# Complete Problems for Valiant's Class of qp-Computable Families of Polynomials

Markus Bläser

Institut für Theoretische Informatik, Med. Universität zu Lübeck
Wallstr. 40, 23560 Lübeck, Germany
blaeser@tcs.mu-luebeck.de

**Abstract.** We prove that the families *matrix powering*, *iterated matrix product*, and *adjoint matrix* are VQP–complete, where VQP denotes Valiant's class of quasipolynomial–computable families of multivariate polynomials. This proves a conjecture by Bürgisser [3, Conjecture 8.1].

## 1 Introduction

In connection with his famous #P–completeness result [11] for the permanent, Valiant presented an algebraic analogue of the theory of NP–completeness [10] (a decade before the proposal of Blum, Shub, and Smale [2]). In the present work, we prove the completeness of various families of multivariate polynomials for Valiant's algebraic class of qp–computable families of multivariate polynomials. For the reader's convenience, we first present the relevant details of Valiant's theory. More material can be found in [4, 3].

A function $t : \mathbb{N} \to \mathbb{N}$ is called *p–bounded* if $t(n) \le O(n^c)$ for some constant $c$. The function $t$ is called *p–bounded from above and below* if in addition $t(n) \ge \Omega(n^{1/c})$. A function $u : \mathbb{N} \to \mathbb{N}$ is called *qp–bounded* if $u(n) \le n^{O(\log^c n)}$.

The main objects in Valiant's algebraic NP–completeness theory are certain families of multivariate polynomials. Throughout the remainder of this work, $k$ denotes a field.

**Definition 1.** *A sequence $f = (f_n)$ of multivariate polynomials over $k$ is called a p–family if the number of variables and the degree of $f_n$ are both p–bounded functions in $n$.*

The *complexity* $L(f)$ of a multivariate polynomial $f \in k[X_1, \dots, X_m]$ is the size of a smallest arithmetic circuit over the basis $\{+, -, *\}$ (all operations with fanin two) that computes $f$ from the indeterminates $X_1, \dots, X_m$ and the scalars in $k$.

**Definition 2.**
1. *A p–family $f = (f_n)$ is* p–computable *if the complexity $L(f_n)$ is a p–bounded function in $n$. The class of all p–computable families is denoted by* VP *(or* $\mathsf{VP}_k$*).*
2. *The p–family $f$ is* qp–computable *if $L(f_n)$ is a qp–bounded function in $n$. The class of all qp–computable families is denoted by* VQP *(or* $\mathsf{VQP}_k$*).*

In the same way, we can also define the class $\mathsf{VNP}$, an algebraic analogue of $\mathsf{NP}$. Since a detailed definition of $\mathsf{VNP}$ is more complicated than those of the classes $\mathsf{VP}$ and $\mathsf{VQP}$, the reader is referred to [4, 3]. The following hypotheses play a central role in Valiant's theory—like Cook's Hypothesis in structural complexity theory.

**Hypothesis 1.** *1.* Valiant's Hypothesis: $\mathsf{VP} \subsetneq \mathsf{VNP}$ *over any field.*
*2.* Extended Valiant's Hypothesis: $\mathsf{VNP} \setminus \mathsf{VQP} \neq \emptyset$ *over any field.*

In Valiant's model, families of polynomials are compared by a simple type of reductions, namely *projections*. A polynomial $f(X_1, \ldots, X_m)$ is called a projection of another polynomial $g(Y_1, \ldots, Y_n)$ if there are $s_1, \ldots, s_n \in k \cup \{X_1, \ldots, X_m\}$ such that $f(X_1, \ldots, X_m) = g(s_1, \ldots, s_n)$. In other words, $f$ is obtained from $g$ by replacing each of the $Y_1, \ldots, Y_n$ by a scalar from $k$ or by one of the $X_1, \ldots, X_m$.

