Factorization of singular integer matrices

Patrick Lenders *

School of Mathematics, Statistics and Computer Science,
University of New England, Armidale, NSW 2351, Australia

Jingling Xue

School of Computer Science and Engineering, University of New South Wales,
Sydney, NSW 2052, Australia

Abstract

It is well known that a singular integer matrix can be factorized into a product of integer idempotent matrices. In this paper, we prove that every $n \times n$ ($n > 2$) singular integer matrix can be written as a product of $3n + 1$ integer idempotent matrices. This theorem has some application in the field of synthesizing VLSI arrays and systolic arrays.

Key words: Factorization of matrices, Integer matrices, Idempotent matrices
1991 MSC: 15A36, 15A23

1 Introduction

In [1], it was proved that a singular rational matrix can be factorized into a product of rational idempotent matrices. In particular, every 2×2 rational matrix can be written as a product of two rational idempotent matrices. This is no longer possible for integer matrices. For example, $\begin{pmatrix} 8 & 11 \\ 0 & 0 \end{pmatrix}$ cannot be written as a product of two integer idempotent matrices. In [3], Laffey proved that every singular $n \times n$ ($n > 2$) integer matrix is the product of $36n + 217$ idempotent matrices with integer entries. In the present paper, we improve

* Corresponding author.
Email address: pat@turing.une.edu.au (Patrick Lenders).

Laffey's result, and prove that every $n \times n$ ($n > 2$) singular integer matrix can be written as a product of $3n+1$ integer idempotent matrices.

This theorem has some application in the field of synthesizing VLSI arrays and systolic arrays. Indeed the algorithm to be synthesized is generally given as a set of recurrent equations, with data dependencies expressed as the product of an integer matrix and a vector. The physical constraints on the arrays are such that only unit or idempotent matrices are easily implementable [6]. Thus our theorem demonstrates that any data dependency whose matrix is singular can be implemented on a systolic array through a set of idempotent matrices.

This paper is organized as follows. We first present some definitions and theorems. The next section proves the main theorem (*Any singular integer $n \times n$ ($n > 2$) matrix can be factorized into a product of $3n+1$ integer idempotent matrices*). The proof is followed by an example that illustrates the methodology. The final section shows how to implement a data dependency whose matrix is singular through a set of integer idempotent matrices.

2 Definitions and theorems

Let I_m be the $m \times m$ unit matrix. If A is a square matrix, $b(A)$ denotes its bottom row (with $b_i(A)$ as its i-th element), and $C_{ij}(A)$ denotes the cofactor of its element in row i and column j.

Definition 1 *An $m \times n$ integer matrix of full row rank is said to be in Hermite normal form if it has the form $(D\ 0)$, where D is non-singular, lower triangular, non-negative, in which each row has a unique maximum entry located on the diagonal.*

Theorem 2 *An $m \times n$ integer matrix B of full row rank can be written as $B = (D\ 0)U$ where $(D\ 0)$ is the Hermite normal form of B and U is unimodular.*

For a proof of this theorem, see [7, page 45].

Definition 3 *An $m \times n$ integer matrix B of full row rank is said to be extended unimodular if and only if one of the following equivalent conditions is met:*

(1) The g.c.d of the sub-determinants of B of order m is 1;
(2) The system $Bx = b$ has an integer solution x, for each integer vector b;
(3) For each vector y, if yB is integer, then y is integer.

For a proof of the equivalence of these conditions, see [7, page 47].

Definition 4 *An $n \times n$ integer matrix A of rank m is said to be pseudo uni-*

modular if it can be written: $A = \begin{pmatrix} B_0 \\ 0 \end{pmatrix}$ *where B_0 is an extended unimodular matrix of rank m.*

Theorem 5 *An $m \times n$ integer matrix B of full row rank is extended unimodular if and only if another $m \times n$ integer matrix B_1 can be found such that $BB_1^T = I_m$.*

Proof:

- *Sufficient condition:* This can be proved by applying Condition 2 of Definition 3.
- *Necessary condition:* Assume that we have found an integer matrix B_1 such that $BB_1^T = I_m$. We have to prove that B is extended unimodular. The matrix B can be written (using the Hermite normal form) $B = (H\ 0)U$, where U is unimodular. Thus, by hypothesis, we have $BB_1^T = (H\ 0)UB_1^T = (H\ 0)C = I_m$. It can be verified that $H = I_m$, which proves that B is extended unimodular.

