SCHOOL OF OPERATIONS RESEARCH
AND INDUSTRIAL ENGINEERING
COLLEGE OF ENGINEERING
CORNELL UNIVERSITY
ITHACA, NEW YORK 14853

TECHNICAL REPORT NO. 737

March 1987

ON ABSTRACT INTEGRAL DEPENDENCE

By

Donna Crystal Llewellyn¹
L.E. Trotter, Jr.²

¹School of ISyE, Georgia Institute of Technology, Atlanta, Georgia. Research supported by NSF grant ECS-81-13534 and NSF Postdoctoral Fellowship DMS 84-14104.

²School of OR & IE, Cornell University, Ithaca, New York. Research supported by NSF grants ECS-13534 and ECS 85-04077.

ABSTRACT

The concept of a tag system is introduced. In its general form the combinatorial structure of a dual pair of tag systems arises through composition of blocking pairs of clutters. This leads to a "painting" characterization for dual pairs of tag systems which is useful for establishing combinatorial theorems of the alternative for certain classes of tag systems. Integral tag systems arise as a natural combinatorial abstraction of integral linear dependence properties of rational vectors in analogy with the manner in which matroids arise from linear dependence properties. Tag systems subsume matroids and several characterizations of matroids as tag systems are given; however, tag systems are shown to be generally less tractable computationally than matroids by establishing NP-completeness for the problem of determining a smallest base for an integral tag system.

1. Introduction

Suppose $A \in \mathbb{Q}^{m \times n}$ and $b \in \mathbb{Q}^m$, where $\mathbb{Q}$ denotes the rationals and (below) $\mathbb{Z}$ denotes the integers. The following three theorems of the alternative are well-known -- see Schrijver (1986) for a discussion of the historical references for these results.

1.1 Theorem: (see, e.g., Gale (1960)): Exactly one holds:

$$(1.1.1) \quad \exists x \in \mathbb{Q}^n \text{ such that } Ax = b;$$

$$(1.1.2) \quad \exists y \in \mathbb{Q}^m \text{ such that } yA = 0 \text{ and } yb \neq 0.$$

□

1.2 Theorem: (Farkas (1902); see, e.g., Dantzig (1963)):

Exactly one holds:

$$(1.2.1) \quad \exists x \in \mathbb{Q}_+^n \text{ such that } Ax = b;$$

$$(1.2.2) \quad \exists y \in \mathbb{Q}^m \text{ such that } yA \geq 0 \text{ and } yb < 0.$$

□

1.3 Theorem: (see, e.g., Edmonds and Giles (1977)):

Exactly one holds:

$$(1.3.1) \quad \exists x \in \mathbb{Z}^n \text{ such that } Ax = b;$$

$$(1.3.2) \quad \exists y \in \mathbb{Q}^m \text{ such that } yA \in \mathbb{Z}^n \text{ and } yb \notin \mathbb{Z}.$$

□

Theorems 1.1 and 1.2 can be derived as direct consequences of "painting" results in matroid theory. Suppose $M = (E, C)$ is the matroid defined on the set $E = \{1, 2, \dots, n, n+1\}$ with circuits C corresponding to minimal (linearly) dependent sets of columns of the matrix $[A \mid -b]$. The

cocircuits C^* of M then correspond to supports of elementary vectors in the row space of $[A \mid -b]$. (For background material in matroid theory we refer the reader to Welsh (1976).) Then 1.1 can be deduced immediately from the following "painting" theorem.

1.4 Theorem: (Minty (1966)): Suppose C and C^* are clutters defined on E . Then (E, C) and (E, C^*) are a dual pair of matroids if and only if for any red (R), blue (B) and white (W) painting of E with $|R| = 1$, exactly one holds:

$$(1.4.1) \quad \exists C \in C \text{ such that } R \subseteq C \subseteq R \cup B;$$

$$(1.4.2) \quad \exists C^* \in C^* \text{ such that } R \subseteq C^* \subseteq R \cup W.$$

□

Restricting attention to orientable matroids leads to a sharpening of 1.4, from which 1.2 is deduced for the $[A \mid -b]$ setting discussed above. A clutter C gives rise to a family $\Sigma(C)$ of "signed sets" through association of signs $+, -$ with individual elements of members of C . I.e., to each $C \in C$ corresponds a signed set $S \in \Sigma(C)$ which is partitioned into positive (S_+) and negative (S_-) elements. Let $\Sigma^-(C)$ denote the "opposite" family of signed sets obtained by reversing the signs on elements of members of $\Sigma(C)$ and let $S = \Sigma(C) \cup \Sigma^-(C)$. We refer to S as an **oriented clutter**.

1.5 Theorem: (Bland and Las Vergnas (1979)): Suppose S and S^* are nontrivial oriented clutters defined on E . Then (E, S) and (E, S^*) are a dual pair of oriented matroids if and only if for any red (R), blue (B) and white (W) painting of E with distinguished element $i \in R$, exactly one holds:

$$(1.5.1) \quad \exists S \in S \text{ with } i \in S_+, S_- \cap R = \emptyset \text{ and } S \subseteq R \cup B;$$

$$(1.5.2) \quad \exists S^* \in S^* \text{ with } i \in S_+^*, S_-^* \cap R = \emptyset \text{ and } S^* \subseteq R \cup W.$$

□

Thus, in the sense described above, 1.1 and 1.2 may be viewed as combinatorial results. In the following section we introduce a combinatorial structure, the "tag system", which generalizes the notion of a matroid. The specific class of tag systems which are "integral" arises through the combinatorial abstraction of integral linear dependence properties of rational vectors in much the same way that matroids arise from rational linear dependence properties. We first define tag systems in terms of a span function in Section 2 below and then give an equivalent "circuit" axiomatization in Section 3. In Section 4 we characterize integral tag systems and show that the problem of determining a smallest base of an integral tag system is NP-Complete in contrast to the corresponding situation for matroids. In Section 5 we discuss the relationship between tag systems and matroids, providing several characterizations of matroids as tag systems.

As generalizations of matroids, tag systems satisfy a "painting" theorem which subsumes 1.4 (see Theorem 3.3 below). This suggests that for certain classes of tag systems one may interpret this "painting" result to derive theorems of the alternative such as those cited earlier. In Section 7 below we obtain Theorem 1.3 from integral tag systems and analogously we show how to derive 1.2 from those tag systems arising from conical (nonnegative) linear dependence.

