n,2n,...,kn.

DEFINITION 1.4. $x,y \in [kn]^r$ are order equivalent over n,2n,...,kn if and only if (x,n,2n,...,kn),(y,n,2n,...,kn) are order equivalent. $A,B \subseteq [kn]^r$ are order equivalent over n,2n,...,kn if and only if every element of A (B) is order equivalent over n,2n,...,kn to some element of B (A).

Thus instead of requiring that

A is stable
R[A] = A'

we require, e.g., that

A is stable
R[A],A' are order equivalent over n,2n,...,kn

DEFINITION 1.5. EFA is exponential function arithmetic, often written $I\Sigma_0(\exp)$. ZFC is the usual set theoretic axioms for mathematics. SRP = ZFC + {($\exists\lambda$)(λ has the k-SRP): $k \geq 1$}. SRP^+ = ZFC + ($\forall$k)($\exists\lambda$)(λ has the k-SRP).

2. UPPER IMAGE EQUATION

UPPER IMAGE EQUATION. UIE. For all $R \subseteq [t]^k \times [t]^k$ there exists $A \subseteq [t]^k$ such that $R_<[A] = A'$. A is unique.

UIE is proved in EFA by an obvious inductive argument well worth reconstructing on one's own.

After one has internalized the obvious proof of UIE, one readily senses that UIE is one of those

fundamental trivialities
of finite combinatorial mathematics

We shall see that an in depth investigation of UIE leads us naturally on a path that cannot be kept within the usual ZFC axioms for mathematics.

THEOREM 2.1. A is the solution of some Upper Image Equation with $R \subseteq [t]^k \times [t]^k$ if and only if $(0,...,0) \in A$.

Proof: Assume $(0,...,0) \in A$. Let R be such that

i. For all $x \in A$, there are no R predecessors of x.
ii. For all $x \notin A$, there is exactly one R predecessor of x, namely $(0,...,0)$.

We claim that $R_<[A] = A'$. To see this, we have to check that

1) $x \in A$ if and only if x has no R predecessor from A with lower max.

The forward direction is immediate. Suppose $x \notin A$. Then x has an R predecessor from A with lower max, namely $(0,...,0)$. QED

So there cannot be any kind of structure theory for solutions to the Upper Image Equation for general R.

But what about for very explicitly given R? Let's move to this restricted form of UIE.

EXPLICIT UPPER IMAGE EQUATION. EUIE. For all order invariant $R \subseteq [t]^k \times [t]^k$ there exists $A \subseteq [t]^k$ such that $R_<[A] = A'$. A is unique.

Now what can we say about the solutions of the Upper Image Equation for order invariant R? Since the number of order invariant R is roughly double exponential in k (and not t), we have definite prospects of a structure theory.

However, we know that these unique solutions have computational completeness properties which we will take up elsewhere. This precludes any structure theory for them in any normal sense. Thus we seek approximate forms of the Upper Image Equation.

3. UPPER IMAGE STABILITY

We now work in $[kn]^k$, n >> k. This signifies the special significance of the numbers

$$n,2n,...,kn$$

We work with $A \subseteq [kn]^k$ and $R \subseteq [kn]^k \times [kn]^k$. Recall the definition of stable $A \subseteq [kn]^k$, which naturally reflects these numbers (Definition 1.3).

We would like to have

PROPOSITION. For all order invariant $R \subseteq [kn]^k \times [kn]^k$, n >> k, there exists stable $A \subseteq [kn]^k$ such that $R_<[A] = A'$.

but this is refutable. As indicated in section 1, we have the very natural move to

THEOREM 3.1. For all order invariant $R \subseteq [kn]^k \times [kn]^k$, n >> k, there exists stable $A \subseteq [kn]^k$ such that $R_<[A]$ and A' are order equivalent over n,2n,...,kn.

I.e., we have moved from Equality to Order Equivalence over n,2n,...,kn.

We have developed a Machine using large cardinal theory for proving statements like Theorem 3.1. For this particular Theorem 3.1, we have been able to do more work and avoid using anything like the full Machine and keep the proof within a very weak fragment of ZFC.

However, as we gradually elaborate on Theorem 3.1 using Cartesian products, we go through versions where we have no idea whether we can stay within ZFC. At some point, we KNOW that the Machine is required, and the resulting statement is provably equivalent to Con(SRP) over EFA.

Let's fast forward to a version where we comfortably know that the Machine is really required.

UPPER IMAGE STABILITY. UIS. For all order invariant $R \subseteq [kn]^k \times [kn]^k$, $n >> k$, there exists nonempty stable $A \subseteq [kn]^k$ such that $R_<[A] \times A^2$ and $A' \times A^2$ are order equivalent over $n,2n,...,kn$. In fact, $n \geq (8k)!!$ is sufficient.

THEOREM 3.2. UIS is provably equivalent to Con(SRP) over EFA.

