Chapter 7

Graphic matroids

Let us summarize some facts on graphic matroids, in particular, those stated in Propositions 1.16 and 1.17 and Corollary 2.15. Every graphic matroid is representable over any field. The same holds for duals of graphic matroids. If G is a graph and $\mathcal{M}(G)$ is the matroid associated to G, then $r_{\mathcal{M}}(X)$ is equal to the number of vertices of G decreased by the number of components of the spanning subgraph of G containing the edges of X.

Matroids associated to planar graphs can be characterized in the spirit of Kuratowski theorem.

Theorem 7.1. *The following statements are equivalent for a graph G:*

(i) The graph G is planar.

(ii) Both matroids $\mathcal{M}(G)$ and $\mathcal{M}^*(G)$ are graphic matroids.

(iii) The matroid $\mathcal{M}(G)$ has no minor isomorphic to $\mathcal{M}(K_5)$ or $\mathcal{M}(K_{3,3})$.

Proof. Since a graph is planar if and only if it does contain K_5 or $K_{3,3}$ as a minor, the equivalence of *(i)* and *(iii)* is just another formulation of Kuratowski's Theorem. By Theorem 2.22, *(i)* implies *(ii)*. On the other hand, if G is a non-planar graph, then G contains a minor isomorphic to either K_5 or $K_{3,3}$. Hence, $\mathcal{M}^*(G)$ contains $\mathcal{M}^*(K_5)$ or $\mathcal{M}^*(K_{3,3})$ as a minor and thus $\mathcal{M}^*(G)$ cannot be graphic by Proposition 2.24. □

7.1 Whitney's theorem

All graphic matroids associated with m-edge trees are isomorphic. Hence, matroids associated to non-isomorphic graphs can be isomorphic. Whitney [28] characterized which graphs have isomorphic graphic matroids. We present this result in this section. In this section, we consider only graphs without isolated vertices since the (non-)presence of isolated vertices in a graph does not change its associated matroid.

Let us introduce a graph operation that preserves the structure of the associated matroid. Let us consider the following three graph operations:

(i) *Vertex identification.* Let v_1 and v_2 be two vertices of distinct components of a graph G. The new graph is obtained from G by identifying v_1 and v_2 to a single vertex. into a new vertex v.

(ii) *Vertex cleaving.* This is the reverse operation of vertex identification. The new graph is obtained by cleaving a cut-vertex of a graph.

(iii) *Twisting.* Suppose that a graph G can be obtained from two vertex-disjoint graphs G_1 and G_2 by identifying vertices u_1 of G_1 and u_2 of G_2 into a vertex u of G, and identifying vertices v_1 of G_1 and v_2 of G_2 into a vertex v of G. The graph obtained from G_1 and G_2 by identifying u_1 with v_2 and v_1 with u_2 is a *twist* of G. The graphs G_1 and G_2 are called *pieces* and the vertices u and v are called *twisting vertices.*

Two graphs are said to be 2-*isomorphic* if they can be transformed to each other by a sequence of vertex identifications, vertex cleavings and twistings. An example of 2-isomorphic graphs can be found in Figures 7.1 and 7.2. The relation of being 2-isomorphic is an equivalence relation on graphs.

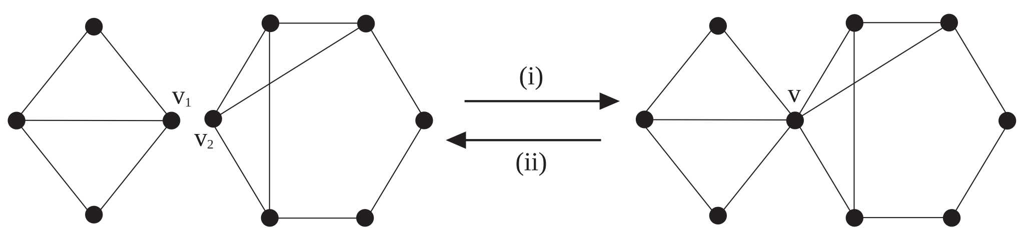

Figure 7.1: An example of vertex identification and vertex cleaving.

Since neither vertex identifications, vertex cleavings nor twistings change the structure of cycles in a graph, the matroids associated to two 2-isomorphic graphs are the same. The rest of the section is devoted to the proof of the converse implication.

