Designs, Codes and Cryptography (2019) 87:2913–2940
https://doi.org/10.1007/s10623-019-00657-2

Efficient explicit constructions of compartmented secret sharing schemes

Qi Chen[1] · **Chunming Tang**[2,3] · **Zhiqiang Lin**[2,3]

Received: 27 May 2018 / Revised: 12 June 2019 / Accepted: 14 June 2019 / Published online: 22 June 2019

Abstract
Multipartite secret sharing schemes have been an important object of study in the area of secret sharing schemes. Two interesting families of multipartite access structures are hierarchical access structures and compartmented access structures. This work deals with efficient and explicit constructions of ideal compartmented secret sharing schemes, while most of the known constructions are either inefficient or randomized. We construct ideal linear secret sharing schemes for three types of compartmented access structures, such as compartmented access structures with upper bounds, compartmented access structures with lower bounds, and compartmented access structures with upper and lower bounds. There exist some methods to construct ideal linear schemes realizing these compartmented access structures in the literature, but those methods are inefficient in general because non-singularity of many matrices has to be determined to check the correctness of the scheme. Our constructions do not need to do these computations. Our methods to construct ideal linear schemes realizing these access structures combine polymatroid-based techniques with Gabidulin codes. Gabidulin codes play a fundamental role in the constructions, and their properties imply that our methods are efficient.

Keywords Secret sharing schemes · Multipartite access structures · Compartmented access structures · Matroids · Polymatroids · Gabidulin codes

Mathematics Subject Classification 94A62 · 94B05

1 Introduction

Secret sharing schemes have been a subject of study for almost 40 years, and have had a number of real-world applications. In a secret sharing scheme, every participant receives a share of a secret value. Only the qualified sets of participants, which form the *access structure* of the scheme, can recover the secret value from their shares. A secret sharing scheme is

Communicated by C. Padro.

✉ Qi Chen
chenqi.math@gmail.com

Extended author information available on the last page of the article

perfect if the unqualified subsets do not obtain any information about the secret. The original motivation for secret sharing was robust key management schemes for cryptographic systems. Nowadays, they are used in many secure protocols and applications, such as multiparty computation [5,10,12,13], threshold cryptography [14], access control [29], and attribute-based encryption [21].

In this paper, we focus on *ideal* and *linear* secret sharing schemes. A scheme is ideal if the share of every participant has the same length as the secret, and it is linear if the linear combination of the shares of different secrets results in shares for the same linear combination of the secret values. The first proposed secret sharing schemes [7,33], which have threshold access structure, are ideal and linear. Nevertheless, not all secret sharing schemes are ideal and linear. Ito et al. [24] showed that a linear secret sharing scheme for every access structure can be obtained in a constructive way, but the schemes are not ideal because the length of the shares grows exponentially with the number of participants. Nevertheless, this does not mean that ideal secret sharing schemes exist only for threshold access structures. Actually, it is worthwhile to find families of access structures that admit ideal linear schemes and have useful properties for the applications of secret sharing.

Several such families are formed by multipartite access structures, in which the participants can be divided into different classes, such as hierarchical organizations, or actions that require the agreement of different parties. A great deal of the ongoing research in this area is devoted to the properties of multipartite access structures and to secret sharing schemes (especially ideal and linear ones) that realize them. Weighted threshold access structures [4,33], hierarchical access structures [15,34,35], and compartmented access structures [8,22,36] are typical examples of such multipartite access structures. Even though the existence of ideal linear secret sharing schemes for some of these access structures has been proved, the known methods to construct such schemes are not efficient in general. This is an important difference to the threshold case, in which the construction proposed by Shamir [33] solves the problem. Here, we mainly focused on how to construct ideal multipartite secret sharing schemes by efficient methods, and in particular, the explicit constructions for compartmented access structures.

1.1 Related work

Ideal multipartite secret sharing and their access structures were initially studied by Kothari [25] and by Simmons [34]. Kothari [25] presented some ideas to construct ideal linear schemes with hierarchical properties. Simmons [34] introduced multilevel (also called disjunctive hierarchical threshold access structures (DHTASs) in [35]) and compartmented access structures, and constructed ideal linear schemes for some of them by geometric method [7], but the method is inefficient. Brickell [8] introduced a linear-algebraic technique to construct ideal linear schemes for non-threshold access structures and presented a more general family, that is the so-called compartmented access structures with lower bounds (LCASs) as a generalization of Simmons' compartmented access structures. Based on the linear-algebraic technique, he offered an efficient method to construct ideal linear schemes realizing DHTASs based on primitive polynomials over finite fields. He offered a method to construct ideal linear schemes realizing LCASs too. This method is efficient to construct the scheme realizing Simmons' compartmented access structures but is inefficient to construct the scheme realizing LCASs in general because non-singularity of an exponentially growing number of matrices has to be determined to check the correctness of the scheme.

Tassa [35] introduced the conjunctive hierarchical threshold access structures (CHTASs) and offered an elegant method to construct ideal linear schemes realizing them based on Birkhoff interpolation. Let $\mathbb{K}$ be a finite field and the secret $s \in \mathbb{K}$ is encoded by the coefficients of an unknown polynomial $f(x) \in \mathbb{K}[x]$. The dealer associates each participant with a unique identity $x_i \in \mathbb{K}$ and gives that participant the share $f^{u_i}(x_i)$ where $f^{u_i}(x)$ is some derivative of $f(x)$, for which u_i is an integer depending i. This differs from Shamir's threshold scheme [33] where the share is $f(x_i)$. Shamir's method is efficient since there exist efficient algorithms to solve Lagrange interpolation in the case of random allocation of participant identities. Nevertheless, Birkhoff interpolation does not always have a solution. Thus Tassa's method is probabilistic, that is, it produces a scheme for the given access structure with high probability, but proving it requires again to check non-singularity for many matrices. Of course, it is desirable to find efficient explicit (that is, non-probabilistic) methods. By allocating participant identities in a monotone way, Tassa obtained an efficient explicit method to construct ideal linear schemes for CHTASs over a sufficiently large prime field. Tassa and Dyn [36] further studied the method to construct secret sharing schemes by polynomial interpolation. Based on bivariate interpolation, they presented probabilistic constructions of ideal linear schemes realizing LCASs, a new class of compartmented access structures called compartmented access structures with upper bounds (UCASs), and CHTASs. In particular, they constructed the scheme for LCASs by duality, that is, they construct the scheme for the dual of LCASs by bivariate interpolation and the scheme for LCASs can be obtained based on the scheme for the dual by using the explicit transformation of [18]. Let $\mathbb{K}$ be a finite field and the secret $s \in \mathbb{K}$ is encoded by the coefficients of an unknown polynomial $f(x, y) \in \mathbb{K}[x, y]$ with some special form. In their construction, the dealer associates each participant with a unique identity $(x_i, y_i) \in \mathbb{K}^2$ and gives that participant the share $f(x_i, y_i)$. This method is probabilistic because bivariate interpolation is not always solvable. In addition, efficient methods to construct schemes for some multilevel access structures with two levels and three levels were presented in [6] and [20], respectively, and efficient methods to construct schemes for the ideal bipartite access structures were presented in [1].

Farràs et al. [15–17] studied the connection of multipartite secret sharing schemes, matroids and polymatroids, based on the relationship between secret sharing schemes and matroids [8,9]. They introduced a unified method based on polymatroid techniques, which simplifies in great measure the task of determining whether a given multipartite access structures is ideal or not. Furthermore, they also presented new families of multipartite access structures and proved the existence of ideal schemes realizing these access structures. Particularly, in [17] a more general family of compartmented access structures called compartmented access structure with upper and lower bounds (ULCASs) was presented which generalizes LCASs and UCASs, and the existence of ideal linear schemes for ULCASs was proved over large enough finite fields. Moreover, they presented a general method to construct ideal linear schemes realizing multipartite access structures. More precisely, to construct a secret sharing scheme realizing a given multipartite access structure, first find an integer polymatroid associated to the access structure, then find a representation of the integer polymatroid over some finite field, and third find a representation of the matroid associated to the access structure over some finite extension of the finite field based on the representation of the integer polymatroid. The result in [16] implies ideal linear scheme realizing the access structure can be constructed by this matroid. Thus the problem that how to construct a scheme realizing a multipartite access structure can be transformed to the problem that how to find a representation of a matroid from a presentation of its associated polymatroid. Nevertheless, Farràs et al. [16,17] pointed out it remains open whether or not there exist efficient algorithms to obtain representations of multipartite matroids from representations of their associated

polymatroids in general. In particular, there does not exist any explicit efficient method to construct ideal linear schemes realizing compartmented access structures.

1.2 Our results

In this paper, we study how to construct secret sharing schemes realizing compartmented access structures by efficient methods. The main result is the construction for ULCASs, a family that contains UCASs and LCASs as particular cases. Since they are simpler, and hence easier to understand, constructions for UCASs and LCASs are presented before presenting the general, and more involved, construction for ULCASs.

We give efficient methods to explicitly construct ideal linear schemes realizing these access structures by the general polymatroid-based method presented in [16]. In particular, to construct the schemes for LCASs, we construct the scheme for the dual of LCASs, and based on it, the scheme for LCASs can be obtained by the explicit transformation of [18]. The integer polymatroids associated to UCASs, the dual of LCASs and ULCASs have been presented in [16,17]. Based on these results, for each of the three types of multipartite access structures, we give an efficient method to find a representation of the integer polymatroid over some finite field, and then over some finite extension of that field, we give an efficient method to find a presentation of the matroid associated to the access structure. Accordingly, we construct ideal linear schemes for these access structures.

In general, it is not easy to construct the representation of a matroid associated a given multipartite access structure. To construct a representation of a matroid based on the polymatroid, there are two problems that must be solved. First, how to obtain a suitable representation of the integer polymatroid that simplifies the second problem, namely how to find from it a representation for the multipartite matroid. In order to solve these questions, we introduce Gabidulin codes [19]. Gabidulin codes play a fundamental role in the constructions. In particular, the representations of the integer polymatroids associated to the three types of compartmented access structures are obtained by Gabidulin codes. Then we construct the representable matroids by these representations. The properties of Gabidulin codes imply that our method is efficient.

1.3 Organization of the paper

Section 2 introduces some knowledge about access structures, secret sharing schemes, polymatroids, matroids, Gabidulin codes, and the methods to construct secret sharing schemes by matroids and polymatroids. Sections 3, 4 and 5 construct ideal linear secret sharing schemes realizing UCASs, LCASs and ULCASs, respectively. Section 6 compares our constructions and the constructions in [36]. Section 7 concludes the paper.

2 Preliminaries

We introduce here some notation that will be used all through the paper. In particular, as in [15–17] we recall the compact and useful representation of multipartite access structures that was introduced in [31] for the bipartite case.

We use $\mathbb{Z}_+$ to denote the set of the non-negative integers. for every positive integer i we use the notation $[i] := \{1, \ldots, i\}$ and for every $i, j \in \mathbb{Z}_+$ we use the notation $[i, j] := \{i, \ldots, j\}$ with $i < j$. Consider a finite set J and given two vectors $\boldsymbol{u} = (u_i)_{i \in J}$ and $\boldsymbol{v} = (v_i)_{i \in J}$ in

$\mathbb{Z}_+^J$, we write $\boldsymbol{u} \leq \boldsymbol{v}$ if $u_i \leq v_i$ for every $i \in J$. The *modulus* $|\boldsymbol{u}|$ of a vector $\boldsymbol{u} \in \mathbb{Z}_+^J$ is defined by $|\boldsymbol{u}| = \sum_{i \in J} u_i$. For every subset $X \subseteq J$, we notate $\boldsymbol{u}(X) = (u_i)_{i \in X} \in \mathbb{Z}_+^X$. For every positive integer m, we notate $J_m = \{1, \ldots, m\}$ and $J'_m = \{0, 1, \ldots, m\}$. Of course the vector notation that has been introduced here applies as well to $\mathbb{Z}_+^m = \mathbb{Z}_+^{J_m}$.

2.1 Access structures and secret sharing schemes

Let $P = \{p_1, \ldots, p_n\}$ denote the set of participants and its power set be denoted by $\mathcal{P}(P) = \{\mathcal{V} : \mathcal{V} \subseteq P\}$ which contains all the subsets of P. A collection $\Gamma \subseteq \mathcal{P}(P)$ is monotone if $\mathcal{V} \in \Gamma$ and $\mathcal{V} \subseteq \mathcal{W}$ imply that $\mathcal{W} \in \Gamma$. An *access structure* is a monotone collection $\Gamma \subseteq \mathcal{P}(P)$ of nonempty subsets of P. Sets in Γ are called *authorized*, and sets not in Γ are called *unauthorized*. An authorized set $\mathcal{V} \in \Gamma$ is called a *minimal authorized set* if for every $\mathcal{W} \subsetneq \mathcal{V}$, the set $\mathcal{W}$ is unauthorized. An unauthorized set $\mathcal{V} \notin \Gamma$ is called a *maximal unauthorized set* if for every $\mathcal{W} \supsetneq \mathcal{V}$, the set $\mathcal{W}$ is authorized. The set $\Gamma^* = \{\mathcal{V} : \mathcal{V}^c \notin \Gamma\}$ is called the *dual* access structure to Γ. It is easy to see that Γ^* is monotone too. In particular, an access structure is said to be *connected* if all participants are in at least one minimal authorized subset.

A family $\Pi = (\Pi_i)_{i \in J_m}$ of subsets of P is called here a *partition* of P if $P = \bigcup_{i \in J_m} \Pi_i$ and $\Pi_i \cap \Pi_j = \emptyset$ whenever $i \neq j$. For a partition Π of a set P, we consider the mapping $\Pi : \mathcal{P}(P) \to \mathbb{Z}_+^m$ defined by $\Pi(\mathcal{V}) = (|\mathcal{V} \cap \Pi_i|)_{i \in J_m}$. We write $\mathbf{P} = \Pi(\mathcal{P}(P)) = \{\boldsymbol{u} \in \mathbb{Z}_+^m : \boldsymbol{u} \leq \Pi(P)\}$. For a partition Π of a set P, a Π-*permutation* is a permutation σ on P such that $\sigma(\Pi_i) = \Pi_i$ for every part Π_i of Π. An access structure on P is said to be Π-*partite* if every Π-permutation is an automorphism of it.

As in [15–17] we describe a multipartite access structure in a compact way by taking into account that its members are determined by the number of elements they have in each part. If an access structure Γ on P is Π-partite, then $\mathcal{V} \in \Gamma$ if and only if $\Pi(\mathcal{V}) \in \Pi(\Gamma)$. That is, Γ is completely determined by the partition Π and the set of vectors $\Pi(\Gamma) \subseteq \mathbf{P} \subseteq \mathbb{Z}_+^m$. Moreover, the set $\Pi(\Gamma) \subseteq \mathbf{P}$ is monotone increasing, that is, if $\boldsymbol{u} \in \Pi(\Gamma)$ and $\boldsymbol{v} \in \mathbf{P}$ is such that $\boldsymbol{u} \leq \boldsymbol{v}$, then $\boldsymbol{v} \in \Pi(\Gamma)$. Therefore, $\Pi(\Gamma)$ is univocally determined by $\min \Pi(\Gamma)$, the family of its minimal vectors, that is, those representing the minimal qualified subsets of Γ. By an abuse of notation, we will use Γ to denote both a Π-partite access structure on P and the corresponding set $\Pi(\Gamma)$ of points in $\mathbf{P}$, and the same applies to $\min \Gamma$.

