Matroids

Example) $v_1 = (1\,0\,0)$ $v_2 = (1\,1\,0)$ $v_3 = (0\,1\,1)$ $v_4 = (1\,1\,1)$ $v_5 = (0\,1\,0)$

$S = (v_1, v_2, v_3, v_4, v_5)$ $\mathcal{I} = \{ I \subseteq S \mid I \text{ is linear independent} \}$

$= \{ \{v_1 v_3 v_5\}\ \{v_1 v_2 v_3\}\ \{v_1 v_2 v_4\}$
$\{v_2 v_3 v_4\}\ \{v_2 v_3 v_5\}\ \{v_3 v_4 v_5\}$
$\{v_1 v_2\}\ \{v_1 v_3\}\ \{v_1 v_4\}\ \{v_1 v_5\}\ \{v_2 v_3\}$
$\{v_2 v_4\}\ \{v_2 v_5\}\ \{v_3 v_4\}\ \{v_3 v_5\}\ \{v_4 v_5\}$
$\{v_1\} \cdots \{v_5\}\ \emptyset\ \}$

Def We say $(S, \mathcal{I})$ is a matroid **if** S is a finite set (ground set)
and $\mathcal{I}$ is a nonempty collection of subsets of S
satisfying ① if $I \in \mathcal{I}$ and $J \subseteq I$ then $J \in \mathcal{I}$
② if $I, J \in \mathcal{I}$ and $|I| < |J|$
then there exists $z \in J \setminus I$
such that $I + z \in \mathcal{I}$

※ $A + x$ denotes $A \cup \{x\}$
$A - x$ denotes $A \setminus \{x\}$

Def Given a matroid, $(S, \mathcal{I})$ we say $I \subseteq S$ is independent if $I \in \mathcal{I}$
and $I \subseteq S$ is dependent if $I \notin \mathcal{I}$

Def We say $(S, \mathcal{I})$ is an independent system if it satisfies ① (but not necessarily ②)

Def Linear Matroid.
Given matrix A, let S denote its cols.
For $I \subseteq S$, let A_I denote the sub matrix of A consisting of the cols in I
Let $\mathcal{I} := \{ I \subseteq S \mid \text{rank}(A_I) = |I| \}$ "full rank" // column-wise independent.
(full rank: column)

Def Graphic Matroid
Given a graph $G = (V, E)$, let $S := E$ and $\mathcal{I} := \{ I \subseteq E \mid (V, I) \text{ is acyclic} \}$
then $(S, \mathcal{I})$ is a graphic matroid.

Thm A graphic matroid is a matroid.

Proof S is finite and $\mathcal{I}$ is a nonempty collection of subsets of S, obviously.

② Suppose that $I, J \in \mathcal{I}$ and $|I| < |J|$
Then, there must exist an edge z in $J \setminus I$ such that connects two different connected components of (V, I). This shows that $\exists z \in J \setminus I$ s.t $I + z \in \mathcal{I}$

① (i) $J \subseteq I$, and I is acyclic, then J is also acyclic $\Rightarrow J \in \mathcal{I}$.

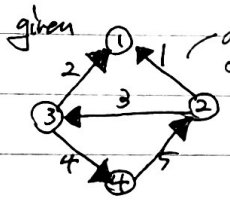
Therefore $(S, \mathcal{I})$ is a matroid.

eg)  I. ⇒ acyclic & connected. component 내 edge
$I = J$
⇒ Connect component 내 edge

Thm A graphic matroid is a linear matroid.

Proof Consider the transpose of the incidence matrix of an arbitrary orientation of the graph.

ex given



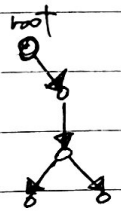
$\Rightarrow$

vertex \ edge	1	2	3	4	5
1	1	1	0	0	0
2	-1	0	-1	0	1
3	0	-1	1	-1	0
4	0	0	0	1	-1

(-1: source 1: terminal)

Since graphic matroid $(S, \mathcal{I})$ has $\mathcal{I} = \{I \subseteq E \mid (V, I) \text{ is } \underline{\text{acyclic}}\}$

Lets define I's incidence orientation has no multiple inward edge or I be a "directed rooted tree" (since acyclic).



