

# Feasible combinatorial matrix theory

Ariel Fernández and Michael Soltys

McMaster University  
Hamilton, Canada  
{fernana, soltys}@mcmaster.ca

**Abstract.** We give the first, as far as we know, feasible proof of König’s Min-Max Theorem (KMM), a fundamental result in combinatorial matrix theory, and we show the equivalence of KMM to various Min-Max principles, with proofs of low complexity.

**Key words:** Proof Complexity, Min-Max principle, **LA**, **VTC**<sup>0</sup>

## 1 Introduction

König’s Mini-Max Theorem (KMM) is a cornerstone result in Combinatorial Matrix Theory. We give the first, as far as we know, feasible proof of KMM, and we show that it is equivalent to a host of other theorems: Menger’s, Hall’s, and Dilworth’s, with the equivalence provable in low complexity.

The standard textbook proof of KMM given in [BR91], can be formalized with  $\Pi_2^B$  reasoning. On the other hand, our approach yields a  $\Sigma_1^B$  proof. We use the theory of Bounded Arithmetic **LA**, introduced by [SC04].

Let  $A$  be an  $n \times m$  0-1 matrix, i.e., a matrix with entries in  $\{0, 1\}$ . A *line* is a row or column of  $A$ ; given an entry  $A_{ij}$  of  $A$ , we say that a line *covers* that entry if this line is either row  $i$  or column  $j$ . KMM states that the minimum number of lines that cover all of the 1s in  $A$  is equal to the maximum number of 1s in  $A$  with no two of the 1s on the same line.

**LA** is a first-order theory, of three sorts: indices, ring elements, and matrices. It formalizes basic index manipulations, as well as ring properties, and has a matrix constructor. The details can be found in [SC04]. While **LA** allows for bounded index quantification and arbitrary matrix quantification, its induction is restricted to be over formulas without matrix quantifiers, i.e., over  $\Sigma_0^B = \Pi_0^B$  formulas. On the other hand,  $\exists$ **LA** allows  $\Sigma_1^B$  induction. When the underlying ring is  $\mathbb{Z}$ , the theorems of **LA** translate into  $\text{TC}^0$ -Frege while the theorems of  $\exists$ **LA** translate into extended Frege, [SC04, §6.5].

It follows more or less directly that our **LA** results can also be formalized in the theory **VTC**<sup>0</sup> (and vice versa), defined in [CN10, pg. 283]. The reason is that the function  $\Sigma A$  is exactly Buss’ function  $\text{Numones}(A)$  ([Bus86] and [Bus90, pg. 6]), i.e., the function that counts the number of 1s in  $A$ , and **TC**<sup>0</sup> is the **AC**<sup>0</sup> closure of  $\text{Numones}$ , [CN10, Proposition IX.3.1]. On the other hand, our  $\exists$ **LA** results can also be formalized in **V**<sup>1</sup>, defined in [CN10, pg. 133].

Recently [LC12] formalized the proof of correctness of the Hungarian algorithm, which is an algorithm based on KMM.

The language of **LA** is well suited to express concepts in combinatorial matrix theory. For example, we say that the matrix  $\alpha$  is a *cover* of a matrix  $A$  with the predicate:

$$\text{Cover}(A, \alpha) := \forall i, j \leq r(A)(A(i, j) = 1 \rightarrow \alpha(1, i) = 1 \vee \alpha(2, j) = 1) \quad (1)$$

We use  $r(A)$  and  $c(A)$  to denote the rows and columns of a matrix  $A$ . We abbreviate  $r(A) \leq n \wedge c(A) \leq n$  with  $|A| \leq n$ . The matrix  $\alpha$  keeps track of the lines that cover  $A$ ; it does so with two rows: the top row keeps track of the horizontal lines, and the bottom row keeps track of the vertical line. The condition ensures that any 1 in  $A$  is covered by some line stipulated in  $\alpha$ .

We say that  $\beta$  is a *selection* of  $A$  with the predicate  $\text{Select}(A, \beta)$  defined as the conjunction of

$$\forall i, j \leq r(A)(\beta(i, j) = 1 \rightarrow A(i, j) = 1),$$

which asserts that  $\beta$  is a selection of 1s from  $A$ , and

$$\forall k \leq r(A)(\beta(i, j) = 1 \rightarrow \beta(i, k) = 0 \wedge \beta(k, j) = 0),$$

which asserts that no two of those 1s are in the same row or column.

We are interested in a minimum cover (as few 1s in  $\alpha$  as possible) and a maximum selection (as many 1s in  $\beta$  as possible). The following two predicates express that  $\alpha$  is a minimum cover and  $\beta$  a maximum selection.

$$\text{MinCover}(A, \alpha) := \text{Cover}(A, \alpha) \wedge \forall \alpha' \leq c(\alpha)(\text{Cover}(A, \alpha') \rightarrow \Sigma \alpha' \geq \Sigma \alpha)$$

$$\text{MaxSelect}(A, \beta) := \text{Select}(A, \beta) \wedge \forall \beta' \leq r(\beta)(\text{Select}(A, \beta') \rightarrow \Sigma \beta' \leq \Sigma \beta)$$

Clearly  $\text{MinCover}$  and  $\text{MaxSelect}$  are  $\Pi_1^B$  formulas. We can now state KMM:

$$\text{MinCover}(A, \alpha) \wedge \text{MaxSelect}(A, \beta) \rightarrow \Sigma \alpha = \Sigma \beta \quad (2)$$

Note that (2) is a  $\Sigma_1^B$  formula. The reason is that in prenex form, the universal matrix quantifiers in  $\text{MinCover}$  and  $\text{MaxSelect}$  become existential as we pull them out of the implication; they are also bounded.