We next introduce some families of compartmented access structures, which are all multipartite access structures. The original compartmented access structures that were presented in [8] are defined as

$$\min \Gamma = \{\boldsymbol{u} \in \mathbf{P} : |\boldsymbol{u}| = k \text{ and } \boldsymbol{u} \geq \boldsymbol{t}\} \tag{1}$$

where $\boldsymbol{t} \in \mathbb{Z}_+^m$ and $k \in \mathbb{N}$ such that $k \geq |\boldsymbol{t}|$. This access structures are called *compartmented access structures with lower bounds* (*LCASs*).

Another family of compartmented access structures called *compartmented access structure with upper bounds* (*UCASs*) was presented in [36] and is defined as

$$\min \Gamma = \{\boldsymbol{u} \in \mathbf{P} : |\boldsymbol{u}| = k \text{ and } \boldsymbol{u} \leq \boldsymbol{r}\} \tag{2}$$

where $\boldsymbol{r} \in \mathbb{Z}_+^m$ and $k \in \mathbb{N}$ such that $\boldsymbol{r} \leq \Pi(P)$ and $r_i \leq k \leq |\boldsymbol{r}|$ for every $i \in J_m$.

The family of compartmented access structures in the following was presented in [17], which generalizes the previous ones. Let $\boldsymbol{t}, \boldsymbol{r} \in \mathbb{Z}_+^m$ and $k \in \mathbb{N}$ such that $\boldsymbol{t} \leq \boldsymbol{r} \leq \Pi(P)$,

$|\boldsymbol{t}| \leq k \leq |\boldsymbol{r}|$ and $r_i \leq k$ for every $i \in J_m$. The following access structures are called the *compartmented access structures with upper and lower bounds* (*ULCASs*)

$$\min \Gamma = \{\boldsymbol{u} \in \mathbf{P} : |\boldsymbol{u}| = k \text{ and } \boldsymbol{t} \leq \boldsymbol{u} \leq \boldsymbol{r}\}. \tag{3}$$

The UCASs and the LCASs correspond to ULCASs defined above with $\boldsymbol{t} = 0$ and with $\boldsymbol{r} = \Pi(P)$, respectively.

Now, we present the definition of *unconditionally secure perfect secret sharing scheme* as given in [3,11]. For more information about this definition and secret sharing schemes in general, see [2].

Definition 1 (*Secret sharing schemes*) Let $P = \{p_1, \ldots, p_n\}$ be a set of participants. A *distribution scheme* $\Sigma = (\Phi, \mu)$ with domain of secrets $\mathcal{S}$ is a pair, where μ is a probability distribution on some finite set $\mathcal{R}$ called the set of random strings and Φ is a mapping from $\mathcal{S} \times \mathcal{R}$ to a set of n-tuples $\mathcal{S}_1 \times \mathcal{S}_2 \times \cdots \times \mathcal{S}_n$, where $\mathcal{S}_i$ is called the domain of shares of p_i. A dealer distributes a secret $s \in \mathcal{S}$ according to Σ by first sampling a random string $r \in \mathcal{R}$ according μ, computing a vector of shares $\Phi(s, r) = (s_1, \ldots, s_n)$, and privately communicating each share s_i to participant p_i. For a set $\mathcal{V} \subseteq P$, we denote $\Phi_{\mathcal{V}}(s, r)$ as the restriction of $\Phi(s, r)$ to its $\mathcal{V}$-entries (i.e., the shares of the participants in $\mathcal{V}$).

Let $\mathcal{S}$ be a finite set of secrets, where $\mathcal{S} \geq 2$. A distribution scheme $\Sigma = (\Phi, \mu)$ with domain of secrets $\mathcal{S}$ is a *secret sharing scheme* realizing an access structure $\Gamma \subseteq \mathcal{P}(P)$ if the following two requirements hold:
CORRECTNESS The secret s can be reconstructed by any authorized set of participants. That is, for any authorized set $\mathcal{V} \in \Gamma$ (where $\mathcal{V} = \{p_{i_1}, \ldots, p_{i_{|\mathcal{V}|}}\}$), there exists a reconstruction function $Recon_{\mathcal{V}} : \mathcal{S}_{i_1} \times \cdots \times \mathcal{S}_{i_{|\mathcal{V}|}} \to \mathcal{S}$ such that for every $s \in \mathcal{S}$ and every random string $r \in \mathcal{R}$,

$$Recon_{\mathcal{V}}\big(\Phi_{\mathcal{V}}(s, r)\big) = s.$$

PRIVACY Every unauthorized set can learn nothing about the secret (in the information theoretic sense) from their shares. Formally, for any unauthorized set $\mathcal{W} \notin \Gamma$, every two secrets $s, s' \in \mathcal{S}$, and every possible $|\mathcal{W}|$-tuple of shares $(s_i)_{u_i \in \mathcal{W}}$,

$$Pr\big[\Phi_{\mathcal{W}}(s, r) = (s_i)_{u_i \in \mathcal{W}}\big] = Pr\big[\Phi_{\mathcal{W}}(s', r) = (s_i)_{u_i \in \mathcal{W}}\big]$$

when the probability is over the choice of r from $\mathcal{R}$ at random according to μ.

Definition 2 (*Ideal linear secret sharing schemes)* Let $P = \{p_1, \ldots, p_n\}$ be a set of participants. Let $\Sigma = (\Phi, \mu)$ be a secret sharing scheme with domain of secrets $\mathcal{S}$, where μ is a probability distribution on a set $\mathcal{R}$ and Φ is a mapping from $\mathcal{S} \times \mathcal{R}$ to $\mathcal{S}_1 \times \mathcal{S}_2 \times \cdots \times \mathcal{S}_n$, where $\mathcal{S}_i$ is called the domain of shares of p_i. We say that Σ is an ideal linear secret sharing scheme over a finite field $\mathbb{K}$ if $\mathcal{S} = \mathcal{S}_1 = \cdots = \mathcal{S}_n = \mathbb{K}$, $\mathcal{R}$ is a $\mathbb{K}$-vector space, Φ is a $\mathbb{K}$-linear mapping, and μ is the uniform probability distribution.

This paper deals exclusively with unconditionally secure perfect ideal linear secret sharing schemes.

2.2 Polymatroids and matroids

In this section we briefly review the definitions and some properties with regard to polymatroids and matroids. Most results of this section are from [15–17]. For more background on matroids and polymatroids the reader is referred to [23,30,32,37].

Definition 3 A *polymatroid* $\mathcal{S}$ is defined by a pair (J, h), where J is the finite *ground set* and $h : \mathcal{P}(J) \to \mathbb{R}$ is the *rank function* that satisfies

(1) $h(\emptyset) = 0$;
(2) h is *monotone increasing*: if $X \subseteq Y \subseteq J$, then $h(X) \leq h(Y)$;
(3) h is *submodular*: if $X, Y \subseteq J$, then $h(X \cup Y) + h(X \cap Y) \leq h(X) + h(Y)$.

An *integer polymatroid* $\mathcal{Z}$ is a polymatroid with an integer-valued rank function h. An integer polymatroid such that $h(X) \leq |X|$ for any $X \subseteq J$ is called a *matroid*.

While matroids abstract some properties related to linear dependency of collections of vectors in a vector space, integer polymatroids do the same with collections of subspaces. Suppose $(V_i)_{i\in J}$ is a finite collection of subspaces of a $\mathbb{K}$-vector space V, where $\mathbb{K}$ is a finite field. The mapping $h(X) : \mathcal{P}(J) \to \mathbb{Z}$ defined by $h(X) = \dim(\sum_{i\in X} V_i)$ is the rank function of an integer polymatroid with ground set J. Integer polymatroids and, in particular, matroids that can be defined in this way are said to be $\mathbb{K}$-*representable*.

Following the analogy with vector spaces we make the following definitions. For an integer polymatroid $\mathcal{Z}$, the set of *integer independent vectors* of $\mathcal{Z}$ is

$$\mathcal{D} = \{\boldsymbol{u} \in \mathbb{Z}_+^J : |\boldsymbol{u}(X)| \leq h(X) \text{ for every } X \subseteq J\},$$

in which the maximal integer independent vectors are called the *integer bases* of $\mathcal{Z}$. Let $\mathcal{B}$ or $\mathcal{B}(\mathcal{Z})$ denote the collection of all integer bases of $\mathcal{Z}$. Then all the elements of $\mathcal{B}(\mathcal{Z})$ have the identical modulus. In fact, every integer polymatroid $\mathcal{Z}$ is univocally determined by $\mathcal{B}(\mathcal{Z})$ since h is determined by $h(X) = \max\{|\boldsymbol{u}(X)| : \boldsymbol{u} \in \mathcal{B}(\mathcal{Z})\}$.

Given an integer polymatroid $\mathcal{Z} = (J, h)$ and a subset $X \subseteq J$, let $\mathcal{Z}|X = (X, h)$ denote a new integer polymatroid restricted $\mathcal{Z}$ ons X, and $\mathcal{B}(\mathcal{Z}, X) = \{\boldsymbol{u} \in \mathcal{D} : \text{supp}(\boldsymbol{u}) \subseteq X \text{ and } |\boldsymbol{u}| = h(X)\}$ where $\text{supp}(\boldsymbol{u}) = \{i \in J : u_i \neq 0\}$. Then there is a natural bijection between $\mathcal{B}(\mathcal{Z}, X)$ and $\mathcal{B}(\mathcal{Z}|X)$.

We next introduce the sum operations on integer polymatroids. Consider two integer polymatroids $\mathcal{Z}_1$ and $\mathcal{Z}_2$ on the same ground set J while with different rank functions h_1, h_2. Their sum is a new integer polymatroid $\mathcal{Z} = (J, h) = \mathcal{Z}_1 + \mathcal{Z}_2$ such that $h = h_1 + h_2$. In particular, if $\mathcal{Z}_1$ and $\mathcal{Z}_2$ are $\mathbb{K}$-representable, then $\mathcal{Z} = \mathcal{Z}_1 + \mathcal{Z}_2$ is $\mathbb{K}$-representable too. Precisely, if $\mathcal{Z}_1$ and $\mathcal{Z}_2$ are represented by vector subspaces $(V_i)_{i\in J}$ of V and $(W_i)_{i\in J}$ of W, respectively, then $\mathcal{Z} = \mathcal{Z}_1 + \mathcal{Z}_2$ is represented by the vector subspaces $(V_i \times W_i)_{i\in J}$ of $V \times W$. In particular, the integer bases of $\mathcal{Z}$ satisfies the following property.

Proposition 1 ([32]) $\mathcal{B}(\mathcal{Z}) = \mathcal{B}(\mathcal{Z}_1) + \mathcal{B}(\mathcal{Z}_2) = \{\boldsymbol{a} + \boldsymbol{b} : \boldsymbol{a} \in \mathcal{B}(\mathcal{Z}_1), \boldsymbol{b} \in \mathcal{B}(\mathcal{Z}_2)\}$.

2.3 Secret sharing schemes, matroids and polymatroids

In this section we introduce the methods to construct ideal linear secret sharing schemes for multipartite access structures based on matroids and polymatroids. Most results of this section are from [15–17]. We first introduce how to construct ideal linear schemes by matroids.

Let $P = \{p_1, \ldots, p_n\}$ be a set of participants and $p_0 \notin P$ be the dealer. Suppose $\mathcal{M}$ is a matroid on the finite set $P' = P \cup \{p_0\}$, and let

$$\Gamma_{p_0}(\mathcal{M}) = \{A \subseteq P : h(A \cup \{p_0\}) = h(A)\}.$$

Then $\Gamma_{p_0}(\mathcal{M})$ is an access structure on P because monotonicity property is satisfied, which is called *the port of the matroid* $\mathcal{M}$ *at the point* p_0.

Matroid ports play a very important role in secret sharing. Brickell [8] proved that the ports of representable matroids admit ideal secret sharing schemes and provided a method to construct ideal linear schemes for the ports ofd $\mathbb{K}$-representable matroids. These schemes are called a $\mathbb{K}$-*vector space secret sharing schemes*. This method was described by Massey [27,28] in terms of linear codes. Suppose M is an $k \times (n+1)$ matrix over $\mathbb{K}$. Then the columns of M determine a $\mathbb{K}$-representable matroid $\mathcal{M}$ with ground set P' such that the columns of M are in one-to-one correspondence with the elements in P'. In this situation, the matrix M is called a $\mathbb{K}$-*representation* of the matroid $\mathcal{M}$. Moreover, M is a generator matrix of some $(n+1, k)$ linear code C over $\mathbb{K}$, that is, a matrix whose rows span C. A code C of length $n+1$ and dimension k is called an $(n+1, k)$ linear code over $\mathbb{K}$ which is a k-dimensional subspace of $\mathbb{K}^{n+1}$. A secret sharing scheme can be constructed by the matrix M based the code C as follows.

Let $s \in \mathbb{K}$ be a secret value. Secret a codeword $\boldsymbol{c} = (c_0, c_1, \ldots, c_n) \in C$ uniformly at random such that $c_0 = s$, and define the share-vector as $(c_1, \ldots, c_n)$, that is c_i is the share of the participant p_i for $i \in [n]$. Let $LSSS(M)$ denote this secret sharing scheme.

Theorem 1 ([27]) *$LSSS(M)$ is a perfect ideal linear scheme such that a set $\mathcal{V} \subset P$ is qualified if and only if the first column in M is a linear combination of the columns with indices in $\mathcal{V}$.*

Remark 1 The *dual code* $C^{\perp}$ for a code C consists of all vectors $\boldsymbol{c}^{\perp} \in \mathbb{K}^{n+1}$ such that $\langle \boldsymbol{c}^{\perp}, \boldsymbol{c} \rangle = 0$ for all $\boldsymbol{c} \in C$, where $\langle \cdot, \cdot \rangle$ denotes the standard inner product. Suppose M and M^* are generator matrices of some $(n+1, k)$ linear code C and its dual $C^{\perp}$ over $\mathbb{K}$, respectively. Then $LSSS(M)$ and $LSSS(M^*)$ realize Γ and Γ^*, respectively.

Sometimes it is not easy to construct an ideal linear scheme for a given access structure Γ directly. In this case we can first construct a scheme for Γ^* and then translate the scheme into an ideal linear scheme for Γ^* using the explicit transformation of [18] based on the duality. In Sect. 4, we will present the construction for LCASs (1) by this method.

Brickell's method can be applied to construct ideal linear secret sharing schemes. Nevertheless, it is difficult to determine whether a given access structure admits an ideal linear secret sharing scheme or not. Moreover, even for access structures that admit such schemes, it may not be easy to construct them. Some strategies based on matroids and polymatroids were presented in [16,17] to attack those problems for multipartite access structures.

