Turing-recognizable versus Turing-decidable

Notes for CS 360, Fall 2019

November 12, 2019

Here is an example of the difference between Turing recognizability and Turing decidability.

Consider two languages over a 1-letter alphabet \{a\}, defined as follows.

\[ L_{\text{sum}} = \{a^k : \exists \text{ prime numbers } p_1, p_2 \text{ such that } k = p_1 + p_2 \} \]
\[ L_{\text{diff}} = \{a^k : \exists \text{ prime numbers } p_1, p_2 \text{ such that } k = p_1 - p_2 \} \]

Then \( L_{\text{sum}} \) is Turing-decidable, and it can be decided as follows: on input \( a^k \), we count the number of \( a \)'s to find \( k \). Then we try every \( j \), \( 0 \leq j \leq k/2 \), and check if \( j \) and \( k - j \) are both prime (using any method, such as trial division to see if there is any divisor other than the number and 1). If we find such a \( j \), then the input is accepted; otherwise it is rejected.

On the other hand, \( L_{\text{diff}} \) is Turing-recognizable, because it can be recognized as follows: on input \( k \), we test every integer \( i \geq 2 \), one after the other, to see if both \( i \) and \( i + k \) are primes. If we find such an \( i \), then we accept the input. If we never find such an \( i \), then the Turing machine fails to halt.

Is \( L_{\text{diff}} \) also Turing-decidable? Good question! The answer is, nobody currently knows. It could be that \( L_{\text{diff}} = L \), where

\[ L = \{a^{p-2} : p \text{ is a prime} \} \cup (aa)^*; \]

this is known as Maillet’s conjecture, and is still unresolved. If Maillet’s conjecture holds, then \( L_{\text{diff}} \) would also be Turing-decidable. Of course, \( L_{\text{diff}} \) could also be Turing-decidable, even if Maillet’s conjecture doesn’t hold.

The big difference between the two languages \( L_{\text{diff}} \) and \( L_{\text{sum}} \) is that in the case of \( L_{\text{sum}} \), the search space to check whether an input is accepted is bounded, and we know what the bound is, so we can just test all possibilities.

The search space for \( L_{\text{diff}} \), on the other hand, is not obviously bounded. It could be bounded, if we knew more about prime numbers. We just don’t know currently, and it is not obvious from the definition.