COMBINATORICA
Bolyai Society – Springer-Verlag

COMBINATORICA **26** (3) (2006) 353–377

SYMPLECTIC SPACES AND EAR-DECOMPOSITION OF MATROIDS

BALÁZS SZEGEDY, CHRISTIAN SZEGEDY

Received September 3, 1999
Revised February 16, 2005

Matroids admitting an odd ear-decomposition can be viewed as natural generalizations of factor-critical graphs. We prove that a matroid representable over a field of characteristic 2 admits an odd ear-decomposition if and only if it can be represented by some space on which the induced scalar product is a non-degenerate symplectic form. We also show that, for a matroid representable over a field of characteristic 2, the independent sets whose contraction admits an odd ear-decomposition form the family of feasible sets of a representable Δ-matroid.

1. Introduction

The aim of this paper is to give new insights into the algebraic structures underlying matching theory, especially the structure of factor-critical graphs and the related ear-matroid introduced by A. Frank and Z. Szigeti in [2], [11] and [12]. We also show that some important results can be generalized from graphs to matroids representable over a field of characteristic 2.

Inherent connections between matching theory and algebra were already recognized by Tutte, who proved his famous characterization of perfectly matchable graphs in [14] using the Tutte-matrix. More recent examples of using similar techniques is L. Lovász's algebraic description of matroid-parity in [9], W. Cunninghams and J. Geelens [3] work on the path-matching problem.

F. Jaeger observed in [5] and [6] that some fundamental properties of graphs and binary matroids, such as bipartiteness, Eulerianness, graphic-

Mathematics Subject Classification (2000): 05C70, 05C50, 05C85 ness or planarity, can be characterized in terms of symmetric representations over GF(2). We give a similar characterization for the factor-criticality: a graph is factor-critical if and only if its cycle matroid can be represented by an alternating projection matrix. This is a more subtle result than the above characterizations, since we cannot restrict ourselves to binary presentations, but must consider arbitrary ground fields of characteristic 2. There are examples of ear-matroids of binary spaces (or even of graphs) that do not have binary representations.

An equivalent and more generic reformulation of the above criterion is: a bridgeless graph is factor critical if and only if its cycle matroid can be represented by a space (over fields of characteristic 2) on which the induced scalar product is a non-degenerate symplectic form.

A novel algabraic method in our treatment is the symplectification of spaces. This allows for constructing a new representation of the matroid, the induced scalar product on which is a symplectic bilinear form. We will show that the bicycle space of the symplectified representation holds important combinatorical information: the bases of its matroid are those minimal edge sets whose contraction results in a factor-critical graph (or matroid, in the general case). This also proves the result conjectured by A. Frank in [2] and first proved by Z. Szigeti in [12]. The proof presented here is basically different. It works for matroids representable over some field of characteristic 2 (instead of graphs) and also yields an explicit representation of the matroid in question.

This result will be further generalized in the following way: those edge sets whose contraction results in a factor-critical graph (or matroid) form the feasible sets of a representable delta-matroid. In fact, we will prove that a submatrix of the projection matrix on the bicycle space of some suitable subdivision of the symplectified cutset space (or simply representing space, in the case of matroids) represents this delta-matroid.

It is worth noting, that in general the matroid of the bicycle space (even its rank) depends on the chosen representation. The above results show that the matroid of the bicycle space of a symplectified representation is uniquely determined by the matroid.

2. Factor-criticality and ear-decomposition

Let $G=(V,E)$ be a graph with vertex set V and edge set E. Throughout the paper we allow loops and multiple edges in G. A *matching* of G is a subset of E consisting of non-loop edges such that no vertex of G is covered by more than one edge. A *perfect matching* or 1-*factor* of G is a matching that covers all vertices of G. A graph G is called *factor-critical* if the subgraph obtained by removal of any vertex has a perfect matching. A simple parity argument shows that factor critical graphs are 2-edge-connected.

An *ear-decomposition* D of a graph G is a sequence $(G_0,\dots,G_k=G)$ of graphs such that G_0 is the one-point graph and G_{i+1} is constructed from G_i by adding a simple path (ear) between two points of G_i such that the other vertices of the path are not in the vertex set of G_i. We denote by $e(D)$ the number of ears with an even number of edges in an ear-decomposition D and by $\varphi(G)$ the minimum of $e(D)$ over all ear-decompositions D of G. Note that if G is 2-edge-connected then it has at least one ear-decomposition. An ear-decomposition D is called *optimal* if $e(D)=\varphi(G)$. One of the basic properties of φ is that inserting new edges parallel to an existing edge of G does not alter its value. It is obvious that each connected graph can be made 2-edge-connected by applying some such operations. So we can define φ for an arbitrary connected graph G by letting $\varphi(G)\overset{\text{def}}{=}\varphi(G')$ for some graph G' extended this way. For an unconnected graph G we define $\varphi(G)$ to be the sum of $\varphi(C)$ over all components C of G.

The following theorem connects factor-criticality with ear-decompositions:

Theorem 2.1 **(Lovász [8]).** *A connected graph G is factor-critical if and only if $\varphi(G)=0$.*

Corollary 2.2. *A connected graph G is factor-critical if and only if G can be obtained from the one-point graph K_1 by using the following operations:*

1. *Add a new edge between two existing (not necessarily different) vertices.*
2. *Replace an edge by a path of length 3.*

The second operation is called *double subdivision* of an edge.

The reader is assumed to be familiar with the basics of matroid theory and we will use the standard notation introduced in [15].

Let M be a matroid with edge set E. An ear-decomposition of M is a sequence of circuits $C_0,C_1,\dots,C_k$ of M with the following properties:

1. $C_i\setminus(\cup_{j=0}^{i-1}C_j)$ is not empty for all $1\le i\le k$
2. $C_i\cap(\cup_{j=0}^{i-1}C_j)$ is not empty for all $1\le i\le k$
3. $C_i\setminus(\cup_{j=0}^{i-1}C_j)$ is a circuit in $M/(\cup_{j=0}^{i-1}C_j)$ for all $1\le i\le k$
4. $\cup_{j=0}^{k}C_j=E$.

The sets $C_i\setminus(\cup_{j=0}^{i-1}C_j)$ and the set C_0 are called *ears*. An ear is said to be odd (resp. even) if it consists of odd (resp. even) number of edges. We say that D is an *odd ear-decomposition* if all ears occurring in D are odd. Let M be a connected, bridgeless matroid. Similarly to graphs, we denote by $\varphi(M)$ the minimal possible value of the number of even ears in an ear-decomposition of M. If M is bridgeless but not connected, we define $\varphi(M)$ to be the sum of $\varphi(K)$ over all blocks K of M. In particular $\varphi(M)=0$ if and only if every block of M has an odd ear-decomposition.

Lemma 2.3. *Let M be a bridgeless matroid. Then $\varphi(M)=0$ if and only if the edge set of M can be partitioned into sets $E_0,E_1,\dots,E_k$ with an odd number of edges in each of them such that E_0 is a circuit and E_i is a circuit in $M/\left(\cup_{j=0}^{i-1}E_j\right)$.* ∎

In other words, $\varphi(M)=0$ if and only if the edge set of M can be eliminated by a process in which we contract an odd circuit in each step.

Definition 2.4. The bridgeless matroid M is defined to be *factor-critical* if $\varphi(M)=0$.

3. (E,F)-spaces

We will extensively use the notion of (E,F)-*spaces*. Let F be an arbitrary field and let E be a finite set. We call a subspace $U\subseteq F^E$ an (E,F)-space and we refer to the elements of E as *edges*. A *generating matrix* of an (E,F)-space U is a matrix over F such that its columns are indexed by the elements of E and its rows generate U. We call a generating matrix *minimal* if its rows are linearly independent. It is well-known that the column matroid of a generating matrix is uniquely determined by the space. So we can associate this matroid $\mathcal{M}(U)$ with the space U itself. Let $S\subseteq E$ be a subset of the edge set and $u\in U$ be a vector. We denote by $u_S\in F^E$ the vector that we obtain by setting to zero all components of u which correspond to edges in S. Let $u|_S\in F^S$ denote the vector that comes from u by omitting the components of u that are not in S. We will use the induced scalar product $\langle x,y\rangle \overset{\text{def}}{=} \sum x_e y_e$ on F^E and we denote by $U^\perp$ the orthogonal subspace of U with respect to this scalar product in F^E. Space U is called symplectic if $\langle x,x\rangle=0$ for all $x\in U$. Obviously, a bilinear form f is symplectic, if and only if $f(x,y)=x^tAy$ where A is an *alternating matrix*, i.e. a skew-symmetric matrix with zero diagonal entries. The condition on the diagonal entries is interesting for fields of characteristic 2. In this case, skew-symmetricity is equivalent to symmetricity.

