What is computability?

Up until this point, the course has focused on tractability: whether problems can be solved by a computer algorithm in a reasonable amount of time with respect to the size of the problem. Here, we consider the broader question of computability, or what can be achieved by a computer at all.

Computability is a property of a computational problem. More specifically, a problem is computable if there exists an algorithm that solves the problem that can be performed by a computer with unlimited memory in finite time. We do not specify any other limit on the running time; it could require exponentially many steps or arbitrarily large amounts of memory to run an algorithm that solves this problem, but if the problem is computable, we know that the algorithm will conclude in a finite amount of time. Even with this unrestricted a bound on what is required to be computable, however, there still exist problems that are uncomputable, i.e. for which we can prove that no such algorithm exists to solve them.

Models of computation and the Church-Turing thesis

The definition of computability given above is informal because we have not yet given formal mathematical meaning to terms such as algorithm and computer. This same issue, of course, affects everything we’ve said about algorithms up until this point in the course. However, it not an important issue when asserting the existence of a particular algorithm to solve a particular problem. The particular algorithm being analyzed is generally presented in a mathematically precise way, and the assertion that it is possible to run the algorithm on a computer is not presented as a mathematical assertion but as a factual claim that you can verify by coding up the algorithm yourself and running it.

On the other hand, when asserting the non-existence of algorithms to solve a particular problem (i.e. when asserting that a problem is uncomputable) the lack of a precise definition of algorithms and computation becomes a fatal flaw in the logic. If one is imprecise about the meanings of these terms, one might always wonder, “Is it really impossible to design an algorithm to solve this problem, or has mankind just failed to come up with the right hardware or software...
feature that makes the problem solvable?"

In the 1930's, mathematicians formalized the definitions of algorithms and computation in different ways. Perhaps the two most famous and influential such definitions are the lambda calculus the Turing machine, both proposed in the 1930's by Alonzo Church and Alan Turing, respectively. Lambda calculus is briefly discussed in CS 3110 and constitutes a core topic of CS 4110. Turing machines, which we’ll encounter later in these notes, are basically discrete finite automata augmented with an infinite memory. These two models of computation, and all of the other universal models of computation proposed before or since, have been found to be computationally equivalent, meaning that any problem which is computable in one model is computable in all of them. These computationally equivalent models are collectively referred to as Turing-complete. Because Turing-complete models are capable of describing every computational process that computer scientists, mathematicians, philosophers, and natural scientists have ever been able to imagine, the scientific community generally subscribes to the Church-Turing thesis, asserting that any computation that can be feasibly performed in our universe can be performed using the lambda calculus, a Turing machine, or any other Turing-complete model of computation. The Church-Turing thesis is not a mathematical theorem, it is a meta-mathematical statement about the meaning of algorithms and computation. In that sense, when we say a problem is uncomputable, the real meaning of the statement is, “No algorithm can solve this problem in a universe where the capabilities of algorithms and computers obey the Church-Turing thesis, and there is strong consensus in the scientific community that our universe is one such universe.” The discovery of a computer that can violate the Church-Turing thesis would be a flabbergasting discovery, akin to the discovery of faster-than-light transportation, but it is not a possibility that can be ruled out mathematically.

Turing-complete models of computation tend to have some key characteristics in common. These are:

1. Algorithms are described by finite-sized programs.
2. Computers execute algorithms using a finite amount of internal state and an infinite amount of memory.
3. The program describing one algorithm can be used as the input to another algorithm.
4. The programming language is sophisticated enough that it is capable of universality: one can write an algorithm that can simulate the execution of any other algorithm, given that algorithm’s

Definition Two models of computation are computationally equivalent if they define the same set of computable problems. The Turing-complete models of computation are those that model the capabilities of general-purpose computers.
The assumption that algorithms run on computers with an infinite amount of memory is clearly not realistic. There are two justifications for making this assumption. First, modern computers have access to so much memory (especially if they are attached to a network) that for most practical purposes one doesn’t have to worry about the limitations on how much data they can store. Second, since our main intent in this part of the course is to prove limitations on the power of computation, if we can prove that a problem is impossible to solve even on a hypothetical computer equipped with infinite memory, it implies a fortiori that the problem is also unsolvable on a real-world computer with finite memory.

You have already learned at least one programming language, e.g. Java, that is Turing-complete. Certain features of the Java language (classes, methods, inheritance, generic types, exception handling, importing packages, etc.) are convenient for the purpose of writing programs but inconvenient for the purpose of reasoning formally about their semantics. Therefore, in these notes, we will formalize the model of computation using two computationally equivalent models: Turing machines, and a very simple programming language we will define called SJAVA or Simplified Java, whose syntax resembles Java minus the object-oriented features of the language. Turing machines furnish an economical definition of computation with the minimum number of conceptual ingredients; however, they are ill-suited for expressing algorithms in a human-readable form. SJAVA is designed to be comparable to Java code in terms of readability, with the benefit that its semantics are much easier to comprehend and formalize than the semantics of Java.

