Complexity Theory
Computability
Charles E. Hughes
COT6410 – Spring 2023 Notes
Slides whose headers are italicized red are not required material
Computability

The study of models of computation and what can/cannot be done via purely mechanical means.
Goals of Computability

• Provide precise characterizations (computational models) of the class of effective procedures / algorithms.
• Study the boundaries between complete and incomplete models of computation.
• Study the properties of classes of solvable and unsolvable problems.
• Solve or prove unsolvable open problems.
• Determine reducibility and equivalence relations among unsolvable problems.
• Our added goal is to apply these techniques and results across multiple areas of Computer Science.
HISTORY

The Quest for Mechanizing Mathematics
Hilbert, Russell and Whitehead

• Until 1800’s there were no formal systems to reason about mathematical properties
• Major advances in late 1800’s/early 1900’s
• Axiomatic schemes
  – Axioms plus sound rules of inference
  – Much of focus on number theory
• First Order Predicate Calculus
  – $\forall x \exists y \ [y > x]$
• Second Order (Peano’s Axiom)
  – $\forall P \ [[P(0) \land \forall x[P(x) \implies P(x+1)]] \implies \forall xP(x)]$
In 1900 declared there were 23 really important problems in mathematics.

Belief was that the solutions to these would help address math’s complexity.

Hilbert’s Tenth asks for an algorithm to find the integral zeros of polynomial equations with integral coefficients. This is now known to be impossible (In 1970, Matiyasevič showed this undecidable).

Davis based on prior work by Julia Robinson, him and Hilary Putnam provided more readable proof in 1972.
Hilbert’s Belief

• All mathematics could be developed within a formal system that allowed the mechanical creation and checking of proofs.
Gödel

• In 1931 he showed that any first order theory that embeds elementary arithmetic is either incomplete or inconsistent.
• He did this by showing that such a first order theory cannot reason about itself. That is, there is a first order expressible proposition that cannot be either proved or disproved, or the theory is inconsistent (some proposition and its complement are both provable).
• Gödel also developed the general notion of recursive functions but made no claims about their strength.
Turing (Post, Church, Kleene)

• In 1936, each presented a formalism for computability.
  – Turing and Post devised abstract machines and claimed these represented all mechanically computable functions.
  – Church developed the notion of lambda-computability from recursive functions (as previously defined by Gödel and Kleene) and claimed completeness for this model.

• Kleene demonstrated the computational equivalence of recursively defined functions to Post-Turing machines.
• Church’s notation was the lambda calculus, which later gave birth to Lisp.
More on Emil Post

• In the 1920’s, starting with notation developed by Frege and others in 1880s, Post devised the truth table form we all use now for Boolean expressions (propositional logic). This was a part of his PhD thesis in which he showed the axiomatic completeness of the propositional calculus (all tautologies can be deduced from a finite set of tautologies and a finite set of rules of inference – substitution and modus ponens).

• In the late 1930’s and the 1940’s, Post devised symbol manipulation systems in the form of rewriting rules (precursors to Chomsky’s grammars). He showed their equivalence to Turing machines.

• In 1940s, Post showed the undecidability of determining what is derivable from an arbitrary set of propositional axioms.
Terminology and Context

Notation and Vocabulary
Procedures vs Algorithms

• Recall that Algorithms always Halt but Procedures Might Not for Some Input

• **Useful Notations**
  – $f(x)\downarrow$ means procedure $f$ converges/halts/produces an output, when evaluated at $x$.
  – $f(x)\uparrow$ means procedure $f$ diverges, when evaluated at $x$.
  – $f$ is an algorithm iff $\forall x \ f(x)\downarrow$
Sets and Decision Problems

• **Set** -- A collection of atoms from some universe $U$. $\emptyset$ denotes the empty set.

• **(Decision) Problem** -- A set of questions about elements of some universe. Each question has answer “yes” or “no”. The elements having answer “yes” constitute a set that is a subset of the corresponding universe. Those having answer “no” constitute the complement of the “yes” set.
Categorizing Problems (Sets)

• **Solvable or Decidable** -- A problem $P$ is said to be solvable (decidable) if there exists an algorithm $F$ which, when applied to a question $q$ in $P$, produces the correct answer ("yes" or "no"). This is an inherent property of $P$.

• **Solved** -- A problem $P$ is said to solved if $P$ is solvable and we have produced its solution. This is a temporal property in that $P$ may have been unsolved for many years before being solved.

• **Unsolved, Unsolvable (Undecidable)** -- Complements of above
Categorizing Problems (Sets) # 2

- **Recursively enumerable** -- A set $S$ is recursively enumerable (re) if $S$ is empty ($S = \emptyset$) or there exists an algorithm $F$, over the natural numbers $\mathbb{N}$, whose range is exactly $S$. A problem is said to be re if the set associated with it is re.

- **Semi-Decidable** -- A problem is said to be semi-decidable if there is an effective procedure $F$ which, when applied to a question $q$ in $P$, produces the answer “yes” if and only if $q$ has answer “yes”. $F$ need not halt if $q$ has answer “no”.

- Semi-decidable is the same as the notion of recognizable used in the text.
Immediate Implications

• $P$ solved implies $P$ solvable implies $P$ semi-decidable (re, recognizable).
• $P$ non-re implies $P$ unsolvable implies $P$ unsolved.
• $P$ finite implies $P$ solvable.
Slightly Harder Implications

• \( P \) enumerable iff \( P \) semi-decidable.
• \( P \) solvable iff both \( S_P \) and \( (U - S_P) \) are re (semi-decidable).

• We will prove these later.
Existence of Undecidables

• A counting argument
  – The number of mappings from $N$ to $N$ is at least as great as the number of subsets of $N$. But the number of subsets of $N$ is uncountably infinite ($\mathbb{N}_1$). However, the number of programs in any model of computation is countably infinite ($\mathbb{N}_0$). This latter statement is a consequence of the fact that the descriptions must be finite and they must be written in a language with a finite alphabet. In fact, not only is the number of programs countable, it is also effectively enumerable; moreover, its membership is decidable.

• A diagonalization argument
  – Will be shown later in class
Hilbert’s Tenth

Diophantine Equations are Unsolvable
One Variable Diophantine Equations are Solvable
Hilbert’s 10th

• In 1900 declared there were 23 really important problems in mathematics.
• Belief was that the solutions to these would help address math’s complexity.
• Hilbert’s Tenth asks for an algorithm to find the integral roots of polynomials with integral coefficients. For example $6x^3yz^2 + 3xy^2 \quad - \quad x^3 \quad - \quad 10 = 0$ has roots $x = 5$; $y = 3$; $z = 0$
• This is now known to be impossible to solve (In 1970, Matiyasevič showed this undecidable).
Hilbert’s 10th is Semi-Decidable

• Consider over one variable: \( P(x) = 0 \)
• Can semi-decide by plugging in 0, 1, -1, 2, -2, 3, -3, …
• This terminates and says “yes” if \( P(x) \) evaluates to 0, eventually. Unfortunately, it never terminates if there is no \( x \) such that \( P(x) = 0 \).
• Can easily extend to \( P(x_1, x_2, \ldots, x_k) = 0 \).
$P(x) = 0$ is Decidable

- $c_n x^n + c_{n-1} x^{n-1} + \ldots + c_1 x + c_0 = 0$
- $x^n = -(c_{n-1} x^{n-1} + \ldots + c_1 x + c_0)/c_n$
- $|x^n| \leq c_{\text{max}}(|x^{n-1}| + \ldots + |x| + 1|)/|c_n|$
- $|x^n| \leq c_{\text{max}}(n \ |x^{n-1}|)/|c_n|$, since $|x| \geq 1$
- $|x| \leq n \times c_{\text{max}}/|c_n|$
\( P(x) = 0 \) is Decidable

- Can bound the search to values of \( x \) in range \( [\pm n \times (\frac{c_{\text{max}}}{c_n})] \), where
  \( n \) = highest order exponent in polynomial
  \( c_{\text{max}} \) = largest absolute value coefficient
  \( c_n \) = coefficient of highest order term
- Once we have a search bound and we are dealing with a countable set, we have an algorithm to decide if there is an \( x \).
- Cannot find bound when more than one variable, so cannot extend to \( P(x_1, x_2, \ldots, x_k) = 0 \).
Undecidability

We Can’t Do It All
Classic Unsolvable Problem

Given an arbitrary program $P$, in some language $L$, and an input $x$ to $P$, will $P$ eventually stop when run with input $x$?

The above problem is called the “Halting Problem.” It is clearly an important and practical one – wouldn't it be nice to not be embarrassed by having your program run “forever” when you try to do a demo?

Unfortunately, there’s a fly in the ointment as one can prove that no algorithm can be written in $L$ that solves the halting problem for $L$. 
Some terminology

We will say that a procedure, \( f \), converges on input \( x \) if it eventually halts when it receives \( x \) as input. We denote this as \( f(x) \downarrow \).

We will say that a procedure, \( f \), diverges on input \( x \) if it never halts when it receives \( x \) as input. We denote this as \( f(x) \uparrow \).

Of course, if \( f(x) \downarrow \) then \( f \) defines a value for \( x \). In fact we also say that \( f(x) \) is defined if \( f(x) \downarrow \) and undefined if \( f(x) \uparrow \).

Finally, we define the domain of \( f \) as \( \{ x \mid f(x) \downarrow \} \).
The range of \( f \) is \( \{ y \mid f(x) \downarrow \text{ and } f(x) = y \} \).
We typically discuss procedures over the Natural Numbers. The Greek symbol μ, μ, is read “the least value.” Specifically, \( \mu y \ [ P(y) ] \), is read “the least of \( y \) such that \( P(y) \) is true. If \( P(y) \) is never true, then \( f(x) = \mu y \ [ P(y) ] \) always diverges. A simple example is \( \uparrow(x) = \mu y \ [ y = y+1 ] \). Note \( \uparrow \) as procedure name.

If \( P(y) \) is true somewhere then we have an algorithm. We often have a second argument here as in \( g(x) = \mu y \ [ P(x,y) ] \). The domain of \( g \) is the set of values, \( x \), for which \( g(x) \) diverges. The range of \( g \) is the union of the set of values it produces for all input.
The universal machine

First, we can all agree that any complete model of computation must be able to simulate programs in its own language. We refer to such a simulator (interpreter) as the Universal machine, denoted **Univ** or sometimes $\varphi$.

This program gets two inputs. The first is a description of the program to be simulated and the second is the input to that program. Since the set of programs in a model is re, we will assume both arguments are natural numbers; the first being the index of the program. The list of programs is $\varphi_0$, $\varphi_1$, $\varphi_2$, …

$$\text{Univ}(x,y) = \varphi(x,y) = \varphi_x(y)$$

We might use any of these notations
Halting Problem

Given procedure index \( x \) and input \( y \), does \( \phi_x (y) \downarrow \\

Assume we can decide the halting problem. Then there exists some total function \( \text{Halt} \) such that

\[
\text{Halt}(x,y) =
\begin{cases} 
1 \text{ (TRUE)} & \text{if } \phi_x (y) \downarrow \\
0 \text{ (FALSE)} & \text{if } \phi_x (y) \uparrow 
\end{cases}
\]

Now we can view \( \text{Halt} \) as a mapping from \( \mathbb{N} \) into \( \mathbb{N} \) by treating its input as a single number representing the pairing of two numbers via the one-one onto function

\[
\text{pair}(x,y) = <x,y> = 2^x (2y + 1) - 1
\]

with inverses

\[
<z>_1 = \log_2(z+1) \\
<z>_2 = (((z + 1) / 2 <z>_1 ) - 1) / 2
\]
If $\text{Halt}$ exist we can create this “lazy” evaluation. Consider diagonal and a procedure defined by

$\text{Disagree}(x) = \mu y \ [ \text{not Halt}(x,x)]$.

So $\text{Disagree}(x)=0$ iff $\varphi_x(x) \uparrow$ and $\text{Disagree}(x) \uparrow$ iff $\varphi_x(x) \downarrow$.

If $\text{Halt}$ exists then so does $\text{Disagree}$ and it is the $d$-th row for some $d$.

But then $\varphi_d(d) \downarrow$ iff not $\text{Halt}(d,d)$ iff $\varphi_d(d) \uparrow$.

<table>
<thead>
<tr>
<th>$\varphi/x$</th>
<th>0</th>
<th>1</th>
<th>.</th>
<th>.</th>
<th>.</th>
<th>$x$</th>
<th>.</th>
<th>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\varphi_0$</td>
<td>$\varphi_0(0) \downarrow$?</td>
<td>$\varphi_0(1) \downarrow$?</td>
<td></td>
<td></td>
<td></td>
<td>$\varphi_0(x) \downarrow$?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\varphi_1$</td>
<td>$\varphi_1(0) \downarrow$?</td>
<td>$\varphi_1(1) \downarrow$?</td>
<td></td>
<td></td>
<td></td>
<td>$\varphi_1(x) \downarrow$?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\varphi_x$</td>
<td>$\varphi_x(0) \downarrow$?</td>
<td>$\varphi_x(1) \downarrow$?</td>
<td></td>
<td></td>
<td></td>
<td>$\varphi_x(x) \downarrow$?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The Contradiction in Text

Now if $\text{Halt}$ exist, then so does $\text{Disagree}$, where

$$
\begin{align*}
\text{Disagree}(x) &= \mu y \left[ \text{not Halt}(x,x) \right] \\
&\uparrow \quad \text{if Halt}(x,x), \text{i.e., if } \varphi_x(x) \uparrow \\
&\downarrow \quad \text{if not Halt}(x,x), \text{i.e., if } \varphi_x(x) \downarrow 
\end{align*}
$$

Since $\text{Disagree}$ is a program from $\mathbb{N}$ into $\mathbb{N}$, $\text{Disagree}$ can be reasoned about by $\text{Halt}$. Let $d$ be such that $\text{Disagree} = \varphi_d$, then

$\text{Disagree}(d)$ is defined $\iff$ not Halt($d,d$) $\iff$ $\varphi_d(d) \uparrow$

$\iff$ $\text{Disagree}(d)$ is undefined

But this means that $\text{Disagree}$ contradicts its own existence. Since every step we took was constructive, except for the original assumption, we must presume that the original assumption was wrong.

Thus, $\text{Halt}$ does not exist and the Halting Problem is not solvable.
Halting is recognizable

While the Halting Problem is not solvable, it is re, recognizable or semi-decidable.
To see this, consider the following semi-decision procedure. Let $P$ be an arbitrary procedure and let $x$ be an arbitrary natural number. Run the procedure $P$ on input $x$ until it stops. If it stops, say “yes.” If $P$ does not stop, we will provide no answer. This semi-decides the Halting Problem. Here is a procedural description.

```plaintext
Semi_Decide_Halting() {
    Read P, x;
    P(x);
    Print “yes”;
}
```
Non-re Problems

- There are even “practical” problems that are worse than unsolvable -- they’re not even semi-decidable.
- The classic non-re problem is the **Uniform Halting Problem**, that is, the problem to decide of an arbitrary effective procedure $P$, whether or not $P$ is an algorithm.
- Assume that the algorithms can be enumerated, and that $F$ accomplishes this. Then

$$F(x) = A_x$$

where $A_0, A_1, A_2, \ldots$ is a list of indexes of all and only the algorithms
### Picture Proof

<table>
<thead>
<tr>
<th>F/x</th>
<th>0</th>
<th>1</th>
<th>.</th>
<th>.</th>
<th>.</th>
<th>x</th>
<th>.</th>
<th>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A₀</td>
<td>A₀(0)</td>
<td>A₀(1)</td>
<td>.</td>
<td>.</td>
<td>.</td>
<td>A₀(x)</td>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td>A₁</td>
<td>A₁(0)</td>
<td>A₁(1)</td>
<td>.</td>
<td>.</td>
<td>.</td>
<td>A₁(x)</td>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td>.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aₓ</td>
<td>Aₓ(0)</td>
<td>Aₓ(1)</td>
<td>.</td>
<td>.</td>
<td>.</td>
<td>Aₓ(x)</td>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td>.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If F exist we can create this “lazy” evaluation. Consider diagonal and an algorithm G defined by

\[ G(x) = \text{Univ}(F(x), x) + 1 = \varphi_{F(x)}(x) = A_x(x) + 1 \]

If F exists then so does G and it is the g-th row for some g.

But then \( G(g) = A_g(g) + 1 = G(g) + 1 \)

As G is an algorithm, this is a contradiction, So F does not exist.
The Contradiction in Text

• Define $G(x) = \text{Univ}(F(x), x) + 1 = \varphi_{F(x)}(x) = A_x(x) + 1$

• But then $G$ is itself an algorithm. Assume it is the $g$-th one

  $F(g) = A_g = G$

Then, $G(g) = A_g(g) + 1 = G(g) + 1$

• But then $G$ contradicts its own existence since $G$ would need to be an algorithm.

• This cannot be used to show that the effective procedures are non-enumerable, since the above is not a contradiction when $G(g)$ is undefined. In fact, we already have shown how to enumerate the procedures, also known as the (partial) recursive functions.
Consequences

• To capture all the algorithms, any model of computation must include some procedures that are not algorithms.

• Since the potential for non-termination is required, every complete model must have some form of iteration that is potentially unbounded.

• This means that simple, well-behaved for-loops (the kind where you can predict the number of iterations on entry to the loop) are not sufficient. While or repeat loops are needed, even if implicit (recursion) rather than explicit.
Insights
Non-re nature of algorithms

• No generative system (e.g., grammar) can produce descriptions of all and only algorithms
• No parsing system (even one that rejects by divergence) can accept all and only algorithms
• Of course, if you buy Church’s Theorem, the set of all procedures can be generated. In fact, we can build an algorithmic acceptor of such programs.
Many unbounded ways

• How do you achieve divergence, i.e., what are the various means of unbounded computation in each of our models?

• GOTO: Turing Machines and Register Machines

• Minimization: Recursive Functions
  – Why not just simple finite iteration or well-behaved recursion?

• Fixed Point: Ordered Petri Nets, (Ordered) Factor Replacement Systems
Non-determinism

• It sometimes doesn’t matter
  – Turing Machines, Finite State Automata,
    Linear Bounded Automata

• It sometimes helps
  – Push Down Automata

• It sometimes hinders
  – Factor Replacement Systems, Petri Nets
Models of Computation

Turing Machines
Register Machines
Factor Replacement Systems
Recursive Functions
Turing Machines

1st Model
A Linear Memory Machine
Typical Textbook Description

• A Turing machine is a 7-tuple
  \((Q, \Sigma, \Gamma, \delta, q_0, q_{\text{accept}}, q_{\text{reject}})\)
• \(Q\) is finite set of states
• \(\Sigma\), is a finite input alphabet not containing the blank symbol \(\sqcup\)
• \(\Gamma\) is finite set of tape symbols that includes \(\Sigma\) and \(\sqcup\) commonly \(\Gamma = \Sigma \cup \{\sqcup\}\)
• \(\delta: Q \times \Gamma \rightarrow Q \times \Gamma \times \{R,L\}\)
• \(q_0\) starts, \(q_{\text{accept}}\) accepts, \(q_{\text{reject}}\) rejects
Turing versus Post

- The Turing description just given requires you to write a new symbol and move off the current tape square.
- Post had a variant where \( \delta: Q \times \Gamma \rightarrow Q \times (\Gamma \cup \{R,L\}) \).
- Here, you either write or move, not both.
- Also, Post did not have an accept or reject state – acceptance is giving an answer of 1; rejection is 0; this treats decision procedures as predicates (functions that map input into \{0,1\}).
- The way we stop our machines from running is to omit actions for some discriminants making the transition function partial.
- I tend to use Post’s notation and to create macros so machines are easy to present.
- I am not a fan of having you build Turing tables.
Basic Description

• We will use a simplified form that is a variant of Post’s models.
• Here, each machine is represented by a finite set of states $Q$, the simple alphabet $\{0,1\}$, where $0$ is the blank symbol, and each state transition is defined by a 4-tuple of form $q a X s$
  where $q a$ is the discriminant based on current state $q$, scanned symbol $a$; $X$ can be one of $\{R, L, 0, 1\}$, signifying move right, move left, print 0, or 1; and $s$ is the new state.
• Limiting the alphabet to $\{0,1\}$ is not really a limitation. We can represent a $k$-letter alphabet by encoding the $j$-th letter via $j$ 1’s in succession. A 0 ends each letter, and two 0’s ends a word.
• We rarely write quads. Rather, we typically will build machines from simple forms.
Base Machines

- R -- move right over any scanned symbol
- L -- move left over any scanned symbol
- 0 -- write a 0 in current scanned square
- 1 -- write a 1 in current scanned square
- We can then string these machines together with optionally labeled arc.
- A labeled arc signifies a transition from one part of the composite machine to another, if the scanned square’s content matches the label. Unlabeled arcs are unconditional. We will put machines together without arcs, when the arcs are unlabeled.
Useful Composite Machines

\( R \) -- move right to next 0 (not including current square)

\[ \ldots \text{?}11\ldots10\ldots \Rightarrow \ldots \text{?}11\ldots10\ldots \]

\( L \) -- move left to next 0 (not including current square)

\[ \ldots011\ldots1\text{?}\ldots \Rightarrow \ldots011\ldots1\text{?}\ldots \]

© UCF CS
Commentary on Machines

• These machines can be used to move over encodings of letters or encodings of unary based natural numbers.

• In fact, any effective computation can easily be viewed as being over natural numbers. We can get the negative integers by pairing two natural numbers. The first is the sign (0 for +, 1 for -). The second is the magnitude.
Computing with TMs

A reasonably standard definition of a Turing computation of some \( n \)-ary function \( F \) is to assume that the machine starts with a tape containing the \( n \) inputs, \( x_1, \ldots, x_n \) in the form

\[
\ldots01^{x_1}01^{x_2}0\ldots01^{x_n}0\ldots
\]

and ends with

\[
\ldots01^{x_1}01^{x_2}0\ldots01^{x_n}01^{y_0}\ldots
\]

where \( y = F(x_1, \ldots, x_n) \)

Why matters – Composition, e.g.,

\[
y = G(x_1, \ldots, x_n, F(x_1, \ldots, x_n))
\]
Addition by TM

Need the copy family of useful submachines, where $C_k$ copies $k$-th preceding value.

