LA, Permutations, and the Hajós Calculus

Michael Soltys

Department of Computing and Software, McMaster University
1280 Main Street West, Hamilton, Ontario L8S4K1, CANADA
soltys@mcmaster.ca

Abstract. **LA** is a simple and natural field independent system for reasoning about matrices. We show that **LA** extended to contain a matrix form of the pigeonhole principle is strong enough to prove a host of matrix identities (so called "hard matrix identities" which are candidates for separating Frege and extended Frege). **LAP** is **LA** with matrix powering; we show that **LAP** extended with quantification over permutations is strong enough to prove theorems such as the Cayley-Hamilton Theorem. Furthermore, we show that **LA** extended with quantification over permutations expresses **NP** graph-theoretic properties, and proves the soundness of the Hajós calculus. A corollary is that a fragment of Quantified Permutation Frege (a novel propositional proof system that we introduce in this paper) is p-equivalent of extended Frege. Several open problems are stated.

1 Introduction

The theory **LA** ([4, 1, 5]) is a field-independent logical theory for expressing and proving matrix properties. **LA** proves all the ring properties of matrices (e.g., $A(BC) = (AB)C$). In this paper, we restrict **LA** to the two element field GF(2).

While **LA** is strong enough to prove all the ring properties of matrices, its propositional proof complexity is low: all the theorems of **LA** translate into $\mathbf{AC}^0[2]$-Frege proofs (see [5] for this result, and [2] for the background). **LA** seems too weak to prove those universal matrix identities which require reasoning about inverses, e.g., $AB = I \supset BA = I$ (which we shall denote by IP_n, the Inversion Principle for $n \times n$ matrices), proposed by Cook as a candidate for separating Frege and extended Frege (this separation remains an important open problem of computer science).

In section 2 we present the theory **LA**, and several of its extensions. In section 3 we show that **LA** strengthened to contain the matrix form of the pigeonhole principle can prove IP_n. It was shown in [6] that a feasible bounded-depth Frege proof of IP_n would lead to a feasible bounded-depth Frege proof of the functional form of the pigeonhole principle, which is not possible, and hence no feasible bounded depth proofs of IP_n exist. Section 3 presents a weak converse of that result.

In section 4 we give a proof of the Cayley-Hamilton Theorem (CHT) based on induction over formulas with quantification over matrix permutations. This

improves the proof of the CHT given in [5], where we used quantification over general matrices. We call the theory that formalized the new proof $\exists P\mathbf{LAP}$ (it is defined in section 2).

In section 5 we show how to express **NP** and co-**NP** graph-theoretic properties in $\exists P\mathbf{LA}$ and $\forall P\mathbf{LA}$. In section 6, we prove the soundness of the Hajós calculus in $\forall P\mathbf{LA}$. In section 7 we obtain a corollary which states that a fragment of Quantified Permutation Frege—a novel proof system that we introduce in this paper—is equivalent to extension Frege. We end with a list of open problems in section 8.

2 The theory LA and its extensions

LA is a three-sorted logical theory designed for reasoning about matrices. It is strong enough to prove all the ring properties of matrices (i.e., commutativity of matrix addition, associativity of matrix products, etc.). The original definition of **LA** had no quantification; in this paper we consider a conservative extension with bounded index quantifiers. This allows us to express that a given matrix is a permutation matrix. A full description of **LA** can be found in [4, 1, 5].

The three sorts are indices, field elements, and matrices. All the usual axioms for equality are in **LA**. We have the usual axioms of Robinson's arithmetic in **LA** together with axioms defining div, rem, and cond, for elements of type index. The axioms for field elements are the usual field axioms, plus the extra axiom: $a = 0 \vee a = 1$, since in this paper we are interested in **LA** restricted to the two element field.

LA is closed under the usual Frege rules for propositional consequence, as well as two special rules. **Induction:** $\alpha(i) \supset \alpha(i+1) \vdash \alpha(0) \supset \alpha(n)$, note that i must be an index variable which does not occur free on the right-hand side of the rule. **Equality:** $r(A) = r(B), c(A) = c(B), e(A,i,j) = e(B,i,j) \vdash A = B$, where i, j are index variables that do not occur free on the right-hand side of the rule.

The theorems of **LA** translate into families of propositional tautologies with $\mathbf{AC}^0[2]$-Frege proofs ([5]). However, in this paper we use a (conservative) extension of **LA** which has bounded index quantifiers. Fortunately, it turns out that the translation result still holds for the extended **LA**. We prove this in the next lemma, which will be used in the proof of corollary 2.