The relationship between ideal multipartite access structures and integer polymatroids is summarized as follows.

Theorem 2 ([16]) *Let $\Pi = (\Pi_i)_{i \in J_m}$ be a partition of the set P, and $\mathcal{Z}' = (J'_m, h)$ is an integer polymatroid such that $h(\{0\}) = 1$ and $h(\{i\}) \leq |\Pi_i|$ for every $i \in J_m$. Take $\Gamma_0(\mathcal{Z}') = \{X \subseteq J_m : h(X \cup \{0\}) = h(X)\}$ and*

$$\Gamma_0(\mathcal{Z}', \Pi) = \{\boldsymbol{u} \in \mathbf{P} : \text{there exist } X \in \Gamma_0(\mathcal{Z}') \text{ and } \boldsymbol{v} \in \mathcal{B}(\mathcal{Z}'|J_m, X) \text{ such that } \boldsymbol{v} \leq \boldsymbol{u}\}.$$

Then $\Gamma = \Gamma_0(\mathcal{Z}', \Pi)$ is a Π-partite access structure on P and a matroid port. Moreover, if $\mathcal{Z}'$ is $\mathbb{K}$-representable, then Γ can be realized by some $\mathbb{L}$-vector space secret sharing scheme over every large enough finite extension $\mathbb{L}$ of $\mathbb{K}$. In addition, $\mathcal{Z}'$ is univocally determined by Γ if it is connected.

We summarize next the general method by Farràs et al. [16] to construct ideal schemes for the multipartite access structures satisfying the conditions in Theorem 2.

Let $\Pi_0 = \{p_0\}$ and $\Pi' = (\Pi_i)_{i\in J'_m}$ be a partition of the set $P' = P \cup \{p_0\}$ such that $|\Pi_i| = n_i$. Given a connected Π-partite access structure Γ satisfying the conditions in Theorem 2.

Step 1. Find an integer polymatroid $\mathcal{Z}'$ such that $\Gamma = \Gamma_0(\mathcal{Z}', \Pi)$;
Step 2. Find a representation $(V_i)_{i\in J'_m}$ of $\mathcal{Z}'$ over some finite field $\mathbb{K}$;
Step 3. Over some finite extension of $\mathbb{K}$, find a representation of the matroid $\mathcal{M}$ such that Γ is a port of $\mathcal{M}$. More precisely, construct a $k\times(n+1)$ matrix $M = (M_0|M_1|\cdots|M_m)$ with the following properties:

1. $k = h(J'_m)$ and $n = \sum_{i=1}^{m} n_i$;
2. M_i is a $k \times n_i$ matrix whose columns are vectors in V_i;
3. $M_{\boldsymbol{u}}$ is nonsingular for any $\boldsymbol{u} \in \mathcal{B}(\mathcal{Z}')$, where $M_{\boldsymbol{u}}$ is the $k \times k$ submatrix of M formed by any u_i columns in every M_i.

Farràs et al. [16,17] proved that all the compartmented access structures introduced in Sect. 2.1 are connected matroid ports. Moreover, they presented the associated integer polymatroids and proved that they are representable. Therefore, the results in [16,17] solve Step 1. In this paper, we will give an efficient method to explicitly solve Steps 2 and 3, and hence to construct ideal linear schemes for those families of access structures. Our method is based on the properties of Gabidulin codes.

2.4 Gabidulin codes

In this section, we present the definition and main properties of Gabidulin codes, which will be used in our constructions. We first introduce linearized polynomials.

Definition 4 A linearized polynomial $L(y)$ over $\mathbb{F}_{q^\lambda}$ of q-degree t has the form

$$L(y) = \sum_{i=0}^{t} a_i y^{q^i},$$

where $a_i \in \mathbb{F}_{q^\lambda}$ and $a_t \neq 0$.

Property 1 For any $\gamma_1, \gamma_2 \in \mathbb{F}_{q^\lambda}$, and $a,\ b \in \mathbb{F}_q$,

$$L(a\gamma_1 + b\gamma_2) = aL(\gamma_1) + bL(\gamma_2).$$

The following useful lemma is from [26].

Lemma 1 *Let $\gamma_1, \gamma_2, \ldots, \gamma_t \in \mathbb{F}_{q^\lambda}$, and the matrix*

$$R = \left(\gamma_j^{q^{i-1}}\right)_{t\times t} \quad i,\ j \in [t],$$

namely,

$$R = \begin{pmatrix} \gamma_1 & \gamma_2 & \cdots & \gamma_t \\ \gamma_1^q & \gamma_2^q & \cdots & \gamma_t^q \\ \vdots & \vdots & \cdots & \vdots \\ \gamma_1^{q^{t-1}} & \gamma_2^{q^{t-1}} & \cdots & \gamma_t^{q^{t-1}} \end{pmatrix}.$$

Then R is nonsingular if and only if $\gamma_1, \gamma_2, \ldots, \gamma_t$ are linearly independent over $\mathbb{F}_q$.

Linearized polynomials can be used to construct codes. A family of codes, called Gabidulin codes, was presented by Gabidulin [19] by linearized polynomials as follows.

Definition 5 (*Gabidulin codes*) Let $\gamma_1, \gamma_2, \ldots, \gamma_n \in \mathbb{F}_{q^\lambda}$ be linearly independent over $\mathbb{F}_q$. Then the (n, k) Gabidulin code over $\mathbb{F}_{q^\lambda}$ $(\lambda \geq n)$ consists of all vectors

$$\boldsymbol{c} = (L_{\boldsymbol{a}}(\gamma_1), L_{\boldsymbol{a}}(\gamma_2), \ldots, L_{\boldsymbol{a}}(\gamma_n)),$$

where $\boldsymbol{a} = (a_0, a_1, \ldots, a_{k-1}) \in \mathbb{F}_{q^\lambda}^k$ and $L_{\boldsymbol{a}}(y) = \sum_{i=0}^{k-1} a_i y^{q^i}$.

The generator matrix of Gabidulin codes can be denoted by

$$G = \left(\gamma_j^{q^{i-1}}\right)_{k\times n} \qquad i \in [k], \quad j \in [n].$$

Lemma 1 implies that any $k \times k$ submatrix of G is nonsingular.

3 Secret sharing schemes for compartmented access structures with upper bounds

In this section, we construct ideal linear secret sharing schemes realizing UCASs combining the polymatroid-based method in Sect. 2.3 and Gabidulin codes. We first introduce an integer polymatroid $\mathcal{Z}'$ satisfying Theorem 2 such that the UCASs (2) are of the form $\Gamma_0(\mathcal{Z}', \Pi)$.

Let $\Pi = (\Pi_i)_{i\in J_m}$ be a partition of the set P, $\boldsymbol{r} \in \mathbb{Z}_+^{J'_m}$ and $k \in \mathbb{N}$ such that $r_0 = 1$, $\boldsymbol{r}(J_m) \leq \Pi(P)$ and $r_i \leq k \leq |\boldsymbol{r}(J_m)|$ for every $i \in J_m$. The following result was presented in Sect. 8.2 of [16].

Lemma 2 *Suppose $\mathcal{Z}' = (J'_m, h)$ is an integer polymatroid with*

$$h(X) = \min\left\{k, |\boldsymbol{r}(X)|\right\} \quad \text{for every} \quad X \subseteq J'_m.$$

Then the UCASs (2) are of the form $\Gamma_0(\mathcal{Z}', \Pi)$.

From this lemma, we have the following result.

Proposition 2 *For the integer polymatroid $\mathcal{Z}'$ defined in Lemma 2,*

$$\mathcal{B}(\mathcal{Z}') = \{\boldsymbol{u} \in \mathbb{Z}_+^{J'_m} : |\boldsymbol{u}| = k \text{ and } \boldsymbol{u} \leq \boldsymbol{r}\}. \tag{4}$$

Proof Since

$$\mathcal{B}(\mathcal{Z}') = \{\boldsymbol{u} \in \mathbb{Z}_+^{J'_m} : |\boldsymbol{u}| = k \text{ and } |\boldsymbol{u}(X)| \leq h(X) \text{ for every } X \subseteq J'_m\},$$

it follows that if $\boldsymbol{u} \in \mathcal{B}(\mathcal{Z}')$, $u_i \leq h(\{i\}) = r_i$ for every $i \in J'_m$. This implies $\boldsymbol{u} \leq \boldsymbol{r}$. On the other hand, if $|\boldsymbol{u}| = k$ and $\boldsymbol{u} \leq \boldsymbol{r}$, then for any $X \subseteq J'_m$, $|\boldsymbol{u}(X)| \leq \min\left\{k, |\boldsymbol{r}(X)|\right\} = h(X)$. This implies the conclusion. □

We next introduce a linear representation of the polymatroid defined in Lemma 2, that is a collection $(V_i)_{i\in J'_m}$ of subspaces of some vector space. Consider the map $\psi : \mathbb{F}_{q^\lambda} \to \mathbb{F}_{q^\lambda}^k$ defined by

$$\psi(\beta) = (\beta, \beta^q, \ldots, \beta^{q^{k-1}}) \tag{5}$$

where $q \geq \max_{i\in J_m}\{|\Pi_i|\}$ is a prime power and $\lambda \geq |\boldsymbol{r}|$. Take elements $\beta_{i,j}$ in $\mathbb{F}_{q^\lambda}$, where $i \in J'_m$ and $j \in [r_i]$, that are linearly independent over $\mathbb{F}_q$. For every $i \in J'_m$, consider the $\mathbb{F}_q$-vector subspace $V_i \subseteq \mathbb{F}_{q^\lambda}^k$ spanned by $\{\psi(\beta_{i,j}) : j \in [r_i]\}$. Let the integer polymatroid $\mathcal{Z}' = (J'_m, h)$ such that

$$h(X) = \dim\left(\sum_{i\in X} V_i\right) \quad \text{for every} \quad X \subseteq J'_m.$$

We have the following result.

Proposition 3 *For the integer polymatroid $\mathcal{Z}'$ defined above, the UCASs (2) are of the form $\Gamma_0(\mathcal{Z}', \Pi)$ and $\mathcal{B}(\mathcal{Z}')$ is the set (4).*

Proof Proving the claim is equivalent to proving that h satisfies the condition in Lemma 2. Let B be the matrix formed by all the column vectors $(\psi(\beta_{i,j}))^T$ with $i \in J'_m$ and $j \in [r_i]$. Then B is a generator matrix of some $(|\boldsymbol{r}|, k)$ Gabidulin code, and consequently, any $k \times k$ submatrix of B is nonsingular. From this with

$$\left|\bigcup_{i\in X}\{\psi(\beta_{i,j}) : j \in [r_i]\}\right| = \left|\boldsymbol{r}(X)\right|$$

for every $X \subseteq J'_m$, we have $h(X) = \min\left\{k, |\boldsymbol{r}(X)|\right\}$ for every $X \subseteq J'_m$, and the claim follows. □

This proposition implies that the collection $(V_i)_{i\in J'_m}$ is a linear representation of the integer polymatroid $\mathcal{Z}'$ associated to the UCASs (2). We proceed to construct a matrix M based on the representable polymatroid $\mathcal{Z}'$. This matrix is a representation of a matroid $\mathcal{M}$ such that the UCASs (2) are of the form $\Gamma_{p_0}(\mathcal{M})$.

Take $\Pi_0 = \{p_0\}$ and let $\Pi' = (\Pi_i)_{i\in J'_m}$ and $\Pi = (\Pi_i)_{i\in J_m}$ be the partition of $P' = P \cup \{p_0\}$ and P, respectively, such that $|\Pi_i| = n_i$. For every $i \in J'_m$, consider the map: $\varphi_i : \mathbb{F}_q \to V_i$ defined by

$$\begin{aligned}\varphi_i(a) &= \psi(\beta_{i,1}) + a\psi(\beta_{i,2}) + a^2\psi(\beta_{i,3}) + \cdots + a^{r_i-1}\psi(\beta_{i,r_i}) \\ &= \psi(\beta_{i,1} + a\beta_{i,2} + a^2\beta_{i,3} + \cdots + a^{r_i-1}\beta_{i,r_i})\end{aligned} \tag{6}$$

and take n_i different elements $a_{i,v} \in \mathbb{F}_q$ with $v \in [n_i]$. Let

$$M = (M_0|M_1|\cdots|M_m) \tag{7}$$

be the $k\times(n+1)$ matrix such that M_i is the block formed by all the column vectors $(\varphi_i(a_{i,v}))^T$ with $v \in [n_i]$.

Obviously, M satisfies the first two conditions in Step 3 presented in Sect. 2.3. We next prove that it satisfies the third condition too.

Proposition 4 *$M_{\boldsymbol{u}}$ is nonsingular for any $\boldsymbol{u} \in \mathcal{B}(\mathcal{Z}')$, (4).*

Proof Without loss of generality, we may assume that $M_{\boldsymbol{u}}$ is the $k \times k$ submatrix of M formed by the first u_i columns in every M_i. In addition, for $i \in J'_m$ and $v \in [n_i]$, take

$$\bar{\beta}_{i,v} = \sum_{j=1}^{r_i} a_{i,v}^{j-1}\beta_{i,j}, \tag{8}$$

then $\varphi_i(a_{i,v}) = \psi(\bar{\beta}_{i,v})$.

Suppose that there exist $\lambda_{i,v}$ with $i \in J'_m$ and $v \in [u_i]$ such that

$$\sum_{i=0}^{m}\sum_{v=1}^{u_i}\lambda_{i,v}\bar{\beta}_{i,v} = 0.$$

Then from (8),

$$\sum_{i=0}^{m}\sum_{v=1}^{u_i}\lambda_{i,v}\left(\sum_{j=1}^{r_i}a_{i,v}^{j-1}\beta_{i,j}\right) = \sum_{i=0}^{m}\sum_{j=1}^{r_i}\left(\sum_{v=1}^{u_i}\lambda_{i,v}a_{i,v}^{j-1}\right)\beta_{i,j} = 0.$$

As $\beta_{i,j}$ with $i \in J'_m$ and $j \in [r_i]$ are linearly independent over $\mathbb{F}_q$, thus

$$\sum_{v=1}^{u_i}\lambda_{i,v}a_{i,v}^{j-1} = 0 \qquad i \in J'_m, \quad j \in [r_i].$$

Therefore, $\sum_{v=1}^{u_i}\lambda_{i,v}(1, a_{i,v}, \ldots, a_{i,v}^{r_i-1}) = 0$ for any $i \in J'_m$. Since the u_i vectors $(a_{i,v}, \ldots, a_{i,v}^{r_i-1})$ are linearly independent, it follows that $\lambda_{i,v} = 0$ for any $v \in [u_i]$. Hence, $\lambda_{i,v} = 0$ for any $i \in J'_m$ and $v \in [u_i]$, and consequently, $\bar{\beta}_{i,v}$ with $i \in J'_m$ and $v \in [u_i]$ are linearly independent over $\mathbb{F}_q$. As the column of $M_{\boldsymbol{u}}$ can be denoted by $(\psi(\bar{\beta}_{i,v}))^T$, thus Lemma 1 implies $M_{\boldsymbol{u}}$ is nonsingular. Using the same method, we can prove $M_{\boldsymbol{u}}$ is nonsingular for any $\boldsymbol{u} \in \mathcal{B}(\mathcal{Z}')$, (4). □

Proposition 4 implies the matrix (7) is a representation of the matroid associated to UCASs. We next prove ideal linear schemes realizing UCASs can be constructed by this matrix. We have the following result.

