Combinatorial Representations

Peter J. Cameron[a,*], Maximilien Gadouleau[b], Søren Riis[c]

[a] *School of Mathematical Sciences, Queen Mary, University of London, Mile End Road, London E1 4NS, UK*
[b] *School of Engineering and Computing Sciences, Durham University, South Road, Durham DH1 3LE, UK*
[c] *School of Electronic Engineering and Computer Science, Queen Mary, University of London, Mile End Road, London E1 4NS, UK*

Abstract

This paper introduces combinatorial representations, which generalise the notion of linear representations of matroids. We show that any family of subsets of the same cardinality has a combinatorial representation via matrices. We then prove that any graph is representable over all alphabets of size larger than some number depending on the graph. We also provide a characterisation of families representable over a given alphabet. Then, we associate a rank function and a closure operator to any representation which help us determine some criteria for the functions used in a representation. While linearly representable matroids can be viewed as having representations via matrices with only one row, we conclude this paper by an investigation of representations via matrices with only two rows.

1. Definition and examples

Combinatorial representations, defined below, generalise the notion of (linear) representations of matroids.

Definition 1.1. *Let E be a set of n elements and $\mathcal{B}$ a family of r-element subsets of E, referred to as* bases.

A combinatorial representation *of $(E, \mathcal{B})$ over an alphabet A is defined to be an n-tuple of functions $f_i : A^r \to A$ such that, for any r distinct indices $i_1, \ldots, i_r \in E$, the map from A^r to A^r given by*

$$(x_1, x_2, \ldots, x_r) \mapsto (f_{i_1}(x_1, \ldots, x_r), \ldots, f_{i_r}(x_1, \ldots, x_r))$$

is bijective if and only if $\{i_1, \ldots, i_r\} \in \mathcal{B}$.

Usually we assume $E = \{1, 2, \ldots, n\}$. We denote the map given by the displayed equation by f_b, where $b = \{i_1, \ldots, i_r\}$. This slight abuse of notation will not be detrimental to the rest of the paper. Remark that the cases where $r = 1$ or n are trivial.

*Corresponding author
Email addresses: p.j.cameron@qmul.ac.uk (Peter J. Cameron), m.r.gadouleau@durham.ac.uk (Maximilien Gadouleau), smriis@eecs.qmul.ac.uk (Søren Riis)

Example 1. Let $n = 4$ and $\mathcal{B} = \{\{1,2\},\{3,4\}\}$. A combinatorial representation over a 3-element set $\{a,b,c\}$ is given by taking f_1 and f_2 to be the two coordinate functions (that is, $f_1(x,y) = x$ and $f_2(x,y) = y$), and f_3 and f_4 by the tables

b	a	a
b	c	b
c	c	a

and

b	b	c
a	c	c
a	b	a

.

Note that $(E,\mathcal{B})$ is not a matroid.

Remark 1. Suppose that $b = \{i_1,\ldots,i_r\} \in \mathcal{B}$. Define functions g_i, for $i \in E$, by $g_i(x_1,\ldots,x_r) = f_i(y_1,\ldots,y_r)$, where $(y_1,\ldots,y_r)$ is the inverse image of $(x_1,\ldots,x_r)$ under the bijection f_b. These functions also define a combinatorial representation, with the property that g_{i_j} is the jth coordinate function. So, where necessary, we may suppose that the first r elements of E form a basis and the first r functions are the coordinate functions. This transformation can be viewed as a change of variables.

Remark 2. The values of the functions f_i are not significant; the definition could be written in terms of the partitions of A^r given by these functions: $\pi_i = \{\{x \in A^r : f_i(x) = a\} : a \in A\}$. Thus, we require that the meet (in the partition lattice) of r partitions is the partition into singletons if and only if the indices of these partitions form a set in $\mathcal{B}$.

Remark 3. The condition that the domain of the functions is A^r is also not essential; any set of cardinality q^r will do (where $q = |A|$), since as in Remark 1 the functions corresponding to a set in $\mathcal{B}$ give this set the structure of a Cartesian power.

Remark 4. Our point of view is similar to that of experimental design in statistics, where functions on (or partitions of) the set of experimental units are called *factors*, see [1, Chapter 10].

To take a very simple example, let us assume that q^2 trees in an orchard are laid out in a $q \times q$ square. Last year, q fertilizers were applied to the trees, using a Latin square layout, so that each fertilizer was used once in each row and column. This year, we want to test q pesticides on the trees, again in a Latin square layout; but, because of possible interaction between fertilizer and pesticide, we would like each combination to occur just once. We can regard rows, columns, fertilizers and pesticides as four functions from the set of trees to a set of size q (or four factors, each with q parts of size q); our requirement is that we have a representation of the complete graph of size 4. We return to this in Example 2.

Remark 5. Combinatorial representations are closely related to secret-sharing matroids (see [2, 3, 4]). However, we note that combinatorial representations are defined for any family of bases, which do not necessarily form a matroid. Also, the conditions are slightly different: if $\mathcal{B}$ is the set of bases of a matroid, then a combinatorial representation is a secret-sharing representation if for every subset $X \subseteq E$, the number of images of the function $f_X : A^r \to A^{|X|}$ is equal to $|A|^{r(X)}$, where $r(X)$ is the rank of X in the matroid $(E,\mathcal{B})$. This distinction is crucial, since we shall show that any family of bases has a combinatorial representation, while the Vámos matroid does not have a secret-sharing representation [3].

Theorem 1.2. *A set family is a linearly representable matroid if and only if it has a combinatorial representation by linear functions.*

PROOF. The family $(E, \mathcal{B})$ is a linearly representable matroid over F if there exist n vectors $v_1, \ldots, v_r \in F^r$ such that $v_{i_1}, \ldots, v_{i_r}$ is a basis of F^r if and only if $i_1, \ldots, i_r \in \mathcal{B}$. Defining $f_i : F^r \to F$ as $f_i(x) = v_i \cdot x$, we see that f_b forms a bijection if and only if $v_{i_1}, \ldots, v_{i_r}$ is a basis. Therefore, (f_i) is a combinatorial representation of $(E, \mathcal{B})$ by linear functions. The argument reverses.

Example 2. A combinatorial representation of the uniform matroid $U_{2,n}$ on a set of size q is equivalent to a set of $n-2$ mutually orthogonal Latin squares of order q (see [4]). More generally, a representation of $U_{r,n}$ over A is equivalent to an (n, r) MDS code over A.

2. All set families are representable

In this section, we show that any family is representable over some finite alphabet by giving an explicit construction via matrix linear functions.

