선형대수

2016년 1학기

중간고사

서울시립대학교
컴퓨터과학부

주의사항

- **시험지는 앞/뒤로 인쇄되어 있으니 유의하시기 바랍니다.**
- 만점은 100점입니다.
- 부정행위가 발각되면 즉시 시험지가 압수되고 0점 처리 됩니다.
- 처음부터 모든 문제를 풀지 말고, 문제를 모두 훑어본 후 풀 수 있다고 생각되는 문제부터 풀 것을 권장합니다.
- 교재에 있는 lemma, theorem 등을 이용할 경우, 해당 lemma/theorem을 증명할 필요 없이 어떤 것인지를 밝히고 이용하여도 좋습니다.
- 강의시간에 배운 범위안의 내용에만 근거해서 답변해야 합니다. 예를 들어, 아직 배우지 않은 내용을 근거로 답하는 경우, 맞더라도 감점이 됩니다.

1. 20점 Challenge-response 방식으로 인증을 하는 서버가 있다. 암호는 9비트로 되어 있고, challenge는 3비트의 데이터로 되어 있다. reponse는 암호의 각 3비트마다 challenge 값과 dot-product를 수행하여 얻은 3비트 결과로 이루어진다. 즉, 만약 암호 p가 다음과 같고

$$p := [p_0, p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8]$$

challange c가 다음과 같다면

$$c := [c_0, c_1, c_2]$$

response r은 다음과 같이 3비트 벡터로 계산된다.

$$r = \begin{bmatrix} [p_0, p_1, p_2] \cdot [c_0, c_2, c_2] \\ [p_3, p_4, p_5] \cdot [c_0, c_2, c_2] \\ [p_6, p_7, p_8] \cdot [c_0, c_2, c_2] \end{bmatrix}$$

A가 이 서버에서 인증을 받은 데이터를 B가 중간에 가로채서 다음과 같은 challenge-response 쌍의 정보를 모았다고 하자.

회수	challenge	response
1	$[1, 0, 1]$	$[0, 1, 1]$
2	$[0, 1, 1]$	$[1, 0, 1]$

이렇게 얻은 정보에 기반하여 아래의 각 challenge에 대한 reponse를 구하라. 만약 response를 구할 수 없을 경우 왜 그런지 설명하라.

(주의: 모든 벡터는 $GF(2)$ field에서 정의된다. 따라서 이에 해당하는 연산을 적용해야 한다.)

(a) 10점 $[1, 1, 0]$

(b) 10점 $[1, 0, 0]$

Solution:

(a)

$$\begin{aligned} [p_0, p_1, p_2] \cdot [1, 0, 1] &= 0 \\ [p_0, p_1, p_2] \cdot [0, 1, 1] &= 1 \\ [p_3, p_4, p_5] \cdot [1, 0, 1] &= 1 \\ [p_3, p_4, p_5] \cdot [0, 1, 1] &= 0 \\ [p_6, p_7, p_8] \cdot [1, 0, 1] &= 1 \\ [p_6, p_7, p_8] \cdot [0, 1, 1] &= 1 \end{aligned}$$

Since

$$[1, 1, 0] = [1, 0, 1] + [0, 1, 1],$$

We get

$$[p_0, p_1, p_2] \cdot [1, 1, 0] = [p_0, p_1, p_2] \cdot ([1, 0, 1] + [0, 1, 1]) = 0 + 1 = 1$$
$$[p_3, p_4, p_5] \cdot [1, 1, 0] = [p_3, p_4, p_5] \cdot ([1, 0, 1] + [0, 1, 1]) = 1 + 0 = 1$$
$$[p_6, p_7, p_8] \cdot [1, 1, 0] = [p_6, p_7, p_8] \cdot ([1, 0, 1] + [0, 1, 1]) = 1 + 1 = 0$$

and therefore the response is

$$[1, 1, 0].$$

(b) All the possible linear combintations of $[1, 0, 1]$ and $[0, 1, 1]$ are

$$0[1, 0, 1] + 0[0, 1, 1] = [0, 0, 0]$$
$$0[1, 0, 1] + 1[0, 1, 1] = [0, 1, 1]$$
$$1[1, 0, 1] + 0[0, 1, 1] = [1, 0, 1]$$
$$1[1, 0, 1] + 1[0, 1, 1] = [1, 1, 0]$$

therefore

$$\text{Span}\,([1, 0, 1], [0, 1, 1]) = \{[0, 0, 0], [0, 1, 1], [1, 0, 1], [1, 1, 0]\}.$$

Since $[1, 0, 0] \notin \text{Span}\,([1, 0, 1], [0, 1, 1])$, we cannot compute the response.

