Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 122 (2024)

A high dimensional Cramer's rule connecting homogeneous multilinear equations to hyperdeterminants

ANTOINE JOUX[1] AND ANAND KUMAR NARAYANAN[2]

[1] *CISPA – Helmholtz Center for Information Security, Saarbrücken, Germany.*
[2] *SandboxAQ, Palo Alto, California, USA.*
joux@cispa.de, anand.kumar@sandboxaq.com

Abstract. We present a new algorithm for solving homogeneous multilinear equations, which are high dimensional generalisations of solving homogeneous linear equations. First, we present a linear time reduction from solving generic homogeneous multilinear equations to computing hyperdeterminants, via a high dimensional Cramer's rule. Hyperdeterminants are generalisations of determinants, associated with tensors of formats generalising square matrices. Second, we devise arithmetic circuits to compute hyperdeterminants of boundary format tensors. Boundary format tensors are those that generalise square matrices in the strictest sense. Consequently, we obtain arithmetic circuits for solving generic homogeneous boundary format multilinear equations. The complexity as a function of the input dimension varies across boundary format families, ranging from quasi-polynomial to sub exponential. Curiously, the quasi-polynomial complexity arises for families of increasing dimension, including the family of multipartite quantum systems made of d qubits and one qudit. Finally, we identify potential directions to resolve the hardness the hyperdeterminants, notably modulo prime numbers through the cryptographically significant tensor isomorphism complexity class.

1. Introduction

1.1. **Homogeneous multilinear systems.** The familiar problem of solving homogeneous linear equations is to take a square matrix A and find a non zero vector x such that Ax is the zero vector. We devise algorithms for the natural high dimensional generalisation, which we call solving homogeneous multilinear equations. Let us rephrase what it means to solve homogeneous linear equations, to emphasise the motif that generalises. Given a square matrix A, find a pair of non zero vectors $\left(x^{(0)}, x^{(1)}\right)$ such that removing one of the vectors from the bilinear product $x^{(0)}Ax^{(1)}$ equals the zero vector. The solutions are merely pairs of non zero vectors $\left(x^{(0)}, x^{(1)}\right)$ with $x^{(0)}$ in the left kernel of A and $x^{(1)}$ in the right kernel of A. In homogeneous multilinear equations, a tensor A of dimension $r+1$ will be cast as the input in place of the square matrix. Multiplying A by the vectors $\left(x^{(0)}, x^{(1)}, \ldots, x^{(r)}\right)$ in the corresponding dimensions is a multilinear map taking this tuple

[1] The authour was supported by the European Union's H2020 Programme (grant agreement #ERC-669891).

ISSN 1433-8092

of vectors to a scalar. If we remove one of the vectors from the multiplication, the result is a vector. The solution we demand is a tuple of vectors $\left(x^{(0)}, x^{(1)}, \ldots, x^{(r)}\right)$ such that removing one of the vectors from the multilinear product gives the zero vector, irrespective of which one was removed. See definition 3.1 for the formal statement. We address the problem over the field of complex numbers and describe algorithms in the formalism of arithmetic circuits. Key to our approach is the hyperdeterminant.

1.2. **Hyperdeterminants.** The determinant of a square matrix is a homogeneous integer polynomial in the matrix entries that vanishes precisely when the matrix is singular. The hyperdeterminant is a high dimensional analogue of the determinant conceived by Cayley [3]. The hyperdeterminant is a homogeneous integer polynomial in the coordinates of the tensor that vanishes precisely when the tensor is singular. This notion of singularity is geometric and defined through projective duality. Except for a foray by Schläfli, the subject remained dormant for nearly a century and a half [22]. It was revived in the comprehensive work of Gelfand, Kapranov and Zelevinsky [11, 12], which contains most of the mathematical ingredients required in this paper.

1.2.1. *Tensor formats.* Just as the determinant is only defined for square matrices, the hyperdeterminant is only defined for certain formats of tensors. An $(r+1)$-dimensional tensor product of complex vector spaces of dimensions $k_0+1, k_1+1, \ldots, k_r+1$ constitutes a $(k_0+1) \times (k_1+1) \times \ldots \times (k_r+1)$ format. Say $k_0 \geq k_1 \geq \ldots \geq k_r$. The hyperdeterminant is defined for formats where the largest vector space dimension k_0 satisfies the convexity constraint $k_0 \leq k_1 + k_2 + \ldots + k_r$. Such formats generalise square matrices. Boundary formats are those satisfying the convexity constraint with equality, that is, $k_0 = k_1 + k_2 + \ldots + k_r$. The special case $r = 1$ corresponds to square matrices. Boundary formats generalise square matrices to higher dimensions in the strictest sense. To quote Gelfand, Kapranov and Zelevinsky [11], *"It is instructive to think of matrices of boundary format as proper high dimensional analogs of ordinary square matrices"*. Formats satisfying $k_0 < k_1 + k_2 + \ldots + k_r$ are called interior formats.

1.2.2. *Hardness of Hyperdeterminants.* We use hyperdeterminants as a means to solve homogeneous multilinear equations, but they are of intrinsic interest in complexity theory. The computational complexity of hyperdeterminants remains a mystery, either restricted to three dimensions or in general. Unlike the determinant (the two dimensional case), computing the hyperdeterminant (in three or more dimensions) is believed to be VNP-hard, yet a proof remains elusive. Testing if a given tensor is singular (has hyperdeterminant zero) is conjectured to be NP-hard [10]. Likewise, computing the hyperdeterminant is conjectured to be #P-hard in the counting model and VNP-hard in the arithmetic circuit model [10]. Several closely related three dimensional problems (such as zero testing singular values, defined for general formats in [16]) are proven to be NP, VNP or #P hard, but these instance are of formats where the hyperdeterminant is not defined. In particular, known hardness reductions to tensor problems seem to fall apart in formats satisfying the convexity constraint. Computing the combinatorial hyperdeterminant is known to be hard [10]. But the combinatorial hyperdeterminant more closely resembles the permanent and does not have the algebraic/geometric structure that underlies the hyperdeterminant. Another aspect to keep in mind is that the hyperdeterminant can have degree exponential in the size of the input, even in three dimensions. For instance, to write down a $(2n+1) \times (n+1) \times (n+1)$ boundary format tensor takes only cubic in n entries. However the degree of the hyperdeterminant is $(2n+1)!/n!^2 \approx 2^n$.

1.2.3. *Hyperdeterminants and quantum information.* Hyperdeterminants arise in quantum information when the amplitudes of quantum states are considered as normalised tensors in a projective space. The absolute value of the hyperdeterminant of three qubits ($r = 2, k_0 = k_1 = k_2 = 1$) is known as 3-tangle, an important entanglement measure generalising concurrence (the usual determinant) of bipartite systems [6]. In particular, the hyperdeterminant is invariant under local operations and classical communication (LOCC). Further significance of hyperdeterminants to quantum information was identified by Miyake and Wadati [18], through projective duality between separability and singularity.

1.3. **Our Contribution.**

1.3.1. *Reducing homogeneous multilinear systems to hyperdeterminants.* The geometric notion of singularity of a tensor (the hyperdeterminant vanishing) is equivalent to the algebraic notion of degeneracy that ensures the existence of a solution to homogeneous multilinear equations. Therefore, we may test if there is a solution to the homogeneous multilinear equation by checking if the hyperdeterminant of the tensor is zero. This correspondence begs the question as to if the solutions of the multilinear equation can be inferred through computation of the hyperdeterminant. It is important to consider the model of computation for the hyperdeterminant. The minimal computational assumption is a black-box that computes the hyperdeterminant of a given tensor. But, it is not obvious how useful black-box access is. The exponential degree of the hyperdeterminant and the lack of obvious structure (such as sparsity) make interpolating the hyperdeterminant as a polynomial using black-box evaluations difficult. We instead consider white-box computation: an arithmetic circuit that takes tensor entries as inputs and outputs the hyperdeterminant.

