UNIVERSAL PROPERTIES AND INCOMPLETENESS

by
Harvey M. Friedman*
Distinguished University Professor of
Mathematics, Philosophy, and Computer Science
Emeritus
Ohio State University
October 4, 2014
EXTENDED ABSTRACT

*This research was partially supported by the John Templeton Foundation grant ID #36297. The opinions expressed here are those of the author and do not necessarily reflect the views of the John Templeton Foundation.

Abstract. Every order invariant subset of $Q[-r,r]^{2n}$ has a maximal square whose sections at the $x \in \{0,...,r\}^{n<}$ agree below 0. Every universal property of the $f::Q[-n,n]^n \rightarrow Q[-n,n]^n$ with no constants, has a 1-maximal regressive solution with $f(0,...,n-1) \equiv f(1,...,n)$. We prove such purely order theoretic statements in the rationals within ZFC augmented with a standard large cardinal hypothesis, and show that ZFC does not suffice (assuming ZFC is consistent). These statements are implicitly Π^0_1. We also establish this for explicitly Π^0_1 forms. We refer to these developments as "Π^0_1 mathematical incompleteness".

1. INTRODUCTION AND PRELIMINARIES

In this extended abstract we present the current state of the art with regard to the search for mathematically natural Π^0_1 sentences independent of ZFC. Each of our examples is provable from certain large cardinal hypotheses but not in ZFC (assuming ZFC is consistent).

In all of our examples, we impose a universal property on a set of rational vectors or partially defined function of several variables on the rationals, and ask for a maximal solution (variants of inclusion maximal) which obeys a second universal property. This leads to complexities that can be handled well by certain large cardinal hypotheses, but not without. For example, see the Master Template (set,1-max) in section 5.1

There are three main competing approaches, each with its advantages and disadvantages. From a combinatorial point of view, the most familiar approach is through squares, roots, and cliques in section 3 - with cliques (in graphs) the most familiar. The basis approach in section 3 is also combinatorial friendly, with algebraic overtones. Both of these approaches are based on the notion of order invariance. The universal properties approach in section 5, particularly for functions, would be closer to analysis. The examples of statements provable using large cardinals but not in ZFC start in section 2.2.

Here are some formalities that we use throughout the abstract. For additional for mal systems used, see section 8.

DEFINITION 1.1. Q,Z,Z^+,N is the set of all rationals, integers, positive integers, nonnegative integers, respectively. We use k,n,m,r,s,t,i,j exclusively for positive integers unless otherwise indicated. We use p,q exclusively for rational numbers unless otherwise indicated. Let $x \in Q^r$, $y \in Q^s$, $D \subseteq Q$, $S \subseteq Q^n$. $D^{\leq n} = D^1 \cup \ldots \cup D^n$. max(x), min(x) are the largest and smallest coordinates of x, respectively. $S^{\leq}, S^{<}$ is the set of all $x \in S$ whose terms are $\leq, <$, respectively. $x*y$ is the concatenation of x and y. S_x is the section at x, which is $\{y \in Q^{n-r}: x*y \in S\}$. Since $Q^s = \emptyset$ for $s \leq 0$, we see that for $r \geq n$, $S_x = \emptyset$. $S_Q = \cup_{x\in Q}S_x$. $x \leq y$, $x < y$ if and only if $\max(x) \leq \max(y)$, $\max(x) < \max(y)$, respectively. $S|{\leq}x$, $S|{<}x$, $S|{\geq}x$, $S|{>}x$ are $S \cap (-\infty,\max(x)]^n$, $S \cap (-\infty,\max(x))^n$, $S \cap [\max(x),\infty)^n$, $S \cap (\max(x),\infty)^n$, respectively.

DEFINITION 1.2. J is a rational interval if and only if $(\forall x,y,z \in Q)(x < y < z \wedge x,z \in J \rightarrow y \in J) \wedge \inf(J), \sup(J) \in Q \cup \{-\infty,\infty\}$. $Q[a,b] = J \cap [a,b]$, and similarly for $Q[a,b)$, $Q(a,b]$, $Q(a,b)$, where a can be $-\infty$ and b can be ∞, provided they are not next to brackets. J will always denote a Q interval.

DEFINITION 1.3. $f::A \rightarrow B$ if and only if f is a partial function from A into B. I.e., a function whose domain is a subset of A and whose range is a subset of B. We treat functions as sets of ordered pairs. I.e., $f \subseteq A \times B$. Let α,β be mathematical expressions. $\alpha \leq \beta$, $\alpha < \beta$, $\alpha \geq \beta$, $\alpha > \beta$, $\alpha = \beta$, $\alpha \neq \beta$ requires that α,β be both defined. $\alpha\downarrow$, $\alpha\uparrow$ means that α is defined, undefined, respectively. $\alpha \equiv \beta$ if and only if $\alpha = \beta$ or α,β are undefined. $f::Q^n \rightarrow Q^m$ is regressive if and only if for all $x \in dom(f)$, $\max(f(x)) < \min(x)$.

DEFINITION 1.4. Let $h::Q \rightarrow Q$ and $S \subseteq Q^n$. $h(S) = \{h(x): x \in S\}$. $D,E \subseteq Q^n$ agree below x if and only if $D \cap (-\infty,\max(x))^n = E \cap (-\infty,\max(x))^n$.

DEFINITION 1.4. Let λ be a limit ordinal. $E \subseteq \lambda$ is stationary if and only if E meets every closed unbounded subset of λ. For $k \geq 1$, λ has the k-SRP if and only if every partition of the unordered k tuples from λ into two pieces has a homogenous set which is stationary in λ.

Here SRP abbreviates "stationary Ramsey property".

DEFINITION 1.5. SRP is the formal system ZFC + $\{(\exists\lambda)(\lambda$ is k-SRP$)\}_k$. SRP^+ is ZFC + $(\forall k)(\exists\lambda)(\lambda$ is k-SRP$)$. SRP[k] is ZFC + $(\exists\lambda)(\lambda$ is k-SRP$)$.

