Linearly dependent vectorial decomposition of clutters

Jaume Martí-Farré [1,2]

Departament de Matemàtica Aplicada IV
Universitat Politècnica de Catalunya, BarcelonaTech
Barcelona, Spain

Abstract

This paper deals with the question of completing a monotone increasing family of subsets Γ of a finite set Ω to obtain the linearly dependent subsets of a family of vectors of a vector space. Specifically, we demonstrate that such vectorial completions of the family of subsets Γ exist and, in addition, we show that the minimal vectorial completions of the family Γ provide a decomposition of the clutter Λ of the inclusion-minimal elements of Γ. The computation of such vectorial decomposition of clutters is also discussed in some cases.

Keywords: Clutter, Antichain, Hypergraph, Matroid, Decomposition.

1 Introduction

A *monotone increasing* family of subsets Γ of a finite set Ω is a collection of subsets of Ω such that any superset of a set in the family Γ must be in Γ. All the inclusion-minimal elements of Γ determine a *clutter* Λ, that is, a collection

of subsets of Ω none of which is a proper subset of another. Clutters are also known as *antichains*, *Sperner systems* or *simple hypergraphs*.

A wide variety of examples of monotone increasing families exist, among which we find the collection of the linearly dependent subsets of vectors in a vector space. We say that a clutter Λ is *LD-vectorial* if its elements are the inclusion-minimal linearly dependent subsets of an indexed family of vectors of a vector space. In other words, the LD-vectorial clutters are exactly those corresponding to the set of *circuits of representable matroids*.

In some cases it is convenient to use clutters that are either LD-vectorial or are closed to be LD-vectorial. Examples of this situation can be found in the context of secret-sharing schemes [3,5], or in the framework of algebraic combinatorics and commutative algebra [1,6]. For instance, in the context of secret-sharing schemes, the LD-vectorial clutters become a crucial issue for providing general bounds on the optimal information rate of the scheme, while in the framework of algebraic combinatorics and commutative algebra, they are useful for controlling certain arithmetic properties of either monomial ideals or the face rings of simplicial complexes.

In general, a clutter is far from being LD-vectorial. Therefore it is of interest to determine how it can be transformed into an LD-vectorial clutter. This paper deals with this issue; that is, with the question of finding *LD-vectorial completions of a clutter*. Specifically, the goal of this paper is to prove that these completions exist and that the *minimal* ones provide a *decomposition* of the clutter.

The outline of the paper is as follows. In Section 2 we recall some definitions and basic facts about clutters and present the problem of the LD-vectorial completion of a clutter. Our main results are gathered in Section 3; namely, we present two theorems concerning LD-vectorial decomposition of clutters (Theorem 3.1 and Theorem 3.2). Finally, Section 4 is devoted to analyzing the computation of such decompositions (Proposition 4.1). Due to limitations of space, the proofs are omitted.

2 LD-vectorial clutters and LD-vectorial completions

In this section we present the definitions and basic facts concerning families of subsets, clutters and LD-vectorial clutters that are used in the paper.

Let Ω be a finite set. A family of subsets Γ of Ω is *monotone increasing* if any superset of a set in Γ must be in Γ; that is, if $A \in \Gamma$ and $A \subseteq A' \subseteq \Omega$, then $A' \in \Gamma$. A *clutter* of Ω is a collection of subsets Λ of Ω, none of which is a proper subset of another; that is, if $A, A' \in \Lambda$ and $A \subseteq A'$ then $A = A'$.

Observe that if Γ is a monotone increasing family of subsets of Ω, then the collection $\min(\Gamma)$ of its inclusion-minimal elements is a clutter; while if Λ is a clutter on Ω, then the family $\Lambda^+ = \{A \subseteq \Omega : A_0 \subseteq A \text{ for some } A_0 \in \Lambda\}$ is a monotone increasing family of subsets. Clearly $\Gamma = (\min(\Gamma))^+$ and $\Lambda = \min(\Lambda^+)$. So a monotone increasing family of subsets Γ is determined uniquely by the clutter $\min(\Gamma)$, while a clutter Λ is determined uniquely by the monotone increasing family Λ^+.