In § 3, we present a reduction. Given an arithmetic circuit that computes the hyperdeterminant (for a tensor format), we build an arithmetic circuit of asymptotically the same size that solves generic multilinear equations (of the same format). The key to the reduction is a theorem of Gelfand, Kapranov and Zelevinsky relating the Segre embedding of solutions of multilinear equations with partial derivatives of the hyperdeterminant. It may be thought of as a high dimensional generalisation of Cramer's rule. We invoke the Baur-Strassen algorithm to construct arithmetic circuits for all these partial derivatives at once from the arithmetic circuit computing the hyperdeterminant, thereby completing the reduction with only linear complexity.

The qualifier "generic" in generic homogeneous multilinear equations refers to there being at most one projective solution. Geometrically, this translates to the input tensor either being non-singular or a simple singularity. That is, the tensor cannot be a zero of the hyperdeterminant of multiplicity greater than one. Weyman and Zelevinsky proved that non-generic tensors (roots of the hyperdeterminant of multiplicity greater than one) form a co-dimension one projective subvariety of singular tensors [30]. Therefore non-generic tensors fall into a Zariski closed subspace, justifying the "generic" label. It remains an open problem if the non generic case can be handled by methods similar to our reduction.

1.3.2. *Computing Hyperdeterminants of boundary formats.* In § 4, we devise arithmetic circuits to compute hyperdeterminants of boundary format tensors. There is one circuit for each boundary format. The tensor entries are the inputs to the arithmetic circuit. The main ingredient in the construction is a correspondence between the hyperdeterminant of boundary format tensors and the determinant of a linear transformation connecting sections of vector bundles built from the tensor [11][Theorem 4.3](see also, [7]). Concretely, the linear transformation is between two spaces of multihomogeneous polynomials in the coordinate ring with prescribed degrees. The square matrix of this linear transformation is of dimension equal to the degree $(k_0+1)!/(k_1!k_2!\dots k_r!)$ of the hyperdeterminant, which could range from 2^{k_0} to $(k_0+1)!$. By choosing a monomial bases for the polynomial spaces, we ensure that the matrix entries are either zero or entries from the tensor. An arithmetic circuit for computing the determinant for this square matrix yields an arithmetic circuit for computing the hyperdeterminant. The circuit complexity is the degree of the hyperdeterminant $(k_0+1)!/(k_1!k_2!\dots k_r!)$ raised to small exponent to account for determinant computation. In many cases this exponent can be taken to be the matrix multiplication exponent ω. At worst, the exponent is 4, for division-free circuits that accommodate computation over arbitrary rings, including fields of positive characteristic dividing the degree of the hyperdeterminant.

1.3.3. *Complexity.* The reduction and the algorithm for computing the hyperdeterminant in concert yield $O\left(\left(\frac{(k_0+1)!}{k_1!k_2!\dots k_r!}\right)^{\omega}\right)$ sized arithmetic circuits to solve generic homogeneous boundary format multilinear equations. To make sense of this complexity, consider the following two families of boundary format tensors. For the three dimensional family $(2n+1)\times(n+1)\times(n+1)$, the complexity is $O\left(\left((2n+1)!/n!^2\right)^{\omega}\right)$. This is roughly $O\left(2^{n\omega}\right)$, simply exponential in the dimension $4n+3$ of the output. This is subexponential in the dimension $(2n+1)(n+1)^2$ of the input. For the $d+1$ dimensional family $(d+1)\times\underbrace{2\times 2\times\dots\times 2}_{d}$, the circuit complexity $O\left((d+1)!\right)$ is quasi polynomial in the input dimension $(d+1)2^d$. It is remarkable that a natural tensor problem without structure has a quasi polynomial time algorithm time for a family of increasing dimension. Further, this family captures $(d+1)$-partite quantum system consisting of d qubits and a qudit. The hyperdeterminant vanishing is related to the existence of a partition of the $(d+1)$-partite system across which the quantum state splits into a product [18]. For the most common d-partite setting consisting of d qubits, Schläfli's method [22] suggests an algorithm to compute hyperdeterminants that is recursive across the dimensions. A rigorous analysis of such a recursive algorithm based on Schläfli's method is left for future work.

In terms of algorithms to compare with, Gröbner basis methods can be deployed to solve homogeneous multilinear equations. But applying them naively only guarantees a solution in double exponential time (over Global fields such as $\mathbb{C}$). The performance of Gröbner basis techniques tailored to this problem warrants further investigation. For instance, determinantal structure was exploited in Gröbner basis algorithms addressing similar problems by Spaenlehauer [26, 27] and M. Safey El Din, and Ê. Schost [21]. Our results hint that there are monomial orderings for which Gröbner methods tailored to solving homogeneous multilinear equations are fast.

1.3.4. *Towards proving hardness of hyperdeterminants.* The mystery surrounding the hardness of computing the hyperdeterminant drew us to the problems addressed in this work. A technical difficulty in proving the hardness of the hyperdeterminants using well known techniques (such as in [16]) is the following. When one tries to embed a hard computational problem into computing hyperdeterminants of three dimensional tensors, one of the dimensions of blows up and we land in a tensor format for which the hyperdeterminant does not exist. An important consequence of our reduction is that *if solving homogeneous multilinear equations is hard for some family boundary or interior formats, then so is computing the hyperdeterminant! Therefore, to prove the hardness of computing hyperdeterminants, it now suffices to prove the hardness of solving homogeneous multilinear equations for some family of boundary or interior formats.* To this end, an intermediate step might be to reduce solving inhomogeneous multilinear equations to solving homogeneous multilinear equations, since it seems easier to encode known NP-hard problems as the former. Further, our work suggests it may be fruitful to consider boundary formats such as $(2n+1) \times (n+1) \times (n+1)$, for they may accommodate more geometric methods.

Finally, in § 5, we investigate the possibility of proving the hardness computing hyperdeterminants modulo primes. To this end, we identify the (cryptographically significant) complexity class (**TI**) of tensor isomorphism problems as candidates to reduce from. In particular, we reduce the tensor isomorphism problem with respect to the special linear group action to computing hyperdeterminants modulo primes. But the tensor isomorphism complexity class is defined with isomorphisms under the general linear group action. It is not known if the tensor isomorphism problem with the special linear group action is **TI**-hard. If the answer turns out to be yes, then our reduction implies that computing hyperdeterminants modulo primes is cryptographically hard, in the sense that the average case **TI** instances are distinguished from random tensor pairs by the hyperdeterminant. If the hyperdeterminant were easy, those cryptosystems would be broken. Over fixed field sizes, it might be possible to prove that the tensor isomorphism problem with the special linear group action is indeed **TI**-hard, following ideas similar to [24]. We thank an anonymous referee for pointing out this possibility and leave this to future work.

2. Preliminaries: Tensor singularity and hyperdeterminants

2.1. **Cayley's hyperdeterminants.** Let $V_0, V_1, \ldots, V_r$ be $r+1$ vector spaces over the complex numbers $\mathbb{C}$ of respective dimensions $k_0+1, k_1+1, \ldots, k_r+1$. Fix a coordinate system $x^{(j)} = (x_0^{(j)}, x_1^{(j)}, \ldots, x_{k_j}^{(j)})$ for the j^{th}-vector space V_j, or equivalently an ordered basis for the dual V_j^*. Identify an $(r+1)$ dimensional tensor $A \in V_0^* \otimes V_1^* \otimes \ldots \otimes V_r^*$ with an $r+1$-dimensional matrix

$$A = (a_{i_0,i_1,\ldots,i_r}, 0 \leq i_0 \leq k_0, 0 \leq i_1 \leq k_1, \ldots, 0 \leq i_r \leq k_r)$$

of format $(k_0+1) \times (k_1+1) \times \ldots \times (k_r+1)$.

