A CONSISTENCY PROOF FOR ELEMENTARY ALGEBRA AND GEOMETRY

by
Harvey M. Friedman
Department of Mathematics
Ohio State University
August 10, 1999
August 23, 1999

ABSTRACT

We give a consistency proof within a weak fragment of arithmetic of elementary algebra and geometry. For this purpose, we use EFA (exponential function arithmetic), and various first order theories of algebraically closed fields and real closed fields.

We actually prove in EFA that RCF (real closed fields) is consistent and complete. The completeness proof is an adaptation of known constructions.

We also obtain a proof in EFA that every quantifier free formula provable in RCF has a quantifier free proof in the theory of real fields and in the theory of ordered fields.

As a Corollary, we obtain an interpretation of RCF into EFA in the sense of model theory, as well as interpretations of finitely axiomatized extensions of RCF into EFA.

The development can be used to provide fixed length iterated exponential estimates in connection with Hilbert's seventeenth problem. This application will appear elsewhere.

INTRODUCTION

to be written. discusses Hilbert's program briefly. discusses systems of arithemetic briefly. introduces EFA = exponential function arithmetic. reference to Hajek/Pudlak. disclaimer that we make no attempt here to obtain more precise information.

1. PRELIMINARIES ABOUT LOGIC

In the free variable predicate calculus with equality, we start with a signature Σ consisting of a set of constant, relation, and function symbols. Formulas are built up in the usual way using the variables $v_1, v_2, \ldots,$ connectives not, or,

and, implies, iff, =, and the symbols in $\sum$. There are no quantifiers.

The variables are literally the v_i, $i \geq 1$. We use this to define the universal closure of a formula φ. This is obtained from φ by successively universally quantifying by the free variables of φ in reverse order of their subscripts. If φ is a sentence then the universal closure of φ is φ.

The logical axioms are

1. All tautologies in the language.

The equality axioms are

2. x = x, where x is a variable.
3. x = y implies (φ implies φ'), where x,y are variables, φ,φ' are atomic formulas, and φ' is the result of replacing some occurrences of x in φ by y.

The rules of inference are

4. From φ and (φ implies ψ) derive ψ.
5. From φ derive any term substitution of φ in the language.

Suppose we are given a set T of proper axioms; i.e., a set of quantifier free formulas in the language. Then a proof in T is a finite sequence of formulas, every one of which is either a logical axiom, an equality axiom, a proper axiom, or follows from previous formulas in the finite sequence by one or more rules of inference. The proof in T is said to be a proof in T of the last formula. We say that the last formula is free variable provable in T.

We begin by stating the well known completeness theorem for free variable predicate calculus.

THEOREM 1.1. Let T be a set of quantifier free formulas and φ be a quantifier free formula based on the signature $\sum$. The following are equivalent.
i) Every equality model universally satisfying all elements of X universally satisfies φ;
ii) φ is free variable provable in T;
iii) some finite set of subsitution instances of elements of T and the equality axioms tautologically implies φ.

Theorem 1.1 is an infinitary statement becuase of clause i), and also becuase X may be infinite. However, we have the following finite statement:

THEOREM 1.2. (EFA) Let T be a finite set of quantifier free formulas and φ be a quantifier free formula based on the signature Σ. The following are equivalent.
i) φ is free variable provable in T;
ii) some set of substitution instances of elements of T and the equality axioms tautologically implies φ.

We use the following terminology in connection with ii) above. An instantiation of T is a finite set of substitution instances of elements of X together with a finite set of substitution instances of equality axioms. All of this is required to take place in the signature sigma.

A special proof in T of a quantifier free formula phi in the language of sigma is an instantiation of T which tautologically implies φ. Thus condition ii) above asserts that "φ has a special proof in T."

In the predicate calculus with equality, we start with a signature sigma consisting of a set of constant, relation, and function symbols. Formulas are built up in the usual way using the variables $x_1, x_2, \ldots$, connectives $\neg$, $\vee$, $\wedge$, $\rightarrow$, $\leftrightarrow$, quantifiers $\forall$, $\exists$, =, and the symbols in Σ.

The logical axioms are

1. All tautologies in the language.
2. $(\forall x)(\varphi) \rightarrow \varphi[x/t]$, where t is a term free for the variable x in φ.
3. $\varphi[x/t] \rightarrow (\exists x)(\varphi)$, where t is a term free for the variable x in φ.

The equality axioms are

4. x = x, where x is a variable.
5. $x = y \rightarrow (\varphi \rightarrow \varphi')$, where x,y are variables, φ, φ' are atomic formulas, and φ' is the result of replacing some occurrences of x in φ by y.

The rules of inference are

6. From φ and $\varphi \rightarrow \psi$ derive ψ.

7. From φ → ψ derive φ → (∀x)(ψ), where the variable x is not free in φ.
8. From φ → ψ derive (∃x)(φ) → ψ, where the variable x is not free in ψ.

Suppose we are given a set T of proper axioms; i.e., a set of formulas in the language. Then a proof in T is a finite sequence of formulas, every one of which is either a logical axiom, an equality axiom, a proper axiom, or follows from previous formulas in the finite sequence by one or more rules of inference. The proof in T is said to be a proof of the last formula. We say that the last formula is provable in T.

Of course, we have the celebrated Gödel completeness theorem.

THEOREM 1.4. Let T be a set of formulas and phi be a formula based on the signature ∑. The following are equivalent.
i) Every equality model universally satisfying all elements of T universally satisfies φ;
ii) φ is provable in T.

There is an important consequence of Theorems 1.2 and 1.4 for quantifier free formulas.

THEOREM 1.5. Let T be a set of quantifier free formulas and φ be a quantifier free formula based on the signature ∑. The following are equivalent.
i) φ is provable in T;
ii) φ is free variable provable in T;
iii) φ has a special proof in T.

Notice that Theorem 1.5 does not mention infinitary objects. However, we know that it cannot be proved in EFA. The usual proof of Theorem 1.5 is to pass through Theorem 1.4, which is infinitary. Theorem 1.5 can also be proved using the cut elimination theorem for predicate calculus with equality. However, the cut elimination theorem can only be proved by going slightly beyond EFA.

A formula is said to be existential if and only if it starts with a block of zero or more existential quantifiers which are followed by a quantifier free formula. We are interested in a criterion for a set of existential formulas to logically imply an existential formula. Obviously, we can simply use derivability in predicate calculus with equality because of Theorem 1.4. But we are looking for something more "local"

such as special proofs. For this purpose, we introduce iterated instantiations.

Let T be a set of existential formulas in $\sum$. An iterated instantiation of T is any finite set of quantifier free formulas obtained in the following way. First select an element of T and make any term substitution not mentioning the bound variables in that element of T. Then add variables witnessing their existential quantifiers. These witness variables must all be distinct, and distinct from any variables appearing earlier. Then select another element of T and make any term substitution not mentioning the bound variables in that element of T. Then add variables witnessing their existential quantifiers, which must be distinct and distinct from all variables appearing earlier. Continue in this manner for finitely many steps.

NOTE: In subsequent sections, all formulas in the X's considered will have at most one existential quantifier, and so at most one witness variable is introduced at each step.

For each introduction of witness variables, there is the corresponding witness formula asserting that the substitution instance of the element of X in question holds at the witness variables.

The iterated instantiation consists of all these witness formulas. It should be noted that some elements of T may be quantifier free. Substitution instances of them may appear in the iterated instantiation without introducing any witness variables.

Let φ be an existential formula in $\sum$. A special proof of φ in T is an iterated instantiation X of the union of T and the set of equality axioms, such that

i) X tautologically implies some instantiation of the existential quantifiers in φ by terms;
ii) no witness variables in T appear free in φ.

It is clear that there is no conflict of notation with the earlier definition of special proof; the definitions coincide if X and φ are quantifier free.

There is a close relationship between special proofs of existential formulas from a set of existential formulas, and

cut free proofs of existential formulas from a set of existential formulas in the Gentzen sequent calculus.

THEOREM 1.6. Let T be a set of existential formulas and φ be an existential formula. The following are equivalent.
i) φ is provable in T;
ii) φ has a cut free proof from the universal closures of elements of T and the equality axioms;
iii) φ has a special proof in T.

Proof: In ii), we are referring to the usual Gentzen sequent calculus; i.e., there is a sequent whose antecedent is a finite sequence of universal closures of elements of T and whose consequent is φ. i) implies ii) is the standard Gentzen cut elimination theorem. And iii) implies i) is obvious. QED

We are interested in which systems of arithmetic the equivalence of ii) and iii) can be proved. For this purpose, we assume that T is finite.

It is possible to go directly from cut free proofs to special proofs and vice versa in an explicit way that is easily sufficient to establish the equivalence of ii) and iii) in EFA.

However, it is known that the equivalence between i) and ii) - i.e., the cut elimination theorem - cannot be proved in EFA. It can, however, be proved just beyond EFA. More specifically, let EFA' be the same as EFA except that indefinite exponentiation is added with the obvious quantifier free axiom. Of course, one uses induction for all bounded formulas in the language.