Proposition 2.1. *Let $(E, \mathcal{B}_1)$ and $(E, \mathcal{B}_2)$ be families of r-sets, which have representations over finite alphabets A_1 and A_2 respectively. Then $(E, \mathcal{B}_1 \cap \mathcal{B}_2)$ has a representation over $A_1 \times A_2$.*

PROOF. Let (f_e) and (g_e) be representations of $(E, \mathcal{B}_1)$ and $(E, \mathcal{B}_2)$ over the alphabets A_1 and A_2 respectively. Consider the functions $h_e : (A_1 \times A_2)^r \to A_1 \times A_2$ given by $h_e((a_1, b_1), \ldots, (a_r, b_r)) = (f_e(a_1, \ldots, a_r), g_e(b_1, \ldots, b_r))$. It is tedious but routine to show that, for any $b \subseteq E$, h_b is a bijection if and only if both f_b and g_b are bijections. So the functions $(h_e : e \in E)$ represent $(E, \mathcal{B}_1 \cap \mathcal{B}_2)$.

Theorem 2.2. *Any family is representable over some finite alphabet by matrix linear functions.*

PROOF. First of all, if $\mathcal{B} = U_{r,n}$, then it has a representation by linear functions. Otherwise, we can express $\mathcal{B}$ as $\mathcal{B} = \bigcap_{c \in U_{r,n} \setminus \mathcal{B}} U_{r,n} \setminus \{c\}$. We now give a linear representation of $U_{r,n} \setminus \{c\}$; without loss, let $c = \{1, \ldots, r\}$. For any prime power $p \geq \binom{n-1}{r-1} + 1$, there are $n-1$ vectors $v_2, \ldots, v_n \in \mathrm{GF}(p)^r$ such that $v_{i_1}, \ldots, v_{i_r}$ are linearly independent for any choice of indices; moreover, there is $v_1 \in \langle v_2, \ldots, v_r \rangle$ such that $v_1 \notin \langle v_{i_1}, \ldots, v_{i_{r-1}} \rangle$ for any other choice of indices, since

$$\left| \langle v_2, \ldots, v_r \rangle \setminus \bigcup_{i_1, \ldots, i_{r-1}} \langle v_{i_1}, \ldots, v_{i_{r-1}} \rangle \right| \geq p^{r-1} - \binom{n-1}{r-1} p^{r-2} > 0.$$

These vectors thus form a linear representation. Finally, by applying the cartesian product construction in Proposition 2.1, we obtain a matrix linear representation of $(E, \mathcal{B})$.

3. Representations of graphs

Representability is not a monotonic property of alphabet size. For example, a representation of the complete graph on 4 vertices is equivalent to a pair of orthogonal Latin squares; these exist over alphabets of sizes 3, 4 and 5 but not 6. However, we will prove the following for set systems with $r = 2$, that is, graphs.

Theorem 3.1. *Let $(E, \mathcal{B})$ be a graph. Then $(E, \mathcal{B})$ has combinatorial representations over all sufficiently large finite alphabets.*

The theorem follows from the two propositions below.

We say that a representation $(f_e : e \in E)$ of the graph $(E, \mathcal{B})$ is *idempotent* if $f_e(x, x) = x$ for all $x \in A$ and all $e \in E$, where A is the alphabet.

Proposition 3.2. *Let $(E, \mathcal{B}_1)$ and $(E, \mathcal{B}_2)$ be graphs, which have idempotent representations over alphabets A_1 and A_2 respectively. Then $(E, \mathcal{B}_1 \cap \mathcal{B}_2)$ has an idempotent representation over $A_1 \times A_2$.*

The proof is the same as the one for Proposition 2.1 and hence omitted.

For the second proposition, we need to recall the terminology of Richard Wilson [5]. A *pairwise balanced design* consists of a set X and a family $\mathcal{L}$ of subsets of X with the property that any two distinct elements of X are contained in a unique member of $\mathcal{L}$. It is a PBD(K), where K is a set of positive integers, if the cardinality of every member of $\mathcal{L}$ is contained in K. The elements of X and $\mathcal{L}$ are called *points* and *lines* respectively.

A set K of positive integers is *PBD-closed* if, whenever there exists a PBD(K) with v points, then $v \in K$. Given any set K of positive integers, define $\alpha(K) = \gcd\{k - 1 : k \in K\}$, $\beta(K) = \gcd\{k(k-1) : k \in K\}$. Wilson's main theorem asserts that a PBD-closed set K contains all but finitely many integers v such that $\alpha(K) \mid v-1$ and $\beta(K) \mid v(v-1)$.

Proposition 3.3. *Let $(E, \mathcal{B})$ be a graph. Then the set of cardinalities of alphabets over which $(E, \mathcal{B})$ has an idempotent combinatorial representation is PBD-closed.*

Proof. Let K be the set of alphabet sizes for which the graph $G = (E, \mathcal{B})$ has an idempotent representation. To show that K is PBD-closed, let $(X, \mathcal{L})$ be a PBD(K) on v points; we have to show that $v \in K$.

By assumption, for each line L of the PBD, we have an idempotent representation (f_e^L) with the alphabet L. We construct a representation (f_e) with alphabet X by the following rule: $f_e(x, x) = x$; if $x \neq y$, and L is the unique line containing x and y, then $f_e(x, y) = f_e^L(x, y)$. We claim that this is a representation.

Take $e_1 \neq e_2$. Suppose first that (f_{e_1}, f_{e_2}) is not a bijection. Then there exist distinct pairs (x, y) and (x', y') such that $f_{e_i}(x, y) = f_{e_i}(x', y')$ for $i = 1, 2$. We consider three cases.

First, if $x = y$ and $x' = y'$, then $x = f_{e_i}(x, y) = f_{e_i}(x', y') = x'$.

Second, suppose that $x = y$ and $x' \neq y'$. Then $f_{e_i}(x', y') = f_{e_i}(x, y) = x$, so x lies in the line L containing x' and y'. Then $(f_{e_1}^L, f_{e_2}^L)$ is not a bijection, so $\{e_1, e_2\} \notin \mathcal{B}$.

Third, suppose that $x \neq y$ and $x' \neq y'$. If $f_{e_1}(x, y) \neq f_{e_2}(x, y)$, then both of these points lie in the line L containing x and y; hence x' and y' also lie in this line. Now $(f_{e_1}^L, f_{e_2}^L)$ fails to be a bijection, and so $\{e_1, e_2\} \notin \mathcal{B}$. So we can suppose that $f_{e_1}(x, y) =$

$f_{e_2}(x,y) = z$, say, with $x, y, z \in L$. Then $(f_{e_1}(x,y), f_{e_2}(x,y)) = (f_{e_1}(z,z), f_{e_2}(z,z))$, and again $(f^L_{e_1}, f^L_{e_2})$ fails to be a bijection.

Conversely, suppose that $\{e_1, e_2\} \notin \mathcal{B}$. Then, for any line L, $(f^L_{e_1}, f^L_{e_2})$ is not a bijection; so (f_{e_1}, f_{e_2}) is not a bijection.

Our claim is proved, and with it, the proposition.

Proof of Theorem 3.1. First, we observe that the complete graph K_n has an idempotent representation over any field with at least n elements: simply associate a distinct field element $\lambda(e)$ with each $e \in E$, and put $f_e(x,y) = \lambda(e)x + (1-\lambda(e))y$.

