6-1-1994

Modular mappings of rectangular algorithms

Hyuk J. Lee
Purdue University School of Electrical Engineering

José A.B. Fortes
Purdue University School of Electrical Engineering

MODULAR MAPPINGS OF RECTANGULAR ALGORITHMS

HYUK J. LEE
JOSÉ A.B. FORTES

TR-EE 94-22
JUNE 1994

SCHOOL OF ELECTRICAL ENGINEERING
PURDUE UNIVERSITY
WEST LAFAYETTE, INDIANA 47907-1285

Modular mappings of rectangular algorithms*

Hyuk J. Lee and José A.B. Fortes
School of Electrical Engineering
Purdue University
W. Lafayette, IN 47907, USA

*This research was partially funded by the National Science Foundation under grant number CDA-9015696.

Abstract

Affine space-time mappings have been extensively studied for systolic array design and parallelizing compilation. However, there are practical important cases that require other types of transformations. This paper considers so-called modular mappings described by linear transformations modulo a constant vector. Sufficient conditions for these mappings to be one-to-one are investigated for rectangular domains of arbitrary dimensions. It is shown that a sufficient condition for a modular mapping to be one-to-one is that its (n x n) coefficient matrix T has entries $t_{ii} = \pm 1$ and $t_{ij} = 0$ for $i > j$ where $>$ is a total order on $\{1, 2, \cdots, n\}$, n = domain dimension. These conditions are strengthened and extended for particular types of rectangular domains and affine transformations modulo a constant vector. The results of this paper can be used to identify a space of valid modular mappings of specific algorithms into time and space. They are illustrated by examples which include Cannon's matrix multiplication algorithm.

Contents

1 Introduction 1

2 Modular time-space transformation 2

3 Generator matrices 6

4 Sufficient conditions on generator matrices for one-to-cone modular transformations 8

5 Sufficient conditions on transformation matrices for one-to-one modular transformations 12

6 Extensions 16

6.1 Permutations of the boundary vector 16

6.2 Identical entries in the boundary vector 17

6.3 Necessary and sufficient conditions 19

6 . Affine modular mappings 19

6.j Examples 20

7 Conclusion 23

8 Appendix 25

1 Introduction

Many techniques of systolic array design and parallelizing compilation are based on systematic mappings of index sets of regular algorithms into time and space. Most studies have concentrated on affine mappings for which a large body of theory and practical techniques have been accumulated. This paper considers a different class of mappings described by linear transformations modulo a constant vector(called modular mappings). Sufficient conditions for these mappings to be one-to-one are derived. They provide a basis for identifying a space of valid modular time-space mappings of specific regular algorithms.

A large number of systolic arrays for linear recurrence algorithms can be derived systematically using affine space-time mappings(see for example [1]-[7] and references therein). Similarly, many parallel compiler optimized versions of nested loop programs result from such mappings. However, there are practical important cases that require other types of transformations. For example, Cannon's algorithm for matrix-matrix multiplication [8]does not result directly from an affine mapping [10],[12]. The corresponding mapping is modular and can be guessed but, to our knowledge, no systematic derivation has been provided for it. Partitioning mappings [9] and loop rotations [10] also correspond to modular transformations. Systematic derivation of programs that take advantage of wrap-around connectivity in networks such as rings and torus may also require modular transformations. These mappings can be used to identify equally efficient processor array algorithms that require distinct data distributions. They may also be necessary to mechanically derive other involved mappings such as those used in [11]- [14].

The rest of the paper is organized as follows. Section 2 defines and characterizes modular mappings. Sections **3,** 4, and 5 derive sufficient conditions for a modular mapping to be one-to-one. Section **3** studies the generators of the set of points that are mapped into $\bar{0}$ by a modular transformation. Necessary and sufficient conditions on these generators for injectivity of transformations are discussed in Section 4 (similar conditions appeared in [19]). Section 5 establishes the relation between a modular mapping and the generator matrix induced by it. This relation is then used to derive sufficient conditions for the

modular mapping to be one-to-one. Section 6 extends the results to affine mappings and strengthens injectivity conditions for special types of domains. To illustrate the results of this paper, Section 6 also includes examples of modular mappings for $(n \times m)$ matrix multiplication. Section 7 concludes the paper.

2 Modular time-space transformation

In this section, *modular time-space transformations* are defined in terms of two operations, a linear transformation and a 'mod' operation.

Definition 1 (Modular function): A modular function, $T_{\bar{m}} : \boldsymbol{Z^n} \rightarrow \mathrm{Z}^k$, is a mapping of tht: form:

$$T_{\bar{m}}(\bar{j}) = \begin{bmatrix} T(1) \cdot \bar{j}_{(mod\ m_1)} \\ T(2) \cdot \bar{j}_{(mod\ m_2)} \\ \vdots \\ T(k) \cdot \bar{j}_{(mod\ m_k)} \end{bmatrix} \tag{1}$$

where $T(i)$ is a row vector. The matrix $T = \begin{bmatrix} T(1) \\ \vdots \\ T(k) \end{bmatrix}$ and vector $\bar{m} = (m_1, \cdots, m_k)^T$ are called the *transformation matrix* and *modulus vector,* respectively. □

Definition 2 (Modular time-space transformation): A *modular time-,spacetransformation,* $T_{\bar{m}}$, is a modular function that is *injective* when its domain is restricted to the index set J of an algorithm, i.e., $T_{\bar{m}} : \mathrm{J} \rightarrow Z^k$ is injective. □

Any (k x n) transformation matrix T and k dimensional modulus vector $\bar{m}$ can make a modular function. However, in order for any modular function to be a modular transformation of a given algorithm, T and m must be carefully chosen so that the transformation is injective when its domain is restricted to the index set of the algorithm. This paper considers only the case when $n = k$.

Let $\bar{u}$ and $\bar{v}$ be two vectors with the same number of elements. The notation $\bar{u}_{(mod\ \bar{v})}$ denotes a vector $((u_1)_{(mod\ v_1)}, (u_2)_{(mod\ v_2)}, \ldots, (u_n)_{(mod\ v_n)})$. Therefore the modular func-

tion can be described as $T_{\bar{m}}(\bar{j}) = (T\bar{j})_{(mod\ \bar{m})}$.

Linear transformations can be considered particular cases of modular mappings for large enough moduli and finite domains. The need for modular transformations with "small" moduli arises for several reasons. Regarding space allocation, they are well suited for processor arrays with wrap-around connections which are mathematically captured by the "mod" operation. Similarly, they are well suited to derive schedules that (re)order antichains of computations and/or chains of commutative operations.