THEOREM 1.7. (EFA) Let T be a finite set of existential formulas and φ be an existential formula. Then φ has a cut free proof from universal closures of elements of T and the equality axioms if and only if phi has a special proof in T. Also, Theorem 1.6 for finite T is provable in EFA'. In fact, ii) implies i) is provably equivalent to EFA' over EFA for finite T.

Proof: It is easy to go from a special proof to a corresponding cut free proof. This is because the substitution instances correspond to universal introductions on the left side, the witnesses correspond to existential

introductions on the left side, and any tautological implication has a cut free proof.

We now indicate how to go from a cut free proof of the relevant kind to a special proof. For this purpose, it is convenient to change the definition of special proof. Under this new definition, we consider special proofs of existential formulas from sets T of ∀∃ formulas. Here only universal quantifiers give rise to substitutions. As before, existential quantifiers give rise to witnesses. There is no significant blowup in the size of the proof, so the construction can be easily carried out in EFA.

Now let π be a cut free proof of the relevant kind. We show by induction that each sequent has a special proof in the sense that there is an iterated instantiation of the left side that tautologically implies the right side. The right side is interpreted disjunctively if there is more than one formula on the right side. Again, there is no significant blowup in the size of the proof. QED

2. QUANTIFIER ELIMINATION AND CONSISTENCY

Throughout the rest of the paper, we let $E_c(x)$ be an exponential stack of c 2's with an x on top. I.e., $E_0(x) = x$, $E_1(x) = 2^x$. We let E_c be $E_c(1)$.

The special consistency of an existential theory asserts that the formula $x \neq x$ does not have a special proof in the theory. Of course, the consistency of any theory asserts that the formula x not= x does not have a proof in the theory. According to Theorem 1.7, it is provable in EFA that the consistency and the special consistency are equivalent for existential theories with finitely many axioms.

It is the purpose of this section to prove that if, provably in EFA, an existential theory has a certain property related to quantifier elimination, then, provably in EFA, consistency is equivalent to special consistency. We also obtain some additional results involving conservative extensions.

An EFA existential theory T consists of a finite signature, an integer constant $c \geq 1$, and a Turing machine TM, such that EFA proves

i) TM accepts or rejects strings in time bounded by $E_c(x)$;

ii) TM accepts only existential formulas in the signature.

Proofs and special proofs in T refer to proofs and special proofs in the set of all existential formulas accepted by TM.

THEOREM 2.1. Suppose T is an EFA existential theory. Then EFA′ proves the equivalence of consistency and special consistency of T. In fact, EFA′ proves that every existential formula has a proof in T if and only if it has a special proof in T.

Proof: This follows immediately from the finite case in Theorem 1.7. QED

We make the following definitions in EFA. For formulas φ, write $\#(\varphi)$ for the size of φ, which is the total number of symbols in φ, assuming a base 2 representation of all subscripts of variables. The size of a proof or a special proof is the total number of symbols involved, again with base 2 representation of all subscripts of variables.

We say that T is an EFA qe existential theory if and only if T is an EFA existential theory with constants c such that the following is provable in EFA. (Here qe stands for "quantifier elimination").

Let $(\exists x)(\varphi(x, y_1, \ldots, y_n))$ be a formula in the signature of X, where phi is quantifier free, $x, y_1, \ldots, y_n$ are distinct variables, and all variables in φ are among those shown. There is a quantifier free $\psi(y_1, \ldots, y_n)$ with all variables among those shown and special proofs of

$$\varphi(x, y_1, \ldots, y_n) \rightarrow \psi(y_1, \ldots, y_n)$$

and

$$(\exists x)(\psi(y_1, \ldots, y_n) \rightarrow \varphi(x, y_1, \ldots, y_n))$$

in T of size $\leq 2^{[\log(\#(phi))^{E_c(n)}]}$.

We say that T is a strong EFA qe existential theory if and only if

i) T is an EFA existential theory with integer constant c;

ii) EFA proves that T is specially consistent in the sense that there is no special proof in T of any quantifier free formula and its negation;
iii) EFA proves that if φ is a quantifier free sentence in the signature of T, then there is a special proof of φ or of $\neg\varphi$ in T of size $\leq E_c(\#(\varphi))$ using only the quantifier free elements of T;
iv) the following is provable in EFA:

Let $(\exists x)(\varphi(x,y_1,...,y_n))$ be a formula in the signature of X, where φ is quantifier free, $x,y_1,...,y_n$ are distinct variables, and all variables in φ are among those shown. There is a quantifier free $\psi(y_1,...,y_n)$ with all variables among those shown and special proofs of

$$\varphi(x,y_1,...,y_n) \to \psi(y_1,...,y_n)$$

and

$$(\exists x)(\psi(y_1,...,y_n) \to \varphi(x,y_1,...,y_n))$$

in T of size $\leq 2^{[\log(\#(\varphi))^{E_c(n)}]}$, where the first special proof uses only the quantifier free formulas in T.

Until further notice, we fix an EFA qe existential theory T with constant c. In EFA, let H map each quantifier free $\varphi(x,y_1,...,y_n)$ to the first special proofs given by the definition, where they are ordered first by size and second by lexicographic order. We also let H' map each quantifier free $\varphi(x,y_1,...,y_n)$ to to the quantifier free formula $\psi(y_1,...,y_n)$ used in the value of H.

Obviously EFA proves the inequalities $H(x),H'(x) \leq 2^{\log(x)^{E_c(n)}}]$ in terms of sizes of formulas and special proofs, where n is one less than the number of variables in the formula x. Obviously if c is, say, at least 4, then EFA proves the inequalities $H(x),H'(x) \leq E_c(x)$. We assume that $c \geq 4$.

In order to simultaneously handle the case of a strong EFA qe existential theory, we assume that H gives the first special proofs given by the definition of strong EFA qe existential theory if this is possible. We can do this, since we have placed a size bound on the special proofs being searched for.

For every formula phi we define a quantifier free formula $\varphi^\star$ in the language of fields as follows. If φ is atomic then $\varphi^\star$ = φ. $(\neg\varphi)^\star = \neg(\varphi^\star)$. $(\varphi \vee \psi)^\star = \varphi^\star \vee \psi^\star$. $(\varphi \wedge \psi)^\star = \varphi^\star \wedge \psi^\star$. $(\varphi \rightarrow \psi)^\star = \varphi^\star \rightarrow \psi^\star$. $(\exists x)(\varphi)^\star = H'((\exists x)(\varphi^\star))$. $(\forall x)(\varphi)^\star = (\neg(\exists x)(\neg\varphi))^\star$. We have to argue that this definition can be given in EFA.

LEMMA 2.2. There is a bounded formula $\rho(x,y)$ with the free variables shown, and a constant c' such that the following is provable in EFA. $\rho(x,y)$ defines a function obeying the definition of the $\star$ function. $(\forall x)(\exists y \leq E_{c'}(x))(\rho(x,y))$.

Proof: It suffices to prove in EFA that for any formula φ, we can assign to each direct subformula ρ of φ, a formula $\varphi^\star$ so that the clauses in the definition of $\star$ above are obeyed, Let φ be given, and let n be the greatest of all subscripts of variables in φ. All of the direct subformulas and their $\star$'s will have at most n variables. We can give fixed length iterated exponential upper bound for the $\star$'s of the direct subformulas in #(φ) by iterating the function $2^{[\log(x)^{E_c(n)}]}$ as a function of x, at most #(φ) times, where c,n are fixed. QED

LEMMA 2.3. There is an integer c' such that the following is provable in EFA. Let φ be a formula provable in predicate calculus. Then $\varphi^\star$ has a special proof in T of size $\leq E_{c'}(\#(\varphi))$.

Proof: It suffices to handle formulas that use the existential quantifier and not the universal quantifier. This is because the usual replacement of the universal quantifiers with existential quantifiers preserves $\star$. I.e., the $\star$ of any formula provable in predicate calculus is the $\star$ of an ostensibly equivalent formula without universal quantifiers provable in the predicate calculus for formulas without universal quantifiers. Futhermore, this conversion at most doubles the size of the formulas and the proofs involved.

We take as axioms

1. All tautologies.
2. Quantifier free axioms for equality.
3. $\varphi[x/t] \rightarrow (\exists x)(\varphi)$, where t is a term free for x in φ.

And we have the two rules

4. From φ and φ → ψ derive ψ.
5. From φ → ψ derive (∃x)(φ) → ψ, where x is not free in ψ.

Let $\varphi_1, \varphi_2, \ldots, \varphi_m$ be a proof in this system, where all formulas are in the signature of X. Fix n to be the total number of variables present in the proof.

Let c′ be as given by Lemma 2.3, which we can assume is greater than c. We will prove that for all $1 \le i \le m$, there is a special proof of φ_i* in T of size $\le E_{c'}(\#(\varphi_1) + \ldots + \#(\varphi_i))$.

Clearly, if φ_i is an instance of axiom 1 or 2 then there is a special proof of φ_i* in T of size $\le E_{c'}(\#(\varphi_i))$.

Let φ_i = φ[x/t]* → (∃x)(φ)*.