Now we obtain an idempotent representation of the complete graph minus an edge: if e_1 and e_2 are the two nonadjacent vertices, take the above representation of the graph on $E \setminus \{e_1\}$, and let $f_{e_2} = f_{e_1}$.

Next, an arbitrary graph is the intersection of graphs each of which is a complete graph minus an edge, and so has an idempotent representation, by Proposition 3.2. If the alphabet size of this representation is N, we obtain further representations over alphabets of size qN, for any q large enough (by Proposition 3.2 again, intersecting with a complete graph).

Now to prove the Theorem, we know from Proposition 3.3 that the set K of alphabet sizes over which idempotent representations exist is PBD-closed; so by Wilson's theorem we have only to show that $\alpha(K) = 1$ and $\beta(K) = 2$.

Suppose that $\alpha(K) > 1$. Then every number of the form qN as above is congruent to 1 mod $\alpha(K)$, contradicting the fact that we can choose q to be a multiple of $\alpha(K)$. So $\alpha(K) = 1$. The argument for $\beta(K)$ is similar.

4. Families representable over a given finite alphabet

We now characterize families which are representable over a given alphabet. Clearly, if $(E, \mathcal{B})$ is representable over a finite alphabet A, then it is representable over any other alphabet with the same cardinality, so we assume $A = \mathbb{Z}_q$ unless otherwise specified. Furthermore, if $(E, \mathcal{B})$ is representable over A, then any section hypergraph of $(E, \mathcal{B})$ is as well.

First of all, the definitions below easily generalize concepts for matroids. For any $e \in E$, let $\mathcal{B}(e) := \{b \subseteq E \setminus \{e\} : |b| = r - 1, b \cup \{e\} \in \mathcal{B}\}$.

Definition 4.1.

- *l is a* loop *if no basis contains l, that is, $\mathcal{B}(l) = \emptyset$.*
- *l_1 and l_2 are* parallel *if each can be replaced by the other in a basis, that is, $\mathcal{B}(l_1) = \mathcal{B}(l_2)$.*
- *The subset I of E is* dependent *if no basis contains I.*

These definitions are absolute, that is, independent of representation. However, given a representation $f = (f_i : i \in E)$, we can say:

- l is an *f-loop* if the partition corresponding to l does not have all its parts of the same size.
- l_1 and l_2 are *f-parallel* if the corresponding partitions are equal. (A statistician would say that these factors are *aliased*.)

- A subset I of E, with $|I| = s$, is *f-dependent* if the meet of the partitions indexed by I in the partition lattice does not have q^s parts of size q^{r-s}.

The representation-specific notions just defined imply the absolute notions given earlier. In the case of a linear representation of a matroid, the concepts are equivalent.

We say that a set I is *f-independent* if it is not f-dependent.

Remark: if $\{l_1, l_2\}$ is f-independent, then the partitions corresponding to l_1 and l_2 are orthogonal in the statistical sense. The converse is false, but in fact l_1 and l_2 are independent if and only if the partitions are orthogonal and their join is the partition with a single part. See [1, Chapter 10] for definitions.

It is clear that the parallel relation is an equivalence relation. An obvious choice can be made to represent a family with loops and parallel elements: use constant functions for loops, and use the same function for any set of parallel elements. We clarify this idea below.

Definition 4.2. *A function $f : A^r \to A$ is* balanced *if for all $a \in A$, $|f^{-1}(a)| = q^{r-1}$. Two balanced functions $f, g : A^r \to A$ are* parallel *if $f = \pi \circ g$ for some permutation $\pi \in S_A$.*

Again, the parallel relation for functions is an equivalence relation, where each equivalence class contains $q!$ functions. Indeed, any balanced function can be viewed as a partition of A^r into q^{r-1} parts of q elements each (the set of pre-images $f^{-1}(a)$ for all a). Two functions are parallel if and only if they induce the same partition, and the equivalence class can be viewed as that partition, which we shall denote as $\bar{f}$.

Proposition 4.3. *Let $(E, \mathcal{B})$ be a family of bases of rank r represented by (f_i) over A. Then*

1. *If $l \in E$ is not a loop, then f_l is balanced. Otherwise, f_l can be chosen to be any imbalanced function.*
2. *If l and m are not parallel, then f_l and f_m are not parallel either. Otherwise, f_l and f_m can be chosen to be parallel.*

Proof. 1. If l is not a loop, then there exists $b \in \mathcal{B}$ which contains l, say $b = \{l_1 = l, l_2, \ldots, l_r\}$. Therefore, $|f_b^{-1}(x)| = 1$ for all $x \in A^r$ which implies $|f_l^{-1}(x_1)| = q^{r-1}$ for all $x_1 \in A$ and hence f_l is balanced.

2. If f_l and f_m are parallel and f_l can be extended to a bijection by $f_2, \ldots, f_r$, then we easily obtain that f_m can also be extended by the same functions. Therefore, l and m are parallel.

We refer to a family of bases as *simple* if it contains neither loops nor parallel elements. Any family $(E, \mathcal{B})$ can be turned into a simple one $(E^*, \mathcal{B}^*)$ by removing loops and considering one element per parallel class. Proposition 4.3 then indicates that $(E, \mathcal{B})$ is representable over an alphabet A if and only if $(E^*, \mathcal{B}^*)$ is representable over the same alphabet.

By Proposition 4.3 above, all functions in the representation of a simple family are balanced and non-parallel to one another. As a corollary, they are all distinct, which

shows that there are only finitely many representable simple families of a given rank and over a given alphabet. We can now characterise these families.

Definition 4.4. *Let $P(q,r)$ be the set of partitions of A^r into q equal parts and denote its elements as $\bar{f}_1,\dots,\bar{f}_k$. Let $\mathcal{M}(q,r)=(P(q,r),\mathcal{B})$, where $\mathcal{B}=\{\{\bar{f}_{i_1},\dots,\bar{f}_{i_r}\}:\bar{f}_{\{i_1,\dots,i_r\}}$ has q^r parts$\}$.*

Clearly, $\mathcal{M}(q,r)$ is simple and representable over A: to any partition $\bar{f}_i$ associate the corresponding function f_i. Therefore, all its section hypergraphs are also representable over A (but may not be simple). Moreover, all representable families 'belong to' $\mathcal{M}(q,r)$.

Theorem 4.5. *The family $(E,\mathcal{B})$ of rank r is representable over A if and only if $(E^*,\mathcal{B}^*)$ is isomorphic to a section hypergraph of $\mathcal{M}(q,r)$.*

Proof. First, as mentioned above, $(E,\mathcal{B})$ is representable over A if and only if $(E^*,\mathcal{B}^*)$ is representable over A. The latter is equivalent to the existence of functions (f_e) such that $\{i_1,\dots,i_r\}\in\mathcal{B}^*$ if and only if $f_{\{i_1,\dots,i_r\}}$ is a bijection, which holds if and only if $\{\bar{f}_{i_1},\dots,\bar{f}_{i_r}\}$ is a basis of $\mathcal{M}(q,r)$.

