Computers Math. Applic. Vol. 23, No. 12, pp. 13–24, 1992
Printed in Great Britain.

0097-4943/92 $5.00 + 0.00

A PARALLEL ALGORITHM FOR EXACT SOLUTION OF LINEAR EQUATIONS VIA CONGRUENCE TECHNIQUE

ÇETIN K. KOÇ
Department of Electrical Engineering, University of Houston
Houston, TX 77204, U.S.A.

(Received April 1990 and in revised form November 1990)

Abstract—We present a parallel algorithm for computing the exact solution of a system of linear equations via the congruence technique. The basic idea of the technique is to convert the original system of equations into a system of congruences modulo various primes, and combine the solutions by the application of the Chinese remainder theorem. The parallel congruence algorithm proposed in this paper requires only local communication among the processors and is particularly suitable for implementation on distributed-memory multiprocessors and systolic computing systems. We have implemented the parallel congruence algorithm on an Intel cube and obtained an efficiency of greater than 90%.

1. INTRODUCTION

We consider the solution of the system of linear equations

$$\mathbf{A}\mathbf{x} = \mathbf{b}, \tag{1}$$

where $\mathbf{A}$ is a $k \times k$ invertible matrix, and $\mathbf{x}$ and $\mathbf{b}$ are $k \times 1$ vectors. This problem has been studied intensively. There are several methods to solve (1) most notably the Gauss and the Gauss-Jordan elimination methods. There are situations, however, in which these methods are inadequate; for example, when one is interested in the *exact* solution of (1), or when $\mathbf{A}$ is ill-conditioned.

The exact solution of (1) can be found by either the direct computation method using multiple-precision integer arithmetic or the residue arithmetic techniques. The residue arithmetic techniques find the result by either using multiple moduli (the congruence technique) or the single modulus (p-adic expansions). Algorithms using p-adic expansions are given by Dixon [1] and by Gregory and Krishnamurthy [2].

We should note that all of these methods require that the entries of $\mathbf{A}$ and $\mathbf{b}$ be integers. However, this is not a serious restriction, since the rational number or the floating-point number entries of $\mathbf{A}$ and $\mathbf{b}$ can be converted to integers by scaling.

Parallel implementations of the p-adix expansion and the direct computation methods are given by Villard [3]. In this paper, we focus on parallel implementation of the congruence technique which solves (1), by first solving $n+1$ such systems in $\mathbb{Z}_{m_i}$ (the ring of integers modulo m_i) for $0 \leq i \leq n$. These results are then combined using the Chinese remainder theorem to find the solution in $\mathbb{Z}_M$ where $M = m_0 m_1 m_2 \cdots m_n$. The reader is referred to the papers by Takashi and Ishibashi [4], Borosh and Fraenkel [5], Newman [6], Howell and Gregory [7,8], Fraenkel and Loewenthal [9], Cabay [10], Bareiss [11], and Cabay and Lam [12] for further details of this technique. The books by Knuth [13], Lipson [14], Mackiw [15], and Young and Gregory [16] contain discussions on the congruence technique and various algorithms to find exact solutions of linear equations with integer and rational entries. Programs implementing the congruence technique are described in [6,17,18]. McClellan extended the congruence techniques to solve linear equations with polynomial or rational function entries [19–21].

The author wishes to thank the anonymous referee for the comments which greatly improved the paper, and Rose Marie Piedra for her programming efforts on the Intel hypercube.

We would like to state the following assumptions for the timing analysis of the algorithm presented in this paper.

- We choose the moduli $m_i \leq W$ for $0 \leq i \leq n$. W is the wordsize of the computer, i.e., the largest integer which can be operated on by the arithmetic unit of the computer.
- An arithmetic operation ($\in \{+, -, \times\}$) on integers $\leq W$ is assumed to take 1 unit of time, defined as an arithmetic step.
- For operations on integers $> W$, we implement multi-precision arithmetic.
- The multiplicative inverse of $a \leq W$ in $\mathbb{Z}_b$ exists if $\gcd(a, b) = 1$. It is defined as the integer $x \leq W$ such that

$$a\,x = 1 \pmod{b},$$

  and can be computed using the extended Euclid algorithm [13,14]. We denote the operation to find the inverse of a in $\mathbb{Z}_b$ by INVERSE(a,b). If $a, b \leq W$, then Euclid's algorithm requires $O(\log W)$ arithmetic operations to compute INVERSE(a,b). Since W is independent of n, we assume that the INVERSE operation on single-precision numbers takes only $O(1)$ arithmetic operations.
- Our computer is also capable of carrying out arithmetic operations ($\in \{+, -, \times, \div\}$) on floating-point numbers. A floating-point arithmetic operations is also assumed to take 1 step.

For the parallel implementation of the congruence technique, we assume that we have a distributed-memory multiprocessor with p processors. The processors are connected with communication links, forming a network topology. Examples of network topologies are linear arrays, rings, trees, 2-dimensional and multi-dimensional meshes, and hypercubes. The communication cost of the parallel algorithm is measured by counting the total number of parallel routing steps, where a routing step is defined as the time required to send an operand (i.e., a single-precision integer) from a processor to one of its neighboring processors on a path between these two processors, and the routing cost is taken to be the length of the path.

We describe the congruence technique in Section 2. When the solutions in $\mathbb{Z}_{m_i}$ are combined using the Chinese remainder theorem to find the solution in $\mathbb{Z}_M$, we may pick either the single-radix conversion algorithm or the mixed-radix conversion algorithm. We describe these algorithms in Section 3. The mixed-radix conversion algorithm is chosen for parallel implementation of the congruence technique. In Section 4, we present the parallel congruence algorithm and time-optimal and spacetime-optimal systolic schedules for parallel implementation of the mixed-radix conversion algorithm. An actual implementation of the congruence technique for the exact solution of linear equations has been realized on an Intel hypercube. Our implementation has shown that up to 92% efficiency can be obtained on the first generation Intel cube, which is a very slow machine in terms of interprocessor communication. In Section 5, we report the implementation results and discuss several variations of the parallel congruence algorithm and point out some future topics for research.

2. CONGRUENCE ALGORITHM

Let $m_0, m_1, m_2, \ldots, m_n$ be a set of pairwise relatively prime numbers and $M = m_0 m_1 m_2 \cdots m_n$. We denote the determinant of $\mathbf{A}$ by $d = \det(\mathbf{A})$ and the adjoint of $\mathbf{A}$ by $\mathbf{A}^{\text{adj}}$. Since we assume $d \neq 0$, $\mathbf{A}^{\text{adj}}$ is also a nonsingular integral matrix satisfying

$$\mathbf{A}\,\mathbf{A}^{\text{adj}} = \mathbf{A}^{\text{adj}}\mathbf{A} = d\,\mathbf{I},$$

where $\mathbf{I}$ is the $k \times k$ unit matrix. For a matrix $\mathbf{B} = [b_{ij}]$, we also define MAX($\mathbf{B}$)=$\max_{i,j}|b_{i,j}|$. The solution of (1) can be written as

$$x = \frac{1}{d}\,\mathbf{A}^{\text{adj}}\,\mathbf{b} = \frac{1}{d}\,\mathbf{z},$$

where $\mathbf{z} = \mathbf{A}^{\text{adj}}\,\mathbf{b}$.

