Maximal Bilinear Complexity and Codes*

Joachim von zur Gathen
Department of Computer Science
University of Toronto
Toronto, Ontario M5S 1A4, Canada

Submitted by Richard A. Brualdi

ABSTRACT

The connection between bilinear complexity and error-correcting codes, discovered by Brockett and Dobkin in 1973, yields lower bounds on the maximal ranks of tensors with a given shape. The resulting bounds are linear, and thus interesting only for "unbalanced" shapes like $(n, n, 2)$ and $(n, n, n^2 - k)$ with $k \leqslant n$. As an example, for odd n the maximal rank of $(n, n, 2)$-tensors is larger over $\mathbb{Z}_2$ than over an algebraic closure of $\mathbb{Z}_2$.

1. INTRODUCTION

One of the central topics in algebraic complexity theory is the bilinear complexity (or rank) of sets of bilinear forms; Strassen (1973) initiated a systematic study, Strassen (1984), Heintz (1985), and von zur Gathen (1988) give surveys, and de Groote (1987) gives a detailed introduction into this subject. We refer to de Groote for notation and terminology. The area has some definite answers (e.g., multiplication of polynomials, or in finite algebraic extension fields) and major open problems (such as matrix multiplication).

Within this theory, an interesting problem is the determination of the maximal bilinear complexity of p bilinear forms in m and n variables (for

*This work was supported by National Science and Engineering Council of Canada, grant A2514.

655 Avenue of the Americas, New York, NY 10010 0024-3795/91/$3.50

fixed m, n, p), or, in other words, of the maximal rank $R_F(m,n,p)$ of tensors in $F^m \otimes F^n \otimes F^p$, where F is a field. Howell (1978) gives upper and lower bounds on $R_F(m,n,p)$ for both finite and infinite fields F. As a general upper bound, Atkinson and Stephens (1979) prove $R_F(m,n,p) \leqslant m + \lceil p/2 \rceil n$ if $m \leqslant n$ and F is algebraically closed.

In 1973, Brockett and Dobkin (1978) showed how to obtain good linear error-correcting codes from good bilinear computations; see also Lempel and Winograd (1977). Standard bounds from coding theory then lead over $F = \mathbb{Z}_2$ to lower bounds for matrix multiplication (Bshouty 1987), higher than the best known lower bound over an infinite field, and for polynomial multiplication (Brown and Dobkin 1980, Kaminski and Bshouty 1987), higher than the corresponding upper bound over an infinite field.

We work out some lower bounds on $R_F(m,n,p)$ provided by this connection. They are only linear, while the true order is quadratic when m, n, p are of not too different size. Thus we obtain (very modest) improvements only for very unbalanced shapes like $(n,n,2)$ or (n,n,n^2-k) with $k \leqslant n$. It is a well-known phenomenon that the rank of individual tensors may decrease when computations over larger fields are allowed. We show that a similar decrease may occur for maximal tensor rank, namely for the shape $(n,n,2)$ with n odd. The rank of such tensors is completely understood over algebraically closed fields, in terms of their Weierstrass-Kronecker canonical form (Grigoryev 1978, Ja'ja' 1979), and our lower bound over finite fields matches Ja'ja's (1980) upper bound. The result also shows that the maximal rank over $\mathbb{Z}$ may be larger than over $\mathbb{C}$.

For perspective, we mention the important notion of the *border rank* of a tensor t, which is at most r if t can be approximated arbitrarily well by tensors of rank r (Bini et al. 1979, Alder 1983). Thus for the maximal border rank $\underline{R}$ we have

$$\underline{R}_F(m,n,p) \leqslant R_F(m,n,p).$$

$\underline{R}$ is much better behaved than R. For example, if F is algebraically closed, then both the rank and the border rank are equal to $\underline{R}_F(m,n,p)$ for all tensors in some dense set of tensors (open in the Zariski topology). However, there may be exceptional tensors with larger rank. As an example,

$$\underline{R}_F(n,n,2) = n < \lfloor 3n/2 \rfloor = R_F(n,n,2)$$

(Grigoryev 1978, Ja'ja' 1979), and we show $R_{\mathbb{Z}_2}(n,n,2) = \lceil 3n/2 \rceil$.

