SIAM J. Discrete Math.
Vol. 27, No. 3, pp. 1482–1491

ON THE REPRESENTABILITY OF THE BIUNIFORM MATROID[*]

SIMEON BALL[†], CARLES PADRÓ[‡], ZSUZSA WEINER[§], AND CHAOPING XING[‡]

Abstract. Every biuniform matroid is representable over all sufficiently large fields. But it is not known exactly over which finite fields they are representable, and the existence of efficient methods to find a representation for every given biuniform matroid has not been proved. The interest of these problems is due to their implications to secret sharing. The existence of efficient methods to find representations for all biuniform matroids is proved here for the first time. The previously known efficient constructions apply only to a particular class of biuniform matroids, while the known general constructions were not proved to be efficient. In addition, our constructions provide in many cases representations over smaller finite fields.

Key words. matroid theory, representable matroid, biuniform matroid, secret sharing

AMS subject classifications. 05B35, 94A62

DOI. 10.1137/120886960

1. Introduction.

Given a class of representable matroids, the following are two basic questions about the class. Over which fields are the members of the class representable? Are there efficient algorithms to construct representations for every member of the class? Here an algorithm is efficient if its running time is polynomial in the size of the ground set. For instance, every transversal matroid is representable over all sufficiently large fields [16, Corollary 12.2.17], but it is not known exactly over which fields they are representable, and the existence of efficient algorithms to construct representations is an open problem too.

The interest in these problems has been mainly motivated by their connections to coding theory and cryptology, mainly to secret sharing. Determining over which fields the uniform matroids are representable is equivalent to solving the main conjecture for maximum distance separable codes. For more details, and a proof of this conjecture in the prime case, see [1], and for further information on when the conjecture is known to hold, see [11, section 3]. As a consequence of the results by Brickell [4], every representation of a matroid M over a finite field provides ideal linear secret sharing schemes for the access structures that are ports of the matroid M. Because of that, the representability of certain classes of matroids is closely connected to the search for efficient constructions of secret sharing schemes for certain classes of access structures. The reader is referred to [12] for more information about secret sharing and its connections to matroid theory.

[*] Received by the editors August 3, 2012; accepted for publication (in revised form) June 18, 2013; published electronically August 22, 2013. This research was (partially) completed while the first author was visiting the Institute for Mathematical Sciences, National University of Singapore in 2011.

http://www.siam.org/journals/sidma/27-3/88696.html

[†] Department de Matemàtica Applicada IV, Universitat Politècnica de Catalunya, Barcelona, Spain (simeon@ma4.upc.edu). The author acknowledges the support of the project MTM2008-06620-C03-01 of the Spanish Ministry of Science and Education and the project 2009-SGR-01387 of the Catalan Research Council.

[‡] School of Physical and Mathematical Sciences, Nanyang Technological University, 63731 Singapore (cpadro@ma4.upc.edu, xingcp@utv.edu.sg). The work of the second and fourth authors was supported by the Singapore National Research Foundation under research grant NRF-CRP2-2007-03.

[§] Computer Science, Eötvös Loránd University, 14-1117, Budapest, Hungary (weiner@cs.elte.hu). This author was supported by K 81310 grant and by the ERC grant 227701 DISCRETECONT.

Several constructions of ideal linear secret sharing schemes for families of relatively simple access structures with interesting properties for the applications have been proposed [2, 4, 7, 8, 10, 14, 17, 20, 21, 22]. They are basic and natural generalizations of Shamir's [18] threshold secret sharing scheme. A unified approach to all those proposals was presented in [5]. As a consequence, the open questions about the existence of such secret sharing schemes for some sizes of the secret value and the possibility of constructing them efficiently are equivalent to determining the representability of some classes of multiuniform matroids. See [6, 8] for more information on this line of work.

In this paper, we analyze the representability of the biuniform matroids. They were introduced by Ng and Walker [15], but ideal secret sharing schemes for the access structures that are determined by them were previously presented in [17]. Biuniform matroids are defined in terms of their symmetry properties, specifically the number of clonal classes, a concept introduced in [9]. Two elements in the ground set of a matroid are said to be *clones* if the map that interchanges them and fixes all other elements is an automorphism of the matroid. Being clones is clearly an equivalence relation, and its equivalence classes are called the *clonal classes* of the matroid. Uniform matroids are precisely those having only one clonal class. A matroid is said to be biuniform if it has at most two clonal classes. Of course, this definition can be generalized to *m-uniform matroids* for every positive integer m. A biuniform matroid is determined by its rank, the number of elements in each clonal class, and the ranks of the two clonal classes, which are called the *subranks* of the biuniform matroid.