For a vector $u\in U$ let $\operatorname{supp} u\subseteq E$ denote the set of indices of non-zero components of u and let $\operatorname{supp} U \overset{\text{def}}{=} \bigcup_{u\in U} \operatorname{supp} u$. Note that $\operatorname{supp} U$ consists exactly of the non-loop elements of $\mathcal{M}(U)$. The characteristic vector of set $S\subseteq E$ in F^E will be denoted by χ_S. We will make use of the following well known facts:

Lemma 3.1. *Let U be an (E,F)-space. Edge $e\in E$ is a bridge in $\mathcal{M}(U)$ if and only if $\chi_e\in U$.* ▮

Let M be an arbitrary matroid with edge set E and let $C(e)$ denote the set of all circuits containing an edge $e\in E$. We say that e and e' are in the same *series class* if $C(e)=C(e')$.

Lemma 3.2. *Let U be an (E,F)-space. Then two edges e and e' are in the same series class if and only if $\chi_e+a\chi_{e'}\in U$ for some $0\neq a\in F$.* ▮

We will also use the following notation:

$$U/S \overset{\text{def}}{=} \left\{u|_{E\setminus S} \in F^{E\setminus S} \mid \operatorname{supp} u \subseteq E\setminus S\right\} \text{ and}$$
$$U\setminus S \overset{\text{def}}{=} \left\{u|_{E\setminus S} \in F^{E\setminus S} \mid u\in U\right\}.$$

Note that both U/S and $U\setminus S$ are $(E\setminus S,F)$ spaces.

The following well-known formulas will also prove useful.

Proposition 3.3.

$$\mathcal{M}(U\setminus S)=\mathcal{M}(U)\setminus S\ ,\ \mathcal{M}(U/S)=\mathcal{M}(U)/S\ ,\ \mathcal{M}(U^\perp)=\mathcal{M}^*(U).$$
$$U/S\subseteq U\setminus S\ ,\ (U\setminus S)^\perp=U^\perp/S\ ,\ (U/S)^\perp=U^\perp\setminus S$$
$$(U\cap V)/S=(U/S)\cap(V/S)\ ,\ (U\cap V)\setminus S\subseteq(U\setminus S)\cap(V\setminus S).$$ ▮

We will use the shorthand notation U/e and $U\setminus e$ for $U/\{e\}$ and $U\setminus\{e\}$, respectively.

We call a subset S of the edge set of a graph a *cut* or a *cutset* if there is a bipartition of the vertex set of G so that S is the set of edges having an incident vertex on both sides of the bipartition. For example, $\emptyset$ is a cut of every graph. The set of characteristic vectors of all cuts of a graph $G=(V,E)$ over GF(2) is an $(E,\mathrm{GF}(2))$-space $S(G)$, called the *cutset space of* G. It is well-known that $\mathcal{M}(S(G))$ is the cycle-matroid of G.

4. The bicycle space of an (E,F)-space

Let U be an (E,F)-space. We define the *bicycle space* $\mathcal{B}(U)$ of U by $\mathcal{B}(U)\overset{\text{def}}{=}U\cap U^\perp$ and $\beta(U)$ will denote its dimension. The following lemma describes how to determine $\beta(U)$ in terms of a generating matrix of U, the straightforward proof of which is left to the reader:

Lemma 4.1. *Let G be a generating matrix of an (E,F)-space U. Then $\beta(U)=\dim(U)-\mathrm{rk}(GG^T)$. If G is minimal then U is bicycle free if and only if det$(GG^T)\neq 0$.* ∎

Note that $\mathcal{B}(U)=0$ means that the scalar product induced on U is non-degenerate.

Lemma 4.2. *If U is an (E,F)-space and $S\subseteq E$, then:*

1. $\mathcal{B}(U)/S\subseteq\mathcal{B}(U/S)$,
2. $e\in\operatorname{supp}\mathcal{B}(U)\Longrightarrow\mathcal{B}(U/e)=\mathcal{B}(U)/e$.

Proof. The first statement is an immediate consequence of the formulas of Proposition 3.3:

$$\mathcal{B}(U)/S=(U\cap U^{\perp})/S=(U/S)\cap(U^{\perp}/S)\subseteq(U/S)\cap(U^{\perp}\setminus S)=\mathcal{B}(U/S).$$

The inclusion $\mathcal{B}(U)/e\subseteq\mathcal{B}(U/e)$ from the second statement follows from the first statement. To prove the other inclusion, take an arbitrary vector $v\in\mathcal{B}(U/e)$. By definition, there is a vector v_1 in U such that the e component of v_1 is 0 and the restriction of v_1 to $E\setminus\{e\}$ is v. We have to prove that $v_1\in U^{\perp}$. Assume the contrary, $v_1\notin U^{\perp}$. Then, since $v\in(U/e)^{\perp}=U^{\perp}\setminus e$, there is a non-zero $\alpha\in F$ such that $v_1+\alpha\chi_e\in U^{\perp}$. So we obtain that $\chi_e\in U+U^{\perp}=\mathcal{B}(U)^{\perp}$, contradicting $e\in\operatorname{supp}\mathcal{B}(U)$. ∎

Theorem 4.3. *Let U be an (E,F)-space and $M\subseteq 2^E$ the family of sets $S\subseteq E$ for which $\dim\mathcal{B}(U/S)=\dim\mathcal{B}(U)-|S|$. Then M is exactly the family of the independent sets of $\mathcal{M}(\mathcal{B}(U))$ and for any $S\in M$, we have $\mathcal{B}(U/S)=\mathcal{B}(U)/S$.*

Proof. First we show that if S is an independent set of $\mathcal{M}(\mathcal{B}(U))$ then $\dim\mathcal{B}(U/S)=\dim\mathcal{B}(U)-|S|$. For $|S|=0$ the statement is trivial. We go by induction on $|S|$. Assume that the statement holds for every $|T|<|S|$ and (E',F)-space V, where E' is an arbitrary finite set. Let e be an element of S. Since e is not a loop of $\mathcal{M}(\mathcal{B}(U))$ we know that $\mathcal{B}(U/e)=\mathcal{B}(U)/e$ by Lemma 4.2. It follows that $\dim\mathcal{B}(U/e)=\dim\mathcal{B}(U)-1$. Now $S\setminus\{e\}$ is an independent set of $\mathcal{B}(U)/e$, and so we can use our induction hypothesis:

$$\begin{aligned}\dim\mathcal{B}(U)/S=\dim\mathcal{B}(U/e)/(S\setminus\{e\})&=\dim\mathcal{B}(U/e)-(|S|-1)\\&=\dim\mathcal{B}(U)-|S|.\end{aligned}$$

This also proves the last statement of the theorem.

For the other direction, assume that $\dim \mathcal{B}(U)/S = \dim \mathcal{B}(U) - |S|$ and S is dependent in $\mathcal{M}(\mathcal{B}(U))$. So there is an $e \in S$ such that e is a loop in $\mathcal{M}(\mathcal{B}(U/(S \setminus \{e\})))$. By Lemma 4.2, this implies

$$\mathcal{B}(U/S) \supseteq \mathcal{B}(U/(S \setminus \{e\}))/e \supseteq \mathcal{B}(U)/(S \setminus \{e\})$$

and so

$$\dim \mathcal{B}(U/S) \geq \dim \mathcal{B}(U)/(S \setminus \{e\}) \geq \dim \mathcal{B}(U) - |S| + 1$$

which is a contradiction. ∎

5. Tools from commutative algebra

Let F be an arbitrary field and U be an (E,F)-space. Associate algebraically independent indeterminates $X \overset{\text{def}}{=} \{x_e \mid e \in E\}$ with the elements of E. Let $I(U)$ be the ideal generated by the set of linear polynomials $\{\sum_{e\in E} v_e x_e \mid v \in U\}$. Then the ring $R_U \overset{\text{def}}{=} F[X]/I(U)$ is again a polynomial ring in $|E| - \operatorname{rk}(\mathcal{M}(U))$ variables. This can be seen in the following way: Let $B \subseteq E$ be a basis of $\mathcal{M}(U)$. We can represent U by a block matrix $M = [I \ A]$, where I is an identity matrix, $A = (a_{e,f})_{\substack{e\in B \\ f \in E\setminus B}}$, the columns of M are indexed by the elements of E (the first $|B|$ columns are indexed by elements of B) and the rows are also indexed by the elements of B.