Given a matrix  $A$ , its  $n$ -th *principal minor* consists of  $A$  with the first  $r(A) - n$  rows deleted, and the first  $c(A) - n$  columns deleted. For instance, for a square matrix  $A$ , when  $n = |A|$ , the  $n$ -th submatrix is just  $A$ , and when  $n = 1$ , then  $n$ -th submatrix is just  $[A_{|A|, |A|}]$ , i.e., the matrix consisting of just the lower-right entry. Let  $A[n]$  denote the  $n$ -th principal minor, and note that  $A[n]$  can be expressed as follows in the language of **LA**:  $\lambda ij \langle n, n, e(A, r(A) - n + i, c(A) - n + j) \rangle$ .

Let  $\text{KMM}(A, n)$  assert that formula (2) holds for the  $n$ -th submatrix of  $A$ . More precisely,  $\text{KMM}(A, n)$  is the prenex form of (2) with  $A$  replaced by  $A[n]$ . Thus,  $\text{KMM}(A, n)$  is a  $\Sigma_1^B$  formula. Let  $l_A = \Sigma \alpha$  where  $\text{MinCover}(A, \alpha)$ , and  $o_A = \Sigma \beta$  where  $\text{MaxSelect}(A, \beta)$ . It can be stated with a  $\Sigma_0^B$  predicate that a matrix  $P$  is a permutation matrix. That is,

$$\text{Perm}(P) := (\forall i \leq |P| \exists j \leq |P| P_{ij} = 1) \wedge (\forall i, j \neq k \leq |P| (P_{ij} = 0 \vee P_{ik} = 0)).$$

## 2 Feasible proof of KMM

We prove the main theorem with a sequence of Lemmas.

**Theorem 1**  $\exists \mathbf{LA}$  *proves König's Min-Max (KMM) Theorem.*

We prove KMM for any matrix  $A$  by induction on the principal minors of  $A$ .

**Lemma 2**  $\exists \mathbf{LA} \vdash \forall n \text{KMM}(A, n)$ .

Recall that the predicate  $\text{KMM}(A, n)$  has been defined in the last paragraph of the previous section. Showing  $\forall n \text{KMM}(A, n)$  is enough to prove KMM for  $A$  since letting  $n = |A|$  we obtain  $A[n] = A$ .

We start by showing the following technical Lemma which states that  $l_A$  and  $o_A$  are invariant under permutations of rows and columns.

**Lemma 3** *Given a matrix  $A$ , and given any permutation matrix  $P$ , we have that  $\mathbf{LA} \vdash l_{PA} = l_{AP} = l_A$  and  $\mathbf{LA} \vdash o_{PA} = o_{AP} = o_A$ .*

*Proof.*  $\mathbf{LA}$  shows that if we reorder the rows or columns (or both) of a given matrix  $A$ , then the new matrix, call it  $A'$ , where  $A' = PA$  or  $A' = AP$ , has the same size minimum cover and the same size maximum selection. Of course, we can reorder both rows and columns by applying the statement twice:  $A' = PA$  and  $A'' = A'Q = PAQ$ .

$\mathbf{LA}$  proves  $\text{Cover}(A, \alpha) \rightarrow \text{Cover}(A', \alpha')$  and  $\text{Select}(A, \beta) \rightarrow \text{Select}(A', \beta')$ , where  $A'$  is defined as in the above paragraph, and  $\alpha'$  is the same as  $\alpha$ , except the first row of  $\alpha$  is now reordered by the same permutation  $P$  that multiplied  $A$  on the left (and the second row of  $\alpha$  is reordered if  $P$  multiplied  $A$  on the right). The matrix  $\beta$  is even easier to compute, as  $\beta' = P\beta$  if  $A' = PA$ , and  $\beta' = \beta P$  if  $A' = AP$ . It follows from  $P$  being a permutation matrix that  $\Sigma\alpha = \Sigma\alpha'$  and  $\Sigma\beta = \Sigma\beta'$ : we can show by  $\mathbf{LA}$  induction on the size of matrices that if  $X'$  is the result of rearranging  $X$  (i.e.,  $X' = PXQ$ , where  $P, Q$  are permutation matrices), then  $\Sigma X = \Sigma X'$ . We do so first on  $X$  consisting of a single row, by induction on the length of the row. Then we take the single row as the basis case for induction over the number of rows of a general  $X$ .

It is clear that given  $A'$ , the cover  $\alpha'$  has been adjusted appropriately; same for the selection  $\beta'$ . We can prove it formally in  $\mathbf{LA}$  by contradiction: suppose some 1 in  $A'$  is not covered in  $\alpha'$ ; then the same 1 in  $A$  would not be covered by  $\alpha$ . For the selections, note that reordering rows and/or columns we maintain the property of being a selection: we can again prove this formally in  $\mathbf{LA}$  by contradiction: if  $\beta'$  has two 1s on the same line, then so would  $\beta$ .

The last thing to show is that  $\mathbf{LA}$  proves  $\text{MinCover}(A, \alpha) \rightarrow \text{MinCover}(A', \alpha')$   $\text{MaxSelect}(A, \beta) \rightarrow \text{MaxSelect}(A', \beta')$ . If the right-hand side does not hold, we would get that the left-hand side does not hold by applying the inverse of the permutation matrix.  $\square$

We are going to prove Lemma 2 by induction on  $n$ , breaking it down into Claims 4 and 7.

**Claim 4**  $\mathbf{LA} \vdash o_A \leq l_A$ .

*Proof.* Given a covering of  $A$  consisting of  $l_A$  lines, we know that every 1 we pick for a maximal selection of 1s has to be on one of the lines of the covering. We also know that we cannot pick more than one 1 from each line. Thus, the number of lines in the covering provide an upper bound on the size of such selection, giving us  $o_A \leq l_A$ .