Proposition 4.6 below enumerates some properties of $\mathcal{M}(q,r)$, which yield criteria on representability of families.

Proposition 4.6. *The hypergraph $\mathcal{M}(q,r)$ satisfies the following properties.*

1. *$\mathcal{M}(q,r)$ has $|P(q,r)|=\frac{1}{q!}\binom{q^r}{q^{r-1},\dots,q^{r-1}}=\frac{q^r!}{q!(q^{r-1}!)^q}$ vertices.*
2. *$\mathcal{M}(q,r)$ is regular in the following sense. For any set of $1\le k\le r$ partitions $\{\bar{f}_1,\dots,\bar{f}_k\}$ which are in a basis of $\mathcal{M}(q,r)$, there are $N(q,r;k,l)$ sets of l partitions $\{\bar{f}_{k+1},\dots,\bar{f}_{k+l}\}$ such that $\bar{f}_1,\dots,\bar{f}_{k+l}$ belong to a basis, where*

$$N(q,r;k,l)=\frac{1}{l!(q!)^l}\binom{q^{r-k}}{q^{r-k-l},\dots,q^{r-k-l}}^{q^k}=\frac{(q^{r-k}!)^{q^k}}{q!^l(q^{r-k-l}!)^{q^{k+l}}}.$$

3. *$\mathcal{M}(q,r)$ is regular of valency $N(q,r;1,r-1)=\frac{(q^{r-1}!)^q}{(r-1)!(q!)^{r-1}}$ and has $|\mathcal{B}|=\frac{q^r!}{r!(q!)^r}$ bases.*
4. *$\mathcal{M}(q,r)$ contains $\mathcal{M}(q,r-1)$ in the following sense. Let $g_0(x,x_r)=x_r$ for all $x=(x_1,\dots,x_{r-1})$; for any partition $\bar{f}\in P(q,r-1)$, let $\bar{g}\in P(q,r)$ be defined as $g(x,x_r)=f(x)$. Then $\{\bar{f}_1,\dots,\bar{f}_{r-1}\}\in\mathcal{M}(q,r-1)$ if and only if $\{\bar{g}_0,\bar{g}_1,\dots,\bar{g}_{r-1}\}\in\mathcal{M}(q,r)$.*

Proof. 1. The number of balanced functions of A^r to A is exactly the multinomial coefficient $\binom{q^r}{q^{r-1},\dots,q^{r-1}}$. Since any balanced function has exactly $q!$ parallel functions, we obtain the value of $|P(q,r)|$.

2. Let us denote the function generated by $f_1,\dots,f_k$ as f, the one generated by $f_{k+1},\dots,f_{k+l}$ as g, and the one generated by $f_1,\dots,f_{k+l}$ as h. The set $\{\bar{f}_1,\dots,\bar{f}_{k+l}\}$ belongs to a basis if and only if $h:A^r\to A^{k+l}$ is balanced. In other words, g must be balanced over all pre-images $f^{-1}(a)$ and hence can be viewed as q^k functions

$g_a : A^{r-k} \to A^l$. There are exactly $\binom{q^{r-k}}{q^{r-k-l},\ldots,q^{r-k-l}}$ choices for each g_a, and hence $\binom{q^{r-k}}{q^{r-k-l},\ldots,q^{r-k-l}}^{q^k}$ choices for g. Accounting for all parallel functions and all permutations of $\{\bar{f}_{k+1},\ldots,\bar{f}_{k+l}\}$, we must divide by $l!(q!)^l$ to obtain the value of $N(q,r;k,l)$.

3. $N(q,r;1,r-1)$ is a special case of Property 2, while $|\mathcal{B}|$ is obtained by double counting.

4. This is clear by definition of $\mathcal{M}(q,r)$.

Corollary 4.7. *Let $(E,\mathcal{B})$ be a simple family of rank r. If $|E| > |P(q,r)|$ or if there exists a set X of k elements such that there are more than $N(q,r;k,l)$ sets Y of l elements such that $X \cup Y$ is in a basis of $\mathcal{B}$, then $(E,\mathcal{B})$ is not representable over any alphabet of size up to q.*

We remark that a clique of size n in $\mathcal{M}(q,r)$ corresponds to an (n,r) MDS code over an alphabet of size q. Therefore, the MDS conjecture [6, Research Problem 11.4] can be recast a conjecture of the clique number of $\mathcal{M}(q,r)$.

Proposition 4.8 below gives necessary and sufficient conditions for adjacency in the hypergraph $\mathcal{M}(q,r)$. For any two functions $f,g : A^r \to A$, we define the Hamming distance between f and g as $d_H(f,g) := |\{x \in A^r : f(x) \neq g(x)\}|$.

Proposition 4.8. *Let $\bar{f},\bar{g} \in P(q,r)$, then the following are equivalent.*

1. *They are adjacent in $\mathcal{M}(q,r)$, i.e. $\{\bar{f},\bar{g}\} \subseteq b$ for some $b \in \mathcal{M}(q,r)$.*
2. *The function g restricted to the set $f^{-1}(a)$ is balanced for all $a \in A$.*
3. *For all f' parallel to f, $d_H(f',g) = (q-1)q^{r-1}$.*
4. *There exists $T \subseteq S_A$ such that $|T| = (q-1)^2$; there exist $a,b \in A$ with $a\pi \neq b$ for all $\pi \in T$; the set of permutation matrices, $\{M_\pi \in \mathbb{R}^{q\times q} : \pi \in T\}$, is linearly independent in the space of $q \times q$ real matrices; and $d_H(\pi \circ f, g) = (q-1)q^{r-1}$ for all $\pi \in T$.*

Proof. The first two conditions are clearly equivalent (see the proof of Proposition 4.6). Let us prove that condition 2 implies condition 3. Suppose g is balanced over all pre-images of f (and hence, over all pre-images of f' for any parallel f' of f). Then g agrees with f' in q^{r-2} positions on each pre-image; there are q pre-images, yielding $d_H(f',g) = q^r - q^{r-1}$.

Also, let us show that Property 3 implies Property 4. Foremost, recall that the subspace P of $\mathbb{R}^{q\times q}$ spanned by all $q \times q$ permutation matrices has dimension $(q-1)^2+1$ [7]. A basis is given by the permutation matrices of the identity 1, the transpositions $(1,i)$, and the 3-cycles $(1,i,j)$ for all $1 \neq i \neq j$, all elements of A. Condition 3 is equivalent to $d_H(\pi \circ f, g) = (q-1)q^{r-1}$ for all $\pi \in S_A$; this applies in particular to all the elements of the basis but the identity, which form the desired set T from Property 4 (with $a = b = 1$).