(∃x)(φ)* is the quantifier free equivalent ψ of (∃x)(φ*) as given by H, and x is not in ψ. Also φ[x/t]* = φ*[x/t]. There is a special proof of

φ* arrows ψ

in T of size $\le 2^{[\log(\#(phi*))^{E_c(n)}]} \le E_{c'+4}(\#(\varphi))$. We can adjust this special proof so that no witness is x and no witness appears in t. Hence there is a special proof of

φ*[x/t] → ψ

in T of size $\le E_{c'+8}(\#(\varphi_i))$, by substituting t for x in the adjusted special proof.

Suppose φ_i follows from φ_j and φ_k by rule 4. Then we can obviously combine the special proofs of φ_j* and φ_k* of sizes $\le E_{c'+8}(\#(\varphi_1) + \ldots + \#(\varphi_j))$ and $E_{c'+8}(\#(\varphi_1) + \ldots + \#(\varphi_k))$ to get a special proof in T of size $\le E_{c'+8}(\#(\varphi_1) + \ldots + \#(\varphi_i))$.

Finally suppose φ_i is obtained by rule 5. Let φ_i = (∃x)(φ) → ψ, and φ_j = φ → ψ, where j < i. We have a special proof of φ* → ψ* in T of size $\le E_{c'+8}(\#(\varphi_1) + \ldots + \#(\varphi_j))$. Let ρ be the quantifier free equivalent of (∃x)(φ*) given by H′. We must find a special proof of ρ → ψ* in T of size $\le E_{c'+8}(\#(\varphi_1) + \ldots + \#(\varphi_i))$.

Evidently we have a special proof of (∃x)(ρ → φ*) in T of size $\le E_c(\#(\varphi))$. By combining this with the special proof of φ* → ψ* in T, we obtain a special proof of ρ → ψ* in T of

size $\leq E_{c'+8}(\#(\varphi_1)+\ldots+\#(\varphi_j))+E_c(\#(\varphi)) \leq E_{c'+8}(\#(\varphi_1)+\ldots+\#(\varphi_i))$.
QED

LEMMA 2.4. There is an integer c' such that the following is provable in EFA. Let φ be quantifier free and have a special proof in T of size $\leq n$. Then $(\forall x)(\varphi)^*$ has a special proof in T of size $\leq E_{c'}(\#(\varphi))+n$.

Proof: $(\exists x)(\psi \rightarrow \neg\varphi)$ has a special proof in T of size $\leq E_d(\#(\neg\varphi)) \leq E_{d+1}(\#(\varphi))$, where ψ is given by H' at $(\exists x)(\neg\varphi)$. This can be combined with a special proof of φ in T to produce a special proof of $\neg\psi$ in T of size $\leq E_{d+1}(\#(\varphi))+n \leq E_{d+2}(n)$ since $\#(\varphi) \leq n$. Note that $(\forall x)(\varphi)^* = (\neg(\exists x)(\neg\varphi))^* = \neg\psi$. QED

LEMMA 2.5. There is an integer c' such that the following is provable in EFA. Let φ be quantifier free and have a special proof in T of size $\leq n$. Then the * of the universal closure of phi has a special proof in T of size $\leq E_{c'}(n)$.

Proof: Let c' be as given by Lemma 2.4. Let $\varphi(x_1,\ldots,x_m)$ be as given, where $x_1,\ldots,x_m$ is a listing without repetition of the free variables of phi in strictly increasing order of subscripts (see the definition of universal closure made in section 1). We iterate the construction in Lemma 2.4 for m steps. We get the estimate $mE_{c'}(2\#(\varphi))+n \leq E_{c'+4}(n)$. QED

LEMMA 2.6. There is an integer c' such that the following is provable in EFA. The * of the universal closure of every axiom φ of T has a special proof in X of size $\leq E_{c'}(\#(\varphi))$.

Proof: By Lemma 2.5 it suffices to show that every axiom φ of T has a special proof in X of size $\leq E_2(\#(\varphi))$. This is obvious. QED

LEMMA 2.7. There is an integer c' such that the following is provable in EFA. Let φ be a formula with a proof in T of size $\leq n$. Then φ^* has a special proof in T of size $\leq E_{c'}(n)$.

Proof: Let c' be the max of the constants in Lemmas 2.3 and 2.6. Let φ have a proof in T of size n. Let $\psi_1,\ldots,\psi_n$ be the universal closures of the axioms of T that are used in this proof, listed without repetition. Then there is a proof of $(\psi_1 \wedge \ldots \wedge \psi_n) \rightarrow \varphi$ in predicate calculus of size $\leq E_4(n)$. By Lemma 2.3, $(\psi_1^* \wedge \ldots \wedge \psi_n^*) \rightarrow \varphi^*$ has a special proof in T of size $\leq E_{c'+4}(n)$. By Lemma 2.6, $\psi_1^*,\ldots,\psi_n^*$ have special proofs

in T of size $\leq E_{c'}(n)$. Hence φ has a special proof in T of size $\leq E_{c'+5}(n)$. QED

LEMMA 2.8. There is an integer c' such that the following is provable in EFA. Let φ be an existential formula with a proof in T of size $\leq n$. Then φ has a special proof in T of size $\leq E_{c'}(n)$.

Proof: Let c' be the maximum of c and the constants given by Lemmas 2.2 and 2.7. Let $\varphi = (\exists x_1)(\exists x_2)...(\exists x_r)(\psi(x_1,...,x_r,y_1,...,y_m))$ have a proof in T of size n.

For $0 \leq j \leq r$, let $\varphi_j = (\exists x_{j+1})...(\exists x_r)(\psi(x_1,...,x_r,y_1,...,y_m))$. Then for $0 \leq j \leq r-1$, $\varphi_j{}^\star$ is the quantifier free equivalent of $(\exists x_{j+1})(\varphi_{j+1}{}^\star)$ given by H'. Note that each $\#(\varphi_j{}^\star) \leq \#(\varphi_0{}^\star)$, and so By Lemma 2.2, the $\varphi_j{}^\star$ all have sizes $\leq E_{c'}(\#(\varphi_0))$. And we have special proofs in T of the formulas

$\varphi_r{}^\star \rightarrow \varphi_r$
$(\exists x_r)(\varphi_{r-1}{}^\star \rightarrow \varphi_r{}^\star)$
$(\exists x_{r-1})(\varphi_{r-2}{}^\star \rightarrow \varphi_{r-1}{}^\star)$
...
$(\exists x_2)(\varphi_1{}^\star \rightarrow \varphi_2{}^\star)$
$(\exists x_1)(\varphi_0{}^\star \rightarrow \varphi_1{}^\star)$

of sizes $\leq E_d(\#\varphi_0{}^\star) \leq E_d(E_{c'}(\#(\varphi_0))) \leq E_{d+c'}(n)$. Note that $\varphi_r = \psi(x_1,...,x_r,y_1,...,y_m)$ and $\varphi_0 = \varphi$. Hence we have a special proof in T of $\varphi^\star \rightarrow \varphi$ of size $\leq E_{d+c'+1}(n)$.

By Lemma 2.7, $\varphi^\star$ has a special proof in T of size $\leq E_{c'}(n)$. Hence φ has a special proof in T of size $\leq E_{d+c'+2}(n)$. QED

LEMMA 2.9. There is an integer c' such that the following is provable in EFA. Assume T is a strong EFA qe existential theory. Let phi be a quantifier free formula with a proof in T of size n. Then phi has a special proof in the quantifier free part of T of size $\leq E_{c'}(n)$.

Proof: Let c' be the max of c,d and the constant given by Lemma 2.2. Let $\varphi(x_1,...,x_r)$ be as given, with a proof of size n. For $0 \leq j \leq r$, let $\varphi_j = (\forall x_{j+1})...(\forall x_r)(\varphi(x_1,...,x_r,y_1,...,y_m))$. Then for $0 \leq j \leq r-1$, $\varphi_j{}^\star$ is the negation of the quantifier free eqvuialent of $(\exists x_{j+1})(\neg\varphi_{j+1}{}^\star)$ given by H'. By Lemma 2.2, the each $\#(\varphi_j{}^\star) \leq \#(\varphi_0{}^\star) \leq E_{c'}(4n)$. We have special proofs in T of the formulas

$(\exists x_r)(\neg\varphi_{r-1}\star \rightarrow \neg\varphi_r\star)$
$(\exists x_{r-1})(\neg\varphi_{r-2}\star \rightarrow \neg\varphi_{r-1}\star)$
...
$(\exists x_2)(\neg\varphi_1\star \rightarrow \neg\varphi_2\star)$
$(\exists x_1)(\neg\varphi_0\star \rightarrow \neg\varphi_1\star)$

of sizes $\leq E_d(E_{c'+4}(n)) \leq E_{2c'+4}(n)$. Note that $\varphi_r = \varphi_r\star = \varphi$, and $\varphi_0 = (\forall x_1)...(\forall x_r)(\varphi_1,...,x_r,y_1,...,y_m))$. So $\varphi_r\star$ has a special proof in T of size $\leq n$. Therefore we successively obtain special proofs in T of $\varphi_{r-1}\star$, $\varphi_{r-2}\star$, ..., $\varphi_0\star$, of size $\leq E_{2c'+5}(n)$.