The add machine is then

$$\begin{array}{c}
C_2 \ C_2 \ L \ 1 \ R \ L \ 0
\end{array}$$
Turing Machine Variations

• Two tracks
• N tracks
• Non-deterministic *********
• Two-dimensional
• K dimensional
• Two stack machines
• Two counter machines
Register Machines

2\textsuperscript{nd} Model
Feels Like Assembly Language
Register Machine Concepts

• A register machine consists of a finite length program, each of whose instructions is chosen from a small repertoire of simple commands.

• The instructions are labeled from 1 to m, where there are m instructions. Termination occurs as a result of an attempt to execute the m+1-st instruction.

• The storage medium of a register machine is a finite set of registers, each capable of storing an arbitrary natural number.

• Any given register machine has a finite, predetermined number of registers, independent of its input.
Computing by Register Machines

• A register machine partially computing some n-ary function \( F \) typically starts with its argument values in registers 1 to \( n \) and ends with the result in the 0-th register.

• We extend this slightly to allow the computation to start with values in its \( k+1 \)-st through \( k+n \)-th register, with the result appearing in the \( k \)-th register, for any \( k \), such that there are at least \( k+n+1 \) registers.
Register Instructions

• Each instruction of a register machine is of one of two forms:
  \( \text{INC}_r[i] \) –
  increment \( r \) and jump to \( i \).
  \( \text{DEC}_r[p, z] \) –
  if register \( r > 0 \), decrement \( r \) and jump to \( p \)
  else jump to \( z \)
• Note, we do not use subscripts if obvious.
Addition by RM

Addition \( r_0 \leftarrow r_1 + r_2 \)

1. DEC0[1,2] : Zero result \( r_0 \) and work \( r_3 \) registers
2. DEC3[2,3]
3. DEC1[4,6] : Add \( r_1 \) to \( r_0 \), saving original \( r_1 \) in \( r_3 \)
4. INC0[5]
5. INC3[3]
6. DEC3[7,8] : Restore \( r_1 \)
7. INC1[6]
8. DEC2[9,11] : Add \( r_2 \) to \( r_0 \), saving original \( r_2 \) in \( r_3 \)
9. INC0[10]
10. INC3[8]
11. DEC3[12,13] : Restore \( r_2 \)
13. : Halt by branching here

In many cases we just assume registers, other than those with input, are zero at start. That would remove the need for instructions 1 and 2.
Limited Subtraction by RM

Subtraction (r0 ← r1 - r2, if r1≥r2; 0, otherwise)

1. DEC0[1,2] : Zero result (r0) and work (r3) registers
2. DEC3[2,3]
3. DEC1[4,6] : Add r1 to r0, saving original r1 in r3
4. INC0[5]
5. INC3[3]
6. DEC3[7,8] : Restore r1
7. INC1[6]
8. DEC2[9,11] : Subtract r2 from r0, saving original r2 in r3
9. DEC0[10,10] : Note that decrementing 0 does nothing
10. INC3[8]
11. DEC3[12,13] : Restore r2
13. : Halt by branching here
Factor Replacement Systems

3rd Model
Deceptively Simple
Factor Replacement Concepts

• A factor replacement system (FRS) consists of a finite (ordered) sequence of fractions, and some starting natural number $x$.

• A fraction $a/b$ is applicable to some natural number $x$, just in case $x$ is divisible by $b$. We always chose the first applicable fraction $(a/b)$, multiplying it times $x$ to produce a new natural number $x*a/b$. The process is then applied to this new number.

• Termination occurs when no fraction is applicable.

• A factor replacement system partially computing $n$-ary function $F$ typically starts with its argument encoded as powers of the first $n$ odd primes. Thus, arguments $x_1,x_2,...,x_n$ are encoded as $3^{x_1}5^{x_2}...p_n^{x_n}$. The result then appears as the power of the prime 2.
Addition by FRS

Addition is 3x15x2 becomes 2x1+x2
or, in more details, 203x15x2 becomes 2x1+x2 3050

2 / 3
2 / 5

Note that these systems are sometimes presented as rewriting rules of the form

bx → ax

meaning that a number that has can be factored as bx can have the factor b replaced by an a.
The previous rules would then be written

3x → 2x
5x → 2x
Limited Subtraction by FRS

Subtraction is $3^x \cdot 5^x$ becomes $2^{\max(0,x^1-x^2)}$

$3 \cdot 5^x \rightarrow x$
$3^x \rightarrow 2x$
$5^x \rightarrow x$
Ordering of Rules

• The ordering of rules are immaterial for the addition example but are critical to the workings of limited subtraction.

• In fact, if we ignore the order and just allow any applicable rule to be used, we get a form of non-determinism that makes these systems equivalent to Petri nets.

• The ordered kind are deterministic and are equivalent to a Petri net in which the transitions are prioritized.
Why Deterministic?

To see why determinism makes a difference, consider

\[3 \cdot 5x \rightarrow x\]
\[3x \rightarrow 2x\]
\[5x \rightarrow x\]

Starting with \(135 = 3^35^1\), deterministically we get

\[135 \Rightarrow 9 \Rightarrow 6 \Rightarrow 4 = 2^2\]

Non-deterministically we get a larger, less selective set.

\[135 \Rightarrow 9 \Rightarrow 6 \Rightarrow 4 = 2^2\]
\[135 \Rightarrow 90 \Rightarrow 60 \Rightarrow 40 \Rightarrow 8 = 2^3\]
\[135 \Rightarrow 45 \Rightarrow 3 \Rightarrow 2 = 2^1\]
\[135 \Rightarrow 45 \Rightarrow 15 \Rightarrow 1 = 2^0\]
\[135 \Rightarrow 45 \Rightarrow 15 \Rightarrow 5 \Rightarrow 1 = 2^0\]
\[135 \Rightarrow 45 \Rightarrow 15 \Rightarrow 3 \Rightarrow 2 = 2^1\]
\[135 \Rightarrow 45 \Rightarrow 9 \Rightarrow 6 \Rightarrow 4 = 2^2\]
\[135 \Rightarrow 90 \Rightarrow 60 \Rightarrow 40 \Rightarrow 8 = 2^3\]

\[\ldots\]

This computes \(2^z\) where \(0 \leq z \leq x_1\). Think about it.
More on Determinism

In general, we might get an infinite set using non-determinism, whereas determinism might produce a finite set. To see this, consider a system

\[
2x \rightarrow x
\]

\[
2x \rightarrow 4x
\]

starting with the number 2.
Sample RM and FRS

Present a Register Machine that computes IsOdd. Assume R1=x at starts; at termination, set R0=1 if x is odd; 0 otherwise. We assume R0=0 at start. We also are not concerned about destroying input.

1. DEC1[2, 4]
2. DEC1[1, 3]
3. INC0[4]

4. Present a Factor Replacement System that computes IsOdd. Assume starting number is $3^x$; at termination, result is $2=2^1$, if $x$ is odd; $1=2^0$, otherwise.

$3 \times 3 \ x \rightarrow x$

$3 \ x \rightarrow 2 \ x$
Sample FRS

Present a Factor Replacement System that computes IsPowerOf2. Assume starting number is $3 \times 5$; at termination, result is $2^{\text{if } x \text{ is a power of } 2}; 1 = 2^0$, otherwise

$3^2 \times 5 \times x \rightarrow 5 \times 7 \times x$

$3 \times 5 \times 7 \times x \rightarrow x$

$3 \times 5 \times x \rightarrow 2 \times x$

$5 \times 7 \times x \rightarrow 7 \times 11 \times x$

$7 \times 11 \times x \rightarrow 3 \times 11 \times x$

$11 \times x \rightarrow 5 \times x$

$5 \times x \rightarrow x$

$7 \times x \rightarrow x$
Systems Related to FRS

- **Petri Nets:**
  - Unordered
  - Ordered
  - Negated Arcs

- **Vector Addition Systems:**
  - Unordered
  - Ordered

- **Factors with Residues:**
  - $a \cdot x + c \rightarrow b \cdot x + d$

- **Finitely Presented Abelian Semi-Groups**
Petri Net Operation

- Finite number of places, each of which can hold zero or more markers.
- Finite number of transitions, each of which has a finite number of input and output arcs, starting and ending, respectively, at places.
- A transition is enabled if all the nodes on its input arcs have at least as many markers as arcs leading from them to this transition.
- Progress is made whenever at least one transition is enabled. Among all enabled, one is chosen randomly to fire.
- Firing a transition removes one marker per arc from the incoming nodes and adds one marker per arc to the outgoing nodes.
Petri Net Computation

• A Petri Net starts with some finite number of markers distributed throughout its n nodes.
• The state of the net is a vector of n natural numbers, with the i-th component’s number indicating the contents of the i-th node. E.g., \(<0,1,4,0,6>\) could be the state of a Petri Net with 5 places, the 2nd, 3rd and 5th, having 1, 4, and 6 markers, resp., and the 1st and 4th being empty.
• Computation progresses by selecting and firing enabled transitions. Non-determinism is typical as many transitions can be simultaneously enabled.
• Petri nets are often used to model coordination algorithms, especially for computer networks.
Variants of Petri Nets

• A Petri Net is not computationally complete. In fact, its halting and word problems are decidable. However, its containment problem (are the markings of one net contained in those of another?) is not decidable.
• A Petri net with prioritized transitions, such that the highest priority transitions is fired when multiple are enabled is equivalent to an FRS. (Think about it).
• A Petri Net with negated input arcs is one where any arc with a slash through it contributes to enabling its associated transition only if the node is empty. These are computationally complete. They can simulate register machines. (Think about this also).
Petri Net Example
Vector Addition

- Start with a finite set of vectors in integer n-space.
- Start with a single point with non-negative integral coefficients.
- Can apply a vector only if the resultant point has non-negative coefficients.
- Choose randomly among acceptable vectors.
- This generates the set of reachable points.
- Vector addition systems are equivalent to Petri Nets.
- If order vectors, these are equivalent to FRS.
Vectors as Resource Models

• Each component of a point in n-space represents the quantity of a particular resource.
• The vectors represent processes that consume and produce resources.
• The issues are safety (do we avoid bad states) and liveness (do we attain a desired state).
• Issues are deadlock, starvation, etc.
Factors with Residues

• Rules are of form
  – \( a_i x + c_i \rightarrow b_i x + d_i \)
  – There are \( n \) such rules
  – Can apply if number is such that you get a residue (remainder) \( c_i \) when you divide by \( a_i \)
  – Take quotient \( x \) and produce a new number \( b_i x + d_i \)
  – Can apply any applicable one (no order)

• These systems are equivalent to Register Machines.
Abelian Semi-Group

\[ S = (G, \cdot) \] is a semi-group if

1. Closure: If \( x, y \in G \) then \( x \cdot y \in G \)
2. Associativity: \( x \cdot (y \cdot z) = (x \cdot y) \cdot z \)

\( S \) is a monoid if

3. Identity: \( \exists e \in G \ \forall x \in G \ [e \cdot x = x \cdot e = x] \)

\( S \) is a group if

4. Inverse: \( \forall x \in G \ \exists x^{-1} \in G \ [x^{-1} \cdot x = x \cdot x^{-1} = e] \)

\( S \) is Abelian if \( \cdot \) is commutative
Finitely Presented

• $S = (G, \cdot)$, a semi-group (monoid, group), is finitely presented if there is a finite set of symbols, $\Sigma$, called the alphabet or generators, and a finite set of equalities ($\alpha_i = \beta_i$), the reflexive transitive closure of which determines equivalence classes over $G$.

• Note, the set $G$ is the closure of the generators under the semi-group’s operator $\cdot$.

• The problem of determining membership in equivalence classes for finitely presented Abelian semi-groups is equivalent to that of determining mutual derivability in an unordered FRS or Vector Addition System with inverses for each rule.
Recursive Functions

Primitive and $\mu$-Recursive
Primitive Recursive

An Incomplete Model
Basis of PRFs

• The primitive recursive functions are defined by starting with some base set of functions and then expanding this set via rules that create new primitive recursive functions from old ones.

• The base functions are:
  \[ C_a(x_1, \ldots, x_n) = a \] : constant functions
  \[ I^n_i(x_1, \ldots, x_n) = x_i \] : identity functions
  \[ S(x) = x + 1 \] : an increment function
Building New Functions

• **Composition:**
  If $G, H_1, \ldots, H_k$ are already known to be primitive recursive, then so is $F$, where

  $$F(x_1, \ldots, x_n) = G(H_1(x_1, \ldots, x_n), \ldots, H_k(x_1, \ldots, x_n))$$

• **Iteration (aka primitive recursion):**
  If $G, H$ are already known to be primitive recursive, then so is $F$, where

  $$F(0, x_1, \ldots, x_n) = G(x_1, \ldots, x_n)$$
  $$F(y+1, x_1, \ldots, x_n) = H(y, x_1, \ldots, x_n, F(y, x_1, \ldots, x_n))$$

  We also allow definitions like the above, except iterating on $y$ as the last, rather than first argument.
Addition & Multiplication

Example: Addition

\[ + (0, y) = I^1_1(y) \]
\[ + (x+1, y) = H(x, y, +(x, y)) \]

where \( H(a, b, c) = S(l^3_3(a, b, c)) \)

Example: Multiplication

\[ * (0, y) = C_0(y) \]
\[ * (x+1, y) = H(x, y, *(x, y)) \]

where \( H(a, b, c) = +(l^3_2(a, b, c), l^3_3(a, b, c)) \)

\[ = b+c = y + *(x, y) = (x+1)*y \]
Intuitive Composition

- Any time you have already shown some functions to be primitive recursive, you can show others are by building them up through composition.
- Example #1: If g and h are primitive recursive functions (prf) then so is \( f(x) = g(h(x)) \). As an explicit example, \( \text{Add2}(x) = S(S(x)) = x+2 \) is a prf.
- Example #2: This can also involve multiple functions and multiple arguments like, if g, h and j are prf’s then so is \( f(x,y) = g(h(x), j(y)) \).

The problem with giving an explicit example here is that interesting compositions tend to also involve induction.
Intuitive Inductions

• A function $F$ can be defined inductively using existing prf’s. Typically, we have one used for the basis and another for building inductively.

• Example#1: We can build addition from successor ($S$)
  $x + 0 = x$ (formally $+ (x, 0) = I(x)$)
  $x + y + 1 = S(x + y)$ (more formally $+ (x, y + 1) = S(+ (x, y))$)

• Example#2: We can build multiplication from addition
  $x * 0 = 0$ (formally $*(x, 0) = C_0$)
  $x * (y + 1) = + (x, x * y)$ (more formally $*(x, y + 1) = + (x, *(x, y))$)
Basic Arithmetic

\[ x + 1: \quad // \text{aka } S(x) - \text{successor} \]
\[ x + 1 = S(x) \]

\[ x - 1: \quad // \text{aka } P(x) - \text{predecessor} \]
\[ 0 - 1 = 0 \]
\[ (x+1) - 1 = x \]

\[ x + y: \]
\[ x + 0 = x \]
\[ x + (y+1) = (x+y) + 1 \]

\[ x - y: \quad // \text{limited subtraction} \]
\[ x - 0 = x \]
\[ x - (y+1) = (x-y) - 1 \]
2nd Grade Arithmetic

\[ x \times y: \]
\[ x \times 0 = 0 \]
\[ x \times (y+1) = x \times y + x \]

\[ x!: \]
\[ 0! = 1 \]
\[ (x+1)! = (x+1) \times x! \]
Basic Relations

x == 0:
   0 == 0 = 1
   (y+1) == 0 = 0
x == y:
   x==y = ((x – y) + (y – x )) == 0
x ≤ y:
   x≤y = (x – y) == 0
x ≥ y:
   x≥y = y≤x
x > y :
   x>y = ~(x≤y) /* See ~ on next page */
x < y :
   x<y = ~(x≥y)
Basic Boolean Operations

\(~x:\)
\[\sim x = 1 - x \text{ or } (x==0)\]

\(\text{signum}(x):\)
1 if \(x>0\); 0 if \(x==0\)
\[\sim(x==0)\]

\(x && y:\)
\[x&&y = \text{signum}(x*y)\]

\(x || y:\)
\[x||y = \sim((x==0) && (y==0))\]
Definition by Cases

One case
\[
f(x) = \begin{cases} 
  g(x) & \text{if } P(x) \\
  h(x) & \text{otherwise}
\end{cases}
\]

\[
f(x) = P(x) \cdot g(x) + (1-P(x)) \cdot h(x)
\]

Can use induction to prove this is true for all \( k>0 \), where
\[
f(x) = \begin{cases} 
  g_1(x) & \text{if } P_1(x) \\
  g_2(x) & \text{if } P_2(x) \land \lnot P_1(x) \\
  \vdots \\
  g_k(x) & \text{if } P_k(x) \land \lnot(P_1(x) \lor \cdots \lor \lnot P_{k-1}(x)) \\
  h(x) & \text{otherwise}
\end{cases}
\]
Bounded Minimization 1

\[ f(x) = \mu z \ (z \leq x) \ [ P(z) ] \] if \( \exists \) such a \( z \),

\[ = x+1, \text{ otherwise} \]

where \( P(z) \) is primitive recursive.

Can show \( f \) is primitive recursive by

\[ f(0) = 1-P(0) \]

\[ f(x+1) = f(x) \quad \text{if} \quad f(x) \leq x \]

\[ = x+2-P(x+1) \quad \text{otherwise} \]
Bounded Minimization 2

\[ f(x) = \mu z \ (z < x) \ [ P(z) ] \] if \( \exists \) such a \( z \),

= \( x \), otherwise

where \( P(z) \) is primitive recursive.

Can show \( f \) is primitive recursive by
\[ f(0) = 0 \]
\[ f(x+1) = \mu z \ (z \leq x) \ [ P(z) ] \]
Intermediate Arithmetic

\( x \parallel y: \) 
- \( x \parallel 0 = 0 \) : silly, but want a value 
- \( x \parallel (y+1) = \mu z (z < x) \left[ (z+1)(y+1) > x \right] \)

\( x \mid y: x \) is a divisor of \( y \) 
- \( x \mid y = ((y/x) \ast x) == y \)
Primality

firstFactor(x): first non-zero, non-one factor of x.
  firstfactor(x) = \( \mu z \ (2 \leq z \leq x) \ [z|x] \),
  \( x+1 \) if none

isPrime(x):
  isPrime(x) = firstFactor(x) == x && (x>1)

prime(i) = i-th prime:
  prime(0) = 2
  prime(x+1) = \( \mu z(\text{prime}(x)< z \leq \text{prime}(x)!+1)[\text{isPrime}(z)] \)
We will abbreviate this as \( p_i \) for prime(i)
Exponents

$x^y$:

$x^0 = 1$

$x^{y+1} = x \times x^y$

$\text{exp}(x,i)$: the exponent of $p_i$ in number $x$.

$\text{exp}(x,i) = \mu \ z \ (z<x) \ [ \sim(p_i^{z+1}) \ | \ x \ ]$
Pairing Functions

• pair(x, y) = \langle x, y \rangle = 2^x \ (2y + 1) – 1

• with inverses
  \langle z \rangle_1 = \exp(z+1,0)

  \langle z \rangle_2 = ((( z + 1 ) \ // \ 2 \ \langle z \rangle_1 ) – 1 ) \ // \ 2

• These are very useful and can be extended to encode n-tuples
  \langle x, y, z \rangle = \langle x, \langle y, z \rangle \rangle \ (note: \ stack \ analogy)
Pairing Function is 1-1 Onto

Prove that the pairing function \( <x,y> = 2^x (2y + 1) - 1 \) is 1-1 onto the natural numbers.

Approach 1:
We will look at two cases, where we use the following modification of the pairing function, \( <x,y>+1 \), which implies the problem of mapping the pairing function to \( \mathbb{Z}^+ \).
Case 1 (x=0)

Case 1:
For $x = 0$, $<0,y>+1 = 2^0(2y+1) = 2y+1$. But every odd number is by definition of the form $2y+1$, where $y\geq0$; moreover, a particular value of $y$ is uniquely associated with each such odd number and no odd number is produced when $x=0$. Thus, $<0,y>+1$ is 1-1 onto the odd natural numbers.
Case 2 (x > 0)

Case 2:
For $x > 0$, $<x,y>+1 = 2^x(2y+1)$, where $2y+1$ ranges over all odd number and is uniquely associated with one based on the value of $y$ (we saw that in case 1). $2^x$ must be even, since it has a factor of 2 and hence $2^x(2y+1)$ is also even. Moreover, from elementary number theory, we know that every even number except zero is of the form $2^xz$, where $x>0$, $z$ is an odd number and this pair $x,y$ is unique. Thus, $<x,y>+1$ is 1-1 onto the even natural numbers, when $x>0$.

The above shows that $<x,y>+1$ is 1-1 onto $\mathbb{Z}^+$, but then $<x,y>$ is 1-1 onto $\mathbb{N}$, as was desired.
Pairing Function is 1-1 Onto

Approach 2:
Another approach to show a function $f$ over $S$ is 1-1 onto $T$ is to show that
$f^{-1}(f(x)) = x$, for arbitrary $x \in S$ and that
$f(f^{-1}(z)) = z$, for arbitrary $z \in T$.

Thus, we need to show that
$(<x,y>_1,<x,y>_2) = (x,y)$ for arbitrary $(x,y) \in \mathbb{N} \times \mathbb{N}$ and
$<<z>_1,<z>_2> = z$ for arbitrary $z \in \mathbb{N}$. 
Alternate Proof

Let $x,y$ be arbitrary natural number, then $<x,y> = 2^x(2y+1)-1$.
Moreover, $<2^x(2y+1)-1>_1 = \text{Factor}(2^x(2y+1),0) = x$, since $2y+1$ must be odd, and
$<2^x(2y+1)-1>_2 = ((2^x(2y+1)/2^{\text{Factor}(2^x(2y+1),0)})-1)/2 = 2y/2 = y$.
Thus, $(<x,y>_1,<x,y>_2) = (x,y)$, as was desired.