It is not difficult to check that every biuniform matroid is a transversal matroid, and hence it is representable over all sufficiently large fields. Moreover, as a consequence of the results in [5], every biuniform matroid is representable over all fields with at least $\binom{N}{k}$ elements, where N is the size of the ground set and k is the rank. The same result applies to triuniform matroids [5], but it does not apply to 4-uniform matroids because the Vamos matroid is not representable [16, Proposition 6.1.10].

Even though the proof in [5] is constructive, no efficient method to find representations for the biuniform matroids can be derived from it. A method to construct a representation for every biuniform matroid was presented by Ng [13], but it was not proved to be efficient. Efficient methods to find representations for the biuniform matroids in which one of the subranks is equal to the rank can be derived from the constructions of ideal hierarchical secret sharing schemes by Brickell [4] and by Tassa [21]. These constructions are analyzed in section 2.

In this work, we prove for the first time that there exist efficient algorithms to find representations for *all* biuniform matroids. In addition, our constructions provide representations over finite fields that are in many cases smaller than the ones used in [4, 13, 21]. A detailed comparison is given in section 2.

More specifically, we present three different representations of biuniform matroids. All of them can be obtained in time polynomial in the size of the ground set. An important parameter in our discussions is $d = m + \ell - k$, where k is the rank of the matroid while m and ℓ are its subranks. The cases $d = 0$ and $d = 1$ are reduced to the representability of the uniform matroid. Our first construction (Theorem 5.1) corresponds to the case $d = 2$, and we prove that every such biuniform matroid is representable over $\mathbb{F}_q$ if q is odd and every clonal class has at most $(q-1)/2$ elements. The other two constructions apply to the general case, and they are both based on a family of linear evaluation codes. Our second construction (Theorem 5.2) provides a representation of the biuniform matroid over $\mathbb{F}_{q_0^s}$, where $s > d(d-1)/2$ and q_0 is a prime power larger than the size of each clonal class. Finally, we present a third construction in Theorem 5.4. In this case, if $m \geq \ell$, a representation of the biuniform matroid is obtained over every prime field $\mathbb{F}_p$ with $p > K^h$, where K is larger than half the number of elements in each clonal class and $h = md(1 + d(d-1)/2)$.

2. Related work. The existence of ideal secret sharing schemes for the so-called bipartite and tripartite access structures was proved in [17] and in [5], respectively. These proofs are constructive and, in particular, they provide a method to find representations for all biuniform matroids. Such a representation can be found over every field with at least $\binom{N}{k}$ elements, where N is the size of the ground set and k is the rank. This method is not efficient because exponentially many determinants have to be computed to find a valid representation.

This problem is avoided in the method proposed by Ng [13], which provides a representation for every given biuniform matroid. Specifically, Ng gives a representation for the biuniform matroid with rank k and subranks m, ℓ over every finite field of the form $\mathbb{F}_{q_0^s}$, where $q_0 > 14$, each clonal class has at most q_0 elements, and s is at least k and co-prime with $d = m + \ell - k$. This method may be efficient, but this fact is not proved in [13]. In addition, the degree s of the extension field depends on the rank k, while in our efficient construction in Theorem 5.2, this degree depends only on d. Therefore, if d is small compared to k, our construction works over smaller fields.

Efficient methods to construct ideal hierarchical secret sharing schemes were given by Brickell [4] and by Tassa [21]. When applied to some particular cases, these methods provide representations for biuniform matroids in which one of the subranks is equal to the rank.

Brickell's construction provides a representation for every such biuniform matroid over fields of the form $\mathbb{F}_{q_0^s}$, where q_0 is a prime power larger than the size of each clonal class and s is at least the square of the rank of the matroid. An irreducible polynomial of degree s over $\mathbb{F}_{q_0}$ has to be found, but this can be done in time polynomial in q_0 and s by using the algorithm given by Shoup [19]. Therefore, a representation can be found in time polynomial in the size of the ground set. Clearly, the size of the field is much smaller in the representations that are obtained by the method described in Theorem 5.2.

Representations for those biuniform matroids are efficiently obtained from Tassa's construction over prime fields $\mathbb{F}_p$ with p larger than $N^{(k-1)(k-2)/2}$, where N is the number of elements in the ground set. If d is small compared to n, the size of the field in our construction (Theorem 5.4) is smaller.

Representations for biuniform matroids in which one of the subranks is equal to the rank of the matroid and the other one is equal to 2 are obtained from the constructions of ideal hierarchical secret sharing schemes in [3]. These are representations over $\mathbb{F}_q$, where the size of the ground set is at most $q + 1$ and the size of each clonal class is around $q/2$. These parameters are similar to the ones in Theorem 5.1, but our construction is more general.

3. The biuniform matroid. A matroid $M = (E, F)$ is a pair in which E is a finite set, called the *ground set*, and F is a nonempty set of subsets of E, called *independent sets*, such that

1. every subset of an independent set is an independent subset, and
2. for all $A \subseteq E$, all maximal independent subsets of A have the same cardinality, called the rank of A and denoted $r(A)$.