Another interesting characteristic of modular mappings is that they can potentially yield many equally efficient schedules. Suppose that the index set of a given algorithm is rectangular (a precise definition is given in Definition *3)*. Then, it is possible to choose the modulus vector $\bar{m}$ that tightly bounds the index set, i.e., any p $\in Z^n, \bar{0} \leq \bar{p} < \mathrm{m}$ is an element of the index set. Then, the index set is transformed into another rectangular set with the same cardinality. This means that no single processor is ever idle during the execution of the given algorithm. Hence, any valid modular transformation is optimal in the sense of processor utilization. Valid means that data dependencies and possibly other correctness constraints are satisfied.

Example 1: Consider the matrix-matrix multiplication algorithm.

```
DO i = 0,4
   DO j = 0,4
      DO k = 0,4
         c(i,j) = c(i,j) + a(i,k) × b(k,j)
CONTINUE
```

Cannon's algorithm is particularly efficient and frequently used in actual parallel processors whose interconnection network is a torus[15],[16]. In Cannon's algorithm, the elements of matrix *a* and b are initially aligned and multiplied by each other as shown in Figure 1. The next step is to shift matrix a to the left and matrix b up to neighbor processors where elementwise multiplication can take place again and its result can be

$i \backslash j$	0	1	2	3	4
0	$a_{0,0}/b_{0,0}$	$a_{0,1}/b_{1,1}$	$a_{0,2}/b_{2,2}$	$a_{0,3}/b_{3,3}$	$a_{0,4}/b_{4,4}$
1	$a_{1,1}/b_{1,0}$	$a_{1,2}/b_{2,1}$	$a_{1,3}/b_{3,2}$	$a_{1,4}/b_{4,3}$	$a_{1,0}/b_{0,4}$
2	$a_{2,2}/b_{2,0}$	$a_{2,3}/b_{3,1}$	$a_{2,4}/b_{4,2}$	$a_{2,0}/b_{0,3}$	$a_{2,1}/b_{1,4}$
3	$a_{3,3}/b_{3,0}$	$a_{3,4}/b_{4,1}$	$a_{3,0}/b_{0,2}$	$a_{3,1}/b_{1,3}$	$a_{3,2}/b_{2,4}$
4	$a_{4,4}/b_{4,0}$	$a_{4,0}/b_{0,1}$	$a_{4,1}/b_{1,2}$	$a_{4,2}/b_{2,3}$	$a_{4,3}/b_{3,4}$

Figure 1: Initial data alignment of Cannon's algorithrn.

added to the current value of $c(i, \mathbf{j})$. This shift and multiply step is repeated until all elements in a row of matrix a are multiplied by all elements in a column of matrix b. Cannon's algorithm can be described by the following program where $a'(i, \mathbf{j})$ and $b'(i, \mathbf{j})$ are aligned copies of $a(i, \mathbf{j})$ and $b(i, \mathrm{j})$ according to the expressions $a'(i, \mathbf{j}) = a(i, (\mathrm{i} + j)_{mod\ 5})$, $b'(i, j) = b((i + j)_{mod\ 5}, j)$.

DO $t = 0, 4$
  DOALL $i = 0, 4$
    DOALL $j = 0, 4$
      $c(i, j) = c(i, j) + a'(i, j) \times b'(i, j)$
      $a'(i, j)^t = a'(i, (j + 1)_{mod\ 5})^{t-1}$
      $b'(i, j)^t = b'((i + 1)_{mod\ 5}, j)^{t-1}$
CONTINUE

It is not possible to use affine mappings to derive Cannon's algorithm from the sequential matrix-matrix multiplication algorithm. Instead, the following modular transformation is required.

$$T_{\bar{b}}(i, j, k) = (\begin{pmatrix} -1 & -1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} (i, j, k))_{(mod\ (5,5,5)))}. \qquad (2)$$

This :modular transformation yields the following program (which is equivalent to the previously described program for Cannon's algorithm):

```
DO t = 0,4
    DOALL p1 = 0,4
        DOALL p2 = 0,4
            i = p1
            j = p2
            k = (t + p1 + p2)mod 5
            c(i, j) = c(i, j) + a(i, k) x b(k, j)
CONTINUE
```

The advantages mentioned above come from the 'mod' operation. However, it also causes drawbacks. One of them is that it is not trivial to check whether a modular function is injective. Therefore, it is necessary to carefully choose the transformation matrix T and the modulus vector m. Sufficient conditions on the transformation matrix of modular functions are therefore desirable.

A modular function induces the following equivalence relation on its domain: $\bar{p}$ and $\bar{q}$ are equivalent if and only if $T_{\bar{m}}(\bar{p}) = T_{\bar{m}}(\bar{q})$. It is easy to verify that this relation satisfies the reflexive, symmetric, and transitive properties [17]. A modular function is injective if and only if there do not exist two equivalent index points. It is not clear how this condition can be tested efficiently in the general case. If it is assumed that a given index set is rectangular, then it becomes much simpler to check the existence of equivalent points.

Definition 3 (Rectangular index set and boundary vector): An index set J is rectangular and denoted $J_{\bar{b}}$ if

$$J = \{\bar{j} \in Z^n | \bar{0} \leq \bar{j} < b). \tag{3}$$

The vector b is called the boundary vector of $J_{\bar{b}}$. o.

In the above definition, the lower bound is assumed to be zero. When this is not the case it is always possible to translate the set so that the lower bound becomes zero. Therefore, the ensuing discussions and results are valid for arbitrary rectangular index

sets. A non-rectangular set must either be transformed into a rectangular one by a change of basis or, if not possible, extended to the minimal rectangular set that includes it. This does not imply that the transformed algorithm has poor efficiency. Consider processor array algorithms, i.e., algorithms that have already been mapped into a processor array. Assume such an algorithm executes in x units of time on a two dimensional processor array of p_1 x p_2 processors. One can think of this algorithm as having a rectangular index set of size x x p_1 x p_2. Possibly this index set includes points where processors are idle. However, as mentioned just before Example 1, a modular transformation with modulus vector (x, p_1, p_2) will yield new algorithms that are as optimal as the original one. This may be necessary, for example, to identify algorithms that accept distinct data distributions with equal efficiency.

3 Generator matrices

This section investigates conditions for injectivity of a modular function when the domain is rectangular. These conditions are valid only for the case when the modulus vector equals the boundary vector of the domain, i.e., m = b. Some other cases are discussed in Section 6.

