刘彦佩

半闲数学集锦

Semi-Empty Collections in Mathemetics by Y.P.Liu

第四编

时代文化出版社

刘彦佩

半闲数学集锦

Semi-Empty Collections in Mathemetics by Y.P.Liu

第四编

时代文化出版社

半闲数学集锦（第四编）

作　　者：刘彦佩
出版单位：时代文化出版社
地　　址：香港湾仔骆克道骆基中心23楼C座

编辑设计：北京时代弄潮文化发展有限公司
地　　址：北京市海淀区中关村创业大街25号家谱传记楼
电　　话：010-68920114　13693651386
网　　址：www.grcsw.com

印　　刷：京冀印刷厂
开　　本：880×1230　1/16
版　　次：2016年9月第1版

书　　号：ISBN 978-988-18455-0-4
定　　价：全套 1890.00元（共22编）

第四编序

在平面可嵌入性的问题被解决之后, 有两个方向要考虑. 因为平面是 2-维欧式空间, 自然会想到图在什么条件下, 可以嵌入到 3-维空间. 似乎一想到, 就被人们, 通过构造, 而得到完满解决.

这就是, 将图的节点放到一条曲线段上, 只要这条曲线, 从一端到另一端, 在三个相互独立的方向上, 变化率的阶, 互不相同, 因为这时, 此线段的任何互不相同的四个点, 不会落在同一个平面上, 只要图的任何一对相邻的节点, 连一条直线段, 就得这个图, 在 3-维空间, 的一个嵌入. 因此, 这个方向已经不足道了.

另一方面, 平面也可视为, 一类特殊的 2-流形, 即亏格为零的曲面, 考虑图, 在亏格非零曲面上, 的可嵌入性, 主要源自围绕以下五个层次的基本问题:

(1) 每一个图, 是否都存在一个曲面, 使得它在这个曲面上, 有一个嵌入?

对于拓扑上的一般嵌入, 容易从图的, 一个支撑子树的, 平面嵌入导出. 若曲面是不可定向的, 任何一个图(非树!), 都可嵌入到, 亏格不小于其 Betti 数(非 0!), 的曲面.

若曲面是可定向的, 任何一个图, 都可嵌入到, 亏格不小于其 Betti 数之半, 的曲面.

但通常, 一个嵌入, 对于曲面补的连通片, 可以不同伦于 0. 引出要研究, 所有连通片, 都同伦于 0 的嵌入, 即所谓*胞腔嵌入*. 这就是为什么, 从一开始, 就选中多面形, 作为主要研究工具.

(2) 对于胞腔嵌入, 任何一个图, 都存在一个曲面, 使得在它上, 有一个这样的嵌入. 从多面形的 Heffter-Edmonds 模型, 即可导出. 不过实际上, 只是对于可定向曲面.

因为树, 不能嵌入到, 任何不可定向曲面, 这个存在性是否定的. 在不可定向曲面上, 图的这种嵌入的存在性, 是由 1.08[010] 中的一个定理导出.

图 G 的 Betti 数 $\beta(G)$, 为图中基本圈的树目. 一个图(连通!), 不是树, 就至少有一个圈. 可见, 定理中的 $\beta(G)$ 为, 不小于 1 的整数. 换一句话说, 总存在一个不可定向曲面, 使得 G 在它上, 有一个胞腔嵌入.

因为别的嵌入对于我们已经没有实际意义, 允许就直接用嵌入, 而无需总提胞腔嵌入.

对于胞腔嵌入, 任何一个图, 它可嵌入曲面的亏格, 既有一个有限的下界, 也有一个有限的上界, 分别称它们, 为这个图的, *最小亏格*和*最大亏格*. 这个最小亏格, 也就是人们通常称的, 这个图的*亏格*.

(3) 是否每一个图, 它可嵌入曲面的亏格, 都能充满, 最小亏格和最大亏格区间内, 所有整数? 如果充满, 就称图对于曲面亏格, 具有*插值性质*. 关于图, 对曲面亏格, 插值性质的, 完满解决, 可以从 2.14(引理12.1.2 和引理12.1.3)看

出. 然而那时, Duke 所解决的, 只是对于可定向曲面的情形.

(4) 如何确定图的最小和最大亏格?

虽然确定图的最小亏格, 曾一度成为热点, 但只是利用商嵌入, 如电流图, 或电压图. 这就带来了, 要考虑高对称性的图. 实际上, 就是拓扑学中, 覆盖空间方法. 只有 $K_n - K_3$ 的 $n = 8 (\bmod\ 12)$ 和 $n = 11 (\bmod\ 12)$ 两种情形不是直接利用商嵌入, 而用演示法, 参见 1.10[014], 或 1.13[017].

关于最大亏格, 受最小亏格的影响, 人们开始时, 也是瞄准高对称图. 从小图最大亏格的经验, 使我意识到, 不必如此. 开始寻找, 与对称性无关的, 一些代数运算, 使得只通过这些运算, 就可确定这个最大亏格. 首先, 对于不可定向曲面, 取得了成功, 这就是 1.08[010]. 对于可定向曲面, 则只能通过简约, 而导出这个亏格的一些表征, 由此引出了, 确定上可嵌入性, 与估界最大亏格问题. 参见 1.09[011], 特别是 2.14[137] 或 3.24[141].