3 Turing machines

A Turing machine can be thought of as a finite state machine sitting on an infinitely long tape containing symbols from some finite alphabet $\Sigma$. Based on the symbol it’s currently reading, and its current state, the Turing machine writes a new symbol in that location (possibly the same as the previous one), moves left or right or stays in place, and enters a new state. It may also decide to halt. The machine’s transition function is the “program” that specifies each of these actions (next state, next symbol to write, and direction to move on the tape) given the current state and the symbol the machine is currently reading.

Actually, we will base our model of computation on a generalization of this idea, the multi-tape Turing machine, which has a finite
number of infinite tapes (potentially more than one) each with its own read-write head that can move independently of the others. A single finite state controller jointly controls all of the read-write heads.

**Specification of a Turing machine**

**Definition 1.** A Turing machine is specified by:

1. a finite set $\Sigma$ called the *alphabet*, with a distinguished subset $\Omega$ called the set of *input symbols* and a distinguished element of $\Sigma \setminus \Omega$ called the *blank symbol* and denoted by underscore (_);

2. a finite set of states $Q$ with two distinguished elements: $s$ (the starting state) and $t$ (the terminal or halting state);

3. a finite set of tapes $[T] = \{1, 2, \ldots, T\}$ with two distinguished subsets $I$ (the input tapes) and $O$ (the output tapes);

4. a *transition function*

$$
\delta : Q \times \Sigma^T \to Q \times \Sigma^T \times \{-1, 0, 1\}^T
$$

that specifies, for any given state and $T$-tuple of symbols, what the machine should do next: the state to which it transitions, the $T$-tuple of symbols that it writes on its tapes, and the $T$-tuple of directions that it moves on each tape.

Often, a Turing machine is defined as having a single tape that serves as both the input and the output tape (i.e., the case $T = 1$ and $I = O = [T]$). This definition is conceptually simpler and is computationally equivalent in the sense that any function computable by a multi-tape Turing machine is also computable by a single-tape Turing machine. However algorithms implemented on single-tape Turing machines often have asymptotically slower running times than the same algorithm implemented on modern computing hardware with random-access memory. Multi-tape Turing machines, which lacking an abstraction of random access memory, tend to permit implementations of algorithms whose running time has the same asymptotic order of growth as if they were implemented on a random-access machine. For this reason, we prefer the multi-tape formalism in CS 4820.

**Configurations and computations**

Having defined the *specification* of a Turing machine, we must now pin down a definition of *how they operate* and *what they compute*. This has been informally described above, but it’s time to make it
formal. That begins with formally defining the configuration of the Turing machine at any time (the contents of its tapes, as well as the machine’s own state and its position on each tape) and the rules for how its configuration changes over time.

The set \( \Sigma^* \) is the set of all finite sequences of elements of \( \Sigma \), and \( \Sigma^\infty \) is the set of all infinite sequences of elements of \( \Sigma \) that are finitely supported, meaning that all but finitely many elements of the sequence are equal to \( \_ \). When an element of \( \Sigma^* \) is denoted by a letter such as \( x \), then the elements of the sequence \( x \) are denoted by \( x[0], x[1], x[2], \ldots, x[n - 1] \), where \( n \) is the length of \( x \) and is denoted by \( |x| \). Similarly for an infinite sequence \( x \in \Sigma^\infty \), the elements of \( x \) are denoted by \( x[0], x[1], \ldots \).

A configuration of a Turing machine is an ordered triple \((q, x, k) \in Q \times (\Sigma^\infty)^T \times \mathbb{N}^T\), where \( q \) denotes the machine’s current state, \( x = (x_1, x_2, \ldots, x_T) \) denotes \( T \)-tuple of strings on the tapes, and \( k = (k_1, k_2, \ldots, k_T) \) denotes the \( T \)-tuple of positions of the machine on the tapes.

Suppose \( M \) is a Turing machine and \((q, x, k) \) is its configuration at any point in time. If \( q \neq t \) (the machine hasn’t halted) then the configuration at the following point in time, \((q', x', k') \), is determined as follows. Let \( \sigma = (\sigma_1, \ldots, \sigma_T) \) denote the \( T \)-tuple of symbols that the machine is reading, i.e. \( \sigma_i = x_i[k_i] \) for all \( i \in [T] \). Let \((q', \rho, \ell) = \delta(q, \sigma) \). For all \( i \in [T] \) the new string on tape \( i \), \( x'_i \), is obtained from \( x_i \) by changing \( x_i[k_i] \) to \( \rho_i \). The new position \( k'[i] \) is equal to \( k[i] + \ell[i] \) unless \( k[i] + \ell[i] = -1 \), in which case \( k'[i] = 0 \). We say that \( M \) transitions from \((q, x, k) \) to \((q', x', k') \).