The results we present here were developed primarily in Crystal (1984), proceeding from a circuit axiomatization of tag systems to an equivalent span axiomatization, i.e., the reverse of that given in Sections 2 and 3 below. We are indebted to an anonymous referee who introduced us to work of Higgs (1969) and Klee (1971) and its intimate relation to tag systems. This relationship is discussed in Section 2, where we now introduce tag systems through the span axiomatization in order to make use of the earlier Higgs and Klee material. We are also indebted to R.G. Bland for the observation that dual pairs of general tag systems may be viewed as "compositions" of blocking pairs of clutters. This equivalence is presented in Section 6 below.

2. Span Axiomatization

We define a **tag system** as a pair, (E, σ) , where E is a finite **ground set** and $\sigma: 2^E \rightarrow 2^E$ is the **span function**, which must satisfy $S_1 \subseteq \sigma(S_1) \subseteq \sigma(S_2)$ whenever $S_1 \subseteq S_2 \subseteq E$. This corresponds to an "enlarging operator" of Klee (1971) and a "space" in Higgs (1969) where every set is required to be "pithy."

Given a tag system $T = (E, \sigma)$, define the function $\sigma^*: 2^E \rightarrow 2^E$ by $\sigma^*(S) = S \cup \{j: j \notin \sigma((E \setminus S) \setminus \{j\})\}$. Then (E, σ^*) is also a tag system, called the **dual tag system**. Further, for $\sigma^{**}(S) = S \cup \{j: j \notin \sigma^*((E \setminus S) \setminus \{j\})\}$, one sees easily that $\sigma^{**} = \sigma$; hence we will refer to the tag systems $T = (E, \sigma)$ and $T^* = (E, \sigma^*)$ as a **dual pair of tag systems**, noting that $T^{**} = (E, \sigma^{**}) = T$.

The following painting result is analogous to those cited above for matroids and oriented matroids.

2.1 Theorem (Higgs (1969)): Tag systems (E, σ_1) and (E, σ_2) are a dual pair of tag systems if and only if for all paintings of E into red (R), blue (B) and white (W), with $|R| = 1$, exactly one holds:

$$(2.1.1) \quad R \subseteq \sigma_1(B);$$

$$(2.1.2) \quad R \subseteq \sigma_2(W).$$

□

We call a set S **spanning** if $\sigma(S) = E$. If B is spanning and $i \notin \sigma(B \setminus \{i\})$, $\forall i \in B$, then B is called a **base**. Then B is a base of (E, σ) if and only if $E \setminus B$ is a base of (E, σ^*) .

We say a tag system $T = (E, \sigma)$ satisfies **span exchange** if $j \notin \sigma(S)$ and $j \in \sigma(S \cup \{i\}) \Rightarrow i \in \sigma(S \cup \{j\})$. Further, we call the tag system T **locally transitive** if $\sigma(\sigma(S)) = \sigma(S)$ for all subsets S .

2.2 Proposition (Higgs (1969)): The tag system $T = (E, \sigma)$ satisfies span exchange if and only if the dual tag system $T^* = (E, \sigma^*)$ is locally transitive.

□

3. Circuit Axiomatization

We now examine tag systems in terms of their "circuits." This axiom structure served as the foundation for the initial development of tag systems in Crystal (1984). It arose from a study of the combinatorial properties of integral dependence through the analogy to abstract linear dependence provided by matroids (see Section 4 below).

For tag system $T = (E, \sigma)$, we define for each $S \subseteq E$,

$$\mu(S) = \{i \in S: i \in \sigma(S \setminus \{i\}); i \notin \sigma(S \setminus \{i, k\}), \forall k \in S \setminus \{i\}\}.$$

Then for $C \subseteq E$ with $\mu(C) \neq \emptyset$, we call C a **circuit** of T and we denote $\tau(C) = \mu(C)$, the **tag function** of the circuit C . Often we will refer to $\tau(C)$ as a **tag set**. Any subset of E containing a circuit is termed a **dependent** set in T and sets containing no circuit are termed **independent**.

3.1 Theorem: $\mathcal{C} \subseteq 2^E$ is the collection of circuits of a tag system on E with tag function τ if and only if

$$(3.1.1) \quad \emptyset \neq \tau(C) \subseteq C, \quad \forall C \in \mathcal{C},$$

$$(3.1.2) \quad C_1 \subseteq C_2, C_1 \neq C_2 \Rightarrow \tau(C_1) \cap \tau(C_2) = \emptyset, \quad \forall C_1, C_2 \in \mathcal{C}.$$

Proof: First suppose that $\mathcal{C}$ and τ are given so that (3.1.1) and (3.1.2) are satisfied. We then define $\sigma: 2^E \rightarrow 2^E$ as follows,

$$\sigma(S) = S \cup \{j: \exists C \in \mathcal{C} \text{ with } C \subseteq S \cup \{j\}, j \in \tau(C)\}.$$

We will show that (E, σ) is a tag system. Let $S_1 \subseteq S_2 \subseteq E$. Clearly, $S_1 \subseteq \sigma(S_1)$. Let $j \in \sigma(S_1)$. Now either $j \in S_2$ which would imply $j \in \sigma(S_2)$, or else $j \notin S_2$. Since $j \in \sigma(S_1)$, there exists a circuit $C \in \mathcal{C}$ with $C \subseteq S_1 \cup \{j\}$ and $j \in \tau(C)$. Thus $C \subseteq S_1 \cup \{j\} \subseteq S_2 \cup \{j\}$, and so $j \in \sigma(S_2)$. It is straightforward to verify that $\mathcal{C}$ and τ are, respectively, the circuits and the tag function of the tag system (E, σ) .