由于这个问题, 以及随之而来的, 确定一个图的手柄多项式和叉帽多项式. 自嵌入联树模型, 在专著组合地图进阶[292](12.39—12.62) 中, 提出之后, 又在专著地图的代数原理[354](13.27—13.56) 和专著*Introductory Map Theory*[459](16.01—16.33) 中, 臻于完善, 开始对于一批困难, 而带有程度不同高普遍性的图类, 取得了, 用现有其它方法, 尚还无路通往的结果. 就更普遍的意义而言, 至今仍然, 尚未能, 完满解决. 这又导致研究下面问题的重要性.

(5) 对于任何一个整数 $p \geq 1$, 如何判定一个图, 在亏格 p 可定向曲面上, 是否有一个嵌入? 对于任何一个整数 $q \geq 1$, 如何判定一个图, 在亏格 q 不可定向曲面上, 是否有一个嵌入?

这个问题, 直到专著*Topological Theory on Graphs*[400](17.01—17.20), 图的可嵌入性理论(第二扩充版)[438](5.01—5.23), 以及专著*Elements of Algebraic Graphs*[486](19.11—19.36), 才算在理论上, 得到完满解决. 不过, 在运行有效化和利用智能化方面, 仍然是对未来发展的挑战.

本编关联专著图的可嵌入性理论[137](2.01—2.20) 和专著*Embeddability in Graphs*[141](3.11—3.29) 中, 包括平面性与平面嵌入在内, 曲面可嵌入性与曲面嵌入, 以及它们的引伸.

例如, 文 4.01[190], 4.39[229], 4.45[242] 提供, 平面性理论引起的, 在拟阵图性与上图性, 超大规模集成电路(VLSI)的布线, 及其自动化等方面的新进展.

文 4.16[178], 4.21[192] 和 4.51[269], 讨论非平面性的一个度量, 图的交数(或交叉数), 的一些上界.

文 4.02[156], 4.04[159], 4.07[164], 4.13[174], 4.15[177], 4.18[181]— 4.20[189], 4.22[195], 4.24[199], 4.25[200], 4.27[204], 4.28[205], 4.31[213], 4.34[220]— 4.38[227], 4.41[231]— 4.43[233], 4.46[243]— 4.48[245], 4.50[266], 4.63[207], 4.65[313] 提供了, 有关图的最大亏格的各种估界, 以及最大亏格与图的色数, 独立数, 邻域, 最短圈长, 连通度, 直径, 因子, 以及嵌入的面边缘长等的关系.

在上可嵌入性, 及其与其它不变量的关系方面, 所取得的进展, 见文 4.06[163], 4.09[167]— 4.11[171], 4.14[175], 4.17[179], 4.23[198], 4.26[003], 4.32[021] 和 4.60 [029] 等.

关于给定亏格非零曲面上的可嵌入性, 在 1.08[010] 和 2.09[137] 基础上,

导出了文 4.03[158], 4.05[160], 4,06[163], 4.08[165] 和 4.12[172] 等.

对于曲面嵌入的一般理论, 双迂覆盖与双圈覆盖, 以及强嵌入和强最大亏格等的新研究, 见文 4.56[287], 4.58[291], 4.64[308], 4.30[208], 4.29[206], 4.33[216], 4.40[230], 4.44[237], 4.49[260], 4.52[277]— 4.55[286], 4.62[301] 和 4.66[319] 等. 前面的三篇文章, 为形成多面形的一般理论, 奠定了一个基础.

还要提一提文 4.30[208]. 第一次遇到双圈覆盖时, 我就想到, 无隔边的平面嵌入, 都提供一个双圈覆盖, 和一般曲面嵌入都是双迂覆盖. 当用文 4.03[158] 中揭示的方法, 通过变换, 总可得到, 除非有桥(即隔边), 一个双圈覆盖, 就企图证明这是一个事实, 而未终.

在这个过程中, 使我除澄清, 双圈覆盖与曲面嵌入, 的关系外, 还发现了一批, 与之密切相关的猜想. 这就形成了文 4.30[208].

考虑到结构对称性的研究, 见文 4.57[288], 4.59[293], 4.61[298] 和 4.67 [327] 等. 这些对于此后, 将一个图所产生的曲面嵌入, 以至地图, 进行分类, 提供了一些基础性的贮备.

刘彦佩
2015 年 5 月
於北京上园村

第四编目录

Vol. 12 Suppl. Systems Science and Mathematical Sciences May, 1999

NEW APPROACHES TO THE GRAPHICNESS OF A MATROID

Dedicated to Professor Wu Wenjun on the occasion of his 80-th birthday

LIU Yanpei
(*Institute of Mathematics, Northern Jiaotong University, Beijing 100044 China*)

Abstract. This article provides some new characterizations for testing if a matroid is graphic. One of them can be seen as a consequence deduced from the Wu's theory on the planarity of graphs.