We can formalize this argument in  $\mathbf{LA}$  as follows: let  $\mathcal{A}$  be an  $l_A \times o_A$  matrix whose rows represent the lines of the covering, and whose columns represent the 1s no two on the same line. Let  $\mathcal{A}(i, j) = 1 \iff$  the line labeled with  $i$  covers the 1 labeled with  $j$ . Then,

$$o_A = c(\mathcal{A}) \leq \Sigma \mathcal{A} \tag{a}$$

$$= \Sigma_i (\Sigma \lambda p q \langle 1, c(\mathcal{A}), \mathcal{A}(i, q) \rangle) \tag{b}$$

$$\leq \Sigma_i 1 = r(\mathcal{A}) = l_A, \tag{c}$$

where (a) can be shown by induction on the number of columns of  $\mathcal{A}$  which has the condition that each column contains at least one 1 (i.e., each 1 from the selection must be covered by some line); (b) follows from the fact that we can add all the entries in a matrix by rows; and (c) can be shown by induction on the number of rows of  $\mathcal{A}$  which has the condition that each row contains at most one 1 (i.e., no two 1s from the selection can be on the same line).  $\square$

Note that in the proof of Claim 4 we implicitly show the Pigeonhole Principle (PHP). We showed that if we have a set of  $n$  items  $\{i_1, i_2, \dots, i_n\}$  and a second set of  $m$  items  $\{j_1, j_2, \dots, j_m\}$ , and we represent the matching by  $A$  as follows:  $A(p, q) = 1 \iff i_p \mapsto j_q$ , then injectivity means that each column of  $A$  has at most one 1. Thus:

$$n \leq \Sigma A = \Sigma_i (\text{col } i \text{ of } A) \leq \Sigma_i 1 \leq m.$$

This is to be expected as we already mentioned that  $\mathbf{LA}$  over  $\mathbb{Z}$  corresponds to  $\mathbf{VTC}^0$ , which proves PHP.

Bondy's Theorem states that for any  $n \times n$  0-1 matrix whose rows are distinct, we can always delete a column so that the remaining  $n \times (n - 1)$  matrix still has  $n$  distinct rows. [CN10, §IX.3.8] investigate the connection between Bondy's Theorem (BONDY) and PHP, and they show that  $\mathbf{V}^0 \vdash \text{BONDY} \leftrightarrow \text{PHP}$ . It would be interesting to know if  $\mathbf{V}^0 \vdash \text{KMM} \leftrightarrow \text{PHP}$ .

As Claim 4 shows,  $\mathbf{LA}$  is sufficient to prove  $o_A \leq l_A$ ; on the other hand, we seem to require the stronger theory  $\exists \mathbf{LA}$  (which is  $\mathbf{LA}$  with induction over  $\Sigma_1^B$  formulas) in order to prove the other direction of the inequality. We start with the following definition.

**Definition 5** *We say that an  $n \times n$  0-1 matrix has the diagonal property if for each diagonal entry  $(i, i)$  of  $A$ , either  $A_{ii} = 1$ , or  $\forall j \geq i [A_{ij} = 0 \wedge A_{ji} = 0]$ .*

**Claim 6** *Given any matrix  $A$ ,  $\mathbf{LA}$  proves that there exist permutation matrices  $P, Q$  such that  $PAQ$  has the diagonal property.*

*Proof.* We construct  $P, Q$  inductively on  $n = |A|$ . Let the  $i$ -th layer of  $A$  consist of the following entries of  $A$ :  $A_{ij}$ , for  $j = i, \dots, n$  and  $A_{ji}$  for  $j = i + 1, \dots, n$ . Thus, the first layer consists of the first row and column of  $A$ , and the  $n$ -th layer (also the last layer), is just  $A_{nn}$ . We transform  $A$  by layers,  $i = 1, 2, 3, \dots$ . At step  $i$ , let  $A'$  be the result of having dealt already with the first  $i - 1$  layers. If  $A'_{ii} = 1$  move to the next layer,  $i + 1$ . Otherwise, find a 1 in layer  $i$  of  $A'$ . If there is no 1, also move on to the next layer,  $i + 1$ . If there is a 1, permute it from position  $A'_{ij'}$ ,  $j' \in \{i, \dots, n\}$  to  $A'_{ii}$ , or from position  $A'_{j'i}$ ,  $j' \in \{i + 1, \dots, n\}$ . Note that such a permutation does not disturb the work done in the previous layers; that is, if  $A'_{kk}$ ,  $k < i$ , was a 1, it continues being a 1, and if it was not a 1, then there are no 1s in layer  $k$  of  $A'$ . Note that each layer can be computed independently of the others.  $\square$

**Claim 7**  $\exists \mathbf{LA} \vdash o_A \geq l_A$ .

*Proof.* Let

$$A = \left[ \begin{array}{c|c} a & R \\ \hline S & M \end{array} \right], \quad (3)$$

where  $a$  is the top-left entry, and  $M$  the principal sub-matrix of  $A$ , and  $R$  (resp.  $S$ ) is  $1 \times (n - 1)$  (resp.  $(n - 1) \times 1$ ).

By Claim 6 we can ensure that  $A$  has the diagonal property, which simplifies the analysis of the cases. Indeed, from the diagonal property we know that one of the following two cases is true:

**Case 1.**  $a = 1$

**Case 2.**  $a, R, S$  consist entirely of zeros

In the second case,  $o_A \geq l_A$  follows directly from the induction hypothesis,  $o_M \geq l_M$ , as  $o_A = o_M \geq l_M = l_A$ . Thus, it is the first case,  $a = 1$ , that is interesting. The first case, in turn, can be broken up into two subcases:  $l_M = n - 1$  and  $l_M < n - 1$ .