Square matrices are a special case ($r = 1$ and $k_0 = k_1$) and come with the familiar determinant whose vanishing characterises singularity/degeneracy. The hyperdeterminant is a multidimensional generalisation of the determinant that characterises singularity/degeneracy for tensors formats that generalise square matrices. We start with a geometric definition, equivalent analytic (singularity) and algebraic (degeneracy) formulations follow thereafter.

2.1.1. *Geometric definition.* Let $\mathbb{P}(V_j) \cong \mathbb{P}^{k_j}$ be the projectivisation of V_j. We need the Cartesian product of these projective spaces, yet desire that the product itself is projective. Let X be the image of the Cartesian product (purely separable tensors) $\mathbb{P}^{k_0} \times \mathbb{P}^{k_1} \times \ldots \times \mathbb{P}^{k_r}$ under the Segre embedding

$$\mathbb{P}(V_0) \times \mathbb{P}(V_1) \times \ldots \times \mathbb{P}(V_r) \hookrightarrow \mathbb{P}\left(V_0 \otimes V_1 \otimes \ldots \otimes V_r\right) \cong \mathbb{P}^{(k_0+1)(k_1+1)\ldots(k_r+1)-1}$$

$$\left(\left(x_0^{(0)} : x_1^{(0)} : \ldots : x_{k_0}^{(0)}\right), \ldots, \left(x_0^{(r)} : x_1^{(r)} : \ \ldots : x_{k_r}^{(r)}\right)\right) \tag{2.1}$$

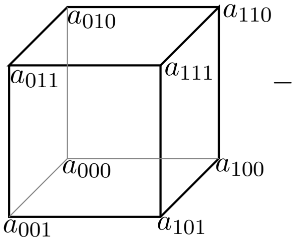
$$\longmapsto \left(x_0^{(0)} x_0^{(1)} \ldots x_0^{(r)} : \ldots : x_{k_0}^{(0)} x_{k_1}^{(1)} \ldots x_{k_r}^{(r)}\right). \tag{2.2}$$

The image under the embedding is a smooth projective variety called the Segre variety, which we denote by X. Let $X\check{}$ denote the projectively dual variety of X consisting of all hyperplanes in the ambient projective space $\mathbb{P}\left(V_0 \otimes V_1 \otimes \ldots \otimes V_r\right)$ tangent to X at some point. By projective duality (hyperplanes ↔ points), $X\check{}$ is a variety in the dual projective space $\mathbb{P}\left(V_0 \otimes V_1 \otimes \ldots \otimes V_r\right)^*$. Gelfand, Kapranov and Zelevinsky characterised precisely when $X\check{}$ is a hypersurface (that is, co-dimension one). It is when the convexity condition

$$\forall\ 0 \leq j \leq r, \qquad k_j \leq \sum_{\ell \neq j} k_\ell$$

holds, which we assume from here on. Being a hypersurface, the defining equation of $X\check{}$ is a homogeneous polynomial in the coefficients $a_{i_1,i_2,\ldots,i_d}$, defined to be the hyperdeterminant $Det()$. It is an irreducible polynomial with integer coefficients. It can be made unique by insisting that the coefficients are co-prime and choosing a sign.

2.1.2. *Example.* The first example is the $r = 1$ case, of the usual 2 dimensional matrices. The convexity constraint simplifies to $k_0 = k_1$, confining to square matrices. For square matrices, the hyperdeterminant coincides with the classical determinant. The following first example in 3 dimensions goes back to Cayley [3] and the advent of hyperdeterminants. It is synonymous with the tripartite entanglement measure 3-tangle of three qubits. The hyperdeterminant of a $2 \times 2 \times 2$ format tensor A indexed by the vertices of a cube is



$$\begin{aligned}Det(A) = a_{000}^2 a_{111}^2 + a_{001}^2 a_{110}^2 + a_{010}^2 a_{101}^2 + a_{011}^2 a_{100}^2 \\ -2(a_{000}a_{001}a_{110}a_{111} + a_{000}a_{010}a_{101}a_{111} + a_{000}a_{011}a_{100}a_{111} \\ +a_{001}a_{010}a_{101}a_{110} + a_{001}a_{011}a_{110}a_{100} + a_{010}a_{011}a_{101}a_{100}) \\ +4(a_{000}a_{011}a_{101}a_{110} + a_{001}a_{010}a_{100}a_{111}).\end{aligned}$$

The first group of monomials correspond to the four opposing vertices across the main diagonals. The second group to the six pairs of opposing sides. The last group to the two tetrahedrons with edges on the diagonals of the faces.

2.1.3. *Boundary and interior formats.* Without loss of generality, assume from here on that $k_0 \geq k_1 \geq \ldots \geq k_r$. The convexity condition (which we remind, we always assume) simplifies to $k_0 \leq \sum_{\ell=1}^r k_\ell$. Boundary formats are those meeting the convexity constraint with equality, that is $k_0 = \sum_{\ell=1}^r k_\ell$. Interior formats are those satisfying the strict convexity constraint $k_0 < \sum_{\ell=1}^r k_\ell$.

3. Solving multilinear equations through hyperdeterminants

3.1. **Hyperdeterminants, degeneracy of tensors and multilinear equations.**

Definition 3.1. (Solving homogeneous multilinear equations) Given a tensor A, decide if there is a $w \in X$ such that in every dimension j,

$$\nabla_{A,j}(w) := \sum_{0 \leq i_j \leq k_j} \left(\sum_{\substack{0 \leq i_0 \leq k_0 \\ \cdots \\ 0 \leq i_r \leq k_r}} a_{i_0,i_1,\ldots,i_r} w_{i_0}^{(0)} w_{i_1}^{(1)} \ldots w_{i_{j-1}}^{(j-1)} w_{i_{j+1}}^{(j+1)} \ldots w_{i_r}^{(r)} \right) x_{i_j}^{(j)} = 0 \left(\in V_j^*\right).$$

The inner summation is over all dimensions except j. If such a solution w exists, find one. A tensor A is said to be degenerate if there is such a w.

Since the Segre variety X lives in the projective tensor space $\mathbb{P}\left(V_0 \otimes V_1 \otimes \ldots \otimes V_r\right)$, it is expensive to write down the solution $w \in X$ as a tensor. Instead, we may output a tuple of vectors in the Cartesian space $\mathbb{P}^{k_0} \times \mathbb{P}^{k_1} \times \ldots \times \mathbb{P}^{k_r}$ whose image under the Segre embedding is a solution $w \in X$.

Lemma 3.2. [12, Chap 14, Prop. 1.1] *A tensor A is degenerate if and only if $Det(A) = 0$.*

Proof. We sketch the proof from [12, Chap 14, Prop. 1.1] to give an impression of the connection between degeneracy and hyperdeterminants. To this end, consider the following analytic notion of singularity to complement the geometric definition of hyperdeterminants. To clarify the relation of hyperdeterminants to singularity of tensors, ask when the hyperplane $\{A = 0\}$ carved by A is in $X\check{}$. It is precisely when there is a point $x \in X$ at which the hyperplane $\{A = 0\}$ is tangent. This happens precisely when there is a point $x \in X$ such that the multilinear form (arising from the restriction of A on X)

$$f_A(x) := \sum_{\substack{0 \le i_0 \le k_0 \\ \cdots \\ 0 \le i_r \le k_r}} a_{i_0,i_1,\ldots,i_r} x^{(0)}_{i_0} x^{(1)}_{i_1} \ldots x^{(r)}_{i_r} \text{ and all its partial derivatives } \frac{\partial f_A(x)}{\partial x^{(j)}_{i_j}}, \quad \forall j, i_j$$

vanish. In particular, such an x is a singular point of the hyperplane $\{A = 0\}$. We may thus identify the hyperdeterminantal variety $X\check{}$ with singular tensors. By inspection, we see that the condition for singularity and degeneracy are the same. □

Therefore the decision making part of solving homogeneous multilinear equations is equivalent to testing if $Det(A) = 0$. Can hyperdeterminants be used to find solutions? We prove that they can, for the generic case of the problem, which we next define.