Now suppose that $T = (E, \sigma)$ is a tag system and $\mathcal{C}$ is the collection of circuits of T with tag function τ . Then (3.1.1) follows immediately from the definition of τ . Now suppose that circuit C_1 is a proper subset of circuit C_2 , and further suppose that $i \in \tau(C_1) \cap \tau(C_2)$. Then, where $k \in C_2 \setminus C_1$, since $i \in \tau(C_2)$, we must have $i \notin \sigma(C_2 \setminus \{i, k\})$. Similarly, $i \in \tau(C_1)$ implies $i \in \sigma(C_1 \setminus \{i\})$. On the other hand, since T is a tag system and $C_1 \setminus \{i\} \subseteq C_2 \setminus \{i, k\}$, we must have $\sigma(C_1 \setminus \{i\}) \subseteq \sigma(C_2 \setminus \{i, k\})$, a contradiction.

□

3.2 Proposition: If $\mathcal{C}$ and τ satisfy (3.1.1) and (3.1.2) then they are the circuits and tag function, respectively, of a unique tag system.

Proof: By 3.1, we have that $\mathcal{C}$ and τ define a tag system, say $T = (E, \sigma)$, for which $\sigma(S) = S \cup \{j : \exists C \in \mathcal{C} \text{ with } C \subseteq S \cup \{j\}, j \in \tau(C)\}$, $\forall S \subseteq E$. Suppose that $T' = (E, \sigma')$ is a tag system with circuits $\mathcal{C}' = \mathcal{C}$ and tag function $\tau' = \tau$. It then follows from the definition of $\mathcal{C}'$ and τ' that $\sigma'(S) = S \cup \{j : \exists C \in \mathcal{C}' \text{ with } C \subseteq S \cup \{j\}, j \in \tau'(C)\}$, $\forall S \subseteq E$. Since $\mathcal{C}' = \mathcal{C}$ and $\tau' = \tau$, we conclude that $\sigma'(S) = \sigma(S)$, $\forall S \subseteq E$; i.e., $T = T'$.

□

This last result allows us to refer to a tag system either in terms of its span representation or its circuit and tag function definition. Defining $\mathcal{C}^*$ and τ^* from σ^* in an analogous manner to the way $\mathcal{C}$ and τ were defined from σ , we obtain the following result (compare Theorems 1.4 and 1.5).

Theorem 3.3: Suppose $T = (E, C, \tau)$ and $T^* = (E, C^*, \tau^*)$ are tag systems. Then T and T^* are a dual pair of tag systems if and only if for any red (R), blue (B) and white (W) painting of E with $|R| = 1$, exactly one of the following holds:

$$(3.3.1) \quad \exists C \in \mathcal{C} \text{ with } C \subseteq R \cup B \text{ and } R \subseteq \tau(C);$$

$$(3.3.2) \quad \exists C^* \in \mathcal{C}^* \text{ with } C^* \subseteq R \cup W \text{ and } R \subseteq \tau^*(C^*).$$

□

We discuss other properties of $\mathcal{C}^*$ and τ^* in Section 6 when we develop the relationship between dual pairs of tag systems and blocking pairs of clutters.

4. Integral Dependence

A set of rational m -vectors $\{a_1, \dots, a_n\}$ is **integrally dependent** if some element, say a_i , is an integral linear combination of the remaining vectors; i.e., $a_i = \sum_{j \neq i} (a_j x_j)$, where $x_j \in \mathbb{Z}$. Thus any rational matrix $A \in \mathbb{Q}^{m \times n}$ gives rise to a tag system $T = (E, C, \tau)$ defined on $E = \{1, \dots, n\}$, the column indices of A , by $C \in \mathcal{C}$ with $i \in \tau(C)$ if and only if the i^{th} column of A is integrally dependent on the columns indexed by $C \setminus \{i\}$ and C is minimal with respect to this property. Any tag system $T = (E, C, \tau)$ to which there corresponds a rational matrix whose integrally dependent column sets give rise to C and τ in this manner will be called **integral**. Integral tag systems thus generalize in an obvious way the combinatorial abstraction of linear dependence leading to the notion of a matroid. In the present section we characterize integral tag systems in several ways, returning to study further the relationship between tag systems and matroids in Section 5.

4.2 Proposition: Dual integral tag systems are tag-determined.

Proof: Suppose $T = (E, C, \tau)$ is the dual integral tag system defined by rational matrix A . Then for $i \in C \in C$ there corresponds a rational vector x in the row space of A , for which $i \in F(x) = C$. Thus there must exist a vector z in the row space of A for which $F(z) \subseteq F(x)$ and $F(z)$ is minimal with respect to the condition $i \in F(z)$. I.e., for $C' = F(z)$ we have $C' \in C$, $C' \subseteq C$ and $i \in \tau(C')$.

□

The converse of Proposition 4.2 holds as well, even when we restrict attention to those dual integral tag systems arising from matrices with a single row.

4.3 Theorem: Suppose $T = (E, C, \tau)$ is a tag system defined on $E = \{1, \dots, n\}$. If T is tag-determined, then T is the dual integral tag system defined by some matrix $A \in \mathbb{Z}^{1 \times n}$.

Proof: Given $T = (E, C, \tau)$ we define $A = [a_1, \dots, a_n] \in \mathbb{Z}^{1 \times n}$ as follows. Suppose $C = \{C_i : 1 \leq i \leq m\}$ and to each C_i associate a distinct prime $p_i \in \mathbb{Z}$. Then for $1 \leq j \leq n$ we define

$$a_j = \begin{cases} 0, & j \text{ is in no } C_i \\ \prod_{j \in C_i} (p_i), & \text{otherwise.} \end{cases}$$

Let $T' = (E, C', \tau')$ denote the dual integral tag system defined by matrix A . By assumption and by 4.2, both T and T' are tag-determined. We thus show $T = T'$ by showing $C = C'$.

First note that any nontrivial union of circuits of C , say $C = \bigcup (C_i : i \in I)$ for $I \subseteq \{1, \dots, m\}$, corresponds to the fractional support $F(\delta A)$ for $\delta = \frac{1}{\prod (p_i : i \in I)}$; this follows immediately from the construction of A . The converse is also true, for suppose $\alpha \in \mathbb{Q}$ and

consider $F(\alpha A) \neq \emptyset$. If $a_j = 0$ for all $j \notin F(\alpha A)$ (note this includes the case $F(\alpha A) = E$), then $F(\alpha A) = F(\delta A)$ for $\delta = \frac{1}{\pi(p_i: 1 \leq i \leq m)}$. If $a_j \neq 0$

for some $j \notin F(\alpha A)$, then let $\alpha = q/r$, where $q, r \in \mathbb{Z}$ with no common factors. Then $F(\alpha A) = F\left[\left[\frac{1}{r}\right]A\right]$ and r divides $a_j = \pi(p_i: j \notin C_i)$. Hence $F(\alpha A) = F(\delta A)$ where $\delta = \frac{1}{\pi(p_i: i \in I)}$ for some $I \subseteq \{i: j \notin C_i\}$.

