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

June 10, 2010

Abstract

LA is a simple and natural logical system for reasoning about matrices. We show that **LA**, over finite fields, proves a host of matrix identities (so called "hard matrix identities") from the matrix form of the pigeonhole principle. **LAP** is **LA** with matrix powering; we show that **LAP** extended with quantification over permutations is strong enough to prove fundamental theorems of linear algebra (such as the Cayley-Hamilton Theorem). Furthermore, we show that **LA** with quantification over permutations expresses **NP** graph-theoretic properties, and proves the soundness of the Hajós Calculus. Several open problems are stated.

1 Introduction

The theory **LA** ([5, 1, 6]) 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 [6] 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). IP_n was proposed by Cook as a candidate for separating Frege and extended Frege propositional proof systems (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 [7] 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. Since it was shown ([3] and [8]) that no such proofs of the pigeonhole exist, it follows that no feasible bounded depth Frege proofs of IP_n exist. Section 3 shows a converse, namely that the matrix form of the pigeonhole principle implies IP_n (in **LA**, over finite fields).

In section 4 we give a proof of the Cayley-Hamilton Theorem (CHT) in **LA** with quantification over permutation matrices. This improves the proof of the CHT given in [6], 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 $\forall P\mathbf{LA}$, respectively. In section 6, we prove the soundness of the Hajós Calculus (HC) in $\forall P\mathbf{LA}$. We end with a list of open problems in section 7.

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 [5, 1, 6]; here we just give a brief tour.

In this paper we are mainly interested in **LA** over the field of two elements GF(2)—but all the results hold over general finite fields, and the new proof of the CHT holds over any field (finite or infinite). Since we represent graphs by adjacency matrices, GF(2) is all we need in this paper. See [6] for the translation results over different fields. Over GF(2) the theorems of **LA** translate into families of propositional tautologies with polynomial size bounded-depth Frege proofs, with "$\oplus$" gates of unbounded fan-in, i.e., $\mathbf{AC}^0[2]$-Frege (again, see [6] for a proof of this).

LA has three sorts: **indices**, **field elements** (or, if we ignore multiplicative inverses, just elements of a **commutative ring**), and **matrices**. We denote index variables by i, j, k, field variables by a, b, c, and matrix variables by A, B, C. We shall denote formulas by α, β. There are the usual arithmetic function symbols for indices: addition, multiplication, subtraction, and also function symbols for division and remainder. There is also addition and multiplication for field elements, as well as additive and multiplicative inverses for field elements. When considering a commutative ring rather than a field, the multiplicative inverse is not added.

If m, n are index terms, then so are

$$(m +_{\mathrm{i}} n), (m *_{\mathrm{i}} n), (m -_{\mathrm{i}} n), \mathrm{div}(m, n), \mathrm{rem}(m, n)$$

(where the subscript "$_{\mathrm{i}}$" indicates that these are index operations), and if t, u are terms of type field, then so are

$$(t +_{\mathrm{f}} u), (t *_{\mathrm{f}} u), (-_{\mathrm{f}} t), (t^{-1})$$

(where the subscript "$_\mathrm{f}$" indicates that these are field operations). When it is clear from the context, the subscripts "$_\mathrm{i}$" and "$_\mathrm{f}$" are omitted.

If T is a term of type matrix, then $r(T), c(T)$ are terms of type index which denote the number of rows and columns of T, respectively, and $\Sigma(T)$ is a term of type field that denotes the sum of all the entries of T, and if m, n are terms of type index, then $e(m, n, T)$ is a term of type field which denotes the (m, n) entry of the matrix T. All matrix variables $A, B, C, \ldots$ are matrix terms. We construct new matrices using rudimentary λ-calculus: if m, n are terms of type index, and t is a term of type field, then $\lambda ij\langle m, n, t\rangle$ is a **constructed term of type matrix** (note that the index variables i, j cannot occur free in m, n). Constructed terms obey the following obvious properties:

$$r(\lambda ij\langle m,n,t\rangle) = m \quad c(\lambda ij\langle m,n,t\rangle) = n \quad e(i,j,\lambda ij\langle m,n,t\rangle) = t \tag{1}$$

Rather than introducing a plethora of matrix operations, we define them using constructed matrices. For example, $A + B$ (for A, B $n \times n$ matrices) can be stated as $\lambda ij\langle n, n, e(i, j, A) + e(i, j, B)\rangle$.