Key words. Matroid, graphicness, basic order.

1. Introduction

Many equivalent definitions used for matroids appear in the literature. We here adopt that a *matroid* is a family $\mathcal{Z}$ of subsets on a finite set E, which is called the *base set*, with the two axioms below being satisfied. The cardinality of E is called the *order* of M, and that of $\mathcal{Z}$, the *size* of M.

Axiom 1 No member of $\mathcal{Z}$ is a proper subset of another.

Axiom 2 Let a and b be two distinct elements of E. Let X and Y be members of $\mathcal{Z}$ such that $a \in X \cap Y$ and $b \in X \setminus Y$. Then, there exists $Z \in \mathcal{Z}$ such that $b \in Z \subseteq (X \cup Y) - a$.

A matroid is usually denoted by $M = (\mathcal{Z}, E)$, or simply M when it is not necessary to identify the base set E. Members of $\mathcal{Z}$ are said to be *circuits*. An element of E is called a *cell* of M. Two matroids $M_1 = (\mathcal{Z}_1, E_1)$ and $M_2 = (\mathcal{Z}_2, E_2)$ are said to be *isomorphic* if there is a bijection $\tau : E_1 \to E_2$ such that $\forall C_1 = \{e_1, e_2, \cdots, e_s\} \in \mathcal{Z}_1$,

$$\tau(C_1) = \{\tau(e_1), \tau(e_2), \cdots, \tau(e_s)\} = C_2 \in \mathcal{Z}_2. \tag{1}$$

Two isomorphic matroids M_1 and M_2 are represented by $M_1 \cong M_2$. Although only one element is allowed to be a circuit which is called a *loop*, we shall never consider a matriod with a loop because loops are inessential for our purpose here.

Let $G = (V, E)$ be a graph. It is easily checked that the set $\mathcal{Z}(G)$ of all circuits in G forms a matroid $M(G) = (\mathcal{Z}(G), E)$ which is called the *circuit matroid* of G. Similarly, the set $\mathcal{Z}^*(G)$ of all cocircuits in G forms another matroid $M^*(G) = (\mathcal{Z}^*(G), E)$ called the *cocircuit matroid* of G.

For a matroid M, if there is a graph G such that M is isomorphic to $M(G)$, or $M^*(G)$, then it is respectively said to be *graphic*, or *cographic*.

The determination of a matroid for the graphicness or cographicness was first done by Tutte in the 50s[1]. However, in this article, we provide some new characterizations of the graphicness or cographicness of a matroid in a way different from Tutte's.

Although one of them can be seen as a consequence deduced from the Wu's theory [2–3] on the planarity of graphs with involvements, to find a direct way for doing so is still an open problem.

2. Spaces Over GF(2)

Let $\mathcal{E}$ be the space generated by $\{e \mid \forall e \in E\}$ and denoted by $\langle e \mid \forall e \in E\rangle$ over a field $\boldsymbol{F}$. For a vector $f \in \mathcal{E}$, let $E(f)$ be the subset of E, in which each element corresponds to a nonzero component of f. We also employ the notation f itself instead of $E(f)$ if there is no confusion and call $E(f)$ the *support* of f. An *integral vector* f, that is, one with all its components being integers in the group $\mathcal{N}$ of vectors over the integer ring, is called *elementary* if the support $E(f)$ is minimal for $\mathcal{N}$, i.e., no vector g in $\mathcal{N}$ has the property that $E(g)$ is a proper subset of $E(f)$.

If $\mathcal{E}$ is binary, i.e., over $\boldsymbol{F} = \mathrm{GF}(2)$, then it is easily checked that the family $\mathcal{Z}(\mathcal{N};2)$ which consists of all the subsets corresponding to the elementary vectors in $\mathcal{N}$ forms a matroid which is denoted by $M(\mathcal{N};2)$. A matroid which is isomorphic to $M(\mathcal{N};2)$ for a group $\mathcal{N}$, a subspace as well if $\mathcal{N} \subseteq \mathcal{E}$ over GF(2) is said to be *binary* as well. In general, we may take $\boldsymbol{F}$ to be the rational field or the real field. If an elementary vector for a group $\mathcal{N}$ of vectors over the integer ring has all its nonzero components be 1 or -1, then it is said to be *primitive*. It is also easily shown that the family of subsets which correspond to primitive vectors in $\mathcal{N}$ forms a matroid as well, which is denoted by $M(\mathcal{N})$. A matroid which is isomorphic to $M(\mathcal{N})$ for a group $\mathcal{N}$, called *regular*, i.e., to each elementary vector there corresponds a primitive one with the same support, is said to be *regular* as well. Because for each primitive vector there exists an elementary one with the same support, we soon see that any regular matriod is binary.