Then, since N acyclic edges forms $(N+1)$ vertex tree with 1 root node.

$\Rightarrow$ by column matrix operations, root $\begin{bmatrix} -1 & -1 & -1 & \cdots & -1 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & & 0 \\ \vdots & & 1 & & 0 \\ & \cdots & & & 0 \end{bmatrix}$ $(N+1)$ will be generated which indicates that I has N row rank (and N column rank)

$\Rightarrow N = |I| = \text{rank}(A_I)$

$\therefore (S, \mathcal{I})$ is a linear matroid.

(// multiple components 인 경우 $\sum_{\text{component } C} \text{rank}(A_C) = |I|$)

Def Uniform matroid.

For some finite nonempty set S and $k \geq 0$. Let $\mathcal{I} := \{I \mid I \subseteq S, |I| \leq k\}$

Then $(S, \mathcal{I})$ is a uniform matroid.

Thm Uniform matroid is a matroid.

Proof since S is finite, $\mathcal{I}$ also is a nonempty collection.

① Suppose that $I \in \mathcal{I}$ and $J \subseteq I$. $\Rightarrow$ Then $|J| \leq |I|$ obviously.

by def of $\mathcal{I}$, $|I| \leq k \Rightarrow |J| \leq k \Rightarrow J \in \mathcal{I}$

② Suppose that $I, J \in \mathcal{I}$ and $|I| < |J|$

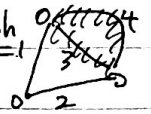
by def of $\mathcal{I}$, $|I| < |J| \leq k$ and $\exists$ at least one z s.t. $z \in J \setminus I$.

since $|I + z| \leq |J| \leq k$, $I + z \in \mathcal{I}$.

by ① and ②, a Uniform matroid is a matroid.

ex Consider $|S| = 4$ $k = 2$.

Matt. graph



$S = \{1, 2, 3, 4\}$ $(S, \mathcal{I}) \Rightarrow \mathcal{I} = \{\{\}, \{1\}, \{2\}, \{3\}, \{4\}, \{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}\}$

↳ Cyclic ✱✱

Def Partition Matroid.

Let $S_1, S_2, \cdots S_n$ be a partition of S (→ disjoint set & $\left(\bigcup_{i=1}^{n} S_i = S\right)$) for some finite nonempty set S.

and $\mathcal{I} := \{I \mid I \subseteq S \text{ and } |I \cap S_i| \leq k_i \text{ for } \theta\, i \in \{1, 2, \cdots n\}\}$

where $k_i \geq 0$ for $\theta\, i \in \{1, 2, \cdots n\}$

Then, $(S, \mathcal{I})$ is a partition Matroid.

Thm Partition Matroid is a matroid.

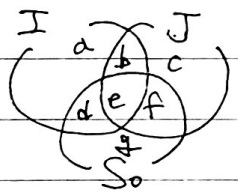
Proof S is finite & $\mathcal{I}$ is also a finite collection.

① if $I \in \mathcal{I}$ and $J \subseteq I$

for $\theta\, S_i$, $|I \cap S_i| \leq k_i$ therefore $|J \cap S_i| \leq k_i \Rightarrow J \in \mathcal{I}$

② if $I, J \in \mathcal{I}$ and $|I| < |J|$

for $\theta\, S_i$, $\begin{cases} |I \cap S_i| \leq k_i \\ |J \cap S_i| \leq k_i \end{cases}$ (Let's Suppose that ~~that~~ for a certain S_0, $\nexists\, z$ s.t $z \in J \setminus I$ and $|(I+z) \cap S_0| \leq k_0$

$\Rightarrow$ 

- $d+e \leq k_0$
- $e+f \leq k_0$ … ①
- $a+d < c+f$ (since $|I| < |J|$) … ②

since $\nexists\, z$ s.t $z \in J \setminus I$ and $|(I+z) \cap S_0| \leq k_0$

$\Rightarrow d+e+1 = k_0+1 > k_0$

$\Rightarrow d+e = k_0$ and $c = 0$

$\Rightarrow$ ① $\Rightarrow e+f \leq k_0 \Rightarrow f \leq d$.