If m, n, t, u, T, U are terms, then $(m \leq_\mathrm{i} n), (m =_\mathrm{i} n), (t =_\mathrm{f} u), (T =_\mathrm{M} U)$ are atomic formulas of the appropriate kind (index, index, field, matrix, respectively). We build general formulas in the usual way: if α, β are formulas, then so are: $(\neg\alpha)$, $(\alpha \vee \beta)$ and $(\alpha \wedge \beta)$. Also, we allow bounded index quantification, so if n is a term of type index, we can also build formulas as follows: $(\exists i \leq n)\alpha$ and $(\forall i \leq n)\alpha$.

Finally, if α is a formula where all the atomic subformulas are of type index, then $\mathrm{cond}_\mathrm{i}(\alpha, m, n)$ and $\mathrm{cond}_\mathrm{f}(\alpha, t, u)$ are terms of type index and field, respectively, and the idea is that $\mathrm{cond}_\mathrm{i}(\alpha, m, n)$ is m if α is true, and n otherwise, and similarly for cond_f. The restriction that all the atomic subformulas of α are of type index is there because in the translation into propositional formulas, all the free index variables get values, and therefore, α becomes true or false.

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:

$$a = 0 \vee a = 1 \tag{2}$$

since in this paper we are interested in **LA** restricted to the two element field.

The axioms for matrices include (1), as well as axioms defining Σ: first on row matrices: $\Sigma([a]) = a$, and $\Sigma([a_1 a_2 \ldots a_{n+1}]) = \Sigma([a_1 a_2 \ldots a_n]) + a_{n+1}$, and then for general matrices: $\Sigma(A) = a_{11} + \Sigma(R) + \Sigma(S) + \Sigma(A[1|1])$, where a_{11} is the top-left entry of A, and R, S are the first row and first column *without* the top-left entry, respectively, and $A[1|1]$ is the standard terminology for the principal sub-matrix of A. Note that $R, S, A[1|1]$ can be easily defined using constructed terms. For the complete list of axioms see [6].

With Σ we can define dot products, and hence products of matrices as follows $A * B := \lambda ij\langle n, n, \Sigma\lambda kl\langle 1, n, e(A, i, l) * e(B, l, j)\rangle\rangle$, A, B are $n \times n$ matrices (but we can extend the definition to matrices of incompatible sizes by padding them with zeros). Usually, we omit "$*$" and write AB instead of $A * B$.

All the above mentioned axioms are really *axiom-schemes*, since we allow substitution of terms for variables in the axioms. Thus axiom (2) is really an axiom scheme where for any field term t we have $t = 0 \vee t = 1$. Equivalently, we could have defined **LA** with the substitution rule, where any variable can be replaced by a term. In fact, since the axioms are axiom-schemes, **LA** is closed under the substitution rule.

LA is a theory of sequents, closed under the usual Gentzen PK rules for propositional consequence, with the following four rules for introducing bounded index quantifiers: $\exists$-introduction left and right:

$$\frac{i \leq n \wedge \alpha(i), \Gamma \rightarrow \Delta}{(\exists x \leq n)\alpha(x), \Gamma \rightarrow \Delta} \qquad \frac{\Gamma \rightarrow \Delta, m \leq n \wedge \alpha(m)}{\Gamma \rightarrow \Delta, (\exists x \leq n)\alpha(x)}$$

with the requirement that the variable i in bounded existential introduction left does not occur free in the lower sequent, and $\forall$-introduction left and right:

$$\frac{m \leq n \supset \alpha(n), \Gamma \rightarrow \Delta}{(\forall x \leq m)\alpha(x), \Gamma \rightarrow \Delta} \qquad \frac{\Gamma \rightarrow \Delta, i \leq n \supset \alpha(i)}{\Gamma \rightarrow \Delta, (\forall x \leq n)\alpha(x)}$$

with the requirement that the variable i in bounded universal introduction right does not occur free in the lower sequent.

Finally, we have two special rules: the **Matrix equality rule:**

$$\frac{\Gamma \rightarrow \Delta, e(T,i,j) = e(U,i,j) \quad \Gamma \rightarrow \Delta, r(T) = r(U) \quad \Gamma \rightarrow \Delta, c(T) = c(U)}{\Gamma \rightarrow \Delta, T = U}$$

Here the variables i, j may not occur free in the bottom sequent; otherwise T and U are arbitrary matrix terms. And, the **Induction rule:**

$$\frac{\Gamma, \alpha(i) \rightarrow \alpha(i+1), \Delta}{\Gamma, \alpha(0) \rightarrow \alpha(n), \Delta}$$

Here the variable i (of type index) may not occur free in either Γ or Δ. Also $\alpha(i)$ is any formula, n is any term of type index, and $\alpha(n)$ indicates n is substituted for free occurrences of i in $\alpha(i)$. (Similarly for $\alpha(0)$.)