Definition 3.3. (Solving generic homogeneous multilinear equations) Given a tensor A with a promise that A is either non singular or a non singular point of $X\check{}$, solve the homogeneous multilinear equation with input A.

We next justify why this promise version captures generic instances of the problem. As we saw before, by projective duality, there is a point $w \in X$ in the Segre variety solving the homogeneous multilinear equation corresponding to A if and only if A is in the Hyperdeterminantal variety $X\check{}$. Further, A could either be a singular point (that is, a zero of multiplicity greater than one) or a non singular point on $X\check{}$. If A is a non singular point in $X\check{}$, then there is a unique solution w, which the problem demands that we find. If A is a singular point in $X\check{}$, then we have to detect that this is the case. But, we do not have to find a solution. Remarkably, for dimension at least three (that is, $r > 1$), excluding the interior format $2 \times 2 \times 2$, Weyman and Zelevinsky proved that the singular points of $X\check{}$ form a co-dimension one projective sub variety [30]. Therefore, by dimension considerations, a generic singular tensor is indeed a non singular point on $X\check{}$. The non-generic tensor inputs we abandon are in a Zariski closed subspace.

A high dimensional Cramer's rule. We reduce solving generic homogeneous multilinear equation to computing hyperdeterminants through the following characterisation of the unique solution by Gelfand, Kapranov and Zelevinsky [11, Proposition 1.2]. Let A be the input describing the homogeneous multilinear equation with the promise that A is a non singular point of $X\check{}$. If $Det(A) \neq 0$, output that there is no solution. If $Det(A) = 0$, then the promise ensures that there is a unique solution w. Let B be a tensor of the same format as the input A, but with with entries $b_{i_0,i_1,\ldots,i_r}$ that are commuting indeterminates. The hyperdeterminant $Det(B)$ is then an integer polynomial in the indeterminates $b_{i_0,i_1,\ldots,i_r}$. Up to a normalisation factor, for all $i_0, i_1, \ldots, i_r$, the unique solution

$$w = \left(w^{(0)}_0 w^{(1)}_0 \ldots w^{(r)}_0 : \ldots : w^{(0)}_{k_0} w^{(1)}_{k_1} \ldots w^{(r)}_{k_r} \right) \in X \subseteq \mathbb{P}\left(V_0 \otimes V_1 \otimes \ldots \otimes V_r\right)$$

in the Segre variety satisfies

$$w^{(0)}_{i_0} w^{(1)}_{i_1} \ldots w^{(r)}_{i_r} = \frac{\partial Det(B)}{\partial b_{i_0,i_1,\ldots,i_r}} \Big|_{B=A} . \tag{3.1}$$

It is too expensive to write out w as a point in the ambient tensor space $\mathbb{P}\left(V_0 \otimes V_1 \otimes \ldots \otimes V_r\right)$. Its pre-image

$$\left(\left(w_0^{(0)} : w_1^{(0)} : \ldots : w_{k_0}^{(0)}\right), \ldots, \left(w_0^{(r)} : w_1^{(r)} : \ldots : w_{k_r}^{(r)}\right)\right) \in \mathbb{P}(V_0) \times \mathbb{P}(V_1) \times \ldots \times \mathbb{P}(V_r)$$

in the Cartesian space is a succinct representation that we can explicitly write down. Returning a tuple of vectors as the solution is also in the spirit of the homogeneous linear equations that we are generalising. Since A is a non singular point of $X^{\vee}$, there is at least one $(\widehat{i_0}, \widehat{i_1}, \ldots, \widehat{i_r})$ such that $\frac{\partial Det(B)}{\partial b_{\widehat{i_0}, \widehat{i_1}, \ldots, \widehat{i_r}}} \Big|_{B=A} \neq 0$. By equation 3.1, $w^{(0)}_{\widehat{i_0}}, w^{(1)}_{\widehat{i_1}}, \ldots, w^{(r)}_{\widehat{i_r}}$ are all non zero, which allows us to set them all to one as normalisation,

$$w^{(0)}_{\widehat{i_0}} = w^{(1)}_{\widehat{i_1}} = \ldots, w^{(r)}_{\widehat{i_r}} = 1.$$

With one non zero coordinate in each vector set to one, the i_j-th coordinate of the j-th vector is given by

$$w^{(j)}_{i_j} = \frac{\partial Det(B)}{\partial b_{\widehat{i_0}, \ldots, \widehat{i_{j-1}}, i_j, \widehat{i_{j+1}}, \ldots, \widehat{i_r}}} \Big|_{B=A} . \tag{3.2}$$

Given an arithmetic circuit to compute the hyperdeterminant (for the format of A), the Baur-Strassen algorithm [1] constructs an arithmetic circuit that computes all $k_0 k_1 \ldots k_r$ of the partial derivatives

$$\left(\frac{\partial Det(B)}{\partial b_{i_0, i_1, \ldots, i_r}} \Big|_{B=A}, 0 \leq j \leq r, 1 \leq i_0 \leq k_0, 1 \leq i_1 \leq k_1, \ldots, 1 \leq i_r \leq k_r\right)$$

sought (in determining non zero coordinates and in equation 3.2) at once. Remarkably, the size of this arithmetic circuit is only a small constant times that of the circuit for computing the hyperdeterminant.

Remark 3.4. *For our reduction of solving multilinear equations to hyperdeterminants to hold for quantum algorithms, we need a quantum version of Baur-Strassen that converts a quantum circuit computing the hyperdeterminant into one computing all its partial deivatives demanded by equation 3.2. While there is work on quantum versions of Baur-Stassen/automatic differentiation, they are not known to work in generality. But there is an approximate algorithm of Jordan* [13] *for computing the gradient that suffices if we are only interested in solving the multilinear system up to first order errors.*

4. Hyperdeterminants of boundary format

In this section, we devise an algorithm that given a boundary format tensor A, computes its hyperdeterminant. The algorithm can be realised as an arithmetic circuit. Recall that for boundary formats, $k_0 = k_1 + k_2 + \ldots + k_r$. Hyperdeterminants of boundary formats have a simple interpretation as resultants of a system of multilinear forms following the "Cayley trick". Slices of A in the first dimension form a collection of $k_0 + 1$ multilinear forms

$$f_A^{(i_0)}(x) := \sum_{\substack{0 \le i_1 \le k_1 \\ \cdots \\ 0 \le i_r \le k_r}} a_{i_0,i_1,\ldots,i_r} x_{i_1}^{(1)} x_{i_2}^{(2)} \ldots x_{i_r}^{(r)}, \quad 0 \le i_0 \le k_0. \tag{4.1}$$

The hyperdeterminant $Det(A)$ vanishes precisely when the resultant of $f_A^{(i_0)}(x),\ 0 \le i_0 \le k_0$ does. For positive integers $s_1, s_2, \ldots, s_r$, let

$$S(s_1, s_2, \ldots, s_r) \cong \mathrm{Sym}^{s_1}(V_1) \otimes \mathrm{Sym}^{s_2}(V_2) \otimes \ldots \otimes \mathrm{Sym}^{s_r}(V_r)$$

denote the space of polynomials that are for each $j \in 1, 2, \ldots, d$ homogeneous of degree s_j in the coordinates $x_{i_j}^{(j)}, 0 \le i_j \le k_j$. Set $m_1 := 0$ and for $j > 1$, set $m_j := k_1 + k_2 + \ldots + k_{j-1}$. The conception of our algorithms is primarily due to the following theorem relating boundary format hyperdeterminants to determinants of large matrices built with the above slices.

