**Discrete Methods in Informatics** November 7, 2005

Lecture 4 (Matroid)

*Lecturer*: *Satoru Iwata* *Scribe*: *Mizuyo Takamatsu, Kenjiro Takazawa*

# 1 Matroid

In 1935, Whitney introduced the notion of *matroid* for the sake of a combinatorial abstraction of matrices with respect to linear independence. It is named after "matrix" and "-oid."

First, we consider a matrix $Q$ over a field $\mathbb{K}$ with the row set $R$ and the column set $E$. Let us denote by $Q[X, Y]$ the submatrix of $Q$ determined by $X \subseteq R$ and $Y \subseteq E$. A subset family $\mathcal{I} \subseteq 2^E$ defined by

$$\mathcal{I} = \{J \mid J \subseteq E,\ \operatorname{rank} Q[R, J] = |J|\} \tag{1}$$

satisfies the following (I0)–(I2):

**(I0)** $\emptyset \in \mathcal{I}$,

**(I1)** $I \subseteq J \in \mathcal{I} \Rightarrow I \in \mathcal{I}$,

**(I2)** $I, J \in \mathcal{I},\ |I| < |J| \Rightarrow \exists j \in J \setminus I,\ I \cup \{j\} \in \mathcal{I}$.

In general, a *matroid* is a pair $(E, \mathcal{I})$ of a finite set $E$ and its subset family $\mathcal{I}$ satisfying (I0)–(I2). We call $E$ the *ground set*, $\mathcal{I}$ the *independent set family*, and $I \in \mathcal{I}$ an *independent set*. The pair $(E, \mathcal{I})$ defined by (1) is an example of matroids, called a *linear matroid* represented by $Q$ over $\mathbb{K}$.

Given a matroid $(E, \mathcal{I})$, a subset $B \subseteq E$ is called a *base* if $B$ is an inclusion-wise maximal independent set. The following proposition immediately follows from (I2).

**Proposition 1.** *All bases of a matroid have the same cardinality.*

In a linear matroid represented by $Q$, the cardinality of a base equals to $\operatorname{rank} Q$. In this case, Proposition 1 shows that in Gaussian elimination, the number of nonzero rows of the resulting matrix, which is equal to $\operatorname{rank} Q$, does not depend on the choice of the pivoting elements.

We call the collection of all the bases the *base family*. The base family $\mathcal{B}$ satisfies the following (B0)–(B1):

**(B0)** $\mathcal{B} \neq \emptyset$,

**(B1)** $B, B' \in \mathcal{B},\ b \in B \setminus B' \Rightarrow \exists e \in B' \setminus B,\ (B \setminus \{b\}) \cup \{e\} \in \mathcal{B}$.

Note that (B1) follows from (I2) by putting $J = B'$ and $I = B \setminus \{b\}$.

For a matroid $(E, \mathcal{I})$, we define the *rank function* $\rho : 2^E \to \mathbb{Z}_+$ by

$$\rho(X) = \max\{|J| \mid J \subseteq X, J \in \mathcal{I}\} \quad (X \subseteq E).$$

Then, $\rho$ satisfies the following (R0)–(R3):

**(R0)** $\rho(\emptyset) = 0$,

**(R1)** $\forall X \subseteq E,\ \rho(X) \leq |X|$,

**(R2)** $X \subseteq Y \Rightarrow \rho(X) \leq \rho(Y)$,

**(R3)** $\forall X, Y \subseteq E,\ \rho(X) + \rho(Y) \geq \rho(X \cup Y) + \rho(X \cap Y)$ (i.e., $\rho$ is submodular).

*Proof of* (R3). Let $H$ be a base of $X \cap Y$, $I$ a base of $X$ containing $H$, and $J$ a base of $X \cup Y$ containing $I$. Then, $|H| = \rho(X \cap Y)$, $|I| = \rho(X)$, and $|J| = \rho(X \cup Y)$. Moreover, $|J \cap Y| = |J \setminus X| + |H| = |J| - |I| + |H|$. Hence,

$$\begin{aligned} |J \cap Y| &= |J| - |I| + |H| \\ &= \rho(X \cup Y) - \rho(X) + \rho(X \cap Y). \end{aligned}$$

Meanwhile, $J \cap Y \in \mathcal{I}$ implies $|J \cap Y| \leq \rho(Y)$. Therefore, $\rho(X) + \rho(Y) \geq \rho(X \cup Y) + \rho(X \cap Y)$ holds. □

In a matroid $(E, \mathcal{I})$ defined by (1), the rank function is given by $\rho(X) = \operatorname{rank} Q[R, X]$.

It is known that both of (B0)–(B1) and (R0)–(R3) are equivalent to (I0)–(I2). That is, if we define $\mathcal{I} = \{J \mid J \subseteq B \in \mathcal{B}\}$ or $\mathcal{I} = \{J \mid \rho(J) = |J|\}$, $\mathcal{I}$ satisfies (I0)–(I2). In other words, we can define a matroid with (B0)–(B1) or (R0)–(R3).