Now let $C_i \in \mathcal{C}$ with $\tau(C_i) = C_i \cup (C \in \mathcal{C}: C \subsetneq C_i)$. Then $C_i = F\left[\left[\frac{1}{p_i}\right]A\right]$ and the above argument shows that $F\left[\left[\frac{1}{p_i}\right]A\right]$ is minimal for $\tau(C_i)$. Thus $C_i \in \mathcal{C}'$. Similarly, if $C' \in \mathcal{C}'$, the above argument shows $C' = \bigcup (C_i: i \in I)$ for some $I \subseteq \{1, \dots, m\}$. We have just shown that each $C_i \in \mathcal{C}'$; thus if $C' = C_i$ for no $i \in I$, we would have $C_i \cap \tau'(C') \neq \emptyset$ for some i , in contradiction to the fact that T' is tag-determined. Hence $C' = C_i \in \mathcal{C}$ for some $i \in I$.

□

4.4 Proposition: Suppose $T = (E, \mathcal{C}, \tau)$ and $T^* = (E, \mathcal{C}^*, \tau^*)$ are a dual pair of tag systems and T^* is the dual integral tag system defined by $A \in \mathbb{Z}^{1 \times n}$. Then T is the integral tag system defined by A .

Proof: Suppose $T' = (E, \mathcal{C}', \tau')$ is the integral tag system defined by A . We prove that T' and T^* are a dual pair of tag systems by illustrating that together they satisfy the painting conditions of Theorem 3.3. Suppose $E = \{1, \dots, n\}$ is painted red (R), blue (B) and white (W) with $R = \{j\}$.

First suppose there exist both $C' \in \mathcal{C}'$ with $C' \subseteq R \cup B$ and $j \in \tau'(C')$ and $C^* \in \mathcal{C}^*$ with $C^* \subseteq R \cup W$ and $j \in \tau^*(C^*)$. Since T' is integral we must have some $x \in \mathbb{Z}^n$ for which $x_j = 1$, $Ax = 0$ and $x_i \neq 0$ if and only if $i \in C'$. Since T^* is dual integral we must have $\delta \in \mathbb{Q}$ with $F(\delta A) = C^*$. Thus, denoting $A = [a_1, \dots, a_n]$,

$$0 = \delta Ax = \sum_{i=1}^n (\delta a_i) x_i = \delta a_j x_j + \sum_{i \in B} \delta a_i x_i + \sum_{i \in W} \delta a_i x_i.$$

Now, $x_i = 0$ for $i \notin C' \subseteq R \cup B$, hence $\sum_{i \in W} \delta a_i x_i = 0$. Also,

$(\sum_{i \in B} \delta a_i x_i) \in Z$, since $x_i \in Z$ and $(\delta a_i) \in Z$ for $i \in C^* \subseteq R \cup W$. But

$\delta a_j x_j \notin Z$, because $x_j = 1$ and $j \in C^* = F(\delta A)$, yielding a contradiction.

Next suppose $g = \text{g.c.d.}\{a_i : i \in B\}$. If g does not divide a_j , then we have $(a_i/g) \in Z$ for all $i \in B$ and $(a_j/g) \notin Z$. That is, $\{j\} = R \subseteq F\left[\left[\frac{1}{g}\right]A\right] \subseteq R \cup W$, and so $C^* \subseteq R \cup W$ and $R \subseteq \tau^*(C^*)$ for some $C^* \in C^*$, by Proposition 4.2. On the other hand, when g does divide a_j , then g (and hence a_j) can be written as an integral combination of the a_i , $i \in B$. A minimal such combination yields a circuit $C' \in C'$ with $C' \subseteq R \cup B$ and $j \in \tau'(C')$.

□

4.5 Proposition: The tag system $T = (E, C, \tau) = (E, \sigma)$ is tag-determined if and only if it satisfies span exchange.

Proof: Assuming T satisfies span exchange, let $C \in C$ with $i \in C \setminus \tau(C)$, $j \in \tau(C)$. Then $j \in \sigma(C \setminus \{j\})$ but, as in the proof of 3.1, $j \notin \sigma(C \setminus \{i, j\})$. Thus for $S = C \setminus \{i, j\}$, span exchange implies $i \in \sigma(C \setminus \{i\})$. Hence there exists a circuit $C_i \in C$ with $C_i \subseteq C$ and $i \in \tau(C_i)$.

Alternatively, if T is tag-determined, suppose $S \subseteq E$ and $i, j \in E$ are chosen so that $j \notin \sigma(S)$ and $j \in \sigma(S \cup \{i\})$. Thus there exists a circuit $C \in C$ with $i \in C \subseteq S \cup \{i, j\}$; so for some $C_i \subseteq C$, we have $C_i \in C$ and $i \in \tau(C_i)$. Consequently, $i \in \sigma(C_i \setminus \{i\}) \subseteq \sigma(S \cup \{j\})$, as required.

□

4.6 Proposition: The tag system $T = (E, C, \tau) = (E, \sigma)$ satisfies TCE if and only if it is locally transitive.

Proof: If TCE fails for T , then there exist $C_1, C_2 \in C$ for which $i \in \tau(C_1) \cap C_2$ and $j \in \tau(C_2) \setminus C_1$ but j is in the tag set of no circuit contained in $(C_1 \cup C_2) \setminus \{i\}$. Thus for $S = (C_1 \cup C_2) \setminus \{i, j\}$ we have $j \notin \sigma(S)$ and $j \in \sigma(\sigma(S))$.

