Journal of Combinatorial Theory, Series B 177 (2026) 105–142

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series B

journal homepage: www.elsevier.com/locate/jctb

Reconfiguration of basis pairs in regular matroids [☆]

Kristóf Bérczi [a,b], Bence Mátravölgyi [c,d], Tamás Schwarcz [e,a]

[a] *MTA-ELTE Matroid Optimization Research Group and HUN-REN–ELTE Egerváry Research Group, Department of Operations Research, Eötvös Loránd University, Pázmány Péter sétány 1/C, H-1117, Budapest, Hungary*
[b] *HUN-REN Alfréd Rényi Institute of Mathematics, Reáltanoda utca 13–15, H-1053, Budapest, Hungary*
[c] *ETH Zurich, Rämistrasse 101, 8092, Zürich, Switzerland*
[d] *MTA-ELTE Matroid Optimization Research Group, Pázmány Péter sétány 1/C, H-1117, Budapest, Hungary*
[e] *London School of Economics and Political Science, Department of Mathematics, Houghton Street, WC2A 2AE, London, United Kingdom*

A R T I C L E I N F O

Article history:
Received 22 June 2024
Available online xxxx

Keywords:
Exchange graph
Max-flow min-cut matroid
Reconfiguration problem
Regular matroid
Symmetric exchange
Toric ideal

A B S T R A C T

In recent years, combinatorial reconfiguration problems have attracted great attention due to their connection to various topics such as optimization, counting, enumeration, or sampling. One of the most intriguing open questions concerns the exchange distance of two matroid basis sequences, a problem that appears in several areas of computer science and mathematics. White (1980) proposed a conjecture for the characterization of two basis sequences being reachable from each other by symmetric exchanges, which received a significant interest also in algebra due to its connection to toric ideals and Gröbner bases. In this work, we verify White's conjecture for basis sequences of length two in regular matroids, a problem that was formulated as a separate question by Farber, Richter, and Shank (1985) and Andres, Hochstättler, and Merkel (2014). Most of previous work on White's conjecture has not considered the question from an algorithmic perspective. We study the problem from an optimization point of view: our proof implies a polynomial algorithm for determining a sequence of symmetric exchanges that transforms a basis pair into an-

☆ An extended abstract of the paper appeared at 56th Annual ACM Symposium on Theory of Computing (STOC 2024).

E-mail addresses: kristof.berczi@ttk.elte.hu (K. Bérczi), bmatravoelgy@student.ethz.ch (B. Mátravölgyi), t.b.schwarcz@lse.ac.uk (T. Schwarcz).

https://doi.org/10.1016/j.jctb.2025.10.009

other, thus providing the first polynomial upper bound on the exchange distance of basis pairs in regular matroids. As a byproduct, we verify a conjecture of Gabow (1976) on the serial symmetric exchange property of matroids for the regular case.

1. Introduction

The *basis exchange axiom* of matroids implies that for any pair X, Y of bases, there exists a sequence of exchanges that transforms X into Y. White [47] studied the analogous problem for basis sequences instead of single bases. Let $\mathcal{X} = (X_1, \ldots, X_k)$ be a sequence of – not necessarily disjoint – bases of a matroid, and let $e \in X_i - X_j$ and $f \in X_j - X_i$ with $1 \leq i < j \leq k$ be such that both $X_i - e + f$ and $X_j + e - f$ are bases. Then, the sequence $\mathcal{X}' = (X_1, \ldots, X_{i-1}, X_i - e + f, X_{i+1}, \ldots, X_{j-1}, X_j + e - f, X_{j+1}, \ldots, X_k)$ is obtained from $\mathcal{X}$ by a *symmetric exchange*. Two sequences $\mathcal{X}$ and $\mathcal{Y}$ are called *equivalent* if $\mathcal{Y}$ can be obtained from $\mathcal{X}$ by a composition of symmetric exchanges. The question naturally arises: what is the characterization of two basis sequences being equivalent?

There is an easy necessary condition for the equivalence of two sequences $\mathcal{X}$ and $\mathcal{Y}$: since a symmetric exchange does not change the number of bases in the sequence that contain a given element, the union of the members of $\mathcal{X}$ must coincide with the union of the members of $\mathcal{Y}$ as multisets. Motivated by this observation, $\mathcal{X}$ and $\mathcal{Y}$ are called *compatible* if $|\{i \mid e \in X_i, i \in \{1, \ldots, k\}\}| = |\{i \mid e \in Y_i, i \in \{1, \ldots, k\}\}|$ for every $e \in E$, where E denotes the ground set of the matroid. White [47] conjectured that compatibility is not only necessary but also sufficient for two sequences to be equivalent.

Conjecture 1 *(White). Two basis sequences $\mathcal{X}$ and $\mathcal{Y}$ of the same length are equivalent if and only if they are compatible.*

Conjecture 1 received a significant interest also in algebra due to its connection to toric ideals and Gröbner bases, see [9] and [34, Chapter 13] for further details. However, despite all the efforts, White's conjecture remains open even for sequences of length two. In this special setting, Farber, Richter, and Shank [17] verified the statement for graphic and cographic matroids, and noted that their proof does not seem to generalize for regular matroids. Andres, Hochstättler and Merkel [2] formulated White's conjecture for regular matroids as a separate question, and noted that Seymour's decomposition theorem [40] might help to find a proof.

White's conjecture has no implications on the minimum number of exchanges needed to transform two equivalent sequences into each other, called their *exchange distance*. For basis pairs, Gabow [20] formulated the following problem, later stated as a conjecture by Wiedemann [48] and by Cordovil and Moreira [11], and posed as an open problem in Oxley's book [36, Conjecture 15.9.11].

Conjecture 2 *(Gabow). Let X_1 and X_2 be disjoint bases of a rank-r matroid M. Then, the exchange distance of (X_1, X_2) and (X_2, X_1) is r.*

Note that Conjecture 2 would imply Conjecture 1 for sequences of the form (X_1, X_2) and (X_2, X_1). Since the rank of the matroid is a trivial lower bound on the minimum number of exchanges needed to transform (X_1, X_2) into (X_2, X_1), the essence of Gabow's conjecture is that rank many steps might always suffice. This also implies that the conjecture can be rephrased as a generalization of the symmetric exchange axiom as follows: If X_1 and X_2 are bases of the same matroid, then there are orderings $X_1 = (x_1^1, \dots, x_r^1)$ and $X_2 = (x_1^2, \dots, x_r^2)$ such that $\{x_1^1, \dots, x_i^1, x_{i+1}^2, \dots, x_r^2\}$ and $\{x_1^2, \dots, x_i^2, x_{i+1}^1, \dots, x_r^1\}$ are bases for $i = 0, \dots, r$. This property is often referred to as *serial symmetric exchange property*.

The focus of this paper is on regular matroids, a fundamental class that generalizes graphic and cographic matroids. Our main tool is Seymour's celebrated decomposition theorem, which gives a method for decomposing any regular matroid into matroids which are either graphic, cographic, or isomorphic to a simple 10-element matroid. Regular matroids play a crucial role in both matroid theory and optimization, since those are exactly the matroids that can be represented over $\mathbb{R}$ by totally unimodular matrices [36, Theorem 6.6.3]. This connection has far-reaching implications, e.g. the fastest known algorithm for testing total unimodularity of a matrix is based on the ability to find such a decomposition if one exists [43].

Interest in exchange properties of matroids originally arose in part from the fact that they serve as an abstraction of pivot algorithms of linear algebra [22,47]. In the past decades, however, problems appeared in many different areas of computer science and mathematics that are actually based on exchange properties of matroid bases, though these problems have never been explicitly linked together in previous work. Implicitly, one of the goals of the paper is to draw attention to these connections.

1.1. The role of equivalent sequences

Though finding a sequence of symmetric exchanges between basis sequences may seem to be a structural question purely on matroids, it has been identified as the key ingredient in a range of problems. In what follows, we give an overview of the main applications where the reconfiguration of basis sequences shows up.

Sampling common bases. A long line of work concentrated on designing efficient algorithms for sampling bases of matroids [1,18]. Most of the results relied on the Markov Chain Monte Carlo technique: for any matroid, the basis exchange property defines a natural random walk over all bases, also known as "down-up" random walk. Sampling common bases of two matroids is, however, significantly more difficult. Unlike in the case of a single matroid, the intersection of two matroids does not satisfy the exchange property, making it impossible to define a simple down-up-type random walk in general. Partitions of the ground set of a matroid M into two disjoint bases can be identified with common bases of M and its dual M^*. From this perspective, White's conjecture states that there is a sequence of exchanges between any pair of common bases of M and M^*. Thus verifying Conjecture 1 would open up the possibility for a natural down-up random walk for matroid intersection in the special case when the two matroids are dual to each other.

Equitability of matroids. A matroid whose ground set E partitions into disjoint bases is called *equitable* if for any set $Z \subseteq E$, there exists a partition into disjoint bases $E = X_1 \cup \cdots \cup X_k$ such that $\lfloor |Z|/k \rfloor \leq |X_i \cap Z| \leq \lceil |Z|/k \rceil$. The Equitability Conjecture states that every matroid whose ground set partitions into disjoint bases is equitable. The existence of such a partition would follow from both Conjecture 1 and Conjecture 2. To see this, first observe that it suffices to consider the case $k = 2$, since for general k the statement then follows by repeated application of the problem restricted to $X_i \cup X_j$ for $1 \leq i < j \leq k$; see [25, Discussion page] for details. Then, for any partition of the ground set into two bases X_1 and X_2, both Conjecture 1 and Conjecture 2 imply the existence of a sequence of symmetric exchanges that transforms (X_1, X_2) into (X_2, X_1). One of the basis pairs of the sequence thus obtained must satisfy $\lfloor |Z|/2 \rfloor \leq |X_i \cap Z| \leq \lceil |Z|/2 \rceil$ for $i = 1, 2$. Apart from the matroid classes for which Conjecture 1 or 2 was settled, the Equitability Conjecture was verified for base orderable matroids [19] only.

Fair allocations. In fair allocation problems, the goal is to find an allocation of a set E of m indivisible items among n agents so that each agent finds the allocation fair. Biswas and Barman [8] and Dror, Feldman, and Segal-Halevi [14] studied the existence of allocations under matroid constraints that are *envy-free up to one good* (EF1), in which the bundle of each agent is required to form an independent set of a matroid. The problem remains open even when the agents share the same matroid constraints and binary valuation. In such a case, there exists a $Z \subseteq E$ such that the value of any subset X of items is $|X \cap Z|$ for every agent, and a feasible EF1 allocation corresponds to a partition of the ground set into n independent sets $X_1, \ldots, X_n$ such that $\lfloor |Z|/n \rfloor \leq |X_i \cap Z| \leq \lceil |Z|/n \rceil$ for every $1 \leq i \leq n$. The existence of such an allocation would follow from the Equitability Conjecture, and hence from both Conjecture 1 and Conjecture 2.

Unimodular triangulations. For a polytope $P \subseteq \mathbb{R}^n$ with vertices $v_1, \ldots, v_p$, a *triangulation* $\mathcal{T}$ of P is a collection of simplices on the vertices of P such that (i) if $T \in \mathcal{T}$ then all faces of T are in $\mathcal{T}$, (ii) if $T_1, T_2 \in \mathcal{T}$ then $T_1 \cap T_2$ is a face of both T_1 and T_2, and (iii) $\bigcup_{T \in \mathcal{T}} \mathrm{conv}(T) = P$. A triangulation $\mathcal{T}$ is *unimodular* if the volume of every highest dimensional simplex of $\mathcal{T}$ is the same. As a geometric variant of Conjecture 1, Haws [23] conjectured that every matroid base polytope has a unimodular triangulation. One motivation behind the conjecture was that the existence of such a triangulation implies a bound of n on the Carathéodory rank of a connected matroid base polytope, a result that was proved only later in [21]. Recently, Backman and Liu [4] verified Haws' conjecture by showing that every matroid base polytope admits a regular unimodular triangulation.

Toric ideals. Consider a matroid $M = (E, \mathcal{B})$ where E denotes the ground set and $\mathcal{B}$ is the family of bases of M. For a field $\mathbb{K}$, let S_M denote the noncommutative polynomial ring $\mathbb{K}\langle y_B \mid B \in \mathcal{B}\rangle$. The *toric ideal* I_M *associated to* M is the kernel of the $\mathbb{K}$-homomorphism $\varphi_M \colon S_M \to \mathbb{K}[x_e \mid e \in E]$ given by $y_B \mapsto \prod_{e \in B} x_e$. Assume now that the basis pair (Y_1, Y_2) is obtained from (X_1, X_2) by a symmetric exchange, that is, $Y_1 = X_1 - e + f$ and $Y_2 = X_2 + e - f$ for some $e \in X_1 - X_2$ and $f \in X_2 - X_1$. Then, the quadratic binomial corresponding to the symmetric exchange is $y_{X_1} y_{X_2} - y_{Y_1} y_{Y_2}$. It is not difficult to see that such binomials belong to the ideal I_M. In algebraic terms, Conjecture 1 states that I_M is generated by quadratic binomials corresponding to symmetric exchanges for every matroid M. For discussions on further variants of White's conjecture, see [29,30].

Reconfiguration problems. The vertices of the *exchange graph* of a matroid correspond to basis sequences of a given length, two vertices being connected by an edge if the corresponding basis sequences can be obtained from each other by a single symmetric exchange. In this context, Conjecture 1 aims at characterizing reachability in the exchange graph, and states that the connected components are exactly the equivalence classes of compatibility. An analogous problem can be formulated for the intersection of two matroids, i.e. given two common bases of two matroids, decide if one can be obtained from the other by always changing a single element while maintaining independence in both matroids. Such a sequence of exchanges is known to exist in special cases, e.g. for arborescences, or more generally, for k-arborescences [26]. Recently, the problem was shown to be oracle hard by Kobayashi, Mahara, and Schwarcz [26]. For sequences of length two, Conjecture 1 corresponds to the special case of the common basis reconfiguration problem when the two matroids are dual to each other.

1.2. Our results

Motivated by the significance of equivalent basis sequences in various applications and by the fact that it was formulated as an interesting open problem in [2,17], we study the exchange distance of basis pairs in regular matroids. First, we give a polynomial upper bound on the exchange distance of compatible basis pairs, which proves Conjecture 1 for sequences of length two in regular matroids. Our proof is algorithmic, which allows us to determine a sequence of symmetric exchanges that transforms a given pair of bases into another in polynomial time. As usual in matroid algorithms, we assume that the matroid is given by an independence oracle and the running time is measured by the number of oracle calls and other conventional elementary steps. For the sake of simplicity, by “polynomial number” of oracle calls we mean “polynomial in the number of elements of the ground set”.

Theorem 1.1. *Let $\mathcal{X} = (X_1, X_2)$ and $\mathcal{Y} = (Y_1, Y_2)$ be compatible basis pairs of a regular matroid M of rank $r \geq 2$. Then, there exists a sequence of symmetric exchanges that transforms $\mathcal{X}$ into $\mathcal{Y}$, has length at most $2 \cdot r^2$, and uses each element at most $4 \cdot (r-1)$ times. Furthermore, such a sequence can be determined using a polynomial number of oracle calls.*

A fine-grained analysis of the algorithm shows that the number of steps can be bounded better when the basis pairs are inverses of each other. Our second result is an improved upper bound on the exchange distance of such pairs, which proves Conjecture 2 for regular matroids.

Theorem 1.2. *Let X_1, X_2 be disjoint bases of a regular matroid M of rank r. Then, there exists a sequence of symmetric exchanges that transforms (X_1, X_2) into (X_2, X_1) and has length r. Furthermore, such a sequence can be determined using a polynomial number of oracle calls.*

In particular, by the reduction described in Section 1.1, an important corollary is that the Equitability Conjecture holds for regular matroids, a result that might be of independent interest on its own.

Corollary 1.3. *If M is a regular matroid whose ground set decomposes into disjoint bases, then M is equitable.*

Our results give the first polynomial bound on the exchange distance of basis pairs and are the first to settle the conjectures of White and Gabow in regular matroids. We hope that our paper will help proving White's conjecture in regular matroids for sequences of arbitrary length, as well as obtaining better bounds for the exchange distance of basis pairs.

1.3. Related work

When restricted to sequences of length two, White's conjecture was verified for graphic and cographic matroids by Farber, Richter, and Shank [17], for transversal matroids by Farber [16], and for split matroids by Bérczi and Schwarcz [7]. For sequences of arbitrary length, Blasiak [9] confirmed the conjecture for graphic matroids. It is not difficult to check that the conjecture holds for a matroid M if and only if it holds for its dual M^*, therefore Blasiak's result settles the cographic case as well. Further results include lattice path matroids by Schweig [38], sparse paving matroids by Bonin [10], strongly base orderable matroids by Lasoń and Michałek [30], and frame matroids satisfying a linearity condition by McGuinness [32].

Gabow [20] observed that Conjecture 2 holds for partition matroids, transversal matroids, and matching matroids. An easy proof shows that it also holds for strongly base orderable matroids. The graphic case was independently proved by Wiedemann [48], Kajitani, Ueno, and Miyano [24], and Cordovil and Moreira [11]. The cases of sparse paving and split matroids were settled in [10] and [7], respectively.

For the case of basis pairs, a common generalization of the conjectures of White and Gabow was proposed by Hamidoune [11] stating that the exchange distance of compatible basis pairs is at most the rank of the matroid. A strengthening was proposed by Bérczi, Mátravölgyi, and Schwarcz [6] who considered a weighted variant of Hamidoune's conjecture and verified it for strongly base orderable matroids, split matroids, spikes, and graphic matroids of wheel graphs.

A rank-r matroid $M = (E, \mathcal{B})$ with $|E| = n$ is called *cyclically orderable* if there exists an ordering $S = \{e_1, \ldots, e_n\}$ such that $\{e_i, e_{i+1}, \ldots, e_{i+r-1}\} \in \mathcal{B}$ for every $i \in [n]$, where indices are understood in a cyclic order. Furthermore, M is *uniformly dense* if $|E| \cdot r_M(X) \geq r_M(E) \cdot |X|$ holds for every $X \subseteq E$, where r_M denotes the rank function of M. As a variant of Conjecture 2 where the matroid does not necessarily decompose into two disjoint bases, Kajitani, Ueno, and Miyano [24] conjectured that a matroid is cyclically orderable if and only if it is uniformly dense. Van den Heuvel and Thomassé [46] showed that this is true if $|E|$ and $r_M(E)$ are coprimes, and Bonin's result [10] for sparse paving matroids extends to this setting as well. Recently, Bérczi, Jánosik and Mátravölgyi [5] verified the conjecture for split matroids whose ground set is the disjoint union of bases.