The Congruence Algorithm

Step 0. Choose the moduli set $m_0, m_1, \ldots, m_n$ such that $M > 2\max(|d|, |MAX(\mathbf{A})|)$ and $\gcd(M, d) = 1$.

Step 1. Solve the $n+1$ systems $\mathbf{A}\,\mathbf{y}_i = \mathbf{b} \pmod{m_i}$ for $0 \leq i \leq n$. Compute the determinant $d_i = \det(\mathbf{A}) \pmod{m_i}$ for $0 \leq i \leq n$. Also compute $\mathbf{z}_i = d_i\,\mathbf{y}_i \pmod{m_i}$ for $0 \leq i \leq n$.

Step 2. Use the Chinese remainder theorem to solve the simultaneous congruences $\mathbf{z} = \mathbf{z}_i \pmod{m_i}$ for $0 \leq i \leq n$. Also, the simultaneous congruences $d = d_i \pmod{m_i}$ for $0 \leq i \leq n$ are solved by the application of the Chinese remainder theorem.

Step 3. The solution of (1) is found as $\mathbf{x} = \frac{1}{d}\,\mathbf{z}$.

We have the following observations:

- The choice of m_i, such that the conditions in Step 0 hold, may be a difficult and time consuming process. It is possible to estimate the determinant by the use of Hadamard inequality. We then have to choose m_i such that $\gcd(m_i, d) = 1$ for $0 \leq i \leq n$. Newman suggests the use of a predetermined prime moduli set, with the full knowledge that in certain instances the method will fail [6]. By choosing large primes, the probability of the occurence $\gcd(m_i, d) > 1$ can be made very small [6,11,16].
- In Step 1, the operations are performed using single-precision integer arithmetic. We choose $m_i < W$ for $0 \leq i \leq n$, and then implement the Gaussian elimination algorithm in single-precision integer arithmetic. As matrix $\mathbf{A}$ is triangularized, determinant $d_i = \det(\mathbf{A}) \pmod{m_i}$ is also computed in single-precision.
- In Step 2, the Chinese remainder theorem is used to find the weighted-radix representation of the residue numbers d_i and $\mathbf{z}_i$, for $0 \leq i \leq n$. The methods for conversion of a residue number to a weighted number system are based on two different constructive proofs of the Chinese remainder theorem. In the first case, the number is converted to a *single-radix* weighted number system, whereas in the second case it is converted to a *mixed-radix* weighted number system. Since during the computation of d or $\mathbf{z}$, the intermediate and the resulting values can be larger than W, the single-radix conversion algorithm requires the implentation of multi-precision integer arithmetic.
- In Step 3, floating-point arithmetic is used to compute the solution $\mathbf{x}$

$$\mathbf{x} = [x_0, x_1, \ldots, x_{k-1}]^{\mathsf{T}} = \frac{1}{d}\,[z_0, z_1, \ldots, z_{k-1}]^{\mathsf{T}}.$$

THEOREM 1. *The congruence algorithm finds the solution of (1) using $O(nk^3 + n^2k)$ arithmetic steps.*

PROOF. The solution of the systems $\mathbf{A}\mathbf{y}_i = \mathbf{b} \pmod{m_i}$ and the computation of the determinant $d_i = \det(\mathbf{A}) \pmod{m_i}$ for $0 \leq i \leq n$ are achieved by the use of the Gaussian elimination algorithm. First the coefficient matrix is triangularized; then backward-substitution is performed to solve for $\mathbf{y}_i$. During these computations, multiplicative inverses of the nonzero elememts of $\mathbf{A}$ are computated using the extended Euclid algorithm. It becomes evident that one such system is solved in $O(k^3)$ arithmetic steps (see also, e.g., [6,11,14]). Thus, the solution $(n+1)$ of these systems requires $O(n\,k^3)$ arithmetic steps. Since the computation of $\mathbf{z}_i = d_i\,\mathbf{y}_i \pmod{m_i}$ requires $O(n\,k)$ arithmetic steps for $0 \leq i \leq n$, the number of arithmetic operations required in Step 2 is $O(n\,k^3)$.

In Step 2, we use either the single-radix conversion algorithm or the mixed-radix conversion algorithm to find the weighted-radix representation of the numbers $\mathbf{z}_i$ and d_i for $0 \leq i \leq n$. The single-radix conversion algorithm (as well as the mixed-radix conversion algorithm) requires $O(n^2)$ arithmetic steps to find the integer d, using the residue numbers $d_i = d \pmod{m_i}$ for $0 \leq i \leq n$. Since the vector $\mathbf{z}_i$ has k components, we see that Step 3 of the congruence algorithm requires $O(n^2k)$ arithmetic operations.

In Step 3, we compute the solution by performing k floating-point division operations. According to our assumption, this takes $O(k)$ arithmetic steps.

Thus, the total number of arithmetic operations required by the congruence algorithm is found to be $O(n\,k^3 + n^2k)$. ∎

3. CHINESE REMAINDERING ALGORITHMS

We now describe the single-radix and the mixed-radix conversion algorihtms and give two theorems regarding the number of arithmetic operations required. The detailed proofs of these theorems can be found in [14,22,23]. We assume that we are given the residues u_i of a weighted number u with respect to each modulus m_i, i.e.,

$$u = u_i \pmod{m_i}, \qquad \text{for } 0 \leq i \leq n.$$

The single-radix conversion algorithm computes u, whereas the mixed-radix conversion algorithm computes the mixed-radix coefficients $(v_0, v_1, \ldots, v_n)$ of u. Once the mixed-radix coefficients have been obtained, u is written in terms of these coefficients and the moduli as

$$u = v_0 + v_1 m_0 + v_2 m_0 m_1 + \cdots + v_n m_0 m_1 \cdots m_{n-1}. \tag{2}$$

The Single-Radix Conversion Algorithm

Step 1. Compute $M = m_0 m_1 \cdots m_n$ and $m_0 m_1 \cdots m_{i-1} m_{i+1} \cdots m_n = \frac{M}{m_i}$ using multi-precision arithmetic.

