RIMS Preprint No. 1269, Kyoto University, February 2000

On Circuit Valuation of Matroids [1]

Kazuo Murota and Akihisa Tamura

February 14, 2000

Abstract

The concept of valuated matroids was introduced by Dress and Wenzel as a quantitative extension of the base exchange axiom for matroids. This paper gives several sets of cryptomorphically equivalent axioms of valuated matroids in terms of $(R\cup\{-\infty\})$-valued vectors defined on the circuits of the underlying matroid, where R is a totally ordered additive group. The dual of a valuated matroid is characterized by an orthogonality of $(R \cup \{-\infty\})$-valued vectors on circuits. Minty's characterization for matroids by the painting property is generalized for valuated matroids.

Kazuo Murota
Research Institute for Mathematical Sciences,
Kyoto University, Kyoto 606-8502, Japan.
phone: +81-75-753-7221, facsimile: +81-75-753-7272
e-mail: murota@kurims.kyoto-u.ac.jp.

Akihisa Tamura
Research Institute for Mathematical Sciences,
Kyoto University, Kyoto 606-8502, Japan.
phone: +81-75-753-7236, facsimile: +81-75-753-7272
e-mail: tamura@kurims.kyoto-u.ac.jp.

[1] This work is supported by a Grant-in-Aid of the Ministry of Education, Science, Sports and Culture of Japan.

1 Introduction

Matroids are one of the most widely studied combinatorial objects. There are many cryptomorphically equivalent axioms of a matroid in terms of bases, independent sets, circuits, rank functions and so on (see [21, 26, 27], and see [27] for the terminology of cryptomorphism). The concept of matroids has been extended in two different directions, oriented matroids introduced independently by Bland and Las Vergnas [4] and Folkman and Lawrence [10] (see also [2]) and valuated matroids introduced by Dress and Wenzel [7, 9] (see also [20]).

Oriented matroids have cryptomorphically equivalent axioms in terms of bases, circuits, vectors, etc. In particular, circuit (or vector) families play an important role in optimization on oriented matroids. The linear programming problem and the linear complementarity problem are abstracted on oriented matroids [3, 23, 24] and algorithms (e.g., [3, 22, 24, 11]) for those problems rely on the properties of circuit families.

Valuated matroids afford another nice combinatorial framework for optimization. Variations of greedy algorithms for maximizing a matroid valuation on the bases have been proposed [1, 6, 7, 13]. Valuated matroids are characterized by a kind of greedy algorithms [7] and by the maximizers of a valuation [16]. The matroid intersection problem [5] is extended to valuated matroids [14, 15, 18] (see [20] for engineering applications). Moreover, these results on valuated matroids have been extended to discrete convex functions [16, 19]. Those previous studies focus mainly on valuations on the base family (i.e., the exchange property in base axioms of valuated matroids), although valuated matroids have other cryptomorphically equivalent axioms in terms of hyperplane and circuit functions [8] and independent sets [17].

The main objective of this paper is to investigate 'circuits' of valuated matroids with the hope of laying the foundation for a novel framework of optimization on valuated matroids. We give circuit axioms and vector axioms in terms of $(R \cup \{-\infty\})$-valued vectors which are called chain-groups in [25], where R is a totally ordered additive group (typically $R = \mathbf{R}$ (reals), $\mathbf{Q}$ (rationals), or $\mathbf{Z}$ (integers)). We also discuss the duality of valuated matroids by referring to 'orthogonality' of circuits or vectors.

Before introducing our axioms of a valuated matroid, we briefly explain base and circuit axioms of a matroid. Let V be a finite set V, and denote by 2^V the family of all the subsets of V.

The *base family* of a matroid on V is a family $\mathcal{B} \subseteq 2^V$ such that

(MB1) $\mathcal{B} \neq \emptyset$,

(MBX) for $B_1, B_2 \in \mathcal{B}$ and $u \in B_1 - B_2$, there exists $v \in B_2 - B_1$ such that

$$B_1 - u + v \in \mathcal{B} \text{ and } B_2 - v + u \in \mathcal{B},$$

where $B_1 - B_2$ denotes the difference set $\{v \mid v \in B_1,\ v \notin B_2\}$ and $B_1 - u + v$ is a short-hand notation of $(B_1 - \{u\}) \cup \{v\}$. We denote the matroid as $\mathbf{M} = (V, \mathcal{B})$. By (MBX), every base has the same cardinality, which is called the *rank* of $\mathbf{M}$. (MB1) and (MBX) are called *base axioms* of a matroid. In particular, (MBX) is called the *(simultaneous) exchange property*.

A minimal subset of V not belonging to any base of $\mathbf{M}$ is called a *circuit* of $\mathbf{M}$. The family $\mathcal{C}$ of circuits of $\mathbf{M}$ satisfies the following properties, which are called *circuit axioms* of a matroid:

(MC1) $\emptyset \notin \mathcal{C}$,

(MC2) if $C_1 \neq C_2 \in \mathcal{C}$ then $C_1 \not\subseteq C_2$,

(MCE) for $C_1, C_2 \in \mathcal{C}$, $u \in C_1 \cap C_2$ and $v \in C_1 - C_2$, there exists $C_3 \in \mathcal{C}$ such that $v \in C_3 \subseteq (C_1 \cup C_2) - u$.

(MCE) is called the *elimination property*. Conversely, if $\mathcal{C} \subseteq 2^V$ satisfies (MC1), (MC2) and (MCE), then the family $\mathcal{B}$ of maximal subsets not containing any element of $\mathcal{C}$ forms the base family of a matroid. Furthermore, this construction establishes a one-to-one correspondence between the base families and the circuit families of matroids on V.

Valuated matroids are defined as follows. Given a function $\omega : 2^V \to (R \cup \{-\infty\})$, we define $\mathcal{B}$ by

$$\mathcal{B} = \{B \in 2^V \mid \omega(B) \neq -\infty\}. \tag{1.1}$$

A *valuated matroid* is defined in [7, 9] as a pair (V,ω) of a finite set V and a function $\omega : 2^V \to (R \cup \{-\infty\})$ such that

(VB1) $\mathcal{B} \neq \emptyset$,

(VBX) for $B_1, B_2 \in \mathcal{B}$ and $u \in B_1 - B_2$, there exists $v \in B_2 - B_1$ such that $B_1 - u + v, B_2 - v + u \in \mathcal{B}$ and

$$\omega(B_1) + \omega(B_2) \leq \omega(B_1 - u + v) + \omega(B_2 - v + u). \tag{1.2}$$

We call (VB1) and (VBX) *base axioms* of a valuated matroid and denote a valuated matroid as $(V,\mathcal{B},\omega)$. In particular, we call (VBX) the *exchange property* which is a quantitative generalization of (MBX) in two ways. First, (VBX) guarantees that $\mathcal{B}$ induced from ω by (1.1) is the base family of a matroid, and hence, ω can

be regarded as a valuation on the matroid $\mathbf{M} = (V, \mathcal{B})$. Second, every matroid $\mathbf{M} = (V, \mathcal{B})$ has a *trivial valuation* ω defined by

$$\omega(B) = \begin{cases} 0 & \text{if } B \in \mathcal{B} \\ -\infty & \text{otherwise.} \end{cases} \tag{1.3}$$

Following Dress and Wenzel [8], we define a valuation on the circuit family $\mathcal{C}$ of a matroid on V as a set $\mathcal{X}$ of $(R \cup \{-\infty\})$-valued vectors such that $\underline{\mathcal{X}} = \mathcal{C}$, where for any vector $X = (X_i : i \in V) \in (R \cup \{-\infty\})^V$, its *support* $\underline{X}$ is defined by $\underline{X} = \{i \in V \mid X_i \neq -\infty\}$ and $\underline{\mathcal{X}} = \{\underline{X} \mid X \in \mathcal{X}\}$. The elimination property (MCE) of a matroid is generalized to

(VCE) for $X, Y \in \mathcal{X}$ and $u, v \in V$ with $X_u = Y_u \neq -\infty$ and $X_v > Y_v$, there exists $Z \in \mathcal{X}$ such that $Z_u = -\infty, Z_v = X_v$ and $Z \leq \max(X, Y)$.

In the case of a trivial valuation, an element of $\mathcal{X}$ can be regarded as a $(0, -\infty)$-valued vector, and therefore, $X_v > Y_v$ and $Z \leq \max(X, Y)$ in (VCE) reduce respectively to $v \in \underline{X} - \underline{Y}$ and $\underline{Z} \subseteq (\underline{X} \cup \underline{Y}) - v$. Hence (VCE) is identical with (MCE) for the trivial valuation. It is emphasized that we can select an element of $\underline{X} \cap \underline{Y}$ as v with $X_v > Y_v$ in the general case.

(VBX) and (VCE) are 'global' properties in the sense that they refer to any two bases and circuits, respectively. Local exchange and elimination properties are also considered in the literature. For the local exchange property, the following fact is known.

Theorem 1.1 ([8]; see [20, Theorem 5.2.25]) *Let $\mathcal{B}$ be the base family of a matroid. Then a function $\omega : \mathcal{B} \to R$ is a valuation if and only if ω satisfies*

($\mathrm{VBX}_{\mathrm{loc}}$) *for $B_1, B_2 \in \mathcal{B}$ with $|B_1 - B_2| = 2$, there exist $u \in B_1 - B_2$ and $v \in B_2 - B_1$ satisfying (1.2).* ∎

The elimination property on circuit functions introduced in [8] can be regarded as the following local elimination property:

(DW) for $X_1, X_2, X_3 \in \mathcal{X}$ such that $D = \underline{X_1} \cup \underline{X_2} \cup \underline{X_3}$ satisfies $D = \underline{X_i} \cup \underline{X_j}$ for $i \neq j$ and $\mathrm{rank}(D) = |D| - 2$, there exist $\alpha, \beta \in R$ such that $X_3 \leq \max(X_1 + \alpha\mathbf{1}, X_2 + \beta\mathbf{1})$ and $(X_3)_i = \max((X_1)_i + \alpha, (X_2)_i + \beta)$ for any i with $(X_1)_i + \alpha \neq (X_2)_i + \beta$,

where $\max(X, Y)$ denotes the vector whose ith component is $\max(X_i, Y_i)$ and $\mathbf{1}$ denotes the vector of all ones. In this paper, we deal with two global elimination properties ((VCE) and its variant labeled ($\mathrm{VCE}_{\mathrm{W}}$), to be introduced in Section 3) and three local ones (($\mathrm{VCE}_{\mathrm{loc1}}$), ($\mathrm{VCE}_{\mathrm{loc2}}$) and ($\mathrm{VCE}_{\mathrm{loc3}}$) to be introduced in Section 3), and verify the relationship (essential equivalence) among

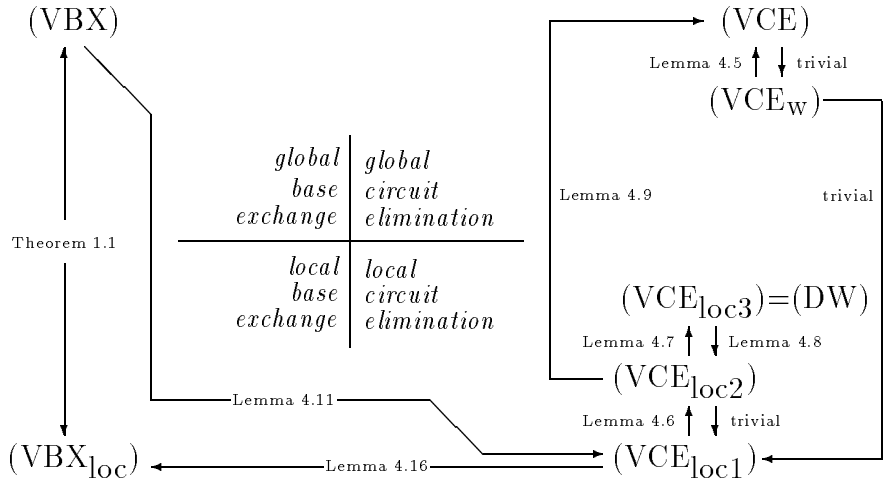

Figure 1: Relationship among global/local exchange and elimination properties

those global/local exchange and elimination properties as illustrated in Figure 1, where arrows mean implications under certain assumptions.

This paper is organized as follows. Section 2 explains a linear algebraic motivation of the circuit elimination property. Section 3 states our results: circuit axioms, vector axioms and the duality of valuated matroids in terms of circuits and vectors. Section 4 proves the results.

2 Linear algebraic motivation

A matroid captures combinatorial features of a matrix $A = (A_{ij} \in F : i \in I, j \in V)$ over a field F, where I and V respectively denote the row-set and the column-set of A. To be specific,

$$\mathcal{B} = \{B \subseteq V \mid \det A[B] \neq 0\}$$

is the base family of a matroid. Here $A[B]$ denotes the submatrix of A consisting of column indices in B. On the other hand, the family $\mathcal{C}$ of the supports of all elementary vectors of a linear subspace L satisfies the circuit axioms (MC1), (MC2) and (MCE). A vector $x = (x_i : i \in V) \in L$ is called an *elementary vector* of L if it has a nonempty minimal support, where the *support* is defined as the set $\{i \in V \mid x_i \neq 0\}$. If L is the kernel of A, $\mathcal{B}$ and $\mathcal{C}$ are the base and circuit families of the same matroid.

Suppose that $F = \mathbf{R}(s)$, the field of rational functions in a variable s with real coefficients. That is, consider a rational matrix $A(s) = (A_{ij}(s) \in \mathbf{R}(s) : i \in I, j \in V)$ with a variable s, where each component $A_{ij}(s)$ is a rational function in s over $\mathbf{R}$. The degree $\deg_s f$ of a rational function $f(s) = p(s)/q(s)$ expressed by two

polynomials $p(s)$ and $q(s)$ is defined to be $\deg_s p - \deg_s q$. Then the function ω on 2^V defined by

$$\omega(B) = \deg_s \det A[B], \tag{2.1}$$

that is, the degree of the determinant of $A[B]$ as a polynomial in s, is a valuation of the matroid defined by A as above ([9]; see also [20, §5.2.2]). The exchange property (VBX) can be understood as a combinatorial abstraction of the Grassmann-Plücker identity with respect to the degree; see [9] and [20, Remark 2.1.8].

The 'circuit family' and 'vector family' of a valuated matroid extract the combinatorial properties of a linear subspace L of $\mathbf{R}(s)^V$ with respect to the degree. Define $\mathcal{V} = \{\deg_s x = (\deg_s x_i : i \in V) \mid x \in L\}$ and let $\mathcal{X}$ be a subfamily of $\mathcal{V}$ consisting of the degrees of elementary vectors of L, i.e.,

$$\mathcal{X} = \{\deg_s x \mid x : \text{an elementary vector of } L\}.$$

The circuit axioms and the vector axioms, to be introduced in Section 3, are satisfied by $\mathcal{X}$ and $\mathcal{V}$, respectively. In particular, the elimination property (VCE) is a combinatorial abstraction of the following phenomenon. Take $x, y \in L$ and assume that $x_u = y_u = 1$. Since L is a subspace, $z = x - y$ belongs to L. For $X = \deg_s x$, $Y = \deg_s y$ and $Z = \deg_s z$, we have $X_u = Y_u \neq -\infty$ and $Z_i \leq \max(X_i, Y_i)$ for all $i \in V$. A crucial observation is that if $X_v > Y_v$, then no cancellation occurs in the leading term of z, and therefore $Z_v = X_v$. This is the content of (VCE). When the subspace L is defined as the kernel of a rational matrix $A(s)$, the valuated matroid defined from L in terms of the circuit family $\mathcal{X}$ (or vector family $\mathcal{V}$) coincides with the valuated matroid determined from $A(s)$ in terms of the function ω.

By way of a concrete example, let us consider the linear subspace L defined as the kernel of a polynomial matrix

$$A = \begin{bmatrix} 1 & 0 & s & s-1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \tag{2.2}$$

with a variable s and column-set $V = \{v_1, v_2, v_3, v_4\}$. The degrees of the elementary vectors of L are given as

$$\left\{ \begin{array}{l} (1,1,0,-\infty) + \alpha\mathbf{1}, (1,1,-\infty,0) + \alpha\mathbf{1}, \\ (0,-\infty,1,1) + \alpha\mathbf{1}, (-\infty,0,1,1) + \alpha\mathbf{1} \end{array} \middle| \, \alpha \in \mathbf{Z} \right\}. \tag{2.3}$$

For two vectors $X = (1,1,0,-\infty)$ and $Y = (-1,-\infty,0,0)$ in (2.3), we can select $v_1 \in \underline{X} \cap \underline{Y}$ as v with $X_v > Y_v$ in (VCE), and v_3 as u with $X_u = Y_u \neq -\infty$. Then $Z = (1,1,-\infty,0)$ is a valid choice in (VCE). Note that $X = \deg_s x$ and $Y = \deg_x y$ for $x = (-s, s-1, 1, 0)$ and $y = (1/(s-2), 0, 1, (-s+1)/(s-2))$, and $Z = \deg_s z$ for $z = x - y = ((-s^2+2s-1)/(s-2), s-1, 0, (s-1)/(s-2))$. Thus (VCE) is an

abstraction of a key combinatorial property of a linear subspace over $\mathbf{R}(s)$ (more generally, over a non-archimedian valuated field).