Over an algebraically closed field, Strassen (1983) shows with methods from algebraic geometry that $\underline{R}_F(m,n,p)$ is $mnp/(m+n+p-2)$ asymptotically, for "balanced" shapes (m,n,p) in quite a generous sense. Howell (1978) proved this number to be a lower bound on $R_F(m,n,p)$ for infinite F, and a slightly smaller bound $mnp/[m+n+p-2\log_q(q-1)]$ for a finite field $F=\mathbb{F}_q$ with q elements; in Sections 4 and 5, we compare our results with Howell's. Our bounds are "constructive" in that we exhibit specific tensors requiring the stated number of bilinear multiplications. They also apply to bilinear computations for tensors over $\mathbb{Z}$ using only integer coefficients.

Apart from the Griesmer bound, we use no fact from algebraic coding theory, but rather mimic its notions in settings of no relevance to the error-correction problem. Thus we consider "codes" over infinite fields, for which the question of asymptotic bounds—central in combinatorial coding theory—turns out to be trivial. We also use affine linear "codes," where each codeword has large Hamming weight, but the distance between codewords may be 1.

2. BOUNDS ON CODES

Let F be an arbitrary field. For a vector $u \in F^r$, the *Hamming weight* $w(u)$ is the number of nonzero entries in u. An *affine* $[r,s,d]$-code over F is an affine linear s-dimensional subspace $C \subseteq F^r$ such that $w(u) \geqslant d$ for each nonzero $u \in C$. We say that C has weight at least d. When F is finite and C is linear, i.e., $0 \in C$, we have the standard notion of *linear codes*. These are sufficient for our bounds on $R_F(m,n,p)$ with p small (allowing also infinite F). For p large, say $p=mn-m$, we use affine codes with large weight but small distance $w(u-v)$ between distinct codewords $u,v \in C$; in fact, this distance is only 1 in the application. Such "codes" are useless for the purpose of coding theory, namely detecting and correcting transmission errors. If C is an affine $[r,s,d]$-code and $u \in C$, then the translate $C-u$ is a linear $[r,s,d']$-code. However, this d' is only the minimum distance between distinct codewords of C. If C is linear, the minimum distance equals the minimum weight.

If $F=\mathbb{F}_q$ is a finite field with q elements and $s \in \mathbb{N}$, let

$$\eta(q,s)=\frac{q^s-1}{q^{s-1}(q-1)}, \qquad \eta(q)=\frac{q}{q-1}.$$

Then

$$\eta(q,s) < \eta(q,s+1) < \eta(q) = \lim_{s\to\infty} \eta(q,s).$$

Van Lint (1981, Theorem 5.2.6) gives the following bound.

FACT 1 (Griesmer bound). *For any linear $[r,s,d]$-code over $\mathbb{F}_q$, we have*

$$r \geqslant \sum_{0\leqslant i<s} \left\lceil \frac{d}{q^i} \right\rceil \geqslant \eta(q,s)\cdot d.$$

For any field F and $r,d \in \mathbb{N}$, let

$$\sigma_F(r,d) = \max\{s : \text{a linear } [r,s,d]\text{-code exists over } F\}.$$

When F is finite and one allows also nonlinear codes C in this definition (replacing s by $\#C$), the study of the resulting numbers $A_F(r,d)$ "is considered to be the central problem in combinatorial coding theory" (van Lint 1981, §5). For our purposes it is more convenient to look at the problem from a different perspective, and we define for $s,d \in \mathbb{N}$

$$\rho_F(s,d) = \min\{r : \text{a linear } [r,s,d]\text{-code exists over } F\}.$$

Then

$$\sigma_F(\rho_F(s,d),d) \geqslant s, \tag{2.1}$$

$$\rho_F(\sigma_F(r,d),d) \leqslant r. \tag{2.2}$$

In fact, the usual operations on codes (van Lint 1981, §4.4) show that equality holds.