For a basis pair (X_1, X_2) we say that the basis pair $(X_1 - e + f, X_2 + e - f)$ is obtained by a *left unique symmetric exchange* if for the element $e \in X_1 - X_2$, f is the unique element of $X_2 - X_1$ such that both $X_1 - e + f$ and $X_2 + e - f$ are bases. White [47] observed that a matroid is series-parallel if and only if for any compatible basis pairs $\mathcal{X}$ and $\mathcal{Y}$, $\mathcal{X}$ can be obtained from $\mathcal{Y}$ by left unique symmetric exchanges, while McGuinness [31] showed that any basis pair of a regular matroid admits a left unique symmetric exchange. Furthermore, White [47, Conjecture 8] conjectured that for any two compatible basis pairs $\mathcal{X}$ and $\mathcal{Y}$ of a regular matroid, $\mathcal{Y}$ can be obtained from $\mathcal{X}$ if, besides left unique symmetric exchanges, switching the order of the bases is also allowed.[1] A strengthening of this conjecture only allows left unique symmetric exchanges and right unique symmetric exchanges to be used, where the latter is defined analogously to the former. This variant formally appeared in [2, Conjecture 5] where it was also attributed to White following personal communication with him, see also [47, Remark 4].

Paper organization. The rest of the paper is organized as follows. In Section 2, we recall basic definitions, notation, and some results on the decomposition of regular matroids

[1] In fact, White formulated the conjecture for basis sequences of arbitrary length; see [47] for further details.

that we will use in our proofs. In Section 3, we show how Conjecture 1 for sequences of length two and Conjecture 2 can be reduced to 3-connected matroids not containing cocircuits of size at most three. Then, in Section 4, we explain how a quadratic bound on the number of exchanges can be derived for graphs using the aforementioned reductions, and prove strengthenings of White's and Gabow's conjectures for graphic matroids. The rest of the paper is devoted to proving Theorem 1.1 and Theorem 1.2. Our proofs rely on the regular matroid decomposition theorem of Seymour. Nevertheless, solving the problems for each matroid in the decomposition in parallel and then simply merging the solutions does not work. The key ingredient that leads to Theorem 1.1 and Theorem 1.2 is a careful combination of the solutions of these subproblems that results in a sequence of exchanges whose length is polynomially bounded. For ease of reading, we encourage first-time readers to skip the technical parts of Section 3.

2. Preliminaries

Basic notation and definitions. Given a ground set E, the *difference* of $X, Y \subseteq E$ is denoted by $X - Y$. If Y consists of a single element y, then $X - \{y\}$ and $X \cup \{y\}$ are abbreviated as $X - y$ and $X + y$, respectively. The *symmetric difference* of X and Y is defined as $X \triangle Y := (X - Y) \cup (Y - X)$.

Graphs. Throughout the paper, we consider loopless graphs that might contain parallel edges. For a graph $G = (V, E)$, the *set of edges incident to a vertex* $v \in V$ is denoted by $\delta_G(v)$ and the *degree of* v is $d_G(v) = |\delta_G(v)|$. We dismiss the subscript if the graph is clear from the context. For a subset $F \subseteq E$, we denote the *set of vertices of the edges in* F by $V(F)$. For $X \subseteq V$, we denote by $F[X]$ the *set of edges in* F *induced by* X. The *graph obtained by deleting* F *and* X is denoted by $G - F - X$. A *cut* of G is a subset $F \subseteq E$ of edges whose deletion increases the number of components. A cut is *trivial* if $F = \delta(w)$ for some $w \in V$ and *nontrivial* otherwise. A graph is called *bispanning* if its edge set can be decomposed into two spanning trees. By a classical result of Tutte [45] and Nash-Williams [35], a graph $G = (V, E)$ is bispanning if and only if $|E| = 2 \cdot |V| - 2$ and $|E[X]| \leq 2 \cdot |X| - 2$ for every $\emptyset \neq X \subseteq V$.

Matroids. For basic definitions on matroids, we refer the reader to [36]. A *matroid* $M = (E, \mathcal{I})$ is defined by its *ground set* E and its *family of independent sets* $\mathcal{I} \subseteq 2^E$ that satisfies the *independence axioms*: (I1) $\emptyset \in \mathcal{I}$, (I2) $X \subseteq Y,\ Y \in \mathcal{I} \Rightarrow X \in \mathcal{I}$, and (I3) $X, Y \in \mathcal{I},\ |X| < |Y| \Rightarrow \exists e \in Y - X$ *s.t.* $X + e \in \mathcal{I}$. Members of $\mathcal{I}$ are called *independent*, while sets not in $\mathcal{I}$ are called *dependent*. The *rank* $r_M(X)$ of a set X is the maximum size of an independent set in X. The maximal independent subsets of E are called *bases* and their family is usually denoted by $\mathcal{B}$. If the matroid is given by its family of bases instead of independent sets, then we write $M = (E, \mathcal{B})$. The *dual* of M is the matroid $M^* = (E, \mathcal{I}^*)$ where $\mathcal{I}^* = \{X \subseteq E \mid E - X \text{ contains a basis of } M\}$. For technical reasons, we allow the ground set of the matroid to be the empty set, in which case the matroid is simply the *empty matroid* $M = (\emptyset, \{\emptyset\})$.

Let $\mathcal{X} = (X_1, \ldots, X_k)$ and $\mathcal{Y} = (Y_1, \ldots, Y_k)$ be sequences of bases of M. A sequence of symmetric exchanges that transforms $\mathcal{X}$ into $\mathcal{Y}$ is called an *$\mathcal{X}$-$\mathcal{Y}$ exchange sequence*. The *width* of an exchange sequence is the maximum number of occurrences of any element in it. If the symmetric exchanges do not involve the elements in $F \subseteq E$ then the exchange sequence is called *F-avoiding*. The *exchange distance* of $\mathcal{X}$ and $\mathcal{Y}$ is the minimum length of an $\mathcal{X}$-$\mathcal{Y}$ exchange sequence if one exists and $+\infty$ otherwise.

A *circuit* is an inclusionwise minimal dependent set, while a *loop* is a circuit consisting of a single element. A *cocircuit* is an inclusionwise minimal set that intersects every basis, or equivalently, a circuit of the dual matroid. A set is said to be *coindependent* if it contains no cocircuit of the matroid, or equivalently, it is independent in the dual matroid. Two elements $e, f \in E$ are *parallel* if they form a circuit of size two. A circuit of size three is called a *triangle*, while a cocircuit of size three is called a *triad*. A *cycle* of a matroid is a (possibly empty) subset of its ground set which can be partitioned into circuits. For a matroid M, we denote its *families of independent sets*, *bases* and *circuits* by $\mathcal{I}(M)$, $\mathcal{B}(M)$ and $\mathcal{C}(M)$, respectively. Unlike in graphs, the intersection of a circuit and a cocircuit of a matroid might have odd size. Nevertheless, the intersection never consists of a single element, see e.g. [36, Proposition 2.1.11].

Lemma 2.1. *Let C and T be a circuit and a cocircuit of a matroid M. Then $|C \cap T| \neq 1$.*

Let $M = (E, \mathcal{I})$ be a matroid and $E', E'' \subseteq E$. The *restriction to E'* and the *deletion of $E - E'$* result in the same matroid $M|E' = M \backslash (E - E') = (E', \mathcal{I}')$ with independence family $\mathcal{I}' = \{I \in \mathcal{I} \mid I \subseteq E'\}$. The *contraction to E''* and the *contraction of* $(E - E'')$ result in the same matroid $M.E'' = M/(E - E'') = (E'', \mathcal{I}'')$ where $\mathcal{I}'' = \{I \in \mathcal{I} \mid I \subseteq E'', I \cup Z \in \mathcal{I}$ for any $Z \in \mathcal{I}, Z \subseteq E - E''\}$. A matroid N that can be obtained from M by a sequence of restrictions and contractions is called a *minor* of M. The *union* or *sum* of two matroids $M_1 = (E, \mathcal{I}_1)$ and $M_2 = (E, \mathcal{I}_2)$ over the same ground set is the matroid $M_\Sigma = (E, \mathcal{I}_\Sigma)$ where $\mathcal{I}_\Sigma = \{I \subseteq E \mid I = I_1 \cup I_2$ for some $I_1 \in \mathcal{I}_1, I_2 \in \mathcal{I}_2\}$. We use $M_1 + M_2$ for denoting the sum of M_1 and M_2. Edmonds and Fulkerson [15] showed that the rank function of the sum of two matroids is $r_\Sigma(Z) = \min\{\sum_{i=1}^{2} r_i(X) + |Z - X| \mid X \subseteq Z\}$. In particular, E is independent in the sum of M_1 and M_2 if and only if $r_{M_1}(X) + r_{M_2}(X) \geq |X|$ for every $X \subseteq E$.

A matroid is *representable over some field* $\mathbb{F}$ if there exists a family of vectors from a vector space over $\mathbb{F}$ whose linear independence relation is the same as the independence relation of the matroid. The matroid is *binary* if it is representable over $GF(2)$, and is *regular* if it can be represented over any field. The following lemma gives a characterization of binary matroids in terms of cycles, see e.g. [36, Theorem 9.1.2].

Lemma 2.2. *A matroid is binary if and only if $C_1 \triangle C_2$ is a cycle for any cycles C_1, C_2.*

We will further rely on the following observation.

$$\begin{bmatrix} 0&1&1&1&0&0&1&0&1&1 \\ 0&0&1&1&1&1&0&1&0&1 \\ 1&0&0&1&1&1&1&0&1&0 \\ 1&1&0&0&1&0&1&1&0&1 \\ 1&1&1&0&0&1&0&1&1&0 \end{bmatrix} \begin{matrix} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{matrix}$$

(a) Representation of the binary matroid R_{10} over $GF(2)$.

(b) Representation of R_{10} as an even-cycle matroid.

(c) The bases of F_7 are the non-line 3-element sets of the Fano plane.

Fig. 1. Representations of R_{10} and F_7.

Lemma 2.3. *Let $T = \{t_1, t_2, t_3\}$ be a triangle of a binary matroid $M = (E, \mathcal{B}(M))$ and let $F \subseteq E - T$. Then, $F + t_i \in \mathcal{B}(M)$ for either none or exactly two of the indices $i \in \{1, 2, 3\}$.*

Proof. Assume first that at least two of the three sets form bases of M. We may assume that $F + t_1$ and $F + t_2$ are bases. Then, there exists a circuit $C \subseteq F + t_1 + t_2$ and necessarily $t_1, t_2 \in C$. The set $C \triangle T$ is a cycle such that $t_3 \in C \triangle T \subseteq F + t_3$, hence $F + t_3$ is not a basis of M. This shows that at most two of the sets $F + t_1$, $F + t_2$ and $F + t_3$ are bases.

Suppose now that at most one of the three sets forms a basis. We may assume that $F + t_1$ and $F + t_2$ are not bases. If F is not independent, then $F + t_3$ is clearly not a basis. Otherwise, let C_1 and C_2 be circuits such that $t_1 \in C_1 \subseteq F + t_1$ and $t_2 \in C_2 \subseteq F + t_2$. Then, $C_1 \triangle C_2 \triangle T$ is a cycle such $t_3 \in C_1 \triangle C_2 \triangle T \subseteq F + t_3$, hence $F + t_3$ is not a basis. This concludes the proof of the lemma. □

The matroid R_{10} is a binary matroid that can be represented as the ten vectors in the five-dimensional vector space over $GF(2)$ that have exactly three nonzero entries, see Fig. 1a. The *Fano matroid* F_7 is obtained from the Fano plane by calling a set independent if it contains at most two points or it has three points which are not lines of the plane, see Fig. 1c. In other words, F_7 is the matroid with ground set $E = \{a, b, c, d, e, f, g\}$ whose bases are all subsets size of 3 except $\{a, b, d\}$, $\{b, c, e\}$, $\{a, c, f\}$, $\{a, e, g\}$, $\{c, d, g\}$, $\{b, f, g\}$ and $\{d, e, f\}$.

Decomposition of regular matroids. Let M_1 and M_2 be binary matroids on ground sets E_1 and E_2, respectively, such that $|E_1|, |E_2| < |E_1 \triangle E_2|$. Then, we denote by $M_1 \triangle M_2$ the binary matroid on ground set $E = E_1 \triangle E_2$ with cycles being the sets of the form $C_1 \triangle C_2$ where C_i is a cycle of M_i for $i = 1, 2$.

When $E_1 \cap E_2 = \emptyset$, then $M_1 \oplus_1 M_2 := M_1 \triangle M_2$ is called the *1-sum* or *direct sum of M_1 and M_2*. Its family of bases is

$$\mathcal{B}(M_1 \oplus_1 M_2) = \{B_1 \cup B_2 \mid B_1 \in \mathcal{B}(M_1), B_2 \in \mathcal{B}(M_2)\}.$$

When $|E_1 \cap E_2| = 1$, say $E_1 \cap E_2 = \{t\}$, such that t is nor a loop nor a coloop of M_1 or M_2, then $M_1 \oplus_2 M_2 \coloneqq M_1 \triangle M_2$ is called the *2-sum of M_1 and M_2 along t*. Its family of bases is

$$\begin{aligned}\mathcal{B}(M_1 \oplus_2 M_2) = \{B_1' \cup B_2 \mid B_1' \in \mathcal{B}(M_1/t), B_2 \in \mathcal{B}(M_2 \backslash t)\} \\ \cup \{B_1 \cup B_2' \mid B_1 \in \mathcal{B}(M_1 \backslash t), B_2' \in \mathcal{B}(M_2/t)\}.\end{aligned}$$

When $|E_1 \cap E_2| = 3$ and $E_1 \cap E_2 = T$ is a coindependent triangle of both M_1 and M_2, then $M_1 \oplus_3 M_2 \coloneqq M_1 \triangle M_2$ is called the *3-sum of M_1 and M_2 along T*. The matroid $M_1 \oplus_3 M_2$ has rank $r(M_1) + r(M_2) - 2$, and its family of bases is (see [3, Section 2.1] together with Lemma 2.3)

$$\begin{aligned}\mathcal{B}(M_1 \oplus_3 M_2) = \{B_1'' \cup B_2 \,|B_1'' \in \mathcal{B}(M_1/T), B_2 \in \mathcal{B}(M_2 \backslash T)\} \\ \cup \{B_1' \cup B_2' \,|B_1' \subseteq E_1 \setminus T, B_2' \subseteq E_2 \setminus T, \exists i, j, k : \{i, j, k\} = \{1, 2, 3\}, \\ B_1' + t_i, B_1' + t_j \in \mathcal{B}(M_1), B_2' + t_i, B_2' + t_k \in \mathcal{B}(M_2)\} \\ \cup \{B_1 \cup B_2'' \,|B_1 \in \mathcal{B}(M_1 \backslash T), B_2'' \in \mathcal{B}(M_2/T)\}.\end{aligned}$$

Seymour's fundamental decomposition theorem [40] gives a constructive characterization of regular matroids.

Theorem 2.4 *(Seymour's decomposition theorem). A matroid is regular if and only if it is obtained by means of 1-, 2-, and 3-sums, starting from graphic and cographic matroids and copies of a certain 10-element matroid R_{10}.*

A binary matroid is said to be *connected* or *2-connected* if it is not a 1-sum, and *3-connected* if it is not a 1-sum or a 2-sum of two matroids. While studying the extension complexity of the independence polytope of regular matroids, Aprile and Fiorini [3] recently gave a refinement of Seymour's result in the 3-connected case.

Theorem 2.5 *(Aprile and Fiorini). Let M be a 3-connected regular matroid distinct from R_{10}. There exists a tree $\mathcal{T}$ such that each node $v \in V(\mathcal{T})$ is labeled with a graphic or cographic matroid M_v, each edge $uv \in E(\mathcal{T})$ has a corresponding 3-sum $M_u \oplus_3 M_v$, and M is the matroid obtained by performing all the 3-sum operations corresponding to the edges of $\mathcal{T}$ in arbitrary order. Moreover, if $v \in V(\mathcal{T})$ is such that M_v is the cographic matroid of a nonplanar graph G_v, then no nontrivial cut of G_v is involved in any of the 3-sums.*

A tree $\mathcal{T}$ satisfying the conditions of Theorem 2.5 is called a *decomposition tree*[2] of M, and the matroids corresponding to the nodes of $\mathcal{T}$ are referred to as *basic* matroids. It

[2] We note that our definition of a decomposition tree corresponds to a decomposition tree without bad nodes in [3].

is worth mentioning that an analogous result was proved by Dinitz and Kortsarz in [13], but their decomposition tree may involve 1- and 2-sums, and also 3-sums along nontrivial cuts.

To describe the dual of a 3-sum, we need the notion of Δ-Y exchanges. In case of graphs, if T is a triangle of a graph G, then we perform a Δ-Y exchange on G by deleting the edges of T, adding a new vertex v and edges joining v to vertices of T. More generally, consider a binary matroid M and let T be a coindependent triangle of M. Let N be a matroid isomorphic to the graphic matroid of K_4 on ground set $T \cup T'$ where T is a triangle of N, and the triad T' of N is disjoint from the ground set of M. We say that the matroid $\Delta_T(M) \coloneqq M \oplus_3 N$ is obtained from M by performing a *Δ-Y exchange*. McGuinness [31] gave a characterization of the dual of a 3-sum.

Proposition 2.6 *(McGuinness). Consider a 3-sum $M_1 \oplus_3 M_2$ along a coindependent triangle T of M_1 and M_2. Then, $(M_1 \oplus_3 M_2)^* = \Delta_T(M_1)^* \oplus_3 \Delta_T(M_2)^*$, where the Δ-Y exchanges $\Delta_T(M_1)$ and $\Delta_T(M_2)$ are performed using the same matroid N on ground set $T \cup T'$ and the 3-sum $\Delta_T(M_1)^* \oplus_3 \Delta_T(M_2)^*$ is performed using the common triangle T' of $\Delta_T(M_1)^*$ and $\Delta_T(M_2)^*$.*

The reverse operation of a Δ-Y exchange is called a Y-Δ exchange. If T is an independent triad of a binary matroid M, then we say that the matroid $\nabla_T(M) \coloneqq \Delta_T(M^*)^*$ is obtained from M by performing a Y-Δ exchange. The Δ-Y and Y-Δ exchanges are indeed reverse operations of each other, see [36, Proposition 11.5.11]. If u is a degree 3 vertex of a graph G with distinct adjacent vertices x, y and z, then we can perform the Y-Δ operation on the graphic matroid $M(G)$ by deleting u and adding the edges xy, yz and xz. In particular, if T is an independent triad of a graphic matroid $M(G)$ corresponding to the edges adjacent to a trivial cut G, then $\nabla_T(M(G))$ is a graphic matroid. This implies the following.