Theorem 4.1. *(Gelfand-Kapranov-Zelevinsky,* [11]*[Theorem 4.3]) The hyperdeterminant $Det(A)$ of a boundary format $A \in V_0^* \otimes V_1^* \otimes \ldots \otimes V_r^*$ equals (up to sign) the determinant of the linear operator*

$$\delta_A : S(m_1, m_2, \ldots, m_r)^{k_0+1} \longrightarrow S(m_1+1, m_2+1, \ldots, m_r+1)$$

$$(g_0, g_1, \ldots, g_{k_0}) \longmapsto \sum_{i_0=0}^{k_0} f_A^{(i_0)} g_{i_0}.$$

Proof. See [11][Theorem 4.3] or [7] for proofs. □

The matrix of δ is indeed square. We may count monomials and verify that the dimensions

$$\dim\left(S(m_1, m_2, \ldots, m_r)^{k_0+1}\right) = \frac{(k_0+1)!}{k_1!k_2!\ldots k_r!}$$

and

$$\dim\left(S(m_1+1, m_2+1, \ldots, m_r+1)\right) = (k_1 + k_2 + \ldots + k_r + 1)\binom{k_1 + k_2 + \ldots + k_r}{k_1, k_2, \ldots, k_r}$$

of the two spaces of polynomials are the same. By theorem 4.1, this count is also the degree of the hyperdeterminant

$$\deg(Det(A)) = \frac{(k_0+1)!}{k_1!k_2!\ldots k_r!} = (k_1 + k_2 + \ldots + k_r + 1)\binom{k_1 + k_2 + \ldots + k_r}{k_1, k_2, \ldots, k_r}. \tag{4.2}$$

Theorem 4.1 gives a determinantal identity for each choice of permutation of the vector spaces $V_1, V_2, \ldots, V_r$, which is implicit in the statement. It is not clear if there is a choice of permutation better suited to computation than the others. We now have all the ingredients to describe the hyperdeterminant computation.

Computation of the hyperdeterminant. Let A be the input tensor. Fix lexicographic ordered monomial bases P and Q respectively for $S(m_1, m_2, \dots, m_r)$ and $S(m_1+1, m_2+1, \dots, m_r+1)$. With bases fixed, we will also denote the matrix of δ_A by δ_A. For $p \in P, q \in Q$, the (p,q)-th entry $\delta_A^{(p,q)}$ of δ_A is either 0 or an $a_{i'_0, i'_1, \dots, i'_r}$ for some $i'_0, i'_1, \dots, i'_r$. Since $\log(\deg(Det(A)))$ is polynomial in k_0, the encoding $(p,q) \longmapsto 0$ or $i'_0, i'_1, \dots, i'_r$ is easy to compute in time polynomial in k_0. This encoding transforms an arithmetic circuit for computing the determinant of a $\frac{(k_0+1)!}{k_1!k_2!\dots k_r!} \times \frac{(k_0+1)!}{k_1!k_2!\dots k_r!}$ square matrix into an arithmetic circuit to compute the hyperdeterminant. The complexity of the circuit is $O\left(\left(\frac{(k_0+1)!}{k_1!k_2!\dots k_r!}\right)^4\right)$, using a division-free circuit for the determinant [17].
We conclude with an illustrative example of the determinantal identity underlying the hyperdeterminant computation.

Example. Let $A = (a_{i_0, i_1, i_2})$ be a tensor of the simplest three dimensional boundary format, namely $3 \times 2 \times 2$. Through lexicographic monomial orderings, fix ordered bases $\left(x_0^{(2)}, x_1^{(2)}\right)$ of $S(0,1)$ and $\left(x_0^{(1)}x_0^{(2)}x_0^{(2)}, x_0^{(1)}x_0^{(2)}x_1^{(2)}, x_0^{(1)}x_1^{(2)}x_1^{(2)}, x_1^{(1)}x_0^{(2)}x_0^{(2)}, x_1^{(1)}x_0^{(2)}x_1^{(2)}, x_1^{(1)}x_1^{(2)}x_1^{(2)}\right)$ of $S(1,2)$. Then

$$\delta_A : S(0,1)^3 \longrightarrow S(1,2)$$

corresponds to the matrix

$$\begin{pmatrix} a_{000} & 0 & a_{100} & 0 & a_{200} & 0 \\ a_{001} & 0 & a_{101} & 0 & a_{201} & 0 \\ a_{010} & a_{000} & a_{110} & a_{100} & a_{210} & a_{200} \\ a_{011} & a_{001} & a_{111} & a_{101} & a_{211} & a_{201} \\ 0 & a_{010} & 0 & a_{110} & 0 & a_{210} \\ 0 & a_{011} & 0 & a_{111} & 0 & a_{211} \end{pmatrix}.$$

5. On the hardness of computing hyperdeterminants modulo primes

Let p denote a prime. Recall from § 2 that for valid tensor formats, $Det()$ is a polynomial with integer coefficients, that is primitive and uniquely defined by choosing a sign. We prove that given a tensor $A = (a_{i_0,i_1,i_2}, 0 \le i_0, i_1, i_2 \le n)$ of "cubical" format $(n+1) \times (n+1) \times (n+1)$ with integer coordinates (that is, $\forall (i_0, i_1, i_2), a_{i_0,i_1,i_2} \in \mathbb{Z}$), it is hard to compute $Det(A)$ mod p, under certain post-quantum cryptographic assumptions.

Let $\mathbb{F}_p$ denote the finite field with a prime number p element. Fix an algebraic closure $\bar{\mathbb{F}}_p$ of $\mathbb{F}_p$. The theory of hyperdeterminants is yet to be worked out rigorously over $\bar{\mathbb{F}}_p$, unlike the theory over complex numbers developed by Gelfand, Kapranov and Zelevinsky. The key issue is that the geometric theory of projective duality used in the very definition of hyperdeterminants does not in general translate to positive characteristic. Thankfully, in our particular context, the duality used to define and prove the existence of hyperdeterminants is proven to hold true over $\overline{\mathbb{F}_p}$ for all primes p by Kaji [14]. We will work under the assumption that the basic properties of hyperdeterminants from [11] translate to $\bar{\mathbb{F}}_p$. In particular, the hyperdeterminant over $\bar{\mathbb{F}}_p$ is $Det(A)$ mod p, the hyperdeterminant over the integers modulo p. We defer rigorous proofs to later works, focusing instead on sketching the main ideas in the reduction.

We next state the computational problem of computing hyperdeterminants modulo primes. To control the length of the input, without loss of generality, we may assume that the coordinates $a_{i_0,i_1,i_2} \in \mathbb{F}_p$ instead of being integers. It is therefore convenient to think of the input as being

$$A = (a_{i_0,i_1,i_2}, 0 \leq i_0, i_1, i_2 \leq n) \in (\mathbb{F}_p^{n+1})^* \otimes (\mathbb{F}_p^{n+1})^* \otimes (\mathbb{F}_p^{n+1})^*$$

of "cubical" format $(n+1)\times(n+1)\times(n+1)$ over $\mathbb{F}_p$. Let $Det_{n+1,p}()$ denote the polynomial over $\mathbb{F}_p$ obtained by reducing $Det()$ modulo p. In particular,

$$Det_{n+1,p}() \in \mathbb{F}_p[a_{i_0,i_1,i_2}, 0 \leq i_0, i_1, i_2 \leq n]$$

is a non zero polynomial in the coordinate ring of A. As a convention, we will use $Det_{n+1,p}()$ to denote the polynomial and $Det_{n+1,p}(A)$ to denote its evaluation at a tensor A. The computational problem in question is then given a tensor A to compute $Det_{n+1,p}(A) \in \mathbb{F}_p$. Associated with a cubical tensor $A \in (\mathbb{F}_p^{n+1})^* \otimes (\mathbb{F}_p^{n+1})^* \otimes (\mathbb{F}_p^{n+1})^*$ is the trilinear form

$$f_A(x^{(0)}, x^{(1)}, x^{(2)}) := \sum_{0 \leq i_0, i_1, i_2 \leq n} a_{i_0,i_1,i_2} x^{(0)}_{i_0} x^{(1)}_{i_1} x^{(2)}_{i_2}.$$

Triples $(G_0, G_1, G_2) \in (GL_{n+1}(\mathbb{F}_p))^3$ of invertible $(n+1) \times (n+1)$ matrices act on A (or equivalently f_A) in the natural way,

$$(G_0, G_1, G_2) \circ f_A := f_A(G_0 x^{(0)}, G_1 x^{(1)}, G_2 x^{(2)}).$$

Call two tensors A and B as isomorphic if there exists a triple $(G_0, G_1, G_2) \in (GL_{n+1}(\mathbb{F}_p))^3$ such that $f_B = (G_0, G_1, G_2) \circ f_A$. This is indeed an equivalence relation. In particular, it is symmetric since $f_B = (G_0, G_1, G_2) \circ f_A$ if and only if $f_A = (G_0^{-1}, G_1^{-1}, G_2^{-1}) \circ f_B$.