Lemma 1. *The theorems of* **LA***-with-bounded-index-quantifiers, and over the field of two elements, translate into families of tautologies with* $\mathbf{AC}^0[2]$*-Frege proofs.*

Proof. Let σ assign values to the index parameters of a formula, and let $|\sigma|$ be the largest value in the assignment σ. Let $\|\alpha\|_\sigma$ be the translation of α into a family of propositional tautologies, parametrized by σ.

We know from [5], that if α is a formula over the language of **LA**, then, there exists a polynomial p_α and a constant d_α such that for every σ, the size of $\|\alpha\|_\sigma$ is bounded by $p_\alpha(|\sigma|)$, and the depth of $\|\alpha\|_\sigma$ is bounded by d_α. If α

is a true formula (in the standard model) then, the propositional formula $\|\alpha\|_\sigma$ is a tautology. Furthermore, if α is a theorem of **LA**-without-index-quantifiers, then, there exists a polynomial q_α and a positive integer d_α such that for every σ, $\|\alpha\|_\sigma$ has an $\mathbf{AC}^0[2]$-Frege derivation $\pi_{\alpha,\sigma}$ such that the size of $\pi_{\alpha,\sigma}$ is bounded by $q_\alpha(|\sigma|)$ and the depth of $\pi_{\alpha,\sigma}$ is bounded by the constant d_α.

Now consider **LA** formulas with bounded index quantifiers. We translate quantifiers in the obvious manner:

$$\|(\exists i \le n)\alpha\|_\sigma \longmapsto \bigvee_{1\le j\le \|n\|} \|\alpha\|_{\sigma(i/j)} \qquad \|(\forall i \le n)\alpha\|_\sigma \longmapsto \bigwedge_{1\le j\le \|n\|} \|\alpha\|_{\sigma(i/j)}$$

where $\sigma(i/j)$ is σ with i replaced by j. As in any **LA** proof the number of quantifiers is bounded (and hence in particular the number of *alternations* of quantifiers is bounded), we still have a bounded depth d_α.

Furthermore, $(Q_1 i_1 \le n_1)(Q_2 i_2 \le n_2)\dots(Q_k i_k \le n_k)\alpha$, where $Q_i \in \{\forall, \exists\}$ are alternating quantifiers, translates into a formula of size

$$O(\|n_1\|_\sigma \cdot \|n_2\|_\sigma \cdot \dots \cdot \|n_k\|_\sigma \cdot \text{size}(\|\alpha\|_\sigma)) \tag{1}$$

where in any **LA** proof, the k is bounded by a constant, and so (1) is bounded by some polynomial in $|\sigma|$.

The reason why we want bounded index quantification is that it allows us to state that a given matrix P is a permutation matrix:

$$[r(P) = c(P)] \wedge [(\forall i \le r(P))(\exists! j \le c(P))e(P,i,j) = 1] \wedge [PP^t = I] \tag{2}$$

(as we are dealing with a field of two elements, if $e(P,i,j) \neq 1$, it follows that $e(P,i,j) = 0$). Let (2) be abbreviated by $\text{Perm}(P)$. Then, $(\exists P \le n)\alpha$ abbreviates $(\exists P)[r(P) \le n \wedge c(P) \le n \wedge \text{Perm}(P) \wedge \alpha]$. Similarly, $(\forall P \le n)\alpha$ abbreviates the same formula but with the last "$\wedge$" replaced by "$\supset$."

Definition 1. *Let* $\exists P\mathbf{LA}$ *denote the theory* **LA** *with bounded* existential *permutation quantification; in particular,* $\exists P\mathbf{LA}$ *allows induction over formulas of the form* $(\exists P \le n)\alpha$. *Let* $\forall P\mathbf{LA}$ *be an analogous theory, but with bounded* universal *permutation quantification instead.*

Definition 2. *Let* **LAP** *be the theory* **LA** *with the matrix powering function* **P**, *which is defined by the axioms:* $\mathbf{P}(0, A) = I$ *and* $\mathbf{P}(n+1, A) = \mathbf{P}(n, A) * A$. *Let* $\exists P\mathbf{LAP}$ *and* $\forall P\mathbf{LAP}$ *be the extensions of* **LAP** *that allow bounded existential, respectively universal, permutation quantification.*

3 Matrix Form of the Pigeonhole Principle

The functional form of the **Pigeonhole Principle (PHP)** states that an injective function from a finite set into itself must necessarily be surjective. Over the field GF(2), there are 2^{n^2} matrices of size $n \times n$, and so the **Matrix form of**

the Pigeonhole Principle (MPHP) states that any injective function from the set of $n \times n$ matrices (over a fixed finite field) into itself must be surjective.