Proposition 5.1. *Let $Y \subseteq X$ be the set of algebraically independent indeterminates associated with the elements of $E \setminus B$. Then the kernel of the homomorphism of F-algebras $\varphi_B : F[X] \longrightarrow F[Y]$ defined by*

$$\varphi_B(x_e) \overset{\text{def}}{=} \begin{cases} x_e & \text{for } e \in E \setminus B, \\ -\sum\limits_{f\in E\setminus B} a_{e,f} x_f & \text{for } e \in B \end{cases}$$

is $I(U)$ and so it gives an isomorphism between R_U and $F[Y]$.

Proof. Let S be the set of linear polynomials $p_e = x_e + \sum\limits_{f\in E\setminus B} a_{e,f} x_f$ where $e \in B$ and let I be the ideal generated by S. Since the vectors formed by the coefficients of the polynomials p_e generate the space U we have that $I = I(U)$. From $\varphi_B(p_e) = 0$ we obtain that I is contained in the kernel of φ_B. To see the other inclusion let p be an arbitrary polynomial from the kernel of φ_B. The definition of φ_B shows that $x_e - \varphi_B(x_e) \in I$ for all $e \in E$ or in other words $x_e \equiv \varphi_B(x_e)$ modulo I. This means that $g \equiv \varphi_B(g)$ modulo I for all $g \in F[X]$. From $\varphi_B(p) = 0$ we obtain that $p \in I$. ∎

The fact that R_U is a polynomial ring itself will be frequently used throughout the paper. One very important application of it is that R_U is an integral domain so we can do linear algebra over its quotient field. If U and W are both (E,F)-spaces with $U \subseteq W$ then $I(U) \subseteq I(W)$. The homomorphism $F[X]/I(U) \to F[X]/I(W)$ results in a natural ring homomorphism from R_U to R_W. We will need the following Lemma.

Lemma 5.2. *Let U and W be two (E,F)-spaces and let φ be the natural homomorphism from R_U to R_W. Assume that $A=(a_{i,j})$ is an n by m matrix with entries from R_U and let $\varphi(A)=(\varphi(a_{i,j}))$ be its image under the map φ. Then $rk(\varphi(A)) \leq rk(A)$.*

Proof. The rank of a matrix is the size of the largest $r \times r$ sub-matrix with non-zero determinant. If a sub-matrix of A has determinant d then the corresponding sub-matrix in $\varphi(A)$ has determinant $\varphi(d)$. This implies that singular sub-matrices of A are singular in $\varphi(A)$. ∎

Abusing the notation, we identify the variables x_e with their images under various algebra homomorphisms. To avoid confusion, we will always indicate in which algebra we are working. For example $x_e \in R_U$ denotes the image of x_e under the map $F[X] \to R_U$. The proofs of the following two lemmas are left to the reader.

Lemma 5.3. *Let U be an (E,F)-space and let $S \subseteq E$ be an independent set in $\mathcal{M}(U)$. Then there is a unique isomorphism $\varphi: R_{U/S} \to R_U$ with $\varphi(x_e)=x_e$ for all $e \in E \setminus S$.* ∎

Lemma 5.4. *Let U be an (E,F)-space and let S be an arbitrary subset of E. Moreover, let V_S denote the space formed by all $v \in F^E$ with $\operatorname{supp} v \subseteq S$ and let W denote the space spanned by U and V_S. Then there is a unique isomorphism $\varphi: R_{U \setminus S} \to R_W$ with $\varphi(x_e)=x_e$ for all $e \in E \setminus S$.* ∎

We will also make use of the following theorem (see e.g. [7] Chapter V):

Theorem 5.5. *If F is a field then the polynomial ring $F[x_1,\ldots,x_k]$ is a unique factorization domain, i.e. every polynomial can be written as a product of irreducible polynomials, and such factorizations are unique up to multiplication of the factors with some scalars.* ∎

6. A field associated with graphs

Let $G=(V,E)$ be a graph. We denote by GF(2) the field with two elements. Associate algebraically independent indeterminates $X=\{x_e\}_{e \in E}$ over GF(2) with the edges of G. Let I be the ideal in $\mathrm{GF}(2)[X]$ generated by the sums $\sum_{e\in S} x_e$ for all cutsets S of G. In the language used in Section 5 we have that $I=I(U)$ where U is the cutset subspace of G. We define

$$F(G) \overset{\text{def}}{=} Q(\mathrm{GF}(2)[X]/I),$$

where $Q(R)$ denotes the quotient field of ring R. The validity of this definition follows from Proposition 5.1 which shows that $R_U=\mathrm{GF}(2)[X]/I$ is an integral domain. Another consequence of Proposition 5.1 is the following.

Proposition 6.1. *Let $T\subseteq E$ be a spanning forest of G and Y the set of the indeterminates associated with the edges not in T. We denote by $S(T,e)$, for $e\in T$, the cutset induced by the components of $T\setminus\{e\}$ in $G\setminus\{e\}$ (so we have $e\notin S(T,e)$). Then kernel of the* GF(2)*-algebra homomorphism*

$$f : \mathrm{GF}(2)[X] \longrightarrow \mathrm{GF}(2)[Y]$$

defined by

$$f(x_e) = \begin{cases} x_e & \text{for } e \notin T, \\ \sum\limits_{d\in S(T,e)} x_d & \text{for } e \in T \end{cases}$$

is I and so it gives an algebra isomorphism between $\mathrm{GF}(2)[X]/I$ *and* $\mathrm{GF}(2)[Y]$. ∎

The previous statement also implies that the field $F(G)$ is always isomorphic to a function field over GF(2) with corank(G) algebraically independent indeterminates. We could formulate our subsequent results using this explicite function f. This is practical for computing examples or constructing algorithms, but from a theoretic point of view the original definition has the advantage of not depending on the choice of a special tree. Another advantage is that proving theorems will be technically simpler if the indeterminates associated with the edges are treated homogeneously. The next lemma is an immediate consequence of Lemma 5.3.

Lemma 6.2. *Let $G=(V,E)$ be a graph and $T\subseteq E$ be the edge set of a forest of G. Then the map $f : F(G/T) \longrightarrow F(G)$ defined by $f(x_e)=x_e$ is an isomorphism of fields.*

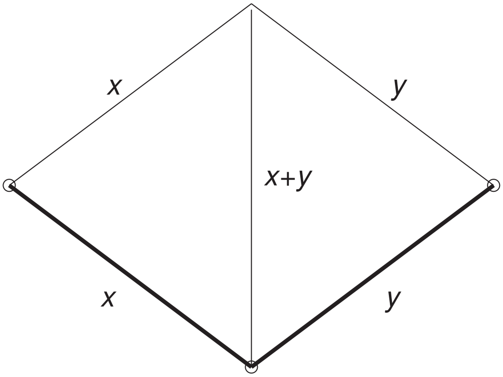
7. Representation of the ear-matroid and its consequences

On the analogy of the incidence matrix of G, let $D(G)=(d_{ev})_{e\in E,v\in V}$ be the $E\times V$ matrix over $F(G)$ defined by

$$d_{ev} \overset{\text{def}}{=} \begin{cases} x_e & \text{if } e \text{ and } v \text{ are incident,} \\ 0 & \text{otherwise.} \end{cases}$$

We define the $V\times V$ matrix $T(G)=(t_{uv})$ over $F(G)$ by $t_{uv} \overset{\text{def}}{=} \sum x_e$ over all edges that connect u and v.

To illuminate the real nature of these matrices, we give a simple example using the above isomorphism given in Proposition 6.1. The graph G on the figure is K_4 with one edge deleted. The subgraph consisting of the two bold arcs is cotree $T'=E\setminus T$. We associate two algebraically independent indeterminates x and y with the bold edges. With each arc e of T we associate the sum of indeterminates associated with the arcs n the interesection of T' and the fundamental cut of e with respect to T.



Now we get the matrices $D(G)$ and $T(G)$:

$$D(G)=\begin{pmatrix} x & y & x+y & 0 & 0 \\ x & 0 & 0 & x & 0 \\ 0 & y & 0 & 0 & y \\ 0 & 0 & x+y & x & y \end{pmatrix}, \qquad T(G)=\begin{pmatrix} 0 & x & y & x+y \\ x & 0 & 0 & x \\ y & 0 & 0 & y \\ x+y & x & y & 0 \end{pmatrix}.$$

Proposition 7.1. *For any graph G, let $T'(G)=(t'_{uv}) \overset{\text{def}}{=} D(G)D(G)^T$. Then $t'_{uv}=(t_{uv})^2$, where t_{uv} denotes the corresponding entry in $T(G)$.*

Proof. Using the identity $(a+b)^2=a^2+b^2$, the equalities for the nondiagonal elements are clear. The diagonal elements of the product are zero because they are equal to $(\sum_{e\in S} x_e)^2=0$ for the star S of the corresponding vertex. ∎

Here is an easy consequence of this:

Proposition 7.2. *For each graph G holds:* $\mathrm{rk}\,(D(G)D(G)^T) = \mathrm{rk}\,(T(G))$, *where the rank of graph G is defined to be the rank of its cycle matroid.*

Proof. This follows from the last proposition, because in the expansion of a subdeterminant each term on the left-hand side is the square of a term in the expansion of the corresponding subdeterminant of the right side, and these terms are in one-to-one correspondence. So using the identity $(a+b)^2 = a^2+b^2$ we can see that each subdeterminant on the left-hand side equals the square of the corresponding subdeterminant on the right-hand side. ∎

It should be mentioned that $x_e \neq 0$ if and only if e is no bridge, so we can easily see that $\mathrm{rk}\,(D(G)) \leq \mathrm{rk}\,(G)$, with equality if G is 2-edge-connected. Denote by $T(G)[U]$ the symmetric submatrix of $T(G)$ induced by the rows and columns associated with the vertices of $U \subseteq V$.