Let Λ_1, Λ_2 be two clutters on Ω. It is clear that if $\Lambda_1 \subseteq \Lambda_2$ then $\Lambda_1^+ \subseteq \Lambda_2^+$. However, the converse is not true; that is, there exist clutters with $\Lambda_1 \nsubseteq \Lambda_2$ and $\Lambda_1^+ \subseteq \Lambda_2^+$. For instance, on the finite set $\Omega = \{1, 2, 3\}$, let us consider the clutters $\Lambda_1 = \{\{1, 2\}, \{2, 3\}\}$ and $\Lambda_2 = \{\{1\}, \{2, 3\}\}$. Then $\Lambda_1 \nsubseteq \Lambda_2$, while $\Lambda_1^+ = \{\{1, 2\}, \{2, 3\}, \{1, 2, 3\}\} \subseteq \{\{1\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\} = \Lambda_2^+$.

This fact leads us to consider a binary relation $\leq$ defined on the set of clutters on Ω. Namely, if Λ_1 and Λ_2 are two clutters on Ω, then we say that $\Lambda_1 \leq \Lambda_2$ if and only if $\Lambda_1^+ \subseteq \Lambda_2^+$. The following lemma will be used several times throughout the paper.

Lemma 2.1 *Let Ω be a finite set. The following statements hold:*

(i) *If Λ_1, Λ_2 are two clutters on Ω then, $\Lambda_1 \leq \Lambda_2$ if and only if for all $A_1 \in \Lambda_1$ there exists $A_2 \in \Lambda_2$ such that $A_2 \subseteq A_1$.*

(ii) *The binary relation $\leq$ is a partial order on the set of clutters of Ω.*

There are many interesting families of clutters that can be considered. However, because of their applications, we are interested in those clutters that are *LD-vectorial*.

Let $\Omega = \{x_1, \ldots, x_n\}$ be a finite set of n elements. A monotone increasing family Γ of subsets of Ω is said to be an *LD-vectorial family* if there exists an indexed family of vectors $v_1, \ldots, v_n$ of a $\mathbb{K}$-vector space (that can be $v_i = v_j$) such that $\{x_{i_1}, \ldots, x_{i_r}\} \in \Gamma$ if and only if $\{v_{i_1}, \ldots, v_{i_r}\}$ is a linearly dependent set of vectors. A clutter Λ on Ω is said to be an *LD-vectorial clutter* if the monotone increasing family Λ^+ is an LD-vectorial family.

In other words, a monotone increasing family of subsets Γ is LD-vectorial if Γ is the family of the *dependent sets of a representable matroid* $\mathcal{M}$ with ground set Ω; whereas a clutter Λ is LD-vectorial if the clutter Λ is the set of *circuits of a representable matroid* $\mathcal{M}$ with ground set Ω. (The reader is referred to [4,7] for general references on matroid theory). Observe that since the binary relation $\leq$ is a partial order on the set of clutters of Ω, it is also a partial order on the set of LD-vectorial clutters, and therefore $\leq$ is a partial order on the set of representable matroids. In matroid theory, this is

equivalent to the *weak order* (see [4, Proposition 7.3.11]).

There are clutters on a finite set Ω that are not LD-vectorial (in fact, there are matroids that are not representable matroids). So, a natural question that arises at this point is to determine how to complete a clutter Λ to obtain an LD-vectorial clutter. In order to look for LD-vectorial completions, it is important to take into account the binary relation $\leq$ rather than the inclusion $\subseteq$. This is due to the fact that, as the following example shows, there exist clutters Λ such that $\Lambda \nsubseteq \Lambda'$ for any LD-vectorial clutter Λ'.