Let $z$ be an arbitrary natural number, then the inverse of the pairing is $<z>_1, <z>_2$
Moreover, $<<z>_1,<z>_2> = 2^{<z>_1} * (2^{<z>_2}+1)-1$
$= 2^{\text{Factor}(z+1,0)} * ( (z+1)/ 2^{\text{Factor}(z+1,0)})/2 - 1 + 1)-1$
$= (z+1) - 1$
$= z$, as was desired.
Show that prfs are closed under Fibonacci induction. Fibonacci induction means that each induction step after calculating the base is computed using the previous two values, where the previous values for \( f(1) \) are \( f(0) \) and 0; and for \( x>1 \), \( f(x) \) is based on \( f(x-1) \) and \( f(x-2) \).

The formal hypothesis is:
Assume \( g \) and \( h \) are already known to be prf, then so is \( f \), where

\[
\begin{align*}
f(0,x) &= g(x); \\
f(1,x) &= h(f(0,x), 0); \text{ and} \\
f(y+2,x) &= h(f(y+1,x), f(y,x))
\end{align*}
\]

Proof is by construction
Fibonacci Recursion

Let $K$ be the following primitive recursive function, defined by induction on the primitive recursive functions, $g$, $h$, and the pairing function.

$K(0, x) = B(x)$

$B(x) = < g(x), C_0(x) >$  // this is just $<g(x), 0>$

$K(y+1, x) = J(K(y, x))$

$J(z) = < h(<z>_1, <z>_2), <z>_1 >$

// this is $< f(y+1, x), f(y, x) >$, even though $f$ is not yet shown to be prf!!

This shows $K$ is prf.

$f$ is then defined from $K$ as follows:

$f(y, x) = <K(y, x)>_1$  // extract first value from pair encoded in $K(y, x)$

This shows it is also a prf, as was desired.
µ Recursive

4th Model
A Simple Extension to Primitive Recursive
μ Recursive Concepts

• All primitive recursive functions are algorithms since the only iterator is bounded. That’s a clear limitation.

• There are algorithms like Ackerman’s function that cannot be represented by the class of primitive recursive functions.

• The class of recursive functions adds one more iterator, the minimization operator (μ), read “the least value such that.”
Ackermann’s Function

- $A(1, j)=2j$ for $j \geq 1$
- $A(i, 1)=A(i-1, 2)$ for $i \geq 2$
- $A(i, j)=A(i-1, A(i, j-1))$ for $i, j \geq 2$
- Wilhelm Ackermann observed in 1928 that this is not a primitive recursive function.
- Ackermann’s function grows too fast to have a for-loop implementation.
- The inverse of Ackermann’s function is important to analyze Union/Find algorithm. Note: $A(4,4)$ is a super exponential number involving six levels of exponentiation. $A(5,5)$ exceeds the number of atoms in known universe.
- $\alpha(n) = A^{-1}(n,n)$ grows so slowly that it is less than 5 for any value of $n$ that can be written.
Union/Find

- Start with a collection $S$ of unrelated elements – singleton equivalence classes
- $\text{Union}(x,y)$, $x$ and $y$ are in $S$, merges the class containing $x$ ($[x]$) with that containing $y$ ($[y]$)
- $\text{Find}(x)$ returns the canonical element of $[x]$
- Can see if $x \equiv y$, by seeing if $\text{Find}(x) == \text{Find}(y)$
- How do we represent the classes?
The $\mu$ Operator

- Minimization:
  If $G$ is already known to be recursive, then so is $F$, where
  $$F(x_1,\ldots,x_n) = \mu y \ (G(y,x_1,\ldots,x_n) == 1)$$
- We also allow other predicates besides testing for one. In fact, any predicate that is recursive can be used as the stopping condition.
Equivalence of Models

Equivalency of computation by
Turing machines,
register machines,
factor replacement systems,
recursive functions
Proving Equivalence

• Constructions do not, by themselves, prove equivalence.

• To do so, we need to develop a notion of an “instantaneous description” (id) of each model of computation (well, almost as recursive functions are a bit different).

• We then show a mapping of id’s between the models.
Instantaneous Descriptions

- An instantaneous description (id) is a finite description of a state achievable by a computational machine, \( M \).
- Each machine starts in some initial id, \( id_0 \).
- The semantics of the instructions of \( M \) define a relation \( \Rightarrow_M \) such that, \( id_i \Rightarrow_M id_{i+1}, i \geq 0 \), if the execution of a single instruction of \( M \) would alter \( M \)'s state from \( id_i \) to \( id_{i+1} \) or if \( M \) halts in state \( id_i \) and \( id_{i+1} = id_i \).
- \( \Rightarrow^+_M \) is the transitive closure of \( \Rightarrow_M \)
- \( \Rightarrow^*_M \) is the reflexive transitive closure of \( \Rightarrow_M \).
id Definitions

- For a register machine, $M$, an id is an $s+1$ tuple of the form $(i, r_1, \ldots, r_s)_M$ specifying the number of the next instruction to be executed and the values of all registers prior to its execution.
- For a factor replacement system, an id is just a natural number.
- For a Turing machine, $M$, an id is some finite representation of the tape, the position of the read/write head and the current state. This is usually represented as a string $\alpha q x \beta$, where $\alpha$ ($\beta$) is the shortest string representing all non-blank squares to the left (right) of the scanned square, $x$ is the symbol at the scanned square and $q$ is the current state.
- Recursive functions do not have id’s so we will handle their simulation by an inductive argument, using the primitive functions as the basis and composition, induction and minimization in the inductive step.
Equivalence Steps

• Assume we have a machine $M$ in one model of computation and a mapping of $M$ into a machine $M'$ in a second model.
• Assume the initial configuration of $M$ is $id_0$ and that of $M'$ is $id'_0$.
• Define a mapping, $h$, from id’s of $M$ into those of $M'$, such that, $R_M = \{ h(d) \mid d \text{ is an instance of an id of } M \}$, and
  – $id'_0 \Rightarrow^*_{M'} h(id_0)$, and $h(id_0)$ is the only member of $R_M$ in the configurations encountered in this derivation.
  – $h(id_i) \Rightarrow^+_{M'} h(id_{i+1})$, $i \geq 0$, and $h(id_{i+1})$ is the only member of $R_M$ in this derivation.

• The above, in effect, provides an inductive proof that
  – $id_0 \Rightarrow^*_M id$ implies $id'_0 \Rightarrow^*_{M'} h(id)$, and
  – If $id'_0 \Rightarrow^*_{M'} id'$ then either $id_0 \Rightarrow^*_M id$, where $id' = h(id)$, or $id' \not\in R_M$. 
All Models are Equivalent

Equivalency of computation by Turing machines, register machines, factor replacement systems, recursive functions
Our Plan of Attack

• We will now show $\text{TURING} \leq \text{REGISTER} \leq \text{FACTOR} \leq \text{RECURSIVE} \leq \text{TURING}$

  where, by $A \leq B$, we mean that every instance of $A$ can be replaced by an equivalent instance of $B$.

• The transitive closure will then get us the desired result.
TURING $\leq$ REGISTER
Encoding a TM’s State

• Assume that we have an $n$ state Turing machine. Let the states be numbered $0,\ldots, n-1$.
• Assume our machine is in state $7$, with its tape containing
  \[ \ldots 0 0 1 0 1 0 0 1 1 \underline{q7 0 0 0} \ldots \]
• The underscore indicates the square being read. We denote this by the finite id
  \[ 1 0 1 0 0 1 1 \underline{q7 0} \]
• In this notation, we always write down the scanned square, even if it and all symbols to its right are blank.
More on Encoding of TM

• An id can be represented by a triple of natural numbers, \((R,L,i)\), where \(R\) is the number denoted by the reversal of the binary sequence to the right of the \(q_i\), \(L\) is the number denoted by the binary sequence to the left, and \(i\) is the state index.

• So, 
  \[\ldots 0 0 1 0 1 0 0 1 1 q7 0 0 0 \ldots\]
  is just \((0, 83, 7)\).
  \[\ldots 0 0 1 0 q5 1 0 1 1 0 0 \ldots\]
  is represented as \((13, 2, 5)\).

• We can store the \(R\) part in register 1, the \(L\) part in register 2, and the state index in register 3.
Simulation by RM

1. DEC3[2,q0] : Go to simulate actions in state 0
2. DEC3[3,q1] : Go to simulate actions in state 1
...

n. DEC3[ERR,qn-1] : Go to simulate actions in state n-1
...

qj. IF_r1_ODD[qj+2] : Jump if scanning a 1
qj+1. JUMP[set_k] : If (qj 0 0 qk) is rule in TM
qj+1. INC1[set_k] : If (qj 0 1 qk) is rule in TM
qj+1. DIV_r1_BY_2 : If (qj 0 R qk) is rule in TM
    MUL_r2__BY_2
    JUMP[set_k]
qj+1. MUL_r1_BY_2 : If (qj 0 L qk) is rule in TM
    IF_r2_ODD then INC1
    DIV_r2__BY_2[set_k]
...

set_n-1. INC3[set_n-2] : Set r3 to index n-1 for simulating state n-1
set_n-2. INC3[set_n-3] : Set r3 to index n-2 for simulating state n-2
...

set_0. JUMP[1] : Set r3 to index 0 for simulating state 0

3/1/23
Fixups

• Need epilog so action for missing quad (halting) jumps beyond end of simulation to clean things up, placing result in $r0$.

• Can also have a prolog that starts with arguments in registers $r1$ to $rn$ and stores values in $r1$, $r2$ and $r3$ to represent Turing machines starting configuration.
Prolog

Example assuming \( n \) arguments (fix as needed)

1. \( \text{MUL}_{rn+1} \_\text{BY}_2[2] \): Set \( rn+1 = 11\ldots10_2 \), where, \#1's = \( r1 \)
2. \( \text{DEC1}[3,4] \): \( r1 \) will be set to 0
3. \( \text{INCn+1}[1] \):
4. \( \text{MUL}_{rn+1} \_\text{BY}_2[5] \): Set \( rn+1 = 11\ldots1011\ldots10_2 \), where, \#1's = \( r1 \), then \( r2 \)
5. \( \text{DEC2}[6,7] \): \( r2 \) will be set to 0
6. \( \text{INCn+1}[4] \):

\[
\begin{align*}
3n-2. \quad & \text{DECn[3n-1,3n+1]} : \text{Set } rn+1 = 11\ldots1011\ldots1011\ldots1_2, \text{ where, } \#1's = r1, r2, \\
3n-1. \quad & \text{MUL}_{rn+1} \_\text{BY}_2[3n] : \text{rn will be set to 0} \\
3n. \quad & \text{INCn+1[3n-2]} : \\
3n+1 \quad & \text{DECn+1[3n+2,3n+3]} : \text{Copy } rn+1 \text{ to } r2, \text{rn+1 is set to 0} \\
3n+2. \quad & \text{INC2[3n+1]} : \\
3n+3. \quad & r2 = \text{left tape, } r1 = 0 \text{ (right), } r3 = 0 \text{ (initial state)}
\end{align*}
\]
Epilog

1. DEC3[1,2] : Set r3 to 0 (just cleaning up)
2. IF_r1_ODD[3,5] : Are we done with answer?
3. INC0[4] : putting answer in r0
4. DIV_r1_BY_2[2] : strip a 1 from r1
5. : Answer is now in r0
REGISTER ≤ FACTOR
Encoding a RM’s State

• This is an easy one based on the fact that every member of \( \mathbb{Z}^+ \) (the positive integers) has a unique prime factorization. Thus, all such numbers can be uniquely written in the form

\[
p_{i_1}^{k_1} p_{i_2}^{k_2} \ldots p_{i_j}^{k_j}
\]

where the \( p_i \)'s are distinct primes and the \( k_i \)'s are non-zero values, except that the number 1 would be represented by \( 2^0 \).

• Let \( R \) be an arbitrary \( n+1 \)-register machine, having \( m \) instructions.

Encode the contents of registers \( r_0, \ldots, r_n \) by the powers of \( p_0, \ldots, p_n \).

Encode rule number's \( 1, \ldots, m \) by primes \( p_{n+1}, \ldots, p_{n+m} \).

Use \( p_{n+m+1} \) as prime factor that indicates simulation is done.

• This is, in essence, a Gödel number of the RM’s state.
Simulation by FRS

• Now, the j-th instruction \((1 \leq j \leq m)\) of \(R\) has associated factor replacement rules as follows:

  j. \(\text{INCr}[i]\)
  
  \[ p_{n+j}x \rightarrow p_{n+i}p_r x \]

  j. \(\text{DECr}[s, f]\)
  
  \[
  \begin{align*}
  p_{n+j}p_r x & \rightarrow p_{n+s} x \\
p_{n+j}x & \rightarrow p_{n+f} x
  \end{align*}
  \]

• We also add the halting rule associated with \(m+1\) of

  \[ p_{n+m+1}x \rightarrow x \]
Importance of Order

• The relative order of the two rules to simulate a **DEC** are critical.

• To test if register \( r \) has a zero in it, we, in effect, make sure that we cannot execute the rule that is enabled when the \( r \)-th prime is a factor.

• If the rules were placed in the wrong order, or if they weren't prioritized, we would be non-deterministic.
Sample RM and FRS (repeat)

Present a Register Machine that computes \texttt{IsOdd}. Assume \texttt{R1=x} at starts; at termination, set \texttt{R0=1}, if \texttt{x} is odd; \texttt{0}, otherwise. We assume \texttt{R0=0} at start. We also are not concerned about destroying input.

1. \texttt{DEC1[2, 4]}
2. \texttt{DEC1[1, 3]}
3. \texttt{INC0[4]}
4. Present a Factor Replacement System that computes \texttt{IsOdd}. Assume starting number is \texttt{3^x}; at termination, result is \texttt{2=2^1}, if \texttt{x} is odd; \texttt{1=2^0}, otherwise.

\begin{align*}
3 \times 3 & \rightarrow x \\
3 & \rightarrow 2 \times x
\end{align*}
Example of Order

Consider the simple machine to compute $r_0 := r_1 - r_2$ (limited)

1. DEC2[2,3]
2. DEC1[1,1]
3. DEC1[4,5]
4. INC0[3]
5. 
Subtraction Encoding

Start with $3 \times 5 \cdot 7$

- $7 \cdot 5 \times x \rightarrow 11 \times x$
- $7 \times x \rightarrow 13 \times x$
- $11 \cdot 3 \times x \rightarrow 7 \times x$
- $11 \times x \rightarrow 7 \times x$
- $13 \cdot 3 \times x \rightarrow 17 \times x$
- $13 \times x \rightarrow 19 \times x$
- $17 \times x \rightarrow 13 \cdot 2 \times x$
- $19 \times x \rightarrow x$
Analysis of Problem

• If we don't obey the ordering here, we could take an input like $3^55^27$ and immediately apply the second rule (the one that mimics a failed decrement).

• We then have $3^55^213$, signifying that we will mimic instruction number 3, never having subtracted the 2 from 5.

• Now, we mimic copying r1 to r0 and get $2^55^219$.

• We then remove the 19 and have the wrong answer.
FACTOR $\leq$ RECURSIVE
Universal Machine

• In the process of doing this reduction, we will build a Universal Machine.
• This is a single recursive function with two arguments. The first specifies the factor system (encoded) and the second the argument to this factor system.
• The Universal Machine will then simulate the given machine on the selected input.
Encoding FRS

• Let \((n, ((a_1, b_1), (a_2, b_2), \ldots, (a_n, b_n)))\) be some factor replacement system, where \((a_i, b_i)\) means that the \(i\)-th rule is \(a_ix \rightarrow b_ix\)

• Encode this machine by the number \(F\),

\[
2^n 3^{a_1} 5^{b_1} 7^{a_2} 11^{b_2} \ldots p_1^{a_n} p_2^{b_n} p_{2n-1} p_{2n} p_{2n+1} p_{2n+2}
\]
Simulation by Recursive # 1

• We can determine the rule of $F$ that applies to $x$ by

\[
\text{RULE}(F, x) = \mu z \ (1 \leq z \leq \exp(F, 0)+1) \ [ \exp(F, 2z-1) \mid x ]
\]

• Note: $\exp(F, 2i-1) = a_i$ where $a_i$ is the exponent of the prime factor $p_{2i-1}$ of $F$.

• If $x$ is divisible by $a_i$, and $i$ is the least integer, $1 \leq i \leq n$, for which this is true, then \( \text{RULE}(F, x) = i \).

If $x$ is not divisible by any $a_i$, $1 \leq i \leq n$, then $x$ is divisible by 1, and $\text{RULE}(F, x)$ returns $n+1$. That’s why we added $p_{2n+1} p_{2n+2}$.

• Given the function $\text{RULE}(F, x)$, we can determine $\text{NEXT}(F, x)$, the number that follows $x$, when using $F$, by

\[
\text{NEXT}(F, x) = (x \div \exp(F, 2\times\text{RULE}(F, x)-1)) \times \exp(F, 2\times\text{RULE}(F, x))
\]
Simulation by Recursive # 2

• The configurations listed by $F$, when started on $x$, are
  $\text{CONFIG}(F, x, 0) = x$
  $\text{CONFIG}(F, x, y+1) = \text{NEXT}(F, \text{CONFIG}(F, x, y))$

• The number of the configuration on which $F$ halts is
  $\text{HALT}(F, x) = \mu y \ [\text{CONFIG}(F, x, y) == \text{CONFIG}(F, x, y+1)]$

This assumes we converge to a fixed point as our means of halting. Of course, no applicable rule meets this definition as the $n+1$-st rule divides and then multiplies the latest value by 1.
Simulation by Recursive # 3

• A Universal Machine that simulates an arbitrary Factor System, Turing Machine, Register Machine, Recursive Function can then be defined by

\[ \text{Univ}(F, x) = \exp(\text{CONFIG}(F, x, \text{HALT}(F, x)), 0) \]

• This assumes that the answer will be returned as the exponent of the only even prime, 2. We can fix F for any given Factor System that we wish to simulate. It is that ability that makes this function universal.
FRS Subtraction

- $2^{03^a5^b} \Rightarrow 2^{a-b}$
  - $3*5x \rightarrow x$ or $1/15$
  - $5x \rightarrow x$ or $1/5$
  - $3x \rightarrow 2x$ or $2/3$
- Encode $F = 2^3 3^{15} 5^1 7^5 11^1 13^3 17^2 19^1 23^1$
- Consider $a=4, b=2$
- $\text{RULE}(F, x) = \mu \ z (1 \leq z \leq 4) \ [ \exp(F, 2^z-1) \mid x \ ]$
  - $\text{RULE}(F, 3^4 5^2) = 1$, as $15$ divides $3^4 5^2$
- $\text{NEXT}(F, x) = (x \ // \ \exp(F, 2^{\text{RULE}(F, x)-1})) \ * \ \exp(F, 2^{\text{RULE}(F, x)})$
  - $\text{NEXT}(F, 3^4 5^2) = (3^4 5^2 \ // \ 15 \ * \ 1) = 3^3 5^1$
  - $\text{NEXT}(F, 3^3 5^1) = (3^3 5^1 \ // \ 15 \ * \ 1) = 3^2$
  - $\text{NEXT}(F, 3^2) = (3^2 \ // \ 3 \ * \ 2) = 2^1 3^1$
  - $\text{NEXT}(F, 2^1 3^1) = (2^1 3^1 \ // \ 3 \ * \ 2) = 2^2$
  - $\text{NEXT}(F, 2^2) = (2^2 \ // \ 1 \ * \ 1) = 2^2$
Rest of simulation

- \( \text{CONFIG}(F, x, 0) = x \)
  \( \text{CONFIG}(F, x, y+1) = \text{NEXT}(F, \text{CONFIG}(F, x, y)) \)

- \( \text{CONFIG}(F, 3^4 \cdot 5^2, 0) = 3^4 \cdot 5^2 \)
  \( \text{CONFIG}(F, 3^4 \cdot 5^2, 1) = 3^3 \cdot 5^1 \)
  \( \text{CONFIG}(F, 3^4 \cdot 5^2, 2) = 3^2 \)
  \( \text{CONFIG}(F, 3^4 \cdot 5^2, 3) = 2^1 \cdot 3^1 \)
  \( \text{CONFIG}(F, 3^4 \cdot 5^2, 4) = 2^2 \)
  \( \text{CONFIG}(F, 3^4 \cdot 5^2, 5) = 2^2 \)

- \( \text{HALT}(F, x) = \mu y [\text{CONFIG}(F, x, y) = \text{CONFIG}(F, x, y+1)] = 4 \)

- \( \text{Univ}(F, x) = \exp (\text{CONFIG}(F, x, \text{HALT}(F, x)), 0) \)
  \( = \exp(2^2, 0) = 2 \)
Simplicity of Universal

- A side result is that every computable (recursive) function can be expressed in the form

\[ F(x) = G(\mu y \ H(x, y)) \]

where \( G \) and \( H \) are primitive recursive.
RECURSIVE $\leq$ TURING
Standard Turing Computation

• Our notion of standard Turing computability of some \( n \)-ary function \( F \) assumes that the machine starts with a tape containing the \( n \) inputs, \( x_1, \ldots, x_n \) in the form

\[
\ldots 01^{x_1}01^{x_2}0\ldots 01^{x_n}0\ldots
\]

and ends with

\[
\ldots 01^{x_1}01^{x_2}0\ldots 01^{x_n}01^y0\ldots
\]

where \( y = F(x_1, \ldots, x_n) \).
More Helpers

• To build our simulation we need to construct some useful submachines, in addition to the $R$, $L$, $R$, $L$, and $C_k$ machines already defined.