A *basis* B of M is a maximal independent set. Obviously all bases have the same cardinality, which is called the rank of M. If E can be mapped to a subset of vectors of a vector space over a field $\mathbb{K}$ so that $I \subseteq E$ is an independent set if and only if the vectors assigned to the elements in I are linearly independent, then the matroid is said to be representable over $\mathbb{K}$.

The independent sets of the uniform matroid of rank k are all the subsets B of the set E with the property that $|B| \leq k$. If the uniform matroid is representable over a field $\mathbb{K}$, then there is a map

$$f \ : \ E \to \ \mathbb{K}^k$$

such that $f(E)$ is a set of vectors with the property that every subset of $f(E)$ of size k is a basis of $\mathbb{K}^k$.

For positive integers k, m, ℓ with $1 \leq m, \ell \leq k$, and $m + \ell \geq k$, and a partition $E = E_1 \cup E_2$ of the ground set with $|E_1| \geq m$ and $|E_2| \geq \ell$, the independent sets of the biuniform matroid of rank k and subranks m, ℓ are all the subsets B of the ground set with the property that $|B| \leq k$, $|B \cap E_1| \leq m$, and $|B \cap E_2| \leq \ell$. Since the maximal independent subsets of E_1 have m elements, $r(E_1) = m$. Similarly, $r(E_2) = \ell$.

If the biuniform matroid is representable over a field $\mathbb{K}$, then there is a map

$$f \ : \ E \to \ \mathbb{K}^k$$

such that $f(E)$ is a set of vectors with the property that every subset D of $f(E)$ of size k with $|D \cap f(E_1)| \leq m$ and $|D \cap f(E_2)| \leq \ell$ is a basis of $\mathbb{K}^k$. The dimensions of $\langle f(E_1)\rangle$ and $\langle f(E_2)\rangle$ are $m = r(E_1)$ and $\ell = r(E_2)$, respectively. Thus, if the biuniform matroid is representable over $\mathbb{K}$, then we can construct a set $S \cup T$ of vectors of $\mathbb{K}^k$ such that $\dim(\langle S\rangle) = m$ and $\dim(\langle T\rangle) = \ell$ with the property that every subset B of $S \cup T$ of size k with $|B \cap S| \leq m$ and $|B \cap T| \leq \ell$ is a basis.

4. Necessary conditions.

We present here some necessary conditions for a biuniform matroid to be representable over a finite field $\mathbb{F}_q$.

The following lemma implies that restricting a representation of the biuniform matroid on $E = E_1 \cup E_2$, one gets a representation of the uniform matroid on E_1 of rank m and the uniform matroid on E_2 of rank ℓ. Therefore, the known necessary conditions for the representability of the uniform matroid over $\mathbb{F}_q$ can be applied to the biuniform matroid.

LEMMA 4.1. *If f is a map from E to $\mathbb{K}^k$ which gives a representation of the biuniform matroid of rank k and subranks m and ℓ, then $f(E_1)$ has the property that every subset of $f(E_1)$ of size m is a basis of $\langle f(E_1)\rangle$. Similarly, $f(E_2)$ has the property that every subset of $f(E_2)$ of size ℓ is a basis of $\langle f(E_2)\rangle$.*

Proof. If L' is a set of m vectors of $f(E_1)$ which are linearly dependent, then $L' \cup L$, where L is a set of $k - m$ vectors of $f(E_2)$, is a set of k vectors of $f(E)$ which do not form a basis of $\mathbb{K}^k$. □

The *dual* of a matroid M is the matroid M^* on the same ground set such that its bases are the complements of the bases of M. Given a representation of M over $\mathbb{K}$, simple linear algebra operations provide a representation of M^* over the same field [16, section 2.2]. In particular, if $\mathbb{K}$ is finite, a representation of M^* can be efficiently obtained from a representation of M. By the following proposition, the dual of a biuniform matroid is a biuniform matroid with the same partition of the ground set.

PROPOSITION 4.2. *The dual of the biuniform matroid of rank k and subranks m and ℓ on the ground set $E = E_1 \cup E_2$ is the biuniform matroid of rank $k^* = |E_1| + |E_2| - k$ and subranks $m^* = |E_1| + \ell - k$ and $\ell^* = |E_2| + m - k$.*

Proof. Clearly, a matroid and its dual have the same automorphism group. This implies that the dual of a biuniform matroid is biuniform for the same partition of the ground set. The values for the rank and the subranks of M^* are derived from the formula that relates the rank function r of matroid M to the rank function r^* of its dual M^*. Namely, $r^*(A) = |A| - r(E) + r(E \setminus A)$ for every $A \subseteq E$ [16, Proposition 2.1.9]. □

