Quantifier Elimination and Real Closed Ordered Fields with a Predicate for the Powers of Two

Yimu Yin

December 17, 2005

Abstract

In this thesis we first review the model theory of quantifier elimination and investigate the logical relations among various quantifier elimination tests. In particular we prove the equivalence of two quantifier elimination tests for countable theories. Next we give a procedure for eliminating quantifiers for the theory of real closed ordered fields with a predicate for the powers of two. This result was first obtained by van den Dries [20]. His method is model-theoretic, which provides no apparent bounds on the complexity of a decision procedure. In the last section we give a complete axiomatization of the theory of real closed ordered fields with a predicate for the Fibonacci numbers.

Acknowledgements

I thank my advisor Jeremy Avigad for the guidance he has provided me. I am grateful to James Cummings and Rami Grossberg for many helpful suggestions. I also thank Chris Miller for suggesting the problem considered in the last section of this thesis.

1 Introduction

A "decision procedure" for mathematics is, roughly, a procedure for determining whether or not a mathematical statement is true. Of course, any proof can be viewed as a procedure for determining that a particular theorem is true; but when we talk about decision procedures, we usually mean a procedure for deciding a class of statements. Some decision procedures have been around for a very long time. For example, Euclid's algorithm is such a procedure. It provides a method to determine, among many things, whether two integers p and q are relatively prime. Another example is Newton's method, following which one can approximate a real root of a polynomial equation with real coefficients, though the result is not guaranteed to converge. On the other hand, in the case of a p-adic field this method, where it is known as Hensel's Lemma, is guaranteed to produce a root. Yet another example is Sturm's Theorem which is closely related with the present thesis: it enables one to decide how many roots a given polynomial has; that is it determines the truth-value of sentences of the form "the polynomial p has exactly k roots."

These decision procedures do not deal with just one particular problem, but rather a collection of problems that can be singled out by a formal description, and whose solutions are uniform in the sense that the specifics of each one of them have no influence on how to apply the logical steps of the procedure. This feature was stressed and generalized by Hilbert, who initiated the systematic modern study of decision problems. Since whether a decision problem is well-defined has much to do with how to fix a collection of problems, Hilbert's work in axiomatics and the foundation of mathematics led him to formulate decision problems in the most general form possible. In the second edition of their book *Principles of Mathematical Logic* [11], Hilbert and Ackermann ask:

> Is it possible to determine whether or not a given statement pertaining to a field of knowledge is a consequence of the axioms?

They proceed to demonstrate that for their predicate calculus, which is essentially the first-order predicate calculus, this question can be reduced to the question of whether a given formula of the calculus is or is not universally valid, that is satisfied by every model of the axioms in question. The key here is certainly Gödel's Completeness Theorem. This is why this reduction is not present in the the first edition of their book. However, to solve the decision problem, as required in both editions, one has to find a process by which the derivablility of any given logical expression can in principle be determined.

By the year 1938, in which the second edition first appeared, Turing and Church's landmark papers on decidability had already been published. So unlike the first edition, in which Hilbert and Ackermann are rather vague about what they mean by "a process," they write in the second edition:

> We shall only remark that a general method of decision would consist of a certain recursive procedure for the individual formulas which would finally yield for each formula the value truth or the value falsehood. Church's work proves, however, the nonexistence of such a recursive procedure; at least, the necessary recursions would not fall under the general type of recursion set up by Church, who has given to the somewhat vague intuition concept of recursion a certain precise formalization.

This is essentially the same as our understanding of what a decision method is today.

It should be noted here that Hilbert and Ackermann's decision problem is meant for logical calculi rather than for specific mathematical theories. That is, given any logical calculus, their decision problem asks for a method, which should be uniform for all mathematical systems that employ the logical calculus, that decides which statements are logically valid. This is quite different from asking for a decision method for determining the consequences of a particular mathematical system that is nonlogical but axiomatized, for example Peano Arithmetic. In [19] Tarski describes the latter problem as follows:

> By a *decision method* for a class K of sentences (or other expressions) is meant a method by means of which, given any sentence θ, one can always decide in a finite number of steps whether θ is in K; by a *decision problem* for a class K we mean the problem of finding a decision method for K. A decision method must be like a recipe, which tells one what to do at each step so that no intelligence is required to follow it; and the method can be applied by anyone so long as he is able to read and follow directions.

This summarizes nicely the modern concept of decidability, which we shall discuss in the present thesis.

All of Tarski's decidability results used the method of quantifier elimination. This is indeed a very old method. Anyone who has been exposed to elementary algebra knows the mechanical procedure that eliminates unknowns from a system of linear equations. Logically this is just quantifier elimination for certain kinds of existential formulas in the language of algebra. Of course it was the modern logical machinery that made this method explicit. This dates back to as early as the 1910s in the work of Löwenheim and Skolem. One of the first important results that consciously followed the modern formulation of the method was Langford's axiomatization of several kinds of linear orderings in [14] and [15]. In particular he showed that the axiom system in each of these cases proves that every first-order sentence in the language of orderings is equivalent to a sentence with fewer quantifiers and hence the elementary theory of each of these orderings is decidable. This example illustrates nicely how valuable the method is: when it can be carried out for a theory, it yields a tremendous amount of information about the behaviors of all formulas in the language of the theory, relative to the theory itself and a chosen set of well-understood formulas. Usually it also provides an algorithm for reducing formulas to these well-understood formulas and hence proves that the theory is decidable.

However, as far as algorithm is concerned, there is no a general theory of quantifier elimination. This means whenever we want to apply the method to a new theory T we must analyze T specifically so that each step of the method can be carried out. In general, the method runs as follows. First we fix a suitable set Σ of formulas in the language of T, called *basic formulas*. This, of course, is the part that heavily depends on our analysis of T. Then we proceed to prove that every formula in the language is T-equivalent to a Boolean combination of basic formulas, that is T proves that every formula in the language is equivalent to a Boolean combination of basic formulas. Easily it is enough to show the following:

1. Every atomic formula is T-equivalent to a Boolean combination of basic formulas.

2. If φ is a Boolean combination of basic formulas, then $\exists x\ \varphi$ is T-equivalent to a Boolean combination of basic formulas.

The second item justifies why the method is called "quantifier elimination." Also, very often in practice, Σ is chosen to be the set of quantifier-free formulas.

One well-known way to characterize the relation between Σ and the set of all formulas is through a corollary of Stone's Representation Theorem, since the set of all formulas in a language can be viewed as a Boolean algebra and a consistent complete type, which we shall define below, can be viewed as an ultrafilter in the corresponding Boolean algebra.

Fact 1.1. *Let B be a Boolean algebra and $S(B)$ its Stone space of ultrafilters. Let $\Sigma \subseteq B$. If the map $F \longmapsto F \cap \Sigma$ from $S(B)$ into the powerset of Σ is injective, then Σ generates B as a Boolean algebra.*

Now proving that every formula can be reduced to some formula in Σ is equivalent to proving that the restriction map $F \longmapsto F \cap \Sigma$ is injective.

If an algorithm for quantifier elimination is given, then we shall call it "effective quantifier elimination." This is because nowadays, that is after Abraham Robinson's pioneering model theoretic work in this area, people often speak of quantifier elimination when there is no algorithm other than the one that blindly searches all provable formulas.

Before diving into technical discussions we shall briefly describe the notations and the terminology employed in this thesis. First we shall emphasize that ordered real closed fields and real closed ordered fields are different kinds of things. The first is just real closed fields with a definable ordering, namely the one defined by the formula $\exists z\; z \times z = y - x$. The second is ordered fields that are real closed.

We shall write QE for "quantifier elimination" throughout the rest of the thesis. All basic formulas are quantifier-free. For a theory T we shall use $L(T)$ to denote its language. It is convenient to let $\varphi \in L(T)$ mean that φ is a formula in the language $L(T)$. Very often we expand a language with a set of new constants. To avoid burdening our discussion with cumbersome notational remarks, we do not mention these expansions in context as long as there is no danger of confusion.

If Γ is a consistent set of formulas in a language, then sometimes we abuse Γ to denote its deductive closure in sentences such as "The theory Γ so-and-so." In particular if we add Γ to a theory T, then by "$T \cup \Gamma$" we always mean the deductive closure of $T \cup \Gamma$.

All sequences of variables are finite, and $\bar{x}$ and $\mathrm{lh}(\bar{x})$ are used to denote a sequence of variables and its length respectively. $\bar{x} \in X$ means that every member in the sequence $\bar{x}$ is a member of X.

For a model M we write $|M|$ for its universe and $\|M\|$ for the cardinality of $|M|$. However, sometimes we shall abuse "M" slightly to mean both a model and its universe. In this thesis we do not use the word "substructure" (except this one here, of course). Hence by "submodel" we always mean a subset of some model which is also a structure of the language in question. For two models M, N we write $M \subseteq N$ to denote that M is a submodel of N. If $M \subseteq N$ and $M, N \models T$ for some theory T then N is a T-extension of M. Next, for any $A \subseteq |M| \cap |N|$ we say M can be embedded into N over A if there is a monomorphism $f : M \longrightarrow N$ such that $f \restriction A = \mathrm{id}_A$. If the image of M under f, denoted by $f[M]$, is an elementary submodel of N then we call f an elementary embedding.

The thesis is organized as follows. In the next section we review the model theory of quantifier elimination and investigate the logical relations among various quantifier elimination tests. In particular, we prove a new result that establishes the equivalency of two quantifier elimination tests for countable theories. The third section is joint work [1] with Jeremy Avigad in which we give a procedure for eliminating quantifiers for the theory of real closed ordered fields with a predicate for the powers of two. In the last section we give a complete axiomatization of the theory of real closed ordered fields with a predicate for the Fibonacci numbers.

2 Quantifier Elimination Tests

A very important concept in model theory is that of a type, which is a generalization of the concept of a variety in algebraic geometry. It will play an important role in the discussion below.

Definition 2.1. Let T be a theory. Let M be a model of T. Let $A \subseteq |M|$.

1. Given a finite sequence $\bar{x}$ of variables we say a collection p of formulas in $L(T)$ is a *T-type in $\bar{x}$* if all free variables in any $\varphi \in p$ are in $\bar{x}$ and $T \cup \{\exists\bar{x} \bigwedge q\}$ is consistent for any finite $q \subseteq p$. If p is a T-type in $\bar{x}$ then we write $p(\bar{x})$. The *arity* of p is $\mathrm{lh}(\bar{x})$.

2. A T-type p in $\bar{x}$ is a *complete type* if for any $\varphi(\bar{x}) \in L(T)$ either $\varphi(\bar{x}) \in p$ or $\neg\varphi(\bar{x}) \in p$.

3. For any $\bar{b} \in |M|$ let

$$\mathrm{tp}(\bar{b}/A, M) = \left\{\varphi(\bar{x}; \bar{a}) : \varphi(\bar{x}; \bar{y}) \in L(T), \bar{a} \in A, M \models \varphi(\bar{b}; \bar{a})\right\}.$$

   Clearly $\mathrm{tp}(\bar{b}/A, M)$ is a $\mathrm{Th}(\langle M, a\rangle_{a\in A})$-type. More conveniently we say that p is an *M-type over A*.

4. For any $\bar{b} \in |M|$, sometimes we only want to collect certain kinds of formulas with parameters from A that $\bar{b}$ satisfies. This is denoted by $\mathrm{tp}_\Gamma(\bar{b}/A, M)$, where Γ is a set of conditions. For example, $\mathrm{tp}_{qf}(\bar{b}/A, M)$ is the collection of all quantifier-free formulas in $\mathrm{tp}(\bar{b}/A, M)$.

Very often we shall investigate translations of a type from one model to another model. This arises typically in the following situation. Let M, N be two models, $f : M \longrightarrow N$ a monomorphism, $A \subseteq |M|$, and p an M-type over A. The *translation of p from M to N via f*, denoted by $f(p)$, is the set $\{\varphi(\bar{x}; f(\bar{a})) : \varphi(\bar{x}; \bar{a}) \in p, \bar{a} \in A\}$, which is guaranteed to be an N-type over $f[A]$ if f is elementary.

There are many fundamental results in model theory that we shall need below. For example, the Tarski-Vaught test:

Fact 2.2 (Tarski-Vaught Test)**.** *$N \preceq M$ if and only if*

1. $N \subseteq M$, and

2. *for all formulas $\varphi(x;\bar{a})$ with $\bar{a} \in |N|$, if $M \models \exists x\, \varphi(x;\bar{a})$ then there is an element $b \in |N|$ such that $M \models \varphi(b;\bar{a})$.*

Definition 2.3. Let M be a model.

1. For a cardinal number λ, M is *λ-saturated* if and only if for every $A \subseteq |M|$ of cardinality less than λ any M-type p over A is realized in M.

2. M is *saturated* if and only if M is $\|M\|$-saturated.

Definition 2.4. Let M be a model and $A \subseteq |M|$. Let N be the model $\langle M, a\rangle_{a\in A}$.

1. The theory $\mathrm{Th}(N)$, denoted by $\mathrm{CD}(A, M)$, is called the *complete diagram of A in M*. If $A = |M|$ we simply write $\mathrm{CD}(M)$.

2. The set of all quantifier-free sentences in $\mathrm{Th}(N)$, denoted by $\mathrm{ED}(A, M)$, is called the *elementary diagram of A in M*. Again if $A = |M|$ we simply write $\mathrm{ED}(M)$.

Obviously if $N \preceq M$ then $\mathrm{CD}(N, M) = \mathrm{CD}(N)$ and if $N \subseteq M$ then $\mathrm{ED}(N, M) = \mathrm{ED}(N)$.

Definition 2.5. We say a theory T is *model complete* if and only if, for every pair of models $N, M \models T$, $N \subseteq M$ implies $N \preceq M$.

Abraham Robinson showed that under certain conditions a model complete theory admits QE. This was one of the first results that inaugurated the model-theoretic method in the study of QE. However, since we are not aiming at a thorough historical survey and Robinson's results involve other concepts that are not quite relevant to the present thesis, we shall not discuss them here in details. We only note the following fact.

Theorem 2.6. *Let T be any theory. The following are equivalent:*

1. *T is model complete.*

2. *For any two models $N, M \models T$ with $N \subseteq M$ there is an $N^* \models T$ such that $N \preceq N^*$ and M can be embedded into N^* over N.*

3. *For any $M \models T$ the theory $T \cup \mathrm{ED}(M)$ is complete.*

4. *For any two models $N, M \models T$ with $N \subseteq M$, every existential formula $\varphi(\bar{x})$, and every $\bar{b} \in N$, we have $M \models \varphi(\bar{b})$ if and only if $N \models \varphi(\bar{b})$.*

5. *For every existential formula $\varphi(\bar{x})$ there is a universal formula $\varphi^*(\bar{x})$ such that $T \vdash \varphi(\bar{x}) \leftrightarrow \varphi^*(\bar{x})$.*

6. *For every formula $\varphi(\bar{x})$ there is a universal formula $\varphi^*(\bar{x})$ such that $T \vdash \varphi(\bar{x}) \leftrightarrow \varphi^*(\bar{x})$.*

Proof. $1 \Rightarrow 2$: This is immediate.

$2 \Rightarrow 3$: Since every T-extension of M can be embedded into an elementary extension of M, it follows that $T \cup \mathrm{ED}(M)$ is $\mathrm{CD}(M)$ and hence is complete.

$3 \Rightarrow 4$: This is clear since $T \cup \mathrm{ED}(M)$ is complete and N is a model of $T \cup \mathrm{ED}(M)$.

$4 \Rightarrow 5$: Let $\varphi(\bar{x})$ be an existential formula in $L(T)$. Let $\bar{c}$ be new constants. Let Γ be a set that contains exactly the following formulas:

- $T \cup \{\neg\varphi(\bar{c})\}$, and
- every formula $\psi(\bar{c})$ such that $\psi(\bar{c})$ is universal and $T \vdash \forall\bar{x}\ (\varphi(\bar{x}) \to \psi(\bar{x}))$.

