

제 1 절 Matroid

Definition 1.1. 유한집합 E 와 E 의 부분집합족 $\mathcal{I}$ 에 대해 $M = (E, \mathcal{I})$ 이 아래 조건을 만족할 경우 M 은 **Matroid**라고 부른다.

1. $\{\} \in \mathcal{I}$
2. $B \subset A \in \mathcal{I} \Rightarrow B \in \mathcal{I}$ (hereditary property)
3. $A, B \in \mathcal{I}, |A| > |B| \Rightarrow \exists x \in A \setminus B$ s.t. $B \cup \{x\} \in \mathcal{I}$ (augmentation property)

Matroid M 에서 $\mathcal{I}$ 의 각 원소를 독립집합(Independent set)이라고 부르며, E 의 부분집합이지만 $\mathcal{I}$ 에 포함되지 않는 집합은 종속집합(Dependent set)이라고 부른다.

Definition 1.2. E 의 부분집합 B 가 아래 조건을 만족할 경우 B 는 Matroid $M = (E, \mathcal{I})$ 의 **Base**라고 부른다.

1. $B \in \mathcal{I}$
2. $\forall A$ s.t. $B \subset A \subset E, A \neq B \Rightarrow A \notin \mathcal{I}$

모든 Matroid는 **Base**를 가진다.

Theorem 1.1. Matroid $M = (E, \mathcal{I})$ 의 모든 Base의 크기는 같다.

Proof. 두 Base B_1, B_2 가 존재하여 $|B_1| < |B_2|$ 라고 가정하자. Matroid의 정의에 의해 $x \in B_2 \setminus B_1$ 인 x 가 존재하여 $B_1 \cup \{x\} \in \mathcal{I}$ 이고, 이는 B_1 이 Base인 것에 모순이다. 따라서 모든 Base의 크기는 같다. 또한 Base와 크기가 같은 독립집합은 모두 Base이다. $\square$

Definition 1.3. E 의 부분집합 C 가 아래 조건을 만족할 경우 C 는 Matroid $M = (E, \mathcal{I})$ 의 **Circuit**이라고 부른다.

1. $C \notin \mathcal{I}$
2. $\forall A$ s.t. $A \subset C, A \neq C \Rightarrow A \in \mathcal{I}$

독립집합의 부분집합에는 **Circuit**이 존재할 수 없고, 종속집합의 부분집합에는 무조건 **Circuit**이 존재한다.

Theorem 1.2. Matroid $M = (E, \mathcal{I})$ 의 두 Circuit $C_1 \neq C_2$ 와 $x \in C_1 \cap C_2$ 에 대해 $(C_1 \cup C_2) \setminus \{x\}$ 는 종속집합이다.

Proof. $A = (C_1 \cup C_2) \setminus \{x\}$ 가 독립집합이라고 가정하자. $I = C_1 \cap C_2$ 로 두면 Circuit의 정의에 의해 C_1 과 C_2 는 포함관계를 가질 수 없으므로 $I \subset C_1, I \neq C_1$ 이고, 따라서 I 는 독립집합이다.

Case 1. $|I| < |A|$

Matroid의 정의에 의해 I 에 $x \in A \setminus I$ 인 원소 x 를 추가하여 $|I|$ 를 독립집합으로 유지하면서 크기를 1 증가시킬 수 있다.

Case 2. $|I| = |A|$

$|I| = |A| = |C_1 \cup C_2| - 1$ 이고 $C_1 \cap C_2 \subset I$ 이므로 $C_1 \subset I$ 또는 $C_2 \subset I$ 를 만족해야 한다. 일반성을 잃지 않고 $C_1 \subset I$ 라고 하면, 종속집합 C_1 이 독립집합 I 의 부분집합이므로 Matroid의 정의에 모순이다. 따라서 A 는 종속집합이다.

□

Theorem 1.3. Matroid $M = (E, \mathcal{I})$ 에서 $A \in \mathcal{I}, a \notin A$ 를 고르면 다음 두가지중 하나가 성립한다.

1. $A \cup \{a\} \in \mathcal{I}$
2. $B \subset A \cup \{a\}$ 인 Circuit B 가 유일하게 존재하여 임의의 $b \in B$ 에 대해 $(A \cup \{a\}) \setminus \{b\}$ 가 독립집합이다.