Conversely, if for some $S \subseteq E$ we have $j \in \sigma(\sigma(S)) \setminus \sigma(S)$, then $j \in \sigma(\sigma(S))$ implies the existence of $C_2 \in \mathcal{C}$ with $C_2 \subseteq \sigma(S) \cup \{j\}$ and $j \in \tau(C_2)$. Furthermore, $j \notin \sigma(S)$ implies $C_2 \setminus \{j\}$ is not contained in S , and so for $i \in (\sigma(S) \setminus S) \cap C_2$ we have $C_1 \setminus \{i\} \subseteq S$ for some $C_1 \in \mathcal{C}$ with $i \in \tau(C_1)$. Now $i \in \tau(C_1) \cap C_2$ and $j \in \tau(C_2) \setminus C_1$. If TCE fails for C_1, C_2, i and j , then the proof is complete. Otherwise, we apply TCE to obtain $C'_2 \in \mathcal{C}$ with $C'_2 \subseteq (C_1 \cup C_2) \setminus \{i\} \subseteq (\sigma(S) \setminus \{i\}) \cup \{j\}$ and $j \in \tau(C'_2)$. Repeating the above argument we determine $C'_1 \in \mathcal{C}$ with $C'_1 \setminus \{i'\} \subseteq S$ and $i' \in \tau(C'_1)$, where $i' \in (\sigma(S) \setminus (S \cup \{i\})) \cap C'_2$. If TCE fails for C'_1, C'_2, i' and j , the proof is complete. If not, we iterate as above, next removing i' from $\sigma(S) \setminus \{i\}$. Since we remove a new element from $\sigma(S) \setminus S$ at each iteration, the process eventually terminates with failure of TCE.

□

Hence the following result is a direct consequence of 2.2.

4.7 Corollary: A tag system T satisfies TCE if and only if its dual, T^* , is tag-determined.

□

4.8 Corollary: If $T = (E, \mathcal{C}, \tau)$ is a tag system for which $\tau(C) = C$ for all $C \in \mathcal{C}$, then T^* satisfies TCE.

□

Combining all of the above results we obtain that dual integral tag systems are precisely the duals of integral tag systems, that tagged circuit exchange characterizes integral tag systems and that dual integral tag systems are characterized as tag-determined. Note also that we need only consider one-rowed integral matrices in these characterizations.

4.9 Theorem: For a dual pair of tag systems T, T^* , the following are equivalent:

- (1) T is integral;
- (2) T satisfies TCE;
- (3) T is locally transitive;
- (4) T^* satisfies span exchange;
- (5) T^* is tag-determined;
- (6) T^* is dual integral.

Proof: By 4.1, 4.2, 4.5, 4.6, 4.7 and 2.2 we have
 $(1) \Rightarrow (2) \Leftrightarrow (3) \Leftrightarrow (4) \Leftrightarrow (5) \Leftarrow (6)$. From 4.3 we obtain $(5) \Rightarrow (6)$
 and from 4.3 and 4.4 we have finally that $(5) \Rightarrow (1)$.

□

Let $G = (V, E)$ be a simple graph with vertex set V and edge set E . We now define two tag systems on V . First, let $T = (V, E, \tau)$ with $\tau(e) = e$ for $e \in E$. It is clear from Theorem 3.3 that the dual of T is given by $T^* = (V, C^*, \tau^*)$, where $C^* \in C^*$ with $i \in \tau^*(C^*)$ if and only if $C^* = \{i\} \cup \{j: \{i, j\} \in E\}$. Note that an independent set in T is simply a stable set in G and the bases of T are the maximal stable sets in G . We now relate these tag systems to the following existence question.

4.10 Problem: Given a matrix $A \in \mathbb{Z}^{1 \times n}$ and a positive integer k , is there a base of the integral tag system defined by A of size at most k ?

4.11 Theorem: Problem 4.10 is NP-Complete.

Proof: Since the Euclidean algorithm can be used to perform g.c.d. calculations for any subset of the entries in A , Problem 4.10 is in the class NP of decision problems (see Garey and Johnson (1979)). To see that 4.10 is complete in NP, we reduce the maximum stable set problem to 4.10. Let $G = (V, E)$ be an arbitrary simple graph and define tag systems $T = (V, E, \tau)$ and $T^* = (V, C^*, \tau^*)$ as indicated above. By Corollary 4.8, T^* satisfies TCE, and thus by the results of 4.9, T^* is an integral tag system arising from some matrix $A \in \mathbb{Z}^{l \times n}$, where $n = |V|$.

Clearly G has a stable set of size at least l precisely when T has a base of size at least l or equivalently (from Section 2), when T^* has a base of size at most $k = n - l$. I.e., Problem 4.10 can be used to find a maximum stable set in an arbitrary graph. Finally, note that the reduction indicated is of time polynomial in the size of G , because the construction of A as in the proof of Theorem 4.3 requires only $|C| = |E| = m$ distinct primes. Now since the number of primes not exceeding integer d is at least $\frac{d}{12 \log d}$ (see page 149, Sierpinski (1964)), these m primes can be determined and listed explicitly in polynomial time (in m).

□

5. Matroids

Suppose $M = (E, C)$ is a matroid. Then M gives rise to a tag system $T = (E, C, \tau)$ by defining $\tau(C) = C$, for each $C \in C$. If $M^* = (E, C^*)$ is the matroid dual to M , then C^* is the clutter which satisfies Minty's Painting Theorem (1.4) with C . It follows from 3.3 that the tag system dual to T is given by $T^* = (E, C^*, \tau^*)$, where $\tau^*(C^*) = C^*$ for each $C^* \in C^*$. That is, the dual pair of matroids M, M^* gives rise to the dual pair of tag systems T, T^* . Note that when this is the case, Corollary 4.8 shows that both T and T^* satisfy TCE and it thus follows that **both** T and

T^* satisfy the various properties itemized in Theorem 4.9 (both are integral, both are dual integral, etc.) In the present section we show that this is true for no other tag systems; e.g., if the tag system $T = (E, C, \tau)$ is both integral and dual integral, then $\tau(C) = C$ for all $C \in \mathcal{C}$ and $M = (E, C)$ is a matroid. This characterizes matroids as tag systems.

For a tag system $T = (E, C, \tau)$ with span function σ we enumerate now the various properties considered in Section 4:

- (1) T satisfies TCE;
- (2) T is integral;
- (3) T is locally transitive;
- (4) T is tag-determined;
- (5) T is dual integral;
- (6) T satisfies span exchange;
- (7) $\tau(C) = C$, for all $C \in \mathcal{C}$.