A computation of a Turing machine is a sequence of configurations \((q^0, x^0, k^0) \) indexed by a sequence of consecutive time steps \( j \) starting from \( 0 \), that satisfies:

- The machine starts in a valid starting configuration, meaning that \( q^0 = s \) and \( k^0 = (0, 0, \ldots, 0) \).
- Each pair of consecutive configurations represents a valid transition of \( M \).
- If the sequence is infinite we say that the computation does not halt.
- If the sequence is finite and its length in \( m \), we require that the final state \( q^{m-1} \) is equal to the halting state \( t \), we say that the computation halts, and we refer to \( m \) as the running time of the computation.

Finally, having specified how Turing machines compute, let us now specify what they compute. First we must define two functions

\[
\text{pad} : \Sigma^* \rightarrow \Sigma^\infty, \quad \text{unpad} : \Sigma^\infty \rightarrow \Sigma^*
\]
as follows. If \( y \in \Sigma^* \) then \( \text{pad}(y) \) is formed from \( y \) by appending an infinite sequence of blank symbols. If \( x \in \Sigma^\omega \) then \( \text{unpad}(x) \) is the longest initial subsequence of \( x \) that contains no blank symbols. Note that if \( y \in \sigma^* \) contains no blank symbols then \( \text{unpad}(\text{pad}(y)) \) is equal to \( y \) but otherwise it is strictly shorter than \( y \).

Suppose we are given an \( I \)-tuple of strings, \( y = (y_i)_{i \in I} \). The computation of \( M \) with input \( y \) is the unique computation of \( M \) that starts with tape contents \( x_i = \text{pad}(y_i) \) for \( i \in I \) and \( x_i = \text{pad}(\epsilon) \) for \( i \notin I \). Here \( \epsilon \) denotes the empty string, so \( \text{pad}(\epsilon) \) denotes a tape containing nothing but blank symbols. If the computation of \( M \) with input \( y \) halts, we say that \( M \) halts on \( y \). Letting \( x = (x_1, \ldots, x_T) \) denote the tape contents in the final configuration of the computation, and letting \( z_i = \text{unpad}(x_i) \) for each \( i \), we call the \( O \)-tuple \( z = (z_i)_{i \in O} \) the output of the Turing machine, and we write \( M(y) = z \). If \( M \) does not halt on \( y \) we write \( M(y) = \uparrow \).

A partial function between two sets \( A \) and \( B \) is a function \( f : D \rightarrow B \) where \( D \) is a subset of \( A \) called the domain of \( f \). If \( f : (\Omega^*)^I \rightarrow (\Sigma^*)^O \) is a partial function from \( I \)-tuples of input strings to \( O \)-tuples of output strings, and if \( D \) is the domain of \( f \), then we say that Turing machine \( M \) computes \( f \) if \( M(y) = f(y) \) for all \( y \in D \) and \( M(y) = \uparrow \) for all \( y \notin D \).

**Example: computing the substring relation**

To illustrate how Turing machines work, in this section we present a Turing machine that computes whether one string is a substring of another. Recall that \( x_1 \) is said to be a substring of \( x_2 \) if the symbols in \( x_1 \) form a contiguous subsequence of the symbols in \( x_2 \). We will design a Turing machine \( M \) with input alphabet \( \Omega = \{0,1\} \) such that \( M(x_1, x_2) = 1 \) if \( x_1 \) is a substring of \( x_2 \) and \( M(x_1, x_2) = 0 \) otherwise.

Our machine will have three tapes: two input tapes containing \( x_1 \) and \( x_2 \) respectively, and an output tape that is only used in the final transition of the computation to write a 1 or 0. The algorithm that we will use to test if \( x_1 \) is a substring of \( x_2 \) is the obvious one: for each starting position \( p = 0,1,\ldots,|x_2| - |x_1| \) we will test if a substring of \( x_2 \) starting at \( p \) matches \( x_1 \). Thus, there will be an outer loop that iterates over \( p \), and an inner loop that iterates over the symbols in \( x_1 \). Of course, loops are not explicitly defined in the semantics of Turing machine computations, but we’ll use the state transition rules to implement a loop. A more challenging problem concerns the fact that \( |Q| \), the size of the state set, might be much smaller than \( |x_1| \) and \( |x_2| \), so the loop counters can’t be stored in the Turing machine’s internal state. Instead loop counters have to be stored, either explicitly or implicitly, in the form of information on the tapes.
or information about the positions of the tape heads. In particular, when an iteration of the inner loop ends without finding a match between \( x_1 \) and a contiguous subsequence of \( x_2 \), we need to return to the position in \( x_2 \) where began checking for a match. However, the Turing machine’s internal state can’t store enough information to locate that position. Instead we’ll record the location by writing a blank symbol (\( \_ \)) on the input tape containing \( x_2 \). This will overwrite one of the symbols of \( x_2 \), but it won’t matter because the overwritten symbol cannot belong to a substring that matches \( x_1 \).