We now use that T is a strong EFA qe existential theory. We have special proofs in T of the formulas

$\neg\varphi_r\star \rightarrow \neg\varphi r-1\star$
$\neg\varphi_{r-1}\star \rightarrow \neg\varphi_{r-2}\star$
...
$\neg\varphi_1\star \rightarrow \neg\varphi_0\star$

in the quantifier free part of T of sizes $\leq E_{2c'+4}(n)$. Hence we have a special proof of $\varphi_0\star \rightarrow \varphi_r\star = \varphi$ in the quantifier free part of T of size $\leq E_{2c'+5}(n)$.

Now $\varphi_0\star$ is a quantifier free sentence. Hence there is a special proof in the quantifier free part of T of either $\varphi_0\star$ or $\neg\varphi_0\star$ of size $\leq E_c(\#\varphi_0\star) \leq E_{c'+1}(n)$. Since there is a special proof of $\varphi_0\star$ in T, and T is specially consistent, we see that there is a special proof in the quantifier free part of T of $\varphi_0\star$ of size $\leq E_{c'+1}(n)$. Hence there is a special proof in the quantifier free part of T of φ of size $\leq E_{2c'+6}(n)$. QED

LEMMA 2.10. There is an integer c' such that the following is provable in EFA. Let φ be a formula. There is a proof of φ iff $\varphi\star$ in T of size $\leq E_{c'}(\#(\varphi))$.

Proof: Let c' be the maximum of c and the constant given by Lemma 2.2. We prove by induction that for every formula phi, there is a proof of φ iff $\varphi\star$ in T of size $\leq E_{c'+(\#(\varphi))}$. Let φ be given and assume that this is true for all psi with $\#(\psi) \leq \#(\varphi)$. If φ is atomic then this is trivial. If $\varphi = \neg\psi$ then there is a proof of ψ iff $\psi\star$ in T of size $\leq E_{c'+(\#(\psi))}$. Hence there is a proof of φ iff $\varphi\star$ in T of size $\leq E_{c'+(\#(\varphi))}$. If $\varphi = \psi$ or ρ then there is a proof of ψ iff $\psi\star$ in T of size $\leq E_{c'+(\#(\psi))}$ and a proof of ρ iff $\rho\star$ in T of size $\leq E_{c'+(\#(\rho))}$. These can be

combined to give a proof of φ iff φ^* in T of size $\leq E_{c'+(\#(\varphi))}$. The conjunction and implication cases are handled analogously.

Suppose $\varphi = (\exists x)(\psi)$. Then φ^* is the quantifier free equivalent of $(\exists x)(\psi^*)$ given by H'. Hence there is a proof of ψ^* iff $(\exists x)(\psi^*)$ in T of size $\leq E_{c'+4}(\#(\psi^*)) \leq E_{2c'+4}(\#(\psi))$. By induction hypothesis, there is a proof of ψ iff ψ^* in T of size $\leq E_{2c'+4}(\#(\psi))$. Hence there is a proof of phi iff φ^* in T of size $\leq E_{2c'+4}(\#(\varphi))$.

Finally suppose $\varphi = (\forall x)(\psi)$. Then $\varphi^* = \neg((\exists x)(\neg\psi)^*)$, which is the negation of the quantifier free equivalent of $(\exists x)(\neg\psi^*)$ given by H'. Hence there is a proof of ρ iff $(\exists x)(\neg\psi^*)$ in T of size $\leq E_{c'+4}(\#(\neg\psi^*)) <= E_{2c'+4}(\#(\psi))$, where $\psi^* = \neg\rho$. By induction hypothesis, there is a proof of ψ iff ψ^* in T of size $\leq E_{2c'+4}(\#(\psi))$. Hence there is a proof of $\neg\rho$ iff $(\forall x)(\psi)$ in T of size $\leq E_{2c'+4}(\#(\varphi))$. QED

We have now shown the following.

THEOREM 2.11. Let T be an EFA qe existential theory. Then EFA proves that every existential formula provable in T has a special proof in T. And EFA proves that every formula is provably equivalent, in T, to a quantifier free formula. Let T be a strong EFA qe existential theory. Then EFA proves that T is consistent. EFA proves that every quantifier free formula provable in T has a special proof in the quantifier free part of T. And EFA proves that every sentence is provable or refutable in T.

Proof: From the above. QED

We can also state a sharper version, which we have also proved.

THEOREM 2.12. Let T be an EFA qe existential theory. There is an integer constant c' such that the following are provable in EFA. Every existential formula with a proof in T of size n has a special proof in T of size $\leq E_{c'}(n)$. For every formula φ, there is a quantifier free formula ψ such that ψ iff ψ has a proof in T of size $\leq E_{c'}(\#(\varphi))$. Let T be a strong EFA qe existential theory. There is an integer constant c' such that the following are provable in EFA. Every quantifier free formula with a proof in T of size n has a special proof in the quantifier free part of T of size $\leq E_{c'}(n)$. Every sentence

φ is provable or refutable in T by a proof of size ≤ $E_{c'}(\#(\varphi))$.

3. CONSISTENCY AND COMPLETENESS OF ALGEBRAICALLY CLOSED FIELDS

We formulate the field axioms FLD in the signature $0,1,\bullet,-,/$ with =, as follows.

1. $a+0 = 0$, $a+b = b+a$, $a+(b+c) = (a+b)+c$, $a+(-a) = 0$.
2. $a\bullet 0 = 0$, $a\bullet 1 = a$, $a\bullet b = b\bullet a$, $a\bullet(b\bullet c) = (a\bullet b)\bullet c$.
3. $a\bullet(b+c) = a\bullet b + a\bullet c$, $a/0 = 0$, $b \neq 0 \rightarrow b\bullet(a/b) = a$.
4. $1 \neq 0$, $a\bullet b = 0 \rightarrow (a = 0 \vee b = 0)$.

FLD(0) consists of FLD together with the axioms

5. $1+1+...+1 \neq 0$, where there is at least one 1.

Let p be a prime. FLD(p) consists of FLD together with the axioms

6. $1+1+...+1 \neq 0$, where there are at least one but fewer than p 1's.
7. $1+1+...+1 = 0$, where there are p 1's.

Whenever we write FLD(p), it is understood that p is either a prime or 0.

In the context of fields, we will frequently write terms of the form

$$t_0 x^n + t_1 x^{n-1} + ... + t_{n-1}x + t_n$$

where $t_0,...,t_n$ are terms not mentioning x. It is understood that the addition is associated to the left and $t_i x^{n-i}$ is $t_i(x x \quad x)$, where there are n-i x's associated to the left. Of course, in the presence of the field axioms, such details make no difference. However, we need to be specific, particularly in connection with section 3 where we consider semifields that do not universally satisfy the field axioms.

If p is a prime or 0, then we write ACF(p) for FLD(p) plus the root axioms

$$(\exists x)(x^n + c_1 x^{n-1} + ... + c_{n-1}x + cn = 0)$$

where n ≥ 1 and the c's are variables other than x.

LEMMA 3.1. ACF(0) is an EFA qe existential theory with constant 4. Moreover, clause iv) in the definition of strong EFA qe existential theory holds, with constant 4.

Proof: This kind of information is implicit in the well known work on elimination of quantifiers that yield decision procedures that are elementary recursive, thus improving Tarski's original elimination of quantifiers. We will provide self contained details in the next draft of this paper. QED

We want to show that ACF(0) is a strong EFA qe existential theory with constant c = 4. It remains to verify clauses i) - iii) in that definition.

LEMMA 3.2. (EFA) ACF(0) is specially consistent in the sense that there is no special proof of any quantifier free formula and its negation.

Proof: Let X be an iterated instantiation of ACF(0). It suffices to give an interpretation of X where the variables that are not witnesses are assigned 0. Let p be a prime greater than the number of 1's used in any axiom of the form 1+1...+1 not= 0 that appears in X.

We start with the finite field Z_p. Then make finitely many successive field extensions according to the construction of X', in the standard way that is used in ordinary field theory to construct the algebraic closure of Z_p. Note that these field extensions are finite and of at most double exponentiatial size, so that they can be constructed within EFA. QED

LEMMA 3.3. (EFA) If φ is a quantifier free sentence in the signature of fields, then there is a special proof of phi or of notphi of size ≤ $E_4(\#(\varphi))$ using only the quantifier free axioms of ACF(0).

Proof: By straightforward induction on $\#(\varphi)$. QED

We have now proved the following.

LEMMA 3.4. ACF(0) is a strong EFA qe existential theory.

We also want to treat the characteristic p case. We want to prove in EFA that certain properties of ACF(p) hold for all primes p. This is stonger than saying that for all primes p, EFA proves certain properties of ACF(p).

In order to get such uniformity, we need to expand the concept of (strong) EFA (qe) existential theory to that of a (strong) EFA (qe) existential theory family.

An EFA existential theory family $T*$ consists of a finite signature, an integer constant $c \geq 1$, and a Turing machine TM, such that EFA proves

i) TM accepts or rejects inputs in time bounded by $E_c(x)$;
ii) TM accepts only pairs consisting of an integer $k \geq 0$ and an existential formula in the signature.