DEFINITION 1.6. RCA_0 and WKL_0 are the first two of our five main systems of reverse mathematics. See [WIKIa]. EFA is exponential (elementary) function arithmetic. I originally introduced the system as "exponential function arithmetic". See [WIKIb].

DEFINITION 1.7. A Π^0_1 sentence is a sentence asserting that some given Turing machine never halts at the empty input tape. A Π^0_2 sentence is a sentence asserting that some given Turing machine halts at every finite input tape.

2. SQUARES, ROOTS, CLIQUES

Squares, roots, and cliques are closely related, and each has its advantages and disadvantages. So we state all propositions using all three notions.

DEFINITION 2.1. Let $R \subseteq Q^{2n}$. A square in R is a set $S^2 \subseteq R$. A maximal square in R is a square in R which is not a proper subset of any square in R. A root in R is a set S such that $S^2 \subseteq R$. A maximal root in R is a root in R which is not a proper subset of any root in R.

DEFINITION 2.2. A graph is a G = (V,E), where $E \subseteq V^2$ is irreflexive and symmetric. x,y are adjacent in G if and only if x E y. We say that G is a graph on V. A clique in G is an $S \subseteq V$ such that any two distinct elements of S are adjacent. A maximal clique in G is a clique in G which is not a proper subset of any clique in G.

2.1. ORDER INVARIANT, ORDER THEORETIC

DEFINITION 2.1.1. $x,y \in Q^{\leq n}$ are order equivalent if and only if lth(x) = lth(y), and for all $1 \leq i,j \leq$ lth(x), $x_i < x_j \leftrightarrow y_i < y_j$.

DEFINITION 2.1.2. $A \subseteq J^n$ is order invariant if and only if for all order equivalent $x,y \in J^k$, $x \in A \rightarrow y \in A$. An order invariant graph on J^n is a graph (J^n,E), where $E \subseteq J^{2n}$ is order invariant.

THEROEM 2.1.1. Let $A \subseteq J^n$. The following are equivalent.
i. A is order invariant.
ii. A is the union of equivalence classes of order equivalence on J^n.
iii. A can be defined using $x_i < x_j$ and $\neg,\wedge,\vee,\rightarrow,\leftrightarrow$, $1 \leq i,j \leq k$, where the x's range over J.

EXAMPLES. (1,-1,7,1/2) and (9/2,3,9,7/2) are order equivalent. $\{x \in Q[0,1]^4: x_1 \leq x_2 < x_3 < x_4 \vee x_3 \leq x_1 < x_2\}$ is an order invariant subset of $Q[0,1]^4$.

THEOREM 2.1.2. If $J \subseteq J'$ and $A \subseteq J'$ is order invariant, then $A \subseteq J$ is order invariant.

DEFINITION 2.1.3. $x,y \in Q^{\leq n}$ are order equivalent over $u \in Q^r$ if and only if $x*u$ and $y*u$ are order equivalent. Let $A \subseteq Q^n$. A is order invariant over $u \in Q^s$ if and only if for all $x,y \in Q^n$, order equivalent over u, $x \in A \rightarrow y \in A$. A is order theoretic if and only if there exists r,u such that A is order invariant over $u \in Qr$.

THEOREM 2.1.3. Let $A \subseteq Q^n$ and $u \in Q^r$. The following are equivalent.
i. A is order invariant over u.
ii. A can be defined using $x_i < x_j$, $x_i < p$, $p < x_i$, $1 \leq i,j \leq n$, and $\neg,\wedge,\vee,\rightarrow,\leftrightarrow$, where every p is a coordinate of u, and the x's range over Q.

EXAMPLE. $\{x \in Q[0,1]^4 : x_1 \leq x_2 < x_3 < x_4 \vee x_3 \leq x_1 < x_2 \leq 1/5\}$ is an order theoretic subset of $Q[0,1]^4$.

THEROEM 2.1.4. Let $A \subseteq Q^n$. The following are equivalent.
i. A is order theoretic.
ii. There exists r and $u \in Q^r$, such that A is order invariant over u.
iii. A can be defined using $x_i < x_j$, $x_i < p$, $p < x_i$, $1 \leq i,j \leq n$, and $\neg,\wedge,\vee,\rightarrow,\leftrightarrow$, where the p's are constants frosm Q, and the x's range over Q.

THEOREM 2.1.5. If $A \subseteq J^n$ is order theoretic then A is order theoretic. For each fixed n,J, there are only finitely many order invariant subsets of J^n. For each $u \in Q^r$, there are only finitely many $A \subseteq Q^n$ that are order invariant over u. The number depends only on n and the number of distinct coordinates of u.

We will be using order invariant subsets of J^n, order theoretic subsets of Q, and order theoretic $f::Q \rightarrow Q$. The latter two have important characterizations.

THEOREM 2.1.6. $A \subseteq Q$ is order theoretic if and only if A is the union of rational intervals. $f::Q \rightarrow Q$ is order theoretic if and only if f is the union of finitely many $g::Q \rightarrow Q$ whose domain is a rational interval, and which is either constant or the identity on its domain.

2.2. MAXIMALITY

THEOREM 2.2.1. Let X be a set. Every $R \subseteq X^2$ has a maximal square and a maximal root. Every graph on X has a maximal clique.

Proof: Standard by Zorn's Lemma. In fact, any one of the three statements is equivalent to the axiom of choice over ZF. In case X is countable, no axiom of choice is needed. QED

In fact, we consider only squares, roots, and cliques for countable X. Specifically, only for $X = J^k$.

DEFINITION 2.2.1. Let $S \subseteq Q^n$ and $h::Q \to Q$. $h[S] = \{(h(x_1),\ldots,h(x_n)): (x_1,\ldots,x_n \in S\}$.

We begin with three Master Templates.

MASTER TEMPLATE (square). Let $k,n,R,h_1,\ldots,h_k$ be given, where $R \subseteq Q^{2n}$ and $h_1,\ldots,h_k::Q \to Q$ are order theoretic. R has a maximal square $S \supseteq h_1[S] \cup \ldots \cup h_k[S]$.