Lemma 1 *If $M = (\mathcal{Z}, E)$ is a binary matroid, then $\forall C_1, C_2 \in \mathcal{Z}$,*

$$\exists C_3 \in \mathcal{Z} : C_3 \subseteq C_1 \bigoplus C_2 \tag{2}$$

where $C_1 \bigoplus C_2 = (C_1 \cup C_2)\backslash(C_1 \cap C_2)$ is called the symmetric difference between C_1 and C_2.

Proof Because M is binary, there exists a group $\mathcal{N}$ in $\mathcal{E}$ over GF(2) such that M is isomorphic to $M(\mathcal{N};2)$. Since the vector $f = f(C_1) + f(C_2) \in \mathcal{N}$ and $E(f) = C_1 \bigoplus C_2 \in \mathcal{Z}(\mathcal{N};2) = \mathcal{Z}$, we have an elementary vector f_0 in $\mathcal{N}$ such that $E(f_0) \subseteq E(f)$. Hence, $C_3 = E(f_0)$ satisfies (2). ∎

If $M = (\mathcal{Z}, E)$ is a binary matroid which is isomorphic to $M(\mathcal{N})$ for $\mathcal{N}$ as an Abelian group in $\mathcal{E}$ over GF(2), then the matriod which is isomorphic to $M(\mathcal{N}^{\perp})$ for the orthogonal subspace $\mathcal{N}^{\perp}$ of $\mathcal{N}$ in $\mathcal{E}$ is called the *dual matroid* of M and denoted by $M^* = (\mathcal{Z}^*, E)$. Members of $\mathcal{Z}^*$ are called *cocircuits*. Of course, $\mathcal{Z}^*$ is a binary matroid as well.

Lemma 2 *If M is a binary matroid and M^*, its dual, then $\forall C \in \mathcal{Z}, C^* \in \mathcal{Z}^*$,*

$$| C \bigcap C^* | = 0 \pmod 2. \tag{3}$$

Proof A direct consequence of the orthogonality between $\mathcal{Z}$ and $\mathcal{Z}^*$. ∎

A subset of E which does not contain a circuit is said to be *independent*, and otherwise, *dependent*. Because $\emptyset$ is never a circuit, we see that $\emptyset$ is independent. Moreover, it is also easy to verify that any subset of an independent subset is independent.

Lemma 3 *For a binary matroid $M = (\mathcal{Z}, E)$, let C_1 and C_2 be two distinct circuits and $A = C_1 \bigoplus C_2$. Then, $\exists C_1, \cdots, C_s \in \mathcal{Z} \ni$*

$$A = \sum_{i=1}^{s} C_i \tag{4}$$

where the summation represents the disjoint union of sets.

Proof Suppose M is isomorphic to $M(\mathcal{N})$ for $\mathcal{N}$ in $\mathcal{E}$ over GF(2). We know that every non-zero vector of $\mathcal{N}$ corresponds to a dependent subset of E. From Lemma 1, A contains a circuit C_1. Because the vector $f(A_1)$ for $A_1 = A \bigoplus C_1$ is in $\mathcal{N}$, A_1 is dependent either. Let C_2 be a circuit in A_1. We consider $A_2 = A_1 \bigoplus C_2$ instead of A_1. From the finiteness of E, the expression (4) can always be found. ∎

Because for two independent subsets X and Y, if $|X| = |Y| + 1$, then there exists $x \in X \backslash Y$ such that $Y \cup x$ is independent, it can be verified that all *maximal independent subsets*, i.e., each of which is not a proper subset of an independent subset, have the same cardinality which is called the *rank* of the matroid. A maximal independent subset is called a *base* denoted by $B(M)$, or simply B. We may also show that for $e \notin B$, there is exactly one circuit in $B \cup e$, which is called the *fundamental circuit* denoted by $C(B; e)$ of e on the matroid for B.

Lemma 4 *For a binary matroid $M = (\mathcal{Z}, E)$, let B be a base of M. Then, for a circuit C, $C \backslash B = \{e_1, e_2, \cdots, e_s\}$, we have*

$$C = \bigoplus_{1 \leq i \leq s} C(B; e_i). \tag{5}$$

Proof From what was discussed in [4, Chapter 3], we see that all the fundamental circuits form a basis of the subspace generated by the group $\mathcal{N}$ for which M is isomorphic to $M(\mathcal{N}; 2)$. Because any circuit corresponds to a vector in $\mathcal{N}$, the expression of C as a linear combination of vectors w.r.t. the basis just corresponds to (5). ∎

Let $M = (\mathcal{Z}, E)$ be a matroid, not necessarily binary. For a subset S of E, let

$$\mathcal{L} = \{A \mid (A \subseteq S) \wedge (A \in \mathcal{Z})\} = \mathcal{Z} \cap S.$$

Easy to check that $L = (\mathcal{L}, S)$ is a matroid. L is called the *reduction* of M to S and denoted by $M \cdot S$. For a subset $T \subseteq E$, let

$$\mathcal{P} = \{A \mid A = C \cap T \neq \emptyset, C \in \mathcal{Z}\}.$$

Easy to check that $P = (\mathcal{P}, T)$ is a matroid as well. P is called the *contraction* of M to T and denoted by $M \times T$. A matroid which can be represented in the form $(M \cdot S) \times T$ is called a *minor* of M. It can be shown that a minor of a minor of a matroid M is a minor of M.