For all $n \geq 0$, proofs and special proofs in $T*[k]$ refer to proofs and special proofs in the set of all existential formulas φ in the signature for which (k,φ) is accepted by TM.

We say that $T*$ is an EFA qe existential theory family if and only if $T*$ is an EFA existential theory with constant c such that the following is provable in EFA. For all $k \geq 0$, the following holds:

Let $(\exists x)(\varphi(x,y_1,\ldots,y_n))$ be a formula in the signature of $T*$, where φ is quantifier free, $x,y_1,\ldots,y_n$ are distinct variables, and all variables in φ are among those shown. There is a quantifier free $\psi(y_1,\ldots,y_n)$ with all variables among those shown and special proofs of

$$\varphi(x,y_1,\ldots,y_n) \rightarrow \psi(y_1,\ldots,y_n)$$

and

$$(\exists x)(\psi(y_1,\ldots,y_n) \rightarrow \varphi(x,y_1,\ldots,y_n))$$

in $T*[k]$ of size $\leq 2\wedge[\log(\#(phi))\wedge E_c(n+k)]$.

We say that $T*$ is a strong EFA qe existential theory family if and only if

i) $T*$ is an EFA existential theory with integer constant c;

ii) EFA proves that T* is specially consistent in the sense that there is no special proof in T of any quantifier free formula and its negation;

iii) EFA proves that for all k, if phi is a quantifier free sentence in the signature of T*[k], then there is a special proof of phi or of notphi in T*[k] of size $\leq E_c(\#(\varphi))$ using only the quantifier free elements of T*[k];

iv) the following is provable in EFA. For all k ≥ 0, the following holds:

Let $(\exists x)(\varphi(x, y_1, \ldots, y_n))$ be a formula in the signature of T*, where φ is quantifier free, $x, y_1, \ldots, y_n$ are distinct variables, and all variables in φ are among those shown. There is a quantifier free $\psi(y_1, \ldots, y_n)$ with all variables among those shown and special proofs of

$$\varphi(x, y_1, \ldots, y_n) \rightarrow \psi(y_1, \ldots, y_n)$$

and

$$(\exists x)(\psi(y_1, \ldots, y_n) \rightarrow \varphi(x, y_1, \ldots, y_n))$$

in T*[k] of size $\leq 2^{\wedge}[\log(\#(\varphi))^{\wedge}E_c(n+k)]$, where the first special proof uses only the quantifier free formulas in T*[k].

We can view the ACF(p), p prime, as an EFA existential theory family T* in the obvious way. Here it is convenient to take T*(n) to be ACF(n) if n is prime; ACF(0) otherwise. We write this EFA existential theory family as ACF*.

LEMMA 3.5. ACF* is a strong EFA qe existential theory.

Proof: This is proved analogously to Lemma 3.4. A new point is a uniform proof that ACF(p), p prime, is specially consistent within EFA. The proof is the same as that proof of Lemma 3.2, where p is obviously given and doesn't have to be chosen. QED

Theorems 2.10 and 2.11 have obvious generalizations to EFA existential theory families T*.

THEOREM 3.6. Let T* be an EFA qe existential theory. Then EFA proves that for all k, every existential formula provable in T*[k] has a special proof in T*[k]. And EFA proves that for all k, every formula is provably equivalent, in T*[k], to a

quantifier free formula. Let T* be a strong EFA qe existential theory. Then EFA proves that for all k, T*[k] is consistent. EFA proves that for all k, every quantifier free formula provable in T*[k] has a special proof in the quantifier free part of T*[k]. And EFA proves that for all k, every sentence is provable or refutable in T*[k].

Proof: From the above. QED

We can also state a sharper version.

THEOREM 3.7. Let T* be an EFA qe existential theory. There is an integer constant c′ such that the following is provable in EFA. For all k, every existential formula with a proof in T*[k] of size n has a special proof in T*[k] of size $\leq E_{c'}(n)$. For all k, every formula φ, there is a quantifier free formula ψ such that φ iff ψ has a proof in T*[k] of size $\leq E_{c'}(\#(\varphi)+k)$. Let T* be a strong EFA qe existential theory. There is an integer constant c′ such that the following is provable in EFA. For all k, every quantifier free formula with a proof in T*[k] of size n has a special proof in the quantifier free part of T*[k] of size $\leq E_{c'}(n+k)$. For all k, every sentence φ is provable or refutable in T*[k] by a proof of size $\leq E_{c'}(\#(\varphi)+k)$.

We can apply Theorems 3.6 and 3.7 to ACF(0), to ACF(p) for any specific prime p, and to ACF* in the obvious way.

THEOREM 3.8. (EFA) Let p be a prime or 0. ACF(p) is consistent and complete, and conservative over FLD(p) for quantifier free formulas. Every existential formula provable in ACF(p) has a special proof in ACF(p). Also, there exists a positive integer c such that EFA proves the preceding statements with upper bounds using the function E_c.

4. COMPLETENESS OF OF REAL CLOSED FIELDS WITH INTERMEDIATE VALUE THEOREM

In this section we take much of the previous development into the context of real closed fields. There are several axiomatizations of real closed fields that we need to consider here. They are well known to be equivalent (in the appropriate sense) using unrestricted methods. We need the more delicate arguments of this paper to establish their equivalence in EFA.

One of these axiomatizations, RCFI, is based on the intermediate value theorem, and is the axiomatization that is normally used for elimination of quantifiers in the context of real closed fields.

The aim of this section is to carry out the previous development of this paper for RCFI, except for issues of consistency. The consistency of RCFI is not proved until section 6.

FLD(<) is the usual theory of ordered fields, whose signature is the signature of fields together with the binary relation symbol <. The axioms are as follows.

1. FLD.
2. < is a strict linear ordering of the domain, where $0 < 1$.
3. $(x > 0 \ \& \ y > 0)$ implies $x+y > 0 \ \& \ x \bullet y > 0$.

RCFI is the theory of real closed fields based on the intermediate value theorem for polynomials. Its signature is the signature of ordered fields. The axioms are as follows.

1. FLD(<).
2. (therexists y)$(x > 0$ implies $y^2 = x)$.
3. (therexists x)$((b < c \wedge P(b) < u < P(c))$ implies $b < x < c$ $\& \ P(x) = u)$, where $P(x)$ is $x^n + a_1 x^{n-1} + ... + a_{n-1}x + a_n$, $n \geq 1$.

Note that FLD(<) is the quantifier free part of the existential theory RCFI.

LEMMA 4.1. RCFI is an EFA qe existential theory with constant 4. Moreover, clause iv) in the definition of strong EFA qe existential theory holds, with constant 4.

Proof: This kind of information is implicit in the well known work on elimination of quantifiers that yield decision procedures that are elementary recursive, thus improving Tarski's original elimination of quantifiers. We will provide self contained details in the next draft of this paper. QED

LEMMA 4.2. EFA proves that if phi is a quantifier free sentence in the signature of RCFI, then there is a special proof of phi or of notphi in FLD(<) of size $\leq E_c(\#(\varphi))$.

Proof: Straightforward induction. QED

LEMMA 4.3. Suppose EFA proves the special consistency of RCFI. Then RCFI is a strong EFA qe existential theory with constant 4.

Proof: From Lemmas 4.1 and 4.2. QED

We can immediately conclude the following, using Theorems 2.11 and 2.12.

THEROEM 4.4. (EFA) RCFI is complete. Every existential formula provable in RCFI has a special proof in RCFI. If RCFI is specially consistent then RCFI is consistent, and is a conservative extension of FLD(p) for quantifier free formulas. Also, there exists a positive integer c such that EFA proves the preceding statements with upper bounds using the function E_c.

Thus obtaining the provability in EFA of the special consistency of RCFI is crucial.

5. SPECIAL CONSISTENCY OF REAL CLOSED FIELDS

The weakest commonly considered theory of real closed fields is RCF, whose signature is the same as that of fields, and whose axioms are as follows.

1. FLD.
2. $(\exists y)(y^2 = x \lor y^2 = -x)$.
3. $x_1^2 + \ldots + x_n^2 \neq -1$, where $n \geq 1$.
4. $(\exists x)(x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n = 0)$, where n is odd.

We let RF be the subsystem consisting of axioms 1 and 3. RF is the quantifier free part of RCF.

In this section we prove the special consistency of RCF in EFA; i.e., that $0 = 0$ does not have a special proof in RCF. But in order to apply Theorem 4.4, we need to prove the special consistency of RCFI in EFA. That is achieved in section 6.

It is convenient to introduce finite approximations to fields. We take this to be a special case of the following more general construction.

Let M be a finite relational structure in a finite relational type, with a distinguished subset of the domain that we always write as A. We inductively define M[0] = A, and M[i+1] to be the elements of M[i] together with all values of the functions of M at arguments from M[i].

Let d ≥ 0 and phi be a quantifier free formula in the language of M. We say that φ is d-true in M if and only if phi holds for all assignments from M[d] to the variables appearing in φ.

We apply these concepts to the language of fields, =,0,1,+,-,•,/.

Let d ≥ 0. A d-semifield is a relational structure in the language of fields in which the field axioms are d-true.

A d-real semifield is a d-semifield in which the statement

$$x_1^2 + \ldots + x_d^2 \neq -1$$

written left associatively, is d-true.