We showed in [6] that over GF(2), the theorems of **LA** translate into families of propositional tautologies with $\mathbf{AC}^0[2]$-Frege proofs. For example:

$$\|(a * (b + c)) = ((a * b) + (a * c))\| \longmapsto (a \wedge (b \oplus c)) \leftrightarrow ((a \wedge b) \oplus (a \wedge c))$$

and the formula $A = A$ would translate into a family of formulas

$$\left\{ \bigwedge_{1 \leq i \leq \sigma(r(A)), 1 \leq j \leq \sigma(c(A))} (A_{ij} \leftrightarrow A_{ij}) \right\}_{\sigma}$$

parametrized by σ which assigns values to the number of rows and columns of A; we get a different propositional formula for each $\sigma(r(A))$ and $\sigma(c(A))$.

Note that when translating theorems of **LA** into families of propositional tautologies, we are translating sequents into Frege-style proofs. That is fine because Gentzen's system PK and Frege are p-equivalent: proofs in one system can be restate in the other with at most a polynomial increase in size.

The original definition of **LA** given in [6] has no index quantification. The definition that we need in this paper has bounded index quantification. It turns out that the translation result still holds.

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 [6], 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:

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

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

$$O(\|n_1\|_\sigma \cdot \|n_2\|_\sigma \cdot \ldots \cdot \|n_k\|_\sigma \cdot \text{size}(\|\alpha\|_\sigma)) \tag{3}$$

where in any **LA** proof, the k is bounded by a constant, and so (3) is bounded by some polynomial in $|\sigma|$. □

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

$$\begin{aligned}&[r(P) = c(P)]\\ &\wedge [(\forall i \leq r(P))(\exists! j \leq c(P))e(P,i,j) = 1]\\ &\wedge [(\forall j \leq c(P))(\exists! i \leq r(P))e(P,i,j) = 1]\end{aligned} \tag{4}$$

(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 (4) be abbreviated by Perm(P). Let $A \leq n$ abbreviate the formula $(r(A) \leq n \wedge c(A) \leq n)$.

Finally, let $(\exists P \leq n)\alpha$ abbreviate $(\exists P)[(P \leq n \wedge \mathrm{Perm}(P)) \wedge \alpha]$. Similarly, $(\forall P \leq n)\alpha$ abbreviates the same formula but with the main "$\wedge$" replaced by "$\supset$."

Note that **LA** with bounded index quantification is conservative over the original definition of **LA**, in the sense that all the theorems in the language of the original **LA**, provable in the new **LA**, are still provable in the original **LA**. This can be seen by adapting the cut-elimination argument to **LA**.

We have the following rules for introducing permutation quantifiers (similar to the rules for introducing general matrix quantifiers): $\exists$-introduction left and right:

$$\frac{(P \leq n \wedge \mathrm{Perm}(P)) \wedge \alpha, \Gamma \to \Delta}{(\exists P \leq n)\alpha, \Gamma \to \Delta} \qquad \frac{\Gamma \to \Delta, (P \leq n \wedge \mathrm{Perm}(P)) \wedge \alpha}{\Gamma \to \Delta, (\exists P \leq n)\alpha}$$

where we have the usual restriction in the left rule that P does not occur free in the conclusion, and $\forall$-introduction left and right:

$$\frac{(P \leq n \wedge \mathrm{Perm}(P)) \supset \alpha, \Gamma \to \Delta}{(\forall P \leq n)\alpha, \Gamma \to \Delta} \qquad \frac{\Gamma \to \Delta, (P \leq n \wedge \mathrm{Perm}(P)) \supset \alpha}{\Gamma \to \Delta, (\forall P \leq n)\alpha}$$

where in the right rule P does not occur free in the conclusion.

Definition 1 *Let* $\exists P$**LA** *denote the theory* **LA** *with bounded* existential *permutation quantification; in particular,* $\exists P$**LA** *allows induction over formulas of the form* $(\exists P \leq n)\alpha$*. Let* $\forall P$**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* $\mathbf{P}$*, which is defined by the axioms:* $\mathbf{P}(0, A) = I$ *and* $\mathbf{P}(n+1, A) = \mathbf{P}(n, A) * A$*. Let* $\exists P$**LAP** *and* $\forall P$**LAP** *be the extensions of* **LAP** *that allow bounded existential, respectively universal, permutation quantification.*

See Figure 1 for a summary of the theories and their properties.

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 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**,

LA **LA** with bounded index quantification. We show in section 3 that it proves hard matrix identities from the matrix form of the pigeonhole principle (over finite fields).