Theorem 3 *Suppose M is the matrix (7). Then $LSSS(M)$ realizes the UCASs (2) over $\mathbb{F}_{q^\lambda}$ where $q \geq \max_{i\in J_m}\{n_i\}$ and $\lambda \geq 1 + |\boldsymbol{r}(J_m)|$.*

Proof Theorem 1 implies that proving this claim is equivalent to proving that $\boldsymbol{u}(J_m) \in \Gamma$ if and only M_0 is a linear combination of all the columns in $M_{\boldsymbol{u}(J_m)}$.

In the case of $\boldsymbol{u}(J_m) \in \min\Gamma$, (2), if $u_0 = 0$, then $\boldsymbol{u}(J'_m) \in \mathcal{B}(\mathcal{Z}')$. Proposition 4 implies $M_{\boldsymbol{u}(J_m)}$ is nonsingular. Therefore, M_0 can be denoted by a linear combination of all the columns in $M_{\boldsymbol{u}(J_m)}$, and consequently, it is a linear combination of the columns in $M_{\boldsymbol{u}(J_m)}$ for any $\boldsymbol{u}(J_m) \in \Gamma$.

We next prove the claim in the case of $\boldsymbol{u}(J_m) \notin \Gamma$. As $h(\{i\}) = r_i$ for every $i \in J_m$, thus any $r_i + 1$ columns of M_i are linearly dependent. Therefore, without loss of generality, we may assume that $\boldsymbol{u}(J_m) \leq \boldsymbol{r}(J_m)$. Furthermore, we may assume that $|\boldsymbol{u}(J_m)| = k - 1$, since if $|\boldsymbol{u}(J_m)| < k - 1$, we may find a vector $\boldsymbol{u'}(J_m) \geq \boldsymbol{u}(J_m)$ such that $\boldsymbol{u'}(J_m) \leq \boldsymbol{r}(J_m)$ and $|\boldsymbol{u'}(J_m)| = k - 1$. In this case if $u_0 = 1$, then $\boldsymbol{u}(J'_m) \in \mathcal{B}(\mathcal{Z}')$. Proposition 4 implies $M_{\boldsymbol{u}(J'_m)}$ is nonsingular, and consequently, M_0 must not be a linear combination of all the columns in $M_{\boldsymbol{u}(J_m)}$. □

4 Secret sharing schemes for compartmented access structures with lower bounds

In this section, we describe ideal linear secret sharing schemes realizing LCASs based on the schemes for the dual access structures of LCASs.

The dual access structures of LCASs (1) are described in [36] as follows

$$\Gamma^* = \{\boldsymbol{u} \in \mathbf{P} : |\boldsymbol{u}| \geq l \text{ or } u_i \geq \tau_i \text{ for some } i \in J_m\} \tag{9}$$

where $l = |P| - k + 1$, $\tau_i = |\Pi_i| - t_i + 1$ for $i \in J$, and $|\boldsymbol{\tau}| \geq l + m - 1$.

We will present an ideal linear scheme for Γ^*. First, we introduce an integer polymatroid $\mathcal{Z}'$ satisfying Theorem 2 such that the access structures (9) are of the form $\Gamma_0(\mathcal{Z}', \Pi)$.

Let $\Pi = (\Pi_i)_{i \in J_m}$ be a partition of the set P. Take $\boldsymbol{\tau}, \boldsymbol{\tau'} \in \mathbb{Z}_+^{J'_m}$ and $l \in \mathbb{N}$ such that $\tau_0 = 1$, $\boldsymbol{\tau}(J_m) \leq \Pi(P)$, $|\boldsymbol{\tau}(J_m)| \geq l + m - 1$ and $\tau'_i = \tau_i - 1$ for every $i \in J'_m$. The following result was presented in Sect. IV-D of [17].

Lemma 3 *Suppose $\mathcal{Z}' = (J'_m, h)$ is an integer polymatroid with h satisfying*

(1) $h(\{0\}) = 1$;
(2) $h(X) = \min\{l, 1 + |\boldsymbol{\tau'}(X)|\}$ *for every* $X \subseteq J_m$;
(3) $h(X \cup \{0\}) = h(X)$ *for every* $X \subseteq J_m$.

Then the access structures (9) *are of the form* $\Gamma_0(\mathcal{Z}', \Pi)$.

From this lemma, we have the following result.

Proposition 5 *For the integer polymatroid $\mathcal{Z}'$ defined in Lemma 3, $\mathcal{B}(\mathcal{Z}') = \mathcal{B}_1 \cup \mathcal{B}_2$, where*

$$\begin{aligned} \mathcal{B}_1 = \{\boldsymbol{u} \in \mathbb{Z}_+^{J'_m} :\ & |\boldsymbol{u}| = l,\ u_0 = 0,\ u_{i'} \leq \tau_{i'} \quad \text{for some} \quad i' \in J_m \\ & \text{and } u_i \leq \tau_i - 1 \quad \text{for all} \quad i \in J_m \backslash \{i'\}\}, \\ \mathcal{B}_2 = \{\boldsymbol{u} \in \mathbb{Z}_+^{J'_m} :\ & |\boldsymbol{u}| = l,\ u_0 = 1 \text{ and } \boldsymbol{u}(J_m) \leq \boldsymbol{\tau'}(J_m)\}. \end{aligned} \tag{10}$$

Proof If $u_0 = 0$, then $\boldsymbol{u} \in \mathcal{B}(\mathcal{Z}')$ if and only if $\boldsymbol{u}(J_m) \in \mathcal{B}(\mathcal{Z}'|J_m)$. Since the access structures (9) are of the form $\Gamma_0(\mathcal{Z}', \Pi)$, it follows that

$$\begin{aligned} \mathcal{B}(\mathcal{Z}'|J_m) = \{\boldsymbol{u} \in \mathbb{Z}_+^m :\ & |\boldsymbol{u}| = l,\ u_{i'} \leq \tau_{i'} \text{ for some } i' \in J_m \\ & \text{and } u_i \leq \tau_i - 1 \text{ for all } i \in J_m \backslash \{i'\}\}. \end{aligned}$$

This implies $\boldsymbol{u} \in \mathcal{B}(\mathcal{Z}')$ with $u_0 = 0$ if and only if $\boldsymbol{u} \in \mathcal{B}_1$. In addition, since

$$\mathcal{B}(\mathcal{Z}') = \{\boldsymbol{u} \in \mathbb{Z}_+^{J'_m} : |\boldsymbol{u}| = l \text{ and } |\boldsymbol{u}(X)| \leq h(X) \text{ for every } X \subseteq J'_m\},$$

it follows that if $u_0 = 1$ and $\boldsymbol{u} \in \mathcal{B}(\mathcal{Z}')$, then for every $i \in J_m$,

$$|\boldsymbol{u}(\{0, i\})| = 1 + u_i \leq h(\{0, i\}) = h(\{i\}) = \tau_i.$$

This implies that $\boldsymbol{u}(J_m) \leq \boldsymbol{\tau'}(J_m)$, and consequently, $\boldsymbol{u} \in \mathcal{B}_2$.

On the other hand, if $\boldsymbol{u} \in \mathcal{B}_2$, then for every $X \subseteq J_m$,

$$\begin{aligned} |\boldsymbol{u}(X)| &\leq \min\{l - 1, |\tau'(X)|\} \leq h(X), \\ |\boldsymbol{u}(X \cup \{0\})| &\leq \min\{l, |\tau'(X)| + 1\} = h(X) = h(X \cup \{0\}). \end{aligned}$$

This implies that $\boldsymbol{u} \in \mathcal{B}(\mathcal{Z}')$. Therefore, $\boldsymbol{u} \in \mathcal{B}(\mathcal{Z}')$ with $u_0 = 1$ if and only if $\boldsymbol{u} \in \mathcal{B}_2$, and the result follows. □

Now, we introduce a linear representation of the polymatroid defined in Lemma 3 by Gabidulin codes. Similar to (5), we define the map $\psi : \mathbb{F}_{q^\lambda} \to \mathbb{F}_{q^\lambda}^l$ by

$$\psi(\beta) = (\beta, \beta^q, \ldots, \beta^{q^{l-1}})$$

where $q \geq 1 + \max_{i \in J_m}\{|\Pi_i|\}$ and $\lambda \geq 1 + |\boldsymbol{\tau'}|$. Take elements $\beta_{i,j}$ in $\mathbb{F}_{q^\lambda}$, where $i \in J'_m$ and $j \in [\tau_i]$, such that

- $\beta_{i,1} = \beta_0$ for all $i \in J'_m$ and
- the elements β_0 and $\beta_{i,j}$ with $i \in J_m$ and $j \in [2, \tau_i]$ are linearly independent over $\mathbb{F}_q$.

For every $i \in J'_m$, consider the $\mathbb{F}_q$-vector subspace $V_i \subseteq \mathbb{F}_{q^\lambda}^l$ spanned by the set $\{\psi(\beta_{i,j}) : j \in [\tau_i]\}$. Let the integer polymatroid $\mathcal{Z}' = (J'_m, h)$ such that $h(X) = \dim\left(\sum_{i\in X} V_i\right)$ for every $X \subseteq J'_m$.

Proposition 6 *For the integer polymatroid $\mathcal{Z}'$ defined above, the access structures (9) are of the form $\Gamma_0(\mathcal{Z}', \Pi)$ and $\mathcal{B}(\mathcal{Z}') = \mathcal{B}_1 \cup \mathcal{B}_2$, (10).*

Proof As $\dim(V_0) = 1$, thus $h(\{0\}) = 1$. We next prove h satisfies the other two conditions. Let B be the matrix formed by the column vectors $(\psi(\beta_0))^T$ and $(\psi(\beta_{i,j}))^T$ with $i \in J_m$ and $j \in [2, \tau_i]$. Then B is a generator matrix of some $(1 + |\boldsymbol{\tau}'|, l)$ Gabidulin code. Accordingly, any $l \times l$ submatrix of B is nonsingular. From this with

$$\left|\bigcup_{i\in X}\left\{\psi(\beta_{i,j}) : j \in [\tau_i]\right\}\right| = 1 + \left|\boldsymbol{\tau}'(X)\right|$$

for every $X \subseteq J_m$, we can obtain $h(X) = \min\left\{l, 1 + |\boldsymbol{\tau}'(X)|\right\}$ for every $X \subseteq J_m$. Moreover, $V_0 \subseteq V_i$ for every $X \subseteq J_m$, Therefore, $h(X \cup \{0\}) = h(X)$ for every $X \subseteq J_m$. □

We proceed to construct a matrix M which is a representation of a matroid $\mathcal{M}$ such that the access structures (9) are of the form $\Gamma_{p_0}(\mathcal{M})$.

Suppose $\Pi_0 = \{p_0\}$ and let $\Pi' = (\Pi_i)_{i\in J'_m}$ and $\Pi = (\Pi_i)_{i\in J_m}$ be the partition of $P' = P \cup \{p_0\}$ and P, respectively, such that $|\Pi_i| = n_i$. Similar to (6), for every $i \in J'_m$ let the map: $\varphi_i : \mathbb{F}_q \to V_i$ be defined by

$$\begin{aligned}\varphi_i(a) &= \psi(\beta_{i,1}) + a\psi(\beta_{i,2}) + a^2\psi(\beta_{i,3}) + \cdots + a^{\tau_i-1}\psi(\beta_{i,\tau_i}) \\ &= \psi(\beta_{i,1} + a\beta_{i,2} + a^2\beta_{i,3} + \cdots + a^{\tau_i-1}\beta_{i,\tau_i})\end{aligned}$$

Take $a_{0,1} = 0$ and for every $i \in J_m$, take n_i different elements $a_{i,v} \in \mathbb{F}_q$ with $v \in [n_i]$ such that $a_{i,v} \neq 0$. Let

$$M = (M_0|M_1|\cdots|M_m) \tag{11}$$

be the $l \times (n+1)$ matrix such that M_i is the block formed by all the column vectors $(\varphi_i(a_{i,v}))^T$ with $v \in [n_i]$.

Obviously, M satisfies the first two conditions in Step 3 in Sect. 2.3. We next prove that it satisfies the third condition. For $i \in J'_m$ and $v \in [n_i]$, take

$$\bar{\beta}_{i,v} = \sum_{j=1}^{\tau_i} a_{i,v}^{j-1}\beta_{i,j},$$

then $\varphi_i(a_{i,v}) = \psi(\bar{\beta}_{i,v})$, $\bar{\beta}_{0,1} = \beta_0$, and for $i \in J_m$ and $v \in [n_i]$,

$$\bar{\beta}_{i,v} = \beta_{i,1} + \sum_{j=2}^{\tau_i} a_{i,v}^{j-1}\beta_{i,j} = \beta_0 + \sum_{j=2}^{\tau_i} a_{i,v}^{j-1}\beta_{i,j} \tag{12}$$

as $\beta_{i,1} = \beta_0$ for $i \in J'_m$. We have the following results.

Proposition 7 *$M_{\boldsymbol{u}}$ is nonsingular for any $\boldsymbol{u} \in \mathcal{B}_1$, (10).*

Proof Without loss of generality, we may assume that $u_1 \le \tau_1$, $u_i \le \tau_i - 1$ for $i \in [2, m]$, and $M_{\boldsymbol{u}}$ is the $l \times l$ submatrix of M formed by the first u_i columns in every M_i with $i \in J_m$. Suppose that there exist $\lambda_{i,v}$, with $i \in J_m$ and $v \in [u_i]$ such that $\sum_{i=1}^{m}\sum_{v=1}^{u_i} \lambda_{i,v}\bar{\beta}_{i,v} = 0$. Then from (12),

$$\sum_{i=1}^{m}\sum_{v=1}^{u_i}\lambda_{i,v}\left(\beta_0 + \sum_{j=2}^{\tau_i} a_{i,v}^{j-1}\beta_{i,j}\right) = \sum_{i=1}^{m}\sum_{v=1}^{u_i}\lambda_{i,v}\beta_0 + \sum_{i=1}^{m}\sum_{j=2}^{\tau_i}\left(\sum_{v=1}^{u_i}\lambda_{i,v}a_{i,v}^{j-1}\right)\beta_{i,j} = 0.$$

As β_0 and $\beta_{i,j}$ with $i \in J_m$ and $j \in [2, \tau_i]$ are linearly independent over $\mathbb{F}_q$, thus

$$\sum_{i=1}^{m}\sum_{v=1}^{u_i}\lambda_{i,v} = 0 \quad \text{and} \quad \sum_{v=1}^{u_i}\lambda_{i,v}a_{i,v}^{j-1} = 0 \qquad i \in J_m,\ j \in [2, \tau_i]. \tag{13}$$

Therefore, $\sum_{v=1}^{u_i}\lambda_{i,v}(a_{i,v}, \ldots, a_{i,v}^{\tau_i - 1}) = 0$ for every $i \in J_m$.