Remark 2.1 The circuit family of an oriented matroid captures combinatorial properties of a linear subspace L over an ordered field. More precisely, the set

$$\{\mathrm{sign}(x) = (\mathrm{sign}(x_i) : i \in V) \mid x : \text{an elementary vector of } L\}$$

is a canonical example of the circuit family of an oriented matroid. For any oriented matroid, the underlying matroid is obtained by ignoring signs. Conversely, a matroid is said to be orientable if there exists an oriented matroid associated in this way. We remark that there is a non-orientable matroid (see [4]), whereas every matroid admits a trivial valuation defined by (1.3).

Remark 2.2 A linear weighting yields a valuation in a natural way. Let p be an R-valued vector. A function $\omega : 2^V \to (R \cup \{-\infty\})$ defined by

$$\omega(B) = \begin{cases} \sum_{i \in B} p_i & \text{if } B \in \mathcal{B} \\ -\infty & \text{otherwise} \end{cases} \tag{2.4}$$

yields a valuation of a matroid $(V, \mathcal{B})$. It is emphasized, however, that not every valuation arises from a linear weighting. For instance, the valuation defined by (2.1) for the matrix $A(s)$ in (2.2) cannot be obtained from the linear weighting (2.4) by a vector p.

3 Results

3.1 Axioms of a valuated matroid

Cryptomorphically equivalent axioms of a valuated matroid in terms of bases, circuits and vectors are given as the main results of this paper.

We first derive axioms for circuits from those for bases. Let $(V, \mathcal{B}, \omega)$ be a valuated matroid. For each base $B \in \mathcal{B}$ and $v \in V - B$, we define $X(B, v) = (X(B, v)_u \mid u \in V) \in (R \cup \{-\infty\})^V$ by

$$X(B, v)_u = \omega(B - u + v) - \omega(B) \quad \text{for } u \in V. \tag{3.1}$$

From ω, we construct a family $\mathcal{X} = \Phi_{\omega \to \mathcal{X}}(\omega)$ of vectors in $(R \cup \{-\infty\})^V$ by

$$\Phi_{\omega \to \mathcal{X}}(\omega) = \{X(B, v) + \alpha \mathbf{1} \mid B \in \mathcal{B},\ v \in V - B,\ \alpha \in R\}. \tag{3.2}$$

Then $\underline{X(B, v)}$ coincides with the fundamental circuit $C(B, v)$ relative to B and v in matroid $(V, \mathcal{B})$, and hence, $\underline{\mathcal{X}} = \{\underline{X} \mid X \in \mathcal{X}\}$ is the circuit family of matroid $(V, \mathcal{B})$. Accordingly, we call $\mathcal{X} = \Phi_{\omega \to \mathcal{X}}(\omega)$ defined by (3.2) the *circuit family* of valuated matroid $(V, \mathcal{B}, \omega)$.

We can prove further properties of the circuit family as follows.

Theorem 3.1 *Given a valuated matroid $(V, \mathcal{B}, \omega)$, the circuit family $\mathcal{X} = \Phi_{\omega \to \mathcal{X}}(\omega)$ defined by (3.2) has the following properties:*

(VC1) $(-\infty, \cdots, -\infty) \notin \mathcal{X}$,

(VC2) *if* $X, Y \in \mathcal{X}$ *with* $\underline{X} \neq \underline{Y}$ *then* $\underline{X} \not\subseteq \underline{Y}$,

(VC3) *for* $X \in \mathcal{X}$ *and* $\alpha \in R$, $X + \alpha \mathbf{1} \in \mathcal{X}$ *holds,*

($\mathrm{VC3_e}$) *for* $X, Y \in \mathcal{X}$ *with* $\underline{X} = \underline{Y}$, *there exists* $\beta \in R$ *such that* $Y = X + \beta \mathbf{1}$,

($\mathrm{VCE_W}$) *for* $X, Y \in \mathcal{X}$ *and* $u, v \in V$ *with* $X_u = Y_u \neq -\infty$ *and* $v \in \underline{X} - \underline{Y}$, *there exists* $Z \in \mathcal{X}$ *such that* $Z_u = -\infty, Z_v = X_v$ *and* $Z \leq \max(X, Y)$,

(VCE) *for* $X, Y \in \mathcal{X}$ *and* $u, v \in V$ *with* $X_u = Y_u \neq -\infty$ *and* $X_v > Y_v$, *there exists* $Z \in \mathcal{X}$ *such that* $Z_u = -\infty, Z_v = X_v$ *and* $Z \leq \max(X, Y)$. ∎

The properties listed above are quantitative generalizations of the circuit axioms (MC1), (MC2) and (MCE) of matroids. To see this let us consider the case of a trivial valuation ω defined by (1.3). In this case, $X(B, v)$'s are $(0, -\infty)$-valued vectors, and (VC3) and ($\mathrm{VC3_e}$) together show that a member X of $\mathcal{X}$ can be identified with its support $\underline{X}$. Then (VC2) is identical with (MC2), and both ($\mathrm{VCE_W}$) and (VCE) reduce to the elimination property (MCE) of matroids, where it is noted that $X_v > Y_v$ in (VCE) is equivalent to $v \in \underline{X} - \underline{Y}$ in ($\mathrm{VCE_W}$) in this case. It is emphasized, however, that in the general case, we can select an element of $\underline{X} \cap \underline{Y}$ as v with $X_v > Y_v$ in (VCE) (e.g., see the example in (2.3)). This is a distinctive feature of valuated matroids.

We adopt properties (VC1), (VC2), (VC3) and (VCE) as *circuit axioms* of a valuated matroid. It will be shown in Theorem 3.3 that these axioms are cryptomorphically equivalent to base axioms (VB1) and (VBX).

Conditions ($\mathrm{VCE_W}$) and (VCE) are 'global' elimination properties in the sense that any two circuits can be selected, while the following are 'local' ones containing rank restrictions:

($\mathrm{VCE_{loc1}}$) for $X, Y \in \mathcal{X}$ and $u, v \in V$ such that $X_u = Y_u \neq -\infty$, $v \in \underline{X} - \underline{Y}$ and $\mathrm{rank}(\underline{X} \cup \underline{Y}) = |\underline{X} \cup \underline{Y}| - 2$, there exists $Z \in \mathcal{X}$ such that $Z_u = -\infty, Z_v = X_v$ and $Z \leq \max(X, Y)$,

($\mathrm{VCE_{loc2}}$) for $X, Y \in \mathcal{X}$ and $u \in V$ such that $X_u = Y_u \neq -\infty$ and $\mathrm{rank}(\underline{X} \cup \underline{Y}) = |\underline{X} \cup \underline{Y}| - 2$, there exists $Z \in \mathcal{X}$ such that $Z_u = -\infty$, $Z \leq \max(X, Y)$ and $Z_i = \max(X_i, Y_i)$ for any i with $X_i \neq Y_i$,

($\mathrm{VCE_{loc3}}$) for $X, Y, Z \in \mathcal{X}$ such that $\underline{X}$, $\underline{Y}$ and $\underline{Z}$ are mutually distinct and $\mathrm{rank}(\underline{X} \cup \underline{Y} \cup \underline{Z}) = |\underline{X} \cup \underline{Y} \cup \underline{Z}| - 2$, there exist $\alpha, \beta \in R$ such that $Z \leq$

$\max(X+\alpha\mathbf{1}, Y+\beta\mathbf{1})$ and $Z_i = \max(X_i+\alpha, Y_i+\beta)$ for any i with $X_i+\alpha \neq Y_i+\beta$.

We remark that ($\mathrm{VCE}_{\mathrm{loc3}}$) is a restatement of (DW), by Lemma 4.3 to be stated in Section 4. Note that ($\mathrm{VCE}_{\mathrm{W}}$) is a special case of (VCE) and that ($\mathrm{VC3}_{\mathrm{e}}$) follows from (VC2), (VC3) and (VCE). It is also true that (VCE) follows from ($\mathrm{VC3}_{\mathrm{e}}$) and ($\mathrm{VCE}_{\mathrm{W}}$), as is stated below. Furthermore, the above local elimination properties are also equivalent to (VCE).

Theorem 3.2 *Suppose that* $\mathcal{X} \subseteq (R\cup\{-\infty\})^V$ *satisfies* (VC1), (VC2) *and* (VC3). *Then the following statements are equivalent:*

(a) $\mathcal{X}$ *has* (VCE),

(b) $\mathcal{X}$ *has* ($\mathrm{VC3}_{\mathrm{e}}$) *and* ($\mathrm{VCE}_{\mathrm{W}}$),

(c) $\mathcal{X}$ *has* ($\mathrm{VC3}_{\mathrm{e}}$) *and* ($\mathrm{VCE}_{\mathrm{loc1}}$), *and* $\underline{\mathcal{X}}$ *has* (MCE),

(d) $\mathcal{X}$ *has* ($\mathrm{VC3}_{\mathrm{e}}$) *and* ($\mathrm{VCE}_{\mathrm{loc2}}$), *and* $\underline{\mathcal{X}}$ *has* (MCE),

(e) $\mathcal{X}$ *has* ($\mathrm{VC3}_{\mathrm{e}}$) *and* ($\mathrm{VCE}_{\mathrm{loc3}}$), *and* $\underline{\mathcal{X}}$ *has* (MCE). ∎

We next consider a construction of a valuation on bases from the circuit family. Let $\mathcal{X}$ be a subset of $(R\cup\{-\infty\})^V$ satisfying (VC1), (VC2), (VC3) and (VCE). Then $\underline{\mathcal{X}}$ is the circuit family of a matroid $\mathbf{M}$, with which the base family $\mathcal{B}$ is associated. We will define a function ω on $\mathcal{B}$. For a fixed base $B_0 \in \mathcal{B}$, we assign an arbitrary value in R to $\omega(B_0)$. For $u \in B_0$ and $v \in V - B_0$ with $B = B_0 - u + v \in \mathcal{B}$, by (VC3) and ($\mathrm{VC3}_{\mathrm{e}}$), there is a unique $X \in \mathcal{X}$ such that $\underline{X} = C(B_0, v)$ and $X_v = 0$. Then we set $\omega(B) = \omega(B_0) + X_u$. We determine $\omega(B)$ for any $B \in \mathcal{B}$ in a similar manner from those bases which are already assigned ω-values. More precisely, consider a graph $G(\mathcal{B})$ with vertex set $\mathcal{B}$, in which two bases B and B' are adjacent to each other if and only if $|B \triangle B'| = 2$. The graph $G(\mathcal{B})$ is sometimes called the *base graph*. From (MBX), $G(\mathcal{B})$ is connected. That is, for any base B, there is a path P from B_0 to B, where we think of P as a sequence $B_0, B_1, \ldots, B_k = B$ of bases. For each base B_i ($i = 0, 1, \ldots, k-1$), let $\{v_i\} = B_{i+1} - B_i$, $\{u_i\} = B_i - B_{i+1}$ and X^i be the unique element in $\mathcal{X}$ such that $\underline{X}^i = C(B_i, v_i)$ and $X^i_{v_i} = 0$. We define the value $\omega_P(B)$ of B along P by

$$\omega_P(B) = \omega(B_0) + \sum_{i=0}^{k-1} X^i_{u_i}.$$

In Theorem 3.3, we will prove that $\omega_P(B)$ is determined independently of the choice of a path P connecting B_0 to B. Thus, we can define ω by

$$\omega(B) = \omega(B_0) + \sum_{i=0}^{k-1} X^i_{u_i} \quad \text{for any } B \in \mathcal{B}, \tag{3.3}$$

where $B_0, B_1, \ldots, B_k = B$ is a path in $G(\mathcal{B})$. We denote by $\Phi_{\mathcal{X}\to\omega}$ the above construction of a function ω on bases from a family $\mathcal{X}$ satisfying (VC1) to (VCE).

Theorem 3.3 *For a family $\mathcal{X}$ of vectors in $(R\cup\{-\infty\})^V$ satisfying* (VC1), (VC2), (VC3) *and* (VCE),

(1) *$\omega = \Phi_{\mathcal{X}\to\omega}(\mathcal{X})$ is well-defined, i.e., $\omega(B)$ for each $B \in \mathcal{B}$ is uniquely determined from $\omega(B_0)$ by (3.3),*

(2) *ω is a valuation on bases, i.e., ω satisfies* (VB1) *and* (VBX),

(3) *$\Phi_{\omega\to\mathcal{X}}(\Phi_{\mathcal{X}\to\omega}(\mathcal{X})) = \mathcal{X}$ and $\Phi_{\mathcal{X}\to\omega}(\Phi_{\omega\to\mathcal{X}}(\omega)) = \omega + \text{constant}$.* ∎

Theorems 3.1 and 3.3 together say that base axioms and circuit axioms of a valuated matroid are cryptomorphically equivalent. To be more precise, let Ω be the set of $\omega : 2^V \to (R \cup \{-\infty\})$ satisfying (VB1) and (VBX), and Γ be the set of $\mathcal{X} \subseteq (R \cup \{-\infty\})^V$ satisfying (VC1), (VC2), (VC3) and (VCE). Then we have $\Phi_{\omega\to\mathcal{X}} : \Omega \to \Gamma$ and $\Phi_{\mathcal{X}\to\omega} : \Gamma \to \Omega$, where the mapping $\Phi_{\mathcal{X}\to\omega}$ is dependent on the fixed initial value $\omega(B_0)$. Theorem 3.3(3) shows that $\Phi_{\omega\to\mathcal{X}}$ and $\Phi_{\mathcal{X}\to\omega}$ establish a bijection between Γ and the equivalence classes of Ω, in which ω and ω' are equivalent if and only if $\omega = \omega' + \alpha$ for some constant $\alpha \in R$. Hence we may write a valuated matroid as $(V, \mathcal{B}, \omega, \mathcal{X})$, $(V, \omega, \mathcal{X})$ or $(V, \mathcal{X})$.

We next discuss cryptomorphic equivalence between circuits and vectors of valuated matroids. Given a valuated matroid $(V, \mathcal{X})$, we define a family $\mathcal{V} = \Phi_{\mathcal{X}\to\mathcal{V}}(\mathcal{X})$ by taking componentwise maxima of any finite collection of circuits, i.e.,

$$\Phi_{\mathcal{X}\to\mathcal{V}}(\mathcal{X}) = \{X \mid X = \max(X^1, \ldots, X^k), k \geq 0, X^i \in \mathcal{X}\}, \tag{3.4}$$

where $(-\infty, \ldots, -\infty) = \max(\emptyset)$ by convention.

Theorem 3.4 *For a family $\mathcal{X} \subseteq (R \cup \{-\infty\})^V$ satisfying the circuit axioms* (VC1), (VC2), (VC3) *and* (VCE) *of a valuated matroid, $\mathcal{V} = \Phi_{\mathcal{X}\to\mathcal{V}}(\mathcal{X})$ defined by (3.4) has the following properties:*

(VV1) *$(-\infty, \ldots, -\infty) \in \mathcal{V}$,*

(VV2) *if $X, Y \in \mathcal{V}$, then $\max(X, Y) \in \mathcal{V}$,*

(VV3) *for $X \in \mathcal{V}$ and $\alpha \in R$, we have $X + \alpha\mathbf{1} \in \mathcal{V}$,*

(VVE) *for $X, Y \in \mathcal{V}$ and $u \in V$ with $X_u = Y_u \neq -\infty$, there is $Z \in \mathcal{V}$ such that $Z_u = -\infty$, $Z \leq \max(X, Y)$ and $Z_i = \max(X_i, Y_i)$ for all i with $X_i \neq Y_i$.* ∎

We call a member of $\mathcal{V}$ a *vector* of the valuated matroid and conditions (VV1) through (VVE) *vector axioms*.

For $\mathcal{S} \subseteq (R \cup \{-\infty\})^V$ in general, let us define

$$\text{Minsupp}(\mathcal{S}) = \{S \in \mathcal{S} \mid S \text{ has a nonempty minimal support in } \mathcal{S}\}. \tag{3.5}$$

Given a family $\mathcal{V}$ of vectors satisfying the vector axioms, we define $\Phi_{\mathcal{V}\to\mathcal{X}}$ by

$$\Phi_{\mathcal{V}\to\mathcal{X}}(\mathcal{V}) = \text{Minsupp}(\mathcal{V}). \tag{3.6}$$

Theorem 3.5 *For a family $\mathcal{V}$ of vectors satisfying the vector axioms* (VV1), (VV2), (VV3) *and* (VVE), *$\mathcal{X} = \Phi_{\mathcal{V}\to\mathcal{X}}(\mathcal{V})$ defined by (3.6) satisfies the circuit axioms* (VC1), (VC2), (VC3) *and* (VCE). ∎

Theorem 3.6 *Let $\mathcal{X}$ and $\mathcal{V}$ be families of vectors in $(R \cup \{-\infty\})^V$ satisfying the circuit axioms and the vector axioms, respectively. Then, $\Phi_{\mathcal{V}\to\mathcal{X}}(\Phi_{\mathcal{X}\to\mathcal{V}}(\mathcal{X})) = \mathcal{X}$ and $\Phi_{\mathcal{X}\to\mathcal{V}}(\Phi_{\mathcal{V}\to\mathcal{X}}(\mathcal{V})) = \mathcal{V}$.* ∎

Theorems 3.4, 3.5 and 3.6 say that the circuit axioms and the vector axioms are cryptomorphically equivalent. Hence, the base axioms and the vector axioms are also cryptomorphically equivalent. The correspondence between valuations on bases and vector families is given by

$$\Phi_{\omega\to\mathcal{V}} = \Phi_{\mathcal{X}\to\mathcal{V}} \circ \Phi_{\omega\to\mathcal{X}} \quad \text{and} \quad \Phi_{\mathcal{V}\to\omega} = \Phi_{\mathcal{X}\to\omega} \circ \Phi_{\mathcal{V}\to\mathcal{X}}.$$

We may write a valuated matroid as a full tuple $(V, \mathcal{B}, \omega, \mathcal{X}, \mathcal{V})$ or as its sub-tuple.