Proof. $A \cup \{a\} \in \mathcal{I}$ 인 경우는 자명하므로 $A \cup \{a\} \notin \mathcal{I}$ 라고 가정하자. $B \subset A \cup \{a\}$ 인 Circuit B 가 존재한다. $B \neq C$ 이고 $C \subset A \cup \{a\}$ 인 Circuit C 가 존재한다면 A 가 독립집합이기 때문에 $a \in B, C$ 이다. Theorem 1.2에 의해 $(B \cup C) \setminus \{a\}$ 는 종속집합이다. 그런데 $(B \cup C) \setminus \{a\} \subset A$ 이므로 Matroid의 정의에 모순이다. 따라서 $A \cup \{a\}$ 에 포함되는 Circuit은 유일하게 존재한다. 또한 Circuit의 정의에 의해 $A \cup \{a\}$ 의 부분집합이 종속집합이라면 B 를 포함해야 한다. 모든 $b \in B$ 에 대해 $(A \cup \{a\}) \setminus \{b\}$ 는 B 를 포함할 수 없고, 따라서 모두 독립집합이 된다. □

Theorem 1.4. Matroid $M = (E, \mathcal{I})$ 과 각 원소의 비용함수 $w : E \rightarrow \mathbb{R}$, 집합의 비용함수 $W : \mathcal{I} \rightarrow \mathbb{R}$ 이 주어지고 $W(X) = \sum_{x \in X} w(x)$ 일 경우, 아래 알고리즘은 함수 $W(R)$ 이 최대가 되는 집합 R 를 구한다.

1. E 의 원소 $e_1, e_2, \dots, e_n$ 이 모든 $2 \leq i \leq n$ 에 대해 $w(e_{i-1}) \geq w(e_i)$ 를 만족하도록 순서를 정한다.
2. $R = \{\}$ 으로 둔다. R 은 독립집합이다.
3. i 를 1부터 n 까지 보면서 $w(e_i) > 0$ 이고 $R \cup \{e_i\}$ 가 독립집합일 경우 R 에 e_i 를 추가한다.
4. R 은 $W(R)$ 이 최대가 되는 집합이다.

Proof. $w(e) \leq 0$ 인 e 는 선택할 필요가 없으므로 없는 것으로 생각할 수 있다. $i = k$ 까지 보았을 때의 집합 R 을 R_k 로 두자. ($R_0 = \{\}$) 모든 $0 \leq i \leq n$ 에 대해 $R_i \subset A_i, A_i \setminus R_i \subset \{e_{i+1}, \dots, e_n\}$ 이고 $W(A_i)$ 가 최대인 M 의 Base A_i 가 존재함을 수학적 귀납법으로 보이자.

Case 1. $k = 0$

$\mathcal{I}$ 가 유한집합이므로 $W(X)$ 가 최대인 $X \in \mathcal{I}$ 가 존재하고, $A_0 = X$ 로 두면 성립한다.

Case 2. $k \geq 1$

수학적 귀납법의 가정에 의해 조건을 만족하는 A_{k-1} 이 존재한다.

$R_{k-1} \cup \{e_k\} \notin \mathcal{I}$ 인 경우 $R_{k-1} = R_k$ 이다. $e_k \in A_{k-1}$ 라고 가정하면 $R_{k-1} \cup \{e_k\} \subset A_{k-1} \in \mathcal{I}$ 이므로 모순이다. 따라서 $A_k = A_{k-1}$ 으로 충분하다.

$R_{k-1} \cup \{e_k\} \in \mathcal{I}$ 인 경우 $R_{k-1} \cup \{e_k\} = R_k$ 이다. $e_k \in A_{k-1}$ 라면 $A_k = A_{k-1}$ 으로 충분하다.

마지막으로 $e_k \notin A_{k-1}$ 인 경우만 확인하면 된다. R_i 와 A_{k-1} 은 독립집합이므로 Matroid의 정의를 이용하여 R_i 가 Base가 될 때까지 A_{k-1} 의 원소를 추가할 수 있다. 이 집합을 B 로 쓰자. $R_k \setminus \{e_k\} \subset A_{k-1}, \{e_k\} \not\subset A_{k-1}$ 이므로 $B \setminus A_{k-1} = \{e_k\}$ 이다. Base의 성질에 의해 $|A_{k-1}| = |B|$ 이므로 $|A_{k-1} \setminus B| = 1$ 이고, $A_{k-1} \setminus B = \{e_l\}$ 으로 쓰자. $A_{k-1} \setminus R_k = A_{k-1} \setminus (R_{k-1} \cup \{e_k\}) \subset \{e_{k+1} \dots e_n\}$ 이므로 $l \geq k+1$ 이고 $w(e_l) \leq w(e_k)$ 이다. 따라서 $W(B) = W(A_{k-1}) + w(e_k) - w(e_l) \geq W(A_{k-1})$ 이고, $W(A_{k-1})$ 은 최대이기 때문에 $W(A_{k-1}) \geq W(B)$ 이므로 $W(A_{k-1}) = W(B)$ 이고, $A_k = B$ 로 두면 충분하다.