Let us now show that condition 4 implies condition 2. For all $0 \leq i \leq q-1$, let $R_i \in \mathbb{R}^{q\times q}$ be the matrix whose entries are 1 on row i and 0 elsewhere and denote $C_j = R_j^T$ for all j. Together, these $2q$ matrices span a linear subspace CR of dimension $2q-1$. Let us prove that $\dim(CR \cap P) = 1$ (the all-ones matrix $\mathbf{1}^{q\times q}$ is in the intersection). Suppose $N \in CR \cap P$, then $N = \sum_\pi \gamma_\pi M_\pi = \sum_i \alpha_i R_i + \sum_j \beta_j C_j$. The sum of all entries

on each row and each column is equal to $s = \sum_\pi \gamma_\pi$. For row i, this yields $s = \sum_j \beta_j + q\alpha_i$ and $\alpha_i = \alpha$ is a constant; similarly, we have $\beta_j = \beta$ and $N = (\alpha + \beta)\mathbf{1}^{q\times q}$.

Since the (a, b) entry of M_π is zero for all $\pi \in T$, the subspace Q spanned by the permutation matrices in T does not contain the all-ones matrix and hence $Q \oplus CR = \mathbb{R}^{q\times q}$. We now expand those matrices to q^2-dimensional row vectors by concatenating their rows. We can represent g via a column vector $\gamma \in \mathbb{R}^{q^2}$ where $\gamma_{i+qj} = |f^{-1}(i) \cap g^{-1}(j)|$. The fact that g is balanced is equivalent to $C_j\gamma = q^{r-1}$ for all j; similarly, f balanced yields $R_i\gamma = q^{r-1}$ for all $0 \le i \le q-2$. Also, $d_H(\pi \circ f, g) = q^r - q^{r-1}$ yields $M_\pi\gamma = q^{r-1}$ for all $\pi \in T$. Overall, we obtain $M\gamma = q^{r-1}\mathbf{1}^{q^2\times 1}$, where $M \in \mathbb{R}^{q^2\times q^2}$ is non-singular. Thus there is a unique solution, given when g satisfies condition 2.

Condition 3 could be replaced by: $d_H(f', g)$ is a constant for all f' parallel to f. This holds since double counting yields $\sum_{\pi\in S_A} d_H(\pi \circ f, g) = q^r(q-1)(q-1)!$ for any function $g : A^r \to A$. However, this simplification cannot be applied to Condition 4.

5. Rank and closure

5.1. Rank

This section generalises some concepts from matroid theory to the idea of combinatorial representations. Let us first define a rank function.

Definition 5.1. *Let $(E, \mathcal{B})$ be a family of bases of rank r. A function* $\mathrm{rk} : 2^E \to [0, r]$ *is a* rank function *for $(E, \mathcal{B})$ if for all $X, Y \subseteq E$:*

- $0 \le \mathrm{rk}(X) \le |X|$*;*
- *if $X \subseteq Y \subseteq E$, then* $\mathrm{rk}(X) \le \mathrm{rk}(Y)$*;*
- $\mathrm{rk}(X \cup Y) + \mathrm{rk}(X \cap Y) \le \mathrm{rk}(X) + \mathrm{rk}(Y)$*, i.e.* rk *is submodular;*
- *if $|X| = r$, then* $\mathrm{rk}(X) = r$ *if and only if $X \in \mathcal{B}$.*

This definition implies that if $X \subseteq b \in \mathcal{B}$, then $|X| = \mathrm{rk}(X)$. Below we show that every representation leads to a rank function. In particular, if f is a representation by matrix-linear functions, then its corresponding rank function takes rational values.

Proposition 5.2. *Let $(E, \mathcal{B})$ be a family of bases and let $f = (f_1, \ldots, f_n)$ be a representation for it over a finite alphabet of size q. Then r_f defined as*

$$\begin{aligned} r_f(X) := H(f_X) &= -\sum_{a\in f_X(A^r)} \frac{|f_X^{-1}(a)|}{q^r} \log_q \left\{ \frac{|f_X^{-1}(a)|}{q^r} \right\} \\ &= r - q^{-r} \sum_{a\in f_X(A^r)} |f_X^{-1}(a)| \log_q |f_X^{-1}(a)| \end{aligned}$$

where H is the q-ary entropy function, is a rank function for $(E, \mathcal{B})$.

PROOF. The proof of submodularity simply follows Shannon's inequality [8, Eq. (2.93)] and was already given in [9]. The other properties are straightforward.

Remark 6. A subset I of E is f-independent if and only if $r_f(I) = |I|$.

Remark 7. From a secret sharing point of view, the rank function $r_f(X)$ describes the amount of information about $x_1, \ldots, x_r$ given away by the function f_X. Following that approach, one would want to minimise the rank of X if it does not belong to any basis.

Remark 8. The converse of Proposition 5.2 is not true: there exist rank functions which do not correspond to any combinatorial representation. This fact was proved in [9], where they showed that any entropy function satisfies an additional inequality. In particular, they demonstrate that the rank function rk_2 defined below over the family $(E = \{1,2,3,4\}, \mathcal{B} = \{\{1,2\}\})$ cannot be viewed as the entropy function of any representation for $(E, \mathcal{B})$.

Let us denote $\mathrm{mr}(X) = \max_{b\in\mathcal{B}} |b \cap X|$, when $(E, \mathcal{B})$ is a matroid, this is its rank function. The rank function for the uniform matroid $U_{r,n}$ is given by $\mathrm{Mr}(X) = \min\{r, |X|\}$. It is easily shown that for any family $(E, \mathcal{B})$ and any rank function, we have $\mathrm{mr}(X) \leq \mathrm{rk}(X) \leq \mathrm{Mr}(X)$. Therefore, $(E, \mathcal{B})$ is a matroid if and only if it has an *integer-valued* rank function. Therefore, although matroids are viewed as special due to the submodularity of the rank function, it seems that the particularity of matroids actually resides in the *integrality* of the rank function. In fact, it can be easily shown that the function $\mathrm{rk}_p(X)$ defined for any integer $p \geq 2$ by

$$\mathrm{rk}_p(X) := \begin{cases} |X| & \text{if } |X| \leq r-1 \text{ or } X \in \mathcal{B} \\ r - \frac{1}{p} & \text{if } |X| = r, X \notin \mathcal{B} \\ r & \text{if } |X| \geq r+1 \end{cases}$$

is a rank function for $(E, \mathcal{B})$. Thus, for any $p \geq 2$, $(E, \mathcal{B})$ has a rank function which takes values over the integers divided by p. This also shows that the supremum $\mathrm{Mr}(X)$ of all rank functions can be approached. Therefore, one can only expect to derive lower bounds on any rank function, but not any upper bound other than $\mathrm{Mr}(X)$.

In view of Proposition 5.2, studying rank functions in general can help determine some constraints on the functions used in a representation. The lower bound of $\mathrm{mr}(X)$ for any rank function is tight for the rank function of a matroid. However, the exchange axiom implies that matroids are typically dense, i.e. the number of bases is large, and (leaving out trivial cases) for any basis b, there exists another basis b' with $|b \cap b'| = r-1$. Therefore, we consider sparse families to obtain lower bounds which differ from $\mathrm{mr}(X)$.

Proposition 5.3 shows that a single "isolated basis" yields a significant gap between $\mathrm{mr}(X)$ and the rank of X for some X. The restriction on fractions only serves the sake of conciseness.