LEMMA 5.1. (EFA) For all d ≥ 0, there is a d-real semifield.

Proof: Set D to be the set of all values in the rationals of the field terms with no variables, of depth at most 2d+3. Note that D is of double exponential size rather than of indefinitely iterated exponential size, so that there is no trouble handling it within EFA. Set A = {0,1}. Define the four operations from D in the standard way. If we are thrown out of D then set the value to be 0. QED

LEMMA 5.2. (EFA) Let d ≥ 16 and M = (D,A,0,1,+,-,•,/) be a 16d-real semifield. Let a be an element of M[d] that is not the left associative sum of d squares of elements of M[6d]. Then there is a d-real semifield M' = (D',A',0,1,+', -',•',/') extending M and x in A' such that $x^2 = -a$.

Proof: We will adjoin a root x to the equation $x^2 = -a$ in the manner normally done in field theory. If $x^2 = -a$ has a solution x in M[15d], then take M' to be the same as M with x thrown into A'. Note that M'[d] containedin M[16d]. Hence M' is as required. So we assume otherwise.

We take D' to be the expressions px + q, where p,q lie in D. We can view D as the subset of D' where p = 0. Set A' = A ∪ {x} = A ∪ {1•x + 0}. +' and -' are defined in the obvious way. Multiplication and divison are defined in the standard way modulo x^2 + a via long division for polynomials in M. The usual laws may not hold when the coefficients bump up against the "top" of M[16d]. But we can ignore this and get values anyways. And if division by zero occurs, then this is fine since we have a default value of 0.

A tedious calculation shows that if p,q,r,s lie in M[i], i ≤ 15d, then the operations of M' applied to px + q and rx + s have coefficients in M[d+i+4].

Suppose (px + q) •' (rx + s) = 0, where the displayed coefficients lie in M[14d]. We wish to show p = q = 0 or r = s = 0. When computed normally in M, (px + q)(rx + s) is a constant multiple of x^2 + a, where the coefficients lie in M[14d+4] and the constant factor lies in M[14d+5]. If the constant factor is 0 then p = q = 0 or r = s = 0, and we are done. Assume the constant factor is nonzero. If p is nonzero then x = -(q/p) is a solution to x^2 = -a lying in M[15d], which is a contradiction. Hence p = 0. This is a contradiction.

We conclude that all of the field axioms are true in M' for all expressions whose coefficients lie in M[14d]. Note that all coefficients of all elements of M'[3d] lie in M[14d]. Therefore M' is a 3d-semifield.

Now suppose that

$(p_1x + q_1)^2$ +' ... +' $(p_dx + q_d)^2$ = -1

holds in M', where the sum is computed left associatively, the squares are in terms of •', and where the coefficients lie in M'[d] containedin M[5d]. We wish to obtain a contradiction.

We are well within the "good" part of M and M', so that various elementary algebraic manipulations are valid, and we see that

$(p_1x + q_1)^2$ + ... + $(p_dx + q_d)^2$ + 1

computed as a polynomial in M is divisible by x^2 + a by long division in M. All of the sums, differences, products, and divisions that we will use below will lie in M[6d].

There cannot be any cross terms, and so for each i, either p_i = 0 or q_i = 0. So the left side is of the form px^2 + q, where p,q are sums of squares in M. Thus px^2 + q+1 is divisible by x^2 + a by long division in M. Hence q+1 = pa. Now p is nonzero since M is a 16d-real semifield. Hence a = q/p + 1/p, and so a is a sum of d squares of elements of M[6d], which is a contradiction. QED

LEMMA 5.3. (EFA) Let d ≥ 16 and M = (D,A,0,1,+,-,•,/) be a 16d-real semifield. Let a in M[d]. Then there is a d-real semifield M' = (D',A',0,1,+',-',•',/') extending M and x in A' such that x^2 = a or x^2 = -a.

Proof: We can assume that a is not 0. By Lemma 5.2, it suffices to assume that a and -a are both the left associative sum of d squares of elements of M[6d] and obtain a contradiction. By adding the two equations, we see that 0 is the sum of 2d squares of elements of M[6d], where at least one term is nonzero. We can then divide the equation by that nonzero square and obtain -1 as a sum of 2d squares of elements of M[7d]. This is impossible since M is a 16d-real semifield. QED

LEMMA 5.4. (EFA) Let d ≥ 32 and M = (D,A,0,1,+,-,•,/) be a $16d^4$-real semifield. Let 1 ≤ i ≤ d-2 and P1(x),...,Pd(x),Q(x) be polynomials of degree ≤ d with coefficients from M[16d^3(d-1)]. Let Q(x) be of odd degree. Then $P_1(x)^2$ + ... + $P_d(x)^2$ + 1 is not divisible by Q(x) by long division in M.

Proof: Let $P_i'(x)$ be the remainder resulting from long division in M of Q(x) into Pi(x). Then the coefficients of the $P_i'(x)$ lie in M[16d^3(i) + d^2]. Since $P_1(x)^2$ + ... + $P_d(x)^2$ + 1 is divisible by Q(x) by long division in M, we see that $P_1'(x)^2$ + ... + $P_d'(x)^2$ + 1 is divisible by Q(x) by long division in M. The result of that long division, $Q_1(x)$, has coefficients from M[16d^3(i) + 2d^2].

Write $P_1'(x)^2$ + ... + $P_d'(x)^2$ = $Q_1(x)Q(x)$. The P_i' have degrees < deg(Q).

We claim that the degree of the left side is even. To see this, let j be the highest of the degrees of the Pi'. The

coefficient of x^j in the expansion of the left side must be
a sum of squares of elements of M[16d^3(i+1)], at least one
of which is nonzero. Therefore the sum must be nonzero since
M is a $16d^4$-real semifield.

So the degree of the left side is even and < 2deg(Q). Hence
deg(Q_1) < deg(Q) and odd.

Therefore we can repeat this process, obtaining an equation
of the form

$P_1''(x)^2$ + ... + $P_d''(x)^2$ = $Q_2(x)Q_1(x)$,

where the Pi'' have degress < deg(Q_1), and deg(Q_2) < deg(Q_1)
is odd, all coefficients of the Pi'' lie in M[16d^3i + $3d^2$],
and all coefficients of Q2(x) lie in M[16d^3i + $4d^2$]. Note
that this process will continue for more than d steps. This
is because the coefficients involved stay in M[16d^3(i+1)]
for more than d steps, and the relevant sums of nonzero
squares are nonzero. But at every stage in the process, the
degree drops. This is a contradiction. QED

LEMMA 5.5. (EFA) Let d ≥ 32 and M = (D,A,0,1,+,-,•,/) be a
$16d^4$-real semifield. Let P(x) be a polynomial in one variable
of odd degree ≤ d with coefficients from M[d]. Then there is
a d-real semifield M' = (D',A',0,1,+',-',•',/') extending M
and x in A' such that P(x) = 0.

Proof: We define a sequence of polynomials Q(x) as follows.
Write P(x) = Q(x)R(x), where Q,R are of nonzero degree, and
their coefficients lie in M[$16d_3$]. Set Q1(x) to be the factor
of odd degree. Write Q1(x) = Q(x)R(x), where Q,R are of
nonzero degree, and their coefficients lie in M[16d^3(2)].
Set $Q_2(x)$ to be the factor of odd degree. Continue in this
way, raising the M-level by $16d^3$ each time, until the required
factorization does not exist. Thus process cannot go on for
more than d/2 steps because P has degree at most d, and we
drop degree by at least 2 at each stage.

We have obtained a polynomial S(x) and 1 ≤ i ≤ d-8 such that

i) S(x) is of odd degree d' ≤ d with coefficients from
M[16di];
ii) S(x) cannot be written as a product of two polynomials of
nonzero degree whose coefficients lie in M[16d^3(i+1)];

iii) if M' is any d-real semifield extending M and x is an element of A' such that S(x) = 0, then P(x) = 0.

The first two claims are immediate. The third claim follows by following the chain of equations in the construction of S(x) back from the end in which S(x) appears on the right side to the beginning equation P(x) = Q(x)R(x).

S(x) has a strong enough irreducibility property for us to adjoin a root of Q(x) in essentially the same way we would in ordinary field theory. Condition iii) tells us that it is sufficient to adjoin a root of S(x).

We take D' to be the polynomials R(x) of degree < d' with coefficients from D. We view D as a subset of D' consisting of the elements of D' of degree 0. We let A' = A $\cup$ {x}, where x is viewed as such a polynomial. +',-' are defined in the obvious way. Multiplication and division are defined in the standard way modulo S(x) via long division for polynomials in M. The usual laws may not hold when the coefficients bump up against the "top" of $M[16d^4]$. But we can ignore this and get values anyways. And if division by zero occurs, then this is fine since we have a default value of 0.

A tedious calculation shows that if $R_1(x),R_2(x)$ have coefficients from M[j], j $\leq$ 16d^3(d-1), then the operations of M' applied to $R_1(x),R_2(x)$ have coefficients from M[16d^3i + j+4d].