Lemma 2.7. *If T is a coindependent triangle of a cographic matroid $M^*(G)$ corresponding to a trivial cut of G, then $\Delta_T(M^*(G))$ is cographic.*

Remark 2.8. We note that if T does not correspond to a trivial cut of G, then $\Delta_T(M^*(G))$ might not be a cographic matroid. As an example, if e is an edge of K_5 and T is the edge set of the triangle of K_5 formed by the vertices not adjacent to e, then, $\Delta_T(M(K_5-e)) = M(K_{3,3})$, see also [36, Figure 11.20]. Since $K_5 - e$ is a planar and $K_{3,3}$ is a nonplanar graph, $M(K_5 - e)$ is a cographic matroid while $M(K_{3,3})$ is not.

Algorithms and oracles. In matroid algorithms, it is usually assumed that the matroid is given by an *oracle* and the running time is measured by the number of oracle calls and other conventional elementary steps. There are many different types of oracles that are often used, the independence, circuit and rank oracles probably being the most standard ones. For a matroid $M = (E, \mathcal{I})$ and set $X \subseteq E$ as an input, an independence oracle answers *"Yes"* if X is independent and *"No"* otherwise, a circuit oracle answers *"Yes"* if X is a circuit and *"No"* otherwise, and a rank oracle gives back $r_M(X)$.

In fact, these oracles have the same computational power. An oracle $\mathcal{O}_1$ is *polynomially reducible* to another oracle $\mathcal{O}_2$ if $\mathcal{O}_1$ can be implemented by using a polynomial number of oracle calls to $\mathcal{O}_2$ measured in terms of the size of the ground set. Two oracles are *polynomially equivalent* if they are mutually polynomially reducible to each other. It is not difficult to show that the independence, circuit and rank oracles are polynomially equivalent, see e.g. [37].

Let E denote the ground set of M, and X and Y be disjoint subsets of E. Then the rank function of the minor $M/X\setminus Y$ is $r_{M/X\setminus Y}(Z) = r(Z \cup X) - r(Z)$ for $Z \subseteq E - (X \cup Y)$, and the rank function of the dual M^* is $r_{M^*}(Z) = |Z| - (r_M(E) - r_M(E - Z))$ for $Z \subseteq E$, see e.g. [36]. That is, given an independence oracle access to the matroid M, independence oracles can be implemented for any minor and the dual of M by the polynomial equivalence of the rank and independence oracles. Therefore, we will use these basic matroid operations in our algorithm.

For a binary matroid M, it can be decided if M is not connected, connected but not 3-connected, or 3-connected using a polynomial number of oracle calls [43, Theorem 8.4.1]. Moreover, the algorithm also provides a 1-sum decomposition in the first case, a 2-sum decomposition in the second case, and a 3-sum decomposition if it exists in the third case. When applied to a regular matroid recursively, the algorithm eventually gives a decomposition M into basic matroids each of which is either graphic, cographic or isomorphic to R_{10}. If the matroid is 3-connected and is not R_{10}, then [3] describes an algorithm how to modify this decomposition until it gives a decomposition tree as in Theorem 2.5 using a polynomial number of oracle calls.

3. Reduction to 3-connected case without small cocircuits

In this section, we focus on how the exchange distance behaves for basic matroid operations such as contraction and taking 1- or 2-sums. Furthermore, we identify structural properties of regular matroids such as the existence of a *tight set* or a *triad* that allow for reduction in the problem size. As mentioned in the introduction, these reduction steps will eventually make it possible to write up the matroid as the 3-sum of a regular matroid and the graphic matroid of a 4-regular graph. Algorithmic aspects of the preprocessing steps are discussed at the end of the section.

Let M be the 1-, 2- or 3-sum of binary matroids $M_\circ = (E_\circ, \mathcal{B}(M_\circ))$ and $M_\bullet = (E_\bullet, \mathcal{B}(M_\bullet))$ along T where T is empty in case of 1-sums, it consists of a single element in case of 2-sums and of three elements in case of 3-sums. For any set $X \subseteq E_\circ \cup E_\bullet$, we define $X^\circ := X \cap (E_\circ - T)$ and $X^\bullet := X \cap (E_\bullet - T)$. In particular, for any basis $B \in \mathcal{B}(M)$, we have $B^\circ = B \cap E_\circ$ and $B^\bullet = B \cap E_\bullet$. Note that for 2- and 3-sums, B° and $B^\bullet$ are not necessarily bases of $M_\circ$ and $M_\bullet$, respectively; see the characterization of bases in Section 2.

Since we will prove Theorem 1.1 and Theorem 1.2 in a stronger form for graphic matroids, we formulate some of the reductions for F-avoiding exchange sequences whose last step is partially fixed. This results in a series of rather technical lemmas, but this should not deter the interested reader from the later sections. We encourage first-time readers to skip these technical parts and only return to them after getting a general understanding of the structure of the proof.

Operations similar to those discussed in Section 3.1 and Section 3.2 were implicitly mentioned in [47], while an operation similar to the one discussed in Section 3.3 was considered in [42]. However, we will deduce stronger properties of the reduction steps and also discuss the algorithmic aspects.

3.1. Making the bases disjoint

We start with the simple observation that it suffices to consider compatible pairs consisting of disjoint bases. Recall that the width of an exchange sequence is the maximum number of occurrences of any element in it.

Lemma 3.1. *Let $\mathcal{X} = (X_1, X_2)$ and $\mathcal{Y} = (Y_1, Y_2)$ be compatible pairs of bases of a matroid M and let $F \subseteq (X_1 \cap Y_1) \cup (X_2 \cap Y_2)$. Define $\mathcal{X}' \coloneqq (X_1 - X_2, X_2 - X_1)$, $\mathcal{Y}' \coloneqq (Y_1 - Y_2, Y_2 - Y_1)$ and $F' \coloneqq F - (X_1 \cap X_2)$. If there exists an F'-avoiding $\mathcal{X}'$-$\mathcal{Y}'$ exchange sequence in $M/(X_1 \cap X_2)$ of width w and length ℓ, then there exists an F-avoiding $\mathcal{X}$-$\mathcal{Y}$ exchange sequence in M of width w and length ℓ. Furthermore, if $h \in E - (X_1 \cap X_2)$ is used in the last step of the $\mathcal{X}'$-$\mathcal{Y}'$ exchange sequence, then it can be assumed to be used in the last step of the $\mathcal{X}$-$\mathcal{Y}$ exchange sequence as well.*

Proof. Recall that (X_1, X_2) and (Y_1, Y_2) are compatible if $X_1 \cap X_2 = Y_1 \cap Y_2$ and $X_1 \cup X_2 = Y_1 \cup Y_2$. This implies that $\mathcal{X}'$ and $\mathcal{Y}'$ form compatible basis pairs of $M/(X_1 \cap X_2)$. As any sequence of symmetric exchanges that transforms $\mathcal{X}'$ into $\mathcal{Y}'$ also transforms $\mathcal{X}$ into $\mathcal{Y}$, the lemma follows. □

By the lemma, it suffices to consider instances where $X_1 \cap X_2 = Y_1 \cap Y_2 = \emptyset$. Furthermore, since the elements not contained in any of the bases cannot participate in exchanges and hence can be deleted, we can assume without loss of generality that $E = X_1 \cup X_2 = Y_1 \cup Y_2$ holds.

3.2. Excluding tight sets

Given a matroid M over ground set E, a set $Z \subseteq E$ is called *tight* if $|Z| = 2 \cdot r_M(Z)$. A tight set Z is called *nontrivial* if $\emptyset \neq Z \subsetneq E$. Nontrivial tight sets are special for the following reason: every partition $E = X_1 \cup X_2$ into two disjoint bases necessarily satisfies $|X_i \cap Z| = r_M(Z)$ for $i = 1, 2$. In other words, pairs of disjoint bases of M are exactly the pairs of disjoint bases of the matroid $M|Z \oplus_1 M/Z$. This observation allows us to reduce the size of the problem along a nontrivial tight set.

Lemma 3.2. *Let $\mathcal{X} = (X_1, X_2)$ and $\mathcal{Y} = (Y_1, Y_2)$ be compatible pairs of disjoint bases of a matroid M, $F \subseteq (X_1 \cap Y_1) \cup (X_2 \cap Y_2)$, and let $\emptyset \neq Z \subsetneq X_1 \cup X_2$ be a tight set. Define $F' := F \cap Z$, $F'' := F - Z$, $\mathcal{X}' := (X_1 \cap Z, X_2 \cap Z)$, $\mathcal{X}'' := (X_1 - Z, X_2 - Z)$, $\mathcal{Y}' := (Y_1 \cap Z, Y_2 \cap Z)$ and $\mathcal{Y}'' := (Y_1 - Z, Y_2 - Z)$. If there exists an F'-avoiding $\mathcal{X}'$-$\mathcal{Y}'$ exchange sequence in $M|Z$ of width w' and length ℓ' and an F''-avoiding $\mathcal{X}''$-$\mathcal{Y}''$ exchange sequence in M/Z of width w'' and length ℓ'', then there exists an F-avoiding $\mathcal{X}$-$\mathcal{Y}$ exchange sequence in M of width $\max\{w', w''\}$ and length $\ell' + \ell''$. Furthermore, if $h \in E$ is used in the last step of the $\mathcal{X}''$-$\mathcal{Y}''$ exchange sequence, then it can be assumed to be used in the last step of the $\mathcal{X}$-$\mathcal{Y}$ exchange sequence as well.*

Proof. By the definition of contraction, the concatenation of the two exchange sequences results in an $\mathcal{X}$-$\mathcal{Y}$ exchange sequence with the properties stated. □

If M is the 1-sum of matroids $M_\circ = (E_\circ, \mathcal{B}(M_\circ))$ and $M_\bullet = (E_\bullet, \mathcal{B}(M_\bullet))$, then $M|E_\circ = M_\circ$ and $M/E_\circ = M_\bullet$. Furthermore, the bases of M are exactly the unions of a basis of $M_\circ$ and a basis of $M_\bullet$. Hence, for any pair (X_1, X_2) of disjoint bases of M, the set $X_1^\circ \cup X_2^\circ$ is tight since $|X_1^\circ \cup X_2^\circ| = 2 \cdot r_{M_\circ}(X_1^\circ \cup X_2^\circ) = 2 \cdot r_M(X_1^\circ \cup X_2^\circ)$. Therefore, Lemma 3.2 implies the following.

Corollary 3.3. *Let $\mathcal{X} = (X_1, X_2)$ and $\mathcal{Y} = (Y_1, Y_2)$ be compatible pairs of disjoint bases of a matroid $M = M_\circ \oplus_1 M_\bullet$. Define $\mathcal{X}' := (X_1^\circ, X_2^\circ)$, $\mathcal{X}'' := (X_1^\bullet, X_2^\bullet)$, $\mathcal{Y}' := (Y_1^\circ, Y_2^\circ)$ and $\mathcal{Y}'' := (Y_1^\bullet, Y_2^\bullet)$. If there exists an $\mathcal{X}'$-$\mathcal{Y}'$ exchange sequence in $M_\circ$ of width w' and length ℓ' and an $\mathcal{X}''$-$\mathcal{Y}''$ exchange sequence in $M_\bullet$ of width w'' and length ℓ'', then there exists an $\mathcal{X}$-$\mathcal{Y}$ exchange sequence in M of width $\max\{w', w''\}$ and length $\ell' + \ell''$.*

3.3. Reduction to 3-connected matroids

When the matroid happens to be the 2-sum of matroids, the problem admits a reduction similar to the one used for tight sets. However, while merging the solutions to the subproblems was trivial for tight sets, it becomes much more involved for 2-sums. To get a better understanding of this difficulty, let X_1 and X_2 be disjoint bases of $M = M_\circ \oplus_2 M_\bullet$ where the 2-sum is along an element t. Assume that $X_1^\circ \in \mathcal{B}(M_\circ \backslash t)$ and $X_2^\circ \in \mathcal{B}(M_\circ / t)$. This implies that X_1° and $X_2^\circ + t$ are bases of $M_\circ$, and that $X_1^\bullet \in \mathcal{B}(M_\bullet / t)$ and $X_2^\bullet \in \mathcal{B}(M_\bullet \backslash t)$ by the definition of 2-sums. Consider a symmetric exchange $X_1^\circ - f + t, X_2^\circ + f$ between X_1° and $X_2^\circ + t$ in $M_\circ$. Then, unfortunately, this step does not correspond to a feasible symmetric exchange between X_1 and X_2 in M, since both $X_1^\circ - f \in \mathcal{B}(M_\circ / t)$ and $X_1^\bullet \in \mathcal{B}(M_\bullet / t)$.

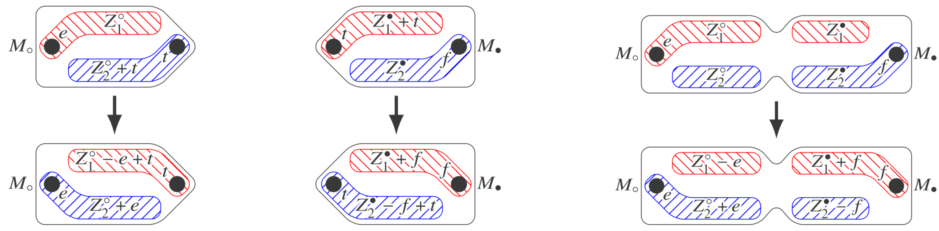
The main result of this section is to show that the exchanges can be scheduled on the two sides of the 2-sum in a way that avoids the problem described above. The next lemma, when used in conjunction with Lemma 3.2, eventually reduces the problem to the case of 3-connected matroids.

Lemma 3.4. *Let $\mathcal{X} = (X_1, X_2)$ and $\mathcal{Y} = (Y_1, Y_2)$ be compatible pairs of disjoint bases of a matroid $M = M_\circ \oplus_2 M_\bullet$ where the 2-sum is along an element t. For $i = 1, 2$, set $X'_i \coloneqq X^\circ_i, X''_i \coloneqq X^\bullet_i + t$ if $X^\circ_i \in \mathcal{B}(M_\circ \backslash t)$ and $X'_i \coloneqq X^\circ_i + t, X''_i \coloneqq X^\bullet_i$ otherwise, and $Y'_i \coloneqq Y^\circ_i, Y''_i \coloneqq Y^\bullet_i + t$ if $Y^\circ_i \in \mathcal{B}(M_\circ \backslash t)$ and $Y'_i \coloneqq Y^\circ_i + t, Y''_i \coloneqq Y^\bullet_i$ otherwise. Define $\mathcal{X}' \coloneqq (X'_1, X'_2)$, $\mathcal{X}'' \coloneqq (X''_1, X''_2)$, $\mathcal{Y}' \coloneqq (Y'_1, Y'_2)$ and $\mathcal{Y}'' \coloneqq (Y''_1, Y''_2)$. If there exists an $\mathcal{X}'$-$\mathcal{Y}'$ exchange sequence in $M_\circ$ of width w' and length ℓ' and an $\mathcal{X}''$-$\mathcal{Y}''$ exchange sequence in $M_\bullet$ of width w'' and length ℓ'', then there exists an $\mathcal{X}$-$\mathcal{Y}$ exchange sequence in M of width at most $w' + w''$ and length at most $\ell' + \ell'' - 1$ if both exchange sequences involve t and $\ell' + \ell''$ otherwise.*

Proof. Using the description of $\mathcal{B}(M_\circ \oplus_2 M_\bullet)$, we may assume that $X^\circ_1 \in \mathcal{B}(M_\circ \backslash t)$ and $X^\bullet_1 \in \mathcal{B}(M_\bullet / t)$. If $X^\circ_2 \in \mathcal{B}(M_\circ \backslash t)$, then $X^\circ_1 \cup X^\circ_2$ is a tight set in M and the statement follows from Lemma 3.2. Otherwise, $X^\circ_2 \in \mathcal{B}(M_\circ / t)$ and thus $X^\bullet_2 \in \mathcal{B}(M_\bullet \backslash t)$. We prove the lemma in two steps.

First, consider the case when the $\mathcal{X}'$-$\mathcal{Y}'$ exchange sequence in $M_\circ$ does not involve the element t. Note that in this case $\mathcal{X}' = (X^\circ_1, X^\circ_2 + t)$, $\mathcal{X}'' = (X^\bullet_1 + t, X^\bullet_2)$, $\mathcal{Y}' = (Y^\circ_1, Y^\circ_2 + t)$ and $\mathcal{Y}'' = (Y^\bullet_1 + t, Y^\bullet_2)$. We construct an $\mathcal{X}$-$\mathcal{Y}$ exchange sequence as follows. We start with the steps of the $\mathcal{X}'$-$\mathcal{Y}'$ exchange sequence, which transform $\mathcal{X} = (X_1, X_2)$ into the basis pair $(Y^\circ_1 \cup X^\bullet_1, Y^\circ_2 \cup X^\bullet_2)$. By the symmetric exchange axiom, there exists $e \in Y^\circ_1 - (Y^\circ_2 + t)$ such that $Y^\circ_1 - e + t, Y^\circ_2 + e \in \mathcal{B}(M_\circ)$. From this point, we perform the steps of the $\mathcal{X}''$-$\mathcal{Y}''$ exchange sequence, but whenever a symmetric exchange uses t and some other element f, then exchange e and f instead. Formally, if a symmetric exchange transforms $(Z^\bullet_1 + t, Z^\bullet_2)$ into $(Z^\bullet_1 + f, Z^\bullet_2 - f + t)$, then this is replaced by the symmetric exchange that transforms $(Y^\circ_1 \cup Z^\bullet_1, Y^\circ_2 \cup Z^\bullet_2)$ into $((Y^\circ_1 - e) \cup (Z^\bullet_1 + f), ((Y^\circ_2 + e) \cup (Z^\bullet_2 - f))$ in M. Similarly, if a symmetric exchange transforms $(Z^\bullet_1, Z^\bullet_2 + t)$ into $(Z^\bullet_1 - f + t, Z^\bullet_2 + f)$, then this step is replaced by the symmetric exchange that transforms $((Y^\circ_1 - e) \cup Z^\bullet_1, (Y^\circ_2 + e) \cup Z^\bullet_2)$ into $(Y^\circ_1 \cup (Z^\bullet_1 - f), Y^\circ_2 \cup (Z^\bullet_2 + f))$. In both cases, the pair obtained consists of disjoint bases of M due to the choice of e. It is not difficult to check that at the end of the procedure, we arrive at the basis pair (Y_1, Y_2). The $\mathcal{X}$-$\mathcal{Y}$ exchange sequence thus obtained has width at most $w' + w''$ and length $\ell' + \ell''$.