MASTER TEMPLATE (root). Let $k,n,R,h_1,\ldots,h_k$ be given, where $R \subseteq Q^{2n}$ and $h_1,\ldots,h_k::Q \to Q$ are order theoretic. R has a maximal root $S \supseteq h_1[S] \cup \ldots \cup h_k[S]$.

MASTER TEMPLATE (clique). Let $k,n,J,G,h_1,\ldots,h_k$ be given, where the graph G is on Q^n and $h_1,\ldots,h_k::Q \to Q$ are order theoretic. G has a maximal clique $S \supseteq h_1[S] \cup \ldots \cup h_k[S]$.

THEOREM 2.2.2. Every instance of the above three templates is provably equivalent to a Π^0_1 sentence over WKL_0.

Here are some weak sufficient conditions for the Master Templates above.

PROPOSITION 2.2.3. Every order invariant subset of $Q[-m,m]^{2n}$ has a maximal square whose sections at the $x \in \{0,\ldots,m\}^{n<}$ agree below 0.

PROPOSITION 2.2.4. Every order invariant subset of $Q[-m,m]^{2n}$ has a maximal root whose sections at the $x \in \{0,\ldots,m\}^{n<}$ agree below 0.

PROPOSITION 2.2.5. Every order invariant graph on $Q[-m,m]^n$ has a maximal clique whose sections at the $x \in \{0,\ldots,m\}^{n<}$ agree below 0.

At the strong end, we have the following.

PROPOSITION 2.2.6. Every order invariant subset of $Q[-m,m]^{2n}$ has a maximal square whose sections at order equivalent x,y $\in \{0,...,m\}^{\leq n}$ agree below min(x*y).

PROPOSITION 2.2.7. Every order invariant subset of $Q[-m,m]^{2n}$ has a maximal root whose sections at order equivalent x,y $\in \{0,...,m\}^{\leq n}$ agree below min(x*y).

PROPOSITION 2.2.8. Every order invariant graph on $Q[-m,m]^n$ has a maximal clique whose sections at order equivalent x,y $\in \{0,...,m\}^{\leq n}$ agree below min(x*y).

We can use blocks here.

DEFINITION 2.2.2. A block in N^k is a sequence (i,...,i+k-1), i $\geq$ 0.

PROPOSITION 2.2.9. Every order invariant subset of $Q[-m,m]^{2n}$ has a maximal square whose sections at equal length blocks x,y $\in \{0,...,m\}^{\leq n}$ agree below min(x*y).

PROPOSITION 2.2.10. Every order invariant subset of $Q[-m,m]^{2n}$ has a maximal root whose sections at equal length blocks x,y $\in \{0,...,m\}^{\leq n}$ agree below min(x*y).

PROPOSITION 2.2.11. Every order invariant graph on $Q[-m,m]^n$ has a maximal clique whose sections at equal length blocks x,y $\in \{0,...,m\}^{\leq n}$ agree below min(x*y).

THEROEM 2.2.12. Propositions 2.2.3 – 2.2.11 are provably equivalent over RCA_0, and provably equivalent to the consistency of SRP over WKL_0. It follows that Propositions 2.2.3 - 2.2.11 are
i. provable in SRP^+ but not in SRP (assuming SRP is consistent).
ii. unprovable in ZFC (assuming ZFC is consistent).
iii. neither provable nor refutable in SRP (assuming SRP is 1-consistent).
iv. neither provable nor refutable in ZFC (assuming SRP is 1-consistent).

THEROEM 2.2.13. For each fixed n,m, Propositions 2.2.3 - 2.2.11 are provable in SRP. For each k and each of these propositions, there exists n,m and an order invariant set or graph, such that the proposition is not provable in SRP[k], assuming SRP is consistent. These results hold even if we require that the maximal square, root, or clique, be recursive in 0′ (i.e., Δ^0_2) in the sense of recursion theory.

We do not know if Propositions 2.2.3 - 2.2.11 with Q[-m,m] replaced by Q are provable in ZFC. We need the right endpoint of J to establish unprovability.

CONJECTURE 2.2.14. Every instance of the three Master Templates is either provable in SRP or refutable in RCA_0. We know that this statement is false for any SRP[k], assuming SRP is consistent.

This is a tractable conjecture, although there are some clear difficulties that need to be overcome.

2.3. STEP MAXIMALITY

Step maximality is stronger than maximality, and allows us Let G = (Q^n,E) be a graph on Q^n. G|≤x = $(Q^n|{\leq}x,E|{\leq}x)$.

DEFINITION 2.3.2. Let R ⊆ Q^{2n}. A step maximal square in R is an X ⊆ Q^{2n} such that for all n ≥ 0, X|≤n is a maximal square in R|≤n. A step maximal root in R is an S ⊆ Q^{2n} such that for all n ≥ 0, S|≤n is a maximal root in R|≤n. Let G be a graph on Q^n. A step maximal clique is an S ⊆ Q^n such that for all n ≥ 0, S|≤n is a maximal clique in G|≤n.

THEOREM 2.3.1. Every subset of Q^{2n} has a step maximal square and a step maximal root. Every graph on Q^n has a step maximal clique.

MASTER TEMPLATE (square,step). Let k,n,J,R,$h_1,...,h_k$ be given, where R ⊆ J^{2n} is order invariant, and $h_1,...,h_k$::J → J are order theoretic. R has a step maximal square, which is preserved by $h_1,...,h_k$.

MASTER TEMPLATE (root,step). Let k,n,J,R,$h_1,...,h_k$ be given, where R ⊆ J^{2n} is order invariant, and $h_1,...,h_k$:J → J are order theoretic. R has a step maximal root, which is preserved by $h_1,...,h_k$.

MASTER TEMPLATE (clique,step). Let k,n,J,G,$h_1,...,h_k$ be given, where G is an order invariant graph on J^n, and

$h_1,\ldots,h_k:J \to J$ are order theoretic. G has a step maximal clique, which is preserved by $h_1,\ldots,h_k$.