Clearly, $k = m = \ell$ if and only if $m^* = |E_1|$ and $\ell^* = |E_2|$, and in this case both M and M^* are uniform matroids. We assume from now on that $m < k$ or $\ell < k$ and that $m < |E_1|$ or $\ell < |E_2|$,

The results in this paper indicate that the value $d = m + \ell - k$, which is equal to the dimension of $\langle S\rangle \cap \langle T\rangle$, is maybe the most influential parameter when studying the representability of the biuniform matroid over finite fields. Observe that the value of this parameter is the same for a biuniform matroid M and for its dual M^*. If $d = 0$, then the problem reduces to the representability of the uniform matroid. Similarly, if $d = 1$, then, by adding to $S \cup T$ a nonzero vector in the one-dimensional intersection of $\langle S\rangle$ and $\langle T\rangle$, the problem again reduces to the representability of the uniform matroid. From now on, we assume that $d = m + \ell - k \geq 2$.

PROPOSITION 4.3. *If $k \leq m + \ell - 2$ and the biuniform matroid of rank k and subranks m, ℓ is representable over $\mathbb{F}_q$, then $|E| \leq q + k - 1$.*

Proof. Take a subset A of S of size $k - \ell$. Then $\langle A\rangle \cap \langle T\rangle = \{0\}$ because $A \cup C$ is a basis for every subset C of T of size ℓ. Since $k - \ell \leq m - 2$, we can project the points of $S \setminus A$ onto $\langle S\rangle \cap \langle T\rangle$, by defining A' to be a set of $|S| - (k - \ell)$ vectors, each a representative of a distinct one-dimensional subspace $\langle x, A\rangle \cap (\langle S\rangle \cap \langle T\rangle)$ for some $x \in (S \setminus A)$.

Let B be a subset of T of size $\ell - 2$. For all $x \in A'$, if $\langle B, x\rangle$ contains $\ell - 1$ points of T, then $\langle A, B, x\rangle$ is a hyperplane of $\mathbb{F}_q^k$ containing k points of $S \cup T$, at most $m - 1$ points of S, and $\ell - 1$ points of T. This cannot occur since such a set must be a basis, by hypothesis.

Thus, each of the $q + 1$ hyperplanes containing $\langle B\rangle$ contains at most one vector of $A' \cup (T \setminus B)$. This gives $|T| - (\ell - 2) + |S| - (k - \ell) \leq q + 1$, which gives the desired bound, since $E = S \cup T$. □

PROPOSITION 4.4. *If $q \leq k \leq m + \ell - 2$, then the biuniform matroid is not representable over $\mathbb{F}_q$.*

Proof. Assume that the biuniform matroid is representable and we have the sets of vectors S and T as before. Let $e_1, \dots, e_m$ be vectors of S. These vectors form a basis for $\langle S\rangle$ and we can extend them with $k - m$ vectors $e_{m+1}, \dots, e_k$ of T to a basis of $\langle S, T\rangle$. For every vector in T that is not in the basis $\{e_1, \dots, e_k\}$, all its coordinates in this basis are nonzero. Indeed, if there is such a vector with a zero coordinate in the $i \geq m + 1$ coordinate, then the hyperplane $X_i = 0$ contains m vectors of S and $k - m$ vectors of T, which does not occur. Similarly, if the zero coordinate is in the $i \leq m$ coordinate, then the hyperplane $X_i = 0$ contains $m - 1$ vectors of S and $k - m + 1$ vectors of T, which also does not occur. Thus, by multiplying the vectors in the basis by some nonzero scalars, we can assume that $e_1 + \cdots + e_k$ is a vector of T and all the coordinates of the other vectors in $T \setminus \{e_{m+1}, \dots, e_k\}$ are nonzero.

Since $\ell \geq k - m + 2$, there is a vector $z \in T \setminus \{e_{m+1}, \dots, e_k, e_1 + \cdots + e_k\}$. Since $k \geq q$ there are coordinates i and j such that $z_i = z_j$. If $1 \leq i \leq m$ and $1 \leq j \leq m$, then the hyperplane $X_i = X_j$ contains $m - 2$ vectors of S and $k - m + 2 \leq \ell$ vectors of T, which cannot occur. If $1 \leq i \leq m$ and $m + 1 \leq j \leq k$, then the hyperplane $X_i = X_j$ contains $m - 1$ vectors of S and $k - m + 1$ vectors of T, which also cannot occur. Finally, if $m + 1 \leq i \leq k$ and $m + 1 \leq j \leq k$, then the hyperplane $X_i = X_j$ contains m vectors of S and $k - m$ vectors of T, which cannot occur, a contradiction. □

5. Representations of the biuniform matroid.

THEOREM 5.1. *The biuniform matroid of rank k and subranks m and ℓ with $d = m+\ell-k = 2$ is representable over $\mathbb{F}_q$ if q is odd and* $\max\{|E_1|, |E_2|\} \le (q-1)/2$.