Suppose $R_1(x)$ •' $R_2(x)$ = 0, where $R_1(x),R_2(x)$ have nonzero degrees < d', and all their coefficients lie in M[16d^3i + d^3]. We will obtain a contradiction. This will establish that "no zero divisors" is 16d^3(i+1)-true in M'.

Apply the Euclidean algorithm to $R_1(x)$ and S(x) in order to compute the "gcd" in M. All relevant coefficients will stay within M[16d^3i + 2d^3]. The "gcd" so computed must in fact be a common divisor of $R_1(x)$ and $S_1(x)$ by algebraic manipulations where the relevant coefficients remain in M[16d^3i + 3d^3]. According to ii), this gcd computed in M must be of degree zero. But R1(x) must divide all of the remainders in the Euclidean algorithm accoding to polynomial division in M. Carrying out the algebra explicitly produces coefficients staying within M[16d^3i + 4d^3]. This is a contradiction.

We conclude that all of the field axioms are true in M' for all polynomials of degree < d' whose coefficients lie in $M[16d^{3i} + d^3]$. Note that all coefficients of all elements of $M'[16d]$ lie in $M[16d^{3i} + d$^3]. Therefore M' is a 16d-semifield.

Now suppose that

$(T_1(x))^2 +' \ldots +' (T_d(x))^2 = -1$

holds in M', where the sum is computed left associatively, the squares are in terms of ', and where the coefficients of the T's lie in $M'[d]$ containedin $M[16d^{3i} + d^3]$. We wish to obtain a contradiction.

We are well within the "good" part of M and M', so that various elementary algebraic manipulations are valid, and we see that

$(T_1(x))^2 + \ldots + (T_d(x))^2 + 1$

computed as a polynomial in M is divisible by S(x) by long division in M. All of the relevant coefficients involved in this algebra lie in $M[16d$^3(i+1)]. This contradicts Lemma 2.5. Thus we have shown that M' is a d-real semifield. QED

LEMMA 5.6. (EFA) Let X be an iterated instantiation of axioms 2 and 4 of RCF, and n ≥ 1. There is an n-real semifield M = (D,A,0,1,+,-,•,/) and an interpretation of X in which the variables are assigned elements of A.

Proof: Let X and n be given. It is convenient to let X' be essentially the same iterated instantiation of axioms 2 and 4 of RCF, but with some modifications:

i) every variable whose first appearance in X' is not as a witness is replaced by 0;
ii) the equations in the instances of axiom 4 being witnessed are put in polynomial form P(x) = 0, where x is the variable being existentially quantified and P is a polynomial in x whose coefficients are terms not mentioning x.

We claim that it suffices to establish the result for X'. Modification i) merely amounts to a predetermination of part of the interpretation being sought for X. Modification ii)

preserves the values of the terms in any n-real semifield where n is sufficiently large.

Now let n ≥ 2 be larger than
a) the length of X'; i.e., the number of formulas witnessed;
b) the depth of all terms used for coefficients in the polynomials occurring in X';
c) the degrees of the polynomials occurring in X'.

For $i,m \geq 1$, let $h_1(m) = 16m^4$, $h_{i+1}(m) = h_1(h_i(m))$. By Lemma 4.1, let M_0 be any $h_n(n)$-real semifield. If the first axiom witnessed in X' is an instance of axiom 2, then the term we are witnessing the square root of (or its negative) is closed and its value lies in $M_0[n]$ containedin $M_0[h_{n-1}(n)]$. We can apply Lemma 4.3 to obtain an $h_{n-1}(n)$-real semifield M1 extending M_0 and assign the witness to be an element of the A1 of M_1. If the first axiom witnessed in X' is an instance of axiom 3, then the terms that serve as coefficients are closed and their values lie in $M_0[h_{n-1}(n)]$. We can apply Lemma 4.5 to again obtain an $h_{n-1}(n)$-real semifield M_1 extending M_0 and assign the witness to be an element of the A_1 of M_1.

If the second axiom witnessed in X' is an instance of axiom 2, then the term we are witnessing the square root of (or its negative) mentions only the first witness and its value lies in $M_1[n]$ containedin $M_1[h_{n-2}(n)]$. We can apply Lemma 4.3 to obtain an $h_{n-2}(n)$-real semifield M_2 extending M_1 and assign the witness to be an element of the A_2 of M_2. If the first axiom witnessed in X' is an instance of axiom 3, then the terms that serve as coefficients mention only the first witness and their values lie in $M_1[h_{n-2}(n)]$. We can apply Lemma 4.5 to again obtain an $h_{n-2}(n)$-real semifield M_2 extending M_1 and assign the witness to be an element of the A_2 of M_2.

We continue this construction in this manner obtaining a tower of structures $M_0 \subseteq M_1 ... \subseteq M_n$, where each M_i is an $h_{n-i}(n)$-real semifield, and M_0 is an n-real semifield. The witnesses get assigned to be elements of $A_1 \subseteq A_2 ... \subseteq M_n$. And the binary function hi(m) is easily handled within EFA. QED

LEMMA 5.7. (EFA) Let X be an iterated instantiation of RCF, and n ≥ 1. There is an n-real semifield M = (D,A,0,1,+,-,•,/) and an interpretation of X in which the variables are assigned elements of A. There is no special proof in RCF of 0 ≠ 0.

Proof: This follows immediately from Lemma 5.6. The instantiations of axioms 1 and 3 obviously hold in the construction in the proof of Lemma 5.6. QED

LEMMA 5.8. (EFA) Let X be an iterated instantiation of RCF whose first variables introduced are by term substitution and are $x_1,...,x_r$ without repetition, and let $n \geq 1$. Let M_0 be any m-real semifield, where m is sufficiently large relative to X and n. Assume that $x_1,...,x_r$ have been assigned elements of A_0. Then there exists $M_0 \subseteq ... \subseteq M_n$, where M_n is an n-real semifield, and X has an interpretation extending the interpretation of $x_1,...,x_r$. Furthermore, there is an integer constant $c \geq 1$ such that, provably in EFA, we can take $m = E_c(\#(X)+n)$.

Proof: This is proved completely analogously to Lemma 5.7. QED

THEOREM 5.9. (EFA) RCF is specially consistent; i.e., there is no special proof in RCF of $0 \neq 0$. A quantifier free formula has a special proof in RCF if and only if it has a special proof in RF. There is an integer constant $c \geq 1$ such that the following is provable in EFA. Let φ be a quantifier free formula. If there is a special proof of φ in RCF of size n then there is a special proof in RF of size $\leq E_c(n)$.

Proof: The first claim is by Lemma 5.7. For the remaining claims, let $\varphi(x_1,...,x_r)$ be as given. Assume that φ has a special proof in RCF of size n. Let X be the relevant instantiation of RCF. By Lemma 5.8, let m be so large that the following holds. Let M_0 be any m-real semifield. Assume that $x_1,...,x_r$ have been assigned elements of A_0. Then there exists $M_0 \subseteq ... \subseteq M_n$, where M_n is an n-real semifield, and X has an interpretation extending the interpretation of $x_1,...,x_r$. We can now construct a special proof of $\varphi(x_1,...,x_r)$ in RF. Simply take all substitution instances of axioms of RF involving only the variables $x_1,...,x_r$, of depth at most m. The estimate in Lemma 5.8 obviously carries over to this context. QED

We can obtain all of the desired properties of RCF and RF in the stronger metatheory EFA′ using the second to last claim in Theorem 1.7.

THEOREM 5.10. (EFA′) RCF is consistent and complete, and conservative over RF for quantifier free formulas. Every

existential formula provable in RCF has a special proof in RCF. Also, there exists a positive integer c such that EFA′ proves the preceding statements with upper bounds using the function E_c.

6. REDUCTION OF REAL CLOSED FIELDS FROM INTERMEDIATE VALUES TO COMPLEX ROOTS

We wish to obtain Theorem 5.10 with EFA instead of EFA′, and also with RCF replaced by other axiomatizations of real closed fields such as RCFI (with quantifier free part FLD(<)). We do this by establishing that well known relationships between RCF and RCFI are provable in EFA, and then applying Theorems 4.4 and 5.9.

We first establish the equivalence between RCF and RCF(fta). RCF(fta) is an axiomatization of real closed fields in the signature of fields based on the fundamental theorem of algebra, which asserts that every polynomial of nonzero degree has a root in the field of complexes.

In order to formulate the fundamental theorem of algebra in the signature of fields, note that we can view the field of complexes as pairs of field elements with the usual complex addition and multiplication. This can be proved to be a field just using FLD. The usual proof is a special proof in RF.

The axioms of RCF(fta) are as follows.

1. RF.
2. There exists a complex z such that $z^n + a_1 z^{n-1} + \ldots + a_{n-1} z + an = 0$. Here $n \geq 1$.

Note that 2 is stated with coefficients from the real field, and not more generally with coefficients from the complex numbers. However, this can be formally derived. Thus we take the axioms of RCF(fta′) to be

1. RF.
2. There exists a complex z such that $z^n + a_1 z^{n-1} + \ldots + a_{n-1} z + a_n$, where the a's are complexes. Here $n \geq 1$.