THEOREM 2.3.2. Every instance of the above three templates is provably equivalent to a Π^0_1 sentence over WKL_0.

Theorem 2.3.2 can be shown to be provably equivalent to Π^0_1 sentence over WKL_0 using the Gödel Completeness Theorem.

The following Propositions do not fall under the Master Templates because they use all of N. However, if N is replaced by {0,...,r}, then the Propositions fall under the Master Templates. Nevertheless, they can be shown to be provably equivalent to Π^0_1 sentences over WKL_0 by Gödel's Completeness Theorem.

PROPOSITION 2.3.3. Every order invariant subset of Q^{2n} has a step maximal square whose sections at the $x \in N^{n<}$ agree below 0.

PROPOSITION 2.3.4. Every order invariant subset of Q^{2n} has a step maximal root whose sections at the $x \in N^{n<}$ agree below 0.

PROPOSITION 2.3.5. Every order invariant graph on Q^n has a step maximal clique whose sections at the $x \in N^{n<}$ agree below 0.

PROPOSITION 2.3.6. Every order invariant subset of Q^{2n} has a step maximal square whose sections at order equivalent $x,y \in N^{\leq n}$ agree below $\min(x*y)$.

PROPOSITION 2.3.7. Every order invariant subset of Q^{2n} has a step maximal root whose sections at order equivalent $x,y \in N^{\leq n}$ agree below $\min(x*y)$.

PROPOSITION 2.3.8. Every order invariant graph on Q^n has a step maximal clique whose sections at order equivalent $x,y \in N^{\leq n}$ agree below $\min(x*y)$.

We can use blocks here.

DEFINITION 2.3.3. A block in N^k is a sequence $(i,\ldots,i+k-1)$, $i \geq 0$.

PROPOSITION 2.3.9. Every order invariant subset of Q^{2n} has a step maximal square whose sections at equal length blocks $x,y \in N^{\leq n}$ agree below min(x*y).

PROPOSITION 2.3.10. Every order invariant subset of Q^{2n} has a step maximal root whose sections at equal length blocks $x,y \in N^{\leq n}$ agree below min(x*y).

PROPOSITION 2.3.11. Every order invariant graph on Q^n has a step maximal clique whose sections at equal length blocks $x,y \in N^{\leq n}$ agree below min(x*y).

All of these Propositions can be shown to be provably equivalent to a Π^0_1 sentence over WKL_0 using Gödel's Completeness Theorem.

THEOREM 2.3.12. Theorems 2.2.12 and 2.2.13 apply to Propositions 2.3.3 - 2.3.11.

CONJECTURE 2.3.13. Every instance of the three Master Templates is either provable in SRP or refutable in RCA_0. We know that this statement is false for any SRP[k], assuming SRP is consistent.

We are definitely closer to establishing this than Conjecture 2.2.14.

3. #-BASES, #≤-BASES

DEFINITION 3.1. Let $R \subseteq Q^{2n}$. S is a basis for R if and only if

$$S = \{x \in Q^n: \neg(\exists y \in S)(x\ R\ y \wedge x > y)\}.$$

We think of the relation $x\ R\ y \wedge x > y$ as "x reduces to y". So the above equation says that S is the set of all things that don't reduce to anything in S. So nothing in S can reduce to anything in S, and everything outside S does reduce to something in S. This earns the name "basis".

Unfortunately, bases do not generally exist.

THEROEM 3.1. For each n there exists an order invariant $R \subseteq Q^{2n}$ with no basis.

DEIFNITION 3.2. For $S \subseteq Q^n$, S# is the least D^n containing S

$\cup \{0\}^n$. Let $R \subseteq Q^{2n}$. S is a #-basis for R if and only if

$$S = \{x \in S\#: \neg(\exists y \in S)(x\ R\ y \wedge x > y)\} \subseteq Q^n.$$

So again, nothing in S reduces to anything in S. Also, everything in S#\S reduces to something in S.

Obviously every $R \subseteq Q^{2n}$ has the #-basis $\{0\}^n$.

DEFINITION 3.3. The upper shift is ush:Q → Q with h(p) = p+1 if p ≥ 0; p otherwise.

THEOREM 3.2. Every order invariant subset of Q^{2n} has a #-basis $S \supseteq S|{\geq}0 + 1$. For all n there exists an order invariant subset of Q^{2n} with no #-basis $S \supseteq S+1$.

PROPOSITION 3.3. Every order invariant subset of Q^{2n} has a #-basis $S \supseteq ush(S)$.

THEOREM 3.4. Theorems 2.2.12 and 2.2.13 apply to Proposition 3.3.

With some effort we can establish a priori that Proposition 3.3 is provably equivalent to a Π^0_1 sentence over WKL_0.

To Template Proposition 3.3, we use rational piecewise linear f::Q → Q.

DEFINITION 3.4. $A \subseteq Q^n$ is rational piecewise linear if and only if A can be defined using rational linear inequalities, in variables $x_1,\ldots,x_n$ ranging over Q, and $\neg,\wedge,\vee,\rightarrow,\leftrightarrow$.

THEOREM 3.5. $A \subseteq Q$ is rational piecewise linear if and only if A is order theoretic. f::Q → Q is rational piecewise linear if and only if f is the union of finitely many g::Q → Q whose domain is a rational interval, and which is rational linear on that domain.

We are now ready for the Templates.

TEMPLATE (#,ord). Let h::Q → Q be order theoretic. Every order invariant subset of Q^{2n} has a #-basis $S \supseteq h[S]$.

TEMPLATE (#,lin). Let h::Q → Q be rational piecewise linear. Every order invariant subset of Q^{2n} has a #-basis ⊇ h[S].

We also have the obvious multiple forms.

TEMPLATE (#,ord,many). Let $h_1,...,h_k$::Q → Q be order theoretic. Every order invariant subset of Q^{2n} has a #-basis S ⊇ $h_1[S] \cup ... \cup h_k[S]$.