Proof. Let L denote the set of nonzero squares of $\mathbb{F}_q$ and $(-1)^{\ell+m}\eta$ a fixed nonsquare of $\mathbb{F}_q$. Consider the subsets of $\mathbb{F}_q^k$

$$S = \{(t, t^2, \dots, t^{m-2}, 1, t^{m-1}, 0, \dots, 0) \mid t \in L\}$$

and

$$T = \{(0, \dots, 0, \eta, t^{\ell-1}, t^{\ell-2}, \dots, t) \mid t \in L\},$$

where the coordinates are with respect to the basis $\{e_1, \dots, e_k\}$. We prove in the following that any injective map which maps the elements of E_1 to a subset of S and the elements of E_2 to a subset of T is a representation of the biuniform matroid.

Since every set of $S \cup \{e_{m-1}, e_m\}$ of size m is a basis of $\langle S\rangle$, every set formed by $m-2$ vectors in S and ℓ vectors in T is a basis. Symmetrically, the same holds for every m vectors in S and $\ell-2$ vectors in T.

The proof is concluded by showing that there is no hyperplane H of $\mathbb{F}_q^k$ containing $m-1$ points of S and $\ell-1$ points of T. Suppose that, on the contrary, such a hyperplane H exists. Since $S \cup A$ span $\mathbb{F}_q^k$ for every $A \subseteq T$ of size $\ell-2$, the hyperplane H intersects $\langle S\rangle$ in an $(m-1)$-dimensional subspace. Symmetrically, $H \cap \langle T\rangle$ has dimension $\ell-1$. Therefore, H intersects $\langle e_{m-1}, e_m\rangle = \langle S\rangle \cap \langle T\rangle$ in a one-dimensional subspace. Take elements a_1 and a_2 of $\mathbb{F}_q$, not both zero, with $a_1 e_{m-1} + a_2 e_m \in H$. The $m-1$ vectors of $H \cap S$ together with $a_1 e_{m-1} + a_2 e_m$ are linearly dependent. Thus, there are $m-1$ different elements $t_1, \dots, t_{m-1}$ of L such that

$$\det\left(\sum_{i=1}^{m-2} t_1^i e_i + e_{m-1} + t_1^{m-1} e_m, \dots, \sum_{i=1}^{m-2} t_{m-1}^i e_i \right.$$
$$\left. + e_{m-1} + t_{m-1}^{m-1} e_m, a_1 e_{m-1} + a_2 e_m\right) = 0.$$

Expanding this determinant by the last column gives

$$a_2(-1)^m V(t_1, \dots, t_{m-1}) = a_1 V(t_1, \dots, t_{m-1}) \prod_{i=1}^{m-1} t_i,$$

where $V(t_1, \dots, t_{m-1})$ is the determinant of the Vandermonde matrix. Since $a_1 = 0$ implies $a_2 = 0$, we can assume that $a_1 \neq 0$ and so $a_2 a_1^{-1}(-1)^m \in L$. Analogously, the $\ell-1$ vectors of $H \cap T$ together with $a_1 e_{m-1} + a_2 e_m$ are linearly dependent, and hence there are $\ell-1$ elements $u_1, \dots, u_{\ell-1}$ of L such that

$$\det\left(\eta e_{m-1} + \sum_{i=1}^{\ell-1} u_1^i e_{k+1-i}, \dots, \eta e_{m-1} + \sum_{i=1}^{\ell-1} u_{\ell-1}^i e_{k+1-i}, a_1 e_{m-1} + a_2 e_m\right) = 0.$$

Expanding this determinant by the last column gives

$$\eta a_2 (-1)^\ell V(u_1, \dots, u_{\ell-1}) = a_1 V(u_1, \dots, u_{\ell-1}) \prod_{i=1}^{\ell-1} u_i.$$

Since $a_1 = 0$ implies $a_2 = 0$, we can assume that $a_1 \neq 0$ and so $\eta a_2 a_1^{-1}(-1)^\ell \in L$, and since $a_2 a_1^{-1}(-1)^m \in L$, this gives $\eta(-1)^{\ell+m} \in L$. However, η was chosen so that this is not the case. ▯

We describe in the following a family of linear evaluation codes that will provide different representations of the biuniform matroid for all possible values of the rank k and the subranks m, ℓ. Take $\beta \in \mathbb{F}_q$ and the subspace V of $\mathbb{F}_q[x] \times \mathbb{F}_q[y]$ defined by

$$V = \{(f(x), g(y)) \mid f(x) = f_1(x) + x^{m-d} g_1(\beta x),\ g(y) = g_1(y) + y^d g_2(y),$$
$$\deg(f_1) \leq m-d-1,\ \deg(g_1) \leq d-1,\ \deg(g_2) \leq \ell - d - 1\},$$

where $d = m + \ell - k$. Let $F_1 = \{x_1, \ldots, x_{N_1}\}$ and $F_2 = \{y_1, \ldots, y_{N_2}\}$ be subsets of $\mathbb{F}_q \setminus \{0\}$, where $N_1 = |E_1|$ and $N_2 = |E_2|$. Define $C = C(F_1, F_2, \beta)$ to be the linear evaluation code

$$C = \{((f(x_1), \ldots, f(x_{N_1}), g(y_1), \ldots, g(y_{N_2})) \mid (f, g) \in V\}.$$

Note that $\dim C = \dim V = m - d + \ell - d + d = k$.