The constructed terms of **LA**, i.e., terms of the form $\lambda ij\langle n, n, t\rangle$, define functions from matrices to matrices in a very natural way: $A \longmapsto \lambda ij\langle n, n, t(A)\rangle$ is a function from the set of all matrices into the set of $n \times n$ matrices. If we restrict A to be an $n \times n$ matrix, we obtain a function from the set of $n \times n$ matrices into itself. This observation can be used to define the MPHP in **LA**, with bounded matrix quantification. We can state that the above mapping is injective as follows:

$$(\forall X_1 \leq n)(\forall X_2 \leq n)[\lambda ij\langle n, n, t(X_1)\rangle = \lambda ij\langle n, n, t(X_2)\rangle \supset X_1 = X_2] \quad (3)$$

and we can state that it is surjective with:

$$(\forall Y \leq n)(\exists X \leq n)[\lambda ij\langle n, n, t(X)\rangle = Y] \quad (4)$$

Notice that we could have stated the above more generally for $n \times m$ matrices, but the resulting formulas would be less readable, as we would have to state $(\forall X_1)[r(X_1) \leq n \wedge c(X_1) \leq m]$, instead of the handy $(\forall X_1 \leq n)$. In any case, square matrices are sufficient for what we want, and rectangular matrices can be padded to become square. We define MPHP to be the scheme of formulas (3) $\supset$ (4) for all n, t. We let $\mathbf{LA}^{\mathrm{MPHP}}$ be **LA** with the MPHP scheme.

Note that despite the fact that we employed bounded matrix quantification to express MPHP in **LA**, the theory $\mathbf{LA}^{\mathrm{MPHP}}$ is still allowed to have induction over formulas *without* quantifiers only.

An important reason why **LA** was designed in the first place was to study the proof theoretic complexity of the derivations of **hard matrix identities**. These are universal matrix identities, stated without quantifiers but implicitly universally quantified, that seem to require reasoning about inverses to prove them. The canonical example is IP_n, which can be stated in **LA** as follows:

$$\lambda ij\langle n, n, \Sigma\lambda kl\langle 1, n, A_{il}B_{lj}\rangle\rangle = I_n \supset \lambda ij\langle n, n, \Sigma\lambda kl\langle 1, n, B_{il}A_{lj}\rangle\rangle = I_n \quad (5)$$

where I_n is given by $\lambda ij\langle n, n, \mathrm{cond}(i = j, 1, 0)\rangle$.

It turns out that there are a host of matrix identities, that can be derived with "basic" properties from the IP_n, such as $AB = I \wedge AC = I \supset B = C$ or $AB = I \supset (AC = 0 \supset C = 0)$ (see [5] for more examples). All these identities are equivalent to IP_n in **LA** (hence they can be shown equivalent with basic ring properties). Let $\mathbf{LA}^{\mathrm{ID}}$ be **LA** extended by some matrix identity ID (formally, ID is any **LA**-formula). We say that ID is a hard matrix identity if $\mathbf{LA}^{\mathrm{IP}_n} = \mathbf{LA}^{\mathrm{ID}}$.

We can prove hard matrix identities in **LA** if at least one matrix is symmetric (next lemma). It remains an open question whether **LA** can prove hard matrix identities for general matrices, but we conjecture that it cannot. On the other hand, **LAP** can prove hard matrix identities for triangular matrices, since **LAP** proves the CHT for such matrices.

Lemma 2. **LA** *proves hard matrix identities for symmetric matrices.*

Proof. If at least one of A, B is symmetric ($A = A^t$ or $B = B^t$), and $AB = I$, then $(AB)^t = I^t = I$. And $(AB)^t = B^t A^t$. Suppose A is the symmetric one, then $B^t A = I$. Since $AB = I$ implies in **LA** that $A(BA - I) = 0$, it follows that $BA - I = 0$, so $BA = I$. Similar argument if B is the symmetric matrix.

In [6] we showed that IP_n does not have a bounded depth Frege proof, since we can derive from IP_n (in bounded depth Frege) the functional form of the PHP, which does not have a bounded depth Frege proof. Here we show a weak converse of that result; **LA** with the matrix form of the pigeonhole principle can prove IP_n(over the field of two elements, and over any finite field).

Lemma 3. $\mathbf{LA}^{\mathrm{MPHP}}$ *proves hard matrix identities.*

Proof. Suppose that we want to prove $AB = I \supset BA = I$. Given $AB = I$, let $f_A(X) := XA$. The function f_A can be defined in **LA** with a constructed term. If $XA = YA$, then $(XA)B = (YA)B$, so by associativity $X(AB) = Y(AB)$, so $X = Y$. Hence f_A is 1-1. By the PHP, $(\exists X) f_A(X) = I$, so $XA = I$. This gives us a left-inverse for A. Since $AB = I$ implies (in **LA**) that $A(BA - I) = 0$, it follows from this that $BA - I = 0$, so $BA = I$. Since all the hard matrix identities can be shown equivalent in **LA** (by definition), we have the result.

