

SNU 046.016 컴퓨터과학이 여는 세계, 2017 봄 기말고사

이름:

학번:

Problem 1 [15×(3점|-3점)] O/X 로 답하라.

1. 하나의 컴퓨터(universal turing machine)는 임의의 소프트웨어(a turing machine)를 메모리에 받아 그 소프트웨어를 해석 실행한다.
2. 현재의 디지털 컴퓨터가 실행할 수 있는 모든 소프트웨어는 ‘그리고’, ‘또는’, ‘아닌’으로 조립할 수 있다.
3. 현재의 디지털 컴퓨터 프로그램으로 적당히 답할 수 밖에 없는 문제들이 무수히 많다.
4. 알고리즘의 계산 복잡도의 상대적인 크기를 예로들면 다음과 같다:

$$O(\log_2 n) < O(\sqrt{n}) < O(n) < O(n \log_2 n) < O(n^{2017}) < O(2^n) < O(n^n).$$

5. 양자컴퓨터의 비상한 효율은 양자레벨에서 일어나는 중첩(superposition), 얽힘(entanglement), 확률진폭(probability amplitude)을 이용하고 있고, 완전한 무작위(random) 함수도 실현할 수 있지만, 그렇다고 튜링기계의 한계를 넘어서는 것은 아니다.
6. 다양한 레벨의 컴퓨터 언어들 존재하는데, 컴퓨터 언어들 사이의 번역은 항상 자동으로 가능하며, 이 때 동원하는 지혜는 조립식(compositonality)과 불변성질(invariant)유지하기 이다.
7. 지금의 디지털 컴퓨터 하드웨어는 기계어 프로그램의 해석실행기라고 할 수 있다.
8. 모든 프로그래밍 언어의 해석실행기는 모두 튜링기계라고 볼 수 있다.
9. 프로그램짜기와 증명하기는 서로의 거울이다. 이 사실이 드러난 데는 프로그램을 람다계산(lambda calculus)식으로 보는 시각을 통해서였다.
10. 소프트웨어의 검진은 다양한 레벨에서 이루어 질 수 있다. 타입검증(type checking)은 그 중 한 레벨이다.
11. 소프트웨어의 엄밀한 검진에는, 소프트웨어가 실행되는 실제 상황을 모두 포섭하면서 간단하게 살펴보는 요약(abstraction)의 지혜가 동원된다.
12. 사람이 새로운 지식을 만드는 방식으로 디덕(deduction, 반드시이끌기)이외에 앱덕(abduction, 원인 짐작하기)과 인덕(induction, 짐작해서 이끌기)이 있고, 기계학습(machine learning)은 앱덕과 인덕을 자동화하는 기술이다.
13. 앱덕하는 기계학습이 빠질 수 있는 함정이 있다. 한 결과(B)에 대해서 파악하고있는 인과관계($A_1 \Rightarrow B, A_2 \Rightarrow B$)가 모든 경우를 커버하지 않을 수 있고, 관찰한 수 많은 데이터($b_1, \dots, b_{218} \in B$)에 숨은 소수의 중요한 시그널(b_{2017})이 대다수의 다른 데이터에 묻혀버릴 수 있다는 것이다.

14. 어떤 일을 위해서 많은 사람들을 동원해야만 할 때 컴퓨터게임이 효과적일 수 있다.
15. 현재의 암호기술은 현재의 디지털 컴퓨터로도 풀기 어려운 계산문제에 기대고 있다. 양자컴퓨터가 출현하면 그러한 문제들을 새로 찾아야 하지만 수학에는 이미 그러한 문제들이 알려진게 있다.

Problem 2 [5점, 5점]

디지털 컴퓨터와 통신의 원천기술을 만든 네 살 차이의 두 청년. 그 둘의 논문은 구조가 똑같다. 아래 빈칸을 메꾸라.

알랜 튜링(Alan Turing)	클로드 섀넌(Claude Shannon)
A 이란 무엇인가를 정의했다	통신이란 무엇인가를 정의했다
튜링기계를 정의했다	메세지의 B 을 정의했다
A 의 한계를 증명했다	통신의 한계를 증명했다

Problem 3 [5점] 프로그래밍 언어의 한 원조로서 람다계산법(lambda calculus)이 있다. 다음의 람다식이 계산되는 과정을 메꾸라: $(\lambda x.(xx)z)(\lambda y.y) \rightarrow \square \rightarrow \square \rightarrow \square$.

Problem 4 [5점, 5점, 5점] 아래 각각의 방법을 가능하게 하는 가장 가까운 원천기술을 다음에서 찾아서 옮겨써라.

{튜링기계, 해석실행, 정보이론, 오류수정코드, 동형암호, 디지털논리회로, 짝궁열쇠(RSA) 기술, 공개키암호기술, 번역사술, 람다계산법, 인간계산}

사진을 온전히 전달하고, 누가 엿보지 못하게 하고, 원작자가 누구인지 확인할 수 있는데는 “, , ” 덕택이다.

암호를 건 비밀스런 사진을 아무에게나 안심하고 포토샵처리를 부탁할 수 있는데는 “” 덕택이다.

프로그램의 구도를 잡고 짠 프로그램이 무난히 잘 돌지를 확인하는 기술이 제대로 정립될 수 있었던데에는 프로그램을 “”의 관점에서 바로 본 덕분이다.

Problem 5 [5점|-5점] O/X 로 답하라.

블록체인(block chain)은 모두가 모든 정보를 똑같이 공유하면서, 이미 공유한 정보를 특정인이 조작하는 것이 거의 불가능하도록 만든 방법이다. 이 방법을 이용하면 새로운 디지털 화폐의 유통이 중앙은행 없이도 안전하게 이루어질 수 있다. 이 방법을 이용하면 중앙공공기관에 기대지않고 ‘공인인증서’를 구현할 수 있고, 짝궁열쇠(RSA) 기술 없이도 스마트화폐를 실현할 수 있다.

Problem 6 [10점] 강의에서 다룬 두 개의 언어(정수식 언어와 동전통 언어) 사이의 번역을 생각하자. 출발어는 정수식 언어이고 도착어는 동전통 언어이다. 정수식 “ $-(1+2) \times (-3)$ ”을 번역한 결과는 무엇인가?

Problem 7 [5점, 5점] 인류의 지식표현 방식이 어떻게 발전해 왔는지를 설명하라. 그리고 컴퓨터가 가져온 새로운 지식표현의 한 예를 들라.