The Tensor Isomorphism Problem. To decide if two cubical tensors over finite fields are isomorphic is the tensor isomorphism problem, which is believed to be hard. Grochow and Qiao built an intricate web of hard problems that reduce to tensor isomorphism, including some longstanding hard problems that lay at the foundation of multivariate cryptography. Complexity theoretically, the tensor isomorphism problem is $NP \cap co-AM$, and believed to be hard on average in theory and practice [9]. The best known run time of $p^{O(n^{11/6})}$ is through Sun's p-group isomorphism algorithm [28] (in conjunction with a reduction in [8]). The promise search version, given two isomorphic A, B to find a $(G_0, G_1, G_2) \in (GL_{n+1}(\mathbb{F}_p))^3$ such that $f_B = (G_0, G_1, G_2) \circ f_A$ is also believed hard. Spurred on by this hardness, several post-quantum digital signature schemes including MEDS [5] and ALTEQ [2, 29] have recently been proposed and submitted to NIST call for post-quantum signatures, all reliant on tensor isomorphism hardness assumptions, or hardness assumptions that reduce to tensor isomorphism.

We focus our attention on MEDS which involves the exact tensor isomorphism stated in our context. The signature scheme is built as follows. First a zero-knowledge interactive protocol is constructed based on the Goldreich-Micali-Wigderson protocol for graph isomorphisms. Except, the graph isomorphism problem is recast with tensor isomorphism problem. Then the interaction in the zero-knowledge protocol is removed using the Fiat-Shamir transformation to yield a signature scheme. We identify the following hardness assumption underlying the soundness and zero-knowledge proofs of the interactive protocol as one that easily relates to hyperdeterminants.

Assumption 5.1. Draw a tensor $A \in (\mathbb{F}_p^{n+1})^* \otimes (\mathbb{F}_p^{n+1})^* \otimes (\mathbb{F}_p^{n+1})^*$ uniformly at random. Draw a triple $(G_0, G_1, G_2) \in (GL_{n+1}(\mathbb{F}_p))^3$ of invertible matrices uniformly at random and set $f_B := (G_0, G_1, G_2) \circ f_A$. The pair (A, B) is computationally indistinguishable from a uniformly random pair of tensors in $\left((\mathbb{F}_p^{n+1})^* \otimes (\mathbb{F}_p^{n+1})^* \otimes (\mathbb{F}_p^{n+1})^*\right)^2$.

An algorithm that distinguishes such an isomorphic pair (A, B) from a uniformly random pair of tensors can be used to either recover the key in a No-Message-Attack or forge the signature in a Chosen-Message-Attack.

Unfortunately, we don't quite know how to use the hyperdeterminant to build a distinguisher for assumption 5.1. The reason being that the hyperdeterminant is only a relative invariant of the $(GL_{n+1}(\mathbb{F}_p))^3$ action. That is, for all $A \in (\mathbb{F}_p^{n+1})^* \otimes (\mathbb{F}_p^{n+1})^* \otimes (\mathbb{F}_p^{n+1})^*$ and for all $(G_0, G_1, G_2) \in (GL_{n+1}(\mathbb{F}_p))^3$,

$$Det_{n+1,p}((G_0, G_1, G_2) \circ f_A) = C(G_0, G_1, G_2) Det_{n+1,p}(f_A),$$

where the "constant" $C(G_0, G_1, G_2)$ depends on the acting matrices. However, if we restrict to $(SL_{n+1}(\mathbb{F}_p))^3$ action, then the hyperdeterminant is an invariant, that is, for all $A \in (\mathbb{F}_p^{n+1})^* \otimes (\mathbb{F}_p^{n+1})^* \otimes (\mathbb{F}_p^{n+1})^*$ and for all $(G_0, G_1, G_2) \in (SL_{n+1}(\mathbb{F}_p))^3$,

$$Det_{n+1,p}((G_0, G_1, G_2) \circ f_A) = Det_{n+1,p}(f_A).$$

We observe that there is a natural hardness reduction from the tensor isomorphism problem restricted to the $(SL_{n+1}(\mathbb{F}_p))^3$ action to the hyperdeterminant. To this end, we next write out the hardness assumption restricted to the $(SL_{n+1}(\mathbb{F}_p))^3$ action, followed by the distinguisher with blackbox access to the hyperdeterminant that reduces the tensor isomorphism problem with the $(SL_{n+1}(\mathbb{F}_p))^3$ action to the hyperdeterminant.

Assumption 5.2. Draw a tensor $A \in (\mathbb{F}_p^{n+1})^* \otimes (\mathbb{F}_p^{n+1})^* \otimes (\mathbb{F}_p^{n+1})^*$ uniformly at random. Draw a triple $(G_0, G_1, G_2) \in (SL_{n+1}(\mathbb{F}_p))^3$ of determinant one matrices uniformly at random and set $f_B := (G_0, G_1, G_2) \circ f_A$. The pair (A, B) is computationally indistinguishable from a uniformly random pair of tensors in $\left((\mathbb{F}_p^{n+1})^* \otimes (\mathbb{F}_p^{n+1})^* \otimes (\mathbb{F}_p^{n+1})^*\right)^2$.

Distinguisher: Given a pair of tensors $(A, B) \in \left((\mathbb{F}_p^{n+1})^* \otimes (\mathbb{F}_p^{n+1})^* \otimes (\mathbb{F}_p^{n+1})^*\right)^2$, decide that the input is a pair of isomorphic tensors if and only if $Det_{n+1,p}(A) = Det_{n+1,p}(B)$.

By invariance, if A and B are isomorphic, then indeed $Det_{n+1,p}(A) = Det_{n+1,p}(B)$, meaning the distinguisher is always correct when presented with two isomorphic tensors.

Therefore, for our distinguisher to succeed, it suffices to prove that for a uniformly random tensor A, $det(A)$ is not concentrated on a particular value in $\mathbb{F}_p$. In the following lemma, for large enough field size p (growing exponentially with n), we prove for uniformly random A that $Det(A)$ is close to uniformly distributed. For such large p, our distinguisher succeeds with probability close to $1 - 1/p$. We take the lemma as strong evidence that there is no arithmetic obstruction to equidistribution, meaning equidistribution should hold for even for small p. The requirement on p being large is merely an artifact our proof methods and our distinguisher should succeed with probability close to $1 - 1/p$ for all p.

Lemma 5.3. *Fix the tensor dimension n and a positive parameter $c > 1$. For every large enough prime $p \geq (n/2)^{\frac{c-1}{c}} 2^{\frac{(c-1)n}{c}\left(1+\frac{3}{2}\log_2 n\right)}$, and for every $u \in \mathbb{F}_p$,*

$$Prob_A\left(Det_{n+1,p}(A) = u\right) \leq \frac{1}{p^{1/c}} + o\left(\frac{1}{p^{\frac{1}{c}}}\right),$$

where the probability is taken over uniform $A \in (\mathbb{F}_p^{n+1})^* \otimes (\mathbb{F}_p^{n+1})^* \otimes (\mathbb{F}_p^{n+1})^*$. For even larger primes p with $p \geq 5(n/2)^{13/3} 2^{\frac{13n}{3}\left(1+\frac{3}{2}\log_2 n\right)}$, for every $u \in \mathbb{F}_p$,

$$Prob_A\left(Det_{n+1,p}(A) = u\right) \leq \frac{1}{p} + o\left(\frac{1}{p}\right),$$

a tighter bound showing that the Hyperdeterminant values are nearly uniformly distributed.