Proposition 7.3. *For each $v \in V$ holds:* $\mathrm{rk}\,(T(G)) = \mathrm{rk}\,(T(G)[V \setminus \{v\}])$.

Proof. This can be seen using the fact that the sum of the rows and the sum of the columns of $T(G)$ are both 0. ∎

The aim of this section is to show that the graph invariant

$$\psi(G) \overset{\mathrm{def}}{=} \mathrm{rk}\,(G) - \mathrm{rk}\,(T(G))$$

is nothing else that $\varphi(G)$ from section 2. Before we can prove it we need some preparation.

Denote by $\mathcal{R}(G)$ the row space of $D(G)$. Obviously, by Lemma 4.1:

Proposition 7.4. $\dim \mathcal{B}(\mathcal{R}(G)) = \psi(G)$. ∎

Lemma 7.5. *If G is a connected graph then*

$$\psi(G) = 0 \Leftrightarrow \varphi(G) = 0\,.$$

Proof. $\Rightarrow$: Let v be an arbitrary vertex of G. By Proposition 7.3 and $\mathrm{rk}\,(G) = |V \setminus \{v\}|$, we have that $\psi(G) = 0$ implies $T(G)[V \setminus \{v\}]$ having a non-zero determinant. The expansion of this determinant is a sum of some products over all 1-factors of $G \setminus \{v\}$. Hence, for all $v \in V$, $G \setminus \{v\}$ has a 1-factor i.e. G is factor-critical. Using Theorem 2.1 we obtain that $\varphi(G) = 0$.

$\Leftarrow$: The statement is true for the one-point graph K_1. Using Theorem 2.1 and Corollary 2.2 it is enough to show that if G is connected, $\psi(G) = 0$ and G' is obtained from G by one of the operations described in Corollary 2.2 then $\psi(G') = 0$.

Case 1. Assume that G' is constructed by adding a new edge e between two vertices of G. Since G is a connected graph $\mathrm{rk}(G') = \mathrm{rk}(G)$. On the other hand it is clear, that $F(G') = F(G)(x_e)$, where x_e is an indeterminate over $F(G)$. Thus substituting $x_e = 0$ in $T(G')$ yields $T(G)$. This implies by Lemma 5.2 that $\mathrm{rk}(T(G')) \geq \mathrm{rk}(T(G)) = \mathrm{rk}(G)$. Using that $\mathrm{rk}(G) \geq \mathrm{rk}(T(G'))$, we obtain that $\psi(G') = \psi(G) = 0$.

Case 2. Assume that G' is constructed from G by double subdivision of some edge e. It is obvious that $\mathrm{rk}(G') = \mathrm{rk}(G) + 2$. We will show $\mathrm{rk}(T(G')) = \mathrm{rk}(T(G)) + 2$. It is clear, by the construction of our field $F(G)$, that the indeterminates associated with the edges involved in the subdivision are all equal. We denote them by x_e. By Lemma 6.2, $F(G) = F(G')$, in the natural way. $T(G')$ can be written as follows:

$$T(G') = \begin{pmatrix} & & & & 0 & 0 \\ & T(G\setminus\{e\}) & & & \vdots & \vdots \\ & & & & 0 & x_e \\ & & & & x_e & 0 \\ 0 & \cdots & 0 & x_e & 0 & x_e \\ 0 & \cdots & x_e & 0 & x_e & 0 \end{pmatrix}$$

The four x_e entries not in the lower-right corner can be eliminated so that one obtains a block matrix with blocks $T(G)$ and $\left(\begin{smallmatrix} 0 & x_e \\ x_e & 0 \end{smallmatrix}\right)$, which implies $\mathrm{rk}(T(G')) = \mathrm{rk}(T(G)) + 2$. ∎

Theorem 7.6. *For any graph G*

$$\psi(G) = \varphi(G).$$

Proof. Since both φ and ψ are additive under taking disjoint union of graphs, we can assume that G is connected. We prove by induction on a that $\psi(G) = a \Leftrightarrow \varphi(G) = a$ holds for any connected graph G. According to Lemma 7.5, the statement is true for $a = 0$. Assume that it is true for all $a \leq k-1$ where $k > 0$. We show both implications for k:

$\Rightarrow$: Assume that $\psi(G) = k$. Using our induction hypothesis, we have that $\varphi(G) \geq k$. By Lemma 6.2 there is an edge $e \in \mathrm{supp}\,\mathcal{B}(\mathcal{R}(G))$. Using Lemma 4.2 we obtain that $\psi(G/e) = \psi(G) - 1 = k - 1$. From the induction hypothesis it follows that $\varphi(G/e) = k - 1$. Using that $\varphi(G/e) \geq \varphi(G) - 1$ we get that $\varphi(G) \leq k$.

$\Leftarrow$: Assume that $\varphi(G) = k$. Using our induction hypothesis we have that $\psi(G) \geq k$. Let e be an edge of an even ear of an optimal ear-decomposition D. It is clear that $\varphi(G/e) = \varphi(G) - 1 = k - 1$. From the induction hypothesis it follows that $\psi(G/e)=k-1$. Lemma 4.2 implies that $\psi(G/e)\geq\psi(G)-1$. Now $\psi(G)\leq k$ completes the proof. ∎

A consequence of this characterization of φ is a simple proof of

Corollary 7.7 **(Szigeti [11]).** *Let G be a graph such that $G\setminus v$ has a unique perfect matching containing no bridge of G, then G is factor-critical.*

Proof. The unique matching produces a unique non-zero product in the expansion of $\det T(G)[V\setminus\{v\}]$. A different combinatorial proof can be found in [11]. ∎

It is more interesting that our results yield a representation of the ear-matroid $\mathcal{E}(G)$ of G. We emphasize that the verification of the matroid axioms for $\mathcal{E}(G)$ by combinatorial means is not trivial at all (see [12]). Now this follows from our foregoing results and moreover we obtain a representation of $\mathcal{E}(G)$.

Theorem 7.8. *Let $G=(V,E)$ be a graph and $M\subseteq 2^E$ the family of the subsets $S\subseteq E$ for which $\varphi(G/S)=\varphi(G)-|S|$. This family is identical to the family of the independent sets of $\mathcal{M}(\mathcal{B}(\mathcal{R}(G)))$. Moreover for each set $S\in M$ $\mathcal{E}(G/S)=\mathcal{E}(G)/S$.*

The proof is an immediate consequence of Theorem 4.3, Lemma 6.2 and 7.4 and Theorem 7.6. ∎

Now given our algebraic machinery we can prove the following corollaries:

Corollary 7.9. *Let G be a graph. A dependent set in the cycle or in the cocycle matroid of G is also dependent in $\mathcal{E}(G)$.* ∎

Corollary 7.10. *Let G be a 2-edge-connected graph. G is factor-critical if and only if, for each basis F of the cutset space, there is a partition of F into pairs so that, for each pair $\{S_1,S_2\}$ of the partition, $S_1\cap S_2$ is not a cutset of G.*

Proof. For the *if* part of the statement one can choose any basis of the cutset space consisting of $|V|-1$ stars and obtains the factor-criticality immediately. For the other direction, let D' be the generating matrix of $\mathcal{R}(G)$ constructed on the analogy of D, but using the basis F for the rows. Then

$$0=\varphi(G)=\dim\mathcal{B}(\mathcal{R}(G))=\dim\mathcal{B}(\mathcal{R}(D'))=\mathrm{rk}\,(G)-\mathrm{rk}\,(D'D'^T).$$

So $\mathrm{Pf}(D'D'^T)^2=\det D'D'^T\neq 0$ and every non-zero term in the expansion of the Pfaffian[1] yields a suitable partition. ∎

[1] See for example [4].