Step 2. Compute the multiplicative inverses of $\frac{M}{m_i}$ in $\mathbb{Z}_{m_i}$ for $0 \leq i \leq n$, i.e., compute

$$c_i = \text{INVERSE}\left(\frac{M}{m_i}, m_i\right), \qquad \text{for } 0 \leq i \leq n. \tag{3}$$

Step 3. Compute u by performing the sum

$$u = \frac{M}{m_0} c_0 u_0 + \frac{M}{m_1} c_1 u_1 + \cdots + \frac{M}{m_n} c_n u_n \tag{4}$$

in multi-precision arithmetic.

THEOREM 2. *Given the moduli $m_0, m_1, \ldots, m_n$ and the remainders $u_0, u_1, \ldots, u_n$, such that $m_i \leq W$ for $0 \leq i \leq n$, the number u can be computed in $O(n^2)$ arithmetic steps with the single-radix conversion algorithm.*

The Mixed-Radix Conversion Algorithm

Step 1. Compute the inverses c_{ij} for $0 \leq i < j \leq n$, where

$$c_{ij} = \text{INVERSE}(m_i, m_j). \tag{5}$$

Step 2. Compute

$$\begin{aligned}
v_0 &= u_0 \pmod{m_0}, \\
v_1 &= (u_1 - v_0)\, c_{01} \pmod{m_1}, \\
v_2 &= ((u_2 - v_0)\, c_{02} - v_1)\, c_{12} \pmod{m_2}, \\
&\vdots \\
v_n &= (\cdots((u_n - v_0)\, c_{0n} - v_1)\, c_{1n} - \cdots - v_{n-1})\, c_{n-1,n} \pmod{m_n}.
\end{aligned}$$

THEOREM 3. *Given the moduli $m_0, m_1, \ldots, m_n$ and the remainders $u_0, u_1, \ldots, u_n$, such that $m_i \leq W$ for $0 \leq i \leq n$, the mixed-radix number representation $(v_0, v_1, \ldots, v_n)$ of u can be computed in $O(n^2)$ arithmetic steps with the mixed-radix conversion algorithm.*

The mixed-radix representation can be converted to single-radix representation by applying Horner's algorithm to formula (2), i.e.,

$$u = (\cdots((v_n m_{n-1} + v_{n-1}) m_{n-2} + v_{n-2}) m_{n-3} + \cdots + v_1)\, m_0 + v_0. \tag{6}$$

If $v_i, m_i \leq W$ for $0 \leq i \leq n$, then the application of Horner's algorithm to compute a single-radix representation of u requires $O(n^2)$ arithmetic steps using multi-precision arithmetic [14].

We also note that the above theorems are true for *preconditioned* Chinese remaindering as well. In this case, the constants c_i, (i.e., Equation (3)) and c_{ij} (i.e., Equation (5)) are precomputed for the single-radix and the mixed-radix conversion algorithms, respectively.

4. PARALLEL CONGRUENCE ALGORITHM

A remarkable property of the congruence algorithm is its parallelism. Since the solution of equation $\mathbf{A}\,\mathbf{y}_i = \mathbf{b} \pmod{m_i}$ is independent for every $i = 0, 1, 2, \ldots, n$, the algorithm is very suitable for implementation on parallel computers. Once the solutions in $\mathbb{Z}_{m_i}$ are computed, we need to apply a Chinese remaindering algorithm to compute the solution in $\mathbb{Z}_M$.

Let $n + 1 = q\,p$, where $n + 1$ is the number of moduli, p is the number of processors, and $q \leq 1$ is an integer. For the time being we assume that $q = 1$. We partition the moduli set in such a way that processor i executes Step 1 of the algorithm modulo m_i, and thus, solves system $\mathbf{A}\,\mathbf{y}_i = \mathbf{b} \pmod{m_i}$ and computes determinant $d_i = \det(\mathbf{A}) \pmod{m_i}$. It then proceeds to compute $\mathbf{z}_i = d_i\,\mathbf{y}_i \pmod{m_i}$. This computation is performed by all processors for $i = 0, 1, \ldots, n$.

Thus at the end of Step 1, we will have a $k \times 1$ vector $\mathbf{z}_i$ and an integer d_i in processor i, for all $0 \leq i \leq n$. We now need to apply the Chinese remainder theorem to compute a $k \times 1$ vector $\mathbf{z}$ and an integer d. Notice that if the single-radix conversion algorithm is implemented, then the components of $\mathbf{z}$ and the determinant d are multi-precision integers. If the mixed-radix conversion algorihtm is employed, then we can avoid the implementation of the multiple-precision arithmetic, and compute the mixed-radix coefficients in single-precision. We can then use floating point arithmetic to compute the solution vector $\mathbf{x}$ with these mixed-radix coefficients.

Let the $(k + 1) \times 1$ vector $\mathbf{u}_i$ be

$$\mathbf{u}_i = \begin{bmatrix} \mathbf{z}_i \\ d_i \end{bmatrix}.$$

This vector is available in processor i. We now use the mixed-radix conversion algorithm to compute the $(k + 1) \times 1$ vector $\mathbf{u}$ such that

$$\mathbf{u} = \mathbf{u}_i \pmod{m_i}.$$

The distributed mixed-radix conversion algorithm picks the r^{th} element of each vector $\mathbf{u}_i$ from processor i, for $0 \leq i \leq n$, and computes the mixed-radix coefficients of the r^{th} element of the vector $\mathbf{u}$, for all $r = 1, 2, 3, \ldots, k + 1$. Denote the r^{th} conponent of vector $\mathbf{u}_i$ with u_{ir}. We need to compute v_{ir}, for $0 \leq i \leq n$ and $1 \leq r \leq k + 1$, such that

$$u_{ir} = v_{0r} + v_{1r}\,m_0 + v_{2r}\,m_0\,m_1 + \cdots + v_{nr}\,m_0\,m_1 \cdots m_{n-1} \pmod{m_i}. \tag{7}$$

We define the $(k + 1) \times 1$ vector $\mathbf{V}_{ij}$ for $0 \leq i < j \leq n$, such that $\mathbf{V}_{-1,i} = \mathbf{u}_i$ for $0 \leq i \leq n$ and $\mathbf{V}_{i-1,i} = \mathbf{v}_i$ for $0 \leq i \leq n$. $\mathbf{V}_{ij}$ for $0 \leq i < j \leq n$ are the temporary values of $\mathbf{v}_i$ resulting from the operations in Step 2 of the mixed-radix conversion algorithm. We construct a triangular table of values, with diagonal entries $\mathbf{v}_i = \mathbf{V}_{i-1,i}$ for $0 \leq i \leq n$. For $n = 3$, it is as follows:

$$\begin{array}{lll}
\mathbf{V}_{03} = (\mathbf{V}_3 - \mathbf{V}_0)\,c_{03} \pmod{m_3} & \mathbf{V}_{13} = (\mathbf{V}_{03} - \mathbf{V}_{01})\,c_{13} \pmod{m_3} & \mathbf{V}_{23} = (\mathbf{V}_{13} - \mathbf{V}_{12})\,c_{23} \pmod{m_3} \\
\mathbf{V}_{02} = (\mathbf{V}_2 - \mathbf{V}_0)\,c_{02} \pmod{m_2} & \mathbf{V}_{12} = (\mathbf{V}_{02} - \mathbf{V}_{01})\,c_{12} \pmod{m_2} & \\
\mathbf{V}_{01} = (\mathbf{V}_1 - \mathbf{V}_0)\,c_{01} \pmod{m_1} & &
\end{array}$$