5.1 Theorem: Suppose $T = (E, C, \tau) = (E, \sigma)$ and $T^* = (E, C^*, \tau^*) = (E, \sigma^*)$ are a dual pair of tag systems. The following are equivalent:

(5.1.1) $M = (E, C)$ and $M^* = (E, C^*)$ are dual matroids defining T and T^* ;

(5.1.2) T satisfies (i) and T^* satisfies (j), where $i, j \in \{1, 2, 3\}$;

(5.1.3) T satisfies (i) and (j), where $i \in \{1, 2, 3\}$ and $j \in \{4, 5, 6, 7\}$;

(5.1.4) T satisfies (i) and T^* satisfies (j), where $i, j \in \{4, 5, 6, 7\}$.

Proof: Higgs (1969) shows that if both T and T^* are locally transitive, then in fact they are matroids. Hence using Theorem 4.9 and Corollary 4.8 yields the result. $\square$

6. Blocking Systems

In this section we relate tag systems to blocking pairs of clutters. A **clutter** on a finite set E is any family of noncomparable subsets of E . The **blocking clutter** C^* for a clutter C is the collection of subsets of E which have nonempty intersection with each member of C and are minimal with respect to this property. Edmonds and Fulkerson (1970) showed that the blocking clutter of C^* is C and thus (C, C^*) may be termed a **blocking pair of clutters**; they also established the following painting theorem for blocking pairs of clutters.

6.1 Theorem: (Edmonds and Fulkerson (1970)): Suppose C, C^* are clutters defined on the finite set E . Then (C, C^*) is a blocking pair of clutters if and only if for any blue (B) and white (W) painting of the elements of E , exactly one of the following holds:

$$(6.1.1) \quad \exists C \in C \text{ such that } C \subseteq B;$$

$$(6.1.2) \quad \exists C^* \in C^* \text{ such that } C^* \subseteq W.$$

$\square$

Suppose now that $E = \{1, \dots, n\}$ and that $\{(C_i, C_i^*) : 1 \leq i \leq n\}$ is a family of n blocking pairs of clutters with C_i and C_i^* defined on $E \setminus \{i\}$, $1 \leq i \leq n$. We then define $C \subseteq 2^E$ and $\tau: C \rightarrow 2^E$ as follows:

$$(6.2) \quad \begin{cases} C = \{C \subseteq E : C = C_i \cup \{i\}, C_i \in C_i \text{ for some } 1 \leq i \leq n\}, \\ \tau(C) = \{i \in C : (C \setminus \{i\}) \in C_i\}. \end{cases}$$

Denoting $T = (E, C, \tau)$ and defining $T^* = (E, C^*, \tau^*)$ analogously we then have the following direct consequence of Theorem 6.1.

6.3 Theorem: Suppose the elements of E are painted red (R), blue (B) and white (W), with $|R| = 1$ and T, T^* are defined as above. Then exactly one holds:

$$(6.3.1) \quad \exists C \in C \text{ such that } C \subseteq R \cup B \text{ and } R \subseteq \tau(C);$$

$$(6.3.2) \quad \exists C^* \in C^* \text{ such that } C^* \subseteq R \cup W \text{ and } R \subseteq \tau^*(C^*).$$

□

It is clear from Theorem 3.1 that T and T^* above are tag systems; hence Theorems 3.3 and 6.3 imply that T and T^* are a dual pair of tag systems. Thus the composition of clutters as described above gives rise to a dual pair of tag systems. On the other hand, if $T = (E, C, \tau)$ and $T^* = (E, C^*, \tau^*)$ are a dual pair of tag systems, then for each $i \in E$ we define

$$C_i = \{C_i \in E \setminus \{i\} : (C_i \cup \{i\}) \in C \text{ and } i \in \tau(C_i \cup \{i\})\},$$

$$C_i^* = \{C_i^* \in E \setminus \{i\} : (C_i^* \cup \{i\}) \in C^* \text{ and } i \in \tau^*(C_i^* \cup \{i\})\}.$$

Theorem 3.1 then shows that for each i , C_i and C_i^* are clutters on $E \setminus \{i\}$. By Theorems 3.3 and 6.1, we have that each C_i, C_i^* must be a blocking pair of clutters.

□

Hence, the construction of T and T^* via blocking pairs of clutters is equivalent to the definition of T and T^* as a dual pair of tag systems.

7. Theorems of the Alternative

We now consider again the theorem of the alternative for integer-valued solutions to rational equality systems, stated earlier as Theorem 1.3. We show below (Theorem 7.2) that for any rational matrix, say A , the integral and dual integral tag systems defined by A are dual to one another (compare Proposition 4.4 and the strengthening of Theorem 4.9 which will result). One then establishes Theorem 1.3 by applying the painting conditions of Theorem 3.3 to the dual pair of tag systems arising from the matrix $[A \mid b]$, with (column indices for) A painted blue and b red. It is of interest that this approach involves an elimination scheme for simultaneous linear congruences and that one can proceed in an exactly analogous manner to derive Farkas' Theorem 1.2.

Suppose we are given a system of linear congruence relations for a single variable, with all data integral:

$$\begin{cases} y \equiv c_1 \pmod{n_1} \\ \vdots \\ y \equiv c_r \pmod{n_r} \end{cases}.$$

Such a system has a solution if and only if each pair of relations, $y \equiv c_i \pmod{n_i}$, $y \equiv c_j \pmod{n_j}$ has a solution -- see, e.g., Theorem 3.16, page 62 of Le Veque (1977). Furthermore, any system of the more general form

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ \vdots \\ a_r x \equiv b_r \pmod{m_r} \end{cases},$$

still defined by integral data, is easily seen to be equivalent to a system of the former form by using the correspondence $y = lx$, where l is the least common multiple of $a_1, \dots, a_r$ and for $1 \leq i \leq r$, $c_i = l_i b_i$ and $n_i = l_i m_i$ with $l_i = l/a_i$. It then follows easily that any linear congruence system in a single variable defined by integral data is consistent if and only if it is pairwise consistent.