② $\Rightarrow a+d < f+c \Rightarrow f > a+d$ where $a \geq 0$.] Contradiction

$\therefore \exists\, z \in J \setminus I$ s.t $|(I+z) \cap S_i| \leq k_i$ for $\theta\, i$

by ① and ② Partition matroid is a matroid.

Consider a matroid $(S, \mathcal{I})$

Def We say $x \in S$ is a **loop**, if $\{x\} \notin \mathcal{I}$ (therefore $\{x\}$ is a dependent set)

Remark] a loop cannot appear in any independent set

Remark] loop ≒ 필요없는 원소

Def We call a (inclusion-wise) maximal independent set a **base**.

Lemma] If B and B' are bases, then $|B| = |B'|$

proof) Suppose that $|B| < |B'|$

then by def, $\exists\, x \in B' \setminus B$ s.t. $B + x \in \mathcal{I}$

that is B is not inclusion-wise maximal. // Contradiction.

Lemma] Let B and B' be bases and $x \in B' \setminus B$

then $\exists\, y \in B \setminus B'$ such that $B' - x + y$ is a base.

proof) Since $B' - x \in \mathcal{I}$,

$\exists$ some $y \in B \setminus (B' - x) = B \setminus B'$ s.t. $(B' - x) + y \in \mathcal{I}$. by def.

Now. $(B' - x + y)$ is a base since $|B' - x + y| = |B'|$.

Def Let $(S, \mathcal{I})$ be a matroid and $\hat{S} \subseteq S$.

For $\hat{\mathcal{I}} := \{\hat{I} \mid \hat{I} \subseteq \hat{S},\ \hat{I} \in \mathcal{I}\}$, $(\hat{S}, \hat{\mathcal{I}})$ is called the restriction of $(S, \mathcal{I})$ to $\hat{S}$

Pos $(\hat{S}, \hat{\mathcal{I}})$ is a matroid.

proof) since $\hat{S} \subseteq S$ and $\hat{\mathcal{I}} \subseteq \mathcal{I}$, finite.

① Suppose that $J \in \hat{\mathcal{I}}$ and $I \subseteq J$.

since $J \subseteq \hat{S}$, $I \subseteq \hat{S}$

since $J \in \mathcal{I}$, $I \subseteq \mathcal{I}$ (def of matroid)

$I \subseteq \hat{S}$ and $I \in \mathcal{I} \Rightarrow I \in \hat{\mathcal{I}}$

② Suppose that $I, J \in \hat{\mathcal{I}}$ and $|I| < |J|$

then $I, J \in \mathcal{I}$, $\exists\, z \in J \setminus I$ such that $(I + z) \in \mathcal{I}$

$\Rightarrow$ since $(I + z) \in \mathcal{I}$ and $(I + z) \subseteq \hat{S}$, $(I + z) \in \hat{\mathcal{I}}$

by ① and ② $(\hat{S}, \hat{\mathcal{I}})$ is a matroid.

Def For $\hat{S} \subseteq S$, we say $\hat{B}$ is a base for $\hat{S}$

if $\hat{S}$ is a base of the restriction of $(S, \mathcal{I})$ to $\hat{S}$ $= (\hat{S}, \hat{\mathcal{I}})$

[Lemma] Let B be a base for some $X \subseteq S$ then for $\forall Y \supseteq X$,

$\exists$ a base B' for Y s.t. $B' \supseteq B$.

(proof) Note that B is independent in the restriction of the matroid to Y

$\Rightarrow (\hat{Y}, \hat{\mathcal{I}})$

Let B' be a maximal independent set that contains B in this matroid.

(Def) A circuit is a minimal dependent set.

