Aspects of tensor products over finite fields and Galois geometries

Michel Lavrauw and John Sheekey

December 31, 2012

Abstract

Tensor products play an important role in both mathematics and physics, with applications in e.g. complexity theory, algebraic statistics, tensor networks in quantum information theory, and representation theory. A good recent reference is the book "Tensor products: Geometry and Applications", by J. M. Landsberg [8].

Although there are still many interesting open problems, tensor products are well studied objects. However, most of the research on tensor products (including [8]) only considers tensor products over the complex numbers. Sometimes this is extended to general algebraically closed fields, but few consider the case where the ground field is finite.

In this paper, we will focus on tensor products over finite fields, explain the connections with Galois geometries, and survey what is known, including some recent results concerning rank, decomposition and orbits, from [10, 11, 12].

1 Introduction

Consider the tensor product $\bigotimes_{i\in I} V_i$ ($I = \{1,\ldots,m\}$, $m \geq 2$), where the vector spaces V_i are assumed to have finite dimension n_i over a field $\mathbb{F}$. The V_i are called the *factors* of $\bigotimes_{i=1}^m V_i$, and the *fundamental tensors* (or *pure tensors*) of $\bigotimes_{i=1}^m V_i$ are the tensors that can be written as $v_1 \otimes \ldots \otimes v_m$, $v_i \in V_i$. A general element $\tau \in \bigotimes_{i\in I} V_i$ can be written as a sum of the fundamental tensors

$$\tau = \sum_i v_{1i} \otimes \ldots \otimes v_{mi}.$$

For each tensor $\tau \in \bigotimes_{i=1}^m V_i$, by choosing bases for the factors V_i we obtain a *hypercube* $(a_{i_1 i_2 \ldots i_m})$ associated to τ, where

$$\tau = \sum_{i_1,\ldots,i_m} a_{i_1 i_2 \ldots i_m} e_{1 i_1} \otimes \ldots \otimes e_{m i_m}.$$

Obviously, hypercubes generalize the concept of a matrix (a hypercube with $m = 2$). Also, one verifies that

$$\Psi \ : \ v_1 \otimes v_2 \mapsto [v_1^\vee \mapsto v_1^\vee(v_1) v_2] \tag{1}$$

defines an isomorphism between the vector spaces $V_1 \otimes V_2$ and $\mathrm{Hom}(V_1^\vee, V_2)$. For example, if $\tau = \sum_{ij} a_{ij} e_i \otimes f_j$ then $\tau^\Psi \ : \ v_1^\vee \mapsto \sum_{ij} a_{ij} v_1^\vee(e_i) f_j$, and in particular

$$\tau^\Psi \ : \ e_k^\vee \mapsto \sum_{ij} a_{ij} e_k^\vee(e_i) f_j = \sum_j a_{kj} f_j.$$

Using an analogous isomorphism for tensor products with more than two factors one obtains an isomorphism between the tensor product $\bigotimes_{i=1}^m V_i$ and the vector space of multilinear maps.

As is well established, considering linear transformations can be preferable to matrices. Even more so, the coordinate free approach of tensor products with more than two factors is preferable to hypercubes.

Amongst the numerous applications of the theory of tensor products we mention: computational complexity theory; quantum mechanical systems (entanglement); data analysis; signal processing and source separation; psychometrics. See [8] for more details.

The main problems that turn up from the applications are concerned with the *decomposition*

$$\tau = \sum_{i=1}^k v_{1i} \otimes \ldots \otimes v_{mi} \tag{2}$$

of a tensor $\tau \in \bigotimes_{i=1}^m V_i$. In particular we distinguish the following four essential issues.

(E) Existence: given a tensor τ and an integer k, does there exist an expression of the form (2)?

(U) Uniqueness: given an expression of the form (2) for a tensor τ, is this expression essentially unique?

(A) Algorithm: given a tensor τ and an integer k, does there exist an algorithm that decomposes τ into an expression of the form (2) (in the case where it exists)?

(O) Orbits: can we determine the number of orbits and describe the orbits of the natural group action of $\mathrm{GL}(V_1) \times \ldots \times \mathrm{GL}(V_m)$ on $\bigotimes_{i=1}^m V_i$?

In this paper we will focuss on the issues (E) (Section 2) and (O) (Section 3) with particular focus on the relationship with finite fields and Galois Geometry.