As $a_{i,v} \neq 0$ and $u_i \le \tau_i - 1$ for $i \in [2, m]$, thus the u_i vectors $(a_{i,v}, \ldots, a_{i,v}^{\tau_i-1})$ are linearly independent. This implies $\lambda_{i,v} = 0$ for any $i \in [2, m]$ and $v \in [u_i]$. From this with (13), $\sum_{v=1}^{u_1}\lambda_{1,v} = 0$ and $\sum_{v=1}^{u_1}\lambda_{1,v}(a_{1,v}, \ldots, a_{1,v}^{\tau_1-1}) = 0$. Therefore,

$$\sum_{v=1}^{u_1}\lambda_{1,v}(1, a_{1,v}, \ldots, a_{1,v}^{\tau_1-1}) = 0.$$

As $u_1 \le \tau_1$, similarly, we can prove $\lambda_{1,v} = 0$ for any $v \in [u_1]$. Therefore, $\bar{\beta}_{i,v}$ with $i \in J_m$ and $v \in [u_i]$ are linearly independent over $\mathbb{F}_q$. Lemma 1 implies $M_{\boldsymbol{u}}$ is nonsingular since the column of $M_{\boldsymbol{u}}$ can be denoted by $(\psi(\bar{\beta}_{i,v}))^T$. Using the same method, we can prove $M_{\boldsymbol{u}}$ is nonsingular for any $\boldsymbol{u} \in \mathcal{B}_1$, (10). □

Proposition 8 *$M_{\boldsymbol{u}}$ is nonsingular for any $\boldsymbol{u} \in \mathcal{B}_2$,* (10).

Proof Without loss of generality, we may assume that $M_{\boldsymbol{u}}$ is the $l \times l$ submatrix of M formed by the first u_i columns in every M_i. Suppose that there exist $\lambda_{i,v}$, with $i \in J'_m$ and $v \in [u_i]$ such that $\sum_{i=0}^{m}\sum_{v=1}^{u_i}\lambda_{i,v}\bar{\beta}_{i,v} = 0$. Then from (12),

$$\begin{aligned}&\lambda_{0,1}\beta_0 + \sum_{i=1}^{m}\sum_{v=1}^{u_i}\lambda_{i,v}\left(\beta_0 + \sum_{j=2}^{\tau_i} a_{i,v}^{j-1}\beta_{i,j}\right)\\ &= \left(\lambda_{0,1} + \sum_{i=1}^{m}\sum_{v=1}^{u_i}\lambda_{i,v}\right)\beta_0 + \sum_{i=1}^{m}\sum_{j=2}^{\tau_i}\left(\sum_{v=1}^{u_i}\lambda_{i,v}a_{i,v}^{j-1}\right)\beta_{i,j} = 0.\end{aligned}$$

This implies that

$$\lambda_{0,1} + \sum_{i=1}^{m}\sum_{v=1}^{u_i}\lambda_{i,v} = 0 \quad \text{and} \quad \sum_{v=1}^{u_i}\lambda_{i,v}a_{i,v}^{j-1} = 0 \quad i \in J_m, \quad j \in [2, \tau_i] \tag{14}$$

since β_0 and $\beta_{i,j}$ with $i \in J_m$ and $j \in [2, \tau_i]$ are linearly independent over $\mathbb{F}_q$. Therefore, as in the proof of Proposition 7, we can obtain that $\lambda_{i,v} = 0$ for $i \in J_m$ and $j \in [u_i]$. From this with (14), we have $\lambda_{0,1} = 0$. Hence, $\bar{\beta}_{i,v}$ with $i \in J'_m$ and $j \in [u_i]$ are linearly independent over $\mathbb{F}_q$. This implies the conclusion. □

Propositions 7 and 8 imply that the matrix (11) is a representation of the matroid associated to the access structures (9). Now, we prove ideal linear schemes realizing access structures (9) can be obtained by the matrix.

Theorem 4 *Suppose M is the matrix (11). Then $LSSS(M)$ realizes the access structures (9) over $\mathbb{F}_{q^\lambda}$ where $q \geq 1 + \max_{i\in J_m}\{n_i\}$ and $\lambda \geq 1 + |\boldsymbol{\tau}'|$.*

Proof Let $\boldsymbol{u}(J_m) \in \Gamma^*$, (9), be a minimal set, then $|\boldsymbol{u}(J_m)| = l$ and $\boldsymbol{u}(J_m) \leq \boldsymbol{\tau}'(J_m)$, or $u_i = \tau_i$ for some $i \in J_m$. In the first case, Proposition 7 implies $M_{\boldsymbol{u}(J_m)}$ is nonsingular, and consequently, M_0 is a linear combination of all the columns in $M_{\boldsymbol{u}(J_m)}$. In addition, Proposition 7 implies any τ_i columns of M_i are linearly independent. From this with $h(\{0, i\}) = h(\{i\}) = \tau_i$ for every $i \in J_m$, M_0 is a linear combination of any τ_i columns in M_i. Hence, in the second case M_0 can be denoted by a linear combination of all the columns in $M_{\boldsymbol{u}(J_m)}$ too.

Assume that $\boldsymbol{u}(J_m) \notin \Gamma^*$, (9). Then $\boldsymbol{u}(J_m) \leq \boldsymbol{\tau}'(J_m)$ and $|\boldsymbol{u}(J_m)| \leq l - 1$. Without loss of generality, we may assume that $|\boldsymbol{u}(J_m)| = l - 1$, since if $|\boldsymbol{u}(J_m)| < l - 1$, we may find a vector $\boldsymbol{u}'(J_m) \geq \boldsymbol{u}(J_m)$ such that $\boldsymbol{u}'(J_m) \leq \boldsymbol{\tau}'(J_m)$ and $|\boldsymbol{u}'(J_m)| = l - 1$. As $l \leq |\boldsymbol{\tau}'| + 1$, i.e., $|\boldsymbol{\tau}'| \geq l - 1$, the above-described procedure is possible. In this case if $u_0 = 1$, $\boldsymbol{u}(J'_m) \in \mathcal{B}_2$. Proposition 8 implies $M_{\boldsymbol{u}(J'_m)}$ is nonsingular. Accordingly, M_0 must not be a linear combination of all the columns in $M_{\boldsymbol{u}(J_m)}$, and the result follows. □

From the dual relationship of the access structures (9) and the LCASs (1), we can translate the scheme in Theorem 4 into an ideal linear scheme for the LCASs (1) using the explicit transformation of [18].

Corollary 1 *The efficient construction of ideal linear scheme realizing LCASs (1) can be obtained over $\mathbb{F}_{q^\lambda}$ where $q \geq 1 + \max_{i\in J_m}\{n_i\}$ and $\lambda \geq 1 + \sum_{i=1}^{m}(n_i - t_i)$.*

5 Secret sharing schemes for compartmented access structures with upper and lower bounds

In this section, we study how to construct ideal linear secret sharing schemes realizing ULCASs by an efficient method.

5.1 A representable integer polymatroid

In this section, we construct a $\mathbb{K}$-representable integer polymatroid $\mathcal{Z}'$ satisfying Theorem 2 such that the ULCASs (3) are of the form $\Gamma_0(\mathcal{Z}', \Pi)$ by Gabidulin codes.

Take $\Pi = (\Pi_i)_{i\in J_m}$ be a partition of the set P. Let $\boldsymbol{t}, \boldsymbol{r} \in \mathbb{Z}_+^{J'_m}$ and $k \in \mathbb{N}$ such that $\boldsymbol{t}(J_m) \leq \boldsymbol{r}(J_m) \leq \Pi(P)$, $|\boldsymbol{t}(J_m)| \leq k \leq |\boldsymbol{r}(J_m)|$, $r_i \leq k$ for every $i \in J_m$, $t_0 = 0$ and $r_0 = 1$.Take $k_1 = |\boldsymbol{t}(J_m)|$ and $k_2 = k - k_1$.

Lemma 4 *Suppose $\mathcal{Z}' = (J'_m, h)$ is an integer polymatroid with h satisfying*

(1) $h(\{0\}) = 1$;
(2) $h(X) = \min\{|\boldsymbol{t}(X)| + k_2, |\boldsymbol{r}(X)|\}$ *for every* $X \subseteq J_m$;
(3) $h(X \cup \{0\}) = \min\{k, h(X) + 1\}$ *for every* $X \subseteq J_m$.

Then the ULCASs (3) are of the form $\Gamma_0(\mathcal{Z}', \Pi)$ and $\mathcal{B}(\mathcal{Z}') = \mathcal{B}_1 \cup \mathcal{B}_2 \cup \mathcal{B}_3$, where

$$\begin{aligned}
\mathcal{B}_1 &= \{\boldsymbol{u} \in \mathbb{Z}_+^{J'_m} : |\boldsymbol{u}| = k,\ u_0 = 0 \text{ and } \boldsymbol{t}(J_m) \leq \boldsymbol{u}(J_m) \leq \boldsymbol{r}(J_m)\},\\
\mathcal{B}_2 &= \{\boldsymbol{u} \in \mathbb{Z}_+^{J'_m} : |\boldsymbol{u}| = k,\ u_0 = 1 \text{ and } \boldsymbol{t}(J_m) \leq \boldsymbol{u}(J_m) \leq \boldsymbol{r}(J_m)\},\\
\mathcal{B}_3 &= \{\boldsymbol{u} \in \mathbb{Z}_+^{J'_m} : |\boldsymbol{u}| = k,\ u_0 = 1,\ u_{i'} = t_{i'} - 1 \quad \text{for some} \quad i' \in J_m\\
&\qquad \text{and} \quad u_i \in [t_i, r_i] \quad \text{for all} \quad i \in J_m \backslash \{i'\}\}.
\end{aligned} \tag{15}$$

Proof Since for every $X \subseteq J_m$, $h(X \cup \{0\}) = h(X)$ if and only if $h(X) = k$, that is, if and only if $X = J_m$, Theorem 2 implies that $\boldsymbol{u} \in \Gamma_0(\mathcal{Z}', \Pi)$ if and only if there exists $\boldsymbol{v} \in \mathcal{B}(\mathcal{Z}'|J_m)$ such that $\boldsymbol{v} \le \boldsymbol{u} \le (|\Pi_i|)_{i \in J_m}$.

Let $\mathcal{Z}_1 = (J_m, h_1)$ be the integer polymatroid with $h_1(X) = |\boldsymbol{t}(X)|$ for every $X \subseteq J_m$ and $\mathcal{Z}_2 = (J_m, h_2)$ be the integer polymatroid with $h_2(X) = \min\{k_2, |\boldsymbol{r}(X)| - |\boldsymbol{t}(X)|\}$ for every $X \subseteq J_m$. Note that $h(X) = h_1(X) + h_2(X)$ for every $X \subseteq J_m$. Therefore, $\mathcal{Z}'|J_m = \mathcal{Z}_1 + \mathcal{Z}_2$. As

$$\mathcal{B}(\mathcal{Z}_1) = \{\boldsymbol{t}\} \quad \text{and} \quad \mathcal{B}(\mathcal{Z}_2) = \{\boldsymbol{v} \in \mathbb{Z}_+^m : |\boldsymbol{v}| = k_2 \quad \text{and} \quad \boldsymbol{v} \le \boldsymbol{r} - \boldsymbol{t}\}, \tag{16}$$

thus from Proposition 1,

$$\mathcal{B}(\mathcal{Z}'|J_m) = \{\boldsymbol{u} \in \mathbb{Z}_+^m : |\boldsymbol{u}| = k \quad \text{and} \quad \boldsymbol{t} \le \boldsymbol{u} \le \boldsymbol{r}\}.$$

This implies the first claim.

We proceed to prove the second claim. If $u_0 = 0$, then $\boldsymbol{u} \in \mathcal{B}(\mathcal{Z}')$ if and only if $\boldsymbol{u}(J_m) \in \mathcal{B}(\mathcal{Z}'|J_m)$, that is, if and only if $\boldsymbol{u} \in \mathcal{B}_1$. In addition, we know

$$\mathcal{B}(\mathcal{Z}') = \{\boldsymbol{u} \in \mathbb{Z}_+^{J'_m} : |\boldsymbol{u}| = k \quad \text{and} \quad |\boldsymbol{u}(X)| \le h(X) \quad \text{for every} \quad X \subseteq J'_m\}.$$

In the case of $\boldsymbol{u} \in \mathcal{B}(\mathcal{Z}')$ with $u_0 = 1$, suppose $u_{i'} = t_{i'} - 2$ for some $i' \in J_m$, then

$$\left|\boldsymbol{u}(J_m \backslash \{i'\})\right| \le h(J_m \backslash \{i'\}) \le \left|\boldsymbol{t}(J_m \backslash \{i'\})\right| + k_2.$$

This implies that $|\boldsymbol{u}(J_m)| \le |\boldsymbol{t}(J_m)| + k_2 - 2 = k - 2$. This leads to contradictions as $|\boldsymbol{u}(J_m)| = k - 1$. Therefore, $u_{i'} \ge t_{i'} - 1$.

Suppose $u_{i_1} = t_{i_1} - 1$ and $u_{i_2} = t_{i_2} - 1$ for $i_1, i_2 \in J_m$ with $i_1 \ne i_2$. Then

$$\left|\boldsymbol{u}(J_m \backslash \{i_1, i_2\})\right| \le h(J_m \backslash \{i_1, i_2\}) \le \left|\boldsymbol{t}(J_m \backslash \{i_1, i_2\})\right| + k_2.$$

Accordingly, $|\boldsymbol{u}(J_m)| \le k - 2$. This leads to contradictions too. Moreover, $u_i \le h(\{i\}) = r_i$ for every $i \in J_m$. Therefore, $\boldsymbol{u} \in \mathcal{B}_2 \cup \mathcal{B}_3$.

On the other hand, if $\boldsymbol{u} \in \mathcal{B}_2$, then for every $X \subseteq J_m$, $|\boldsymbol{u}(X)| \le k - 1$ and $\boldsymbol{t}(X) \le \boldsymbol{u}(X) \le \boldsymbol{r}(X)$. From (16),

$$|\boldsymbol{u}(X)| \le \min\{k - 1, |\boldsymbol{t}(X)| + k_2, |\boldsymbol{r}(X)|\} \le h(X),$$

and consequently, $|\boldsymbol{u}(X \cup \{0\})| = |\boldsymbol{u}(X)| + 1 \le h(X) + 1$. This implies

$$\left|\boldsymbol{u}(X \cup \{0\})\right| \le \min\{k, h(X) + 1\} = h(X \cup \{0\}).$$

Hence, $\boldsymbol{u} \in \mathcal{B}(\mathcal{Z}')$.