**Subcase (1-a)**  $l_M = n - 1$

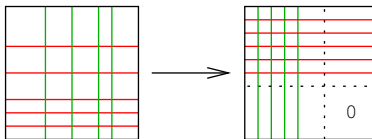
By induction hypothesis,  $o_M \geq l_M = n - 1$ . We also have that  $a = 1$ , and  $a$  is in position  $(1, 1)$ , and hence no matter what subset of 1s is selected from  $M$ , none of them lie on the same line as  $a$ . Therefore,  $o_A \geq o_M + 1$ . Since  $o_M \geq n - 1$ ,  $o_A \geq n$ , and since we can *always* cover  $A$  with  $n$  lines, we have that  $n \geq l_A$ , and so  $o_A \geq l_A$ .

**Subcase (1-b)**  $l_M < n - 1$

Let  $A$  and  $M$  be as in (3), and let  $\alpha_M$  be a set of lines of  $M$ , i.e.,  $\alpha_M$  consists of rows  $i_1, i_2, \dots, i_k$ , and columns  $j_1, j_2, \dots, j_\ell$ . The *extension* of  $\alpha_M$  to  $A$ , denoted  $\hat{\alpha}_M$ , is simply the set of rows  $i_1 + 1, i_2 + 1, \dots, i_k + 1$ , and the set of columns  $j_1 + 1, j_2 + 1, \dots, j_\ell + 1$ .

We say that a minimal cover  $\alpha_A$  is proper if it does not consist entirely of all the rows or of all the columns of  $A$ ; that is,  $\alpha_A$  is proper if it is minimal, i.e.,  $|\alpha_A| = l_A$ , and each row of  $\alpha_A$  has at least one zero. If  $l_M < n - 1$ , then we know that  $\alpha_A$  has a proper cover, as we can always cover  $A$  with  $\hat{\alpha}_M$  plus the first row and column of  $A$ .

Let  $\alpha_A$  be a proper minimal cover of  $A$ , and let  $P, Q$  be two permutations that place all the rows of the cover in the initial position, and place all the columns of the cover in the initial position—Figure 1 illustrates this.



**Fig. 1.** Permuting the rows and columns of the cover to be in initial positions.

Now suppose that  $\alpha_A$  consists of  $e$  rows and  $f$  columns (in the diagram,  $e$  horizontal lines and  $f$  vertical lines). Clearly  $l_A = e + f$ . The rearranging of  $A$  produces four quadrants; the lower-right quadrant, of size  $(|A| - f) \times (|A| - e)$ , consists entirely of zeros (since no lines cross it), and since  $\alpha_A$  is proper, we know that it is not empty. The upper-right quadrant is of size  $e \times (|A| - f)$ , and it cannot be covered by fewer than  $e$  lines. The lower-left quadrant is of size  $(|A| - e) \times f$  and cannot be covered by fewer than  $f$  lines.

**Claim 8**  $\exists$ LA shows that if  $X$  is an  $e \times h$  matrix, and  $l_X = e$ , then  $o_X \geq e$ .

*Proof.* We state the claim formally as follows:

$$[\forall \alpha \leq r(A) \text{Cover}(A, \alpha) \rightarrow \Sigma \alpha \geq r(A)] \rightarrow [\exists \beta \leq r(A) \text{Select}(A, \beta) \wedge \Sigma \beta \geq r(A)]$$

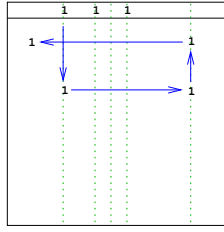
and we prove it by induction on the number of rows of  $A$ . To this end, let  $A_n$  denote the first  $n$  rows of  $A$ , so that  $A_{r(A)} = A$ . We now prove the  $\Sigma_1^B$  formula:

$$\exists \alpha, \beta \leq n [(\text{Cover}(A_n, \alpha) \wedge \Sigma \alpha < n) \vee (\text{Select}(A_n, \beta) \wedge \Sigma \beta \geq n)],$$

which is equivalent to the formula above it for  $n = r(A)$ . The claim holds for  $n = 1$ , as in that case we have a single row, which is either zero and hence has a cover of size 0, or the row has a 1, in which case we can select it. For the induction step, suppose the claim holds for  $n = k$ . Suppose that any cover for  $A_{k+1}$  requires  $k + 1$  rows. Then,  $A_k$  requires  $k$  rows (for otherwise, a cover of  $A_k$  of size  $< k$  plus row  $k + 1$  would give a cover of size  $\leq k$  of  $A_{k+1}$ , which is a contradiction). By IH,  $A_k$  has a selection of size at least  $k$ .

Let  $\mathcal{S} = \{(1, \ell_1), (2, \ell_2), \dots, (k, \ell_k)\}$  be a selection from  $A_k$ . Let  $C_{\mathcal{S}}$  be the set of  $k$  vertical lines going through  $\mathcal{S}$ . Consider row  $k + 1$ ; we know that this row cannot be empty. If there is a 1 in row  $k + 1$  not covered by  $C_{\mathcal{S}}$ , then select that 1. Otherwise, suppose that there are  $p > 0$  1s in row  $k + 1$ ; label their columns as  $c_1, c_2, \dots, c_p$ . Let  $r_i$  be the row with the unique 1 in  $\mathcal{S}$  such that  $\ell_{r_i} = c_i$ .

Let  $\rho_i = \{(k + 1, c_i), (r_i, c_i), (r_i, x_1), (y_1, x_1), (y_1, x_2), \dots, (a, b)\}$ , so that each position has a 1 in  $A_{k+1}$ , and in particular  $(a, b)$  corresponds to a 1 not covered by  $C_{\mathcal{S}}$ . Then,  $\rho_i$  describes a re-arrangement of the selection. A  $\rho_i$  with  $(a, b)$  not covered by  $C_{\mathcal{S}}$  must exist. See Figure 2 for an illustration.  $\square$



**Fig. 2.**  $\rho_1$  consisting of five positions.

Since the size of selections is invariant under permutations, it follows that  $o_A \geq e + f = l_A$ .  $\square$

As an aside, we present a recursive algorithm for computing minimal covers. It would be interesting to know if it has a polytime proof of correctness. First convert  $A$  into diagonal form.