Corollary 7.11. *Let $G=(V,E)$ be a factor-critical graph. Define $G'=(V,E')$ by*

$$E' \overset{\text{def}}{=} \left\{ \{u,v\} \in \binom{V}{2} \mid \exists z \in V \setminus \{u,v\} : \{u,z\} \in E \text{ and } \{v,z\} \in E \right\}.$$

Then G' is factor-critical.

Proof. It is straightforward that all $(V\setminus v)\times(V\setminus v)$ subdeterminants of $T(G)$ are equal. $T(G)T(G)$ is a alternating matrix. If an entry of $T(G)T(G)$ is non-zero, then the corresponding vertices must have a common neighbour in G. From the Cauchy–Binet formula and since $|V|$ is odd, the determinant of $T(G)T(G)[V\setminus v]$ is $\det T(G)[V\setminus v]^2$, which is non-zero. Therefore, every induced subgraph $G'[V\setminus v]$ has a perfect matching. ∎

8. Symplectification of Spaces

Now we will generalize the result of the last section to arbitrary matroids representable over some field of characteristic 2. For this reason, we will start with extending the notion introduced in Section 6.

Let F be a field of characteristic 2 and U be an (E,F)-space. Let R_U be the ring described in Section 6 and let F_U be its quotient field. This field is isomorphic to a rational function field over F in $\operatorname{corank}(U)$ indeterminates. As in Section 6, we identify the variables x_e with their images under the map $F[X]\to F[X]/I(U)=R_U\subseteq F_U$. Let A be a generating matrix of U, and let A_e denote its column corresponding to e.

Let D be the $E\times E$ diagonal matrix with $x_e\in F_U$ at the row indexed by e. We define the *symplectification* $\mathrm{S}(U)$ of U to be the row space of the matrix AD. Clearly, $\mathrm{S}(U)$ is the row space of the matrix G which is obtained from A by multiplying each column A_e by the element $x_e\in F_U$. Note that the space $\mathrm{S}(U)$ is an (E,F_U)-space and that it does not depend on the choice of the generating matrix A (it only depends on the space U). As the name suggests, the symplectification of the space U has the following property:

Lemma 8.1. *The induced scalar product on the space $\mathrm{S}(U)$ is symplectic, i.e. $(v,v)=0$ for all $v\in\mathrm{S}(U)$.*

Proof. First we prove the statement for a vector v which is a row of the matrix AD. Such a vector has the form $(u_ix_i)_{i\in E}$ where $(u_i)_{i\in E}$ is in U. Using that $\operatorname{char}(F)=2$ we have that $(v,v)=\sum_{i\in E}u_i^2x_i^2=(\sum_{i\in E}u_ix_i)^2$. The sum $\sum_{i\in E}x_iu_i\in F(X)$ is an element of $I(U)$ and thus its image under the homomorphism $F[X]\to F[X]/I(U)$ is zero.

If v is an arbitrary element in $S(U)$ then $v=\sum\lambda_i v_i$ where v_i is the i-th row of AD. Using again that $\mathrm{char}(K)=2$ we have that $(v,v)=\sum\lambda_i^2(v_i,v_i)=0$. ∎

The good thing about symplectification is that it doesn't really alter the matroid structure on E. To be more precise, if $\mathcal{M}(U)$ has no bridge, then $\mathcal{M}(\mathrm{S}(U))=\mathcal{M}(U)$ since we just multiplied the columns of G by some nonzero scalars. In fact, the only difference between $\mathcal{M}(U)$ and $\mathcal{M}(\mathrm{S}(U))$ is that the bridges of $\mathcal{M}(U)$ are replaced by loops. It will prove crucial that $\mathrm{S}(U/e)$ and $\mathrm{S}(U)/e$ are basically indentical up to the natural isomorphism (see Lemma 5.3).

Lemma 8.2. *The symplectification* $\mathrm{S}(U)$ *of a bicycle free symplectic* (E,F)*-space* U *is a bicycle free symplectic space.*

Proof. The symplectification of any space is symplectic, so we have to show that $\mathrm{S}(U)$ is bicycle free. Let v be the everywhere 1 vector from F^E. Since U is symplectic, it is contained in the space $W=v^\perp$. It is easy to see that R_W is a polynomial ring in one variable x and that the natural homomorphism $\varphi: R_U\to R_W$ maps x_e to x for all $e\in E$. We obtain that $\varphi(\det(ADD^TA^T))=x^2\det(AA^T)$. This means that $\det(AA^T)\neq 0$ implies $\det(ADD^TA^T)\neq 0$. Lemma 4.1 completes the proof. ∎

9. A Δ-Matroid

A Δ-*matroid* is a non-empty set-system $\mathcal{F}\subseteq 2^E$ satisfying the symmetric exchange axiom: For $F_1,F_2\in\mathcal{F}$ and $e\in F_1\triangle F_2$, there exists $f\in F_1\triangle F_2$ such that $F_1\triangle\{e,f\}\in\mathcal{F}$. The members of set-system $\mathcal{F}$ are called *feasible* sets of the Δ-matroid. A Δ-matroid is *even* if all feasible sets are of the same parity. If F is a subset of E then $F\triangle\mathcal{F}\overset{\text{def}}{=}\{F\triangle F' \mid F'\in\mathcal{F}\}$ is called the *twist* of $\mathcal{F}$ by F, and it also satisfies the symmetric exchange axiom. While matrices give rise to matroids, representable Δ-matroids arise from symmetric or skew-symmetric matrices:

Theorem 9.1 (Bouchet [1]). *If A is a symmetric or skew-symmetric $E\times E$ matrix, then $\mathcal{F}(A)\overset{\text{def}}{=}\{F\subseteq E \mid A[F,F]$ is regular$\}$ form the family of feasible sets of a Δ-matroid and A is called a (skew-)symmetric representation of $\mathcal{F}(A)$.*

A Δ-matroid $\mathcal{F}$ is called *representable* if some twist of it arises from a symmetric or skew-symmetric matrix in the above way.

We will also need the concept of subdivision of edges of an (E,F)-space U. Let $e\in E$ be an arbitrary element. We introduce a new edge e' and we denote by E' the set $E\cup\{e'\}$. Space U is naturally embedded into $F^{E'}$ by extending every vector $u\in U$ with a 0 coordinate corresponding to e'. Let U' denote the (E',F) space which is obtained from U by switching the coordinates corresponding to e and e'. We define the (E',F)-space $U\div e$ resulting from the *subdivision* of edge e as the space spanned by U and U'. One can easily see (for example, by looking at the generating matrices) that the subdivision of an edge increases the dimension of the space by exactly one.

Since the subdivisions of distinct edges commute, $U\div S$ can be defined to be the subsequent subdivision of all edges in $S\subseteq E$. It can easily be checked that $\dim(U\div S)=\dim(U)+|S|$. Another simple but useful fact is that if S and T are disjoint subsets of E, then $(U\div S)/T=(U/T)\div S$.

Later on, we will need the following simple facts:

Lemma 9.2. *Let U be a symplectic (E,F)-space and assume that $\operatorname{supp}(v)\subseteq\{e,f\}$ with $v\in U$ and $e,f\in E$. Then $v=c(\chi_e+\chi_f)$ for some scalar $c\in F$. In particular e and f are in the same series class of $\mathcal{M}(U)$ if and only if $\chi_e+\chi_f\in U$.*

Proof. Since $\operatorname{supp}(v)\subseteq\{e,f\}$ we have that $v=a\chi_e+b\chi_f$ for some scalars $a,b\in F$. Using that the space is symplectic we obtain that $0=\langle v,v\rangle=a^2+b^2=(a+b)^2$. It follows that $a+b=0$ and so $a=b$. The second statement follows from Lemma 3.2. ■

Proposition 9.3. *Let U be a symplectic space and e,f two series elements of $\mathcal{M}(U)$, then $(U/e)\div f=U$ if we identify the newly created edge f' and e.*

Proof. Since e and f are series, $\chi_e+\chi_f\in U$. The dimension of U and $U/e\div f$ coincide, so we must only show that $U/e\div f$ is contained in U. Take an arbitrary vector of $v\in U/e$. Since switching f and $e=f'$ is equivalent to adding $\chi_e+\chi_f$ to v, therefore the inclusion is clear. ■

The straightforward proof of the following Lemma is left to the reader.