• $T$ -- translate moves a value left one tape square
  \[
  \ldots ?01^x0\ldots \Rightarrow \ldots ?1^x00\ldots
  \]

• Shift -- shift a rightmost value left, destroying value to its left
  \[
  \ldots 01^x101^x20\ldots \Rightarrow \ldots 01^x20\ldots
  \]

• $\text{Rot}_k$ -- Rotate a $k$ value sequence one slot to the left
  \[
  \ldots 01^x101^x20\ldots 01^xk0\ldots \Rightarrow \ldots 01^x20\ldots 01^xk01^x10\ldots
  \]
Basic Functions

All Basis Recursive Functions are Turing computable:

- $C_a^n(x_1, \ldots, x_n) = a$
- $I_i^n(x_1, \ldots, x_n) = x_i$
- $S(x) = x + 1$
Closure Under Composition

If $G, H_1, \ldots, H_k$ are already known to be Turing computable, then so is $F$, where

$$F(x_1, \ldots, x_n) = G(H_1(x_1, \ldots, x_n), \ldots, H_k(x_1, \ldots, x_n))$$

To see this, we must first show that if $E(x_1, \ldots, x_n)$ is Turing computable then so is

$$E^{<m>}(x_1, \ldots, x_n, y_1, \ldots, y_m) = E(x_1, \ldots, x_n)$$

This can be computed by the machine

$$L^{n+m} (\text{Rot}_{n+m})^n R^{n+m} E \quad L^{n+m+1} (\text{Rot}_{n+m})^m R^{n+m+1}$$

Can now define $F$ by

$$H_1 H_2^{<1>} H_3^{<2>} \ldots H_k^{<k-1>} G \text{ Shift}^k$$
Closure Under Induction

To prove that Turing Machines are closed under induction (primitive recursion), we must simulate some arbitrary primitive recursive function $F(y, x_1, x_2, \ldots, x_n)$ on a Turing Machine, where $F(0, x_1, x_2, \ldots, x_n) = G(x_1, x_2, \ldots, x_n)$ $F(y+1, x_1, x_2, \ldots, x_n) = H(y, x_1, x_2, \ldots, x_n, F(y, x_1, x_2, \ldots, x_n))$

Where, $G$ and $H$ are Standard Turing Computable. We define the function $F$ for the Turing Machine as follows:

\[
\begin{array}{c}
G \quad \downarrow \quad L^{n+1} \\
0 \quad \quad \quad R^{n+2} \\
\quad \quad \quad \downarrow \\
1 \quad 0 R^{n+2} H \quad \text{Shift} \quad L^{n+2} \quad 1
\end{array}
\]

This is a bit tricky!!
Recall computing at $y+1$ wants $y$ as the first argument.

Since our Turing Machine simulator can produce the same value for any arbitrary PRF, $F$, we show that Turing Machines are closed under induction (primitive recursion).
Closure Under Minimization

If $G$ is already known to be Turing computable, then so is $F$, where

$$F(x_1,\ldots,x_n) = \mu y \ (G(x_1,\ldots,x_n, y) == 1)$$

This can be done by

This assume $G$ is a predicate that returns 0 or 1.
Consequences of Equivalence

• Theorem: The computational power of Recursive Functions, Turing Machines, Register Machine, and Factor Replacement Systems are all equivalent.

• Theorem: Every Recursive Function (Turing Computable Function, etc.) can be performed with just one unbounded type of iteration.

• Theorem: Universal machines can be constructed for each of our formal models of computation.
Undecidability

We Can’t Do It All
Let’s go over some important facts to this point:

1. $\Sigma^*$ denotes the set of all strings over some finite alphabet $\Sigma$
2. $|\Sigma^*| = |\mathbb{N}|$, where $\mathbb{N}$ is the set of natural numbers = the smallest infinite cardinal (the countable infinity)
3. A language $L$ over $\Sigma$ is a subset of $\Sigma^*$; that is, $L \in \mathcal{P}(\Sigma^*) = 2^{\Sigma^*}$
   Here $\mathcal{P}$ denotes the power set constructor
4. $|L|$ is countable because $L \subseteq \Sigma^*$ (that is, $|L| \leq |\Sigma^*| = |\mathbb{N}|$)
5. $|\Sigma^*| < |\mathcal{P}(\Sigma^*)|$ (uncountable infinity) implies there are an uncountable number of languages over a given alphabet, $\Sigma$.
6. A program, $P$, in some programming language $L$, can be represented as a string over a finite alphabet, $\Sigma_P$ that obeys the rules of constructing programs defined by $L$. As $P \in \Sigma_P^*$, there are at most a countably infinite number of programs that can be formed in the language $L$. 
Computable Languages 2

7. Each program, \( P \), in a programming language \( L \), defines a function, \( F_P: \Sigma_I^* \rightarrow \Sigma_O^* \) where \( \Sigma_I \) is the input alphabet and \( \Sigma_O \) is the output alphabet.

8. \( F_P \) defines an input language \( P_I \) for which \( F_P \) is defined (halts and produces an output). This is referred to as its domain in our terminology (\( \Sigma_I \) is its universe of discourse). The range of \( F_P \), \( P_O \), is the set of outputs. That is, 
\[
P_O = \{ y | \exists x \text{ in } P_I \text{ and } y = F_P(x) \}
\]

9. Since there are a countable number of programs, \( P \), there can be at most a countable number of functions \( F_P \) and consequently, only a countable number of distinct input languages and output languages associated with programs in \( L_P \). Thus, there are only a countable number of languages (input or output) that can be defined by any program, \( P \).

10. But there are an uncountable number of possible languages over any given alphabet – see 3 and 5.

11. Thus, there must be languages over a given alphabet that have no descriptions – in terms of a program – or in terms of an algorithm. Thus, there are only a countably infinite number of languages that are computable among the uncountable number of possible languages.
1. Programming languages that we use as software developers are in a sense “complete.” By complete we mean that they can be used to implement all procedures that we think are computable (definable by a computational model that we can “agree” covers all procedural activities).

2. **Challenge: Why did I say “agree” rather than “prove”?**

3. We mostly like programs that halt on all input (we call these algorithms), but we know it’s always possible to do otherwise in every programming language we think is complete (C, C++, C#, Java, Python, et al.)

4. We can, of course, define programming languages that define only algorithms.

5. Unfortunately, we cannot define a programming language that produces all and only algorithms (all and just programs that always halt).

6. The above (#5) is one of the main results shown in this course

7. However, before focusing on #5 we should recall that finite-state, push down and linear bounded automata are computational models that produce only algorithms (when we monitor the latter two for loops) – it’s just that these get us a subset of algorithms.
Additional Notations

Includes comment on our notation versus that of others
Universal Machine

• Others consider functions of \( n \) arguments, whereas we had just one. However, our input to the FRS was actually an encoding of \( n \) arguments.

• The fact that we can focus on just a single number that is the encoding of \( n \) arguments is easy to justify based on the pairing function.

• Some presentations order arguments differently, starting with the \( n \) arguments and then the Gödel number of the function, but closure under argument permutation follows from closure under projection/substitution.
Universal Machine Mapping

- $\varphi^{(n)}(f, x_1, \ldots, x_n) = \text{Univ} (f, \prod_{i=1}^{n} p_{i}^{x_i})$
- We will sometimes adopt the above and also its common shorthand
  $\varphi_f^{(n)}(x_1, \ldots, x_n) = \varphi^{(n)}(f, x_1, \ldots, x_n)$
  and the even shorter version
  $\varphi_f(x_1, \ldots, x_n) = \varphi^{(n)}(f, x_1, \ldots, x_n)$
SNAP and TERM

• Our CONFIG is essentially a snapshot function as seen in other presentations of a universal function

\[
\text{SNAP}(f, x, t) = \text{CONFIG}(f, x, t)
\]

• Termination in our notation occurs when we reach a fixed point, so

\[
\text{TERM}(f, x) = (\text{NEXT}(f, x) == x)
\]

• Again, we used a single argument but that can be extended as we have already shown.
STP Predicate

• \( \text{STP}(f, x_1, \ldots, x_n, t) \) is a predicate defined to be true iff \( \varphi_f(x_1, \ldots, x_n) \) converges in at most \( t \) steps.

• \textbf{STP} is primitive recursive since it can be defined by

\[
\text{STP}(f, x, t) = \text{TERM}(f, \text{CONFIG}(f, x, t))
\]

Extending to many arguments is easily done as before.
VALUE PRF

- VALUE(f, x1,...,xn, t ) is a primitive recursive function (algorithm) that returns $\varphi_f(x_1,...,x_n)$ so long as
  STP(f, x1,...,xn, t ) is true.

- VALUE(f, x1,...,xn, t) = $\exp\ (\text{CONFIG} ( F, x, t), 0)$, where
  x is an encoding of $<x_1,...,x_n>$

- VALUE(f, x1,...,xn, t ) returns a value if
  STP(f, x1,...,xn, t ) is false, but the returned value is meaningless.
Recursively Enumerable

Properties of re Sets
Definition of re

• Some texts define re in the same way as I have defined semi-decidable.
  \( S \subseteq \mathbb{N} \) is semi-decidable iff there exists a partially computable function \( g \) where
  \[
  S = \{ \, x \in \mathbb{N} \mid g(x) \downarrow \, \}
  \]

• I prefer the definition of re that says
  \( S \subseteq \mathbb{N} \) is re iff \( S = \emptyset \) or there exists a totally computable function \( f \) where
  \[
  S = \{ \, y \mid \exists x \ f(x) = y \, \}
  \]

• We will prove these equivalent. Actually, \( f \) can be a primitive recursive function.
Semi-Decidable Implies re

Theorem: Let \( S \) be semi-decided by \( G_S \). Assume \( G_S \) is the \( g_S \)-th function in our enumeration of effective procedures. If \( S = \emptyset \) then \( S \) is re by definition, so we will assume wlog that there is some \( a \in S \). Define the enumerating algorithm \( F_S \) by

\[
F_S(<x,t>) = x \cdot \text{STP}(g_S, x, t) + a \cdot (1 - \text{STP}(g_S, x, t))
\]

Note: \( F_S \) is primitive recursive and it enumerates every value in \( S \) infinitely often. Note this is an existence proof in that we may not know \( a \).
re Implies Semi-Decidable

Theorem: By definition, $S$ is re iff $S = \emptyset$ or there exists an algorithm $F_S$, over the natural numbers $\mathbb{N}$, whose range is exactly $S$. Define

$$\mu y \ [y == y+1] \text{ if } S == \emptyset$$

$$\psi_S(x) = \exists y[F_S(y)==x], \text{ otherwise}$$

This achieves our result as the domain of $\psi_S$ is the range of $F_S$, or empty if $S == \emptyset$. Note that this is an existence proof in that we cannot test if $S == \emptyset$. 
Domain of a Procedure

Corollary: $S$ is re/semi-decidable iff $S$ is the domain / range of a partial recursive predicate $F_S$.

Proof: The predicate $\psi_S$ we defined earlier to semi-decide $S$, given its enumerating function, can be easily adapted to have this property.

$$\mu y \ [y == y+1] \quad \text{if } S == \emptyset$$

$$\psi_S(x) =$$

$$x * \exists y [F_S(y) == x], \text{ otherwise}$$
Theorem: Recursive implies re.
Proof: $S$ is recursive implies there is a total recursive function $f_S$ such that

$$S = \{ x \in \mathbb{N} | f_S(x) == 1 \}$$

Define $g_S(x) = \mu y (f_S(x) == 1)$

Clearly

$$\text{dom}(g_S) = \{ x \in \mathbb{N} | g_S(x) \downarrow \}$$

$$= \{ x \in \mathbb{N} | f_S(x) == 1 \}$$

$$= S$$
Related Results

Theorem: $S$ is re iff $S$ is semi-decidable.
Proof: That’s what we proved.

Theorem: $S$ and $\sim S$ are both re (semi-decidable) iff $S$ (equivalently $\sim S$) is recursive (decidable).

Proof: Let $f_S$ semi-decide $S$ and $f_{\sim S}$ semi-decide $\sim S$. We can decide $S$ by $g_S$

$$g_S(x) = \text{STP}(f_S, x, \mu t (\text{STP}(f_S, x, t) \parallel \text{STP}(f_{\sim S}, x, t)))$$

$\sim S$ is decided by $g_{\sim S}(x) = \sim g_S(x) = 1 - g_S(x)$.

The other direction is immediate since, if $S$ is decidable then $\sim S$ is decidable (just complement $g_S$) and hence they are both re (semi-decidable).
Enumeration Theorem

• Define
  \[ W_n = \{ x \in \mathbb{N} \mid \varphi(n,x)\downarrow \} \]

• Theorem: A set \( B \) is re iff there exists an \( n \) such that \( B = W_n \).
  Proof: Follows from definition of \( \varphi(n,x) \).

• This gives us a way to enumerate the recursively enumerable sets.

• Note: We cannot enumerate the recursive sets as they are non-re.
The Set $K$

- $K = \{ n \in \mathbb{N} \mid n \in W_n \}$
- Note that $n \in W_n \iff \varphi(n,n)\downarrow \iff \text{HALT}(n,n)$
- Thus, $K$ is the set consisting of the indices of each program that halts when given its own index
- $K$ can be semi-decided by the $\text{HALT}$ predicate above, so it is re.
K is not Recursive

• Theorem: We can prove this by showing \( \sim K \) is not re.
• If \( \sim K \) is re then \( \sim K = W_i \), for some \( i \).
• However, this is a contradiction since
  \[ i \in K \iff i \in W_i \iff i \in \sim K \iff i \not\in K \]
re Characterizations

Theorem: If $S \neq \emptyset$ then the following are equivalent:

1. $S$ is re
2. $S$ is the range of a primitive rec. function
3. $S$ is the range of a recursive function
4. $S$ is the range of a partial rec. function
5. $S$ is the domain of a partial rec. function
6. $S$ is the range/domain of a partial rec. function whose domain is the same as its range and which acts as an identity when it converges. Below, assume $f_S$ enumerates $S$.

$$g_S(x) = x \ast \text{STP}(f_S, x, \mu t \text{ (STP}(f_S, x, t)))$$

or

$$g_S(x) = x \ast \exists t \text{ STP}(f_S, x, t)$$
S-m-n Theorem
Parameter (S-m-n) Theorem

• Theorem: For each \( n,m>0 \), there is a prf \( S_m^n(y, u_1, \ldots, u_n) \) such that

\[
\varphi^{(m+n)}(y, x_1, \ldots, x_m, u_1, \ldots, u_n) = \varphi^{(m)}(S_m^n(y, u_1, \ldots, u_n), x_1, \ldots, x_m)
\]

• The proof of this is highly dependent on the system in which you proved universality and the encoding you chose.
S-m-n for FRS

- We would need to create a new FRS, from an existing one F, that fixes the value of $u_i$ as the exponent of the prime $p_{m+i}$.
- Sketch of proof:
  Assume we normally start with $p_1^{x_1} \ldots p_m^{x_m} p_1^{u_1} \ldots p_{m+n}^{u_n} \sigma$
  Here the first $m$ are variable; the next $n$ are fixed; $\sigma$ denotes prime factors used to trigger first phase of computation.
  Assume that we use fixed point as convergence.
  We start with just $p_1^{x_1} \ldots p_m^{x_m}$, with $q$ the first unused prime.

$$q \alpha x \rightarrow q \beta x$$ replaces $\alpha x \rightarrow \beta x$ in F, for each rule in F
$$q x \rightarrow q x$$ ensures we loop at end
$$x \rightarrow q p_{m+1}^{u_1} \ldots p_{m+n}^{u_n} \sigma x$$ adds fixed input, start state and $q$
this is selected once and never again

Note: $q = \text{prime}(\text{max}(n+m, \text{lastFactor(Product[i=1 to r] } \alpha_i \beta_i ))+1)$
where $r$ is the number of rules in F.
Details of $S_{m,n}$ for FRS

- The number of $F$ (called $F$, also) is $2^r 3^{a_1} 5^{b_1} \ldots p_{2r-1}^{a_r} p_{2r}^{b_r}$
- $S_{m,n}(F, u_1, \ldots, u_n) = 2^{r+2} q^{x_1} 5^{q \times b_1} \ldots p_{2r-1}^{q \times a_r} p_{2r}^{q \times b_r}$
  $p_{2r+1} q^{p_{2r+2}} p_{2r+3} q^{p_{2r+4}} q^{p_{m+1} u_1} \ldots p_{m+n} u_n \sigma$

- This represents the rules we just talked about. The first added rule pair means that if the algorithm does not use fixed point, we force it to do so. The last rule pair is the only one initially enabled and it adds the prime $q$, the fixed arguments $u_1, \ldots, u_n$, the enabling prime $q$, and the $\sigma$ needed to kick start computation. Note that $\sigma$ could be a $1$, if no kick start is required.

- $S_{m,n} = S_{m}^n$ is clearly primitive recursive. I’ll leave the precise proof of that as a challenge to you.
Quantification
Quantification#1

• $S$ is decidable iff there exists an algorithm $\chi_S$ (called $S$’s characteristic function) such that
  $x \in S \iff \chi_S(x)$
  This is just the definition of decidable.

• $S$ is re iff there exists an algorithm $A_S$ where
  $x \in S \iff \exists t \ A_S(x,t)$
  This is clear since, if $g_S$ is the index of the procedure $\psi_S$ that semi-decides $S$, then
  $x \in S \iff \exists t \ \text{STP}(g_S, x, t)$
  So, $A_S(x,t) = \text{STP}_{g_S}(x, t)$, where $\text{STP}_{g_S}$ is the STP function with its first argument fixed.

• Creating new functions by setting some one or more arguments to constants is an application of $S_m^n$. 

Quantification#2

- S is re iff there exists an algorithm $A_S$ such that
  \[ x \not\in S \iff \forall t \ A_S(x,t) \]
  This is clear since, if $g_S$ is the index of the procedure $\psi_S$ that semi-decides $S$, then
  \[ x \not\in S \iff \exists t \ STP(g_S, x, t) \iff \forall t \neg STP(g_S, x, t) \]
  So, $A_S(x,t) = \neg STP_{g_S}(x, t)$, where $STP_{g_S}$ is the STP function with its first argument fixed.

- Note that this works even if $S$ is recursive (decidable). The important thing there is that if $S$ is recursive then it may be viewed in two normal forms, one with existential quantification and the other with universal quantification.

- The complement of an re set is co-re. A set is recursive (decidable) iff it is both re and co-re.
The **Uniform Halting Problem** was already shown to be non-re. It turns out its complement is also not re. In fact, we can show that TOT requires an alternation of quantifiers as it is neither re nor co-re. Specifically,

\[ f \in \text{TOT} \iff \forall x \exists t \, ( \text{STP}(f, x, t) ) \]

and this is the minimum quantification we can use, given that the quantified predicate is total recursive (actually primitive recursive here).
Comments About Set of Algorithms
The Set TOT

• The listing of all algorithms can be viewed as
  \[ TOT = \{ f \in \mathbb{N} \mid \forall x \varphi(f, x) \downarrow \} \]

• We can also note that
  \[ TOT = \{ f \in \mathbb{N} \mid W_f = \mathbb{N} \} \]

• Theorem: TOT is not re.
Consequences

• To capture all the algorithms, any model of computation must include some procedures that are not algorithms.

• Since the potential for non-termination is required, every complete model must have some form of iteration that is potentially unbounded.

• This means that simple, well-behaved for-loops (the kind where you can predict the number of iterations on entry to the loop) are not sufficient. While type loops are needed, even if implicit rather than explicit.
Reducibility
Reduction Concepts

• Proofs by contradiction are tedious after you’ve seen a few (we saw three—Halt, TOTAL, and ¬K). We really would like proofs that build on known unsolvable problems to show other, open problems are unsolvable. The technique commonly used is called reduction. It starts with some known unsolvable problem and then shows that this problem is no harder than some open problem in which we are interested.
Diagonalization is a Bummer

• The issues with diagonalization are that it is tedious and is applicable as a proof of undecidability or non-re-ness for only a small subset of the problems that interest us.
• Thus, we will now seek to use reduction wherever possible.
• To show a set, $S$, is undecidable, we can show it is as least as hard as the set $\text{HALT} = K_0$. That is, $K_0 \leq S$. Here the mapping used in the reduction does not need to run in polynomial time, it just needs to be an algorithm.
• To show a set, $S$, is co-re, non-recursive, we can show it is the complement of some re, non-recursive set.
• To show a set, $S$, is not re and not even co-re, we can show it is as least as hard as the set $\text{TOTAL (the set of algorithms)}$. That is, $\text{TOTAL} \leq S$. We can also do this by showing it is the complement of a non-re, non-co-re set.
Some Precise Upper Bounds

- \( \langle f, x \rangle \in \text{HALT} \iff \exists t \ [\text{STP}(f, x, t)] \)
  Hence re upper bound
- \( \langle f, x \rangle \in \text{NON}_\text{HALT} \iff \forall t \ [\neg \text{STP}(f, x, t)] \)
  Hence co-re upper bound

- \( f \in \text{TOTAL} \iff \forall x \ \exists t \ [\text{STP}(f, x, t)] \)
  Non-re, Non-co-re upper bound
- \( f \in \text{NON}_\text{TOTAL} \iff \exists x \ \forall t \ [\neg \text{STP}(f, x, t)] \)
  Non-re, Non-co-re upper bound
Reduction Example#1

• We can show that the set $K_0$ (Halting) is no harder than the set $\text{TOTAL}$ (Uniform Halting). Since we already know that $K_0$ is unsolvable, we would now know that $\text{TOTAL}$ is also unsolvable. We cannot reduce in the other direction since $\text{TOTAL}$ is in fact harder than $K_0$.
• Let $\varphi_F$ be some arbitrary effective procedure and let $x$ be some arbitrary natural number.
• Define $F_x(y) = \varphi_F(x)$, for all $y \in \mathbb{N}$
• Then $F_x$ is an algorithm if and only if $\varphi_F$ halts on $x$.
• Thus, $K_0 \leq \text{TOTAL}$, and so a solution to membership in $\text{TOTAL}$ would provide a solution to $K_0$, which we know is not possible.
Reduction Examples #2 & #3

In all cases below we are assuming our variables are over $\mathcal{X}$.

HALT = $\{<f,x>| \varphi_f(x)\downarrow\}$ is unsolvable (undecidable, non-recursive)

TOTAL = $\{f|\forall x \varphi_f(x)\downarrow\} = \{f|W_f = \mathcal{X}\}$ is not even recursively enumerable (re, semidecidable)

Consider ZERO = $\{f|\forall x \varphi_f(x) = 0\}$

$f \in $ ZERO $\iff \forall x \exists t[\text{STP}(f,x,t) && \text{VALUE}(f,x,t)==0]$ gives upper bound

- Show ZERO = $\{f|\forall x \varphi_f(x) = 0\}$ is unsolvable – Show lower bound $<f,x> \in$ HALT iff $g(y) = \varphi_f(x) - \varphi_f(x)$ is zero for all y.
  Thus, $<f,x> \in$ HALT iff $g \in$ ZERO (really the index of g).
  A solution to ZERO implies one for HALT, so ZERO is unsolvable.