Let us start with 3-connected graphs. Clearly, each 3-connected graph is the only element of its equivalence class under 2-isomorphism.

Lemma 7.2. *Let G and H be loopless graphs without isolated vertices and let G be 3-connected. If $\varphi : E(G) \to E(H)$ is an isomorphism from $\mathcal{M}(G)$ to $\mathcal{M}(H)$, then the mapping φ induces an isomorphism between the graphs G and H.*

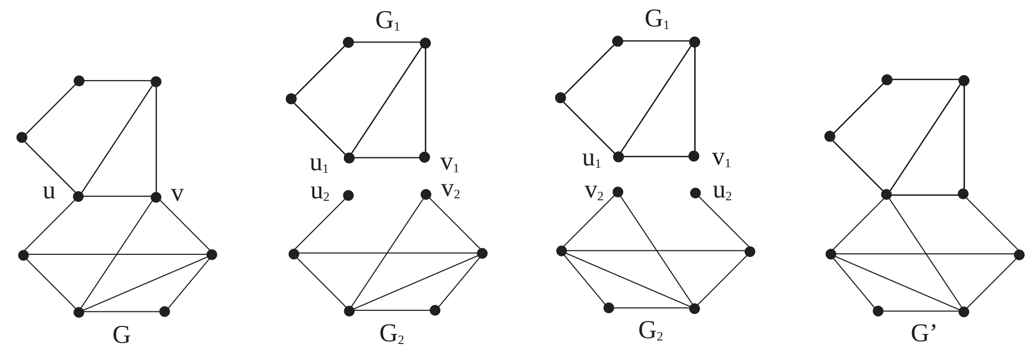

Figure 7.2: An example of twisting.

Proof. A *vertex bond* is the set of all edges incident with a single vertex. The complement of every vertex bond of G is connected in $\mathcal{M}(G)$ (since G stays 2-connected after removing any vertex) and it is a hyperplane of $\mathcal{M}(G)$, i.e., an inclusion-wise maximal subset of rank $r(\mathcal{M}(G)) - 1$. Since every connected hyperplane in a graphic matroid must be a complement of a vertex bond (but, in general, there can be complements of vertex bonds that are not connected), no graphic matroid can contain more than $r(\mathcal{M}(G)) + 1$ connected hyperplanes. Hence, if a graphic matroid associated to a graph G' contains $r(\mathcal{M}(G')) + 1$ connected hyperplanes, they uniquely determine vertex bonds of G'. As the matroids $\mathcal{M}(G)$ and $\mathcal{M}(H)$ are isomorphic, $\mathcal{M}(H)$ contains $r(\mathcal{M}(G)) + 1 = r(\mathcal{M}(H)) + 1$ connected hyperplanes and they uniquely determine the vertex bonds of H. It follows that the graphs G and H are isomorphic and the mapping φ induces an isomorphism between them. $\square$

In the analysis of 2-connected graphs, we will have to employ Tutte's structural characterization of these graphs. A *generalized cycle* is a graph obtained from a cycle of length $k \geq 2$ by replacing some of its edges with 2-connected graphs H in the following way: an edge of the cycle is removed and its end-vertices are identified with two distinct vertices of H. The two vertices shared by H and the rest of the graph are called *contact vertices*.

We show that every 2-connected graph is a generalized cycle.

Lemma 7.3. *Let G be a 2-connected graph with at least four vertices. If G is not 3-connected graph, then G is a generalized cycle.*

Proof. Let $\{u, v\}$ be a vertex cut of G. Let H_1 be any component of $G \setminus \{u, v\}$ and let H_2 be the graph $G \setminus (\{u, v\} \cup V(H_1))$. For $i = 1, 2$, let G_i be the subgraph of G induced by $V(H_i) \cup \{u, v\}$. Finally, G_2' is the graph obtained from G_2 by deleting all edges joining u and v. If both G_1 and G_2' are 2-connected, then G is a generalized cycle obtained by identifying vertices of G_1 and G_2'. If G_1 is not 2-connected, it has a cut-vertex w. As G is 2-connected, the vertex w is neither u nor v. The vertex w splits G_1 into parts $G_{1,1}$ and $G_{1,2}$. If all $G_{1,1}$, $G_{1,2}$ and G_2' are 2-connected, then G is a generalized cycle obtained from $G_{1,1}$, $G_{1,2}$ and G_2'. If not, we split the one that is not into two parts delimited by its cut-vertex. We continue until we obtain a sequence of 2-connected graphs that form the generalized cycle isomorphic to G. $\square$

Using Lemma 7.3, we can make the first step towards the proof of Whitney's theorem.

