18.438 Advanced Combinatorial Optimization	October 15, 2009
Lecture 9	
Lecturer: Michel X. Goemans	*Scribe: Shashi Mittal**

(*This scribe borrows material from scribe notes by Nicole Immorlica in the previous offering of this course.)

1 Circuits

Definition 1 *Let $\mathcal{M} = (S, \mathcal{I})$ be a matroid. Then the circuits of $\mathcal{M}$, denoted by $C(\mathcal{M})$, is the set of all minimally dependent sets of the matroid.*

Examples:

1. For a graphic matroid, the circuits are all the simple cycles of the graph.
2. Consider a uniform matroid, U_n^k $(k \leq n)$, then the circuits are all subsets of S with size exactly $k+1$.

Proposition 1 *The set of circuits $C(\mathcal{M})$ of a matroid $\mathcal{M} = (S, \mathcal{I})$ satisfies the following properties:*

1. *$X, Y \in C(\mathcal{M})$, $X \subseteq Y \Rightarrow X = Y$.*
2. *$X, Y \in C(\mathcal{M})$, $e \in X \cap Y$ and $X \neq Y \Rightarrow$ there exists $C \in C(\mathcal{M})$ such that $C \subseteq X \cup Y \setminus \{e\}$.*

(Note that for circuits we implicitly assume that $\emptyset \notin C(\mathcal{M})$, just as we assume that for matroids $\emptyset \in \mathcal{I}$.)

Proof: 1. follows from the definition that a circuit is a minimally dependent set, and therefore a circuit cannot contain another circuit.

2. Let $X, Y \in C(\mathcal{M})$ where $X \neq Y$, and $e \in X \cap Y$. From 1, it follows that $X \setminus Y$ is non-empty; let $f \in X \setminus Y$. Assume on the contrary that $(X \cup Y) - e$ is independent. Since X is a circuit, therefore $X - f \in \mathcal{I}$. Extend $X - f$ to a maximal independent set in $X \cup Y$, call it Z. Then $Z \subseteq X \cup Y$, and Z does not contain Y (otherwise Y would be an independent set as well). Therefore $|Z| < |(X \cup Y) - e|$, which is a contradiction to the maximality of Z. □

One can give an alternative definition of matroids in terms of circuits as follows; this is given without proof.

Proposition 2 *Let $C(\mathcal{M})$ be the set of circuits corresponding to a ground set S. Then the set $(S, \mathcal{I})$ where $\mathcal{I} = \{I \subseteq S : \forall C \in C(\mathcal{M}) \quad C \subsetneq I\}$ is a matroid, and C is the set of circuits of this matroid.*

The bases of a matroid satisfy the following property.

Proposition 3 *Let B be a basis of a matroid $\mathcal{M} = (S, \mathcal{I})$, and $e \notin B$. Then $B + e$ contains a unique circuit. Moreover, one can remove any element from this circuit to get another basis of $\mathcal{M}$.*

Proof: Suppose $B + e$ contains to distinct circuits, C_1 and C_2. Clearly, $e \in C_1 \cap C_2$. Therefore by Proposition 1, $(C_1 \cup C_2) - e$ contains a circuit C, and hence B contains a circuit, which contradicts the definition of a basis. □

2 Operations on a Matroid

Given a matroid $\mathcal{M} = (S, \mathcal{I})$, we define two operations on a matroid: deletion and contraction.

Definition 2 *Let $Z \subseteq S$, then the matroid obtained by* deleting Z*, denoted by $\mathcal{M} \setminus Z$, is $\mathcal{M}' = (S \setminus Z, \mathcal{I}')$, where*

$$\mathcal{I}' = \{I \subseteq S \setminus Z : I \in \mathcal{I}\}.$$

Definition 3 *Let $Z \subseteq S$, then the matroid obtained by* contracting Z*, denoted by $\mathcal{M}/Z$, is given by*

$$\mathcal{M}/Z = (\mathcal{M}^* \setminus Z)^*,$$

where $\mathcal{M}^*$, as usual, denotes the dual of the matroid $\mathcal{M}$.

