ECE471/571 Malware & IDS

Virus Detection

There is no program that detects all viruses!

i.e. Virus detection is undecidable

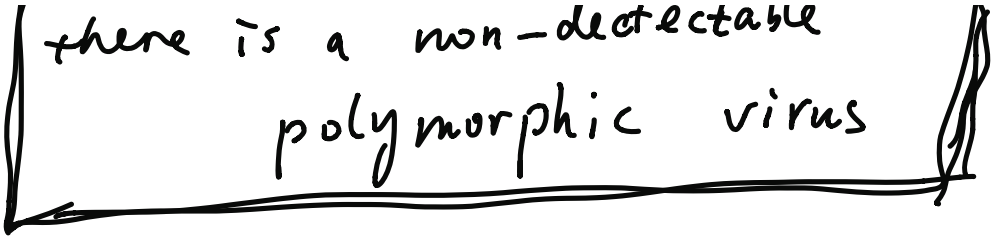
Halting problem

1. Assume such A exists

2. $P \equiv$ {
   char * S
   S = <text of P>.
   <define subroutine A>
   if A(S) = true then loop
   else halt
   }

$P \equiv$ { if A(P) then loop, else halt }

$P \equiv$ { if A(P) then stop; else spread }


there is a non-detectable
polymorphic virus