**Definition 3.** *1. A family $f = (f_n)$ is a p–projection of $g = (g_m)$, in symbols $f \leq_{\mathrm{p}} g$, if there exists a function $r$ that is p–bounded from above and below such that*

$$\exists n_0\, \forall n \geq n_0 : f_n \text{ is a projection of } g_{r(n)} .$$

*2. A family $f = (f_n)$ is a qp–projection of $g = (g_m)$, in symbols $f \leq_{\mathrm{qp}} g$, if there exists a qp–bounded function $r$ that is also p–bounded from below such that*

$$\exists n_0\, \forall n \geq n_0 : f_n \text{ is a projection of } g_{r(n)} .$$

The relations "is a p–projection of" and "is a qp–projection of" are both transitive. Obviously, if $g \leq_{\mathrm{p}} f$, then also $g \leq_{\mathrm{qp}} f$.

The next step is to define $\mathsf{VQP}$–complete families.

**Definition 4.** *A qp–computable family $f$ is called* $\mathsf{VQP}$*–complete if $g \leq_{\mathrm{qp}} f$ for all $g \in \mathsf{VQP}$.*

As expected, if $f$ is $\mathsf{VQP}$–complete and $f \leq_{\mathrm{qp}} h$, then $h$ is also $\mathsf{VQP}$–complete.

Up to now, the only known $\mathsf{VQP}$–complete family is the *determinant* family defined by

$$DET_n = \det(X_{i,j})_{1 \leq i,j \leq n} .$$

(For a proof, see [3, Corollary 2.29].) As our main results, we exhibit further $\mathsf{VQP}$–complete families of multivariate polynomials. Specifically, we show that the families *iterated matrix multiplication $IMM$*, *matrix powering $POW$*, and *adjoint matrix $ADJ$* defined by

$$\begin{aligned} IMM_n &= \operatorname{trace}(X_1 \cdots X_n), \\ POW_n &= \operatorname{trace}(X^{\lfloor n/3 \rfloor}), \\ ADJ_n &= \operatorname{trace}(\det(X) \cdot X^{-1}) \end{aligned}$$

are all $\mathsf{VQP}$–complete. (Above, $X$ and the $X_\nu$ denote $n \times n$–matrices with independent indeterminate entries.) This proves a conjecture by Bürgisser [3, Conjecture 8.1]. The original conjecture for $POW$ made by Bürgisser is that $(\operatorname{trace}(X^n))$ is $\mathsf{VQP}$–complete. This remains an open problem.

The main technical problems we are confronted with are that we have a very weak type of reductions, namely qp–projections, and that we only compute one result.

For any constant $c \in \mathbb{N}$, let the family *constant size c iterated matrix multiplication c–CIMM* be defined through

$$c\text{–}CIMM_n = \mathrm{trace}(Y_1 \cdots Y_n)\,,$$

where the $Y_\nu$ are $c \times c$–matrices (and *not* $n \times n$–matrices) with independent indeterminate entries. Strengthening the above $\mathsf{VQP}$–completeness result for *IMM*, we also show that for any $c \geq 3$, the family $c$–*CIMM* is $\mathsf{VQP}$–complete. This follows from the results by Ben-Or and Cleve [1].

## 2 Auxiliary Results

We briefly review some (well known) results, which we will need later on, and provide some useful variations of these auxiliaries. For a multivariate polynomial $f \in k[X_1, \ldots, X_m]$ the *depth* $D(f)$ is the minimal depth of an arithmetic circuit over the basis $\{+, -, *\}$ (all operations with fanin two) that computes $f$ from the indeterminates $X_1, \ldots, X_m$ and the scalars in $k$.

**Theorem 1 (Hyafil, Valiant et al.).** *If $f$ is an $n$–variate polynomial of degree $d \geq 1$, then*

$$D(f) \leq O(\log(d \cdot L(f)) \log d + \log n).$$

*Moreover, there is an arithmetic circuit of depth $O(\log(d \cdot L(f)) \log d + \log n)$ and size $d^6 L(f)^3$ that computes $f$.*

For a proof of the first part of the statement, see [7]. It can also be shown that the constant hidden in the $O$–notation is universal. The second claim is due to Valiant et al. [9]. The reader is also referred to [4, Thm. 21.35]. Miller et al. [8] present an online construction.

For technical reasons, we introduce the family $c$–*CIMM*$'$ defined through

$$c\text{–}CIMM'_n = \text{the entry in position } (1,1) \text{ of } Y_1 \cdots Y_n,$$

where the $Y_\nu$ are $c \times c$–matrices with independent indeterminate entries. The family 3–*CIMM*$'$ plays an important role for our completeness results.