We end the introduction with the geometry and groups relevant for what follows.

The *Segre embedding* is defined by

$$\begin{aligned} \sigma \ : \ \mathrm{PG}(V_1) \times \mathrm{PG}(V_2) \times \ldots \times \mathrm{PG}(V_m) \ &\rightarrow \ \mathrm{PG}(\bigotimes_i V_i) \\ : (\langle v_1 \rangle, \langle v_2 \rangle, \ldots, \langle v_m \rangle) &\mapsto \langle v_1 \otimes v_2 \otimes \ldots \otimes v_m \rangle, \end{aligned} \quad (3)$$

and its image $S_{n_1,n_2,\ldots,n_m}(\mathbb{F}) = Im(\sigma)$ is called the *Segre variety.*

An element $(g_1, g_2, \ldots g_m)$ of $\mathrm{GL}(V_1) \times \mathrm{GL}(V_2) \times \ldots \times \mathrm{GL}(V_m)$ acts on points of the Segre variety as follows:

$$\langle v_1 \otimes v_2 \otimes \ldots \otimes v_m \rangle \mapsto \langle v_1^{g_1} \otimes v_2^{g_2} \otimes \ldots \otimes v_m^{g_m} \rangle.$$

If $V_i = V = V(n, \mathbb{F})$ for all i, then we also have an action of S_m:

$$\pi : \langle v_1 \otimes v_2 \otimes \ldots \otimes v_m \rangle \mapsto \langle v_{\pi(1)} \otimes v_{\pi(2)} \otimes \ldots \otimes v_{\pi(m)} \rangle.$$

Together the wreath product $\mathrm{GL}(V) \wr S_m$ induces a subgroup G_m of $\mathrm{PGL}(n^m, \mathbb{F})$. Clearly G_m stabilizes $X := S_{n,\ldots,n}$ and the set of maximal subspaces of X, for example $\sigma(PG(V_1) \times \langle v_2 \rangle \times \ldots \times \langle v_m \rangle)$.

2 Existence

2.1 The rank of a tensor

As before, we consider a tensor product $\bigotimes_{i=1}^m V_i$, where all factors are finite dimensional over some field $\mathbb{F}$. The "Existence" problem mentions above

(E), naturally gives rise to the notion of "rank" of a tensor: the *rank* of a tensor $\tau \in \bigotimes_{i=1}^{m} V_i$ (notation $\mathrm{rk}(\tau)$) is the minimum natural number k such that an expression of the form (2) exists. This notion was introduced by F. L. Hitchcock in 1927 [5]. It is not difficult to see that the rank of a tensor in a two-fold tensor product is equal to the rank of any matrix associated to the tensor. However, while determining the rank of a matrix (naively) takes about $n \cdot n^3$ multiplications, in general computing the rank of a tensor in an m-fold tensor product with $m \geq 3$ is very difficult, and no algorithms are available.

A very interesting problem which is equivalent to a rank problem is the computational complexity of matrix multiplication. If $M_{n,n,n} \in \mathrm{Bil}(\mathbb{F}^{n^2} \times \mathbb{F}^{n^2}, \mathbb{F}^{n^2})$ denotes the bilinear form associated to the multiplication of $n \times n$-matrices, then to $M_{n,n,n}$ corresponds a tensor in the three fold tensor product $(\mathbb{F}^{n^2})^\vee \otimes (\mathbb{F}^{n^2})^\vee \otimes \mathbb{F}^{n^2}$, as the image under the isomorphism between $\mathrm{Bil}(A \times B, C)$ and $A^\vee \otimes B^\vee \otimes C$ defined by

$$\alpha \otimes \beta \otimes c \;\mapsto\; [(\alpha, \beta) \mapsto \alpha(a)\beta(b)c]. \tag{4}$$

If we denote the rank of this tensor by $R(M_{n,n,n})$, then from the above isomorphism it follows that $R(M_{n,n,n})$ measures the number of multiplications in the underlying field that are required to perform the multiplication. This is a central open problem in complexity theory. It's intriguing nature is illustrated by the following. While the usual multiplication of 2×2 matrices takes 8 multiplications, Strassen [14] showed that $R(M_{2,2,2}) \leq 7$, and Winograd [15] proved that $R(M_{2,2,2}) = 7$. We note that the algorithm that Strassen provided can also be applied to larger matrices, by dividing the matrices into blocks of 2×2-matrices. For more on complexity theory and matrix multiplication we refer to [2] and [8, Chapter 11].