Lemma 1: Let $J_{\bar{b}}$ be a rectangular index set with a boundary vector $\bar{b}$. Let $\hat{J} = \{\bar{p} \in Z^n | -b < \bar{p} < b\}$. A modular function $T_{\bar{b}}$ is injective if and only if

$$T_{\bar{b}}(\bar{p}) \neq \bar{0} \text{ for } all \ p \in \hat{J} \text{ except } \bar{p} = \bar{0} \ \square \tag{4}$$

Lemma 1 makes it possible to check the injectivity of a modular function by examining points equivalent to $\bar{0}$. Therefore, the set of integer points that are equivalent to zero, i.e., the equivalence class

$$S^0 = \{p \in Z^n | T_{\bar{b}}(\bar{p}) = 0\} \tag{5}$$

is studied next. In the appendix, it is proven that S^0 is a module [1] and there exist n points $\bar{g}_i, i = 1, \cdots, n$ that generate the set S^0, i.e., every element in S^0 can be represented

[1] A module is very much like a vector space except that the scalars need not form a field(set of real numbers) but need only form a ring(set of integers).

by a. (integer) linear combination of $\bar{g}_i s$ [17]. These points $\bar{g}_i s$ are the *generators* of the class S^0 and G, a matrix whose i^{th} column is **g;,** is the *generator matrix* of S^0 induced by the modular function $T_{\bar{b}}$. *A* modular function that induces the generators is implicitly represented by a generator matrix.

There are many generator matrices that generate the same set S^0. Therefore, the following lemma investigates the class of generators that generate the same set S^0.

Lemma 2: Let $J_{\bar{b}}$ be a rectangular index set with a boundary vector b. Let $T_{\bar{b}}$ be a modular function of the index set $J_{\bar{b}}$. Let $G \in Z^{nxn}$ be a generator matrix. **A** new matrix $G' \in Z^{nxn}$ is also a generator matrix if and only if there exists a unimodular matrix $U \in Z^{nXn}$ such that $G' = GU$.

It is said that matrices G and G' are *(right) equivalent* if there exists a unimodular matrix U such that $G' = GU$[18]. Lemma 2 shows that all right equivalent matrices generate the same set S^0.

Example 2: Consider an index set $J_{\bar{b}}$ with the boundary vector b ==$(4,3)^T$. Suppose that a modular function is

$$T_{\bar{b}}(\bar{j}) = (\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \bar{j})_{(mod\ (4,3))}. \tag{6}$$

Then, $G = \begin{pmatrix} 4 & 1 \\ 0 & 3 \end{pmatrix}$ is a generator matrix of the set S^0. For any unimodular matrix U, GU is also a generator matrix of S^0. For examples, the unimodular matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, and $\begin{pmatrix} 0 & -1 \\ 1 & 4 \end{pmatrix}$ yield the new generator matrices $\begin{pmatrix} 4 & 5 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 5 & 1 \\ 3 & 3 \end{pmatrix}$, and $\begin{pmatrix} 1 & 0 \\ 3 & 12 \end{pmatrix}$, respectively. □

4 Sufficient conditions on generator matrices for one-to-one modular transformations

In this section, Lemma 3 provides sufficient conditions on a generator matrix that guarantee satisfaction of the injectivity condition on $T_{\bar{b}}$ expressed by Lemrna 1. It is assumed that the modulus vector is the same as the boundary vector of an index set (Section 6 considers the case when the modulus vector results from a permutation of the entries of the boundary vector). Lemma 3 restates Theorem 1 of [19] in the terminology of this paper. The proof in the appendix is very similar to that of [19].

Lemma *3:* Let $J_{\bar{b}}$ be a rectangular index set with a boundary vector b. Let $T_{\bar{b}}$ be a modular function of the index set $J_{\bar{b}}$ and G be a corresponding generator matrix. $T_{\bar{b}}$ is injective if G satisfies the following equations:

1. $g_{ii} = b_i$
2. $g_{ij} = 0$ if $i > j$ □

Ir. the condition of Lemma 3, the n^{th} row of the generator matrix should be all zeros except g_{nn}. For the $(n-1)^{th}$ row, all entries should be zero except the last two entries, $g_{(n-1)(n-1)}$ and $g_{(n-1)n}$. Among these two entries, $g_{(n-1)(n-1)}$ should be b_{n-1}, but $g_{(n-1)n}$ can be chosen arbitrarily in order to obtain a modular function. Similarly, in the $(n-i)'th$ row, $n-i$ entries are fixed and the remaining i entries can be chosen arbitrarily.

Example **3:** Consider an index set $J_{\bar{b}}$ with the boundary vector $\bar{b} = (4,3)^T$. The following generator matrices satisfy the condition of Lemma **3:**

$$G = \begin{pmatrix} 4 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 4 & 1 \\ 0 & 3 \end{pmatrix}. \tag{7}$$

However, the following generator matrices do not satisfy the condition of Lemma **3:**

$$G = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}, or \begin{pmatrix} 4 & 1 \\ 1 & 3 \end{pmatrix}. \tag{8}$$

Figure 2 shows the relationship between the generators and the equivalence relation. Figure 2 is for the case of $G = \begin{pmatrix} 4 & 0 \\ 0 & 3 \end{pmatrix}$. The shaded rectangle represents the original index set. All small circles represent the points equivalent to zero. Among them, two black circles represent the generator $(4,0)^T$ and $(0,3)^T$. Each small circle is associated with a rectangle that represents the coset of the original index set. Thus, each point in a rectangle corresponds to an index point and each rectangle can be considered as a copy of the original index set. Figures 2 (b),(c), and (d) show the case of

$$G = \begin{pmatrix} 4 & 1 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}, \text{ and } \begin{pmatrix} 4 & 1 \\ 1 & 3 \end{pmatrix}, \tag{9}$$

respectively. In Figures 2 (c) and (d), there are points which are included in two different rectangles, e.g. , those in the upper left corners of the re tangles. These points are identified by the symbol x. Since these points are equivalent, the corresponding modular functions are not injective. □

Example 4: Consider an index set $J_{\bar{b}}$ with the boundary vector $\bar{b} = (2,3,5)^T$. Then, the generator matrix $G = \begin{pmatrix} 2 & * & * \\ 0 & 3 & * \\ 0 & 0 & 5 \end{pmatrix}$ satisfies the condition in Lemma 3, where *s denote arbitrary integers that are not necessarily identical. □

In the condition of Lemma 3, there is more freedom in the choice of row i than in choosing row i + 1. However, this is not a necessary condition and permutations of rows yield other acceptable generator matrices. Let $x \succ y$ denote the fact there is more freedom of choice for row x than for row y. A more general form of the generator matrix that ,guarantees the injectivity of the modular transformation is provided in the next lemma. This turns out to a be necessary and sufficient condition as originally proven in Theorem 4 of [19].