Example 2.2 Let us consider the clutter $\Lambda = \{\{1,2\}, \{1,3\}, \{2,3,4\}\}$ on the finite set $\Omega = \{1,2,3,4\}$. Observe that $(\{1,2\} \cup \{1,3\}) \setminus \{1\} = \{2,3\} \subset \{2,3,4\}$. Hence it follows that Λ is not an LD-vectorial clutter and, moreover, $\Lambda \nsubseteq \Lambda'$ for any LD-vectorial clutter Λ'. However, we have that $\Lambda \leq \Lambda'$, where Λ' is the LD-vectorial clutter $\Lambda' = \{\{1\}, \{2,3,4\}\}$ (an LD-vectorial realization of Λ' is given by the set of vectors $\{v_1, v_2, v_3, v_4\}$ where $v_1 = (0,0,0)$, $v_2 = (1,0,0)$, $v_3 = (0,1,0)$ and $v_4 = (0,0,1)$). Futhermore, if Λ'' is the clutter on Ω defined by $\Lambda'' = \{\{1,2\}, \{1,3\}, \{2,3\}\}$, then we have that $\Lambda \leq \Lambda''$ and that the clutter Λ'' is also an LD-vectorial clutter (an LD-vectorial realization of Λ'' is given by the set of vectors $\{w_1, w_2, w_3, w_4\}$ where $w_1 = (1,1)$, $w_2 = (1,1)$, $w_3 = (1,1)$ and $w_4 = (0,1)$). Notice that now the clutter Λ can be obtained from the LD-vectorial clutters Λ' and Λ''. Indeed, it is easy to check that $\Lambda = \min\{A' \cup A'' \text{ where } A' \in \Lambda' \text{ and } A'' \in \Lambda''\}$. Therefore, the clutters Λ' and Λ'' in some way provide a decomposition of Λ.

The above example leads us to the following definition. Let Λ be a clutter on a finite set Ω. An *LD-vectorial completion* of the clutter Λ is an LD-vectorial clutter Λ' on the finite set Ω such that $\Lambda \leq \Lambda'$.

The set of all the LD-vectorial completions of a clutter Λ is denoted by LD-Vect(Λ). Observe that if $\emptyset \in \Lambda$, then $\Lambda = \{\emptyset\}$, and thus LD-Vect(Λ) = $\emptyset$. So, from now on, throughout the paper we assume that $\emptyset \notin \Lambda$ if Λ is a clutter. As shown in the next section, this assumption guarantees that LD-Vect(Λ) $\neq \emptyset$ for all clutters and, in addition, we demonstrate that suitable clutters in the non-empty set LD-Vect(Λ) provide a decomposition of the clutter Λ in the same way as in Example 2.2.

3 Two results on LD-vectorial decompositions

The aim of this section is to present two theoretical results concerning the "decomposition" of a clutter Λ into LD-vectorial clutters $\Lambda_1, \ldots, \Lambda_r$, (Theorem 3.1 and Theorem 3.2). The general case is considered in the first theorem,

while the second deals with those "decompositions" of Λ whose LD-vectorial components $\Lambda_1, \ldots, \Lambda_r$ admit vectorial realizations over a fixed field $\mathbb{K}$.

Let Λ be a clutter on a finite set Ω. Our first result, Theorem 3.1, states that the set LD-Vect (Λ) of its LD-vectorial completions is a non-empty set and that its minimal elements provide a decomposition of Λ (in the sense that the elements A of the clutter Λ can be obtained from the elements A_i of its minimal LD-vectorial completions $\Lambda_1, \ldots, \Lambda_r$).

Theorem 3.1 *Let Λ be a clutter on a finite set Ω. Then, LD-Vect $(\Lambda) \neq \emptyset$ and $\Lambda = \min \{A_1 \cup \ldots \cup A_r$ where $A_i \in \Lambda_i\}$ where $\Lambda_1, \ldots, \Lambda_r$ are the minimal elements of the poset $(LD\text{-}Vect(\Lambda), \leq)$ of the LD-vectorial completions of Λ. In particular, the clutter Λ has a unique minimal LD-vectorial completion if, and only if, Λ is an LD-vectorial clutter.*

Observe that the previous theorem, Theorem 3.1, deals with LD-vectorial completions and decompositions in the case where no field restrictions are assumed. The next theorem, Theorem 3.2, states that a similar result occurs if we consider only the case in which the vector spaces of the LD-vectorial completions are over a fixed field $\mathbb{K}$. Before stating the theorem, we introduce some notations.