2. [20점] 다음과 같이 정의된 vector space over $GF(2)$의 모든 vector를 각각 구하라. (중복되는 vector는 하나만 포함할 것)

   (a) [10점] Span $([1,0,1],[0,1,1],[1,1,0])$

   (b) [10점] 다음 homogeneous linear system의 solution set

$$\begin{bmatrix}1 & 0 & 1\\ 0 & 1 & 1\end{bmatrix}\mathbf{x}=\begin{bmatrix}0\\0\end{bmatrix}$$

Solution:

(a)

$$\begin{aligned}
0[1,0,1]+0[0,1,1]+0[1,1,0]&=[0,0,0]\\
0[1,0,1]+0[0,1,1]+1[1,1,0]&=[1,1,0]\\
0[1,0,1]+1[0,1,1]+0[1,1,0]&=[0,1,1]\\
0[1,0,1]+1[0,1,1]+1[1,1,0]&=[1,0,1]\\
1[1,0,1]+0[0,1,1]+0[1,1,0]&=[1,0,1]\\
1[1,0,1]+0[0,1,1]+1[1,1,0]&=[0,1,1]\\
1[1,0,1]+1[0,1,1]+0[1,1,0]&=[1,1,0]\\
1[1,0,1]+1[0,1,1]+1[1,1,0]&=[0,0,0]
\end{aligned}$$

$\rightarrow \{[0,0,0],[0,1,1],[1,1,0],[1,0,1]\}$

(b)

$$\begin{bmatrix}1 & 0 & 1\\ 0 & 1 & 1\end{bmatrix}\begin{bmatrix}0\\0\\0\end{bmatrix}=\begin{bmatrix}0\\0\end{bmatrix}\qquad \begin{bmatrix}1 & 0 & 1\\ 0 & 1 & 1\end{bmatrix}\begin{bmatrix}0\\0\\1\end{bmatrix}=\begin{bmatrix}1\\1\end{bmatrix}$$

$$\begin{bmatrix}1 & 0 & 1\\ 0 & 1 & 1\end{bmatrix}\begin{bmatrix}0\\1\\0\end{bmatrix}=\begin{bmatrix}0\\1\end{bmatrix}\qquad \begin{bmatrix}1 & 0 & 1\\ 0 & 1 & 1\end{bmatrix}\begin{bmatrix}0\\1\\1\end{bmatrix}=\begin{bmatrix}1\\0\end{bmatrix}$$

$$\begin{bmatrix}1 & 0 & 1\\ 0 & 1 & 1\end{bmatrix}\begin{bmatrix}1\\0\\0\end{bmatrix}=\begin{bmatrix}1\\0\end{bmatrix}\qquad \begin{bmatrix}1 & 0 & 1\\ 0 & 1 & 1\end{bmatrix}\begin{bmatrix}1\\0\\1\end{bmatrix}=\begin{bmatrix}0\\1\end{bmatrix}$$

$$\begin{bmatrix}1 & 0 & 1\\ 0 & 1 & 1\end{bmatrix}\begin{bmatrix}1\\1\\0\end{bmatrix}=\begin{bmatrix}1\\1\end{bmatrix}\qquad \begin{bmatrix}1 & 0 & 1\\ 0 & 1 & 1\end{bmatrix}\begin{bmatrix}1\\1\\1\end{bmatrix}=\begin{bmatrix}0\\0\end{bmatrix}$$

$\rightarrow \{[0,0,0],[1,1,1]\}$

3. [10점] Matrix M이 있다고 하자. Row M의 임의의 vector와 Null M의 임의의 vector를 dot-product하면 항상 0이 됨을 보여라.