LEMMA 6.1. There is a positive integer c such that the following is provable in EFA. Let phi be an axiom of RCF(fta′). Then phi has a special proof in RCF(fta) of size ≤ $E_c(\#(\varphi))$.

Proof: In EFA, we can formalize the usual proof of the underlying algebraic result which goes as follows. Let $P(z)$ be a monic polynomial of nonzero degree with complex coefficients. Let $Q(z)$ be obtained from $P(z)$ by conjugating the coefficients of $P(z)$. Then $P(z)Q(z)$ is a monic polynomial of nonzero degree with real coefficients, and so must have a root, z_0. Hence $P(z_0) = 0$ or $Q(z_0) = 0$. We may assume $Q(z_0) = 0$. Now $Q(z_0)$ is the conjugate of $P(z_0{*})$, where $z_0{*}$ is the conjugate of z_0. Hence P has the zero $z_0{*}$. QED

We need to interpret RCFI in RCF(fta). For this purpose, we introduce an equivalent of RCF(fta). A well known consequence of the fundamental theorem of algebra is that every polynomial of degree $n >= 1$ with real coefficients can be factored into linear and quadratic factors, the sum of whose degrees is n. This consequence does not mention complexes - all coefficients involved in the statement are real.

Thus we let RCF(fact) be in the signature of fields with the following axioms.

1. RF.
2. $(\exists y)(y^2 = x \lor y^2 = -x)$.
3. $x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + an$ can be factored into linear and quadratic factors, the sum of whose degrees is n. Here n ≥ 1.

LEMMA 6.2. There is a positive integer c such that the following is provable in EFA. Let φ be an axiom of RCF(fact). Then φ has a special proof in RCF(fta) of size $\leq E_c(\#(\varphi))$.

Proof: In EFA, we can formalize the usual proof of the underlying algebraic result which goes as follows. By using n long divisions, we can factor $x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n$ into a product of n linear factors in the complexes, $(x-z_1)(x-z2)\ldots(x-z_n)$. These z's are exactly the roots, perhaps with repetitions. Now the conjugate of a root must be a root of the conjugate polynomial, and so the conjugate of a root must be a root. Let i be least such that z_i is not real, and let z_j be the conjugate of z_i. Throw these two factors out. Since their product is real, the remaining product is a real polynomial of lower degree. Apply this process again and again, until we are left with only real factors. This shows that the z's come in conjugate pairs. Multiply all conjugate

pairs. This is the required factorization into real linear and real quadratic factors. QED

We now show in EFA that RCFI is contained in RCF(fact) in an appropriate strong sense. Note that the signature of RCFI is larger than the signature of RCF(fact).

Let φ be a formula in the signature of RCFI. The field interpretation of phi is the result of replacing every atomic subformula s < t in φ by (therexists x)(x not= 0 $\land$ t-s = x^2), where x is the first variable not appearing in s,t.

LEMMA 6.3. There is a positive integer c such that the following is provable in EFA. Let phi be an axiom of RCFI. The field interpretation of phi has a special proof in RCF(fact) of size $\leq E_c(\#(\varphi))$.

Proof: In EFA, we can formalize the usual proof of the underlying algebraic result which goes as follows. Let x <' y be $(\exists z)(z \neq 0 \land y-x = z^2)$. There is a special proof in RCF(fact) that <' is a linear ordering and 0 <' 1, and that <' provides an ordereed field. It remains to show that there is a special proof in RCF(fact) of the intermediate value theorem for polynomials with respect to <'. It suffices to assume that the given polynomial is negative at a and postitive at b, where a < b, and show that it has a zero between a and b. By Lemma 6.2, we can factor the polynomial into linear and quadratic factors. Since we have a sign change from a to b, we must have a sign change in at least one factor from a to b. That factor must have a zero between a and b. QED

THEOREM 6.4. (EFA) If RCF(fta) is specially consistent then RCFI is specially consistent. There is a positive integer c such that the following is provable in EFA. Let φ be an axiom of RCFI. The field interpretation of phi has a special proof in RCF(fta) of size $\leq E_c(\#(\varphi))$.

Proof: From Lemmas 6.2 and 6.3. QED

We have already proved in section 5 that EFA proves the special consistency of RCF. In the next section we use this to show that EFA proves the special consistency of RCF(fta).

7. SPECIAL CONSISTENCY OF REAL CLOSED FIELDS WITH INTERMEDIATE VALUE THEOREM

We now prove the special consistency of RCFI. By Theorem 6.4, it suffices to prove the special consistency of RCF(fta) in EFA. In this section, we reduce the special consistency of RCF(fta) to the special consistency of RCF, within EFA. This is sufficient because we have already proved the special consistency of RCF within EFA (Theorem 5.9).

LEMMA 7.1. (EFA) Every axiom of RCF(fta) has a proof in RCF. There is a positive integer c such that EFA proves the following. Let phi be an axiom of RCF(fta). Then there is a proof in RCF of phi of size $\leq E_c(\#(\varphi))$.

Proof: We can use the proof of the fact that in a real closed field, adjoining i creates an algebraically closed field, in B.L. van der Waerden, Algebra, vol. 1, 7th edition, page 251, Springer Verlag, 1991. This can be turned into a formal proof in RCF of a complex root to any polynomial of degree n, where n >= 1 is fixed. One of the important steps is to formalize within RCF the root adjunction construction in terms of tuples of real closed field elements of specified size. QED

Note that Lemma 7.1 is not quite good enough since it is not a special proof in RCF.

LEMMA 7.2. (EFA) Every axiom of RCF(fta) has a special proof in RCF. There is a positive integer c such that EFA proves the following. Let phi be an axiom of RCF(fta). Then there is a special proof in RCF of phi of size $\leq E_c(\#(\varphi))$.

Proof: The natural proof has cuts. However, the cuts are applied to the assertion that certain polynomials have no zeros in certain field extensions defined by quantifier free formulas. So the cuts are applied to formulas with single quantifiers. Cut elimination can then be applied, with only an exponential blowup in the length of the proof. Alternatively, one can show that the natural proof uses only formulas of bounded complexity, where complexity is defined liberally. Then using the cut elimination theorem for the liberal definition of complexity - due to me and elaborated on by my Ph.D. student Leou in his Ph.D. thesis at OSU - one also can obtain a fixed length iterated exponential blowup. QED

LEMMA 7.3. (EFA) The field interpretation of every axiom of RCFI has a special proof in RCF. There is a positive integer

c such that EFA proves the following. Let φ be an axiom of RCFI. Then there is a special proof in RCF of the field interpretation of phi of size $\leq E_c(\#(\varphi))$.

Proof: By Lemmas 6.4 and 7.2. QED

THEOREM 7.4. (EFA) If RCF is specially consistent then RCFI is specially consistent. There is a positive integer c such that the following is provable in EFA. Let phi be an axiom of RCFI. The field interpretation of phi has a special proof in RCF(fta) of size <= Ec(#(phi)).

Proof: By Lemmas 6.4 and 7.3. QED

THEOREM 7.5. (EFA) RCF is consistent and complete, and conservative over RF for quantifier free formulas. Every existential formula provable in RCF has a special proof in RCF. Also, there exists a positive integer c such that EFA proves the preceding statements with upper bounds using the function Ec.

Proof: By Lemmas 4.4, 5.9, and Theroem 7.4.

THEROEM 7.6. (EFA) RCFI is consistent and complete, and conservative over FLD(<) for quantifier free formulas. Every existential formula provable in RCFI has a special proof in RCFI. Also, there exists a positive integer c such that EFA proves the preceding statements with upper bounds using the function Ec.

Proof: From Theroem 7.5 by the field interpretation of <. QED

We can also obtain the same results for RCF(lub), which is the theory of real closed fields in the signature of FLD(<), based on the least upper bound axiom scheme, which we state informally. The axioms are as follows.

1. FLD(<).
2. If a formula with parameters holds of no positive elements, then there is a least $x \geq 0$ such that it holds of no elements greater than x.

8. APPLICATION TO HILBERT'S 17TH PROBLEM

We can use the results of this paper to prove in EFA that every polynomial of several variables with rational

coefficients, which is nonnegative at all rational arguments, can be formally written as the sum of squares of rational functions with rational coefficients. And there is a positive integer c such that this statement is provable in EFA with the relevant estimate using the function E_c.

9. INTERPRETATIONS OF RCF AND FINITELY AXIOMATIZED EXTENSIONS IN EFA AND Q

There is an interpretation of the signature of fields into the signature of EFA such that EFA proves the interpretation of every theorem of RCF is a theorem of EFA. This can be done with a relatively mild estimate. And there is an interpretation of the signature of fields with a satisfaction relation into the signature of EFA such that the interpretation of every axiom of RCF with a satisfaction predicate (there are only finitely many) is a theorem of EFA.

It follows from general results of the author that there is an interpretation of RCF into Robinson's Q.

10. NEGATIVE RESULTS

The consistency of RCF cannot be proved in various weaker systems than EFA that are commonly considered. Specifically, systems based on subexponential functions such as $n^{\log(n)}$.

[1] S. Simpson and R. Smith, Factorization of polynomials and $\sum$-0-1 induction, Annals of Pure and Applied Logic 31 (1986), 289-306.