QED

Definition 6 *Let $r = (r_1, r_2, \ldots, r_n)$ be a vector. We define a column operation matrix (denoted $C_k(r)$) with elements:*

$$e_{i,j} = \begin{cases} 1 & j \neq k, i = j \\ 0 & j \neq k, i \neq j \\ r_i & j = k \end{cases}$$

For example, the column operation matrix $C_2(2, 0, 1)$ is the matrix:

$$\begin{pmatrix} 1 & 2 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

Note that any *elementary* column operation matrix (see for example [7, page 45]) can be factorized into a product of our column operation matrices.

Theorem 7 *Any lower triangular matrix A of order n can be factorized into a product of n column operation matrices.*

Proof:

$$D = (r_1, r_2, \ldots, r_n) = C_1(r_1) \times C_2(r_2) \times \cdots \times C_n(r_n)$$

QED

Theorem 8 *A column operation matrix $C_j(r)$ is idempotent if $r_j = 0$.*

Theorem 9 *Let $A = \begin{pmatrix} 0 & 0 \\ 0 & C_j(r) \end{pmatrix}$ be an $n \times n$ integer matrix, where C is a $(n-1) \times (n-1)$ column operation matrix. Then A can be factorized into a product of 2 integer idempotent matrices.*

Proof:

$$A = \begin{pmatrix} 0 & 0 \\ 0 & C_j(r) \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ P & I_{n-1} \end{pmatrix} \begin{pmatrix} 0 & Q \\ 0 & I_{n-1} \end{pmatrix}$$

where the elements of the $(n-1) \times 1$ matrix P are defined as:

$$p_i = \begin{cases} r_i & i \neq j \\ r_i - 1 & i = j \end{cases}$$

and the elements of the $1 \times (n-1)$ matrix Q are defined as:

$$q_i = \begin{cases} 1 & i = j \\ 0 & \text{otherwise} \end{cases}$$

QED

3 Factorization theorem

In this section, we first prove that any pseudo unimodular matrix can be factorized into a product of idempotent matrices. The general theorem will follow easily.

Lemma 10 *Let $A = \begin{pmatrix} B & 0 \\ 0 & 0 \end{pmatrix}$ be an $n \times n$ $(n > 2)$ integer matrix, where B is a $(n-1) \times (n-1)$ matrix. Then A can be factorized into a product of $3n-2$ integer idempotent matrices.*

Proof: We use an integral similarity to transform B into D with $d_{ij} = 0$ if $j > i+1$ (cf. for example [5]).

$$A = \begin{pmatrix} B & 0 \\ 0 & 0 \end{pmatrix} = U \begin{pmatrix} d_{1,1} & d_{1,2} & 0 & \cdots & 0 & 0 \\ d_{2,1} & d_{2,2} & d_{2,3} & \cdots & 0 & 0 \\ \cdots & & & & & \\ d_{n-1,1} & d_{n-1,2} & d_{n-1,3} & \cdots & d_{n-1,n-1} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} U^{-1}$$

$$= U \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \cdots & & & & & \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ d_{1,1} & d_{1,2} & 0 & \cdots & 0 & 0 \\ d_{2,1} & d_{2,2} & d_{2,3} & \cdots & 0 & 0 \\ \cdots & & & & & \\ d_{n-1,1} & d_{n-1,2} & d_{n-1,3} & \cdots & d_{n-1,n-1} & 0 \end{pmatrix} U^{-1}$$

$$= U \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ \cdots & & & & & \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}^T \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ d_{1,1} & d_{1,2} & 0 & \cdots & 0 & 0 \\ d_{2,1} & d_{2,2} & d_{2,3} & \cdots & 0 & 0 \\ \cdots & & & & & \\ d_{n-1,1} & d_{n-1,2} & d_{n-1,3} & \cdots & d_{n-1,n-1} & 0 \end{pmatrix} U^{-1}$$

The two matrices are upper triangular, and thus can be factorized into a product of column operation matrices (cf. theorem 7). We can apply theorem 8 to all the column operation matrices related to the first upper triangular matrix. We can apply theorem 8 to two column operation matrices related to the second upper triangular matrix. Theorem 9 applies to the rest of the column operation matrices. Thus we can factorize the matrix A into a product of $3n-2$ idempotent matrices.