We make a similar definition for affine codes:

$$\tau_F(s,d) = \min\{r : \text{an affine } [r,s,d]\text{-code, not containing 0, exists over } F\}.$$

Both ρ and τ are weakly monotone in either argument.

In the following theorem, the bound (i) on ρ is known as the *Singleton bound* over finite fields, and (ii) shows that this bound is sharp for large fields (and fixed s,d). This is, of course, not the perspective of coding theory,

where one usually considers a fixed finite field and growing s and d. One interpretation of (ii) is that coding theory over infinite fields is uninteresting.

THEOREM 2. *Let F be a field, and $s, d \geqslant 1$. Then*

(i) $\rho_F(s,d) \geqslant s+d-1$;
(ii) *if*

$$\#F > \binom{s+d-2}{s-1},$$

then $\rho_F(s,d) = s+d-1$;
(iii) $\tau_F(s,d) = s+d$.

Proof. For the lower bounds in (i) and (iii), it is sufficient to consider an affine $[r,s,d]$-code C over F of minimum weight exactly d. Let $a = (a_1,\ldots,a_r) \in C$ with $w(a) = d$, renumber the coordinates so that $a = (a_1,\ldots,a_d,0,\ldots,0)$, and let

$$L = \{(b_1,\ldots,b_r) \in F^r : b_{d+1} = \cdots = b_r = 0\}.$$

Then the "$r-d$ times punctured code" $C' = C \cap L$ has dimension $s' \geqslant s-(r-d)$. If $C' = \{a\}$, then $0 = s' \geqslant s-r+d$ and $r \geqslant s+d$. Now assume $C' \neq \{a\}$. We claim that $C' = Fa$ is a line. Then $0 \in C' \subseteq C$, C is linear, and $1 = s' \geqslant s-r+d$; thus the lower bounds in (i) and (iii) will follow. So let $b \in C'$, $b \neq a$. Then $a + \lambda(b-a) \in C'$ for all $\lambda \in F$. For the claim, it is sufficient to show that b is a scalar multiple of a. We may assume that $a_d \neq b_d$, after possibly reordering the coordinates. Set $\lambda = a_d/(a_d - b_d) \in F$. Then $a + \lambda(b-a) \in C$ has coordinates $d, d+1, \ldots, r$ equal to zero, so that $a + \lambda(b-a) = 0$, and thus $b = (b_d/a_d)a \in Fa$. This proves the claim.

(ii): Set $r = s+d-1$, $R = \{1,\ldots,r\}$, consider a set $X = \{x_{ij} : 1 \leqslant i \leqslant s, 1 \leqslant j \leqslant r\}$ of indeterminates over F, and for any subset

$$S = \{i_1,\ldots,i_s\} \in \binom{R}{s} = R_s$$

of R with s elements, let

$$f_S = \det \begin{pmatrix} x_{1i_1} & \cdots & x_{1i_s} \\ \vdots & & \vdots \\ x_{si_1} & \cdots & x_{si_s} \end{pmatrix} \in F[X].$$

Then f_S is a nonzero polynomial of degree 1 in each variable occurring in f_S. Let

$$f = \prod_{S \in R_s} f_S.$$

Each x_{ij} occurs in

$$m = \binom{r-1}{s-1}$$

polynomials f_S. Thus f is nonzero of degree m in each variable.

Let $a \in F^{s \times r}$ with $f(a) \neq 0$, and $C \subseteq F^r$ be the linear code generated by the rows $a_1, \ldots, a_s$ of a. If $\#F > m$, then such an a exists (Schwartz 1980). If $\lambda_1, \ldots, \lambda_s \in F$ are such that $\Sigma_i \lambda_i a_i$ has less than d nonzero coordinates, then it has at least s coordinates equal to zero. Then $f(a) \neq 0$ implies that $\lambda_1 = \cdots = \lambda_s = 0$. Thus C is a linear $[r, s, d]$-code.

