Capabilities of Computing Systems

Mathematical models of computing (developed before computers came into existence) include

$\rightsquigarrow$ Turing machines (Turing)
$\rightsquigarrow$ λ-Calculus (Church)
$\rightsquigarrow$ Recursive functions (Kleene)
$\rightsquigarrow$ Goedel numbers (Goedel)

$\rightarrow$ the equivalence of these models 'defines' what is to be understood as intuitively computable functions

$\rightarrow$ the Church / Turing thesis :
Intuitively computable functions
$\Leftrightarrow$ Turing computable functions

Hilbert's 23rd problem to be solved by Turing machines
$\rightarrow$ Is there a mechanical procedure to decide about truth or falsity of all mathematical | logical conjectures ?

Four principal ingrediences of Turing machines $\rightarrow$ considered essential for mathematical reasoning

$\rightsquigarrow$ a set of rules for transforming mathematical statements made in symbolic form
$\rightsquigarrow$ a mechanism to decide which rule to apply next
$\rightsquigarrow$ a recording method for transformation steps
$\rightsquigarrow$ the ability to go back and forth over the steps executed so far

$\rightarrow$ representation of symbols as sequences of 0s and 1s

- The deterministic Turing machine (DTM)
  $\rightarrow$ applies to each constellation (state) a unique rule (of a finite set of rules) to produce exactly one successor constellation ($\rightarrow$ constellation is made up from the contents of the tape on the right and left of the head and of the state of the head)

- The probabilistic Turing machine (PTM)
  $\rightarrow$ given some constellation, there may be multiple transformation rules to produce different successor states, of which one is chosen with some probability
  $\rightarrow$ the PTM can compute exactly the same functions as the DTM but may arrive at solutions much faster

- The quantum Turing machine (QTM)
  $\rightarrow$ the constellation (the quantum state) of the machine is a probabilistic superposition of classical constellations | states
  $\rightsquigarrow$ the computation is realized as a continuously evolving quantum state which results | terminates with a superposition of all reachable classical states
  $\rightsquigarrow$ observing | measuring the superimposed state results in its collapse and in returning just the classical states reached that has highest probability

  $\rightarrow$ the QTM follows all possible traces concurrently but, when observed, returns the constellation reached along one of the traces only
  $\rightarrow$ the classical PTM follows only one of the traces with some probability

The classical TM halting problem

$\rightarrow$ does there exist a mechanical procedure to decide whether or not any given Turing machine acting on any given input halts | terminates after some finite number of steps
$\rightsquigarrow$ is equivalent to deciding whether or not the truth or falsity of conjectures can be decided $\rightarrow$ Hilbert's 23th problem
$\rightarrow$ proof by contradiction (assuming that such a TM | procedure can be constructed) shows that such TM does not exist $\rightsquigarrow$ the problem is not computable | not decidable
$\rightsquigarrow$ the proof is based on the construction of a TM which, when applied to itself, cannot terminate and cannot not terminate

relates to Goedel's theorems on formal systems
$\rightarrow$ any sufficiently strong formal system L (a set of axioms) is incomplete if it is consistent $\rightsquigarrow$ there are statements P which can neither be proven true or false, using the rules of L
$\rightsquigarrow$ since P and its negation are contradictory, one of them must be true $\rightsquigarrow$ there must be statements about L that cannot be proven
$\rightsquigarrow$ truth and theoremhood are different concepts
$\rightsquigarrow$ consistency of L cannot be proven in itself $\rightarrow$ there must be some deep-seated contradictions in L

Quantum computing
is based on a formal (mathematical) apparatus | system
→ describes | models physics | behavior of nature
→ features contradictions | undecidable problems
⇝ precise predictions about the state(s) of quantum system are possible but cannot be validated by experiments | observations | measurements → the state collapses
⇝ given precisely specified initial states, almost all questions relating to the long-term dynamic behavior are undecidable
→ is the consequence of a self-referential theory which tries to describe its own means of verification ⇝ is not a consequence of quantum theory per se.

Quantum computability
→ it is always possible to construct a QTM which simulates a DTM | PTM ⇝ computes the same class of functions
⇝ operates on so-called base quantum states
⇝ takes the same number of steps to run a program
→ QTM's can generate truly random numbers (which are not values of functions)
→ QTM's apply functions to superpositions of all possible initial states at once ⇝ quantum 'parallelism' ⇝ all function values are computed in the same time it takes to compute one value but ⇝ only one value may be obtained by observation | measurement