Lemma 4: Let $J_{\bar{b}}$ be a rectangular index set with a boundary vector $\bar{b}$. Let $T_{\bar{b}}$ be a modular function of the index set $J_{\bar{b}}$. Let G be a generator matrix. Let $\succ$ be an arbitrary order on the set $\{1,2,\cdots,n\}$. $T_{\bar{b}}$ is injective if and only if G satisfies the following equations:

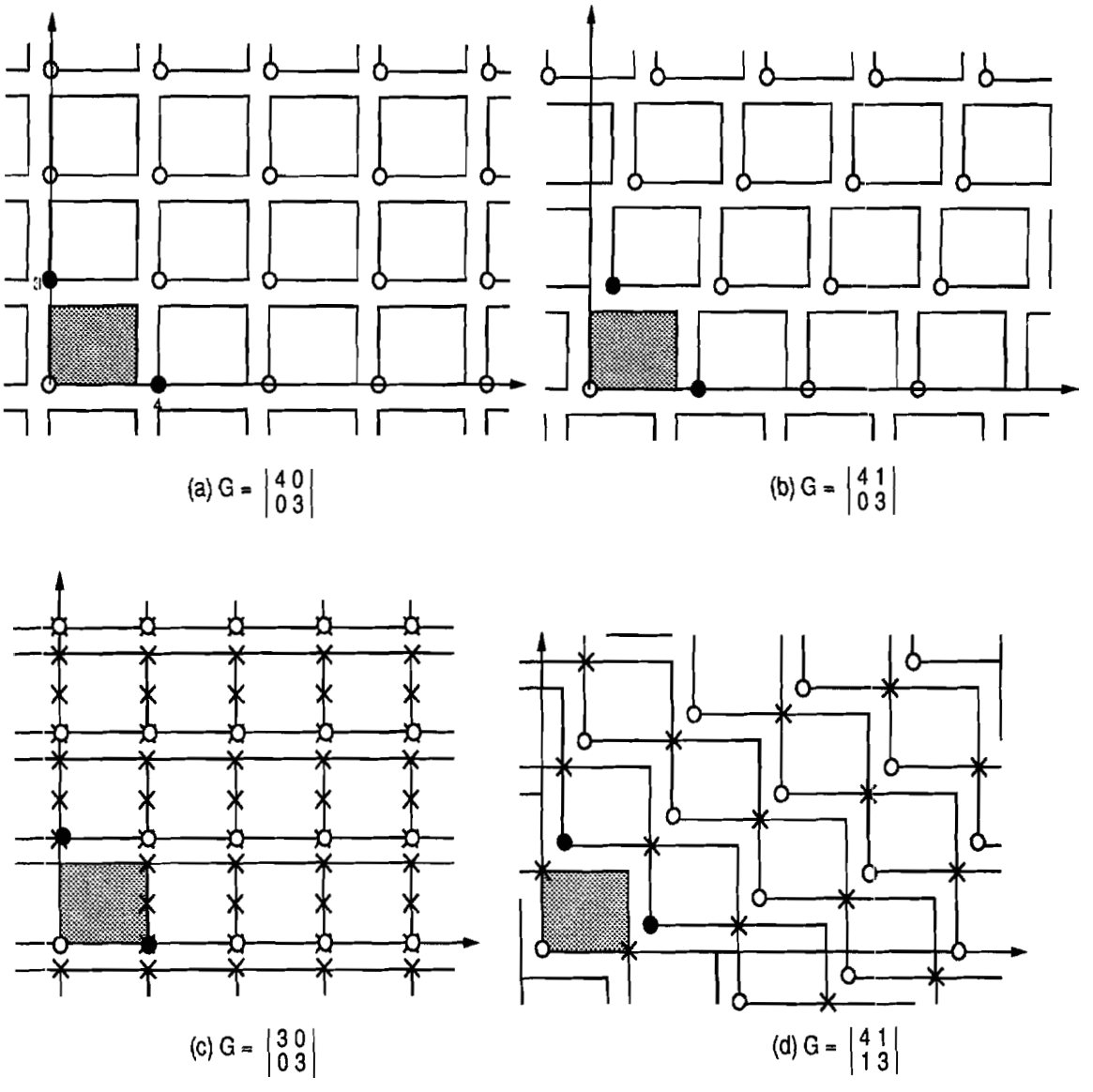

Figure 2: Index set, coset, and zero-equivalent points for distinct generators; (a) and (b) corresponds to injective mappings

1. $g_{ii} = b_i$

2. $g_{ij} = 0$ if $i \succ j$ □

Lemma 3 is a special case of Lemma 4 such that $i \succ$ j if $i >$ j. If there exist n rows, then there are $n!$ possible orders. Each order has a generator matrix that satisfies the condition of Lemma 1. Therefore, Lemma 4 provides $n!$ times more possibilities than Lemma 3.

Example 5: Consider an index set $J_{\bar{b}}$ with the boundary vector b $= (2,3,5)^T$. Example 4 shows that the generator matrix G $= \begin{pmatrix} 2 & * & * \\ 0 & 3 & * \\ 0 & 0 & 5 \end{pmatrix}$ guarantees the injectivity of the modular function. Lemma 4 shows that the following generator matrices also satisfy the injectivity condition:

$$\begin{pmatrix} 2 & * & * \\ 0 & 3 & 0 \\ 0 & * & 5 \end{pmatrix}, \begin{pmatrix} 2 & 0 & * \\ * & 3 & * \\ 0 & 0 & 5 \end{pmatrix}, \begin{pmatrix} 2 & 0 & 0 \\ * & 3 & * \\ * & 0 & 5 \end{pmatrix},$$

$$\begin{pmatrix} 2 & * & 0 \\ 0 & 3 & 0 \\ * & * & 5 \end{pmatrix}, or \begin{pmatrix} 2 & 0 & 0 \\ * & 3 & 0 \\ * & * & 5 \end{pmatrix} \square$$

Since any right equivalent matrices generate the same set S^0, it is possible to generalize the generator matrices that satisfy Lemma 4 into their right equivalence classes.

Corollary 1: Let $J_{\bar{b}}$ be a rectangular index set with a boundary vector $\bar{b}$. Let $T_{\bar{b}}$ be a modular function of the index set $J_{\bar{b}}$. Let G be a generator matrix. Let $\succ$ be an arbitrary order of the set $\{1,2,\cdot\cdot,n)$. $T_{\bar{b}}$ is one-to one if there exists a unimodular matrix U such that the matrix $G' = GU$ satisfies the following equations:

1. $g'_{ii} = b_i$

2. $g'_{ij} = 0$ if $i \succ j$,

where g'_{ij} represents the (i, $j)^{th}$ entry of the matrix G' □

Lemma 3 and Lemma 4 consider specific matrix forms of generator matrices. In other words, of all possible generator matrices for a given modular transformation, the ones of interest (if any exist) have the form specified by the above lemmata. Alternatively one may restate Lemma 3 and Lemma 4 in terms of Hermite Normal Form as in [19]. This is not necessary for the derivation of sufficient conditions for injectivity of modular mappings in the next section.