2.2 The rank of a subspace and contractions

Generalizing the rank of a tensor, we can define the rank of a subspace as follows. If U is subspace of $\bigotimes_{i=1}^{m} V_i$, then the *rank* of U is the minimum number of fundamental tensors needed to span a subspace containing U. An important proposition concerning the rank of a subspace requires the following definition. For every $u_i^\vee \in V_i^\vee$, we define the *contraction* $u_i^\vee(\tau)$ of $\tau = v_1 \otimes v_2 \otimes \ldots \otimes v_m$ by

$$u_i^\vee(\tau) = u_i^\vee(v_i)\ v_1 \otimes \ldots \otimes v_{i-1} \otimes v_{i+1} \otimes \ldots \otimes v_m. \tag{5}$$

Extending this definition linearly, we obtain the notion of a contraction

$$u_i^\vee \ : \ \bigotimes_{i=1}^{m} V_i \ \to \ V_1 \otimes \ldots V_{i-1} \otimes V_{i+1} \otimes V_m. \tag{6}$$

The following proposition is often useful in determining the rank.

Proposition 2.1 *If $\tau \in \bigotimes_{i=1}^m V_i$, then for each $j \in \{1, \ldots, m\}$, we have* $\mathrm{rk}(\tau) = \mathrm{rk}(T_j)$, *where* $T_j := \langle u_j^\vee(\tau) \ : \ u_j^\vee \in V_j^\vee \rangle$.

Proof: First suppose $\mathrm{rk}(\tau) = r$, with $\tau = \sum_{i=1}^r v_{1i} \otimes \ldots \otimes v_{mi}$. Then for any $u_j^\vee \in V_j^\vee$,

$$u_j^\vee(\tau) = \sum_i u_j^\vee(v_{ji}) v_{1i} \otimes \ldots \otimes v_{j-1,i} \otimes v_{j+1,i} \otimes \ldots \otimes v_{mi},$$

which is contained in

$$\langle v_{1i} \otimes \ldots \otimes v_{j-1,i} \otimes v_{j+1,i} \otimes \ldots \otimes v_{mi} \ : \ i = 1, \ldots, r \rangle,$$

and so $\mathrm{rk}(T_j) \leq \mathrm{rk}(\tau)$.

Conversely, suppose $\mathrm{rk}(T_j) = s$ and $T_j \leq \langle v_{1i} \otimes \ldots \otimes v_{j-1,i} \otimes v_{j+1,i} \otimes \ldots \otimes v_{mi} \ : \ i = 1, \ldots, s \rangle$. Let $\{e_1, \ldots, e_{n_j}\}$ be a basis for V_j and $\{e_1^\vee, \ldots, e_{n_j}^\vee\}$ its dual basis. Then there exists scalars α_{ik} such that

$$e_k^\vee(\tau) = \sum_{i=1}^{s} \alpha_{ik} v_{1i} \otimes \ldots \otimes v_{j-1,i} \otimes v_{j+1,i} \otimes \ldots \otimes v_{mi}.$$

Let $v_{ji} = \sum \alpha_{ik} e_k$. Then

$$\tau = \sum_{i=1}^{s} v_{1i} \otimes \ldots \otimes v_{mi}$$

and $\mathrm{rk}(\tau) \leq s = \mathrm{rk}(T_j)$, and hence $\mathrm{rk}(\tau) = \mathrm{rk}(T_j)$, as claimed. □

2.3 The rank in $\mathbb{F}^n \otimes \mathbb{F}^n \otimes \mathbb{F}^n$

Here we focus on the maximum rank of a tensor in a three-fold tensor product ($m = 3$), being the first nontrivial case, since $m = 1$ is trivial and $m = 2$ corresponds to the rank of linear maps. The rank depends on the dimensions of the factors and on the ground field. We will focus on the case where all factors have the same dimension, i.e. $n_1 = n_2 = n_3 =: n$. If follows from the Proposition above that n^2 is a trivial upper bound. Atkinson and Stephens showed the following.

Theorem 2.2 (Atkinson-Stephens [1]) *If* $\tau \in \mathbb{C}^n \otimes \mathbb{C}^n \otimes \mathbb{C}^n$ *then* $\mathrm{rk}(\tau) \leq \frac{1}{2}n^2 + O(n)$.