- Show ZERO = $\{f|\forall x \varphi_f(x) = 0\}$ is non-re – Attain upper bound $f \in$ TOTAL iff $h(x) = \varphi_f(x) - \varphi_f(x)$ is zero for all x.
  Thus, $f \in$ TOTAL iff $h \in$ ZERO (really the index of h).
  A semi-decision procedure for ZERO implies one for TOTAL, so ZERO is non-re.
Classic Undecidable Sets

- The universal language
  \[ \text{HALT} = K_0 = L_u = \{ \langle f, x \rangle \mid \varphi_f(x) \text{ is defined} \} \]
- Membership problem for \( L_u \) is the Halting Problem.

- The sets \( L_{ne} \) and \( L_e \), where

  \[
  \text{NON-EMPTY} = L_{ne} = \{ f \mid \exists x \varphi_f(x) \downarrow \}
  \]
  \[ f \in \text{NON-EMPTY} \iff \exists \langle x, t \rangle [\text{STP}(f, x, t)] - \text{re upper bound} \]

  \[
  \text{EMPTY} = L_e = \{ f \mid \forall x \varphi_f(x) \uparrow \}
  \]
  \[ f \in \text{EMPTY} \iff \forall \langle x, t \rangle [\neg \text{STP}(f, x, t)] - \text{co-re upper bound} \]

are the next sets we will study.
L_{\text{ne}} \text{ is re}

• \( L_{\text{ne}} \) is enumerated by

\[ F( <f, x, t> ) = f \times \text{STP}( f, x, t ) \]

• This assumes that 0 is in \( L_{\text{ne}} \) since 0 probably encodes some trivial machine. If this isn’t so, we’ll just slightly vary our enumeration of the recursive functions, so it is true.

• Thus, the range of this total function \( F \) is exactly the indices of functions that converge for some input, and that’s \( L_{\text{ne}} \).
L_{ne} is Non-Recursive

• Note in the previous enumeration that $F$ is a function of just one argument, as we are using an extended pairing function $<x, y, z> = <x, <y, z>>$.

• We can show $\text{Halt} = L_u = K_0 \leq L_{ne}$ This shows $L_{ne}$ cannot be recursive, for if it were then $K_0$ is recursive.

• Let $f, x$ be a pair of natural number where $f$ is an arbitrary function index and $x$ is an arbitrary input.

• Define $f_x(y) = \varphi_f(x)$, for all $y \in \mathbb{N}$.

• Then $<f, x> \in K_0 \iff \forall y f_x(y) \downarrow \Rightarrow f_x \in L_{ne}$
else $<f, x> \notin K_0 \iff \forall y f_x(y) \uparrow \Rightarrow f_x \notin L_{ne}$

• Thus, a decision procedure for $L_{ne}$ (equivalently for $L_e$) implies one for $K_0$.
$L_{ne}$ is re by Quantification

- Can do by observing that

$$f \in L_{ne} \iff \exists <x,t> \ STP(f, x, t)$$

- By our earlier results, any set whose membership can be described by an existentially quantified recursive predicate is re (semi-decidable).
\( L_e \) is not re

- If \( L_e \) were re, then \( L_{\text{ne}} \) would be recursive since it and its complement would be re.

- Can also observe that \( L_e \) is the complement of an re set since

\[
\begin{align*}
f & \in L_e \iff \forall <x,t> \sim \text{STP}(f, x, t) \\
& \iff \sim \exists <x,t> \text{STP}(f, x, t) \\
& \iff f \notin L_{\text{ne}}
\end{align*}
\]
Reduction and Equivalence

m-1, 1-1, Turing Degrees
Many-One Reduction

- Let $A$ and $B$ be two sets.
- We say $A$ many-one reduces to $B$, $A \leq_m B$, if there exists a total recursive function $f$ such that $x \in A \iff f(x) \in B$
- We say that $A$ is many-one equivalent to $B$, $A \equiv_m B$, if $A \leq_m B$ and $B \leq_m A$
- Sets that are many-one equivalent are in some sense equally hard or easy.
Many-One Degrees

• The relationship $A \equiv_m B$ is an equivalence relationship (why?)
• If $A \equiv_m B$, we say $A$ and $B$ are of the same many-one degree (of unsolvability).
• Decidable problems occupy three $m$-1 degrees: $\emptyset$, $\mathbb{N}$, all others.
• The hierarchy of undecidable $m$-1 degrees is an infinite lattice (I’ll discuss in class)
One-One Reduction

• Let $A$ and $B$ be two sets.

• We say $A$ one-one reduces to $B$, $A \leq_1 B$, if there exists a total recursive 1-1 function $f$ such that
  $$x \in A \iff f(x) \in B$$

• We say that $A$ is one-one equivalent to $B$, $A \equiv_1 B$, if $A \leq_1 B$ and $B \leq_1 A$

• Sets that are one-one equivalent are in a strong sense equally hard or easy.
One-One Degrees

• The relationship $A \equiv_1 B$ is an equivalence relationship (why?)
• If $A \equiv_1 B$, we say $A$ and $B$ are of the same one-one degree (of unsolvability).
• Decidable problems occupy infinitely many 1-1 degrees: each cardinality defines another 1-1 degree (think about it).
• The hierarchy of undecidable 1-1 degrees is an infinite lattice.
Turing (Oracle) Reduction

• Let $A$ and $B$ be two sets.
• We say $A$ Turing reduces to $B$, $A \leq_t B$, if the existence of an oracle for $B$ would provide us with a decision procedure for $A$.
• We say that $A$ is Turing equivalent to $B$, $A \equiv_t B$, if $A \leq_t B$ and $B \leq_t A$
• Sets that are Turing equivalent are in a very loose sense equally hard or easy.
Turing Degrees

• The relationship $A \equiv_t B$ is an equivalence relationship (why?)
• If $A \equiv_t B$, we say $A$ and $B$ are of the same Turing degree (of unsolvability).
• Decidable problems occupy one Turing degree. We really don’t even need the oracle.
• The hierarchy of undecidable Turing degrees is an infinite lattice.
Complete re Sets

• A set $C$ is re 1-1 (m-1, Turing) complete if, for any re set $A$, $A \leq_1 (\leq_m, \leq_t) C$.
• The set $\textbf{HALT}$ is an re complete set (in regard to 1-1, m-1 and Turing reducibility).
• The re complete degree (in each sense of degree) sits at the top of the lattice of re degrees.
The Set \( \text{Halt} = K_0 = L_u \)

- \( \text{Halt} = K_0 = L_u = \{ <f, x> \mid \varphi_f(x) \downarrow \} \)
- Let \( A \) be an arbitrary re set. By definition, there exists an effective procedure \( \varphi_a \), such that \( \text{dom}(\varphi_a) = A \). Put equivalently, there exists an index, \( a \), such that \( A = W_a \).
- \( x \in A \) iff \( x \in \text{dom}(\varphi_a) \) iff \( \varphi_a(x) \downarrow \) iff \( <a, x> \in K_0 \)
- The above provides a 1-1 function that reduces \( A \) to \( K_0 \) (\( A \leq_1 K_0 \))
- Thus, the universal set, \( \text{Halt} = K_0 = L_u \), is an re (1-1, m-1, Turing) complete set.
The Set K

- $K = \{ f \mid \varphi_f(f) \downarrow \}$
- Define $f_x(y) = \varphi_f(x)$, for all $y$. The index for $f_x$ can be computed from $f$ and $x$ using $S_{1,1}$, where we add a dummy argument, $y$, to $\varphi_f$. Let that index be $f_x$. (Yeah, that’s overloading.)
- $\langle f, x \rangle \in K_0$ iff $x \in \text{dom}(\varphi_f)$ iff $\forall y[\varphi_{f_x}(y) \downarrow] \Rightarrow f_x \in K$
  $\langle f, x \rangle \notin K_0$ iff $x \notin \text{dom}(\varphi_f)$ iff $\forall y[\varphi_{f_x}(y) \uparrow] \Rightarrow f_x \notin K$
- The above provides a 1-1 function that reduces $K_0$ to $K$, i.e., $K_0 \leq_1 K$.
- Since $K_0$ is an re (1-1, m-1, Turing) complete set and $K$ is re, then $K$ is also re (1-1, m-1, Turing) complete.
More re Complete Sets

- **HasIdentity (HId)** = \{ f | \exists x \ f(x) = x \}
  \[ f \in \text{HId} \iff \exists <x,t> [ \text{STP}(f,x,t) \&\& \text{VALUE}(f,x,t)=x ] \]

- **Halt \leq HId**;
  Given \( <f,x> \), define \( g_{f,x}(y) = f(x) - f(x) + y \)
  \( <f,x> \in \text{Halt} \iff \forall y [g_{f,x}(y)=y] \Rightarrow g_{f,x} \in \text{HId} \)
  \( <f,x> \notin \text{Halt} \iff \forall y [g_{f,x}(y)\uparrow] \Rightarrow g_{f,x} \notin \text{HId} \)

- **HasZero (HZ)** = \{ f | \exists x \ f(x) = 0 \}
  \[ f \in \text{HZ} \iff \exists <x,t> [ \text{STP}(f,x,t) \&\& \text{VALUE}(f,x,t)=0 ] \]
  Given \( <f,x> \), define \( g_{f,x}(y) = f(x) - f(x) \)
  \( <f,x> \in \text{Halt} \iff \forall y [g_{f,x}(y)=0] \Rightarrow g_{f,x} \in \text{HZ} \)
  \( <f,x> \notin \text{Halt} \iff \forall y [g_{f,x}(y)\uparrow] \Rightarrow g_{f,x} \notin \text{HZ} \)

- **This shows HId and HZ are re-complete**
Id Equivalent to TOT

- Identity (Id) = \{ f | \forall x \ f(x) = x \} \\
f \in id \iff \forall x \exists t \ [ \text{STP}(f,x,t) \land \text{VALUE}(f,x,t)=x ]

- TOT ≤ Id; \\
Given f, define \( g_f(x) = f(x) - f(x) + x \) \\
f \in TOT \iff \forall x [g_f(x)=x] \iff g_f \in Id

Id ≤ TOT; \\
Given f, define \( g_f(x) = \mu y \ [f(x) = x] \) \\
f \in Id \iff \forall x [g_f(x)\downarrow] \iff g_f \in TOT

- TOT ≡_1 Id
MI Equivalent to TOT

• MonolIncreasing (MI) = \{ f | \forall x \; f(x+1) > f(x) \} \\
f \in MI \iff \forall x \exists t \; [ \text{STP}(f,x,t) \&\& \text{STP}(f,x+1,t) \&\& \text{VALUE}(f,x+1,t) > \text{VALUE}(f,x,t) ]

• TOT \leq MI; \\
Given f, define \( g_f(x) = f(x) - f(x) + x \) \\
f \in TOT \iff \forall x [g_f(x) = x] \Rightarrow g_f \in MI \\
f \notin TOT \iff \exists x [g_f(x) \uparrow] \Rightarrow g_f \notin MI

• MI \leq TOT; \\
Given f, define \( g_f(x) = \mu y \; [f(x+1) > f(x)] \) \\
f \in MI \iff \forall x [g_f(x) \downarrow] \iff g_f \in TOT

• MI \equiv_1 TOT
Common Reductions (Halt)

- \( \text{Halt} = K_0 = L_u = \{ <f, x> \mid \varphi_f(x) \downarrow \} \)
- Define \( f_x(y) = \varphi_f(x) \), for all \( y \)
- Can use for
  - \( K = \{ f \mid \varphi_f(f) \downarrow \} \)
  - \( \text{Halt} \leq_1 \text{NE} = \{ f \mid \text{dom} (\varphi_f) \text{ is non-empty} \} \)
  - \( \text{Halt} \leq_1 \text{Infinite} = \{ f \mid \text{dom} (\varphi_f) \text{ is infinite} \} \)
  - \( \text{Halt} \leq_1 \text{TOTAL} = \{ f \mid \text{dom} (\varphi_f) \text{ is infinite} \} \)

© UCF CS
Common Reductions (Halt)

- Halt = $K_0 = L_u = \{ <f, x> \mid \varphi_f(x) \downarrow \}$
- Define $f_x(y) = \varphi_f(x) - \varphi_f(x) + z$, for all $y$
- Can use for
  - $\text{Halt} \leq_1 \text{HZ} = \{ f \mid \text{dom}(\varphi_f) \text{ contains } 0 \}$ with $z = 0$
  - $\text{Halt} \leq_1 \text{HasC} = \{ f \mid \exists x \ f(x) = C, \ C \text{ a constant} \}$ with $z = C$
  - $\text{Halt} \leq_1 \text{InfRange} = \{ f \mid \text{range}(\varphi_f) \text{ is infinite} \}$ with $z = y$
  - $\text{Halt} \leq_1 \text{HasMI} = \{ f \mid \exists x \ f(x+1) > f(x) \}$ with $z = y$
  - $\text{Halt} \leq_1 \text{HasId} = \{ f \mid \exists x \ f(x) = x \}$, with $z = y$
  - $\text{Halt} \leq_1 \text{Total} = \{ f \mid \text{dom}(\varphi_f) \text{ is } \aleph \}$ with $z = y$
Common Reductions (Total)

- Total = \{ f \mid \varphi_f(x) \downarrow \}
- Define \( f_x(y) = \varphi_f(x) - \varphi_f(x) + z \)
- Can use for
- Can use for
  - Total \( \leq_1 \text{IsZero} = \{ f \mid \text{dom}(\varphi_f) = \{0\} \} \) with \( z = 0 \)
  - Total \( \leq_1 \text{IsC} = \{ f \mid \text{dom}(\varphi_f) = \{C\} \} \) with \( z = C \)
  - Total \( \leq_1 \text{MI} = \{ f \mid \forall x \ f(x+1) > f(x) \} \) with \( z = y \)
  - Total \( \leq_1 \text{Id} = \{ f \mid \forall x \ f(x) = x \}, \) with \( z = y \)
The Overall Picture
UNIVERSE OF SETS

NonRE = (NRNC \cup Co\-RE) - REC
Reduction and Rice’s
What Rice’s is All About

• Let \( P \) be some property of subsets of re languages.

• Let \( L_P \) be the set of languages having property \( P \).

• For example, if \( P \) is the property that a language is infinite then \( L_P = \{ L \mid L \text{ is infinite re} \} \).

• Said differently, \( L_P = \{ f \mid \text{domain}(\varphi_f) \text{ is infinite} \} \) or even \( L_P = \{ g \mid \text{range}(\varphi_g) \text{ is infinite} \} \).

• In addition to limiting its applicability to properties of re languages (alternatively procedures that define those languages), Rice’s also limits its focus to properties that are non-trivial. A property is trivial if it applies to all re sets (procedures) or no re sets (procedures).
Rice Focused on Procedures

• As noted, we can view re languages by talking about the procedures that define them (either by domain or range or even both).

• Rice’s Theorem deals with properties that split the set of procedures (really their indices) in two partitions: those procedures that have the property and those that do not have the property.

• For Rice’s Theorem to apply, the property must be about the non-implementation dependent behaviors of procedures, not how they might be implemented or even how efficient they are.
Operational Aspects of Rice

• Operationally, this means if \( f \) and \( g \) are two arbitrary function indices such that \( \forall x \varphi_f(x) = \varphi_g(x) \) then Rice’s theorem cannot differentiate \( f \) from \( g \). That is, either \( f \) and \( g \) both have the property or neither does.

• This means, if we want to differentiate procedures based on how fast they compute values, Rice’s Theorem is useless.

• The above is what I call the Strong Version of Rice’s Theorem
Weaker Versions of Rice

• We will show that if \( f \) and \( g \) are two arbitrary function indices such that \( \text{domain } \varphi_f = \text{domain } \varphi_g \) then Rice’s theorem cannot differentiate \( f \) from \( g \).

• We will also show that if \( f \) and \( g \) are two arbitrary function indices such that \( \text{range } \varphi_f = \text{range } \varphi_g \) then Rice’s theorem cannot differentiate \( f \) from \( g \).

• The domain form is what Rice originally proved but we extend it here to three versions so one can choose the one that is best for a particular property.
Non-Trivial versus Trivial

• An example probably bring this home best
• Let $Doppel = \{ f \mid \text{there is a } g \neq f \text{ where } \forall x \quad \varphi_f(x) = \varphi_g(x) \}$
• It is the case that all procedures have twins (doppelgangers) so $Doppel$ applies to all procedures and $Doppel$ is the set of Natural Numbers.
• For this reason, Rice’s does not apply.
Comment about Ø

• Consider the set of indices of procedures that have empty domains.

• If \( f \) and \( g \) have the same domain then \( \text{domain}(f) = \emptyset \iff \text{domain}(g) = \emptyset \). 

• By our previous discussion Rice’s Theorem cannot differentiate \( f \) from \( g \) as it cannot look at how each computes its domain. It can only observe that both have the same domain (\( \emptyset \)), so they are indistinguishable.

• Moreover, if \( f \) and \( g \) have empty domains, they have empty ranges and they diverge everywhere, so they cannot be distinguished by their ranges or their mappings from input to output.
Rice’s Original Theorem

**Rice’s Theorem:** Let $P$ be some non-trivial property of the re languages. Then

$$L_P = \{ x \mid \text{dom} [x] \text{ is in } P \text{ (has property } P) \}$$

is undecidable. Note again that membership in $L_P$ is based purely on the domain of a function, not on any aspect of its implementation.

**Note:** Rice’s Theorem focuses on re sets as being domains of procedures. As noted previously, we will extend this to also consider ranges of procedures and even functional properties (mappings from domains to ranges.)
Rice’s Proof-1

**Proof:** We will assume, *wlog*, that \( P \) does not contain \( \emptyset \) (functions that have empty domains). If it does, we switch our attention to the complement of \( P \). Now, since \( P \) is non-trivial, there exists some language \( L \) with property \( P \). Let \([r]\) be a procedure (recursive function) whose domain is \( L \) (\( r \) is the index of a semi-decision procedure for \( L \)). Suppose \( P \) were decidable. We will use this decision procedure and the existence of \( r \) to decide \( \text{Halt} \ (K_0) \).
First, we define a function $F_{x,y,r}$ for $r$ and each function index $x$ and input $y$ as follows.

$$F_{x,y,r}(z) = \varphi(x, y) + \varphi(r, z)$$

The domain of this function is $L$ if $\varphi_x(y)$ converges, otherwise it’s $\emptyset$. Now if we can determine membership in $L_P$, we can use this algorithm to decide $K_0$ merely by applying it to $F_{x,y,r}$. An answer as to whether or not $F_{x,y,r}$ has property $P$ is also the correct answer as to whether or not $\varphi_x(y)$ converges.
Rice’s Proof-3

Thus, there can be no decision procedure for $P$. And consequently, there can be no decision procedure for any non-trivial property of re languages.

Note: This does not apply if $P$ is trivial, nor does it apply if $P$ can differentiate indices that converge for precisely the same values.

If the latter were true, it might be able to differentiate $\varphi_r$ from $F_{x,y,r}$. as they have different indices (different implementations) even if they might have the same domains.
I/O Property

• An I/O property, $\mathcal{P}$, of indices of recursive function is one that cannot differentiate indices of functions that produce precisely the same value for each input.

• This means that if two indices, $f$ and $g$, are such that $\varphi_f$ and $\varphi_g$ converge on the same inputs and, when they converge, produce precisely the same result, then both $f$ and $g$ must have property $\mathcal{P}$, or neither one has this property.

• Note that any I/O property of recursive function indices also defines a property of re languages, since the domains of functions with the same I/O behavior are equal.

• However, not all properties of re languages or procedures are I/O properties.
Example of Non-I/O Property

- $X_{10} = \{ f \mid \forall x \ f(x) \text{ converges by } 10 \text{ units of time} \}$
- Can describe as $f \in X_{10} \iff \forall x [ \text{STP}(f,x,10) ]$
- Consider two TMs to compute the function $Z(x) = 0$
- Can do by TM $Z_1$ with one instruction, $R$. $Z_1 \in X_{10}$
- Can do by less efficient TM $Z_2$, $L \ R \ R$. $Z_2 \not\in X_{10}$
- We now have two implementations of $Z$, one of which has the $X_{10}$ property and the other of which does not have the $X_{10}$ property, yet both have the same I/O behavior. Thus, $X_{10}$ is not an I/O property and Rice’s Theorem has nothing to say about the decidability or undecidability of membership in $X_{10}$.
- I will tell you, however, that $X_{10}$ is co-re, unsolvable.
**Rice’s Theorem**: Let $\mathcal{P}$ be some non-trivial I/O property of the indices of recursive functions. Then

$$S_\mathcal{P} = \{ x \mid \varphi_x \text{ has property } \mathcal{P} \}$$

is undecidable.

Membership in $S_\mathcal{P}$ is based purely on the input/output behavior of a function, not on any aspect of its implementation.
Strong Rice’s Proof

• Given \( x, y, r \), where \( r \) is in the set \( S_\mathcal{P} = \{ f | \varphi_f \text{ has property } \mathcal{P} \} \), define the function

\[
f_{x,y,r}(z) = \varphi_x(y) - \varphi_x(y) + \varphi_r(z)
\]

• \( f_{x,y,r}(z) = \varphi_r(z) \) if \( \varphi_x(y) \downarrow \); Otherwise \( \forall z \ f_{x,y,r}(z) \uparrow \) and \( \text{dom}(f_{x,y,r}) = \emptyset \).

Thus, \( \varphi_x(y) \downarrow \) iff \( f_{x,y,r} \) has property \( \mathcal{P} \), and so \( K_0 \leq S_\mathcal{P} \).
Black is for standard Rice’s Theorem; Black and Red are needed for Strong Version. Blue is just another version based on range.
Weak Rice’s Theorems

Weak Rice’s Theorem 1: Let $P$ be some non-trivial, implementation-independent property of the indices of recursive functions. Then

$$S_P = \{ x | \text{dom}(\varphi_x) \text{ has property } P \}$$

is undecidable.

$$\text{dom}(f_{x,y,r}) = \text{dom}(\varphi_r) \text{ if } \varphi_x(y) \downarrow ; = \phi \text{ if } \varphi_x(y) \uparrow$$

Weak Rice’s Theorem 2: Let $P$ be some non-trivial, implementation-independent property of the indices of recursive functions. Then

$$S_P = \{ x | \text{range}(\varphi_x) \text{ has property } P \}$$

is undecidable.

$$\text{range}(f_{x,y,r}) = \text{range}(\varphi_r) \text{ if } \varphi_x(y) \downarrow ; = \phi \text{ if } \varphi_x(y) \uparrow$$
Corollaries to Rice’s

Corollary: The following properties of re sets are undecidable

a) \( L = \emptyset \)
b) \( L \) is finite
c) \( L \) is a regular set
d) \( L \) is a context-free set

For all of these, Rice’s shows that the complements are undecidable but operationally it doesn’t matter.