The mixed-radix conversion algorithm computes $\mathbf{V}_{ij}$ for $0 \leq i < j \leq n$, by performing the following operations on single-precision integer operands:

$$c_{ij} = \text{INVERSE}(m_i, m_j), \tag{8}$$

$$\mathbf{V}_{ij} = (\mathbf{V}_{i-1,j} - \mathbf{V}_{i-1,i})\,c_{ij} \pmod{m_j}, \tag{9}$$

where (9) is performed for all $k + 1$ entries of vector $\mathbf{V}_{ij}$.

The data dependences among the entries in the above table lend themselves to systolic implementation. The first step in achieving a systolic implementation is to form the *process dependence graph* of the mixed-radix conversion algorithm. The coefficient c_{ij} is in column i and row j. The positions of terms $\mathbf{V}_{ij}$ are arranged as follows: First, a term of the form $\mathbf{V}_{i-1,i}$ is computed on the diagonal, then this term is used in every operation along the i^{th} column. Based on these observations, Figure 1 presents the process dependence graph of the mixed-radix conversion algorithm for $n = 7$. The graph is drawn on the (i, j) coordinate system. The nodes of this directed

acyclic graph (dag) represent the operations, and the arcs correspond to dependences between the variables used in the operations. The node at point (i, j) computes $\mathbf{V}_{ij}$ by performing the operations given in (8) and (9).

This formulation of the processes at each node allows *preconditioned* Chinese remaindering as well. In this case, the constraints c_{ij} are precomputed and saved at the nodes. The node at point (i, j) now executes only (9).

Koç and Cappello give several time-optimal and spacetime-optimal systolic arrays for the mixed-radix conversion algorithm [24]. The arrays and their corresponding schedules in [24] assume that m_i and $\mathbf{u}_i$ are being fed to the array from the south-end. For our problem, however, this is not the case; m_i and $\mathbf{u}_i$, for $0 \leq i \leq n$, are already available in the i^{th} processor after Step 1 of the congruence algorithm. In the following, we introduce two new systolic arrays which use the data available in the processors.

As a first step, we modify the data dependence graph in Figure 1 in order to achieve local dependence, i.e., a node is dependent only on its neighboring nodes. Discussions and several examples of transformation of data dependence graphs to achieve local dependence can be found in [25]. The resulting dag representing the operations performed by the mixed-radix conversion algorithm is given in Figure 2. We then embed the localized process dependence graph of the mixed-radix conversion algorithm in spacetime to produce a time-optimal and a spacetime-optimal systolic array. The reader is referred to [25] (and the references therein) for spacetime embedding techniques.

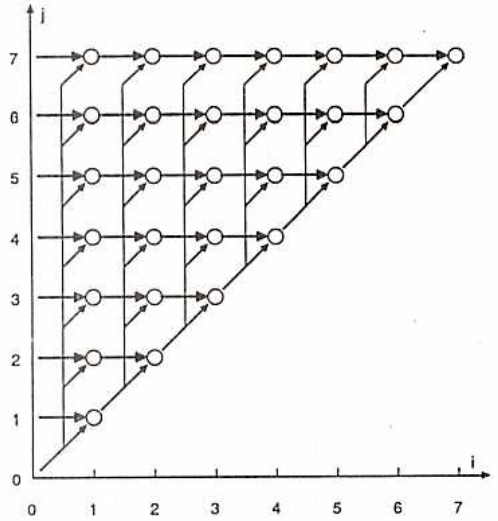

Figure 1. The process dependence graph of the mixed-radix conversion algorithm for $n = 7$.

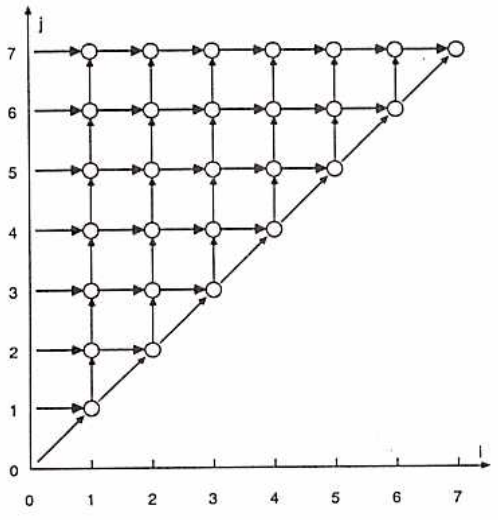

Figure 2. The graph in Figure 1 with localized dependence.

A Time-Optimal Systolic Schedule

We embed the process dependence graph for the mixed-radix conversion algorithm in spacetime. The abscissa is interpreted as time t; the ordinate as space s. The linear embedding E_1 is as follows:

$$t := i + j;$$
$$s := j.$$

The result, depicted in Figure 3 for $n = 7$, is a time-optimal array. Data that flows west $\longrightarrow$ east in Figure 2 flows in the direction of time (perpendicular to space) in this design: it is in the processors' memory. Data that flows south $\longrightarrow$ north in Figure 2 flows up through the array. Data that flows south $\longrightarrow$ east in Figure 2 also flows up through the array, but at half the speed of the south $\longrightarrow$ north data.

Process (i, j) is executed at time $i + j$ in processor j. By inspection, we see that the array uses n processors, finishing the computation in $2n$ steps. The number of vertices (processes) in

longest directed path in any process dependence graph is a lower bound on the number of steps of any schedule for computing the processes. In our graph, the number of vertices in longest path is $2n$. Thus, this array uses a spacetime embedding that is optimal with respect to the number of steps used. Such an embedding is referred to as *time-optimal.*

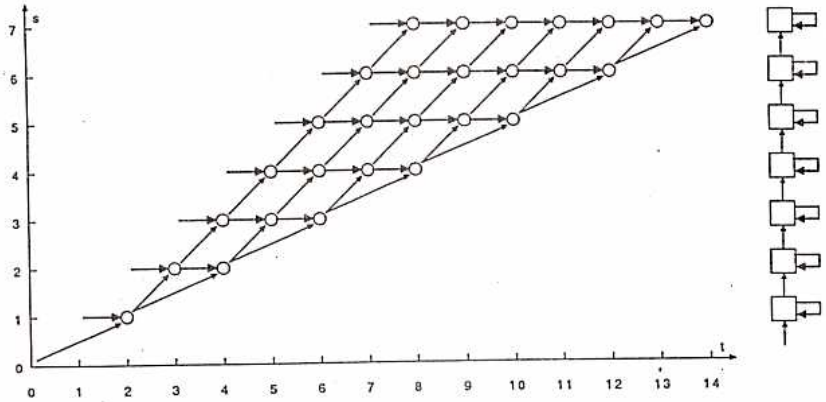

Figure 3. A time-optimal systolic schedule for the mixed-radix conversion algorithm. The resulting algorithm uses n processors and requires $2n$ time steps.