$\exists P$**LA** The theory **LA** with bounded existential permutation quantification. In particular, with induction over formulas of the type $(\exists P \leq n)\alpha$. It expresses **NP** graph-theoretic properties.

$\forall P$**LA** The theory **LA** with bounded universal permutation quantification. In particular, with induction over formulas of the type $(\forall P \leq n)\alpha$. It expresses co-**NP** graph-theoretic properties, and we show in section 6 that it proves the soundness of the HC.

LAP The theory **LA** with the matrix powering function **P**.

$\exists P$**LAP** The theory **LAP** with bounded existential permutation quantification. We show in section 4 that this theory can prove the CHT (and hence hard matrix identities), as well as the multiplicativity of the determinant.

Figure 1: Summary of theories and their properties.

with bounded matrix quantification. We can state that the above mapping is injective as follows:

$$(\forall X_1 \leq n)(\forall X_2 \leq n)[\lambda ij\langle n, n, t(X_1)\rangle = \lambda ij\langle n, n, t(X_2)\rangle \supset X_1 = X_2] \tag{5}$$

and we can state that it is surjective with:

$$(\forall Y \leq n)(\exists X \leq n)[\lambda ij\langle n, n, t(X)\rangle = Y] \tag{6}$$

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 sequents $(5) \rightarrow (6)$ for all n, t. We let $\mathbf{LA}^{\text{MPHP}}$ be **LA** with the MPHP scheme.

Note that despite the fact that we employed bounded matrix quantification to express MPHP in **LA**, the theory $\mathbf{LA}^{\text{MPHP}}$ 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:

$$\lambda ij\langle n, n, \Sigma\lambda kl\langle 1, n, A_{il}B_{lj}\rangle\rangle = I_n \rightarrow \lambda ij\langle n, n, \Sigma\lambda kl\langle 1, n, B_{il}A_{lj}\rangle\rangle = I_n \tag{7}$$

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

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 [6] for more examples). All these identities are equivalent to IP_n in **LA** (hence they can be shown equivalent with basic ring properties). Let $\mathbf{LA}^{\text{ID}}$ be **LA** extended by some matrix identity ID (formally, ID is any **LA**-formula). We say that ID is a hard matrix identity if $\mathbf{LA}^{\text{IP}_n} = \mathbf{LA}^{\text{ID}}$.

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: First of all, we can prove in **LA** that for all matrices A, B, if $AB = I$ then $A(BA - I) = 0$ (from $AB = I$ we obtain $(AB)A = A$, and by associativity and distributivity we obtain $A(BA - I) = 0$). Also note that $AB = I$ implies $B^tA^t = (AB)^t = I^t = I$ (which can also be shown in **LA**). Therefore, if A is symmetric, then $A^t = A$, so if $AB = I$, B^t is the left inverse of A, which allows us to conclude $BA = I$ from $A(BA - I) = 0$. A similar argument applies if B is symmetric. □

In [7] 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 in fact over any finite field).

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

Note that $\mathbf{LA}^{\text{MPHP}}$ (as was noted on the previous pages) is a theory with (bounded) matrix quantification, but that the induction is still restricted to formulas *without* matrix quantifiers.

Proof:[of lemma 3] Suppose that we want to prove IP_n. 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 MPHP, $(\exists X)f_A(X) = I$, 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. □

Next, we show that $\mathbf{LAP}^{\text{MPHP}}$ can prove a weak version of the CHT; namely that any matrix has an annihilating polynomial. (Recall that a polynomial $p(x) = c_kx^k + \cdots + c_1x + c_0$ is an **annihilating polynomial** of a matrix A if $c_k \neq 0$ and $p(A) = c_kA^k + \cdots + c_1A + c_0I = 0$.) This is interesting as the proof of the CHT itself requires a much stronger theory ($\exists P\mathbf{LAP}$). Thus, MPHP is really a very strong assertion (again, true over finite fields only). Note that the proof (lemma 4 below) is not constructive—it does not give the annihilating polynomial itself.

Lemma 4 **LAP**$^{\mathrm{MPHP}}$ *proves that every matrix has an annihilating polynomial.*

Proof: Let A be any matrix, and define $f_A(C) := c_{n^2}A^{n^2} + \cdots + c_1A^1$. Here A is an $n \times n$ matrix, and C is a $1 \times n^2$ matrix. Thus f is a function from the space of $1 \times n^2$ matrices into the space of $n \times n$ matrices—matrices over the field of two elements.