Let Λ be a clutter on a finite set Ω and let $\mathbb{K}$ be a field. Let us denote by LD-Vect $_{\mathbb{K}}(\Lambda)$ the set whose elements are the LD-vectorial completions of Λ over $\mathbb{K}$; that is, the elements of LD-Vect $_{\mathbb{K}}(\Lambda)$ are the LD-vectorial clutters Λ' over $\mathbb{K}$ with $\Lambda \leq \Lambda'$. Therefore, LD-Vect $(\Lambda) = \bigcup_{\mathbb{K}}$ LD-Vect $_{\mathbb{K}}(\Lambda)$.

The next theorem states that the set LD-Vect $_{\mathbb{K}}(\Lambda)$ is a non-empty set and that its minimal elements provides a decomposition of the clutter Λ (in the sense that the elements of Λ can be obtained from the elements of its minimal LD-vectorial completions over $\mathbb{K}$).

Theorem 3.2 *Let Λ be a clutter on a finite set Ω and let $\mathbb{K}$ be a field. Then, LD-Vect$_{\mathbb{K}}(\Lambda) \neq \emptyset$ and $\Lambda = \min \{A_1 \cup \ldots \cup A_r$ where $A_i \in \Lambda_i\}$ where $\Lambda_1, \ldots, \Lambda_r$ are the minimal elements of the poset $(LD\text{-}Vect_{\mathbb{K}}(\Lambda), \leq)$. In particular, the clutter Λ has a unique minimal LD-vectorial completion over $\mathbb{K}$ if, and only if, Λ is an LD-vectorial clutter over $\mathbb{K}$.*

4 Computing LD-vectorial decompositions

This section is devoted to the computation of the LD-vectorial decomposition of clutters. First we present a partial result (Proposition 4.1). After this, several examples are given in order to illustrate this proposition (Example 4.2 and

Example 4.3). Finally, an example where the proposition cannot be applied is analyzed (Example 4.4).

Our result, Proposition 4.1, provides a complete description of the minimal LD-vectorial completion of a clutter Λ on a finite set Ω of size at most seven. In order to state this proposition, we need to introduce two transformations of clutters, the *I-transformation* and the $\mathcal{T}$*-transformation* (see [2]).

Let Λ be a clutter on a finite set Ω. For a subset $X \subseteq \Omega$, we denote by $I_\Lambda(X)$ the intersection of the subsets A in Λ contained in X, that is, $I_\Lambda(X) = \bigcap_A A$ where $A \in \Lambda$ and $A \subseteq X$, (this intersection is the one involved in the characterization of the set of circuits in connected matroids, see [4, Theorem 4.3.2]). We say that a clutter Λ' is an *I-transformation* of the clutter Λ if $\Lambda' = \min(\Lambda \cup \{A_1 \cap A_2\})$ where $A_1, A_2 \in \Lambda$ are two different subsets with $I_\Lambda(A_1 \cup A_2) \neq \emptyset$.

The definition of $\mathcal{T}$*-transformation* is more involved. Let Λ be a clutter. We define the elementary transformations $\mathcal{T}^{(1)}(\Lambda)$ and $\mathcal{T}^{(2)}(\Lambda)$ of the clutter Λ as the clutters $\mathcal{T}^{(1)}(\Lambda) = \min(\Lambda \cup \{(A_1 \cup A_2) \setminus \{x\}$, where $A_1, A_2 \in \Lambda$ are different and $x \in A_1 \cap A_2\})$ and $\mathcal{T}^{(2)}(\Lambda) = \min(\Lambda \cup \{(A_1 \cup A_2) \setminus I_\Lambda(A_1 \cup A_2)$, where $A_1, A_2 \in \Lambda$ are different$\})$. Since $\mathcal{T}^{(1)}(\Lambda)$ and $\mathcal{T}^{(2)}(\Lambda)$ are clutters, we can apply the elementary transformations again. Hence, for $(i_1, i_2) \in \{1, 2\} \times \{1, 2\}$ we can consider the clutter $\mathcal{T}^{(i_2)}(\mathcal{T}^{(i_1)}(\Lambda))$. At this point we proceed in a recursive way. Let $r \geq 2$ be a non-negative integer and let $(i_1, \ldots, i_r) \in \{1, 2\}^r$ be an r-tuple. Then we define the clutter $\mathcal{T}^{(i_1, \ldots, i_r)}(\Lambda)$ by the recursion formula $\mathcal{T}^{(i_1, \ldots, i_r)}(\Lambda) = \mathcal{T}^{(i_r)}(\mathcal{T}^{(i_1, \ldots, i_{r-1})}(\Lambda))$; that is, $\mathcal{T}^{(i_1, \ldots, i_r)}(\Lambda)$ is the i_r elementary transformation of $\mathcal{T}^{(i_1, \ldots, i_{r-1})}(\Lambda)$. We say that a clutter Λ' is a $\mathcal{T}$*-transformation* of the clutter Λ if it is obtained from Λ in this way, that is, if $\Lambda' = \mathcal{T}^{(i_1, \ldots, i_r)}(\Lambda)$ for some r-tuple $(i_1, \ldots, i_r)$.