$R_n \subset A_n, A_n \setminus R_n \subset \{\}$ 이므로 $R_n = A_n$ 이고, R_n 은 $W(R_n)$ 을 최대로 하는 집합이 된다. $\square$

Theorem 1.5. *hereditary property*를 만족하지 않는 $M = (E, \mathcal{I})$ 과 각 원소의 비용함수 $w : E \rightarrow \mathbb{R}$, 집합의 비용함수 $W : \mathcal{I} \rightarrow \mathbb{R}$ 이 주어지고 $W(X) = \sum_{x \in X} w(x)$ 일 경우, Theorem 1.4의 알고리즘이 함수 $W(R)$ 이 최대가 되는 집합 R 를 구하지 못하게 하는 비용함수 w 가 존재한다.

Proof. $A \subset B \subset E$ 이고 $A \notin \mathcal{I}, B \in \mathcal{I}$ 인 A, B 가 존재한다. 다음과 같은 비용함수를 정의하자.

$$w(x) = \begin{cases} 2 & (x \in A) \\ 1 & (x \in B \setminus A) \\ 0 & (\text{otherwise}) \end{cases} \quad (1)$$

1.4의 알고리즘은 A 의 원소를 모두 고르지는 못하고, 나머지를 고른 뒤 끝난다. 이 때 총 비용은 최대 $2(|A| - 1) + (|B| - |A|)$ 이다. 그러나 B 의 원소를 모두 고른 경우 총 비용은 $2|A| + (|B| - |A|)$ 로 더 높다. 따라서 1.4의 알고리즘은 실패한다. $\square$

Theorem 1.6. *augmentation property*를 만족하지 않는 $M = (E, \mathcal{I})$ 과 각 원소의 비용함수 $w : E \rightarrow \mathbb{R}$, 집합의 비용함수 $W : \mathcal{I} \rightarrow \mathbb{R}$ 이 주어지고 $W(X) = \sum_{x \in X} w(x)$ 일 경우, Theorem

1.4의 알고리즘이 함수 $W(R)$ 이 최대가 되는 집합 R 를 구하지 못하게 하는 비용함수 w 가 존재한다.

Proof. $|A| < |B|$ 이고 임의의 $a \in B \setminus A$ 에 대해 $A \cup \{a\} \notin \mathcal{I}$ 인 $A, B \in \mathcal{I}$ 가 존재한다. 다음과 같은 비용함수를 정의하자.

$$w(x) = \begin{cases} 1 + \frac{1}{2|A|+1} & (x \in A) \\ 1 & (x \in B \setminus A) \\ 0 & (\text{otherwise}) \end{cases} \quad (2)$$

Theorem 1.4의 알고리즘은 A 의 원소를 모두 고른 뒤, $B \setminus A$ 의 원소를 하나도 고르지 못하고 비용이 0인 것들을 고른 뒤 끝난다. 이 때 총 비용은 $|A| \left(1 + \frac{1}{2|A|+1}\right) < |A| + \frac{1}{2}$ 이다. 그러나 B 의 원소만 모두 고른 경우 총 비용은 $|B| \geq |A| + 1$ 로 더 높다. 따라서 Theorem 1.4의 알고리즘은 실패한다. $\square$

제 2 절 Span

Definition 2.1. Matroid $M = (E, \mathcal{I})$ 에 대해 **Rank** 함수 $r_M : 2^E \rightarrow \mathbb{N}_0$ 은 $r_M(X) = \max_{Y \in \mathcal{I}, Y \subset X} (|Y|)$ 로 정의된다. X 에 대해 $Y \in \mathcal{I}, Y \subset X$ 이고 $r_M(X) = |Y|$ 가 되는 Y 를 X 의 극대독립집합이라고 부른다. 추가로 Matroid M 의 **Rank**는 $r_M(E)$ 로 정의되며, M 의 Base의 크기와 같다. 다루는 Matroid가 하나일 때는 편의상 $r_M = r$ 으로 쓰자.