4 The Cayley-Hamilton Theorem

We show that the CHT can be proven in the theory $\exists P\mathbf{LAP}$. In fact, $\forall P\mathbf{LAP}$ also proves the CHT, as the two theories prove the same theorems in the language of **LAP**. Many other universal properties of matrices follow from the CHT within **LAP** (see [4, Chapter 5]), so we have their proofs in $\exists P\mathbf{LAP}$ as well.

The characteristic polynomial of a matrix A can be given as a term p_A in the language of **LAP**, using Berkowitz's algorithm (see [4, Chapter 4]). Let $p_A(A)$ be the **LAP**-term expressing the result of plugging A into its characteristic polynomial. The CHT states that $p_A(A) = 0$.

If A is a square matrix, define $A[n]$ to be the n-th principal submatrix of A; that is, $A[1]$ is A with the first row and column removed, $A[2]$ is A with the first two rows and columns removed, and so on until $A[r(A)-1]$ which is just the 1×1 matrix consisting of the bottom-right corner entry of A (here $r(A) = c(A) =$ rows and columns of A). Formally in **LAP**,

$$A[n] =_{\mathrm{def}} \lambda kl\langle r(A) - n, c(A) - n, e(A, n + k, n + l)\rangle.$$

Note that $A[0] = A$.

Let $CH(A, n)$ be a **LAP** formula stating that the CHT holds for the matrices

$$A[n], A[n + 1], \ldots, A[r(A) - 1].$$

Formally, $CH(A, n)$ is given by

$$(\forall n \leq i < r(A)) p_{A[i]}(A[i]) = 0$$

Note that the $\forall$-index quantifier could be replaced with a λ-construction, but we assume that we have bounded index quantifiers.

Lemma 4. $\exists P\mathbf{LAP}$ *proves the following:*

$$\neg CH(A,n) \supset (\exists P \leq r(A))\neg CH(PAP^t, n+1). \tag{6}$$

Proof. If $\neg CH(A,n)$, then there exists a $k \in \{n, n+1, \ldots, r(A)-1\}$ such that

$$p_{A[k]}(A[k]) \neq 0.$$

We choose the *largest* such k, and consider two cases.

Case 1 If $k \neq n$, then $k \geq n+1$, so let $P = I$, and clearly $\neg CH(A^\sigma, n+1)$ holds.

Case 2 If $k = n$, then by definition of k,

$$p_{A[n+1]}(A[n+1]) = \ldots = p_{A[r(A)-1]}(A[r(A)-1]) = 0 \tag{7}$$

We now find the *first* non-zero column of $p_{A[n]}(A[n])$, and call it j. Note that $j \neq 1$ since $p_{A[n+1]}(A[n+1]) = 0$, and we know by [4, lemma 8.2.1] that in that case the first column of $p_{A[n]}(A[n])$ must be zero. Thus $1 < j \leq r(A)-n$. Let I_k be the matrix obtained from the identity matrix by permuting rows k and $k+1$. I_k can be easily expressed with a λ-construction. We now run the program given in Figure 1 for finding a permutation P and an integer $0 \leq i < n$ such that $p_{(PAP^t)[n+j-i]}((PAP^t)[n+j-i]) \neq 0$.
The program clearly terminates (in at most $j \leq r(A)$ steps). It must output a correct P before i reaches the value $j-1$, since otherwise it would follow that

$$p_{(PAP^t)[n+1]}((PAP^t)[n+1]) = 0 \text{ with } P = I_n I_{n+1} \cdots I_{n+j-1}.$$

This is not possible, since it means that column j of A is in position n of PAP^t, and

$$p_{(PAP^t)[n+1]}((PAP^t)[n+1]) = 0$$

so again by [4, lemma 8.2.1] it would follow that the j-th column is zero. This contradicts the original assumption about the j-th column of A.
Note that the program is a search over finitely many matrices, using iterated matrix products. Thus, it can be formalized in **LAP**. Since $j > 1$ and $i \geq 0$,

$$p_{(PAP^t)[n+j-i]}((PAP^t)[n+j-i]) \neq 0$$

implies $\neg CH(PAP^t, n+1)$.

This ends the two cases and the proof of (6).

Theorem 1. $\exists P\mathbf{LAP}$ *proves the CHT, i.e.,* $\exists P\mathbf{LAP} \vdash p_A(A) = 0$.

Proof. From (6) we can easily obtain:

$$(\exists P \leq r(A))\neg CH(PAP^t, n) \supset (\exists P \leq r(A))\neg CH(PAP^t, n+1) \tag{8}$$

$P \leftarrow I$
$i \leftarrow 0$
while $i < j$
    if $p_{(PAP^t)[n+j-i]}((PAP^t)[n+j-i]) = 0$ **then**
        $P \leftarrow I_{n+j-i-1}P$
        $i \leftarrow i+1$
    else
        output P
        break

Fig. 1. Program for computing the permutation P.