(iii): For the upper bound, we take $e = (1, \ldots, 1) \in F^d$ and $C = \{e\} \times F^s$. ■

We note that with the method of (ii) one can also find affine $[s + d, s, d]$-codes which are not of the form $\{e\} \times F^s$ for some $e \in F^d$, if

$$\#F > \binom{s+d}{s}.$$

The proof of (ii) is nonconstructive, but indicates how to produce concrete examples. Trivially, entries of a which are algebraically independent over the prime field F_0 of F are sufficient. If $r = s + d - 1$, $p_1, \ldots, p_s \geqslant r$ are pairwise distinct prime numbers, $\alpha_i \in F$ for $1 \leqslant i \leqslant s$ algebraic of degree p_i over F_0, and $a_i = (1, \alpha_i, \alpha_i^2, \ldots, \alpha_i^{r-1}) \in F^r$, then $a_1, \ldots, a_s$ generate a linear $[r, s, d]$-code. If $F = \mathbb{Q}$, one can also use sufficiently fast-growing sequences of integers.

3. BILINEAR COMPLEXITY AND CODES

Let F be an arbitrary field, $A_0, A_1, \ldots, A_t \in F^{m \times n}$,

$$L = A_0 + \sum_{1 \leqslant i \leqslant t} FA_i$$

the affine linear space generated by $A_0, A_0 + A_1, \ldots, A_0 + A_t$, $s = \dim L$,

$$d = \min\{\operatorname{rank} B : B \in L,\ B \neq 0\},$$

and r the bilinear complexity of $(A_0, \ldots, A_t)$. (A definition of r will be given in the proof below.) Brockett and Dobkin (1978) discovered in 1973 the following connection with codes; see also Lempel and Winograd (1977). This connection was stated in the standard framework of coding theory, where $A_0 = 0$ and F is finite.

THEOREM 3. *In the above notation, there exists an affine* $[r, s, d]$*-code over* F. *Furthermore, if* $0 \notin L$, *then there exists such a code not containing* 0.

Proof. Using a linear transformation, we may assume that $A_0 = 0$ if L is linear. Furthermore, we may assume $s = t$, since removing linearly dependent matrices changes neither L nor r. By definition of bilinear complexity, there exist $a_1, \ldots, a_r \in F^m$, $b_1, \ldots, b_r \in F^n$, and $U \in F^{(s+1)\times r}$ such that

$$(A_0, A_1, \ldots, A_s)^T = Uv^T,$$

where

$$v = (v_1, \ldots, v_r) = (a_1 \otimes b_1, \ldots, a_r \otimes b_r) \in (F^{m\times n})^r$$

is a vector of matrices of rank 1. In other words, the vector $(A_0, A_1, \ldots, A_s)^T$ of matrices is the product of the matrix U and the vector $(a_1 \otimes b_1, \ldots, a_r \otimes b_r)$ of matrices, each of rank 1. Or, equivalently, each matrix A_i is a linear combination of these matrices of rank 1. The bilinear complexity of $(A_0, A_1, \ldots, A_s)$ is the minimal r for which such data exist.

Let $u_0, \ldots, u_s \in F^r$ be the rows of U, with $u_0 = 0$ if $A_0 = 0$, and $U' = (u_1, \ldots, u_s)^T \in F^{s\times r}$. We consider the affine linear code $C = u_0 + \Sigma_{1\leqslant i\leqslant s} Fu_i \subseteq F^r$. C is linear if $A_0 = 0$. Since

$$L' = \sum_{1\leqslant i\leqslant s} FA_i = U'\Big(\sum_{1\leqslant j\leqslant r} Fv_i\Big),$$

we have $\operatorname{rank} U' \geqslant \dim L' = s$, so that $\dim C \geqslant s$. Now take a nonzero codeword $c = u_0 + \Sigma_{1\leqslant i\leqslant s}\lambda_i u_i \in C$ with $\lambda_1, \ldots, \lambda_s \in F$, and

$$B = A_0 + \sum_{1\leqslant i\leqslant s} \lambda_i A_i = \sum_{1\leqslant j\leqslant r} \Big(u_{0j} + \sum_{1\leqslant i\leqslant s} \lambda_i u_{ij}\Big) v_j.$$