Now suppose we are given a system of linear congruence relations in variables $x_1, \dots, x_n$, with all data integral:

$$(I) \quad \begin{cases} a_{11}x_1 + \dots + a_{1n}x_n \equiv b_1 \pmod{m_1} \\ \vdots \\ a_{r1}x_1 + \dots + a_{rn}x_n \equiv b_r \pmod{m_r} \end{cases}.$$

We then consider the following system with variables $x_2, \dots, x_n$:

$$(II) \quad \begin{cases} (a) \ a_{i2}x_2 + \dots + a_{in}x_n \equiv b_i \pmod{m_i}, \ 1 \leq i \leq r \text{ and } a_{i1} = 0, \\ (b) \ a_{i1}(a_{j2}x_2 + \dots + a_{jn}x_n) - a_{j1}(a_{i2}x_2 + \dots + a_{in}x_n) \equiv \\ \quad (a_{i1}b_j - a_{j1}b_i) \pmod{g_{ij}}, \\ \quad 1 \leq i < j \leq r \text{ and } a_{i1} \neq 0 \neq a_{j1}, \text{ where } g_{ij} = \text{g.c.d.}(a_{i1}m_j, a_{j1}m_i). \end{cases}$$

7.1 Theorem: If $(x_1, x_2, \dots, x_n)$ solves (I), then $(x_2, \dots, x_n)$ solves (II); conversely, if $(x_2, \dots, x_n)$ solves (II), then there exists an x_1 such that $(x_1, x_2, \dots, x_n)$ solves (I).

Proof: Denote $x' = (x_2, \dots, x_n)$ and suppose (x_1, x') solves (I). Then clearly x' satisfies all relations (IIa). Further, if $1 \leq i < j \leq r$ and $a_{i1} \neq 0 \neq a_{j1}$, then

$$a_{i1}x_1 + \dots + a_{in}x_n - b_i = m_i k_i, \quad \text{for some } k_i \in \mathbb{Z},$$

$$a_{j1}x_1 + \dots + a_{jn}x_n - b_j = m_j k_j, \quad \text{for some } k_j \in \mathbb{Z}.$$

Thus we have

$$\begin{aligned} & a_{i1}(a_{j2}x_2 + \dots + a_{jn}x_n) - a_{j1}(a_{i2}x_2 + \dots + a_{in}x_n) \\ &= a_{i1}(b_j + m_j k_j - a_{j1}x_1) - a_{j1}(b_i + m_i k_i - a_{i1}x_1) \\ &= (a_{i1}b_j - a_{j1}b_i) + (a_{i1}m_j k_j - a_{j1}m_i k_i) \\ &= (a_{i1}b_j - a_{j1}b_i) + kg_{ij}, \quad \text{for some } k \in \mathbb{Z}; \end{aligned}$$

i.e., x' satisfies relations (IIb) also.

Now suppose x' solves (II) and note that with x' fixed, we may view (I) as a system of congruence relations in a single variable, x_1 . We thus complete the proof by demonstrating that this system is pairwise consistent.

Suppose that $1 \leq i < j \leq r$ and $a_{i1} \neq 0 \neq a_{j1}$; clearly we need only consider pairs of relations in (I) indexed by such i and j . Thus we wish to determine $x_1(i, j)$ so that

$$\begin{cases} a_{i1}x_1(i, j) = b_i - a_{i2}x_2 - \dots - a_{in}x_n + m_i k_i, & \text{for some } k_i \in \mathbb{Z} \\ a_{j1}x_1(i, j) = b_j - a_{j2}x_2 - \dots - a_{jn}x_n + m_j k_j, & \text{for some } k_j \in \mathbb{Z}, \end{cases}$$

or equivalently, we wish to determine integers k_i and k_j so that

$$a_{j1}(b_i - a_{i2}x_2 - \dots - a_{in}x_n + m_i k_i) = a_{i1}(b_j - a_{j2}x_2 - \dots - a_{jn}x_n + m_j k_j).$$

From (IIb) we have that

$$a_{i1}(b_j - a_{j2}x_2 - \dots - a_{jn}x_n) = a_{j1}(b_i - a_{i2}x_2 - \dots - a_{in}x_n) + g_{ij}k_{ij}, \text{ for some } k_{ij} \in \mathbb{Z}.$$

Thus we must determine integers k_i, k_j so that

$$a_{j1}m_i k_i - a_{i1}m_j k_j = g_{ij}k_{ij}.$$

But this is clearly possible, since $g_{ij} = \text{g.c.d.}(a_{i1}m_j, a_{j1}m_i)$ and hence there are integers p and q so that $g_{ij} = pa_{i1}m_j + qa_{j1}m_i$. Thus for $k_i = qk_{ij}$ and $k_j = -pk_{ij}$, the desired relationship holds.

□

We now use the elimination scheme specified by Theorem 7.1 to show that the integral and dual integral tag systems arising from a given rational matrix constitute a dual pair of tag systems.

7.2 Theorem: Suppose $A \in \mathbb{Q}^{m \times n}$ and let $T = (E, C, \tau)$ and $T' = (E, C', \tau')$ denote, respectively, the integral and dual integral tag systems defined by A . Then T and T' are a dual pair of tag systems.

Proof: We verify the duality of T and T' by showing that the painting condition of Theorem 3.3 holds. Without loss of generality, we may assume that $A \in \mathbb{Z}^{m \times n}$. Suppose the columns of A are painted red, blue and white, with a single red column. The proof given for Proposition 4.4 again demonstrates that both painting stipulations 3.3.1 and 3.3.2 cannot hold simultaneously. Thus we assume that 3.3.1 fails and we show below that 3.3.2 must hold.

Failure of 3.3.1 implies that there is no integer-valued vector z such that $Bz = r$, where B is the blue submatrix of A and r is the red column. That is, the linear congruence system

$$\begin{cases} Bx \equiv r \pmod{0} \\ Ix \equiv 0 \pmod{1} \end{cases}$$

has no solution. Assuming that columns $1, \dots, p$ of A are blue, the successive removal of each variable x_j in this system using the elimination scheme described earlier yields a system in which each congruence relation is of the form $0x_1 + \dots + 0x_p \equiv s \pmod{m}$, where $s, m \in \mathbb{Z}$. Since the resulting system is infeasible (Theorem 7.1), it must contain a relation $0 \equiv s \pmod{m}$ for which m does not divide s . Furthermore, any congruence relation derived in the elimination process is easily seen to be an integer linear combination of the congruence relations in the original system. Hence there exist integer-valued vectors y, z for which $yB + z = 0$ and $yr = s$. Let $y' = (1/m)y$. Then $y'B = (-1/m)z$ and $y'r = s/m \notin \mathbb{Z}$.

