Lecture Notes in
Computer Science

Edited by G. Goos and J. Hartmanis

179

Victor Pan

How to Multiply Matrices Faster

Springer-Verlag
Berlin Heidelberg New York Tokyo 1984

Author

Victor Pan
State University of New York at Albany
Department of Computer Science
1400 Washington Avenue, Albany, NY 12222, USA

CR Subject Classification (1982): F.2.1, G.1.3

ISBN 3-540-13866-8 Springer-Verlag Berlin Heidelberg New York Tokyo
ISBN 0-387-13866-8 Springer-Verlag New York Heidelberg Berlin Tokyo

Printed in Germany

Printing and binding: Beltz Offsetdruck, Hemsbach / Bergstr.
2146/3140-543210

CONTENTS

Some Notation and Abbreviations

Notation	Meaning, Comments	Defined or First Used In Section(s) (see also Index)
A	algorithm	19,23
ar(A);ar(P)	number of arithmetical operations involved in A; required in order to solve a problem P	19,23
as(A)	number of additions/subtractions involved in A	32,33
AAPR	accumulation of the accelerating power via recursion	6
$b_{\gamma}(X,Y)$	bilinear form in X,Y	2
BA(n)	bilinear algorithm for nXn MM	2,22,23
BA(n,λ)	bilinear λ-algorithm for nXn MM	23
BBM	Boolean MM	18
bs(A)	bit-space used by A	23
bt(A)	bit-time used by A	23
bt(s),bt(*,s),bt($\pm$,s)		18
bs(P),bt(P)	bit-time and bit-space of a computational problem P	23
C	the field of complex numbers	2
$c\rho$	commutative rank	32
$cb\rho$	commutative λ-rank	33
C(g,h)	g!/(h!(g-h)!)	8,9
cond	condition	25
D	domain of definition of problem or algorithm	Part 2 (Summary); 23
d	degree of λ-algorithm	6
d	shortest distance	18 only

det(W)	determinant of a matrix W	19
Det(n)	the problem of the evaluation of the determinant of an nXn matrix	Part 2 (Summary); 19
DFT(n)	discrete Fourier transform,	38,39
E	extension of a ring (field)	5
E,E(n),e(n),E(A,D,h), E(Z(V),D,h)	error bounds	Part 2 (Summary); 23-30
F	ring,field	2
$F[\lambda]$	ring of polynomials over F	6
$f(i,j,q)$, $f'(j,k,q)$, $f''(k,i,q)$, $f(\alpha,q)$, $f'(\beta,q)$, $f''(\gamma,q)$	constant coeficients (from F) of bilinear algorithms	2
$f(i,j,q,\lambda)$, $f'(j,k,q,\lambda)$, $f''(k,i,q,\lambda)$, $f(\alpha,q,\lambda)$, $f'(\beta,q,\lambda)$, $f''(\gamma,q,\lambda)$	coefficients (from $F[\lambda]$) of bilinear λ-algorithms	6
$f,f',f'',\tilde{f},\tilde{f}',\tilde{f}''$		23
FFT	fast Fourier transform	Intr.,2,38
h(s)	2^{1-s}	23
u^H,W^H	complex conjugate of number u, conjugate transpose of matrix W	19
I (also I_n))	identity matrix (of size nXn)	19
ℓ_h(ℓ_2, ℓ_∞)	ℓ_h-norm of a matrix or of a vector	24
log u	logarithm to the base 2 of u	1

L_q, L_q'		2
L_q''		10
M	rank of algorithm, λ-rank of λ-algorithm	2,4,6
MA,MS	matrix addition,subtraction	20
MI	matrix inversion	Part 2 (Summary); 19
MM	matrix multiplication	Intr., 1
(m,n,p); also mXnXp MM	the problem of mXn by nXp MM	2
O(g(s)),o(g(s))	see Notation 18.1	Intr.,1,18
$0, 0_n$	null matrix	19,20
PM	polynomial multiplication	2
Q	field of rational numbers	2
Q	unitary matrix (a QR-factor)	20
Q(s)	computed approximation to Q	26-30
$QR, \tilde{Q}R, QR^*$		20
R	upper triangular matrix (a QR-factor)	20
R(s)	computed approximation to R	26-30
R	field of real numbers	2
$\underline{R}$	set of vectors in the proof of Theorem 7.2	9 only
SLE	the problem of solving a system of linear equations	Part 2 (Summary); 19
sm(A)	number of scalar multiplications in A	32,33
T	trilinear form	10
TA	trilinear aggregating	Intr.,3,11

Tr(W)	trace of a matrix W	10
TMI	triangular matrix inversion	21
t	tensor	2,10
U,V,W,X,Y,Z	matrices	1,2,4,6,10
Z	ring of integers	2,5
$Z(\nu)$	ring of integers modulo ν	2,5
Z(V)	output matrix	24-30
$\delta(i,j)$	$\delta(i,j)=0, i \neq j; \delta(i,i)=1$	2
Δ, Δ'	error value,error matrix	23-30
λ	see λ-algorithms	4,6
ρ , ρ_F	rank, rank over a ring F	2
$\rho(m,n,p)$	rank of mXnXp MM	2
$b\rho$	λ-rank	36
ω	exponent of MM	2
ω_F	exponent of MM over a ring F of constants	2
Σ,Π	symbols of sums, products	
Σ	diagonal matrix	20 only
$\lfloor u \rfloor$, $\lceil u \rceil$	see Notation 18.1	18
$\oplus$	direct sum of disjoint problems	8
$\ominus$	direct sum of identical disjoint problems	2,5,8
$\otimes$	(tensor) product of bilinear problems	2,5,8
$\otimes$	direct (Kronecker) product of vectors, matrices, tensors, and of linear, bilinear, or polylinear forms	10,14,16

$\otimes$	generalized MM	18 only
$\|\|\underline{v}\|\|, \|\|W\|\|$	norms of vector $\underline{v}$, matrix W	24
$t \leftarrow t'$	mapping (algorithm)	5,8
$\|S\|$	cardinality of a set S	
$\|u\|$	absolute value (modulus) of a number u	
$\subset$, $\subseteq$	inclusion of one set into another	5
$\in$	inclusion of an element into a set	9
$\cup$	union of sets	5
$\blacksquare$	end of clause, of proof, of algorithm	