In more detail, the Turing machine has states \( s, c, r, t \) with the following meanings and functionalities.

- \( s \) is the **starting** state. This state is used not only at the start of the entire computation but at the start of each iteration of the outer loop. In state \( s \) we check whether the first symbol of \( x_1 \) matches the earliest symbol of \( x_2 \) that hasn’t yet been tested as a potential beginning of substring that matches \( x_1 \). We also overwrite this symbol of \( x_2 \) with \( \_ \) to mark the position on the tape where this iteration of the outer loop began.

- \( c \) is the **comparing** state. This state checks whether a symbol of \( x_1 \) matches the corresponding symbol of \( x_2 \).

- \( r \) is the **returning** state. It is used after an iteration of the outer loop fails to find a match, to return to the position where we began the outer loop iteration.

- \( t \) is the **terminating** state. It is used to halt the Turing machine after writing the output.

The transition function is represented in Table 1. For brevity, we have omitted the lines of the table that specify the value of \( \delta(q, \sigma_1, \sigma_2, \sigma_3) \) when the symbol on the output tape, \( \sigma_3 \), is not the blank symbol. That is because those transitions are irrelevant: the machine we are designing never writes a non-blank symbol on the output tape until the moment that it terminates. For the same reason, we have omitted the lines of the table that specify the value of \( \delta(t, \sigma_1, \sigma_2, \sigma_3) \) since there can be transitions out of the terminal state \( t \).

4 **SJava: a simplified Java-like syntax for expressing algorithms**

It’s probably clear from the example in Table 1 that Turing machine transition functions are actually a terrible way of presenting algorithms to human beings. For the purpose of reasoning about algorithms and computability in these notes, it will be convenient to have a syntax for expressing algorithms which is human-readable,
<table>
<thead>
<tr>
<th>q</th>
<th>σ₁</th>
<th>σ₂</th>
<th>σ₃</th>
<th>q'</th>
<th>ρ₁</th>
<th>ρ₂</th>
<th>ρ₃</th>
<th>ℓ₁</th>
<th>ℓ₂</th>
<th>ℓ₃</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>s</td>
<td>0</td>
<td>t</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td>x₁ is the empty string</td>
</tr>
<tr>
<td>s</td>
<td>1</td>
<td>t</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>s</td>
<td>_</td>
<td>t</td>
<td>_</td>
<td>_</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>s</td>
<td>0</td>
<td>c</td>
<td>0</td>
<td>_</td>
<td>_</td>
<td>+1</td>
<td>+1</td>
<td>0</td>
<td></td>
<td></td>
<td>symbols match; keep checking</td>
</tr>
<tr>
<td>s</td>
<td>1</td>
<td>c</td>
<td>1</td>
<td>_</td>
<td>_</td>
<td>+1</td>
<td>+1</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>s</td>
<td>0</td>
<td>r</td>
<td>0</td>
<td>_</td>
<td>_</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td>mismatch</td>
</tr>
<tr>
<td>s</td>
<td>1</td>
<td>r</td>
<td>1</td>
<td>_</td>
<td>_</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>s</td>
<td>_</td>
<td>t</td>
<td>0</td>
<td>_</td>
<td>_</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td>reached end of x₂; x₁ can't be a substring</td>
</tr>
<tr>
<td>s</td>
<td>1</td>
<td>t</td>
<td>1</td>
<td>_</td>
<td>_</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c</td>
<td>0</td>
<td>t</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td>reached end of x₁; match found!</td>
</tr>
<tr>
<td>c</td>
<td>_</td>
<td>t</td>
<td>_</td>
<td>_</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c</td>
<td>_</td>
<td>t</td>
<td>_</td>
<td>_</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c</td>
<td>0</td>
<td>c</td>
<td>0</td>
<td>_</td>
<td>_</td>
<td>+1</td>
<td>+1</td>
<td>0</td>
<td></td>
<td></td>
<td>symbols match; keep checking</td>
</tr>
<tr>
<td>c</td>
<td>1</td>
<td>c</td>
<td>1</td>
<td>_</td>
<td>_</td>
<td>+1</td>
<td>+1</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c</td>
<td>_</td>
<td>r</td>
<td>0</td>
<td>_</td>
<td>_</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td>mismatch</td>
</tr>
<tr>
<td>c</td>
<td>_</td>
<td>r</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c</td>
<td>0</td>
<td>t</td>
<td>0</td>
<td>_</td>
<td>_</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td>reached end of x₂; x₁ can't be a substring</td>
</tr>
<tr>
<td>c</td>
<td>1</td>
<td>t</td>
<td>1</td>
<td>_</td>
<td>_</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>r</td>
<td>0</td>
<td>t</td>
<td>0</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td></td>
<td></td>
<td>this line irrelevant: σ₁ is never _ in state r</td>
</tr>
<tr>
<td>r</td>
<td>_</td>
<td>t</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>r</td>
<td>_</td>
<td>t</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>r</td>
<td>0</td>
<td>r</td>
<td>0</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td></td>
<td></td>
<td>keep moving left; don't overwrite symbols</td>
</tr>
<tr>
<td>r</td>
<td>0</td>
<td>r</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>r</td>
<td>1</td>
<td>r</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>r</td>
<td>1</td>
<td>r</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>r</td>
<td>0</td>
<td>s</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td>+1</td>
<td>0</td>
<td></td>
<td>returned to _ on tape 2; start again at next symbol</td>
</tr>
<tr>
<td>r</td>
<td>1</td>
<td>s</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td>_</td>
<td>+1</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1: Turing machine to compute the substring relation
like pseudocode. On the other hand, since our aim is to reason in a logically rigorous way about the limits of computation, rather than using pseudocode containing natural-language phrases whose meaning is subject to interpretation, it will be convenient when possible to express algorithms in a language with precisely-defined semantics.