From the definitions, it is clear that both $\mathcal{M} \setminus Z$ and $\mathcal{M}/Z$ are matroids. To get more intuition about the contraction operation, we compute the rank function for the matroid $\mathcal{M}/Z$. Recall that for the dual matroid $\mathcal{M}^*$, the rank function is given by $r_{\mathcal{M}^*}(U) = |U| - r_{\mathcal{M}}(S) + r_{\mathcal{M}}(S \setminus U)$. Using this, we get

$$\begin{aligned} r_{\mathcal{M}/Z}(U) &= |U| - r_{\mathcal{M}^*\setminus Z}(S \setminus Z) + r_{\mathcal{M}^*\setminus Z}((S \setminus Z) \setminus U) \\ &= |U| - r_{\mathcal{M}^*}(S \setminus Z) + r_{\mathcal{M}^*}(S \setminus Z) \\ &= |U| - (|S \setminus Z| - r_{\mathcal{M}}(S) + r_{\mathcal{M}}(Z)) + (|(S \setminus Z) \setminus U| - r_{\mathcal{M}}(S) + r(Z \cup U)) \\ &= r_{\mathcal{M}}(Z \cup U) - r_{\mathcal{M}}(Z). \end{aligned}$$

This gives us the following interpretation for $\mathcal{M}/Z$. Fix any maximal independent subset B of Z, clearly $|B| = r_{\mathcal{M}}(Z)$. Then $U \in \mathcal{I}(\mathcal{M}/Z)$, if and only if $B \cup U \in \mathcal{I}(\mathcal{M})$.

3 Some Results on Representation of a Matroid

We first give the definition of a minor of matroid.

Definition 4 *Given a matroid $\mathcal{M} = (S, \mathcal{I})$, the matroid given by $(\mathcal{M} \setminus Z)/Y$, for some $Z \subseteq S$ and $Y \subseteq S \setminus Z$, is called a* minor *of the matroid $\mathcal{M}$.*

Recall that in the previous lecture, we had shown that if $\mathcal{M}$ is representable over a field F, then its dual is also representable over the same field F. This implies that any minor of $\mathcal{M}$ is also representable over the field F.

The question we pose is: What are the conditions we need on a matroid $\mathcal{M}$, so that it is representable over a finite field F? We present some results here which give characterization of matroids representable over finite fields in terms of the minors of the matroids.

The following is a well known result due to Tutte, on the representability of a matroid over $GF(2)$.

Theorem 4 (Tutte(1958) [6]) *$\mathcal{M}$ is a binary matroid iff $\mathcal{M}$ has no U_4^2 minor.*

One direction is clear; a binary matroid cannot contain U_4^2 as a minor since we argued last time that U_4^2 is not binary. The proof of the converse given here is based on the proof in Schrijver's book [4]. We first prove a lemma in the preparation of the proof of Tutte's theorem.

Lemma 5 *Let $\mathcal{M}$ and $\mathcal{N}$ be distinct matroids defined on the same ground set S. Let B be a common basis of $\mathcal{M}$ and $\mathcal{N}$, such that there is there is no set X with the following two properties:*

P1. *X is a basis of exactly one of $\mathcal{M}$ and $\mathcal{N}$.*

P2. $|B\Delta X| = 2$.

Then $\mathcal{M}$ or $\mathcal{N}$ has a U_4^2 minor.

Proof: Suppose $\mathcal{M}$, $\mathcal{N}$ are counterexamples to the above statement. Let B be a common basis of $\mathcal{M}$ and $\mathcal{N}$, and let X be a set satisfying property P1 only. Without loss of generality, we assume:

A1. $|B\Delta X|$ is minimum, and

A2. X is a base of $\mathcal{M}$ but not of $\mathcal{N}$.

Further, we have $|B\Delta X| > 2$ (so in fact $|B\Delta X| \geq 4$). If we take a smallest (in terms of the size of the common ground set), the above assumptions imply that

B1. $B \cup X = S$ (otherwise delete $S \setminus (B \cup X)$ from S.)

B2. $B \cap X = \emptyset$ (otherwise contract $B \cap X$ in S.)

B3. X is the only subset of S satisfying property $P1$. (This is implied by B1 and B2.)