Suppose for contradiction that Γ is consistent. Take any model $M \models \Gamma$. Consider the set $T \cup \mathrm{ED}(M) \cup \{\varphi(\bar{c})\}$ of formulas. If this is not consistent, then there is a quantifier-free formula $\sigma(\bar{a}; \bar{c}) \in \mathrm{ED}(M)$ such that $\bar{a}$ are parameters from $|M|$ other than $\bar{c}$ and $T \cup \{\varphi(\bar{c})\} \vdash \neg\sigma(\bar{a}; \bar{c})$. So $T \cup \{\varphi(\bar{c})\} \vdash \forall\bar{y}\ \neg\sigma(\bar{y}; \bar{c})$, so $T \vdash \varphi(\bar{c}) \to \forall\bar{y}\ \neg\sigma(\bar{y}; \bar{c})$, so $T \vdash \forall\bar{x}\ (\varphi(\bar{x}) \to \forall\bar{y}\ \neg\sigma(\bar{y}; \bar{x}))$, so $\forall\bar{y}\ \neg\sigma(\bar{y}; \bar{c}) \in \Gamma$, so $M \models \forall\bar{y}\ \neg\sigma(\bar{y}; \bar{c})$. But this is clearly a contradiction as $\sigma(\bar{a}; \bar{c}) \in \mathrm{ED}(M)$. So $T \cup \mathrm{ED}(M) \cup \{\varphi(\bar{c})\}$ is consistent. Let $N \models T \cup \mathrm{ED}(M) \cup \{\varphi(\bar{c})\}$. So $M \subseteq N$, so by the assumption we have $M \models \varphi(\bar{c})$ as $\varphi(\bar{x})$ is existential, which is a contradiction.

So Γ is not consistent. This means that there are finitely many universal formulas $\psi_i(\bar{x})$ such that $T \vdash \forall\bar{x}\ (\varphi(\bar{x}) \to \psi_i(\bar{x}))$ for every i and $T \vdash \forall\bar{x}\ (\bigwedge_i \psi_i(\bar{x}) \to \varphi(\bar{x}))$. Since $\bigwedge_i \psi_i(\bar{x})$ is clearly equivalent to a universal formula $\rho(\bar{x})$, we conclude $T \vdash \forall\bar{x}\ (\varphi(\bar{x}) \leftrightarrow \rho(\bar{x}))$, as desired.

$5 \Rightarrow 6$: By an induction on the complexity of formulas clearly it is enough to show that any formula of the form $\exists\bar{x}\ \forall\bar{y}\ \psi(\bar{x}; \bar{y}; \bar{z})$ with $\psi(\bar{x}; \bar{y}; \bar{z})$ quantifier-free is equivalent to a universal formula. By the assumption this can be reduced to showing that $\exists\bar{x}\ \forall\bar{y}\ \psi(\bar{x}; \bar{y}; \bar{z})$ is equivalent to an existential formula. But $\exists\bar{x}\ \forall\bar{y}\ \psi(\bar{x}; \bar{y}; \bar{z})$ is equivalent to an existential formula if and only if $\neg\exists\bar{x}\ \forall\bar{y}\ \psi(\bar{x};\bar{y};\bar{z})$ is equivalent to a universal formula if and only if $\forall\bar{x}\ \exists\bar{y}\ \neg\psi(\bar{x};\bar{y};\bar{z})$ is equivalent to a universal formula, which is implied by 5.

6 $\Rightarrow$ 1: Let $N, M \models T$ with $N \subseteq M$. For any formula $\varphi(x;\bar{a})$ with $\bar{a} \in |N|$ and $M \models \exists x\ \varphi(x;\bar{a})$, let $\rho(\bar{a})$ be a universal formula such that $T \vdash \exists x\ \varphi(x;\bar{a}) \leftrightarrow \rho(\bar{a})$, then $M \models \rho(\bar{a})$, so $N \models \rho(\bar{a})$, so $N \models \exists x\ \varphi(x;\bar{a})$. By the Tarski-Vaught Test we conclude $N \preceq M$. □

Note that if T proves that every formula is equivalent to a universal formula, then it proves that every formula is equivalent to an existential formula. This is simply because T proves that the negation of every formula is equivalent to a universal formula. So Theorem 2.6 says that if T is model complete then both the set of all universal formulas and the set of all existential formulas can serve as a set of basic formulas as we reduce $L(T)$ to "simple" formulas. However this does not imply that T admits QE (recall that by our convention we take the quantifier-free formulas as our basic formula for QE). In fact there are theories which are model complete but do not admit QE. A very relevant example is the theory of real closed fields which is a complete theory and is model complete. But the formula $\exists x\ x \times x = y$ is not equivalent to any quantifier-free formula in this theory. See [5] for details. However, some of the conditions listed in Theorem 2.6 can be strengthened to imply QE.

Definition 2.7. Let T be any theory.

1. T is *submodel complete* if and only if for any model $M \models T$ and any $N \subseteq M$ the theory $T \cup \mathrm{ED}(N)$ is complete.

2. T is *submodel amalgamatable* if and only if for any $M_1, M_2 \models T$ and any $N \subseteq M_1, M_2$ there is an $M^* \models T$ such that $M_1 \preceq M^*$ and M_2 can be embedded into M^* over N via a monomorphism f, that is the following diagram

$$\begin{tikzcd}
M_1 \arrow[r, "\preceq"] & M^* \\
N \arrow[u, "\subseteq"] \arrow[r, "\subseteq"'] & M_2 \arrow[u, "f"']
\end{tikzcd}$$

commutes.

3. T has the *Shoenfield property* (S-property for short) if and only if for any two models $M_1, M_2 \models T$ such that M_2 is $\|M_1\|^+$-saturated and any isomorphism $f : N_1 \longrightarrow N_2$ with $N_1 \subseteq M_1$ and $N_2 \subseteq M_2$, there is a monomorphism $f^* : M_1 \longrightarrow M_2$ extending f.

4. T has the *strong Shoenfield property* (SS-property for short) if and only if

   (a) For every two models $M_1, M_2 \models T$ and every two models $N_1 \subseteq M_1$ and $N_2 \subseteq M_2$, if $f : N_1 \longrightarrow N_2$ is an isomorphism, then there is an isomorphism $f^* : N_1^* \longrightarrow N_2^*$ which is an extension of f, where $N_1^* \subseteq M_1$, $N_2^* \subseteq M_2$, and $N_1^*, N_2^* \models T$;

   (b) For every two models $N, M \models T$ with $N \subseteq M$, every existential formula $\varphi(\bar{x})$, and every $\bar{b} \in N$, we have $M \models \varphi(\bar{b})$ if and only if $N \models \varphi(\bar{b})$.

5. T has the *van den Dries property* (D-property for short) if and only if

   (a) For any model N, if there exists a model $M \models T$ such that $N \subseteq M$, then there is a T-closure N^* of N, that is $N \subseteq N^* \models T$ and N^* can be embedded over N into any T-extension of N;

   (b) If $N, M \models T$ and $N \subsetneq M$, then there is an $a \in |M| \setminus |N|$ such that $N(a)$ can be embedded into an elementary extension of N over N, where $N(a)$ is the smallest submodel of M that contains $|N| \cup \{a\}$ (sometimes this is also denoted by $N + a$ below).

Notice the similarities between 2.6 2 and 2.7 2, 2.6 3 and 2.7 1. Also, the two conditions 2.6 4 and 2.7 4 (b) are the same. In fact the proof of "4 $\Rightarrow$ 5" in Theorem 2.6, which establishes a crucial connection between model-theoretic properties and syntactical properties, can be slightly modified to show how 2.7 4 (a) achieves QE on top of model-completeness.

Proposition 2.8. *Let T be a theory in a language with at least one constant symbol. Suppose that T satisfies 2.7 4 (a). For any formula φ, if T proves that φ is equivalent to both a universal formula and an existential formula, then T proves that T is equivalent to a quantifier-free formula.*

Proof. Let $\varphi(\bar{x}) \in L(T)$ be such a formula. Without loss of generality we may assume $\varphi(\bar{x})$ is a universal formula. Let $\varphi^*(\bar{x})$ be an existential formula such that $T \vdash \varphi(\bar{x}) \leftrightarrow \varphi^*(\bar{x})$. Let $\bar{c}$ be new constants. Let Γ be a set that contains exactly the following formulas:

- $T \cup \{\varphi(\bar{c})\}$, and
- every quantifier-free $\neg\psi(\bar{c})$ such that $T \vdash \forall\bar{x}\ (\psi(\bar{x}) \to \varphi(\bar{x}))$.

Suppose for contradiction that Γ is consistent. Take any model $M \models \Gamma$. Let $N \subseteq M$ be the minimal submodel generated by $\bar{c}$. Note that every member in N can be written as a term that only involves $\bar{c}$, the constants of $L(T)$, and the functions of $L(T)$. Now, if $T \cup \mathrm{ED}(N)$ does not prove $\varphi(\bar{c})$, then fix a model $M^* \models T \cup \mathrm{ED}(N) \cup \{\neg\varphi(\bar{c})\}$. By the assumption we can find an $N_1 \models T \cup \mathrm{ED}(N)$ in M and an $N_2 \models T \cup \mathrm{ED}(N)$ in M^* such that they are isomorphic over N. So $N_2 \models \varphi(\bar{c})$, so $N_2 \models \varphi^*(\bar{c})$, so $M^* \models \varphi^*(\bar{c})$, so $M^* \models \varphi(\bar{c})$, contradiction. So $T \cup \mathrm{ED}(N) \vdash \varphi(\bar{c})$. So there is a quantifier-free formula $\psi(\bar{c}) \in \mathrm{ED}(N)$ such that $T \cup \{\psi(\bar{c})\} \vdash \varphi(\bar{c})$, so $T \vdash \psi(\bar{c}) \to \varphi(\bar{c})$. But $\bar{c}$ are new constants, so $T \vdash \forall\bar{x}\ (\psi(\bar{x}) \to \varphi(\bar{x}))$. So $\neg\psi(\bar{c}) \in \Gamma$, contradiction again.

So Γ is not consistent. This means that there are finitely many quantifier-free formulas $\psi_i(\bar{x})$ such that $T \vdash \forall\bar{x}\ (\psi_i(\bar{x}) \to \varphi(\bar{x}))$ for every i and $T \vdash \forall\bar{x}\ (\varphi(\bar{x}) \to \bigvee_i \psi_i(\bar{x}))$. So $T \vdash \forall\bar{x}\ (\varphi(\bar{x}) \leftrightarrow \bigvee_i \psi_i(\bar{x}))$, as desired. $\square$

The reason that we have assumed that the language of T has at least one constant symbol is to avoid certain pathology. That is, if φ is a sentence and $L(T)$ has no constant symbol, then $\bar{c}$ is the empty sequence and cannot generate any submodel as we do not allow an empty model. The reader should observe that in this case the above proof will not go through if we simply use an arbitrary submodel. An alternative way to go around this is to deal with $\varphi \wedge x = x$ instead of φ if φ is a sentence. Of course this requires that $L(T)$ has equality. Anyway, in the sequel we shall assume that one of the solutions is applied whenever we are in a similar situation and hence avoid mentioning these cumbersome assumptions again.

The SS-property first appeared in Shoenfield's textbook [17]. He subsequently modified it into the S-property and proved its equivalency to QE in [18]. The D-property was given by Lou van den Dries in [20], [21]. All of these properties in the above definition can serve as a QE-test. In general some of them are more effective than others, especially the D-property, although this also depends on the theory that is being tested. Note that the D-property is a direct strengthening of the SS-property, though for all practical purposes, in the light of some of the theorems below, its main advantage over the SS-property is its conceptual concreteness rather than its logical strength.

Theorem 2.9. *Let T be any theory. For the following statements,*

1. *T is submodel complete,*
2. *T is submodel amalgamatable,*
3. *T has the S-property,*
4. *T has the SS-property,*
5. *T has the D-property,*
6. *T admits QE,*

these logical implications hold:

$$\begin{tikzcd}
 & 6 \arrow[dr, Rightarrow] & & & \\
1 \arrow[ur, Rightarrow] & & 3 \arrow[dl, Rightarrow] & 4 \arrow[l, Rightarrow] & 5 \arrow[l, Rightarrow] \\
 & 2 \arrow[ul, Rightarrow] & & &
\end{tikzcd}$$

Proof. 2 ⇒ 1: Let $N \subseteq M_0^1, M_0^2 \models T$. Using the assumption iteratively we construct the following diagram:

$$\begin{tikzcd}
 & M_0^1 \arrow[r, "\preceq"] \arrow[ddr, "g_0"] & M_1^1 \arrow[r, "\preceq"] \arrow[ddr, "g_1"] & M_2^1 \arrow[r, "\preceq"] \arrow[ddr, "g_2"] & \cdots \\
N \arrow[ur, "\subseteq"] \arrow[dr, "\subseteq"'] & & & & \\
 & M_0^2 \arrow[r, "\preceq"'] \arrow[uur, "f_0"] & M_1^2 \arrow[r, "\preceq"'] \arrow[uur, "f_1"] & M_2^2 \arrow[r, "\preceq"'] \arrow[uur, "f_2"] & \cdots
\end{tikzcd}$$

where f_i's and g_i's are monomorphisms. Let $M^1 = \bigcup_{i<\omega} M_i^1$ and $M^2 = \bigcup_{i<\omega} M_i^2$. Let $f = \bigcup_{i<\omega} f_i$ and $g = \bigcup_{i<\omega} g_i$. That $f = g^{-1}$ is an isomorphism between M^1 and M^2 is a basic fact in model theory. So

$$\langle M^1, a \rangle_{a \in |N|} \equiv \langle M^2, a \rangle_{a \in |N|}.$$

So $T \cup \mathrm{ED}(N)$ is complete.

1 ⇒ 6: Let $\varphi(\bar{x})$ be a formula in $L(T)$. Let $\bar{c}$ be new constants. Let Γ be a set that contains exactly the following formulas:

- $T \cup \{\varphi(\bar{c})\}$, and
- every quantifier-free $\neg\psi(\bar{c})$ such that $T \vdash \forall\bar{x}\ (\psi(\bar{x}) \rightarrow \varphi(\bar{x}))$.

Suppose for contradiction that Γ is consistent. Take any model $M \models \Gamma$. Let $N \subseteq M$ be the minimal submodel generated by $\bar{c}$. Note that every member in N can be written as a term that only involves $\bar{c}$, the constants of $L(T)$, and the functions of $L(T)$. Since T is submodel complete, we have $T \cup \mathrm{ED}(N) \vdash \varphi(\bar{c})$. So there is a quantifier-free formula $\psi(\bar{c}) \in \mathrm{ED}(N)$ such that $T \cup \{\psi(\bar{c})\} \vdash \varphi(\bar{c})$. So $T \vdash \psi(\bar{c}) \rightarrow \varphi(\bar{c})$. But $\bar{c}$ are new constants, so $T \vdash \forall\bar{x}\ (\psi(\bar{x}) \rightarrow \varphi(\bar{x}))$. So $\neg\psi(\bar{c}) \in \Gamma$. This is a contradiction.

So Γ is not consistent. This means that there are finitely many quantifier-free formulas $\psi_i(\bar{x})$ such that $T \vdash \forall\bar{x}\ (\psi_i(\bar{x}) \rightarrow \varphi(\bar{x}))$ for every i and $T \vdash \forall\bar{x}\ (\varphi(\bar{x}) \rightarrow \bigvee_i \psi_i(\bar{x}))$. So $T \vdash \forall\bar{x}\ (\varphi(\bar{x}) \leftrightarrow \bigvee_i \psi_i(\bar{x}))$, as desired.