This is a representation of $B \in L$ as a linear combination of matrices of rank

1, so that

$$w(c) = \#\Big\{ j \leqslant r : u_{0j} + \sum_{1 \leqslant i \leqslant s} \lambda_i u_{ij} \neq 0 \Big\} \geqslant \operatorname{rank} B \geqslant d.$$

Thus we obtain an (affine) linear $[r, s, d]$-code. (In fact, $\dim C = s$ by the minimality of the computation.) ■

4. THIN TENSORS

Let $R_F(m, n, p)$ denote the maximal bilinear complexity of matrices $A_1, \ldots, A_p \in F^{m \times n}$, i.e. the maximal rank of tensors in $F^m \otimes F^n \otimes F^p$. In this section we deal with the case where p is small, say $p = 2$ or $p = 3$.

THEOREM 4. *Let $m \leqslant n$ and $p \leqslant n$. Then*

(i) $R_F(m, n, p) \geqslant p + m - 1$;
(ii) *if $F = \mathbb{F}_q$ is finite, then*

$$R_F(m, n, p) \geqslant \sum_{0 \leqslant i < p} \left\lceil \frac{m}{q^i} \right\rceil \geqslant \eta(q, p) m.$$

Proof. For $1 \leqslant i \leqslant n$, let

$$A_i = \begin{pmatrix} & & \overset{i}{1} & & 0 \\ & & & \ddots & \\ & & & & 1 \\ 1 & & 0 & & \\ & \ddots & & & \\ 0 & & 1 & & \end{pmatrix} \in F^{m \times n},$$

i.e.,

$$(A_i)_{\mu\nu} = \begin{cases} 1 & \text{if } \nu - \mu \equiv i - 1 \bmod n, \\ 0 & \text{otherwise.} \end{cases}$$

Thus A_1 is the $m \times m$ identity matrix with $n - m$ zero columns appended, and A_i is a cyclic shift of the columns of A_1 obtained by labeling the

columns $1,\dots,n$ of A_1 as $i, i+1,\dots,n,1,\dots,i-1$. We have a total of $n \geqslant p$ matrices. Let $A_1,\dots,A_p$ be the first p of them, L their linear span (containing 0), and $r = \operatorname{rank}(A_1,\dots,A_p)$ their bilinear complexity. Then $\dim L = p$, and $\operatorname{rank} B = m$ for each nonzero $B \in L$. By Theorem 3, there exists a linear $[r,p,m]$-code over F. The claims follow from Theorem 2 and Fact 1. ■

Instead of allowing just the multiples of $(1,\dots,1)$ on the shifted diagonals in the proof, we can use the codewords of a linear $[m,k,m-k+1]$-code on each diagonal, assuming F is large enough [Theorem 2(ii)], where $k = \lceil p/n \rceil$. Then for $p \leqslant mn$ we find

$$R_F(m,n,p) \geqslant p + m - \left\lceil \frac{p}{n} \right\rceil.$$

COROLLARY 5.