So now suppose that the CHT theorem fails for some matrix A, so $p_A(A) \neq 0$. Then $\neg CH(A, 0)$, so certainly $(\exists P \leq r(A))\neg CH(PAP^t, 0)$, where we can take $P = I$. This is our basis case, and (6) is our induction step, so we can conclude by the induction rule that $\neg CH(A, r(A) - 1)$. But that means that the CHT fails for a 1×1 matrix. It is easy to show in **LAP** that the CHT holds for 1×1 matrices, and so we obtain a contradiction.

The above theorem is also provable with the following induction hypothesis:

$$(\forall P \leq r(A))\neg CH(PAP^t, n+1) \supset (\forall P \leq r(A))\neg CH(PAP^t, n)$$

and so it follows, as was stated in the first paragraph of this section, that $\forall P$**LAP** proves the CHT as well.

Since $\exists P$**LAP** proves the CHT, it follows (by [5, theorem 4.1]) that $\exists P$**LAP** ($\forall P$**LAP**) also proves hard matrix identities, and, by further results in [5], the multiplicativity of the determinant.

Corollary 1. $\exists P$**LAP** *proves hard matrix identities and the multiplicativity of the determinant.*

5 Expressing graph-theoretic properties

In this section we show that the theories $\exists P$**LA** and $\forall P$**LA** are very well suited for expressing graph-theoretic properties. In the next section we show that $\forall P$**LA** can actually prove the soundness of the Hajós Calculus. Not surprisingly, $\exists P$**LA** can express **NP** graph problems, and $\forall P$**LA** can express co-**NP** graph problems.

Recall that **Graph Isomorphism (GI)** is the decision problem of whether two graphs $G_1 = (V, E_1)$ and $G_2 = (V, E_2)$, on the same set of nodes V, are isomorphic. That is, whether there is a permutation (i.e., *re-labeling*) π of the nodes V such that $G_2 = \pi(G_1)$, where $\pi(G_1) = (V, \{(\pi(u), \pi(v))|(u, v) \in E_1\})$. GI is one of the few examples of decision problems that are in **NP** and not believed to be in **P** or **NP**-complete.

We can express GI succinctly in $\exists P$**LA** as follows:

$$(\exists P \leq r(A))[A = PBP^t]$$

here A and B are the **adjacency** matrices for graphs G_1 and G_2 (recall that A is the adjacency matrix for $G = (V, E)$ if $r(A) = c(A) = |V|$ and $e(A, i, j) = 1$ iff $(i, j) \in E$). Note that the (i, j)-th entry of PBP^t, $(PBP^t)_{ij}$, is given by $\sum_{1 \leq k,l \leq n} P_{ik} B_{kl} P^t_{lj} = \sum_{1 \leq k,l \leq n} P_{ik} B_{kl} P_{jl}$ (assuming that A, B, P are $n \times n$ matrices). Note that $P^t_{lj} = P_{jl}$ since for permutation matrices $P^t = P^{-1}$. Since P is a permutation matrix, it can be regarded as a function $P : [n] \longrightarrow [n]$ where $P(i) = j$ iff $P_{ij} = 1$. Hence, $(PBP^t)_{ij} = B_{P(i)P(j)}$.

We can also express the decision problem **Path** in $\exists P\mathbf{LA}$. Path on input (G, s, t, k) decides if there is a path in G from node s to node t of length k. If there is such a path, then there is a sequence of nodes $s = i_1, i_2, \ldots, i_k = t$ such that $(i_j, i_{j+1}) \in E$ for all j. Given $i_1, i_2, \ldots, i_k$, there is a re-labeling π of the nodes so that in $\pi(G)$ we have $\pi(s) = 1, 2, \ldots, k = \pi(t)$, and $(i, i+1)$ is an edge in $\pi(G)$. Thus, Path can be expressed in $\exists P\mathbf{LA}$ as follows:

$$(\exists P \leq r(A))[(\forall 0 < i < k) e(PAP^t, i, i+1) = 1 \wedge Ps = e_1 \wedge Pt = e_k]$$

The formula $(\forall 0 < i < k) e(PAP^t, i, i+1) = 1$ in the above expression is stating that the upper-left $k \times k$ corner of PAP^t has 1s on the diagonal above the main diagonal.

Hamiltonian Path (HP) can be stated as:

$$(\exists P \leq r(A))(\forall 0 < i < r(A))[e(PAP^t, i, i+1) = 1]$$

The idea is that we have 1s above the main diagonal, so that for $1 \leq i \leq n-2$ there is an edge $(i, i+1)$ in the re-labeled graph.