Theorem 2.1. $A \subset B \Rightarrow r(A) \leq r(B)$

Proof. A 의 극대독립집합은 B 에 포함되므로 $r(A) \leq r(B)$ 이다. $\square$

Theorem 2.2. $r(A) + r(B) \geq r(A \cup B) + r(A \cap B)$

Proof. $A \cap B$ 의 극대독립집합을 I_1 로 쓰자. Matroid의 정의에 의해 $I_1 \subset I$ 인 $A \cup B$ 의 극대독립집합 I 를 만들 수 있다. $I_2 = I \cap (A \setminus B), I_3 = I \cap (B \setminus A), I_4 = I \cap (A \cap B)$ 으로 정의하면 $r(A \cup B) = |I| = |I_2| + |I_3| + |I_4|$ 이다. $I_1 \subset I_4$ 이고 I_1 이 극대독립집합이므로 $I_1 = I_4$ 이다. $I_1 \cup I_2 \subset I, A$ 이므로 $I_1 \cup I_2$ 는 독립집합이고 $|I_1| + |I_2| \leq r(A)$ 이며, $I_1 \cup I_3 \subset I, B$ 이므로 $I_1 \cup I_3$ 는 독립집합이고 $|I_1| + |I_3| \leq r(B)$ 이다. 식을 정리하면 $r(A) + r(B) \geq 2|I_1| + |I_2| + |I_3| = r(A \cup B) + r(A \cap B)$ 이다. $\square$

Definition 2.2. Matroid $M = (E, \mathcal{I})$ 와 $A \subset E$ 에 대해 M 에서 A 의 **Span**은 $\text{span}(A) = \{a \in E \mid r(A \cup \{a\}) = r(A)\}$ 로 정의된다.

Theorem 2.3. $A \subset B \Rightarrow \text{span}(A) \subset \text{span}(B)$

Proof. $a \in \text{span}(A)$ 인 모든 a 에 대해 Theorem 2.2를 사용하자.

$$r(A \cup \{a\}) + r(B) \geq r((A \cup \{a\}) \cup B) + r((A \cup \{a\}) \cap B) \geq r(B \cup \{a\}) + r(A) \quad (3)$$

$a \in \text{span}(A)$ 이므로 span 의 정의에 의해 $r(A \cup \{a\}) = r(A)$ 이고, 부등식은 $r(B) \geq r(B \cup \{a\})$ 가 된다. Theorem 2.1에 의해 $r(B) \leq r(B \cup \{a\})$ 이므로 $r(B) = r(B \cup \{a\})$ 이고, span 의 정의에 의해 $a \in \text{span}(B)$ 이다. 따라서 $\text{span}(A) \subset \text{span}(B)$ 이다. $\square$

Theorem 2.4. $a \in \text{span}(A) \Rightarrow \text{span}(A \cup \{a\}) = \text{span}(A)$

Proof. Theorem 2.3에 의해 $\text{span}(A) \subset \text{span}(A \cup \{a\})$ 이다. $\text{span}(A \cup \{a\}) \subset \text{span}(A)$ 를 보이자. $b \in \text{span}(A \cup \{a\})$ 인 모든 b 에 대해 Theorem 2.2를 사용하자.

$$r(A \cup \{a\}) + r(A \cup \{b\}) \geq r(A \cup \{a\} \cup \{b\}) + r(A \cup (\{a\} \cap \{b\})) \geq r(A \cup \{a\} \cup \{b\}) + r(A) \quad (4)$$

$a \in \text{span}(A)$ 이므로 span 의 정의에 의해 $r(A \cup \{a\}) = r(A)$ 이므로 부등식은 $r(A \cup \{b\}) \geq r(A \cup \{a\} \cup \{b\})$ 가 된다. Theorem 2.1에 의해 $r(A \cup \{b\}) \leq r(A \cup \{a\} \cup \{b\})$ 이므로 $r(A \cup \{b\}) = r(A \cup \{a\} \cup \{b\})$ 이다. $b \in \text{span}(A \cup \{a\})$ 이므로 $r(A \cup \{b\}) = r(A \cup \{a\})$ 이고, $a \in \text{span}(A)$ 이므로 $r(A \cup \{b\}) = r(A)$ 이고, span 의 정의에 의해 $b \in \text{span}(A)$ 이다. 따라서 $\text{span}(A \cup \{a\}) = \text{span}(A)$ 이다. $\square$