(i)

$$R_{\mathbb{Z}_2}(n,n,2) = \lceil 3n/2 \rceil,$$

(ii)

$$R_{\mathbb{Z}_2}(n,n,3) \geqslant n + \left\lceil \frac{n}{2} \right\rceil + \left\lceil \frac{n}{4} \right\rceil \geqslant \left\lceil \frac{7n}{4} \right\rceil.$$

Proof. The upper bound in (i) is in Ja'Ja' (1980, Theorem 2.8). ■

We now compare our results with the bounds in the literature. Brockett and Dobkin (1978) prove

$$R_F(m,n,p) \leqslant \min\{mn, mp, np\},$$

and Howell (1978) shows

$$R_F(m,n,p) \geqslant \frac{mnp}{m+n+p-2} \qquad \text{for infinite } F,$$

$$R_F(m,n,p) \geqslant \frac{mnp}{m+n+p-2\log_q(q-1)} \qquad \text{for } F = \mathbb{F}_q.$$

Howell's lower bounds are quadratic in m,n,p, and ours only linear. Thus these are interesting only when the shape (m,n,p) is very unbalanced,

TABLE 1
THE LOWER BOUNDS OF HOWELL AND THEOREMS 4 AND 6 ON $R_F(n,n,p)$ FOR CERTAIN UNBALANCED SHAPES (n,n,p).[a]

Shape	$\#F$	Howell	Theorems 4 and 6
$(n,n,2)$	2	n	$\frac{3}{2}n$
$(n,n,3)$	2	$\dfrac{3n^2}{2n+3}$	$\frac{7}{4}n$
(n,n,p)	∞	$\dfrac{n^2p}{2n+p-2}$	$p+\sqrt{2(n^2-p+1)}-3$
(n,n,p)	q	$\dfrac{n^2p}{2n+p-2\log_q(q-1)}$	$p+\sqrt{2(n^2-p+1)}-3$

[a]The last two entries assume $p \leqslant (n+1)^2/2$.

say for (n,n,p) with $p \leqslant 3$ or $n^2-2n < p \leqslant n^2$ (at least when F is infinite). (See Table 1.)

Grigoryev (1978) and Ja'ja' (1979) show that $R_K(n,n,2) = \lfloor 3n/2 \rfloor$ if K is algebraically closed. Thus for odd n there exist $(n,n,2)$-tensors over $\mathbb{Z}_2$ with rank $r = (3n+1)/2$ over $\mathbb{Z}_2$, while all tensors of this shape have rank at most $r-1$ over an algebraic closure of $\mathbb{Z}_2$.

Grigoryev's proof of his lower bound shows that for any field F there exist $(n,n,2)$-tensors over F with rank $\lfloor 3n/2 \rfloor$, even when computations over an algebraic closure of F are allowed; this is much better than our bound $n+1$ for infinite F. Ja'ja' (1980) shows that

$$R_{\mathbb{F}_q}(n,n,2) \geqslant n + \left\lceil \frac{n-1}{q} \right\rceil,$$

$$R_{\mathbb{Z}_2}(n,n,3) \geqslant \left\lceil \frac{3n-1}{2} \right\rceil + \left\lceil \frac{n}{4} \right\rceil,$$

which are only improved by 1 in Corollary 5, for odd n and $q = 2$.

As a further example, we let F be an algebraic closure of $\mathbb{Z}_2$. Then Strassen (1983) and Lickteig (1985) show the equality in

$$\underline{R}_F(n,n,3) = \left\lceil \frac{3n}{2} \right\rceil < n + \left\lceil \frac{n}{2} \right\rceil + \left\lceil \frac{n}{4} \right\rceil \leqslant R_{\mathbb{Z}_2}(n,n,3);$$

$$10 = 5 + \left\lceil \tfrac{5}{2} \right\rceil + \left\lceil \tfrac{5}{4} \right\rceil \leqslant R_{\mathbb{Z}_2}(5,5,3) \qquad \text{(Atkinson and Stephens 1979)},$$

$$\underline{R}_F(5,5,3) = 8 \qquad \text{(Strassen 1983)}.$$

For small cubic shapes (n,n,n) we find, mainly from the literature,

$$\underline{R}_F(2,2,2) = 2 < 3 = R_F(2,2,2) = R_{\mathbb{Z}_2}(2,2,2),$$

$$\underline{R}_F(3,3,3) = 5 \leqslant R_F(3,3,3) \leqslant 6 \leqslant R_{\mathbb{Z}_2}(3,3,3) \leqslant 8,$$