Since you are all familiar with Java, we have chosen in these notes to express algorithms in a language with Java-like syntax, but omitting superfluous object-oriented features of Java that are irrelevant for present purposes. We keep only the bare essentials of an imperative programming language: variables, arrays, functions, assignment statements, control flow. We call this language Simplified Java, or SJ\textsuperscript{ava}.

By way of illustration, we have rewritten the program for computing whether $x_1$ is a substring or $x_2$ in SJ\textsuperscript{ava} in Figure 1.

```java
boolean substring(string x\textsubscript{1}, string x\textsubscript{2}) {
    pos\textsubscript{2} = 0;
    while (pos\textsubscript{2} < length(x\textsubscript{2})) {
        if (testMatch(x\textsubscript{1}, x\textsubscript{2}, pos\textsubscript{2})) {
            return true;
        }
        pos\textsubscript{2} = pos\textsubscript{2} + 1;
    }
    return false;
}

boolean testMatch(string s\textsubscript{1}, string s\textsubscript{2}, int offset) {
    // Does s\textsubscript{1} match s\textsubscript{2} starting from offset?
    if (length(s\textsubscript{1}) > (length(s\textsubscript{2}) − offset)) {
        return false; // s\textsubscript{1} is too long
    }
    pos\textsubscript{1} = 0;
    pos\textsubscript{2} = offset;
    while (pos\textsubscript{1} < length(s\textsubscript{1})) {
        // main loop: look for mismatches
        if (s\textsubscript{1}[pos\textsubscript{1}] != s\textsubscript{2}[pos\textsubscript{2}]) {
            return false;
        }
        pos\textsubscript{1} = pos\textsubscript{1} + 1;
        pos\textsubscript{2} = pos\textsubscript{2} + 1;
    }
    return true; // loop completed; no mismatch found
}
```

Figure 1: SJ\textsuperscript{ava} program to compute the substring relation.
Data types

Each expression in a SJava program has a value in one of the following data types.

- **boolean**: a value that is either **true** or **false**.
- **int**: a value in \( \mathbb{Z} \cup \{\perp\} \), where \( \perp \) is a special “not a number” value used to handle cases such as division by zero.
- **char**: a character from a pre-specified set \( \Sigma \). Specifying the character set \( \Sigma \) is part of specifying the model of computation. For concreteness, we take \( \Sigma \) to be the ASCII character set.
- **string**: a finite sequence of characters.
- **array**: a finite sequence of integers.

There is no limitation on the number of characters in a string or the number of elements in an array. Note that SJava only allows arrays of integers. A string is, in effect, the same thing as an array of characters. But one cannot create an array of Booleans, strings, or arrays, nor can one create an array whose contents constitute a mixture of integers and characters.

Each data type has a default value: **false** for Booleans, 0 for integers, _ for characters, \( \epsilon \) for strings, and \( \emptyset \) for arrays.

Program structure

A SJava program is organized as a sequence of function definitions. The first function in the sequence (called the base function) is interpreted as the “main” function (even if it is not called “main”) and the value it returns is interpreted as the program’s output.