By symmetry, it remains to consider the case when both the $\mathcal{X}'$-$\mathcal{Y}'$ exchange sequence in $M_\circ$ and the $\mathcal{X}''$-$\mathcal{Y}''$ exchange sequence in $M_\bullet$ use the element t at least once. Let m' and m'' denote the number of occurrences of t in these sequences; we may assume that $m' < m''$. We construct an $\mathcal{X}$-$\mathcal{Y}$ exchange sequence as follows. We perform the steps of both the $\mathcal{X}'$-$\mathcal{Y}'$ and $\mathcal{X}''$-$\mathcal{Y}''$ exchange sequences, but we align the exchanges involving t on both sides, see Fig. 2. Formally, we always perform the steps of the $\mathcal{X}'$-$\mathcal{Y}'$ exchange sequence until we reach the next step that involves t, say, transforms a basis pair $(Z^\circ_1, Z^\circ_2 + t)$ into $(Z^\circ_1 - e + t, Z^\circ_2 + e)$. From this point, we perform the steps of the $\mathcal{X}''$-$\mathcal{Y}''$ exchange sequence until we reach the next step that involves t, say, transforms $(Z^\bullet_1 + t, Z^\bullet_2)$ into $(Z^\bullet_1 + f, Z^\bullet_2 - f + t)$. Then these two steps are replaced by the symmetric exchange that transforms $(Z^\circ_1 \cup Z^\bullet_1, Z^\circ_2 \cup Z^\bullet_2)$ into $((Z^\circ_1 - e) \cup (Z^\bullet_1 + f), (Z^\circ_2 + e) \cup (Z^\bullet_2 - f))$ in M. Once there are no more steps using t on the side of $M_\circ$, the exchange sequence can



(a) A step of the $\mathcal{X}'$-$\mathcal{Y}'$ exchange sequence transforming $(Z_1^\circ, Z_2^\circ + t)$ into $(Z_1^\circ - e + t, Z_2^\circ + e)$.

(b) A step of the $\mathcal{X}''$-$\mathcal{Y}''$ exchange sequence transforming $(Z_1^\bullet + t, Z_2^\bullet)$ into $(Z_1^\bullet + f, Z_2^\bullet - f + t)$.

(c) The corresponding step of the $\mathcal{X}$-$\mathcal{Y}$ exchange sequence transforming $(Z_1^\circ \cup Z_1^\bullet, Z_2^\circ \cup Z_2^\bullet)$ into $((Z_1^\circ - e) \cup (Z_1^\bullet + f), (Z_2^\circ + e) \cup (Z_2^\bullet - f))$.

Fig. 2. Illustration of Lemma 3.4, where steps of the $\mathcal{X}'$-$\mathcal{Y}'$ and $\mathcal{X}''$-$\mathcal{Y}''$ exchange sequences involving t are combined to obtain a step of the $\mathcal{X}$-$\mathcal{Y}$ exchange sequence.

be finished as discussed in the previous case. The $\mathcal{X}$-$\mathcal{Y}$ exchange sequence thus obtained has width at most $w' + w''$ and length $\ell' + \ell'' - m' \leq \ell' + \ell'' - 1$. □

3.4. Excluding cocircuits of size three

Recall that a triad is a cocircuit of size three. Let M be a matroid, $\mathcal{X} = (X_1, X_2)$ and $\mathcal{Y} = (Y_1, Y_2)$ be compatible pairs of disjoint bases of M, and $T = \{t_1, t_2, t_3\}$ be a triad of M such that $T \subseteq X_1 \cup X_2 = Y_1 \cup Y_2$. The pairs $\mathcal{X}$ and $\mathcal{Y}$ are called *consistent on* T if $X_1 \cap T = Y_1 \cap T$ or $X_1 \cap T = Y_2 \cap T$, that is, the bases in $\mathcal{X}$ partition the elements of T the same way as the bases in $\mathcal{Y}$. We will use the following simple technical claim.

Claim 3.5. *Let $\mathcal{X} = (X_1, X_2)$ be a pair of disjoint bases of a matroid M and $T = \{t_1, t_2, t_3\} \subseteq X_1 \cup X_2$ be a triad of M such that $|X_1 \cap T| = 2$. Then, $((X_1 - T) + \{t_i, t_j\}, (X_2 - T) + t_k)$ forms a pair of disjoint bases for at least two choices of indices satisfying $\{i, j, k\} = \{1, 2, 3\}$.*

Proof. Without loss of generality, we may assume that $t_1, t_2 \in X_1$. Since X_1 is a basis of M, $X_1 + t_3$ contains a unique circuit C. By Lemma 2.1, the intersection of C and T has size different from one, hence $C \cap \{t_1, t_2\} \neq \emptyset$. We may assume that $t_1 \in C$, implying $X_1 - t_1 + t_3$ being a basis. It remains to show that $X_2 + t_1 - t_3$ is also a basis. Suppose to the contrary that this does not hold, that is, $X_2 + t_1 - t_3$ contains a circuit C'. Then, by $X_2 \cap T = \{t_3\}$, we get $C' \cap T = \{t_1\}$, contradicting Lemma 2.1. □

First, we show that if the basis pairs $\mathcal{X}, \mathcal{Y}$ are not consistent on a triad T, then one can obtain pairs $\mathcal{X}', \mathcal{Y}'$ that are consistent on T at the cost of at most two symmetric exchanges.

Lemma 3.6. *Let $\mathcal{X} = (X_1, X_2)$ and $\mathcal{Y} = (Y_1, Y_2)$ be compatible pairs of disjoint bases of a matroid M that are not consistent on a triad $T = \{t_1, t_2, t_3\} \subseteq X_1 \cup X_2$. Then, there exist compatible pairs of disjoint bases $\mathcal{X}' = (X_1', X_2')$ and $\mathcal{Y}' = (Y_1', Y_2')$ that are* *consistent on T, obtained by applying at most one symmetric exchange to $\mathcal{X}$ and to $\mathcal{Y}$, respectively, where only elements of T are involved in these symmetric exchanges.*

Proof. Define $\mathcal{P}_1 \coloneqq \{((X_1-T)+\{t_i,t_j\},(X_2-T)+t_k) \mid \{i,j,k\}=\{1,2,3\}\}$ if $|X_1\cap T|=2$ and $\mathcal{P}_1 \coloneqq \{((X_1-T)+t_i,(X_2-T)+\{t_j,t_k\}) \mid \{i,j,k\}=\{1,2,3\}\}$ otherwise. Observe that each member of $\mathcal{P}_1$ can be obtained from $\mathcal{X}$ by exchanging at most one pair of elements; however, this might not be a feasible symmetric exchange. Similarly, define $\mathcal{P}_2 \coloneqq \{((Y_1-T)+\{t_i,t_j\},(Y_2-T)+t_k) \mid \{i,j,k\}=\{1,2,3\}\}$ if $|Y_1\cap T|=2$ and $\mathcal{P}_2 \coloneqq \{((Y_1-T)+t_i,(Y_2-T)+\{t_j,t_k\}) \mid \{i,j,k\}=\{1,2,3\}\}$ otherwise. Observe that each member of $\mathcal{P}_2$ can be obtained from $\mathcal{Y}$ by exchanging at most one pair of elements; again, this might not be a feasible symmetric exchange.

By Claim 3.5, at least two members of $\mathcal{P}_1$ and at least two members of $\mathcal{P}_2$ consist of disjoint bases. Therefore, there exist $\mathcal{X}'\in\mathcal{P}_1$ and $\mathcal{Y}'\in\mathcal{P}_2$ that are consistent on T, concluding the proof of the lemma. □

Once the basis pairs are consistent on a triad, the problem size can be decreased by contracting and deleting appropriate elements of the triad.

Lemma 3.7. *Let $\mathcal{X}=(X_1,X_2)$ and $\mathcal{Y}=(Y_1,Y_2)$ be compatible pairs of disjoint bases of a matroid M that are consistent on a triad $T=\{t_1,t_2,t_3\}\subseteq X_1\cup X_2$ where $t_1,t_2\in X_1$, and let $F\subseteq((X_1\cap Y_1)\cup(X_2\cap Y_2))-T$. Define $\mathcal{X}' \coloneqq (X_1-t_2,X_2-t_3)$, and set $\mathcal{Y}' \coloneqq (Y_1-t_2,Y_2-t_3)$ if $t_1,t_2\in Y_1$ and $\mathcal{Y}' \coloneqq (Y_1-t_3,Y_2-t_2)$ otherwise. If there exists an F-avoiding $\mathcal{X}'$-$\mathcal{Y}'$ exchange sequence in $M/t_2\backslash t_3$ of width w and length ℓ, then there exists an F-avoiding $\mathcal{X}$-$\mathcal{Y}$ exchange sequence in M of width w and length at most $\ell+w$. Furthermore, if $h\in E-(T\cup F)$ is used in the last step of the $\mathcal{X}'$-$\mathcal{Y}'$ exchange sequence, then it can be assumed to be used in the last step of the $\mathcal{X}$-$\mathcal{Y}$ exchange sequence as well.*

Proof. For any pair of disjoint bases $\mathcal{Z}=(Z_1,Z_2)$ of $M/t_2\backslash t_3$, we denote by $\mathcal{Z}^+=(Z_1,Z_2)^+=(Z_1^+,Z_2^+)$ the pair where, for $i=1,2$, $Z_i^+ \coloneqq Z_i+t_2$ if $t_1\in Z_i$ and $Z_i^+ \coloneqq Z_i+t_3$ otherwise. Observe that $\mathcal{Z}^+$ is a pair of disjoint bases of M. Indeed, $Z_i^+=Z_i+t_2$ is a basis of M by the definition of contraction. If $t_1\notin Z_i$, then $Z_i+\{t_2,t_3\}$ contains a unique circuit C that contains t_3. By Lemma 2.1, the intersection of C and T cannot have size one, hence $t_2\in C$ as well, showing that Z_i+t_3 is a basis of M.

Fix an F-avoiding $\mathcal{X}'$-$\mathcal{Y}'$ exchange sequence in $M/t_2\backslash t_3$ of length ℓ and width w. The idea is to add certain extra steps to obtain a solution to the original instance. Consider a symmetric exchange in the sequence that transforms (Z_1,Z_2) into (Z_1-e+f,Z_2-f+e). Without loss of generality, we may assume that $t_1\in Z_1$. If e is distinct from t_1, then $(Z_1,Z_2)^+=(Z_1+t_2,Z_2+t_3)$ and $(Z_1-e+f,Z_2-f+e)^+=(Z_1-e+\{t_2,f\},Z_2-f+\{t_3,e\})$, hence these pairs also differ in a single symmetric exchange in M. However, if $e=t_1$ then $(Z_1,Z_2)^+=(Z_1+t_2,Z_2+t_3)$ and $(Z_1-t_1+f,Z_2-f+t_1)^+=(Z_1-t_1+\{t_3,f\},Z_2-f+\{t_1,t_2\})$, and these pairs cannot be obtained from each other by a single symmetric exchange. In this case, consider the pairs (Z_1+t_3,Z_2+t_2) and $(Z_1-t_1+\{t_2,t_3\},Z_2+t_1)$.

By Claim 3.5, at least one of these pairs consists of disjoint bases of M. Furthermore, any of them can be obtained from both $(Z_1, Z_2)^+$ and $(Z_1 - t_1 + f, Z_2 - f + t_1)^+$ by using a single symmetric exchange.

Summarizing the above, a symmetric exchange of elements e and f in the $\mathcal{X}'$-$\mathcal{Y}'$ exchange sequence is left unchanged if $e, f \neq t_1$. Otherwise, if, say, $e = t_1$, it is replaced by two steps: the first exchanging t_1 and t_i and the second exchanging t_j and f for some appropriate choice of i and j satisfying $\{i, j\} = \{2, 3\}$. Observe that these modifications do not increase the usage of an element in $E - \{t_2, t_3\}$, hence the width of the new sequence is also w. Furthermore, the length of the sequence increases by the number of symmetric exchanges involving t_1, hence the length of the new sequence is at most $\ell + w$. Finally, note that the new sequence is F-avoiding as well, and its last step uses the elements of $E - (T \cup F)$ that were involved in the last step of the $\mathcal{X}'$-$\mathcal{Y}'$ exchange sequence, thus concluding the proof of the lemma. □

The two lemmas allow us to reduce the problem size if the matroid contains a triad. Indeed, the basis pairs can be made consistent on any triad with the help of Lemma 3.6, which requires at most two symmetric exchanges. Once the basis pairs are consistent on a triad, we can decrease the number of elements as in Lemma 3.7. If the exchange sequence in the reduced instance has width w and length ℓ, then we get an exchange sequence of width $w + 2$ and length $\ell + w + 2$ for the original instance.

3.5. Algorithmic aspects

The preprocessing steps discussed in the previous subsections do not only reduce the problem size in a theoretical sense, but are also algorithmically tractable if the matroid M is given by an independence oracle. Recall that a 1-sum or 2-sum decomposition of M can be determined, if exists, efficiently. Thus it suffices to show that one can find a triad or a tight set of a matroid using a polynomial number of oracle calls.

By definition, a triad is a cocircuit of size three, or equivalently, a circuit of size three of the dual matroid. Since an independence oracle of the dual matroid can be implemented using the independence oracle of M, the existence of such a circuit can be decided by checking every 3-elements subset of the ground set.

Assume now that the ground set of M is the disjoint union of two bases, say X_1 and X_2. Then for any set Z, we have $2 \cdot r_M(Z) \geq |X_1 \cap Z| + |X_2 \cap Z| = |Z|$, and equality holds if and only if Z is tight. Hence to decide whether $X_1 \cup X_2$ properly contains a nonempty tight set of M, it suffices to minimize the submodular function $f(Z) := r_M(Z) - |Z|/2$ over the sets $\emptyset \neq Z \subsetneq X_1 \cup X_2$, which can be performed in strongly polynomial time if given access to the independence oracle [12].

Finally, we show that the width and length bounds of Lemma 3.1, Lemma 3.2, Lemma 3.4, Lemma 3.6 and Lemma 3.7 are consistent with the statement of Theorem 1.1. Before that, we need the following simple observation.

Claim 3.8. *Let $\mathcal{X} = (X_1, X_2)$ and $\mathcal{Y} = (Y_1, Y_2)$ be compatible basis pairs of a matroid M of rank $r \leq 2$, $F \subseteq (X_1 \cap Y_1) \cup (X_2 \cap Y_2)$. Then there exists an F-avoiding $\mathcal{X}$-$\mathcal{Y}$ exchange sequence of width at most 1 and length at most r. Furthermore, if $h \in (X_1 \cup X_2) - F$, then the last step of the sequence can be assumed to use h.*

Proof. The claim is straightforward to check for matroids of rank at most two. □

With the help of the claim, we are now ready to prove that the inverse operations of the reduction steps preserve the quadratic running time. Since 2-sum behaves differently for F-avoiding exchange sequences than the other operations, we do this in the form of two corollaries. Moreover, we state the corollaries parameterized by a constant $c \geq 1$; the reason is that we will choose c to be 1 for graphic matroids and 2 for general regular matroids. For nondisjoint bases, tight sets, and triads, we get the following.

Corollary 3.9. *Let $\mathcal{X} = (X_1, X_2)$ and $\mathcal{Y} = (Y_1, Y_2)$ be compatible pairs of bases of a matroid $M = (E, \mathcal{I})$ of rank $r \geq 3$ and let $F \subseteq (X_1 \cap Y_1) \cup (X_2 \cap Y_2)$. Assume that for any minor $M' = (E', \mathcal{I}')$ of M and for any pair $\mathcal{X}' = (X_1', X_2'), \mathcal{Y}' = (Y_1', Y_2')$ of compatible pairs of disjoint bases of M' with $F' \coloneqq F \cap E' \subseteq (X_1' \cap Y_1') \cup (X_2' \cap Y_2')$, there exists an F'-avoiding $\mathcal{X}'$-$\mathcal{Y}'$ exchange sequence in M' of width at most $2 \cdot c \cdot (r' - 1)$ and length at most $c \cdot r'^2$, where $2 \leq r' < r$ is the rank of M' and $c \geq 1$. If either $X_1 \cap X_2 \neq \emptyset$, M has a tight set $\emptyset \neq Z \subsetneq X_1 \cup X_2$, or M has a triad $T \subseteq (X_1 \cup X_2) - F$, then there exists an F-avoiding $\mathcal{X}$-$\mathcal{Y}$ exchange sequence in M of width at most $2 \cdot c \cdot (r - 1)$ and length at most $c \cdot r^2$.*

Proof. If $X_1 \cap X_2 \neq \emptyset$, then let r' denote the rank of $M/(X_1 \cap X_2)$. Note that $r' < r$ holds. Our assumption, Claim 3.8, and Lemma 3.1 then imply the existence of an F-avoiding $\mathcal{X}$-$\mathcal{Y}$ exchange sequence of width at most $\max\{1, 2 \cdot c \cdot (r' - 1)\} < 2 \cdot c \cdot (r - 1)$ and length at most $\max\{1, c \cdot r'^2\} < c \cdot r^2$.

Otherwise, $X_1 \cap X_2 = Y_1 \cap Y_2 = \emptyset$. If $\emptyset \neq Z \subsetneq X_1 \cup X_2$ is a tight set, then let r' and r'' denote the ranks of $M|Z$ and M/Z, respectively. Note that $r = r' + r''$ holds. Our assumption, Claim 3.8, and Lemma 3.2 then imply the existence of an F-avoiding $\mathcal{X}$-$\mathcal{Y}$ exchange sequence of width at most $\max\{\max\{1, 2 \cdot c \cdot (r' - 1)\}, \max\{1, 2 \cdot c \cdot (r'' - 1)\}\} < 2 \cdot c \cdot (r - 1)$ and length at most $\max\{1, c \cdot r'^2\} + \max\{1, c \cdot r''^2\} < c \cdot r^2$.