We let c_i be the i-th entry of C, i.e., $c_i := e(C, 1, i)$, $1 \leq i \leq n^2$. Clearly, $f_A(C)$ can be given as a constructed term over **LAP**. If f_A is not 1-1, then there exist $C_1 \neq C_2$, such that $f_A(C_1) = f_A(C_2)$, so $f_A(C_1 - C_2) = f_A(C_1) - f_A(C_2) = 0$, and since $C_1 - C_2 \neq 0$, they provide the coefficients of an annihilating polynomial for A. Suppose on the other hand that f_A is 1-1. Then, there exists a C such that $f_A(C) = I$. Then, $c_{n^2}x^{n^2} + \cdots + c_1x - 1$ is an annihilating polynomial of A.

Note that the MPHP is stated for square matrices, but C above is a $1 \times n^2$ matrix. This is a minor technical point that can be resolved simply by padding C with $(n^2 - 1)$ rows of zeros, so it is an $m \times m$ matrix, with $m = n^2$. □

4 The Cayley-Hamilton Theorem

We show that the CHT can be proved in the theory $\exists P$**LAP**. In fact, $\forall P$**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 [5, Chapter 5]), so we have their proofs in $\exists P$**LAP** as well.

The characteristic polynomial of a matrix A ($p_A(x) = \det(xI - A)$) can be given as a term p_A in the language of **LAP**, using Berkowitz's algorithm (see [5, 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 first column removed, $A[2]$ is A with the first two rows and the first two 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 an **LAP** formula stating that the CHT holds for all the matrices in

$$\{A[n], A[n + 1], \ldots, A[r(A) - 1]\}. \tag{8}$$

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

$$(\forall i < r(A))[n \leq i \supset p_{A[i]}(A[i]) = 0] \tag{9}$$

Note that the $\forall$-index quantifier could be replaced with a λ-construction that encodes all the matrices in (8), but we have bounded index quantifiers in **LAP**, so it can be stated with the simpler **LAP**-formula (9).

We show that $\exists P\mathbf{LAP} \vdash CH(A,0)$, which implies $p_A(A) = 0$ (the CHT).

The proof is by induction on n. We show that $(\exists P \leq r(A))\neg CH(PAP^t, n)$ implies $(\exists P \leq r(A))\neg CH(PAP^t, n{+}1)$ (the induction step). Thus, if we assume $\neg CH(A,0)$ (the basis case), we can conclude $(\exists P \leq r(A))\neg CH(PAP^t, r(A){-}1)$ (by the induction rule). This in turn implies that the CHT fails for $1{\times}1$ matrices, which is a contradiction (even **LAP** proves the CHT for matrices of constant size). Hence the original assumption that $\neg CH(A,0)$ must be wrong, and so $CH(A,0)$. The following lemma is needed to prove the induction step.

Lemma 5 $\exists P\mathbf{LAP}$ *proves the following:*

$$\neg CH(A,n) \to (\exists P \leq r(A))\neg CH(PAP^t, n+1). \tag{10}$$

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 $\neg CH(A, n+1)$ holds.

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

$$p_{A[n+1]}(A[n+1]) = \ldots = p_{A[r(A)-1]}(A[r(A)-1]) = 0 \tag{11}$$

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 [5, 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 transposing rows k and $k+1$. I_k can be easily expressed with a λ-construction. We now run the program given in Figure 2 for finding a permutation P and an integer $0 \leq i < j$ 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 $A[n]$ is in position n of PAP^t, and

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

so again by [5, 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 $A[n]$.

```
$P \leftarrow I$
$i \leftarrow 0$
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
```

Figure 2: Program for computing the permutation P.

Note that the program is a search over polynomially 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 (10). □

Theorem 1 $\exists P$**LAP** *(and hence* $\forall P$**LAP***) proves the CHT.*

Proof: From (10) we can obtain

$$(\exists P \leq r(A))\neg CH(PAP^t, n) \rightarrow (\exists P \leq r(A))\neg CH(PAP^t, n+1) \tag{12}$$

as follows: replace A in (10) by QAQ^t. It is easy to show, for any formula α, that $(\exists P \leq n)\alpha(PQAQ^tP^t) \rightarrow (\exists P \leq n)\alpha(PAP^t)$, since $Q^tP^t = (PQ)^t$, and the product of two permutations is still a permutation (this can be shown in **LAP**). Then, introduce $\exists Q$ on the left-hand side of (10) (since the restriction is preserved). Since $(\exists P \leq n)\alpha \rightarrow (\exists Q \leq n)\alpha(Q/P)$, we easily obtain (12).