For a function $\omega : 2^V \to (R \cup \{-\infty\})$ and $p \in R^V$, we define $\omega[p]$ by

$$\omega[p](B) = \omega(B) + \sum_{i\in B} p_i.$$

For any family $\mathcal{S}$ of vectors in $(R \cup \{-\infty\})^V$ and any $p \in R^V$, we define $\mathcal{S}[p]$ by

$$\mathcal{S}[p] = \{X + p \mid X \in \mathcal{S}\}.$$

The relation

$$\omega[p](B - i + v) - \omega[p](B) = \omega(B - i + v) - \omega(B) + p_v - p_i$$

implies that, if $(V, \omega, \mathcal{X}, \mathcal{V})$ is a valuated matroid, so is $(V, \omega[p], \mathcal{X}[-p], \mathcal{V}[-p])$. In particular,

$$\Phi_{\omega\to\mathcal{X}}(\omega[p]) = \mathcal{X}[-p] \quad \text{and} \quad \Phi_{\omega\to\mathcal{V}}(\omega[p]) = \mathcal{V}[-p]. \tag{3.7}$$

By (VBX), the maximizers of ω forms the base family of some matroid. We mention in passing a characterization of the maximizers of ω in terms of circuits

of the valuated matroid. For any $X = (X_i \mid i \in V) \in (R \cup \{-\infty\})^V$, let $\mathrm{Max}(X)$ denote the maximizers of X, that is,

$$\mathrm{Max}(X) = \{i \in V \mid X_i = \max(X_1, \ldots, X_{|V|})\}.$$

Given a set $\mathcal{S}$ of vectors in $(R \cup \{-\infty\})^V$, we define

$$\mathrm{Max}(\mathcal{S}) = \{\mathrm{Max}(X) \mid X \in \mathcal{S}\}.$$

We also define $\mathrm{Minsupp}(\mathcal{S}) = \{S \in \mathcal{S} \mid S \text{ is nonempty minimal in } \mathcal{S}\}$ for a family $\mathcal{S}$ of subsets of V with a slight abuse of notation (3.5).

Theorem 3.7 *Let $(V, \mathcal{B}, \omega, \mathcal{X})$ be a valuated matroid. Suppose that $\mathcal{B}_0$ denotes the family of maximizers in $\mathcal{B}$ with respect to ω, i.e., $\mathcal{B}_0 = \{B \in \mathcal{B} \mid \omega(B) = \max_{B' \in \mathcal{B}} \omega(B')\}$, and that $\mathcal{C}_0$ is the circuit family of matroid $\mathbf{M}_0 = (V, \mathcal{B}_0)$. Then $\mathcal{C}_0 = \mathrm{Minsupp}(\mathrm{Max}(\mathcal{X}))$.* ∎

3.2 Duality

Given a valuated matroid $\mathbf{M} = (V, \mathcal{B}, \omega)$, its *dual* $\mathbf{M}^* = (V, \mathcal{B}^*, \omega^*)$ is defined by

$$\mathcal{B}^* = \{V - B \mid B \in \mathcal{B}\}, \tag{3.8}$$

$$\omega^*(B^*) = \omega(V - B^*) \quad \text{for } B^* \in \mathcal{B}^*. \tag{3.9}$$

Then the circuit family $\mathcal{X}^*$ and the vector family $\mathcal{V}^*$ of $\mathbf{M}^*$ are induced from ω^* as $\mathcal{X}^* = \Phi_{\omega \to \mathcal{X}}(\omega^*)$ and $\mathcal{V}^* = \Phi_{\omega \to \mathcal{V}}(\omega^*)$, respectively. Hence $\mathcal{X}^*$ and $\mathcal{V}^*$ are determined from $\mathcal{X}$ and $\mathcal{V}$ by

$$\mathcal{X}^* = \Phi_{\omega \to \mathcal{X}}(\Phi_{\mathcal{X} \to \omega}(\mathcal{X})^*) = \Phi_{\omega \to \mathcal{X}}(\Phi_{\mathcal{V} \to \omega}(\mathcal{V})^*),$$
$$\mathcal{V}^* = \Phi_{\omega \to \mathcal{V}}(\Phi_{\mathcal{X} \to \omega}(\mathcal{X})^*) = \Phi_{\omega \to \mathcal{V}}(\Phi_{\mathcal{V} \to \omega}(\mathcal{V})^*).$$

The objective of this section is to characterize $\mathcal{X}^*$ and $\mathcal{V}^*$ in terms of the orthogonality to $\mathcal{X}$ and $\mathcal{V}$ without referring to the defining relation (3.9) between ω and ω^*. We call an element of $\mathcal{X}^*$ a *cocircuit* of $\mathbf{M}$ and that of $\mathcal{V}^*$ a *covector* of $\mathbf{M}$.

For $X, Y \in (R \cup \{-\infty\})^V$, we say that X and Y are *orthogonal* to each other if

$$|\mathrm{Max}(X + Y)| \neq 1, \tag{3.10}$$

where we assume that $\mathrm{Max}((-\infty, \ldots, -\infty)) = \emptyset$. We write $X \perp Y$ if X and Y are orthogonal. Note that if $\underline{X} \cap \underline{Y} = \emptyset$ then $\mathrm{Max}(X + Y) = \emptyset$, and hence, $X \perp Y$. Given a set $\mathcal{S}$ of vectors in $(R \cup \{-\infty\})^V$, let us define $\mathcal{S}^\perp$ by

$$\mathcal{S}^\perp = \{Y \in (R \cup \{-\infty\})^V \mid X \perp Y \text{ for all } X \in \mathcal{S}\}. \tag{3.11}$$

Theorem 3.8 *For a valuated matroid* $(V, \mathcal{X}, \mathcal{V})$ *and its dual* $(V, \mathcal{X}^*, \mathcal{V}^*)$,

(1) $\mathcal{V}^* = \mathcal{X}^\perp = \mathcal{V}^\perp$,

(2) $\mathcal{X}^* = \mathrm{Minsupp}(\mathcal{X}^\perp) = \mathrm{Minsupp}(\mathcal{V}^\perp)$. ∎

Theorem 3.8 is a generalization of a well-known statement in matroid theory: a set $\mathcal{C}^*$ of subsets of V is the set of cocircuits of a matroid $\mathbf{M}$ on V if and only if $\mathcal{C}^*$ consists of the nonempty minimal subsets C^* of V such that $|C \cap C^*| \neq 1$ for every circuit C of $\mathbf{M}$.

Let p be any vector in R^V. From (3.10), $X, Y \in (R \cup \{-\infty\})^V$ are orthogonal if and only if $(X + p) \perp (Y - p)$. Hence, for any family $\mathcal{S}$ of vectors in $(R \cup \{-\infty\})^V$,

$$(\mathcal{S}[p])^\perp = \mathcal{S}^\perp[-p].$$

Theorem 3.8 immediately implies the following observation.

Corollary 3.9 *For a valuated matroid* $(V, \mathcal{X}, \mathcal{V})$ *and* $p \in R^V$,

(1) $(\mathcal{V}[p])^* = \mathcal{V}^*[-p]$,

(2) $(\mathcal{X}[p])^* = \mathcal{X}^*[-p]$. ∎

Minty's painting theorem for matroids can be generalized for valuated matroids. Consider a partition of V into three disjoint subsets G, B, W with $|G| = 1$. We call such a partition a *painting*, since we can regard the partition as a painting on V by green, black and white. Minty [12] (see also [26]) proposed a characterization of a matroid via an alternative property.

Theorem 3.10 ([12]) *Let* $\mathcal{C}$ *and* $\mathcal{D}$ *be two families of subsets of* V *each satisfying* (MC1) *and* (MC2). *Then,* $\mathcal{C}$ *and* $\mathcal{D}$ *are the families of circuits and cocircuits of a matroid if and only if the following conditions hold:*

(1) *for any* $C \in \mathcal{C}$ *and* $D \in \mathcal{D}$, *it holds that* $|C \cap D| \neq 1$;

(2) *for any painting* G, B, W *of* V, *either*

  (a) $\exists C \in \mathcal{C}$ *such that* $G \subseteq C \subseteq G \cup B$, *or*

  (b) $\exists D \in \mathcal{D}$ *such that* $G \subseteq D \subseteq G \cup W$. ∎

The generalization to a valuated matroid is as follows. We say that a pair of families $\mathcal{S}$ and $\mathcal{T}$ of vectors in $(R \cup \{-\infty\})^V$ satisfies an *alternative painting property* if for any painting of V, either

(a) $\exists X \in \mathcal{S}$ such that $G \subseteq \mathrm{Max}(X) \subseteq G \cup B$, or

(b) $\exists Y \in \mathcal{T}$ such that $G \subseteq \mathrm{Max}(Y) \subseteq G \cup W$.

We obtain two characterizations of valuated matroids by using the alternative painting property as below.

Theorem 3.11 *Let $\mathcal{X}$ and $\mathcal{Y}$ be two families of vectors in $(R \cup \{-\infty\})^V$, each satisfying* (VC1), (VC2), (VC3) *and* (VC3$_{\mathrm{e}}$). *Then, $\mathcal{X}$ and $\mathcal{Y}$ are the families of circuits and cocircuits of a valuated matroid if and only if the following conditions hold:*

(1) *for any $X \in \mathcal{X}$ and $Y \in \mathcal{Y}$, it holds that $|\mathrm{Max}(X + Y)| \neq 1$, i.e., $X \perp Y$;*

(2) *the pair of $\mathcal{X}[p]$ and $\mathcal{Y}[-p]$ satisfies the alternative painting property for any $p \in R^V$.* ∎

Theorem 3.12 *Let $\mathcal{X}$ be a family of vectors in $(R \cup \{-\infty\})^V$ satisfying* (VC1), (VC2), (VC3) *and* (VC3$_{\mathrm{e}}$). *Then, $\mathcal{X}$ is the circuit family of a valuated matroid if and only if the pair of $\mathcal{X}[p]$ and $\mathrm{Minsupp}(\mathcal{X}^\perp[-p])$ satisfies the alternative painting property for any $p \in R^V$.* ∎

Remark 3.13 We cannot delete (VC3$_{\mathrm{e}}$) from the assumptions in Theorem 3.12. For example, consider a family $\mathcal{X} = \{(\alpha, \alpha, \beta, \beta) \mid \alpha, \beta \in R\}$ of R-valued vectors on $V = \{v_1, v_2, v_3, v_4\}$. Obviously, $\mathcal{X}$ satisfies (VC1), (VC2) and (VC3), but violates (VC3$_{\mathrm{e}}$). Thus, $\mathcal{X}$ is not the circuit family of any valuated matroid. $\mathcal{X}[p]$, however, satisfies the alternative painting property for all $p \in R^V$ as below. By the definition of orthogonality, we have

$$(0, 0, -\infty, -\infty), (-\infty, -\infty, 0, 0) \in \mathrm{Minsupp}(\mathcal{X}^\perp).$$

Given a vector p, let M be a number larger than $\max(p_1, p_2, p_3, p_4)$. From the symmetry of $\mathcal{X}$, we may assume that v_1 is painted by green (i.e., $G = \{v_1\}$), and consider two cases when either $v_2 \in B$ or $v_2 \in W$. In the first case, if $p_1 \geq p_2$ then $(0, 0, -M, -M) \in \mathcal{X}$ satisfies (a) of the alternative painting property; otherwise, $(0, 0, -\infty, -\infty) \in \mathrm{Minsupp}(\mathcal{X}^\perp)$ does (b) of the alternative painting property. In the second case, if $p_1 > p_2$ then $(0, 0, -M, -M) \in \mathcal{X}$ satisfies (a) of the alternative painting property; otherwise, $(0, 0, -\infty, -\infty) \in \mathrm{Minsupp}(\mathcal{X}^\perp)$ meets (b) of the alternative painting property. ∎

4 Proofs

The proofs of the theorems are given in this section.

4.1 Preliminaries

Let $(V, \mathcal{B}, \omega)$ be a valuated matroid. For $B \in \mathcal{B}$ and $B' \subseteq V$, we consider a weighted bipartite graph $G(B, B')$ with vertex bipartition $(B - B', B' - B)$, edge set $\{(u, v) \mid u \in B - B',\ v \in B' - B,\ B - u + v \in \mathcal{B}\}$ and edge weight $w((u, v)) = \omega(B - u + v) - \omega(B)$ for every edge (u, v). We call $G(B, B')$ the *exchangeability graph* for B, B'. We denote by $\widehat{\omega}(B, B')$ the maximum weight of a perfect matching in $G(B, B')$. The following two lemmas are known.

Lemma 4.1 (Upper-bound lemma [14]; see [20, Lemma 5.2.29]) *For $B, B' \in \mathcal{B}$,*

$$\omega(B') \leq \omega(B) + \widehat{\omega}(B, B').$$ ∎

The following lemmas are also useful in our proofs.

Lemma 4.2 *Let $(V, \mathcal{B}, \omega)$ be a valuated matroid, B and B' be two distinct bases and u an element of $B - B'$. If*

$$\omega(B) + \omega(B') < \max_{v \in B' - B} \{\omega(B - u + v) + \omega(B' - v + u)\},$$

then there are at least two maximizers $v \in B' - B$. In other words, if the maximizer is unique, then

$$\omega(B) + \omega(B') = \max_{v \in B' - B} \{\omega(B - u + v) + \omega(B' - v + u)\}.$$

Proof. Let $B' - B = \{v_1, v_2, \ldots\}$, $B_i = B - u + v_i$ and $B'_i = B' - v_i + u$. From (VBX) for B_i, B'_i, v_i, there exists $e \in B'_i - B_i = (B' - B) + u - v_i$ such that

$$\begin{aligned} \omega(B_i) + \omega(B'_i) &\leq \omega(B_i - v_i + e) + \omega(B'_i - e + v_i) \\ &= \omega(B - u + e) + \omega(B' - e + u). \end{aligned}$$

Without loss of generality, we assume that v_1 is a maximizer of $\max_{v \in B' - B} \{\omega(B - u + v) + \omega(B' - v + u)\}$. Since $\omega(B) + \omega(B') < \omega(B_1) + \omega(B'_1)$, u cannot be e. Hence $e = v_j$ for some $j \neq 1$, i.e.,

$$\omega(B_1) + \omega(B'_1) \leq \omega(B_j) + \omega(B'_j).$$

Since v_1 is a maximizer, the above inequality holds as equality, and hence, v_j is also a maximizer. ∎

Lemma 4.3 *Let C_1, C_2 and C_3 be distinct circuits of a matroid on V.*

(1) *The following three conditions are equivalent:*

(a) $\mathrm{rank}(C_1 \cup C_2) = |C_1 \cup C_2| - 2$,

(b) *for any circuit* $C \subseteq C_1 \cup C_2$, *we have* $C = C_1$ *or* $C = C_2$ *or* $C_1 \triangle C_2 \subseteq C$,

(c) *for any* $u \in C_1 - C_2$, *there exist a base* B *and* $v \in C_2 - C_1$ *such that* $C_1 = C(B,u)$ *and* $C_2 = C(B,v)$.

(2) *If* $\mathrm{rank}(C_1 \cup C_2) < |C_1 \cup C_2| - 2$, *there exists a circuit* $C \subseteq (C_1 \cup C_2) - \{u,v\}$ *for any* $u \in C_1 - C_2$ *and* $v \in C_2 - C_1$.

(3) *If* $\mathrm{rank}(C_1 \cup C_2 \cup C_3) = |C_1 \cup C_2 \cup C_3| - 2$, *then* $C_1 \cup C_2 \cup C_3 = C_i \cup C_j$ *for any* i, j *with* $i \neq j$.

Proof. We first prove the assertion (1).

(a)⇒(c): For any $u \in C_1 - C_2$, $C_1 - u$ is independent. Let I be a maximal independent set containing $C_1 - u$ in $C_1 \cup C_2$ and B be a base containing I. Since $\mathrm{rank}(C_1 \cup C_2) = |C_1 \cup C_2| - 2$, there exist a unique element $v \in C_2 - B$. Hence $C_1 = C(B,u)$ and $C_2 = C(B,v)$.

(c)⇒(b): Let u be any element in $C_1 - C_2$ and let B and v be a base and an element of $C_2 - C_1$ such that $C_1 = C(B,u)$ and $C_2 = C(B,v)$. Let C be any circuit with $C \subseteq C_1 \cup C_2$. Since C is dependent, C contains u or v. If C contains exactly one of u and v, then C coincides with $C_1 = C(B,u)$ or $C_2 = C(B,v)$. Suppose that C contains both u and v, and that $C_1 \triangle C_2 \not\subseteq C$. Let w be any element in $(C_1 \triangle C_2) - C$. Without loss of generality, we assume $w \in C_1$. Obviously, $B' = B - w + u$ is a base and $B' + v$ contains distinct circuits C and C_2 both containing v. This is a contradiction. Hence (b) holds.