If $T = \{t_1, t_2, t_3\} \subseteq (X_1 \cup X_2) - F$ is a triad of M, then let r' denote the rank of $M/t_2 \backslash t_3$. Note that $r' = r - 1 \geq 2$ holds. Our assumption, Claim 3.8, Lemma 3.6 and Lemma 3.7 then imply the existence of an F-avoiding $\mathcal{X}$-$\mathcal{Y}$ exchange sequence of width at most $2 \cdot c \cdot (r' - 1) + 2 \leq 2 \cdot c \cdot (r - 1)$ and length at most $c \cdot r'^2 + 2 \cdot c \cdot (r' - 1) + 2 \leq c \cdot r^2$, where the $+2$ terms come from the steps needed to make the basis pairs consistent on T, as explained in Lemma 3.6. □

For 2-sums, we get the following.

Corollary 3.10. *Let $\mathcal{X} = (X_1, X_2)$ and $\mathcal{Y} = (Y_1, Y_2)$ be compatible pairs of disjoint bases of a matroid M of rank $r \geq 3$ where M contains no nontrivial tight set. Assume that for any minor M' of M and for any pair $\mathcal{X}', \mathcal{Y}'$ of compatible pairs of disjoint bases of M', there exists an $\mathcal{X}'$-$\mathcal{Y}'$ exchange sequence in M' of width at most $2 \cdot c \cdot (r' - 1)$ and length at most $c \cdot r'^2$, where $2 \leq r' < r$ is the rank of M' and $c \geq 1$. If M is the 2-sum of two matroids, then there exists an $\mathcal{X}$-$\mathcal{Y}$ exchange sequence in M of width at most $2 \cdot c \cdot (r - 1)$ and length at most $c \cdot r^2$.*

Proof. If $M = M_\circ \oplus_2 M_\bullet$, then both $M_\circ$ and $M_\bullet$ are minors of M [36, Proposition 7.1.21]. Let r' and r'' denote the ranks of $M_\circ$ and $M_\bullet$, respectively. Note that $r = r' + r'' - 1$ holds. Moreover, we claim that $r', r'' \geq 2$. Indeed, e.g. $r' \geq 1$ and $|E_\circ| \geq 3$ hold by the definition of 2-sums, and $r' = 1$ would imply that M contains a nontrivial tight set. Our assumption and Lemma 3.4 then imply the existence of an $\mathcal{X}$-$\mathcal{Y}$ exchange sequence of width at most $2 \cdot c \cdot (r' - 1) + 2 \cdot c \cdot (r'' - 1) = 2 \cdot c \cdot (r - 1)$ and length at most $c \cdot r'^2 + c \cdot r''^2 \leq c \cdot r^2$. $\square$

4. Bounding the number of exchanges for graphs

White's conjecture was settled for graphic matroids in [17] for sequences of length two, and in [9] for sequences of arbitrary length. Both results rely on the same algorithm, and in fact imply Gabow's conjecture as well for the graphic case. However, neither discusses the length of the resulting exchange sequence.

The goal of this section is to prove strengthenings of Theorem 1.1 and Theorem 1.2 for graphs. Due to the fact that most of the work has already been done in Section 3, the proofs are simple and compact. Throughout the section, we use the fact that every minor of a graphic matroid is graphic again without explicitly mentioning it.

4.1. Quadratic upper bound

We give the first polynomial bound on the exchange distance of compatible basis pairs in graphic matroids. In addition, through an analysis of the degree sequences of graphs that can be partitioned into two forests, we show how to exclude certain edges to participate in the exchange sequence. This observation plays a key role in the proof of Theorem 1.1: when considering the 3-sum of a regular and a graphic matroid along a triad T, one can solve the two subproblems corresponding to the two sides of the 3-sum while restricting the usage of the elements of T, which in turn allows for an efficient merging of the sequences.

Theorem 4.1. *Let $\mathcal{X} = (X_1, X_2)$ and $\mathcal{Y} = (Y_1, Y_2)$ be compatible pairs of bases of a graphic matroid M of rank $r \geq 2$ where the underlying graph is $G = (V, E)$, and let $F \subseteq (X_1 \cap Y_1) \cup (X_2 \cap Y_2)$ be such that $|V(F)| \leq 3$. Then, there exists an F-avoiding $\mathcal{X}$-$\mathcal{Y}$ exchange sequence of width at most $2 \cdot (r - 1)$ and length at most r^2.*

(a) The pair $\mathcal{X} = (X_1, X_2)$ of disjoint bases of M. (b) The pair $\mathcal{Y} = (Y_1, Y_2)$ of disjoint bases of M.

Fig. 3. Example showing that Theorem 4.1 no longer holds if F consists of a pair of disjoint edges. For the choice $F = \{b, e\} \subseteq (X_1 \cap Y_1) \cup (X_2 \cap Y_2)$, every $\mathcal{X}$-$\mathcal{Y}$ exchange sequence uses at least one of b and e.

Proof. We prove the theorem by induction on the rank. For $r = 2$, the statement holds by Claim 3.8. Therefore, we consider the case $r \geq 3$, implying that $|V| \geq 4$. Since the elements not contained in any of the bases cannot participate in an $\mathcal{X}$-$\mathcal{Y}$ exchange sequence, we may assume without loss of generality that $X_1 \cup X_2 = Y_1 \cup Y_2 = E$. That is, G is a graph whose edge set can be partitioned into two forests. Furthermore, by the induction hypothesis and Corollary 3.9, we may assume that $X_1 \cap X_2 = Y_1 \cap Y_2 = \emptyset$. If there are isolated vertices in the graph, then those can be deleted without changing the problem. Since E can be partitioned into two forests, we have $\sum_{v \in V} d(v) = 2 \cdot |E| \leq 4 \cdot (|V| - 1)$. This implies that G contains a vertex u of degree at most 3. Since both forests are bases in the graphic matroid, those are maximal forests, implying that $d(u) \geq 2$.

Assume first that G has a vertex u of degree 2. Then u is a leaf vertex in both X_1 and X_2, implying $r_M(E - \delta(u)) = r_M(E) - 1$. Since $|E| = 2 \cdot r_M(E)$, we get $|E - \delta(u)| = |E| - 2 = 2 \cdot r_M(E) - 2 = 2 \cdot r_M(E - \delta(u))$. That is, $\emptyset \neq E - \delta(u) \subsetneq E$ is a tight set, and the statement follows by the induction hypothesis and Corollary 3.9.

If G contains no vertex of degree 2, then it has at least four vertices of degree 3. By condition $|V(F)| \leq 3$, there exists a vertex u such that $d(u) = 3$ and $\delta(u) \cap F = \emptyset$. That is, $\delta(u)$ defines a triad of M disjoint from F, and the statement follows by the induction hypothesis and Corollary 3.9. $\square$

Remark 4.2. The assumption of Theorem 4.1 on $|V(F)| \leq 3$ is tight in the sense that an F-avoiding $\mathcal{X}$-$\mathcal{Y}$ exchange sequence might not exist, even if F consists of a pair of disjoint edges. For an example, let $\mathcal{X} = (\{a, b, c\}, \{d, e, f\})$ and $\mathcal{Y} = (\{b, d, f\}, \{a, c, e\})$ be pairs of disjoint bases of the graphic matroid of a complete graph on four vertices, see Fig. 3. Note that any symmetric exchange between $\{a, b, c\}$ and $\{d, e, f\}$ uses at least one of b and e. Therefore, for the choice $F = \{b, e\}$, there exists no F-avoiding $\mathcal{X}$-$\mathcal{Y}$ exchange sequence.

4.2. Strictly monotone sequences

Given compatible basis pairs $\mathcal{X}, \mathcal{Y}$ of a matroid, an $\mathcal{X}$-$\mathcal{Y}$ exchange sequence is called *strictly monotone* if each step decreases the difference between the first members of the pairs. Using this terminology, Conjecture 2 states that for any pair of disjoint bases X_1, X_2 of a matroid, there exists a strictly monotone exchange sequence between (X_1, X_2) and (X_2, X_1).

Theorem 4.3. *Let X_1, X_2 be disjoint bases of a graphic matroid M. Then, for any $h \in X_1 \cup X_2$, there exists a sequence of symmetric exchanges that transforms (X_1, X_2) into (X_2, X_1), has length r and exchanges h in the last step.*

Proof. Similarly to the proof of Theorem 4.1, we can assume that $X_1 \cup X_2 = Y_1 \cup Y_2 = E$, and hence G contains a vertex u of degree at most 3. Furthermore, if u has degree 2 then $E - \delta(u)$ is a nonempty proper tight set of M, while if $d(u) = 3$ then $\delta(u)$ is a triad of M. Therefore, the statement follows by the induction hypothesis, Claim 3.8, Lemma 3.2 and Lemma 3.7. □

Remark 4.4. Theorem 4.3 settles a special case of a conjecture of Kotlar and Ziv that aims at extending the notion of serial symmetric exchanges to subsets of bases. Namely, suppose X_1 and X_2 are bases of a matroid M. Two subsets $A_1 \subseteq X_1$ and $A_2 \subset X_2$ are called *serially exchangeable* if there exist orderings $A_1 = \{a_1^1, \dots, a_q^1\}$ and $A_2 = \{a_1^2, \dots, a_q^2\}$ such that $X_1 - \{a_1^1, \dots, a_i^1\} + \{a_1^2, \dots, a_i^2\}$ and $X_2 - \{a_1^2, \dots, a_i^2\} + \{a_1^1, \dots, a_i^1\}$ are bases for $i = 1, \dots, q$. Kotlar and Ziv [28] conjectured that for any $A \subseteq X_1$, there exists a set $B \subseteq X_2$ for which A and B are serially exchangeable. Note that this conjecture implies Gabow's conjecture.

As a relaxation, a matroid has the *k-serial exchange property* for some positive integer k if for any two bases X_1, X_2 and any subset $A_1 \subseteq X_1$ of size k, there is a subset $A_2 \subseteq X_2$ for which A_1 and A_2 are serially exchangeable. It was shown in [28] that every matroid has the 2-serial exchange property. Kotlar [27] further verified that for matroids of rank at least three, for any two bases X_1, X_2 there exist $A_1 \subseteq X_1$ and $A_2 \subseteq X_2$ such that $|A_1| = |A_2| = 3$ and A_1 and A_2 are serially exchangeable. Recently, McGuinness [33] showed that all binary matroids of rank at least three have the 3-serial exchange property. However, it is still unknown whether all matroids of rank at least three have the 3-exchange property.

Using this terminology, the statement of Theorem 4.3 is equivalent to the $(r-1)$-serial exchange property of graphic matroids.

5. Finding a sequence of exchanges in polynomial time

This section is dedicated to the proofs of Theorem 1.1 and Theorem 1.2.

5.1. Preparations

For proving the theorems, we need some preliminary observations. We first discuss the structure of bispanning graphs, and characterize their partitions into disjoint spanning trees in terms of intersections with a triangle. We then verify the theorems for the matroid

R_{10}, and prove an analogous result to F_7 as well. Recall that the matroid R_{10} is one of the basic building blocks of regular matroids, while F_7 is considered here to extend our results to max-flow min-cut matroids, see Section 6. Finally, we show that it suffices to consider the problem for matroids that arise as the 3-sum of a regular matroid and the graphic matroid of a 4-regular graph.

5.1.1. Partitions of bispanning graphs

Binary matroids have distinguished structural properties, which implies the following.

Lemma 5.1. *Let $T = \{t_1, t_2, t_3\}$ be a triangle of a binary matroid M on ground set E. Then, the following are equivalent:*

(i) $E - T$ partitions into a basis of M and a basis of M/T,
(ii) $E - t_i$ partitions into two bases of M for each $i \in \{1, 2, 3\}$,
(iii) $|E| = 2 \cdot r_M(E) + 1$ and $|X| \leq 2 \cdot r_M(X)$ holds if $T \not\subseteq X \subseteq E$.

Proof. Condition (i) implies (ii), since if $E-T = B \cup B'$ is a partition such that $B \in \mathcal{B}(M)$ and $B' \in \mathcal{B}(M/T)$, then $E - t_i = B \cup (B' + T - t_i)$ is a partition into two bases of M for $i \in \{1, 2, 3\}$.

Condition (ii) is equivalent to (iii), since $E - t_i$ partitions into two bases of M if and only if $|E - t_i| = 2 \cdot r_M(E)$ and $|X| \leq 2 \cdot r_M(X)$ holds for $X \subseteq E - t_i$.

It remains to show that (iii) implies (i). Since $r_M(E) + r_{M/T}(E) = 2 \cdot r_M(E) - 2 = |E| - 3 = |E - T|$, it is enough to show that $E - T$ is independent in the sum of the matroids M and M/T, which is equivalent to $r_M(X) + r_{M/T}(X) \geq |X|$ for every $X \subseteq E - T$. Since $r_{M/T}(X) = r_M(X \cup T) - r_M(T) = r_M(X \cup T) - 2$, it suffices to show that

$$r_M(X) + r_M(X \cup T) \geq |X| + 2 \text{ for } X \subseteq E - T.$$

If $r_M(X \cup T) = r_M(X)$, then $r_M(X) + r_M(X \cup T) = 2 \cdot r_M(X + t_1 + t_2) \geq |X + t_1 + t_2| = |X| + 2$. If $r_M(X \cup T) = r_M(X) + 2$, then the desired inequality follows from $2 \cdot r_M(X) \geq |X|$. It remains to consider the case $r_M(X \cup T) = r_M(X) + 1$. Then, M being binary implies that X spans at least one of t_1, t_2 and t_3. Indeed, if X does not span t_1 or t_2, then $r_M(X + t_1 + t_2) = r_M(X) + 1$ implies that there is a circuit $C \subseteq X + t_1 + t_2$ containing both t_1 and t_2, thus $C \triangle T \subseteq X + t_3$ is a cycle containing t_3, hence X spans t_3. If X spans t_i, then

$$r_M(X) + r_M(X \cup T) = 2 \cdot r_M(X) + 1 = 2 \cdot r_M(X + t_i) + 1 \geq |X + t_i| + 1 = |X| + 2,$$

concluding the proof of the lemma. □

Remark 5.2. We note that (ii) does not necessarily imply (i) for nonbinary matroids. For example, consider the matroid on ground set $\{e_1, e_2, t_1, t_2, t_3\}$ in which e_1 and e_2 are parallel and the matroid obtained by deleting e_1 is the rank-2 uniform matroid. Then, $\{e_1, t_j\}, \{e_2, t_k\}$ is a partition of $E - t_i$ into two bases of M for any choice of indices satisfying $\{i, j, k\} = \{1, 2, 3\}$. However, $E - T = \{e_1, e_2\}$ consists of parallel elements in M and of loops in M/T, hence it can not be decomposed into a basis of M and a basis of M/T.

We will use the following corollary of the lemma for graphic matroids.

Corollary 5.3. *Let $G = (V, E)$ be a graph and $T = \{t_1, t_2, t_3\}$ be the edge set of a triangle of G. Then, there exists a partition $E - T = F_1 \cup F_2$ such that $F_1 + \{t_1, t_2\}$ and F_2 are disjoint spanning trees of G if and only if $|E| = 2 \cdot |V| - 1$ and*

$$|E[U]| \leq \begin{cases} 2 \cdot |U| - 2 & \text{if } V(T) \nsubseteq U, \\ 2 \cdot |U| - 1 & \text{if } V(T) \subseteq U \end{cases}$$

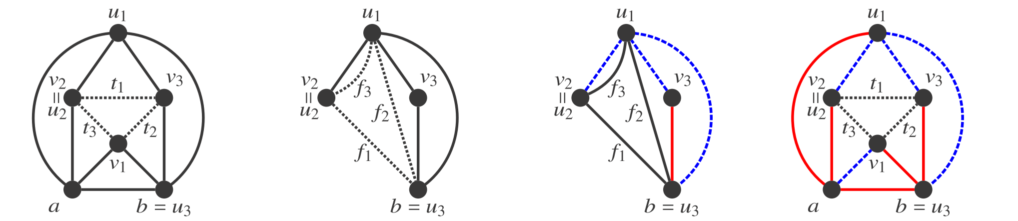
holds for each $\emptyset \neq U \subseteq V$.

Proof. By Nash-Williams' theorem [35], the graphs $G - t_1$, $G - t_2$, $G - t_3$ can each be decomposed into two spanning trees if and only if $|E| = 2 \cdot |V| - 1$, and the number of edges induced by any nonempty subset $U \subseteq V$ in each of the graphs is at most $2 \cdot |U| - 2$. The latter condition is equivalent to $|E[U]| \leq 2 \cdot |U| - 2$ if $V(T) \nsubseteq U$, and to $|E[U]| \leq 2 \cdot |U| - 1$ if $V(T) \subseteq U$. Therefore, the statement follows from the equivalence of Lemma 5.1(i) and Lemma 5.1(ii) applied to the graphic matroid of G. □

The proof of Theorem 1.1 will rely on the following lemma.

Lemma 5.4. *Let $G = (V, E)$ be a simple 4-regular graph and $T = \{t_1, t_2, t_3\}$ be the edge set of a triangle of G. Assume that $|(E - T)[U]| \leq 2 \cdot |U| - 3$ holds for each $U \subseteq V$ with $|U| \geq 2$. Then, there exists a partition $E - T = F_1 \cup F_2$ and an edge $e \in F_1$ such that each of F_1, $F_2 + t_2$, $F_2 + t_3$, $F_1 - e + t_2$, $F_1 - e + t_3$, and $F_2 + e$ is a spanning tree of G.*

Proof. Let v_1, v_2, and v_3 denote the vertices of T such that $t_1 = v_2v_3$, $t_2 = v_1v_3$, and $t_3 = v_1v_2$. We denote by a and b the neighbors of v_1 distinct from v_2 and v_3, and by u_1, u_2, and u_3 the neighbors of a distinct from v_1. Let f_i be a new edge between vertices $u_{i+1}u_{i+2}$, where indices are meant in a cyclic order. Let $G' = (V', E')$ denote the graph $G - \{v_1, a\} - t_1 + \{f_1, f_2, f_3\}$ (see Fig. 4 for an illustration). Note that $|E'| = |E| - 5 = 2 \cdot |V| - 5 = 2 \cdot |V'| - 1$. Consider a subset $U \subseteq V'$ with $|U| \geq 2$. If $\{u_1, u_2, u_3\} \nsubseteq U$, then $|E'[U]| \leq |(E - T)[U]| + 1 \leq 2 \cdot |U| - 2$, while if $\{u_1, u_2, u_3\} \subseteq U$, then $|E'[U]| = |(E - T)[U + a]| \leq 2 \cdot |U + a| - 3 = 2 \cdot |U| - 1$ holds. This shows that the conditions of Corollary 5.3 are satisfied, hence there exists a partition $E' - \{f_1, f_2, f_3\} = F_1' \cup F_2'$ such that $F_1' + \{f_2, f_3\}$ and F_2' are spanning trees of G'. Let $F_1 \coloneqq F_1' + \{au_1, au_2, au_3, v_1b\}$, $F_2 \coloneqq F_2' + v_1a$, $e \coloneqq v_1b$. Then $F_1 - e$ is a spanning tree of $G - v_1$, hence F_1, $F_1 - e + t_2$



(a) Graph $G = (V, E)$ and triangle $T = \{t_1, t_2, t_3\}$.
(b) Graph $G' = (V', E')$ with new edges f_1, f_2, f_3.
(c) Partition into F_1' (red) and F_2' (blue, dashed).
(d) Construction of F_1 (red) and F_2 (blue, dashed).