Lemma 5 *A minor of a binary matroid is binary.*

Proof Because the corresponding operations; reduction and contraction, on a group in a space produce new groups in the space over GF(2), by the definition of binary matroid the lemma is found. ∎

By no means any matroid is binary. It can be seen that the matroid $U(4, 3)$, whose base set consists of four elements a, b, c and d with all the subsets which consist of three elements as circuits, has two circuits $\{a, b, c\}$ and $\{a, b, d\}$ with the symmetric difference $\{c, d\}$ without a subset which is a circuit. From Lemma 1, $U(4, 3)$ is not binary. Moreover, $U(4, 3)$ is the only non-binary matroid with the least order and size.

Lemma 6 *For a binary matroid M,*

$$\nexists S, T \subseteq E: \ (M \cdot S) \times T \cong U(4, 3). \tag{6}$$

Proof A direct consequence of Lemma 5. ∎

Furthermore, all the concepts on independence, cocircuits, base, duality and so on introduced above for binary matroids can be extended to those for general matroids. A subset of E is said to be *independent* for a matroid $M = (\mathcal{Z}, E)$ not necessarily to be binary if it does not contain a circuit in $\mathcal{Z}$. A *base* of M is a maximal independent subset. Because all maximal independent subsets have the same cardinality, the cardinality of a base is called the *rank* of M. A subset of E is called a *cocircuit* for M if it is miminal for the property that it has non-null intersection with any base of M. It can be shown that the family $\mathcal{Z}^*$ of all cocircuits for M determines a matroid on E which is called the *dual matroid* of M, denoted by $M^* = (\mathcal{Z}^*, E)$. Easy to see that $M^{**} = M$. The complement of a base of M on E is a base of M^* which is called a *cobase* of M. The cardinality of a cobase is called the *corank* of M. Because we also have that each element in a cobase $\bar{B}$ of M forms exactly one circuit with its corresponding base B, the circuit is call a *fundamental circuit* of M. Likewise, the cocircuit formed by an element in B with $\bar{B}$ is called a *fundamental cocircuit* of M.

Lemma 7 *For a matroid M not necessarily to be binary, the conditions* (2–6) *are all equivalent one to another.* ∎

Because of the limitation of space, we are not allowed to present a complete proof of the lemma, the reader is referred to [5–7],[8] and [9].

Theorem 1 *A matroid $M = (\mathcal{Z}, E)$ is binary iff one of the conditions* (2–6) *is satisfied.*

Proof From Lemmas 1–4 and Lemmas 6–7, it suffices to prove that one of the conditions (2–6) is sufficient for M to be binary. We only take condition (5). If a subset S of E is represented by the vector $f(S)$ over GF(2) such that a component of f is non-zero, *i.e.* 1, iff its corresponding element is in the subset S, then the symmetric difference on subsets is just the addition (mod 2) on vectors. Because the condition (5) provides the expression of a vector which corresponds to a circuit in M as a linear combination of vectors w.r.t. a basis, which correspond to the fundamental circuits, it is allowed to extend all the linear combinations of the vectors corresponding to fundamental circuits of M to a subspace $\mathcal{N}$ which is an Abelian group as well in $\mathcal{E}$ over GF(2). From Axiom 2 of a matriod, all the elementary vectors have to be circuits in $\mathcal{Z}$. Therefore, $M = (\mathcal{Z}, E) \cong M.(\mathcal{N}; 2)$, and hence is binary. ∎

Lemma 8 *A matroid M is binary iff so is its dual matroid M^**

Proof In fact, M and M^* are respectively produced by two subspaces: $\mathcal{N}$ and its orthogonal $\mathcal{N}^{\perp}$ in $\mathcal{E}$. The lemma is obtained. ∎

From Lemma 8 and Theorem 1, we may soon find

Theorem 2 *A matroid $M = (\mathcal{Z}, E)$ is binary iff one of the following conditions is satisfied:*

(i) *For any two cocircuits C_1^* and C_2^* of M, there exists a cocircuit C_3^* such that $C_3^* \subseteq C_1^* \bigoplus C_2^*$;*

(ii) *For any two distinct cocircuits C_1^* and C_2^*, the symmetric difference of them can be expressed as a disjoint union of cocircuits of M;*

(iii) *For a cobase $\bar{B} = \{e_1, e_2, \cdots e_s\}$, any cocircuit can be represented by the symmetric difference of the fundamental cocircuits;*

(iv) *The dual matroid M^* does not have a minor isomorphic to $U(4, 3)$.* ∎

In fact, one may see that any subset of two elements in $\{a, b, c, d\}$ is a base of the matroid

$$U(4,3) = (\{abc, abd, acd, bcd\}, \{a, b, c, d\})$$

and hence a cobasis. That means $U(4,3) = U^*(4,3)$. A matroid whose dual matroid is isomorphic to itself is said to be *self-dual.* Thus, $U(4,3)$ is a self-dual matroid.