Both the property and its complement are non-trivial, and each is implementation-independent.
Known Results:

HALT = \{ <f,x> \mid f(x)\downarrow \} is re (semi-decidable) but undecidable
TOTAL = \{ f \mid \forall x \; f(x)\downarrow \} is non-re (not even semi-decidable)

1. Use reduction from HALT to show that one cannot decide \textbf{NonTrivial}, where
\textbf{NonTrivial} = \{ f \mid \text{for some } x, y, x \neq y, f(x)\downarrow \text{ and } f(y)\downarrow \text{ and } f(x) \neq f(y) \}

2. Show that \textbf{Non-Trivial} reduces to HALT. (1 plus 2 show they are equally hard)

3. Use Reduction from TOTAL to show that \textbf{NoRepeats} is not even re, where
\textbf{NoRepeats} = \{ f \mid \text{for all } x, y, f(x)\downarrow \text{ and } f(y)\downarrow , \text{ and } x \neq y \Rightarrow f(x) \neq f(y) \}

4. Show \textbf{NoRepeats} reduces to TOTAL. (3 plus 4 show they are equally hard)

5. Use Rice’s Theorem to show that \textbf{NonTrivial} is undecidable

6. Use Rice’s Theorem to show that \textbf{NoRepeats} is undecidable
Practice Classifications

1. Use quantification of an algorithmic predicate to estimate the complexity (decidable, re, co-re, non-re) of each of the following, (a)-(d):
   a) \( \text{NonTrivial} = \{ f \mid \text{for some } x, y, x \neq y, f(x) \downarrow \text{ and } f(y) \downarrow \text{ and } f(x) \neq f(y) \} \)
   b) \( \text{NoRepeats} = \{ f \mid \text{for all } x, y, f(x) \downarrow \text{ and } f(y) \downarrow, \text{ and } x \neq y \Rightarrow f(x) \neq f(y) \} \)
   c) \( \text{FIN} = \{ f \mid \text{domain}(f) \text{ is finite} \} \)

2. Let set \( A \) be non-empty recursive, and let \( B \) be re non-recursive. Consider \( C = \{ z \mid z = x * y, \text{ where } x \in A \text{ and } y \in B \} \). For (a)-(c), either show sets \( A \) and \( B \) with the specified property or demonstrate that this property cannot hold.
   a) Can \( C \) be recursive?
   b) Can \( C \) be re non-recursive (undecidable)?
   c) Can \( C \) be non-re?
Sample Question#1

1. Given that the predicate $\text{STP}$ and the function $\text{VALUE}$ are algorithms, show that we can semi-decide

$$HZ = \{ f \mid \varphi_f \text{ evaluates to } 0 \text{ for some input} \}$$

Note: $\text{STP}(f, x, s)$ is true iff $\varphi_f(x)$ converges in $s$ or fewer steps and, if so, $\text{VALUE}(f, x, s) = \varphi_f(x)$. 
Sample Questions#2,3

2. Use Rice’s Theorem to show that $H_Z$ is undecidable, where $H_Z$ is

$$H_Z = \{ f \mid \varphi_f \text{ evaluates to 0 for some input} \}$$

3. Redo using Reduction from $HALT$. 
4. Let $P = \{ f \mid \exists x [ \text{STP}(f, x, x) ] \}$. Why does Rice’s theorem not tell us anything about the undecidability of $P$?
5. Let $S$ be an re (recursively enumerable), non-recursive set, and $T$ be an re, possibly recursive non-empty set. Let $E = \{ z \mid z = x + y, \text{ where } x \in S \text{ and } y \in T \}$. Answer with proofs, algorithms or counterexamples, as appropriate, each of the following questions:

(a) Can $E$ be non re?
(b) Can $E$ be re non-recursive?
(c) Can $E$ be recursive?
Constant time:
Not amenable to Rice’s
Constant Time

- \( \text{CTime} = \{ M \mid \exists K \ [ M \text{ halts in at most } K \text{ steps independent of its starting configuration } ] \} \)

- \( \text{CTime} \) cannot be shown undecidable by Rice’s Theorem as it breaks property 2 (it is implementation dependent)
  - Choose \( M_1 \) and \( M_2 \) to each Standard Turing Compute (STC) ZERO
  - \( M_1 \) is \( R \) (move right to end on a zero)
  - \( M_2 \) is \( L \ R \ R \) (time is dependent on argument length)
  - \( M_1 \) is in \( \text{CTime} \); \( M_2 \) is not , but they have same I/O behavior, so \( \text{CTime} \) does not adhere to property 2
Quantifier Analysis

- \( \text{CTime} = \{ M \mid \exists K \forall C \left[ \text{STP}(M, C, K) \right] \} \)

- This would appear to imply that \( \text{CTime} \) is not even re. However, a TM that only runs for \( K \) steps can scan at most \( K \) distinct tape symbols. Thus, if we use unary notation, \( \text{CTime} \) can be expressed

- \( \text{CTime} = \{ M \mid \exists K \forall C_{|C|\leq K} \left[ \text{STP}(M, C, K) \right] \} \)

- We can dovetail over the set of all TMs, \( M \), and all \( K \), listing those \( M \) that halt in constant time.
Complexity of CTime

• Can show it is equivalent to the Halting Problem for TM’s with Infinite Tapes (not unbounded but truly infinite)
• This was shown in 1966 to be undecidable.
• It was also shown to be re, just as we have done so for CTime.
• Details Later (maybe)
What We’ve Done in Computability
List Minus Some Tedious Stuff

- A question with multiple parts that uses quantification (STP/VALUE)
- Various re and recursive equivalent definitions
- Proofs of equivalence of definitions
- Consequences of recursiveness or re-ness of a problem
- Closure of recursive/re sets
- Gödel numbering (pairing functions and inverses)
- Models of computation/equivalences (not details but understanding)
- Primitive recursion and its limitation; bounded versus unbounded $\mu$
- Notion of universal machine
- A proof by diagonalization (there are just two possibilities)
- A question about $K$ and/or $K_0$
- Many-one reduction(s)
- Rice’s Theorem (its proof and its variants)
- Applications of Rice’s Theorem and when it cannot be applied
More Practice Problems
Sample Question#1

1. Prove that the following are equivalent
   a) $S$ is an infinite recursive (decidable) set.
   b) $S$ is the range of a monotonically increasing total recursive function.

Note: $f$ is monotonically increasing means that $\forall x \ f(x+1) > f(x)$. 
Sample Question#2

2. Let A and B be re sets. For each of the following, either prove that the set is re, or give a counterexample that results in some known non-re set.

a) $A \cup B$

b) $A \cap B$

c) $\sim A$
3. Present a demonstration that the *even* function is primitive recursive.
   
   ```
   even(x) = 1 if x is even  
   even(x) = 0 if x is odd  
   ```

   You may assume only that the base functions are prf and that prf’s are closed under a finite number of applications of composition and primitive recursion.
4. Given that the predicate \texttt{STP} and the function \texttt{VALUE} are prf’s, show that we can semi-decide 

\{ f \mid \varphi_f \text{ evaluates to 0 for some input} \}

Note: \texttt{STP}( f, x, s ) is true iff $\varphi_f(x)$ converges in $s$ or fewer steps and, if so, $\texttt{VALUE}(f, x, s) = \varphi_f(x)$. 
Sample Question#5

5. Let $S$ be an re (recursively enumerable), non-recursive set, and $T$ be an re, possibly recursive set. Let
$$E = \{ z \mid z = x + y, \text{ where } x \in S \text{ and } y \in T \}.$$ 
Answer with proofs, algorithms or counterexamples, as appropriate, each of the following questions:
(a) Can $E$ be non re?
(b) Can $E$ be re non-recursive?
(c) Can $E$ be recursive?
6. Assuming that the Uniform Halting Problem (TOTAL) is undecidable (it’s actually not even re), use reduction to show the undecidability of

\[ \{ f \mid \forall x \; \phi_f(x+1) > \phi_f(x) \} \]
7. Let $\text{Incr} = \{ f \mid \forall x, \varphi_f(x+1) > \varphi_f(x) \}$. Let $\text{TOT} = \{ f \mid \forall x, \varphi_f(x) \downarrow \}$. Prove that $\text{Incr} \equiv_m \text{TOT}$. Note Q#6 starts this one.
8. Let $\text{Incr} = \{ f \mid \forall x \quad \varphi_f(x+1) > \varphi_f(x) \}$. Use Rice’s theorem to show $\text{Incr}$ is not recursive.
9. Let $S$ be a recursive (decidable set), what can we say about the complexity (recursive, re non-recursive, non-re) of $T$, where $T \subset S$?
Sample Question#10

10. Define the pairing function \(<x,y>\) and its two inverses \(<z>_1\) and \(<z>_2\), where if \(z = <x,y>\), then \(x = <z>_1\) and \(y = <z>_2\).
11. Assume $A \leq_m B$ and $B \leq_m C$. Prove $A \leq_m C$. 
12. Let $P = \{ f | \exists x [ \text{STP}(f, x, x) ] \}$. Why does Rice’s theorem not tell us anything about the undecidability of $P$?
D2 = \{ f \mid \text{Domain}(f) > 1 \}

Use Rice’s Theorem to prove that D2 is undecidable. Be Complete.

Note \( f \in D2 \iff \exists <x,y,t> [\ STP(f,x,t) \& STP(f,y,t) \& x \neq y \] 

D2 is non-trivial as \( C0(x) = 0 \in D2 \) and \( \uparrow \not\in D2 \)

Let \( f, g \) be two arbitrary indices of procedures such that

\( \text{Domain}(f) = \text{Domain}(g) \)

\( f \in D2 \iff |\text{Domain}(f)| > 1 \)

\( \iff |\text{Domain}(g)| > 1 \)

as \( \text{Domain}(f) = \text{Domain}(g) \)

and so cardinalities are the same

\( \iff g \in D2 \)

Thus, \( D2 \) is undecidable by Rice’s Weak Form#1
Use Rice’s Theorem to prove that $R_2$ is undecidable. Be Complete.

Note $f \in R_2 \iff \exists <x,y,t> \left[ \text{STP}(f,x,t) \& \text{STP}(f,y,t) \& \text{skipped } x \neq y? \right. $
\left. (\text{VALUE}(f,x,t) \neq \text{VALUE}(f,y,t)) \right]$

$R_2$ is non-trivial as $S(x) = x+1 \in R_2$ and $C_0(x) = 0 \notin R_2$

Let $f,g$ be two arbitrary indices of procedures such that
$\text{Range}(f) = \text{Range}(g)$

$f \in R_2 \iff |\text{Range}(f)| > 1$

$\iff |\text{Range}(g)| > 1$

as $\text{Range}(f) = \text{Range}(g)$

and so cardinalities are the same

$\iff g \in R_2$

Thus, $R_2$ is undecidable by Rice’s Weak Form#2
HasDup(HD) = \{ f \mid \exists x, y, x \neq y, f(x) \downarrow, f(y) \downarrow, \& f(x) = f(y) \} 

Show a minimal quantification of some known primitive recursive predicate that provides an upper bound for the complexity of HD.

\[ \exists <x,y,t> \ [ \ STP(f,x,t) \ & \ STP(f,y,t) \ & \ x \neq y \ & \ (\text{VALUE}(f,x,t) = \text{VALUE}(f,y,t))] \]

Thus, HD \leq_m K_0
HasDup(HD) = \{ f | \exists x, y, x \neq y, f(x) \downarrow, f(y) \downarrow, \\
& f(x) = f(y) \} \\

Use Rice’s Theorem to prove that HD is undecidable. Be Complete.

HD is non-trivial as C0(x) = 0 ∈ HD and S(x) = x+1 ∉ HD

Let f,g be two arbitrary indices of procedures such that
\forall x \ f(x) = g(x)

f ∈ HD ⇔ \exists x, y \ [(x \neq y), f(x) \downarrow, f(y) \downarrow & f(x) = f(y)]
                   ⇔ \exists x, y \ [(x \neq y), g(x) \downarrow, g(y) \downarrow & g(x) = g(y)]
                                      as \forall x \ f(x) = g(x) and so g has same I/O properties
               ⇔ g ∈ HD

f \notin HD ⇔ \forall x, y \ [(x \neq y) \Rightarrow \text{either } f(x) \uparrow \text{ or } f(y) \uparrow \text{ or } f(x) \neq f(y)]
                        ⇔ \forall x, y \ [(x \neq y) \Rightarrow \text{either } g(x) \uparrow \text{ or } g(y) \uparrow \text{ or } g(x) \neq g(y)]
                                     as \forall x \ f(x) = g(x) and so g has same I/O properties
                            ⇔ g \notin HD

Thus, HD is undecidable by Rice’s Strong Form
HasDup(HD)={ \( f \mid \exists x,y, x\neq y, f(x)\downarrow, f(y)\downarrow, \) \\
& \( f(x) = f(y) \) }

Show that \( K = \{ f \mid f(f) \text{ converges} \} \) is many-one reducible to HD.

Let \( f \) be an arbitrary index.

From \( f \), define \( \forall x \ F_f(x) = f(f) - f(f) \).

\( f \in K \) implies \( \forall x \ F_f(x) = 0 \) implies \( F_f \in HD \).

\( f \notin K \) implies \( \forall x \ F_f(x) \uparrow \) implies \( F_f \notin HD \).

Thus, \( K \leq_m HD \)
HasDup(HD) = \{ f \mid \exists x, y, x \neq y, f(x) \downarrow, f(y) \downarrow, \\
& f(x) = f(y) \} \\

Show that HD is many-one reducible to 
K = \{ f \mid f(f) \text{ converges} \} \\

Let f be an arbitrary index. From f, define  
\forall z \ F_f(z) = \exists <x, y, t> \ [\text{STP}(f, x, t) \& \text{STP}(f, y, t) \& x \neq y \\
& \& \text{VALUE}(f, x, t) = \text{VALUE}(f, xyt)] \\

f \in HD \Rightarrow \forall z \ F_f(z) \downarrow \Rightarrow F_f(F_f) \text{ converges} \Rightarrow F_f \in K \\
f \notin HD \Rightarrow \forall z \ F_f(z) \uparrow \Rightarrow F_f \notin K. \\

Thus, HD \leq_m K
AllDup(AD) = \{ f | \forall x \ f(x) \downarrow \ & \exists y, \ x \neq y, \\
\text{where } f(y) \downarrow \ & \ f(x) = f(y) \ \} \\

Show a minimal quantification of some known primitive recursive predicate that provides an upper bound for the complexity of AD.

\forall x \ \exists <y,t> \ [\text{STP}(f,x,t) \ & \ \text{STP}(f,y,t) \ & \ x \neq y \\
\text{& (VALUE}(f,x,t) = \text{VALUE}(f,y,t)))]]

AD looks to be up there with TOT
AllDup(AD) = \{ f \mid \forall x \ f(x)\downarrow \ & \exists y, \ x \neq y, \\
\text{where } f(y)\downarrow \ & f(x) = f(y) \ \} \\

Use Rice’s Theorem to prove that AD is undecidable. Be Complete.

AD is non-trivial as \( C_0(x) = 0 \in AD \) and \( S(x) = x+1 \notin AD \)

Let \( f,g \) be two arbitrary indices of procedures such that
\( \forall x \ f(x) = g(x) \)

\( f \in AD \iff \forall x \ f(x)\downarrow \ & \exists y, \ x\neq y, \ where \ f(y)\downarrow \ & f(x) = f(y) \)
\( \iff \text{given any } x, \ f(x)\downarrow \ & \exists y\neq x, \ f(y)\downarrow \ & f(x) = f(y) \)
\( \iff \text{given any } x, \ g(x)\downarrow \ & \exists y\neq x, \ g(y)\downarrow \ & g(x) = g(y) \)
\( \text{as } \forall x \ f(x) = g(x) \text{ and so } g \text{ has same I/O properties} \)
\( \iff g \in AD \)

Thus, HD is undecidable by Rice’s Strong Form
AllDup(AD) = \{ f \mid \forall x \; f(x) \downarrow \; \& \; \exists y, \; x \neq y, \\
where \; f(y) \downarrow \; \& \; f(x) = f(y) \} \\

Show that TOT = \{ f \mid \text{for all } x, \; f(x) \text{ converges} \} is many-one reducible to AD.

Let \( f \) be an arbitrary index.

From \( f \), define \( \forall x \; F_f(x) = f(x) - f(x) \).

\( f \in TOT \Rightarrow \forall x \; F_f(x) = 0 \Rightarrow F_f \in AD \).

\( f \notin TOT \Rightarrow \exists x \; F_f(x) \uparrow \Rightarrow F_f \notin AD \).

Thus, TOT \leq_m AD
AllDup(AD) = \{ f \mid \forall x \ f(x) \downarrow \ & \exists y, \ x \neq y, \\
where f(y) \downarrow \ & \ f(x) = f(y) \}\}

Show that AD is many-one reducible to

\[ TOT = \{ f \mid \text{for all } x, \ f(x) \text{ converges} \} \]

Let \( f \) be an arbitrary index.

From \( f \), define \( \forall x \ F_f(x) = \exists y \ [x \neq y \ & \ f(x) = f(y)] \)

\( f \in AD \Rightarrow \forall x \ F_f(x) \downarrow \Rightarrow F_f \in TOT \)

\( f \notin AD \Rightarrow \exists x \ F_f(x) \uparrow \Rightarrow F_f \notin TOT. \)

Thus, \( AD \leq_m TOT \)

Note it is rare to use \( \exists \) without using STP but I am fine with
the search failing as a result of \( f \) diverging on either \( x \) or
some \( y \) or failing in a never-ending search.
Challenge

Semi-Constant(SC) = { f | ∃C, ∀x f(x)↓ ⇒ f(x) = C } 
Note: ↑ ∈ SC and C₀(x)=0 ∈ SC
Can describe as f ∈ SC ⇔
    ∃C ∀<x,t> [ STP(f,x,t) ⇒ VALUE(f,x,t) = C ]
This implies SC is as hard as Non-TOT={ f |∃x f(x)↑ } as
    f ∈ Non-TOT ⇔ ∃x ∀t [ ~STP(f,x,t) ]
However, SC only takes one quantifier and is undecidable (one of the weaker versions of Rice shows its undecidability).
I can tell you that either SC ≡ₘ HALT or SC ≡ₘ Non-HALT where Non-HALT = { <f,x> | f(x)↑ }.
Your job is to figure out which and rewrite the quantifier expression. You should also apply Rice’s to verify undecidability.
Nasty Challenge

RangeFinite = RF = \{ f \mid \text{Range}(f) \text{ is finite} \} ss

Things to do:
Present a minimum quantifier description (Easy)
Use Rice to show undecidable (Easy)

Here’s the hard part
Consider
\[ \text{NotTotal (NT)} = \{ f \mid \exists x \ f(x) \uparrow \} \]
Show equivalence of NT to RF. Must go both ways.
Rewriting Systems
Post Systems
Thue Systems

- Devised by Axel Thue
- Just a string rewriting view of finitely presented monoids (assoc. + identity)
- $T = (\Sigma, R)$, where $\Sigma$ is a finite alphabet and $R$ is a finite set of bi-directional rules of the form $\alpha_i \leftrightarrow \beta_i$, $\alpha_i, \beta_i \in \Sigma^*$
- We define $\leftrightarrow^*$ as the reflexive, transitive closure of $\leftrightarrow$, where $w \leftrightarrow x$ iff $w = y\alpha z$ and $x = y\beta z$, where $\alpha \leftrightarrow \beta$
Semi-Thue Systems

• Devised by Emil Post
• A one-directional version of Thue systems; one-way versus two ways
• \( S = (\Sigma, R) \), where \( \Sigma \) is a finite alphabet and \( R \) is a finite set of rules of form \( \alpha_i \rightarrow \beta_i, \alpha_i, \beta_i \in \Sigma^* \)
• We define \( \Rightarrow^* \) as the reflexive, transitive closure of \( \Rightarrow \), where \( w \Rightarrow x \) iff \( w = y\alpha z \) and \( x = y\beta z \), where \( \alpha \rightarrow \beta \)
Word Problems

- Let $S = (\Sigma, R)$ be some Thue (Semi-Thue) system, then the word problem for $S$ is the problem to determine of arbitrary words $w$ and $x$ over $S$, whether or not $w \equiv^* x$ ($w \Rightarrow^* x$).
- The Thue system word problem is the problem of determining membership in equivalence classes. This is not true for Semi-Thue systems.
- We can always consider just the relation $\Rightarrow^*$ since the symmetric property of $\equiv^*$ comes directly from the rules of Thue systems.
Simulating Turing Machines

• Basically, we need at least one rule for each 4-tuple in the Turing machine’s description.
• The rules lead from one instantaneous description to another.
• The Turing ID $\alpha q a \beta$ is represented by the string $h\alpha q a \beta h$, $a$ being the scanned symbol.
• The tuple $q a b s$ leads to $qa \rightarrow sb$
• Moving right and left can be harder due to blanks.
Details of \textit{Halt(TM)} \leq \textit{Word(ST)}

- Let $M = (Q, \{0,1\}, T)$, $T$ is Turing table.
- If $q_{abs} \in T$, add rule $q_a \to sb$ \hspace{1cm} // simple rewrite of scan
- If $q_aR_s \in T$, add rules
  - $q_{1b} \to 1sb \hspace{1cm} a=1$, $\forall b \in \{0,1\}$ \hspace{1cm} // left non-blank; scan not blank
  - $q_{1h} \to 1s0h \hspace{1cm} a=1$ \hspace{1cm} // right blank; scan not blank
  - $cq_{0b} \to c0sb \hspace{1cm} a=0$, $\forall b,c \in \{0,1\}$ \hspace{1cm} // left and right non-blank; scan blank
  - $hq_{0b} \to hsb \hspace{1cm} a=0$, $\forall b \in \{0,1\}$ \hspace{1cm} // left blank; right not blank; scan blank
  - $cq_{0h} \to c0s0h \hspace{1cm} a=0$, $\forall c \in \{0,1\}$ \hspace{1cm} // left not blank; right blank; scan blank
  - $hq_{0h} \to hs0h \hspace{1cm} a=0$ \hspace{1cm} // blank tape to blank tape
- If $q_aL_s \in T$, add rules
  - $bq_{ac} \to sbac \hspace{1cm} \forall a,b,c \in \{0,1\}$ \hspace{1cm} // left and right had non-blanks
  - $hq_{ac} \to hs0ac \hspace{1cm} \forall a,c \in \{0,1\}$ \hspace{1cm} // left blank; right not blank
  - $bq_{1h} \to sb1h \hspace{1cm} a=1$, $\forall b \in \{0,1\}$ \hspace{1cm} // left not blank; right blank; scan not blank
  - $hq_{1h} \to hs01h \hspace{1cm} a=1$ \hspace{1cm} // left blank; right blank; scan not blank
  - $bq_{0h} \to sbh \hspace{1cm} a=0$, $\forall b \in \{0,1\}$ \hspace{1cm} // left not blank; right blank; scan blank
  - $hq_{0h} \to hs0h \hspace{1cm} a=0$ \hspace{1cm} // blank tape to blank tape
Clean-Up

• Assume $q_1$ is start state and only one accepting state exists $q_0$.
• We will start in $h1^*q_10h$, seeking to accept $x$ (enter $q_0$) or reject (run forever).
• Add rules
  \[
  \begin{align*}
  &q_0a \rightarrow q_0 & \forall a \in \{0,1\} \\
  &bq_0 \rightarrow q_0 & \forall b \in \{0,1\}
  \end{align*}
  \]
• The added rule allows us to “erase” the tape if we accept $x$.
• This means that acceptance can be changed to generating $hq_0h$.
• The next slide shows the consequences.
Semi-Thue Word Problem

- Construction from TM, $M$, gets:
  - $h1^xq_10h \Rightarrow_{\Sigma(M)}^\ast hq_0h$ iff $x \in \mathcal{L}(M)$.
  - $hq_0h \Rightarrow_{\Pi(M)}^\ast h1^xq_10h$ iff $x \in \mathcal{L}(M)$.
  - $hq_0h \Leftrightarrow_{\Sigma(M)}^\ast h1^xq_10h$ iff $x \in \mathcal{L}(M)$.