For example, in the undirected graph G given in Fig. 2, if we re-label the nodes according to the permutation P: $1 \mapsto 1, 2 \mapsto 5, 3 \mapsto 4, 4 \mapsto 3, 5 \mapsto 2$, we obtain the graph G' on the right with a HP 1-2-3-4-5 indicated by the arrows.

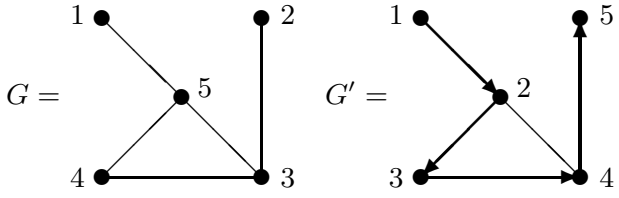

Fig. 2. Graph G and its re-labeling G'.

We can express the k**-Colorability** of graphs in $\exists P\mathbf{LA}$. Let 0_k denote the $k \times k$ matrix of zeros. Let G be a graph, and A_G its corresponding adjacency matrix. We can state that G is k-colorable, for any fixed k, as follows:

$$(\exists P \leq r(A_G))(\exists i_1, i_2, \ldots, i_k \leq r(A_G))[PA_GP^t = \left[\begin{array}{c|c|c|c} 0_{i_1} & * & \cdots & * \\ \hline * & 0_{i_2} & \cdots & * \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline * & * & * & 0_{i_k} \end{array}\right]]$$

The unspecified entries in the above graph (i.e., the entries in the blocks labeled by "$*$") can be anything. For $k = 3$, let **Non-3-Col**(A) be the negation of the above formula, stating that the graph whose adjacency matrix is A is *not* 3 colorable. Note that **Non-3-Col**(A) is a formula in the language of $\forall P\mathbf{LA}$.

Hamiltonian Cycle, **Vertex Cover** and **Clique** can also be stated using similar techniques.

6 The Hajós Calculus

In this section we will show that the theory $\forall P\mathbf{LA}$ proves the soundness of the Hajós calculus. The Hajós calculus is a very simple non-deterministic procedure for building non-3-colorable graphs. It can also be used as a propositional refutation system, and as such it is p-equivalent to extended Frege—see [3].

The Hajós calculus has the 4-clique as its only axiom: let K_4 denote the 4-clique (a complete graph on 4 vertices). $\forall P\mathbf{LA}$ can show that K_4 is not 3-colorable, that is $\forall P\mathbf{LA} \vdash$ **Non-3-Col**(A_{K_4}). Furthermore, the Hajós calculus has the following three rules for building bigger non-3-colorable graphs:

1. **Addition Rule:** Add any number of vertices and/or edges.
2. **Join Rule:** Let G_1 and G_2 be two graphs with disjoint sets of vertices. Let (i_1, j_1) and (i_2, j_2) be edges in G_1 and G_2, respectively. Construct G_3 as follows: remove edges (i_1, j_1) and (i_2, j_2), and add the edge (j_1, j_2), and contract vertices i_1 and i_2 into the single vertex i_1. See Fig. 3 for an example.

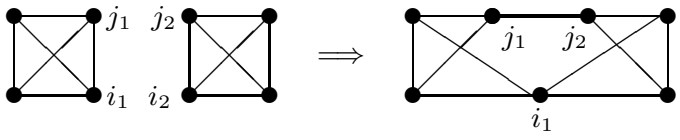

Fig. 3. The join rule applied to two K_4 graphs.

3. **Contraction Rule:** Contract two nonadjacent vertices into a single vertex, and remove the resulting duplicated edges. The new vertex can be either of the two original vertices.

A **derivation** in the Hajós calculus is a sequence of graphs $\{G_1, G_2, \ldots, G_n\}$ such that each G_i is either K_4, or follows from previous G_j's by one of the three rules. G_n is the graph being derived, i.e., the conclusion. The Hajós calculus is both **complete** (any non-3-colorable graph can be derived in it), and **sound** (only non-3-colorable graphs can be derived). See [3] for proofs of completeness and soundness.

Lemma 5. $\forall P\mathbf{LA}$ *proves the soundness of the rules of the Hajós Calculus.*

Before giving the proof, note that a formula stating the completeness of the Hajós calculus would have to be a $\forall X \exists Y$-formula (for *any* A, if **Non-3-Col**(A), then *there exists* a derivation (i.e., there exists a long matrix encoding a derivation) of A). Thus, completeness cannot be expressed in $\forall$**LA**. (Furthermore, a matrix encoding a derivation is not going to be a permutation matrix in general.) We conjecture that the stronger theory $\exists$**LA** can prove completeness.

