LIBERTAS MATHEMATICA, VOL. XIX (1999)

A NEW PROOF FOR THE TUTTE'S EXCLUDED CRITERION FOR A MATROID TO BE BINARY

GABRIELA ALEXE

Abstract. *In this note, we give a new proof for the Tutte's Excluded Criterion for a matroid to be binary, namely: A matroid is binary if and only if it contains no minor isomorphic to* $U_{2,4}$. *The original proof is due to Tutte. Other proofs are presented in [Oxl], [Tru] and [Welsh].*

In this note, all the definitions and notations for matroids are similar to those given in Welsh, [Welsh].

The aim of this paper is to give a new proof for the following basic Criterion due to Tutte, namely:

Tutte's Excluded Criterion for a matroid to be binary. *A matroid* M *is binary if and only if it has no minor isomorphic to* $U_{2,4}$.

As Welsh mentioned, the original proof of the Tutte's Excluded Criterion for a matroid to be binary appeared in W. T. Tutte: *Lectures on matroids.* J. Res. Nat. Bur. Stand. **69B** (1965), 1-48 and the proof presented in [Welsh], p. 167, appeared in M. J. Piff: *Some problems in combinatorial theory.* (D. Phil. thesis) Oxford (1972). Another proof appeared in J. G.. Oxley: *Matroid Theory.* Oxford University Press (1992), [Oxl]. In [Sey] it is presented a proof of Tutte's criterion, due essentially to K. Truemper. Also, it is mentioned that Tutte's criterion appeared in the paper: W. T. Tutte: *A homotopy theorem for matroids*, I, II, Trans. Amer. Math. Soc. **88**, 144-174, [Tutte].

1. THE NEW PROOF FOR THE TUTTE'S EXCLUDED CRITERION FOR A MATROID TO BE BINARY.

The main result used in the new proof of the Excluded Criterion is the next characterization theorem for binary matroids, [Welsh], p. 162:

Theorem 1 *The following statements about a matroid* M *are equivalent:*

(a) For any circuit C *and cocircuit* C^*, $|C \cap C^*|$ *is even;*

(b) The symmetric difference of any collection of distinct circuits of M *is the union of distinct circuits of* M;

(c) If C_1, C_2 are distinct circuits of M, the symmetric difference $C_1 \Delta C_2$ contains a circuit of M;

(d) For any base B and circuit C of M, if $C - B = \{e_1, .., e_q\}$, and if $C(e_i)$ is the fundamental circuit of e_i in the base B, then $C = C(e_1)\Delta ... \Delta C(e_q)$;

(e) M is binary.

We give now the proof for the *Tutte's Excluded Criterion:*

Proof. First, we will prove using induction on $|S|$, that any matroid on the finite set S which contains no minor isomorphic to $U_{2,4}$ is binary. Since it is known that $U_{2,4}$ is the smallest matroid which is not binary, we will consider only the case $|S| \geq 4$. Suppose that $|S| \geq 4$ and that the theorem is true for all matroids on sets having less elements than $|S|$. We will prove that M is binary.

The plan of the proof is the following:

1. We suppose on the contrary, that there are two different circuits C_1 and C_2 of M such that $C_1 \Delta C_2$ is an independent set of M and we prove that $C_1 \Delta C_2$ is a base of M.
2. We prove that $\max(|C_1 - C_2|, |C_2 - C_1|)$ and $|C_1 \cap C_2|$ are ≥ 2.
3. For an arbitrary element $x \in C_1 \cap C_2$, we find a cocircuit C^* of $M.(S - x)$ such that $|C^* \cap (C_1 - x)|$ and $|C^* \cap (C_2 - x)|$ are not both even, which, by theorem 1, is a contradiction with the fact that $M.(S - x)$ is a binary matroid.

Now, we present the proof in detail. It is sufficient to prove that the symmetric difference of any two different circuits C_1 and C_2 of M is a dependent set of M.

Suppose on the contrary that there are two different circuits of M, denoted by C_1 and C_2, such that $C_1 \Delta C_2$ is an independent set of M. Let $C_1 := \{a_1, .., a_k, x_1, .., x_p\}$ and $C_2 := \{b_1, .., b_l, x_1, .., x_p\}$, where k, l, p are natural numbers, $C_1 - C_2 = \{a_1, .., a_k\}$, $C_2 - C_1 = \{b_1, .., b_l\}$ and $C_1 \cap C_2 = \{x_1, .., x_p\}$. For simplicity, let $A := \{a_1, .., a_k\}$, $B := \{b_1, .., b_l\}$ and $X := \{x_1, .., x_p\}$.

It is obvious that $p \geq 1$ (otherwise $C_1 \Delta C_2 = C_1 \cup C_2$ would be a dependent set of M, contradicting the hypothesis) and also $k \geq 1$, $l \geq 1$ (otherwise, for $k = l = 0$, the circuits would be equal, contradiction, else, a circuit would properly contain another circuit, contradicting the first axiom of circuits).

We remark that if C' and C'' are two different circuits of M such that $C' \cup C'' \neq S$, then $M|(S - (C' \cup C''))$ is a binary matroid, and by theorem 1, $C' \Delta C''$ is a disjoint union of circuits of M. In particular, $C' \Delta C''$ is a dependent set of M.

We may suppose in the following that $C_1 \cup C_2 = S$.