QED

Theorem 11 *Any $n \times n$ $(n > 2)$ pseudo unimodular matrix A can be factorized into the product $EP_3P_2P_1$ where E is a pseudo unimodular matrix with all zeros in its last column and P_i are idempotent matrices.*

Proof: To factorize a pseudo unimodular matrix $A = \begin{pmatrix} B \\ 0 \end{pmatrix}$ (with B extended unimodular), we build iteratively the product $P = A_{2p} \cdots A_3^T A_2 A_1^T A_0$ such that P is equal to A_0, and is also equal to the desired product $(EP_3P_2P_1)$.

We start with A_0 chosen as follows. Let m be the rank of A. We have:

$$A = \begin{pmatrix} B \\ 0 \end{pmatrix} = \begin{pmatrix} I_m & 0 \\ 0 & 0 \end{pmatrix} U$$

where U is an $n \times n$ unimodular matrix. We choose $A_0 = \begin{pmatrix} I_{n-1} & 0 \\ 0 & 0 \end{pmatrix} U$. Thus A_0 is pseudo unimodular, with the first m rows from the matrix A, the next $n-m-1$ rows from the matrix U, and all zeros in the last row. We choose A_1 such that $A_1 A_0^T = \begin{pmatrix} I_{n-1} & 0 \\ 0 & 0 \end{pmatrix}$. According to theorem 5, this is possible because A_0 is pseudo unimodular. The same theorem also implies that A_1 is pseudo unimodular. At each step, we choose A_{i+1} such that

$$A_{i+1} A_i^T = \begin{pmatrix} I_{n-1} & 0 \\ 0 & 0 \end{pmatrix} \tag{1}$$

Thus all the matrices A_i are pseudo unimodular, and we can write:

$$A_i = \begin{pmatrix} B_i \\ 0 \end{pmatrix}$$

where B_i is an $(n-1) \times n$ extended unimodular matrix. We will prove that we can choose the A_i such that (for some $p \geq 0$) $B_{2p} = (B' \ 0)$.

Since B_i is extended unimodular, we have:

$$B_i = (I_{n-1} \ 0) U_i \tag{2}$$

where U_i is an $n \times n$ unimodular matrix. The iteration on B_i is given by:

$$B_{i+1}B_i^T = I_{n-1} = (I_{n-1}\ 0)U_{i+1}U_i^T \begin{pmatrix} I_{n-1} \\ 0 \end{pmatrix}$$

which implies that the top $n-1$ rows of U_{i+1} and U_i^{-T} can be the same, and that the only constraint on the bottom row of U_{i+1} is $det(U_{i+1}) = \pm 1$.

We replace the iteration on A_i by an iteration on U_i, with Equation (2) giving the corresponding B_i. We start with $A_0 = \begin{pmatrix} B_0 \\ 0 \end{pmatrix}$. We calculate U_0 from Equation (2). Then at every step of the iteration, we calculate U_{i+1} from U_i until the last row is $b(U_{2p}) = (0, 0, \cdots, 0, 1)$. At every step, U_{i+1} is chosen such that $\det(U_{i+1}) = \pm 1$.

$$\begin{array}{ccccccc}
A_0 \Rightarrow B_0 \Rightarrow U_0 \Rightarrow & U_1 & \Rightarrow & U_2 & \Rightarrow \cdots \Rightarrow & U_{2p} & \\
& \Downarrow & & \Downarrow & & \Downarrow & \\
& B_1 & & B_2 & & B_{2p} & = (B\ 0) \\
& \Downarrow & & \Downarrow & & \Downarrow & \\
& A_1 & & A_2 & & A_{2p} &
\end{array}$$