(Thm) If C is a circuit, then for $\forall x \in C$, $C - x \in \mathcal{I}$

(means $(C-x)$ is independent)

(Lemma) [Unique circuit property]

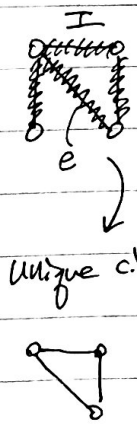
: Suppose that $I \in \mathcal{I}$ and $I + e \notin \mathcal{I}$ for some $I \subseteq S$ and $e \in S \setminus I$

Then, $\exists$ a unique circuit $C \subseteq I + e$.

(proof) 1. "Existance of circuit" follows directly from the def

2. In order to prove the uniqueness, suppose towards contradiction.

that $(I+e)$ contains two circuits C_1, C_2 and $C_1 \neq C_2$.



- Since C_2 is minimal, $\exists f \in C_1 \setminus C_2$ (since $C_1 \neq C_2$)

$\Rightarrow$ for $e \in C_2$, $e \neq f \in C_1 \setminus C_2$.

- Since $C_1 - f \in \mathcal{I}$, we can extend $C_1 - f$ to a maximal independent set X of $(I+e)$
- Since I is a maximal independent of $(I+e)$, $|I| = |X|$
- Moreover, since $e \in C_1 - f$, we have $e \in X$

since $(C_1 - f) + f = C_1 \notin \mathcal{I}$, we have $f \notin X$

Thus, $X = I + e - f$ is maximal independent.

since $f \in C_1 \setminus C_2$, This implies that $C_2 \subseteq I + e - f = X$

and C_2 is independent $\Rightarrow$ contradiction

$\therefore C_1 = C_2$: Unique circuit.

Cor Let C be the unique circuit in $(I+e)$ for some $I \in \mathcal{I}$ and $e \in S \setminus I$

For $\forall f \in C$, we have $\underline{(I+e)-f \in \mathcal{I}}$: independent

(※ dependent $(I+e)$ 에서 unique circuit 에서 edge (아무거나) 하나만 빼면,
// (I) 는 independent $\Rightarrow$ $(I+e-f)$ 는 다시 independent)

Pf Suppose towards contradiction that $(I+e-f)$ is dependent.

then, $\exists$ a circuit $C' \subseteq (I+e-f)$

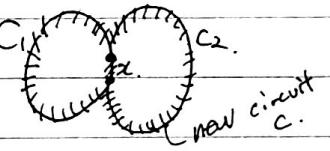
since $f \in C$, $f \notin C' \subseteq (I+e-f) \Rightarrow C \neq C'$

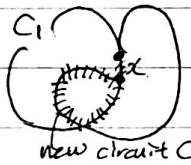
but $(I+e)$ has only one unique circuit ··· contradiction.

Corr Let C_1 and C_2 be two circuits s.t. $\underline{C_1 \neq C_2}$ and $\underline{x \in C_1 \cap C_2}$.

Then, for every $e \in C_1 \setminus C_2$, $\exists$ a circuit C such that $e \in C$ and $C \subseteq C_1 \cup C_2 - x$

In particular, $\underline{(C_1 \cup C_2 - x)}$ contains a circuit.

(e.g.) 

(e.g.) 

두개 겹치고 하나 빼면
⇒ 반드시 circuit이 생김,
⇒ 모든 edge는 이런 circuit에 포함된다.

Proof

We first show that $C(C_1 \cup C_2 - x)$ is dependent (thus, contains a circuit)

- Suppose that $C(C_1 \cup C_2 - x)$ is independent. (※ given $x \in C_1 \cap C_2$)

since C_1 is a circuit, $C(C_1 - f) \in \mathcal{I}$ (※ $f \in C_1 \setminus C_2$)

Let Z be: Extend $C(C_1 - f)$ to a maximal independent set in $(C_1 \cup C_2)$

then $Z \subseteq (C_1 \cup C_2)$ and $Z \in \mathcal{I}$.