$6 \Rightarrow 3$: Without loss of generality let $M_1, M_2 \models T$, $N \subseteq M_1, M_2$, and let M_2 be $\|M_1\|^+$-saturated. Consider the type $p = \mathrm{tp}(a/\left|N\right|, M_1)$ for some $a \in |M_1| \setminus |N|$. Since T admits QE, any formula $\exists x\ \varphi(x;\bar{b})$ with $\varphi(x;\bar{b}) \in p$ is equivalent to a quantifier-free formula $\varphi^*(\bar{b})$. So $N \models \varphi^*(\bar{b})$. So $M_2 \models \exists x\ \varphi(x;\bar{b})$. So p is also an M_2-type. So p is realized in M_2, say, by d. Clearly setting $a \longmapsto d$ induces an isomorphism between the two submodels $N + a$ and $N + d$. By iterating this procedure we see that M_1 can be embedded into M_2 over N.

$3 \Rightarrow 2$: We use the fact that for any infinite model M and any cardinality κ there is an elementary extension N of M such that N is κ-saturated. The logical implication in question follows readily from this fact.

$4 \Rightarrow 3$: Again let $M_1, M_2 \models T$, $N \subseteq M_1, M_2$, and let M_2 be $\|M_1\|^+$-saturated. By the first condition of the SS-property fix two T-extensions N_1, N_2 of N in M_1, M_2 respectively that are isomorphic over N. Let the isomorphism be f. Pick an $a \in |M_1| \setminus |N_1|$ and consider any quantifier-free formula $\varphi(x;\bar{b})$ with $\bar{b} \in N_1$ such that $M_1 \models \varphi(a;\bar{b})$. Since $M_1 \models \exists x\ \varphi(x;\bar{b})$, by the second condition of the SS-property we have $N_1 \models \exists x\ \varphi(x;\bar{b})$, so $N_2 \models \exists x\ \varphi(x; f(\bar{b}))$, so $M_2 \models \exists x\ \varphi(x; f(\bar{b}))$. Hence the quantifier-free type $f(p)$ is realized in M_2, say, by d, where $p = \mathrm{tp}_{qf}(a/\left|N_1\right|, M_1)$. If we set $a \longmapsto d$ then we get an induced isomorphism between $N_1 + a$ and $N_2 + d$. By iterating this procedure to exhaust all elements in M_1 we see that M_1 can be embedded into M_2 over N.

$5 \Rightarrow 4$: Trivially the closure property implies the first condition of the SS-property. For the second condition of the SS-property, let $N, M \models T$ with

$N \subseteq M$. Consider an existential formula $\exists \bar{x}\ \varphi(\bar{x}; \bar{b})$ that is satisfied in M, where $\bar{b} \in N$ and $\varphi(\bar{x}; \bar{b})$ is quantifier-free. So let $\bar{c}$ be such that $M \models \varphi(\bar{c}; \bar{b})$. We construct the following diagram:

$$\begin{tikzcd}
N_0 \arrow[r, "\subseteq"] \arrow[dr, "\preceq"'] & N_0 + a_0 \arrow[r, "\subseteq"] \arrow[d] & N_1 \arrow[r, "\subseteq"] \arrow[dl, "f_0"] \arrow[dr, "\preceq"'] & N_1 + a_1 \arrow[r, "\subseteq"] \arrow[d] & N_2 \arrow[rr, dotted, "\subseteq"] \arrow[dl, "f_1"] \arrow[dr] & & M \\
& N_0^* & & N_1^* & & \cdots &
\end{tikzcd}$$

where $N_0 = N$, each N_{i+1} is the T-closure of $N_i + a_i$ promised by the closure property, each a_i and N_i^* are as described in the second condition of the D-property, all arrows are monomorphisms, and at the limit stage we simply take the union of all previous N_i's.

Now, let i be the least index such that $\bar{c} \in N_i$. Note that i cannot be a limit ordinal. So $N_i \models \exists \bar{x}\ \varphi(\bar{x}; \bar{b})$, so $N_{i-1}^* \models \exists \bar{x}\ \varphi(\bar{x}; \bar{b})$, so $N_{i-1} \models \exists \bar{x}\ \varphi(\bar{x}; \bar{b})$, etc. If γ is a limit ordinal and $N_\gamma \models \exists \bar{x}\ \varphi(\bar{x}; \bar{b})$, then there is a $\bar{d} \in |N_\gamma|$ such that $N_\gamma \models \varphi(\bar{d}; \bar{b})$, so by the construction there is a $j < \gamma$ such that $\bar{d} \in |N_j|$, so $N_j \models \varphi(\bar{d}; \bar{b})$, so $N_j \models \exists \bar{x}\ \varphi(\bar{x}; \bar{b})$. As we trace back in the diagram we see that $N = N_0 \models \exists \bar{x}\ \varphi(\bar{x}; \bar{b})$. □

The logical implications in the above theorem are all well-known. In fact there are still more model-theoretic tests that are equivalent to QE. They are all more or less variations of the three equivalent tests in the above theorem. See Hodges [12] for more details about this. On the other hand, it is tempting to ask if in the above theorem all of the statements are indeed equivalent.

Jeremy Avigad has an example which shows that QE is strictly weaker than the SS-property. Consider the set 2^ω of all binary sequences of length ω. For each $n \in \omega$ let Z_n be a unary predicate such that, for any $\eta \in 2^\omega$, $Z_n(\eta)$ if and only if $(\eta)_n = 0$. Let $T = \mathrm{Th}(\langle 2^\omega, Z_n \rangle_{n \in \omega})$. Since except equality all predicates in the language are unary, every existential formula $\exists x\ \varphi(x; \bar{y})$ is equivalent to a formula of the form $\bigvee_i (\theta_i(\bar{y}) \wedge \exists x\ \phi_i(x; \bar{y}))$, where $\phi_i(x; \bar{y})$ is a conjunction of literals each of which contains x. If the unary predicates in the formula $\exists x\ \phi_i(x; \bar{y})$ describe a "consistent" finite sequence, then it can be translated into an equivalent quantifier-free formula that only involves $\bar{y}$. So T proves that every existential formula is equivalent to a quantifier-free formula, which means that T admits QE. So actually T can be axiomatized with only existential and universal formulas. Now, it is easy to see that any dense subset of 2^ω is a model of T. Let $S_0 \subseteq 2^\omega$ be the set of those sequences that have only finitely many 0's. Let $S_1 \subseteq 2^\omega$ be the set of those sequences that have only finitely many 1's and the constant sequence $\bar{1}$. So both S_0 and S_1 are models of T. Notice that $\{\bar{1}\}$ is a submodel of both models as there is no function symbol in the language. Clearly there cannot be isomorphic T-extensions of $\{\bar{1}\}$ in S_0 and S_1.

What about the SS-property and the D-property then? First of all it is trivial that if a theory T admits QE then the second condition of the D-property holds, because, by Theorem 2.6, if $N, M \models T$ and $N \subseteq M$ then M itself is an elementary extension of N. The closure property, however, is much harder to achieve. We prove below that the arrow between (4) and (5) in Theorem 2.9 can be reversed for countable theories. That is, the SS-property and the D-property are equivalent for countable theories. As the question of QE rarely arises for uncountable theories, this result means that for all practical purposes the two properties are really the same. The argument for this result involves some basic facts in infinitary combinatorics. Also we need more concepts in model theory and Henkin's Omitting Type Theorem.

Definition 2.10. Let $\bar{x}$ be a sequence of variables. Let T be a theory.

1. Let p and q be two T-types in $\bar{x}$. We write $p \vdash q$ if the following holds: For every model $M \models T$ and every $\bar{a} \in {}^{\mathrm{lh}(\bar{x})}|M|$, if $\bar{a}$ realizes p then $\bar{a}$ realizes q.

2. For a T-type p, if there exists a formula $\varphi(\bar{x})$ such that $\varphi(\bar{x}) \vdash p$, then we say that p is *isolated by* $\varphi(\bar{x})$ *via* T. In general if there exists a T-type q such that $q \vdash p$ and $|q| < \kappa$, then we say that p is κ*-isolated by* q *via* T. If in context it is clear which theory is being discussed then we omit T.

Note that any type p is trivially $|p|^+$-isolated. If p is a complete T-type, then p is κ-isolated via T if and only if there exists a $q \subseteq p$ such that $q \vdash p$ and $|q| < \kappa$. In particular p is isolated via T if and only if there exists a $\varphi \in p$ such that $\varphi \vdash p$.

Definition 2.11. Let M be a model that satisfies a theory T and A a subset of its universe. We say M is *almost* T*-primary over* A if there exists an ordinal α and a sequence $\langle (N_i, b_i) : i < \alpha \rangle$ such that

1. N_0 is the minimal submodel of M that contains A,

2. $b_i \notin |N_i|$ and N_{i+1} is the minimal submodel of M that contains $\{b_i\} \cup |N_i|$ for each $i < \alpha$ (if $\alpha = \beta + 1$ then b_β is not defined),

3. $N_\beta = \bigcup_{i<\beta} N_i$ if β is a limit ordinal and $\bigcup_{i<\alpha} N_i = M$,

4. the type $\mathrm{tp}(b_j/ |N_j|, M)$ is isolated via T_j for every $j < \alpha$, where $T_j = T \cup \mathrm{CD}(N_j, M)$.

The sequence $\langle (N_i, b_i) : i < \alpha \rangle$ is called an *almost isolating sequence* for M over A. The ordinal α is the *length* of the sequence.

For convenience, if $T = \mathrm{Th}(M)$ then we omit T. Also, sometimes we allow an almost isolating sequence to have repeated consecutive b_i's. Of course in this case we no longer require $b_i \notin |N_i|$ for the repeated occurrences. Note that this definition is a variation of the notion of a primary model, which plays an important role in the proof of Morley's Theorem.

Definition 2.12. Let M be a model that satisfies a theory T and A a subset of its universe. We say M is *T-primary over A* if there exists an ordinal α and an enumeration $\langle b_i : i < \alpha \rangle$ of $|M| \setminus A$ such that the type

$$\mathrm{tp}(b_j/A \cup \{b_i : i < j\}, M)$$

is isolated via T_j for every $j < \alpha$, where $T_j = T \cup \mathrm{CD}(A \cup \{b_i : i < j\}, M)$. The sequence $\langle b_i : i < \alpha \rangle$ is called an *isolating sequence* for M over A. The ordinal α is the *length* of the sequence.

It is not hard to see that if T is submodel complete and $N \subseteq M \models T$ then M is *almost T-primary over N* if and only if M is *T-primary over N*. We prefer the concept of an almost primary model below because it is more explicit about what property is being exploited, namely submodel completeness. For much more materials on primary models see Grossberg's textbook [10].

Next we state Henkin's Omitting Type Theorem. In his textbook [16] Gerald Sacks quotes a "not well-known" model theorist: "Any fool can realize a type, but it takes a model theorist to omit one." To be on the safe side we also include a proof of Henkin's Omitting Type Theorem below, which is borrowed from [10]. Here we assume that the reader is familiar with the concepts of a poset, a dense subset, a generic filter, etc. and the basic facts about them.

Theorem 2.13 (Henkin's Omitting Type Theorem). *Let T be a countable theory. Let Γ be a countable collection of T-types. If p is not isolated for every type $p \in \Gamma$, then there exists a countable model $M \models T$ that omits all the types in Γ.*

Proof. Let $C = \{c_i : i < \omega\}$ be a set of new constants that are not in $L(T)$. Let $L^* = L(T) \cup C$. Define

$$P = \{p : p \text{ is a finite set of sentences in } L^* \text{ and } T \cup p \text{ is consistent}\}.$$

P is a poset ordered by inclusion.

For each sentence $\varphi \in T$ it is easy to see that the set $E_\varphi = \{p \in P : \varphi \in p\}$ is dense in P. For each formula $\varphi(x)$ in $L(T)$ such that $T \vdash \exists x\ \varphi(x)$ let

$$D_\varphi = \{p \cup \{\exists x\ \varphi(x) \to \varphi(c_i)\} \in P : c_i \in C \text{ and } c_i \text{ does not appear in } p\}.$$

D_φ is also dense in P. To see this, suppose for contradiction there is a $p \in P$ such that for no $q \in D_\varphi$ do we have $p \subseteq q$, that is for every $c_i \in C$ that does not appear in p we have that $\{\exists x\ \varphi(x) \to \varphi(c_i)\} \cup T \cup p$ is inconsistent. So $T \cup p \vdash \neg(\exists x\ \varphi(x) \to \varphi(c_i))$, so $T \cup p \vdash \exists x\ \varphi(x) \wedge \neg\varphi(c_i)$. Since c_i does not appear in p, we deduce $T \cup p \vdash \exists x\ \varphi(x) \wedge \forall x\ \neg\varphi(x)$, that is $T \cup p \vdash \exists x\ \varphi(x) \wedge \neg\exists x\ \varphi(x)$, contradicting the assumption that $T \cup p$ is consistent.

Next, for each function symbol $f \in L(T)$ and each tuple of constants $\bar{c} \in L^*$ let

$$D_{f,\bar{c}} = \{p \cup \{f(\bar{c}) = d\} \in P : d \text{ does not appear in } p\}.$$

By an argument similar to the previous one we see that each $D_{f,\bar{c}}$ is dense in P.

Now since there are only countably many dense subsets of P of the three sorts defined in the last paragraph, we may find a generic filter G of P that intersects them all. Clearly $T \subseteq \bigcup G$. Let $\bigcup G \subseteq T^*$ be a complete theory in L^*. We define a binary relation "$\approx$" on C as follows:

$$c_i \approx c_j \text{ iff } T^* \vdash c_i = c_j.$$

It should be clear that "$\approx$" is an equivalence relation on C. In fact the reader should observe at this point that what we have done so far is just a

Henkin-style construction for the theory T. So if we let $[c_i]_\approx$ denote the $\approx$-equivalence class of c_i and interpret the relations and functions in the usual way, we actually get a countable model of T^*.

Of course we still need to omit all the types in Γ. Let $\langle p_n : n < \omega \rangle$ enumerate all the types in Γ. We use $k(n)$ to denote the arity of p_n. For each $n < \omega$ and each $\bar{c} \in C$ with $\mathrm{lh}(\bar{c}) = k(n)$, define

$$O_{n,\bar{c}} = \{q \in P : \text{ there is a } \varphi(\bar{x}) \in p_n \text{ such that } \neg\varphi(\bar{c}) \in q\}.$$

We claim that $O_{n,\bar{c}}$ is dense in P. To prove it, suppose for contradiction that there is a $q \in P$ such that for every $\varphi(\bar{x}) \in p_n$ the set $\{\neg\varphi(\bar{c})\} \cup T \cup q$ is inconsistent. So $T \cup q \vdash \varphi(\bar{c})$. So $T \vdash \bigwedge q \to \varphi(\bar{c})$, where $\bigwedge q$ is the conjunction of all the formulas in q. Now let $\bar{d} \in C$ be the constants in q that are different from $\bar{c}$. We have $T \vdash \forall\bar{x}\ \forall\bar{y}\ (\bigwedge q \to \varphi(\bar{x}))$, where $\mathrm{lh}(\bar{x}) = \mathrm{lh}(\bar{c})$ and $\mathrm{lh}(\bar{y}) = \mathrm{lh}(\bar{d})$. This means that the formula $\forall\bar{y}\ \bigwedge q$ isolates the type p_n, contradicting the assumption.