Proof (of lemma 5). For the addition rule, let G' be G with new vertices/edges. This can be stated as follows:

$$r(A_G) \leq r(A_{G'}) \wedge (\forall i, j \leq r(A_G))[e(i, j, A_G) = 1 \supset e(i, j, A_{G'}) = 1]$$

So, $A_{G'}$ contains A_G in its upper-left corner, with, possibly, certain 0s replaced by 1s, and so it is easy to derive the sequent **Non-3-Col**$(A_G) \rightarrow$ **Non-3-Col**$(A_{G'})$.

For the join rule, let G_1 and G_2 be the two graphs as in the statement of the rule, and A_{G_1} and A_{G_2} the corresponding adjacency matrices. Suppose that $e(A_{G_1}, i_1, j_1) = e(A_{G_2}, i_2, j_2) = 1$. Then A_G is given by a constructed matrix with $r(A_{G_1}) + r(A_{G_2}) - 1$ rows (and columns), and of the form:

$$\left[\begin{array}{cc|c} A_{G_1}[i_1|i_1] & & D_1 \\ & A_{G_2}[i_2|i_2] & D_2 \\ \hline D_1^t & D_2^t & 0 \end{array}\right] \tag{9}$$

where $A[i|j]$ is standard notation for a matrix with row i and column j removed, and D_1 is a column vector with a 1 in position j iff $e(A_{G_1}, i_1, j) = 1$, and D_2 is a column vector with a 1 in position j iff $e(A_{G_2}, i_2, j) = 1$. Matrix (9) can be given as a constructed matrix over **LA**. It is not difficult to derive the sequent:

$$\textbf{Non-3-Col}(A_{G_1}) \wedge \textbf{Non-3-Col}(A_{G_2}) \rightarrow \textbf{Non-3-Col}(A_G)$$

The soundness of the contraction rule can be shown in a similar way.

There are two versions of the Hajós calculus: with labeled and un-labeled graphs. The two versions are p-equivalent. In fact, this can be shown in $\forall P$**LA**, as we can derive $(\forall Q \leq r(A))$**Non-3-Col**(QAQ^t) from **Non-3-Col**(A) (this derivation is very easy, practically by definition of **Non-3-Col**).

Theorem 2. $\forall P$**LA** *proves the soundness of the Hajós Calculus.*

Proof. A derivation in the Hajós Calculus is given by a sequence of graphs $\{G_1, G_2, \ldots, G_n\}$, where G_n is the conclusion, and each G_i is either K_4 or follows from previous G_j's by the application of one of the three rules. We can encode the derivation as a long matrix $[A_{G_1} A_{G_2} \ldots A_{G_n}]$. Using induction on n, lemma 5, and the observation that $\forall P$**LA** $\vdash$ **Non-3-Col**(A_{K_4}), we can show **Non-3-Col**(A_{G_n}).

7 Quantified Permutation Frege

Permutation Frege is a well studied propositional proof system where, besides the usual Frege rules for propositional consequence, we have a restricted substitution rule $\alpha \vdash \alpha^\pi$ which allows us to permute the variables of α (according to π) to obtain α^π. As the permutation rule is a kind of restricted substitution, we know that Permutation Frege can be p-simulated by extended Frege. It remains an interesting open problem whether Permutation Frege and extended Frege are in fact p-equivalent, or whether Permutation Frege is strictly weaker.

We introduce a novel propositional proof system, which we call **Quantified Permutation Frege (QPF)**. As the name suggests, QPF allows quantification over permutations, just as Quantified Frege ([2, §4.6]) allows quantification over variables.

In this paper we shall consider two fragments of QPF, namely $\exists\sigma$-Frege and $\forall\sigma$-Frege. In $\exists\sigma$-Frege we allow propositional formulas plus formulas of the form $\exists\sigma_S\alpha$, where α is a propositional formula *without* any quantifiers. Here σ_S denotes an automorphism (permutation) of the variables in the finite set S, and $\sigma_S|_{S^c} = \mathrm{id}$. Similarly, $\forall\sigma$-Frege consists of propositional formulas plus formulas of the form $\forall\sigma_S\alpha$. Note that the restriction on quantification is *strict* in the sense that we allow one quantifier in prenex form only. (Since S can consist of any finite number of variables, we can always express a block of existential (universal) permutation quantifiers with one existential (universal) permutation quantifier.)

The semantic of $\exists\sigma_S\alpha$ is as follows: given a truth value assignment t, $t \vDash \exists\sigma_S\alpha$ iff there exists a permutation of the variables in S such that $t^{\sigma_S} \vDash \alpha$, where $t^{\sigma_S}(x) = t(\sigma_S(x))$. The semantic of $\forall\sigma_S\alpha$ is defined analogously.