(b)⇒(a): Let u and v be any elements in $C_1 - C_2$ and $C_2 - C_1$, respectively. Obviously, $\mathrm{rank}((C_1 \cup C_2) - \{u,v\}) = \mathrm{rank}(C_1 \cup C_2)$. If $\mathrm{rank}(C_1 \cup C_2) \leq |C_1 \cup C_2| - 3$, then $(C_1 \cup C_2) - \{u,v\}$ is dependent, and therefore, it contains a circuit C which satisfies $C \neq C_1, C_2$ and $C_1 \triangle C_2 \not\subseteq C$. This argument also shows the assertion (2).

We finally prove (3). Suppose there exists $u \in C_3 - (C_1 \cup C_2)$, and put $X = (C_1 \cup C_2 \cup C_3) - u$. Since $\mathrm{rank}(X) = |X| - 1$, $X - v$ is independent for some $v \in X$, where $v \in C_1 \cap C_2$ must hold. The elimination axiom (MCE) shows that $(C_1 \cup C_2) - v$ contains a circuit, whereas it is contained in an independent set $X - v$. This is a contradiction, and hence, $C_3 \subseteq C_1 \cup C_2$. ∎

4.2 Proofs of Theorems 3.1 and 3.2

First we prove Theorem 3.2. We have obvious implications:

- (VCE) ⇒ ($\mathrm{VCE_W}$) ⇒ ($\mathrm{VCE_{loc1}}$),
- (VC3) and (VCE) ⇒ $\underline{\mathcal{X}}$ has (MCE),

- $(\mathrm{VCE}_{\mathrm{loc2}}) \Rightarrow (\mathrm{VCE}_{\mathrm{loc1}})$.

We prove the remaining parts of Theorem 3.2 by establishing the following lemmas.

Lemma 4.4 *Conditions* (VC2), (VC3) *and* (VCE) *imply* $(\mathrm{VC3_e})$.

Proof. Suppose that there exist $X, Y \in \mathcal{X}$ such that $\underline{X} = \underline{Y}$ and $Y \neq X + \beta\mathbf{1}$ for any $\beta \in R$. For any $u \in \underline{X}$, consider $\beta \in R$ with $Y_u = X_u + \beta$. The assumption says that there exists $v \in \underline{X}$ with $Y_v \neq X_v + \beta$. (VC3) guarantees that $X + \beta\mathbf{1} \in \mathcal{X}$, and furthermore, (VCE) for $Y, X + \beta\mathbf{1}, u, v$ implies that there exists $Z \in \mathcal{X}$ such that $\emptyset \neq \underline{Z} \subsetneq \underline{X}$. This contradicts (VC2). Hence, $(\mathrm{VC3_e})$ holds. ∎

Lemma 4.5 *Conditions* (VC2), (VC3), $(\mathrm{VC3_e})$ *and* $(\mathrm{VCE_W})$ *imply* (VCE).

Proof. From (VC3), fix $X, Y \in \mathcal{X}$ and $u, v \in V$ with $X_u = Y_u = 0$ and $X_v > Y_v$. If $Y_v = -\infty$, then (VCE) follows immediately from $(\mathrm{VCE_W})$. Hence we assume that $Y_v \neq -\infty$. We prove (VCE) by induction on $|\underline{Y} - \underline{X}|$. From $(\mathrm{VC3_e})$, we have $\underline{X} \neq \underline{Y}$. Furthermore, by (VC2), $|\underline{Y} - \underline{X}| \geq 1$. In other word, if $|\underline{Y} - \underline{X}| = 0$ then (VCE) holds. Let v' be any element of $\underline{Y} - \underline{X}$. From $(\mathrm{VCE_W})$ for Y, X, u, v', there exists $\widehat{Z} \in \mathcal{X}$ such that $\widehat{Z}_u = -\infty$, $\widehat{Z}_{v'} = Y_{v'}$ and $\widehat{Z} \leq \max(Y, X)$. If $\widehat{Z}_v = X_v$ then $Z = \widehat{Z}$ is a valid choice in (VCE) for X, Y, u, v. Assume that $\widehat{Z}_v < X_v$. By applying $(\mathrm{VCE_W})$ for $Y, \widehat{Z}, v', u$, we obtain $\widehat{Y} \in \mathcal{X}$ such that $\widehat{Y}_{v'} = -\infty$, $\widehat{Y}_u = Y_u = 0$ and $\widehat{Y} \leq \max(Y, \widehat{Z}) \leq \max(X, Y)$. In particular, $\widehat{Y}_v \leq \max(Y_v, \widehat{Z}_v) < X_v$ holds. Since $|\underline{\widehat{Y}} - \underline{X}| < |\underline{Y} - \underline{X}|$, the induction hypothesis guarantees the existence of $Z \in \mathcal{X}$ such that $Z_u = -\infty$, $Z_v = X_v$ and $Z \leq \max(X, \widehat{Y}) \leq \max(X, Y)$. Hence, $\mathcal{X}$ has (VCE). ∎

Lemma 4.6 *Suppose that* $\underline{\mathcal{X}}$ *is the circuit family of a matroid. Then* $(\mathrm{VC3_e})$ *and* $(\mathrm{VCE}_{\mathrm{loc1}})$ *imply* $(\mathrm{VCE}_{\mathrm{loc2}})$.

Proof. Let X and Y be any elements of $\mathcal{X}$ with $\mathrm{rank}(\underline{X} \cup \underline{Y}) = |\underline{X} \cup \underline{Y}| - 2$ and u be any element with $X_u = Y_u \neq -\infty$. Suppose that v is any element of $\underline{X} - \underline{Y}$. By $(\mathrm{VCE}_{\mathrm{loc1}})$ for X, Y, u, v, there exists $Z \in \mathcal{X}$ such that $Z_u = -\infty$, $Z_v = X_v$ and $Z \leq \max(X, Y)$. Lemma 4.3 guarantees that $\underline{X} \triangle \underline{Y} \subseteq \underline{Z}$ because $\underline{Z} \neq \underline{X}, \underline{Y}$. Furthermore, we have $\mathrm{rank}(\underline{X} \cup \underline{Z}) = \mathrm{rank}(\underline{Y} \cup \underline{Z}) = |\underline{X} \cup \underline{Z}| - 2 = |\underline{Y} \cup \underline{Z}| - 2$.

Claim 1: $Y_i \leq \max(X_i, Z_i)$. By $(\mathrm{VCE}_{\mathrm{loc1}})$ for X, Z, v, u, there exists $W \in \mathcal{X}$ such that $W_v = -\infty$, $W_u = X_u = Y_u$ and $W \leq \max(X, Z)$. Obviously, $\underline{W} \subseteq \underline{X} \cup \underline{Y}$ holds. Since $W_v = -\infty$, we have $\underline{W} \neq \underline{X}$ and $\underline{X} \triangle \underline{Y} \not\subseteq \underline{W}$. If the claim failed, we would have $\underline{W} \neq \underline{Y}$ from $W_u = Y_u \neq -\infty$, $W_i \leq \max(X_i, Z_i) < Y_i$ and $(\mathrm{VC3_e})$. This contradicts (1) of Lemma 4.3.

Claim 2: $X_i \leq \max(Y_i, Z_i)$. Let w be any element of $\underline{Y} - \underline{X}$. Claim 1 says that $Z_w = Y_w$. From $(\mathrm{VCE}_{\mathrm{loc1}})$ for Y, Z, w, u, there exists $W \in \mathcal{X}$ such that $W_w = -\infty$, $W_u = Y_u = X_u$ and $W \leq \max(Y, Z)$. The claim can be proven similarly as Claim 1.

Claims 1 and 2 imply that $Z_i = \max(X_i, Y_i)$ if $X_i \neq Y_i$, i.e., that Z is a valid choice in ($\mathrm{VCE}_{\mathrm{loc2}}$). ∎

Lemma 4.7 *Suppose that $\underline{\mathcal{X}}$ is the circuit family of a matroid. Then* (VC3), ($\mathrm{VC3_e}$) *and* ($\mathrm{VCE}_{\mathrm{loc2}}$) *imply* ($\mathrm{VCE}_{\mathrm{loc3}}$).

Proof. Assume that X, Y and Z satisfy the assumption of ($\mathrm{VCE}_{\mathrm{loc3}}$). Let $\widehat{\alpha}$ and $\widehat{\beta}$ be the minimum numbers among α and β satisfying

$$Z_{\underline{X}-\underline{Y}} \leq (X + \alpha\mathbf{1})_{\underline{X}-\underline{Y}} \quad \text{and} \quad Z_{\underline{Y}-\underline{X}} \leq (Y + \beta\mathbf{1})_{\underline{Y}-\underline{X}}.$$

Lemma 4.3 and (VC3) guarantee the existence of these numbers. Let $\widehat{X} = X + \widehat{\alpha}\mathbf{1}$ and $\widehat{Y} = Y + \widehat{\beta}\mathbf{1}$. Suppose that $Z_a = \widehat{X}_a$ and $Z_b = \widehat{Y}_b$ for $a \in \underline{X} - \underline{Y}$ and $b \in \underline{Y} - \underline{X}$. Lemma 4.3 guarantees that

$$\mathrm{rank}(\underline{\widehat{X}} \cup \underline{\widehat{Y}}) = \mathrm{rank}(\underline{\widehat{X}} \cup \underline{Z}) = |\underline{\widehat{X}} \cup \underline{\widehat{Y}}| - 2 = |\underline{\widehat{X}} \cup \underline{Z}| - 2. \tag{4.1}$$

By ($\mathrm{VCE}_{\mathrm{loc2}}$) for $\widehat{X}, Z, a$, there exists $W \in \mathcal{X}$ such that $W_a = -\infty$, $W \leq \max(\widehat{X}, Z)$ and $W_i = \max(\widehat{X}_i, Z_i)$ if $\widehat{X}_i \neq Z_i$. Obviously,

$$\underline{W} \subseteq \underline{\widehat{X}} \cup \underline{\widehat{Y}} \tag{4.2}$$

holds. Since $W_a = -\infty$, we have

$$\underline{W} \neq \underline{\widehat{X}} \quad \text{and} \quad \underline{\widehat{X}} \triangle \underline{\widehat{Y}} \not\subseteq \underline{W}. \tag{4.3}$$

Claim 1: $Z_{\underline{X}-\underline{Y}} = \widehat{X}_{\underline{X}-\underline{Y}}$ and $Z_{\underline{Y}-\underline{X}} = \widehat{Y}_{\underline{Y}-\underline{X}}$. Suppose that there exists $j \in \underline{X} - \underline{Y}$ with $Z_j < \widehat{X}_j$. In this case, $W_j = \widehat{X}_j \neq -\infty$ holds, and hence, $\underline{W} \neq \underline{\widehat{Y}}$. However, (4.1), (4.2), (4.3) and this contradict (1) of Lemma 4.3. Hence we obtain $Z_{\underline{X}-\underline{Y}} = \widehat{X}_{\underline{X}-\underline{Y}}$. We can similarly prove that $Z_{\underline{Y}-\underline{X}} = \widehat{Y}_{\underline{Y}-\underline{X}}$ by taking W for $\widehat{Y}, Z, b$ instead of one for $\widehat{X}, Z, a$.

Claim 2: $Z \leq \max(\widehat{X}, \widehat{Y})$. Suppose to the contrary that there exists j with $Z_j > \max(\widehat{X}_j, \widehat{Y}_j)$. Claim 1 says that $j \in \widehat{X} \cap \widehat{Y}$. In this case, we have $\underline{W} \neq \underline{Y}$ by $W_j = Z_j > \widehat{Y}_j$, $W_b = \widehat{Y}_b$ and ($\mathrm{VC3_e}$). However, (4.1), (4.2), (4.3) and this contradict (1) of Lemma 4.3. Hence, we obtain $Z \leq \max(\widehat{X}, \widehat{Y})$.

Claim 3: $[\widehat{X}_j > \widehat{Y}_j \Rightarrow Z_j = \widehat{X}_j]$ and $[\widehat{Y}_j > \widehat{X}_j \Rightarrow Z_j = \widehat{Y}_j]$. Suppose that $\widehat{X}_j > \widehat{Y}_j$ and $Z_j < \widehat{X}_j$. In this case, we have that $W_j = \widehat{X}_j > \widehat{Y}_j$ and $W_b = \widehat{Y}_b$, which implies that $\underline{W} \neq \underline{\widehat{Y}}$ by ($\mathrm{VC3_e}$). However, (4.1), (4.2), (4.3) and this contradict (1) of Lemma 4.3. Hence we prove the first implication. By taking W for $\widehat{Y}, Z, b$, we can also prove the second implication.

Claims 1, 2 and 3 say that $\widehat{\alpha}$ and $\widehat{\beta}$ are valid choices in ($\mathrm{VCE}_{\mathrm{loc3}}$). ∎

Lemma 4.8 *Suppose that $\underline{\mathcal{X}}$ is the circuit family of a matroid. Then* (VC3) *and* ($\mathrm{VCE}_{\mathrm{loc3}}$) *imply* ($\mathrm{VCE}_{\mathrm{loc2}}$).

Proof. Let X and Y be any elements of $\mathcal{X}$ with $\mathrm{rank}(\underline{X} \cup \underline{Y}) = |\underline{X} \cup \underline{Y}| - 2$, and let u be an element with $X_u = Y_u \neq -\infty$. Since $\underline{\mathcal{X}}$ is the circuit family, there exists $Z \in \mathcal{X}$ such that $\underline{Z} \subseteq (\underline{X} \cup \underline{Y}) - u$. By (VC3), we can assume that $Z \leq \max(X, Y)$ and $Z_j = \max(X_j, Y_j)$ for some $j \in \underline{X} \cup \underline{Y}$. Obviously, X, Y and Z satisfy the assumptions of ($\mathrm{VCE}_{\mathrm{loc3}}$). Thus, there exist $\alpha, \beta \in R$ such that

$$\begin{aligned} Z &\leq \max(X + \alpha\mathbf{1}, Y + \beta\mathbf{1}), \\ Z_i &= \max(X_i + \alpha, Y_i + \beta) \quad \text{if } X_i + \alpha \neq Y_i + \beta. \end{aligned} \tag{4.4}$$

We have $\alpha = \beta$ from $Z_u = -\infty$, $X_u = Y_u \neq -\infty$ and (4.4). Since $Z_j = \max(X_j, Y_j)$, we have $\alpha \geq 0$. Furthermore, $\alpha = 0$ must hold because $Z \leq \max(X, Y)$ and $Z_i = X_i + \alpha$ for any $i \in \underline{X} - \underline{Y} \neq \emptyset$. Hence, Z is a valid choice in ($\mathrm{VCE}_{\mathrm{loc2}}$). ∎

Lemma 4.9 *Suppose that $\underline{\mathcal{X}}$ is the circuit family of a matroid.* (VC3), ($\mathrm{VC3_e}$) *and* ($\mathrm{VCE}_{\mathrm{loc2}}$) *imply* (VCE).

Proof. Let X, Y be any elements of $\mathcal{X}$ and u, v elements of V such that $X_u = Y_u \neq -\infty$ and $X_v > Y_v$. We prove (VCE) by induction on $\underline{X} \cup \underline{Y}$. ($\mathrm{VC3_e}$) implies $\underline{X} \neq \underline{Y}$, and hence, $\mathrm{rank}(\underline{X} \cup \underline{Y}) \leq |\underline{X} \cup \underline{Y}| - 2$. If $\mathrm{rank}(\underline{X} \cup \underline{Y}) = |\underline{X} \cup \underline{Y}| - 2$, ($\mathrm{VCE}_{\mathrm{loc2}}$) immediately implies (VCE). In the sequel, we assume that $\mathrm{rank}(\underline{X} \cup \underline{Y}) < |\underline{X} \cup \underline{Y}| - 2$ and that (VCE) holds for $\widehat{X}$ and $\widehat{Y}$ with $\underline{\widehat{X}} \cup \underline{\widehat{Y}} \subsetneq \underline{X} \cup \underline{Y}$. Let $a \in \underline{X} - \underline{Y}$ and $b \in \underline{Y} - \underline{X}$. From Lemma 4.3, there exists $W \in \mathcal{X}$ with $a, b \notin \underline{W} \subseteq \underline{X} \cup \underline{Y}$. In addition, from (VC3), we assume that $W \leq \max(X, Y)$ and $W_c = \max(X_c, Y_c)$ for some $c \in \underline{X} \cup \underline{Y}$. We divide into five cases.

Case 1: $W_v = X_v$ and $W_u = X_u$. Since $\underline{W} \cup \underline{Y} \subsetneq \underline{X} \cup \underline{Y}$, by induction hypothesis, there exists $Z \in \mathcal{X}$ such that $Z_u = -\infty$, $Z_v = W_v = X_v$ and $Z \leq \max(W, Y) \leq \max(X, Y)$. This Z is valid in (VCE) for X, Y, u, v.

Case 2: $W_v < X_v$ and $W_u = X_u$. Since $\underline{X} \cup \underline{W} \subsetneq \underline{X} \cup \underline{Y}$, by induction hypothesis, there exists $Z \in \mathcal{X}$ such that $Z_u = -\infty$, $Z_v = X_v$ and $Z \leq \max(X, W) \leq \max(X, Y)$. This Z is valid in (VCE) for X, Y, u, v.