**Case 1.** If  $a = 0$  (so  $R = S = 0$ , by the diagonal form of  $A$ ), then  $l_A = l_M$ , and proceed to compute  $\alpha_M$ ; output  $\hat{\alpha}_A$ .

**Case 2.** If  $a \neq 0$ , we first examine  $R$  to see if the matrix  $M'$ , consisting of the columns of  $M$  minus those columns of  $M$  which correspond to 1s in  $R$ , has a cover of size  $l_M - \Sigma R$  (of course, if  $l_M < \Sigma R$ , then the answer is “no”).

If the answer is “yes”, compute the minimal cover of  $M'$ ,  $\alpha_{M'}$ . Then let  $\alpha_M$  be the cover of  $M$  consisting of the lines in  $\alpha_{M'}$  properly renamed to account for the deletion of columns that transformed  $M$  into  $M'$ , plus the columns of  $M$  corresponding the 1s in  $R$ . Let  $\alpha_A = \hat{\alpha}_A \cup \{\text{1st column of } A\}$ .

If the answer is “no”, repeat the same with  $S$ : check whether  $M'$  has a cover of size  $l_M - \Sigma S$ . If the answer is “yes” then  $\alpha_A = \hat{\alpha}_A \cup \{\text{1st row of } A\}$ .

If the answer is “no”, then compute any minimal cover for  $M$ , extend it to  $A$ , and add the first row and column of  $A$ ; this results in a cover for  $A$ .

### 3 Equivalence of various Min-Max principles

**Theorem 9** *The theory LA proves the equivalence of KMM, Menger’s, Hall’s and Dilworth’s Theorems.*

#### 3.1 Menger’s Theorem

Given a graph  $G = (V, E)$ , an  $x, y$ -path in  $G$  is a sequence of distinct vertices  $v_1, v_2, \dots, v_n$  such that  $x = v_1$  and  $y = v_n$  and for all  $1 \leq i < n$ ,  $(v_i, v_{i+1}) \in E$ . The vertices  $\{v_2, \dots, v_{n-1}\}$  are called *internal vertices*; we say that two  $x, y$ -paths are *internally disjoint* if they do not have internal vertices in common. We also say that  $S \subseteq V$  is an  $x, y$ -cut if there is no path from  $x$  to  $y$  in the graph  $G' = (V - S, E')$ , where  $E'$  is the subset of those edges in  $E$  which have no end-point in  $S$ .

Let  $\kappa(x, y)$  represent the size of the smallest  $x, y$ -cut, and let  $\lambda(x, y)$  represent the size of the largest set of pairwise internally disjoint  $x, y$ -paths. Menger's theorem states that for any graph  $G = (V, E)$ , if  $x, y \in V$  and  $(x, y) \notin E$ , then the minimum size of an  $x, y$ -cut equals the maximum number of pairwise internally disjoint  $x, y$ -paths. That is,  $\kappa(x, y) = \lambda(x, y)$ . Menger's Theorem is of course the familiar Min-Cut Max-Flow Theorem where all edges have capacity 1. For more details on Menger's Theorem turn to [Men27, Gör00, Pym69].

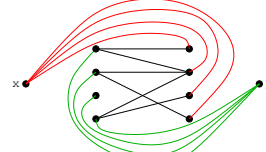
Let  $\beta$  be a matrix that encodes disjoint paths; the rows of  $\beta$  correspond to the paths, and the columns to the vertices of  $G$ , where  $\beta(i, j) = 1$  if path  $i$  contains vertex  $j$ . The disjointness can be stated by insisting that each column has at most one 1. Let  $\gamma$  be a  $1 \times |V|$  matrix that encodes a cut in the natural way. Maximality and minimality can be expressed as in the KMM Theorem. We leave the details to the reader:

$$\text{Menger}(A) := \text{MaxDisj}(A, x, y, \beta) \wedge \text{MinCut}(A, x, y, \gamma) \rightarrow \Sigma\beta = \Sigma\gamma \quad (4)$$

**Lemma 10**  $\text{LA} \cup \text{Menger} \vdash \text{KMM}$ .

*Proof.* Consider a bipartite graph  $G = (V_0 \cup V_1, E)$ , where  $E \subseteq V_0 \times V_1$ . Let  $A$  be the adjacency matrix for  $G$  where  $A(i, j) = 1$  iff  $i \in V_0$  and  $j \in V_1$  and  $(i, j) \in E$ . We now extend  $G$  to  $G_{x,y}$  by adding two new vertices,  $x$  and  $y$ , and edges  $\{(x, v) : v \in V_1\}$ , denoted “red edges”, and edges  $\{(y, v) : v \in V_0\}$ , denoted “green edges.”

The adjacency matrix  $A_{x,y}$  of  $G_{x,y}$  is of size  $(|A| + 1) \times (|A| + 1)$  and:

$$A_{x,y}(i, j) = \begin{cases} A(i, j) & \text{for } 1 \leq i, j \leq |A| \\ 1 & \text{one } \{i, j\} \text{ equals } |A| + 1 \\ 0 & \text{both } \{i, j\} \text{ equal } |A| + 1 \end{cases}$$


i.e.,  $\lambda_{ij}(r(A) + 1, c(A) + 1, \text{cond}(1 \leq i, j \leq |A|, A(i, j), \text{cond}(i = j = |A| + 1, 0, 1)))$ .

As the graphs related to Menger's Theorem are not bipartite, we convert  $A_{x,y}$  to a non-bipartite graph  $A'$  as follows:

$$A' = \begin{bmatrix} 0 & A_{x,y} \\ A_{x,y}^T & 0 \end{bmatrix},$$

Let  $G'$  be the non-bipartite graph represented by  $A'$ . We now finish the proof of the Lemma with a sequence of claims.