Solution: Let all vectors be represented as column vectors.

1. $\mathbf{x} \in \text{Row}\, M \Leftrightarrow$ There exists a row vector $\mathbf{y}^T$ such that $\mathbf{x}^T = \mathbf{y}^T M$.
2. $\mathbf{z} \in \text{Null}\, M \Leftrightarrow M\mathbf{z} = \mathbf{0}$.

Therefore,

$$\mathbf{x} \cdot \mathbf{z} = \mathbf{x}^T\mathbf{z} = (\mathbf{y}^T M) \cdot \mathbf{z} = \mathbf{y}^T(M\mathbf{z}) = \mathbf{y}^T\mathbf{0} = \mathbf{y} \cdot \mathbf{0} = 0.$$

4. 10점 Hamming(7,4)-coding 방법으로 데이터를 송수신하는 경우 2비트 데이터 에러는 detect할 수 있으나 correct할 수 없음을 보여라.
(Hint: 에러가 correct되지 않음을 보일 경우, 해당하는 예를 보여라.)

Solution: Let $\mathbf{x}$ is the original data.

- Encoding
$$\mathbf{y} := G\mathbf{x}$$
Then we can make two-bits error by adding $\mathbf{e}_i + \mathbf{e}_j$ $(i \neq j)$ to $\mathbf{y}$.
- Parity checking

$$H(\mathbf{y} + \mathbf{e}_i + \mathbf{e}_j) = H\mathbf{y} + H(\mathbf{e}_i + \mathbf{e}_j) = HG\mathbf{x} + H(\mathbf{e}_i + \mathbf{e}_j) = H\mathbf{e}_i + H\mathbf{e}_j$$

Since

$$\begin{aligned} H\mathbf{e}_1 &= [1,0,0] \\ H\mathbf{e}_2 &= [0,1,0] \\ H\mathbf{e}_3 &= [1,1,0] \\ H\mathbf{e}_4 &= [0,0,1] \\ H\mathbf{e}_5 &= [1,0,1] \\ H\mathbf{e}_6 &= [0,1,1] \\ H\mathbf{e}_7 &= [1,1,1] \end{aligned}$$

there are no $\mathbf{e}_i$ and $\mathbf{e}_j$ $(i \neq j)$ such that

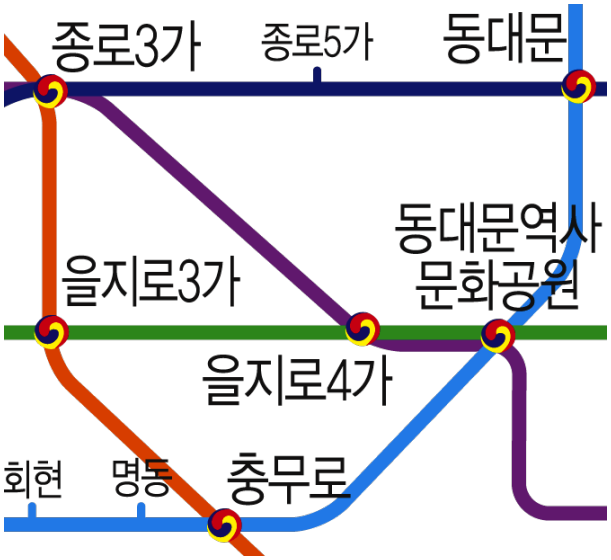
$$H\mathbf{e}_i + H\mathbf{e}_j = [0,0,0]$$

hence we can detect any two-bit error. But we cannot correct it since there are ambiguous cases. For example,

$$H(\mathbf{e}_4 + \mathbf{e}_5) = H \cdot [1,0,0] \text{ and } H(\mathbf{e}_6 + \mathbf{e}_7) = H \cdot [1,0,0]$$

which we cannot distinguish.

5. [40점] 다음은 서울 지하철 노선도의 일부이다.



(a) [10점] 위 노선도를 기반으로, 갈아타는 역(태극문양)들을 node로 하고 갈아타는 역들 간의 노선을 edge로 하는 그래프를 그려라. 이 때, 갈아타는 역 이외의 역은 무시한다.