Case 3: $W_u < X_u$ and $c \in \underline{Y} - \underline{X}$. We have $Y_c = W_c$ and $Y_u > W_u$. Then (VCE) for Y, W, c, u implies the existence $\widehat{W} \in \mathcal{X}$ such that $\widehat{W}_c = -\infty$, $\widehat{W}_u = Y_u$ and $\widehat{W} \leq \max(Y, W) \leq \max(X, Y)$. Since $a, c \notin \underline{\widehat{W}}$, we can prove the assertion from Case 1 or 2.

Case 4: $W_u < X_u$ and $c \in \underline{X} - \underline{Y}$. In the same way as Case 3, we can prove the assertion.

Case 5: $W_u < X_u = Y_u$ and $c \in \underline{X} \cap \underline{Y}$. If $W_v = X_v$, from (VCE) for X, W, v, u, there exists $\widehat{W} \in \mathcal{X}$ such that $\widehat{W}_v = -\infty$, $\widehat{W}_u = X_u$ and $\widehat{W} \leq \max(X, W) \leq \max(X, Y)$. In this case, since $b, v \notin \underline{\widehat{W}}$, we can prove the assertion by Case 2. Suppose that $W_v < X_v$ holds. Let W^X and W^Y be elements of $\mathcal{X}$ such that

$W^X_c = X_c$, $W^Y_c = Y_c$ and $\underline{W^X} = \underline{W^Y} = \underline{W}$. We note that one of W^X and W^Y equals to W and the other is less than or equal to W. By (VCE) for X, W^X, c, u, there exists $\widehat{W}^X \in \mathcal{X}$ such that $\widehat{W}^X_c = -\infty$, $\widehat{W}^X_u = X_u = Y_u$, $\widehat{W}^X \leq \max(X, Y)$ and $b \notin \underline{\widehat{W}^X}$. Moreover, by (VCE) for Y, W^Y, c, u, there exists $\widehat{W}^Y \in \mathcal{X}$ such that $\widehat{W}^Y_c = -\infty$, $\widehat{W}^Y_u = X_u = Y_u$, $\widehat{W}^Y \leq \max(X, Y)$ and $a \notin \underline{\widehat{W}^Y}$. If $\widehat{W}^X_v < X_v$ then Case 2 for $\widehat{W}^X$ and X implies the assertion. Suppose that $\widehat{W}^X_v = X_v$. Since $\underline{\widehat{W}^X} \cup \underline{\widehat{W}^Y} \subsetneq \underline{X} \cup \underline{Y}$ and $\widehat{W}^Y_v \leq \max(W_v, Y_v) < X_v$, (VCE) for $\widehat{W}^X, \widehat{W}^Y, u, v$, implies the existence of $Z \in \mathcal{X}$ such that $Z_u = -\infty$, $Z_v = \widehat{W}^X_v = X_v$ and $Z \leq \max(\widehat{W}^X, \widehat{W}^Y) \leq \max(X, Y)$. ∎

Proof of Theorem 3.2 Lemmas 4.4 and 4.5 say the equivalence between (a) and (b). Lemmas 4.7 and 4.8 show that (d) and (e) are equivalent. Lemma 4.6 proves the implication: (c) ⇒ (d). The implications: (a) ⇒ (c) and (d) ⇒ (c) are trivial. Finally, Lemma 4.9 which verifies (d) ⇒ (a) proves the equivalence of all five statements. ∎

We prove Theorem 3.1 in the remainder of this subsection. From the definition of $\mathcal{X} = \Phi_{\omega \to \mathcal{X}}(\omega)$, (VC1), (VC2) and (VC3) hold. By Theorem 3.2, it is sufficient to show (VC3$_{\rm e}$) and (VCE$_{\rm loc1}$). We first prove (VC3$_{\rm e}$).

Lemma 4.10 *$\mathcal{X} = \Phi_{\omega \to \mathcal{X}}(\omega)$ has* (VC3$_{\rm e}$).

Proof. Let X and Y be elements of $\mathcal{X}$ satisfying $\underline{X} = \underline{Y}$. Since $\mathcal{X}$ satisfies (VC3), we can assume that there exist $B, B' \in \mathcal{B}$ and $v, v' \in V$ such that $X = X(B, v)$ and $Y = X(B', v')$ using the notation (3.1).

We first suppose that $v = v'$. If $|\underline{X}| = 1$ then there is nothing to prove. We suppose that $|\underline{X}| \geq 2$ in the rest of this proof. Let u be any element of $\underline{X} - v$. From (VBX) for $B' - u + v, B, v$, there exists $w \in B - (B' - u + v) = (B - B') + u$ such that

$$\omega(B' - u + v) + \omega(B) \leq \omega(B' - u + w) + \omega(B - w + v).$$

Since $\underline{X}$ is dependent, $\underline{X} \not\subseteq B - w + v$, whereas $\underline{X} \cap (B - B') = \emptyset$. Hence $w = u$ must hold. Thus, we have

$$\omega(B' - u + v) + \omega(B) \leq \omega(B') + \omega(B - u + v).$$

By replacing the roles of B and B', we can also show the reversed inequality. Hence

$$\omega(B' - u + v) - \omega(B') = \omega(B - u + v) - \omega(B) \quad \text{for all } u \in \underline{X}.$$

That is, $X = Y$ holds.

We next suppose that $v \neq v'$. Let u be any element of $\underline{X} - \{v, v'\}$. By (VBX) for $B, B' - u + v', u$, there exists $w \in (B' - u + v') - B = B' - B$ such that

$$\omega(B) + \omega(B' - u + v') \leq \omega(B - u + w) + \omega(B' - w + v').$$

Since $\underline{Y}$ is dependent and $\underline{Y} \cap (B' - B) = \{v\}$, $B - w + v' \not\supseteq \underline{Y}$ and $w = v$ must hold. Thus, we have

$$\omega(B) + \omega(B' - u + v') \leq \omega(B - u + v) + \omega(B' - v + v'). \tag{4.5}$$

By (VBX) for $B' - v + v', B - u + v, u$, there exists $w \in (B - u + v) - (B' - v + v') = ((B - B') - v') + v$ such that

$$\omega(B - u + v) + \omega(B' - v + v') \leq \omega(B - w + v) + \omega(B' - v - u + w + v').$$

Since $\underline{X}$ is dependent, $B - w + v \not\supseteq \underline{X}$, and hence, $w = v$ must hold. Then

$$\omega(B - u + v) + \omega(B' - v + v') \leq \omega(B) + \omega(B' - u + v'). \tag{4.6}$$

(4.5) and (4.6) imply

$$\omega(B - u + v) - \omega(B) = \omega(B' - u + v') - \omega(B' - v + v').$$

This equation can be proven similarly for $u = v'$, whereas it trivially holds for $u = v$. Hence, $Y = X + \beta\mathbf{1}$ with $\beta = \omega(B' - v + v') - \omega(B')$. ∎

Lemma 4.11 *$\mathcal{X} = \Phi_{\omega \to \mathcal{X}}(\omega)$ satisfies* ($\mathrm{VCE}_{\mathrm{loc1}}$).

Proof. Let X, Y be any elements of $\mathcal{X}$ and u, v be elements of V such that $\mathrm{rank}(\underline{X} \cup \underline{Y}) = |\underline{X} \cup \underline{Y}| - 2$, $X_u = Y_u \neq -\infty$ and $v \in \underline{X} - \underline{Y}$. From Lemma 4.3, there exist a base B and $w \in \underline{Y} - \underline{X}$ so that $\underline{X} = C(B, v)$ and $\underline{Y} = C(B, w)$. Let $B' = B - u + w$. Obviously, B' is also a base. Assume that Z is an element of $\mathcal{X}$ such that $\underline{Z} = C(B', v)$ and $Z_v = X_v$. Then $Z_u = -\infty$ holds. It remains to prove $Z \leq \max(X, Y)$. Without less of generality, we assume that $X_u = Y_u = 0$. Then, we have

$$\begin{aligned} X_i &= \omega(B - i + v) - \omega(B - u + v), \\ Y_i &= \omega(B - i + w) - \omega(B - u + w). \end{aligned}$$

By $Z_v = X_v = \omega(B) - \omega(B - u + v)$, we have

$$\begin{aligned} Z_i &= \omega(B' - i + v) - \omega(B') - \omega(B - u + v) + \omega(B) \\ &= \omega(B - i - u + v + w) - \omega(B - u + w) - \omega(B - u + v) + \omega(B) \end{aligned}$$

for any $i \in V$. Moreover, Lemma 4.1 implies

$$\begin{aligned} Z_i &\leq \max \left\{ \begin{array}{l} \omega(B - i + v) - \omega(B - u + v) \\ \omega(B - i + w) - \omega(B - u + w) \end{array} \right\} \\ &= \max(X_i, Y_i) \end{aligned}$$

for any $i \in V$. Hence $Z \leq \max(X, Y)$. ∎

4.3 Proof of Theorem 3.3

The assertions (1), (2), and (3) of Theorem 3.3 are proven in Lemmas 4.15, 4.16 and 4.17, respectively.

We arbitrarily fix orientations of edges of $G(\mathcal{B})$ and define a weight $w(e)$ of edge $e = (B, B') = (B, B - u + v)$ by

$$w(e) = X_u - X_v \tag{4.7}$$

using $X \in \mathcal{X}$ with $\underline{X} \subseteq B \cup B'$. Note that $w(e)$ is independent of the choice of X by (VC3e), and that $w(e^*) = -w(e)$ if e^* is the reorientation of e. For any directed path (or cycle) P, we define its weight $w(P)$ by

$$\begin{aligned} w(P) \;=\; & \sum\{w(e) \mid \; e \text{ is forward in } P\} \\ & -\sum\{w(e) \mid \; e \text{ is backward in } P\}. \end{aligned} \tag{4.8}$$

We are to prove that (3.3) is determined independently of the choice of a path from B_0 to B. It is easy to see that this is tantamount to showing that $w(D) = 0$ for any directed cycle D in $G(\mathcal{B})$.

Lemma 4.12 *Let w be defined by (4.7). Then $w(D) = 0$ for a directed cycle D of length 3.*

Proof. Let B, B_1, B_2 be the bases on D. We denote by $\omega'(B_1)$ and $\omega'(B_2)$ values of B_1 and B_2 determined from $\omega(B)$ by the path B, B_1, B_2. Since the length of the cycle is three, it is enough to consider only two cases when B_1 and B_2 are expressed as follows:

Case 1: $B_1 = B - u_1 + v$ and $B_2 = B - u_2 + v$,

Case 2: $B_1 = B - u + v_1$ and $B_2 = B - u + v_2$.

In Case 1, consider two circuits X and Y such that $\underline{X} = C(B, v)$, $X_v = 0$ and $\underline{Y} = C(B_1, u_1)$, $Y_{u_1} = 0$. Then we have $\omega'(B_1) = \omega(B) + X_{u_1}$ and $\omega'(B_2) = \omega'(B_1) + Y_{u_2}$. Since $\underline{X}, \underline{Y} \subseteq B + v$, $\underline{X} = \underline{Y}$ must hold. (VC3e) implies that $Y = X + \alpha \mathbf{1}$ for some $\alpha \in R$. Furthermore, $\alpha = -X_{u_1}$ follows form $Y_{u_1} = 0$. Hence

$$\omega'(B_2) = \omega(B) + X_{u_1} + Y_{u_2} = \omega(B) + X_{u_2}.$$

This equals to the value of ω at B_2 determined by the path B, B_2 because $B_2 = B - u_2 + v \subseteq B + v$.

In Case 2, consider two circuits X and Y such that $\underline{X} = C(B, v_1)$, $X_{v_1} = 0$ and $\underline{Y} = C(B_1, v_2)$, $Y_{v_2} = 0$. Then $\omega'(B_1) = \omega(B) + X_u$ and $\omega'(B_2) = \omega'(B_1) + Y_{v_1} = \omega(B) + X_u + Y_{v_1}$. Since $\underline{X} = C(B_1, u)$ and $\underline{Y} = C(B_1, v_2)$, we have $\mathrm{rank}(\underline{X} \cup \underline{Y}) =$

$|\underline{X} \cup \underline{Y}| - 2$. From ($\mathrm{VCE}_{\mathrm{loc1}}$) for $Y - Y_{v_1}\mathbf{1}, X, v_1, v_2$, there exists $\hat{Z} \in \mathcal{X}$ such that $\hat{Z}_{v_1} = -\infty$, $\hat{Z}_{v_2} = Y_{v_2} - Y_{v_1} = -Y_{v_1}$ and $\hat{Z} \leq \max(X, Y - Y_{v_1}\mathbf{1})$. On the other hand, from ($\mathrm{VCE}_{\mathrm{loc1}}$) for $X, Y - Y_{v_1}\mathbf{1}, v_1, u$, there exists $\tilde{Z} \in \mathcal{X}$ such that $\tilde{Z}_{v_1} = -\infty$, $\tilde{Z}_u = X_u$ and $\tilde{Z} \leq \max(X, Y - Y_{v_1}\mathbf{1})$. The equality $\underline{\hat{Z}} = \underline{\tilde{Z}}$ must hold because $\underline{\hat{Z}}, \underline{\tilde{Z}} \subseteq B + v_2$. Moreover, since $\hat{Z}_{v_2} = \max(X_{v_2}, Y_{v_2} - Y_{v_1})$ and $\tilde{Z}_u = \max(X_u, Y_u - Y_{v_1})$, we have $\hat{Z} = \tilde{Z}$. Let Z be a circuit in $\mathcal{X}$ such that $\underline{Z} = C(B, v_2) = \underline{\hat{Z}}$ and $Z_{v_2} = 0$. Then, we obtain

$$Z_u = \hat{Z}_u - \hat{Z}_{v_2} = \tilde{Z}_u - \hat{Z}_{v_2} = X_u + Y_{v_1}.$$

The value of ω at B_2 determined by the path B, B_2 is given by $\omega(B_2) + Z_u = \omega(B) + X_u + Y_{v_1}$ which is equal to $\omega'(B_2)$. ∎

Lemma 4.13 *Let w be defined by (4.7). Then $w(D) = 0$ for a directed cycle D of length 4.*

Proof. Let B, B_1, B', B_2 be the bases on D. We assume that D has no chord, since otherwise the assertion follows from Lemma 4.12. Without loss of generality, we assume that $B_1 = B - u_1 + v_1$, $B_2 = B - u_2 + v_2$ and $B' = B - u_1 - u_2 + v_1 + v_2$. We denote by $\omega_1(B_1)$ and $\omega_1(B')$ the values of ω at B_1 and B' determined by the path B, B_1, B', and define $\omega_2(B_2)$ and $\omega_2(B')$ to be the values determined along the other path B, B_2, B'. Let X, Y, W, Z be circuits in $\mathcal{X}$ such that

$$\begin{aligned} &\underline{X} = C(B, v_1),\ X_{v_1} = 0, \quad \underline{W} = C(B_1, v_2),\ W_{v_2} = 0, \\ &\underline{Y} = C(B, v_2),\ Y_{v_2} = 0, \quad \underline{Z} = C(B_2, v_1),\ Z_{v_1} = 0. \end{aligned}$$

From the definition of $\Phi_{\mathcal{X}\to\omega}$, we have

$$\begin{aligned} &\omega_1(B') = \omega_1(B_1) + W_{u_2}, \quad \omega_1(B_1) = \omega(B) + X_{u_1}, \\ &\omega_2(B') = \omega_2(B_2) + Z_{u_1}, \quad \omega_2(B_2) = \omega(B) + Y_{u_2}. \end{aligned} \tag{4.9}$$

We consider three cases on the exchangeability graph $G(B, B')$:

Case 1: four edges $(u_1, v_1), (u_1, v_2), (u_2, v_1), (u_2, v_2)$ exist in $G(B, B')$,

Case 2: exactly three edges $(u_1, v_1), (u_2, v_1), (u_2, v_2)$ exist in $G(B, B')$,

Case 3: exactly two edges $(u_1, v_1), (u_2, v_2)$ exist in $G(B, B')$.

We first consider Case 3. In this case, $\underline{X} \cap \{u_1, u_2, v_1, v_2\} = \{u_1, v_1\}$ and $\underline{Y} \cap \{u_1, u_2, v_1, v_2\} = \{u_2, v_2\}$ must hold. That is, $\underline{W} = \underline{Y}$ and $\underline{Z} = \underline{X}$. Furthermore, since $W_{v_2} = Y_{v_2} = 0$ and $Z_{v_1} = X_{v_1} = 0$, we see that $W = Y$ and $Z = X$ by ($\mathrm{VC3_e}$). From (4.9), $\omega_1(B') = \omega(B) + X_{u_1} + Y_{u_2} = \omega_2(B')$.

In the other cases, we have $\underline{X} \cap \{u_1, u_2, v_1, v_2\} = \{u_1, u_2, v_1\}$ and $\{u_2, v_2\} \subseteq \underline{Y} \cap \{u_1, u_2, v_1, v_2\} \subseteq \{u_1, u_2, v_2\}$. Obviously, $\mathrm{rank}(\underline{X} \cup \underline{Y}) = |\underline{X} \cup \underline{Y}| - 2$ holds.