Proposition 5.3. *Let $(E, \mathcal{B})$ be a family of rank r, and let $I := \min_{b\in\mathcal{B}} \max_{c\in\mathcal{B}, c\neq b} |b \cap c|$. Then if $r \equiv I \mod 2$, there exists $X \subseteq E$ such that $|X| = r$, $\mathrm{mr}(X) = \frac{r+I}{2}$, and for any rank function $\mathrm{rk}(X)$ for $\mathcal{B}$, we have $\mathrm{rk}(X) \geq \frac{3r+I}{4}$. Thus $\mathrm{rk}(X) - \mathrm{mr}(X) \geq \frac{r-I}{4}$*

PROOF. Let $b \in \mathcal{B}$ such that the intersection of any basis with b has size at most I and let $c \in \mathcal{B}$ such that $|b \cap c| = I$. Define two sets $X, Y \subseteq E$ as follows: $X = (b \cap c) \cup X' \cup Z$ and $Y = (b \cap c) \cup Y' \cup Z$, where $X', Y' \subseteq b$ and $Z \subseteq c$ have cardinality $J = \frac{r-I}{2}$ and none of the constituents intersect. Therefore, $|X| = |Y| = r$ and $\mathrm{rk}(X) + \mathrm{rk}(Y) \geq r + I + J$, since $X \cup Y \supseteq b$ and $X \cap Y = Z \cup (b \cap c) \subseteq c$. Without loss, suppose $\mathrm{rk}(X) \geq \mathrm{rk}(Y)$, then $\mathrm{rk}(X) \geq \frac{r+I+J}{2} = \frac{3r+I}{4}$. Let us now show that $\mathrm{mr}(X) = I + J = \frac{r+I}{2}$. First, we have $|b \cap X| = |c \cap X| = I + J$. Second, for any other $d \in \mathcal{B}$, we have the following inequalities: $|d \cap Z| \leq |Z| = J$ and $|d \cap X'| + |d \cap (b \cap c)| \leq |d \cap b| \leq I$, and hence $|d \cap X| = |d \cap (b \cap c)| + |d \cap X'| + |d \cap Z| \leq J + I$.

The argument is strengthened in Theorem 5.4 below, which exhibits a set with $\mathrm{mr}(X) = 1$ and yet for which the rank is arbitrarily close to r. Recall that a *transversal* for $(E, \mathcal{B})$ is a set of elements such that any basis contains at least one element of the transversal.

Theorem 5.4. *Let k denote the minimum size of a transversal for $(E, \mathcal{B})$, then there exists a set X of k elements such that* $\mathrm{mr}(X) = 1$ *and* $\mathrm{rk}(X) \geq r\left(1 - \left(1 - \frac{1}{r}\right)^k\right)$.

PROOF. We prove, by induction on $1 \leq i \leq k$, that there exists a set $X_i = \{e_1, \ldots, e_i\}$ with $\mathrm{mr}(X_i) = 1$ and $\mathrm{rk}(X_i) \geq r_i = r\left(1 - \left(1 - \frac{1}{r}\right)^i\right)$. This trivially holds for $i = 1$, let us assume this holds for $i - 1$. Let $b = \{e_i^1, \ldots, e_i^r\}$ be a basis which does not intersect with $\{e_1, \ldots, e_{i-1}\}$. Note that such a basis exists, as $\{e_1, \ldots, e_{i-1}\}$ is not a transversal by definition of k. We have $\sum_{j=1}^{r} \mathrm{rk}(X_{i-1} \cup \{e_i^j\}) \geq \mathrm{rk}(X_{i-1} \cup b) + (r-1)\,\mathrm{rk}(X_{i-1}) \geq r + (r-1)r_{i-1}$, and hence $\mathrm{rk}(X_{i-1} \cup \{e_i^j\}) \geq 1 + (1 - 1/r)r_{i-1} = r_i$ for some j.

5.2. Representation by matrices with 2 rows

In this section, we are interested in families which are "nearly" linearly representable matroids: those for which there is a representation with matrices with only two rows.

Formally, a representation of $(E, \mathcal{B})$ using matrices with 2 rows is defined as follows. Let p be any prime power, and consider $A = \mathrm{GF}(p)^2$, then we can express $x_i \in A$ as $(x_{i,1}, x_{i,2}) \in \mathrm{GF}(p)^2$. The functions representing $(E, \mathcal{B})$ are of the form $f_i(x_{1,1}, x_{1,2}, \ldots, x_{r,1}, x_{r,2}) = \mathbf{F}_i(x_{1,1}, x_{1,2}, \ldots, x_{r,1}, x_{r,2})^\top$, where $\mathbf{F}_i \in \mathrm{GF}(p)^{2 \times 2r}$.

By Proposition 2.1, if $(E, \mathcal{B})$ is the intersection of 2 linear matroids representable over the same field, then it has a representation by matrices with 2 rows. Proposition 5.5 gives a counterexample of the converse.

Proposition 5.5. *Let $E = \{1, \ldots, 6\}$ and $\mathcal{B} = \{12, 34, 56\}$. Then $(E, \mathcal{B})$ is not the intersection of two matroids, yet it has a representation by matrices with 2 rows.*

PROOF. Suppose on the contrary that $\mathcal{B} = \mathcal{B}_1 \cap \mathcal{B}_2$, where $\mathcal{B}_i$ is a matroid on E for $i \in \{1, 2\}$. We view them as graphs, and we say that two vertices are adjacent if they form a basis. By the exchange axiom, for each vertex e and each basis $b \in \mathcal{B}$ not containing e, e is adjacent in $\mathcal{B}_1$ and $\mathcal{B}_2$ to one or two vertices of b. Since such an edge does not appear in $\mathcal{B}_1 \cap \mathcal{B}_2$, we conclude that e is adjacent in $\mathcal{B}_1$ to exactly one vertex of b

and is adjacent in $\mathcal{B}_2$ to the other vertex of b. Without loss of generality, let $13, 15 \in \mathcal{B}_1$, then $23, 25 \notin \mathcal{B}_1$ by applying the conclusion above to $b = 12$ and $e = 3$ and $e = 5$, respectively. However $13, 15 \notin \mathcal{B}_2$ show that $1, 3, 5$ are parallel in $\mathcal{B}_2$ and hence $35 \notin \mathcal{B}_2$. Therefore, $35 \in \mathcal{B}_1$ while $23, 25 \notin \mathcal{B}_1$, and the exchange axiom is violated.