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 (10) 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 is also provable with the following induction hypothesis:

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

(by restating lemma 5 in terms of $\forall P$**LAP**), and so $\forall P$**LAP** proves the CHT as well. □

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

PROOF: By theorem 1, $\forall P$**LAP** proves the CHT, and the hard matrix identities follow (in **LAP**) from the CHT (by [6, theorem 4.1]). To show that $\forall P$**LAP** proves the multiplicativity of the determinant, i.e., $\det(AB) = \det(A)\det(B)$, we adapt the proof of [6, theorem 5.2] to $\forall P$**LAP**. First of all, by [6, theorem 4.2], we know that **LAP** proves the equivalence of the CHT and the axiomatic definition of the determinant, and the cofactor expansion. Using this, we can show in $\forall P$**LAP** the following:

$$\det(AB) = \sum_{k=1}^{n}\sum_{l=1}^{n}(-1)^{1+l} b_{k1} a_{lk} \det(A[l|k]B[k|1]) \tag{13}$$

where $A[i|j]$ denotes the matrix A with row i and column j removed. At this point, in $\forall$**LAP** we could have used the induction hypothesis on smaller matrices to conclude that $\det(A[l|k]B[k|1]) = \det(A[l|k])\det(B[k|1])$. But in $\forall P$**LAP** we cannot quantify over general matrices, so we need to state things differently. We need to state things so that we quantify over permutations. Note that:

$$A[i|j] = (I_{12}\cdots I_{(i-2)(i-1)} I_{(i-1)i} A I_{j(j-1)} I_{(j-1)(j-2)} \cdots I_{21})[1] \tag{14}$$

where I_{pq} denotes the permutation matrix with rows p and q exchanged. To see this, note that the effect of multiplying A on the left by $I_{12}\cdots I_{(i-2)(i-1)} I_{(i-1)i}$ is that of bringing row i to position 1, and moving all the rows numbered 1 through $(i-1)$ up by one position, and leaving all the rows above row i in place. Similarly, the effect of multiplying A on the right by $I_{j(j-1)} I_{(j-1)(j-2)} \cdots I_{21}$ is that of bringing column j to position 1, and moving all the rows numbered 1 through $(j-1)$ up by one position, and leaving all the columns above column j in place.

Thus, we prove the following:

$$(\forall P, Q, R \leq n)[\det((PAQ^t)[k](QBR^t)[k]) = \det((PAQ^t)[k])\det((QBR^t)[k])]$$

for all k (and $n \times n$ matrices A, B). $\forall P$**LAP** proves this by induction using (13) and (14). When $k = 0, P = Q = R = I$, we obtain $\det(AB) = \det(A)\det(B)$. □

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 HC. 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 $P^t_{lj} = P_{jl}$ by definition of transpose. 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 $\exists P$**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 $\exists P$**LA** as follows:

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

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 is of the form:

$$\begin{bmatrix} * & \mathbf{1} & * & \cdots & * & * \\ * & * & \mathbf{1} & \cdots & * & * \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ * & * & * & \cdots & \mathbf{1} & * \\ * & * & * & \cdots & * & * \end{bmatrix} \tag{15}$$

The ones above the main diagonal of (15) assert that for $1 \leq i \leq (k-1)$, $(i, i+1)$ is an edge in the re-labeled graph. Also, $Ps = e_1$ and $Pt = e_k$ assert that node s is node 1 and node t is node k in the re-labeled graph. (We let e_i denote the i-th vector of the standard basis; that is, e_i is a column vector with zeros everywhere except in the i-th position where it has a 1.) We assume that the last row and column of (15) represent $(n - k)$ rows and columns.

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. 3, 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.

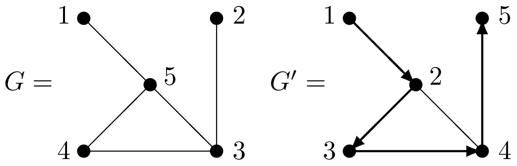

Figure 3: Graph G and its re-labeling G'.

In terms of matrices, the relationship in Fig. 3 can be succinctly stated as $PA_GP^t = A_{G'}$, which is:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}^t$$
$$= \begin{bmatrix} 0 & \mathbf{1} & 0 & 0 & 0 \\ 1 & 0 & \mathbf{1} & 1 & 0 \\ 0 & 1 & 0 & \mathbf{1} & 0 \\ 0 & 1 & 1 & 0 & \mathbf{1} \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

where the middle matrix on the left-hand side is the adjacency matrix of G, with the permutation matrix P on the left and P^t on the right; here $P_{ij} = 1$ iff $i \mapsto j$ in the above permutation. Note that the matrix on the right-hand side (the adjacency matrix of G') has 1s above the main diagonal, as required.

To express **Hamiltonian Cycle (HC)**) in $\exists P$**LA** we would only need to add a 1 in position $(n, 1)$ in matrix (15), to state that from the n-th node there is an edge back to the first node.