From ($\mathrm{VCE}_{\mathrm{loc1}}$) for $X - X_{u_2}\mathbf{1}, Y - Y_{u_2}\mathbf{1}, u_2, v_1$, there exists $\hat{Z} \in \mathcal{X}$ such that $u_2 \notin \underline{\hat{Z}}$, $\hat{Z}_{v_1} = X_{v_1} - X_{u_2} = -X_{u_2}$ and $\hat{Z} \leq \max(X - X_{u_2}\mathbf{1}, Y - Y_{u_2}\mathbf{1})$. Since $\underline{\hat{Z}} \subseteq B - u_2 + v_2 + v_1$, $\underline{\hat{Z}} = C(B_2, v_1) = \underline{Z}$ must hold. Furthermore, because $\hat{Z}_{v_1} = -X_{u_2}$ and $Z_{v_1} = 0$, we have

$$Z_{v_2} = \hat{Z}_{v_2} + X_{u_2} \leq Y_{v_2} - Y_{u_2} + X_{u_2} = X_{u_2} - Y_{u_2}, \tag{4.10}$$

$$Z_{u_1} \leq \max(X_{u_1}, Y_{u_1} - Y_{u_2} + X_{u_2}). \tag{4.11}$$

The relations that $B' = B_2 - u_1 + v_1$ and $\underline{Z} = C(B_2, v_1)$ imply $u_1 \in \underline{Z}$. Since $B - u_2 + v_1$ is a base, $\underline{X} = C(B - u_2 + v_1, u_2)$ and $\underline{Z} = C(B - u_2 + v_1, v_2)$, we have $\mathrm{rank}(\underline{X} \cup \underline{Z}) = |\underline{X} \cup \underline{Z}| - 2$. From ($\mathrm{VCE}_{\mathrm{loc1}}$) for $X - X_{u_1}\mathbf{1}, Z - Z_{u_1}\mathbf{1}, u_1, u_2$, there exists $\widehat{W} \in \mathcal{X}$ such that $u_1 \notin \underline{\widehat{W}}$, $\widehat{W}_{u_2} = X_{u_2} - X_{u_1}$ and $\widehat{W} \leq \max(X - X_{u_1}\mathbf{1}, Z - Z_{u_1}\mathbf{1})$. Since $\underline{\widehat{W}} \subseteq B - u_1 + v_1 + v_2$, we have $\underline{\widehat{W}} = C(B_1, v_2) = \underline{W}$, and therefore, $W = \widehat{W} - \widehat{W}_{v_2}\mathbf{1}$ by $W_{v_2} = 0$ and ($\mathrm{VC3_e}$). Thus, we have

$$W_{u_2} = X_{u_2} - X_{u_1} - \widehat{W}_{v_2} \quad \text{and} \quad \widehat{W}_{v_2} \leq Z_{v_2} - Z_{u_1}. \tag{4.12}$$

(4.9), (4.10) and (4.12) imply

$$\omega_2(B') = \omega(B) + Z_{u_1} + Y_{u_2} \leq \omega(B) + W_{u_2} + X_{u_1} = \omega_1(B'). \tag{4.13}$$

In Case 1 we can exchange the roles of X and Y to obtain $\omega_1(B') \leq \omega_2(B')$. Hence $\omega_1(B') = \omega_2(B')$.

In Case 2, we have $\underline{Y} \cap \{u_1, u_2, v_1, v_2\} = \{u_2, v_2\}$, $Y = W$ and $Z_{u_1} \leq X_{u_1}$ by (4.13). On the other hand, from ($\mathrm{VCE}_{\mathrm{loc1}}$) for $X - X_{u_2}\mathbf{1}, Y - Y_{u_2}\mathbf{1}, u_2, u_1$, there exists $\tilde{Z} \in \mathcal{X}$ such that $u_2 \notin \underline{\tilde{Z}}$, $\tilde{Z}_{u_1} = X_{u_1} - X_{u_2}$ and $\tilde{Z} \leq \max(X - X_{u_2}\mathbf{1}, Y - Y_{u_2}\mathbf{1})$. Since $\underline{\tilde{Z}} \subseteq B - u_2 + v_2 + v_1$, $\underline{\tilde{Z}} = C(B_2, v_1) = \underline{Z}$. Thus, we have

$$Z = \tilde{Z} - \tilde{Z}_{v_1}\mathbf{1} \quad \text{and} \quad \tilde{Z}_{v_1} \leq X_{v_1} - X_{u_2} = -X_{u_2}.$$

Hence, $Z_{u_1} = X_{u_1} - X_{u_2} - \tilde{Z}_{v_1} \geq X_{u_1}$. Therefore, we obtain $Z_{u_1} = X_{u_1}$ and $\omega_1(B') = \omega_2(B')$. ∎

Lemma 4.14 *Let w be any edge weight. If any directed cycle in $G(\mathcal{B})$ of length 3 or 4 has weight 0, then $w(D) = 0$ for any directed cycle D in $G(\mathcal{B})$.*

Proof. We prove the assertion by induction on the length k of a cycle. Assume that a cycle of length less than k ($k \geq 5$) has weight 0. Let D be a cycle of length k, where it may be assumed that D is a simple cycle consisting of distinct bases $B_0, B_1, \ldots, B_{k-1}$.

We first treat the case where there exist two bases B_i, B_j such that $|B_i \triangle B_j|/2$ is less than the length of shorter path between B_i and B_j in D. In this case, there exists a directed path P of length $|B_i \triangle B_j|/2$ in $G(\mathcal{B})$ between B_i and B_j. The set

$D \cup P \cup (-P)$ of directed edges can be partitioned into two directed cycles D_1 and D_2 whose lengths are less than k, where $-P$ denotes the directed path having the opposite directed edges of P. Furthermore, $w(D) = w(D_1) + w(D_2)$ holds. Hence we obtain $w(D) = 0$ from the induction hypothesis.

We now suppose that the length of shorter path in D between any two bases B_i and B_j is equal to $|B_i \triangle B_j|/2$. Then, we can express $B_1 = B_0 - u_1 + v_1$ and $B_\ell = B_0 - \{u_1, \ldots, u_\ell\} + \{v_1, \ldots, v_\ell\}$ for $\ell = \lfloor k/2 \rfloor$. Let $B_{k-1} = B_0 - u + v$. From the above assumption, we see that u_1, u, v_1 and v are mutually distinct. In case of even k, $u \in \{u_2, \ldots, u_\ell\}$ and $v \in \{v_2, \ldots, v_\ell\}$ must hold because the distance between B_ℓ and B_{k-1} is $\ell - 1$. In case of odd k, either $u \in \{u_2, \ldots, u_\ell\}$ or $v \in \{v_2, \ldots, v_\ell\}$ must hold because the distance between B_ℓ and B_{k-1} is ℓ in D. Since u_1, u, v_1, v are mutually distinct, from (MBX) for B_1, B_{k-1}, v_1, we have

$$\begin{aligned} &\text{(a)} \quad B_0 - u_1 - u + v_1 + v \in \mathcal{B} \quad \text{or} \\ &\text{(b)} \quad B_0 - u_1 + v \in \mathcal{B} \text{ and } B_0 - u + v_1 \in \mathcal{B}. \end{aligned}$$

If the first case holds, we set $\widehat{B} = B_0 - u_1 - u + v_1 + v$; otherwise, if $v \in \{v_1, \ldots, v_\ell\}$ then we set $\widehat{B} = B_0 - u_1 + v$; otherwise ($u \in \{u_1, \ldots, u_\ell\}$ holds), we set $\widehat{B} = B_0 - u + v_1$. Then, there exists a directed path P between B_ℓ and $\widehat{B}$ whose length is at most $\ell - 1$. By using the edges of $D, P, -P$ and four directed edges $(B_1, \widehat{B})$, $(\widehat{B}, B_1)$, $(B_{k-1}, \widehat{B})$, $(\widehat{B}, B_{k-1})$, we can construct three directed cycles D_1, D_2, D_3 with lengths less than k. From the induction hypothesis, we have $w(D) = w(D_1) + w(D_2) + w(D_3) = 0$. ∎

It is noted that Lemma 4.14 is independent of the circuit axioms of valuated matroids.

Lemma 4.15 *$\omega = \Phi_{\mathcal{X} \to \omega}(\mathcal{X})$ is well-defined.*

Proof. Let w be the weight function on the edges of $G(\mathcal{B})$ defined by (4.7). The construction $\Phi_{\mathcal{X} \to \omega}$ determines the value at B by $\omega(B_0) + w(P)$ along a directed path P from B_0 to B, where $w(P)$ is defined by (4.8). Lemmas 4.12 and 4.13 guarantee that any directed cycle of length 3 or 4 in $G(\mathcal{B})$ has weight 0. From Lemma 4.14, any directed cycle in $G(\mathcal{B})$ has weight 0. Hence $\omega(B)$ is uniquely determined by $\Phi_{\mathcal{X} \to \omega}$ for a fixed $\omega(B_0)$. ∎

Lemma 4.16 *$\omega = \Phi_{\mathcal{X} \to \omega}(\mathcal{X})$ satisfies* (VB1) *and* (VBX).

Proof. Since $\mathcal{B}$ is the family of bases, obviously (VB1) holds. To prove (VBX), it suffices, by Theorem 1.1, to show (VBX_{loc}) for ω. For any two bases B, B' with $|B - B'| = 2$, let us denote $B' = B - u_1 - u_2 + v_1 + v_2$ and $B_{ij} = B - u_i + v_j$ for $i, j = 1, 2$. Take circuits X and Y in $\mathcal{X}$ such that

$$\underline{X} = C(B, v_1),\ X_{v_1} = 0 \quad \text{and} \quad \underline{Y} = C(B, v_2),\ Y_{v_2} = 0.$$

Obviously, $\mathrm{rank}(\underline{X} \cup \underline{Y}) = |\underline{X} \cup \underline{Y}| - 2$ holds. From the definition of $\Phi_{\mathcal{X}\to\omega}$,

$$\omega(B_{i1}) = \omega(B) + X_{u_i} \quad \text{and} \quad \omega(B_{i2}) = \omega(B) + Y_{u_i}, \tag{4.14}$$

where if $B_{ij} \notin \mathcal{B}$, we have $\omega(B_{ij}) = -\infty$.

We first assume that the exchangeability graph $G(B, B')$ has a unique perfect matching and that $B_{11}, B_{22} \in \mathcal{B}$ and $B_{12} \notin \mathcal{B}$. In this case, $v_1, u_1 \notin \underline{Y} \supseteq \{u_2, v_2\}$. Since $\underline{Y} \subseteq B - u_1 + v_1 + v_2$, $\underline{Y} = C(B_{11}, v_2)$ holds. Thus, we have

$$\omega(B') = \omega(B_{11}) + Y_{u_2}.$$

This and (4.14) imply $\omega(B) + \omega(B') = \omega(B_{11}) + \omega(B_{22})$. Hence ($\mathrm{VBX}_{\mathrm{loc}}$) holds.

In the remaining case where $G(B, B')$ is the complete bipartite graph $K_{2,2}$, we have $B_{ij} \in \mathcal{B}$ for $i, j = 1, 2$. From ($\mathrm{VCE}_{\mathrm{loc}1}$) for $Y - Y_{u_1}\mathbf{1}, X - X_{u_1}\mathbf{1}, u_1, v_2$, there exists $\widehat{Z} \in \mathcal{X}$ such that

$$u_1 \notin \underline{\widehat{Z}},\ \widehat{Z}_{v_2} = Y_{v_2} - Y_{u_1} = -Y_{u_1} \ \text{ and } \ \widehat{Z}_i \le \max(Y_i - Y_{u_1}, X_i - X_{u_1}). \tag{4.15}$$

Let $Z = \widehat{Z} - \widehat{Z}_{v_2}\mathbf{1}$. By (4.15), we have

$$Z_{u_2} + X_{u_1} \le \max(Y_{u_2} + X_{u_1}, X_{u_2} + Y_{u_1}). \tag{4.16}$$

Since $\underline{Z} \subseteq B - u_1 + v_1 + v_2$, $\underline{Z} = C(B_{11}, v_2)$ must hold. Furthermore, it follows from $B' = B_{11} - u_2 + v_2$, $Z_{v_2} = 0$ and (4.14) that

$$\omega(B') = \omega(B_{11}) + Z_{u_2} = \omega(B) + X_{u_1} + Z_{u_2}. \tag{4.17}$$

By (4.14), (4.16) and (4.17), we obtain

$$\omega(B) + \omega(B') \le \max(\omega(B_{11}) + \omega(B_{22}), \omega(B_{12}) + \omega(B_{21})).$$

Hence ($\mathrm{VBX}_{\mathrm{loc}}$)holds. ∎

Lemma 4.17 *$\Phi_{\omega\to\mathcal{X}}(\Phi_{\mathcal{X}\to\omega}(\mathcal{X})) = \mathcal{X}$ and $\Phi_{\mathcal{X}\to\omega}(\Phi_{\omega\to\mathcal{X}}(\omega)) = \omega + \text{constant}$.*

Proof. By the definitions of $\Phi_{\omega\to\mathcal{X}}$ and $\Phi_{\mathcal{X}\to\omega}$, obviously $\underline{\mathcal{X}} = \underline{\Phi_{\omega\to\mathcal{X}}(\Phi_{\mathcal{X}\to\omega}(\mathcal{X}))}$ holds. It is enough to show that $\Phi_{\omega\to\mathcal{X}}(\Phi_{\mathcal{X}\to\omega}(X)) = X$ for any $X \in \mathcal{X}$ with $X_v = 0$ for some $v \in \underline{X}$. Let B be a base including $\underline{X} - v$ and put $B_i = B - i + v$ for any $i \in V$. The construction $\Phi_{\mathcal{X}\to\omega}$ yields

$$\omega(B_i) = \omega(B) + X_i.$$

On the other hand, $X(B, v) \in \Phi_{\omega\to\mathcal{X}}(\Phi_{\mathcal{X}\to\omega}(\mathcal{X}))$ and

$$X(B, v)_i = \omega(B - i + v) - \omega(B) = \omega(B_i) - \omega(B) = X_i.$$

Hence $\mathcal{X} = \Phi_{\omega\to\mathcal{X}}(\Phi_{\mathcal{X}\to\omega}(\mathcal{X}))$ holds.

Let $\omega' = \Phi_{\mathcal{X}\to\omega}(\Phi_{\omega\to\mathcal{X}}(\omega))$. It is enough to prove that $\omega'(B) = \omega(B)$ for all bases B under the condition that $\omega'(B_0) = \omega(B_0)$. Let $B = B_0 - u + v \in \mathcal{B}$. Since $X(B_0, v) \in \Phi_{\omega\to\mathcal{X}}(\omega)$, $X(B_0, v)_u = \omega(B) - \omega(B_0)$ and $X(B_0, v)_v = 0$, we have

$$\omega'(B) = \omega'(B_0) + X(B_0, v)_u = \omega(B).$$

Similarly, we can prove that $\omega' = \omega$. ∎

4.4 Proofs of Theorems 3.4, 3.5 and 3.6

We consider the following condition weaker than (VVE):

(VVE$_{\rm W}$) For $X, Y \in \mathcal{V}$ and $u, v \in V$ such that $X_u = Y_u \neq -\infty$ and $X_v > Y_v$, there exists $Z \in \mathcal{V}$ such that $Z_u = -\infty$, $Z_v = X_v$, $Z \leq \max(X, Y)$.

Lemma 4.18 *Let $\mathcal{V}$ be a set of vectors in $(R \cup \{-\infty\})^V$ having* (VV2). *Then, $\mathcal{V}$ satisfies* (VVE) *if and only if it does* (VVE$_{\rm W}$).

Proof. If $\mathcal{V}$ satisfies (VVE) then it obviously satisfies (VVE$_{\rm W}$). We prove the converse. Let X and Y be elements of $\mathcal{V}$ with $X_u = Y_u \neq -\infty$ for a fixed $u \in V$. For each $v \in V$ with $X_v \neq Y_v$, there exists $Z^v \in \mathcal{V}$ such that $Z^v_u = -\infty$, $Z^v_v = \max(X_v, Y_v)$ and $Z^v \leq \max(X, Y)$, from (VVE$_{\rm W}$). Since $\mathcal{V}$ satisfies (VV2), $Z = \max(Z^v : v \in V \text{ with } X_v \neq Y_v)$ satisfies (VVE) for X, Y, u. ∎

Proof of Theorem 3.4 Trivially, $\mathcal{V} = \Phi_{\mathcal{X}\to\mathcal{V}}(\mathcal{X})$ satisfies (VV1), (VV2) and (VV3). By Lemma 4.18, it suffices to show that $\mathcal{V}$ satisfies (VVE$_{\rm W}$). Assume $X_u = Y_u \neq -\infty$ and $X_v > Y_v$ for $X, Y \in \mathcal{V}$ and $u, v \in V$. From the definition of $\mathcal{V}$, there exist circuits $X^1, \ldots, X^k$ and $Y^1 \ldots, Y^\ell$ with $X = \max(X^1, \ldots, X^k)$ and $Y = \max(Y^1, \ldots, Y^\ell)$. Without loss of generality, we assume that $X_u = X^1_u$ and $Y_u = Y^1_u$. Suppose that $X_v = X^1_v$. Since $X^1_v > Y_v \geq Y^1_v$, from (VCE), there exists $Z \in \mathcal{X} \subseteq \mathcal{V}$ such that $Z_u = -\infty$, $Z_v = X^1_v = X_v$ and $Z \leq \max(X^1, Y^1) \leq \max(X, Y)$. Thus Z satisfies (VVE$_{\rm W}$) for X, Y, u, v. Suppose that $X_v > X^1_v$ and that $X_v = X^2_v$. Let $\alpha = X_u - X^2_u \geq 0$. From (VCE) for $X^2 + \alpha\mathbf{1}, X^1, u, v$, there exists $\widehat{Z} \in \mathcal{X}$ such that $\widehat{Z}_u = -\infty$, $\widehat{Z}_v = X^2_v + \alpha$ and $\widehat{Z} \leq \max(X^1, X^2 + \alpha\mathbf{1})$. From (VC3), $Z = \widehat{Z} - \alpha\mathbf{1} \in \mathcal{X}$, $Z_u = -\infty$, $Z_v = X^2_v = X_v$ and $Z \leq \max(X^1 - \alpha\mathbf{1}, X^2) \leq \max(X^1, X^2) \leq \max(X, Y)$. Hence Z satisfies (VVE$_{\rm W}$) for X, Y, u, v. ∎

Proof of Theorem 3.5 Trivially, $\mathcal{X} = \Phi_{\mathcal{V}\to\mathcal{X}}(\mathcal{V})$ satisfies (VC1), (VC2) and (VC3). Let X and Y be elements of $\mathcal{X}$ with $\underline{X} = \underline{Y}$, and $\beta = \max_{i\in V}(Y_i - X_i)$. Then $Y \leq X + \beta\mathbf{1}$ and there is $u \in V$ with $Y_u = X_u + \beta$. If $Y = X + \beta\mathbf{1}$ then we obtain (VC3$_{\rm e}$). Suppose to the contrary that $Y \neq X + \beta\mathbf{1}$. That is, there is $v \in V$ with $X_v + \beta > Y_v$. From (VVE) for $X + \beta\mathbf{1}, Y, u, v$, there exists $Z \in \mathcal{V}$ such that $Z_u = -\infty$, $Z_v = X_v + \beta$ and $Z \leq X + \beta\mathbf{1}$. However, $\underline{Z}$ is a nonempty proper subset of $\underline{X}$ and this contradicts the definition of $\mathcal{X}$.