As a sample, we can use, e.g.,

$(R_<[A] \times A)^k$ and $(A' \times A)^k$ are order equivalent over $n,2n,...,kn$

and the proof sketch in the next section will work just fine.

4. PROOF SKETCH

Here we sketch a proof of UIS using SRP^+. Fix an order invariant $R \subseteq [kn]^k \times [kn]^k$, $n >> k$. Using large cardinal theory in a standard way, we obtain the following.

1. Countable ordinals $\lambda_1 < \lambda_2 < ... < \lambda$, where λ is the limit of the λ_i.
2. R lifts to order invariant $R^* \subseteq \lambda^k \times \lambda^k$.
3. $S \subseteq \lambda^k$ is the unique solution to the Upper Image Equation with R^*. I.e., $R^*_<[S] = S'$.
4. $(0,...,0) \in S$.
5. S is stable in the following sense. For $\alpha < \lambda_1$, $S(\alpha,\lambda_1,...,\lambda_{k-1}) \leftrightarrow S(\alpha,\lambda_2,...,\lambda_k)$.

We now build a finite subset E_0 of λ_k+1, $|E_0| << n$. The idea is that $S \cap E_0^k$ is the small part of S that we need in order to witness the needed positive information related to the Upper Image Equation $R^*_<[S] = S'$.

First we throw $0,\lambda_1,...,\lambda_k$ into E_0. Look at $(S' \times S^2)|{\leq}\lambda_k$. The number of these tuples under "order equivalence over $\lambda_1,...,\lambda_k$" is $<< n$.

a. Choose one representative from each such equivalence class over $\lambda_1,...,\lambda_k$.
b. Let (y,z) be one of the representatives, $y \in S'|{\leq}\lambda_k$, $z \in S^2$.

c. Throw all ordinal coordinates of y,z into E_0.
d. Note that $y \in R^*_<[S]$. Throw all ordinal coordinates of some $x R^* y$, $x \in S$, $\max(x) < \max(y)$, into E_0.

We now form the structure $(E_0,<,\lambda_1,\ldots,\lambda_k,S|E_0)$, where $S|E_0$ is the k-ary predicate on $E_0 \subseteq \lambda_k+1$. This is a small structure since $|E_0| << n$.

We now expand this small structure to $(E_1,<,\lambda_1,\ldots,\lambda_k,S|E_1)$ with finite $E_1 \subseteq \lambda_k+1$, as follows.

We merely require that

1) each $|E_1 \cap \lambda_i| = in$.

This is easily arranged since $\lambda_1,\ldots,\lambda_k$ are limit ordinals and $n >> k$.

We now verify that

2) $(E_1,<,\lambda_1,\ldots,\lambda_k,S|E_1)$ has nonempty stable $S|E_1$, where $R^*_<[S|E_1] \times (S|E_1)^2$ and $(S|E_1)' \times (S|E_1)^2$ are order equivalent over $\lambda_1,\ldots,\lambda_k$.

Note that the complementation ' here is of course with respect to the domain E_1.

Note that since $R^*_<[S|E_1]$ and $S|E_1$ are disjoint, the forward direction of this claimed order equivalence is immediate. It remains to verify the nonempty stability, and the reverse direction of this order equivalence.

Suppose $\alpha \in E_1 \cap \lambda_1$. Then $(\alpha,\lambda_1,\ldots,\lambda_{k-1}) \in S|E_1 \leftrightarrow (\alpha,\lambda_2,\ldots,\lambda_k) \in S|E_1$ because this equivalence holds without $|E_1$ by 5 above.

S|E1 contains $(0,\ldots,0)$ since $0 \in E1$ and $(0,\ldots,0) \in S$.

Finally, let $v \in (S|E_1)' \times (S|E_1)^2$. Since $v \in E_1^{3k}$, the first part of v lies outside S. In the construction of E_0, we chose some (y,z) order equivalent to v over $\lambda_1,\ldots,\lambda_k$, $y \in (S|E_0)'$, $z \in (S|E_0)^2$, and then chose some $x R^* y$, $x \in S$, with $\max(x) < \max(y)$, $x \in E_0^k$. So v is order equivalent over

$\lambda_1,...,\lambda_k$ to some element of $R^*_<[S|E_0] \times (S|E_0)^2$, and hence to some element of $R^*_<[S|E_1] \times (S|E_1)^2$.

We have now verified 2).

Using 1) above, let h be the unique strictly increasing isomorphism from $(E_1,<,\lambda_1,...,\lambda_k,S|E_1)$ onto $([kn],<,n,...,kn,A)$. Then $(0,...,0) \in A \subseteq [kn]^k$ is stable and $R_<[A] \times A^2$, $A' \times A^2$ are order equivalent over $n,2n,...,kn$, since these properties are preserved under isomorphism. QED