$$\underline{R}_F(4,4,4) = 7 \leqslant R_F(4,4,4) \leqslant 12,$$

$$8 \leqslant R_{\mathbb{Z}_2}(4,4,4) \leqslant 16$$

$$\underline{R}_F(5,5,5) = 10 \leqslant R_F(5,5,5) \leqslant 15,$$

$$12 \leqslant R_{\mathbb{Z}_2}(5,5,5) \leqslant 25.$$

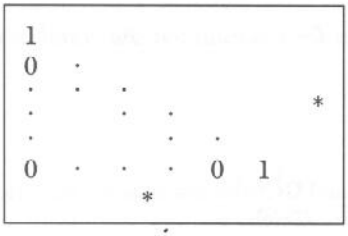
5. THICK TENSORS

In this section, we deal with "thick" tensors of the shape (m,n,p) with p close to mn. When $p \geqslant mn$, then $R_F(m,n,p) = mn$ (Howell 1978).

THEOREM 6. *Let F be a field, $m \leqslant n$, $1 \leqslant k \leqslant mn$, and $p = mn - k + 1$.*

(i) *If $d \leqslant m$ and $d^2 + d \leqslant 2k$, then $R_F(m,n,p) \geqslant p + d - 1$.*
(ii) *If $k \geqslant 2$, then $R_F(m,n,p) \geqslant p + \lfloor \sqrt{2k} \rfloor - 2$.*

Proof. (i): Let $A_0 \in F^{m \times n}$ be the matrix with $(A_0)_{ij} = 1$ for $1 \leqslant i = j \leqslant d$, and $(A_0)_{ij} = 0$ otherwise. Let $A_1, \ldots, A_{p-1} \in F^{m \times n}$ be distinct matrices with exactly one 1, this in some position (i,j) with $i > j$ or $j > d$ or $i > d$. In the picture



A_0 has the d 1's at top left, each other A_i has one 1 in some $*$-position, and each matrix has 0 in the 0-triangle.

Such matrices exist, since $d \leqslant m$ and

$$p-1 = mn-k \leqslant mn-\binom{d+1}{2}.$$

Let r be the bilinear complexity of $(A_0, \ldots, A_{p-1})$, and

$$L = A_0 + \sum_{1 \leqslant i < p} FA_i \subseteq F^{m \times n}.$$

Then $\dim L = p-1$ and $\operatorname{rank} B \geqslant d$ for each $B \in L$. By Theorem 3, there exists an affine $[r, p-1, d]$-code C over F, with $0 \notin C$. By Theorem 2(iii), $r \geqslant p+d-1$.

(ii): For $d = \lfloor \sqrt{2k} \rfloor - 1 \leqslant \sqrt{2k} - 1$ we have $d \leqslant m$ and $d^2 + d \leqslant 2k$. ■

It is clear that the tensor given in the proof actually has rank equal to $p+d-1$. A result of Meshulam (1989) shows that the method will not yield larger bounds, at least not over algebraically closed fields.

Atkinson and Stephens (1979) reduce the general problem of determining $R_F(m, n, mn-k)$ with $k \leqslant \min\{m, n\}$ to that of $R_F(n, n, n^2-n)$. They conjecture that $R_F(n, n, n^2-n) = n^2 - \lceil n/2 \rceil$, and mention an unpublished proof of this, by Lloyd. Theorem 6(i) gives the conjectured lower bound for $n = 1, 2, 3$, and 5.

Our bounds in lines 3 and 4 of Table 1 are larger than Howell's for $p \geqslant mn-2n$ and $n \geqslant 4$.