Fig. 4. Illustration of Lemma 5.4.

and $F_1 - e + t_3$ are spanning trees of G. Since F_2 is a forest such that v_1a is one of its two components, we get that $F_2 + t_3$, $F_2 + t_2$ and $F_2 + e$ are also spanning trees of G. □

5.1.2. Solving the problem for R_{10} and F_7

We now verify Theorem 1.1 and Theorem 1.2 for the matroid R_{10}. Recall that R_{10} is the binary matroid represented by a matrix $A \in GF(2)^{5\times 10}$ in which the columns are different and each of them contains exactly two zero entries.

Proposition 5.5. *R_{10} satisfies Theorem 1.1 and Theorem 1.2.*

Proof. Let $\mathcal{X} = (X_1, X_2)$ be a basis pair of R_{10}. It follows from Theorem 2.4 that each proper minor of R_{10} is graphic or cographic, hence we may assume that X_1 and X_2 are disjoint by Lemma 3.1.

We will use the representation of R_{10} as the even-cycle matroid of the complete graph K_5 on vertices $\{v_1, v_2, v_3, v_4, v_5\}$, see e.g. [36, page 238]. The ground set of this matroid is the edge set of K_5 and the circuits are the cycles of length four and the unions of two triangles having exactly one vertex in common. To get an isomorphism between this matroid and the binary matroid represented by A, map an edge v_iv_j to the column of A in which the ith and jth entries are zero, see Fig. 1b. The bases are the sets of five edges containing no even cycles and exactly one odd cycle of K_5. This implies that (Z_1, Z_2) is a basis pair for a partition $E = Z_1 \cup Z_2$ if and only if Z_1 is a 5-cycle of K_5 or $Z_1 = \{v_iv_j, v_iv_k, v_jv_k, v_jv_l, v_kv_m\}$ for some $\{i, j, k, l, m\} = \{1, 2, 3, 4, 5\}$. Observe that there is an isomorphism that maps a basis of the latter form into a 5-cycle, e.g. $(v_1v_2, v_1v_3, v_2v_3, v_2v_4, v_3v_5)$ can be mapped to $(v_1v_3, v_1v_2, v_4v_5, v_2v_4, v_3v_5)$ by mapping $(v_1v_4, v_1v_5, v_2v_5, v_3v_4, v_4v_5)$ to $(v_1v_5, v_1v_4, v_2v_5, v_3v_4, v_2v_3)$. Therefore, to prove Theorems 1.1 and 1.2 for R_{10}, we may assume that X_1 is a 5-cycle. Fig. 5 illustrates that each pair of disjoint bases of R_{10} is reachable from this basis pair with at most 5 exchanges. □

Though it is not needed in the proof of Theorem 1.1 and Theorem 1.2, we verify analogous statements for the Fano matroid as well. This will allow us to extend our results to max-flow min-cut matroids.

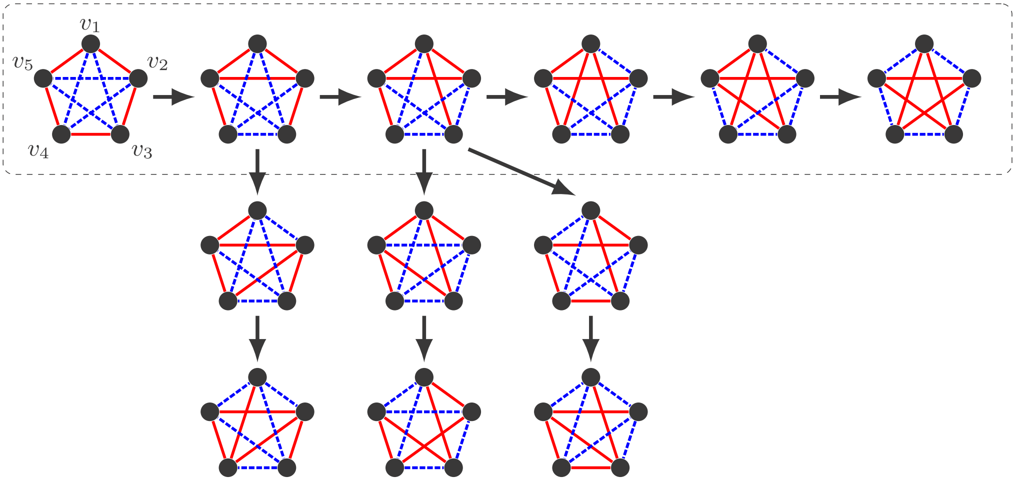


Fig. 5. Exchange sequences starting from a basis pair (X_1, X_2) where X_1 and X_2 are 5-cycles. Basis pairs in the dashed set show a sequence of length 5 to (X_2, X_1). From each basis pair of R_{10}, one can obtain a basis pair shown on the figure with reflections and rotations, thus each pair of bases can be obtained from (X_1, X_2) with at most 5 exchanges by its symmetry.

Proposition 5.6. *For any pair $\mathcal{X}, \mathcal{Y}$ of compatible basis pairs of the Fano matroid, there exists an $\mathcal{X}$-$\mathcal{Y}$ exchange sequence of width at most 4 and length at most 9. For disjoint bases X_1, X_2 of the Fano matroid, there exists an (X_1, X_2)-(X_2, X_1) exchange sequence of length 3. Furthermore, such sequences can be determined in polynomial time.*

Proof. The matroid F_7 is an excluded minor of graphic matroids, see [36, Theorem 10.3.1]. For any pair of bases $\mathcal{X} = (X_1, X_2)$, the restriction $F_7|(X_1 \cup X_2)$ is a proper minor of F_7, thus it is graphic. Since the rank of F_7 is 3, the statements follow from Theorems 4.1 and 4.3. □

5.1.3. Reducing the graphic part to 4-regular graphs

This section is devoted to proving our main structural observation. The proposition is based on a careful combination of the result of Aprile and Fiorini on decomposition trees of 3-connected matroids (Theorem 2.5), the result of McGuinness on the dual of 3-sums (Proposition 2.6), our observation on the cographicness of a matroid obtained from a cographic matroid by a Δ - Y exchange using a coindependent triangle (Lemma 2.7), and the reduction steps introduced in Section 3.

Proposition 5.7. *Let M be a 3-connected regular matroid that is not graphic, cographic or isomorphic to R_{10}. Then, there exists a regular matroid $M_\circ$ and a graphic matroid $M_\bullet$ such that $M_\circ \oplus_3 M_\bullet \in \{M, M^*\}$, and such a decomposition can be determined using a polynomial number of oracle calls. Moreover, if M contains no circuit or cocircuit of size at most 3, its ground set can be partitioned into two bases and it contains no nontrivial tight set, then $M_\bullet$ is the graphic matroid of a simple 4-regular graph.*

Proof. By Theorem 2.5, M can be written in the form $M = M_1 \oplus_3 M_2$, where M_1 is a regular matroid and M_2 is a graphic or cographic matroid. Moreover, if M_2 is not graphic, then it is the cographic matroid of a graph G such that the 3-sum is taken along a triangle T of the matroids which is a trivial cut of G. If M_2 is graphic, then let $M_\circ := M_1$ and $M_\bullet := M_2$. If M_2 is not graphic, then $M^* = \Delta_T(M_1) \oplus_3 \Delta_T(M_2)$ by Proposition 2.6, where $\Delta_T(M_2)$ is a cographic matroid by Lemma 2.7, thus $M_\circ := \Delta_T(M_1)^*$ and $M_\bullet := \Delta_T(M_2)^*$ satisfy the requirements of the first part of the statement.

Assume now that M satisfies all the conditions of the proposition. Let $E_\circ$ and $E_\bullet$ denote the ground sets of $M_\circ$ and $M_\bullet$, respectively, and let $T := E_\bullet \cap E_\circ$. The ground set of M can be partitioned into two bases and M contains no nontrivial tight set, hence the same holds for M^* as well. Since $M_\circ \oplus_3 M_\bullet \in \{M, M^*\}$ contains no nontrivial tight set, the restrictions of $M_\circ \oplus_3 M_\bullet$ and $M_\bullet$ to $E_\bullet - T$ are the same, and T is coindependent in $M_\bullet$, we get

$$|E_\bullet - T| \leq 2 \cdot r_{M_\circ \oplus_3 M_\bullet}(E_\bullet - T) - 1 = 2 \cdot r_{M_\bullet}(E_\bullet - T) - 1 = 2 \cdot r_{M_\bullet}(E_\bullet) - 1.$$

Let $G = (V, E_\bullet)$ be a connected graph whose graphic matroid is $M_\bullet$ and let v_1, v_2, and v_3 denote the vertices of the triangle T. We define $V' := V - \{v_1, v_2, v_3\}$. It follows from the description of $\mathcal{B}(M_\circ \oplus_3 M_\bullet)$ that the cocircuits of $M_\circ \oplus_3 M_\bullet$ and $M_\bullet$ contained in $E_\bullet - T$ are the same. Indeed, a subset of $E_\bullet - T$ intersects each basis of $M_\bullet$ if and only if it intersects each basis of $M_\circ \oplus_3 M_\bullet$. Since each cocircuit of $M_\circ \oplus_3 M_\bullet$ has size at least 4, each vertex in V' has degree at least 4 in G. As $M_\bullet - T$ contains no nontrivial tight set, $E_\bullet - T$ contains no parallel edges. These imply $|V'| \geq 2$, since $V' = \emptyset$ would contradict $|E_\bullet - T| \geq 4$, and $|V'| = 1$ would contradict that the vertices in V' have degree at least 4. Since $|V'| \geq 2$ and $M_\bullet \backslash T$ contains no nontrivial tight set, $|E_\bullet[V']| \leq 2 \cdot |V'| - 3$ follows. Therefore,

$$\begin{aligned} 4 \cdot |V'| \leq \sum_{v \in V'} d(v) &= 2 \cdot |E_\bullet[V']| + \sum_{i=1}^{3} d(v_i) - 2 \cdot |E_\bullet[\{v_1, v_2, v_3\}]| \\ &\leq 2 \cdot (2 \cdot |V'| - 3) + \sum_{i=1}^{3} d(v_i) - 6, \end{aligned} \tag{$*$}$$

thus $\sum_{i=1}^{3} d(v_i) \geq 12$. Using that $r_{M_\bullet}(E_\bullet) = |V| - 1 = |V'| + 2$, we obtain

$$2 \cdot |E_\bullet| = \sum_{v \in V'} d(v) + \sum_{i=1}^{3} d(v_i) \geq 4|V'| + 12 = 4 \cdot r_{M_\bullet}(E_\bullet) + 4,$$

which yields $|E_\bullet - T| = |E_\bullet| - 3 \geq 2r_{M_\bullet}(E_\bullet) - 1$. As we have already shown that $|E_\bullet - T| \leq 2r_{M_\bullet}(E_\bullet) - 1$, we obtain $|E_\bullet - T| = 2 \cdot r_{M_\bullet}(E_\bullet) - 1$ and all the inequalities in $(*)$ hold with equality. This implies that $d(v) = 4$ for each $v \in V'$, $|E_\bullet[V']| = 2 \cdot |V'| - 3$, $\sum_{i=1}^{3} d(v_i) = 12$ and $|E_\bullet[\{v_1, v_2, v_3\}]| = 3$. The last equality implies that the only edges

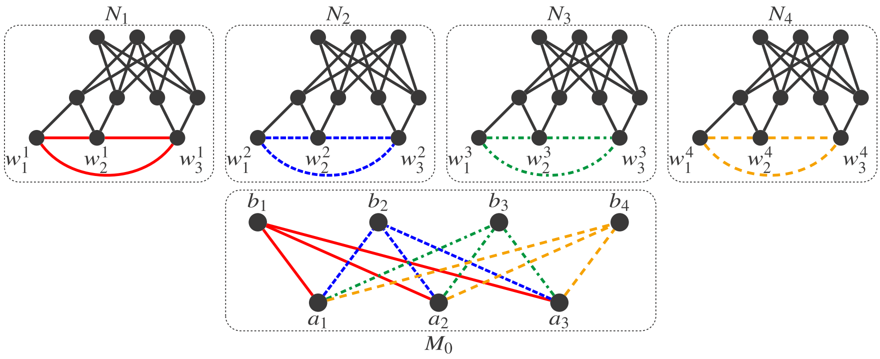


Fig. 6. Illustration of Remark 5.8, where M_0 is the cographic matroid of G and N_i is the graphic matroid of H_i for $1 \leq i \leq 4$. The matroid M is obtained by taking the 3-sum of M_0 with the N_is in an arbitrary order along the triangles using the same color and line style.

spanned by $\{v_1, v_2, v_3\}$ are the edges of T, hence G is a simple graph, as $E_\bullet - T$ contains no parallel edges.

It remains to show that $d(v_1) = d(v_2) = d(v_3) = 4$. Since $|E_\bullet[V'+v_i]| \leq 2\cdot|V'+v_i|-3 = 2 \cdot |V'| - 1$ holds for $i \in \{1, 2, 3\}$, we get

$$|E_\bullet[V']| + 2 = 2 \cdot |V'| - 1 \geq |E_\bullet[V' + v_i]| = |E_\bullet[V']| + d(v_i) - 2,$$

where the last equality follows from $E_\bullet[\{v_1, v_2, v_3\}] = T$. This yields $d(v_i) \leq 4$ for $i \in \{1, 2, 3\}$, hence $\sum_{i=1}^{3} d(v_i) = 12$ implies that $d(v_1) = d(v_2) = d(v_3) = 4$. □

Remark 5.8. Though Proposition 5.7 significantly reduces the number of matroids for which Theorem 1.1 and Theorem 1.2 need to be verified, there indeed exist regular matroids for which none of the reduction steps apply. As an example, let G be a complete bipartite graph with color classes $A = \{a_1, a_2, a_3\}$ and $B = \{b_1, b_2, b_3, b_4\}$. Furthermore, let H be the graph obtained from G by deleting the edge a_1b_1 and adding three new vertices w_1, w_2, w_3 with the extra edges $w_1a_1, w_1b_1, w_2b_1, w_2b_2, w_3b_3, w_3b_4, w_1w_2, w_1w_3$ and w_2w_3. Let H_i be a copy of H for $1 \leq i \leq 4$ with vertices $a_1^i, a_2^i, a_3^i, b_1^i, b_2^i, b_3^i, b_4^i, w_1^i, w_2^i, w_3^i$. Let M_0 denote the cographic matroid of G, and N_i the graphic matroid of H_i for $1 \leq i \leq 4$. Note that $\delta(b_i)$ is a coindependent triangle of M and $\{w_1^iw_2^i, w_1^iw_3^i, w_2^iw_3^i\}$ is a coindependent triangle of N_i for $1 \leq i \leq 4$.

Let M denote the matroid that is obtained by taking the 3-sum of M_0 with the N_is in an arbitrary order; see Fig. 6 for an illustration. Here the 3-sum with N_i is along $\delta(b_i)$ and $\{w_1^iw_2^i, w_1^iw_3^i, w_2^iw_3^i\}$, where the edge b_ia_j is identified with $w_j^iw_{j+1}^i$ for $j = 1, 2, 3$ (indices are in a cyclic order). It is not difficult to check that the ground set of M partitions into two disjoint bases. Also, an easy case analysis shows that none of the reduction operations can be applied to M and M^*, i.e., both M and M^* are 3-connected and contain neither a tight set nor a cocircuit of size at most three. Observe that the example is consistent with the statement of Proposition 5.7 in that N_i is a graphic matroid of a 4-regular graph for $1 \leq i \leq 4$.

Interestingly, the bound on the minimum size of a cocircuit of M and M^* is tight. More precisely, if M is a regular matroid whose ground set partitions into two disjoint bases, then it contains a circuit or cocircuit of size at most 4. This immediately follows from Proposition 5.7 if M is 3-connected and contains no nontrivial tight set; the remaining cases can be verified using Seymour's decomposition.

5.2. Proof of White's conjecture for basis pairs of regular matroids

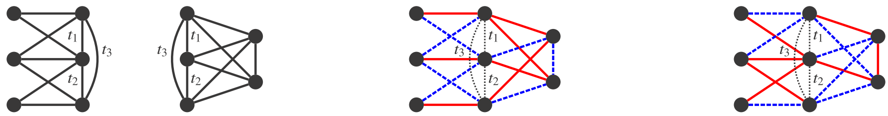
Proof of Theorem 1.1. We prove by induction on the rank of the matroid. The statement holds when $r_M(E) \leq 2$ by Claim 3.8, therefore we consider the case $r_M(E) \geq 3$. We may assume that $X_1 \cup X_2 = Y_1 \cup Y_2 = E$ by deleting the elements in $E - (X_1 \cup X_2)$. Using the induction hypothesis and Corollary 3.9 with $c = 2$ and $F = \emptyset$, we may assume that $X_1 \cap X_2 = Y_1 \cap Y_2 = \emptyset$, M contains no nontrivial tight set and contains no triad. As E can be partitioned into two bases, the pairs of disjoint bases of M and M^* are the same, hence we may also assume that M^* contains no triad, that is, M contains no triangle. Note that the assumption that M contains no nontrivial tight set implies that it is 2-connected and has no circuit or cocircuit of size at most two. Using the induction hypothesis and Corollary 3.10 with $c = 2$, we may assume that M is 3-connected. Using Theorem 4.1 and Proposition 5.5, we may assume that M is not graphic, cographic, or isomorphic to R_{10}. Then, by Proposition 5.7, there exist regular matroids $M_\circ$ and $M_\bullet$ such that $M_\circ \oplus_3 M_\bullet \in \{M, M^*\}$ and $M_\bullet$ is the graphic matroid of a simple 4-regular graph G. Since the pairs of disjoint bases of M and M^* are the same, we may assume that $M_\circ \oplus_3 M_\bullet = M$.

