- Now observe: A has infinitely many points in this interval: just repeatedly take midpoints $(a_j + a_{j+1})/2$ etc. a_j a_{j+1}
- midpoints exist by RCOF axioms and are in A since a_j, a_{j+1} are
- thus we can find some $c \in A \cap (a_j, a_{j+1})$ that makes all $g_j \neq 0$ ✓

<u>Corollary</u> RCOF is complete and hence decidable

<u>Pf</u>: - because of the order axiom $x<y \Rightarrow x+z<y+z$ it follows $\underbrace{1+1+1 \cdots +1}_{n\text{-times}} \neq 0$ for any n, i.e. all RCCFs have characteristic 0.

- let n denote $1+1+\cdots+1$ (n-times)
- not hard to check: all q.f. sentences equiv to one of form $n=0$, $n \neq 0$, $n>0$ and truth of all of these decided (same truth value as in $\mathbb{R}$)

$\Rightarrow$ RCCF is complete ✓

Presburger arithmetic

- We showed in 117b that $Th(\mathbb{N}, 0, S, +, \cdot, <)$ is undecidable and incomplete
- We also mentioned the fact: $+$ can be defined in $(\mathbb{N}, 0, S, \cdot, <)$ and so the theory of this structure is undecidable

- We are now going to show:
  $Th(\mathbb{N}, 0, S, +, <)$
  is decidable!
  ↳ follows: multiplication not definable in this structure.

- Let PrA ("Presburger Arithmetic") denote $Th(\mathbb{N}, 0, S, +, <)$

<u>Theorem</u> PrA is decidable.

- to prove theorem, need quant. elim'n result
- PrA itself doesn't have quant. elim'n
- e.g. the simple fmla
  $\exists y (x = y + y)$ "x is even"
  is not equiv. to a q.f. one over PrA.
- turns out this is essentially only obstacle.

- For each n, define the relation $\equiv_n$ on $\mathbb{N}$ by $k \equiv_n k'$ iff $k \equiv k \pmod{n}$
- Let $T = Th(\mathbb{N}, 0, S, +, \cdot, \equiv_2, \equiv_3, \dots)$

<u>Theorem</u> T has quantifier elim'n.

<u>Pf</u>: We first establish

<u>Lemma</u> Sps $t(x_1, \dots, x_n)$ is a term (in lang of T). Then T proves is $=$ to a term of the form

$$n + n_1 x_1 + \dots + n_k x_k$$

(where $n := \underbrace{S(S(\dots(S(0))\dots))}_{n\text{-times}}$

($n_i x_i$ denotes $\underbrace{x_i + \dots + x_i}_{n_i\text{-times}}$)

<u>Pf</u>: Induction on construction of fmlas.

- point is: if $t = t_1 + t_2 = (n + n_1 x_1 + \dots + n_k x_k) + (m + m_1 x_1 + \dots + m_k x_k)$

then T proves $t = (n+m) + (n_1 + m_1) x_1 + \dots + (n_k + m_k) x_k$ ✓

- We'll show T has quant elim'n by showing simple formulas are algorithmically (provably) equiv to q.f. fmlas

- Sps φ is simple: $\varphi := \exists x (\varphi_1 \wedge \dots \wedge \varphi_k)$
- each φ_i is atomic or neg'n of atomic, hence has form
  $t_1 = t_2$, $t_1 \neq t_2$, $t_1 < t_2$, $t_1 \not< t_2$,
  $t_1 \equiv_m t_2$, $t_1 \not\equiv_m t_2$

- We can rewrite $t_1 \not< t_2$ as $t_1 = t_2 \vee t_1 > t_2$ (i.e. is provably equiv) and $t_1 \not\equiv_m t_2$ as the disjunction of $t_1 \equiv_m t_2 + i$, for $i = 1, 2, \dots, m-1$

- as before can rewrite resulting formulas (inside the $\exists x$) in d.n.f., distribute the $\exists x$
- get fmla $\exists x(\dots) \vee \exists x(\dots) \vee \dots \vee \exists x(\dots)$ where each $(\dots)$ is conjunction of atomic fmlas (no neg'ns)
- thus sufficient to show each such equiv. to a q.f. fmla
- as much to say: may assume each φ_i is atomic (no neg'ns)

- rewriting each t_i in these φ_i using our lemma, can assume each φ_i specifically has form

$$nx + t \; R \; lx + s$$

where $R \in \{=, <, \equiv_2, \equiv_3, \ldots\}$ and t, s are terms not containing x

- can further rewrite to a (probably) equiv expression (depending on sign of $n-l$):

$$kx + t = s \quad (\text{or } t = kx + s \text{ — same tho})$$

$k = n - l$ or $l - n$

$$kx + t < s \quad \text{or} \quad t < kx + s \quad (\text{these diff})$$

$$kx + t \equiv_m s \quad (\text{or } t \equiv_m kx + s)$$

We finish proof in three steps

(1) let p be least common multiple of x in the φ_i

- replace each $kx + t = s$ term w/ $px + t' = s'$ (multiplying thru by p/k)
- replace each $kx + t < s$ w/ $px + t' < s'$
  $t < kx + s$ $\quad$ $t' < px + s'$

- replace each $kx + t \equiv_m s$ term w/ $px + t' \equiv_{m'} s'$

where $m' = \frac{p}{k} m$

(using fact that $a \equiv b \pmod{c}$ if <u>and only if</u> $al \equiv bl \pmod{cl}$)

↳ now coeff of x is p in every term.