TEMPLATE (#,lin,many). Let $h_1,...,h_k$::Q → Q be rational piecewise linear. Every order invariant subset of Q^{2n} has a #-basis S ⊇ $h_1[S] \cup ... \cup h_k[S]$.

Instances of Template (#,ord,many) are a priori provably equivalent to Π^0_1 sentences over WKL_0. This likely can be carried out with more difficulty for Template (#,lin).

THEOREM 3.6. Every instance of Template (#,ord,many) is provable in SRP or refutable in RCA_0. For all k there exists an instance of Template (#,ord) that is provable in SRP but not in SRP[k], assuming SRP is consistent.

CONJECTURE 3.7. Every instance of Template (#,lin) is provable in SRP or refutable in RCA_0. Every instance of Template (#,lin,many) is provable in SRP or refutable in RCA_0.

By Theorem 3.5, we know that Conjecture 3.6 fails for every SRP[k], assuming SRP is consistent.

Conjecture 3.7 is entirely tractable, especially for Template (#,lin).

We now weaken #-bases.

DEFINITION 3.5. Let R ⊆ Q^{2n}. S is a #≤-basis if and only if

$$S \subseteq Q^n \wedge S^{\leq} = \{x \in S\#^{\leq}: \neg(\exists y \in S)(x \mathrel{R} y \wedge x > y)\}.$$

PROPOSITION 3.8. Every order invariant subset of Q^{2n} has a #≤-basis, where each $S_{t+(1/2t)} = ush[S_Q]|{\leq}t \subseteq S_Q$.

THEOREM 3.9. Proposition 3.8 is provably equivalent to Con(HUGE) over WKL0.

Proposition 3.8. can be seen to be a priori provably equivalent to a Π^0_1 sentence over WKL_0 using Gödel’s Completeness Theorem.

This approach can be extended to go beyond I3 and even I2. Also, there are many opportunities here for Templating.

4. EXPLICITLY FINITE FORMS

The explicitly Π^0_1 sentence we present here does not involve sections or the upper shift. Instead, it relies on the combinatorial structure of the positive integers.

DEFINITION 4.1. $Q<m> = \{i/j \in Q[-m,m]: |i|,|j| \leq m!\}$. $R \subseteq Q<m>^n$ is order invariant if and only if for all order equivalent $x,y \in Q<m>^n$, $x \in R \leftrightarrow y \in R$. N is the set of all nonnegative integers. $N! = \{1!,2!,...\}$.

DEFINITION 4.2. Let $R \subseteq Q<m>^{2n}$ and $S \subseteq Q<m>^n$. S is R independent if and only if $S \subseteq Q<m>^n$, and no two distinct elements of S are related by R. B red(R,S) C red(R,S) D if and only if for all $x \in (B \cap Q<m>)^n$ $((C \cap Q<m>)^n)$, there exists $y \in C^n$ (D^n) such that x R y and $\max(x) \geq \max(y)$. B red(R,S) C red(R,S) D, with or without p if and only if B red(R,S) C red(R,S) D, and B\{p} red(R,S) C\{p} red(R,S) D\{p}. The latter is read "B R-reduces by S to C, which R-reduces to by S to D, with or without p".

THEOREM 4.1. ($N! \to Z \to Q$). Every order invariant $R \subseteq Q<m>^{2n}$ has an independent S such that N! red(R,S) Z red(R,S) Q.

PROPOSITION 4.2. ($N! \to Z \to Q$). Every order invariant $R \subseteq Q<m>^{2n}$ has an independent S such that N! red(R,S) Z red(R,S) Q, with or without (8n)!-1.

Note that Proposition 4.2 is explicitly Π^0_1.

THEOREM 4.3. Proposition 4.2 is provably equivalent to Con(SMAH) over ACA. (SMAH = strongly Mahlo cardinal hierarchy). It is provable in SMAH+ but not in any consistent SMAH[k]. In particular, it is not provable in ZFC (assuming ZFC is consistent).

For the explicitly Π^0_1 sentence corresponding to Con(HUGE), we stay remarkably close to Proposition 3.8.

DEFINITION 4.3. Let $R \subseteq Q\langle m\rangle^{2n}$ and $S \subseteq Q\langle m\rangle^n$. B $\leq$-red(R,S) C $\leq$-red(R,S) D if and only if for all $x \in (B \cap Q\langle m\rangle)^{n\leq}$ ($(C \cap Q\langle m\rangle)^{n\leq}$), there exists $y \in C^n$ (D^n) such that x R y and $\max(x) \geq \max(y)$.

PROPOSITION 4.4. Every order invariant $R \subseteq Q\langle 9n\rangle^{2n}$ has an independent S such that $Q\langle 4n\rangle$ $\leq$-red(R,S) $Q\langle 6n\rangle$ $\leq$-red(R,S) $Q\langle 8n\rangle$, where each $S_{t+(1/t)} = \text{ush}[S_Q]|{\leq}t \subseteq S_Q$, $t = 2,\ldots,n$.

Note that Proposition 4.4 is explicitly Π^0_1.

THEOREM 4.5. Proposition 4.4 is provably equivalent to Con(HUGE) over EFA. It is provable in HUGE+ but not in any consistent HUGE[k]. In particular, it is not provable in ZFC (assuming ZFC is consistent).

5. UNIVERSAL PROPERTIES

The universal property approach has advantages and disadvantages. It doesn't directly involve order invariant $R \subseteq J^{2n}$. It is more general, and it is particularly well suited to dealing with partial functions from J^n into J^m.

In order to obtain Π^0_1 incompleteness, we cannot use maximality. We instead use 1-maximality, a natural weakened form of maximality. For some, this may not really be a disadvantage.

We begin by introducing the universal properties of the $S \subseteq J^n$.