The body of a function is enclosed in curly braces and consists of a sequence of statements. Each statement is either an assignment, a control-flow statement (if, else, while, or return), or a curly brace denoting the end of a block of code. These are discussed further below. Programs may contain comments, for the sake of readability. If a line of code contains two consecutive slashes (“//”) then any characters from the double-slash until the next new-line are ignored.

Variables

Variables are named by strings that may not contain whitespace and must start with a letter of the English alphabet. The scope of a variable is local to the function in which it is used.; The first time a variable is used in a function must either be in the function declaration (where the variable is declared to be one of the function’s
arguments) or on the left side of an assignment statement. In the latter case the variable’s type is inferred from the expression on the right side of the assignment. Variables are automatically initialized with the default value for their data type.

Expressions

An expression is a segment of code that can be evaluated to yield a value. It must be one of the following.

1. a variable name, such as n
2. a constant, such as 2
3. an array element or string element, such as x[n]
4. a function applied to a tuple of expressions, such as testMatch("Hello",str,n+m)
5. a binary operation applied to two expressions, such as testMatch("Hello",str,o) || testMatch("World",str,o)
6. a string or array element, such as str[n+1]

Assignment statements

Assignment statements are in one of two forms.

```
x = expr;

x[n] = expr;
```

In both cases x is a variable and expr is an expression (which may contain the variables x and n as sub-expressions). Execution of the assignment statement begins by evaluating the expression. The resulting value then replaces the value of x in the first case, or x[n] in the second case, which requires x to be a string or array. If n is less than zero, then x is unchanged. If n+1 exceeds the length of x, then after the expression on the right side is evaluated, x is padded with copies of the relevant default value (i.e., _ for the characters of a string, 0 for the integers in an array) until its length equals n+1, and then the value of the expression on the right side is substituted for x[n].

Control flow

The semantics of if, else, and while statements are exactly as in Java. The conditional expression in an if statement or while loop must be an expression of Boolean type, enclosed in parentheses.

A return statement must be followed by an expression whose type matches the return-value type of the function in which it appears.
When executing a return statement, the expression is first evaluated and then the value is substituted in the expression which called the function. (An exception is the base function which was called when the program first started running; its return value is treated as the program’s output.)

If the execution of a function reaches the last line of the function’s body without executing a return command, the function returns the default value for its return-value type.

**Small-step semantics of SJava**

We have explained the syntax of the SJava language and we have written informally about its semantics, i.e. what it means to execute a SJava program. Towards describing how to write a SJava interpreter, we must now specify its *small-step semantics*. That is, we will specify how the execution state is represented as a program executes, and how the state is updated as steps of the program are executed.

**Function state:** the state of a function as it executes is an ordered pair \((c, \phi)\) where:

- \(c\) is the *program counter*, a natural number denoting the position of the next instruction to be executed. The value of \(c\) is the absolute position of the first character of this instruction in the SJava program to which the function belongs.

- \(\phi\) is a dictionary mapping all the variable names and constant expressions that occur in the function to their current values.

**Execution state:** Since functions in a SJava program may call other functions, the overall state of a program can be conceptualized as a stack of function states, where the top of the stack is the state of the function currently being executed, and the other elements of the stack are the states of the functions whose execution is paused pending a return value from the function above them in the stack. Mathematically, we will represent this stack as a finite sequence of ordered pairs \(\{(c_i, \phi_i)\}_{i=0}^h\), where the last element of the sequence, \((c_h, \phi_h)\), represents the top element in the stack. “Popping the stack” refers to modifying this sequence by deleting its last element, whereas “pushing an element onto the stack” refers to modifying the sequence by appending one element at the end.

**Initial state of a function:** Every function \(f\) has a well-defined initial state \((c_{init}(f), \phi_{init}(f))\). The initial program counter position, \(c_{init}(f)\), is the location of the first non-whitespace character after the curly brace that starts the function body. The initial dictionary, \(\phi_{init}(f)\), assigns to each variable the default value of its associated type.
**Initial execution state of a program:** The initial execution state of a SJAVA program is a one-element stack consisting of the function state \((c_{\text{init}}, \phi_{\text{init}}(b))\), where \(b\) is the base function of the program.

**Evaluating an expression:** The rules for evaluating an expression in a given execution state vary according to the format of the expression.

1. If the expression is a term its value is read from the dictionary \(\phi_h\).
2. If it is a string or array element its value is determined by the rules specified above under “Operations on strings and arrays”.
3. If the expression applies a binary operation or built-in function (such as \(\text{length}(\cdot)\)) to one or two terms, the values of those terms are extracted from the dictionary and the expression’s value is determined as explained above when we described SJAVA’s binary operations and built-in functions.
4. If the expression involves application of a function \(f\), the execution state is changed by pushing the initial state of \(f\) onto the stack.