5 Sufficient conditions on transforrnation matrices for one-to-one modular transforrnations

This section investigates the relationship between generator matrices and transformation matrices. Based on this relationship, conditions for a transformation matrix to be a modular transformation are discussed.

Suppose that a modular function $T_{\bar{b}}$ has a generator matrix G that satisfies the conditions in Lemma 4. Then, the following equation should be satisfied:

$$(TG)_{mod\,\bar{b}} = [\bar{0}, \bar{0}, \cdots, \bar{0}]. \tag{10}$$

Then, there exists a matrix $H \in Z^{n \times n}$ such that

$$TG = \Theta H \tag{11}$$

whert: $\Theta = \begin{pmatrix} b_1 & 0 & \cdots & 0 \\ 0 & b_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \ldots & b_n \end{pmatrix}$. Without loss of generality, it is assumed that any two rows i and j of the generator matrix are such that $i \succ j$ if and only if $i > j$. Then, the generator matrix G satisfies

$$g_{ii} = b_{ii} \tag{12}$$

$$g_{ij} = 0, \quad if \quad i > j. \tag{13}$$

Eq. 11 can be divided into the following n x n equations:

$$\sum_k t_{ik} g_{kj} = \sum_k \theta_{ik} h_{kj} = b_i h_{ij} \quad for \;\; 1 \leq i, j \leq n, \tag{14}$$

where θ_{ik} and h_{kj} represent the $(i,k)^{th}$ entry of Θ and $(k,j)^{th}$ entry of H, respectively. Consider the following n equations:

$$\sum_k t_{1k} g_{kj} = b_1 h_{1j} \quad \textbf{for} \;\; 1 \leq j \leq n. \tag{15}$$

For $j = 1$, Eq. 15 becomes

$$t_{11} g_{11} = b_1 h_{11}. \tag{16}$$

Since $g_{11} = b_1$, we obtain

$$t_{11} = h_{11}. \tag{17}$$

Consider the following n equations:

$$\sum_k t_{2k} g_{kj} = b_2 h_{2j} \quad for \;\; 1 \leq j \leq n. \tag{18}$$

For $j = 1$, Eq. 18 becomes

$$t_{21} g_{11} = t_{21} b_1 = b_2 h_{21}. \tag{19}$$

Since the necessary condition of interest in this section should be generally applicable, it should include the case when b_1 and b_2 are relatively prime. In this case, we have either

$$b_2 \backslash t_{21} \tag{20}$$

or

$$t_{21} = h_{21} = \mathbf{0}. \tag{21}$$

Suppose that b_2 divides t_{21}. Then, t_{21} should be very large. In addition, it is desirable that the entries of the transformation matrix be independent of $b_i s$. Hence, Eq. **21** is a better choice than Eq. **20.**

For $j = 2$, Eq. **18** becomes

$$t_{21} g_{12} + t_{22} g_{22} = b_2 h_{22}. \tag{22}$$

Since $t_{21} = 0, g_{22} = b_2$, we obtain

$$t_{22} = h_{22}. \tag{23}$$

Claim that the transformation matrix T should satisfy the following equations:

$$t_{ij} = 0 \ \ if \ \ i > j, \tag{24}$$

for i = $1, \cdots, l-1$. Then, consider the following n equations:

$$\sum_k t_{lk} g_{kj} = b_l h_{lj} \ \ \textbf{for} \ \ 1 \leq \mathrm{j} \leq n. \tag{25}$$

For $j < 1$, Eq. **25** becomes

$$\sum_{k=l}^{j-1} t_{lk} g_{kj} + t_{lj} b_j = b_l h_{lj}. \tag{26}$$

For $j = 1$, Eq. 26 becomes

$$t_{l1} b_1 = b_l h_{l1} \tag{27}$$

Since b_1 and b_l can be relatively prime, we have

$$t_{l1} = h_{l1} = 0. \tag{28}$$

For $\mathrm{j} = 2$, **Eq.** 26 becomes

$$t_{l2} b_2 = b_l h_{l2}. \tag{29}$$

Therefore, $t_{l2} = h_{l2} = 0$. Similarly, we obtain

$$t_{lj} = h_{lj} = 0, \tag{30}$$

for all $j = 1, \cdots, l-1$. For $\mathrm{j} = \mathrm{l}$, Eq. 26 becomes

$$t_{ll} b_l = b_l h_{ll}, \tag{31}$$

and

$$t_{ll} = h_{ll}. \tag{32}$$

Therefore, by induction, it is proven that **Eq. 24** is necessary for all rows of the transformation matrix. Lemma 6 shows that this is also a sufficient condition (Lemma 5 is necessary for proving Lemma 6).

Lemma 5: Let T be an $n \times n$ matrix and $\succ$ be an arbitrary order on the set $\{1, 2, \ldots, n)$. Suppose that T satisfies the following equations:

1. $$t_{ii} = \pm 1, \tag{33}$$
2. $$t_{ij} = 0 \quad if \ i \succ j. \tag{34}$$

Let t_{ij}^{-1} be the $(i,j)^{th}$ entry of the inverse of T. Then, t_{ij}^{-1} satisfies the following equations:

3. $$t_{ii}^{-1} = \pm 1, \tag{35}$$
4. $$t_{ij}^{-1} = 0 \quad \textbf{if} \ i \succ j. \qquad \square \tag{36}$$

Lemma 6: Let $J_{\bar{b}}$ be a rectangular index set with a boundary vector $\bar{b}$. Let $T_{\bar{b}}$ be a modular function of the index set $J_{\bar{b}}$. Let $\succ$ be an arbitrary order on the set $\{1, 2, \cdots, n)$. There exists a generator matrix G that satisfies the conditions in Lemma 4, if its transformation matrix T satisfies the following equations:

1. $$t_{ii} = \text{f l}\,, \tag{37}$$
2. $$t_{ij} = 0 \quad if \ i \succ j \qquad \square \tag{38}$$

Lemma 6 shows that Eq. 37 and Eq. 38 are sufficient conditions for a transformation matrix to induce a generator matrix that satisfies the conditions in Lemma 4. Since the conditions in Lemma 4 guarantee the injectivity of the modular function, Eq. 37 and Eq. 38 are sufficient conditions for the modular function to be injective as stated by the following theorem.