Let G be a generic filter that intersects all the dense subsets that have been defined so far. As above we can construct a countable model M of the theory T^* which extends T. It is easy to see that all the types in Γ are omitted in M. Hence the reduct of M to $L(T)$ is as desired. □

Notice that the argument in the above proof runs like forcing. In fact this theorem can be slightly generalized as follows. Let $|T| = \kappa$ be any regular cardinal. Let Γ be a collection of at most κ many T-types such that no type in Γ is κ-isolated. Then by a transfinite version of the above argument one easily sees that there exists a model $M \models T$ with $\|M\| = \kappa$ that omits all the types in Γ.

We proceed to develop a couple of technical lemmas. We have the following basic fact about an almost primary model satisfying a submodel complete theory:

Lemma 2.14. *Suppose T is submodel complete. Let $N \subseteq M \models T$. Then: if M is almost T-primary over N, then for every model $M^* \models T \cup \mathrm{ED}(N)$ there is an elementary embedding from M into M^* over N.*

Proof. Since T is submodel complete, the theory $T \cup \mathrm{ED}(N)$ is complete. This means that for any formula $\varphi(\bar{x})$ and any $\bar{a} \in N$ we have

$$M \models \varphi(\bar{a}) \text{ iff } M^* \models \varphi(\bar{a}).$$

Let $\langle (N_i, b_i) : i < \alpha \rangle$ be an almost isolating sequence for M over N. So by definition $N_0 = N$. In order to prove the lemma it is enough to construct a continuous sequence of monomorphisms $g_i : N_i \longrightarrow M^*$ for $i < \alpha$ such that

1. $g_0 = \mathrm{id}_N$,
2. $N_i \models \varphi(\bar{a})$ iff $M^* \models \varphi(g_i(\bar{a}))$ for each formula $\varphi(\bar{x})$ and each $\bar{a} \in N_i$,
3. if $i < j < \alpha$ then $g_i \subseteq g_j$, and
4. if β is a limit then $g_\beta = \bigcup_{i<\beta} g_i$.

The embedding $g = \bigcup_{i<\alpha} g_i$ is as desired. That g is elementary is because submodel completeness implies model completeness (see Theorem 2.6 and Theorem 2.9).

Now we proceed to construct the sequence. Due to the clause 4 all we have to do is to make the successor case work. So suppose we have successfully constructed the sequence up to the ordinal $i < \alpha$. Since the complete type $p_i = \mathrm{tp}(b_i / |N_i|, M)$ is isolated via T_i where $T_i = T \cup \mathrm{CD}(N_i, M)$, there exists a formula $\varphi(x; \bar{a}) \in p_i$ isolating it. By the clause 2 we have

$$\varphi(x; \bar{a}) \vdash p_i \Rightarrow \varphi(x; g_i(\bar{a})) \vdash g_i(p_i). \tag{2.1}$$

Since $M \models \varphi(b_i; \bar{a})$, we have $M \models \exists x\ \varphi(x; \bar{a})$, so $M^* \models \exists x\ \varphi(x; g_i(\bar{a}))$. Let $c_i \in |M^*|$ such that $M^* \models \varphi(c_i; g_i(\bar{a}))$. So by 2.1 c_i realizes the type $g_i(p_i)$. Now define a function g_{i+1} by setting $\tau(b_i) \longmapsto \tau(c_i)$ for each term $\tau(x)$ of $L(T_i)$. It is easy to see that this is a well-defined monomorphism from N_{i+1} into M^* which extends g_i and takes b_i to c_i. □

In order to build almost primary models we need the next crucial lemma.

Lemma 2.15. *Let T be a theory in a countable language. Suppose T has the SS-property. Then for*

1. *every model $M \models T$,*
2. *every countable submodel $N \subseteq M$,*
3. *every formula $\varphi(x; \bar{y})$ and every $\bar{a} \in |N|$ such that $\exists x\ \varphi(x; \bar{a}) \in T \cup \mathrm{ED}(N)$ but $M \models \neg\varphi(b; \bar{a})$ for every $b \in |N|$,*

there is a $c \in |M| \setminus |N|$ such that the type $\mathrm{tp}(c/|N|, M)$ *is isolated and $M \models \varphi(c; \bar{a})$.*

Proof. Fix an M, an N, an $\bar{a}$, and a $\varphi(x;\bar{y})$ as above. Since T has the SS-property, by Theorem 2.9 the theory $T \cup \mathrm{ED}(N)$ is complete. This also means that T is model complete. Fix a countable elementary submodel $M^* \preceq M$ that contains N. We work in M^*. Since $M^* \models T \cup \mathrm{ED}(N)$, by the last condition above we see that M^* is larger than N.

Suppose for contradiction we cannot find a c in M^* as required. Define a collection Γ of $T \cup \mathrm{ED}(N)$-types:

$$\Gamma = \{\mathrm{tp}(c/\left|N\right|, M^*) : c \in \left|M^*\right| \setminus \left|N\right| \text{ and } M^* \models \varphi(c;\bar{a})\}.$$

Since Γ is countable, by Henkin's Omitting Type Theorem there is a model $N^* \models T \cup \mathrm{ED}(N)$ that omits every type in Γ. But T has the SS-property, so we can find two models $M^{**} \subseteq M^*$, $N^{**} \subseteq N^*$ of T such that there is an isomorphism $h : M^{**} \cong N^{**}$ whose restriction to N is id_N. Since $\exists x\ \varphi(x;\bar{a}) \in T \cup \mathrm{ED}(N)$, there must be some $c \in \left|M^{**}\right| \setminus \left|N\right|$ such that $M^{**} \models \varphi(c;\bar{a})$. Since T is model complete, we deduce $M^* \models \varphi(c;\bar{a})$. This means that $h(c)$ realizes the $T \cup \mathrm{ED}(N)$-type $\mathrm{tp}(c, M^*)$ in N^*, contradicting the choice of N^*. □

Note that in the above theorem, if N is not a model of T, then there must exist a formula $\exists x\ \varphi(x;\bar{a}) \in T \cup \mathrm{ED}(N)$ with $\bar{a} \in |N|$ such that $M \models \neg\varphi(b;\bar{a})$ for every $b \in |N|$, because otherwise N would be a model of T by the Tarski-Vaught Test as $T \cup \mathrm{ED}(N)$ is complete. Now, for countable submodels, the SS-property creates an opportunity to build almost primary models. This is exactly what we are going to do next.

Theorem 2.16. *Let T be a theory in a countable language. If T has the SS-property then, for any model $M \models T$ and any countable submodel $N \subseteq M$, N has a T-closure.*

Proof. If T has the SS-property then T is submodel complete. Fix $N \subseteq M \models T$ such that N is countable. Without loss of generality we may assume that M is countable as well. So by Lemma 2.14 all we need to do is to build an almost T-primary model N^* over N inside M. For this it is enough to build an almost isolating sequence for some model of T over N. The idea here is of course to find a suitable Skolem hull of N inside M such that the type of each "key" new element we find is isolated over all the previous elements.

To be precise, we want to build an almost isolating sequence $\langle (N_i, b_i) : i < \omega \cdot \omega \rangle$ over N such that for

- each $n < \omega$,
- each $\bar{a} \in N_{\omega \cdot n}$, and
- each formula $\varphi(x; \bar{y})$ such that $M \models \exists x \; \varphi(x; \bar{a})$,

there is an $m < \omega$ such that $M \models \varphi(\tau(b_{\omega \cdot n+m}); \bar{a})$ for some term $\tau(x)$ in the language $L(T \cup \mathrm{ED}(N_{\omega \cdot n+m}))$. It should be clear that $\bigcup_{i<\omega\cdot\omega} N_i = N^*$ is an elementary submodel of M, and hence is almost T-primary over N.

Now we carry out the construction. Start with $N_0 = N$ of course. Suppose $\langle (N_i, b_i) : i < \omega \cdot n \rangle$ is defined. Let $\langle \varphi_k(x; \bar{a}_k) : k < \omega \rangle$ be an enumeration of all the formulas in $T \cup \mathrm{ED}(N_{\omega \cdot n})$ such that for every $k < \omega$ we have $M \models \exists x \; \varphi_k(x; \bar{a}_k)$ but $M \models \neg\varphi_k(d; \bar{a}_k)$ for every $d \in N_{\omega \cdot n}$. Now suppose we have extended the sequence all the way up to $(N_{\omega \cdot n+k}, b_{\omega \cdot n+k})$ for some $k < \omega$. Let $N_{\omega \cdot n+k+1} = N_{\omega \cdot n+k} + b_{\omega \cdot n+k}$, that is the minimal submodel of M that contains $\{b_{\omega \cdot n+k}\} \cup |N_{\omega \cdot n+k}|$. If there is a $d \in N_{\omega \cdot n+k+1}$ such that $M \models \varphi_{k+1}(d; \bar{a}_{k+1})$ then let $b_{\omega \cdot n+k+1} = b_{\omega \cdot n+k}$. Otherwise by Lemma 2.15 we can pick a $b_{\omega \cdot n+k+1} \in |M| \setminus |N_{\omega \cdot n+k+1}|$ such that $M \models \varphi_{k+1}(b_{\omega \cdot n+k+1}; \bar{a}_{k+1})$ and the type $\mathrm{tp}(b_{\omega \cdot n+k+1}/\left|N_{\omega \cdot n+k+1}\right|, M)$ is isolated. □

The reader may ask: What is preventing us here from simply extending the above theorem to arbitrary theories and arbitrary submodels? One difficulty is this: We do not know how to extend Henkin's Omitting Type Theorem to uncountable theories and hence are unable to develop an analog of Lemma 2.15 for uncountable theories. In fact if we simply drop the countability requirement in Henkin's Omitting Type Theorem then it is false. See [5] for discussions. However, below we will show how to circumvent this difficulty if the language in question is countable. For this we assume the reader is familiar with some of the basic concepts and facts in infinitary combinatorics, in particular stationary sets and Fodor's Lemma.

Throughout the rest of this section T is a theory in a countable language and has the SS-property. Our strategy is to establish an analog of Lemma 2.15 for any submodel. To simplify the discussion we shall adopt a more concise terminology to describe the assumed situation in Lemma 2.15. Let $M \models T$ and $N \subseteq M$ such that N is uncountable and is not a model of T. So there is a formula $\exists x \; \varphi(x; \bar{a}) \in T \cup \mathrm{ED}(N)$ with $\bar{a} \in |N|$ such that $\varphi(M; \bar{a}) \subseteq |M| \backslash |N|$, where $\varphi(M; \bar{a})$ is the set $\{c \in M : M \models \varphi(c; \bar{a})\}$. In this case we say $\varphi(x; \bar{a})$ is *critical* for N. We have two cases to consider, namely $\|N\|$ is regular and $\|N\|$ is singular. By a routine transfinite induction we prove the next two corresponding lemmas.

Lemma 2.17. *Suppose $\|N\| = \kappa$ is regular and $\varphi(x; \bar{a})$ is critical for N. Then there is a $c \in \varphi(M; \bar{a})$ such that the type* $\operatorname{tp}(c/|N|, M)$ *is isolated.*

Proof. Without loss of generality we may assume $\|M\| = \kappa$. Fix a club $C = \langle \alpha_i : i < \kappa \rangle \subseteq \kappa$ and a continuous sequence of submodels $\langle N_i : i < \kappa \rangle$ such that

- for all $\alpha_i, \alpha_j \in C$ and $i < j$ we have $|\alpha_i| \leq |\alpha_j \setminus \alpha_i|$,
- $\|N_i\| = |\alpha_i|$,
- $\bar{a} \in N_0$ and if $i < j < \kappa$ then $N_i \subseteq N_j$,
- $\bigcup_{i<\beta} N_i = N_\beta$ if β is a limit ordinal and $\bigcup_{i<\kappa} N_i = N$.

By the inductive hypothesis we construct a sequence $\langle b_i \in \varphi(M; \bar{a}) : i < \kappa \rangle$ such that each type $\operatorname{tp}(b_i/|N_i|, M)$ is isolated. Fix an enumeration $\langle \phi_i : i < \kappa \rangle$ of all the formulas in the language of $T \cup \operatorname{ED}(N)$ such that for each $\alpha_i \in C$ we have

$$\{i : \phi_i \text{ is a formula in the language of } T \cup \operatorname{ED}(N_i)\} \subseteq \alpha_i.$$

Now define a function $f : C \longrightarrow \kappa$ by letting $f(\alpha_i)$ be the least ordinal such that $\phi_{f(\alpha_i)}$ isolates the type $\operatorname{tp}(b_i/|N_i|, M)$. Since f is a pressing-down function on a stationary subset of κ and κ is regular, by Fodor's Lemma, there is a $\gamma < \kappa$ such that $f^{-1}(\gamma) \subseteq C$ is stationary. Clearly for any $\alpha_i, \alpha_j \in f^{-1}(\gamma)$, if $\alpha_i < \alpha_j$ then $\operatorname{tp}(b_i/|N_j|, M) = \operatorname{tp}(b_j/|N_j|, M)$ as they are both isolated by ϕ_γ. So $\operatorname{tp}(b_i/|N|, M) = \operatorname{tp}(b_j/|N|, M)$ for any $\alpha_i, \alpha_j \in f^{-1}(\gamma)$. And this type is isolated by ϕ_γ as desired. □

For the case that $\|N\|$ is singular we need to work much harder:

Lemma 2.18. *Suppose $\|N\| = \kappa$ is singular and $\varphi(x; \bar{a})$ is critical for N. Then there is a $c \in \varphi(M; \bar{a})$ such that the type* $\operatorname{tp}(c/|N|, M)$ *is isolated.*

Proof. As above we may assume $\|M\| = \kappa$. Let $\lambda = \operatorname{cf}(\kappa) < \kappa$. Let $\langle \mu_i : i < \lambda \rangle \subseteq \kappa$ be a strictly increasing sequence of cardinals such that it is unbounded in κ. Fix an increasing sequence of submodels $\langle N_i : i < \lambda \rangle$ such that

- $\bar{a} \in N_0$ and if $i < j < \lambda$ then $N_i \subseteq N_j$,

- $\|N_i\| = \mu_i$,
- $\bigcup_{i<\lambda} N_i = N$.

We define a *good* sequence $\mathbf{F} = \langle \varphi_i(x) : i < \lambda \rangle$ of formulas for $\varphi(x; \bar{a})$ as follows:

1. each $\varphi_i(x)$ is a formula in the language of $T \cup \mathrm{ED}(N_i)$,
2. $\varphi(M; \bar{a}) \cap \varphi_i(M) \neq \emptyset$ for each $i < \lambda$,
3. if $b \in \varphi(M; \bar{a}) \cap \varphi_i(M)$ then the type $\mathrm{tp}(b/ |N_i|, M)$ is isolated by $\varphi_i(x)$.

The existence of such a good sequence is guaranteed by the inductive hypothesis. Note that this definition works in general for any formula that is critical for some submodel. Let

$$\mathrm{dom}(\mathbf{F}) = \{a \in N : a \text{ occurs as a parameter in some } \varphi_i(x) \in \mathbf{F}\}.$$

So $|\mathrm{dom}(\mathbf{F})| \leq \lambda$ for any good sequence $\mathbf{F}$.