Every linear code determines a matroid, namely, the one that is represented by the columns of a generator matrix G, which is the same for all generator matrices of the code. We analyze now under which conditions the code $C = C(F_1, F_2, \beta)$ provides a representation over $\mathbb{F}_q$ of the biuniform matroid by identifying E_1 and E_2 to F_1 and F_2, respectively (that is, to the first N_1 columns and the last N_2 columns of G, respectively).

Clearly, for every $A \subseteq E$ with $|A \cap E_1| > m$ or $|A \cap E_2| > \ell$, the corresponding columns of G are linearly dependent.

Let B be a basis of the biuniform matroid with $|B \cap E_1| = m - t_1$ and $|B \cap E_2| = \ell - t_2$, where $0 \leq t_i \leq d$ and $t_1 + t_2 = d$. We can assume that $B \cap E_1$ is mapped to $\{x_1, \ldots, x_{m-t_1}\} \subseteq F_1$ and $B \cap E_2$ is mapped to $\{y_1, \ldots, y_{\ell - t_2}\} \subseteq F_2$. The corresponding columns of G are linearly independent if and only if $(f, g) = (0, 0)$ is the only element in V satisfying

$$(f(x_1), \ldots, f(x_{m-t_1}), g(y_1), \ldots, g(y_{\ell-t_2})) = 0. \tag{5.1}$$

Let

$$r(x) = (x - x_1) \cdots (x - x_{m-t_1}) = \sum_{i=0}^{m-t_1} r_i x^i$$

and

$$s(y) = (y - y_1) \cdots (y - y_{\ell - t_2}) = \sum_{i=0}^{\ell - t_2} s_i y^i.$$

Then $(f, g) \in V$ satisfy (5.1) if and only if $f(x) = a(x) r(x)$ for some polynomial $a(x) = \sum_{i=0}^{t_1 - 1} a_i x^i$ and $g(y) = b(y) s(y)$ for some polynomial $b(y) = \sum_{i=0}^{t_2-1} b_i y^i$. Since $f(x) = a(x) r(x) = f_1(x) + x^{m-d} g_1(\beta x)$,

$$g_1(\beta x) = \sum_{i=0}^{t_1 - 1} a_i \left(\sum_{j=0}^{d - t_1 + i} r_{m-d+j-i}\, x^j \right),$$

where $r_j = 0$ if $j < 0$. On the other hand, $g(y) = b(y)s(y) = g_1(y) + y^d g_2(y)$ and so

$$g_1(y) = \sum_{i=0}^{t_2-1} b_i \left(\sum_{j=i}^{d-1} s_{j-i}\, y^j \right),$$

where $s_j = 0$ if $j > \ell - t_2$. Hence,

$$\sum_{i=0}^{t_1-1} a_i \left(\sum_{j=0}^{d-t_1+i} r_{m-d+j-i}\, x^j \right) = \sum_{i=0}^{t_2-1} b_i \left(\sum_{j=i}^{d-1} s_{j-i} (\beta x)^j \right). \tag{5.2}$$

If $(f, g) \neq 0$, then either a or b is nonzero and so there is a linear dependence between the d polynomials in (5.2). Therefore, the determinant of the $d \times d$ matrix

(5.3)

$$\left(\begin{array}{ccccccccc}
r_{m-d} & r_{m-d+1} & \cdots & \cdots & \cdots & r_{m-t_1} & 0 & \cdots & 0 \\
r_{m-d-1} & r_{m-d} & \cdots & \cdots & \cdots & \cdots & r_{m-t_1} & \cdots & 0 \\
\vdots & \vdots & & & & & & \ddots & \vdots \\
 & & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & r_{m-t_1} \\
\hline
s_0 & s_1\beta & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\
0 & s_0\beta & s_1\beta^2 & \cdots & \cdots & \cdots & \cdots & \cdots & \\
\vdots & \ddots & \ddots & \ddots & & & & & \vdots \\
0 & \cdots & 0 & s_0\beta^{t_2-2} & s_1\beta^{t_2-1} & \cdots & \cdots & \cdots & s_{t_1+1}\beta^{d-1} \\
0 & \cdots & \cdots & 0 & s_0\beta^{t_2-1} & s_1\beta^{t_2} & \cdots & \cdots & s_{t_1}\beta^{d-1}
\end{array} \right)$$

is zero.