Theorem 1: Let $J_{\bar{b}}$ be a rectangular index set with a boundary vector 6. Let $T_{\bar{b}}$ be a modular function of the index set $J_{\bar{b}}$. Let $\succ$ be an arbitrary order on the set $\{1, 2, \ldots, n)$. $T_{\bar{b}}$ is a modular transformation if its transformation matrix T satisfies the following equations:

1. $$t_{ii} = 41, \tag{39}$$
2. $$t_{ij} = 0 \quad if \ i \succ \mathbf{j} \qquad \square \tag{40}$$

Example 6: Consider an index set $J_{\bar{b}}$ with the boundary vector $\mathrm{b} = (2, 3, 5)^T$. Lemma 6 shows that the following transformation matrices guarantee the modular function to

be injective:

$$\begin{pmatrix} \pm 1 & * & * \\ 0 & \pm 1 & * \\ 0 & 0 & \pm 1 \end{pmatrix} \begin{pmatrix} \pm 1 & * & * \\ 0 & \pm 1 & 0 \\ 0 & * & \pm 1 \end{pmatrix}, \begin{pmatrix} \pm 1 & 0 & * \\ * & \pm 1 & * \\ 0 & 0 & \pm 1 \end{pmatrix},$$
$$\begin{pmatrix} \pm 1 & 0 & 0 \\ * & \pm 1 & * \\ * & 0 & \pm 1 \end{pmatrix}, \begin{pmatrix} \pm 1 & * & 0 \\ 0 & \pm 1 & 0 \\ * & * & \pm 1 \end{pmatrix}, or \begin{pmatrix} \pm 1 & 0 & 0 \\ * & \pm 1 & 0 \\ * & * & \pm 1 \end{pmatrix} \square$$

6 Extensions

6.1 Permutations of the boundary vector

Theorem 1 provides conditions on the transformation matrix which guarantee the modular Function to be injective. In this theorem, the modulus vector of a modular function is the same as the boundary vector of an index set, i.e. m is equal to b. This condition can be generalized to the case when the modulus vector results from a permutation of the entries of the boundary vector. A modular function is injective if the rows of the transformation matrix correspond to a permutation of the rows of the transformation matrix that yields an injective modular mapping $T_{\bar{b}}$ and this permutation is the same as the permutation of b that yields the modulus vector.

Example 7: Consider an index set $J_{\bar{b}}$ with the boundary vector $\bar{b} = (2,3,5)^T$. In Example 6, six types of the transformation matrices are found. Among those transformations, consider

$$T_{\bar{m}}(\bar{j}) = (\begin{pmatrix} \pm 1 & * & * \\ 0 & \pm 1 & 0 \\ 0 & * & \pm 1 \end{pmatrix} \bar{j})_{(mod\ (2,3,5))}, \tag{41}$$

i.e. the order is such that $2 \succ 3 \succ 1$. Suppose that a new modulus vector $(2,5,3)^T$ is needed. In this case, it is necessary to interchange the second and the third row of the transformation matrix. Hence, we obtain the following transformation:

$$T_{\bar{m}}(\bar{j}) = (\begin{pmatrix} \pm 1 & * & * \\ 0 & * & \pm 1 \\ 0 & \pm 1 & 0 \end{pmatrix} \bar{j})_{(mod\ (2,5,3))}. \tag{42}$$

For other permutations, we obtain the following transformations:

$$(\begin{pmatrix} 0 & \pm 1 & 0 \\ \pm 1 & * & * \\ 0 & * & \pm 1 \end{pmatrix} \bar{j})_{(mod\ (3,2,5))}, (\begin{pmatrix} 0 & \pm 1 & 0 \\ 0 & * & \pm 1 \\ \pm 1 & * & * \end{pmatrix} \bar{j})_{(mod\ (3,5,2))}, \tag{43}$$

$$(\begin{pmatrix} 0 & * & \pm 1 \\ \pm 1 & * & * \\ 0 & \pm 1 & 0 \end{pmatrix} \bar{j})_{(mod\ (5,2,3))}, or, (\begin{pmatrix} 0 & * & \pm 1 \\ 0 & \pm 1 & 0 \\ \pm 1 & * & * \end{pmatrix} \bar{j})_{(mod\ (5,3,2))}. \tag{44}$$

□

6.2 Identical entries in the boundary vector

Another extension of the injectivity condition deals with the special case when there exist identical entries in the boundary vector and other entries have any value (including the case when they are relatively prime). For this particular type of index sets, it is possible to obtain more general conditions. This case often occurs in real computations (See Example 1) and is easy to detect. Consider first the case when all entries of the boundary vector are identical. A sufficient condition for injectivity is that the transformation matrix be unimodular. This is a corollary(Corollary 2) to Lemma 7 dealing with the case when $\bar{b}$ has $m <$ n distinct entries discussed next.

Let $\mathbf{I} = \{1, 2, \cdots, n)$. Suppose that a boundary vector b has m different elements. Consider a partition of the set $\mathbf{I}$ defined as follows: $i, j \in \mathbf{I}$ are in the same block if and only if the i^{th} entry of b is equal to the j^{th} entry of b, i.e. $b_i = b_j$. Suppose that a boundary vector $\bar{b}$ has m different values. Then, the partition of the set $\mathbf{I}$ consists of m blocks, $\{I_{i_1}, \mathbf{I};,,\cdots, \mathbf{I};,)$. The numbering of the subscripts, $\{i_1, i_2, \cdots, i,)$, is defined as follows: Let $\succ$ be an order on the set $\mathbf{I}$. Then, $i_j = k$ for $k \in I_{i_j}$ and $k \succ k'$ for any $k' \in I_{i_j}, k' \neq k$.

The following example illustrates these concepts and notations.

Example 8: Consider a boundary vector $b = (1, 2, 3, 2, 1, 4)^T$. The elements of $\bar{b}$ have four distinct values, thus the set $\mathbf{I}$ can be partitioned into four blocks. Indices 1 and 5 are in the same block because their corresponding entries of $\bar{b}$ are same, i.e., $b_1 = b_5$.

Similarly, 2 and 4 are in the same block. Since b_3 is different from any other entry, **3** forms a one element block $\{3\}$. Similarly, 6 forms also a one element block $\{6\}$. Therefore, there exist four partitions of **I** as follows:

$$\{\{1,5\},\{2,4\},\{3\},\{6\}\}. \tag{45}$$

Consider an order $\succ$ such that i $\succ$ j if and only if i $>$ j. Since $5 \succ 1$, we can define the block $\{1,5\}$ as I_5. Similarly, we have $\{2,4\} = I_4, \{3\} = I_3$ and $\{6\} = I_6$. o.