Now, take an arbitrary good sequence $\mathbf{F}_0$ for $\varphi(x; \bar{a})$. Let $K_0 \subseteq N$ be the submodel generated by $\mathrm{dom}(\mathbf{F}_0) \cup \{\bar{a}\}$. Note that $\varphi(x; \bar{a})$ is critical for K_0. Since $\|K_0\| \leq \lambda < \kappa$, by the inductive hypothesis there is a $c_0 \in \varphi(M; \bar{a})$ such that $\mathrm{tp}(c_0/ |K_0|, M)$ is isolated by some formula $\sigma_0(x)$ in $L(T \cup \mathrm{ED}(K_0))$. Notice that if $\mathbf{F}_0 \subseteq \mathrm{tp}(c_0/ |K_0|, M)$ then we are done: in this case $\sigma_0(x)$ isolates the entire $\mathbf{F}_0$ and each $\varphi_i(x) \in \mathbf{F}_0$ isolates the type $\mathrm{tp}(c_0/ |N_i|, M)$, so the type $\mathrm{tp}(c_0/ |N|, M)$ is isolated by $\sigma_0(x)$. Next, since $\varphi(x; \bar{a}) \wedge \sigma_0(x)$ is critical for N (because it contains $\varphi(x; \bar{a})$ as a conjunct), we can construct a good sequence $\mathbf{F}_1$ for $\varphi(x; \bar{a}) \wedge \sigma_0(x)$. Clearly $\mathbf{F}_1$ is also a good sequence for $\varphi(x; \bar{a})$. Let $K_1 \subseteq N$ be the submodel generated by $|K_0| \cup \mathrm{dom}(\mathbf{F}_1)$. Then we can similarly find $c_1 \in \varphi(M; \bar{a})$ and an isolating formula $\sigma_1(x)$ in $L(T \cup \mathrm{ED}(K_1))$. Continuing in this fashion we can construct a sequence of triples $\langle (\mathbf{F}_i, c_i, \sigma_i(x)) : i < \lambda^+ \rangle$ such that

- $c_i \in \varphi(M; \bar{a})$,
- $\mathbf{F}_{i+1}$ is a good sequence for $\varphi(x; \bar{a}) \wedge \sigma_i(x)$,
- $\sigma_i(x)$ is a formula in the language $L(T \cup \mathrm{ED}(K_i))$ which isolates the type $\mathrm{tp}(c_i/ |K_i|, M)$, where $K_i \subseteq N$ is the submodel generated by the set $\{\bar{a}\} \cup \bigcup_{j \leq i} \mathrm{dom}(\mathbf{F}_j)$,

- if i is a limit ordinal then $\mathbf{F}_i$ is not defined.

Let $K = \bigcup_{j<\lambda^+} K_j$. Let

$$S^\lambda_{\lambda^+} = \left\{\alpha < \lambda^+ : \mathrm{cf}(\alpha) = \lambda\right\},$$

which is a stationary subset of λ^+. Fix an enumeration of all the formulas in $L(T \cup \mathrm{ED}(K))$ such that for each $\alpha \in S^\lambda_{\lambda^+}$ we have

$$\{i : \phi_i \text{ is a formula in the language of } T \cup \mathrm{ED}(K_\alpha)\} \subseteq \alpha.$$

So again by Fodor's Lemma there is a $\sigma_j(x)$ and a stationary subset $S \subseteq S^\lambda_{\lambda^+}$ such that for all $\alpha \in S$ the type $\mathrm{tp}(c_\alpha/\left|K_\alpha\right|, M)$ is isolated by $\sigma_j(x)$.

For any $\alpha, \beta \in S$ with $\alpha < \beta$, consider $\mathbf{F}_{\alpha+1}$. Since $\sigma_\alpha(x)$ is $\sigma_j(x)$, $\mathbf{F}_{\alpha+1}$ is a good sequence for $\varphi(x;\bar{a}) \wedge \sigma_j(x)$, so $M \models \exists x\, (\varphi(x;\bar{a}) \wedge \sigma_j(x) \wedge \varphi_i(x))$ for all $\varphi_i(x) \in \mathbf{F}_{\alpha+1}$ (this is by the second condition in the definition of a good sequence above). Since $\sigma_j(x)$ also isolates the complete type $\mathrm{tp}(c_\beta/\left|K_\beta\right|, M)$ and $\mathrm{dom}(\mathbf{F}_{\alpha+1}) \subseteq |K_\beta|$, we must have $\mathbf{F}_{\alpha+1} \subseteq \mathrm{tp}(c_\beta/\left|K_\beta\right|, M)$, so $\sigma_j(x)$ isolates $\mathbf{F}_{\alpha+1}$. Since each $\varphi_i(x) \in \mathbf{F}_{\alpha+1}$ determines the type over N_i, we see that $\sigma_j(x)$ isolates the type $\mathrm{tp}(c_\beta/\left|N\right|, M)$. □

With these two lemmas we can now simply proceed to build an almost isolating sequence for some model of T over N much in the same way as in Lemma 2.16, only now the length of the almost isolating sequence can go up to $\|N\| \cdot \omega$. So we have the following theorem:

Theorem 2.19. *For a countable theory T the SS-property and the D-property are equivalent.*

We end this section with the following question.

Question 2.20. What is the analog of Theorem 2.19 for uncountable theories? That is, without any additional assumptions Theorem 2.19 is probably not true for uncountable theories, so what “reasonable” assumptions can make it true for uncountable theories?

3 The Quantifier Elimination Procedure for the Theory of Real Closed Ordered Fields with a Predicate for the Powers of Two

It was Tarski who first found a decision procedure for the theory of real closed ordered fields. His method was QE. However, his original proof in [19] ran to several dozens of pages and involved a great deal of complex symbolism. It is a daunting task for anyone to decipher the crucial ideas in the proof. Fortunately many significant simplifications and improvements of Tarski's method have been made since the result was first published. One that is highly recommendable is Kreisel and Krivine's presentation in their textbook [13], though, as far as computational efficiency is concerned, it is really not that far away from Tarski's version.

Here we shall quote two key lemmas from their presentation because many claims in this section are inspired by them. The language of the theory of real closed ordered fields has the symbols 0, 1, $+$, $-$, $\times$, $<$. In this theory each quantifier-free formula $\varphi(x)$ can be written in the form

$$\bigwedge_{i<n} p_i(x) = 0 \wedge \bigwedge_{i<m} q_i(x) > 0,$$

where $p_i(x)$ and $q_i(x)$ are terms in the standard form, that is, polynomials. For any polynomial p we write $\deg(x, p)$ for the highest degree of x in p. The *degree in* x of $p_i(x) = 0$ is $\deg(x, p_i(x))$. The *degree in* x of $q_i(x) > 0$ is $\deg(x, q_i(x)) + 1$. The *degree in* x of $\varphi(x)$ is the maximum of the degrees of its atomic components.

Lemma 3.1. *For any quantifier-free formula $\varphi(x)$ of the form*

$$\bigwedge_{i<n} p_i(x) = 0 \wedge \bigwedge_{i<m} q_i(x) > 0,$$

there is a quantifier-free formula $\psi(x)$ which is equivalent to $\varphi(x)$ such that the degree in x of $\psi(x)$ is less than or equal to the least of the degrees in x of $p_i(x) = 0$ (which we assume is not 0).

Lemma 3.2. *Let $\varphi(x)$ be a quantifier-free formula. Let a, b be two variables that does not occur in $\varphi(x)$. Assume $a < b$. Then the formula $\exists x\ (a < x < b \wedge \varphi(x))$ is equivalent to a quantifier-free formula ψ such that ψ does* *not contain x, each variable in ψ is a, b, or a variable in φ, and no atomic formula in ψ contains both a and b. (Note that the claim can be rephrased accordingly if a, b are closed terms.)*

Now extend the language of real closed ordered fields with a predicate A which, in the intended interpretation, denotes the powers of two, $2^{\mathbb{Z}}$. Adopting the obvious conventions and abbreviations, add the following axioms:

- $\forall x\ (A(x) \rightarrow x > 0)$
- $\forall x, y\ (A(x) \rightarrow (A(y) \leftrightarrow A(xy)))$
- $A(2) \wedge \forall x\ (1 < x < 2 \rightarrow \neg A(x))$
- $\forall x\ (x > 0 \rightarrow \exists y\ (A(y) \wedge y \leq x < 2y))$

The first two imply that the A picks out a multiplicative subgroup of the positive elements. In [20], van den Dries showed that the resulting theory admits quantifier elimination in an expanded language. As a result, it is complete and decidable, and, in particular, axiomatizes the real numbers with a predicate for the powers of two.

The theory we have just described includes not only the theory of real closed ordered fields, but also, via an interpretation of integers as exponents, Presburger arithmetic. Thus, van den Dries's result is particularly interesting in that it subsumes two of the most important decidability results of the twentieth century. In recent years, this result has been extended in various directions (see, for example, [9] and [22]).

To establish QE, van den Dries gave a model-theoretic argument. In particular his argument shows that the theory in question has the D-property and QE follows from Theorem 2.9. The proof does not provide an explicit procedure, nor does it provide a bound on the length of the resulting formula. Here, we present a proof that makes use of nested calls to a QE procedure for real closed ordered fields, yielding a procedure that is primitive recursive but not elementary. In particular, it requires time $2^0_{O(n)}$ to eliminate a single block of existential quantifiers, or even a single existential quantifier, where n is the length of the input formula and 2^0_k denotes a stack of k exponents. Thus, the best bound we can give on the time complexity of the full QE procedure involves $O(n)$ iterates of the stack-of-twos function. We leave it as an open question as to whether one can avoid such nesting and, say, obtain elementary bounds for the elimination of a single existential quantifier.

In Section 3.1, we describe the extension of the theory above that admits QE. Our method of eliminating an existential quantifier proceeds in two steps: first, we eliminate that quantifier in favor of a multiple existential quantifiers over powers of two (the number of which is bounded by the length of the original formula); then we successively eliminate each of these. The first step is described in Section 3.1. In Section 3.2, we prove a number of lemmas that fill out the relationship between the powers of two and the underlying model of real closed ordered fields in a model of the relevant theory; this contains the bulk of the syntactic and algebraic work. In Section 3.3, we use these results to carry out the second step. Finally, in Section 3.4, we show that our procedure satisfies the complexity bounds indicated above.

3.1 The first step

Expand the language of real closed ordered fields to include a unary function λ and a unary predicate D_n for each $n \geq 1$. Let T be the theory given by the axioms above together with the following:

- $D_n(x) \leftrightarrow \exists y \ (A(y) \wedge y^n = x)$
- $\forall x \ (x \leq 0 \rightarrow \lambda(x) = 0)$
- $\forall x \ (x > 0 \rightarrow A(\lambda(x)) \wedge \lambda(x) \leq x < 2\lambda(x))$

In the standard interpretation, λ maps negative real numbers to 0 and rounds positive reals down to the nearest power of two, and D_n holds of numbers of the form 2^i where i is an integer divisible by n.[1] Note that A and D_1 are equivalent; we will treat them as the same symbol and use the two notations interchangeably.

Our goal is to prove the following:

Theorem 3.3. *T admits QE.*

[1] For parsimony, 0 can be defined as $1 - 1$ and $A(x)$ by $x > 0 \wedge \lambda(x) = x$. In the next section, we will see that the division symbol is another inessential addition to the language. But in contrast to QE for real closed ordered fields, one can't eliminate $-$ in terms of $+$; for example, the quantifier-free formula $A(x - y)$, if replaced by $\exists z \ (z + y = x \wedge A(z))$, would have no quantifier-free equivalent.

This is Theorem II of [20]. Henceforth, by "formula," we mean "formula in the language of T." We will use $\bar{x}$ to denote a sequence of variables $x_0, x_1, \ldots, x_{k-1}$, and we will use notation like $A(\bar{x})$ to denote $A(x_0) \wedge A(x_1) \ldots \wedge A(x_{k-1})$.

To eliminate quantifiers from any formula it suffices to be able to eliminate a single existential quantifier, that is transform a formula $\exists x\ \varphi$, where φ is quantifier-free, to an equivalent quantifier-free formula. Since $\exists x\ (\varphi \vee \psi)$ is equivalent to $\exists x\ \varphi \vee \exists x\ \psi$, we can always factor existential quantifiers through a disjunction. In particular, since any quantifier-free formula can be put in disjunctive normal form, it suffices to eliminate existential quantifiers from conjunctions of atomic formulas and their negations. Also, since $\exists x\ (\varphi \wedge \psi)$ is equivalent to $\exists x\ \varphi \wedge \psi$ when x is not free in ψ, we can factor out any formulas that do not involve x. Furthermore, whenever we can prove $\forall x\ (\theta \vee \eta)$, $\exists x\ \varphi$ is equivalent to $\exists x\ (\varphi \wedge \theta) \vee \exists x\ (\varphi \wedge \eta)$; so we can "split across cases" as necessary. We will use all of these facts freely below.

In [20], van den Dries established quantifier elimination by establishing the D-property. The novelty of this test, as compared to more common ones (see Definitions 2.7), lies in the prover's right to choose an appropriate b in the second clause (see also the discussion in [21]). This clause implies that any existential formula with parameters from the smaller model N that is true in the T-closure of $N + b$ is true in N; the test works because this clause can be iterated in a countable model to obtain a sequence of T-extensions $N = N_0 \subseteq N_1 \subseteq N_2 \ldots \subseteq M$ that eventually picks up every element of M, so any existential formula with parameters from N true in M is true in N (see Theorem 2.9). On the syntactic side, this iteration translates to the simple observation that to eliminate a single existential quantifier from an otherwise quantifier-free formula, it suffices to eliminate additional existential quantifiers from an equivalent existential formula. Thus, our effective proof is based on the following two lemmas:

Lemma 3.4. *Every formula of the form $\exists w\ \psi$, with ψ quantifier-free, is equivalent to a disjunction of formulas of the form $\exists \bar{x}\ (A(\bar{x}) \wedge \varphi)$, with φ quantifier-free.*

Lemma 3.5. *Every formula of the form $\exists x\ (A(x) \wedge \varphi)$, with φ quantifier-free, is equivalent to a formula that is quantifier-free.*

The remainder of this section is devoted to proving the first of these two lemmas. The next lemma explains why the new existentially quantified variables are helpful.

Lemma 3.6. *Every existential formula is equivalent, in T, to an existential formula in which λ does not occur and the predicates D_i are applied only to variables.*

Proof. First, replace $\ldots D_i(t) \ldots$ by $\exists z\ (z = t \wedge \ldots D_i(z) \ldots)$. Then, iteratively simplify terms involving λ, noting that $\psi(\lambda(t))$ is equivalent to

$$(t \leq 0 \wedge \psi(0)) \vee \exists z\ (A(z) \wedge z \leq t < 2z \wedge \psi(z)),$$

and that the existential quantifier can be brought to the front. □

Thus to prove Lemma 3.4, we are reduced to showing that when ψ is quantifier-free, λ does not occur in ψ, and the predicates D_i occurring in ψ are applied only to variables, the formula $\exists \bar{x}\ \psi$ is equivalent to one of the form $\exists \bar{x}\ (A(\bar{x}) \wedge \varphi)$, where φ is quantifier-free. In general, $\exists x\ \theta(x)$ is equivalent to

$$\exists x > 0\ \theta(x) \vee \theta(0) \vee \exists x > 0\ \theta(-x).$$

Moreover, assuming $x > 0$, any subformula of the form $D_i(-x)$ is equivalent to falsity. So, across a disjunction, we are reduced to proving the claim for formulas of the form $\exists \bar{x} > 0\ \psi(\bar{x})$, where ψ satisfies the criteria above.

In T we can factor out the greatest power of two from any positive x, that is we can prove

$$x > 0 \rightarrow \exists y\ \exists z\ (A(y) \wedge 1 \leq z < 2 \wedge x = yz).$$

Since we have $1 \leq z < 2 \leftrightarrow (z = 1 \vee 1 < z < 2)$, we can transform our formula into a disjunction of formulas of the form

$$\exists \bar{y}, \bar{z}\ (A(\bar{y}) \wedge 1 < \bar{z} < 2 \wedge \psi)$$

where ψ once again meets the criteria above, except that the predicates D_i are applied to expressions of the form yz. When $1 < z < 2$, each $D_i(yz)$ is false, so we can rewrite the formula above as

$$\exists \bar{y}\ (A(\bar{y}) \wedge \theta \wedge \exists \bar{z}\ \eta)$$

where θ is a conjunction of predicates of the form $D_n(y)$ and negations of such, and $\exists \bar{z}\ \eta$ is in the language of real closed ordered fields. We can therefore replace $\exists \bar{z}\ \eta$ by a quantifier-free formula, using any QE procedure for real closed ordered fields.