We can express the k**-Colorability** of graphs in $\exists P$**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 $\forall P$**LA**.

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

Finally, **Boolean matrix multiplication** can be expressed in **LAP**. Recall that the (i, j)-th entry of the Boolean product of two $n \times n$ matrices A, B is given by $\bigvee_{1\leq k\leq n}(a_{ik}\wedge b_{kj})$. The formula $(a_1\vee a_2\vee\ldots\vee a_n)$ can be expressed (over GF(2)) with $1-(1-a_1)(1-a_2)\cdots(1-a_n)$. Let "$\star$" denote Boolean products of matrices. Then, the (i,j)-th entry of $A\star B$ is given by $1-\prod_{1\leq k\leq n}(1-a_{ik}*b_{kj})$, where $a_{ik}*b_{kj}$ is the usual algebraic product of field elements. Therefore, we can define $A\star B$, for $n\times n$ matrices A,B, with the following constructed term:

$$\lambda ij\langle n,n,1-e(n+1,n+1,\mathbf{P}(n,\lambda kl\langle n+1,n+1,\text{cond}(k+1=l,1-(a_{ik}*b_{kj}),0)\rangle))\rangle$$

Note that $A\star B$ translates into $\mathbf{NC}^1$ circuits, despite the use of $\mathbf{P}$, because we compute the n-th power of the matrix:

$$\begin{bmatrix} 0 & (1-a_{i1}b_{1j}) & 0 & \ldots & 0 \\ 0 & 0 & (1-a_{i2}b_{2j}) & \ldots & 0 \\ 0 & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & (1-a_{n1}b_{nj}) \\ 0 & 0 & 0 & \ldots & 0 \end{bmatrix}$$

This can be done by repeated squaring, and at each stage we square a matrix which has non-zero entries only on a single diagonal; so each stage can be computed with formulas of bounded depth. If A,B are $n\times n$ matrices, there are $\log(n)$ such stages, and so the resulting circuit is of polynomial size and depth $\log(n)$.

The **Transitive Closure (TC)** of an $n\times n$ matrix A is defined as $A\star A\star\cdots\star A$, n-times. The (i,j)-th entry of the TC of a given matrix A is non-zero (i.e., 1) iff there is a path in the graph G with adjacency matrix A, from node i to node j.

We define the Boolean matrix powering function, denoted by $\mathbf{P}_\star$, analogously to $\mathbf{P}$ as follows: $\mathbf{P}_\star(0,A)=I$ and $\mathbf{P}_\star(n+1,A)=\mathbf{P}_\star(n,A)\star A$. Note that if A is an $n\times n$ matrix, then $\mathbf{P}_\star(n,A)$ is the TC of A, and the (i,j)-th entry of $\mathbf{P}_\star(k,A)$ (with $k\leq n$) is non-zero iff there is a path in the corresponding graph from node i to node j of length at most k.

By adding the function symbol $\mathbf{P}_\star$ to **LAP**, together with the two defining axioms, we obtain a theory where we can express transitive closure, but the theory still translates into $\mathbf{NC}^2$ tautologies, with $\mathbf{NC}^2$-Frege proofs.

6 The Hajós Calculus

In this section we will show that the theory $\forall P\mathbf{LA}$ proves the soundness of the Hajós Calculus (HC). The HC 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 [4].

Let K_4 denote the 4-clique, that is, a complete graph of 4 vertices.

The K_4 graph is the only axiom of the HC. Let A_{K_4} be the adjacency matrix of the K_4 graph (a 4×4 matrix, with zeros on the main diagonal, and ones everywhere else). By the results of the previous section, **Non-3-Col**(A_{K_4}) is a

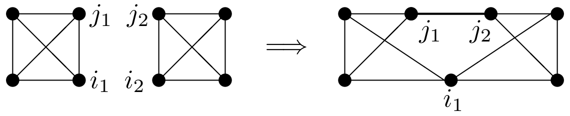

Figure 4: The join rule applied to two K_4 graphs.

formula in the language of $\forall P\mathbf{LA}$, and it is easy to see that $\forall P\mathbf{LA}$ can show that K_4 is not 3-colorable, that is $\forall P\mathbf{LA} \vdash \textbf{Non-3-Col}(A_{K_4})$.

The HC 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. 4 for an example.

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 HC 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 HC is both **complete** (any non-3-colorable graph can be derived in it), and **sound** (only non-3-colorable graphs can be derived). See [4] for proofs of completeness and soundness.