[$C_1 \not\subseteq Z$ since C_1 dependent
$C_2 \not\subseteq Z$ since C_2 dependent] $\quad |Z| < |(C_1 \cup C_2) - x|$

C_1에 있는 f랑 C_2에 있는 최소 1개 뺐기에.

(※ so, $((C_1 \cup C_2) - x) \setminus Z$ 에 원소 z 를 expand 가능.

$\therefore C(C_1 \cup C_2 - x)$ contains a circuit. $\Rightarrow$ a contradiction to the maximality of Z.

// Let B_1 be a base for $C_1 \cup C_2$ that contains $C_1 - x_1 \Rightarrow x_1 \notin B_1$

(B_2 be a base for $C_1 \cup C_2$ that contains $C_2 - x_2$. $\Rightarrow x_2 \notin B_2$.

If $x_1 \notin B_2$ then $B_2 + x_1$ must have a circuit.

If $x_1 \in B_2$ then $\exists\ \hat{x} \in B_1 \setminus B_2$ s.t. $\hat{B} = B_2 - x_1 + \hat{x}$ (also a base for $C_1 \cup C_2$)

since $C_2 \not\subseteq \hat{B}$ $\hat{x} \neq x$ thus, $x_1 \notin \hat{B}$ and $\hat{B} + x_1$ must have a circuit.

Def Let $M = (S, \mathcal{I})$ be a matroid.
Its rank function denoted $r_M(\cdot)$, is a function $r_M : 2^S \to \mathbb{N}$
defined by $r_M(X) = \max\{|I| \mid I \subseteq X,\ I \in \mathcal{I}\}$

Def A set function $f : 2^S \to \mathbb{R}$ is called

★ submodular (def) $f(T) + f(U) \geq f(T \cup U) + f(T \cap U)$ for $\forall T, U \subseteq S$

supermodular (def) $f(T) + f(U) \leq f(T \cup U) + f(T \cap U)$ "

modular (def) $f(T) + f(U) = f(T \cup U) + f(T \cap U)$ "

[Alternatives of submodular] ← [Lemma] For a set function $f : 2^S \to \mathbb{R}$

TFAE

① $f(T) + f(U) \geq f(T \cup U) + f(T \cap U)$ for $\forall T, U \subseteq S$: (def) of submodular

② $f(T+s) - f(T) \geq f(U+s) - f(U)$ for $\forall T \subseteq U \subseteq S$ and $s \in S \setminus U$
(1→0) (1→0)

③ "diminishing return"

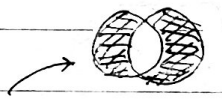
① → ② : $f(T+s) + f(U) \geq \underbrace{f((T+s) \cup U)}_{= f(U+s)} + \underbrace{f((T+s) \cap U)}_{= f(T)}$ since $T \subseteq U \subseteq S$

$\Rightarrow f(T+s) - f(T) \geq f(U+s) - f(U)$

③ $f(T+s) + f(T+t) \geq f(T) + f(T+s+t)$ for $\forall T \subseteq S$
and $s, t \in S \setminus T$ and $s \neq t$.

② → ③ (when $T + t = U$).

③ → ①



given ③, we prove ① by induction on $|T \triangle U|$ where $T \triangle U := (T \setminus U) \cup (U \setminus T)$

If $|T \triangle U| = 0$ ⋯ $T = U$ identical ① satisfied.

$|T \triangle U| = 1$ ⋯ $T \subseteq U$ or $U \subseteq T$ ⋯ ① satisfied.

$|T \triangle U| = 2$ ⋯ $T \subseteq U$ or $T \supseteq U$ or $|T \setminus U| = |U \setminus T| = 1$
(① satisfied)
① ⇒ $2k+2 \geq 2k+2$. satisfied.

If $|T \triangle U| \geq 3$ and WLOG assume that $|T \setminus U| \geq 2$.

by induction, for $t \in T \setminus U$ $f(T \cup U) - f(T) \leq f((T-t) \cup U) - f(T-t)$

Lemma] Let r be the rank function of any matroid $(S, \mathcal{I})$

Then the following holds.