**Theorem 2 (Ben-Or & Cleve).** *Let $f$ be a multivariate polynomial. Moreover, let $\ell = 4^{D(f)}$. Then $f$ is a projection of* $3\text{–}CIMM'_\ell$.

For a proof, see [1, Thm. 1]. Since Ben-Or and Cleve focused on computing polynomial size formulas with polynomial length straight-line programs that use a constant number of registers, they only stated the above theorem for formulas. Nevertheless, Ben-Or and Cleves approach also works for arbitrary straight-line programs, since a straight-line program of depth $d$ induces a formula of depth $d$ and size at most $2^d$.

Since

$$(1,1)\text{–entry of } Y_1 \cdots Y_n = \operatorname{trace}(E_{1,1} \cdot Y_1 \cdots Y_n \cdot E_{1,1}),$$

where $E_{1,1}$ denotes the $c \times c$–matrix that has a one in position $(1,1)$ and zeros elsewhere, $c$–$CIMM'_n$ is a projection of $c$–$CIMM_{n+2}$. Therefore, the below theorem follows.

**Theorem 3.** *Let $f$ be a multivariate polynomial and let $\ell = 4^{D(f)} + 2$. Then $f$ is a projection of $3$–$CIMM_\ell$.*

## 3 Completeness Results

In this section, we prove as our main result the VQP–completeness of the families $IMM$, $POW$, and $ADJ$. Since each of these three families is in VP, it suffices to show the hardness.

### 3.1 Iterated Matrix Multiplication

**Theorem 4.** *For any $c \geq 3$, $c$–CIMM is VQP–complete (under qp–projections). The same is true for $c$–CIMM′.*

*Proof.* The polynomial $c$–$CIMM_n$ can be computed by an arithmetic circuit of size $O(n)$. Thus $c$–$CIMM \in \mathsf{VP} \subseteq \mathsf{VQP}$.

Since obviously $c$–$CIMM_n$ is a projection of $c'$–$CIMM_n$ for each $n$ and each $c' \geq c$, it is sufficient to show that for any $f = (f_n) \in \mathsf{VQP}$, $f \leq_{\mathrm{qp}} 3$–$CIMM$. By definition, we know that the number of variables and the degree of $f_n$ are p–bounded functions and that $L(f_n)$ is a qp-bounded function. By Theorem 1, $D(f_n) \leq O(\log^m n)$ for some constant $m$. By Theorem 3, $f_n$ is a projection of $3$–$CIMM_\ell$ where $\ell = n^{O(\log^{m-1} n)}$. Hence $f$ is a qp–projection of $3$–$CIMM$.

The result for $c$–$CIMM'$ follows completely alike. □

Since $3$–$CIMM_n$ is a projection of $IMM_n$, we immediately obtain the following corollary.

**Corollary 1.** *The family IMM is VQP–complete (under qp–projections).*

The next corollary is of rather technical nature. It describes a "self reducibility" property of $c$–$CIMM$. We will rely on the corollary in the subsequent sections.

**Corollary 2.** *Let $c \geq 3$ and let $i$ and $j$ be functions $\mathbb{N} \to \{1, 2, \dots, c\}$. Furthermore, let $(\alpha_n)$ and $(\beta_n)$ be sequences of scalars from $k$ and define $w(n) = \min\{i \geq n \mid \alpha_i \neq 0\}$. If $w$ is qp–bounded, then $(\alpha_n \cdot f_n + \beta_n)$ is VQP–complete, where $f_n$ is the entry in position $(i(n), j(n))$ of a generic iterated $3 \times 3$–matrix product of length $n$.*

*Proof.* We first prove that $(c\text{–}\mathit{CIMM}'_n + \beta_n)$ is $\mathsf{VQP}$–complete. Then we reduce $(c\text{–}\mathit{CIMM}'_n + \beta_n)$ to $(\alpha_n \cdot f_n + \beta_n)$.