Lemma 6 *$\forall P\mathbf{LA}$ proves the soundness of the rules of the HC.*

Proof: 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 $\textbf{Non-3-Col}(A_G) \rightarrow \textbf{Non-3-Col}(A_{G'})$.

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:

$$\left[\begin{array}{cc|c} A_{G_1}[i_1|i_1] & & D_1 \\ & A_{G_2}[i_2|i_2] & D_2 \\ \hline D_1^t & D_2^t & 0 \end{array}\right] \tag{16}$$

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 (16) 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. □

Let $\textbf{HC}(Y)$, where $Y = [X_1 X_2 \ldots X_n]$, be an **LA** formula stating that Y encodes a HC refutation. Y is a sequence of n blocks, each block is the adjacency matrix of a graph. The blocks can be made of equal size by padding them with zeros. The formula $\textbf{HC}(Y)$ can be easily defined in **LA** thanks to to bounded index quantifiers: for all i, the i-th block of Y is either K_4 (i.e., equal to A_{K_4}), or follows from previous blocks; for example, $\exists j_1, j_2$ such that block i is the join of blocks j_1 and j_2. Thus, $\exists$**LA** can state the completeness of the HC:

$$\textbf{Non-3-Col}(X) \supset \exists Y(\textbf{HC}(Y) \wedge Y = [X_1 X_2 \ldots X_n] \wedge X_n = X) \qquad (17)$$

If (17) is put in prenex form, the universal permutation quantifier in the subformula $\textbf{Non-3-Col}(X)$ becomes an existential quantifier. Since it is not difficult to prove a witnessing theorem for $\exists$**LA** (i.e., if $\exists\textbf{LA} \vdash \exists Y \alpha(X, Y)$, then there exists a polytime function f such that $f(X) = Y$), it follows that (17) is not provable in $\exists$**LA** *unless* the HC refutations can be generated in polytime (i.e., given a non-3-colorable X, we can generate its HC refutation in polytime in the size of X). This seems very unlikely, because it would imply that $\mathbf{P} = \mathbf{NP}$.

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

Proof: Recall that the **LA** formula $\textbf{HC}(Y)$ states that the matrix Y encodes a HC refutation (see paragraph above (17)). That is, $Y = [X_1 X_2 \ldots X_n]$, where X_i is the adjacency matrix (perhaps padded with zeros) of a graph G_i, where $G_i = K_4$, or G_i follows from previous graphs by one of the three rules. Let the soundness of the HC be stated with the formula:

$$\textbf{HC}([X_1 X_2 \ldots X_n]) \supset \textbf{Non-3-Col}(X_n) \qquad (18)$$

Note that (18) is a $\forall P$**LA** formula.

We prove by induction on k that:

$$(\forall i \leq k)[\textbf{HC}([X_1 X_2 \ldots X_n]) \supset \textbf{Non-3-Col}(X_i)]$$

Since X_1 must encode K_4, it follows that $\textbf{Non-3-Col}(X_1)$, and hence we have the Basis Case. The Induction Step follows from lemma 6. When $k = n$ we have that $\textbf{Non-3-Col}(X_n)$, which implies that the conclusion of the HC refutation is non-3-colorable, which gives us (18). □

7 Open Problems

There are many open problems related to this area of research. First of all, is there an **LAP** proof of the CHT? In other words, can the CHT be proved feasibly from mere properties of matrix powering? A related question is: can we prove hard matrix identities in **LAP**? Hard matrix identities have been proposed by Cook as candidates for separating Frege and extended Frege—do they, or can they be proved in Frege, or somewhere in between (eg., Permutation Frege, if indeed it is strictly "in between")? Can we show that hard matrix identities are independent of **LA** (i.e., can we show that they don't follow feasibly from basic ring properties of matrices?).

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, Paul Beame, and Russell Impagliazzo. Exponential lower bounds for the pigeonhole principle. *Computational Complexity*, 3:97–140, 1993.

[4] Toniann Pitassi and Alasdair Urquhart. The complexity of the Hajós calculus. *SIAM J. Disc. Math.*, 8(3):464–483, August 1995.

[5] Michael Soltys. *The Complexity of Derivations of Matrix Identities.* PhD thesis, University of Toronto, 2001.

[6] Michael Soltys and Stephen Cook. The complexity of derivations of matrix identities. *Annals of Pure and Applied Logic*, 130(1–3):277–323, December 2004.

[7] Michael Soltys and Alasdair Urquhart. Matrix identities and the pigeonhole principle. *Archive for Mathematical Logic*, 43(3):351–357, April 2004.

[8] Alasdair Urquhart and Xudong Fu. Simplified lower bounds for propositional proofs. *Notre Dame Journal of Formal Logic*, 37:523–544, 1996.