The first three cases don’t change the execution state but they do yield a value; we will call this *immediate evaluation*. The remaining case, which we will call *pending evaluation*, changes the program state by pushing a new function state onto the stack.

**Updating the execution state:** SJAVA programs are deterministic, meaning that for every execution state there is a uniquely defined subsequent state. The subsequent state depends on the current state \(\{(c_i, \phi_i)\}_{i=0}^{h}\) and on the instructions contained in the line of code that starts at position \(c_h\) in the program, i.e. the line of code pointed to by the program counter of the function state at the top of the stack. After discarding comments from the end of the line, there are six types of lines of code, and each of them changes the execution state in a different way. In the following discussion, “program counter” and “dictionary” refer to \(c_h\) and \(\phi_h\), the program counter and dictionary of the function state residing at the top of the stack before executing the line of code.

1. **Blank lines:** A line consisting entirely of whitespace is executed by advancing the program counter to the next line (i.e., the character immediately following the \(\leftarrow\) at the end of the line).

2. **Assignment statements:** The right side of an assignment statement is an expression. To execute the assignment statement, the first step is to evaluate the expression on the right side. An
immediate evaluation yields a value, and the execution state is modified as follows. The dictionary is modified by substituting that value for the value of the variable appearing on the left side of the assignment statement. The program counter is advanced to the next line. A pending evaluation doesn’t change $\phi_h$ or $c_h$ but increases the stack depth.

3. if statements: The conditional expression is evaluated. In the case of an immediate evaluation, the program counter is updated to the first (non-whitespace) character of the “then block” or the “else block”, depending if the value is true or false. A pending evaluation doesn’t change $\phi_h$ or $c_h$ but increases the stack depth.

4. while statements: The conditional expression is evaluated. In the case of an immediate evaluation yielding true, the program counter is updated to the first (non-whitespace) character inside the body of the while loop. In the case of an immediate evaluation yielding false, the program counter is updated to the first (non-whitespace) character following the body of the while loop. A pending evaluation doesn’t change $\phi_h$ or $c_h$ but increases the stack depth.

5. return statements: The expression following the keyword return is evaluated. A pending evaluation doesn’t change $\phi_h$ or $c_h$ but increases the stack depth. An immediate evaluation yielding value $v$ is more interesting. If $h = 0$ then the stack contains only one function state, namely the base function. Execution terminates and the program outputs $v$. If $h > 0$ then the stack is popped. The function state $(c_{h-1}, \phi_{h-1})$ is now at the top of the stack, and the program counter $c_{h-1}$ is at the start of a line of code whose execution produced a pending expression evaluation. The execution state is now updated as if the expression in that line of code had evaluated immediately to $v$.

6. End of a block: A right curly brace represents the end of a function body, a while loop, or one of the two blocks of an if statement. Upon reaching the end of a function body, the execution state changes as if it had reached a return statement whose expression immediately evaluated to the default value of the function’s return type. Reaching the end of a while loop moves the program counter back to the beginning of the line containing the corresponding while statement. Reaching the end of one of the blocks of an if statement moves the program counter to the first non-whitespace character following the conclusion of all blocks of the if statement.

We conclude this section with a remark about running times. It is tempting to model the execution of one line of a SJava program
as taking $O(1)$ time. Unfortunately that model doesn’t accurately reflect the amount of time it takes to run a program on an actual computer. The issue is that the integer, string, and array data types in SJava store an unbounded number of bits. Operations performed on these data types in a single line of code (such as multiplying two integers, or copying the value of a string to another variable) would take an amount of time that depends on the number of bits required to represent the operands.

To illustrate the issue concretely, consider the following SJava program.

```java
def doubleExponential(n):
    x = 3
    while (n > 0):
        x = x * x
        n = n - 1
    return x
```

This program performs $n$ loop iterations, each of which performs only 2 arithmetic operations. Yet it returns the integer $3^{2^n}$; merely writing the return value in binary requires $2^{O(n)}$ digits. So the running time of this innocuous-looking program is actually exponential in $n$.

The standard model of computation assumes that when one executes a program on an input of size $n$ bits, operations performed on blocks of bits of size $O(\log n)$ take constant time. For operations that manipulate objects larger than $O(\log n)$ in a single line of code, the algorithm designer is responsible for thinking about how to implement the operation as a sequence of constant-time steps each of which reads and writes at most $O(\log n)$ bits of data. This assumption that the number of bits that can be manipulated in one time step scales logarithmically with the size of the program’s input appears strange at first, but it turns out to be roughly consistent with the history of how datasets and computer architecture have co-evolved. Computers with 16-bit architectures used to be commonplace, they were eventually supplanted by 32-bit computers, which in turn were supplanted by 64-bit computers. Meanwhile, with each doubling of the number of bits, the size of the datasets encountered in typical computing workloads roughly squared.