A Spacetime-Optimal Systolic Schedule

We now give another embedding that achieves spacetime-optimality, i.e., it is space-minimal among all designs that are time-optimal. We nonlinearly embed the process dependence graph as follows:

$$t := i + j;$$
$$s := j \mod \left\lfloor \frac{n}{2} \right\rfloor.$$

This embedding E_2 is illustrated in Figure 4 for $n = 7$. Its data flow characteristics are identical to those of embedding E_1, except that the upper processor is attatched to the lower processor forming a ring topology, and data movement wraps around the array. This embedding results in a computation of the process dependence graph that uses $2n$ steps and a ring array of $\lceil \frac{n+1}{2} \rceil$ processors.

The embedding E_2 is space-minimal among time-optimal embeddings. In order to see this, consider time step 8, in which all 4 processors are used. To reduce the number of processors, it is necessary that the process depicted by node (8,3) be rescheduled onto another processor. However, node (8,3) is on a longest directed path in the process dependence graph. This means that it cannot be rescheduled for earlier completion without violating a dependence. Neither can it be scheduled for later completion without either violating a dependence, or extending the overall completion time, violating time-optimality. The number of processors therefore cannot be reduced: the design is spacetime-optimal. Any spacetime embedding of this process dependence graph that completes in $2n$ cycles, must use at least $\lceil \frac{n+1}{2} \rceil$ processors [24].

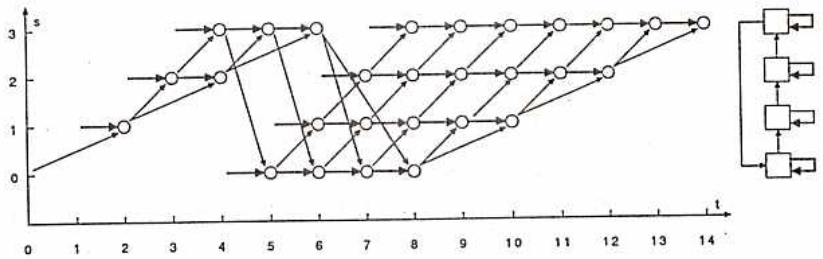

Figure 4. A spacetime-optimal schedule for the mixed-radix conversion algorithm. The resulting algorithm uses $(n + 1)/2$ processors and requires $2n$ time steps.

	Processor 0	Processor 1	Processor 2	Processor 3
	m_0, m_4, $\mathbf{A}$, $\mathbf{b}$	m_1, m_5, $\mathbf{A}$, $\mathbf{b}$	m_2, m_6, $\mathbf{A}$, $\mathbf{b}$	m_3, m_7, $\mathbf{A}$, $\mathbf{b}$
1	$\mathbf{A}\,\mathbf{y}_0 = \mathbf{b}\,[m_0]$ $\mathbf{A}\,\mathbf{y}_4 = \mathbf{b}\,[m_4]$	$\mathbf{A}\,\mathbf{y}_1 = \mathbf{b}\,[m_1]$ $\mathbf{A}\,\mathbf{y}_5 = \mathbf{b}\,[m_5]$	$\mathbf{A}\,\mathbf{y}_2 = \mathbf{b}\,[m_2]$ $\mathbf{A}\,\mathbf{y}_6 = \mathbf{b}\,[m_6]$	$\mathbf{A}\,\mathbf{y}_3 = \mathbf{b}\,[m_3]$ $\mathbf{A}\,\mathbf{y}_7 = \mathbf{b}\,[m_7]$
2	$d_0 = \det(\mathbf{A})\,[m_0]$ $d_4 = \det(\mathbf{A})\,[m_4]$	$d_1 = \det(\mathbf{A})\,[m_1]$ $d_5 = \det(\mathbf{A})\,[m_5]$	$d_2 = \det(\mathbf{A})\,[m_2]$ $d_6 = \det(\mathbf{A})\,[m_6]$	$d_3 = \det(\mathbf{A})\,[m_3]$ $d_7 = \det(\mathbf{A})\,[m_7]$
3	$\mathbf{z}_0 = d_0\,\mathbf{y}_0\,[m_0]$ $\mathbf{z}_4 = d_4\,\mathbf{y}_4\,[m_4]$	$\mathbf{z}_1 = d_1\,\mathbf{y}_1\,[m_1]$ $\mathbf{z}_5 = d_5\,\mathbf{y}_5\,[m_5]$	$\mathbf{z}_2 = d_2\,\mathbf{y}_2\,[m_2]$ $\mathbf{z}_6 = d_6\,\mathbf{y}_6\,[m_6]$	$\mathbf{z}_3 = d_3\,\mathbf{y}_3\,[m_3]$ $\mathbf{z}_7 = d_7\,\mathbf{y}_7\,[m_7]$
4	$\mathbf{V}_0 = \mathbf{u}_0 = [\mathbf{z}_0,\ d_0]^\top$ $\mathbf{V}_4 = \mathbf{u}_4 = [\mathbf{z}_4,\ d_4]^\top$	$\mathbf{V}_1 = \mathbf{u}_1 = [\mathbf{z}_1,\ d_1]^\top$ $\mathbf{V}_5 = \mathbf{u}_5 = [\mathbf{z}_5,\ d_5]^\top$	$\mathbf{V}_2 = \mathbf{u}_2 = [\mathbf{z}_2,\ d_2]^\top$ $\mathbf{V}_6 = \mathbf{u}_6 = [\mathbf{z}_6,\ d_6]^\top$	$\mathbf{V}_3 = \mathbf{u}_3 = [\mathbf{z}_3,\ d_3]^\top$ $\mathbf{V}_7 = \mathbf{u}_7 = [\mathbf{z}_7,\ d_7]^\top$

Figure 5. Step 1 of the parallel congruence algorithm. Here $[m_i]$ denotes (mod m_i).

Thus, the optimal value of q is equal to 2; we partition the moduli set such that each processor executes Step 1 of the congruence algorithm for 2 moduli. In Figures 5 and 6, we describe the steps of the congruence algorithm for $n+1 = 8$ and $p = 4$.