Proof. Since the hyperdeterminant is a primitive polynomial with integer coefficients, reduction by p gives a non zero polynomial $Det_{n+1,p}() \in \mathbb{F}_p[a_{i_0,i_1,i_2}, 0 \leq i_0, i_1, i_2 \leq n]$. By [12, Cor. 2.9], its degree is bounded by

$$\deg(Det_{n+1,p}()) \leq \sum_{0 \leq j \leq k/2} \frac{(j+k_1)!}{j!^3(k-2j)!} 2^{k-2j} \leq \sum_{0 \leq j \leq k/2} n^{3j} 2^{n-2j} \leq \frac{n}{2} 2^{n\left(1+\frac{3}{2}\log n\right)}.$$

Further, $Det_{n+1,p}() - u$ is a non-zero polynomial with the same degree bound. Bounding the number of roots of $Det_{n+1,p}() - u$ by Schwartz-Zippel lemma [23],

$$Prob_A\left(Det_{n+1,p}(A) = u\right) \leq \frac{\deg(Det_{n+1,p}() - u)}{p}.$$

This proves the first bound in the lemma, for every choice of $c > 1$. If one desires a tighter bound towards the uniformity of the hyperdeterminant values, we can resort to the more sophisticated Lang-Weil bound [15]. The fewer the number of components of the variety generated by $Det_{n+1,p}() - u$, the better the Lang-Weil bound. Over the complex numbers, the hyperdeterminant is an absolutely irreducible integer polynomial. By analogy, $Det_{n+1,p}() - u$ is irreducible in $\bar{\mathbb{F}}_p[a_{i_0,i_1,i_2}, 0 \leq i_0, i_1, i_2 \leq n]$. The variety $Det_{n+1,p}() - u$ defines has only one component and the Lang-Weil bound implies

$$Prob_A\left(Det_{n+1,p}(A) = u\right) \leq \frac{1}{p} + O_{\deg(Det_{n+1,p}() - u)}\left(\frac{1}{p}\right).$$

But the asymptotic notation $O_{\deg(Det_{n+1,p}() - u)}()$ in the original Lang-Weil paper hides terms depending on n that are too big. Therefore, we look to the effective version of the Lang-Weil bound, optimized for irreducible hypersurfaces in [25, Thm. 2], which for $p > 5\deg(Det_{n+1,p}() - u)^{13/3}$ implies

$$Prob_A\left(Det_{n+1,p}(A) = u\right) \leq \frac{1}{p} + \frac{(\deg(Det_{n+1,p}() - u) - 1)\,(\deg(Det_{n+1,p}() - u) - 2)}{p^{3/2}} + \frac{5}{p^2}.$$

Therefore, for $p \geq 5(n/2)^{13/3} 2^{\frac{13n}{3}\left(1+\frac{3}{2}\log_2 n\right)} \geq 5\deg(Det_{n+1,p}() - u)^{13/3}$, the second bound claimed in the lemma is true. □

In light of this reduction, to prove tensor isomophism hardness of computing the hyperdeteminant, it suffices to answer the following open question in the affirmative.

Question 5.4. Is the problem of deciding if for two given tensors A and B there exists a triple $(G_0, G_1, G_2) \in (SL_{n+1}(\mathbb{F}_p))^3$ of determinant one matrices such that $f_B = (G_0, G_1, G_2) \circ f_A$ tensor isomorphism hard? In other words, is there a polynomial time reduction from the tensor isomorphism problem with $(GL_{n+1}(\mathbb{F}_p))^3$ action to that with $(SL_{n+1}(\mathbb{F}_p))^3$ action?

We suspect that the answer to the question is yes, but also advise caution. Tensor isomorphism problems with other matrix group actions such as the orthogonal, symplectic or unitary (over complex numbers) are in practice easier than the general linear group actions [4].

Remark 5.5. *For pairs (n, p) such that $p-1$ divides $deg(Det_{n+1,p}())/(n+1)$, our distinguisher for the $(SL_{n+1}(\mathbb{F}_p))^3$ actually also works as a distinguisher for the $(GL_{n+1}(\mathbb{F}_p))^3$ action. Therefore, restricted to the pairs (n, p) satisfying $p-1$ divides $deg(Det_{n+1,p}())/(n+1)$, the hyperdeteminant is at least as hard as the cryptographically hard problem underlying MEDS.*

The reason is that the relative invariance of the hyperdeterminant with respect to the $GL_{n+1}(\mathbb{F}_p)^3$ action takes the following form (c.f. proof of theorem 4.4 in [19]*). For all $A \in (\mathbb{F}_p^{n+1})^* \otimes (\mathbb{F}_p^{n+1})^* \otimes (\mathbb{F}_p^{n+1})^*$ and for all $(G_0, G_1, G_2) \in (GL_{n+1}(\mathbb{F}_p))^3$,*

$$Det_{n+1,p}((G_0, G_1, G_2) \circ f_A) = (Det(G_0)Det(G_1)Det(G_2))^{deg(Det_{n+1,p}())/(n+1)}\, Det_{n+1,p}(f_A).$$

But for p such that $p-1$ divides $deg(Det_{n+1,p}())/(n+1)$,

$$(Det(G_0)Det(G_1)Det(G_2))^{deg(Det_{n+1,p}())/(n+1)} = 1,$$

since raising a non zero element in $\mathbb{F}_p$ to the $p-1$-th power is one. Therefore, for (n, p) such that $p-1$ divides $deg(Det_{n+1,p}())/(n+1)$, the hyperdeterminant is actually an invariant of the $GL_{n+1}(\mathbb{F}_p)^3$ action, not merely a relative invariant.

Let us pause to understand the pairs (n, p) for which the reduction applies. By [12, Cor. 2.9]*, the degree of the cubical hyperdeterminant is*

$$\deg(Det_{n+1,p}()) = \sum_{0\leq j\leq k/2} \frac{(j+k_1)!}{j!^3(k-2j)!} 2^{k-2j} \leq \sum_{0\leq j\leq k/2} n^{3j} 2^{n-2j} \leq \frac{n}{2} 2^{n\left(1+\frac{3}{2}\log n\right)}.$$

Further, $\deg(Det_{n+1,p}())$ *is divisible by* $n+1$*, although it is not apparent from the expression (*[19, Theorem 4.4]*). For a choice of* n*, there are at most finitely many* p *satisfying the condition* $p-1$ *divides* $\deg(Det_{n+1,p}())/(n+1)$*. Some of these primes may be exponential in* n*, which is consistent with the large size of primes chosen in MEDS and ALTEQ. The number of pairs* (n,p) *satisfying the condition should be infinite assuming some widely believed conjectures on the distribution of primes in polynomial values, but is difficult to prove unconditionally.*

Remark 5.6. *Recently, Ran and Samardjiska* [20] *identified a potential weakness in MEDS and ALTEQ signature schemes that rely on the hardness of tensor isomorphism problems. If the public keys chosen turn out to support a certain triple of points they call "triangles", then the isomorphism problem may be easier than the generic case. They further describe Grobner basis based algorithms for detecting and finding triangles. If such triangles exist, their algorithms can strip several bits of security off the schemes. Therefore, careful analysis of the weak key issue they identified is warranted. We observe that in the language of hyperdeterminants these weak keys correspond to singular tensors and the triangles are solutions to the homogeneous multilinear equations in 3.1 modulo* p*. Further, hyperdeterminants play a curious role in analysing this critical weak key security issue. First,* $Det_{n+1,p}()$ *being irreducible over* $\bar{\mathbb{F}}_p$ *means that weak keys arise with probability roughly* $\frac{1}{p}$*. Therefore, increasing* p *to be exponential in the security parameter is an immediate remedy (at the cost of efficiency, needing slightly larger signature lengths etc.). If zero testing the hyperdeterminant (that is, given a tensor* A *deciding if* $Det_{n+1,p}(A)=0$*) turns out to be easy, then it can be used to test and weed out the weak keys. Further, any algorithm for computing the hyperdeterminant* $Det_{n+1,p}()$ *can be turned into one for computing the triangles through our tensor Cramer's rule algorithm in § 3.1.*

References

[1] Walter Baur and Volker Strassen. The complexity of partial derivatives. *Theoretical Computer Science*, 22(3):317–330, 1983. URL: `https://www.sciencedirect.com/science/article/pii/030439758390110X`, `doi:10.1016/0304-3975(83)90110-X`.