If $\boldsymbol{u} \in \mathcal{B}_3$, then for every $X \subseteq J_m$ such that $i' \notin X$, similar to the case of $\boldsymbol{u} \in \mathcal{B}_2$, we can prove that $|\boldsymbol{u}(X)| \le h(X)$ and $|\boldsymbol{u}(X \cup \{0\})| \le h(X \cup \{0\})$. Moreover, for such a set $X \subseteq J_m$,

$$\begin{aligned}\left|\boldsymbol{u}(X \cup \{i'\})\right| &= u_{i'} + |\boldsymbol{u}(X)| \\ &\le \min\{|\boldsymbol{t}(X)| + k_2 + t_{i'} - 1, |\boldsymbol{r}(X)| + t_{i'} - 1\} \\ &\le h(X \cup \{i'\}),\end{aligned}$$

and $\left|\boldsymbol{u}(X \cup \{0, i'\})\right| = \left|\boldsymbol{u}(X \cup \{i'\})\right| + 1 \le h(X \cup \{i'\}) + 1$. Therefore,

$$\left|\boldsymbol{u}(X \cup \{0, i'\})\right| \le \min\{k, h(X \cup \{i'\}) + 1\} = h(X \cup \{0, i'\}).$$

This implies $\boldsymbol{u} \in \mathcal{B}(\mathcal{Z}')$. Accordingly, $\boldsymbol{u} \in \mathcal{B}(\mathcal{Z}')$ with $u_0 = 1$ if and only if $\boldsymbol{u} \in \mathcal{B}_2 \cup \mathcal{B}_3$, and the result follows. □

We next present a linear representation of the polymatroid defined in Lemma 4 based on the sum of two polymatroids.

Let I_{k_1} denote the $k_1 \times k_1$ unit matrix over $\mathbb{F}_q$, and $\bar{t}_i = \sum_{j=0}^{i} t_j$ for $i \in J'_m$. For every $i \in J_m$, consider the $\mathbb{F}_q$-vector subspace E_i spanned by the $(\bar{t}_{i-1}+1)$th column to $\bar{t}_i$th column of I_{k_1}. Let the integer polymatroid $\mathcal{Z}_1 = (J_m, h_1)$ such that

$$h_1(X) = \dim\left(\sum_{i\in X} E_i\right) \quad \text{for every} \quad X \subseteq J_m.$$

In addition, consider the map $\psi : \mathbb{F}_{q^\lambda} \to \mathbb{F}_{q^\lambda}^{k_2}$ defined by

$$\psi(\beta) = (\beta, \beta^q, \ldots, \beta^{q^{k_2-1}})$$

where $q \geq 1 + \max_{i\in J_m}\{|\Pi_i|\}$ and $\lambda \geq 1 + |\boldsymbol{r}(J_m)| - |\boldsymbol{t}(J_m)|$. Take elements $\beta_{i,j}$ in $\mathbb{F}_{q^\lambda}$, where $i \in J_m$ and $j \in [r_i - t_i]$, that are linearly independent over $\mathbb{F}_q$. For every $i \in J_m$, consider the $\mathbb{F}_q$-vector subspace $V_i \subseteq \mathbb{F}_{q^\lambda}^{k_2}$ spanned by $\{\psi(\beta_{i,j}) : j \in [r_i - t_i]\}$. Let the integer polymatroid $\mathcal{Z}_2 = (J_m, h_2)$ such that

$$h_2(X) = \dim\left(\sum_{i\in X} V_i\right) \quad \text{for every} \quad X \subseteq J_m.$$

For $i \in J_m$, let $W_i = E_i \times V_i$, and let W_0 be the $\mathbb{F}_q$-vector subspace spanned by the k-dimensional vector

$$\boldsymbol{\epsilon} = (1, 1, \ldots, 1, \beta_0, \beta_0^q, \beta_0^{q^2}, \ldots, \beta_0^{q^{k_2-1}}),$$

where β_0 and $\beta_{i,j}$ with $i \in J_m$ and $j \in [r_i - t_i]$ are linearly independent over $\mathbb{F}_q$. Let the integer polymatroid $\mathcal{Z}' = (J'_m, h)$ such that

$$h(X) = \dim\left(\sum_{i\in X} W_i\right) \quad \text{for every} \quad X \subseteq J'_m.$$

Proposition 9 *For the polymatroid $\mathcal{Z}' = (J'_m, h)$ defined above, the ULCASs (3) are of the form $\Gamma_0(\mathcal{Z}', \Pi)$ and $\mathcal{B}(\mathcal{Z}') = \mathcal{B}_1 \cup \mathcal{B}_2 \cup \mathcal{B}_3$, (15).*

Proof To prove the claim, we only need to prove the rank function h satisfies the three conditions in Lemma 4. Obviously, $h(\{0\}) = 1$. In addition, h satisfies the second condition as $\mathcal{Z}'|J_m = \mathcal{Z}_1 + \mathcal{Z}_2$. We next prove that h satisfies the third condition. Suppose $F = (F_0|F_1|\cdots|F_m)$, where $F_0 = \boldsymbol{\epsilon}^T$ and for $i \in J_m$

$$F_i = \begin{pmatrix} I'_i & O \\ O & B_i \end{pmatrix}, \tag{17}$$

for which I'_i denotes the $k_1 \times t_i$ block formed by the $(\bar{t}_{i-1}+1)$th column to $\bar{t}_i$th column of I_{k_1} and B_i denotes the $k_2 \times (r_i - t_i)$ block formed by the column vectors $(\psi(\beta_{i,j}))^T$ with $j \in [r_i - t_i]$. For any $X' = X \cup \{0\}$ with $X = \{x_1, x_2, \ldots, x_w\} \subseteq J_m$, by interchanging columns $F_{X'} = (F_0|F_{x_1}|\cdots|F_{x_w})$ can be transform to the following form

$$F'_{X'} = \left(\begin{array}{c|cc} \mathbf{1}_{\boldsymbol{k_1}} & I'_X & O \\ (\psi(\beta_0))^T & O & B_X \end{array}\right),$$

where $\mathbf{1}_{\boldsymbol{k_1}} = (1, 1, \ldots, 1)^T$ is a k_1-dimensional vector, $I'_X = (I'_{x_1}|I'_{x_2}|\cdots|I'_{x_w})$ and $B_X = (B_{x_1}|B_{x_2}|\cdots|B_{x_w})$.

If $X = J_m$, then $h(X) = k$, $I'_X = I_{k_1}$ and $B_X = (B_1|B_2|\cdots|B_m)$. Therefore, $\mathbf{1}_{\boldsymbol{k_1}}$ is a linear combination of all column in I'_X and $(\psi(\beta_0))^T$ is a linear combination of the columns in B_X as B_X is a generator matrix of some $(|\boldsymbol{r}(J_m)| - |\boldsymbol{t}(J_m)|, k_2)$ Gabidulin code. Hence, F_0 is a linear combination of the columns in F_X. This implies $h(X \cup \{0\}) = k$.

If $X \subset J_m$ and $X \neq J_m$, then $h(X) < k$, and $h(X) = |\boldsymbol{r}(X)|$ if $|\boldsymbol{r}(X)| - |\boldsymbol{t}(X)| < k_2$ or $h(X) = |\boldsymbol{t}(X)| + k_2$ if $|\boldsymbol{r}(X)| - |\boldsymbol{t}(X)| \geq k_2$. In the first case, there are at most $k_2 - 1$ columns in B_X, hence $(\psi(\beta_0))^T$ and all columns in B_X are linearly independent. Moreover, $\mathbf{1}_{\boldsymbol{k_1}}$ and all columns in I'_X are linearly independent. This implies all columns in $F'_{X'}$ are linearly independent, and consequently, $h(X \cup \{0\}) = h(X) + 1$.

In the second case, there are at least k_2 columns in B_X. This implies $(\psi(\beta_0))^T$ can be denoted by a linear combination of some columns in B_X. Therefore, by the elementary column operators, $F'_{X'}$ can be transformed to

$$\left(\begin{array}{c|c} \mathbf{1}_{\boldsymbol{k_1}}|I'_X & O \\ \hline O & B_X \end{array}\right).$$

As $\mathbf{1}_{\boldsymbol{k_1}}$ and all columns in I'_X are linearly independent, thus $h(X \cup \{0\}) = h(X) + 1$. □

5.2 A representable matroid

In this section we construct a matrix M based on the representable polymatroid $\mathcal{Z}'$ presented in Sect. 5.1 that is a representation of a matroid $\mathcal{M}$ such that the ULCASs (3) are of the form $\Gamma_{p_0}(\mathcal{M})$, and then prove that the scheme for ULCASs can be obtained by this matrix.

Suppose $\Pi_0 = \{p_0\}$ and let $\Pi' = (\Pi_i)_{i \in J'_m}$ and $\Pi = (\Pi_i)_{i \in J_m}$ be the partition of $P' = P \cup \{p_0\}$ and P, respectively, such that $|\Pi_i| = n_i$. For every $i \in J_m$, take n_i different elements $a_{i,v} \in \mathbb{F}_q$ with $v \in [n_i]$ such that $a_{i,v} \neq 1$ and let

$$A_i = (a_{i,v}^{\ell-1})_{t_i \times n_i} \quad \ell \in [t_i],\ v \in [n_i],$$
$$A'_i = (a_{i,v}^{t_i+\ell-1})_{(r_i-t_i)\times n_i} \quad \ell \in [r_i - t_i],\ v \in [n_i].$$

Let

$$M = (M_0|M_1|\cdots|M_m)$$

be the $k \times (n+1)$ matrix such that $M_0 = \boldsymbol{\epsilon}^T$ and for $i \in J_m$,

$$M_i = F_i \begin{pmatrix} A_i \\ A'_i \end{pmatrix}, \tag{18}$$

where F_i is the matrix (17). Then by computing, we have

$$M = \left(\begin{array}{c|cccc} \mathbf{1}_{\boldsymbol{t_1}} & A_1 & O & \cdots & O \\ \mathbf{1}_{\boldsymbol{t_2}} & O & A_2 & \cdots & O \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{1}_{\boldsymbol{t_m}} & O & O & \cdots & A_m \\ \hline (\psi(\beta_0))^T & B_1A'_1 & B_2A'_2 & \cdots & B_mA'_m \end{array}\right) \tag{19}$$

where $\mathbf{1}_{\boldsymbol{t_i}} = (1, 1, \ldots, 1)^T$ is an t_i-dimensional column vector and B_i is the $k_2 \times (r_i - t_i)$ block formed by the column vectors $(\psi(\beta_{i,v}))^T$ with $v \in [r_i - t_i]$.

From (18), we know that each column of M_i is a vector in W_i for every $i \in J_m$. Therefore, M satisfies the first two conditions in Step 3 in Sect. 2.3. We next prove that the third condition in Step 3 holds.

Proposition 10 *$M_{\boldsymbol{u}}$ is nonsingular for any $\boldsymbol{u} \in \mathcal{B}_1$, (15).*

Proof Without loss of generality, we may assume that $M_{\boldsymbol{u}}$ is the $k \times k$ submatrix of M formed by the first u_i columns in every M_i with $i \in J_m$. Then

$$M_{\boldsymbol{u}} = \left(\begin{array}{cccc} A_1(u_1) & O & \cdots & O \\ O & A_2(u_2) & \cdots & O \\ \vdots & \vdots & \ddots & \vdots \\ \hline O & O & \cdots & A_m(u_m) \\ \hline B_1A_1'(u_1) & B_2A_2'(u_2) & \cdots & B_mA_m'(u_m) \end{array}\right), \tag{20}$$

where $A_i(u_i)$ and $A_i'(u_i)$ are the blocks formed by the first u_i columns of A_i and A_i', respectively. Furthermore, let

$$A_i(u_i) = \big(A_{i,1}|A_{i,2}\big) \quad \text{and} \quad A_i'(u_i) = \big(A_{i,1}'|A_{i,2}'\big),$$

where $A_{i,1}$ and $A_{i,2}$ are the blocks formed by the first t_i columns and the last $u_i - t_i$ columns of $A_i(u_i)$ respectively, $A_{i,1}'$ and $A_{i,2}'$ are the blocks formed by the first t_i columns and the last $u_i - t_i$ columns of $A_i'(u_i)$ respectively. Note that $A_{i,1}$ is a $t_i \times t_i$ block, $A_{i,2}$ is a $t_i \times (u_i - t_i)$ block, $A_{i,1}'$ is a $(r_i - t_i) \times t_i$ block, and $A_{i,2}'$ is a $(r_i - t_i) \times (u_i - t_i)$ block.

As $A_{i,1}$ is nonsingular, thus we can let

$$T_i = \left(\begin{array}{c|c} I_{t_i} & -A_{i,1}^{-1}A_{i,2} \\ \hline O & I_{u_i - t_i} \end{array}\right).$$

Since $A_i(u_i)T_i = \big(A_{i,1}|A_{i,2}\big)T_i = \big(A_{i,1}|O_{t_i \times (u_i - t_i)}\big)$ and

$$\begin{aligned} B_iA_i'(u_i)T_i &= B_i\big(A_{i,1}'|A_{i,2}'\big)T_i \\ &= B_i\big(A_{i,1}'| - A_{i,1}'A_{i,1}^{-1}A_{i,2} + A_{i,2}'\big) \\ &= \big(B_iA_{i,1}'|B_i(-A_{i,1}'A_{i,1}^{-1}A_{i,2} + A_{i,2}')\big), \end{aligned}$$

it follows that

$$M_{\boldsymbol{u}}\left(\begin{array}{ccc} T_1 & & \\ & \ddots & \\ & & T_m \end{array}\right) = \left(\begin{array}{c|c|c|c|c|c|c} A_{1,1} & O & O & O & \cdots & O & O \\ O & O & A_{2,1} & O & \cdots & O & O \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ O & O & O & O & \cdots & A_{m,1} & O \\ \hline B_1A_{1,1}' & B_1D_1 & B_2A_{2,1}' & B_2D_2 & \cdots & B_mA_{m,1}' & B_mD_m \end{array}\right), \tag{21}$$

where $D_i = -A_{i,1}'A_{i,1}^{-1}A_{i,2} + A_{i,2}'$ is a $(r_i - t_i) \times (u_i - t_i)$ matrix over $\mathbb{F}_q$. In particular, by the elementary columns operators on the matrix in the right hand of (21), we can obtain the following matrix

$$\left(\begin{array}{c|c|c|c|c} A_{1,1} & & & & \\ & A_{2,1} & & & \\ & & \ddots & & O \\ & & & A_{m,1} & \\ \hline B_1A_{1,1}' & B_2A_{2,1}' & \cdots & B_mA_{m,1}' & N \end{array}\right), \tag{22}$$

where $N = \big(B_1D_1|\cdots|B_mD_m\big)$ is a $k_2 \times k_2$ block. Hence, $M_{\boldsymbol{u}}$ is nonsingular if the matrix N is nonsingular.