DEFINITION 5.1. The Boolean formulas for the $S \subseteq J^n$ are the proposition combinations $(\neg,\wedge,\vee,\rightarrow,\leftrightarrow)$ of formulas $\alpha_1 < \alpha_2$, $\alpha_1 \leq \alpha_2$, $\alpha_1 = \alpha_2$, $\alpha_1 \neq \alpha_2$, $(\alpha_1,\ldots,\alpha_k) \in S$, where the α's are either variables x_i $i \geq 1$, ranging over J, or constants from J. We can equivalently use only $\neg,\wedge$, $\alpha_1 < \alpha_2$, $(\alpha_1,\ldots,\alpha_n) \in S$.

DEFINITION 5.2. The universal properties of the $S \subseteq J^n$ take the form $(\forall x_1,\ldots,x_r \in J)(\varphi)$, where φ is a Boolean formula for the $S \subseteq J^n$ whose variables are among the distinct variables $x_1,\ldots,x_r$. A solution to P is an $S \subseteq J^n$ for which P holds.

The squares and roots in order invariant $R \subseteq J^{2n}$ and the cliques in order invariant graphs on J^n are each the solution sets to certain universal properties of the $S \subseteq J^{2n}$, the $S \subseteq J^n$, and the $S \subseteq J^n$, as defined in section 2. These corresponding universal properties do not use anything like the full power of $\neg,\wedge,\vee,\rightarrow,\leftrightarrow$, and obey the important condition that any subset of a square, root, clique is also a square, root, clique. This does not hold for general universal properties.

We now introduce the universal properties of the $f::J^n \rightarrow J^m$.

DEFINITION 5.3. The J terms for the $f::J^n \rightarrow J^m$ are the variables x_i, $i \geq 1$, constants from J, and expressions $f_j(\alpha_1,\ldots,\alpha_n)$, where the α's are these variables or constants, and $1 \leq j \leq m$. Here f_j is the jth coordinate function of f. I.e., $f_j(\alpha_1,\ldots,\alpha_n)$ is the jth coordinate of the m-tuple $f(\alpha_1,\ldots,\alpha_n)$. Of course, f1,...,fm,f all have the same domain. If n = 1 then we just write $f(\alpha_1,\ldots,\alpha_n)$.

DEFINITION 5.4. The Boolean formulas for the $f::J^n \rightarrow J^m$ are the propositional combinations $(\neg,\wedge,\vee,\rightarrow,\leftrightarrow)$ of formulas $\alpha < \beta$, $\alpha \leq \beta$, $\alpha = \beta$, $\alpha \neq \beta$, $\alpha \equiv \beta$, $\alpha\uparrow$, $\alpha\downarrow$, where α,β are J terms for the $f::J^n \rightarrow J^m$. The Boolean properties for the $f:J^n \rightarrow J^m$ are the Boolean formulas for the $f::J^n \rightarrow J^m$ that have no variables.

DEFINITION 5.5. The universal properties of the $f::J^n \rightarrow J^m$ take the form $(\forall x_1,\ldots,x_r \in J)(\varphi)$, where $x_1,\ldots,x_r$ are distinct variables, and φ is a Boolean formula for the $f:J^n \rightarrow J^m$ where all variables are among the distinct variables $x_1,\ldots,x_r$. A (regressive) solution to P is an (regressive) $f::J^n \rightarrow J^m$ for which P holds.

THEOREM 5.6. Every universal property of the $S \subseteq J^n$ has the same solutions as ones that only use $\neg,\wedge$, variables, and constants. Every universal property of the $f::J^n \rightarrow J^m$ has the same solutions as ones that only use $\neg,\wedge,<,f$, variables, and constants. I.e., does not use $\leq,=,\neq,\equiv,\uparrow,\downarrow,\vee,\rightarrow,\leftrightarrow$. If we allow nesting of f in Definition 2.6, then we also get the same solution sets.

5.1. MAXIMALITY

We now introduce the crucial notion of maximality. Consideration of maximal solutions leads to Σ^1_1 sentences independent of ZFC. Consideration of the weaker 1-maximality (in fact t-maximality and <∞-maximality) leads to Π^0_1 sentences independent of ZFC. We will focus entirely on the particularly natural 1-maximality.

DEFINITION 5.1.1. Let P be a universal property of the $S \subseteq J^n$ or the $f::J^n \rightarrow J^m$. A maximal solution to P is a solution to P which is not a proper subset of a solution to P. A t-maximal solution to P is a solution to P which is not a proper subset of a solution to P obtained by adding at most t new elements. A <∞-maximal solution to P is a solution to P which is not a proper subset of a solution to P obtained by adding finitely many new elements.

THEROEM 5.1.1. Every universal property of the $S \subseteq J^n$ has a maximal solution. This is provable in WKL_0 (even in RCA_0 + paramterless WKL_0), and the maximal solution can be found recursive in 0′ (or equivalently, can be taken to be Δ^0_2).

MASTER TEMPLATE (set,max). Let n,J,P,P′ be given, where P,P′ are universal properties of the $S \subseteq J^n$. There is a maximal solution to P that is also a solution to P′.

MASTER TEMPLATE (set,<∞-max). Let n,J,P,P′ be given, where P,P′ are universal properties of the $S \subseteq J^n$. There is a <∞-maximal solution to P that is also a solution to P′.

MASTER TEMPLATE (set,t-max). Let n,t,J,P,P′ be given, where P,P′ are universal properties of the $S \subseteq J^n$. There is a t-maximal solution to P that is also a solution to P′.

THEOREM 5.1.2. Every instance of Master Template (set,max) is provably equivalent to a Σ^1_1 sentence over WKL_0. Every instance of Master Template (set,<∞-max) and Template (set,t-max) is provably equivalent to a Π^0_1 sentence over WKL_0.

The proof of Theorem 5.1.2 for max uses standard techniques involving paths through 0,1-trees. The proof of Theorem 5.1.2 for <∞-max and t-max is more basic, and uses only Gödel's Completeness Theorem, as t-maximality can be appropriately stated in terms of satisfiability of sentences in first order logic, and <∞-maximality can be appropriately stated in terms of satisfiability of a recursive set of sentences in first order logic.

There is a useful sufficient condition for the hypothesis of Theorem 5.1.2.