Let $E_\circ$ and $E_\bullet$ denote the ground sets of $M_\circ$ and $M_\bullet$, respectively. Define $T \coloneqq E_\circ \cap E_\bullet = \{t_1, t_2, t_3\}$ and let V denote the set of vertices of G. Since M contains no nontrivial tight set, $|(E-T)[U]| \leq 2 \cdot |U| - 3$ holds for each $U \subseteq V$ with $|U| \geq 2$. As G is 4-regular, $|E_\bullet - T| = |E_\bullet| - 3 = 2 \cdot |V| - 3 = 2 \cdot r_{M_\bullet}(E_\bullet) - 1$, hence $|E_\circ - T| = 2 \cdot r_{M_\circ}(E_\circ) - 3$; see Fig. 7a for an illustration. This together with the characterization of $\mathcal{B}(M_\circ \oplus_3 M_\bullet)$ implies that for a partition $Z_1 \cup Z_2$ of E, $\mathcal{Z} = (Z_1, Z_2)$ is a pair of disjoint bases of M if and only if

- **(Type 1)** $Z_1^\circ + \{t_1, t_2\}$, $Z_2^\circ + t_i$ and $Z_2^\circ + t_j$ are bases of $M_\circ$, $Z_1^\bullet$, $Z_2^\bullet + t_i$ and $Z_2^\bullet + t_k$ are bases of $M_\bullet$ for some i, j, k with $\{i, j, k\} = \{1, 2, 3\}$, or
- **(Type 2)** $Z_1^\circ + t_i$, $Z_1^\circ + t_j$, and $Z_2^\circ + \{t_1, t_2\}$ are bases of $M_\circ$, $Z_1^\bullet + t_i$, $Z_1^\bullet + t_k$ and $Z_2^\bullet$ are bases of $M_\bullet$ for some i, j, k with $\{i, j, k\} = \{1, 2, 3\}$.

Note that $|Z_1^\circ| = r_{M_\circ}(E_\circ) - 2$ if the pair $\mathcal{Z}$ is of Type 1, and $|Z_1^\circ| = r_{M_\circ}(E_\circ) - 1$ if $\mathcal{Z}$ is of Type 2.

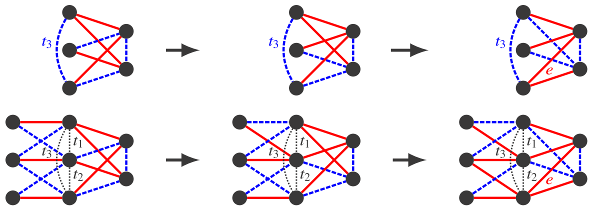
For a pair $\mathcal{Z} = (Z_1, Z_2)$ of disjoint bases of M, let $\{i_\mathcal{Z}, j_\mathcal{Z}, k_\mathcal{Z}\} = \{1, 2, 3\}$ be such that $Z_2^\circ + t_{i_\mathcal{Z}}, Z_2^\circ + t_{j_\mathcal{Z}} \in \mathcal{B}(M_\circ)$ and $Z_2^\bullet + t_{i_\mathcal{Z}}, Z_2^\bullet + t_{k_\mathcal{Z}} \in \mathcal{B}(M_\bullet)$ if $\mathcal{Z}$ is of Type 1, and $Z_1^\circ + t_{i_\mathcal{Z}}, Z_1^\circ + t_{j_\mathcal{Z}} \in \mathcal{B}(M_\circ)$ and $Z_1^\bullet + t_{i_\mathcal{Z}}, Z_1^\bullet + t_{k_\mathcal{Z}} \in \mathcal{B}(M_\bullet)$ if $\mathcal{Z}$ is of Type 2.



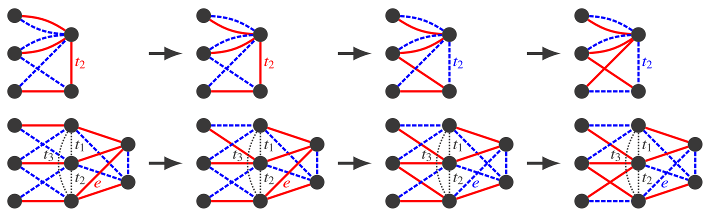
(a) $M_\circ$ and $M_\bullet$ are the graphic matroids of the left and right graphs.

(b) The basis pair $\mathcal{X}$ has Type 1 with $i_\mathcal{X} = 1$, $j_\mathcal{X} = 2$, and $k_\mathcal{X} = 3$.

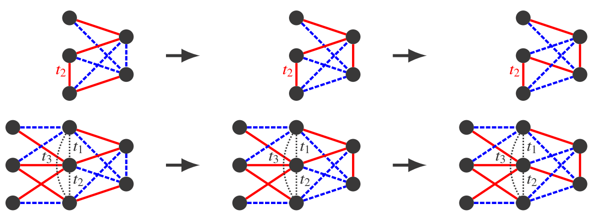
(c) The basis pair $\mathcal{Y}$ has Type 2 with $i_\mathcal{Y} = 3, j_\mathcal{Y} = 2$, and $k_\mathcal{Y} = 1$.



(d) Illustration of (1): a $\{t_3\}$-avoiding sequence from $\mathcal{X}' := (X_1^\bullet, X_2^\bullet + t_3)$ to $\mathcal{F}' := (F_1^\bullet, F_2^\bullet + t_3)$ in $M_\bullet$ and the corresponding sequence from $\mathcal{X}$ to $(X_1^\circ \cup F_1^\bullet, X_2^\circ \cup F_2^\bullet)$ in M. Observe that $e \in F_1^\bullet$ is an edge such that each of $F_1^\bullet$, $F_2^\bullet + t_2$, $F_2^\bullet + t_3$, $F_1^\bullet - e + t_2$, $F_1^\bullet - e + t_3$, and $F_2^\bullet + e$ is a basis of $M_\bullet$.



(e) Illustration of (2): a sequence from $\mathcal{X}'' := (X_1^\circ + t_2, X_2^\circ)$ to $\mathcal{Y}'' := (Y_1^\circ, Y_2^\circ + t_2)$ in $M_\circ/t_1$ and the corresponding sequence from $(X_1^\circ \cup F_1^\bullet, X_2^\circ \cup F_2^\bullet)$ to $(Y_1^\circ \cup \widetilde{F}_1^\bullet, Y_2^\circ \cup \widetilde{F}_2^\bullet)$ in M.



(f) Illustration of (3): a $\{t_2\}$-avoiding sequence from $\mathcal{F}''' := (\widetilde{F}_1^\bullet + t_2, \widetilde{F}_2^\bullet)$ to $\mathcal{Y}''' := (Y_1^\bullet + t_2, Y_2^\bullet)$ in $M_\bullet$ and the corresponding sequence from $(Y_1^\circ \cup \widetilde{F}_1^\bullet, Y_2^\circ \cup \widetilde{F}_2^\bullet)$ to $\mathcal{Y}$ in M.

Fig. 7. Illustrations of sequences (1), (2), and (3) from the proof of Theorem 1.1. Note that $M_\circ \oplus_3 M_\bullet$ is itself graphic and, moreover, it does not satisfy the assumptions of the proof, as it admits reductions that decrease the problem size; nevertheless, we use this example to illustrate sequences (1)–(3).

By Lemma 2.3, the indices $i_\mathcal{Z}$, $j_\mathcal{Z}$ and $k_\mathcal{Z}$ are uniquely defined. By symmetry, we may assume that $|X_1^\circ| = r_{M_\circ}(E_\circ) - 2$, that is, $\mathcal{X}$ is of Type 1. We may also assume that $1 \in \{i_\mathcal{X}, j_\mathcal{X}\} \cap \{i_\mathcal{Y}, j_\mathcal{Y}\}$; see Figs. 7b and 7c. By Lemma 5.4, there exists a partition $E^\bullet - T = F_1^\bullet \cup F_2^\bullet$ and an edge $e \in F_1^\bullet$ such that each of $F_1^\bullet$, $F_2^\bullet + t_2$, $F_2^\bullet + t_3$, $F_1^\bullet - e + t_2$, $F_1^\bullet - e + t_3$ and $F_2^\bullet + e$ is a basis of $M_\bullet$. Moreover, $X_1^\circ + t_1 + t_2$ and $X_2^\circ + t_1$ are bases of $M_\circ$, hence $(X_1^\circ \cup F_1^\bullet, X_2^\circ \cup F_2^\bullet)$ is a pair of disjoint bases of M. Similarly, by letting $(\widetilde{F}_1^\bullet, \widetilde{F}_2^\bullet) := (F_1^\bullet, F_2^\bullet)$ if $\mathcal{Y}$ is of Type 1 and $(\widetilde{F}_1^\bullet, \widetilde{F}_2^\bullet) := (F_1^\bullet - e, F_2^\bullet + e)$ if $\mathcal{Y}$ is of Type 2,

$(Y_1^\circ \cup \widetilde{F}_1^\bullet, Y_2^\circ \cup \widetilde{F}_2^\bullet)$ is a pair of disjoint bases of M. We construct an $\mathcal{X}$-$\mathcal{Y}$ exchange sequence by concatenating exchange sequences

(1) from $\mathcal{X}$ to $(X_1^\circ \cup F_1^\bullet, X_2^\circ \cup F_2^\bullet)$,
(2) from $(X_1^\circ \cup F_1^\bullet, X_2^\circ \cup F_2^\bullet)$ to $(Y_1^\circ \cup \widetilde{F}_1^\bullet, Y_2^\circ \cup \widetilde{F}_2^\bullet)$, and
(3) from $(Y_1^\circ \cup \widetilde{F}_1^\bullet, Y_2^\circ \cup \widetilde{F}_2^\bullet)$ to $\mathcal{Y}$.

For sequence (1), consider the pairs $\mathcal{X}' := (X_1^\bullet, X_2^\bullet + t_{k_\mathcal{X}})$ and $\mathcal{F}' := (F_1^\bullet, F_2^\bullet + t_{k_\mathcal{X}})$ of disjoint bases of the graphic matroid $M_\bullet$. By Theorem 4.1, there exists a $\{t_{k_\mathcal{X}}\}$-avoiding $\mathcal{X}'$-$\mathcal{F}'$ exchange sequence in $M_\bullet$ of width at most $2 \cdot (r_{M_\bullet}(E_\bullet) - 1)$ and length at most $r_{M_\bullet}(E_\bullet)^2$. As none of the exchanges use the element $t_{k_\mathcal{X}}$, each basis pair $\mathcal{Z}'$ of the sequence can be written as $\mathcal{Z}' = (Z_1^\bullet, Z_2^\bullet + t_{k_\mathcal{X}})$. Consider the same symmetric exchanges applied to $\mathcal{X}$ in M, that is, for a basis pair $(Z_1^\bullet, Z_2^\bullet + t_{k_\mathcal{X}})$ of the $\mathcal{X}'$-$\mathcal{F}'$ sequence, consider the basis pair $(X_1^\circ \cup Z_1^\bullet, X_2^\circ \cup Z_2^\bullet)$ of M. Note that this is indeed a basis pair, as $X_1^\circ + \{t_1, t_2\} \in \mathcal{B}_{M_\circ}$, $Z_1^\bullet \in \mathcal{B}_{M_\bullet}$, $X_2^\circ + t_{i_\mathcal{X}}, X_2^\circ + t_{j_\mathcal{X}} \in \mathcal{B}_{M_\circ}$, and $Z_2^\bullet + t_{k_\mathcal{X}} \in \mathcal{B}_{M_\bullet}$. This gives an exchange sequence from $\mathcal{X}$ to $(X_1^\circ \cup F_1^\bullet, X_2^\circ \cup F_2^\bullet)$ of width at most $2 \cdot (r_{M_\bullet}(E_\bullet) - 1)$ and length at most $r_{M_\bullet}(E_\bullet)^2$; see Fig. 7d for an illustration.

For sequence (2), let $\mathcal{X}'' := (X_1^\circ + t_2, X_2^\circ)$ and $\mathcal{Y}'' := (Y_1^\circ + t_2, Y_2^\circ)$ if $\mathcal{Y}$ is of Type 1, and $\mathcal{Y}'' := (Y_1^\circ, Y_2^\circ + t_2)$ if $\mathcal{Y}$ is of Type 2. Both $\mathcal{X}''$ and $\mathcal{Y}''$ are pairs of disjoint bases of the regular matroid $M_\circ / t_1$, hence, by the induction hypothesis, there exists an $\mathcal{X}''$-$\mathcal{Y}''$ exchange sequence in $M_\circ / t_1$ of width at most $4 \cdot r_{M_\circ / t_1}(E_\circ - t_1)$ and length at most $2 \cdot r_{M_\circ / t_1}(E_\circ - t_1)^2$. We perform the steps of this $\mathcal{X}''$-$\mathcal{Y}''$ exchange sequence on $(X_1^\circ \cup F_1^\bullet, X_2^\circ \cup F_2^\bullet)$, but whenever a symmetric exchange uses t_2 and some other element f, then exchange e and f instead. Formally, if a symmetric exchange transforms $(Z_1^\circ + t_2, Z_2^\circ)$ into $(Z_1^\circ + f, Z_2^\circ - f + t_2)$, then this step is replaced by transforming $(Z_1^\circ \cup F_1^\bullet, Z_2^\circ \cup F_2^\bullet)$ into $((Z_1^\circ + f) \cup (F_1^\bullet - e), (Z_2^\circ - f) \cup (F_2^\bullet + e))$. Note that $(Z_1^\circ \cup F_1^\bullet, Z_2^\circ \cup F_2^\bullet)$ is a basis pair of M. Indeed, this follows from $Z_1^\circ + \{t_1, t_2\} \in \mathcal{B}(M_\circ)$, $F_1^\bullet \in \mathcal{B}(M_\bullet)$ and $Z_2^\circ + t_1 \in \mathcal{B}(M_\circ)$, $F_2^\bullet + t_2, F_2^\bullet + t_3 \in \mathcal{B}(M_\bullet)$. Analogously, $((Z_1^\circ + f) \cup (F_1^\bullet - e), (Z_2^\circ - f) \cup (F_2^\bullet + e))$ is a basis pair of M. This follows from $Z_1^\circ + \{f, t_1\} \in \mathcal{B}(M_\circ)$, $F_1^\bullet - e + t_2, F_1^\bullet - e + t_3 \in \mathcal{B}(M_\bullet)$ and $Z_2^\circ - f + \{t_1, t_2\} \in \mathcal{B}(M_\circ)$, $F_2^\bullet + e \in \mathcal{B}(M_\bullet)$. Similarly, if a symmetric exchange transforms $(Z_1^\circ, Z_2^\circ + t_2)$ into $(Z_1^\circ - f + t_2, Z_2^\circ + f)$, then this step is replaced by transforming $(Z_1^\circ \cup (F_1^\bullet - e), Z_2^\circ \cup (F_2^\bullet + e))$ into $((Z_1^\circ - f) \cup F_1^\bullet, (Z_2^\circ + f) \cup F_2^\bullet)$. This gives an exchange sequence from $(X_1^\circ \cup F_1^\bullet, X_2^\circ \cup F_2^\bullet)$ to $(Y_1^\circ \cup \widetilde{F}_1^\bullet, Y_2^\circ \cup \widetilde{F}_2^\bullet)$ in M of width at most $4 \cdot (r_{M_\circ / t_1}(E_\circ - t_1) - 1)$ and length at most $2 \cdot r_{M_\circ / t_1}(E_\circ - t_1)^2$; see Fig. 7e for an illustration.

For sequence (3), the construction is analogous to that of sequence (1). Let $\mathcal{F}''' := (\widetilde{F}_1^\bullet, \widetilde{F}_2^\bullet + t_{k_\mathcal{Y}})$ and $\mathcal{Y}''' := (Y_1^\bullet, Y_2^\bullet + t_{k_\mathcal{Y}})$ if $\mathcal{Y}$ is of Type 1, and let $\mathcal{F}''' := (\widetilde{F}_1^\bullet + t_{k_\mathcal{Y}}, \widetilde{F}_2^\bullet)$ and $\mathcal{Y}''' := (Y_1^\bullet + t_{k_\mathcal{Y}}, Y_2^\bullet)$ if $\mathcal{Y}$ is of Type 2. By Theorem 4.1, there exists a $\{t_{k_\mathcal{Y}}\}$-avoiding $\mathcal{F}'''$-$\mathcal{Y}'''$ exchange sequence in $M_\bullet$ of width at most $2 \cdot (r_{M_\bullet}(E_\bullet) - 1)$ and length at most $r_{M_\bullet}(E_\bullet)^2$, which yields an exchange sequence of the same width and length in M from $(Y_1^\circ \cup \widetilde{F}_1^\bullet, Y_2^\circ \cup \widetilde{F}_2^\bullet)$ to $\mathcal{Y}$; see Fig. 7f for an illustration.

Concatenating the three sequences we obtain an $\mathcal{X}$-$\mathcal{Y}$ exchange sequence in M of width at most

$$\begin{aligned}&2\cdot(r_{M_\bullet}(E_\bullet)-1)+4\cdot(r_{M_\circ/t_1}(E_\circ-t_1)-1)+2\cdot(r_{M_\bullet}(E_\bullet)-1)\\&=4\cdot(r_{M_\circ}(E_\circ)+r_{M_\bullet}(E_\bullet)-3)\\&=4\cdot(r_M(E)-1),\end{aligned}$$

and length at most

$$\begin{aligned}&r_{M_\bullet}(E_\bullet)^2+2\cdot r_{M_\circ/t_1}(E_\circ-t_1)^2+r_{M_\bullet}(E_\bullet)^2\\&=2\cdot(r_{M_\bullet}(E_\bullet)^2+(r_{M_\circ}(E_\circ)-1)^2)\\&\le 2\cdot(r_{M_\bullet}(E_\bullet)+r_{M_\circ}(E_\circ)-2)^2\\&=2\cdot r_M(E)^2,\end{aligned}$$

where $r_{M_\bullet}(E_\bullet)^2+(r_{M_\circ}(E_\circ)-1)^2\le(r_{M_\bullet}(E_\bullet)+r_{M_\circ}(E_\circ)-2)^2$ holds by $r_{M_\bullet}(E_\bullet), r_{M_\circ}(E_\circ) \ge 3$.

