답안지

# 이산수학 중간고사 1

2013.10.22

학번 _____ 이름 _____

1. $P = (s \rightarrow (p \wedge \sim r)) \wedge ((p \rightarrow (r \vee q)) \wedge s)$, $Q = p \vee t$ 이라면 $P \equiv Q$ 인가? 증명 (혹은 반증)하라. [5점]

No. p=T, s=F 인경우 P는 F이지만 Q는 T이다. 두 명제의 값이 모든 진리값 assignment 에 대해 같지 않으므로 P≠Q 이다.

2. **P(x)** 는 **"x is an accountant," Q(x)** 는 **"x owns a Porsche"** 로 정의할 때, 다음의 각 명제와 그 부정을 각각 기호를 써서 (symbolically) 표기하라. [각 2점, 총 8점]

A. **All accountants own Porsche.**

| | |
|---|---|
| $\forall x \quad P(x) \rightarrow Q(x)$ | $\exists x \quad P(x) \wedge \neg Q(x)$ |

B. **Some accountant owns a Porsche.**

| | |
|---|---|
| $\exists x \quad P(x) \wedge Q(x)$ | $\forall x \quad P(x) \rightarrow \neg Q(x)$ |

3. Domain of discourse가 $R \times R$ 일 때 다음 명제가 참인지 거짓인지 결정하고 그 이유를 설명하라. [각 2.5점, 총 5점]

A. $\forall x \exists y \, ((x < y) \rightarrow (x^2 < y^2))$

참. 임의의 실수 x에 대해 $|x| < y$ 인 실수 y를 선택함으로써 주어진 명제를 항상 만족시킬 수 있다.

B. $\forall x \forall y \, ((x < y) \rightarrow (x^2 < y^2))$

거짓. $x = -2$, $y = 1$ 일 때 주어진 명제는 거짓이다. (반례)

4. 다음을 resolution과 간접증명법(proof by contradiction)에 의해 증명하여라. [10점]

$$\begin{array}{l} a \rightarrow (b \rightarrow c) \\ a \rightarrow b \\ \underline{\quad a \quad} \\ \therefore c \end{array}$$

먼저 resolution을 이용하기 위해 주어진 전제를 clause 형태로 바꾸고 결론을 부정하여 전제에 더하면,

(1) $\neg a \vee \neg b \vee c$
(2) $\neg a \vee b$
(3) $a$
(4) $\neg c$

이다. (1)과 (3)으로부터 $\neg b \vee c$ (5), (2)와 (3)으로부터 $b$ (6)을 얻고, (4)와 (5)에서 $c$를 얻으면 (7) 이때 (4)와 (7)은 contradiction이다. 따라서 주어진 argument는 valid 하다.

5. 수학적 귀납법 (mathematical induction)에 의해 $n \geq 1$ 인 모든 $n$ 에 대해 $7^n - 1$이 6으로 나누어 떨어짐을 증명하여라. [10점]

basis $(n=1)$ $7^1 - 1 = 6$ 이므로 6으로 나누어 떨어진다 ✓

I.H. $(n=k)$ $7^k - 1$ 가 6으로 나누어떨어진다면 $(k \geq 1)$

I.S. $(n=k+1)$ $7^{k+1} - 1 = 7(7^k - 1) + 6$ 이고

6 과 $(7^k - 1)$이 6으로 나누어 떨어지므로 (가정) 이 또한 6으로 나누어 떨어진다 ✓

따라서 $n \geq 1$ 인 모든 $n$에 대해 $7^n - 1$은 6으로 나누어 떨어진다.

6. RSA 알고리듬에서 p=3, q=5, n=3으로 선택했다 (변수명은 교과서 기준). 이 때 다음을 구하여라.

A. z: $3 \times 5 = 15$ [1점]

B. $\phi$: $2 \times 4 = 8$ [1점]

C. s: 3 [3점] ← $3 \times 3 + (-1) \times 8 = 1$ ($n$, $s$, $t$, $\phi$; $\gcd(8,3)$)

D. Public key: $(e, n) = (15, 3)$ [2점]

E. 메시지 m=7 에 대한 암호화된 값 $C = 7^3 \bmod 15 = 13$ [5점]

F. 암호화된 값의 복호화 과정 (즉 다시 7을 얻을 수 있는 것을 보임) [5점]

$$m = C^3 \bmod 15$$
$$= 13^3 \bmod 15$$
$$= 2197 \bmod 15 = 7 \quad //$$

7. 어느 나라의 HIV 바이러스 감염율은 1% 이다. 어떤 제약회사가 개발한 감염 판정 테스트 시약은 독감 바이러스를 가진 환자에서 양성 반응이 나올 확률이 95% 이고, 바이러스를 가지지 않은 사람에서 양성 반응이 나올 확률이 2% 이라고 한다.