As far as we know, this is still the best result of its kind. The proof uses the fact that $\mathbb{C}$ is algebraically closed and separable. For general fields one easily verifies that the rank of a tensor in $\mathbb{F}^2 \otimes \mathbb{F}^2 \otimes \mathbb{F}^2$ is at most 3, since each line of $\mathrm{PG}(3, \mathbb{F})$ lies in a plane spanned by three points of $S_{2,2}(\mathbb{F})$. To our knowledge, the best result for general fields is the following.

Theorem 2.3 ([7]) *If* $\tau \in \mathbb{F}^n \otimes \mathbb{F}^n \otimes \mathbb{F}^n$ *then* $\mathrm{rk}(\tau) \leq \frac{3n}{2}\lceil \frac{n}{2} \rceil$. *If* $|\mathbb{F}|$ *is large enough, then* $\mathrm{rk}(\tau) \leq \frac{3n^2}{4}$.

For $n = 3$ we have the following recent result, and we give a sketch of the proof.

Theorem 2.4 (ML - A. Pavan - C. Zanella [11]) *The rank of a* $3 \times 3 \times 3$ *tensor is at most six over any field.*

The proof basically proceeds as follows. We need to prove that each point of $\langle S_{3,3,3}(\mathbb{F}) \rangle$ is contained in a subspace spanned by six points of $S_{3,3,3}(\mathbb{F})$. Contracting $\tau \in U \otimes V \otimes W$ in the first factor we obtain $N = \langle u_i^\vee(\tau) \ : \ i = 1, 2, 3 \rangle \subset \mathrm{PG}(V \otimes W)$. Since N is contained in a plane of $\langle S_{3,3}(\mathbb{F}) \rangle$ it follows that $N = \langle \alpha, L \rangle$, where $\alpha \in V \otimes W$, for some line L. Next we choose bases v_1, v_2, v_3 and w_1, w_2, w_3 s.t.

$$\alpha \in \langle v_1 \otimes w_1, v_2 \otimes w_2, v_3 \otimes w_3 \rangle =: D,$$

and finally we show that L is contained in the span of D and at most three other points of $S_{3,3}(\mathbb{F})$, completing the proof.

Similarly to the tensor associated to matrix multiplication, one can associate a tensor to any algebra, in particular to a field. It was shown by Winograd in 1979 and de Groote in 1983, that the rank of the tensor associated to a finite field of order q^n considered as an $\mathbb{F}_q$-algebra is at least $2n-1$, with equality if and only if $q \geq 2n - 2$. Hence for $n = 3$, the rank of $\mathbb{F}_{2^3}$ and $\mathbb{F}_{3^3}$ is six, which shows that the above bound in the theorem from [11] cannot be improved in general.

3 Orbits

In this section we study the orbit structure of $\bigotimes_{i=1}^m V_i$. In the projective setting, the aim is to determine the orbits on the points of $\mathrm{PG}(\bigotimes_{i=1}^m V_i)$ under the action of G_m. Since the rank is invariant, the number of orbits is at least the maximum rank in $\bigotimes_{i=1}^m V_i$. In this section we will deal with the orbits in $\mathbb{F}^2 \otimes \mathbb{F}^2 \otimes \mathbb{F}^2$, and determine the orbits in a geometric way, in relation to the Segre variety product of three projective lines (from [10]). We will need the notion of nonsingular tensor, which we introduce below.

3.1 Nonsingular tensors, semifields and projective planes

A tensor τ (or a point $\langle \tau \rangle$) is called *nonsingular* if applying any $m-1$ consecutive nonzero contractions to τ never returns the zero vector. Otherwise the tensor (or point) is called *singular*. Clearly also singularity of a tensor (or point) is an invariant. The nonsingular tensors correspond to non-associative division algebras, called semifields, and hence to semifield planes. These are translation planes (i.e. projective planes with a special line and associated translation group, see e.g. [6]) which are also dual translation planes. For more on semifields, we refer to the chapter [9] and the references therein. Following Liebler [13], in [12] a tensor $T_{\mathbb{S}}$ is associated to each presemifield $\mathbb{S}$, and the following theorem is proved.