Theorem 2.5. $\text{span}(\text{span}(A)) = \text{span}(A)$

Proof. $\text{span}(A) = \{a_1, \dots, a_n\}$ 으로 두자. $\text{span}(A) = \text{span}(A \cup \{a_1\}) = \text{span}(A \cup \{a_1, a_2\}) = \dots = \text{span}(A \cup \{a_1, \dots, a_n\}) = \text{span}(\text{span}(A))$ $\square$

Theorem 2.6 (Strong Base Exchange Theorem). *Matroid $M = (E, \mathcal{I})$ 의 Base $B_1 \neq B_2$ 와 $x \in B_1 \setminus B_2$ 에 대해 $y \in B_2 \setminus B_1$ 가 존재하여 $(B_1 \setminus \{x\}) \cup \{y\}, (B_2 \setminus \{y\}) \cup \{x\}$ 가 모두 M 의 Base이다.*

Proof. $B_2 \cup \{x\}$ 는 종속집합이므로 Theorem 1.3에 의해 $B_2 \cup \{x\}$ 에 포함되는 유일한 Circuit C 이 존재한다. B_2 의 부분집합은 모두 독립집합이므로 $x \in C$ 이다. Theorem 2.3에 의해 $x \in \text{span}(C \setminus \{x\}) \subset \text{span}((B_1 \cup C) \setminus \{x\})$ 이고, $x \in \text{span}((B_1 \cup C) \setminus \{x\})$ 이므로 Theorem 2.4에 의해 $\text{span}((B_1 \cup C) \setminus \{x\}) = \text{span}(B_1 \cup C)$ 이다. B_1 이 Base이므로 $\text{span}((B_1 \cup C) \setminus \{x\}) = \text{span}(B_1 \cup C) = E$ 이다. $\text{span}((B_1 \cup C) \setminus \{x\}) = E$ 인 것은 $(B_1 \cup C) \setminus \{x\}$ 가 Base를 포함하는 것과 동치이다. 이 Base를 B_3 으로 두자.

$B_1 \setminus \{x\}$ 와 B_3 은 독립집합이고, $|B_1 \setminus \{x\}| + 1 = |B_3|$ 이다. 따라서 $y \in B_3 \setminus (B_1 \setminus \{x\})$ 가 존재하여 $(B_1 \setminus \{x\}) \cup \{y\}$ 는 Base가 된다. $B_3 \setminus (B_1 \setminus \{x\}) \subset ((B_1 \cup C) \setminus \{x\}) \setminus (B_1 \setminus \{x\}) \subset C \setminus \{x\}$

이므로 $y \in C \setminus \{x\}$ 가 되어 $y \in B_2 \setminus B_1$ 이다. 또한 Theorem 1.3에 의해 $(B_2 \setminus \{y\}) \cup \{x\}$ 도 Base이다. $\square$

Theorem 2.7. *Matroid $M = (E, \mathcal{I})$ 의 두 독립집합 $A \neq B$ 와 $x \in A \setminus B$ 가 있고 $|A| = |B|$ 이면, $y \in B \setminus A$ 가 존재하여 $(A \setminus \{x\}) \cup \{y\}$ 와 $(B \setminus \{y\}) \cup \{x\}$ 가 독립집합이다.*

Proof. Matroid $N = (E, \{n | n \in \mathcal{I}, |n| \leq |A|\})$ 를 정의하면 N 에서 A, B 는 Base이다. Theorem 2.6에 의해 성립한다. $\square$

제 3 절 Matroid Intersection

Definition 3.1. Matroid $M = (E, \mathcal{I})$ 과 독립집합 X 에 대해 유향이분그래프 $D_M(X)$ 를 아래와 같이 정의한다.

$$D_M(X) = (E, \{(u, v) | u \in X, v \in E \setminus X, (X \setminus \{u\}) \cup \{v\} \in \mathcal{I}\}) \quad (5)$$

Theorem 3.1. *Matroid $M = (E, \mathcal{I})$ 의 두 독립집합 $A \neq B$ 가 $|A| = |B|$ 를 만족하면 $D_M(A)$ 는 $A \Delta B$ 에서 perfect matching을 가진다. ($A \Delta B = (A \setminus B) \cup (B \setminus A)$)*

Proof. $|A \Delta B| = k$ 로 두고 수학적 귀납법을 사용하자.