[2] M. Bläser, D. H. Duong, A. K. Narayanan, T. Plantard, Y. Qiao, A. Sipasseuth, and G. Tang. The alteq signature scheme: Algorithm specifications and supporting documentation, 2023. URL: `https://pqcalteq.github.io/ALTEQ_spec_2023.09.18.pdf`.

[3] Arthur Cayley. *On the Theory of Elimination*, page 370–374. Cambridge Library Collection - Mathematics. Cambridge University Press, 2009.

[4] Zhili Chen, Joshua A. Grochow, Youming Qiao, Gang Tang, and Chuanqi Zhang. On the Complexity of Isomorphism Problems for Tensors, Groups, and Polynomials III: Actions by Classical Groups. In Venkatesan Guruswami, editor, *15th Innovations in Theoretical Computer Science Conference (ITCS 2024)*, volume 287 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 31:1–31:23, Dagstuhl, Germany, 2024. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. URL: `https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.ITCS.2024.31`, `doi:10.4230/LIPIcs.ITCS.2024.31`.

[5] Tung Chou, Ruben Niederhagen, Edoardo Persichetti, Tovohery Hajatiana Randrianarisoa, Krijn Reijnders, Simona Samardjiska, and Monika Trimoska. Take your meds: Digital signatures from matrix code equivalence. In Nadia El Mrabet, Luca De Feo, and Sylvain Duquesne, editors, *Progress in Cryptology - AFRICACRYPT 2023*, pages 28–52, Cham, 2023. Springer Nature Switzerland.

[6] Valerie Coffman, Joydip Kundu, and William K. Wootters. Distributed entanglement. *Phys. Rev. A*, 61:052306, Apr 2000. URL: https://link.aps.org/doi/10.1103/PhysRevA.61.052306, doi:10.1103/PhysRevA.61.052306.

[7] Carla Dionisi and Giorgio Ottaviani. The binet–cauchy theorem for the hyperdeterminant of boundary format multi-dimensional matrices. *Journal of Algebra*, 259(1):87–94, 2003. URL: https://www.sciencedirect.com/science/article/pii/S0021869302005379, doi:10.1016/S0021-8693(02)00537-9.

[8] J. Grochow and Y. Qiao. On the complexity of isomorphism problems for tensors, groups, and polynomials iv: linear-length reductions and their applications. URL: Onthecomplexityofisomorphismproblemsfortensors,groups,andpolynomialsIV:linear-lengthreductionsandtheirapplications.

[9] Joshua Grochow and Youming Qiao. On the complexity of isomorphism problems for tensors, groups, and polynomials i: Tensor isomorphism-completeness. *SIAM Journal on Computing*, 52(2):568–617, 2023. arXiv:https://doi.org/10.1137/21M1441110, doi:10.1137/21M1441110.

[10] Christopher J. Hillar and Lek-Heng Lim. Most tensor problems are np-hard. *J. ACM*, 60(6), November 2013. doi:10.1145/2512329.

[11] M. Kapranov I. Gelfand and A. Zelevinsky. Hyperdeterminants. *Advances in Mathematics*, 96:226–263, 1992.

[12] M. Kapranov I. Gelfand and A. Zelevinsky. *Discriminants, Resultants, and Multidimensional Determinants*. Modern Birkhäuser Classics, 1994.

[13] Stephen P. Jordan. Fast quantum algorithm for numerical gradient estimation. *Phys. Rev. Lett.*, 95:050501, Jul 2005. URL: https://link.aps.org/doi/10.1103/PhysRevLett.95.050501, doi:10.1103/PhysRevLett.95.050501.

[14] H. Kaji. On the duals of segre varieties. *Geometriae Dedicata*, 99:221–229, 2003.

[15] Serge Lang and André Weil. Number of points of varieties in finite fields. *American Journal of Mathematics*, 76(4):819–827, 1954. URL: http://www.jstor.org/stable/2372655.

[16] Lek-Heng Lim. Singular values and eigenvalues of tensors: a variational approach. In *1st IEEE International Workshop on Computational Advances in Multi-Sensor Adaptive Processing, 2005.*, pages 129–132, 2005. doi:10.1109/CAMAP.2005.1574201.

[17] M. Mahajan and V. Vinay. Determinant: Combinatorics, algorithms, and complexity. *Chicago Journal of Theoretical Computer Science*, 5, 1997.

[18] Akimasa Miyake and Miki Wadati. Multipartite entanglement and hyperdeterminants. *Quantum Info. Comput.*, 2(7):540–555, December 2002.

[19] Giorgio Ottaviani. *Introduction to the Hyperdeterminant and to the Rank of Multidimensional Matrices*, pages 609–638. Springer New York, New York, NY, 2013. doi:10.1007/978-1-4614-5292-8_20.

[20] Lars Ran and Simona Samardjiska. Rare structures in tensor graphs - bermuda triangles for cryptosystems based on the tensor isomorphism problem. Cryptology ePrint Archive, Paper 2024/1396, 2024. URL: https://eprint.iacr.org/2024/1396.

[21] Mohab Safey El Din and Éric Schost. Bit complexity for multi-homogeneous polynomial system solving—application to polynomial minimization. *Journal of Symbolic Computation*, 87:176–206, 2018. URL: https://www.sciencedirect.com/science/article/pii/S0747717117300937, doi:10.1016/j.jsc.2017.08.001.

[22] L. Schläfli. *Über die Resultante eines Systemes mehrerer algebraischer Gleichungen*, pages 9–112. Springer Basel, Basel, 1953. doi:10.1007/978-3-0348-4117-7_1.

[23] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27(4):701–717, October 1980. doi:10.1145/322217.322225.

[24] N. Sendrier and D. E. Simos. How easy is code equivalence over fq? In *International Workshop on Coding and Cryptography - WCC 2013*, 2013.

[25] K. Slavov. Improved lang–weil bounds for a geometrically irreducible hypersurface over a finite field. *Canadian Mathematical Bulletin*, 66(2):654–664, 2023.

[26] P-J. Spaenlehauer. *Solving multi-homogeneous and determinantal systems: algorithms, complexity, applications*. PhD thesis, Universitê Pierre et Marie Curie (Univ. Paris 6), 2012.

[27] Pierre-Jean Spaenlehauer. On the complexity of computing critical points with gröbner bases. *SIAM Journal on Optimization*, 24(3):1382–1401, 2014. `arXiv:https://doi.org/10.1137/130936294`, `doi:10.1137/130936294`.

[28] Xiaorui Sun. Faster isomorphism for p-groups of class 2 and exponent p. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, STOC 2023, page 433–440, New York, NY, USA, 2023. Association for Computing Machinery. `doi:10.1145/3564246.3585250`.

[29] Gang Tang, Dung Hoang Duong, Antoine Joux, Thomas Plantard, Youming Qiao, and Willy Susilo. Practical post-quantum signature schemes from isomorphism problems of trilinear forms. Eurocrypt 2022, 2022. URL: `https://eprint.iacr.org/2022/267`.

[30] Jerzy Weyman and Andrei Zelevinsky. Singularities of hyperdeterminants. *Annales de l'institut Fourier*, 46(3):591–644, 1996. URL: `http://eudml.org/doc/75190`.