Theorem 3.1 (from [12]) (i) *The tensor $T_{\mathbb{S}}$ is nonsingular.*
(ii) *To every nonsingular tensor $T \in V_1 \otimes V_2 \otimes V_3$ there corresponds a presemifield $\mathbb{S}$ for which $T = T_{\mathbb{S}}$.*
(iii) *The map $\mathbb{S} \mapsto T_{\mathbb{S}}$ is injective.*

Also, the Knuth orbit of a semifield $\mathbb{S}$ is represented in the projective space $\mathrm{PG}(n^3-1, q)$ as the orbit of $P_{\mathbb{S}}$ under the group G_m (where $P_{\mathbb{S}} = \langle T_{\mathbb{S}} \rangle$ and $\mathbb{S}$ is an n-dimensional algebra over $\mathbb{F}_q$) (see [12]). In our study of the orbits of points in $\mathrm{PG}(\mathbb{F}^2 \otimes \mathbb{F}^2 \otimes \mathbb{F}^2)$, we will use the following characterisation of singular points.

Theorem 3.2 ([12]) *A tensor $\tau \in \mathbb{F}^n \otimes \mathbb{F}^n \otimes \mathbb{F}^n$ is singular if and only if*

$$\langle \tau \rangle \subset \langle x_1, \ldots, x_j, S_{k_1,k_2,k_3}(\mathbb{F}) \rangle$$

for some $j < n$ points and a $S_{k_1,k_2,k_3}(\mathbb{F})$ properly contained in $S_{n,n,n}(\mathbb{F})$.

3.2 The orbits in $\mathbb{F}^2 \otimes \mathbb{F}^2 \otimes \mathbb{F}^2$

The orbits in $\mathbb{F}^2 \otimes \mathbb{F}^2 \otimes \mathbb{F}^2$ were obtained computationally for $\mathbb{F}_2$ by Glynn et al. in [3], and Havlicek et al. proved this geometrically for $\mathbb{F}_2$ in [4]. In [10] we proved the following.

Theorem 3.3 ([10]) *There exist precisely four G_3-orbits of singular tensors in $\mathbb{F}^2 \otimes \mathbb{F}^2 \otimes \mathbb{F}^2$.*

We give some indications towards the proof, and refer to [10] for more details. Put $X = S_{2,2,2}$. It is well known that every point $y = \langle y_1 \otimes y_2 \otimes y_3 \rangle$ lies on precisely three lines of the Segre variety X, and we denote these lines by l_1, l_2, l_3, where for example $l_3(y) := \sigma(\langle y_1 \rangle \times \langle y_2 \rangle \times \mathrm{PG}(V))$. Each pair of lines lie on a sub-Segre variety which is a hyperbolic quadric, which we call $Q_1(y)$, $Q_2(y)$, and $Q_3(y)$, for example $Q_1(y) := \sigma(\langle y_1 \rangle \times \mathrm{PG}(V) \times \mathrm{PG}(V))$. Each quadric spans a 3-space $\mathcal{L}_i(y) := \langle Q_i(y) \rangle$. The *shamrock* of a point y, denoted by $Sh(y)$, is the union of the three 3-spaces $\mathcal{L}_i(y)$, and we call $\mathcal{L}_i(y)$ a *leaf* of the shamrock.

Clearly G_3 sends a shamrock to a shamrock, a leaf to a leaf etc. The enumeration of the orbits goes by the rank of the points. We know from before that the maximum rank in $\mathbb{F}^2 \otimes \mathbb{F}^2 \otimes \mathbb{F}^2$ is three. Also, the rank one points (i.e. the points of X) form an orbit $\mathcal{O}_1$. Any rank 2 point is contained in a line spanned by two points of X, say $\langle y, z \rangle$. Next one needs to show the following.

Lemma 3.4 ([10]) *There exist precisely two orbits of rank two tensors.*

Denote these by $\mathcal{O}_2$ and $\mathcal{O}_3$. Next we consider points of rank three, and therefore planes $\pi = \langle y, z, w \rangle$, $y, z, w \in X$. We can assume π contains no lines of X, and that π is not contained in any leaf (as then everything on π would have rank at most two). We will consider the shamrock of the point $u = \langle y_1 \otimes z_2 \otimes w_3 \rangle$. Then $y \in \mathcal{L}_1(u)$, etc. We define the *type* of π to be (a_1, a_2, a_3), where $a_i = |\{\langle y_i \rangle, \langle z_i \rangle, \langle w_i \rangle\}|$. We need to consider the following four possibilities for the type: $(3,3,3), (2,3,3), (2,2,3)$, and $(2,2,2)$.