For the first part, let $(g_n) \in \mathsf{VQP}$ be given. Then also $(g_n - \beta_n) \in \mathsf{VQP}$. By the $\mathsf{VQP}$–completeness of $c\text{–}\mathit{CIMM}'$, $(g_n - \beta_n)$ is a qp–projection of $c\text{–}\mathit{CIMM}'$. Thus $(g_n)$ is a qp–projection of $(c\text{–}\mathit{CIMM}'_n + \beta_n)$. Since $(g_n)$ was arbitrary, this shows the $\mathsf{VQP}$–completeness of $(c\text{–}\mathit{CIMM}'_n + \beta_n)$.

Now we reduce $(c\text{–}\mathit{CIMM}'_n + \beta_n)$ to $(\alpha_n \cdot f_n + \beta_n)$. To obtain $c\text{–}\mathit{CIMM}'_n + \beta_n$, we substitute $w(n+3) - n - 3$ many copies of the $c \times c$–identity matrix and one $\alpha^{-1}_{w(n+3)}$ multiple of the $c \times c$–identity matrix into $\alpha_{w(n+3)} \cdot f_{w(n+3)} + \beta_{w(n+3)}$ at arbitrary places except the first and the last matrix. (Note that $w(\nu) \geq \nu$ for all $\nu$.) As the first and the last matrix, we substitute appropriate permutation matrices that move the entry in position $(i(n), j(n))$ into position $(1, 1)$. Since $w$ is qp–bounded, $(c\text{–}\mathit{CIMM}'_n + \beta_n)$ is a qp–projection of $(\alpha_n \cdot f_n + \beta_n)$. $\square$

### 3.2 Matrix Powering

Our plan is to modify the reduction to iterated matrix multiplication given by Cook [5]. The weak type of reductions however is a major obstacle.

Let $X_1, \dots, X_m$ be $3 \times 3$–matrices with independent indeterminate entries. Let $Y$ be the block matrix of size $3m \times 3m$

$$Y = \begin{pmatrix} 0 & X_1 & 0 & \cdots & 0 \\ 0 & 0 & X_2 & & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & X_{m-1} \\ X_m & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

(Note the extra $X_m$ in the lower left corner. Without it, all powers of $Y$ would have trace zero.) A straight forward calculation shows that

$$Y^m = \begin{pmatrix} P_1 & 0 & 0 & \cdots & 0 \\ 0 & P_2 & 0 & & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & \cdots & P_m \end{pmatrix}, \tag{1}$$

where $P_\mu = X_\mu X_{\mu+1} \cdots X_m X_1 \cdots X_{\mu-1}$. By the below fact,

$$\operatorname{trace}(Y^m) = m \cdot \operatorname{trace}(X_1 \cdots X_m) = m \cdot 3\text{–}\mathit{CIMM}_m.$$

**Fact 1.** *1. For any two $\ell \times \ell$–matrices $A$ and $B$,* $\operatorname{trace}(AB) = \operatorname{trace}(BA)$.

2. *If we write $A = (A_{i,j})_{1 \leq i,j \leq q}$ as a block matrix with $(\ell/q) \times (\ell/q)$–blocks $A_{i,j}$, then* $\operatorname{trace} A = \operatorname{trace} A_{1,1} + \operatorname{trace} A_{2,2} + \cdots + \operatorname{trace} A_{q,q}$.

Thus $m \cdot 3$–*CIMM*$_m$ is a projection of $POW_{3m}$. If the characteristic of $k$ is zero, then $m \cdot 3$–*CIMM*$_m$ is always nonzero. If the characteristic $p > 0$, then at least every second of the $m \cdot 3$–*CIMM*$_m$ is nonzero. Thus the function $j \mapsto \min\{i \geq j \mid i \not\equiv 0\ (p)\}$ is qp–bounded. Hence by Corollary 2, the family $(m \cdot 3\text{–}\mathit{CIMM}_m)$ is VQP–complete and so is $POW$.

We define the family $m$–$POW$ for a given function $m : \mathbb{N} \to \mathbb{N}$ by

$$m\text{–}POW_n = \operatorname{trace}(X^{m(n)}),$$

where $X$ denotes a matrix with independent indeterminate entries of size $n \times n$.