THEOREM 4. *The parallel congruence algorithm requires $O(k^3 + n\,k)$ arithmetic and $2n\,(k+1)$ routing steps on a ring array with $p = \lceil \frac{n+1}{2} \rceil$ processors.*

PROOF. Assuming that $n+1$ is even, we allocate the moduli set and A and b such that processor i receives m_i and m_{i+p} for $i = 0, 1, 2, \ldots, p$, where $n+1 = 2p$. As illustrated in Figure 5, $\mathbf{y}_i$ and $\mathbf{y}_{i+p}$ are computed by processor i by solving the systems $\mathbf{A}\mathbf{y}_i = \mathbf{b}$ (mod m_i) and $\mathbf{A}\mathbf{y}_{i+p} = \mathbf{b}$ (mod m_{i+p}). Simultaneously, the determinants d_i =det(A) (mod m_i) and $d_{i+p} = \det(\mathbf{A})$ (mod m_{i+p}) are computed. Thus, the computation of $\mathbf{y}_i$ and d_i for all $0 \le i \le n+1$ will take $O(k^3)$ arithmetic steps since all $p = \frac{n+1}{2}$ processors work simultaneously. Similarly, the computation of $\mathbf{z}_i = d_i\mathbf{y}_i$ (mod m_i) $\mathbf{z}_{i+p} = d_{i+p}\,\mathbf{y}_{i+p}$ (mod m_{i+p}) takes $O(k)$ arithmetic steps.

We then start the parallel mixed-radix conversion algorithm which requires $2n$ steps, where at each step the operations given by (8) and (9) are performed, and a vector of dimension $k+1$ may be sent. The steps of the parallel mixed-radix conversion algorithm are illustrated in Figure 6. Since vectors $\mathbf{V}$ are of dimension $k+1$, we perform $O(n\,k)$ arithmetic operations altogether. Furthermore, at most $2n\,(k+1)$ routing steps are needed by the parallel mixed-radix conversion algorithm.

After the execution of the mixed-radix conversion algorithm, processor $(p-1)$ has vectors $\mathbf{V}_{i,i+1} = \mathbf{v_i}$ for $0 \le i \le n$, as can be seen in Figure 6. We compute $\mathbf{u}$ (i.e., $\mathbf{z}$ and d) in processor $(p-1)$ using floating-point arithmetic with Horner's algorithm as

$$\mathbf{u} = \mathbf{v}_0 + \mathbf{v}_1\,m_0 + \mathbf{v}_2\,m_0\,m_1 + \cdots + \mathbf{v}_n\,m_0\,m_1 \cdots m_{n-1}.$$

This step is completely sequential and requires $O(n\,k)$ arithmetic operations.

Therefore, the parallel congruence algorithm requires a total of $O(k^3 + n\,k)$ arithmetic and $2n\,(k+1)$ routing steps on a ring array of $\lceil \frac{n+1}{2} \rceil$ processors. ∎

5. DISCUSSION AND CONCLUSION

The parallel congruence algorithm described in this paper is suitable for implementation on distributed-memory multiprocessors and systolic computing systems. The processors of the parallel computer system must be powerful enough to solve a system of linear equations. Examples of commercially available distributed-memory multiprocessors are Intel iPSC series, NCUBE, and Ametek. Examples of software-oriented systolic/wavefront computing systems include an array of Transputers [26], the Warp [27], and the Matrix-1 [28].

	Processor 0	Processor 1	Processor 2	Processor 3
0	Send($m_0, V_0; 1$)			
1				
2		Receive(m_0, V_0) Send($m_0, V_0; 2$) $V_{01} = (V_1 - V_0)\, c_{01}\ [m_1]$ Send($m_1, V_{01}; 2$)		
3			Receive(m_0, V_0) Send($m_0, V_0; 3$) $V_{02} = (V_1 - V_0)\, c_{02}\ [m_2]$	
4			Receive(m_1, V_{01}) Send($m_1, V_{01}; 3$) $V_{12} = (V_{02} - V_{01})\, c_{12}\ [m_2]$ Send($m_2, V_{12}; 3$)	Receive(m_0, V_0) Send($m_0, V_0; 0$) $V_{03} = (V_3 - V_0)\, c_{03}\ [m_3]$
5	Receive(m_0, V_0) Send($m_0, V_0;\ 1$) $V_{04} = (V_4 - V_0)\, c_{04}\ [m_4]$			Receive(m_1, V_{01}) Send($m_1, V_{01};\ 0$) $V_{13} = (V_{03} - V_{01})\, c_{13}\ [m_3]$
6	Receive(m_1, V_{01}) Send($m, V_{01}; 1$) $V_{14} = (V_{04} - V_{01})\, c_{14}\ [m_4]$	Receive(m_0, V_0) Send($m_0, V_0; 2$) $V_{05} = (V_5 - V_0)\, c_{05}\ [m_5]$		Receive(m_2, V_{12}) Send($m_2, V_{12}; 0$) $V_{23} = (V_{13} - V_{12})\, c_{23}\ [m_3]$ Send($m_3, V_{23}; 0$)
7	Receive(m_2, V_{12}) Send($m_2, V_{12}; 1$) $V_{24} = (V_{14} - V_{12})\, c_{24}\ [m_4]$	Receive(m_1, V_{01}) Send($m_1, V_{01}; 2$) $V_{15} = (V_{05} - V_{01})\, c_{15}\ [m_5]$	Receive(m_0, V_0) Send($m_0, V_0; 3$) $V_{06} = (V_6 - V_0)\, c_{06}\ [m_6]$	
8	Receive(m_3, V_{23}) Send($m_3, V_{23}; 1$) $V_{34} = (V_{24} - V_{23})\, c_{34}\ [m_4]$ Send($m_4, V_{34}; 1$)	Receive(m_2, V_{12}) Send($m_2, V_{12}; 2$) $V_{25} = (V_{15} - V_{12})\, c_{25}\ [m_5]$	Receive(m_1, V_{01}) Send($m_1, V_{01}; 3$) $V_{16} = (V_{06} - V_{01})\, c_{16}\ [m_6]$	Receive(m_0, V_0) $V_{07} = (V_7 - V_0)\, c_{07}\ [m_7]$
9		Receive(m_3, V_{23}) Send($m_3, V_{23}; 2$) $V_{35} = (V_{25} - V_{23})\, c_{35}\ [m_5]$	Receive(m_2, V_{12}) Send($m_2, V_{12}; 3$) $V_{26} = (V_{16} - V_{12})\, c_{26}\ [m_6]$	Receive(m_1, V_{01}) $V_{17} = (V_{07} - V_{01})\, c_{17}\ [m_7]$
10		Receive(m_4, V_{34}) Send($m_4, V_{34};\ 2$) $V_{45} = (V_{35} - V_{34})\, c_{45}\ [m_5]$ Send($m_5, V_{45}; 2$)	Receive(m_3, V_{23}) Send($m_3, V_{23};\ 3$) $V_{36} = (V_{26} - V_{23})\, c_{36}\ [m_6]$	Receive(m_2, V_{12}) $V_{27} = (V_{17} - V_{12})\, c_{27}\ [m_7]$
11			Receive(m_4, V_{34}) Send($m_4, V_{34}; 3$) $V_{46} = (V_{36} - V_{34})\, c_{46}\ [m_6]$	Receive(m_3, V_{23}) $V_{37} = (V_{27} - V_{23})\, c_{37}\ [m_7]$
12			Receive(m_5, V_{45}) Send($m_5, V_{45}; 3$) $V_{56} = (V_{46} - V_{45})\, c_{56}\ [m_6]$ Send($m_5, V_{45}; 2$)	Receive(m_4, V_{34}) $V_{47} = (V_{37} - V_{34})\, c_{47}\ [m_7]$
13				Receive(m_5, V_{45}) $V_{57} = (V_{47} - V_{45})\, c_{57}\ [m_7]$
14				Receive(m_6, V_{56}) $V_{67} = (V_{57} - V_{56})\, c_{67}\ [m_7]$