Lemma 7.4. *Let G be a generalized cycle obtained by replacing edges of a cycle of length k with graphs $G_1, \ldots, G_k$ which are either multiple edges or 2-connected graphs. If the matroid $\mathcal{M}(G)$ is isomorphic to the matroid $\mathcal{M}(H)$ of a graph H, then H is a generalized cycle obtained from a cycle of length k by replacing its edges with graphs $H_1, \ldots, H_k$. Moreover, if φ is an isomorphism of $\mathcal{M}(G)$ and $\mathcal{M}(H)$, then $E(H_i) = \varphi(E(G_i))$ for a suitable permutation of indices.*

Proof. For $i \in \{1, 2, \ldots, k\}$, let H_i be the subgraph of H formed by the edges $\varphi(E(G_i))$ and the vertices incident with at least one of these edges. Further, let $G_{-i} = \bigcup_{j \neq i} G_j$ and $H_{-i} = \bigcup_{j \neq i} H_j$. Our aim is to show that the following holds for every $i = 1, \ldots, k$:

$$|V(H_i) \cap V(H_{-i})| = 2 \tag{7.1}$$

If G_i is a single or multiple edge, then H_i is, too. If G_i is 2-connected, then $\varphi(E(G_i))$ is connected (in the matroidal sense) and thus H_i is a 2-connected subgraph of H. Consider a cycle C of G passing through all the subgraphs $G_1, \ldots, G_k$. Let P be a maximal path of $\varphi(C)$ contained in H_{-i}, and let x and y be the first and the last vertex of P. Clearly, both x and y are contained in both H_i and H_{-i}. The proof of (7.1) will be completed by showing that

$$V(H_i) \cap V(H_{-i}) = \{x, y\} \tag{7.2}$$

Let u be one of the contact vertices of G_i. The set E_u of edges of G_i incident with u is an edge-cut of G_i and thus $H_i \setminus \varphi(E_u)$ has two components. Observe that every circuit of $\mathcal{M}(H)$ that contains both an edge H_i and an edge of H_{-i} must contain an edge of $\varphi(E_u)$: indeed, any cycle of G containing an edge of G_i and an edge G_{-i} must pass through both contact vertices of G_i and thus it contains an edge of E_u.

The vertices x and y are in different components of $H_i \setminus \varphi(E_u)$. If they were in the same components, the path between them and P would be a cycle of H avoiding all the edges of $\varphi(E_u)$ which is impossible since any circuit of $\mathcal{M}(H)$ containing an edge of H_i and an edge of H_{-i} must contain an edge of $\varphi(E_u)$. Let H_i^x be the component of $H_i \setminus \varphi(E_u)$ containing x and H_i^y the one containing y.

If (7.2) does not hold, there is a vertex $z \in (V(H_i) \cap V(H_{-i})) \setminus \{x, y\}$. By symmetry, we can assume that z is contained in H_i^x. Let g be an edge of H_{-i}

incident with z and h such an edge of H_i. Since H is 2-connected, it contains a cycle passing through both g and h. Walk along this cycle from z through an edge g as long as H_i or P is hit. Let w be the vertex that we hit and Q the path we have traversed.

We distinguish three cases based on the position of w: w is a vertex of P, w is a vertex of H_i^x not contained in P, or w is a vertex of H_i^y not contained in P. If w is contained in P, consider the following cycle of H: walk from z to w along Q, continue to x along P and to z along any path in H_i^x. However, this cycle of H corresponds to a circuit of $\mathcal{M}(H)$ containing both an edge of H_i and an edge of H_{-i} avoiding all edges of $\varphi(E_u)$ which is impossible. Hence, w is not contained in the path P.

If w is a vertex of H_i^x, consider the following cycle of H: walk from z to w along Q and then continue from w to z along any path in H_i^x. Again, the obtain cycle corresponds to a circuit of $\mathcal{M}(H)$ containing both an edge of H_i and an edge of H_{-i} avoiding all edges of $\varphi(E_u)$.