In conclusion, the code $C(F_1, F_2, \beta)$ provides a representation over $\mathbb{F}_q$ of the biuniform matroid if and only if the determinant of the matrix (5.3) is nonzero for every choice of $m - t_1$ elements in F_1 and $\ell - t_2$ elements in F_2 with $0 \leq t_i \leq d$ and $t_1 + t_2 = d$. Clearly, this is always the case if $t_1 = 0$ or $t_2 = 0$. Otherwise, that determinant can be expressed as an $\mathbb{F}_q$-polynomial on β. The degree of this polynomial $\varphi(\beta)$ is at most $d(d-1)/2$. In addition, $\varphi(\beta)$ is not identically zero because the term with the minimum power of β is equal to $1\beta \cdots \beta^{t_2-1} s_0^{t_2} r_{m-t_1}^{t_1}$, and $r_{m-t_1} = 1$ and $s_0 \neq 0$. In the next two theorems we present two different ways to select F_1, F_2, β with that property.

THEOREM 5.2. *The biuniform matroid of rank k and subranks m and ℓ with $d = m + \ell - k \geq 2$ is representable over $\mathbb{F}_q$ if $q = q_0^s$ for some $s > d(d-1)/2$ and some prime power $q_0 > \max\{|E_1|, |E_2|\}$. Moreover, such a representation can be obtained in time polynomial in the size of the ground set.*

Proof. Take F_1 and F_2 from $\mathbb{F}_{q_0} \setminus \{0\}$ and take $\beta \in \mathbb{F}_q$ such that its minimal polynomial over $\mathbb{F}_{q_0}$ is of degree s. The algorithm by Shoup [19] finds such a value β in time polynomial in q_0 and s. Then the code $C(F_1, F_2, \beta)$ gives a representation over $\mathbb{F}_q$ of the biuniform matroid. Indeed, all the entries in the matrix (5.3), except the powers of β, are in $\mathbb{F}_{q_0}$. Therefore, $\varphi(\beta)$ is a nonzero $\mathbb{F}_{q_0}$-polynomial on β with degree smaller than s. ▯

Our second construction of a code $C(F_1, F_2, \beta)$ representing the biuniform matroid is done over a prime field $\mathbb{F}_p$. We need the following well-known bound on the roots of a real polynomial.

LEMMA 5.3. *The absolute value of every root of the real polynomial $c_0 + c_1 x + \cdots + c_n x^n$ is at most $1 + \max_{0 \leq i \leq n-1} |c_i|/|c_n|$.*

THEOREM 5.4. *Let M be the biuniform matroid of rank k and subranks m and ℓ with $d = m + \ell - k \geq 2$ and $m \geq \ell$. Take $N = \max\{|E_1|, |E_2|\}$ and $K = \lceil N/2 \rceil + 1$. Then M is representable over $\mathbb{F}_p$ for every prime $p > K^h$, where $h = md(1 + d(d-1)/2)$. Moreover, such a representation can be obtained in time polynomial in the size of the ground set.*

Proof. First, we select the value β and the sets F_1, F_2 among the integers in such a way that the determinant of the real matrix (5.3) is always nonzero. Then we find an upper bound on the absolute value of this determinant. The code $C(F_1, F_2, \beta)$ will represent the biuniform matroid over $\mathbb{F}_p$ if p is larger than that bound.

Consider two sets of nonzero integer numbers F_1, F_2 with $|F_i| = |E_i|$ in the interval $[-(K-1), K-1]$. Take $m - t_1$ values in F_1 and $\ell - t_2$ values in F_2, where $1 \leq t_i \leq d-1$ and $t_1 + t_2 = d$. Then the values r_i appearing in the matrix (5.3) satisfy

$$|r_{m-t_1-i}| \leq \binom{m-t_1}{i}(K-1)^i$$

for every $i = 0, \ldots, m - t_1$, and hence $\sum_{i=0}^{m-t_1} |r_i| \leq K^{m-t_1}$. Analogously, $\sum_{i=0}^{\ell-t_2} |s_i| \leq K^{\ell-t_2}$. Since $r_{m-t_1} = s_{\ell-t_2} = 1$ and $m \geq \ell$, all values $|r_i|$, $|s_j|$ are less than or equal to $K^m - 1$. Then $\varphi(\beta)$ is a real polynomial on β with degree at most $d(d-1)/2$ such that the absolute value of every coefficient is at most $(K^m - 1)^d < K^{md} - 1$. Take $\beta = K^{md}$. By Lemma 5.3, $\varphi(\beta) \neq 0$. Moreover,

$$|\varphi(\beta)| \leq (K^m - 1)^d \, \frac{\beta^{d(d-1)/2+1} - 1}{\beta - 1} < K^h.$$

Finally, consider a prime $p > K^h$ and reduce $\beta = K^{md}$ and the elements in F_1 and F_2 modulo p. The code $C(F_1, F_2, \beta)$ represents the biuniform matroid M over $\mathbb{F}_p$. Observe that the number of bits that are needed to represent the elements in $\mathbb{F}_p$ is polynomial in the size of the ground set. □

REFERENCES

[1] S. BALL, *On sets of vectors of a finite vector space in which every subset of basis size is a basis*, J. Eur. Math. Soc. (JEMS), 14 (2012), pp. 733–748.