Further, $\mathcal{M}$ has a base B' with $|B\Delta B'| = 2$. B' can be obtained from B as follows: Let $x \in X$, then $B + x$ has a unique circuit (Proposition 3), and $B + x - e$ is a basis for some $e \in B$. By uniqueness of X (from B3), B' must be a basis of $\mathcal{N}$ as well. Since we are assuming that $|B\Delta X|$ is minimum, therefore B' does not have the property that there is no set X' satisfying both the properties $P1$ and $P2$. By uniqueness of X (from B3), therefore, $|B'\Delta X| = 2$. Hence we have $|S| = 4$, with $|B| = |X| = 2$ and B, X disjoint.

Let $S = \{a, b, c, d\}$, with $B = \{a, b\}$ and $X = \{c, d\}$. Since we are assuming $\mathcal{M}$ is not U_4^2, it implies that there is subset of size 2, say $\{a, c\}$ that is not a basis of $\mathcal{M}$. We have:

- $\{a\}, \{c, d\}$ independent in $\mathcal{M} \Rightarrow \{a, d\}$ is a basis of $\mathcal{M}$.
- $\{c\}, \{a, b\}$ independent in $\mathcal{M} \Rightarrow \{b, c\}$ is a basis of $\mathcal{M}$.

Both of these follow from the exchange property of the matroids. By assumption on B, $\{a, d\}$ and $\{b, c\}$ must also be basis of of $\mathcal{N}$ (otherwise, with X' equal to, say, $\{a, d\}$, we will be able to satisfy both P1 and P2 in the statement of the Lemma). Hence $\{c\}$ is independent in $\mathcal{N}$. Therefore $\{c\}$ independent in $\mathcal{N}$, $\{a, d\}$ independent in $\mathcal{N}$ implies that either $\{c, a\}$ is independent in $\mathcal{N}$ (otherwise $\{c, a\}$ would satisfy property P2, contradicting B3) or $\{c, d\} (= X)$ is independent in $\mathcal{N}$ (contradicting A2). □

We now complete the proof of Tutte's theorem.

Proof of Theorem 4: The necessity of this theorem is easy to see, as every minor of a binary matroid is also binary, and U_4^2 is not a binary matroid, as shown in the previous lecture.

We now prove the sufficiency part. Let $\mathcal{M}$ be a non-binary matroid on a ground set S. Choose a basis B of $\mathcal{M}$, and let $\{x_b | b \in B\}$ be a collection of linearly independent vectors over $GF(2)$. For each $s \in S \setminus B$, let C_s be the unique circuit (see Proposition 3) contained in $B + s$. We define x_s as

$$x_s = \sum_{b \in C_s - s} x_b.$$

Now consider the binary matroid $\mathcal{N}$ given by $\{x_s | s \in S\}$. Clearly, B is a base of $\mathcal{N}$ as well. We have the following result: for each $b \in B$ and each $s \in S \setminus B$, $B - b + s$ is a base of $\mathcal{M}$ if and only if it is a base of $\mathcal{N}$. This is because if $B - b + s$ contains a circuit of $\mathcal{M}$, then x_s must be linearly dependent with the corresponding vectors of $B - b$, and hence $B - b + s$ will be dependent in $\mathcal{N}$ as well. Similarly the other way round.

This implies that there is no set X which is a basis of only one of $\mathcal{M}$ and $\mathcal{N}$, and for which $|B\Delta X| = 2$. Since $\mathcal{N}$ is a binary matroid, so $\mathcal{M} \neq \mathcal{N}$, and $\mathcal{N}$ has no U_4^2 minor. Therefore, from Lemma 5 , $\mathcal{M}$ must contain a U_4^2 minor. □

A few other results related to representation over $GF(3)$ and $GF(4)$ are given below.

Theorem 6 (Reid 1971) *$\mathcal{M}$ is ternary (i.e. representable over $GF(3)$) iff $\mathcal{M}$ has no F_7, F_7^*, U_5^2 and U_5^3 minors.*

Here, F_7 is the Fano matroid of rank 3 on a set S of size 7, with the dependency structure shown in Figure 1. It can be verified that both F_7, its dual, U_5^2 and U_5^3 are not ternary matroids. (Since duality preserves representability over a field, any list of excluded minors for non-representability should be closed under duality.)