The top $n-1$ rows of the new U_{i+1} are simply the top $n-1$ rows of the transpose of the inverse of the previous U_i. At every step i, we have $U_i^{-T} = (C_{kl}(U_i))$, and thus:

$$b_k(U_i^{-T}) = C_{nk}(U_i) \tag{3}$$

Similarly, $U_i = (C_{kl}(U_i^{-T}))$, and thus

$$b_k(U_i) = C_{nk}(U_i^{-T}) \tag{4}$$

The cofactors of the last row of the two matrices U_i^{-T} and U_{i+1} are the same, and we have (with Equations (3) and (4)):

$$C_{nk}(U_{i+1}) = C_{nk}(U_i^{-T}) = b_k(U_i) = b_k(U_{i+1}^{-T}) \tag{5}$$

The bottom row of the new U_{i+1} is chosen so that it converges toward the vector $b(U_{2p}) = (0, 0, \cdots, 0, 1)$, with the constraint $\sum_j b_j(U_{i+1})C_{nj}(U_{i+1}) = 1$

(U_{i+1} being unimodular), or (with Equation (5)):

$$\sum_j b_j(U_{i+1})b_j(U_i) = 1 \tag{6}$$

In Equation (6), the vector $b(U_{i+1})$ is unknown, and the coefficients $b_j(U_i)$ are known from the previous iteration.

We study in details the six iterations which produce A_6 such that $B_6 = (B'\ 0)$ when $n > 2$. The case where any $b_j(U_0)$ is zero being trivial, we assume that all the coefficients $b_j(U_0)$ are non zero and different. Notice that if $n = 2$, the number of iterations is only bounded by the size of the elements of the matrix A (cf. [3]).

- U_1 For the first iteration, $i = 0$ and Equation (6) can be written (cf. Equation (5)):

  $$\sum_j b_j(U_0^{-T})b_j(U_0) = 1 \tag{7}$$

  which shows that the vector $b(U_0^{-T})$ is a solution. Thus we can choose the new vector $b(U_1)$ such that:

  $$\begin{cases} b_1(U_1) = b_1(U_0^{-T}) + \sum_{j=2}^{j=n} t_j b_j(U_0) \\ b_k(U_1) = b_k(U_0^{-T}) - t_k b_1(U_0) \qquad \forall k \neq 1 \end{cases} \tag{8}$$

  for some integers t_j. We will calculate t_j such that $b_1(U_1)$ is prime. Notice that $b_1(U_0^{-T})$, $b_2(U_0)$, $b_3(U_0)$, $\cdots$, $b_n(U_0)$ are coprime (cf. Equation (7)).

  We first choose t_2 such that $b_1(U_0^{-T})+t_2b_2(U_0) = a_2(b'_1(U_0^{-T})+t_2b'_2(U_0)) = a_2p_2$ (with a_2 such that $b'_1(U_0^{-T})$ and $b'_2(U_0)$ are coprime). Dirichlet proved that *Given an arithmetic progression of terms an+b, for n=1, 2, ..., the series contains an infinite number of primes if a and b are coprime.* Thus we can choose t_2 such that p_2 is a prime number not factor of $b_3(U_0)$. We proceed likewise until all the terms of the sum in Equation (8) have been used. Thus $b_1(U_1) = a_np_n$, and $b_1(U_1)$ is prime because $a_n = 1$. We choose t_n such that $b_1(U_1)$ is not a factor of $b_2(U_1)$. Thus $b_1(U_1)$ and $b_2(U_1)$ are coprime.
- U_2 The second iteration will produce $b_n(U_2) = 0$. As $b_1(U_1)$ and $b_2(U_1)$ are coprime, we can choose $b_1(U_2)$ and $b_2(U_2)$ such that $b_1(U_2)b_1(U_1) + b_2(U_2)b_2(U_1) = 1$ and $b_i(U_2) = 0, \forall i \neq 1, 2$.