Let i be an arbitrary index, $1 \leq i \leq p$. Consider the contraction $M.(S - x_i)$, which, by the induction hypothesis, is a binary matroid. Since $x_i \in C_1 \cap C_2$, both $C_1 - x_i$ and $C_2 - x_i$ are circuits of $M.(S - x_i)$. Consequently, using again theorem 1, $(C_1 - x_i)\Delta(C_2 - x_i)$ is a dependent set of $M.(S - x_i)$, i.e. $A \cup B$ is a dependent set of $M.(S - x_i)$. This means that $A \cup B \cup x_i$ is a dependent set of M (x_i is an independent set of M, being a proper subset of C_1 and also it is the unique maximal independent set of $S - (S - x_i)$). It follows that $A \cup B$ is a maximal independent set of M, i.e. it is a base of M.

Moreover, because $|C_1| - 1 \leq |A \cup B|$ and $|C_2| - 1 \leq |A \cup B|$, we obtain that $p - 1 \leq \min\{k, l\}$ and we may suppose that $p - 1 \leq l \leq k$.

If $p = 1$, then, according to the second circuits' axiom (C_2), $(C_1 \cup C_2) - x_1 = \{a_1, .., a_k, b_1, .., b_l\}$ contains a circuit of M, contradiction. Therefore, we may consider $p \geq 2$. If $k = 1$, then $l = 1$ and because $l \geq p - 1$, we deduce that $p = 2$. But in this case, any 2-subset of S is a base of M. This means that M is isomorphic to $U_{2,4}$, contradiction.

So, we may suppose that $k \geq 2$, $l \geq 1$ and $p \geq 2$. Let x_1, x_2 be two different elements of the set X. Because $\{x_1, x_2\}$ is an independent set of M and $A \cup B$ is a base of M, we deduce from the augmentation theorem that there are two different elements α, $\beta \in A \cup B$, such that $B_0 := \{x_1, x_2\} \cup ((A \cup B) - \{\alpha, \beta\})$ is a base of M. Since $k \geq 2$ and $l \geq 1$, $A \cup B - \{\alpha, \beta\}$ is non-empty. Let b be an arbitrary element from $A \cup B - \{\alpha, \beta\}$. Without any loss of generality, we may suppose that $b \in B$. By the induction hypothesis, the matroid $M.(S - b)$ is binary and this implies that its dual $(M.(S - b))^* = M^*|(S - b)$ is binary, too. Because $S - (A \cup B) = X$ is a base for the matroid M^* and $X \subseteq S - b$, X is also a base for the matroid $M^*|(S - b)$.

Let $C^*(\alpha)$ and $C^*(\beta)$ be the fundamental circuits of M^*, corresponding to the elements α and β, relative to the base X of M^*. Since $C^*(\alpha) \subseteq \alpha \cup X \subseteq S - b$ and $C^*(\beta) \subseteq \beta \cup X \subseteq S - b$, $C^*(\alpha)$ and $C^*(\beta)$ are also circuits of the binary matroid $M^*|(S - b)$. Theorem 1 assures that $C^*(\alpha) \triangle C^*(\beta)$ is a dependent set of $M^*|(S - b)$. This is equivalent to the fact that $C^*(\alpha) \triangle C^*(\beta)$ intersects all the bases of $(M^*|(S - b))^* = M.(S - b)$. Because b is the only maximal independent set of M contained in $S - (S - b)$ and $(B_0 - b) \cup b = B_0$ is a base of M, it follows that $B_0 - b$ is a base of $M.(S - b)$, too. Consequently, $(C^*(\alpha) \triangle C^*(\beta)) \cap (B_0 - b) \neq \emptyset$. Since $C^*(\alpha) \triangle C^*(\beta) \subseteq \{\alpha, \beta\} \cup X$ and $B_0 - b \subseteq ((A \cup B) - \{\alpha, \beta\}) \cup \{x_1, x_2\}$, we deduce that $(C^*(\alpha) \triangle C^*(\beta)) \cap \{x_1, x_2\} \neq \emptyset$. Without any loss of generality, we may suppose that $x_1 \in C^*(\beta) - C^*(\alpha)$. Consider now the matroid $M^*|(S - x_1)$. Clearly, $C^*(\alpha)$ is a circuit of M^* contained in $S - x_1$, so, it is also a circuit of $M^*|(S - x_1)$. Equivalently, $C^*(\alpha)$ is a cocircuit of $(M^*|(S - x_1))^* = M.(S - x_1)$. Since $x_1 \in C_1 \cap C_2$, we deduce that both $C_1 - x_1$ and $C_2 - x_1$ are circuits of the matroid $M.(S - x_1)$, which, by the induction hypothesis, is a binary matroid.

From theorem 1 it follows that both $|(C_1 - x_1) \cap C^*(\alpha)|$ and $|(C_2 - x_1) \cap C^*(\alpha)|$ are even. Since $|((C_1 - x_1) \cap C^*(\alpha)) \triangle ((C_2 - x_1) \cap C^*(\alpha))| = |\alpha| = 1$ is odd, we obtain a contradiction.

Therefore, the assumption that $C_1 \triangle C_2$ is an independent set of M is false and consequently, M is a binary matroid.

The converse implication of the Criterion is obvious, because any minor of a binary matroid is also binary and $U_{2,4}$ is not binary. ■

REFERENCES

[1] J. G.. Oxley: *Matroid Theory.* Oxford University Press (1992).

[2] P. D. Seymour: Ch. 10 *Matroid Minors,* in HANDBOOK OF COMBINATORICS, edited by R. Graham, M. Grötschel and L. Lovász, Elsevier Science (1995).

[3] K. Truemper: *Matroid Decomposition.* Academic Press (1992).

[4] W. T. Tutte: *Lectures on matroids.* J. Res. Nat. Bur. Stand. **69B** (1965), 1-48.

[5] D. J. A. Welsh: *Matroid Theory,* Academic Press, London (1976).