For functions $m$ such that $m(n) \leq \lfloor n/3 \rfloor$ for all $n$, we can embed the above $\lfloor n/3 \rfloor$–powering problem into the $m(n)$–powering problem by placing the $3m(n) \times 3m(n)$–matrix $X$ together with an $(n - 3m(n)) \times (n - 3m(n))$–zero matrix on the diagonal:

$$Z = \begin{pmatrix} X & 0 \\ 0 & 0 \end{pmatrix}.$$

Thus $\operatorname{trace}(Z^{m(n)}) = \operatorname{trace}(X^{m(n)}) = POW_{3m(n)}$ is a projection of $m$–$POW_n$. Therefore, the below theorem follows (by applying the previous construction to $POW_{3m(n)}$, with possibly some of the $X_\mu$ substituted by identity matrices).

**Theorem 5.** *For any function $m$ such that $m(n) \leq \lfloor n/3 \rfloor$ for all $n$ and $m$ is p–bounded from below, the family $m$–$POW$ is* VQP*–complete (under qp–projections).*

### 3.3 Matrix Inversion

Let $X_1, \ldots, X_n$ be $3 \times 3$–matrices with indeterminate and independent entries. Let $N$ be the $3(n+1) \times 3(n+1)$–matrix

$$N = \begin{pmatrix} 0 & X_1 & 0 & \cdots & 0 \\ 0 & 0 & X_2 & & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & X_n \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}. \tag{2}$$

The matrix $N$ is nilpotent and we have

$$(I - N)^{-1} = I + N + N^2 + \cdots + N^n = \begin{pmatrix} I & P_{1,1} & P_{1,2} & \cdots & P_{1,n} \\ 0 & I & P_{2,2} & & P_{2,n} \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & P_{n,n} \\ 0 & 0 & 0 & \cdots & I \end{pmatrix},$$

where $I$ denotes the identity matrix of appropriate size ($3n+3$ on the left-hand and 3 on the right-hand side) and $P_{i,j}$ stands for the product $X_i \cdots X_j$ for $i \leq j$.

Let $S$ be the permutation matrix

$$S = \begin{pmatrix} 0 & I & 0 & \cdots & 0 \\ 0 & 0 & I & & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & I \\ I & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

We have

$$(S^{-1}(I-N))^{-1} = (I-N)^{-1}S = \begin{pmatrix} P_{1,n} & I & P_{1,1} & \cdots & P_{1,n-1} \\ P_{2,n} & 0 & I & & P_{2,n-2} \\ \vdots & & \ddots & \ddots & \vdots \\ P_{n,n} & 0 & 0 & \ddots & I \\ I & 0 & 0 & \cdots & 0 \end{pmatrix}. \tag{3}$$

Thus

$$\operatorname{trace}(S^{-1}(I-N))^{-1} = \operatorname{trace} P_{1,n} = 3\text{–}\mathit{CIMM}_n.$$

Because $\det(S^{-1}(I-N)) = \pm 1$, $\pm 3\text{–}\mathit{CIMM}_n$ is a projection of $\mathit{ADJ}_{3(n+1)}$. (Since $S$ is a permutation matrix, $S^{-1}(I-N)$ is a projection of the generic $3(n+1) \times 3(n+1)$–matrix $X$.) This yields the following completeness result.

**Theorem 6.** *The family $\mathit{ADJ}$ is* VQP*–complete (under qp–projections).*

## 4 Further Directions

What happens if we do not take the trace in the definition of the families $\mathit{IMM}$, $\mathit{POW}$, and $\mathit{ADJ}$, but look at the following families given by

$$\begin{aligned} \mathit{IMM}'_n &= (1,1)\text{–entry of } X_1 \cdots X_n, \\ \mathit{POW}'_n &= (1,1)\text{–entry of } X^{\lfloor n/3 \rfloor}, \\ \mathit{ADJ}'_n &= (1,1)\text{–entry of } \det(X) \cdot X^{-1}\,? \end{aligned}$$

From Theorem 4, (1), and (3), respectively, it follows that these families are also VQP–complete. Thus we have the following theorem.

**Theorem 7.** *The above families $\mathit{IMM}'$, $\mathit{POW}'$, and $\mathit{ADJ}'$ are* VQP*–complete (under qp–projections).*

*Remark 1.* By applying appropriate permutation matrices, we could also define $\mathit{IMM}'$ and $\mathit{ADJ}'$ not by taking the $(1,1)$–entry but any other entry and would still get the same completeness results for these families. Since Valiant's model is nonuniform, the entries may also vary throughout the whole sequence.