2. - replace each appearance of px (in each φ_i) w/ new variable y to get φ_i'
i.e. each φ_i' of form
$y+t=s$, $y+t<s$, $t<y+s$, $y+t \equiv_m s$

- add the formula $y \equiv_p 0$ to our conj'n of the φ_i'
- note that new fmla
$\exists y(\varphi_1' \wedge \ldots \wedge \varphi_k' \wedge y \equiv_p 0)$
is really equiv to original
$\exists x(\varphi_1 \wedge \ldots \wedge \varphi_k)$

(e.g. $\exists x(kx+t=s) \Leftrightarrow \exists x(px+t'=s')$
$\Leftrightarrow \exists y(y+t'=s' \wedge y \equiv_p 0)$)

3. - if any φ_i' of first form $y+t=s$ can simply "substitute" the "term" $s-t$ for all other appearances of y and delete $\exists y$ at front to get q.f. equiv. fmla
(may need to rearrange: $s-t$ not always literally a term - can only use t's!)

- So assume no ψ_i' of first form
- So our fmla has form

$$\exists y \left(\bigwedge_i y + t_i < s_i \quad \wedge \quad \bigwedge_j t_j < y + s_j \quad \wedge \quad \bigwedge_k t_k \equiv_{m_k} s_k \right)$$

(the find $y \equiv_p 0$ occurs in last conj'n)

- Let us suppose for simplicity our fmla in fact has the form

$$\exists y \left(y + t_1 < s_1 \wedge t_2 < y + s_2 \wedge y \equiv_p 0 \right)$$

- We'll show this is equiv. to a q.f. fmla; leave as exercise to handle general case.

- First two conjuncts assert

$$t_2 - s_2 < y < s_1 - t_1$$

which is equiv to

$$t_2 - s_2 + 1 < s_1 - t_1$$

(cf.: may need to rewrite w/o $-$'s to get actual fmla)

- but in view of third conjunct, want to assert not only that $t_2 - s_2$ at least 2 below $s_1 - t_1$ ... but that there is a number divisible by p strictly between them — w/o using $\exists$!

- but this happens iff

$t_2 - s_2 + 1 < s_1 - t_1$ and $p \mid t_2 - s_2 + 1$

or $t_2 - s_2 + 2 < s_1 - t_1$ and $p \mid t_2 - s_2 + 2$

$\vdots$

or $t_2 - s_2 + p < s_1 - t_1$ and $p \mid t_2 - s_2 + p$

(- p cint w: only need div'n cf length p)

- i.e. above fmla is equiv to:

$$\bigvee_{1 \le i \le p} \left[(t_2 - s_2 + i < s_1 - t_1) \wedge (t_2 - s_2 + i \equiv_p 0) \right]$$

suitably rewritten w/o $-$'s
so we actually have formula ✓

Using that T has quant. elim'n can prove our claim that PrA is decidable.

Pf: - sps σ is a sentence in lang $\{<, S, +, 0\}$ of PrA
- then $T \vdash \sigma \Leftrightarrow \sigma^*$ where σ^* is q.f. in lang $\{<, S, +, 0, \equiv_2, \equiv_3, \ldots\}$

- want to decide if $T \vdash \sigma$ (i.e. if $\sigma \in T$) since $\sigma \in T$ iff $\sigma \in PrA$ (i.e. iff $PrA \vdash \sigma$)
  (... remember: T, PrA both the complete theories of arithmetic in their rsp. langs)

- atomic q.f. sentences in T's lang have form $n = k$, $n < k$, $n \equiv_m k$
  (as usual n means S applied to 0 n times)
  (really: each atomic sentence equiv. to one of these, might have $+$'s floating around)
- so σ^* a boolean combo of such
  (i.e. $\neg, \vee, \wedge$)
  atomic sentences

- ez to decide if $\sigma^* \in T$ — exactly if σ^* is true in $\mathbb{N}$, and can (write a program to) decide if each atomic sentence true in $\mathbb{N}$, and then whether a given boolean combo is true.

- hence can compute if $\sigma^* \in T$ and hence if $\sigma \in T$, and hence if $\sigma \in PrA$ ✓