  Notice that this iteration requires that $n > 2$.
- U_3 The third iteration is very similar to the second one except that now we can choose $b_n(U_3) = 1$ (because $b_n(U_2) = 0$).
- U_4 Now that $b_n(U_3) = 1$, we can choose $b(U_4) = (0, 0, \ldots, 0, 1)$.

- U_5 Finally the fifth iteration produces a matrix U_5 with elements $u_{ij} = 0$ (when $i, j = 1, 2, \ldots, n-1$). Thus, $A_5 = \begin{pmatrix} B' & 0 \\ 0 & 0 \end{pmatrix}$, where B' $(n-1 \times n-1)$ is unimodular (because A_5 is pseudo unimodular).
- U_6 For reasons which will be clarified shortly, we need an even number of matrices A_i. Thus we build an additional matrix U_6 which is simply the transpose of the inverse of U_5.

In the product P, we replace A_0 with A: $P = A_6 A_5^T A_4 A_3^T A_2 A_1^T A$. We can pair the matrices $A_{2i} A_{2i-1}^T$. By application of Equation (1), we have $P = A$. Indeed:

$$P = (A_6 A_5^T)(A_4 A_3^T)(A_2 A_1^T)A = A$$

On the other hand, we can pair the matrices $A_{2i+1}^T A_{2i}$:

$$P = A_6(A_5^T A_4)(A_3^T A_2)(A_1^T A)$$

where A_6 is a pseudo unimodular matrix with all zeros in its last column. Moreover, it can be verified that all the products $A_{i+1}^T A_i$ are idempotent matrices. Thus A can be factorized into the product $EP_3P_2P_1$ where E is a pseudo unimodular matrix with all zeros in its last column and P_i are idempotent matrices.

QED

Applying lemma 10, we can deduce a bound for the number of idempotent matrices.

Theorem 12 *Any $n \times n$ $(n > 2)$ pseudo unimodular matrix A can be factorized into a product of $3n + 1$ idempotent matrices.*

The general case follows easily from theorem 11.

Theorem 13 *Any $n \times n$ $(n > 2)$ singular integer matrix A can be factorized into a product of $3n + 1$ integer idempotent matrices.*

Proof: Let m be the rank of A. We first put the matrix A in Smith normal form: $A = U \begin{pmatrix} B & 0 \\ 0 & 0 \end{pmatrix} V$, where U and V are unimodular matrices, and B is a $m \times m$ diagonal matrix. We right multiply by $I_n = UU^{-1}$, and transform the unimodular matrix VU into a pseudo unimodular matrix:

$$A = U \begin{pmatrix} B & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} I_m & 0 \\ 0 & 0 \end{pmatrix} VUU^{-1} = U \begin{pmatrix} B & 0 \\ 0 & 0 \end{pmatrix} EU^{-1}$$

where E is the pseudo unimodular matrix obtained by replacing the last $n-m$ rows of the unimodular matrix VU with all zeros rows. Applying theorem 11 on the pseudo unimodular matrix E, we have:

$$A = U \begin{pmatrix} B & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} C & 0 \\ 0 & 0 \end{pmatrix} P_3 P_2 P_1 U^{-1} = U \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix} P_3 P_2 P_1 U^{-1} \tag{9}$$

where P_i are integer idempotent matrices.

Applying lemma 10 to the matrix $\begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$ we prove that the matrix A can be factorized into a product of $3n+1$ idempotent matrices when $n > 2$.

QED

4 Example

In this example we apply the algorithm described in the theorem 11 to factorize a pseudo unimodular matrix. The following matrix A is pseudo unimodular.

$$A = \begin{pmatrix} 3 & 3 & 8 \\ 3 & 4 & 6 \\ 0 & 0 & 0 \end{pmatrix}$$

We first build a unimodular matrix U_0 from the pseudo unimodular matrix A:

$$U_0 = \begin{pmatrix} 3 & 3 & 8 \\ 3 & 4 & 6 \\ 4 & 6 & 7 \end{pmatrix} \qquad U_0^{-T} = \begin{pmatrix} -8 & 3 & 2 \\ 27 & -11 & -6 \\ -14 & 6 & 3 \end{pmatrix}$$