Can we achieve a similar result for the family $POW'$? In fact, we can. The proof is however a little more elaborate.

**Theorem 8.** *For any functions $i, j : \mathbb{N} \to \mathbb{N}$ with $1 \leq i(n), j(n) \leq n$ for all $n$, the family $((i(n), j(n))$–entry of $X^{\lfloor n/3 \rfloor})$ is a* VQP*–complete family (under qp–projections).*

*Proof.* Let w.l.o.g. $n = 3m$. We distinguish the cases $i(n) = j(n)$ and $i(n) \neq j(n)$. In the first case, note that in (1), each entry on the diagonal corresponds to an entry of an iterated product of $3 \times 3$–matrices of length $m$.

For the case $i(n) \neq j(n)$, note that also the entry in position $(1, 2)$ of $Y^n$ in (1) is an entry of an iterated $3 \times 3$–matrix product. Let $P$ be the permutation matrix that exchanges the first with the $i(n)$th and the second with the $j(n)$th row resp. column. The matrix $P$ is its own inverse. We now consider $PYP$ instead of $Y$ in (1). We have $(PYP)^m = PY^mP$. By the choice of $P$, the entry in position $(i, j)$ of $PY^mP$ is an entry of an iterated $3 \times 3$–matrix product.

Altogether, we obtain a VQP–complete family. □

Over fields of characteristic zero, we can even prove the VQP–completeness of the family $((1, 1)$–entry of $X^n)$ corresponding to the $n$–powering problem, a task which remains unsolved in the case of taking the trace.

**Theorem 9.** *Let $k$ be a field of characteristic zero. For any $i, j : \mathbb{N} \to \mathbb{N}$ with $1 \leq i(n), j(n) \leq n$ for all $n$ and any polynomial $p$, $((i(n), j(n))$–entry of $X^{p(n)})$ is a* VQP*–complete family (under qp–projections).*

*Proof.* Since $p$ is a polynomial, $f$ is in VP $\subseteq$ VQP.

It remains to show the hardness: let $X_1, \ldots, X_n$ be $3 \times 3$–matrices and define $N$ like in (2). The matrix $N$ is nilpotent, specifically, $N^{n+1} = 0$. We have

$$
\begin{aligned}
(I + N)^{p(n)} &= \sum_{\nu=0}^{n} \binom{p(n)}{\nu} N^{\nu} \\
&= \begin{pmatrix}
I & p(n) \cdot P_{1,1} & \binom{p(n)}{2} \cdot P_{1,2} & \cdots & \binom{p(n)}{n} \cdot P_{1,n} \\
0 & I & p(n) \cdot P_{2,2} & & \binom{p(n)}{n-1} \cdot P_{2,n} \\
\vdots & & \ddots & \ddots & \vdots \\
0 & 0 & 0 & \ddots & p(n) \cdot P_{n,n} \\
0 & 0 & 0 & \cdots & I
\end{pmatrix},
\end{aligned}
$$

where $I$ denotes the identity matrix of appropriate size and $P_{i,j}$ stands for the product $X_i \cdots X_j$.

If $i(n) \neq j(n)$, then we can move the entry in position $(1, n)$ to position $(i(n), j(n))$ by switching over from $(I + N)$ to $P(I + N)P$ for an appropriate permutation matrix (like in the proof of Theorem 8). After that, the entry in position $(i(n), j(n))$ is the $\binom{p(n)}{n}$–multiple of an entry of an iterated $3 \times 3$–matrix product.