**Claim 11**  $\text{LA}$  proves that if there is a cut in  $G'$  of size  $k$ , then there is a cut in  $G'$  of size  $k$  that only cuts the red/green edges, i.e., only those edges that are adjacent to either  $x$  or  $y$ .

*Proof.* Suppose that a black edge is part of a cut. Every  $x, y$ -path crosses from  $V_0$  to  $V_1$ , and taking off one black edge can only block one  $x, y$ -path; the same path is blocked by taking off the corresponding red or green edge.  $\square$

**Claim 12**  $\text{LA}$  proves the following two:



1.  $G$  has a matching of size  $k \iff G'$  has  $k$  disjoint  $x, y$ -paths.
2.  $G$  has a vertex cover of size  $k \iff G'$  has an  $x, y$ -cut of size  $k$ .

Claim 12 follows directly from Claim 11. On the other hand, the direct consequence of Claim 12 is that the size of a maximum matching in  $G$  equals the size of a maximum set of disjoint  $x, y$ -paths in  $G'$ ; and the size of the minimum vertex cover in  $G$  equals the size of the minimum  $x, y$ -cut in  $G'$ . All this is provable in **LA**. This ends the proof of Lemma 10 because by Menger's Theorem, the size of the maximum set of disjoint  $x, y$ -paths in  $G'$  equals the size of the minimum  $x, y$ -cut in  $G'$ . Therefore, the size of the maximum matching in  $G$  equals the size of the minimum vertex cover in  $G$ .  $\square$

**Lemma 13** **LA**  $\cup$  **KMM**  $\vdash$  Menger.

*Proof.* Each path in  $\beta$  must have at least one vertex in the cut  $\gamma$  and no vertex of  $\gamma$  can be in more than one path in  $\beta$ , hence  $\lambda \leq \kappa$ . The proof of this is identical to the proof of Claim 4.

Thus, it remains to show, using **KMM**, that  $\lambda \geq \kappa$ . The proof of this is inspired by [Aha83]; we assume that  $G$  is directed, but a simple construction gives us the undirected case as well. Let  $A = \{u \in V : (x, u) \in E\}$  and let  $B = \{v \in V : (v, y) \in E\}$ . Let  $X = V - (A \cup B)$ , and also split every vertex  $v \in V$  into two vertices  $v', v''$ . We now construct a new bipartite graph  $\Gamma$  where the two sides are given by  $A' \cup X'$  and  $B'' \cup X''$ , and where the edges are given by  $\{(u', v'') : (u, v) \in E\} \cup \{(x', x'') : x \in X\}$ . By **KMM** there is a matching  $M$  and a cover  $C$  in  $\Gamma$  of the same size. We let  $\mathcal{P}$  be the set of paths  $\{x_1, x_2, \dots, x_k\}$  such that  $(x'_i, x''_{i+1}) \in M$ , and we let  $\mathcal{S}$  be a cut consisting of  $\{v \in V : v', v'' \in C \text{ or } v' \in A' \cap C \text{ or } v'' \in B'' \cap C\}$ . **LA** can prove that  $\mathcal{P}$  is a set of disjoint paths, and  $\mathcal{S}$  is a cut, and  $|\mathcal{P}| \geq |\mathcal{S}|$ . This is enough to prove the lemma as:  $\lambda \geq |\mathcal{P}| \geq |\mathcal{S}| \geq \kappa$ .  $\square$

### 3.2 Hall's Theorem

Let  $S_1, S_2, \dots, S_n$  be  $n$  subsets of a given set  $M$ . Let  $D$  be a set of  $n$  elements of  $M$ ,  $D = \{a_1, a_2, \dots, a_n\}$ , such that  $a_i \in S_i$  for each  $i = 1, 2, \dots, n$ . Then  $D$  is said to be a *system of distinct representative* (SDR) for the subsets  $S_1, S_2, \dots, S_n$ .

If the subsets  $S_1, S_2, \dots, S_n$  have an SDR, then any  $k$  of the sets must contain between them at least  $k$  elements. The converse proposition is the combinatorial theorem of P. Hall: suppose that for any  $k = 1, 2, \dots, n$ , any  $S_{i_1} \cup S_{i_2} \cup \dots \cup S_{i_k}$  contains at least  $k$  elements of  $M$ ; we call this the *union property*. Then there exists an SDR for these subsets. See [Hal87,EW49,HV50] for more on Hall's theorem.

We formalize Hall's theorem in **LA** with an adjacency matrix  $A$  such that the rows of  $A$  represent the sets  $S_i$ , and the columns of  $A$  represent the indices of the elements in  $M$ , i.e., the columns are labeled with  $[n] = \{1, 2, \dots, n\}$ , and  $A(i, j) = 1 \iff j \in S_i$ . Let  $\text{SDR}(A)$  be the following  $\Sigma_1^B$  formula which states that  $A$  has a system of distinct representatives:

$$\text{SDR}(A) := (\exists P \leq n)(\forall i \leq n)(AP)_{ii} = 1 \quad (5)$$

The next predicate is a  $\Pi_2^B$  formula stating the union property:

$$\text{UnionProp}(A) := (\forall P \leq n \forall k \leq n \exists Q \leq n) [\Sigma \lambda p q \langle 1, k, (PAQ)_{pp} \rangle = k] \quad (6)$$

Therefore, we can state Hall's theorem as a  $\Sigma_2^B$  formula:

$$\text{Hall}(A) := \text{UnionProp}(A) \rightarrow \text{SDR}(A) \quad (7)$$

**Lemma 14**  $\mathbf{LA} \cup \text{KMM} \vdash \text{Hall}$ .

*Proof.* Let  $A$  be a 0-1 sets/elements incidence matrix of size  $n \times n$ . Assume that we have  $\text{UnionProp}(A)$ ; our goal is to show in  $\mathbf{LA}$ , using KMM, that  $\text{SDR}(A)$  holds.