We proceed to prove N is nonsingular. Let

$$\hat{A} = \begin{pmatrix} A_{i,1} & A_{i,2} \\ A'_{i,1} & A'_{i,2} \end{pmatrix},$$

then

$$\hat{A}T_i = \begin{pmatrix} A_{i,1} & O \\ A'_{i,1} & D_i \end{pmatrix}.$$

As

$$\hat{A} = \begin{pmatrix} A_i(u_i) \\ A'_i(u_i) \end{pmatrix} = \left(a_{i,v}^{\ell-1}\right)_{r_i \times u_i} \quad \ell \in [r_i], \quad v \in [u_i]$$

is a Vandermonde matrix, thus all the columns in $\hat{A}$ are linearly independent. Therefore, all the columns in D_i are linearly independent. Suppose

$$D_i := \left(d_{\ell,v}^{(i)}\right)_{(r_i-t_i)\times(u_i-t_i)} \quad \ell \in [r_i - t_i], \quad v \in [u_i - t_i]$$

and for $i \in J_m$ and $v \in [u_i - t_i]$, let

$$\bar{\beta}_{i,v} = \sum_{j=1}^{r_i-t_i} d_{j,v}^{(i)} \beta_{i,j}. \tag{23}$$

Then

$$B_i D_i = (\bar{\beta}_{i,v}^{q^{\ell-1}})_{k_2\times(u_i-t_i)} \quad \ell \in [k_2], \quad v \in [u_i - t_i].$$

Therefore, N is a block formed by the column vectors $(\psi(\bar{\beta}_{i,v}))^T$ with $i \in J_m$ and $v \in [u_i - t_i]$. Hence, Lemma 1 implies that proving the non-singularity of N is equivalent to proving that $\bar{\beta}_{i,v}$ with $i \in J_m$ and $v \in [u_i - t_i]$ are linearly independent over $\mathbb{F}_q$. As in the proof of Proposition 4, suppose there exist $\lambda_{i,v}$ with $i \in J_m$ and $v \in [u_i - t_i]$ such that $\sum_{i=1}^{m} \sum_{v=1}^{u_i-t_i} \lambda_{i,v}\bar{\beta}_{i,v} = 0$. Then

$$\sum_{i=1}^{m} \sum_{v=1}^{u_i-t_i} \lambda_{i,v} \left(\sum_{j=1}^{r_i-t_i} d_{j,v}^{(i)} \beta_{i,j} \right) = \sum_{i=1}^{m} \sum_{j=1}^{r_i-t_i} \left(\sum_{v=1}^{u_i-t_i} \lambda_{i,v} d_{j,v}^{(i)} \right) \beta_{i,j} = 0.$$

As $\beta_{i,j}$ with $i \in J_m$ and $j \in [r_i - t_i]$ are linearly independent over $\mathbb{F}_q$, thus

$$\sum_{v=1}^{u_i-t_i} \lambda_{i,v} d_{j,v}^{(i)} = 0 \quad i \in J_m, \quad j \in [r_i - t_i].$$

Therefore, $\sum_{v=1}^{u_i-t_i} \lambda_{i,v}(d_{1,v}^{(i)}, \ldots, d_{r_i-t_i,v}^{(i)}) = 0$ for every $i \in J_m$. Hence, $\lambda_{i,v} = 0$ for any $i \in J_m$ and $v \in [u_i - t_i]$ since for a given $i \in J_m$, the $u_i - t_i$ vectors $(d_{1,v}^{(i)}, \ldots, d_{r_i-t_i,v}^{(i)})$ are linearly independent. This implies that $\bar{\beta}_{i,v}$ with $i \in J_m$ and $v \in [u_i - t_i]$ are linearly independent over $\mathbb{F}_q$, and consequently, N is nonsingular. Therefore, $M_{\boldsymbol{u}}$ is nonsingular. Using the same method, we can prove that $M_{\boldsymbol{u}}$ is nonsingular for any $\boldsymbol{u} \in \mathcal{B}_1$, (15). □

Proposition 11 *$M_{\boldsymbol{u}}$ is nonsingular for any $\boldsymbol{u} \in \mathcal{B}_2$, (15).*

Proof Without loss of generality, we may assume that $M_{\boldsymbol{u}}$ is the $k \times k$ submatrix of M formed by the first u_i columns in every M_i with $i \in J'_m$. Then

$$M_{\boldsymbol{u}} = \big(M_0 | M_{\boldsymbol{u}(J_m)}\big).$$

Here, $M_{\boldsymbol{u}(J_m)}$ has the identical form with the right hand of (20) and it is a $k \times (k-1)$ block. By the similar method in the proof of Proposition 10, $M_{\boldsymbol{u}(J_m)}$ can be transformed to a matrix with the form (22), and consequently, $M_{\boldsymbol{u}}$ can be transformed to the following form

$$\left(\begin{array}{c|c|c|c|c|c} \mathbf{1}_{\boldsymbol{t_1}} & A_{1,1} & O & \cdots & O & O \\ \mathbf{1}_{\boldsymbol{t_2}} & O & A_{2,1} & \cdots & O & O \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{1}_{\boldsymbol{t_m}} & O & O & \cdots & A_{m,1} & O \\ \hline (\psi(\beta_0))^T & B_1 A'_{1,1} & B_2 A'_{2,1} & \cdots & B_m A'_{m,1} & N \end{array}\right).$$

Here, N is a $k_2 \times (k_2 - 1)$ block.

As $a_{i,v} \neq 1$ with $i \in J_m$ and $v \in [n_i]$, thus for a given $i \in J_m$, $\mathbf{1}_{\boldsymbol{t_i}}$ is a linear combination of the columns in $A_{i,1}$. Therefore, let the columns of $A_{i,1}$ be denoted by $\boldsymbol{x_{i,v}}$ with $v \in [t_i]$, then there exist $b_{i,v} \in \mathbb{F}_q$ such that $\mathbf{1}_{\boldsymbol{t_i}} = \sum_{v=1}^{t_i} b_{i,v} \boldsymbol{x_{i,v}}$. In addition, let

$$\hat{\beta}_{i,v} = \sum_{j=1}^{r_i - t_i} a_{i,v}^{t_i + j - 1} \beta_{i,j}, \tag{24}$$

then $B_i A'_{i,1}$ is formed by the column vectors $(\psi(\hat{\beta}_{i,v}))^T$ with $v \in [t_i]$. Therefore, by computing, M_0 can be transformed to

$$\big(\mathbf{0}_{\boldsymbol{t_1}}, \mathbf{0}_{\boldsymbol{t_2}}, \ldots, \mathbf{0}_{\boldsymbol{t_m}}, \psi(\hat{\beta}_0)\big)^T,$$

where $\mathbf{0}_{\boldsymbol{t_i}} = (0, 0, \ldots, 0)$ is an t_i-dimensional vector and

$$\hat{\beta}_0 = \beta_0 - \sum_{i=1}^{m} \sum_{v=1}^{t_i} b_{i,v} \hat{\beta}_{i,v}. \tag{25}$$

Hence, by the elementary column operators, $M_{\boldsymbol{u}}$ can be transformed to the following form

$$\left(\begin{array}{c|c|c|c|c} A_{1,1} & & & & \\ & A_{2,1} & & & O \\ & & \ddots & A_{m,1} & \\ \hline B_1 A'_{1,1} & B_2 A'_{2,1} & \cdots & B_m A'_{m,1} & (\psi(\hat{\beta}_0))^T | N \end{array}\right).$$

This implies that $M_{\boldsymbol{u}}$ is nonsingular if matrix $\big(\psi(\hat{\beta}_0))^T | N\big)$ is nonsingular.

As in the proof of Proposition 10, the set of columns of N is

$$\big\{\psi(\bar{\beta}_{i,v}))^T : i \in J_m,\ v \in [u_i - t_i]\big\},$$

where $\bar{\beta}_{i,v}$ with $i \in J_m$ and $v \in [u_i - t_i]$ are linearly independent over $\mathbb{F}_q$. From (23), each $\bar{\beta}_{i,v}$ is a linear combination of the elements $\beta_{i,j}$ with $j \in [r_i - t_i]$, and from (24) and (25), $\hat{\beta}_0$ and $\beta_{i,j}$ with $i \in J_m$ and $j \in [r_i - t_i]$ are linearly independent over $\mathbb{F}_q$, we have $\hat{\beta}_0$ and $\bar{\beta}_{i,v}$ with $i \in J_m$ and $v \in [u_i - t_i]$ are linearly independent over $\mathbb{F}_q$. Accordingly, $\big(\psi(\hat{\beta}_0))^T | N\big)$ is nonsingular. This implies that $M_{\boldsymbol{u}}$ is nonsingular, and the result follows. □

Proposition 12 *$M_{\boldsymbol{u}}$ is nonsingular for any $\boldsymbol{u} \in \mathcal{B}_3$, (15).*

Proof Without loss of generality, we may assume that $u_1 = t_1 - 1$ and $M_{\boldsymbol{u}}$ is the $k \times k$ submatrix of M formed by the first u_i columns in every M_i with $i \in J'_m$. Similar to the case in Proposition 11,

$$M_{\boldsymbol{u}} = \left(M_0 | M_{\boldsymbol{u}(J_m)}\right).$$

Here, $M_{\boldsymbol{u}(J_m)}$ has the identical form with the right hand of (20) and it is a $k \times (k-1)$ block. Similar to (21),

$$M_{\boldsymbol{u}(J_m)} \begin{pmatrix} I_{t_1-1} & & & \\ & T_2 & & \\ & & \ddots & \\ & & & T_m \end{pmatrix} = \left(\begin{array}{c|c|c|c|c|c} A_1(t_1-1) & O & O & \cdots & O & O \\ O & A_{2,1} & O & \cdots & O & O \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ O & O & O & \cdots & A_{m,1} & O \\ \hline B_1 A'_1(t_1-1) & B_2 A'_{2,1} & B_2 D_2 & \cdots & B_m A'_{m,1} & B_m D_m \end{array}\right),$$

where $A_1(t_1-1)$ and $A'_1(t_1-1)$ are the blocks formed by the first $t_1 - 1$ columns of A_1 and A'_1, respectively, and T_i, $A_{i,1}$, $A'_{i,1}$, B_i, and D_i have the identical forms with the ones in (21). Therefore, $M_{\boldsymbol{u}(J_m)}$ can be transformed to the following form by the elementary columns operators

$$\left(\begin{array}{c|c|c|c|c} A_1(t_1-1) & A_{2,1} & \ddots & & O \\ & & & A_{m,1} & \\ \hline B_1 A'_1(t_1-1) & B_2 A'_{2,1} & \cdots & B_m A'_{m,1} & N \end{array}\right).$$

Here, $N = (B_2 D_2 | \cdots | B_m D_m)$. As in the proof of Proposition 10, N and $A_{i,1}$ with $i \in [2, m]$ are all nonsingular. Therefore, every column of $B_1 A'_1(t_1-1)$ and $B_i A'_{i,1}$ with $i \in [2, m]$ is a linear combination of the columns in N. Furthermore, $M_{\boldsymbol{u}(J_m)}$ can be transformed to the following diagonal form

$$\begin{pmatrix} A_1(t_1-1) & & & & \\ & A_{2,1} & & & \\ & & \ddots & & \\ & & & A_{m,1} & \\ & & & & N \end{pmatrix}. \tag{26}$$

As N and $A_{i,1}$ with $i \in [2, m]$ are all nonsingular, thus by computing, M_0 can be transformed to

$$\left(\mathbf{1}_{t_1}, \mathbf{0}_{t_2}, \ldots, \mathbf{0}_{t_m}, \mathbf{0}_{k_2}\right)^T,$$

and consequently, by the elementary column operators, $M_{\boldsymbol{u}}$ can be transformed to

$$\begin{pmatrix} \bar{A} & & & & \\ & A_{2,1} & & & \\ & & \ddots & & \\ & & & A_{m,1} & \\ & & & & N \end{pmatrix}$$

where $\bar{A} = \left(\mathbf{1}_{t_1} | A_1(t_1 - 1)\right)$ is an $t_1 \times t_1$ nonsingular matrix. This diagonal matrix is nonsingular as N and $A_{i,1}$ with $i \in [2, m]$ are all nonsingular. Therefore, $M_{\boldsymbol{u}}$ is nonsingular, and result follows. □

Propositions 10, 11, and 12 imply that the matrix (19) is a representation of the matroid associated to ULCASs. We next prove that ideal linear schemes realizing ULCASs can be constructed by this matrix.

Theorem 5 *Suppose M is the matrix (19). Then $LSSS(M)$ realizes the ULCASs (3) over $\mathbb{F}_{q^\lambda}$, where $q \geq 1 + \max_{i \in J_m}\{n_i\}$ and $\lambda \geq 1 + |\boldsymbol{r}(J_m)| - |\boldsymbol{t}(J_m)|$.*

Proof If $\boldsymbol{u}(J_m) \in \min \Gamma$, (3), and $u_0 = 0$, then $\boldsymbol{u}(J'_m) \in \mathcal{B}_1$. Proposition 10 implies $M_{\boldsymbol{u}(J_m)}$ is nonsingular, and consequently, M_0 is a linear combination of all the columns in $M_{\boldsymbol{u}(J_m)}$.

Assume that $\boldsymbol{u}(J_m) \notin \Gamma$, (3). Then $|\boldsymbol{u}(J_m)| < k$, or $u_i < t_i$ for some $i \in J_m$. As $h(\{i\}) = r_i$ for every $i \in J_m$, thus any $r_i + 1$ columns in M_i are linearly dependent. Hence, we may assume that

(1) $|\boldsymbol{u}(J_m)| < k$ and $\boldsymbol{t}(J_m) \leq \boldsymbol{u}(J_m) \leq \boldsymbol{r}(J)$; or
(2) $u_i < t_i$ for some $i \in J_m$ and $\boldsymbol{u}(J_m) \leq \boldsymbol{r}(J_m)$.

In the first case, furthermore, we may assume that $|\boldsymbol{u}(J_m)| = k-1$, since if $|\boldsymbol{u}(J_m)| < k-1$, we may find a vector $\boldsymbol{u'}(J_m) \geq \boldsymbol{u}(J_m)$ such that $\boldsymbol{t}(J_m) \leq \boldsymbol{u'}(J_m) \leq \boldsymbol{r}(J_m)$ and $|\boldsymbol{u'}(J_m)| = k-1$. This procedure is possible since $k - 1 \geq |\boldsymbol{u}(J_m)| \geq |\boldsymbol{t}(J_m)|$ and $|\boldsymbol{r}(J_m)| \geq k > k - 1$. In this case $\boldsymbol{u}(J'_m) \in \mathcal{B}_2$ if $u_0 = 1$. Proposition 11 implies M_0 must not be a linear combination of all the columns in $M_{\boldsymbol{u}(J_m)}$.

