117C

Class info:

Office hours: Tu/Th 2:30 – 4:00pm
Assessment: TBD (will post problems)

Outline of course

- more undecidability results
  incl. undecidability of word problem for groups
- some decidability! + quantifier elim'n
- formalizing computational complexity
- $P \overset{?}{=} NP$
- Parris – Harrington / independence results over PA
- Recursion theoretic forcing
- Some effective descriptive set theory.

More undecidable theories:

Recall: – theory T undecidable if $\langle \mathrm{Conseq}(T) \rangle$ undecidable (not recursive)
- structure $\mathcal{A}$ is strongly undecidable if every T s.t. $\mathcal{A} \models T$ is undecidable.
  ↳ we showed $\mathcal{N} = \langle \mathbb{N}, <, S, +, \cdot, 0 \rangle$ is strongly undecidable

- theorem if $\mathcal{A}$ definable in $\mathcal{B}$ (poss. w/ parameters) and $L_{\mathcal{A}}$ is finite then $\mathcal{B}$ is strongly undecidable.
  ↳ e.g. since in $\mathcal{Z} = \langle \mathbb{Z}, +, \cdot, 0, 1 \rangle$ can ~~define~~ define $\mathcal{N}$, $\mathcal{Z}$ str. undec.
  $\Rightarrow$ theory of rings str. undec.

- we also showed:
  $\exists$ strongly undec. group
  $\exists$ strongly undec. graph.

<u>More examples</u>:

<u>Def'n</u> a <u>poset</u> is a structure $\mathcal{P} = (P, <)$ where $<$ is a binary rel'n satisfying:

$\forall x,y,z \; (x<y \wedge y<z \Rightarrow x<z)$

$\forall x,y \; (x<y \Rightarrow (x \neq y \wedge y \not< x))$

If ~~every~~ every pair x, y has (unique) least upper bound and greatest lower bound, say $\mathcal{P}$ is a <u>lattice</u>

E.g. if X is any set, then $\mathcal{P} = (\mathcal{P}(X), \subsetneq)$ is a lattice, w/ l.u.b of $A, B \subseteq X$ given by $A \cup B$ and g.l.b given by $A \cap B$

Theorem There is a strongly undec. lattice. Hence the theory of lattices and the theory of posets is undecidable.

Pf: - Let $G = (V, E)$ be a str. undec. graph. We will construct a lattice in which G is definable.

- Let P be set of all subsets A of $V \cup E$ corresponding to subgraphs.

i.e. if an edge $(u,v) \in A$ then $u, v \in A$

- order P by strict inclusion $\subsetneq$
- since P closed under $\cup$ and $\cap$, forms a lattice (why?)
- Let $V' \subseteq P$ denote collection of all A s.t. $A = \{v\}$ for some vertex $v \in V$.
- Notice: V' definable by φ (w/ $\emptyset$ as parameter):

$$\varphi(A) := A \neq \emptyset \wedge \forall B \, (B < A \Rightarrow B = \emptyset)$$

- V' is one-one w/ V
- Now define a binary relation E' by ψ:

$A = \{u\}$
$B = \{v\}$
$C = \{u, v\}$
$D = \{u, v, (u,v)\}$

$$\psi(A,B) := \exists C, D \, [(A < C \wedge B < C \wedge C < D) \wedge \forall D' \, (D' < D \wedge \varphi(D') \Leftrightarrow D' = A \vee D' = B)]$$

Clearly, (V', E') is (definable) copy of $G = (V, E)$ in P ✓

Def'n A language L is non-trivial if L contains either a binary relation symbol, or binary function symbol, or two unary function symbols.

Theorem (Church) Sps L is a non-trivial language. Then the collection $Taut(L)$ of all tautologies of L is undecidable.

Pf: ① if $R \in L$ a binary rel'n symbol, we get a strongly undec. L-structure as follows:

- $G = (V, E)$ our str. undec. graph
- form L-structure w/ universe graph ✓
  - interpret R as E
  - interpret any other symbols arbitrarily
- (very) easy to define G in this structure ✓ why?

② if $f \in L$ bin. f'n symbol, same idea, but instead interpret f as characteristic function χ_E (choose two vertices v_0, v_1 to represent $0, 1$) ✓

③ If $d, r \in L$ are unary function symbols, also get strongly undec. structure:

- Let $B = V \cup E$ where $G = (V, E)$ our graph
- interpret d, r as following functions on B:

$$d(a) = r(a) = a \quad \forall a \in V$$
$$d((a,b)) = a \quad r((a,b)) = b \quad \forall (a,b) \in E$$

- interpret any other symbols arbitrarily
- V definable by fmla $d(x) = x$
- E definable by
$$e(x,y) := \exists z (d(z) \neq z \wedge d(z) = x \wedge \cancel{}\ r(z) = y)$$

✓

The word problem for groups:

Def'n A semigroup is a structure of the form $(S, *)$ where $*$ is an associative binary operation on S.