3.2 Reasoning about powers of two

Our goal in this section is to establish some general relationships between the powers of two in a model of our theory, T, and the underlying real closed field.

Definition 3.7. Let φ be a quantifier-free formula. We say φ is *simple in x* if the following hold:

1. every equality or inequality occurring in φ is either of the form $p(x) = 0$ or $q(x) > 0$, where $p(x)$, $q(x)$ are polynomials in x; that is, they are of the form $\sum_{i \leq n} s_i x^i$ where each s_i is a term that does not involve x.
2. for every atomic formula $D_n(t)$ occurring in φ, either t does not contain x or t is of the form $2^r x$ for some integer r such that $0 \leq r < n$.

The main goal of this section is to prove the following proposition:

Proposition 3.8. *Let φ be any quantifier-free formula. Then there is a quantifier-free formula φ' such that φ' is simple in x and T proves $A(x) \to (\varphi \leftrightarrow \varphi')$.*

In semantic terms, this says the following: let N be any model of T, let $M \subseteq N$ be a model of $T^{\forall}$, that is the universal fragment of T, and let x be a power of two in N. Then the structure of $M + x$ is completely determined by the structure of M, the structure of $M + x$ as an ordered ring, and the divisibility properties of the exponent of x.

First, we need to note some easy facts about λ and the predicates D_i.

Lemma 3.9. *For any n, T proves*

$$0 < u < x < 2^n u \wedge A(x) \to (x = 2\lambda(u) \vee \ldots \vee x = 2^n \lambda(u)).$$

Lemma 3.10. *For any n, T proves*

$$A(x) \to D_n(x) \vee D_n(2x) \vee \ldots \vee D_n(2^{n-1}x).$$

Although we have not included the division symbol in the language of T, we can define the function r/s by making $x/y = z$ equivalent to $x = yz \vee (y = 0 \wedge z = 0)$. In the proof of Proposition 3.8, it will be useful to act as though the division symbol is part of the language. The next few lemmas show that if θ is any quantifier-free formula in the expanded language with division, there is a quantifier-free formula θ' in the language without division such that $T \vdash \theta \leftrightarrow \theta'$.

Lemma 3.11. *From the hypotheses* $0 < x$ *and* $0 < y$, T *proves*

$$x\lambda(y) < y\lambda(x) \rightarrow \lambda(x/y) = \lambda(x)/2\lambda(y)$$

and

$$x\lambda(y) \geq y\lambda(x) \rightarrow \lambda(x/y) = \lambda(x)/\lambda(y).$$

Proof. An easy calculation shows that if $x/y < \lambda(x)/\lambda(y)$, then $\lambda(x/y) = \lambda(x)/2\lambda(y)$; and otherwise, $\lambda(x/y) = \lambda(x)/\lambda(y)$. □

Lemma 3.12. *If* θ *is any quantifier-free formula involving the division symbol, there is a quantifier-free formula* θ' *in which the division symbol does not occur in the scope of* λ, *such that* $T \vdash \theta \leftrightarrow \theta'$.

Proof. This can be done by iterating the previous lemma. To measure the nesting of λ's and division symbols, we define the "λ-depth of the division symbol in t," $\Lambda^{\div}(t)$, recursively, as follows:

1. $\Lambda^{\div}(t) = 0$ if the division symbol does not occur in the scope of λ in t;
2. if t is t_1+t_2, t_1-t_2, $t_1 \times t_2$, or t_1/t_2, then $\Lambda^{\div}(t) = \max\{\Lambda^{\div}(t_1), \Lambda^{\div}(t_2)\}$;
3. assuming the division symbol occurs in t, $\Lambda^{\div}(\lambda(t)) = \Lambda^{\div}(t) + 1$.

The previous lemma shows that, using a case disjunction over the possibilities for the signs of the numerator and denominator, we can eliminate one term t such that the λ-depth of the division symbol in t is maximal, in favor of terms in which the λ-depth of the division symbol is smaller. Lemma 3.12 follows, by a primary induction on this maximal depth, and a secondary induction on the number of terms of this depth. □

Lemma 3.13. $T \vdash A(x) \wedge A(y) \rightarrow (D_n(x/y) \leftrightarrow \bigvee_{i<n}(D_n(2^i x) \wedge D_n(2^i y)))$.

Proof. The right-to-left direction is easy: if $z^n = 2^i x$ and $w^n = 2^i y$ then $(z/w)^n = x/y$. Proving the other direction is not much more difficult, using Lemma 3.10. □

Proposition 3.14. *Let* θ *be any quantifier-free formula involving division. Then there is a quantifier-free formula* θ' *that does not involve division, such that* $T \vdash \theta \leftrightarrow \theta'$.

Proof. Using Lemma 3.12, we can assume that division does not occur in the scope of any λ in θ. So each atomic formula $D_n(t)$ can be put in the form $D_n(r/s)$, where the division symbol does not occur in r and s. Across a case disjunct, we can assume r and s are positive. Then $D_n(r/s)$ is equivalent to

$$\lambda(r/s) = r/s \land D_n(\lambda(r/s)).$$

Using Lemma 3.11, we can replace $\lambda(r/s)$ by either $\lambda(r)/\lambda(s)$ or $\lambda(r)/2\lambda(s)$. Then using Lemma 3.13 we can replace $D_n(\lambda(r)/\lambda(s))$ or $D_n(\lambda(r)/2\lambda(s))$ by a disjunction in which the division symbol does not occur.

Once all divisibility symbols are removed from the λ's and D_n's, we can clear division from the remaining equalities and inequalities by multiplying through. □

It therefore suffices to prove Proposition 3.8 where φ' is a quantifier-free formula in the expanded language with the division symbol. The next few lemmas, then, make use of this expanded language.

Lemma 3.15. *Let $p(x)$ be the term $\sum_{i\leq n} a_i x^i$. Then there is a sequence of quantifier-free formulas $\theta_0, \ldots, \theta_{m-1}$ such that T proves*

$$A(x) \land p(x) > 0 \to \bigvee_{k<m} \theta_k,$$

where each θ_k is of one of the following forms:

- $\lambda(p(x)) = 2^r \lambda(a_i) x^i$ *for some* $-1 \leq r \leq n$,
- $x^e = \frac{2^r \lambda(a_i)}{\lambda(-a_j)}$ *or* $x^e = \frac{2^r \lambda(-a_j)}{\lambda(a_i)}$, *for some e, i, j, and r such that* $1 \leq e \leq n$, $0 \leq i, j \leq n$, *and* $-(n+1) \leq r \leq (n+1)$.

Proof. Argue in T. Using a disjunction on all possible cases, we can write $p(x)$ as $a_i x^i + a_j x^j + \hat{p}(x)$, where $a_i x^i$ is the largest summand and $a_j x^j$ the least summand. Note that we have $a_i x^i > 0$, $i \neq j$, $p(x) \leq (n+1)a_i x^i$, and

$$p(x) - a_i x^i = a_j x^j + \hat{p}(x) \geq n a_j x^j.$$

We now distinguish between two cases, depending on whether $p(x)$ is roughly the same size as $a_i x^i$ or sufficiently smaller.

In the first case, suppose we have $p(x) \geq (a_i x^i)/2$. This means we have

$$(a_i/2)x^i \leq p(x) \leq (n+1)a_i x^i \leq 2^n a_i x^i$$

and so

$$(\lambda(a_i)/2)x^i \leq \lambda(p(x)) \leq 2^n\lambda(a_i)x^i.$$

This yields a disjunction of clauses of the first type, by Lemma 3.9.

In the second case, we have $p(x) < (a_ix^i)/2$. This means that a_jx^j must be negative and roughly comparable to a_ix^i in absolute value; that is $a_j < 0$ and

$$(a_i/2)x^i < a_ix^i - p(x) \leq -na_jx^j,$$

and so

$$0 < (a_i/(-a_j))x^{i-j} \leq 2n \leq 2^n.$$

Using Lemma 3.11 and Lemma 3.9 we get a disjunction of clauses of the second type. □

Lemma 3.16. *In Lemma 3.15, if the assumption is changed to $A(x) \wedge p(x) = 0$, then in the conclusion we can assume that each θ_k is of the second form.*

Proof. This is exactly as in the second case of the previous proof. □

Lemma 3.17. *In the conclusion of Lemma 3.15, we may demand that each θ_k is of the form $\lambda(p(x)) = sx^i$ for some $0 \leq i \leq n$ and some term s that does not contain x.*

Proof. The proof is by induction on the degree of x in $p(x)$. The lemma is trivial if the degree of x in $p(x)$ is 0.

Now assume that the degree of x in $p(x)$ is n and the lemma holds whenever the degree is less than n. By Lemma 3.15, T proves a disjunction $\bigvee \sigma_l$, with σ_l of one of those two forms. Each σ_l of the first form there is already as required. For each σ_l of the second form, consider a new term $\hat{p}(x)$, which is obtained by substituting the right-hand side of σ_l for x^e in $p(x)$. Notice that the degree of x in $\hat{p}(x)$ is less than n, and clearly T proves $p(x) = \hat{p}(x) \wedge \hat{p}(x) > 0$. By the inductive hypothesis we may replace σ_l in $\bigvee \sigma_l$ by a disjunction $\bigvee \theta_k$ which is of the required form. □

As was the case with the division symbol, we will iterately "squeeze" x's out from within the λ symbols. Thus we introduce the following definitions:

Definition 3.18. Let t be a term. Define the *λ-depth of x in t*, $\Lambda(x, t)$, recursively, as follows:

1. $\Lambda(x, t) = 0$ if x is not in the scope of any λ;

2. if t is t_1+t_2, t_1-t_2, $t_1\times t_2$, or t_1/t_2, then $\Lambda(x,t)=\max\{\Lambda(x,t_1),\Lambda(x,t_2)\}$;

3. if t is $\lambda(t_1)$ and t_1 contains x, then $\Lambda(x,t)=\Lambda(x,t_1)+1$.

Definition 3.19. Let φ be a formula. Define the *λ-depth of x in φ* by

$$\Lambda(x,\varphi)=\max\{\Lambda(x,t) : t \text{ is a term that contains } x \text{ and occurs in } \varphi\}.$$

Lemma 3.20. *Let φ be any quantifier-free formula. Then there is a quantifier-free formula φ' such that $T\vdash A(x)\to(\varphi\leftrightarrow\varphi')$, and $\Lambda(x,\varphi')=0$.*

Proof. The proof is by induction on the λ-depth of x in φ. The lemma is trivial if $\Lambda(x,\varphi)=0$.

Assume $\Lambda(x,\varphi)=n>0$ and the lemma holds for every quantifier-free formula ψ if $\Lambda(x,\psi)<n$. Let $\lambda(p_0)$, …, $\lambda(p_{m-1})$ be all the different terms in φ with $\Lambda(x,p_i)=0$ for all $i<m$. Across a case disjunction we can assume $p_i>0$ for all $i<m$, since otherwise we can replace $\lambda(p_i)$ by 0. By Lemma 3.12, we may assume that each p_i is a polynomial in x. By Lemma 3.17, T proves $\varphi\leftrightarrow\bigvee(\tau_l\wedge\sigma_l)$, where each τ_l is of the form $\bigwedge_{i<m}\lambda(p_i(x))=s_ix^{j_i}$, and each σ_l is obtained by substituting $s_ix^{j_i}$ for $\lambda(p_i)$ in φ. Clearly T proves $\lambda(p_i(x))=s_ix^{j_i}\leftrightarrow A(s_i)\wedge s_ix^{j_i}\leq p_i(x)<2s_ix^{j_i}$. Now since $\Lambda(x,\sigma_l)<n$, we may apply the inductive hypothesis to each σ_l and the lemma is proved. □

Lemma 3.21. *Let p be a term such that $\Lambda(x,p)=0$. Then for any n there is a sequence of terms p_k such that*

- *T proves $A(x)\wedge p>0\to(D_n(p)\leftrightarrow\bigvee(p=p_k\wedge D_n(p_k)))$,*
- *each p_k is of the form sx^i, where s is a term that does not contain x.*

Proof. Using Lemma 3.13, we can assume that p is a polynomial in x. We can replace $D_n(p)$ by $p=\lambda(p)\wedge D_n(\lambda(p))$, and then by Lemma 3.17, across a disjunction we may replace $\lambda(p)$ in each disjunct by a term of the form sx^i, where s does not contain x. (Note that here no formulas like the τ_l's in the previous lemma are needed.) □

Lemma 3.22. *Let s be a term that does not contain x. Then for any n, i there is a sequence of formulas θ_k such that T proves*

$$A(x)\to(D_n(sx^i)\leftrightarrow\bigvee\theta_k),$$

and each θ_k is of the form $D_n(2^ws)\wedge D_n(2^rx)$ for some $0\leq w,r<n$.

Proof. Since for each n, from the assumption $A(x)$, T proves $\bigvee_{j<n} D_n(2^j x)$, it is straightforward to see that $D_n(sx^i)$ is equivalent to a disjunction each of whose disjuncts is of the specified form. □

We are finally ready to prove Proposition 3.8.

Proof. Given φ, first use Lemma 3.20 to eliminate x from the scope of any λ. Then use Lemma 3.21 to ensure the atomic formulas involving D_n are in the form $D_n(sx^i)$, where s does not involve x. (This will require splitting across cases depending on whether $p > 0$ or $p \leq 0$; in the latter case, $D_n(p)$ is equivalent to $\perp$.) Finally, use Lemma 3.22 to ensure that all the atomic formulas involving D_n are in the required form. □

We close with some consideration about the predicates D_n which are analogous to considerations that arise in the context of QE for Presburger arithmetic. Remember that when n is a positive integer and s is a non-negative integer, $D_n(2^s x)$ asserts, in the intended interpretation, that x is equal to 2^t for some integer t, and n divides $s+t$; in other words, the exponent of x is congruent to $-s$ modulo n. Let θ be any boolean combination of predicates of the form $D_n(2^s x)$, and let M be the least common multiple of these various n. Then in T one can show that there is an x satisfying θ if and only if for any w satisfying $A(w)$ we have

$$\theta(w) \vee \theta(2w) \vee \theta(4w) \vee \ldots \vee \theta(2^{M-1}w),$$

and, in particular, if and only if

$$\theta(1) \vee \theta(2) \vee \theta(4) \vee \ldots \vee \theta(2^{M-1}).$$

Moreover, T can decide the truth or falsity of this last sentence. So we have:

Lemma 3.23. *With θ and M as above, either T proves $\forall x\ \neg\theta$, or it proves*

$$\forall u\ (0 < u \rightarrow \exists x\ (u \leq x < 2^M u \wedge \theta)).$$

3.3 Eliminating a quantifier over powers of two

We are now ready to prove Lemma 3.5, which asserts that every formula of the form $\exists x\ (A(x) \wedge \varphi)$, with φ quantifier-free, is equivalent to a formula that is quantifier-free. By Proposition 3.8, we can assume that φ is simple, which is to say, x does not occur in the scope of any λ and all divisibility assertions involving x are of the form $D_n(2^r x)$. Put φ in disjunctive normal form, replace negated equalities $s \neq t$ by $s < t \vee t < s$, and replace negated inequalities $s \not< t$ by $t < s \vee t = s$. Rewrite equalities and inequalities so that they are of the form $p(x) = 0$ and $q(x) > 0$, where $p(x)$ and $q(x)$ are polynomials in x. Factoring existential quantifiers through disjunctions and getting rid of atomic formulas that do not depend on x, we are reduced to eliminating quantifiers of the form $\exists x\ (A(x) \wedge \varphi)$ where φ is a conjunction of formulas of the following types:

- $p(x) = 0$, where p is a polynomial,
- $q(x) > 0$, where q is a polynomial,
- $D_n(2^r x)$, where $0 \leq r < n$, or
- $\neg D_n(2^r x)$, where $0 \leq r < n$.