Since by Claim 6, every matrix can be put in a diagonal form, using the fact that we have  $\text{UnionProp}(A)$ , it follows that we can find  $P, Q \leq n$  such that  $\forall k \leq n (PAQ)_{kk} = 1$ . Thus we need  $n$  lines to cover all the 1s, but by KMM there exists a selection of  $n$  1s no two on the same line, hence  $o_A = n$ .

But this means that the maximal selection of 1s, no two on the same line, constitutes a permutation matrix  $P$  (since  $A$  is  $n \times n$ , and we have  $n$  1s, no two on the same line). Note that  $AP^T$  has all ones on the diagonal, and this in turn implies  $\text{SDR}(A)$ .  $\square$

**Lemma 15**  $\mathbf{LA} \cup \text{Hall} \vdash \text{KMM}$ .

*Proof.* Suppose that we have  $\text{MinCover}(A, \alpha)$  and  $\text{MaxSelect}(A, \beta)$ ; we want to conclude that  $\Sigma\alpha = \Sigma\beta$  using Hall's Theorem.

As usual, let  $l_A = \Sigma\alpha$  and  $o_A = \Sigma\beta$ , and by Claim 4 we already have that  $\mathbf{LA} \vdash o_A \leq l_A$ . We now show in  $\mathbf{LA}$  that  $o_A \geq l_A$  using Hall's Theorem.

Suppose that the minimum number of lines that cover all the 1s of  $A$  consists of  $e$  rows and  $f$  columns, so that  $l_A = e + f$ . Both  $l_A$  and  $o_A$  are invariant under permutations of the rows and the columns of  $A$  (Lemma 3), and so we reorder the rows and columns of  $A$  so that these  $e$  rows and  $f$  columns are the initial rows and columns of  $A'$ ,

$$A' = \begin{bmatrix} A_1 & A_2 \\ A_3 & A_4 \end{bmatrix},$$

where  $A_1$  is of size  $e \times f$ . Now, we shall work with the term rank of  $A_2$  and  $A_3$  in order to show that  $o_A \geq l_A$ . More precisely, we will show that the maximum number of 1s, no two on the same line, in  $A_2$  is  $e$ , while in  $A_3$  it is  $f$ .

Let us consider  $A_2$  as an incidence matrix for subsets  $S_1, S_2, \dots, S_e$  of a universe of size  $|A| - f$ , and  $A_3^t$  (which is the transpose of  $A_3$ ) as an incidence matrix for subsets  $S'_1, S'_2, \dots, S'_f$  of a universe of size  $|A| - e$ . It is not difficult to prove that  $\text{UnionProp}(A_2)$  and  $\text{UnionProp}(A_3^t)$  holds (and can be proven in  $\mathbf{LA}$ ; this is left to the reader), which in turn implies  $\text{SDR}(A_2)$  and  $\text{SDR}(A_3^t)$ , resp., by Hall's Theorem. But the system of distinct representative of  $A_2$  (resp.  $A_3^t$ ) implies that  $o_{A_2} \geq e$  (resp.  $o_{A_3^t} = o_{A_3} \geq f$ ), and since  $o_A \geq o_{A_2} + o_{A_3}$ , this yields that  $o_A \geq e + f = l_A$ .  $\square$

### 3.3 Dilworth's Theorem

Let  $\mathcal{P}$  be a *finite partially ordered set* or *poset* (we use a “script  $\mathcal{P}$ ” in order to distinguish it from permutation matrices, denoted with  $P$ ). We say that  $a, b \in \mathcal{P}$  are *comparable elements* if either  $a < b$  or  $b < a$ . A subset  $C$  of  $\mathcal{P}$  is a *chain* if any two distinct elements of  $C$  are comparable. A subset  $S$  of  $\mathcal{P}$  is an *anti-chain* (also called an *independent set*) if no two elements of  $S$  are comparable.

We want to partition a poset into chains; a poset with an anti-chain of size  $k$  cannot be partitioned into fewer than  $k$  chains, because any two elements of the anti-chain must be in a different partition. Dilworth's Theorem states that the maximum size of an anti-chain equals the minimum number of chains needed to partition  $\mathcal{P}$ . For more on Dilworth's Theorem see [Dil50,Per63].

In order to formalize Dilworth's theorem in **LA**, we represent finite posets  $\mathcal{P} = (X = \{x_1, x_2, \dots, x_n\}, <)$  with an incidence matrix  $A = A_{\mathcal{P}}$  of size  $|X| \times |X|$ , which expresses the relation  $<$  as follows:  $A(i, j) = 1 \iff x_i < x_j$ . For more material regarding formalizing posets see [Sol11]. Let  $1 \times n$   $\alpha$  encode a chain:

$$\text{Chain}(A, \alpha) := (\forall i \neq j \leq n)[\alpha(i) = \alpha(j) = 1 \rightarrow A(i, j) = 1 \vee A(j, i) = 1]. \quad (8)$$

In a similar fashion we define an anti-chain  $\beta$ ; the only difference is that the succedent of the implication expresses the opposite:  $A(i, j) = 0 \wedge A(j, i) = 0$ .

Dilworth( $A$ ) can be stated as:

$$\text{MinChain}(A, \alpha) \wedge \text{MaxAntiChain}(A, \beta) \rightarrow \Sigma\alpha = \Sigma\beta, \quad (9)$$

where  $\text{MinChain}$  and  $\text{MaxAntiChain}$  are defined in the same style as the predicates expressing the other theorems. Note that (9) also requires a statement that  $A$  encodes a poset, that is,  $A(i, i) = 1$ ,  $A(i, j) = 1 \rightarrow A(j, i) = 1$ , and  $A(i, j) \wedge A(j, k) \rightarrow A(i, k)$ .

