- $\mathbb{C}$ is classic model of ACF (char. 0)
- $\mathbb{R}$ famously $\not\models$ ACF
- also ACFs of finite char > 0.

- Note: ACF infinite collection of axioms
- unlike DLO, ACF not complete
- quant elim'n ⇒ completeness proof for DLO doesn't work for ACF — quite
- Difference is we have constants 0, 1 so there are q.f. sentences not equiv to $\top$ or $\bot$
- turns out important ones are those asserting $1+1+\cdots+1 = 0$ or $1+1+\cdots+1 \neq 0$ (i.e. defining characteristic of field)
- up to these, ACF is complete.

Theorem ACF has quantifier elim'n.

Pf: we verify isomorphism and submodel conditions

① Iso condition:
- Sps $A, B \models$ ACF w/ isomorphic substructures A_0, B_0 w/ isomorphism $\pi_0 : A_0 \to B$.

- WTS: there are $A_1, B_1 \models ACF$ extending A_0, B_0 w/ iso: $\pi_1 : A_1 \to B_1$ ext'n π_0 (isomorphic)
  ↳ follows from general facts about rings + algebraic closures

A sketch:

- first extend A_0 to unique minimal ring A_0' in A extending A_0 – ring axioms guarantee A_0' is unique
- likewise B_0 to B_0' and we get π_0' extending π_0 free
- now extend A_0' to unique minimal field A_0'' in A containing A_0'
- field axioms guarantee uniqueness
- likewise B_0' to B_0'', get $\pi_0'' : A_0'' \to B_0''$ for free
- finally extend A_0'' to algebraic closure A_1, likewise B_0'' to a.c.l. B_1 – field theory guarantees unique way to do this; again get $\pi_1 : A_1 \to B_1$ extending π_0 for free ✓

(e.g. if $A = \mathbb{C}$ and $A_0 = \mathbb{N}$ (min'l substructure in language $\{0,1,+,*\}$)

- unique min'l ring extending $\mathbb{N}$ is $\mathbb{Z}$
- " " field " " is $\mathbb{Q}$
- " " algebraically closed field " " is $\mathbb{Q}^{acl}$ – the minimal algebraically closed extension of $\mathbb{Q}$.

② Submodel condition

- Sps $A \leq B$ are both models of ACF
- Sps φ is simple: $\varphi := \exists x(\varphi_1 \wedge \dots \wedge \varphi_k)$ each φ_i atomic/negation of atomic.
- in this lang, terms t are poly's $f(x_1, \dots, x_k, x)$
- atomic formulas are $t = s$ (no relation symbols)
- hence every φ_i is equiv. to eq'n of form $f(x_1, \dots, x_n, x) = 0$ or $f(x_1, \dots, x_n, x) \neq 0$ where f a poly on n+1 variables w/ coefficients in "$\mathbb{Z}$" (i.e. all coeffs are k or $-k$ for some k, but if char $\neq 0$ not all $k \in \mathbb{Z}$ distinct)

now univariate

- Thus if $a_1, \dots, a_n \in A$ there are poly's $f_1, \dots, f_k, g_1, \dots, g_e$ w/ coeffs in A s.t.

$\mathcal{B} \models \varphi(a_1, .., a_n)$
iff $\exists b \in \mathcal{B}$ s.t. $f_1(b) = 0 \wedge .. \wedge f_k(b) = 0$
$\wedge g_1(b) \neq 0 \wedge .. \wedge g_\ell(b) \neq 0$

— likewise for $\mathcal{A} \models \varphi(a_1, .., a_n)$ but now w/ $\exists b \in \mathcal{A}$ ..

— if $K > 0$, any solution $b \in \mathcal{B}$ is a root of the polynomial $f_1 + .. + f_k$ hence must be in $\mathcal{A}$ since $\mathcal{A}$ is algebraically closed

↳ contains all roots of all poly's (repeatedly apply $\exists$ root axiom and strip off $(x - \alpha)$ factors)

— if $K = 0$ need following fact: every ACF is infinite

why? if only elements were $c_0, .., c_m$ then poly $\prod_{i \leq m} (x - c_i) + 1$ has no root.

— so if $K = 0$ and there is a solution in $\mathcal{B}$ (i.e. each g_i is not the 0 polynomial) (i.e. each g_i has finitely many roots) then there must be a solution in $\mathcal{A}$ as well ✓

- before leaving ACF, let's firm up a claim from above
- Def'n the <u>characteristic</u> of $A \models ACF$ is least n s.t. $\underbrace{1+1+\dots+1}_{n\text{-times}} = 0$, or 0 if no such n exists.

- basic fact: if char(A) $\neq 0$ then is a prime p.
- for a fixed p, either prime or 0, let ACF_p denote theory of ACF + axioms asserting char is p.