Suppose that $X_u = Y_u \neq -\infty$ and $X_v > Y_v$ for $X, Y \in \mathcal{X}$ and $u, v \in V$. By (VVE$_{\rm W}$) for X, Y, u, v, there exists $Z \in \mathcal{V}$ such that

$$Z_u = -\infty,\ Z_v = X_v \text{ and } Z \leq \max(X, Y). \tag{4.18}$$

We claim that such $Z \in \mathcal{V}$ with the minimal support belongs to $\mathcal{X}$. Suppose to the contrary that $Z \notin \mathcal{X}$. Thus, there exists $W \in \mathcal{X}$ such that $\underline{W} \subsetneq \underline{Z}$, $W \leq Z$ and

$W_i = Z_i \neq -\infty$ for some i. If $Z_v = W_v$ then W satisfies (4.18) and this contradicts the minimality of $\underline{Z}$. Assume that $Z_v > W_v$. By ($\mathrm{VVE_W}$) for Z, W, i, v, there exists $\tilde{Z} \in \mathcal{V}$ such that $\tilde{Z}_i = -\infty$, $\tilde{Z}_v = Z_v = X_v$ and $\tilde{Z} \leq \max(Z, W) = Z$. However, we have $\emptyset \neq \underline{\tilde{Z}} \subseteq \underline{Z} - i$ which contradicts the minimality of $\underline{Z}$. Hence, $Z \in \mathcal{X}$. ∎

Proof of Theorem 3.6 Obviously, $\mathcal{S} \subseteq \Phi_{\mathcal{V}\to\mathcal{X}}(\Phi_{\mathcal{X}\to\mathcal{V}}(\mathcal{S})) = \mathrm{Minsupp}(\Phi_{\mathcal{X}\to\mathcal{V}}(\mathcal{S}))$ holds for any family $\mathcal{S}$ of vectors satisfying (VC2). Let X be any member of $\Phi_{\mathcal{V}\to\mathcal{X}}(\Phi_{\mathcal{X}\to\mathcal{V}}(\mathcal{X}))$. From $X \in \Phi_{\mathcal{X}\to\mathcal{V}}(\mathcal{X})$, there exist $X^1, \ldots, X^k \in \mathcal{X}$ with $X = \max(X^1, \ldots, X^k)$. Since X has a minimal support in $\Phi_{\mathcal{X}\to\mathcal{V}}(\mathcal{X})$, $\underline{X} = \underline{X^1} = \cdots = \underline{X^k}$ must hold. By (VC3), we have $X \in \mathcal{X}$. Hence, $\Phi_{\mathcal{V}\to\mathcal{X}}(\Phi_{\mathcal{X}\to\mathcal{V}}(\mathcal{X})) = \mathcal{X}$.

Let Y be any element of $\Phi_{\mathcal{X}\to\mathcal{V}}(\Phi_{\mathcal{V}\to\mathcal{X}}(\mathcal{V}))$. If $Y = (-\infty, \ldots, -\infty)$ then $Y \in \mathcal{V}$ from (VV1); otherwise, there exist $Y^1, \ldots, Y^k \in \Phi_{\mathcal{V}\to\mathcal{X}}(\mathcal{V}) \subseteq \mathcal{V}$ with $Y = \max(Y^1, \ldots, Y^k)$. Since $\mathcal{V}$ satisfies (VV2), $Y \in \mathcal{V}$. Hence $\Phi_{\mathcal{X}\to\mathcal{V}}(\Phi_{\mathcal{V}\to\mathcal{X}}(\mathcal{V})) \subseteq \mathcal{V}$.

Let Y be any member of $\mathcal{V}$ and v any element of $\underline{Y}$. We claim that there exists $Y^v \in \Phi_{\mathcal{V}\to\mathcal{X}}(\mathcal{V})$ with $Y^v \leq Y$ and $Y^v_v = Y_v$. If $Y \in \Phi_{\mathcal{V}\to\mathcal{X}}(\mathcal{V})$ then this trivially holds. Assume that $Y \notin \Phi_{\mathcal{V}\to\mathcal{X}}(\mathcal{V})$. Let X be any member of $\Phi_{\mathcal{V}\to\mathcal{X}}(\mathcal{V})$ such that $X \leq Y$ and $X_u = Y_u$ for some $u \in \underline{X}$. If $X_v = Y_v$ then our claim holds by setting $Y^v = X$; otherwise, from ($\mathrm{VVE_W}$), there exists $\hat{Y} \in \mathcal{V}$ such that $\hat{Y}_u = -\infty$, $\hat{Y}_v = Y_v$ and $\hat{Y} \leq Y$. Since the support of $\hat{Y}$ is a proper subset of that of Y, by repeating the above process, we can obtain Y^v satisfying our claim. Thus, we have $Y = \max(Y^v \mid v \in \underline{Y}) \in \Phi_{\mathcal{X}\to\mathcal{V}}(\Phi_{\mathcal{V}\to\mathcal{X}}(\mathcal{V}))$. Hence $\mathcal{V} \subseteq \Phi_{\mathcal{X}\to\mathcal{V}}(\Phi_{\mathcal{V}\to\mathcal{X}}(\mathcal{V}))$. ∎

4.5 Proof of Theorem 3.7

Lemma 4.19 *For two families $\mathcal{C}$ and $\mathcal{D}$ of subsets of V, if $\mathcal{C}$ satisfies* (MC2) *and* $\mathrm{Minsupp}(\mathcal{D}) \subseteq \mathcal{C} \subseteq \mathcal{D}$, *then* $\mathcal{C} = \mathrm{Minsupp}(\mathcal{D})$.

Proof. It is enough to show that $C \in \mathrm{Minsupp}(\mathcal{D})$ for any $C \in \mathcal{C}$. There exists $D \in \mathrm{Minsupp}(\mathcal{D})$ with $D \subseteq C$ because $\mathcal{C} \subseteq \mathcal{D}$. Since $\mathcal{C}$ satisfies (MC2), we have $D = C$. Hence $\mathcal{C} = \mathrm{Minsupp}(\mathcal{D})$. ∎

Proof of Theorem 3.7 We first show that $\mathcal{C}_0 \subseteq \mathrm{Max}(\mathcal{X})$. For any $C \in \mathcal{C}_0$, there exist $B \in \mathcal{B}_0$ and $v \notin B$ such that $C = C_0(B, v)$ where $C_0(B, v)$ denotes the fundamental circuit relative to B and v in $\mathbf{M}_0$. We have:

$$u \in C_0(B, v) \iff B - u + v \in \mathcal{B}_0 \iff \omega(B - u + v) = \omega(B).$$

Recall that

$$X(B, v) = (\omega(B - u + v) - \omega(B) \mid u \in V).$$

Since $\omega(B - u + v) \leq \omega(B)$ for all $u \in V$, $\mathrm{Max}(X(B, v)) = C_0(B, v)$ holds. Thus, $\mathcal{C}_0 \subseteq \mathrm{Max}(\mathcal{X})$.

Let $X \in \mathcal{X}$ and $v \in \mathrm{Max}(X)$. Then there exist $B \in \mathcal{B}$ and $\alpha \in R$ such that $X = X(B, v) + \alpha \mathbf{1}$. We claim that $\mathrm{Max}(X)$ is dependent in $\mathbf{M}_0$. Suppose to the contrary that $\mathrm{Max}(X)$ is independent in $\mathbf{M}_0$. Then, there exists $B_0 \in \mathcal{B}_0$ with $\mathrm{Max}(X) \subseteq B_0$. Since $v \in B_0 - B$, from (VBX) for B_0, B, v, there is $u \in B - B_0$ such that

$$\omega(B_0) + \omega(B) \leq \omega(B_0 - v + u) + \omega(B - u + v). \tag{4.19}$$

Since $u \notin B_0$ and $\mathrm{Max}(X) \subseteq B_0$, $u \notin \mathrm{Max}(X)$ holds. We have $\omega(B) > \omega(B-u+v)$ because of the definition of $X(B, v)$ and the fact that $u \notin \mathrm{Max}(X)$. On the other hand, $\omega(B_0) \geq \omega(B_0 - v + u)$ holds because $B_0 \in \mathcal{B}_0$. These, however, contradict (4.19). Thus, $\mathrm{Max}(X)$ is dependent in $\mathbf{M}_0$. That is, there exists $C \in \mathcal{C}_0$ with $C \subseteq \mathrm{Max}(X)$. Hence $\mathrm{Minsupp}(\mathrm{Max}(\mathcal{X})) \subseteq \mathcal{C}_0$.

Since $\mathcal{C}_0$ satisfies (MC2), $\mathcal{C}_0 \subseteq \mathrm{Max}(\mathcal{X})$ and $\mathcal{C}_0 \supseteq \mathrm{Minsupp}(\mathrm{Max}(\mathcal{X}))$, we obtain $\mathcal{C}_0 = \mathrm{Minsupp}(\mathrm{Max}(\mathcal{X}))$ by Lemma 4.19. ∎

4.6 Proof of Theorem 3.8

Lemma 4.20 *Let $\mathcal{X}$ be a set of $(R \cup \{-\infty\})$-valued vectors and $\mathcal{V} = \Phi_{\mathcal{X} \to \mathcal{V}}(\mathcal{X})$. Then $\mathcal{X}^\perp = \mathcal{V}^\perp$.*

Proof. Obviously, $\mathcal{X}^\perp \supseteq \mathcal{V}^\perp$ follows from $\mathcal{X} \subseteq \mathcal{V}$. We will prove the converse. It is enough to show that $X \perp Y$ for any $Y \in \mathcal{X}^\perp$ and any $X \in \mathcal{V}$. From (3.4), there exist $X^1, \ldots, X^k \in \mathcal{X}$ with $X = \max(X^1, \ldots, X^k)$. If $\underline{X} \cap \underline{Y} = \emptyset$ then obviously $X \perp Y$. We assume that there is $i_0 \in \mathrm{Max}(X + Y)$. Then, for some $X^\ell \in \{X^1, \ldots, X^k\}$, $X^\ell_{i_0} = X_{i_0}$, and furthermore, $i_0 \in \mathrm{Max}(X^\ell + Y)$. Since $Y \in \mathcal{X}^\perp$ and $X^\ell \in \mathcal{X}$, we have $X^\ell \perp Y$, i.e., $|\mathrm{Max}(X^\ell + Y)| \neq 1$. Thus, there exists $j_0 \in \mathrm{Max}(X^\ell + Y) - i_0$. Therefore, we have $j_0 \in \mathrm{Max}(X + Y)$ because

$$\max_i (X_i + Y_i) = X^\ell_{i_0} + Y_{i_0} = X^\ell_{j_0} + Y_{j_0} \leq \max_i (X_i + Y_i).$$

Hence $|\mathrm{Max}(X + Y)| \geq 2$, that is, $X \perp Y$. ∎

Lemma 4.21 *Let $(V, \mathcal{B}, \omega, \mathcal{X}, \mathcal{V})$ and $(V, \mathcal{B}^*, \omega^*, \mathcal{X}^*, \mathcal{V}^*)$ be the pair of a valuated matroid and its dual. Then*

(1) $\mathcal{X}^* \subseteq \mathcal{X}^\perp$.

(2) $\mathcal{V}^* \subseteq \mathcal{V}^\perp$.

Proof. (1): Let X be any element of $\mathcal{X}$ and Y any element of $\mathcal{X}^*$. If $\underline{X} \cap \underline{Y} = \emptyset$ then $X \perp Y$. We assume that there is $u \in \underline{X} \cap \underline{Y}$. Without loss of generality, we assume that $X_u = Y_u = 0$. Then, there exist $B \in \mathcal{B}$ and $B^* \in \mathcal{B}^*$ such that

$$\begin{aligned} X_i &= \omega(B - i + u) - \omega(B) \\ Y_i &= \omega^*(B^* - i + u) - \omega^*(B^*) \;=\; \omega(B' - u + i) - \omega(B') \end{aligned}$$

where $B' = V - B^*$. We have

$$X_i + Y_i = \omega(B - i + u) + \omega(B' - u + i) - \omega(B) - \omega(B').$$

Let

$$\begin{aligned} \alpha &= \max_{i \in B - B'} \{\omega(B - i + u) + \omega(B' - u + i)\}, \\ H &= \arg\max_{i \in B - B'} \{\omega(B - i + u) + \omega(B' - u + i)\}. \end{aligned}$$

Since $\alpha \geq \omega(B) + \omega(B') > -\infty$ by (VBX), we have $H \neq \emptyset$. If $\alpha > \omega(B) + \omega(B')$ then $|H| \geq 2$ from Lemma 4.2. In this case, $\mathrm{Max}(X + Y) = H$ holds and this implies $X \perp Y$. If $\alpha = \omega(B) + \omega(B')$, then $|\mathrm{Max}(X + Y)| = |H + u| \geq 2$, and therefore $X \perp Y$. Hence $\mathcal{X}^* \subseteq \mathcal{X}^\perp$.

(2): Let X be any element of $\mathcal{V}$ and Y any element of $\mathcal{V}^*$. Then there exist circuits $X^1, \ldots, X^k \in \mathcal{X}$ and cocircuits $Y^1, \ldots, Y^\ell \in \mathcal{X}^*$ such that $X = \max(X^1, \ldots, X^k)$ and $Y = \max(Y^1, \ldots, Y^\ell)$. If $\underline{X} \cap \underline{Y} = \emptyset$ then $X \perp Y$. Assume that $\underline{X} \cap \underline{Y} \neq \emptyset$. There exist $X^{k'} \in \{X^1, \ldots, X^k\}$, $Y^{\ell'} \in \{Y^1, \ldots, Y^\ell\}$ and $i \in \mathrm{Max}(X + Y)$ such that $X_i = X^{k'}_i$ and $Y_i = Y^{\ell'}_i$. From (1) and $i \in \underline{X^{k'}} \cap \underline{Y^{\ell'}}$, we have $|\mathrm{Max}(X^{k'} + Y^{\ell'})| \geq 2$. Furthermore, $\mathrm{Max}(X + Y) \supseteq \mathrm{Max}(X^{k'} + Y^{\ell'})$ holds. Hence we obtain $|\mathrm{Max}(X + Y)| \geq 2$ and $X \perp Y$. ∎

Lemma 4.22 *Let $(V, \mathcal{B}, \omega, \mathcal{X})$ and $(V, \mathcal{B}^*, \omega^*, \mathcal{X}^*)$ be the pair of a valuated matroid and its dual. Then,* $\mathrm{Minsupp}(\mathcal{X}^\perp) \subseteq \mathcal{X}^*$.

Proof. For any $Y \in \mathcal{X}^\perp$ with nonempty support, we claim that $\underline{Y}$ is dependent in matroid $(V, \mathcal{B}^*)$. Suppose to the contrary that $\underline{Y}$ is independent, and hence, there exists $B^* \in \mathcal{B}^*$ with $\underline{Y} \subseteq B^*$. For $v \in \underline{Y}$, let us consider circuit $X = X(B, v) \in \mathcal{X}$, where $B = V - B^*$. Since $\underline{Y} \cap \underline{X} = \{v\}$, we obtain $|\mathrm{Max}(X + Y)| = 1$, a contradiction to $X \perp Y$. From (1) of Lemma 4.21 and Lemma 4.19, we obtain $\underline{\mathrm{Minsupp}(\mathcal{X}^\perp)} = \underline{(\mathcal{X}^*)}$.

