

# SNU 046.016 컴퓨터과학이 여는 세계, 2016 봄

## 기말고사

이름:

학번:

**Problem 1** [7×(5점|-5점)] O/X 로 답하라.

1. 하나의 컴퓨터(universal turing machine)는 임의의 소프트웨어(a turing machine)를 메모리에 받아 그 소프트웨어를 해석실행한다.
2. 다양한 레벨의 컴퓨터 언어들 존재하는데, 컴퓨터 언어들 사이의 번역은 대개 자동으로 가능하며, 이 때 동원하는 지혜는 조립식(전체의 번역결과는 부품들의 번역결과로 조립됨)과 불변성질 유지하기다.
3. 컴퓨터 프로그램으로 해결할 수 없는 문제들이 무한히 많을 수는 없다.
4. 프로그램짜기와 증명하기는 서로의 거울이다. 이 사실이 드러난 데는 프로그램을 람다계산(lambda calculus)식으로 보는 시각을 통해서였다.
5. 양자컴퓨터의 비상한 능력은 양자레벨에서 일어나는 중첩(superposition), 얽힘(entanglement), 확률진폭(probability amplitude)을 이용한다.
6. 사람이 새로운 지식을 짐작하는 방식으로 앵덕(abduction, 원인짐작하기)과 인덕(induction, 짐작해서 이끌기)이 있고, 기계학습(machine learning)은 이 두 방식을 자동화하는 기술이다.
7. 앵덕하는 기계학습이 빠질 수 있는 함정이 있다. 한 결과( $B$ )에 대해서 파악하고있는 인과관계( $A \Rightarrow B, Z \Rightarrow B$ )가 모든 경우를 커버하지 않을 수 있고, 관찰한 수많은 데이터( $B_1, \dots, B_{2^{18}}$ )에 숨은 소수의 중요한 시그널( $B_{2016}$ )이 대다수의 다른 데이터에 묻혀버릴 수 있다는 것이다.

**Problem 2** [5점, 5점]

$\mathcal{NP}$  클래스 문제를 생각하자. 디지털 컴퓨터에서 이런 문제의 모든 경우마다 현실적인 비용으로 답을 정확히 내놓는 하나의 프로그램은 아직 발견되지 않고 있다. 그렇다면 “모든 경우마다”를 “”으로 바꾸면 그런 프로그램은 찾을 수 있지 않을까? 아니면, “정확히”를 “”로 바꾸면 그런 프로그램은 찾을 수 있지 않을까?

**Problem 3** [5점] 컴퓨터를 디지털 논리회로로 구현하는 과정에는, 속내용감추면 차곡차곡쌓기(abstraction hierarchy)라는 지혜가 사용된다. 이 지혜를 간략히 설명하라.

**Problem 4 [5점, 5점]**

디지털 컴퓨터의 원천기술을 만든 네 살 차이의 두 청년. 그들이 쓴 논문은 구조가 똑같다. 아래 빈칸을 메꾸라.

Alan Turing	Claude Shannon
기계적인 계산이란 무엇인가를 정의했다	통신이란 무엇인가를 정의했다
튜링기계를 정의했다	메세지의 <input type="text"/> 을 정의했다
계산의 한계를 증명했다	<input type="text"/> 의 한계를 증명했다

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

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

사진을 온전히 전달할 수 있게된다는 “” 덕택이다. 사진을 누가 엿보지 못하게 하는다는 “” 덕택이다. 작품사진의 작가가 누구인지 확인할 수 있게 하는 방법 “” 덕택이다.

**Problem 6 [5점, 5점, 5점]** 프로그램짜기의 한 땀 한 땀은 증명에서 논리추론의 징검다리를 한 칸 한 칸 건너는 것과 일치한다. 다음의 논리추론 징검다리에 해당하는 프로그램짜기가 무엇인가? (힌트: 함수, 사람, 학생)

- “A가 사실이라는 가정하에 B가 사실이면, A이면 B 가 사실이다.”

$$\frac{\overline{A} \quad \vdots \quad B}{A \Rightarrow B}$$

- “A이면 B 가 사실이고 A가 사실이면, B가 사실이다.”

$$\frac{A \Rightarrow B \quad A}{B}$$

- “A가 사실이면, 임의의 B에 대해서 A또는B 가 사실이다.”

$$\frac{A}{A \vee B}$$

**Problem 7 [10점]** 만난적도 없는 세 사람이 카톡방에서 비밀이야기를 시작하고 싶다. 이 세 명이 공유할 비밀키를 공개적으로 만들 수 밖에 없다. 어떻게 하면 될까? 비유를 통해 설명해 보라.