Finally, if w is a vertex of H_i^y, consider the following cycle of H: walk from z to w along Q, continue from w to y along any path in H_i^y, then from y to x along P and close the close following any path from x to w in H_i^x. Again, the corresponding circuit of $\mathcal{M}(H)$ contains both an edge of H_i and an edge of H_{-i} and avoids all edges of $\varphi(E_u)$.

We have now proven the equation (7.1). Since H is 2-connected, it must be a generalized cycle with parts $H_1, H_2, \ldots, H_k$ (start in H_1 and continue along contact vertices through other parts until H_1 is again reached). $\square$

We are now ready to prove that 2-connected graphs with the same associated matroids can be transformed by a sequence of twistings.

Lemma 7.5. *Let G be a 2-connected graph with $n \geq 2$ vertices. If the matroid $\mathcal{M}(H)$ of a graph H is isomorphic to $\mathcal{M}(G)$, then the graph H can be transformed by at most $n-2$ twistings to a graph H^* isomorphic to G.*

Proof. We prove a slightly stronger statement where we allow a single edge to be directed and require the considered isomorphism between $\mathcal{M}(G)$ and $\mathcal{M}(H)$ to map the directed edge of G to the directed edge of H. Note that the direction of this edge can always be "fixed" by twisting its end-vertices when a particular isomorphism of G and H is considered.

The proof proceeds by induction on n. If $n = 2$, the graphs G and H must be isomorphic (they are either single edges or parallel edges of the same multiplicity). Let $n \geq 3$. If G is 3-connected, then G and H are isomorphic as undirected graphs by Lemma 7.2 and using at most one twisting on a directed edge, they become isomorphic with the directed edges.

Hence, both G and H are generalized cycles by Lemma 7.3. Let $G_1, \ldots, G_k$ be the subgraphs forming the generalized cycle and let $H_1, \ldots, H_k$ be the subgraphs forming the generalized cycle of H in such an order that $E(H_i) = \varphi(E(G_i))$ which exists by Lemma 7.4. Finally, let n_i be the number of vertices of G_i (and thus of H_i).

By symmetry, we can assume that G_1 (and thus H_1) contains the directed edge and the parts $G_1, \ldots, G_k$ follow the original cycle of G in this order. We first apply $k-2$ twistings to rearrange H_i to follow the original cycle of H in the order $H_1, \ldots, H_k$.

Let G_1' be the graph obtained from G_1 by adding an edge between its contact vertices and H_1' the graph obtained from H_1 by adding an edge between its contact vertices. By induction, there exists a sequence of at most $n_1 - 2$ twistings transforming H_1 to H_1^* isomorphic to G_1 while the rest of H is unchanged. Let v_g be the contact vertex shared by G_1 and G_2 and w_g the other contact vertex of G_2. Let v_h be the image of v_g under the isomorphism of G_1 and H_1^*. Using at most one twisting which can be included among the $k-2$ twisting needed to rearrange the parts into the right order, v_h becomes a contact vertex of H_2. Let w_h be the other contact vertex of H_2. Consider graphs G_2' and H_2' obtained from G_2 and H_2 by adding directed edges $v_g w_g$ and $v_h w_h$, respectively. By induction, the graphs H_2' can be transformed to a graph isomorphic to G_2' using at most $n_2 - 2$ twistings. Note that the reversal of the added directed edge corresponds to a twisting around the contact vertices of H_2 in H.

Proceed analogously with $G_3, \ldots, G_k$ and $H_3, \ldots, H_k$. In this way, we have transformed H to a graph H^* isomorphic to G using at most $k-2$ initial twistings to reorder the parts and $n_i - 2$ twistings for each of the parts. Altogether, the number of twistings does not exceed

$$\sum_{i=1}^{k}(n_i - 2) + (k-2) = \sum_{i=1}^{k}(n_i - 1) - 2 = n - 2 .$$

The proof of the lemma is now finished. □

We can now characterize 2-connected graphs with isomorphic graphic matroids.