Lemma 9.4. *Let S be an independent set of the matroid of (E,F)-space U. Then U has a minimal generating matrix of the form $\begin{array}{c|cc} & S & E\backslash S \\ \hline S & I & A \\ E\backslash S & 0 & B \end{array}$, where B is a minimal generating matrix of U/S. In this case,*

$$\begin{array}{c|ccc} & S' & S & E\backslash S \\ \hline S' & I & -I & 0 \\ S & 0 & I & A \\ E\backslash S & 0 & 0 & B \end{array}$$

is a minimal generating matrix of $U\div S$. (I denotes an identity matrix of suitable size.) ■

Using this representation we can show

Lemma 9.5. *Let F be a field of characteristic 2 and let S be an independent set of the matroid of (E,F)-space U. Then $\beta(U\div S)=\beta(U/S)$. ($\beta(V)$ denotes the dimension of the bicycle-space of V as defined in Section 2.)*

Proof. Take a minimal representation M of U according to Lemma 9.4. By Lemma 4.1 we have

$$\begin{aligned}\beta(U\div S) &= \dim(U\div S)-\operatorname{rk}(MM^T)\\ &= 2|S|+\dim(U/S)-\operatorname{rk}\begin{pmatrix}0 & I & 0\\ I & I+AA^T & AB^T\\ 0 & BA^T & BB^T\end{pmatrix},\end{aligned}$$

where I is an identity matrix of suitable size. The rightmost matrix can be transformed to the form $\begin{pmatrix}0 & I & 0\\ I & 0 & 0\\ 0 & 0 & BB^T\end{pmatrix}$ by using rank-preserving column- and row-operations.

Since B is a minimal generating matrix of U/S we obtain $\beta(U\div S)=2|S|-2|S|+\dim(U/S)-\operatorname{rk}(BB^T)=\beta(U/S)$. ∎

Lemma 9.6. *Let F be a field of characteristic 2 and let S and T be two independent sets of the matroid $\mathcal{M}(U)$ of (E,F)-space U. Then $\beta(U/T)=\beta((U\div S)/(T\triangle S))$*

Proof. Since $T\cap S$ is independent in $\mathcal{M}(U/(T\setminus S))$, Lemma 9.5 implies that

$$\begin{aligned}\beta(U/T) &= \beta(U/(T\setminus S)/(T\cap S))\\ &= \beta((U/(T\setminus S))\div(T\cap S))=\beta((U\div S)/(S\triangle T)).\end{aligned}$$ ∎

Let U be a bicycle free (E,F)-space. Then F^E is the direct sum of U and $U^\perp$, so every vector $v\in F^E$ can be uniquely written as $v=v_1+v_2$, where $v_1\in U$ and $v_2\in U^\perp$. This gives rise to the unique orthogonal projections $P_U : F^E\longrightarrow U$ and $P_{U^\perp} : F^E\longrightarrow U^\perp$ which are represented by the symmetric idempotent matrices $\mathbf{P}_U$ and $\mathbf{P}_{U^\perp}$.

Proposition 9.7. *Let U be an (E,F)-space. Let $\mathbf{P}_U$ be the matrix of the orthogonal projection onto U. The following two statements for an independent subset $S\subseteq E$ are equivalent:*

1. *U/S is bicycle free.*
2. *The symmetric submatrix $\mathbf{P}_U[S,S]$ is nonsingular.*

Proof. We use that U/S is naturally embedded into F^E and that this embedding is scalar product preserving. Let V_S be the subspace of all vectors from F^E whose components outside S are zero. The matrix $\mathbf{P}_U[S,S]$ has full rank if and only if $\mathbf{P}_U(V_S)\backslash(E\backslash S)$ is full F^S. It means that $\mathbf{P}_U[S,S]$ has full rank if and only if $\mathbf{P}_U(V_S)+U/S=U$. First assume that $W \overset{\text{def}}{=} \mathbf{P}_U(V_S)+U/S$ is strictly smaller than U. In this case, there is a non-zero vector v in $W^\perp \cap U$. By $v \perp \mathbf{P}_U(V_S)$, we obtain that $v \perp V_S$ and so $v \in U/S$. From $v \perp U/S$ we get that U/S is not bicycle-free. Now, assume that $W=U$. To prove that U/S is bicycle-free, let $v \in (U/E) \cap (U/E)^\perp$. Since $v \in U/E$, we have that $v \perp \mathbf{P}_U(V_S)$. From the assumption $W=U$ follows that $v \in U^\perp$ and so $v=0$. ∎

Theorem 9.8. *Let F be a field of characteristic 2 and U an (E,F)-space. Let $\mathcal{F}$ be the family of those subsets of E which are independent in $\mathcal{M}(U)$ and whose contraction results in a bicycle-free space. Then $\mathcal{F}$ is the family of feasible sets of a representable Δ-matroid.*

Proof. We use Theorem 9.1 and construct a symmetric representation of $\mathcal{F}$. Let B be a basis of $\mathcal{M}(\mathcal{B}(U))$. Then U/B and so $U \div B$ are bicycle-free by Theorem 4.3 and Lemma 9.5. Let $\mathbf{P}$ be the orthogonal projection matrix to the $(E \cup B', F)$-space $U \div B$. Let $T \subseteq E$ be independent in $\mathcal{M}(U)$. Lemma 9.6 yields $\beta(U/T) = \beta((U \div B)/(S \triangle T))$, so by Proposition 9.7 we get that $\mathcal{F} \triangle B$ is represented by $\mathbf{P}[E,E]$. ∎

10. The Characterization Theorem

In this section, we assume that F is a field of characteristic 2. Here, we will prove the central result of this paper: the characterization of factor-critical matroids representable over some field of characteristic 2. Before stating the main theorems we will prove some lemmas.

Lemma 10.1. *Let $\mathcal{F}$ be a family of matroids satisfying the following properties:*

1. *Every matroid in $\mathcal{F}$ is bridgeless.*
2. *If $M \in \mathcal{F}$ and $\mathrm{rk}(M) > 0$ then either there is an $e \in E(M)$ such that $M \setminus e \in \mathcal{F}$ or there is a series class of M consisting of at least three elements e, f, g such that $M/\{e,f\} \in \mathcal{F}$.*

Then every element of $\mathcal{F}$ is factor-critical

Proof. We go by induction on $|E(M)| + \mathrm{rk}(M)$. Let M be a matroid from $\mathcal{F}$ and assume that the statement is true for all $M' \in \mathcal{F}$ with $|E(M')| + \mathrm{rk}(M') < |E(M)| + \mathrm{rk}(M)$. There are two possible cases:

1. Let $e \in E(M)$ such that $M \backslash e$ is factor-critical, and let $\mathcal{P}$ be a partition of $E(M \setminus e)$ described in Lemma 2.3. Since e is contained in some circuit

C we obtain that e is a loop (circuit with one element) in $M/(M\setminus e)$. By extending $\mathcal{P}$ with $\{e\}$ as a last element we obtain a partition of $E(M)$ which proves that M is factor-critical.

2. If there is no such edge, then there is a series class of M with at least three edges $e,f,g\in E(M)$, such that $M/\{e,f\}$ is factor-critical. Let $(C_1,\dots,C_k)$ be an odd ear-decomposition of a block of $M/\{e,f\}$ which contains a circuit C_i containing g. It is easy to check that $(C_1,\dots,C_i\cup\{e,f\},\dots,C_k)$ is an odd ear-decomposition of the block of M containing e,f and g. The existence of an odd ear-decomposition of the other blocks of M follows immediately from the induction hypothesis. ∎

Lemma 10.2. *Let U be an (E,F)-space. The induced scalar product on U is a non-degenerate symplectic form if and only if there is a generating matrix of U, which is an alternating projection.*

Proof. If the induced scalar product is a non-degenerate symplectic form on U, then U is bicycle free and so the matrix $\mathbf{P}_U$ of the orthogonal projection to U is a alternating projection matrix representing U. If U is represented by a alternating projection matrix P, then the induced scalar product on U is clearly symplectic. If we assume that U is not bicycle-free, then there is a vector $v\in F^E\setminus\mathcal{B}(U)^\perp=F^E\setminus(U+U^\perp)$. For an arbitrary vector $w\in U$,

$$\langle v+Pv,w\rangle=\langle v,w\rangle+\langle Pv,w\rangle=\langle v,w\rangle+\langle v,Pw\rangle=\langle v,w\rangle+\langle v,w\rangle=0$$

and therefore $v=Pv+(v+Pv)\in U+U^\perp$, contradicting the choice of v. ∎

Lemma 10.3. *Let U be a symplectic space, e,f series elements of U, then:*

$$\beta(U)=\beta(U/\{e,f\}).$$

In particular, if U is a symplectic bicycle-free space, then so is $U/\{e,f\}$.