Given a matroid $(E, \mathcal{I})$, a member of $2^E \setminus \mathcal{I}$ is called a *dependent set*. A subset $C \subseteq E$ is called a *circuit* if $C$ is an inclusion-wise minimal dependent set. In general, all circuits do not have the same cardinality, which is in contrast to the case of the bases (cf. Proposition 1). We call the collection of all the circuits the *circuit family*. The circuit family $\mathcal{C}$ satisfies the following (C0)–(C2):

**(C0)** $\emptyset \notin \mathcal{C}$,

**(C1)** $C, C' \in \mathcal{C},\ C \subseteq C' \Rightarrow C = C'$,

**(C2)** $C, C' \in \mathcal{C},\ C \neq C',\ e \in C \cap C' \Rightarrow \exists C^\circ \in \mathcal{C},\ C^\circ \subseteq C \cup C' \setminus \{e\}$.

*Proof of* (C2). Because of the minimality of $C$ and $C'$, we have $\rho(C) = |C| - 1$ and $\rho(C') = |C'| - 1$. Since $C \neq C'$, the set $C \cap C'$ is independent, which implies $\rho(C \cap C') = |C \cap C'|$. Then, it follows that

$$\begin{aligned} \rho(C \cup C') &\leq \rho(C) + \rho(C') - \rho(C \cap C') && (\because \text{(R3)}) \\ &= |C| + |C'| - 2 - |C \cap C'| \\ &= |C \cup C'| - 2 && (\because |C| + |C'| = |C \cup C'| + |C \cap C'|). \end{aligned}$$

Therefore, for $e \in C \cap C'$, we have

$$\rho(C \cup C' \setminus \{e\}) \leq \rho(C \cup C') \leq |C \cup C'| - 2 = |C \cup C' \setminus \{e\}| - 1.$$

This implies that $C \cup C' \setminus \{e\}$ is a dependent set. Hence, there exists a circuit $C^\circ \subseteq C \cup C' \setminus \{e\}$. □

A matroid can also be defined with (C0)–(C2).

We define the *closure function* $\mathrm{cl} : 2^E \to 2^E$ by

$$\mathrm{cl}(X) = \{j \mid \rho(X \cup \{j\}) = \rho(X)\}.$$

We can easily see that $\mathrm{cl}\,(X) \supseteq X$ for $X \subseteq E$, and that $\mathrm{cl}\,(B) = E$ for $B \in \mathcal{B}$.

**Proposition 2.** *For any $I \in \mathcal{I}$ and any $j \in \mathrm{cl}(I) \setminus I$, $I \cup \{j\}$ contains a unique circuit.*

*Proof.* Since $j \in \mathrm{cl}(I) \setminus I$, $I \cup \{j\}$ is a dependent set and contains circuits. Let $C$ and $C'$ be circuits in $I \cup \{j\}$. Note that $j \in C \cap C'$. Suppose $C \neq C'$. Then, by (C2), there exists a circuit $C^\circ \subseteq C \cup C' \setminus \{j\} \subseteq I \in \mathcal{I}$, which contradicts (I1). □

Proposition 2 implies that an independent set $I$ and an element $j \in \mathrm{cl}(I)$ determine a circuit, which is called the *fundamental circuit* of $I$ and $j$, and denoted by $C(I|j)$.

## 2 Examples of Matroids

**Binary matroid:** A matroid representable by a matrix over the finite field $\mathbf{GF}(2)$ is called a *binary matroid.*

**Graphic matroid:** Let $G = (V, E)$ be an undirected graph. We call $F \subseteq E$ a *forest* if $F$ does not contain any circuits. The family $\mathcal{I}$ of the collection of the forests satisfies (I0)–(I2), and hence the pair $(E, \mathcal{I})$ forms a matroid, called a *graphic matroid.* In a graphic matroid, a base, a circuit, and the rank $\rho(E)$ can be interpreted into the terms of graph theory as follows:

base ↔ spanning forest,
circuit ↔ elementary circuit, in which no vertex is traversed more than once,
$\rho(E)$ ↔ (the number of vertices)−(the number of components).

The matroid $(E, \mathcal{I})$ is a binary matroid represented by the incidence matrix of $G$.

**Transversal matroid:** For a bipartite graph $G = (U, V; E)$ with the vertex sets $U, V$ and the edge set $E$, we define $\mathcal{I} = \{U \cap \partial M \mid M \subseteq E : \text{a matching}\}$. Then, $(U, \mathcal{I})$ forms a matroid, called a *transversal matroid.*

**Uniform matroid:** Let us denote $|U|$ by $n$. For an integer $k \leq n$, we define $\mathcal{I} = \{J \mid J \subseteq U,\ |J| \leq k\}$. Then, $(U, \mathcal{I})$ forms a matroid, called a *uniform matroid* $U_{n,k}$. This is a transversal matroid for a complete bipartite graph $K_{n,k}$. It is known that $U_{4,2}$ is not a binary matroid.