Let us define $R_{\mathbb{Z}}(m, n, p)$ by considering tensors with integer coefficients and only allowing integer coefficients in the bilinear computation. Since any tensor in $\mathbb{Z}_2$ is the modular image of a tensor over $\mathbb{Z}$, and integer computations yield computations over $\mathbb{Z}_2$, we have $R_{\mathbb{Z}}(m, n, p) \geqslant R_{\mathbb{Z}_2}(m, n, p)$, and our lower bounds on $R_{\mathbb{Z}_2}$ carry over to $R_{\mathbb{Z}}$. In particular, for odd n there exist $(n, n, 2)$-tensors over $\mathbb{Z}$ with rank $r = (3n+1)/2$ over $\mathbb{Z}$, while all tensors of this shape have rank at most $r-1$ over $\mathbb{C}$.

I thank J. H. van Lint for pointing out the equality in (2.2).

REFERENCES

Alder, A. 1983. Grenzrang und Grenzkomplexität aus algebraischer und topologischer Sicht. Dissertation, Univ. Zürich.

Atkinson, M. D. and Stephens, N. M. 1979. On the maximal multiplicative complexity of a family of bilinear forms, *Linear Algebra Appl.* 27:1–8.

Bini, D., Capovani, M., Lotti, G., and Romani, F. 1979. $O(n^{2.7799})$ complexity for matrix multiplication, *Inform. Process. Lett.* 8:234–235.

Brockett, R. W. and Dobkin, D. 1978. On the optimal evaluation of a set of bilinear forms, *Linear Algebra Appl.* 19:207–235.

Brown, M. R. and Dobkin, D. 1980. An improved lower bound on polynomial multiplication, *IEEE Trans. Comput.* 29:337–340.

Bshouty, N. 1987. Lower Bound for Matrix Multiplication, preprint, Technion, Haifa, 10 pp.

von zur Gathen, J. 1988. Algebraic complexity theory, *Ann. Rev. Comput. Sci.* 3:317–347.

Grigoryev, D. Yu. 1978. Some New Bounds on Tensor Rank, LOMI preprint E-2-78, USSR Academy of Science, Leningrad, 13 pp.

de Groote, H. F. 1987. *Lectures on the Complexity of Bilinear Problems*, Lecture Notes in Comput. Sci. 245, Springer-Verlag, 135 pp.

Heintz, J. 1985. Zur Berechnungskomplexität von Polynomen und bilinearen Abbildungen. Ein Exposé. Habilitationsschrift, Fachbereich Mathematik, Univ. Frankfurt. 45 pp.

Howell, T. D. 1978. Global properties of tensor rank, *Linear Algebra Appl.* 22:9–23.

Ja'ja', J. 1979. Optimal evaluation of pairs of bilinear forms, *SIAM J. Comput.* 8:443–462.

Ja'ja', J. 1980. Computation of bilinear forms over finite fields, *J. Assoc. Comput. Mach.* 27:822–830.

Kaminski, M. and Bshouty, N.H. 1987, Multiplicative complexity of polynomial multiplication over finite fields, Proc. 28th IEEE Symp. Foundations of Computer Science, pp. 138–140.

Lempel, A. and Winograd, S. 1977. A new approach to error-correcting codes, *IEEE Trans. Inform. Theory* 23:503–508.

Lickteig, T. 1985. Typical tensor rank, *Linear Algebra Appl.* 69:95–120.

van Lint, J. H. 1981. *Introduction to Coding Theory*, Graduate Text in Math. 86, Springer-Verlag, New York, 171 pp.

Meshulam, R. 1989. On two extremal matrix problems, *Linear Algebra Appl.* 114/115:261–271.

Schwartz, J. T. 1980. Fast probabilistic algorithms for verification of polynomial identities, *J. Assoc. Comput. Mach.* 27:701–717.

Strassen, V. 1973. Vermeidung von Divisionen, *J. Reine Angew. Math.* 264:182–202.

Strassen, V. 1983. Rank and optimal computation of generic tensors, *Linear Algebra Appl.* 52:645–685.

Strassen, V. 1984. Algebraische Berechnungskomplexität, in *Perspectives in Mathematics*, Birkhäuser-Verlag, Basel, pp. 509–550.

Received 19 January 1990; final manuscript accepted 5 February 1990