Splitting across a disjunction, we can assume that when a conjunct of the form $p(x) = 0$, not all the coefficients are zero. By Lemma 3.16, we can assume that one of the conjuncts is of the form $x^e = s$, where x does not occur in s. In that case, each conjunct $D_n(2^r x)$ is equivalent to $D_{ne}(2^{re} x^e)$ and hence $D_{ne}(2^{re} s)$ (and $A(x)$, in particular, is equivalent to $D_e(s)$). But now x no longer occurs in these formulas, and so they can be brought outside the scope of the existential quantifier. The resulting existential formula is then essentially in the language of real closed ordered fields. By this last phrase we mean that it is of the form $\exists x\ \alpha(x, t_0, \ldots, t_{k-1})$, where $\alpha(x, y_0, \ldots, y_{k-1})$ is in the language of real closed ordered fields. Treating the terms $t_0, \ldots, t_{k-1}$ in the expanded language as parameters, we can therefore replace it by an equivalent quantifier-free formula using any QE procedure for real closed ordered fields.

We are thus reduced to eliminating an existential quantifier of the form

$$\exists x\ (\bigwedge q_i(x) > 0 \wedge \theta(x)) \tag{3.1}$$

where θ is a conjunction of formulas of the form $D_n(2^r x)$ and negations of such that includes at least the formula $A(x)$. By Lemma 3.23, either T proves that θ is false for every x, or there is a natural number M such that T proves that for any $u > 0$, that θ is satisfied by some x in the interval $[u, 2^M u]$. In the first case, T proves that formula 3.1 is false. So we only have to worry about the second case. Fix such an M for the remainder of the discussion.

Arguing in T, suppose formula (3.1) holds. There are two possibilities: either there is a "large" interval on which $\bigwedge q_i(x) > 0$, that is, an interval of the form $[u, 2^M u]$; or there is an x satisfying $A(x) \wedge \bigwedge q_i(x) > 0 \wedge \theta$, but it is trapped between a u and a v with $q_i(u) = 0$ for some i, $q_j(v) = 0$ for some j, and $v < 2^M u$. Thus formula (3.1) is equivalent to a disjunction of the formula

$$\exists u > 0\, \forall x\, (u \leq x \leq 2^M u \rightarrow \bigwedge q_i(x) > 0)$$

and the formulas

$$\exists u > 0\, (q_j(u) = 0 \wedge \exists x\, (u < x \leq 2^M u \wedge \bigwedge q_i(x) > 0 \wedge \theta(x))$$

for the various j. To see this, note that if formula (3.1) holds, then by the previous discussion one of these formulas holds; and conversely, each of these formulas implies (3.1).

The first of these formulas is essentially in the language of real closed ordered fields, so these quantifiers can be eliminated. The second formula is equivalent to

$$\exists u_1, u_2\, (A(u_1) \wedge 1 \leq u_2 < 2 \wedge q_j(u_1 u_2) = 0 \wedge \\ \exists x\, (u_1 < x \leq 2^M u_1 \wedge \bigwedge q_i(x) > 0 \wedge \theta(x)).$$

In this case, we can replace the inner existential quantifier over x by a disjunction, so that the entire formula is equivalent to a disjunction of formulas of the form

$$\exists u_1, u_2\, (A(u_1) \wedge 1 \leq u_2 < 2 \wedge q_j(u_1 u_2) = 0 \wedge \bigwedge \hat{q}_i(u_1) > 0 \wedge \hat{\theta}(u_1)),$$

where each $\hat{q}_i(u_1)$ is $q_i(2^r u_1)$ for some r, and similarly for $\hat{\theta}(u_1)$. In particular, $\hat{\theta}(u_1)$ is a conjunction of formulas of the form $D_i(2^r u_1)$, and their negations.

Think of $q_j(u_1 u_2)$ as a polynomial in u_1 with coefficients of the form $s u_2^n$, where s does not involve u_1 or u_2. By Lemma 3.16, across a disjunction we may add a clause of the form $u_1^e = 2^r \lambda(s u_2^n)/\lambda(t u_2^m)$. Splitting on cases of the form $2^l \leq u_2^h < 2^{l+1}$ we can simplify each of these to an expression of the form $u_1^e = 2^k \lambda(s)/\lambda(t)$ for some integer k. By Lemma 3.23, $A(u_1) \wedge \hat{\theta}(u_1)$ is equivalent to a formula $\bar{\theta}$ which now involves neither u_1 nor u_2, and hence can be brought outside the existential quantifier. We are thus reduced to eliminating quantifiers from a formula of the form

$$\exists u_1, u_2 \; (1 \leq u_2 < 2 \wedge u_1^e = 2^k \lambda(s)/\lambda(t) \wedge 2^l \leq u_2^h < 2^{l+1} \wedge \\ q_j(u_1 u_2) = 0 \wedge \bigwedge \hat{q}_i(u_1) > 0).$$

We can eliminate these quantifiers using a QE procedure for real closed ordered fields. This completes the proof of Lemma 3.5, and hence the proof of our main theorem, Theorem 3.3.

Note that there is nothing special about the number 2 in our quantifier elimination procedure: inspection of the proofs shows that the arguments go through unchanged for any real algebraic number $\alpha > 1$. There are various ways to represent the real algebraic numbers; for example, we can represent α by providing a polynomial, $p(x)$, of which it is a root, together by a pair of rational numbers u and v isolating α from the other roots of p. In that case, we simply replace 2 by a new constant, c, in the axioms, and then add the following:

- $p(c) = 0$
- $u < c < v$

As noted in [22], this implies that the resulting theory is decidable. To see this, it suffices to see that any quantifier-free sentence φ is decidable. But we can do this using the decision procedure for real closed ordered fields to iteratively compute the values of $\lambda(t)$ for any t involving the field operations and c, and then to determine the truth of terms of atomic formulas $D_n(t)$. (For explicit algorithms for computing with real algebraic numbers, see [3].)

3.4 Complexity analysis

In this section we establish an upper bound on the complexity of our elimination procedure.

For the theory of real closed ordered fields, the best known upper bound for a QE procedure, in terms of the length of the input formula, is $2^{2^{O(n)}}$. This is originally due to Collins [6], and, independently, Monk and Solovay. There are more precise bounds that depend on various parameters, such as the number of quantifier alternations and the degrees of the polynomials in the formula; see, for example, [2] and [3]. In particular, a block of existential quantifiers can be eliminated in time $2^{O(n)}$. The best lower bound for the full QE procedure is $2^{O(n)}$, by Fischer and Rabin [8], and applies even to just the additive fragment. The best upper bound for Presburger arithmetic is $2_3^{O(n)}$ (see [7] and [23]) and is essentially sharp (see [24]).

Our bounds are far worse. Consider what our procedure does when given a formula with a single block of existential quantifiers:

1. First, replace this by a disjunction of formulas of the form

   $$\exists \bar{y}\ (A(\bar{y}) \wedge \exists \bar{z}\ (1 < \bar{z} < 2 \wedge \psi))$$

   where ψ is in the language of real closed ordered fields.

2. Then, use an elimination procedure for real closed ordered fields to eliminate the quantifiers $\exists \bar{z}$.

3. Successively eliminate the innermost quantifier over a power of two, as follows:

   (a) Call the relevant formula $\exists x\ (A(x) \wedge \varphi)$. Apply Proposition 3.8, to reduce φ to a formula that is simple in x.

   (b) Put the new φ in disjunctive normal form, split across a disjunction, and remove atomic formulas that do not involve x, so that each formula is of the form

   $$\exists x\ (A(x) \wedge \bigwedge p_i(x) = 0 \wedge \bigwedge q_j(x) = 0 \wedge \theta)$$

   where θ is a conjunction of formulas of the form $D_n(2^r x)$ and negations of such, and in each disjunction where a disjunct of the form $p(x) = 0$ occurs, we can assume p is not identically 0.

   (c) In each disjunct where a conjunct of the form $p(x) = 0$ occurs, apply Lemma 3.16, factor out the divisibility predicates, D_n, and call a QE procedure for real closed ordered fields.

   (d) In the remaining disjuncts, again, split across a disjunct; in one case, we call a QE procedure for real closed fields right away; in another, we expand a bounded existential quantifier into a disjunction, and then call the elimination procedure for real closed ordered fields.

Note that each iteration of the inner loop, 3, requires at least one call to a QE procedure for real closed ordered fields. Each of these calls can be carried out in time, say, $2^{2^{O(n)}}$, where n is the length of the relevant formula. But then the next iteration of the loop will involve calls to the QE procedure for real closed ordered fields on a formula that is potentially much longer. Thus, part 3 of the procedure requires an exponential stack of Cm twos, for some constant C, where m is the number of existential quantifiers over powers of two that need to be eliminated.

In this section, we will confirm that such an upper bound can be obtained. To that end, it is sufficient to show that each pass of the inner loop is elementary, which is to say, it can be computed in time bounded by some fixed stack of exponents to the base 2. Note that after the first step, the number of quantifiers over powers of two is bounded by the length of the original formula (in fact, it is bounded by the number of A's and λ's in the original formula). Thus our procedure for eliminating a block of existential quantifiers runs in time $2^0_{O(n)}$, where n is the length of the original formula.

We have been unable to eliminate this nesting of calls to a procedure for real closed ordered fields. Efficient procedures for this latter theory avoid putting formulas in disjunctive normal form; for example, Collins's cylindrical algebraic decomposition procedure obtains a description of cells, depending on the coefficients, on which a set of polynomials have constant sign. In our setting, suppose we are given a formula $\exists \bar{x}\ (A(\bar{x}) \wedge \eta \wedge \theta)$, where η contains only equalities and inequalities between polynomials, and θ consists of divisibility conditions D_n on the exponents of the x's. One might start by applying Collins's procedure to the polynomials occurring in η. Then, given a description of the various cells (depending on the other parameters in the formula), one needs to determine which cells contain points with coordinates that are powers of two, with exponents satisfying the requisite divisibility conditions. For one dimensional cells, our procedure relies on a simple disjunction: if the cell is large enough, one is guaranteed a solution, and otherwise one need only test a finite number of cases. For multidimensional cells, however, the situation is more complex, and we do not see how one can proceed except along the lines we have described above. It is thus an interesting question as to whether it is possible to obtain elementary bounds on a procedure for eliminating a single block of quantifiers. Given our failure to do so, we have not taken great pains to bound the number of exponents in the time bound on the inner loop, which would merely improve the constant bound implicit in the $O(n)$.

For the discussion which follows, we define the *length* of a formula in the language of T to be the number of symbols in a reasonable formulation of the first-order language, with the following exception: we count the length of each symbol D_n as n, rather than, say, one plus the binary logarithm of n. This choice is a pragmatic one in that it simplifies the analysis, and our results below then imply the corresponding results for the alternative definition of length. A more refined analysis might take both the length of the formula and a bound on the n's occurring in atomic formulas $D_n(t)$, but that does not seem to help much.

It seems that the most delicate part of our task is showing that one can remove the division symbols, and "squeeze" variables ranging over powers of two out of the λ symbols that are repeatedly introduced after the first step of the procedure, as required in step 3(a). A priori, the procedures described in Section 3.2 look as though they may be non-elementary. The next few lemmas show that this is not the case, by keeping careful track of the terms and formulas that need to be dealt with in the disjunctions.

Lemma 3.24. *Let t be a term with length l. Then there is a sequence of terms $\langle t_k : k < 2^l \rangle$ such that*

- $T \vdash \bigvee_{k<2^l} t = t_k$,
- *each t_k is of the form r/s, where r and s are division-free terms, and*
- *each t_k has length at most 2^l.*

Proof. This can be proved by a straightforward induction on terms. Suppose t is of the form $t_1 + t_2$, where the length of t_1 is l_1 and the length of t_2 is l_2. By the inductive hypothesis, t is equal to one of at most $2^{l_1}2^{l_2} \leq 2^l$ terms of the form $r_1/s_1 + r_2/s_2$, where r_1, s_1, r_2, and s_2 are division-free, the length of r_1/s_1 is at most 2^{l_1}, and the length of r_2/s_2 is at most 2^{l_2}. But then the length of $(r_1 s_2 + r_2 s_1)/s_1 s_2$ is at most $2(2^{l_1} + 2^{l_2}) < 2^l$, as required.

If t is of the form $\lambda(t_1)$, the claim follows from the inductive hypothesis, using Lemma 3.12. The other cases are similar. □

Lemma 3.25. *Let φ be a quantifier-free formula with length l. Then there is a quantifier-free division-free formula φ' with length $2^{O(l)}$ such that $T \vdash \varphi \leftrightarrow \varphi'$.*

Proof. Enumerate all the different terms $t_0, \ldots, t_{m-1}$ in φ such that, for each $i < m$, s_i is not a proper subterm of any term in φ. Using the above lemma we can have a sequence of quantifier-free formulas φ_j for $j < 2^l$ each of which is obtained by replacing each t_i with an appropriate term and therefore has length less than 2^l. Notice that for each φ_j, as indicated in Lemma 3.12, there are some division-free atomic formulas that T used to derive the equalities in question. Clearly for each φ_j there are less than l such atomic formulas, each of which has length less than $2^{O(l)}$. Let σ_j be the conjunction of them all. Let φ' be the formula $\bigvee_{j<2^l}(\varphi_j \wedge \sigma_j)$. The length of φ' is again bounded by $2^{O(l)}$, and clearly $T \vdash \varphi \leftrightarrow \varphi'$.

Finally, we need to clear denominators from atomic formulas of the form $r/s < t/u$ and $r/s = t/u$, and deal with atomic formulas of the form $D_n(r/s)$. The first two require a disjunction over cases, depending on whether denominators are positive, negative, or zero. The third set of atomic formulas is handled as described in the proofs of Lemma 3.13, 3.14. But each atomic formula occurring in a disjunct occurs to an atomic formula in the original formula, φ, and there are at most l of these. It is not hard to verify that the corresponding increase in length can be absorbed into the bound $2^{O(l)}$. □

Lemma 3.26. *Let $\lambda(t)$ be a term, where the length of t is l and x does not occur in the scope of any division symbol in t. Then there is a sequence of terms $\langle t_k : k < 2^{8l^2 \log l}\rangle$ such that*

- *$T \vdash A(x) \wedge t > 0 \rightarrow \bigvee_{k<2^{8l^2 \log l}}(\lambda(t) = t_k)$,*
- *each t_k is of the form sx^i, where s is a term that does not contain x and $i < l$,*
- *each t_k has length at most $2^{2^{4l}}$.*

Proof. For any polynomial p in x, clearly the number of possible values of $\lambda(p)$ of the form sx^i, as in Lemma 3.17, depends on the degree n of x in p. So let $f(n)$ denote the number of possible values of $\lambda(p)$. Observe that the value of $\lambda(p)$ is determined in the first case of Lemma 3.15, and when $e = 1$ in the second case. An calculation shows that there are no more than $(n+1)(n+2)$ possibilities in the first case, no more than $2n(2n+2)$ possibilities in the second case when $e = 1$, and no more than $(n+1)(n-1)2(n+2)$ possibilities for all the remaining values of e. Hence we have the following equation:

$$f(n) \leq (n+1)(n+2) + 2n(2n+2) + (n+1)(n-1)2(n+2)f(n-1).$$

This can be simplified as $f(n) < 10(n+2)^3 f(n-1)$. So we have $f(n) < 2^{8n\log(n+2)}$. Let the length of p be l. Since $n+2 < l$, we have $f(n) < 2^{8l\log l} < 2^{8l^2\log l}$.