Case 1. $k = 0$

정점이 없으므로 perfect matching이다.

Case 2. $k \geq 1$

2.7에 의해 $x \in A \setminus B, y \in B \setminus A$ 인 x, y 가 존재하여 $C = (B \setminus \{y\}) \cup \{x\}$ 가 독립집합이 된다. $|A \Delta C| < |A \Delta B|$ 이고 $|A| = |C|$ 이므로 수학적 귀납법의 가정에 의해 $D_M(A)$ 는 $|A \Delta C|$ 에서 perfect matching을 가진다. 이 perfect matching에 (x, y) 를 추가하면 $|A \Delta B|$ 에서의 perfect matching이 된다. $\square$

Theorem 3.2. *Matroid $M = (E, \mathcal{I})$ 의 독립집합 A 와 $B \subset E$ 인 두 집합이 존재하여 $|A| = |B|$ 이고, $D_M(A)$ 가 $A \Delta B$ 에서 유일한 perfect matching을 가진다면 B 는 독립집합이다.*

Proof. 먼저 아래 보조정리를 증명하자.

Lemma 3.2.1. *$G = (X, Y, E)$ 가 E 의 각 간선이 X 와 Y 사이를 잇는 이분그래프이고, G 가 유일한 perfect matching M 을 가진다면 아래 조건을 만족하도록 $X = \{x_1, \dots, x_n\}, Y = \{y_1, \dots, y_n\}$ 으로 순열 x, y 를 만들 수 있다.*

$$\{(x_1, y_1), \dots, (x_n, y_n)\} \subset M, \forall 1 \leq i < j \leq n \Rightarrow (x_i, y_j) \notin E \quad (6)$$

Proof. 매칭에 포함되는 간선은 Y 에서 X 로 가도록, 나머지 간선들은 X 에서 Y 로 가도록 간선에 방향을 붙이자. 이 유향그래프에서 사이클이 존재할 경우 사이클 위에 있는 간선들의 방향을 모두 뒤집어서 다른 매칭을 만들 수 있으므로 유일성에 모순된다. 따라서 이 그래프는 DAG 이므로 위상정렬 순서를 붙일 수 있다. 위상정렬 순서를 $T(x)$ 라고 쓰자. 모든 $2 \leq i \leq n$ 에 대해 $T(x_{i-1}) > T(x_i)$ 가 되도록 번호를 붙이면 매칭에 포함된 간선의 방향에 의해 모든 i 에 대해 $T(x_i) > T(y_i)$ 가 된다. 어떤 $1 \leq i < j \leq n$ 가 존재하여 $(x_i, y_j) \in E$ 라고 가정하면, $T(x_j) < T(x_i) < T(y_j) < T(x_j)$ 가 되어 모순이다. 따라서 이 순열은 조건을 만족한다. $\square$

보조정리에 의해 $A \setminus B = \{x_1, \dots, x_n\}, B \setminus A = \{y_1, \dots, y_n\}$ 으로 순열을 만들 수 있다. B 가 종속집합이라고 가정하면 $C \subset B$ 인 Circuit C 가 존재하고, $y_i \in C$ 인 i 가 하나 이상 존재한다. 이러한 i 중 최소를 고르자. $C \setminus \{y_i\}$ 의 원소는 $A \cap B$ 에 속하거나 y_j ($i < j$)이다. 따라서 $C \setminus \{y_i\} \subset \text{span}(A \setminus \{x_i\})$ 이다. Theorem 2.3과 Theorem 2.5에 의해 $\text{span}(C \setminus \{y_i\}) \subset \text{span}(\text{span}(A \setminus \{x_i\})) = \text{span}(A \setminus \{x_i\})$ 이다. C 는 Circuit이기 때문에 $y_i \in \text{span}(C \setminus \{y_i\}) \subset \text{span}(A \setminus \{x_i\})$ 이다. $y_i \in \text{span}(A \setminus \{x_i\})$ 라는 것은 $r(A \setminus \{x_i\}) = r((A \setminus \{x_i\}) \cup \{y_i\})$ 라는 것인데, $r(A \setminus \{x_i\}) < |A| = r((A \setminus \{x_i\}) \cup \{y_i\})$ 이므로 모순이다. 따라서 B 는 독립집합이다. $\square$

Theorem 3.3. Matroid $M_1 = (E, \mathcal{I}_1), M_2 = (E, \mathcal{I}_2)$ 의 Rank function을 각각 r_1, r_2 라고 쓸 때, $\max_{X \in \mathcal{I}_1 \cap \mathcal{I}_2} (|X|) \leq \min_{X \subset E} (r_1(X) + r_2(E \setminus X))$ 이다.