The rules of $\exists\sigma$-Frege and $\forall\sigma$-Frege are the usual Frege rules plus the following four sequent rules for introducing permutation quantifiers:

$$\frac{\Gamma \to \Delta, \alpha}{\Gamma \to \Delta, \exists\sigma_S\alpha^{\pi_S}} \qquad \frac{\alpha, \Gamma \to \Delta}{\exists\sigma_S\alpha^{\pi_S}, \Gamma \to \Delta} \qquad \frac{\Gamma \to \Delta, \alpha}{\Gamma \to \Delta, \forall\sigma_S\alpha^{\pi_S}} \qquad \frac{\alpha, \Gamma \to \Delta}{\forall\sigma_S\alpha^{\pi_S}, \Gamma \to \Delta}$$

where π_S is some permutation of the variables in S, and α^{π_S} is α with the variables permuted according to π_S. There are the following *restrictions*: α may not contain any (permutation) quantifiers, and for $\exists\sigma_S$ introduction left and $\forall\sigma_S$ introduction right, the variables in S are *not free* in the bottom sequent. The variables in a finite set S are **not free** in a given formula β if either they do not occur in β at all, or β is of the form $\exists\sigma_Q\gamma$ (or $\forall\sigma_Q\gamma$), with γ having no quantifiers, and $S \subseteq Q$.

It is easy to check that the four rules are sound. It is an open question whether, with the given definition of restriction, the system is complete (i.e., can we prove all true $\exists\sigma$ and $\forall\sigma$ sequents?). However, here we use $\exists\sigma$-Frege and $\forall\sigma$-Frege to prove propositional formulas without quantifiers, and for these formulas completeness follows from the completeness of Frege. The permutation quantifiers allow us to (apparently) shorten the proofs considerably.

We leave it as future research the definition of a general QPF system, where we allow arbitrary alternations of quantifiers, with a restriction that renders it

complete. We conjecture that a well defined QPF system should be equivalent to the general Quantified Frege (called G in [2, §4.6]).

Define $\exists\sigma$-Frege* and $\forall\sigma$-Frege* to be the same as $\exists\sigma$-Frege and $\forall\sigma$-Frege, but with the additional requirement that the proofs have to be tree-like (i.e., each sequent in the proof occurs at most once). Theorem 2 allows us to prove the following interesting corollary.

Corollary 2. *$\exists\sigma$-Frege* and $\forall\sigma$-Frege* are p-equivalent to extended Frege.*

Proof. $\exists\sigma$-Frege* and $\forall\sigma$-Frege* can be simulated by G_1^* which is p-equivalent to extended Frege ([2, section 4.6]). Conversely, extended Frege and the Hajós calculus are p-equivalent ([3]), and by theorem 2, $\forall P\mathbf{LA}$ proves the soundness of the Hajós calculus. On the other hand, the proof of theorem 2 can be translated into $\forall\sigma$-Frege* (and $\exists\sigma$-Frege*), as can be seen by noting that the theorems of **LA** translate into $\mathbf{AC}^0$[2]-Frege (by lemma 1), and by noting that universal permutation quantifiers occur in the form $(\forall P \leq n)\alpha(PAP^t)$, and so they can be easily translated into $\forall\sigma_A\|\alpha(A)\|_{\sigma'}$. (Note that σ and σ' are different objects; one is permutation quantification, and the other a translation parameter.) It follows that $\forall\sigma$-Frege* (and $\exists\sigma$-Frege*) can simulate the Hajós calculus, and hence extended Frege.

8 Open Problems

Is there an **LAP** proof of the CHT? A related question is: can we prove hard matrix identities in **LAP**? Can we show that hard matrix identities are independent of **LA**? What would be a natural definition of QPF (one that ensures soundness and completeness)? Is (a good definition of) QPF p-equivalent to G?

Acknowledgments. The author would like to thank Toniann Pitassi and Alasdair Urquhart for fruitful discussions that led to this paper.

References

1. Stephen A. Cook and Michael Soltys. The proof complexity of linear algebra. In *Seventeenth Annual IEEE Symposium on Logic in Computer Science (LICS 2002)*, 2002.
2. Jan Krajíček. *Bounded Arithmetic, Propositional Logic, and Complexity Theory.* Cambridge, 1995.
3. Toniann Pitassi and Alasdair Urquhart. The complexity of the Hajós calculus. *SIAM J. Disc. Math.*, 8(3):464–483, August 1995.
4. Michael Soltys. *The Complexity of Derivations of Matrix Identities.* PhD thesis, University of Toronto, 2001.
5. Michael Soltys and Stephen Cook. The complexity of derivations of matrix identities. To appear in the Annals of Pure and Applied Logic, 2004.
6. Michael Soltys and Alasdair Urquhart. Matrix identities and the pigeonhole principle. *Archive for Mathematical Logic*, 43(3):351–357, April 2004.