(b) [10점] 앞의 문제에서 그린 그래프의 adjacency matrix를 구하라.

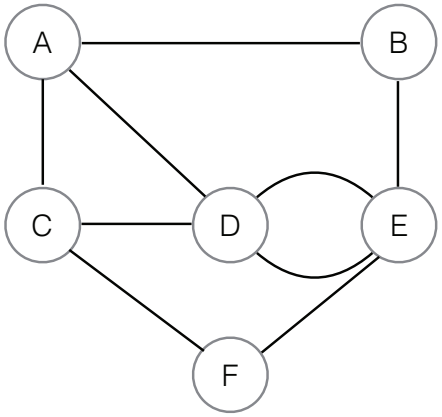
(c) [20점] <종로5가> 역에서 <충무로> 역까지 4번 이하의 회수만큼 열차를 갈아타서 갈 수 있는 경로는 총 몇 개인가? Matrix-matrix multiplication을 활용하여 구하라.

주의:
- 갈아타는 역에서는 (같은 노선을 계속 타는 경우에도) 반드시 열차를 갈아타야 한다. 따라서, 열차는 n번 갈아탄다는 것은 (출발지와 목적지를 제외한) 갈아타는 역을 n번 거친다는 의미이다.
- 동일한 갈아타는 역에서 한 번 이상 갈아타는 것도 가능하다.
- (출발지와 목적지를 제외하고는) 갈아타는 역 이외의 역에서는 내릴 수 없다.
- Matrix-matrix multiplication 방법을 사용하지 않고 일일이 경로를 세어 답을 구하는 것은 인정하지 않는다.

Solution:

(a)

- A: 종로3가
- B: 동대문
- C: 을지로3가
- D: 을지로4가
- E: 동대문역사문화공원
- F: 충무로



(b)

	A	B	C	D	E	F
A	0	1	1	1	0	0
B	1	0	0	0	1	0
C	1	0	0	1	0	1
D	1	0	1	0	2	0
E	0	1	0	2	0	1
F	0	0	1	0	1	0

$$\rightarrow A := \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$

(c) 종로5가에서 출발하는 경우 반드시 종로3가 혹은 동대문에서 갈아타야 한다. 따라서 A혹은 B에서부터 출발하여 F까지 이동하는 경우를 고려하면 된다. A, A^2, A^3, A^4는 각각 1, 2, 3, 4번 갈아타는 경우의 adjacency matrix가 된다.

$$A = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & \boxed{0} \\ 1 & 0 & 0 & 0 & 1 & \boxed{0} \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \quad A^2 = \begin{bmatrix} 3 & 0 & 1 & 1 & 3 & \boxed{1} \\ 0 & 2 & 1 & 3 & 0 & \boxed{1} \\ 1 & 1 & 3 & 1 & 3 & 0 \\ 1 & 3 & 1 & 6 & 0 & 3 \\ 3 & 0 & 3 & 0 & 6 & 0 \\ 1 & 1 & 0 & 3 & 0 & 2 \end{bmatrix},$$

$$A^3 = \begin{bmatrix} 2 & 6 & 5 & 10 & 3 & \boxed{4} \\ 6 & 0 & 4 & 1 & 9 & \boxed{1} \\ 5 & 4 & 2 & 10 & 3 & 6 \\ 10 & 1 & 10 & 2 & 18 & 1 \\ 3 & 9 & 3 & 18 & 0 & 9 \\ 4 & 1 & 6 & 1 & 9 & 0 \end{bmatrix} \quad A^4 = \begin{bmatrix} 21 & 5 & 16 & 13 & 30 & \boxed{8} \\ 5 & 15 & 8 & 28 & 3 & \boxed{13} \\ 16 & 8 & 21 & 13 & 30 & 5 \\ 13 & 28 & 13 & 56 & 6 & 28 \\ 30 & 3 & 30 & 6 & 54 & 3 \\ 8 & 13 & 5 & 28 & 3 & 15 \end{bmatrix}$$

따라서 4번 이하의 회수만큼 갈아타는 경우는 위에서 사각형으로 둘러싸인 수를 모두 더하면 된다.

$$(0+0)+(1+1)+(4+1)+(8+13)=28$$