[2] A. BEIMEL, T. TASSA, AND E. WEINREB, *Characterizing ideal weighted threshold secret sharing*, SIAM J. Discrete Math., 22 (2008), pp. 360–397.

[3] A. BEUTELSPACHER AND F. WETTL, *On 2-level secret sharing*, Des. Codes Cryptogr., 3 (1993), pp. 127–134.

[4] E. F. BRICKELL, *Some ideal secret sharing schemes*, J. Combin. Math. Combin. Comput., 9 (1989), pp. 105–113.

[5] O. FARRÀS, J. MARTÍ-FARRÉ, AND C. PADRÓ, *Ideal multipartite secret sharing schemes*, J. Cryptology, 25 (2012), pp. 434–463.

[6] O. FARRÀS AND C. PADRÓ, *Ideal secret sharing schemes for useful multipartite access structures*, in Proceedings of the International Workshop on Coding and Cryptology IWCC2011, Lecture Notes in Comput. Sci. 6639, Y. M Chee, Z. Guo, S. Ling, F. Shao, Y. Tang, H. Wang, and C. Xing, eds., Springer, Heidelberg, 2011, pp. 99–108.

[7] O. FARRÀS AND C. PADRÓ, *Ideal hierarchical secret sharing schemes*, IEEE Trans. Inform. Theory, 58 (2012), pp. 3273–3286.

[8] O. FARRÀS, C. PADRÓ, C. XING, AND A. YANG, *Natural generalizations of threshold secret sharing*, in Advances in Cryptology, Asiacrypt 2011, Lecture Notes in Comput. Sci. 7073, D. H. Lee and X. Wang, eds., Springer, Heidelberg, 2011, pp. 610–627.

[9] J. GEELEN, J. OXLEY, D. VERTIGAN, AND G. WHITTLE, *Weak maps and stabilizers of classes of matroids*, Adv. in Appl. Math., 21 (1998), pp. 305–341.

[10] J. HERRANZ AND G. SÁEZ, *New results on multipartite access structures*, IET Proceedings of Information Security, 153 (2006), pp. 153–162.

[11] J. W. P. Hirschfeld and L. Storme, *The packing problem in statistics, coding theory and finite projective spaces: Update* 2001, in Developments in Mathematics, Vol. 3, Finite Geometries, Proceedings of the Fourth Isle of Thorns Conference, Kluwer Academic, Norwell, MA, pp. 201–246.

[12] J. Martí-Farré and C. Padró, *On secret sharing schemes, matroids and polymatroids*, J. Math. Cryptol., 4 (2010), pp. 95–120.

[13] S. L. Ng, *A representation of a family of secret sharing matroids*, Des. Codes Cryptogr., 30 (2003), pp. 5–19.

[14] S. L. Ng, *Ideal secret sharing schemes with multipartite access structures*, IEE Proc. Commun., 153 (2006) pp. 165–168.

[15] S. L. Ng and M. Walker, *On the composition of matroids and ideal secret sharing schemes*, Des. Codes Cryptogr. 24 (2001), pp. 49–67.

[16] J. G. Oxley, *Matroid Theory*, Oxford University Press, New York, 1992.

[17] C. Padró and G. Sáez, *Secret sharing schemes with bipartite access structure*, IEEE Trans. Inform. Theory, 46 (2000), pp. 2596–2604.

[18] A. Shamir, *How to share a secret*, Commun. ACM, 22 (1979), pp. 612–613.

[19] V. Shoup, *New algorithms for finding irreducible polynomials over finite fields*, Math. Comp., 54 (1990), pp. 435–447.

[20] G. J. Simmons, *How to (really) share a secret*, in Advances in Cryptology, CRYPTO'88, Lecture Notes in Comput. Sci. 403, S. Goldwasser, ed., Springer, Heidelberg, 1990, pp. 390–448.

[21] T. Tassa, *Hierarchical threshold secret sharing*, J. Cryptology, 20 (2007), pp. 237–264.

[22] T. Tassa and N. Dyn, *Multipartite secret sharing by bivariate interpolation*, J. Cryptology, 22 (2009), pp. 227–258.