- Can recast both Semi-Thue and Thue Systems to ones over alphabet $\{a,b\}$ or $\{0,1\}$. That is, a binary alphabet is sufficient for undecidability.
More on Grammars
Grammars and re Sets

- Every grammar lists an re set.
- Some grammars (regular, CFG and CSG) produce recursive sets.
- Type 0 grammars are as powerful at generating (producing) re sets as Turing machines are at enumerating them (Constructive Proof later).
Formal Language

Undecidability Continued
PCP and Traces
Post Correspondence Problem

- Many problems related to grammars can be shown no harder than PCP
- Each instance of PCP is denoted by an integer $n > 0$, a finite alphabet $\Sigma$ and two $n$-tuples of non-$\lambda$ words over $\Sigma$
  \[ x = (x_1, \ldots, x_n), \quad y = (y_1, \ldots, y_n) \]
- The decision problem is to determine if there is a sequence of indices $i_1, \ldots, i_k$, $1 \leq i_j \leq n$, for $1 \leq j \leq k$, where indices can be repeated, such that
  \[ x_{i_1} \ldots x_{i_k} = y_{i_1} \ldots y_{i_k} \]
PCP Example#1

• Let n=3, \( \Sigma = \{a, b\} \)
  \( x = (a \ b \ a, \ b \ b, \ a); \ y = (b \ a \ b, \ b, \ b \ a \ a) \)

• Must start with the second elements as they both start with b and all others misalign.

• A solution is 2, 3, 1, 2
  \( b \ b \ a \ a \ b \ a \ b \ b = b \ b \ a \ a \ b \ a \ b \ b \)

• Note 2,3,1,2,2,3,1,2 is also a solution
PCP Example#2

• Start with Semi-Thue System
  – aba → ab; a → aa; b → a
  – Instance of word problem: bbbb ⇒*? aa

• Convert to PCP
  – [bbbbb* ab ab aa aa a a a ]
    [ aba aba a a b b _aa]
  – And * * a a b b
     _ _ * a a b b
How PCP Construction Works?

- Using underscored letters avoids solutions that don’t relate to word problem instance. E.g.,
  
  \[
  \begin{align*}
  ab & \quad aa \\
  aba & \quad a
  \end{align*}
  \]

  leads to solution no matter the question

- Top row insures start with \([W_0 \ast]\)
- Bottom row insures end with \(*W_f]\)
- Bottom row matches \(W_i\), while top matches \(W_{i+1}\) (one is underscored)
- Get Solution for PCP iff \(W_0 \Rightarrow * W_f\)
Ambiguity of CFG

- Problem to determine if an arbitrary CFG is ambiguous.

\[
S \rightarrow A \mid B \\
A \rightarrow x_i A [i] \mid x_i [i] \quad 1 \leq i \leq n \\
B \rightarrow y_i B [i] \mid y_i [i] \quad 1 \leq i \leq n \\
A \Rightarrow^* \ x_{i_1} \ldots x_{i_k} [i_k] \ldots [i_1] \quad k > 0 \\
B \Rightarrow^* \ y_{i_1} \ldots y_{i_k} [i_k] \ldots [i_1] \quad k > 0
\]

- Ambiguous if and only if there is a solution to this PCP instance.
Intersection of CFLs

• Problem to determine if arbitrary CFG’s define overlapping languages

• Just take the grammar consisting of all the A-rules from previous, and a second grammar consisting of all the B-rules. Call the languages generated by these grammars, \( L_A \) and \( L_B \). 
  \[ L_A \cap L_B \neq \emptyset \], if and only there is a solution to this PCP instance.

• As intersection of two CFLs is a CSL, this is one proof we can determine is a CSG produces no (or any or finite or infinite) strings.
CSG Produces Something

\[ S \rightarrow x_i S y_i^R | x_i T y_i^R \quad 1 \leq i \leq n \]
\[ a T a \rightarrow * T * \quad a \in \Sigma \]
\[ * a \rightarrow a * \quad a \in \Sigma \]
\[ a * \rightarrow * a \quad a \in \Sigma \]
\[ T \rightarrow * \]

- Our only terminal is *. We get strings of form \(*^{2j+1}\), for some j’s if and only if there is a solution to this PCP instance.
CSG Produces Something

• Our only terminal in previous grammar is *. We get strings of form \(*^{2j+1}\), for some \(j\)'s if and only if there is a solution to this PCP instance. Get \(\emptyset\) otherwise.

• Thus, \(P\) has a solution iff
  – \(L(G) \neq \emptyset\)
  – \(L(G)\) is infinite

• Alternate proof to one on intersections of CFLs (there are many alternate approaches to this one)
Traces and Grammars
Traces

• A valid trace
  - # C₁ # C₂ # C₃ # C₄ … # C_{k-1} # Cₖ #,
  where \( k \geq 1 \) and \( C_i \Rightarrow_M C_{i+1} \), for \( 1 \leq i < k \).
  Here, \( \Rightarrow_M \) means derive in \( \mathbf{M} \), and \( C \) is a valid ID (Instantaneous Description)

• An invalid trace
  - # C₁ # C₂ # C₃ # C₄ … # C_{k-1} # Cₖ #,
  where \( k \geq 1 \) and, for some \( i \), it is false that \( C_i \Rightarrow_M C_{i+1} \).
Traces (Valid Computations)

• A terminating trace of a machine $M$, is a word of the form

$\# \ C_0 \ # \ C_1 \ # \ C_2 \ # \ C_3 \ # \ … \ # \ C_{k-1} \ # \ C_k \ #$

where $C_i \Rightarrow C_{i+1}$ $0 \leq i < k$, $C_0$ is a starting configuration and $C_k$ is a terminating configuration.

• We allow some laxness, where the configurations might be encoded in a manner appropriate to the machine model.
Traces are NOT CFLs

• In the previous, we assumed that a trace is NOT a CFL, but we never proved that.
• To show the trace language for a TM, M,
  \[
  \{ # C_1 # C_2 # C_3 # C_4 \ldots # C_{k-1} # C_k # | \ k \geq 1 \text{ and } C_i \Rightarrow_M C_{i+1}, \text{ for } 1 \leq i < k \} \]
  is not a CFL, we can focus on a simple machine that has just one non-blank \{1\} and one state \{q\} and the rules
  \[
  q \ 0 \ 0 \ q \\
  q \ 1 \ 1 \ q
  \]
• This machine has traces of the form
  \[
  \{ # C # C # C # C \ldots # C # C # \} \]
  as it never changes the tape contents or its state. It’s as hard as \{ww|w\in\{a,b\}^*\}
Using Pumping Lemma

• From previous slide, assume that the language of traces, 
  \( L = \{ \# \ C \# \ C \# \ C \# \ C \# \ ... \# \ C \# \ C \# \} \), involving no changes in the ID is Context Free
• Pumping Lemma gives me an \( N > 0 \)
• I choose the valid trace in \( L \) that is \( \# \ q \ 1^N \# \ q \ 1^N \# \ q \ 1^N \# \)
• PL breaks this up into \( uvwx \), \( |vwx| \leq N \), \( |vx| > 0 \) and \( \forall i \geq 0 \ uv^iwx^i y \in L \)
• Case 1: \( vx \) contains some 1’s. Due to fact that \( |vwx| \leq N \), the 1’s can come from at most two consecutive sequences of 1’s. If \( i=0 \), then we reduce 1’s in at most two subsequences, but not in the third, leading to an imbalance, and so the result is not in \( L \).
• Case 2: \( vx \) contains no 1’s, then it must be either ‘q’, ‘#’, or ‘#q’. In any case, if \( i=0 \) then we remove a state or a divider or both and the result is not a sequence of fixed configurations, so is not in \( L \).
• By PL, \( L \) is not a CFL.
The easiest way to show this for Turing machine traces is to describe an LBA that is given a string and wants to check if it is a valid trace.

The LBA could make a pass over to be sure the string starts with a #, ends with a #, has no 0’s immediately following a #, has a leading 0 immediately prior to a # only if the character preceding that 0 is a state, and has exactly one state between each pair of #’s.

The LBA could then check each pair by copying the second member of a pair under the first (2 tracks) and then marching over the two one character at a time until a state is found in one or the other.

It can then do checks that are based on the Turing machine rules with there being a need to look for differences in only three characters in each track (think about it).

Of course, all parts of configuration that are not altered must be checked to be sure they match on both tracks.
Details of Traces as CSL

• Easiest starting point is not Turing Machines but rather FRS’s with Residue

• Rules are of form
  \[ ax + b \rightarrow cx + d \]
  a, b, c, d are natural numbers,
  \[ 1 \leq b < a; \ 1 \leq d < c \]

• Can show that these systems do not require order as do FRS’s

• Residues can check for non-divisibility
Traces of FRS with Residues

- I have chosen, once again to use the Factor Replacement Systems, but this time, Factor Systems with Residues. The rules are unordered and each is of the form 
  \[ a \, x + b \rightarrow c \, x + d \]

- These systems need to overcome the lack of ordering when simulating Register Machines. This is done by
  \[
  \begin{align*}
  j. & \quad \text{INC}_r[i] \\
  & \quad p_{n+j} \, x \rightarrow p_{n+i} \, p_r \, x \\
  j. & \quad \text{DEC}_r[s, f] \\
  & \quad p_{n+j} \, p_r \, x \rightarrow p_{n+s} \, x \\
  & \quad p_{n+j} \, p_r \, x + k \, p_{n+j} \rightarrow p_{n+f} \, p_r \, x + k \, p_{n+f}, \; 1 \leq k < p_r
  \end{align*}
  \]

  We also add the halting rule associated with \( m+1 \) of 
  \[ p_{n+m+1} \, x \rightarrow 0 \]

- Thus, halting is equivalent to producing 0. We can also add one more rule that guarantees we can reach 0 on both odd and even numbers of moves 
  \[ 0 \rightarrow 0 \]
Non-Traces as Existential

- There are two ways that a string might not be a valid trace.
  - First, it might be ill-formed, but we can easily check if a word looks like a trace. If not, it is in the complement of valid traces.
  - Second, we can check pairs of configurations, \# C_i \# C_{i+1} to see if there is a transcription error; that is, we can check to see if it is the case that C_{i+1} does not follow from C_i in a valid trace.
- This is a non-deterministic process where we “guess” which pair might be in error and then, if the guess is correct, we accept the string as a bad one that just looks like a trace.
Non-Traces as Just One Error

• How hard is it to check for one bad transcription? Well, as noted above it starts with a guess, but then we must check. If it’s a TM trace, we use alternating ID reversals, so such a pair is either $\# C_i \# C_{i+1}^R$ or $\# C_i^R \# C_{i+1}$.

• Checking for an error here is is similar to what was described with the LBA and a single step check and can be done with a stack.

• What the stack cannot do is look at sequences longer than single pairs.
Intersection of CFLs

• Assume computations starts on ID $X_0$ and ends on a unique ID $Z_0$.

• Language of even odd pairs is $L_1$,
  
  $$L_1 = \{ #Y_0 # Y_1 # Y_2 # Y_3 # \ldots # Y_{2j} # Y_{2j+1} # \}$$
  
  where $Y_{2i} \Rightarrow Y_{2i+1}$, $0 \leq i \leq j$.
  
  This checks the even/odd steps of an even length computation.

• Language of of even pairs is $L_2$,
  
  $$L_2 = \{ #X_0 # X_1 # X_2 # X_3 # X_4 # \ldots # X_{2k-1} # X_2k # Z_0 # \}$$
  
  where $X_{2i-1} \Rightarrow X_{2i}$, $1 \leq i \leq k$.
  
  This checks the odd/even steps of an even length computation.

• Both $L_1$ and $L_2$ can be shown to be CFLs.
Intersection Continued

• Now, $X_0$ is chosen as some selected input ID to a machine, and $Z_0$ is the unique ID on which the machine halts. But,

$L_1 \cap L_2 = \{#X_0 # X_1 # X_2 # X_3 # X_4 # \ldots # X_{2k-1} # X_{2k}# Z_0 # \}$

where $X_i \Rightarrow X_{i+1}$, $0 \leq i < 2k$, and $X_{2k} \Rightarrow Z_0$.

• This checks all steps of an even length computation. But our original system halts if and only if it produces $Z_0$ in an even (also odd) number of steps.

• Thus, the intersection is non-empty just in case the machine eventually halts when started on $X_0$.

• This is an independent proof of the undecidability of the non-empty intersection problem for CFGs and the non-emptiness problem for CSGs.
Consequence of Partial Traces Being CFLs

- Now, a context free grammar can be devised which approximates traces by either getting the even-odd pairs right, or the odd-even pairs right.
- The goal is to then intersect the two languages, so the result is a trace.
- This then allows us to create CFLs $L_1$ and $L_2$, where $L_1 \cap L_2 \neq \emptyset$, just in case the machine has an element in its domain.
- Since this is undecidable, the non-emptiness of the intersection problem is also undecidable. This is an alternate proof to one we already showed based on PCP.
**Intersection of CFLs (precise)**

- Let \((n, ((a_1, b_1, c_1, d_1), \ldots, (a_k, b_k, c_k, d_k))\) be some factor replacement system with residues. Define grammars \(G_1\) and \(G_2\) by using the \(4k+2\) rules:
  
  \[
  G : F_i \rightarrow 1^{a_i} F_i 1^{c_i} \mid 1^{a_i+b_i} \# 1^{c_i+d_i} \quad 1 \leq i \leq k
  
  S_1 \rightarrow \# F_i S_1 \mid \# F_i \# \quad 1 \leq i \leq k
  
  S_2 \rightarrow \# 1^{x_0} S_1 1^{z_0} \# \quad Z_0 \text{ is 0 for us}
  
  \(G_1\) starts with \(S_1\) and \(G_2\) with \(S_2\)

- Thus, using the notation of writing \(Y\) in place of \(1^Y\),

  \[
  L_1 = L( G_1 ) = \{ \# Y_0 \# Y_1 \# Y_2 \# Y_3 \# \ldots \# Y_{2j} \# Y_{2j+1} \# \}
  \]

  where \(Y_{2i} \Rightarrow Y_{2i+1}, 0 \leq i \leq j\).

  This checks the even/odd steps of an even length computation.

  But, \(L_2 = L( G_2 ) = \{ \# X_0 \# X_1 \# X_2 \# X_3 \# X_4 \# \ldots \# X_{2k-1} \# X_{2k} \# Z_0 \# \}
  \]

  where \(X_{2i-1} \Rightarrow X_{2i}, 1 \leq i \leq k\).

  This checks the odd/even steps of an even length computation.

- Given that the intersection of two CFLs is at worst a CSL, we now have an indirect way of showing that the valid terminating traces are a CSL.
Intersection Continued

Now, $X_0$ is chosen as some selected input value to the Factor System with Residues, and $Z_0$ is the unique value (0 in our case) on which the machine halts. But,

$L_1 \cap L_2 = \{#X_0 \# X_1 \# X_2 \# X_3 \# X_4 \# \ldots \# X_{2k-1} \# X_{2k} \# Z_0 \# \}$

where $X_i \Rightarrow X_{i+1}$, $0 \leq i < 2k$, and $X_{2k} \Rightarrow Z_0$. This checks all steps of an even length computation. But our original system halts if and only if it produces 0 ($Z_0$) in an even (also odd) number of steps. Thus, the intersection is non-empty just in case the Factor System with residue eventually produces 0 when started on $X_0$, just in case the Register Machine halts when started on the register contents encoded by $X_0$.

This is an independent proof of the undecidability of the non-empty intersection problem for CFGs and the non-emptiness problem for CSGs.
What’s a CSL or CFL?

• Given some machine \( M \) (details are model dependent)
  – The set of valid traces of \( M \) is Context Sensitive
    (can prove by fact that intersection of two CFLs is a CSG or by direct construction)
  – The complement of the valid traces of \( M \) is Context Free; that is, the set of invalid traces of \( M \) is Context Free (just one mistake required)
  – The set of valid terminating traces of \( M \) is Context Sensitive (same as above)
  – The complement of the valid terminating traces of \( M \) is Context Free; again, this requires just one mistake
What’s Undecidable?

• We cannot decide if the set of valid terminating traces of an arbitrary machine $M$ is non-empty (machine accepts something) – $L(M) \neq \emptyset$

• We cannot decide if the complement of the set of valid terminating traces of an arbitrary machine $M$ is everything. In fact, this is not even semi-decidable.
$L = \Sigma^*$?

- If $L$ is regular, then $L = \Sigma^*$? is decidable
  - Easy – Reduce to minimal deterministic FSA, $A_L$ accepting $L$. $L = \Sigma^*$ iff $A_L$ is a one-state machine, whose only state is accepting

- If $L$ is context free, then $L = \Sigma^*$? is undecidable
  - Just produce the complement of a machine’s valid terminating traces; if it’s $\Sigma^*$ then the original machine accepted nothing
Quotients of CFLs (concept)

Let \( L_1 = L( G_1 ) = \{ \# Y_0 \# Y_1 \# Y_2 \# Y_3 \# \ldots \# Y_{2j} \# Y_{2j+1} \# \} \)
where \( Y_{2i} \Rightarrow Y_{2i+1}, \ 0 \leq i \leq j. \)
This checks the even/odd steps of an even length computation.

Now, let \( L_2 = L( G_2 ) = \{ X_0 \# X_0 \# X_1 \# X_2 \# X_3 \# X_4 \# \ldots \# X_{2k-1} \# X_{2k} \# Z_0 \# \} \)
where \( X_{2i-1} \Rightarrow X_{2i}, \ 1 \leq i \leq k \) and \( Z_0 \) is a unique halting configuration.
This checks the odd/steps of an even length computation and includes an extra copy of the starting number prior to its \$.

Now, consider the quotient of \( L_2 / L_1 \). The only way a member of \( L_1 \) can match a final substring in \( L_2 \) is to line up the \$ signs. But then they serve to check out the validity and termination of the computation. Moreover, the quotient leaves only the starting point (the one on which the machine halts.) Thus,

\( L_2 / L_1 = \{ X_0 | \text{the system being traced halts} \}. \)

Since deciding the members of an re set is in general undecidable, we have shown that membership in the quotient of two CFLs is also undecidable.

Note: Intersection of two CFLs is a CSL but quotient of two CFLs is an re set and, in fact, all re sets can be specified by such quotients.
Quotients of CFLs (precise)

- Let \((n, ((a_1, b_1, c_1, d_1), \ldots, (a_k, b_k, c_k, d_k))\) be some factor replacement system with residues. Define grammars \(G_1\) and \(G_2\) by using the \(4k+4\) rules

\[
\begin{align*}
G & : F_i \rightarrow 1^{ai}F_i 1^{ci} | 1^{ai+bi}1^{ci+di} & 1 \leq i \leq k \\
T_1 & \rightarrow \# F_i T_1 | \# F_i \# & 1 \leq i \leq k \\
A & \rightarrow 1 A 1 | $ \# \\
S_1 & \rightarrow $T_1 \\
S_2 & \rightarrow A T_1 \# 1^{z_0} \# \\
\end{align*}
\]

\(G_1\) starts with \(S_1\) and \(G_2\) with \(S_2\)
- Thus, using the notation of writing \(Y\) in place of \(1^Y\),

\[
L_1 = L(G_1) = \{ $ \# Y_0 \# Y_1 \# Y_2 \# Y_3 \# \ldots \# Y_{2j} \# Y_{2j+1} \# \}
\]

where \(Y_{2i} \Rightarrow Y_{2i+1}, 0 \leq i \leq j\).

This checks the even/odd steps of an even length computation.

But, \(L_2 = L(G_2) = \{ X $ \# X_0 \# X_1 \# X_2 \# X_3 \# X_4 \# \ldots \# X_{2k-1} \# X_{2k} \# Z_0 \# \}
\]

where \(X_{2i-1} \Rightarrow X_{2i}, 1 \leq i \leq k\) and \(X = X_0\).