We claim that $(-1/m)z$ is an integer-valued vector. Observe that validation of this claim completes the proof, for if $y'B$ is integer-valued and $y'r \notin \mathbb{Z}$, then for some $C' \in C'$, alternative 3.3.2 must hold. We verify the claim inductively. Note that only coefficients from the relations $Ix \equiv 0 \pmod{1}$ are involved in the claim. Suppose variables are eliminated from the original system, denoted by (1), in the

order $x_1, x_2, \dots, x_p$, with the resulting systems denoted (2), (3), $\dots$, $(p+1)$. Now the relation of (2) derived from $x_1 \equiv 0 \pmod{1}$ and, say, $b_{i1}x_1 + \dots + b_{ip}x_p \equiv r_i \pmod{0}$ is given by (IIb) above as $b_{i2}x_2 + \dots + b_{ip}x_p \equiv r_i \pmod{b_{i1}}$. The resulting modulus, b_{i1} , divides the multiplier for the $x_1 \equiv 0 \pmod{1}$ relation, again b_{i1} , used to produce the indicated relations of (2). Thus the claim holds for the relations of (2). Inductively suppose, then, that the claim is valid for relations derived in systems (2), $\dots$, (k) and consider two relations of system (k) which are combined as in (IIb) to derive a relation for system (k+1), say, $b'_{ik}x_k + \dots + b'_{ip}x_p \equiv r'_i \pmod{m_i}$ and $b'_{jk}x_k + \dots + b'_{jp}x_p \equiv r'_j \pmod{m_j}$. Let $1 \leq l \leq k$ and suppose the relation of (1) given by $x_l \equiv 0 \pmod{1}$ appears with a coefficient $\alpha \in \mathbb{Z}$ in the linear combination of relations of (1) which yields relation i of (k) and with a coefficient $\beta \in \mathbb{Z}$ in the corresponding combination for relation j. It follows from (IIb) that $x_l \equiv 0 \pmod{1}$ has coefficient $\alpha b'_{jk} - \beta b'_{ik}$ in the linear combination producing the derived relation and that $t = \text{g.c.d.}(m_i b'_{jk}, m_j b'_{ik})$ is the new modulus. By induction, $n_i m_i = \alpha$ and $n_j m_j = \beta$, where $n_i, n_j \in \mathbb{Z}$. Thus $\alpha b'_{jk} - \beta b'_{ik} = n_i m_i b'_{jk} - n_j m_j b'_{ik}$, which is clearly divisible by t , completing the induction and establishing the claim.

□

As mentioned earlier, one can now derive Theorem 1.3 by applying Theorem 3.3 to the dual pair of tag systems (by Theorem 7.2) associated with the matrix $[A \mid b]$. We now indicate briefly how one can derive Theorem 1.2 (Farkas' Theorem) through an entirely similar analysis (see Crystal (1984) for details).

Given matrix $A \in \mathbb{Q}^{m \times n}$, we associate two tag systems with A , defined on $E = \{1, \dots, n\}$ as follows: a **conical** tag system $T = (E, C, \tau)$, where $C \in \mathcal{C}$ and $k \in \tau(C)$ when $C \setminus \{k\}$ indexes a minimal set of columns of A whose conical hull (i.e., nonnegative span) includes column k , and a **dual conical** tag system $T' = (E, C', \tau')$, where $C' \in \mathcal{C}'$ and $k \in \tau'(C')$ when C' is a minimal set of indices containing k and corresponding to the negative support of a vector in the row space of A . Fourier-Motzkin elimination can be used in place of the elimination procedure of 7.1 in Theorem 7.2 to prove that T and T' constitute a dual pair of tag systems. Theorem 1.2 then follows by applying Theorem 3.3 to the conical and dual conical tag systems arising from the matrix $[A \mid b]$, with A painted blue and b red.

References

- R. G. Bland and M. Las Vergnas [1979]: Minty colorings and orientations of matroids. *Annals of the New York Academy of Sciences* 319, 86-92.
- Donna Crystal [1984]: Tag systems: a combinatorial abstraction of integral dependence. Ph.D. Thesis, School of Operations Research and Industrial Engineering, Cornell University, Ithaca, New York.
- G. B. Dantzig [1963]: *Linear Programming and Extensions*. Princeton University Press, Princeton, New Jersey.
- J. Edmonds and D. R. Fulkerson [1970]: Bottleneck Extrema. *Journal of Combinatorial Theory* 8, 299-306.
- J. Edmonds and F. R. Giles [1977]: A min-max relation for submodular functions on graphs. *Annals of Discrete Mathematics* 1, 185-204.
- J. Farkas [1902]: Theorie der einfachen Ungleichungen. *J. Reine Angew. Math.* 124, 1-27.
- D. Gale [1960]: *The Theory of Linear Economic Models*. McGraw-Hill, New York.
- M. R. Garey and D. S. Johnson [1979]: *Computers and Intractability: A Guide to the Theory of NP-Completeness*. W. H. Freeman and Company, San Francisco.
- D. A. Higgs [1969]: Matroids and duality. *Colloquium Mathematicum* XX, 215-220.
- V. Klee [1971]: The greedy algorithm for finitary and cofinitary matroids. *Combinatorics Proc. Symposia in Pure Mathematics XIX* (Am. Math. Soc., Providence, RI) pp. 137-152.
- W. J. Le Veque [1977]: *Fundamentals of Number Theory*. Addison-Wesley, Reading, Massachusetts.
- G. J. Minty [1966]: On the axiomatic foundations of the theories of directed linear graphs, electrical networks and network programming. *Journal of Mathematics and Mechanics* 15, 485-520.

- A. Schrijver [1986]: *Theory of Linear and Integer Programming*. John Wiley & Sons, Chichester, England.
- W. Sierpinski [1964]: *Elementary Theory of Numbers*. (Translated from Polish by A. Hulanicki.) Państwowe Wydawnictwo Naukowe, Warszawa, Poland.
- D. J. A. Welsh [1976]: *Matroid Theory*. Academic Press, London, England.