<u>Corollary</u> ACF_p is complete, and hence decidable.

<u>Pf sketch</u>: - ACF_p extends ACF, so also proves every sentence is equiv to a q.f. one
- What are the q.f. sentences in this lang?
- Not too hard to check: every q.f. sentence equiv to $\top$ or $\bot$ or $\underbrace{1+1+\dots+1}_{n\text{-times}} = 0$ or $1+1+\dots+1 \neq 0$
- but truth/falsity of each such sentences is decidable, just depends on whether $1+1+\dots+1 = 0$ is divis by p.

- Hence ACF_p is complete.
  ↳ follows ACF_p is decidable, but unlike in DLO, since our quantifier elimination isn't done algorithmically, to decide truth of sentence σ have to recursively output all proofs from ACF_p until get a proof of σ or $\neg\sigma$ (which terminates, by completeness). ✓

Real closed ordered fields

- Let now $L = \{<, +, \cdot, 0, 1\}$
- the axioms for real closed ordered fields (RCOFs) are:
  - axioms for fields
  - "$<$ is a linear order"
  - $\forall x, y, z \, (x < y \Rightarrow x + z < y + z)$
  - $\forall x \, (x > 0 \Rightarrow \exists y \, (x = y \cdot y))$
  - for every odd n the axiom "$\forall x_0 \ldots \forall x_n \, (x_n \neq 0 \Rightarrow \exists y (x_n y^n + \ldots + x_1 y + x_0 = 0))$"

e.g. $\mathbb{R} \models$ RCOF another example is $\mathbb{R}_{alg}$ = set of algebraic real numbers (a ctbl model!)

<u>Theorem</u> (Tarski) RCOF has quant. elim'n

- We will sketch the proof
- Take following two algebraic lemmas for granted

<u>Lemma #1</u>: Sps $A \models RCOF$. Then A satisfies the intermediate value theorem for polynomials, i.e. if $a, b \in A$, and f is a poly w/ coeffs in A, and $f(a) < 0 < f(b)$, then $\exists x \in A$ s.t. $f(x) = 0$ and x is between a, b.

<u>Lemma #2</u> Sps $A \leq B$ are both RCOFs and f is a poly w/ coeffs in A that has a root $b \in B$. Then in fact $b \in A$.

- With these, we outline proof of Tarski's ~~lemma~~ Theorem.

<u>Pf</u>: we check the isomorphism and submodel conditions for RCOF.

1. Isomorphism cond'n:
- Similar idea to ACFs: if A_0, B_0 are isomorphic substructures of $A, B \models RCOF$, there is a unique way to extend them to RCOFs A_1, B_1 and also the isomorphism $\pi_0 : A_0 \to B_0$ to $\pi_1 : A_1 \to B_1$

2. Submodel condition:
- Sps $A \leq B$ are RCOFs and $\varphi(x_1, .., x_n)$ is simple.
- Convince yourself: atomic/neg'n of atomic fmlas equiv to one of form poly $= 0$, poly $\neq 0$, poly > 0.
- Concretely, given $a_1, .., a_n \in A$, there are poly's (univariate, coeffs in A) $f_1, .. f_k, g_1, .., g_l, h_1, .., h_m$ s.t.

$$B \models \varphi(a_1, .., a_n) \quad \text{iff}$$
$$\exists b \in B \text{ s.t. } f_1(b) = 0 \wedge .. \wedge f_k(b) = 0$$
$$\wedge\, g_1(b) \neq 0 \wedge .. \wedge g_l(b) \neq 0$$
$$\wedge\, h_1(b) > 0 \wedge .. \wedge h_m(b) > 0$$

likewise for $A \models \varphi(a_1, .., a_n)$ but now with $\exists b \in A$

- WTS: if $\exists$ such a $b \in B$, then actually there is a sol'n in A.
- So sps $b \in B$ solves the system above.
- if $k > 0$ then b solves
  $(f_1 + \cdots + f_k)(b) = 0$ and hence $b \in A$ by Lemma #2.

- So assume $k = 0$ and $m > 0$ (if $m = 0$ can get sol'n as in ACF case since all RCOFs infinite - see below)

- may assume each h_i has root in B: if not, not only do we have $h_i(b) > 0$ but actually $h_i(x) > 0$ for all $x \in B$ and so for all $x \in A$, so any sol'n in A for the other conditions solves $h_i > 0$.

- enumerate all the roots of the h_i's in order: $a_0 < a_1 < \cdots < a_p$ (by Lemma #2 these roots are in A)

- Sps our sol'n satisfies $a_j < b < a_{j+1}$ (similar arg when $b < a_0$, $b > a_p$)
- by ~~[illegible]~~ Lemma #1, none of the h_i's change sign in the interval (a_j, a_{j+1}), hence any b' in this interval makes h_i's all > 0