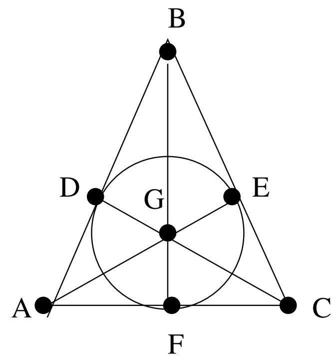

Figure 1: Fano matroid. The ground set of the matroid is the set of vertices of this diagram. All sets of cardinality 3 are independent, except those corresponding to a line in the diagram.

The diagram for the Fano matroid should be interpreted in the following way. All sets of size three corresponding to lines in the diagram (e.g., $\{A, B, D\}$, $\{D, E, F\}$, etc.) are dependent while every other triplet is an independent set in the matroid. Interestingly, the Fano matroid is representable over $GF(2)$, but not over any other field. Over $GF(2)$, the 7 vectors corersponding to the elements of the matroid are all non-zero binary vectors of dimension 3. The Fano matroid is a special case of matroids arising from projective planes, see for example [3].

A similar result for representability of matroids over $GF(4)$ was obtained by Geelen, Gerards and Kapoor (2000) [2], who proved that there is a finite list (7) of matroids to exclude in the minor of a matroid, so that it is representable over $GF(4)$. In 1971, after characterizations of $GF(2)$- and $GF(3)$-representable matroids, Gian-Carlo Rota conjectured that the matroids representable over any finite field can be characterized by a finite list of excluded minors. (The corresponding statement for minor-closed properties of graphs (such as say planarity) is the celebrated and deep result of Robertson and Seymour.) The case of matroids is still open.

Finally, an example of a matroid that is not representable over any field, is the non-Pappus matroid with the following dependency structure.

The non-representability of this matroid follows from a theorem due to Pappus for projective planes, which states that the points d, e, f in the above figure are collinear. Hence no matter under which field the matroid is represented, if the above dependency structure exists, then $\{d, e, f\}$ is a dependent set in that representation. See Oxley [3] for details and proofs..

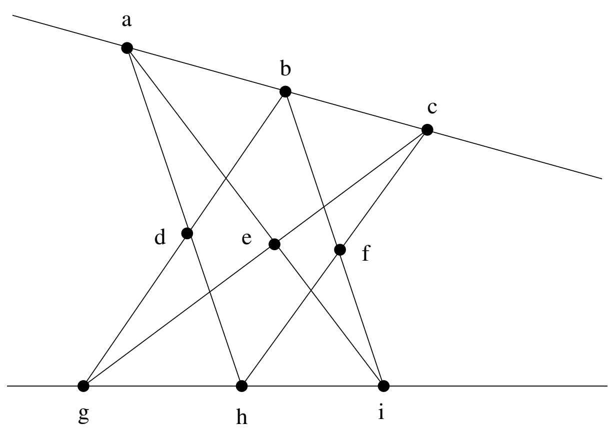

Figure 2: Non-Pappus matroid. All sets of cardinality 3 are independent, except those corresponding to lines in the diagram.

References

[1] R. Bixby. On Reid's characterization of ternary matroids. *J. Combin. Theory Ser. B*, 26:174–204, 1979.

[2] J. F. Geelen, A. M. H. Gerards, and A. Kapoor. The excluded minors for GF(4)-representable matroids. *Journal of Combinatorial Theory Series B*, 79, 2000.

[3] J.G. Oxley. *Matroid Theory.* Oxford University Press, 1992.

[4] A. Schrijver. *Combinatorial Optimization: Polyhedra and Efficiency*, volume B. Springer, 2003.

[5] P. Seymour. Matroid representation over GF(3). *J. Combin. Theory Ser. B*, 26:159–173, 1979.

[6] W. T. Tutte. A homotopy theorem for matroids, i, ii. *Trans. Amer. Math Soc.*, 88:144–174, 1958.

[7] H. Whitney. On the abstract properties of linear dependence. *Amer. J. Math.*, 57:509–533, 1935.