THEOREM 5.1.3. Suppose P is a universal property of the $S \subseteq J^n$ or of the $f::J^n \to J^m$, where every subset of a solution to P is a solution to P. Then every 1-maximal solution to P is a maximal solution to P.

THEOREM 5.1.4. Suppose P is a universal property of the $S \subseteq J^n$ of the form $(\forall x_1,\ldots,x_r \in J)(\varphi \to \psi)$, where φ uses at most $\wedge,\vee,S,x_1,\ldots,x_r$ and constants from J, and ψ does not use S. More generally, where S has only negative occurrences in φ in the sense of propositional calculus. Then every subset of a solution to P is a solution to P, and therefore 1-maximality implies maximality.

In light of these considerations, we focus only on 1-maximality.

MASTER TEMPLATE (set,1-max). Let n,J,P,P' be given, where P,P' are universal properties of the $S \subseteq J^n$. There is a 1-maximal solution to P that is also a solution to P'.

MASTER TEMPLATE (fcn,1-max). Let n,m,J,P,P' be given, where P,P' are universal properties of the $f::J^n \to J^m$. There is a 1-maximal solution to P that is also a solution to P'.

MASTER TEMPLATE (reg,1-max). Let n,m,J,P,P' be given, where P,P' are universal properties of the $f::J^n \to J^m$. There is a 1-maximal regressive solution to P that is also a solution to P'.

The partial function and regressive partial function templates above can easily be seen to be subsumed under the set template. This is because universal properties of $f::J^n \to J^m$ are universal properties of $S \subseteq J^{n+m}$ via graphs. However, using partial functions and partial regressive functions allows us to formulate various P' and categories of P' far more simply and naturally than we could do for sets.

The following is easily proved using Gödel's Completeness Theorem.

THEOREM 5.1.5. The set of true instances of MT(set,1-max), MT(fcn,1-max), MT(reg,1-max) is Π^0_1. This is provable in WKL_0. Each instance is provably equivalent to a Π^0_1 sentence over WKL_0.

A complete analysis of MT(set,1-max) (and MT(fcn,1-max), MT(reg,1-max) is impossible in any standard sense because of the following.

THEOREM 5.1.6. The set in Theorem 5.1.5 is not recursive. I.e., there is no algorithm that determines whether an arbitrary instance of MT(set,1-max), MT(fcn,1-max), MT(reg,1-max) holds.

The following general fact is well known.

THEOREM 5.1.7. Let $A \subseteq N$ be given by a Π^0_1 definition, where A is non recursive. If ZFC is consistent then there exists $n \in A$ such that ZFC does not prove "$n \in A$". Suppose the halting problem has an effective reduction to N\A which provably works in ZFC. If ZFC is consistent then there exists $n \in A$ such that "$n \in A$" is provable in ZFC + Con(ZFC) but not in ZFC.

COROLLARY 5.1.8. Each of MT(set,1-max) (and MT(fcn,1-max), MT(reg,1-max) has instances which are provable in ZFC + Con(ZFC) but not in ZFC (assuming ZFC is consistent).

However Theorems 5.1.6 and 5.1.7 does not tell us that there is any kind of "reasonable" instance that, e.g., is provable in SRP but not in ZFC.

THEOREM 5.1.9. There is an instance of MT(set,1-max) where P,P' each have two occurrences of S, and the statement is neither provable nor refutable in ZFC (assuming SRP is consistent). This holds with ZFC replaced by any consistent SRP[k]. Furthermore, we can take the dimension to be very low.

We are not yet sure just how low the dimension comes out under our methods, and we are not sure how well this profile compares with what you can get from the algorithmic unsolvability. We can attempt to go much further.

CONJECTURE 5.1.10. There is an instance of the MT(set,1-max), neither provable nor refutable in ZFC (assuming SRP is consistent), where the dimension, the number of quantifiers, and the number of occurrences of S, are very low. In fact, we can require that the number of occurrences of $<,\leq,=,\neq$ is also reasonably low.

We haven't focused on the direction of Theorem 5.1.9 and Conjecture 5.1.10. Instead we pursue the following plan.

The crucial point is that the unwanted complexity of P gets washed out by using all P's with no constants. Specifically, in light of this algorithmic unsolvability, we have been pursuing the following plan.

i. Give sufficient conditions on n,m,J,P,P' so that MT(set,1-max), MT(fcn,1-max), MT(reg,1-max) are true.
ii. Weaken MT(set,1-max), MT(fcn,1-max), MT(reg,1-max) so that we can give a complete analysis.

In our development, i invariably gives rise to ii. We have been able to exert strong control over n,m,J,P' (P' very natural), but not on P. The crucial discovery is that the complexity of P can be entirely washed out by simply requiring that P have no constants. The result is perfectly mathematically natural Π^0_1 incompleteness.

5.2. Π^0_1 INCOMPLETENESS

Here are the simplest sufficient conditions that we have found for the Master Templates that cannot be proved in SRP (assuming SRP is consistent).

PROPOSITION 5.2.1. Every universal property of the $S \subseteq Q[-r,r]^n$ with no constants, has a 1-maximal solution such that for all $p < 1$, $(1,\ldots,n-1,p) \in S \leftrightarrow (2,\ldots,n,p) \in S$.

PROPOSITION 5.2.2. Every universal property of the $f::Q[-r,r]^n \to Q[-r,r]^m$ with no constants, has a 1-maximal solution with $f(1,\ldots,n) < 1 \to f(1,\ldots,n) = f(0,\ldots,n-1)$.

PROPOSITION 5.2.3. Every universal property of the $f::Q[-n,n]^n \to Q[-n,n]^n$ with no constants, has a 1-maximal regressive solution with $f(0,\ldots,n-1) \equiv f(1,\ldots,n)$.

Our strongest sufficient conditions for the Master Templates that cannot be proved in SRP are presented next.

PROPOSITION 5.2.4. Every universal property of the $S \subseteq J^n$ with no constants, has a 1-maximal solution, whose sections at any equal length $x,y \in (J \cap N)^{\leq n<}$ agree below $\min(x^*y)$.