Proposition 4.1 *Let Λ be a non-LD-vectorial clutter on a finite set Ω of size $|\Omega| = n \leq 7$. Let Λ' be a clutter such that $\Lambda \leq \Lambda'$. Then the following statements hold:*

(i) *The clutter Λ' is an LD-vectorial completion of Λ if, and only if, Λ' is the unique clutter which can be obtained from Λ' by applying I-transformations or $\mathcal{T}$-transformations.*

(ii) *If the clutter Λ' is a minimal element of the poset $(LD\text{-}Vect(\Lambda), \leq)$, then there is a monotone increasing sequence of clutters $\Lambda = \Lambda_0 < \Lambda_1 < \ldots < \Lambda_r = \Lambda'$ such that for $i \geq 1$, either Λ_i is an I-transformation of Λ_{i-1}, or Λ_i is a $\mathcal{T}$-transformation of Λ_{i-1}.*

We now give two examples to illustrate the above proposition.

Example 4.2 First, let us consider the clutter $\Lambda = \{\{1,2\},\{1,3\},\{2,3,4\}\}$ on the finite set $\Omega = \{1,2,3,4\}$. In this case only two clutters are obtained by using or by combining I-transformations and $\mathcal{T}$-transformations; namely, the clutters $\Lambda_1 = \{\{1\},\{2,3,4\}\}$ and $\Lambda_2 = \{\{1,2\},\{1,3\},\{2,3\}\}$. Therefore, from Proposition 4.1 it follows that the minimal LD-vectorial completions of the clutter Λ are the minimal elements of $\{\Lambda_1,\Lambda_2\}$. In this case, $\Lambda_1 \not\leq \Lambda_2$ and $\Lambda_2 \not\leq \Lambda_1$, and so $\min\left(\text{LD-Vect}\left(\Lambda\right)\right) = \{\Lambda_1,\Lambda_2\}$. Observe that now the LD-vectorial decomposition of Λ given in Example 2.2 can be stated by applying Theorem 3.1.