Figure 6. The parallel mixed-radix conversion algorithm.

Several extensions of the parallel congruence algorithm can be proposed. An important issue arises when the number of processors in the parallel computing system does not match the size of the problem to be solved. There are two cases:

Fewer processors ($2p < n + 1$):

Let $n+1 = q\,p$, where $q > 2$. We partition the moduli set into $2p$ groups where each group contains $\frac{q}{2}$ moduli. The allocation of the data is similar to the case $q = 2$, however, now processor i is assigned to perform computations using the moduli in groups i and $i + p$, for $i = 0, 1, \ldots, p - 1$.

More processors ($2p > n+1$):

In this case, the best approach is to exploit the parallelism inherent in the Gaussian elimination step, and also in vector operations required by the congruence algorithm. As an example, assume that we have p processors where $2p = k\,(n+1)$. We allocate k processors for each of the linear systems of equations solved in Step 1 of the congruence algorithm. We can use these k processors to reduce the number of arithmetic operations required by the Gaussian elimination algorithm, from $O(k^3)$ to $O(k^2)$. Furthermore, the parallel mixed-radix conversion algorithm will now require only $O(n)$ arithmetic operations instead of $O(n\,k)$. Parallel algorithms for Gaussian elimination and LU decomposition are well-known [29]. However, the parallel congruence algorithm requires Gaussian elimination over the ring of integers $\mathbb{Z}_{m_i}$ (of the Galois field $GF(m_i)$ when m_i is prime). Thus, pivoting is necessary, since every $m_i{}^{\text{th}}$ element is zero. Systolic algorithms for Gaussian elimination without pivoting [30,31], and with partial pivoting [32,33] have been proposed. Thus, we see that, depending on the number of processors available in the parallel computer system, different levels of parallelism already inherent in the congruence algorithm can be exploited.

We have implemented the parallel congruence algorithm on a first generation Intel hypercube with $p = 8$ processors (iPSC/d3). The ring topology required for the spacetime-optimal systolic implementation of the mixed-radix conversion algorithm is easily embedded in the hypercube by using the binary-reflected Gray code [29]. The timing results of this implementation are summarized in Figure 7. The values of $n+1$ and k were limited to those given in Figure 7 due to memory limitations (512 KBytes per node on this particular Intel cube).

	$k = 10$			$k = 20$			$k = 30$		
$n+1$	T_{seq}(ms)	T_{par}(ms)	E	T_{seq}(ms)	T_{par}(ms)	E	T_{seq}(ms)	T_{par}(ms)	E
16	3205	600	0.67	16475	2405	0.86	48440	6550	0.92
32	8235	1720	0.60	36450	5700	0.80	102040	14310	0.89
48	15135	3365	0.56	59995	9870	0.76	160920	23315	0.86
64	23965	5400	0.55	87210	14870	0.73	225215	33580	0.84
80	34765	7800	0.56	118195	20710	0.71	295075	45225	0.82
96	47555	10990	0.54	152980	27675	0.69	370540	58180	0.80
112	63050	14875	0.53	192930	35485	0.68	453635	72775	0.78

Figure 7. Implementation results on the Intel hypercube (iPSC/d3).

We should however add the following observations:

- When the number of processors available exceeds $\lceil \frac{n+1}{2} \rceil$, we can allocate more than one processor for each congruent linear system solved, and thus reduce the amount of memory required for each node. This is due to that fact each node receives fewer than k rows, allowing a larger system to be solved for a given memory space.
- The hypercube network is richer in connectivity than a ring array. Thus, it seems worthwhile to investigate how the total number of routing operations required can be reduced by utilizing the additional connections. Also, other distributed-memory architecture topologies (e.g., two or three dimensional mesh, binary tree) can be used for implementing the congruence algorithm. Some of these issues are addressed in [34].

The time for the sequential version of the algorithm is measured by executing the sequential congruence algorithm on one of the eight identical processors. In order to obtain a fair comparison between the sequential and the parallel algorithm, we measure the total execution time, but not the initial loading of the data and the final unloading of the results. The efficiency of the parallel congruence algorithm for $n = 16, 32, \ldots, 112$ and $k = 10, 20, 30$ is plotted in Figure 8. Theoretically, the parallel congruence algorithm should achieve linear speedup (constant

efficiency). However, we observe a decline in the efficiency as n increases. This is due to the fact that $2n(k+1)$ routing operations required by the parallel algorithm start taking a significant amoung of time for large n. Furthermore, the slow communication (*store-and-forward*) mechanism of the first generation hypercubes constitutes an obstacle to high efficiency. We note that the newer message-passing multiprocessors have more advanced, and thus much faster data communication mechanisms [35]. The efficiency becomes higher for larger k, since Step 1 (which requires no communication and $O(k^3)$ parallel arithmetic steps) starts dominating Step 2 (which requires $2n(k+1)$ routing and $O(n\,k)$ parallel arithmetic steps).

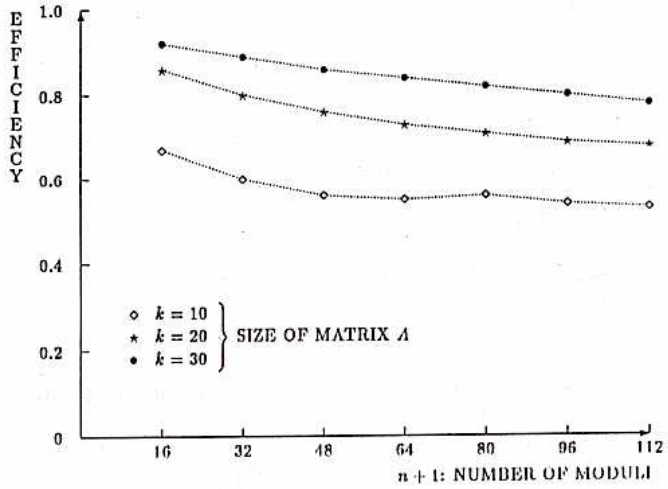

Figure 8. Efficiency of the parallel congruence algorithm on the cube.