Proof. 임의의 $A \in \mathcal{I}_1 \cap \mathcal{I}_2, B \subset E$ 에 대해 $A \cap B \in \mathcal{I}_1, A \setminus B \in \mathcal{I}_2$ 이고, 따라서 $|A| = |A \cap B| + |A \setminus B| \leq r_1(B) + r_2(E \setminus B)$ 이다. $\square$

Definition 3.2. Matroid $M_1 = (E, \mathcal{I}_1), M_2 = (E, \mathcal{I}_2)$ 에 대해 유향이분그래프 $D_{M_1, M_2}(I)$ 는 $D_{M_1}(I)$ 의 간선과 $D_{M_2}(I)$ 의 방향을 거꾸로 돌린 간선을 합집합한 그래프로 정의된다.

Theorem 3.4. $U = \{x | x \in E \setminus I, I \cup \{x\} \in \mathcal{I}_1\}, V = \{x | x \in E \setminus I, I \cup \{x\} \in \mathcal{I}_2\}$ 인 집합 U, V 에 대해 $D_{M_1, M_2}(I)$ 의 간선을 사용해 U 의 정점에서 V 의 정점으로 이동하는 최단 경로를 R 이라고 하자.

1. R 이 존재하지 않는다면 I 는 $\mathcal{I}_1 \cap \mathcal{I}_2$ 에서 가장 큰 집합이고, $|I| = \min_{X \subset E} (r_1(X) + r_2(E \setminus X))$ 이다.

2. R 이 존재한다면 $J = I \Delta R \in \mathcal{I}_1 \cap \mathcal{I}_2$ 이고 $|J| = |I| + 1$ 이다.

따라서 $I = \{\}$ 에서 시작하여 R 이 존재할 경우 I 를 $I \Delta R$ 으로 만들고, R 이 존재하지 않을 때 중단하는 알고리즘은 $\mathcal{I}_1 \cap \mathcal{I}_2$ 에서 가장 큰 집합 I 를 찾는다.

Proof.

Case 1. R 이 존재하지 않음

U 나 V 가 공집합이라면 I 가 최대임은 자명하다. 둘 모두 공집합이 아니라면 X 를 V 로 가는 경로가 존재하는 정점의 집합으로 정의하자. $U \cap X$ 는 공집합이고 $X \subset V$ 이다.

$r_1(X) > |I \cap X|$ 라고 가정하자. Matroid의 정의에 의해 $x \in X \setminus I$ 가 존재하여 $(I \cap X) \cup \{x\} \in \mathcal{I}_1$ 이 된다. x 는 X 에 포함되어 U 에는 포함될 수 없으므로 $I \cup \{x\} \notin \mathcal{I}_1$ 이다. $(I \cap X) \cup \{x\} \in \mathcal{I}_1$ 이고 $I \in \mathcal{I}_1$ 이므로 $y \in I \setminus X$ 가 존재하여 $(I \cup \{x\}) \setminus \{y\} \in \mathcal{I}_1$ 이 된다. 그러면 (y, x) 간선이 존재하고, $x \in X$ 라 $y \notin X$ 임에도 불구하고 y 에서 V 로 가는 경로가 존재하므로 모순이다. 따라서 $r_1(X) \leq |I \cap X|$ 이다.

$r_2(E \setminus X) > |I \setminus X|$ 라고 가정하자. Matroid의 정의에 의해 $x \in (E \setminus X) \setminus I$ 가 존재하여 $(I \cap (E \setminus X)) \cup \{x\} \in \mathcal{I}_2$ 가 된다. x 는 X 에 포함되지 않아 V 에는 포함될 수 없으므로 $I \cup \{x\} \notin \mathcal{I}_2$ 다. $(I \cap (E \setminus X)) \cup \{x\} \in \mathcal{I}_2$ 고 $I \in \mathcal{I}_2$ 이므로 $y \in I \setminus (E \setminus X)$ 가 존재하여 $(I \cup \{x\}) \setminus \{y\} \in \mathcal{I}_2$ 가 된다. 그러면 (x, y) 간선이 존재하고, $y \in X$ 라 $x \notin X$ 임에도 불구하고 x 에서 V 로 가는 경로가 존재하므로 모순이다. 따라서 $r_2(E \setminus X) \leq |I \setminus X|$ 이다.