Let $T^{i,j}$ denote the matrix whose entries are $t_{i,j}$, i $\in I_i$, j $\in I_j$ and preserves the relative positions of the entries, in other words, $T^{i,j}$ is the $|I_i|$ x $|I_j|$ matrix whose (k, l)th entry $t^{i,j}_{k,l}$ and $(k',l')^{th}$ entry $t^{i,j}_{k,l}$ are such that there exist $t_{i,j}$ and $t_{i',j'}$ for $i, i' \in I_i$ and j,$j' \in I_j$ and if i $<$ i' then k $<$ k' and if j $<$ j' then $l < 1'$.

Lemma 7: Let $J_{\bar{b}}$ be a rectangular index set with a boundary vector 6. Let $T_{\bar{m}}$ be a modular transformation of the index set $J_{\bar{b}}$. Let **{I;)**be a partition of the set $\{1,2,\cdots,n)$ and $\succ$ be an arbitrary order of the set $\{1,2,\cdots,n)$. $T_{\bar{m}}$ is a modular transformation if its transformation matrix satisfies

1. $|T^{i,i}| = \pm 1$,
2. $T^{i,j} = 0$, if $i \in I_i$, $i \succ j$ □

Corollary 2: Let $J_{\bar{b}}$ be a rectangular index set with a boundary vector 6. Suppose that all entries of the vector b are same. Let $T_{\bar{b}}$ be a modular function of the index set $J_{\bar{b}}$. Then $T_{\bar{b}}$ is a modular transformation if the transformation matrix is unimodular. □

If the index set is not square (i.e. $\exists i, j \mid b_i \neq b_j$), then it is easy to find a modular mapping whose transformation matrix is unimodular but that is not one-to-one. For example, modular mapping $(\begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix} \bar{j})_{mod\,(3,2)}$ is not one-to-one on the index set $\{(i,j)|0 \leq i \leq 2, 0 \leq j \leq 1)$.

6.3 Necessary and sufficient conditions

It is possible to identify necessary and sufficient conditions for injectivity of a modular mapping when all the entries of the boundary vector have the same value β: the mapping is injective if and only if the determinant of A and β are relatively prime. The proof originally from [20], is reproduced in the appendix. Corollary 2 of Lemma 7 also follows directly from this result. It is desirable to derive mappings that are either independent of β or parameterized by β. In this case, it is not clear whether it is practical to consider transformation matrices whose determinants differ from 1 and depend on the factors of β.

The conditions in Theorem 1 can be extended to

1. $(t_{ii}, b_i) = 1$,
2. $t_{ij} = 0$ if $i \succ j$,

where $(t_{ii}, b_i) = 1$ means that t_{ii} and b_i are relatively prime. In addition, the conditions in Lemma 7 can also be extended to

1. $(|T^{i,i}|, b_i) = 1$,
2. $T^{i,j} = 0$, if i $\in I_i$, $i \succ j$.

The proofs of these two extensions are provided in the appendix. Again it is not clear whether it is practical to consider transformations that satisfy these extended conditions but are not unimodular and have entries that depend on factors of the entries of b.

6.4 Affine modular mappings

Affine modular mappings are of the form $(\bar{c} + A\bar{x})_{mod\,\bar{b}}$ where $\bar{c}$ is an arbitrary integer constant vector. It is easy to show that all conditions derived for modular mappings are also valid for affine modular mappings.

6.5 Examples

Exarnple *1* (continued): Consider the matrix-matrix multiplication algorithm of Example 1 again. The index set is cubic, thus an arbitrary unimodular matrix can be chosen for the transformation matrix. However, there are additional constraints in choosing the schedule vector (the first row of the transformation matrix) to correctly sequence computations and remove data broadcasts. For this algorithm, the condition is that every element of the schedule vector should be different from 0. Hence, all unimodular matrices that satisfy this condition are valid transformation matrices and the corresponding modular mappings yield algorithms which are as efficient as Cannon's algorithm. For example, the following modular transformation

$$T_{\bar{b}}(i,j,k) = \left(\begin{pmatrix} -1 & -1 & 1 \\ -1 & 0 & 1 \\ 0 & -1 & 1 \end{pmatrix} (i,j,k) \right)_{(mod\ (5,5,5))} \tag{46}$$

yields the following program:

DO t = 0,4
  DOALL $p_1 = 0,4$
    DOALL $p_2 = 0,4$
      $i = (-t + p_1)_{mod\ 5}$
      $j = (-t + p_2)_{mod\ 5}$
      $k = (-t + p_1 + p_2)_{mod\ 5}$
      $c(i,\mathrm{j}) = c(i,\mathrm{j}) + a(i,\mathrm{k}) \times b(k,\mathrm{j})$

CON'I'INUE

The initial data alignment is the same as that of Cannon's algorithm. However, the data movement at each iteration is different. Arrays a, b and c are shifted south, east, and southeast directions, respectively. Note that all three arrays are slhifted in this case. Hence, it might increase the communication time although the efficiency in the sense of the processor utilization is the same as that of Cannon's algorithm.

$p_1 \backslash p_2$	0	1	2	3	4
0	$a_{0,0}/b_{0,0}$	$a_{1,1}/b_{1,0}$	$a_{2,2}/b_{2,0}$	$a_{3,3}/b_{3,0}$	$a_{4,4}/b_{4,0}$
1	$a_{1,0}/b_{0,1}$	$a_{2,1}/b_{1,1}$	$a_{3,2}/b_{2,1}$	$a_{4,3}/b_{3,1}$	$a_{0,4}/b_{4,1}$
2	$a_{2,0}/b_{0,2}$	$a_{3,1}/b_{1,2}$	$a_{4,2}/b_{2,2}$	$a_{0,3}/b_{3,2}$	$a_{1,4}/b_{4,2}$
3	$a_{3,0}/b_{0,3}$	$a_{4,1}/b_{1,3}$	$a_{0,2}/b_{2,3}$	$a_{1,3}/b_{3,3}$	$a_{2,4}/b_{4,3}$
4	$a_{4,0}/b_{0,4}$	$a_{0,1}/b_{1,4}$	$a_{1,2}/b_{2,4}$	$a_{2,3}/b_{3,4}$	$a_{2,4}/b_{4,4}$

Figure 3: Initial data alignment different from that of Cannon's algorithm.

Adding communication constraints on T (as in [9], for example) would yield algorithms that are equivalent to Cannon's algorithm in the sense of processor utilization and near neighbor communication. The only difference is on how input/output data arrays are distributed. Consider the modular time-space transformation is

$$T_b(i,j,k) = (\begin{pmatrix} -1 & -1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} (i,j,k))_{(mod\,(5,5,5)))}. \tag{47}$$

The program corresponding to this modular transformation is as follows:

DO $t = 0,4$

DOALL $p_1 = 0,4$

DOALL $p_2 = 0,4$

$i = (t + p_1 + p_2)_{mod\,5}$

$j = p_1$

$k = p2$

$c(i,\mathrm{j}) = c(i,j) + a(i,k)$ x $b(k,\mathrm{j})$

CONTINUE

The initial data alignment is shown as Figure 3. □

Example 9(parallelepiped index set): Consider the matrix-matrix multiplication algorithm for rectangular matrices. The index set is parallelepiped instead of cubic.