A monoid is a semigroup w/ an identity 1:
$$1 * s = s * 1 = s \quad \forall s \in S$$

A **group** is a monoid s.t. $\forall s \in S$ there is an inverse s^{-1} s.t. $ss^{-1} = s^{-1}s = 1$.

A **presentation** for a (finitely generated) semigroup is an expression of the form:

$$S = \langle a_1, \ldots, a_n \mid R_1, \ldots, R_k \rangle$$

where $A = \{a_1, \ldots, a_n\}$ is a set of generators and each R_i is eq'n of form $w_i = v_i$ where w_i, v_i are finite words in the letters $a_1, \ldots, a_n$ (in notation of 117a: $w_i, v_i \in A^*$)

The semigroup S defined by the presentation is the quotient $A^*/\sim$, where the operation is concatenation of words, and two words are considered equal under $\sim$ if one can be obtained from other by repeated application of the relations R_i

Similarly, the group defined by the presentation

$$G = \langle a_1, \ldots, a_n \mid R_1, \ldots, R_k \rangle$$

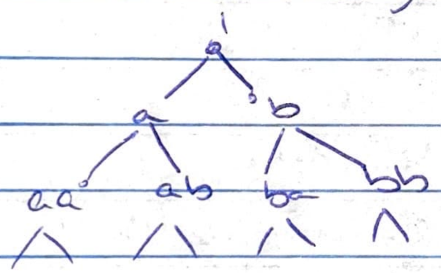
is the quotient $(A \cup A^{-1})^* / \sim$
where $A \cup A^{-1} = \{a_1, .., a_n, a_1^{-1}, .., a_n^{-1}\}$
operation is again concat'n and two words equiv. if can be translated using the R_i as well as the relations $a_i a_i^{-1} = a_i^{-1} a_i = 1$.

<u>Ex's</u> ① the semigroup presentation:

no rel'ns

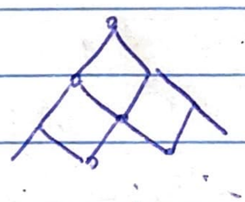
$$F_2^+ = \langle a, b \mid \emptyset \rangle$$

is the free semigroup on 2 generators
= all words in $\{a, b\}$ under concat'n



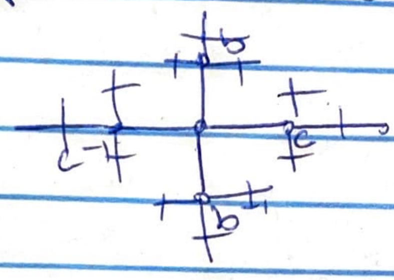
② whereas

$$A_2^+ = \langle a, b \mid ab = ba \rangle$$
= abelian free semigroup on $\{a, b\}$



3 CTGH: the group defined by:

$\mathbb{F}_2 = \langle a, b \mid \emptyset \rangle$ is the free group on $\{a,b\}$
$=$ all words in alphabet $\{a, a^{-1}, b, b^{-1}\}$
up to cancellations between inverses



The word problem

For semigroups: given a semigroup presentation

$$\langle a_1, \dots, a_n \mid R_1, \dots, R_k \rangle$$

find an algorithm that, given $w, v \in A^*$, determines if $w \sim v$ under the R_i.

For groups: analogous.

E.g. in $\mathbb{F}_2^+$ we have $w \sim v$ iff $w = v$ and certainly there is an algorithm to decide if two words equal.

Likewise in A_2^+, every word can be (algorithmically) rewritten in form $a^m b^n$.

So if $w = a^{m_1} b^{n_1}$ $v = a^{m_2} b^{n_2}$

then $w \sim v$ iff $m_1 = m_2$, $n_1 = n_2$

CTOH we have:

Theorem (Post, Markov) There are semigroups for which the word problem is undecidable.

What about groups?
In general, we also have undecidability but turns out this is much harder to show:

Theorem (Novikov, Boone) There are groups for which the word problem is undecidable.

Before proving Post-Markov and Boone-Novikov theorems need to develop theory of semi-Thue processes.

Let $A = \{a_1, \ldots, a_n\}$ be a finite alphabet

A semi-thue production is a pair of words (w, w'); write $w \to w'$

(is a "substitution rule")

A semi-Thue process Π is a finite list of productions P.

If P is $w \to w'$ and $u, v \in A^*$ we write $u \Rightarrow_P v$ if $u = xwy$ and $v = xw'y$ for some $x, y \in A^*$

Likewise $u \Rightarrow_\Pi v$ if there is $P \in \Pi$ s.t. $u \Rightarrow_P v$

Write $u \Rightarrow_\Pi^* v$ if there is a (finite) sequence of substitutions from Π turning u into v.

Word problem for Π: Is there an algorithm that, given $u, v \in A^*$, decides whether $u \Rightarrow_\Pi^* v$?

If yes: say Π is solvable

Facts (1) if $A = \{a\}$, then any Π is solvable

(2) if A is arbitrary, Π is a single rule, Π is solvable.