This checks the odd/steps of an even length computation, and includes an extra copy of the starting number prior to its $.
Summarizing Quotient

Now, consider the quotient $L_2 / L_1$ where $L_1$ and $L_2$ are the CFLs on prior slide. The only way a member of $L_1$ can match a final substring in $L_2$ is to line up the $\$$ signs. But then they serve to check out the validity and termination of the computation. Moreover, the quotient leaves only the starting number (the one on which the machine halts.) Thus, $L_2 / L_1 = \{ X \mid \text{the system F halts on zero} \}$. Since deciding the members of an re set is in general undecidable, we have shown that membership in the quotient of two CFLs is also undecidable.
Traces and Type 0

- Here, it is easier to show a simulation of a Turing machine than of an FRS.
- Assume we are given some machine M, with Turing table T (using Post notation). We assume a tape alphabet of \( \Sigma \) that includes a blank symbol B.
- Consider a starting configuration \( C_0 \). Our rules will be:

\[
\begin{align*}
S & \rightarrow \# C_0 \# \quad \text{where } C_0 = \alpha \varepsilon 0 \varepsilon \beta \text{ is initial ID} \\
q a & \rightarrow s b \quad \text{if } q a b s \in T \\
b q a x & \rightarrow b a s x \quad \text{if } q a R s \in T, a,b,x \in \Sigma \\
b q a # & \rightarrow b a s B # \quad \text{if } q a R s \in T, a,b \in \Sigma \\
# q a x & \rightarrow # a s x \quad \text{if } q a R s \in T, a,x \in \Sigma, a \neq B \\
# q a # & \rightarrow # a s B # \quad \text{if } q a R s \in T, a \in \Sigma, a \neq B \\
# q a x & \rightarrow # s x # \quad \text{if } q a R s \in T, x \in \Sigma, a = B \\
# q a # & \rightarrow # s B # \quad \text{if } q a R s \in T, a = B \\
b q a x & \rightarrow s b a x \quad \text{if } q a L s \in T, a,b,x \in \Sigma \\
# q a x & \rightarrow # s B a x \quad \text{if } q a L s \in T, a,x \in \Sigma \\
b q a # & \rightarrow s b a # \quad \text{if } q a L s \in T, a,b \in \Sigma, a \neq B \\
# q a # & \rightarrow # s B a # \quad \text{if } q a L s \in T, a \in \Sigma, a \neq B \\
b q a # & \rightarrow s b # \quad \text{if } q a L s \in T, b \in \Sigma, a = B \\
# q a # & \rightarrow # s B # \quad \text{if } q a L s \in T, a = B \\
f & \rightarrow \lambda \quad \text{if } f \text{ is a final state} \\
# & \rightarrow \lambda \quad \text{just cleaning up the dirty linen}
\end{align*}
\]

© UCF CS
CSG and Undecidability

• We can almost do anything with a CSG that can be done with a Type 0 grammar. The only thing lacking is the ability to reduce lengths, but we can throw in a character that we think of as meaning “deleted”. Let’s use the letter d as a deleted character and use the letter e to mark both ends of a word.

• Let G = (V, T, P, S) be an arbitrary Type 0 grammar.

• Define the CSG G' = (V ∪ {S', D}, T ∪ {d, e}, S', P'), where P' is

  \[
  \begin{align*}
  S' & \rightarrow e \ S \ e \\
  D \ x & \rightarrow x \ D \quad \text{when } x \in V \cup T \\
  D \ e & \rightarrow e \ d \quad \text{push the delete characters to far right} \\
  \alpha & \rightarrow \beta \quad \text{where } \alpha \rightarrow \beta \in P \text{ and } |\alpha| \leq |\beta| \\
  \alpha & \rightarrow \beta \ D^k \quad \text{where } \alpha \rightarrow \beta \in P \text{ and } |\alpha| - |\beta| = k > 0
  \end{align*}
  \]

• Clearly, \( L(G') = \{ e \ w \ e \ d^m \ | \ w \in L(G) \text{ and } m \geq 0 \text{ is some integer } \} \)

• For each \( w \in L(G) \), we cannot, in general, determine for which values of \( m, e \ w \ e \ d^m \in L(G') \). We would need to ask a potentially infinite number of questions of the form “does \( e \ w \ e \ d^m \in L(G') \)” for some \( m \geq 0 \) to determine if \( w \in L(G) \). That’s a semi-decision procedure because \( m \) can be unbounded above.
Some Consequences

• CSGs are not closed under Init, Final, Mid, quotient with regular sets, substitution and homomorphism (okay for $\lambda$-free homomorphism and non-length reducing substitutions)

• We also have that the emptiness problem is undecidable from this result. That gives us another proof of this one result.

• For Type 0, emptiness and even the membership problems are undecidable.
Undecidability

• Is \( L = \emptyset \), for CSL, \( L \)?
• Is \( L = \Sigma^* \), for CFL (CSL), \( L \)?
• Is \( L_1 = L_2 \) for CFLs (CSLs), \( L_1, L_2 \)?
• Is \( L_1 \subseteq L_2 \) for CFLs (CSLs), \( L_1, L_2 \)?
• Is \( L_1 \cap L_2 = \emptyset \) for CFLs (CSLs), \( L_1, L_2 \)?
• Is \( L \) regular, for CFL (CSL), \( L \)?
• Is \( L_1 \cap L_2 \) a CFL for CFLs, \( L_1, L_2 \)?
• Is \( \sim L \) CFL, for CFL, \( L \)?
More Undecidability

- Is CFL, L, ambiguous?  PCP
- Is L = L^2, L a CFL?  Will Do
- Is L_1/L_2 finite, L_1 and L_2 CFLs?  Language is any RE set
- Membership in L_1/L_2, L_1 and L_2 CFLs?  Language is any RE set
Summary of Grammar Results
Decidability

- Everything about regular
- Membership in CFLs and CSLs
  - CKY for CFLs
- Emptiness for CFLs
- Finiteness of CFLs
Undecidability

• Is \( L = \emptyset \), for CSL, \( L \)?
• Is \( L = \Sigma^* \), for CFL (CSL), \( L \)?
• Is \( L_1 = L_2 \) for CFLs (CSLs), \( L_1, L_2 \)?
• Is \( L_1 \subseteq L_2 \) for CFLs (CSLs ), \( L_1, L_2 \)?
• Is \( L_1 \cap L_2 = \emptyset \) for CFLs (CSLs ), \( L_1, L_2 \)?
More Undecidability

• Is CFL, L, ambiguous?
• Is $L = L^2$, L a CFL?
• Does there exist a finite n, $L^n = L^{n+1}$?
• Is $L_1/L_2$ finite, $L_1$ and $L_2$ CFLs?
• Membership in $L_1/L_2$, where $L_1$ and $L_2$ are CFLs?
Word to Grammar Problem

• Recast semi-Thue system making all symbols non-terminal, adding S and V to non-terminals and terminal set $\Sigma = \{a\}$

$$G: S \rightarrow h1^{x}q_{1}0h$$
$$hq_{0}h \rightarrow V$$
$$V \rightarrow aV$$
$$V \rightarrow \lambda$$

• $x \in \mathcal{L}(M)$ iff $\mathcal{L}(G) \neq \emptyset$ iff $\mathcal{L}(G)$ infinite
  iff $\lambda \in \mathcal{L}(G)$ iff $a \in \mathcal{L}(G)$ iff $\mathcal{L}(G) = \Sigma^{*}$
Consequences for PSG

• Unsolvables
  – \( \mathcal{L}(G) = \emptyset \)
  – \( \mathcal{L}(G) = \Sigma^* \)
  – \( \mathcal{L}(G) \) infinite
  – \( w \in \mathcal{L}(G) \), for arbitrary \( w \)
  – \( \mathcal{L}(G) \supseteq \mathcal{L}(G2) \)
  – \( \mathcal{L}(G) = \mathcal{L}(G2) \)

• Latter two results follow when have
  – G2: \( S \to aS \mid \lambda \quad a \in \Sigma \)
Finite Convergence for Concatenation of Context-Free Languages

Relation to Real-Time (Constant Time) Execution
Traces: Representing IDs

- We create a trace of a Turing Machine model, each ID is of the form $\alpha q \alpha \beta$ where $\alpha$ is the shortest string representing all non-blanks to the left of the scanned square and $\beta$ is the shortest string representing all non-blanks to the left of the scanned square. $q$ is the state and $a$ is the character at the scanned square.

- For a Turing Machine model using binary tapes
  $r = (1(0+1)^* + \lambda) \ q \ (0+1) \ (\lambda + (0+1)^*1)$
  where $q = (q_1 + q_2 + \ldots q_n)$ if $Q = \{q_1, q_2, \ldots, q_n\}$

- A trace-like string is then either
  $t = (#r)^+#$

- As trace-like is Regular so are strings that don’t look like traces since Regular are closed un complement
Traces: Single Steps

• A single step of any derivation in $M$ is a pair of configurations $C_1\#C_2\#$ where $C_1 \Rightarrow_M C_2$.

• For Turing machines, because the strings are over multiple letters, a pair like $C_1\#C_2\#$ is as hard to generate as words of the form
  \{ww \mid w \text{ is over a multi-letter alphabet}\}.

• To circumvent this, we represent TM pairs by reversing one of the two IDs, e.g., $C_1\#C_2^R\#$ or $C_1^R\#C_2\#$
Why CFLs?

• I have glossed over some complexity
• A single step of a TM can be checked by a Deterministic PDA. As DCFLS are closed under complement, we have that incorrect single steps are also DCFLs
• Showing the single step checker is not hard but again requires that we are looking at either $C_1 \# C_2 R \#$ or $C_1 R \# C_2 \#$
Traces: Multiple Steps

• A multistep derivation in $M$ is a sequence of configurations $C_1#C_2# \ldots #C_k#$ where $C_i \Rightarrow_M C_{i+1}$.
• Multistep (>1) traces are Context Sensitive.
• For Turing machines, we often alternate between unreversed and reversed as in $C_1#C_2^R#C_3#C_4^R \ldots$
• This reversing is not needed by the CSG but is convenient when we want to consider that a CFL can get every other pair right or can get a bad trace by just messing up once.
Constant Time Again

• $\textit{CTime} = \{ M \mid \exists K \forall C \left[ \text{STP}(M, C, K) \right] \}$

• This would appear to imply that $\textit{CTime}$ is not even re. However, a TM that only runs for $K$ steps can scan at most $K$ distinct tape symbols. Thus, if we use unary notation, $\textit{CTime}$ can be expressed as:

• $\textit{CTime} = \{ M \mid \exists K \forall C_{|C|\leq K} \left[ \text{STP}(M, C, K) \right] \}$

• We can dovetail over the set of all TMs, $M$, and all $K$, listing those $M$ that halt in constant time.
Powers of CFLs

Let G be a context free grammar.
Consider $L(G)^n$

Question1: Is $L(G) = L(G)^2$?

Question2: Is $L(G)^n = L(G)^{n+1}$, for some finite $n > 0$?

These questions are both undecidable.

Think about why question1 is as hard as whether or not $L(G)$ is $\Sigma^*$.

Question2 requires much more thought.
L(G) = L(G)^2?

• The problem to determine if \( L = \Sigma^* \) is Turing reducible to the problem to decide if \( L \cdot L \subseteq L \), so long as \( L \) is selected from a class of languages \( C \) over the alphabet \( \Sigma \) for which we can decide if \( \Sigma \cup \{\lambda\} \subseteq L \).

• Corollary 1:
The problem “is \( L \cdot L = L \), for \( L \) context free or context sensitive?” is undecidable
L(G) = L(G)^2? is undecidable

- Question: Does L • L get us anything new?
  - i.e., Is L • L = L?
- Membership in a CFL is decidable.
- Claim is that L = Σ* iff
  (1) Σ \cup \{\lambda\} \subseteq L ; and
  (2) L • L = L
- Clearly, if L = Σ* then (1) and (2) trivially hold.
- Conversely, we have Σ* \subseteq L^* = \bigcup_{n \geq 0} L^n \subseteq L
  - first inclusion follows from (1); second from (2)
Finite Power Problem for Turing Machine Model

• The problem to determine, for an arbitrary context free language L, if there exist a finite n such that $L^n = L^{n+1}$ is undecidable.

• $L_1 = \{ C_1 \# C_2^R \$ | C_1, C_2 \text{ are configurations} \}$

• $L_2 = \{ C_1 \# C_2^R \$C_3 \# C_4^R \ldots \$ C_{2k-1} \# C_{2k}^R \$ \mid \text{where } k \geq 1 \text{ and, for some } i, 1 \leq i < 2k, C_i \Rightarrow_M C_{i+1} \text{ is false} \}$

• $L = L_1 \cup L_2 \cup \{ \lambda \}$

• $L$ is context free.
Undecidability of $\exists n L^n = L^{n+1}$

- Any product of $L_1$ and $L_2$, which contains $L_2$ at least once, is $L_2$.
  For instance, $L_1 \cdot L_2 = L_2 \cdot L_1 = L_2 \cdot L_2 = L_2$.
- This shows that $(L_1 \cup L_2)^n = L_1^n \cup L_2$.
- Thus, $L^n = \{\lambda\} \cup L_1 \cup L_1^2 \ldots \cup L_1^n \cup L_2$.
- Analyzing $L_1$ and $L_2$ we see that $L_1^n \cup L_2 \neq L_2$ just in case there is a word
  $C_1 \# C_2^R \$ C_3 \# C_4^R \ldots \$ C_{2n-1} \# C_{2n}^R \$ in $L_1^n$ that is not also in $L_2$.
- But then there is some valid trace of length $2n$.
- $L$ has the finite power property iff $M$ executes in constant time.
Missing Step

• We have that \textbf{CT} (Constant-Time) is many-one reducible to Finite Power Problem (\textbf{FPC}) for CFLs.

• This means that if \textbf{CT} is unsolvable, so is \textbf{FPC} for CFLs.

• However, we still lack a proof that \textbf{CT} is unsolvable. I am keeping that open as one of the problems that you folks can attack in your presentation. It takes two papers to get here. I’ll document that.
Sketch that $CT \equiv \text{Uniform Halting for Infinite Markings}$

- If $M$ is in $CT$ then it halts in a fixed time, then input read is independent of tape markings.
- This implies $M$ halts even if infinitely marked.
- If $M$ halts under all markings, even infinite ones, then there must be some bound on its running time that is independent of its input.
- This implies $M$ is in $CT$. 

3/1/23 © UCF CS
Revisiting PCP

Constrained to a single letter
Single Letter Alphabet PCP

- $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n), \Sigma = \{a\}$
- Can recast as just lengths
  - If $\exists i, 1 \leq i \leq n, |x_i| = |y_i|$, then say YES
  - If $\forall i, 1 \leq i \leq n, |x_i| > |y_i|$, then say NO
  - If $\forall i, 1 \leq i \leq n, |x_i| < |y_i|$, then say NO
- Else $\exists i, j, i \neq j, 1 \leq i, j \leq n, |x_i| > |y_i|$ and $|x_j| < |y_j|
  - Let $s = |x_i| - |y_i|$ and $t = |y_j| - |x_j|$
  - Solution i repeated t times, j repeated s times
  - x part is $|x_i| * (|y_j| - |x_j|) + |x_j| * (|x_i| - |y_i|)$
  - y part is $|y_i| * (|y_j| - |x_j|) + |y_j| * (|x_i| - |y_i|)$

$|x_i|*|y_j| - |x_i|*|x_j| + |x_j|*|x_i| - |x_j|*|y_i| = |x_i|*|y_j| - |x_j|*|y_i|$

$|y_i|*|y_j| - |y_i|*|x_j| + |y_j|*|x_i| - |y_j|*|y_i| = |x_i|*|y_j| - |x_j|*|y_i|$
More Exam Prep
Sample Question

Let $A$ and $B$ be re sets. For each of the following, either prove that the set is re, or give a counterexample that results in some known non-re set.

Let $A$ be semi decided by $f_A$ and $B$ by $f_B$

a) $A \cup B$: must be re as it is semi-decided by
   
   $f_{A \cup B} (x) = \exists t \ [ \text{stp}(f_A, x, t) \lor \text{stp}(f_B, x, t) ]$

b) $A \cap B$: must be re as it is semi-decided by
   
   $f_{A \cap B} (x) = \exists t \ [ \text{stp}(f_A, x, t) \land \text{stp}(f_B, x, t) ]$

c) $\sim A$: can be non-re. If $\sim A$ is always re, then all re are recursive as any set that is re and whose complement is re is decidable. However, $A = K$ is a non-rec, re set and so $\sim A$ is not re.
Sample Question

Given that the predicate $\text{STP}$ and the function $\text{VALUE}$ are prf’s, show that we can semi-decide

\{ f | \varphi_f \text{ evaluates to 0 for some input} \}

This can be shown re by the predicate

\{ f | \exists <x,t> [ \text{stp}(f,x,t) \land \text{value}(f,x,t) = 0 ] \}
Sample Question

Let \( S \) be an re (recursively enumerable), non-recursive set, and \( T \) be re, non-empty, possibly recursive set. Let \( E = \{ z \mid z = x + y, \text{ where } x \in S \text{ and } y \in T \} \).

(a) Can \( E \) be non re? \( \text{No as we can let } S \text{ and } T \text{ be semi-decided by } f_S \text{ and } f_T, \text{ resp.}, E \text{ is then semi-dec. by} \)
\[
f_E(z) = \exists <x,y,t> [ \text{stp}(f_S, x, t) \land \text{stp}(f_T, y, t) \land (z = \text{value}(f_S, x, t) + \text{value}(f_T, y, t))]\
\]

(b) Can \( E \) be re non-recursive? \( \text{Yes, just let } T = \{0\}, \text{ then } E = S \text{ which is known to be re, non-rec.} \)

(c) Can \( E \) be recursive? \( \text{Yes, let } T = \emptyset, \text{ then } E = \{ x \mid x \geq \text{min}(S) \} \text{ which is a co-finite set and hence rec.} \)
Sample Question

Assuming TOTAL is undecidable, use reduction to show the undecidability of

\[ \text{Incr} = \{ f \mid \forall x \; \varphi_f(x+1) > \varphi_f(x) \} \]

Let \( f \) be arb.

Define \( G_f(x) = \varphi_f(x) - \varphi_f(x) + x \)

\( f \in \text{TOTAL} \iff \forall x \varphi_f(x) \downarrow \iff \forall x \; G_f(x) \downarrow \iff \forall x \; \varphi_f(x) - \varphi_f(x) + x = x \) implies \( G_f \in \text{Incr} \)

\( f \notin \text{TOTAL} \iff \exists x \varphi_f(x) \uparrow \iff \exists x \; G_f(x) \downarrow \iff \exists x \; (\varphi_f(x) - \varphi_f(x) + x) \downarrow \) implies \( G_f \notin \text{Incr} \)

You can overload \( f \) to be index and function, i.e., \( f(x) \) as \( \varphi_f(x) \)
Let $\text{Incr} = \{ f \mid \forall x, \varphi_f(x+1) > \varphi_f(x) \}$. Let $\text{TOTAL} = \{ f \mid \forall x, \varphi_f(x) \downarrow \}$. Prove that $\text{Incr} \leq_m \text{TOTAL}$.

Let $f$ be arb. Define $G_f(x) = \exists t[\text{stp}(f,x,t) \land \text{stp}(f,x+1,t) \land (\text{value}(f,x+1,t) > \text{value}(f,x,t))]]$

$f \in \text{Incr}$ iff $\forall x \varphi_f(x+1) > \varphi_f(x)$ iff $\forall x G_f(x) \downarrow$ iff $G_f \in \text{TOT}$.
Let $\text{Incr} = \{ f \mid \forall x \varphi_f(x+1) > \varphi_f(x) \}$. Use Rice’s theorem to show $\text{Incr}$ is not recursive.

Non-Trivial as

$C_0(x) = 0 \notin \text{Incr}$; $S(x) = x+1 \in \text{Incr}$

Let $f, g$ be arb. Such that $\forall x \varphi_f(x) = \varphi_g(x)$

$f \in \text{Incr}$ iff $\forall x \varphi_f(x+1) > \varphi_f(x)$ iff

$\forall x \varphi_g(x+1) > \varphi_g(x)$ iff $g \in \text{Incr}$
Sample Question

Let $S$ be a recursive (decidable set), what can we say about the complexity (recursive, re non-recursive, non-re) of $T$, where $T \subset S$?

Nothing. Just let $S = \emptyset$, then $T$ could be any subset of $\emptyset$. There are an uncountable number of such subsets and some are clearly in each of the categories above.
Let $P = \{ f | \exists x \ [ \text{STP}(f, x, x) ] \}$. Why does Rice’s theorem not tell us anything about the undecidability of $P$?

This is not an I/O property as we can have implementations of $C_0$ that are efficient and satisfy $P$ and others that do not.
True/False

• Membership in Context-Sensitive Languages is unsolvable
• Membership in Regular Languages can be solved in linear time
• We cannot decide if the intersection of two CFLs is a CFL
• The Post Correspondence Problem over a one-letter alphabet is undecidable
We learned that quantification can be used to determine the upper bound of the complexity of some problem. The general form of such expressions is $Q \left[ \text{Algorithmic Predicate} \right]$. Here $Q$ is a sequence of alternating quantifiers. Usually, the predicate is Primitive Recursive involving the functions STP and VALUE. I will give you a set (membership in it is the problem) and an associated predicate. The Quantifier part won't be specified, and you will need to choose from a set of options what that quantifier is.

- $S = \{ f \mid \text{Domain}(f) \text{ is infinite} \}$
- $f \in S \iff Q \left[ \text{STP}(f, x, t) \& x > y \right]$
- $Q$ is the part you must pick from a list
Matching

• When do variants of Rice’s apply. For example, which version would you use for $S = \{ f \mid \text{Range}(f) \text{ is infinite} \}$?
• What is an inherent property of some problem, e.g., HALT is re-complete, TOTAL is non-re
Closures of Languages

• A Regular and B CFL. What about $A \cap B$?
  – Can it be Regular
  – Can it be a CFL, non-Regular
  – Can it be a CSL, non-CFL

• A Recursive non-empty, B non-re. What about $A \cap B$?
  – Can it be Recursive
  – Can it be RE non-Recursive
  – Can it be non-RE
Others

• Properties of various language classes and procedures for analyzing language classes.