The following matrices U_i correspond to the five steps of the algorithm described in the theorem 11.

$$U_1 = \begin{pmatrix} -8 & 3 & 2 \\ 27 & -11 & -6 \\ 5 & -2 & -1 \end{pmatrix} \qquad U_1^{-T} = \begin{pmatrix} -1 & -3 & 1 \\ -1 & -2 & -1 \\ 4 & 6 & 7 \end{pmatrix}$$

$$U_2 = \begin{pmatrix} -1 & -3 & 1 \\ -1 & -2 & -1 \\ 1 & 2 & 0 \end{pmatrix} \qquad U_2^{-T} = \begin{pmatrix} 2 & -1 & 0 \\ 2 & -1 & -1 \\ 5 & -2 & -1 \end{pmatrix}$$

$$U_3 = \begin{pmatrix} 2 & -1 & 0 \\ 2 & -1 & -1 \\ 5 & -2 & 1 \end{pmatrix} \qquad U_3^{-T} = \begin{pmatrix} -3 & -7 & 1 \\ 1 & 2 & -1 \\ 1 & 2 & 0 \end{pmatrix}$$

$$U_4 = \begin{pmatrix} -3 & -7 & 1 \\ 1 & 2 & -1 \\ 0 & 0 & 1 \end{pmatrix} \qquad U_4^{-T} = \begin{pmatrix} 2 & -1 & 0 \\ 7 & -3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$U_5 = \begin{pmatrix} 2 & -1 & 0 \\ 7 & -3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Thus the matrix A can be factorized as follows:

$$\begin{aligned} A &= A_6(A_5^T A_4)(A_3^T A_2)(A_1^T A) \\ &= \begin{pmatrix} -3 & -7 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & -5 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} -4 & -10 & 0 \\ 2 & 5 & 0 \\ 1 & 2 & 1 \end{pmatrix} \begin{pmatrix} 57 & 84 & 98 \\ -24 & -35 & -42 \\ -12 & -18 & -20 \end{pmatrix} \end{aligned}$$

The first matrix (A_6) can be easily factorized into a product of idempotent matrices (cf. lemma 10), and the three last matrices are idempotent.

5 Application in systolic arrays

The growing demand for high speed real-time signal and image processing has led to many new architectures. Very Large Scale Integration (VLSI) processor arrays have many useful properties that make them ideally suited for this class of problems, for example regular short interconnections, extensible design and simple hardware tuned to the application at hand. The problem of synthesizing VLSI arrays from a set of affine recurrent equations (SARE) has been extensively studied (cf. for example [8]). The algorithm is generally given as an SARE in an n dimensional index space. Each variable y_i may be defined by several equations (input, output and computation equations). A typical computation equation has the form:

$$y_i(p) = f_i(\ldots, y_j(Ap), \cdots) \qquad p \in D_i \tag{10}$$

where $p \in \mathbb{Z}^n$ is an *index point*, $A \in \mathbb{Z}^{n \times n}$ is an integer matrix, D_i is the *domain* of the equation and f_i is a strict, single-valued function. In Equation (10) the variable y_i at location p depends on another variable y_j produced at location Ap. A direct map of the problem space onto a systolic array would require a communication channel from location Ap to location p, which is technically unacceptable. Localization is a well-known technique [4] to transform the SARE describing the algorithm into an SARE which satisfies the locality constraints of systolic arrays. Intuitively, localization is a technique for moving the variable y_j from where it is produced (Ap) to where it is used (p). Thus we transform the SARE of the algorithm into another SARE which represents an acceptable systolic array.