It remains the case $i(n) = j(n)$. We may assume that $i(n) = j(n) = 1$. Otherwise, we switch over to $P(I + N)P$ where $P$ is the permutation matrix that exchanges the first and the $i(n)$th row resp. column. Let $T$ be the matrix

$$T = \begin{pmatrix} I & 0 & 0 & \cdots & 0 \\ 0 & I & 0 & & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & 0 \\ I & 0 & 0 & \cdots & I \end{pmatrix}.$$

The inverse of $T$ coincides with $T$ except that the identity matrix in the lower left corner has to be replaced by $-I$. A straight forward calculation shows that the $3 \times 3$–matrix in the upper left block of $(T^{-1}YT)^{p(n)} = T^{-1}Y^{p(n)}T$ equals $\binom{p(n)}{n} \cdot P_{1,n} + I$. Thus the entry in position $(1, 1)$ of $(T^{-1}YT)^{p(n)}$ is just $\binom{p(n)}{n} \cdot 3\text{–}\mathit{CIMM}'_n + 1$.

Since the characteristic of $k$ is zero, the coefficient $\binom{p(n)}{n} \neq 0$. Together with Corollary 2 this proves the claim of the theorem. $\square$

Once we have proven the completeness of $\mathit{IMM}$, $\mathit{POW}$, and $\mathit{ADJ}$, many other families of polynomials corresponding to problems from linear algebra turn out to be $\mathsf{VQP}$–complete.

As an example, we examine the family $\mathit{LINEQ}$

$$\mathit{LINEQ}_n = \text{first entry of } \det(X) \cdot X^{-1}b,$$

which corresponds to solving a system of linear equations $Xa = b$. Above, $X$ denotes an $n \times n$–matrix and $b$ a (column) vector of length $n$ with independent indeterminate entries.

If we specialize $b_1 \mapsto 1$ and $b_\nu \mapsto 0$ for $2 \leq \nu \leq n$, then the image of $\mathit{LINEQ}_n$ under this specialization is $\mathit{ADJ}'_n$. Thus, the family $\mathit{LINEQ}$ is $\mathsf{VQP}$–complete.

**Theorem 10.** *The family LINEQ is* $\mathsf{VQP}$*–complete (under qp–projections).*

Since the permanent family $\mathit{PER}$ is $\mathsf{VNP}$–complete over fields of characteristic other than two, the Extended Valiant's Hypothesis is equivalent to the following completely algebraic statements by our $\mathsf{VQP}$–completeness results: the Extended Valiant's Hypothesis holds iff $\mathit{PER}$ is not a qp–projection of $\mathit{IMM}$ nor of $\mathit{POW}$ nor of $\mathit{ADJ}$ nor of any other of the $\mathsf{VQP}$–complete families considered in this work.

## Acknowledgements

I would like to thank Peter Bürgisser for drawing my attention to the problems considered in the present work. The referees made a lot of thoughtful comments, which helped improving this work.

## References


1. Michael Ben-Or and Richard Cleve. Computing algebraic formulas using a constant number of registers. *SIAM J. Comput.*, 21(1):54–58, 1992.
2. L. Blum, M. Shub, and S. Smale. On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines. *Bulletin of the Amer. Math. Soc.*, 21:1–46, 1989.
3. Peter Bürgisser. *Completeness and Reduction in Algebraic Complexity Theory.* Springer, 2000.
4. Peter Bürgisser, Michael Clausen, and M. Amin Shokrollahi. *Algebraic Complexity Theory.* Springer, 1997.
5. Stephen A. Cook. A taxonomy of problems with fast parallel algorithms. *Information and Computation*, 64:2–22, 1985.
6. Joachim von zur Gathen. Feasible arithmetic computations: Valiant's hypothesis. *J. Symbolic Comput.*, 4:137–172, 1987.
7. Laurent Hyafil. On the parallel evaluation of multivariate polynomials. *SIAM J. Comput.*, 8(2):120–123, 1979.
8. Gary L. Miller, Vijaya Ramachandran, and Erich Kaltofen. Efficient parallel evaluation of straight-line code and arithmetic circuits. *SIAM J. Comput.*, 17(4):686–695, 1988.
9. L. G. Valiant, S. Skyum, S. Berkowitz, and C. Rackoff. Fast parallel computation of polynomials using few processors. *SIAM J. Comput.*, 12(4):641–644, 1983.
10. Leslie G. Valiant. Completeness classes in algebra. In *Proc. 11th Int. ACM Symp. on Theory of Computing (STOC)*, pages 249–261, 1979.
11. Leslie G. Valiant. The complexity of computing the permanent. *Theoret. Comput. Sci.*, 8:189–201, 1979.