REFERENCES

1. J.D. Dixon, Exact solution of linear equations using p-adic expansions, *Numerische Mathematik* **40** (1), 137–141 (1982).
2. R.T. Gregory and E.V. Krishnamurthy, *Methods and Applications of Error-Free Computation*, Springer-Verlag, New York, NY, (1984).
3. G. Villard, Exact parallel solution of linear systems, In *Computer Algebra and Parallelism*, (Edited by J. Della Dora and J. Fitch), pp. 197–205, Academic Press, San Diego, CA, (1989).
4. H. Takashi and Y. Ishibashi, A new method for exact calculations by a digital computer, *Information Processing in Japan* **1**, 28–42 (1961).
5. I. Borosh and A.S. Fraenkel, Exact solutions of linear equations with rational coefficients by congruence techniques, *Mathematics of Computation* **20** (93), 107–112 (January 1966).
6. M. Newman, Solving equations exactly, *Journal of Research of the National Bureau of Standards* **71B** (4), 171–179 (October–December 1967).
7. J.A. Howell and R.T. Gregory, An algorithm for solving linear algebraic equations using residue arithmetic I-II, *BIT* **9** (3/4), 200–224 and 324–337 (1969).
8. J.A. Howell and R.T. Gregory, Solving linear equations using residue arithmetic—Algorithm II, *BIT* **10** (1), 23–37 (1970).
9. A.S. Fraenkel and D. Loewenthal, Exact solutions of linear equations with rational coefficients, *Journal of Research of the National Bureau of Standards* **75B** (1/2), 67–75 (1971).
10. S. Cabay, Exact solution of linear equations, In *Proc. 2nd Symp. Symbolic Algebraic Manipulation*, ACM Press, New York, pp. 392–398, (1971).
11. E.H. Bareiss, Computational solution of matrix problems over an integral domain, *Journal of the Institute of Mathematics and its Applications* **10** (1), 68–104 (1972).
12. S. Cabay and T.P.L. Lam, Congruence techniques for the exact solution of integer systems of linear equations, *ACM Transactions on Mathematical Software* **3** (4), 386–397 (December 1977).
13. D.E. Knuth, *The Art of Computer Programming: Seminumerical Algorithms*, Vol. 2, (Second Edition), Addison-Wesley Publishing Co., Reading, MA, (1981).
14. J.D. Lipson, *Elements of Algebra and Algebraic Computing*, Addison-Wesley Publishing Co., Reading, MA, (1981).
15. G. Mackiw, *Applications of Abstract Algebra*, John Wiley and Sons, Inc., New York, NY, (1985).
16. D.M. Young and R.T. Gregory, *A Survey of Numerical Mathematics*, Vol. 2, Dover Publications Inc., Mineola, NY, (1988).
17. J.A. Howell, Algorithm 406—Exact solutions of the linear equations using the residue arithmetic, *Communications of the ACM* **14** (3), 180–184 (March 1971).

18. S. Cabay and T.P.L. Lam, Algorithm 522 ESOLVE, Congruence techniques for the exact solution of integer systems of linear equations, *ACM Transactions on Mathematical Software* **3** (4), 404–410 (December 1977).
19. M.T. McClellan, The exact solution of systems of linear equations with polynomial coefficients, *Journal of the ACM* **20** (4), 563–588 (October 1973).
20. M.T. McClellan, The exact solution of linear equations with rational function coefficients, *ACM Transactions on Mathematical Software* **3** (1), 1–25 (March 1977).
21. M.T. McClellan, A comparison of the algorithms for the exact solution of linear equations, *ACM Transactions on Mathematical Software* **3** (2), 147–158 (June 1977).
22. J.D. Lipson, Chinese remainder and interpolation algorithms, In *Proc. 2nd Symp. Symbolic and Algebraic Manipulation*, pp. 372–391, ACM Press, New York, NY, (1971).
23. A. Aho, J.E. Hopcroft and J.D. Ullman, *The Design and Analysis of Computer Algorithms*, Addison-Wesley Publishing Co., (1974).
24. Ç.K. Koç and P.R. Cappello, Systolic arrays for integer Chinese remaindering, In *Proceedings of the 9th Symposium on Computer Arithmetic*, (Edited by M.D. Ercegovac and E. Schwartzlander), pp. 216–223, IEEE Computer Society Press, Los Alamitos, California, (1989).
25. S.Y. Kung, *VLSI Array Processors*, Prentice-Hall, Englewood Cliffs, NJ, (1988).
26. INMOS Ltd., *IMS T800 Transputer*, Almondsbury, Bristol, UK, (1986).
27. A.M. Annaratone, E. Arnould, T. Gross, H.T. Kung, M. Lam, O. Menzilcioglu, and J. Webb, The WARP computer: Architecture, implementation, and performance, *IEEE Transactions on Computers* **36** (12), 1523–1538 (December 1987).
28. D.E. Fousler and R. Schreiber, The Saxpy Matrix-1: A general-purpose systolic computer, *IEEE Computer* **20** (7), 35–43 (July 1987).
29. D.P. Bertsekas and J.N. Tsitsiklis, *Parallel and Distributed Computation, Numerical Methods*, Prentice-Hall, Englewood Cliffs, NJ, (1989).
30. W.M. Gentleman and H.T. Kung, Matrix triangularisation by systolic arrays, In *Proc. SPIE298, Real-Time Signal Processing IV*, pp. 19–26, San Diego, CA, (1981).
31. H.M. Ahmed, J.M. Delosme and M. Morf, Highly concurrent computing structures for matrix arithmetic and signal processing, *IEEE Computer* **15** (1), 65–82 (1982).
32. H. Barada and A. El-Amawy, Systolic architecture for matrix triangularisation with partial pivoting, *IEE Proceedings, Part E: Computers and Digital Techniques* **135** (4), 208–213 (July 1988).
33. B. Hochet, P. Quinton and Y. Robert, Systolic Gaussian elimination over $GF(p)$ with partial pivoting, *IEEE Transactions on Computers* **38** (9), 1321–1324 (September 1989).
34. R.M. Piedra, Exact solution of linear equations on distributed-memory multiprocessors, M.S. Thesis, Department of Electrical Engineering, University of Houston, (December 1990).
35. W.C. Athas and C.L. Seitz, Multicomputers: Message-passing concurrent computers, *IEEE Computer* **21** (8), 9–25 (August 1988).