Let Y be any element of $\mathrm{Minsupp}(\mathcal{X}^\perp)$ and u a fixed element of $\underline{Y}$. From the above discussion, there exists $B^* \in \mathcal{B}^*$ with $\underline{Y} - u \subseteq B^*$. Let $B = V - B^*$. For each $v \in \underline{Y} - u$, we denote $X(B, v)$ by X^v. Since $\underline{Y} - u \subseteq B^*$, $\underline{X^v} - v \subseteq B$ and $B \cap B^* = \emptyset$, we have $\underline{X^v} \cap \underline{Y} \subseteq \{u, v\}$. On the other hand, the facts that $v \in \underline{X^v} \cap \underline{Y}$, $\underline{X^v} \in \underline{\mathcal{X}}$ and $\underline{Y} \in \underline{(\mathcal{X}^*)}$ imply $|\underline{X^v} \cap \underline{Y}| \geq 2$. Thus, $\underline{X^v} \cap \underline{Y} = \{u, v\}$ holds. We have

$$X^v_u + Y_u = X^v_v + Y_v$$

because $X^v \perp Y$ and $\underline{X^v} \cap \underline{Y} = \{u, v\}$. Since $X^v_u = \omega(B - u + v) - \omega(B)$ and $X^v_v = 0$,

$$Y_v - Y_u = \omega(B - u + v) - \omega(B) = \omega^*(B^* - v + u) - \omega^*(B^*),$$

for all v. This says that $Y \in \mathcal{X}^*$. Hence $\mathrm{Minsupp}(\mathcal{X}^\perp) \subseteq \mathcal{X}^*$. ∎

Proof of Theorem 3.8

(1): From Lemma 4.20 and (2) of Lemma 4.21, it is sufficient to prove $\mathcal{V}^{\perp} \subseteq \mathcal{V}^*$. Let Y be any element of $\mathcal{V}^{\perp}$ and r_0 the rank of $\underline{Y}$ in the matroid $(V, \mathcal{B}^*)$. We denote by $p \in R^V$ the vector defined by

$$p_i = \begin{cases} Y_i & \text{if } i \in \underline{Y} \\ 0 & \text{otherwise.} \end{cases}$$

We fix $u \in \underline{Y}$. Let B^* be a base in $\mathcal{B}^*$ attaining

$$\max\{\omega^*[p](\tilde{B}) \mid \tilde{B} \in \mathcal{B}^* \text{ with } |\tilde{B} \cap \underline{Y}| = r_0 \text{ and } u \in \tilde{B}\}, \tag{4.20}$$

and put $B = V - B^* \in \mathcal{B}$ and $X = X(B, u) \in \mathcal{X}$. Lemma 4.20 implies $X \perp Y$. Since $u \in \underline{X} \cap \underline{Y}$, there exists $v \in \mathrm{Max}(X + Y) - u$, and hence,

$$X_v + Y_v \geq X_u + Y_u. \tag{4.21}$$

Let $Y^u = (Y^u_i \mid i \in V) \in \mathcal{X}^*$ be defined by $Y^u_i = \omega^*(B^* - i + v) - \omega^*(B^*)$. Since $|B^* \cap \underline{Y}| = r_0$, we have $\underline{Y^u} \subseteq \underline{Y}$. Furthermore, $\underline{X} \cap \underline{Y^u} = \{u, v\}$ holds because $\underline{X} \subseteq B + u$, $\underline{Y^u} \subseteq B^* + v$, and $B \cap B^* = \emptyset$. On the other hand, since B^* is a maximizer of (4.20), for any $i \in \underline{Y^u} - u \subseteq \underline{Y} - u$,

$$\begin{aligned} 0 &\geq \omega^*[p](B^* - i + v) - \omega^*[p](B^*) \\ &= \omega^*(B^* - i + v) - \omega^*(B^*) - Y_i + Y_v \\ &= Y^u_i - Y_i + Y_v. \end{aligned} \tag{4.22}$$

Since $X \perp Y^u$ by Lemma 4.21(1) and $\underline{X} \cap \underline{Y^u} = \{u, v\}$,

$$Y^u_u + X_u = Y^u_v + X_v \tag{4.23}$$

must hold. (4.21) and (4.23) imply

$$Y^u_u - Y^u_v \geq Y_u - Y_v. \tag{4.24}$$

By (4.22), (4.24) and $Y^u_v = 0$, we obtain

$$Y^u_u - Y^u_i \geq Y^u_u - Y_i + Y_v \geq Y_u - Y_i.$$

This and (4.24) guarantee that $\tilde{Y}^u = Y^u + (Y_u - Y^u_u)\mathbf{1} \leq Y$ and $\tilde{Y}^u_u = Y_u$. Hence we obtain $Y = \max(\tilde{Y}^u \mid u \in \underline{Y}) \in \mathcal{V}^*$. That is, $\mathcal{V}^{\perp} \subseteq \mathcal{V}^*$. This and Lemma 4.21(2) imply $\mathcal{V}^{\perp} = \mathcal{V}^*$.

(2): From Lemma 4.20, we prove $\mathcal{X}^* = \mathrm{Minsupp}(\mathcal{X}^{\perp})$. By Lemma 4.22, it is enough to show that $Y \in \mathrm{Minsupp}(\mathcal{X}^{\perp})$ for any $Y \in \mathcal{X}^*$. Since $Y \in \mathcal{X}^* \subseteq \mathcal{X}^{\perp}$ from (1) of Lemma 4.21, there exists $Z \in \mathrm{Minsupp}(\mathcal{X}^{\perp}) \subseteq \mathcal{X}^*$ with $\underline{Z} \subseteq \underline{Y}$. Since $\mathcal{X}^*$ satisfies (VC2), $\underline{Z} = \underline{Y}$ must hold. Hence we obtain $Y \in \mathrm{Minsupp}(\mathcal{X}^{\perp})$. [An alternative shorter proof is given by a combination of (1) of Theorem 3.8, Theorem 3.5 and the relation $\mathcal{X}^* = \mathrm{Minsupp}(\mathcal{V}^*)$.] ∎

4.7 Proofs of Theorems 3.11 and 3.12

We first prove Theorem 3.12.

Proof of Theorem 3.12 To prove the necessity, it is enough to show that the circuit family $\mathcal{X}$ satisfies the alternative painting property, because $\mathcal{X}[p]$ is also the circuit family of some valuated matroid. Let $\omega = \Phi_{\mathcal{X}\to\omega}(\mathcal{X})$ and $\mathcal{B}$ be the base family of the valuated matroid $(V, \mathcal{X})$. Theorem 3.7 says that Minsupp(Max($\mathcal{X}$)) is the circuit family of a matroid $(V, \mathcal{B}')$ defined by

$$\mathcal{B}' = \{B \in \mathcal{B} \mid \omega(B) = \max_{B' \in \mathcal{B}} \omega(B')\},$$

and that Minsupp(Max($\mathcal{X}^*$)), where $(V, \mathcal{X}^*)$ is the dual of $(V, \mathcal{X})$, is the circuit family of another matroid $(V, \mathcal{B}'')$ defined by

$$\mathcal{B}'' = \{B^* \in \mathcal{B}^* \mid \omega^*(B^*) = \max_{B' \in \mathcal{B}^*} \omega^*(B')\}.$$

From (3.8) and (3.9), we have $\mathcal{B}'' = (\mathcal{B}')^*$, and hence, Minsupp(Max($\mathcal{X}$)) and Minsupp(Max($\mathcal{X}^*$)) are the families of circuits and cocircuits of the matroid $(V, \mathcal{B}')$, whereas the latter coincides with Minsupp(Max(Minsupp($\mathcal{X}^\perp$))) by Theorem 3.8. Hence, $\mathcal{X}$ satisfies the alternative painting property by Theorem 3.10.

To prove the sufficiency, we show that $\mathcal{X}$ satisfies (VCE). Since $(\mathcal{X}[p])^\perp = \mathcal{X}^\perp[-p]$, we can rewrite the hypothesis as follows: for any $p \in R^V$ and any painting G, B, W of V, either

(a) $\exists X \in \mathcal{X}$ such that $G \subseteq \mathrm{Max}(X + p) \subseteq G \cup B$, or

(b) $\exists Y \in \mathrm{Minsupp}(\mathcal{X}^\perp)$ such that $G \subseteq \mathrm{Max}(Y - p) \subseteq G \cup W$.

Note that (a) and (b) do not hold simultaneously, from the orthogonality of X and Y.

Let X and Y be elements in $\mathcal{X}$ with $X_u = Y_u \neq -\infty$ and $X_v > Y_v$. We consider a vector p defined by

$$p_i = \begin{cases} -\max(X_i, Y_i) & \text{if } i \in (\underline{X} \cup \underline{Y}) - u \\ M & \text{otherwise} \end{cases}$$

where M is a number larger than $\max\{X'_i - X'_j \mid X' \in \mathcal{X} \text{ and } i, j \in \underline{X'}\} - X_v$. Such M exists by (VC3$_\mathrm{e}$). We paint V as

$$G = \{v\},\ B = (\underline{X} \cup \underline{Y}) - \{u, v\} \quad \text{and} \quad W = (V - (\underline{X} \cup \underline{Y})) + u.$$

We claim that the alternative (a) holds for this painting. Suppose that (b) holds, i.e., there exists $Z' \in \mathcal{X}^\perp$ with $v \in \mathrm{Max}(Z' - p) \subseteq W + v$. Then, we have $\emptyset \neq \mathrm{Max}((X+p)+(Z'-p)) \subseteq \{u, v\}$. From the fact that $\mathrm{Max}((X+p)+(Z'-p)) =$

$\mathrm{Max}(X+Z')$ and the orthogonality of X and Z', $\mathrm{Max}(X+Z') = \{u, v\}$ must hold. Since $X_u = Y_u$ and $(Z'-p)_i < (Z'-p)_v$ for any $i \in \underline{Y} - \{u, v\} \subseteq B$, we have $u \in \mathrm{Max}((Y+p)+(Z'-p)) = \mathrm{Max}(Y+Z') \subseteq \{u, v\}$, whereas $X_v > Y_v$. Thus $\mathrm{Max}(Y+Z') = \{u\}$ must hold. This, however, contradicts the fact that $Z' \in \mathcal{X}^\perp$. Hence (a) must hold. Let Z be an element of $\mathcal{X}$ with $v \in \mathrm{Max}(Z+p) \subseteq (\underline{X} \cup \underline{Y}) - u$. We may assume $Z_v = X_v$. For any $i \in W$, it holds that

$$Z_i + M = (Z+p)_i < (Z+p)_v = X_v - \max(X_v, Y_v) = 0.$$

Since $M > \max\{Z_i - Z_j \mid i, j \in \underline{Z}\} - Z_v$, we have $Z_u = -\infty$ and $Z_i = -\infty$ for $i \notin \underline{X} \cup \underline{Y}$. Similarly, we can prove that $Z \leq \max(X, Y)$. Thus,

$$Z_u = -\infty,\ Z_v = \max(X_v, Y_v) = X_v \text{ and } Z \leq \max(X, Y).$$

Hence $\mathcal{X}$ has (VCE). ∎

Proof of Theorem 3.11 We first prove the necessity of (1) and (2). Theorem 3.8 guarantees that $X \perp Y$ for any $X \in \mathcal{X}$ and $Y \in \mathcal{Y}$. By Theorem 3.8 and Corollary 3.9, $\mathcal{Y}[-p] = \mathcal{X}^*[-p]$ is expressed as $\mathrm{Minsupp}(\mathcal{X}^\perp[-p])$. Theorem 3.12 says that the pair of $\mathcal{X}[p]$ and $\mathcal{Y}[-p]$ satisfies the alternative painting property.

We next prove the sufficiency of (1) and (2). In the same way as in the proof of Theorem 3.12, we can show that $\mathcal{X}$ and $\mathcal{Y}$ each satisfy (VCE). It remains to prove $\mathcal{Y} = \mathcal{X}^*$. Let Y be any element of $\mathcal{X}^*$ and v an arbitrary element of $\underline{Y}$. We consider a vector p defined by

$$p_i = \begin{cases} Y_i & \text{if } i \in \underline{Y} \\ -M & \text{otherwise} \end{cases}$$

where M is a number larger than $\max\{Y'_i - Y'_j \mid Y' \in \mathcal{Y} \text{ and } i, j \in \underline{Y'}\} - Y_v$, and a painting of V defined by

$$G = \{v\},\ B = V - \underline{Y} \quad \text{and} \quad W = \underline{Y} - v.$$

Such M exists because $\mathcal{Y}$ enjoys ($\mathrm{VC3_e}$). By Theorem 3.8, the alternative painting property (a) cannot hold for $\mathcal{X}[p]$ and $\mathcal{Y}[-p]$. Then (b) must be satisfied, that is, there exists $Z^v \in \mathcal{Y}$ with $v \in \mathrm{Max}(Z^v - p) \subseteq \underline{Y}$. For any $i \in V - \underline{Y}$, we have $Z^v_i + M < Z^v_v - Y_v$, and hence, $Z^v_i = -\infty$, because $M > \max\{Z^v_i - Z^v_j \mid i, j \in \underline{Z^v}\} - Y_v$. That is, $\underline{Z^v} \subseteq \underline{Y}$. This implies $\underline{Z^v} = \underline{Y}$, since $Z^v \in \mathcal{Y} \subseteq \mathcal{X}^\perp$ by the assumption (1) and $Y \in \mathcal{X}^* = \mathrm{Minsupp}(\mathcal{X}^\perp)$ by Theorem 3.8. Since $\mathcal{Y}$ satisfies ($\mathrm{VC3_e}$), there exists $Z \in \mathcal{Y}$ such that $\underline{Z} = \underline{Y}$ and $v \in \mathrm{Max}(Z - Y) \subseteq \underline{Y}$ for any element $v \in \underline{Y}$. Hence $Z = Y + \alpha\mathbf{1}$ for some $\alpha \in R$. Therefore $\mathcal{X}^* \subseteq \mathcal{Y} \subseteq \mathcal{X}^\perp$. Since $\mathcal{Y}$ satisfies (VC2), we obtain $\mathcal{Y} = \mathcal{X}^*$. ∎

References

[1] I. Althöfer and W. Wenzel, Two-best solutions under distance constraints: The model and exemplary results for matroids, *Adv. in Appl. Math.* **22** (1999), 155–185.

[2] A. Björner, M. Las Vergnas, B. Sturmfels, N. White and G. M. Ziegler, "Oriented Matroids," Cambridge University Press, Cambridge, 1993.

[3] R. G. Bland, A combinatorial abstraction of linear programming, *J. Combin. Theory Ser. B* **23** (1977), 33–57.

[4] R. G. Bland and M. Las Vergnas, Orientability of matroids, *J. Combin. Theory Ser. B* **24** (1978), 94–123.

[5] W. J. Cook, W. H. Cunningham, W. R. Pulleyblank and A. Schrijver, "Combinatorial Optimization," John Wiley, New York, 1998.

[6] A. W. M. Dress and W. Terhalle, Well-layered maps and the maximum-degree $k \times k$-subdeterminant of a matrix of rational functions, *Appl. Math. Lett.* **8** (1995), 19–23.

[7] A. W. M. Dress and W. Wenzel, Valuated matroid: A new look at the greedy algorithm, *Appl. Math. Lett.* **3** (1990), 33–35.

[8] A. W. M. Dress and W. Wenzel, Perfect matroids, *Adv. Math.* **91** (1992), 158–208.

[9] A. W. M. Dress and W. Wenzel, Valuated matroids, *Adv. Math.* **93** (1992), 214–250.

[10] J. Folkman and J. Lawrence, Oriented matroids, *J. Combin. Theory Ser. B* **25** (1978), 199–236.

[11] K. Fukuda and T. Terlaky, Linear complementarity and oriented matroids, *J. Oper. Res. Soc. Japan* **35** (1992), 45–61.

[12] G. J. Minty, On the axiomatic foundations of the theories of directed linear graphs, electrical networks and network programming, *J. Math. Mech.* **15** (1966), 485–520.

[13] K. Murota, Finding optimal minors of valuated bimatroids, *Appl. Math. Lett.* **8** (1995), 37–42.

[14] K. Murota, Valuated matroid intersection, I: optimality criteria, *SIAM J. Discrete Math.* **9** (1996), 545–561.

[15] K. Murota, Valuated matroid intersection, II: algorithms, *SIAM J. Discrete Math.* **9** (1996), 562–576.

[16] K. Murota, Convexity and Steinitz's exchange property, *Adv. Math.* **124** (1996), 272–311.

[17] K. Murota, Matroid valuation on independent sets, *J. Combin. Theory Ser. B* **69** (1997), 59–78.

[18] K. Murota, Fenchel-type duality for matroid valuations, *Math. Programming* **82** (1998), 357–375.

[19] K. Murota, Discrete convex analysis, *Math. Programming* **83** (1998), 313–371.

[20] K. Murota, "Matrices and Matroids for Systems Analysis," Springer-Verlag, Berlin, 2000.

[21] J. G. Oxley, "Matroid Theory," Oxford Science Publications, Oxford, 1992.

[22] T. Terlaky, A finite criss-cross method for oriented matroids, *J. Combin. Theory Ser. B* **42** (1987), 319–327.

[23] M. J. Todd, Complementarity in oriented matroids, *SIAM J. Alg. Disc. Meth.* **5** (1984), 467–485.

[24] M. J. Todd, Linear and quadratic programming in oriented matroids, *J. Combin. Theory Ser. B* **39** (1985), 105–133.

[25] W. T. Tutte, Lectures on matroids, *J. Res. Nat. Bur. Standards Sect. B* **69B** (1965), 1–47.

[26] D. J. A. Welsh, "Matroid Theory," Academic Press, London, 1976.

[27] N. White (ed.), "Theory of Matroids," Cambridge University Press, London, 1986.