In the second case, furthermore, we may assume that $u_{i'} = t_{i'} - 1$ for some $i' \in J_m$, $t_i \leq u_i \leq r_i$ for all $i \in J_m \backslash \{i'\}$ and $|\boldsymbol{u}(J_m)| \geq k - 1$. Otherwise, we may find a vector $\boldsymbol{u'}(J_m) \geq \boldsymbol{u}(J_m)$ satisfying these conditions. If $|\boldsymbol{u}(J_m)| = k-1$ and $u_0 = 1$, then $\boldsymbol{u}(J'_m) \in \mathcal{B}_3$. Proposition 12 implies M_0 must not be a linear combination of all the columns in $M_{\boldsymbol{u}(J_m)}$. If $|\boldsymbol{u}(J_m)| > k - 1$, then there must exist a vector $\boldsymbol{v}(J'_m)$ with $v_0 = 1$ and $\boldsymbol{v}(J_m) \leq \boldsymbol{u}(J_m)$ such that $v_{i'} = u_{i'} = t_{i'} - 1$, $t_i \leq v_i \leq r_i$ for all $i \in J_m \backslash \{i'\}$ and $|\boldsymbol{v}(J_m)| = k - 1$. We claim that every column in $M_{\boldsymbol{u}(J_m)}$ is a linear combination of the columns in $M_{\boldsymbol{v}(J_m)}$.

As such a vector $\boldsymbol{v}(J'_m) \in \mathcal{B}_3$, thus M_0 must not be a linear combination of all the columns in $M_{\boldsymbol{v}(J_m)}$. Therefore, if this clam is true, then M_0 must not be a linear combination of all the columns in $M_{\boldsymbol{u}(J_m)}$.

We proceed to prove the claim. Recall that $\bar{t}_i = \sum_{j=0}^{i} t_j$ for every $i \in J'_m$. Take $J = J_m \backslash \{i'\}$ and $J' = J'_m \backslash \{i'\}$, and let M' be the $(k - t_{i'}) \times (n + 1 - n_{i'})$ submatrix obtained by removing the $(\bar{t}_{i'-1} + 1)$th to $\bar{t}_{i'}$th rows of the matrix $(M_0 | \cdots | M_{i'-1} | M_{i'+1} | \cdots | M_m)$. Then M' is a representation of the matroid associated to an access structure Γ' with

$$\Gamma' = \{\boldsymbol{u}(J) \in \mathbb{Z}_+^J : |\boldsymbol{u}(J)| = k - t_{i'} \quad \text{and} \quad \boldsymbol{t}(J) \leq \boldsymbol{u}(J) \leq \boldsymbol{r}(J)\}.$$

Proposition 10 implies that $M'_{\boldsymbol{v}(J)}$ is nonsingular. As $M'_{\boldsymbol{v}(J)}$ is a submatrix of $M'_{\boldsymbol{u}(J)}$, thus any column in $M'_{\boldsymbol{u}(J)}$ is a linear combination of the columns in $M'_{\boldsymbol{v}(J)}$. Note that $M'_{\boldsymbol{v}(J)}$ and $M'_{\boldsymbol{u}(J)}$ are the submatrices obtained by removing the $(\bar{t}_{i'-1} + 1)$th to $\bar{t}_{i'}$th rows of $M_{\boldsymbol{v}(J)}$ and $M_{\boldsymbol{u}(J)}$, respectively, and these rows are all zero rows. It follows that any column in $M_{\boldsymbol{u}(J)}$ is a linear combination of the columns in $M_{\boldsymbol{v}(J)}$. This with $M_{\boldsymbol{u}(\{i'\})} = M_{\boldsymbol{v}(\{i'\})}$ imply the claim. □

From the connection of LCASs, UCASs and ULCASs, the following corollary can be obtained directly.

Corollary 2 *Suppose M is the matrix (19), then*

(1) *LSSS*(M) *realizes the LCASs* (1) *over* $\mathbb{F}_{q^\lambda}$, *where* $q \geq 1 + \max_{i\in J_m}\{n_i\}$ *and* $\lambda \geq 1 + |\boldsymbol{n}(J_m)| - |\boldsymbol{t}(J_m)|$ *if* $\boldsymbol{r}(J_m) = \boldsymbol{n}(J_m)$;
(2) *LSSS*(M) *realizes the UCASs* (3) *over* $\mathbb{F}_{q^\lambda}$, *where* $q \geq 1 + \max_{i\in J_m}\{n_i\}$ *and* $\lambda \geq 1 + |\boldsymbol{r}(J_m)|$ *if* $t_i = 0$ *for every* $i \in J_m$.

Note that in the scheme for the UCASs (3) given by Corollary 2, $q \geq 1+\max_{i\in J_m}\{n_i\}$ since we choose n_i different elements $a_{i,v} \in \mathbb{F}_q$ with $v \in [n_i]$ such that $a_{i,v} \neq 1$. Nevertheless, in the scheme given by Theorem 3, $a_{i,v}$ may be equal to 1. In addition, Corollary 2 gives a method to construct the scheme for LCASs directly, which is different from the method based on duality presented in Sect. 4.

6 Comparison to the constructions of Tassa and Dyn

Tassa and Dyn [36] presented a probabilistic method to construct an ideal linear scheme for the LCASs (1) based on a scheme for the dual access structures (9) by bivariate interpolation as follows.

Secret Sharing Scheme (LSSS(I))

1. Let $s \in \mathbb{F}_q$ be a secret value. The dealer chooses randomly a polynomial

$$f(x, y) = \sum_{i=1}^{m}\sum_{j=0}^{\tau_i-1} a_{i,j}y^j \prod_{\substack{j\in J_m\\ j\neq i}} \frac{x - x_j}{x_i - x_j}$$

   such that $a_{i,0} = s$ with $i \in J_m$, where x_i with $i \in J_m$ are m distinct random points in $\mathbb{F}_q$.
2. Each participant $u_{i,j}$ from compartment Π_i is identified by a unique public point $(x_i, y_{i,j})$, where $y_{i,j} \neq 0$ is random, and his share is $f(x_i, y_{i,j})$.
3. In addition, the values of f at $v = \sum_{i=1}^{m}\tau_i - m + 1 - l$ random points (x'_i, z_i) are published, where $x'_i \notin \{x_1, \ldots, x_m\}$, $i \in [v]$.

Tassa and Dyn [36] showed that *LSSS*(I) is an ideal linear scheme realizing the access structures (9) with probability $1 - \binom{n+1}{l}\eta q^{-1}$, where η is a constant depending on m, l, and $\tau_1, \ldots, \tau_m$. This also implies that the existence of ideal linear scheme realizing the access structures (9) over finite fields $\mathbb{F}$ of size

$$|\mathbb{F}| > \eta\binom{n+1}{l}. \tag{27}$$

The value of η was not given in [36]. Farràs et al., [17] pointed out that $\eta \approx \sum_{i=1}^{m}\tau_i n_i$. A similar result was proven by them regarding UCASs.

In Theorem 4, we constructed an ideal linear scheme for the access structures (9) over finite fields $\mathbb{F}$ of size

$$|\mathbb{F}| > \left(1 + \max_{i\in J_m}\{n_i\}\right)^{\sum_{i=1}^{m}\tau_i - m + 1}. \tag{28}$$

If the lower bound (28) is less than the lower bound (27), then estimate (28) is better than (27). This is possible, for example, let the access structures (9) have the parameters that $m = 4$, $n_i = 6$, $\tau_i = 3$, $i \in [4]$. Then $n = \sum_{i=1}^{4} n_i = 24$, $\eta \approx \sum_{i=1}^{4}\tau_i n_i = 72$, and $l \leq \sum_{i=1}^{4}\tau_i - m + 1 = 9$. We have that the lower bound (28) equals to $7^9 = 40353607$.

If $k = 8$, then the lower bound (27) equals to $77873400 > 7^9$. In this case, estimate (28) is better than (27).

Nevertheless, we think the main difference between our method and their method is the efficiency of algorithms. In these two methods, an ideal linear scheme for a given access structure is ultimately determined by a matrix M. If some special submatrices of M are nonsingular then the scheme can realize the access structure. In their method, the nonsingularity of those submatrices depends on the bivariate interpolation used in [36]. To the best of our knowledge, there is not an efficient algorithm to solve the bivariate interpolation. In our method those submatrices are nonsingular based on the the special properties of Gabidulin codes.

7 Conclusion

In this paper, we mainly studied how to construct ideal linear secret sharing schemes realizing compartmented access structures by efficient methods. We constructed ideal linear schemes realizing UCASs, LCASs and ULCASs. In regards to future research directions related to schemes studied here, we will extend our method herein to construct secret sharing schemes for other multipartite access structures such as compartmented access structure with compartmented compartments, compartmented access structures with hierarchical compartments, and others.

Acknowledgements The authors are very grateful to the reviewers and Dr. Yue Zhou for their detailed comments and suggestions that much improved the presentation and quality of this paper. Special thanks to the reviewer who suggests to use polymatroid–based techniques and gives many guidance to improve the presentation of our main result by using polymatroid-based techniques.

Funding This research was supported in part by the Foundation of National Natural Science of China (Nos. 61772147, 61702124), Guangdong Province Natural Science Foundation of major basic research and Cultivation project (No. 2015A030308016) and Project of Ordinary University Innovation Team Construction of Guangdong Province (No. 2015KCXTD014).

References

1. Ball S., Padró C., Weiner Z., Xing C.: On the representability of the biuniform matroid. SIAM J. Discret. Math. **27**(3), 1482–1491 (2013).
2. Beimel A.: Secret-sharing schemes: a survey. In: Chee Y.M., Guo Z., Ling S., Shao F., Tang Y., Wang H., Xing C. (eds.) IWCC 2011. LNCS, vol. 6639, pp. 11–46. Springer, Heidelberg (2011).
3. Beimel A., Chor B.: Universally ideal secret sharing schemes. IEEE Trans. Inf. Theory **40**(3), 786–794 (1994).
4. Beimel A., Tassa T., Weinreb E.: Characterizing ideal weighted threshold secret sharing. SIAM J. Discret. Math. **22**(1), 360–397 (2008).
5. Ben-Or M., Goldwasser S., Wigderson A.: Completeness theorems for noncryptographic fault-tolerant distributed computations. In: Proceedings of the 20th ACM Symposium on the Theory of Computing, pp. 1–10 (1988).
6. Beutelspacher A., Wettl F.: On 2-level secret sharing. Des. Codes Cryptogr. **3**(2), 127–134 (1993).
7. Blakley G.R.: Safeguarding cryptographic keys. In: Proceedings of the National Computer Conference'79, AFIPS Proceedings, vol. 48, pp. 313–317 (1979).
8. Brickell E.F.: Some ideal secret sharing schemes. J. Comb. Math. Comb. Comp. **9**, 105–113 (1989).
9. Brickell E.F., Davenport D.M.: On the classification of ideal secret sharing schemes. J. Cryptol. **4**, 123–134 (1991).
10. Chaum D., Crépeau C., Damgård I.: Multiparty unconditionally secure protocols. In: Proceedings of the 20th ACM Symposium on the Theory of Computing, pp. 11–19 (1988).

11. Chor B., Kushilevitz E.: Secret sharing over infinite domains. J. Cryptol. **6**(2), 87–96 (1993).
12. Cramer R., Damgård I., Maurer U.: General secure multi-party computation from any linear secret-sharing scheme. In: Preneel B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 316–334. Springer, Heidelberg (2000).
13. Cramer R., Daza V., Gracia I., Urroz J., Leander G., Martí-Farré J., Padró C.: On codes, matroids and secure multi-party computation from linear secret sharing schemes. In: Shoup V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 327–343. Springer, Heidelberg (2005).
14. Desmedt Y., Frankel Y.: Threshold cryptosystems. In: Brassard G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 307–315. Springer, Heidelberg (1990).
15. Farràs O., Padró C.: Ideal hierarchical secret sharing schemes. IEEE Trans. Inf. Theory **58**(5), 3273–3286 (2012).
16. Farràs O., Martí-Farré J., Padró C.: Ideal multipartite secret sharing schemes. J. Cryptol. **25**(3), 434–463 (2012).
17. Farràs O., Padró C., Xing C., Yang A.: Natural generalizations of threshold secret sharing. IEEE Trans. Inf. Theory **60**(3), 1652–1664 (2014).
18. Fehr S.: Efficient construction of the dual span program. Manuscript, May (1999).
19. Gabidulin E.M.: Theory of codes with maximum rank distance. Probl. Inf. Transm. **21**, 1–12 (1985).
20. Giulietti M., Vincenti R.: Three-level secret sharing schemes from the twisted cubic. Discret. Math. **310**(22), 3236–3240 (2010).
21. Goyal V., Pandey O., Sahai A., Waters B.: Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the 13th ACM Conference on Computer and Communications Security, pp. 89–98 (2006).
22. Herranz J., Sáez G.: New results on multipartite access structures. IEE Proc. Inf. Secur. **153**(4), 153–162 (2006).
23. Herzog J., Hibi T.: Discrete polymatroids. J. Algebr. Comb. **16**(3), 239–268 (2002).
24. Ito M., Saito A., Nishizeki T.: Secret sharing schemes realizing general access structure. In: Proceedings of the IEEE Global Telecommunication Conference, Globecom 1987, pp. 99–102 (1987).
25. Kothari S.C.: Generalized linear threshold scheme. In: Blakley G.R., Chaum D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 231–241. Springer, Heidelberg (1985).
26. Lidl R., Niederreiter H.: Finite Fields. Cambridge University Press, Cambridge (1997).
27. Massey J.L.: Minimal codewords and secret sharing. In: Proceedings of the 6th Joint Swedish-Russian Workshop on Information Theory, pp. 276–279 (1993).
28. Massey J.L.: Some applications of coding theory in cryptography. Codes Ciphers Cryptogr Coding **4**, 33–47 (1995).
29. Naor M., Wool A.: Access control and signatures via quorum secret sharing. In: 3rd ACM Conference on Computer and Communications Security, pp. 157–167 (1996).
30. Oxley J.G.: Matroid Theory. Oxford University Press, New York (1992).
31. Padró C., Sáez G.: Secret sharing schemes with bipartite access structure. IEEE Trans. Inf. Theory **46**(7), 2596–2604 (2000).
32. Schrijver A.: Combinatorial Optimization. Polyhedra and Efficiency. Springer, Berlin (2003).
33. Shamir A.: How to share a secret. Commun. ACM **22**, 612–613 (1979).
34. Simmons G.J.: How to (really) share a secret. In: Goldwasser, S. (ed.) CRYPTO 1988. LNCS, vol. 403, pp. 390–448. Springer, Heidelberg (1990).
35. Tassa T.: Hierarchical threshold secret sharing. J. Cryptol. **20**, 237–264 (2007).
36. Tassa T., Dyn N.: Multipartite secret sharing by bivariate interpolation. J. Cryptol. **22**, 227–258 (2009).
37. Welsh D.J.A.: Matroid Theory. Academic Press, London (1976).

Affiliations

Qi Chen[1] · Chunming Tang[2,3] · Zhiqiang Lin[2,3]

Chunming Tang
ctang@gzhu.edu.cn

Zhiqiang Lin
linzhiqiang0824@163.com

1 Advanced Institute of Engineering Science for Intelligent Manufacturing, Guangzhou University, Guangzhou 510006, China

2 College of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, China

3 Key Laboratory of Mathematics and Interdisciplinary Sciences of Guangdong Higher Education Institutes, Guangzhou University, Guangzhou 510006, China