The geometric characterization from before implies that every singular point is contained in the span of a point and a quadric $\langle x, Q_i(y) \rangle$, and hence we have the following.

Corollary 3.5 ([10]) *A tensor of rank three is singular if and only if it lies on a plane of type (a_1, a_2, a_3), with some $a_i = 2$.*

Hence, since we are dealing with singular points, we can exclude the case $(3, 3, 3)$. Every point on a $(2, 2, 3)$-plane has rank at most 2, since it can be shown to be contained in a space spanned by two disjoint lines of X.

It can also be shown that every point on a $(2, 3, 3)$-plane has rank at most 2 or lies on a plane of type $(2, 2, 2)$. Finally it is shown that the rank three points on $(2, 2, 2)$-planes form a single orbit $\mathcal{O}_4$. This is summarized in the following theorem.

Theorem 3.6 ([10]) *For $n = 2$, there exist precisely four G_3-orbits of singular tensors over any field.*

As orbits of nonsingular tensors in $\mathbb{F}^2 \otimes \mathbb{F}^2 \otimes \mathbb{F}^2$ correspond to Knuth orbits of two-dimensional semifields one obtains the following corollary.

Corollary 3.7 ([10]) *For $n = 2$, the number of orbits of tensors is*

- *five if F is finite;*
- *five if $F = \mathbb{R}$;*
- *four if F is algebraically closed;*
- *infinite if $F = \mathbb{Q}$.*

Conclusion 3.8 *There are various applications of tensor products over the complex numbers. Similarly, tensor products over finite fields promise many interesting applications. There remain many fundamental open problems. We have shown in this article that progress can be made over finite fields using a geometric approach.*

References

[1] M. D. Atkinson and N.M. Stephens. On the maximal multiplicative complexity of a family of bilinear forms, Linear Algebra Appl. 27 (1979), 1-8.

[2] Burgisser, P.; Clausen, M. and Shokrollahi, M. Algebraic Complexity Theory. Springer-Verlag 1997.

[3] D.G. Glynn, T.A. Gulliver, J.G. Maks and K. Gupta. The geometry of additive quantum codes. Available online from `www.maths.adelaide.edu.au/rey.casse/DavidGlynn/QMonoDraft.pdf`.

[4] H. Havlicek, B. Odehnal, M. Saniga. On invariant notions of Segre varieties in binary projective spaces. Des. Codes Cryptogr. 62: 343–356, 2012.

[5] F. L. Hitchcock (1927). The expression of a tensor or a polyadic as a sum of products. Journal of Mathematics and Physics 6: 164-189.

[6] D. R. Hughes and F. C. Piper. Projective planes. Springer-Verlag, New York, 1973. Graduate Texts in Mathematics, Vol. 6.

[7] J. Ja'Ja'. Optimal evaluation of pairs of bilinear forms, SIAM J. Comput. 8 (1979), 443-462.

[8] J . M. Landsberg. Tensors: Geometry and Applications. 2012. Graduate Studies in Mathematics, 128. American Mathematical Society, Providence, RI, 2012. xx+439 pp. ISBN: 978-0-8218-6907-9.

[9] M. Lavrauw and O. Polverino. Finite Semifields. Chapter in Current research topics in Galois geometries. Nova Academic Publishers (J. De Beule and L. Storme, Eds.).

[10] M. Lavrauw and J. Sheekey. Orbits of the stabiliser group of the Segre variety product of three projective lines. Preprint.

[11] M. Lavrauw, A. Pavan and C. Zanella. On the rank of $3 \times 3 \times 3$-tensors. To appear in *Linear Multilinear Algebra.*

[12] M. Lavrauw. Finite semifields and nonsingular tensors. *Des. Codes Cryptogr.* (2012). Available online: `<http://dx.doi.org/10.1007/s10623-012-9710-6>`

[13] R. Liebler. On nonsingular tensors and related projective planes, Geom. Dedic. 11 (1981), 455-464,

[14] V. Strassen. Gaussian Elimination is not Optimal, Numer. Math. 13, p. 354-356, 1969.

[15] S. Winograd. On multiplication in algebraic extension felds, Theoret. Comput. Sci. 8 (1979), 359-377.