If the matrix A is singular, the localization can be achieved by factoring A into a product of idempotent matrices $A = \prod_{i=1}^{m} B_i$. For example, assuming that we have only two variables y_i and y_j, Equation (10) becomes:

$$y_i(p) = f(y_j(B_1 B_2 \ldots B_m p)) \qquad p \in D_i$$

We can expand the recurrent equation by introducing m new variables Y_i:

$$\left\{ \begin{array}{rll} y_i(p) = & f(Y_m(B_m p)) & p \in D_i \\ Y_m(B_m p) = & Y_{m-1}(B_{m-1} B_m p) & p \in D_i \\ & \cdots & \\ Y_{i+1}(B_{i+1} \cdots B_m p) = & Y_i(B_i \cdots B_m p) & p \in D_i \\ & \cdots & \\ Y_1(B_1 \cdots B_m p) = & y_j(B_1 \cdots B_m p) & p \in D_i \end{array} \right. \tag{11}$$

We execute the renaming transformation $B_i B_{i+1} \cdots B_m$ on the variable Y_i:

$$
\begin{cases}
y_i(p) = f(Y_m(B_m p)) & p \in D_i \\
\quad\cdots & \\
Y_{i+1}(p) = Y_i(B_i p) & p \in B_{i+1} \cdots B_m D_i \\
\quad\cdots & \\
Y_1(p) = y_j(p) & p \in B_1 \cdots B_m D_i
\end{cases}
\tag{12}
$$

Remembering that B_i is an idempotent matrix, we have $B_i p = p$ if p belongs to the range space $R(B_i)$ of B_i, and:

$$Y_{i+1}(p) = Y_i(p) \qquad p \in R(B_i)$$

Similarly, for all the points $p \pm N(B_i)$ (where $N(B_i)$ is a vector in the null space of B_i), we have:

$$Y_{i+1}(p \pm N(B_i)) = Y_i(p) = Y_{i+1}(p) \qquad p \in R(B_i)$$

Thus the new variable $Y_{i+1}(p)$ is the variable $Y_i(p)$ pipelined along the direction of the null space of the matrix B_i. The SARE (12) can be written (assuming that B_m is the unit matrix):

$$
\begin{cases}
y_i(p) = f(Y_m(p)) & p \in D_i \\
\quad\cdots & \\
Y_{i+1}(p) = Y_i(p) & (p \in R(B_i)) \wedge (p \in B_{i+1} \cdots B_m D_i) \\
Y_{i+1}(p) = Y_{i+1}(p \pm N(B_i)) & (p \notin R(B_i)) \wedge (p \in B_{i+1} \cdots B_m D_i) \\
\quad\cdots & \\
Y_1(p) = y_j(p) & p \in B_1 \cdots B_m D_i
\end{cases}
\tag{13}
$$

The $\pm$ sign means that the new variable Y_{i+1} can travel along the null space in two directions. The correct sign is such that the dependency points toward the corresponding range space ($R(B_i)$).

6 Conclusion

In this paper, we have presented a proof that any $n \times n$ ($n > 2$) singular integer matrix can be factorized into a product of $3n+1$ integer idempotent matrices.

We have given an example demonstrating its application in the synthesis of systolic arrays.

Acknowledgments

We are grateful to the referee for very helpful comments. This work was supported in part by the Australian Academy of Science.

References

[1] J. A. Erdos, “On the product of idempotent matrices”, *Glasgow Mathematical Journal*, Vol. 8, 1967.

[2] J. M. Howie, “The subsemigroup generated by the idempotents of a full transformation semigroup”, *Journal of the London Mathematical Society*, Vol. 41, 1966.

[3] T. J. Laffey, ”Factorizations of integer matrices as products of idempotents and nilpotents”, *Linear Algebra and its Applications*, Vol 120, 1989.

[4] P. M. Lenders and S. Rajopadhye, ”Multirate VLSI and their Synthesis”, *IEEE Transactions on Computers*, May 1997.

[5] M. Newman, “Integral Matrices”, *Academic Press*, 1972.

[6] S. Rajopadhye, “Synthesizing systolic arrays with controls signals from recurrence equations”, Distributed Computing, May 1989.

[7] A. Schrijver, “Theory of Linear and Integer Programming”, *Wiley*, 1998.

[8] V. Van Dongen and P. Quinton, “Uniformization of Linear Recurrence Equations: A step towards the automatic synthesis of systolic arrays”, *Proc. International Conference on Systolic Arrays*, 1988.