Now the proof proceeds by induction on the λ-depth of x in t. If $\Lambda(x,t) = 0$, then t is a polynomial in x. So we apply the above analysis to t and obtain no more than $2^{8l\log l}$ possible values of $\lambda(t)$ which are all of the form sx^i for some $i < l$. To compute the length of s, only note that each step of the iteration produces a polynomial whose length is no more than the square of the length of the previous polynomial. So we conclude that the length of s is no more than $l^{2^l} < 2^{2^{4l}}$.

Now suppose the lemma holds for each term s with $\Lambda(x,s) < d$, and suppose $\Lambda(x,t) = d$. Enumerate all the different terms $\lambda(s_0),\ldots,\lambda(s_{m-1})$ in t such that $\lambda(s_i)$ is not in the scope of any λ for each $i < m$. Clearly $\Lambda(x,s_i) < n$ for each $i < m$. So by the inductive hypothesis there are less than $2^{8l_i^2\log l_i}$ possible values for each $\lambda(s_i)$, where l_i is the length of s_i. Since $\sum_{i<m} l_i < l-1$, there are no more than $2^{8(l-1)^2\log l}$ possible values for t. Enumerate these possibilities as $\langle t_k : k < 2^{8(l-1)^2\log l}\rangle$. In each t_k, $\lambda(s_i)$ is replaced by a term of the form sx^j with $j < l_i$. So t_k is a polynomial in x whose degree in x is less than $l-2$. So there are $2^{8(l-1)^2\log l}\cdot 2^{8l\log l} \le 2^{8l^2\log l}$ possible values for $\lambda(t)$. The length of each t_k is bounded by $2^{2^{4(l-1)}}$, so the length of each possible value of $\lambda(t)$ is bounded by $2^{2^{4(l-1)}}\cdot l\cdot l^{2^l} < 2^{2^{4l}}$. □

Lemma 3.27. *Let φ be a quantifier-free formula with length l. Assume x does not occur in the scope of any division symbol in φ. Then there is a quantifier-free formula φ' with length at most $2^{2^{O(l)}}$ such that φ' is simple in x and $T \vdash A(x) \to (\varphi \leftrightarrow \varphi')$.*

Proof. First we claim there is a quantifier-free formula φ^* with length at most $2^{2^{O(l)}}$ such that

- $T \vdash A(x) \to (\varphi \leftrightarrow \varphi^*)$,
- x does not occur in the scope of any division in φ^*,
- $\Lambda(x,\varphi^*) = 0$.

The proof is essentially the same as the proof of Lemma 3.25, using Lemma 3.26 instead of Lemma 3.24.

Next we need to deal with atomic formulas of the form $D_n(p)$ in φ^*, as shown in Lemma 3.21. So p is a polynomial in x whose degree in x is less than l. So there are at most $2^{2^{O(l)}}$ possible values for $\lambda(p)$, the length of each of which is bounded by $2^{2^{O(l)}}$. So each $D_n(p)$ can be replaced by a disjunction whose length is less than $2^{2^{O(l)}}$. So the bound does not change.

The increase in length in transforming φ^* to a formula that is simple in x, as described in the proof of Lemma 3.22, can be absorbed in the bound $2^{2^{O(l)}}$. □

Lemma 3.28. *Let φ be a quantifier-free formula with length l. Then there is a quantifier-free formula φ' with length at most $2_3^{O(l)}$ such that φ' is simple in x and T proves $A(x) \to (\varphi \leftrightarrow \varphi')$.*

Proof. Immediate by Lemma 3.25 and Lemma 3.27. □

Lemma 3.29. *Each iteration of step 3 can be performed by an elementary function.*

Proof. It is straightforward to verify that the procedure implicit in Lemmas 3.28 runs in time polynomial in its output. As a result, step 3(a) is elementary. Step 3(b) is also clearly elementary. In fact, even though putting a formula in disjunctive normal form can result in exponentially many disjuncts, since each disjunct only involves atomic formulas from the original formula, the length of each disjunct is bounded in the length of the original formula.

After step 3(a), the main increase therefore comes from the handling of the cases in (c) and (d), each of which is easily seen to be elementary. Case (c) involves a call to a QE procedure for real closed ordered fields, with a $\forall\exists$ formula; case (d) involves calls to such a procedure, on existential formulas, across a number of disjuncts that is exponential in the length of the original formula. □

Theorem 3.30. *There is a procedure for eliminating a single block of existential quantifiers in theory T in time $2^0_{O(l)}$, where l is the length of the original formula.*

Proof. Steps 1 and 2 are clearly elementary, after which the procedure performs an elementary operation for each quantifier over a power of two. As noted above, the number of such quantifiers can even be bounded by the number of predicates D_n and λ's in the original formula. □

Corollary 3.31. *There is a procedure for eliminating quantifiers in theory T that runs in time bounded by $O(l)$ iterations of the stack-of-twos function, where l is the length of the original formula.*

Proof. Put the formula in prenex form, and iteratively apply the previous theorem to eliminate each block of quantifiers. □

4 Real Closed Ordered Fields with a Predicate for the Fibonacci Numbers

In this section we show that the theory of real closed ordered fields with a predicate for the Fibonacci numbers is recursively axiomatizable and hence is decidable. Moreover, the decision procedure described in the last section can be used to decide this theory.

The Fibonacci numbers are a sequence of natural numbers F_n defined by the recurrence relation

$$F_{n+2} = F_{n+1} + F_n$$

for $n > 0$ with $F_1 = F_2 = 1$. It is conventional to define $F_0 = 0$. The first few Fibonacci numbers are 0, 1, 1, 2, 3, 5, 8, 13, 21, ...

Let $\phi = \frac{1+\sqrt{5}}{2}$. Let A be a predicate for the multiplicative subgroup $\phi^{\mathbb{Z}} \subseteq \mathbb{R}^{>0}$. By Binet's Fibonacci number formula the nth Fibonacci number can be computed as follows:

$$F_n = \frac{\phi^n - \frac{(-1)^n}{\phi^n}}{\sqrt{5}}.$$

Therefore we can introduce a predicate F^* for the Fibonacci numbers with the following defining axiom:

$$F^*(x) \leftrightarrow \Gamma^e(x) \vee \Gamma^o(x), \tag{4.1}$$

where $\Gamma^e(x)$ and $\Gamma^o(x)$ are the formulas

$$\exists y \left(A(y) \wedge y \geq 1 \wedge \exists z \left(A(z) \wedge y = z^2\right) \wedge x = \frac{y - \frac{1}{y}}{\sqrt{5}}\right),$$

$$\exists y \left(A(y) \wedge y \geq 1 \wedge \exists z \left(A(z) \wedge y = \phi z^2\right) \wedge x = \frac{y + \frac{1}{y}}{\sqrt{5}}\right),$$

respectively.

Now we give a complete axiomatization of the theory of real closed ordered fields with the distinguished Fibonacci numbers. We start with the theory of real closed ordered fields and a new predicate F for the Fibonacci numbers. Let $\Delta(x, y)$ abbreviates the formula

$$F(x) \wedge F(y) \wedge x < y \wedge \forall z \left(x < z < y \rightarrow \neg F(z)\right).$$

First we add the following axioms:

(A1) $F(x) \to x \geq 0$;

(A2) $\Delta(0,1) \wedge \Delta(1,2)$;

(A3) $x > 2 \to \big(F(x) \leftrightarrow \exists y, z\ (\Delta(y,z) \wedge x = y + z \wedge \forall w\ (z < w < x \to \neg F(w)))\big)$;

(A4) $z \geq 0 \to \exists x, y\ (\Delta(x,y) \wedge x \leq z < y)$.

Notice the following identities on the Fibonacci numbers:

$$\begin{aligned} F_{2n} &= F_n(2F_{n+1} - F_n), \\ F_{2n+1} &= F_{n+1}^2 + F_n^2. \end{aligned}$$

Generalizing these we let $\Sigma^{(e,o)}(x,y)$ and $\Sigma^{(o,e)}(x,y)$ be the formulas

$$\exists w, z\ (\Delta(w,z) \wedge x = w(2z - w) \wedge y = z^2 + w^2),$$
$$\exists w, z\ (\Delta(w,z) \wedge x = z^2 + w^2 \wedge y = z(2w + z)),$$

respectively and obtain a new axiom:

(A5) $\Delta(x,y) \leftrightarrow \Sigma^{(e,o)}(x,y) \vee \Sigma^{(o,e)}(x,y)$.

This actually enables us to define the predicate A: let $\Theta^e(x)$ and $\Theta^o(x)$ be the formulas

$$\exists y, w, z\ (\Delta(w,z) \wedge y = w(2z - w) \wedge y = \frac{x - \frac{1}{x}}{\sqrt{5}}),$$
$$\exists y, w, z\ (\Delta(w,z) \wedge y = z^2 + w^2 \wedge y = \frac{x + \frac{1}{x}}{\sqrt{5}}),$$

respectively, then

$$A(x) \leftrightarrow x > 0 \wedge (\Theta^e(x) \vee \Theta^o(x) \vee \Theta^e(\frac{1}{x}) \vee \Theta^o(\frac{1}{x})).$$

Now the idea is this. By the results in the last section there is a complete axiomatization of the theory of $(\mathbb{R}, \phi^{\mathbb{Z}})$ (see the last paragraph of Subsection 3.3), we may use F to define the predicate A and subsequently use A to define the predicate F^* via 4.1. Finally we throw in some axioms to guarantee that

- A picks out a suitable multiplicative subgroup and
- F^* and F are the same.

This will axiomatize a complete, hence decidable, theory with a predicate for the Fibonacci numbers.

Let K be an ordered field with a valuation v. Two nonzero elements a, b of K are in the same *Archimedean class* if $\frac{1}{n} < v(\frac{a}{b}) < n$ for some positive integer n. Let us say that a "local relation" is a relation that holds only among elements in the same Archimedean class and a "global relation" is a relation that is not local. Some classic identities on the Fibonacci numbers can, when generalized, control the behaviors of the predicate A, though only locally. For example, it is not hard to deduce the following:

$$\forall x, y\ (\Delta(x, y) \to y^2 - yx - x^2 = 1) \leftrightarrow \forall z\ (A(z) \leftrightarrow A(\phi z)).$$

But one should not think that such local identities are sufficient when elements in different Archimedean classes are involved. In fact an axiom is needed for the predicate A's multiplicative closure:

(A6) $A(x) \wedge A(y) \to A(xy)$.

It is not hard to see that (A4) and (A6) together prove that

$$y > 0 \to \exists x\ (A(x) \wedge x \leq y < \phi x).$$

Finally we stipulate that

(A7) $F(x) \leftrightarrow F^*(x)$.

One may of course recast some of the axioms above into a form that is more explicit about the Fibonacci numbers. The calculations are easy but tedious. We shall not include them here. For example (A7) can be transformed into

$$\begin{aligned} F(x) \leftrightarrow \exists a, b, c, d\ \big(&\Delta(a, b) \wedge \Delta(c, d) \\ &\wedge ((x = a(2b - a) \wedge P_1(a, b, c, d)) \vee (x = a^2 + b^2 \wedge P_2(a, b, c, d)))\big), \end{aligned}$$

where $P_1(a, b, c, d)$ and $P_2(a, b, c, d)$ are the polynomials

$$\begin{aligned} &\big(5c^4(2d - c)^4 + 4c^2(2d - c)^2 - a^2(2b - a)^2\big) \\ &\qquad\qquad\qquad \big(5(c^2 + d^2)^4 - 4(c^2 + d^2)^2 - a^2(2b - a)^2\big) = 0 \end{aligned}$$

and

$$\begin{aligned}&\bigl(5c^4(2d-c)^4+4c^2(2d-c)^2-5(a^2+b^2)c^2(2d-c)^2+(a^2+b^2-1)^2\bigr)\\&\quad\bigl(5(c^2+d^2)^4-4(c^2+d^2)^2-5(a^2+b^2)(c^2+d^2)^2+(a^2+b^2+1)^2\bigr)=0,\end{aligned}$$

respectively. But these do not seem to be more natural than the ones that are listed above, even though it is rather curious why these polynomials are sufficient to determine the complete theory.

References

[1] J. Avigad and Y. Yin, *Quantifier elimination for the reals with a predicate for the powers of two*, submitted.

[2] S. Basu, *New results on quantifier elimination over real closed fields and applications to constraint databases*, J. ACM **46** (1999), no. 4, 537–555.

[3] S. Basu, R. Pollack, and M. F. Roy, *Algorithms in real algebraic geometry*, Algorithms and Computation in Mathematics, vol. 10, Springer-Verlag, Berlin, 2003.

[4] B. F. Caviness and J. R. Johnson (eds.), *Quantifier elimination and cylindrical algebraic decomposition*, Texts and Monographs in Symbolic Computation, Springer-Verlag, Vienna, 1998.

[5] C. C. Chang and H. J. Keisler, *Model theory*, third ed., Studies in Logic and the Foundations of Mathematics, vol. 73, North-Holland, Amsterdam, 1990.

[6] G. E. Collins, *Quantifier elimination for real closed fields by cylindrical algebraic decomposition*, Lecture Notes in Computer Science, vol. 33, pp. 134–183, Springer, Berlin, 1975, reprinted in [4].

[7] J. Ferrante and C. W. Rackoff, *The computational complexity of logical theories*, Lecture Notes in Mathematics, vol. 718, Springer, Berlin, 1979.

[8] M. J. Fischer and M. O. Rabin, *Super-exponential complexity of Presburger arithmetic*, SIAM-AMS Proc., vol. VII, pp. 27–41, Amer. Math. Soc., Providence, R.I., 1974, reprinted in [4].

[9] H. Friedman and C. Miller, *Expansions of o-minimal structures by fast sequences*, Journal of Symbolic Logic **70** (2005), no. 2, 410–418.

[10] R. Grossberg, *A course in model theory*, unpublished manuscript.

[11] D. Hilbert and W. Ackermann, *Principles of mathematical logic*, second ed., AMS Chelsea Publishing, Providence, Rhode Island, 1958, translated from the German by L. M. Hammond, G. G. Leckie, and F. Steinhardt.

[12] W. Hodges, *Model theory*, Cambridge University Press, Cambridge, UK, 1993.

[13] G. Kreisel and J. L. Krivine, *Elements of mathematical logic*, North-Holland Publishing Company, Amsterdam, 1971.

[14] C. H. Langford, *Some theorems on deducibility*, Annals of Mathematics **28** (1927), 16–40.

[15] ——, *Theorems on deducibility (second paper)*, Annals of Mathematics **28** (1927), 459–471.

[16] G. E. Sacks, *Saturated model theory*, W. A. Benjamin, Inc., Reading, Massachusetts, 1972.

[17] J. R. Shoenfield, *Mathematical logic*, Addison-Wesley, Reading, 1967.

[18] ——, *A theorem on quantifier elimination*, Symposia Mathematica **5** (1971), 173–176, INDAM, Rome, 1969/1970, Academic Press, London.

[19] A. Tarski, *A decision method for elementary algebra and geometry*, second ed., University of California Press, Berkeley, CA, 1951, prepared for publication with the assistance of J. C. C. McKinsey.

[20] Lou van den Dries, *The field of reals with a predicate for the powers of two*, Manuscripta Math. **54** (1985), 187–195.

[21] ——, *Alfred Tarski's elimination theory of real closed fields*, The Journal of Symbolic Logic **53** (1988), no. 1, 7–19.

[22] Lou van den Dries and Ayhan Günaydin, *The fields of real and complex numbers with a small multiplicative group*, preprint, 2005.

[23] V. Weispfenning, *The complexity of almost linear Diophantine problems*, J. Symbolic Computation **10** (1990), no. 5, 395–403.

[24] ——, *Complexity and uniformity of elimination in Presburger arithmetic*, pp. 48–53, ACM, New York, 1997, electronic.