A. 감염 여부를 알 수 없는 어떤 불안한 시민이 이 테스트를 받았더니 양성 (positive) 반응이 나왔다. 이 시민이 실제로 감염되었을 확률은 얼마인가? 유도식을 보이고, 소수점 첫째 자리까지 답을 계산하라. 유도식에서 감염 사건은 H, 양성으로 판별되는 사건은 Pos 라고 표기하라. [10점]

$P(H) = 0.01$, $P(Pos|H) = 0.95$, $P(Pos|\overline{H}) = 0.02$ 가 주어졌고

$P(H|Pos)$ 를 구하는 문제이다. Bayes 정리에 의해

$$P(H|Pos) = \frac{P(H) \cdot P(Pos|H)}{P(Pos)}$$
$$= \frac{P(H) \cdot P(Pos|H)}{P(H) \cdot P(Pos|H) + P(\overline{H}) \cdot P(Pos|\overline{H})}$$
$$= \frac{0.01 \times 0.95}{0.01 \times 0.95 + 0.99 \times 0.02}$$
$$= \frac{0.0095}{0.0095 + 0.0198} = \frac{0.0095}{0.0293} \fallingdotseq 0.324.$$

0.3 (문제 문법적: 정답처럼 흘림) 32.4% 로 맞음.

B. (A)에서 얻은 값은 predictive value of a positive test (PVP) 라는 것으로서 양성반응이 나왔을 때 실제로 감염이 되어 있을 확률이다. PVP 값이 50%를 넘어가려면 P(H)는 얼마 이상이어야 하는가? [5점]

$\frac{x \times 0.95}{x \times 0.95 + (1-x) \times 0.02} \geq \frac{1}{2}$ 인 $x$ 를 찾는다.

$\therefore x \fallingdotseq 0.0206$ 즉 2.1% 이상.

8. 사람 n 명을 원탁에 둘러 앉히는 방법은 무엇인가? 식으로 표시하라 [3점] p.280

$(n-1)!$

9. $0 \le x1 < 6$, $1 \le x2 < 9$, $x3 \ge 0$ 일 때 $x1+x2+x3=15$를 만족하는 정수해의 개수는 얼마인가? $C(15+3-1,15) - C(8+3-1,8)$ [6점]

$=$

10. 지수함수 (exponential function)로 표현되는 알고리듬의 복잡도가 얼마나 바람직하지 못한지 생각해 보자. 지구에서 달까지의 평균 거리는 384,400 Km 이다. A4 용지 한 장의 두께를 0.1mm 라고 했을 때, 현실적 한계를 고려하지 않는다면 A4 용지를 최소 몇 번 계속 접어 겹치면 달까지 도달하겠는가? 계산안해도 됨 [3점]

다음을 만족하는 최소의 정수 $d$ : $10^{-7} \cdot 2^d \ge 384400 \Rightarrow d = \lg(3.844 \times 10^{12})$

42번

11. $a>1$, $b>1$ 일 때 $\log_a n = \Omega(\log_b n)$ 임을 보여라 [6점]

$\log_b n = \log_b a \cdot \log_a n \quad (n \ge 1)$

$\Rightarrow \log_b n \ge C \cdot \log_a n, \quad C = \log_b a$

$\therefore \log_b n = \Omega(\log_a n)$ //

12. $i=j-1$ 일 때 $\sum_{i=0}^{n} ir^{n-i}$ 에서 index를 $j$로 바꾸어 표현하여라. [3점]

$\sum_{j=1}^{n+1} (j-1) r^{n-j+1}$

13. 정수 집합에서 divides (나누어 떨어뜨린다) 라는 관계를 생각해보자. 이 관계는

A. Partial order인가? 예/아니오로 답하고 증명하라. [6점]

예. (reflexive) $d|d$ for all $d \in \mathbb{Z}$.

(antisymmetric) if $d|e$ then $e \nmid d$ for all $d, e \in \mathbb{Z}$.

(transitive) if $d|e$ and $e|f$ then $d|f$ for all $d, e, f \in \mathbb{Z}$.

B. Total order인가? 예/아니오로 답하고 증명하라. [3점]

아니오 $2 \nmid 3$ and $3 \nmid 2$ 따라서 2와 3은 incomparable
Incomparable인 경우가 존재하므로 "|"은 total order가 아니다.
(부분순서관계)