A matroid M on E is said to be *representable over a field* $\boldsymbol{F}$ if there exists a bijection $\tau : E \rightarrow \mathcal{V}$ such that τ preserves the linear independence where $\mathcal{V}$ is a subset of a vector space over $\boldsymbol{F}$. For a matroid M, if there exists a field such that M is representable over the field then it is called *representable.*

Lemma 9 *Let $\mathcal{N}$ be a regular group on E over the integer ring. Then, for any $f \neq 0, f \in \mathcal{N}$, being an integral vector, there exist primitive vectors $f_1, f_2, \cdots, f_s$ which are with the same support as f such that*

$$f = \sum_{i=1}^{s} f_i. \tag{7}$$

Proof Let

$$\mathrm{sum}(a) = \sum_{e \in E} | u(e) |$$

for a vector $u \in \mathcal{N}$. We may choose f to be one of those which do not satisfy the lemma with the *sum* minimum if the lemma fails. Suppose g is the primitive vector with the same support as f. We write $h = f - g$. Of course, if $h = 0$ then $f = g$. If $h \neq 0$, from the regularity, we have $\mathrm{sum}(h) < \mathrm{sum}(f)$ and $E(h) = E(f)$. Therefore, h is a sum of primitive vectors with the same support as f. In both cases, we find f is such a sum as the lemma indicates. This is a contradiction to the choice of f. ▮

For an integer $p \geq 2$, if an integral vector f has all its components with absolute values less than p, then it is said to be *standard* for p.

Lemma 10 *Let $\mathcal{N}$ be a regular group on E. Then for each $q \geq 2$ and for each integral vector $g \in \mathcal{N}$, there is a standard vector f such that $f = g$ (mod q).*

Proof For an integral vector j, let $n_q(g)$ be the number of elements $e \in E(g) : | j(e) | \geq q$. We may choose an integral vector f:

$$n_q(f) = \min\{n_q(g) \mid j = g(\bmod\ q)\}.$$

If $n_q(f) > 0$, suppose $| f(a) | \geq q, a \in E(f)$. From Lemma 9, let the primitive vector h be such that $E(h) = E(f)$ and $h(a) \neq 0$. We write $f_1 = f - qh$. From $| f_1(a) | < | f(a) |$ and $f(a) < q \Rightarrow f_1(a) < q$, we have $n_q(f_1) \leq n_q(f)$ with the equality iff $f_1(a) \geq q$. If so, we may do the same procedure for f_1 instead of f. From the finiteness of $f(a)$ we may finally find f' such that $n_q(f') < n_q(f)$. This is a contradiction to the choice of f. ▮

Lemma 11 *Let $M = (\mathcal{Z}, E)$ be a regular metroid. Then for any prime p, there exists a regular group $\mathcal{N}$ on E over GF(p), the field of characteristic p, such that $M = M(\mathcal{N})$.*

Proof Because M is regular, there exists a regular group $\mathcal{N}'$ on E over the rational field such that $M = M(\mathcal{N}')$. For each $f' \in \mathcal{N}'$, let f be the vector over GF(p) defined by

$$f(a) = f'(a)(\bmod\ p), \quad \forall a \in E. \tag{8}$$

It can be shown that the set $\mathcal{N}$ of all standard vectors each of which satisfies (8) for a vector f' in $\mathcal{N}'$ forms a group on E over GF(p). In what follows, we prove that $M(\mathcal{N}') = M(\mathcal{N})$.

Let $C' \in \mathcal{Z}$. From $M = M(\mathcal{N}')$, there exists a primitive vector $h' \in \mathcal{N}'$ such that

$$E(h') = C'.$$

Consider the standard vector h which corresponds to h'. Then $E(h) = C'$. That implies C' is dependent in $M(\mathcal{N})$. Hence, there exists a circuit C of $M(\mathcal{N})$ such that $C \subseteq C$.

On the other hand, let C be a circuit of $M(\mathcal{N})$. There is a vector $f \in \mathcal{N}$ such that

$$E(f) = C.$$

But this means there exists $f' \in \mathcal{N}'$ such that $C \subseteq E(f')$. If $a \in E(f')\backslash C$, then $f'(a) = 0$ (mod p). However, from Lemma 14.2.2, there exists a standard vector h' such that $E(h') = E(f) = C$, or in other words C, is dependent in $M(\mathcal{N}')$. Hence, there exists a circuit C' in $M(\mathcal{N}')$ such that $C' \subseteq C'$.