5 Formalizing uncomputability

Now that we have a model of computation, we need to formalize what it means for something to be computable under a model of
computation. To simplify how we consider computation, we are going to describe all of our problems as decision problems, or problems with a true or false answer. While this might seem like a restriction, this does not affect what we can or cannot compute, as we can use decision problems to reconstruct more complex solutions bit by bit.

Suppose we execute some valid SJava program $M$ for a decision problem with input $x$. There are three possible outcomes:

1. accept: the program terminates and returns true, denoting "yes",
2. reject: the program terminates and returns false, denoting "no", or
3. the program never terminates; i.e., it reaches an infinite loop.

If the program $M$ reaches outcome 1 or 2 for input $x$, where the program terminates, we say that $M$ halts on input $x$. We define the set $L_M$ as the collection of all $x$ accepted by $M$, i.e., such that $M(x)$ terminates and returns true. We can think of $L_M$ as specifying a decision problem solved by $M$: inputs where $M$ returns true are inputs where the answer to the decision problem is “true” or “yes,” which belong in $L_M$, and inputs where $M$ returns false or doesn’t return at all are inputs where the answer is “false” or “no,” which do not belong in $L_M$.

There are two definitions of interest to us, then, with respect to these outcomes:

- **recognizability**: If the program $M$ accepts all and only inputs from $L_M$—meaning outcome 1 is reached by $M$ for input $x$ if and only if $x \in L_M$—we say that $M$ recognizes $L_M$, or that $L_M$ is a problem recognized by $M$. We can also consider a language of strings $\mathcal{L}$ independent of a specific program, such as “the set of all binary strings with an even number of 0s” or “the set of all descriptions of a graph for which there exists a Hamiltonian cycle.” We describe a language $\mathcal{L}$ as being recognizable if there exists any program $M$ for which $M(x)$ returns true if and only if $x$ is in $\mathcal{L}$. If $x$ is not in $\mathcal{L}$ for some decision program $M$, $M$ may either return false (outcome 2) or never terminate (outcome 3).

- **decidability**: We say that $M$ decides $L_M$ if $M$ not only returns true for all $x$ in $L_M$, but also returns false in finite time for all $x$ not in $L_M$. In other words, $M$ must make the correct decision about whether $x$ is in $L_M$ in finite time; it can never achieve outcome 3 above. Just as a language is recognizable if there exists a program that recognizes it, a language is decidable if there exists a program that decides it. Note that decidability is a strictly stronger requirement than recognizability; any program $M$ that decides a

\[\text{Definition} \quad \text{A program } M \text{ halts on an input } x \text{ if it either accepts or rejects that input in finite time.}\]

\[\text{If } M \text{ itself does not compile, or does not return a Boolean value, we treat it as rejecting all input.}\]

\[\text{The set } L_M \text{ of all input strings accepted by } M \text{ is often referred to as the language of } M.\]
language also recognizes it, and any language \( \mathcal{L} \) that is decidable must also be recognizable.

We have encountered a wide variety of decidable problems so far in this course. For instance, SAT (the Boolean satisfiability problem) is NP-complete, but it is still decidable. We can show this by construction: we can write a program that, given a formula, methodically iterates through every single possible assignment of variables to \textbf{true} or \textbf{false} to see if any assignment satisfies the given formula. If the program finds a satisfying assignment, it outputs \textbf{true}; otherwise, after iterating through all possible assignments, it outputs \textbf{false}. In practice, we would never want to run this program for large \( n \), as for \( n \) different variables, it would take exponential time, \( O(2^n) \), before it would output \textbf{false} for an unsatisfiable formula. However, exponential time is still finite, so this program still decides SAT.

When we prove a problem to be uncomputable, we specify one of the definitions above which the problem does not satisfy. For example, we might want to prove that a problem described by some language \( \mathcal{L} \) is \textit{undecidable}, i.e., that there exists no program \( M \) that can for any input \( x \) determine whether \( x \) is in \( \mathcal{L} \) in finite time. Much like in NP-completeness, for most undecidable problems, we prove that they are undecidable using reductions: if we can reduce a known undecidable problem to an unknown problem, then we can show that unknown problem is also undecidable. However, just like in NP-completeness, to use reductions, we need to bootstrap our set of undecidable problems by proving a single problem is undecidable without a reduction. For NP-completeness, that problem is SAT; for uncomputability, that problem is the halting problem, which we will get to in the next section.