PROPOSITION 5.2.5. Every universal property of the $f::J^n \to J^m$ with no constants, has a 1-maximal solution, such that for any equal length $x,y \in (J \cap N)^{\leq n<}$, $f(x) < \min(x^*y) \to f(x) = f(y)$.

PROPOSITION 5.2.6. Every universal property of the $f::J^n \to J^m$ with no constants, $-1 \in J$, has a 1-maximal regressive solution, such that for any equal length $x,y \in (J \cap N)^{\leq n<}$, $f(x) \equiv f(y)$.

THEROEM 5.2.7. Theorems 2.2.12 and 2.2.13 apply to Propositions 5.2.1 – 5.2.6.

We do not know if Propositions 2.2.1 - 2.2.6 for J = Q are provable in ZFC. In case, we need the right endpoint of J to establish unprovability.

The form of Propositions 2.2.1 – 2.2.6 suggest the following additional templates.

TEMBPLATE A. Let n,J,P be given, where P is a universal property of the $S \subseteq J^n$. Every universal property of the $S \subseteq J^n$ with no constants, has a 1-maximal solution, that is also a solution to P.

TEMBPLATE B. Let n,m,J,P be given, where P be a universal property of the $f::J^n \to J^m$. Every universal property of the $f::J^n \to J^m$ with no constants, has a 1-maximal solution, that is also a solution to P.

TEMBPLATE C. Let n,m,J,P be given, where P be a universal property of the $f::J^n \to J^m$. Every universal property of the $f::J^n \to J^m$ with no constants, has a 1-maximal regressive solution, that is also a solution to P.

Templates A,B,C seem much more amenable to a complete analysis than MT(set,1-max), MT(fcn,1-max), MT(reg,1-max). Propositions 2.2.1 – 2.2.3 have rather specific forms that suggest some weaker forms of Templates A,B,C. We will focus on J = Q[0,1].

TEMPLATE D. Let $n \geq 1$ and P be a universal property of the $S \subseteq Q[0,1]^n$ with at most one quantifier. Every universal property of the $S \subseteq Q[0,1]^n$ with no constants, has a 1-maximal solution, that is also a solution to P.

TEMPLATE E. Let $n \geq 1$ and P be a Boolean property of the $f::Q[0,1]^n \rightarrow Q[0,1]$. Every universal property of the $f::Q[0,1]^n \rightarrow Q[0,1]$ with no constants, has a 1-maximal solution, that is also a solution to P.

TEMPLATE F. Let $n \geq 1$ and P be a Boolean property of the $f::Q[0,1]^n \rightarrow Q[0,1]$. Every universal property of the $f::Q[0,1]^n \rightarrow Q]0,1]$ with no constants, has a 1-maximal regressive solution, that is also a solution to P.

Templates D,E,F are should be within reach of complete analysis, although we are not ready to claim this. We can modify these further as follows.

TEMPLATE G. Let $n \geq 1$ and P be a universal property of the $S \subseteq Q[0,1]^n$ with one quantifier and 2 occurrences of S. Every universal property of the $S \subseteq Q[0,1]^n$ with no constants, has a 1-maximal solution, that is also a solution to P.

TEMPLATE H. Let $n \geq 1$ and P be an implications between inequalities in $f::Q[0,1]^n \rightarrow Q[0,1]$. Every universal property of the $f::Q[0,1]^n \rightarrow Q[0,1]$ with no constants, has a 1-maximal solution, that is also a solution to P.

TEMPLATE I. Let $n,m \geq 1$ and P be a finite conjunction of equivalences ($\equiv$) in $f:Q[0,1]^n \rightarrow Q[0,1]^m$. Every universal property of the $f::Q[0,1]^n \rightarrow Q[0,1]^m$ with no constants, has a 1-maximal regressive solution, that is also a solution to P.

THEOREM 5.2.9. Every instance of Templates A-I is provably equivalent to a Π^0_1 sentence over WKL_0. Every instance of Templates G,H,I is either provable in SRP or refutable in RCA_0. This claim is false for any SRP[k], assuming SRP is consistent.

6. PROOFS

The provability of the Propositions from Con(SRP) is done almost exactly as in section 9 of [Fr14] (and earlier in section 4 of [Fr11]). The provability of Con(SRP) from the various Propositions builds on what was essentially done in section 5 of [Fr11].

7. APPENDIX - FORMAL SYSTEMS USED

EFA Exponential function arithmetic. Based on 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].

ACA_0 Arithmetic comprehension axiom naught. Our third level theory for Reverse Mathematics. [Si99,09].

ZF(C) Zermelo set theory (with the axiom of choice). ZFC is the official theoretical gold standard for mathematical proofs. [Je14].

SRP[k] ZFC + $(\exists\lambda)(\lambda$ has the k-SRP), for fixed k. Section 9.1, [Fr14].

SRP ZFC + $(\exists\lambda)(\lambda$ has the k-SRP), as a scheme in k. Section 9.1, [Fr14].

SRP^+ ZFC + $(\forall k)(\exists\lambda)(\lambda$ has the k-SRP). Section 9.1, [Fr14].

HUGE[k] ZFC + $(\exists\lambda)(\lambda$ is k-HUGE), for fixed k.

HUGE ZFC + $(\exists\lambda)(\lambda$ is k-huge), as a scheme in k.

$HUGE^+$ 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). For more about huge cardinals, see [Ka94], p. 331.

REFERENCES

[Fr11] H. Friedman, Invariant Maximal Cliques and Incompleteness, Downloadable Manuscripts, #71, October 7, 2011, 132 pages.

[Fr14] H. Friedman, Invariant Maximality and Incompleteness, Downloadable Manuscripts, #77, https://u.osu.edu/friedman.8/foundationaladventures/downloadable-manuscripts/, to appear, 2014.

[WIKIa] http://en.wikipedia.org/wiki/Reverse_mathematics

[WIKIb]
http://en.wikipedia.org/wiki/Elementary_function_arithmetic