Theorem 7.6. *Let G be a loopless 2-connected graph with n vertices. If the matroid $\mathcal{M}(H)$ of a graph H is isomorphic to $\mathcal{M}(G)$, then H can be transformed into a graph that is isomorphic to G by a sequence of at most $n-2$ twistings. Moreover, for every $d \geq 1$, there exist 2-connected graphs G and H with $3d+2$ vertices such that their associated matroids are isomorphic such that at least $3d$ twistings are needed to transform H into a graph isomorphic to the graph G*

Proof. The first part of the theorem follows directly from Lemma 7.5. To show that the bound is the best possible, we proceed as follows: for $d = 1$, consider two cycles of length five with edges labeled with $1, 2, 3, 4, 5$ and $1, 3, 5, 2, 4$. Replace each edge with the number of parallel edges equal to its label. A straightforward case analysis yields that at least 3 twistings are necessary to transform one of the graphs to one isomorphic to the other one. For $d > 1$, consider several such cycles of length five, each having one edge labeled with 1 and remaining edges with mutually distinct numbers and identify the edges labeled with 1. □

We can now characterize all graphs with isomorphic graphic matroids. Recall that a *block* of a graph G is an inclusion-wise maximal 2-connected subgraph of G.

Theorem 7.7. (Whitney's 2-Isomorphism Theorem) *Let G and H be two graphs without isolated vertices. The matroids $\mathcal{M}(G)$ and $\mathcal{M}(H)$ are isomorphic if and only if the graphs G and H are 2-isomorphic.*

Proof. First, cleave all cut vertices of G to obtain a graph G^+ and cleave all cut vertices of H to obtain H^+. In other words, the components of G^+ are blocks of G and the components of H^+ are blocks of H. Clearly, the graphs G and G^+ are 2-isomorphic as well as the graphs H and H^+ are 2-isomorphic. Since blocks of a graph one-to-one correspond to components of its graphic matroid, the matroids $\mathcal{M}(G^+)$ and $\mathcal{M}(H^+)$ and such an isomorphism naturally gives a one-to-one correspondence between components of G^+ and components of H^+. Components of G^+ can be transformed to components of H^+ by a sequence of twistings by Theorem 7.6. This implies that the graphs G^+ and H^+ are 2-isomorphic which combines with the facts that G and G^+ as well as H and H^+ are 2-isomorphic to the fact that G and H are 2-isomorphic. □

7.2 Recognizing graphic matroids

In this section, we discuss the complexity of testing whether a matroid is graphic. The input matroid will be given by its independence oracle which we introduced in Chapter 3.

The algorithm that we present will be divided into several steps. First, we show that if a matroid $\mathcal{M}$ is graphic, then we can construct a graph G such that the associated matroid $\mathcal{M}(G)$ is isomorphic to $\mathcal{M}$ in polynomial time.

Proposition 7.8. *There exists a polynomial-time algorithm that decides whether an oracle-given binary matroid $\mathcal{M}$ is graphic and if so, it constructs a graph G such that the associated matroid $\mathcal{M}(G)$ is isomorphic to the input matroid $\mathcal{M}$.*

Proof. We first find a base B of $\mathcal{M}$ and fix it. With the base B fixed, we construct its partial representation $[I_r|D]$ with respect to B which can easily be done by identifying fundamental circuits. Since $\mathcal{M}$ is binary, the matrix $[I_r|D]$ is a representation of $\mathcal{M}$ over the field GF(2). Using the matrix $[I_r|D]$, it is easy to decompose the matroid $\mathcal{M}$ into its connectivity components and solve the problem separately for each of these components. Hence, we can assume in the rest that the matroid $\mathcal{M}$ is connected.

Let n be the number of columns of D and let D_k, $1 \leq k \leq n$, be the matrix obtained from D from its first k columns by deleting all the rows that are zero and let $\mathcal{M}_k$ be the binary matroid represented by $[I_m|D_k]$ where m is the number of rows of D_k. Since $\mathcal{M}$ is connected, it is possible to rearrange columns of $\mathcal{M}$ in such a way that all the matroids $\mathcal{M}_1, \ldots, \mathcal{M}_n$ are connected. In other words, if E_k, $1 \leq k \leq n$, is the union of fundamental circuits with respect to B for the elements corresponding to the first k columns, then $\mathcal{M}_k = \mathcal{M}|E_k$.