**Lemma 16**  $\text{LA} \cup \text{KMM} \vdash \text{Dilworth}$

*Proof.* Suppose that  $\text{MinChain}(A, \alpha)$  and  $\text{MaxAntiChain}(A, \beta)$ ; we want to use **LA** reasoning and **KMM** in order to show that  $\Sigma\alpha = \Sigma\beta$ .

As usual we define a matrix  $A'$  whose rows are labeled by the chains in  $\beta$ , and whose columns are labeled by the elements of the poset. As there cannot be more chains than elements in the poset, it follows that the number of rows of  $A'$  is bounded by  $|A|$  (while the number of columns is exactly  $|A|$ ). The proof of this is similar to the proof of Claim 4.

We have that  $A'(i, j) = 1 \iff$  chain  $i$  contains element  $j$ . Clearly each column contains at least one 1, as  $\beta$  is a partition of the poset. On the other hand, rows may contain more than one 1, as in general chains may have more than one element.

Note that a maximal selection of 1s, no two on the same line, corresponds naturally to a maximal anti-chain; such a selection picks one 1 from each line, and so its size is the number of rows of  $A'$ . By **KMM**,  $\Sigma\alpha = o_{A'} = l_{A'} = r(A') = \Sigma\beta$ , where  $r(A')$  is the number of rows of  $A'$ .  $\square$

**Lemma 17**  $\mathbf{LA} \cup \text{Dilworth} \vdash \text{KMM}$ 

*Proof.* It is in fact easier to show that that  $\mathbf{LA} \cup \text{Dilworth} \vdash \text{Hall}$ , and since by Lemma 15 we have that  $\mathbf{LA} \cup \text{Hall} \vdash \text{KMM}$ , we will be done.

Assume that we have 0-1 sets/elements  $n \times n$  matrix  $A$ , and that we have  $\text{UnionProp}(A)$ ; our goal is to show in  $\mathbf{LA}$ , using Dilworth, that  $\text{SDR}(A)$  holds.

Let  $S_1, S_2, \dots, S_n$  be subsets of  $[n]$  where  $n = |A|$ . We define a partial order  $\mathcal{P}$  based on  $A$ ; the universe of  $\mathcal{P}$  is  $X = \{S_1, S_2, \dots, S_n\} \cup [n]$ . The relation  $<_{\mathcal{P}}$  is defined as follows:  $i <_{\mathcal{P}} S_j \iff A(i, j) = 1$ . Note that the the maximum size of an anti-chain in  $\mathcal{P}$  is  $n$ . The  $[n]$  form an anti-chain of length  $n$ , and we cannot add any of the  $S_j$ , as some  $i \in S_j$ , and hence  $i <_{\mathcal{P}} S_j$ .

By Dilworth we can partition  $\mathcal{P}$  into  $n$  chains, where each of the chains has two elements  $\{i, S_j\}$ , giving the set of distinct representatives, and hence  $\text{SDR}(A)$ .  $\square$

**References**

- [Aha83] Ron Aharoni. Menger’s theorem for graphs containing no infinite paths. *European Journal of Combinatorics*, 4:201–204, 1983.
- [BR91] Richard A. Brualdi and Herbert J. Ryser. *Combinatorial Matrix Theory*. Cambridge University Press, 1991.
- [Bus86] Sam R. Buss. *Bounded Arithmetic*. Bibliopolis, Naples, Italy, 1986.
- [Bus90] Samuel R. Buss. Axiomatizations and conservations results for fragments of Bounded Arithmetic. *AMS Contemporary Mathematics*, 106:57–84, 1990.
- [CN10] Stephen A. Cook and Phuong Nguyen. *Logical Foundations of Proof Complexity*. Cambridge Univeristy Press, 2010.
- [Dil50] R. P. Dilworth. A decomposition theorem for partially ordered sets. *Annals of Mathematics*, 51(1):pp. 161–166, January 1950.
- [EW49] C. J. Everett and G. Whaples. Representations of sequences of sets. *American Journal of Mathematics*, 71(2):pp. 287–293, April 1949.
- [Gör00] F. Göring. Short proof of Menger’s theorem. *Discrete Mathematics*, 219:295–296, 2000.
- [Hal87] P. Hall. On representatives of subsets. In Ira Gessel and Gian-Carlo Rota, editors, *Classic Papers in Combinatorics*, Modern Birkhäuser Classics, pages 58–62. Birkhäuser Boston, 1987.
- [HV50] Paul R. Halmos and Herbert E. Vaughan. The marriage problem. *American Journal of Mathematics*, 72(1):pp. 214–215, Januar 1950.
- [LC12] Dai Tri Man Lê and Stephen A. Cook. Formalizing randomized matching algorithms. *Logical Methods in Computer Science*, 8:1–25, 2012.
- [Men27] K Menger. Zur allgemeinen kurventheorie. *Fund. Math*, 10(95-115), 1927.
- [Per63] M. A. Perles. A proof of dilworth’s decomposition theorem for partially ordered sets. *Israel Journal of Mathematics*, 1:105–107, 1963.
- [Pym69] J. S. Pym. A proof of Menger’s theorem. *Monatshefte für Mathematik*, 73(1):81–83, 1969.
- [SC04] Michael Soltys and Stephen Cook. The proof complexity of linear algebra. *Annals of Pure and Applied Logic*, 130(1–3):207–275, December 2004.
- [Sol11] Michael Soltys. Feasible proofs of Szpilrajn’s theorem: a proof-complexity framework for concurrent automata. *Journal of Automata, Languages and Combinatorics (JALC)*, 16(1):27–38, 2011.