The proof leads to a polynomial algorithm for determining a $\mathcal{X}$-$\mathcal{Y}$ exchange sequence. We have already discussed that one can find a decomposition of M into basic matroids and perform the reduction steps using a polynomial number of oracle calls. Once a decomposition of the form $M=M_\circ\oplus_3 M_\bullet$ is identified where $M_\bullet$ is a graphic matroid of $G=(V,E)$, the proof of Lemma 5.4 shows how to find a partition $E-T=F_1\cup F_2$. Finally, above we described how to construct the $\mathcal{X}$-$\mathcal{Y}$ exchange sequence based on these, concluding the proof of the theorem. □

5.3. Proof of Gabow's conjecture for regular matroids

Proof of Theorem 1.2. We prove by induction on the rank of the matroid. The statement holds when $r_M(E)\le 2$ by Claim 3.8, therefore we consider the case $r_M(E)\ge 3$. We may assume that $X_1\cup X_2=E$ by deleting the elements in $E-(X_1\cup X_2)$. If M contains a nontrivial tight set Z, then we apply the induction hypothesis to $M|Z$ and M/Z and use Lemma 3.1 together with the fact that $r(M|Z)+r(M/Z)=r_M(E)$. If $M=M_\circ\oplus_2 M_\bullet$, then we apply the induction hypothesis to $M_\circ$ and $M_\bullet$ and use Lemma 3.4 together with the fact that $r_{M_\circ}(E_\circ)+r_{M_\bullet}(E_\bullet)-1=r_M(E)$. If M contains a triad $T=\{t_1,t_2,t_3\}$ where, say, $t_1,t_2\in X_1$, then there exists an exchange sequence from (X_1-t_2,X_2-t_3) to (X_2-t_2,X_1-t_3) in $M/t_2\backslash t_3$ of length $r_{M/t_2\backslash t_3}(E-\{t_2,t_3\})=r_M(E)-1$ by the induction hypothesis. Hence, the statement follows using Lemma 3.7. Similarly, we are also done if M contains a triangle by taking the dual of M. Using Theorem 4.3 and Proposition 5.5, we may assume that M is not graphic, cographic, or isomorphic to R_{10}. Therefore, we may assume that all conditions of Proposition 5.7 hold and, by taking the dual of M if necessary, $M=M_\circ\oplus_3 M_\bullet$ where $M_\circ$ is a regular matroid and $M_\bullet$ is the graphic matroid of a simple 4-regular graph G.

Similarly to the proof of Theorem 1.1, the pairs of disjoint bases of M can be of Type 1 and Type 2. We may assume by symmetry that (X_1, X_2) is of Type 1 with $i = 1$, $j = 2$ and $k = 3$, that is, $X_1^\circ + t_1 + t_2$, $X_2^\circ + t_1$ and $X_2^\circ + t_2$ are bases of $M_\circ$, and $X_1^\bullet$, $X_2^\bullet + t_1$ and $X_2^\bullet + t_3$ are bases of $M_\bullet$. By the induction hypothesis, there exists an exchange sequence of length $r_{M_\circ/t_2}(E_\circ - t_2)$ transforming $(X_1^\circ + t_1, X_2^\circ)$ into $(X_2^\circ, X_1^\circ + t_1)$ in $M_\circ/t_2$. Exactly one of these exchanges uses t_1, say the $(\ell+1)$th step transforms $(Y_1^\circ + t_1, Y_2^\circ)$ into $(Y_1^\circ + e, Y_2^\circ - e + t_1)$ We construct an exchange sequence from (X_1, X_2) to (X_2, X_1) in M by concatenating exchange sequences

(1) from (X_1, X_2) to $(Y_1^\circ \cup X_1^\bullet, Y_2^\circ \cup X_2^\bullet)$,
(2) from $(Y_1^\circ \cup X_1^\bullet, Y_2^\circ \cup X_2^\bullet)$ to $((Y_1^\circ + e) \cup X_2^\bullet, (Y_2^\circ - e) \cup X_1^\bullet)$, and
(3) from $((Y_1^\circ + e) \cup X_2^\bullet, (Y_2^\circ - e) \cup X_1^\bullet)$, to (X_2, X_1).

For sequence (1), we apply the ℓ symmetric exchanges transforming $(X_1^\circ + t_1, X_2^\circ)$ into $(Y_1^\circ + t_1, Y_2^\circ)$ in M/t_2 to the basis pair (X_1, X_2) in M. As none of these exchanges uses t_1, each member of this sequence in M/t_2 can be written as $(Z_1^\circ + t_1, Z_2^\circ)$, and thus $(Z_1^\circ \cup X_1^\bullet, Z_2^\circ \cup X_2^\bullet)$ is a basis pair of M, since $X_1^\bullet$, $X_2^\bullet + t_1$ and $X_2^\bullet + t_3$ are bases of $M_\bullet$.

For sequence (2), by $Y_2^\circ + t_2 \in \mathcal{B}(M_\circ)$, Lemma 2.3 implies that there exist i, j satisfying $\{i, j\} = \{1, 3\}$, $Y_2^\circ + t_i \in \mathcal{B}(M_\circ)$ and $Y_2^\circ + t_j \notin \mathcal{B}(M_\circ)$. By Theorem 4.3, there exists an exchange sequence of length $r_{M_\bullet}(E_\bullet)$ transforming $(X_1^\bullet, X_2^\bullet + t_j)$ into $(X_2^\bullet + t_j, X_1^\bullet)$ in $M_\bullet$ using t_j in the last step. Assume that this last step exchanges f and t_j, that is, it transforms $(X_2^\bullet + f, X_1^\bullet + t_j - f)$ into $(X_2^\bullet + t_j, X_1^\bullet)$. We apply the steps of this sequence in $M_\bullet$ except the one exchanging f and t_2 to $(Y_1^\circ \cup X_1^\bullet, Y_2^\circ \cup X_2^\bullet)$. As none of these exchanges use t_j, each member of this sequence in $M_\bullet$ can be written as $(Z_1^\bullet, Z_2^\bullet + t_j)$, and thus $(Y_1^\circ \cup Z_1^\bullet, Y_2^\circ \cup Z_2^\bullet)$ is a basis pair of M. This way we transform $(Y_1^\circ \cup X_1^\bullet, Y_2^\circ \cup X_2^\bullet)$ into $(Y_1^\circ \cup (X_2^\bullet + f), Y_2^\circ \cup (X_1^\bullet - f))$ in M using $r_{M_\bullet}(E_\bullet) - 1$ steps. Finally, we obtain $((Y_1^\circ + e) \cup X_2^\bullet, (Y_2^\circ - e) \cup X_1^\bullet)$ by exchanging e and f.

For sequence (3), the construction is analogous to that of sequence (1). We apply the $r(M_\circ/t_2) - \ell - 1$ symmetric exchanges transforming $(Y_1^\circ + e, Y_2^\circ - e + t_1)$ into $(X_2^\circ, X_1^\circ + t_1)$ in M/t_2 to the basis pair $((Y_1^\circ + e) \cup X_2^\bullet, (Y_2^\circ - e) \cup X_1^\bullet)$ in M. The concatenation of the three sequences transforms (X_1, X_2) into (X_2, X_1) using $\ell + r_{M_\bullet}(E_\bullet) + (r(M_\circ/t_2) - \ell - 1) = r_{M_\bullet}(E_\bullet) + r_{M_\circ}(E_\circ) - 2 = r_M(E)$ symmetric exchanges.

Similarly to the proof of Theorem 1.1, the proof leads to a polynomial algorithm for determining an (X_1, X_2)-(X_2, X_1) exchange sequence, concluding the proof of the theorem. $\square$

6. Conclusions

In this work, we verified two long-standing open conjectures on the exchange distance of basis pairs in regular matroids. We presented preprocessing steps that reduce the problems to 3-connected regular matroids not containing small cocircuits. This led to a polynomial upper bound on the number of exchanges needed to transform a basis pair of a graphic matroid into another, a result that is of independent combinatorial interest. By combining a recent refinement of Seymour's decomposition theorem given by Aprile and Fiorini, a result of McGuinness on the dual of the 3-sum of two matroids, and an observation on Δ - Y exchanges in cographic matroids, we showed that the regular matroid can be assumed to have the form $M = M_\circ \oplus_3 M_\bullet$ where $M_\bullet$ is a graphic matroid. This, together with the aforementioned observations for the graphic case, allowed us to bound the exchange distance of basis pairs of regular matroids in general. Our proof implies an algorithm for determining a sequence of symmetric exchanges that transforms a given pair of bases into another using a polynomial number of oracle calls.

Our proof technique allows us to go beyond regular matroids to max-flow min-cut (MFMC) matroids, introduced by Seymour [39] as matroids satisfying a generalization of Menger's theorem on the edge-connectivity of undirected graphs. Seymour [39,41] (see also [36, Corollary 12.3.22]) showed that any MFMC matroid can be constructed by taking 1- and 2-sums of regular matroids and the Fano matroid F_7. Therefore, in order to extend our results to the class of MFMC matroids, it suffices to verify counterparts of Theorem 1.1 and Theorem 1.2 for F_7. This follows by Proposition 5.6, hence our results hold for MFMC matroids as well.

We close the paper by mentioning some open problems:

1. Our main motivation for considering regular matroids was Seymour's decomposition theorem. However, our technique might be applicable to any class of matroids whose members have a decomposition into basic matroids using 1-, 2-, and 3-sums where the exchange distance of basis pairs can be bounded in every basic matroid. In particular, this allowed us to extend our results to MFMC matroids. It would be interesting to identify further matroid classes that admit such decompositions.
2. Seymour's definition of matroid sums breaks down for nonbinary matroids. A vast amount of work has focused on extending this notion to nonbinary matroids as well, see e.g. [44]. Hence a natural question is whether our approach can be applied to these more general definitions of sums.
3. Blasiak [9] settled White's conjecture for sequences of arbitrary length in graphic matroids.
    - (a) The proof recursively reduces the size of the problem by decreasing the number of bases in $(X_1, \ldots, X_k)$ by one, and so it does not lead to an efficient algorithm for determining a sequence of symmetric exchanges between two basis sequences. This raises the following: does there exist a polynomial bound on the exchange distance of basis sequences of graphic matroids in general?
    - (b) While we could verify White's conjecture for basis pairs in regular matroids, the problem remains open for longer sequences. We believe that such a result might follow by combining our techniques with Blasiak's approach for the graphic case.

4. A common generalization of White's conjecture for sequences of length two and Gabow's conjecture was proposed by Hamidoune [11], suggesting that the exchange distance of compatible basis pairs is at most the rank of the matroid. In [6], the conjecture was verified for strongly base orderable matroids, split matroids, spikes, and graphic matroids of wheel graphs. However, it remains open even for graphic matroids in general.

Acknowledgment

The authors are grateful to Dániel Garamvölgyi and Yutaro Yamaguchi for initial discussions on the problem, and to Luis Ferroni for calling their attention to the applications discussed in paragraph "Carathéodory Rank of Matroid Base Polytopes."

Tamás Schwarcz was supported by the ÚNKP-22-3 and ÚNKP-23-3 New National Excellence Programs of the Ministry for Culture and Innovation from the source of the National Research, Development and Innovation Fund. The research was supported by the Lendület Programme of the Hungarian Academy of Sciences – grant number LP2021-1/2021, by the Ministry of Innovation and Technology of Hungary from the National Research, Development and Innovation Fund – grant numbers ADVANCED 150556 and ELTE TKP 2021-NKTA-62, and by Dynasnet European Research Council Synergy project – grant number ERC-2018-SYG 810115. This work was supported in part by EPSRC grant EP/X030989/1. The OTP Bank provided financial support for the authors to attend the STOC'24 conference.

Data availability

No data was used for the research described in the article.

References

[1] N. Anari, K. Liu, S.O. Gharan, C. Vinzant, Log-concave polynomials II: high-dimensional walks and an FPRAS for counting bases of a matroid, Ann. Math. 199 (1) (2024) 259–299.
[2] S.D. Andres, W. Hochstättler, M. Merkel, On a base exchange game on bispanning graphs, Discrete Appl. Math. 165 (2014) 25–36.
[3] M. Aprile, S. Fiorini, Regular matroids have polynomial extension complexity, Math. Oper. Res. 47 (1) (2022) 540–559.
[4] S. Backman, G. Liu, A regular unimodular triangulation of the matroid base polytope, Duke Math. J. 174 (14) (2025) 3047–3061.
[5] K. Bérczi, Á. Jánosik, B. Mátravölgyi, Cyclic ordering of split matroids, arXiv preprint, arXiv:2411.01061, 2024.
[6] K. Bérczi, B. Mátravölgyi, T. Schwarcz, Weighted exchange distance of basis pairs, Discrete Appl. Math. 349 (2024) 130–143.
[7] K. Bérczi, T. Schwarcz, Exchange distance of basis pairs in split matroids, SIAM J. Discrete Math. 38 (1) (2024) 132–147.
[8] A. Biswas, S. Barman, Fair division under cardinality constraints, in: IJCAI'18: Proceedings of the 27th International Joint Conference on Artificial Intelligence, International Joint Conferences on Artificial Intelligence, ijcai.org, 2018, pp. 91–97.
[9] J. Blasiak, The toric ideal of a graphic matroid is generated by quadrics, Combinatorica 28 (3) (2008) 283–297.

[10] J.E. Bonin, Basis-exchange properties of sparse paving matroids, Adv. Appl. Math. 50 (1) (2013) 6–15.
[11] R. Cordovil, M.L. Moreira, Bases-cobases graphs and polytopes of matroids, Combinatorica 13 (2) (1993) 157–165.
[12] W.H. Cunningham, Testing membership in matroid polyhedra, J. Comb. Theory, Ser. B 36 (2) (1984) 161–188.
[13] M. Dinitz, G. Kortsarz, Matroid secretary for regular and decomposable matroids, SIAM J. Comput. 43 (5) (2014) 1807–1830.
[14] A. Dror, M. Feldman, E. Segal-Halevi, On fair division under heterogeneous matroid constraints, J. Artif. Intell. Res. 76 (2023) 567–611.
[15] J. Edmonds, D.R. Fulkerson, Transversals and matroid partition, J. Res. Natl. Bur. Stand. B 69 (1965) 147–153.
[16] M. Farber, Basis pair graphs of transversal matroids are connected, Discrete Math. 73 (3) (1989) 245–248.
[17] M. Farber, B. Richter, H. Shank, Edge-disjoint spanning trees: a connectedness theorem, J. Graph Theory 9 (3) (1985) 319–324.
[18] T. Feder, M. Mihail, Balanced matroids, in: STOC'92: Proceedings of the Twenty-Fourth Annual ACM Symposium on Theory of Computing, Association for Computing Machinery, New York, NY, 1992, pp. 26–38.
[19] Z. Fekete, J. Szabó, Equitable partitions to spanning trees in a graph, Electron. J. Comb. 18 (1) (2011) P221.
[20] H. Gabow, Decomposing symmetric exchanges in matroid bases, Math. Program. 10 (1) (1976) 271–276.
[21] D. Gijswijt, G. Regts, Polyhedra with the integer Carathéodory property, J. Comb. Theory, Ser. B 102 (1) (2012) 62–70.
[22] C. Greene, T.L. Magnanti, Some abstract pivot algorithms, SIAM J. Appl. Math. 29 (3) (1975) 530–539.
[23] D.C. Haws, Matroid polytopes: algorithms, theory, and applications, PhD thesis, University of California, Davis, 2009.
[24] Y. Kajitani, S. Ueno, H. Miyano, Ordering of the elements of a matroid such that its consecutive w elements are independent, Discrete Math. 72 (1–3) (1988) 187–194.
[25] T. Király, Equitability of matroids, https://lemon.cs.elte.hu/egres/open/Equitability_of_matroids, 2015. (Accessed 22 March 2024).
[26] Y. Kobayashi, R. Mahara, T. Schwarcz, Reconfiguration of the union of arborescences, Algorithmica 87 (2025) 1040–1059.
[27] D. Kotlar, On circuits and serial symmetric basis-exchange in matroids, SIAM J. Discrete Math. 27 (3) (2013) 1274–1286.
[28] D. Kotlar, R. Ziv, On serial symmetric exchanges of matroid bases, J. Graph Theory 73 (3) (2013) 296–304.
[29] M. Lasoń, On the toric ideals of matroids of a fixed rank, Sel. Math. 27 (2) (2021).
[30] M. Lasoń, M. Michałek, On the toric ideal of a matroid, Adv. Math. 259 (2014) 1–12.
[31] S. McGuinness, A base exchange property for regular matroids, J. Comb. Theory, Ser. B 107 (2014) 42–77.
[32] S. McGuinness, Frame matroids, toric ideals, and a conjecture of White, Adv. Appl. Math. 118 (2020) 102042.
[33] S. McGuinness, Serial exchanges in matroids, Discrete Math. 345 (2) (2022) 112679.
[34] M. Michałek, B. Sturmfels, Invitation to Nonlinear Algebra, American Mathematical Society, Providence, RI, 2021.
[35] C.St.J.A. Nash-Williams, Decomposition of finite graphs into forests, J. Lond. Math. Soc. 39 (1) (1964) 12.
[36] J. Oxley, Matroid Theory, second edition, Oxford Graduate Texts in Mathematics, vol. 21, Oxford University Press, Oxford, 2011.
[37] G.C. Robinson, D.J.A. Welsh, The computational complexity of matroid properties, Math. Proc. Camb. Philos. Soc. 87 (1) (1980) 29–45.
[38] J. Schweig, Toric ideals of lattice path matroids and polymatroids, J. Pure Appl. Algebra 215 (11) (2011) 2660–2665.
[39] P.D. Seymour, The matroids with the max-flow min-cut property, J. Comb. Theory, Ser. B 23 (2–3) (1977) 189–222.
[40] P.D. Seymour, Decomposition of regular matroids, J. Comb. Theory, Ser. B 28 (3) (1980) 305–359.

[41] P.D. Seymour, Matroids and multicommodity flows, Eur. J. Comb. 2 (3) (1981) 257–290.
[42] K. Shibata, Toric ideals of series and parallel connections of matroids, J. Algebra Appl. 15 (06) (2016) 1650106.
[43] K. Truemper, A decomposition theory for matroids. V. Testing of matrix total unimodularity, J. Comb. Theory, Ser. B 49 (2) (1990) 241–281.
[44] K. Truemper, Matroid Decomposition, Academic Press, Inc., Boston, MA, 1992.
[45] W.T. Tutte, On the problem of decomposing a graph into n connected factors, J. Lond. Math. Soc. 36 (1) (1961) 221–230.
[46] J. van den Heuvel, S. Thomassé, Cyclic orderings and cyclic arboricity of matroids, J. Comb. Theory, Ser. B 102 (3) (2012) 638–646.
[47] N.L. White, A unique exchange property for bases, Linear Algebra Appl. 31 (1980) 81–91.
[48] D. Wiedemann, Cyclic base orders of matroids, Manuscript, 1984.