We will now construct graphs $G_1, \ldots, G_n$ such that the matroid $\mathcal{M}(G_k)$, $1 \leq k \leq n$, is isomorphic to $\mathcal{M}_k$ or decide that no such graph G_k exists. The graph G_1 is easy to construct as it is a cycle comprised of the edges corresponding to the elements of $\mathcal{M}_1$. Since the graph G_1, in general, all graphs G_k, is not unique, we will employ an almost-linear time data structure for representing all graphs 2-isomorphic to a 2-connected graph [2]. Assume that G_{k-1} has already been constructed and test using our data structure whether G_{k-1} contains a path comprised by the elements contained both in E_{k-1} and in the fundamental circuit with respect for the element corresponding to the k-th column of D. If so, we will transform G_{k-1} to a 2-isomorphic graph containing such a path and update the data structure by adding the edges of $E_k \setminus E_{k-1}$. If not, the matroid $\mathcal{M}_k$ is not graphic. The latter implies that the matroid $\mathcal{M}$ is also not graphic. If we obtain in this way a graph G_n, then the matroid associated with G_n is isomorphic to $\mathcal{M}$. □

We now turn our attention to the case of general matroids. We state that it can be tested in polynomial time whether a given matroid is isomorphic to a given graphic matroid. Recall that a *vertex bond* is the set of all edges incident with a single vertex of a graph.

Theorem 7.9. *Let G be a graph and $\mathcal{M}$ a matroid with the ground set $E(G)$. The matroids $\mathcal{M}$ and $\mathcal{M}(G)$ are isomorphic if and only if*

(i) $r(\mathcal{M}) \leq r(\mathcal{M}(G))$ *and*

(ii) every vertex bond of G is a union of cocircuits of $\mathcal{M}$.

Proof. It is easy to see that if the matroids $\mathcal{M}$ and $\mathcal{M}(G)$ are isomorphic, then both (i) and (ii) hold. So, we have to show that the conditions (i) and (ii) are also sufficient to guarantee that $\mathcal{M}$ and $\mathcal{M}(G)$ are isomorphic. We proceed by induction on the number of edges of G. Without loss of generality, we can assume that G is connected. Suppose that (i) and (ii) hold, but $\mathcal{M}$ and $\mathcal{M}(G)$ are not isomorphic. In particular, there exists a set X of elements of $\mathcal{M}$ that is dependent in one of the matroids $\mathcal{M}$ and $\mathcal{M}(G)$ and independent in the other. Such an inclusion-wise minimal set X is a circuit in one of the matroids (and independent in the other).

Fix an edge e of G. For every vertex v of G, the bond of v in $G \setminus \{e\}$ is a union of cocircuits of $\mathcal{M} \setminus \{e\}$ (this directly follows from the definition of a cocircuit as an inclusion-wise minimal set meeting every base of a matroid). If $e \notin X$, then X is dependent in one of the matroids $\mathcal{M} \setminus \{e\}$ and $\mathcal{M}(G \setminus \{e\})$ and independent in the other. By induction, the condition (i) must fail for this pair of matroids, i.e., $r(\mathcal{M} \setminus \{e\}) > r(\mathcal{M}(G \setminus \{e\}))$. Since the choice of $e \notin X$ is arbitrary, we conclude that every edge not contained in X is a bridge of G but not a coloop of $\mathcal{M}$.

Observe that the minimum degree of G is at least two: if G contained a vertex v of degree one, then the single edge e incident with v is a bridge of G and, by (ii), it must be a coloop of $\mathcal{M}$ since $\{e\}$ is cocircuit of $\mathcal{M}$. By the choice of X, e is not contained in X but we have seen that none of the elements not contained in X is a coloop. We have shown that the minimum degree of G is at least two. In particular, X is not independent in $\mathcal{M}(G)$ (otherwise, G would be tree as all the edges not contained in X are bridges in G). Hence, X corresponds to a cycle of the graph G and X is its unique cycle (this follows from the choice of X and the fact that all the edges of G not contained in X are bridges). Since the minimum degree of G is at least two, there are no edges not contained in X and thus G is a cycle. Consequently, $r(\mathcal{M}(G)) = |X| - 1$ and $r(\mathcal{M}) = |X|$ which violates (i). ☐

For 2-connected graphs, Theorem 7.9 implies the following.