Proof.

$$\beta(U)=\beta(U/e\div f)=\beta(U/\{e,f\}).$$

Where the first equality follows from Proposition 9.3, the second one follows from Lemma 9.6. ∎

Lemma 10.4. *Let $\mathrm{S}(U)$ be the symplectification of a bridgeless (E,F)-space U, B a basis of U, A a minimal generating matrix of U and $F(\{y_e\}_{e\in E\setminus B})$ the ground field of $\mathrm{S}(U)$ according to the isomorphism of Proposition 5.1. Let D be the diagonal matrix such that AD is a minimal generating matrix of $\mathrm{S}(U)$. Assume that squaring is an isomorphism on F (i.e. each element $c\in F$ has a square root $\sqrt{c}$). Then $\det(ADD^TA^T)=p^4$ where $p\in F[\{y_e\}_{e\in E\setminus B}]$ is of total degree at most $\dim(U)/2$.*

Proof. For a symplectic $V\times V$ matrix $X=(x_{uv})_{u,v\in V}$ over a field of characteristic 2, we denote by $\mathrm{Pf}(X)\overset{\mathrm{def}}{=}\sum\limits_{M}\prod\limits_{\{v,w\}\in M} x_{vw}$ the Pfaffian of X, where the summation goes over all perfect matchings M of the complete graph on V. It is well-known (see e.g. [4]) that $\mathrm{Pf}(X)^2=\det(X)$. Since ADD^TA^T is an alternating matrix, $\det(ADD^TA^T)$ can be expressed as $\mathrm{Pf}(ADD^TA^T)^2$, where $\mathrm{Pf}(ADD^TA^T)$ is a polynomial in the entries of ADD^TA^T of total degree $\dim(U)/2$. Since the entries of ADD^TA^T are linear polynomials in the squares of the indeterminates and squaring is an endomorphism of the ring in question, we obtain the statement by setting $p\overset{\mathrm{def}}{=}\sqrt{\mathrm{Pf}(ADD^TA^T)}$. ∎

Theorem 10.5. *Let M be a matroid representable over a field of characteristic 2. Then the following statements are equivalent:*

1. *M is factor-critical.*
2. *M is bridgeless and the symplectification of each representation of M by an (E,F)-space U over a field F of characteristic 2 is bicycle free.*
3. *M is bridgeless and the symplectification of some representation of M by an (E,F)-space U over a field F of characteristic 2 is bicycle free.*
4. *M is representable by a space on which the induced scalar product is a non-degenerate symplectic form.*
5. *M is representable by an alternating projection matrix.*

Proof. (1)$\Longrightarrow$(2): If a matroid has an ear-decomposition then every edge is contained in some circuit and so it is bridgeless. We fix an odd ear-decomposition of M and a representation U of M. Clearly, the symplectification of any space is symplectic, so our objective is to prove that $\mathrm{S}(U)$ is bicycle free. Let $\{x_e\}_{e\in E}$ be the indeterminates defined by the symplectification. We proceed by induction on $|E|$. We can assume that the implication holds for any matroid M' with $|E(M')|<|E|$ and have two cases:

Case 1. *The last ear is a single edge e.*

In this case, since e is no bridge, $\mathrm{rk}(U\setminus e)=\mathrm{rk}(U)$. Let A be a minimal generating matrix of U and A' the matrix obtained from A by deleting the e-th column. Clearly A' is a minimal generating matrix of $U\setminus e$. Let $\{y_f\}_{f\in E\setminus e}$ be the indeterminates occuring in the definition of $S(U\setminus e)$. One can check that the substitution $x_f=\begin{cases} y_f \text{ if } f\neq e,\\ 0 \text{ if } f=e\end{cases}$ preserves the dependence between the indeterminates $\{x_f\}_{f\in E}$. This means that $\det(A'(A')^T)\neq 0$ implies $\det(AA^T)\neq 0$. Since the first inequality holds by the induction assumption and Lemma 4.1, so does the latter one, i.e. $\mathrm{S}(U)$ is bicycle free.

Case 2. *The last ear contains at least two independent edges e and f.*

Contracting the last ear by $\{e,f\}$ shows that $M/\{e,f\}$ admits an odd ear decomposition. By Lemma 10.3 and since the symplectification commutes with contraction, we get:

$$\beta(\mathrm{S}(U)) = \beta(\mathrm{S}(U)/\{e,f\}) = \beta(\mathrm{S}(U/\{e,f\})) = 0,$$

where the last equality follows from the induction assumption. Thus, we obtain by Lemma 4.1 that $\mathrm{S}(U)$ is bicycle free.

(2)$\Longrightarrow$(3): Clear.

(3)$\Longrightarrow$(4): Let U be an (E,F)-space which is a non-degenerate (bicycle free) symplectic representation of M. The property that M is bridgeless guarantees that the symplectification of U is a representation of M. Using Lemma 4.1 and Lemma 8.2 we obtain that statement (4) holds for $\mathrm{S}(U)$.

(4)$\Longleftrightarrow$(5): Lemma 10.2.

(4)$\Longrightarrow$(1): Let $\mathcal{F}$ be the family of matroids satisfying (4). We show the implication by checking the conditions of Lemma 10.1 for $\mathcal{F}$. Let M be a matroid in $\mathcal{F}$. Fix an (E,F)-space U which is a representation of M satisfying (4) such that squaring on the ground field F is an isomorphism. (This can always be achieved by tensoring U with the algebraic closure of F, which does not change the involved matrices at all.) The first condition of Lemma 10.1 follows from Lemma 3.1 because a symplectic (E,F)-space can't contain the characteristic vector of an edge e. We have two cases:

Case 1. *There is an edge e such that $\mathrm{S}(U\setminus e)$ is bicycle free.*

If $M\setminus e$ is bridgeless then $\mathrm{S}(U\setminus e)$ represents $M\setminus e$ and so $M\setminus e\in\mathcal{F}$. If there are two bridges f,g in $M\setminus e$ then e,f and g are in the same series class of M and by Lemma 10.3 we have that $M/\{e,f\}\in\mathcal{F}$. Finally we exclude the case that there is exactly one bridge f in $M\setminus e$. To see this, recall that a symplectic, bicycle free space has to be even dimensional. In particular U is even dimensional. Assume that $\operatorname{supp}(v)\subseteq\{e,f\}$ for some vector $v\in U$. Lemma 9.2 shows that $v=c(\chi_e+\chi_f)$ for some scalar $c\in F$. Since e and f are in the same series class, we have that $\chi_e+\chi_f\in U$. These two facts together imply that $\dim(U\setminus\{e,f\})=\dim(U)-1$. Thus $U\setminus\{e,f\}$ is an odd dimensional bridgeless space. Now it is easy to see that $\dim(\mathrm{S}(U\setminus e))=\dim(U\setminus\{e,f\})$ which contradicts the fact that $\mathrm{S}(U\setminus e)$ is bicycle free.

Case 2. *The bicycle space of $\mathrm{S}(U\setminus e)$ is non-zero for all $e\in E$.*

Let $B\subseteq E$ be a basis of M and $\{x_e\}_{e\in E}$ be the elements in F_U occurring in the definition of $\mathrm{S}(U)$. By Lemma 8.2 $\mathrm{S}(U)$ is also bicycle free. We have a unique generating matrix A of U of the form

$$\begin{array}{cc} & \begin{array}{cc} B & E\setminus B \end{array} \\ B & \begin{pmatrix} I & \quad C \quad \end{pmatrix}. \end{array}$$

Set

$$\gamma(B,e) \overset{\text{def}}{=} \begin{cases} \sum\limits_{f\in E\setminus B} A[e,f]x_f & \text{for } e\in B, \\ x_e & \text{otherwise.} \end{cases}$$

By Proposition 5.1, the map $\varphi\colon x_e \to \gamma(B,e)$ induces an isomorphism of rings between F_U and $F[\{x_e\}_{e\in E\setminus B}]$ where the indeterminates x_e for $e\in E\setminus B$ are algebraically independent. Let $A_{E\setminus e}$ be the matrix obtained from A by deleting the e-th column. Then $A' \overset{\text{def}}{=} A_{E\setminus e}D[E\setminus e, E\setminus e]$ is a minimal generating matrix of $S(U\setminus e)$ with entries from the polynomial ring

$$F[\{x_f\}_{f\in E\setminus B}]/(\gamma(B,e))$$

where $(\gamma(B,e))$ denotes the ideal generated by the $\gamma(B,E)$ in $F[\{x_f\}_{f\in E\setminus B}]$. If we compute $A'(A')^T$, we formally obtain ADD^TA^T; we have only changed our ground field. To be more specific, we see, that $A'(A')^T$ is singular if and only if $\det(ADD^TA^T)$ is in the ideal generated by $\gamma(B,e)$ i.e. $\gamma(B,e)$ divides $\det(ADD^TA^T)$. The degree of the polynomial $\det(ADD^TA^T)$ is $2|B|$ and according to Lemma 10.4 it is the 4-th power of some polynomial of degree $|B|/2$. Since the polynomials $\gamma(B,e)$ are linear (and thus irreducible) we obtain that, up to multiplication with scalars, there are at most $|B|/2$ different values of $\gamma(B,e)$. If for $e,f\in B$ holds $\gamma(B,e) = c\gamma(B,f)$, then $\chi_e + c\chi_f \in U$, i.e. e and f are in the same series class of M. Lemma 9.2 shows that in this case $\chi_e + \chi_e \in U$. Using the pigeonhole principle, we can deduce that either there is a series class with at least three elements (M satisfies the conditions of Lemma 10.1) or B can be partitioned into series classes of size two. Since every edge is contained in some basis B of M, we can assume that the whole edge set can be partitioned into series classes each of them having size at least 2. If there is a series class with at least three element we are done. It remains to rule out the case when E is partitioned into series classes with two elements. Because of the symplecticity of U, the characteristic vectors of these classes are all in U, and so the same is true for their sum χ_E. Using again that U is a symplectic space and that F has characteristic 2 one can see easily that χ_E is also in $U^\perp$, contradicting the nondegeneracy of the scalar product on U. ∎

Theorem 10.6. *Let U be a bridgeless (E,F)-space. Then $\varphi(\mathcal{M}(U))$ is the dimension of the bicycle space of* $\mathrm{S}(U)$.