Combining the two facts above, we have $M(\mathcal{N}) = M(\mathcal{N}')$. The lemma is obtained. ▮

Lemma 12 *If a matroid M is regular, then M is representable over every field.*

Proof From the definition of a regular matroid, it is natural that M is representable over the rational field and hence over any field of characteristic zero. Further, from Lemma 11, we can see that M is representable over GF(p) and hence over any field of characteristic p. From the classification of fields according to the characteristic, the lemma is obviously obtained. ▮

Let $D(M)$ be the incident matrix of a matroid $M = (\mathcal{Z}, E)$ with rows corresponding to circuits in $\mathcal{Z}$ and columns, elements in E, and be called the *circuit matrix* of M. Dually, the *cocircuit matrix*, denoted by $D^*(M)$ of M is the incident matrix of circuits in $\mathcal{Z}^*$ against elements in E where $M^* = (\mathcal{Z}^*, E)$ is the dual matroid of M. In other words, the cocircuit matrix of M is the circuit matrix of its dual matriod M^*, *i.e.*,

$$D^*(M) = D(M^*). \tag{9}$$

For a binary matroid M, if it is possible to assign negative sign to some of the non-zero entries in $D = D(M)$ and $D^* = D^*(M)$ such that

$$DD^{*T} = 0 \tag{10}$$

over the integer ring, then M is said to be *orientable*.

Lemma 13 *If a matroid M is regular, then M is orientable.*

Proof Because M on E is regular, there exists a group of integral vectors $\mathcal{N}$ such that $M = M(\mathcal{N})$. For a circuit C of M, we have a primitive vector $f \in \mathcal{N}$ such that $E(f) = C$. In the row of the circuit matrix D of M corresponding to C, we assign a positive or a negative sign to the entry according as the corresponding component is $+1$ or -1. And likewise, orient the cocircuit matrix D^* in agreement with the assignment of signs on the circuit matrix of the dual matroid $M^* = M(\mathcal{N}^*)$. Because of the orthogonality of the groups of vectors $\mathcal{N}$ and $\mathcal{N}^* = \mathcal{N}^{\perp}, D$ and D^* with signs defined on the entries satisfy (10). This is the lemma. ∎

For a binary matroid M with a base B given, the incident matrix of fundamental circuits against elements is called the *fundamental matrix* of M. And, the *cofundamental matrix* of M is defined to be the fundamental circuit of its dual M^* for the cobase $\bar{B}$ corresponding to B. If a matrix over the rational field has all the determinants of its submatrices being 0, 1 or -1, then it is said to be *totally unimodular*.

Lemma 14 *If a matroid M is regular, then for any base its fundamental matrix is totally unimodular.*

Proof From the regularity and Lemma 9, we are allowed only to discuss the total unimodularity for the fundamental matrix of a regular space with basis consisting of primitive vectors.

For convenience, let $J(S,T)$ for $S \subseteq \overline{B}, T \subseteq B, |S| = |T|$ be the submatrix of the fundamental matrix $J(B)$ for base B by the rows corresponding to the elements in S and the columns. to the elements in T. If $\det J(S,T) \neq 0$, then it is seen that $J(B)$ can always be transformed into $J(B'), B' = (B \backslash T) \cup S$ by the operations: permuting the rows, adding to one row another row obtained by multiplying a row by -1, and multiplying a row by -1. This implies there is a nonsingular matrix A with entries 0, 1, and -1 such that

$$\det A \ \det J(S,T) = 1.$$

Because both $\det A$ and $\det J(S,T)$ are integers, it is only possible that

$$\det J(S,T)$$

is 1 or -1. From the arbitrariness of the choices of B and (S,T), the lemma follows. ∎

A binary matroid is said to be *totally unimodular* if so is one of its fundamental matrices.

The simplest example of a binary matroid which is not regular is the *Fano matroid* which is on a set of seven elements $\{e_1, e_2, \cdots, e_7\}$ with the circuits as

$$\{X_{126}, X_{135}, X_{247}, X_{234}, X_{257}, X_{367}, X_{456}\} \tag{11}$$

where $X_{ijk} = \{e_t \mid 1 \le t \le 7, t \ne i, j, \text{and } k\}$ for $1 \le i < j < k \le 7$.

Lemma 15 *If a matroid is regular, then it does not contain Fano matroid or its dual as a minor.*

Proof Because it can be verified as in the proof of Lemmas 5 and 8 that any minor of a regular matroid is also regular and that a matroid is regular iff so is its dual then from the definition of a regular matroid, by the above description of the Fano matroid the lemma is deduced. ∎

For a binary matroid M, if its fundamental matrix over GF(2) does not have a submatrix from which the following matrix

$$X = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}$$

or its transpose X^{T} can be obtained by permuting rows and columns, then M is said to be X-*free*.

Lemma 16 *If a binary matroid M is regular then its fundamental matrix over* GF(2) *is X-free.*

Proof A direct consequence of Lemma 15, by the non-regularity of Fano matroid and its dual none of which is X-free. ∎

Lemma 17 *For a binary matroid M, the following statements are equivalent:*

(i) *M is representable over every field;*

(ii) *M is orientable;*

(iii) *M is totally unimodular;*

(iv) *M has no minor which is isomorphic to Fano matroid or its dual;*

(v) *M is X-free.* ∎

The proof is left to the reader [6, 10, 11].

Theorem 3 *A binary matroid M is regular iff M satisfies one of the statements* (i–v) *in Lemma* 17.