Corollary 7.10. *Let G be a 2-connected graph and $\mathcal{M}$ a matroid with the ground set $E(G)$. The matroids $\mathcal{M}$ and $\mathcal{M}(G)$ are isomorphic if and only if $r(\mathcal{M}) = r(\mathcal{M}(G))$ and every vertex bond of G is a cocircuit of $\mathcal{M}$.*

The main algorithmic result of this section follows.

Theorem 7.11. *There exists a polynomial-time algorithm that decides whether an oracle-given matroid $\mathcal{M}$ is graphic and if so, it constructs a graph G such that the associated matroid $\mathcal{M}(G)$ is isomorphic to the input matroid $\mathcal{M}$.*

Proof. We first construct a partial representation $[I_r|D]$ of $\mathcal{M}$ where r is the rank of $\mathcal{M}$. This allows us to split $\mathcal{M}$ into connectivity components and we then proceed separately for the restrictions of $\mathcal{M}$ to its connectivity components. At the end of the algorithm, the sought graph G is obtained as a disjoint union of the constructed graphs for the restrictions of $\mathcal{M}$. Hence, we assume in the rest that $\mathcal{M}$ is connected.

If $\mathcal{M}$ is binary, it is possible to construct the graph G in polynomial-time by Proposition 7.8. We then verify that $\mathcal{M}(G)$ is isomorphic to G using Corollary 7.10. Clearly, if G is binary, then the above procedure is correct. If G is not binary, then we either fail to construct the graph using the algorithm from Proposition 7.8 (and we correctly output that $\mathcal{M}$ is not graphic) or the test described in Corollary 7.10 fails (and we again correctly output that $\mathcal{M}$ is not graphic). This establishes that the described algorithm is correct. ☐

In the proof of Theorem 7.11, we had to circumvent the test whether an oracle-given matroid is binary. We show that this has been necessary since it is not possible to algorithmically test in subexponential time whether an oracle-given matroid $\mathcal{M}$ is binary.

Proposition 7.12. *There is no subexponential algorithm for testing whether an oracle-given matroid is binary.*

Proof. Fix a $2k$-element set $E = \{x_1, \ldots, x_k, y_1, \ldots, y_k\}$. Let $\mathcal{C}_1$ be the family of all sets of the form $\{x_i, y_i, x_j, y_j\}$, where $1 \leq i < j \leq k$, and let $\mathcal{C}_2$ be the family of all sets $\{z_1, \ldots, z_k\}$, where $z_i \in \{x_i, y_i\}$, $1 \leq i \leq k$, and $|\{z_1, \ldots, z_k\} \cap \{y_1, \ldots, y_k\}|$ is even. The family $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2$ for $k \geq 3$ is a family of circuits of a binary matroid $\mathcal{M}$. Consider the following family of $(k+1)$-dimensional vectors over GF(2): the elements x_i, $1 \leq i \leq k-1$, are represented by vectors $(0|e_i)$ where e_i is the unit vector, the elements y_i, $1 \leq i \leq k-1$, by $(1|e_i)$, the element x_k by $(0, 1, \ldots, 1)$ and y_k by $(1, 1, \ldots, 1)$. The just defined vectors form a binary representation of $\mathcal{M}$.

Observe that every $Z \in \mathcal{C}_2$ is a hyperplane of $\mathcal{M}$. Since Z is both a circuit and a hyperplane of $\mathcal{M}$, we can relax it (see Proposition 6.2) and obtain a matroid $\mathcal{M}_Z$. Since the partial representations of $\mathcal{M}$ and $\mathcal{M}_Z$ with respect to the base $x_1, \ldots, x_{k-1}, y_k$ are the same for $Z \neq \{x_1, \ldots, x_k\}$ and $Z \neq \{x_1, \ldots, x_{i-1}, y_i, x_{i+1}, \ldots, x_{k-1}, y_k\}$, the matroid $\mathcal{M}_Z$ cannot be binary. However, to distinguish $\mathcal{M}$ and $\mathcal{M}_Z$, we have to query the independence of all $2^{k-1} - k$ such subsets Z. Since the number of elements of $\mathcal{M}$ is $2k$, running time of any algorithm deciding whether an oracle-given matroid is binary must be (at least) exponential in the number of its elements. $\square$