Proof. Let us introduce the invariants $\psi(W) \overset{\text{def}}{=} \beta(\mathrm{S}(W))$ and $\varphi(W) \overset{\text{def}}{=} \varphi(\mathcal{M}(W))$ for any (E,F)-space W. Let α be any of the two invariants φ and ψ. One can check easily that α has the following two properties:

1. $\alpha(W/e) \geq \alpha(W) - 1$
2. If $\alpha(W) \neq 0$ then there exists $e \in E$ with $\alpha(W/e) = \alpha(W) - 1$.

By Theorem 10.5 we know that $\varphi(U) = 0$ if and only if $\psi(U) = 0$. Now assume that $\varphi(U) > \psi(U)$. According to the above properties, there is an edge set $S \subseteq E$ such that $|S| = \psi(U)$ and $\psi(U/S) = 0$. Using again the above properties we obtain that $\varphi(U/S) \geq \varphi(U) - |S| = \varphi(U) - \psi(U)$ which is a contradiction. The case $\psi(U) > \varphi(U)$ can be excluded exactly in the same way. ∎

The importance of the theorem is that it allows to compute the ear-decomposition of matroids given by their linear representation over fields of characteristic 2 in randomized polynomial time. Too see this, we will need the following easy lemma.

Lemma 10.7 **(Zippel[16] and Schwartz[10]).** *For a non-zero polynomial $p \in K[x_1, \ldots, x_n]$ of degree d and $S \subseteq K$, the probability that p evaluates to 0 on a random element of S^n is at most $d/|S|$.* ∎

Theorem 10.8. *Let U be a bridgeless (E,F)-space where F is either a finite field of characteristic 2 or the field of fractions of some polynomial ring over a finite field of characteristic 2. Let M be a generating matrix of U. Then the value of $\varphi(\mathcal{M}(U))$ can be computed in randomized polynomial time in terms of the input M.*

Proof. Using Theorem 10.6, Lemma 4.1 we obtain that the computation of φ can be reduced to the computation of the rank of the matrix MDD^TM^T where D is the diagonal matrix occurring in the definition of the symplectification of U. Applying Proposition 5.1, the matrix MDD^TM^T is represented as a matrix where the entries are at most second degree polynomials in the indeterminates $\{y_e\}_{e \in E \setminus B}$ for some basis B of $\mathcal{M}(U)$ such that these polynomials are short (polynomially long in terms of the input data) expressions. The determinant of this matrix is a polynomial with total degree at most $2|E|$. In the case of finite F, by Lemma 10.7, for each ϵ we can choose a suitably large finite extension field F' of F such that the evaluation of the determinant over a random vector in F' is non-zero with probability greater then $1-\epsilon$ whenever the original $\det MDD^TM^T$ does not vanish. The running time of this algorithm is polynomial in the input size and $|\log \epsilon|$, since the evaluation of the determinant over a finite field can be performed in polynomial time. If F is the field of fractions of some polynomials over a finite field $\tilde{F}$, then we can consider $\det MDD^TM^T$ as a polynomial over $\tilde{F}$ and evalute a random substitution of it over a suitably large finite extension of $\tilde{F}$. To compute the rank of the matrix, one can iterate the above procedure to find a maximal submatrix with nonvanishing determinant. ∎

Theorem 10.9. *Let U be an (E,F)-space and $M\subseteq 2^E$ the family of sets $S\subseteq E$ for which $\varphi(U/S)=\varphi(U)-|S|$. Then M is the family of the independent sets in $\mathcal{M}(\mathcal{B}(\mathrm{S}(U)))$.*

Proof. The proof is an immediate consequence of Theorem 10.6, Lemma 4.3 and Lemma 5.3. ∎

11. Factor-criticality revisited

In this section we discuss implications of the main theorem to graphs. We have seen in Section 7 that a graph is factor-critical if and only if the symplectification of its cutset space is bicycle free. Now we can easily deduce the following characterization of factor-criticality from Theorem 10.5:

Corollary 11.1. *A graph G is factor-critical if and only if its cycle matroid can be represented by an alternating projection matrix over some field of characteristic* 2. ∎

Note the simlarity of this result to that of F. Jaeger in [5] and [6]. Our factor-criticality condition are more sophisticated than the results there, since we had to drop the binarity condition and go over to arbitrary fields of characteristic 2. In fact there are examples of factor-critical graphs whose cycle matroid cannot be represented by a binary alternating projection matrix.

Theorem 9.8 specializes to the following statement in the case of graphs:

Corollary 11.2. *In a graph, the family of independent edge sets (with respect to the cycle matroid of G) contracting to a factor-critical graph forms the family of feasible sets of an even Δ-matroid.* ∎

This result generalizes the main result of [12]. Note that the proof of Theorem 9.8 gives an explicit representation of this Δ-matroid and the feasibility of subsets of E can be decided in randomized polynomial time.

Acknowledgement. The authors are grateful to Zoltán Szigeti, András Frank and Jácint Szabó for helpful discussions on the topic of the paper.

References

[1] A. Bouchet: Representability of Δ-matroids, Combinatorics, *Proc. 7th Hung. Colloq., Eger/Hung. 1987*, Colloq. Math. Soc. Janos Bolyai **52** (1988), 167–182.

[2] A. Frank: Conservative Weightings and Ear-Decompositions of Graphs, *Combinatorica* **13** (1993), 65–81.

[3] W. H. Cunningham and J. F. Geelen: The optimal path-matching problem, *Combinatorica* **17** (1997), 315–337.

[4] C. D. Godsil: *Algebraic Combinatorics*, Chapman and Hall, 1993.

[5] F. Jaeger: Symmetric representations of binary matroids, *Ann. Discrete Math.* **17** (1983), 371–376.

[6] F. Jaeger: Graphes de cordes et espaces graphiques (French), *European Journal of Combinatorics* **4** (1983), 319–327.

[7] S. Lang: *Algebra*, Addison Wesley, 1971.

[8] L. Lovász: A Note on Factor-Critical Graphs, *Studia Sci. Math. Hungar.* **7** (1972), 287–290.

[9] L. Lovász: On Determinants, Matchings and Random Algorithms, in *Fundamentals of Computing Theory* (L. Budach, Ed.), Akademia Verlag, Berlin, 1979.

[10] J. Schwartz: Fast probabilistic algorithms for verification of polynomial identities, *Journal of the ACM* **27** (1980), 701–717.

[11] Z. Szigeti: Conservative Weightings of Graphs, PhD Thesis, Eötvös Loránt University, Budapest, 1994.

[12] Z. Szigeti: On a Matroid Defined by Ear-Decomposition of Graphs, *Combinatorica* **16** (1996), 233–241.

[13] Z. Szigeti: On generalizations of matching-covered graphs, *Eur. J. Comb.* **22(6)** (2001), 865–877.

[14] W. T. Tutte: The factorization of linear graphs (English), *J. Lond. Math. Soc.* **22** (1947), 107–111.

[15] D. J. A. Welsh: *Matroid Theory*, Academic Press, 1976.

[16] R. Zippel: Probabilistic algorithms for sparse polynomials, in *International Symposium on Symbolic and Algebraic Computation*, Vol. **72** of *Lecture Notes in Computer Science*, (1979), Berlin, 216–226.

Balázs Szegedy

Institute for Advanced Study
Princeton, NJ 08540
USA
szegedyb@gmail.com

Christian Szegedy

Cadence Berkeley Labs
Berkeley, CA 94702
USA
szegedy@cadence.com