위 두 식과 Theorem 3.3에 의해 $r_1(X) + r_2(E \setminus X) \leq |I \cap X| + |I \setminus X| = |I| \leq r_1(X) + r_2(E \setminus X)$ 이다. 즉, $|I| = r_1(X) + r_2(E \setminus X)$ 이고, Theorem 3.3에 의해 이는 최대이다.

Case 2. R 이 존재함

$R = y_0, x_1, \dots, x_n, y_n$ 으로 두면 $x_i \in I, y_i \notin I$ 이므로 $|J| = |I| + 1$ 이 되고, $J = \{y_0, \dots, y_n\} \cup (I \setminus \{x_1, \dots, x_n\})$ 이다. $A = \{y_1, \dots, y_n\} \cup (I \setminus \{x_1, \dots, x_n\})$ 로 두자. $1 \leq i \leq n$ 에 대해 (x_i, y_i) 를 매칭하면 이 매칭은 D_{M_1} 에서 $A \Delta I$ 의 유일한 perfect matching이다. 유일하지 않다면 Theorem 3.2의 보조정리에 의해 $1 \leq i < j \leq n$ 이고 간선 (x_i, y_j) 가 존재하는데, 이는 R 이 최단경로인 것에 모순이다. $A \Delta I$ 의 유일한 perfect matching이 존재하므로 Theorem 3.2에 의해 A 는 M_1 의 독립집합이다.

R 이 최단경로이기 때문에 $y_0 \in U$ 이고 $i \geq 1$ 에 대해서는 $y_i \notin U$ 이다. $I \cup \{y_i\} \notin \mathcal{I}_1$ 이므로 $r_1(I \cup A) = |I| = |A|$ 이다. $I \cup \{y_0\} \in \mathcal{I}_1$ 이고 $|I| = |A|$ 이므로 $a \in (I \cup \{y_0\}) \setminus A$ 인 a 가 존재하여 $A \cup \{a\} \in \mathcal{I}_1$ 이다. $a \in I$ 라면 $|A| = r_1(I \cup A) \geq |A| + 1$ 가 되어 모순이므로 $a = y_0$ 이다. 따라서 $A \cup \{y_0\} = J \in \mathcal{I}_1$ 이다.

$A = \{y_0, \dots, y_{n-1}\} \cup (I \setminus \{x_1, \dots, x_n\})$ 로 두고 U 대신 V 를 사용하면 $J \in \mathcal{I}_2$ 도 보일 수 있다. 따라서 $J \in \mathcal{I}_1 \cap \mathcal{I}_2$ 이다. □

Theorem 3.5 (Min-max Formula). *Matroid $M_1 = (E, \mathcal{I}_1), M_2 = (E, \mathcal{I}_2)$ 의 Rank function을 각각 r_1, r_2 라고 쓸 때, $\max_{X \in \mathcal{I}_1 \cap \mathcal{I}_2} (|X|) = \min_{X \subset E} (r_1(X) + r_2(E \setminus X))$ 이다.*

Proof. Theorem 3.3과 Theorem 3.4의 construction에 의해 성립한다. □

Theorem 3.6. 3개 이상의 *Matroid Intersection*은 *NP-Hard* 문제이다.

Proof. 유향그래프의 간선 집합 E 를 정의하자. $\mathcal{I}_1$ 을 모든 정점의 indegree가 1 이하인 간선의 집합 모음, $\mathcal{I}_2$ 을 모든 정점의 outdegree가 1 이하인 간선의 집합 모음, $\mathcal{I}_3$ 을 방향을 무시했을 때 forest를 구성하는 간선의 집합 모음으로 정의했을 때, $(E, \mathcal{I}_1), (E, \mathcal{I}_2), (E, \mathcal{I}_3)$ 의 Matroid Intersection은 Hamiltonian path와 동치이고, 이는 NP-Hard 문제이다. $\square$