① $0 \leq r(X) \leq |X|$ for $\forall X \subseteq S$

② $X \subseteq Y \Rightarrow r(X) \leq r(Y)$: monotonicity

③ r is submodular.

(proof) ① and ② by def.

For any $T \subseteq S$ and $s \in S \setminus T$

we have $r(T+s) = r(T)$ or $r(T+s) = r(T)+1$

hence, r is a submodular function.

(pf) for $\forall T \subseteq U \subseteq S$, $f(T+s) - f(T) \geq f(U+s) - f(U)$: def ② of submodular

or $r(U+s) - r(U) = 1$ implies $r(T+s) - r(T) = 1$

(// 다른 경우는 부등호를 만족하므로)

⇒ (pf) $r(U+s) - r(U) = 1$ then every base B for $(U+s)$ contains s

($s \in U$ 와 같이 independent 이므로)

Let B' be a base for T. Since $T \subseteq (U+s)$, we use a base B'' for $(U+s)$ that contains B'

Note that $s \in B''$. observe that $(B'+s)$ is independent since $(B'+s) \subseteq B''$

this shows that $r(T+s) = r(T)+1$

Since $r(U+s) - r(U) = 1$ implies $r(T+s) - r(T) = 1$

, function $r(\cdot)$ is a submodular function.

Span

Def) For $X \subseteq S$, the span of X, denoted by $span(X)$ is defined as.

$$span(X) := \{ y \mid y \in S,\ r(X+y) = r(X) \}$$

X의 rank를 증가시키지 않는 S의 모든 원소의 집합.

(⇒ y는 X에 total independent 할 수 없다)

Lemma ① $T, U \subseteq S$ and $U \subseteq span(T)$ than $span(U) \subseteq span(T)$

proof since $U \subseteq span(T)$,

we have $r(T \cup U) = r(T)$ ·proof suppose that $r(T \cup U) > r(T)$ (cannot trivially false)

maximal independent set의 크기.

Let B be some base for T (maximal independent set),

we can extend B to a base B' for $(T \cup U)$

s.t $|B'| > |B|$

$\Rightarrow \exists x \in U \setminus T$ s.t $r(T+x) > r(T)$

… contradiction.

Let x be an arbitrary element in $span(U)$, i.e $r(U+x) - r(U) = 0$

From the submodularity of $r(\cdot)$

def ② submodular function

$f(T+s) - f(T) \geq f(U+s) - f(U)$ for $\forall T \subseteq U \subseteq S$ and $s \in S \setminus U$

since $(T \cup U) \supseteq U$ $\quad r(U+x) - r(U) \geq r((T \cup U)+x) - r(T \cup U)$

$=0$

$\Rightarrow r((T \cup U)+x) - r(T \cup U) = 0$

$\Rightarrow r(T \cup U) = r(T \cup (U+x)) \geq r(T+x)$: $x \in span(U)$

$\geq r(T) = r(T \cup U)$: premise.

$\Rightarrow$ possibly $r(T+x) = r(T)$ … x is an element in $span(T)$

$\therefore$ if x is in $span(U)$ then also in $span(T)$

$\Rightarrow span(U) \subseteq span(T)$

Lemma ② If $T \subseteq S$, $t \in S \setminus T$ and $s \in span(T+t) \setminus span(T)$

then, $t \in span(T+s)$

proof we have $r(T+t) = r(T+t+s) \geq r(T+s)$

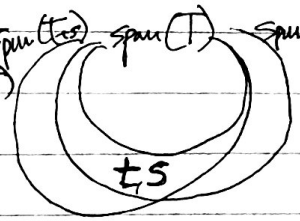
$s \in span(T+t)$ $\quad r(\cdot)$: monotone increasing

$= r(T) + 1$: $s \notin span(T)$

$\geq r(T+t)$

$= r(T)$ or $r(T)+1$

⊖



$\rightarrow r(T+t+s) = r(T+s)$ $\quad \therefore t \in span(T+s)$

Def) We say $X \subseteq S$ is a flat if $span(X) = X$