On the other hand, for any p, the matrices $\mathbf{F}_i \in \mathrm{GF}(p)^{2\times 4}$ given below form a representation of $(E, \mathcal{B})$ using matrices with 2 rows:

$$\mathbf{F}_0 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad \mathbf{F}_1 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \mathbf{F}_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$
$$\mathbf{F}_3 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \mathbf{F}_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \mathbf{F}_5 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

As an application of our study of the rank functions, we now prove that some families of bases do not have a representation by matrices with 2 rows. The proof is based on the Ingleton inequality [10] for the dimensions of vector spaces. Since the rank of any $X = \{i_1, \ldots, i_k\}$ can be expressed as half the dimension of the row space of the matrix $(\mathbf{F}_{i_1}^\top, \ldots, \mathbf{F}_{i_k}^\top)$, the Ingleton inequality is also satisfied by the rank. For any four subsets $X_1, \ldots, X_4$ of a family representable using matrices, we have

$$\begin{aligned} &\mathrm{rk}(X_1) + \mathrm{rk}(X_2) + \mathrm{rk}(X_1 \cup X_2 \cup X_3) + \mathrm{rk}(X_1 \cup X_2 \cup X_4) + \mathrm{rk}(X_3 \cup X_4) \\ &\leq \mathrm{rk}(X_1 \cup X_2) + \mathrm{rk}(X_1 \cup X_3) + \mathrm{rk}(X_1 \cup X_4) + \mathrm{rk}(X_2 \cup X_3) + \mathrm{rk}(X_2 \cup X_4). \end{aligned} \tag{1}$$

Proposition 5.6. *Let $E = \{1, \ldots, 7\}$ and $\mathcal{B} = \{16, 27, 34, 35, 45\}$. Then $(E, \mathcal{B})$ does not have a representation using matrices with 2 rows.*

Proof. Any rank function generated by a representation using matrices with 2 rows takes half-integer values. However, let $\mathrm{rk}(X)$ be a rank function with half-integer values and let us prove that it violates the Ingleton inequality in (1). First, we have $\mathrm{rk}(12), \mathrm{rk}(17) \leq 1.5$ as neither are bases and $\mathrm{rk}(12) + \mathrm{rk}(17) \geq \mathrm{rk}(1) + \mathrm{rk}(127) = 3$, which implies that $\mathrm{rk}(12) = \mathrm{rk}(17) = 1.5$. Second, we have $\mathrm{rk}(123) + \mathrm{rk}(124) \geq \mathrm{rk}(12) + \mathrm{rk}(1234) = 3.5$, and hence $\mathrm{rk}(123) = 2$ or $\mathrm{rk}(124) = 2$; without loss, say $\mathrm{rk}(123) = 2$. By symmetry, we also obtain that $\mathrm{rk}(124) = 2$ or $\mathrm{rk}(125) = 2$; say $\mathrm{rk}(124) = 2$. We can finally check that the sets $X_i = \{i\}$ for $i = 1, \ldots, 4$, violate the Ingleton inequality.

The Ingleton inequality cannot rule out representations by matrices with 3 rows.

Proposition 5.7. *The rank function rk_3 satisfies the Ingleton inequality.*

Proof. We denote the left and right hand sides of the Ingleton inequality in (1) as L and R, respectively. The proof goes by considering any family of four subsets $X_1, \ldots, X_4$ and checking that they satisfy the inequality. We shall split these families of subsets into four cases based on the terms in R. It is important to note the symmetric roles of X_1 and X_2 on one hand and X_3 and X_4 on the other hand in (1). The square brackets indicate where we use the submodular inequality.

Case I: $\mathrm{rk}(X_1 \cup X_2) = \mathrm{rk}(X_1 \cup X_2 \cup X_3)$. We then have

$$\begin{aligned} R &= \mathrm{rk}(X_1 \cup X_2 \cup X_3) + [\mathrm{rk}(X_1 \cup X_3) + \mathrm{rk}(X_1 \cup X_4)] + [\mathrm{rk}(X_2 \cup X_3) + \mathrm{rk}(X_2 \cup X_4)] \\ &\geq \mathrm{rk}(X_1 \cup X_2 \cup X_3) + \mathrm{rk}(X_1) + \mathrm{rk}(X_2) + [\mathrm{rk}(X_1 \cup X_3 \cup X_4) + \mathrm{rk}(X_2 \cup X_3 \cup X_4)] \geq L. \end{aligned}$$

By symmetry, we also rule out the case where $\mathrm{rk}(X_1 \cup X_2) = \mathrm{rk}(X_1 \cup X_2 \cup X_4)$.

Case II: $\mathrm{rk}(X_1 \cup X_3) = \mathrm{rk}(X_1 \cup X_2 \cup X_3)$. We then have

$$R = \mathrm{rk}(X_1 \cup X_2 \cup X_3) + [\mathrm{rk}(X_1 \cup X_2) + \mathrm{rk}(X_1 \cup X_4)] + [\mathrm{rk}(X_2 \cup X_3) + \mathrm{rk}(X_2 \cup X_4)] \geq L$$

We also rule out the cases where $\mathrm{rk}(X_1 \cup X_4) = \mathrm{rk}(X_1 \cup X_2 \cup X_4)$, $\mathrm{rk}(X_2 \cup X_3) = \mathrm{rk}(X_1 \cup X_2 \cup X_3)$, or $\mathrm{rk}(X_2 \cup X_4) = \mathrm{rk}(X_1 \cup X_2 \cup X_4)$.

The case where some term in R has rank r is contained in Case I or II, therefore all ranks in R are less than r in the next cases. Moreover, we shall assume that the conditions for Cases I and II all fail henceforth. Denote

$$\begin{aligned} \bar{L} &:= |X_1| + |X_2| + |X_1 \cup X_2 \cup X_3| + |X_1 \cup X_2 \cup X_4| + |X_3 \cup X_4|, \\ \bar{R} &:= |X_1 \cup X_2| + |X_1 \cup X_3| + |X_1 \cup X_4| + |X_2 \cup X_3| + |X_2 \cup X_4|. \end{aligned}$$

Case III: All terms in R have cardinality at most $r-1$, and hence their rank is equal to their cardinality. The cardinality function satisfies the Ingleton inequality, for $|X| = \dim(V_X)$ for all $X \subseteq E$, where V_X is the subspace generated by the unit vectors $\{e_i : i \in X\}$. Thus, we obtain $L \leq \bar{L} \leq \bar{R} = R$.

Case IV: Some terms in R have rank $r - \frac{1}{3}$, say $1 \leq k \leq 5$ of them. If $k \leq 3$, then $\mathrm{rk}(X_1 \cup X_2 \cup X_3) = r \leq |X_1 \cup X_2 \cup X_3| - 1$ or $\mathrm{rk}(X_1 \cup X_2 \cup X_4) = r \leq |X_1 \cup X_2 \cup X_4| - 1$. This holds since one of those terms must have a greater rank than one of the k terms in R with rank $r - \frac{1}{3}$; its cardinality is hence at least $r+1$. Thus $R = \bar{R} - \frac{k}{3} \geq \bar{R} - 1 \geq \bar{L} - 1 \geq L$. If $k \geq 4$, then both $X_1 \cup X_2 \cup X_3$ and $X_1 \cup X_2 \cup X_4$ have rank r, and $R = \bar{R} - \frac{k}{3} \geq \bar{R} - 2 \geq \bar{L} - 2 \geq L$.