Proof The necessity is obtained from Lemmas 12–16. It suffices to prove the regularity of M from the statement (i) for the sufficiency by using Lemma 17. However, this is obvious from the definition of a regular matroid. ∎

Of course if M is replaced by its dual M^* in (i–v) of Lemma 17, then the theorem assumes its dual form.

3. Graphic Matroids

For a graph $G = (V, E)$, let $\mathcal{R}(G)$ be the space generated by $\{e \mid \forall e \in E\}$ over the rational field. Let $\mathcal{C}$ and $\mathcal{C}^{\perp}$ be the groups of the integral vectors in $\mathcal{R}$, called the cycles and the cocycles of G as discussed in [4,§3.1] respectively. Further, let $Z(G) = M(\mathcal{C})$ and

$$Z^{\perp}(G) = M(\mathcal{C}^{\perp})$$

be the circuit matroid and the cocircuit matroid of G respectively because it can be verified that the families of subsets of E in $Z(G)$ and $Z^{\perp}(G)$ are all circuits and cocircuits on G.

Lemma 18 *Both $Z(G)$ and $Z^{\perp}(G)$ are binary.*

Proof Because if $\mathcal{R}(G)$ is taken to be the space over GF(2), then $\mathcal{C}$ and $\mathcal{C}^{\perp}$ are the cycle space and the cocycle space as shown in [4], from the definition of binary matroids in Section 2, the lemma naturally follows. ∎

Lemma 19 *Let $Z^*(G)$ be the dual matroid of the matroid $Z(G)$ for a graph $G = (V, E)$. Then*

$$Z^*(G) = Z^{\perp}(G).$$

Proof From the orthogonality of the cycle space and the cocycle space of a graph and the definition of the dual matroid of a binary matroid in Section 2, the lemma is obtained. ∎

Lemma 20 *Both $Z(G)$ and $Z^{\perp}(G)$ are regular.*

Proof From Lemma 19 and the fact that a matroid is regular iff so is its dual matroid, it suffices to prove the regularity of $Z(G)$ only. Because $Z(G)$ is binary from Lemma 18, all the members of subsets in $Z(G)$ can be represented by vectors over GF(2). We may assign to each edge a direction on G and define the vector $f = f(C)$ for $C \in Z(G)$ as

$$f(e) = \begin{cases} 1, & \text{if } e \in C \text{ and } e \text{ is in the clockwise direction of } C; \\ -1, & \text{if } e \in C \text{ and } e \text{ is in the anticlockwise direction;} \\ 0, & \text{otherwise.} \end{cases}$$

Because any cocircuit $C^* \in Z^{\perp}(G)$ has the form:

$$C^* = (X, Y) = \{(x, y) \mid \forall x \in X, y \in Y, (x, y) \in E\}$$

where $Y = V \backslash X$, the vector $f^* = f(C^*)$ for $C^* \in Z^{\perp}(G)$ is defined to be

$$f^*(e) = \begin{cases} 1, & \text{if } e = (u, v) \in C^* \text{and } u \in X, v \in Y; \\ -1, & \text{if } e = (u, v) \in C^* \text{and } u \in Y, v \in X; \\ 0, & \text{otherwise.} \end{cases}$$

Because for any $C \in Z(G)$ and $C^* \in Z^{\perp}(G)$, from the orthogonality we always have

$$\sum_{e \in E} f(e) f^*(e) = 0.$$

Such an orientation shows that $Z(G)$ is orientable. From Theorem 3, the lemma is derived. ∎

For a matroid M, if there exist corank$(M) + 1$ circuits (in general, cycles) such that each element of E appears in exactly two circuits among them, then M is said to be *over corank 2-coverable*. Dually, if there exist rank$(M) + 1$ cocircuits (in general, cocycles) such that each element of E appears in exactly two cocircuits among them, then M is said to be *over rank 2-coverable*. Of course, from the duality M is over rank 2-coverable iff M^* is over corank 2-coverable.

Lemma 21 *If M is a graphic matroid, then M^* is over corank 2-coverable.*

Proof Because M is graphic, there is a graph G such that $M \cong Z(G)$, the circuit matroid of $G = (V, E)$. Let $C^*(v)$ be the cocircuit (in general, cocycle) which consists of all the edges incident with v in G. Because each edge has two ends, it appears in exactly two cocircuits among all $C^*(v), v \in V$. Therefore, M^* is over corank 2-coverable. ∎

For a binary matroid $M = (\mathcal{Z}, E)$, let Cycl(M) be the space of vectors over GF(2) which is generated by all the vectors corresponding to the subsets in $\mathcal{Z}$. We call Cycl(M) the *cycle space* of M.

A family of subsets on E, each of which corresponds to a vector of the space Cycl(M) with the property that each element of E belongs to exactly two subsets in the family, is said to be a *double covering* of M. For a double covering $\mathcal{D}$ of M, let Boun$(M; \mathcal{D})$ be the space of vectors over GF(2), which is generated by all the vectors corresponding to the subsets in $\mathcal{D}$. We call the space Boun$(M; \mathcal{D})$ a *boundary space* of M for $\mathcal{D}$.