Example 4.3 Now, on the finite set $\Omega = \{1,2,3,4,5\}$, we consider the clutter $\Lambda = \{\{1,2,3\},\{1,2,4\},\{1,5\},\{4,5\}\}$. In such a case, it is a straightforward calculation to check that by using or by combining I-transformations and $\mathcal{T}$-transformations, eleven clutters $\Lambda_1,\ldots,\Lambda_{11}$ can be obtained. Specifically, by using only I-transformations we obtain the clutters $\Lambda_1 = \{\{5\},\{1,2\}\}$ and $\Lambda_2 = \{\{1\},\{4,5\}\}$. The clutters obtained by using only $\mathcal{T}$-transformations are the clutters $\Lambda_3 = \{\{1,4\},\{1,5\},\{4,5\},\{1,2,3\},\{2,3,4\},\{2,3,5\}\}$ and $\Lambda_4 = \{\{1,3\},\{1,4\},\{1,5\},\{3,4\},\{3,5\},\{4,5\}\}$, whereas the clutters obtained by combining the I-transformations and the $\mathcal{T}$-transformations are the clutters $\Lambda_5 = \{\{1\},\{5\}\}$, $\Lambda_6 = \{\{1\},\{2,4\},\{2,5\},\{4,5\}\}$, $\Lambda_7 = \{\{5\},\{1,2\},\{1,4\},\{2,4\}\}$, $\Lambda_8 = \{\{1,2\},\{1,4\},\{1,5\},\{2,4\},\{2,5\},\{4,5\}\}$, $\Lambda_9 = \{\{5\},\{1,2,3\},\{1,2,4\},\{1,3,4\},\{2,3,4\}\}$, $\Lambda_{10} = \{\{5\},\{3,4\},\{1,2,3\},\{1,2,4\}\}$, and $\Lambda_{11} = \{\{4\},\{1,5\},\{1,2,3\},\{2,3,5\}\}$. Therefore, by applying Proposition 4.1 we obtain that the set of the minimal LD-vectorial completions of the clutter Λ is $\min\left(\text{LD-Vect}\left(\Lambda\right)\right) = \min\{\Lambda_1,\ldots,\Lambda_{11}\} = \{\Lambda_1,\Lambda_2,\Lambda_3,\Lambda_9\}$. So, from Theorem 3.1 we conclude that Λ admits an LD-vectorial decomposition with four components.

To conclude we give an example where Proposition 4.1 cannot be applied. In addition, the clutter in this example reveals the difference between Theorem 3.1 and Theorem 3.2.

Example 4.4 On the finite set $\Omega = \{1,2,3,4\}$ of four points, we consider the clutter $\Lambda = \{\{1,2,3\},\{1,2,4\},\{1,3,4\},\{2,3,4\}\}$. It is easy to prove that the clutter Λ is an LD-vectorial clutter over any field $\mathbb{K} \neq \mathbb{Z}/(2)$. Therefore, by applying Theorem 3.1 and Theorem 3.2 we obtain that $\min\left(\text{LD-Vect}\left(\Lambda\right)\right) = \{\Lambda\}$; that $\min\left(\text{LD-Vect}_{\mathbb{K}}\left(\Lambda\right)\right) = \{\Lambda\}$ if $\mathbb{K} \neq \mathbb{Z}/(2)$, and that $\min\left(\text{LD-Vect}_{\mathbb{Z}/(2)}\left(\Lambda\right)\right)$ has at least two elements. In this example, by an extensive exploration it is not hard to show that $\min\left(\text{LD-Vect}_{\mathbb{Z}/(2)}\left(\Lambda\right)\right)$ has six elements; namely $\min\left(\text{LD-Vect}_{\mathbb{Z}/(2)}\left(\Lambda\right)\right) = \{\Lambda_{1,2},\Lambda_{1,3},\Lambda_{1,4},\Lambda_{2,3},\Lambda_{2,4},\Lambda_{3,4}\}$, where if $1 \leq i_1 < i_2 \leq 4$ and if $\{i_3,i_4\} = \{1,2,3,4\} \setminus \{i_1,i_2\}$, then $\Lambda_{i_1,i_2} = \{\{i_1,i_2\},\{i_1,i_3,i_4\},$

$\{i_2, i_3, i_4\}\}$. Now, from Theorem 3.2 it follows that the clutter Λ admits an LD-vectorial decomposition over $\mathbb{Z}/(2)$ with six components.

References

[1] Herzog, J., and T. Hibi, "Monomial Ideals," Grad. Texts in Math. 260, Springer, London, 2010.

[2] Martí-Farré, J., *From clutters to matroids*, Electronic Journal of Combinatorics, **21(1)** (2014), P1.11 (14 pag.).

[3] Martí-Farré, J., and C. Padró, *On secret-sharing schemes, matroids and polymatroids*, Journal of Mathematical Cryptology, **4** (2010), 95–120.

[4] Oxley, J.G., "Matroid Theory," Oxford Graduate Text in Mathematics. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1992.

[5] Seymour, P.D., *On secret-sharing matroids*, J. Combin. Theory Ser. B, **56** (1992), 69–73.

[6] Stanley, R.P., "Combinatorics and Commutative Algebra," Progress in Mathematics 41. Second Edition. Birkhäuser, 1995.

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