5.3. Closure

We can generalise the idea of parallelism to the concept of closure, defined below. The point is that the closure operator depends on the rank function, not only on the family of bases.

Definition 5.8. *For a rank function* $\mathrm{rk}(X)$ *of* $(E, \mathcal{B})$*, the closure associated to* $\mathrm{rk}(X)$ *of* $X \subseteq E$ *is given by* $\mathrm{cl}(X) = \{e \in E : \mathrm{rk}(X \cup \{e\}) = \mathrm{rk}(X)\}$*. A set equal to its closure is called a* flat*.*

Proposition 5.9. *The closure satisfies the following properties. For any* $X, Y \subseteq E$*,*

1. $X \subseteq \mathrm{cl}(X)$*;*
2. *if* $X \subseteq Y$*, then* $\mathrm{cl}(X) \subseteq \mathrm{cl}(Y)$*;*
3. $\mathrm{rk}(\mathrm{cl}(X)) = \mathrm{rk}(X)$*;*
4. $\mathrm{cl}(\mathrm{cl}(X)) = \mathrm{cl}(X)$*;*
5. $\mathrm{cl}(X) = E$ *if and only if* $\mathrm{rk}(X) = r$*;*
6. $\mathrm{cl}(X)$ *is equal to the intersection of all flats containing* X*;*
7. $\mathrm{cl}(\mathrm{cl}(X) \cap \mathrm{cl}(Y)) = \mathrm{cl}(X) \cap \mathrm{cl}(Y)$*, i.e. the family of flats is closed under intersection;*

8. $\mathrm{cl}(X \cup Y) = \mathrm{cl}(\mathrm{cl}(X) \cup \mathrm{cl}(Y))$.

PROOF. We denote $F := \mathrm{cl}(X)$ and $G := \mathrm{cl}(Y)$. Property 1 is trivial.

2. For any $e \in F$, we have $\mathrm{rk}(Y)+\mathrm{rk}(X) = \mathrm{rk}(Y)+\mathrm{rk}(X \cup \{e\}) \geq \mathrm{rk}(Y \cup \{e\})+\mathrm{rk}(X)$, and hence $e \in G$.

3. Let $F \backslash X = \{e_1, \ldots, e_k\}$, then $k\,\mathrm{rk}(X) = \sum_{i=1}^{k} \mathrm{rk}(X \cup \{e_i\}) \geq \mathrm{rk}(F)+(k-1)\,\mathrm{rk}(X)$, and hence $\mathrm{rk}(F) = \mathrm{rk}(X)$.

4. Let $e \in \mathrm{cl}(F)$, then $\mathrm{rk}(X) = \mathrm{rk}(F) = \mathrm{rk}(F \cup \{e\}) \geq \mathrm{rk}(X \cup \{e\})$, and hence $e \in F$.

5. $\mathrm{rk}(X) = r$ if and only if for any $e \in E$, $\mathrm{rk}(X) = \mathrm{rk}(X \cup \{e\})$ and hence $e \in F$.

6. Let H be a flat containing X and let $e \in F$, then $\mathrm{rk}(H)+\mathrm{rk}(X) = \mathrm{rk}(H)+\mathrm{rk}(X \cup \{e\}) \geq \mathrm{rk}(H \cup \{e\}) + \mathrm{rk}(X)$, and hence $e \in \mathrm{cl}(H) = H$.

7. $F \cap G \subseteq \mathrm{cl}(F \cap G)$ on one hand and $\mathrm{cl}(F \cap G) \subseteq \mathrm{cl}(F) \cap \mathrm{cl}(G) = F \cap G$ on the other.

8. Since $X \cup Y \subseteq F \cup G$, we have $\mathrm{cl}(X \cup Y) \subseteq \mathrm{cl}(F \cup G)$. On the other hand, F and G are both subsets of $\mathrm{cl}(X \cup Y)$ and hence $\mathrm{cl}(F \cup G) \subseteq \mathrm{cl}(\mathrm{cl}(X \cup Y)) = \mathrm{cl}(X \cup Y)$.

We can then define the *lattice of flats*, which is not necessarily semimodular (as the height function is not equal to the rank) but where the rank function is a semivaluation. We finally notice that the closure associated to a given combinatorial representation satisfies

$$\begin{aligned}\mathrm{cl}(X) &:= \{e \in E : r_f(X \cup \{e\}) = r_f(X)\} \\ &= \{e \in E : \bar{f}_{X \cup \{e\}} = \bar{f}_X\} \\ &= \{e \in E : \bar{f}_X \text{ refines } \bar{f}_e\}.\end{aligned}$$

6. Conclusion

The representation of graphs in Section 3 yields a couple of open questions. Given a graph, what is the largest alphabet over which it is not representable? Does Theorem 3.1 hold for r-uniform hypergraphs with $r > 2$?

Also, after generalising loops and parallel elements in Section 4 and rank functions and closure operators in Section 5, one wonders if more concepts from matroid theory could be generalised in the framework of combinatorial representations.

The relation with information theory via rank functions and especially the submodular inequality needs to be further investigated. Indeed, a wealth of non-Shannon inequalities have been discovered recently, see [11] for a survey on this matter. However, it seems rather unclear how much more information can be drawn from all these new inequalities and how hard they are to manipulate. Similarly, non-Ingleton inequalities have been discovered for the dimension of intersections of linear subspaces [12]. Once again, what conclusions can we draw from these inequalities? In particular, can we exhibit families which cannot be represented by matrices with 3 rows, or even more?

Acknowledgement

We would like to thank the anonymous referees for interesting comments and for pointing out the connection to secret-sharing matroids.

References

[1] R. A. Bailey, Design of Comparative Experiments, Cambridge Series in Statistical and Probabilistic Mathematics, Cambridge University Press, Cambridge, 2008.

[2] E. F. Brickell, D. M. Davenport, On the classification of ideal secret sharing schemes, J. Cryptology 4 (1991) 123–134.

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

[4] F. Matúš, Matroid representations by partitions, Discrete Math. 203 (1999) 169–194.

[5] R. M. Wilson, Construction and uses of pairwise balanced designs, Mathematical Centre Tracts 55.

[6] F. J. MacWilliams, N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.

[7] H. Farahat, L. Mirsky, Permutation endomorphisms and a refinement of a theorem of Birkhoff, Math. Proc. Cambridge Philos. Soc. 56 (4) (1960) 322–328.

[8] T. M. Cover, J. A. Thomas, Elements of Information Theory, Wiley series in telecommunications, Wiley-Interscience, New York, 1991.

[9] Z. Zhang, R. W. Yeung, A non-Shannon-type conditional inequality of information quantities, IEEE Trans. Inform. Theory 43 (6) (1997) 1982–1986.

[10] A. W. Ingleton, Representation of matroids, Combinatorial mathematics and its applications (1971) 149–167.

[11] T. Chan, Recent progresses in characterising information inequalities, Entropy 13 (2011) 379–401.

[12] R. Kinser, New inequalities for subspace arrangements, J. Combin. Theory Ser. A 118 (1) (2011) 152–161.