DO $i = 0, 4$
  DO $j = 0, 4$
    DO $k = 0, 1$
      $c(i,j) = c(i,j) + a(i,k) \times b(k,j)$
CONTINUE

Suppose that the following modular-mapping is used for the time-space transformation.

$$T_{\bar{b}}(i,j,k) = \left(\begin{pmatrix} -1 & -1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} (i,j,k) \right)_{(mod\ (2,5,5))}. \tag{48}$$

Then, the following program is derived:

DO $t = 0, 1$
  DOALL $p_1 = 0, 4$
    DOALL $p_2 = 0, 4$
      $i = p_1$
      $j = (t + p_1 + p_2)_{mod\ 5}$
      $k = (p_2)_{mod\ 2}$
      $c(i,j) = c(i,j) + a(i,k) \times b(k,j)$
CONTINUE

The initial distribution for this program is shown as Figure 4. Note that the computation is finished within two time units. □

$p_1 \backslash p_2$	0	1	2	3	4
0	$a_{0,0}/b_{0,0}$	$a_{0,1}/b_{1,1}$	$a_{0,0}/b_{0,2}$	$a_{0,1}/b_{1,3}$	$a_{0,0}/b_{0,4}$
1	$a_{1,0}/b_{0,1}$	$a_{1,1}/b_{1,2}$	$a_{1,0}/b_{0,3}$	$a_{1,1}/b_{1,4}$	$a_{1,1}/b_{0,0}$
2	$a_{2,0}/b_{0,2}$	$a_{2,1}/b_{1,3}$	$a_{2,0}/b_{0,4}$	$a_{2,1}/b_{1,0}$	$a_{2,0}/b_{0,1}$
3	$a_{3,0}/b_{0,3}$	$a_{3,1}/b_{1,4}$	$a_{3,0}/b_{0,0}$	$a_{3,1}/b_{1,1}$	$a_{3,1}/b_{0,2}$
4	$a_{4,0}/b_{0,4}$	$a_{4,1}/b_{1,0}$	$a_{4,0}/b_{0,1}$	$a_{4,1}/b_{1,2}$	$a_{4,0}/b_{0,3}$

Figure 4: Initial data alignment for rectangular index set.

7 Conclusion

The main contribution of this paper is the identification of sufficient conditions for a modular mapping to be injective. Injectivity is an important requirement for mappings of algorithms in time and space because it guarantees that no processor is assigned more than one computation at any given instant of time. Another desirable property is that it either be parameterized by the size of algorithm (e.g., by the number of iterations or the size of data arrays) or independent of it. This guarantees that the compiled mapping works for all instances of the program. The sufficient conditions derived in this paper meet this criteria. As discussed in Section 6, it is not clear that necessary and sufficient conditions (or weaker sufficient ones) can yield other parameterized mappings. Several extensions and further research of this topic are being pursued. Applications that are of interest include data distribution independence and commutative parallel processing. Mappings where the modulus vector is different from the boundary vector are also under investigation.

References

[1] Sun-Yuan Kung, VLSI *array processors,* Prentice-Hall, 1988.

[2] Paul Feautrier "Some efficient solutions to the affine scheduling problem "Part I: one-dimensional time," IBP/MASI, France, Tech. Rep. 92.28, May 1992.

[3] Guo-Jie Li and Benjamin W. Wah, "The design of optimal systolic arrays," *IEEE Trans. Comput.,* vol. C-34, pp. 66-77, Jan. 1985.

[4] Weijia Shang and José A.B. Fortes, "Time optimal linear schedules for algorithms with uniform dependencies," *IEEE Trans. Comput.,* vol. C-40, pp. 723-742, June 1.991.

[5] Alain Darte and Yves Robert, "Affine-by-statement scheduling of uniform loop nests over parametric domains," LIP, Ecole Normale Superieure de Lyon, France, Tech. Rep. 92-16, April 1992.

[6] Jürgen Teich and Lothar Thiele, "Control generation in the design of processor arrays," *Int. J. VLSI Signal Processing* vol. 3, no. 2, pp. 77-92, 1991.

[7] Patrice Quinton and Vincent Van Dongen, "The mapping of lineitr recurrence equations on regular arrays," *Int. J. VLSI Signal Processing,* vol. 1, no. 2, pp. 95-113, 1989.

[8] L.E. Cannon, "A cellular computer to implement the Kalman filter algorithm," Ph.D. dissertation, Montana State Univ., Bozeman, MT, 1969.

[9] Dan I. Moldovan and José A.B. Fortes, "Partitioning and mapping algorithm into fixed size systolic arrays," *IEEE Trans. Comput.,* vol. C-35, pp. 1-12, Jan. 1986.

[10] Michael Wolfe, "Massive parallelism through program restructuring," in *Proc. Frontiers '90: 3rd Symp. Frontiers Massively Parallel Computation,* pp. 407-415, Oct. 1990.

[11] Jorge L. Aravena and William A. Porter, "Nonplanar switchable arrays," *Circuits Systems and Signal Processing,* vol. 7, no. 2, pp. 213-234, 1988.

[12] Chris Scheiman and Peter Cappello, "A period-processor-time-minimal schedule for cubical mesh algorithms," in *Proc. Int. Conf. Application-Specific Array Processors,* pp. 261-272, Oct. 1993.

[13] Vincent Van Dongen, "From systolic to periodic array design," PhD thesis, Université Catholique de Louvain, Jan. 1991.

[14] José A.B. Fortes, "Algorithm reconfiguration techniques for gracefully degradable processor arrays," in *Proc. 1st Int. Conf. Systolic Arrays,* Oxford, pp. 259-268, July 1986.

[15] S. Lennart Johnsson, "Communication efficient basic linear algebra computations on hypercube architectures," *J. Parallel Distributed Computing,* vol 4, no. 2, pp. 132-172, April 1987.

[16] P. Bjørstad, F. Manne, T. Sørevik, and M. Vajteršic, "Efficient matrix multiplication on SIMD computers," *SIAM J. Matrix Anal. Appl.,* vol. 13, no. 1, pp. 386-401, Jan. 1992.

[17] John B. Fraleigh, *A first course in abstract algebra,* 3rd ed., Adclison-Wesley, 1982.

[18] William A. Adkins and Steven H. Weintraub, *Algebra: An approach via module theory,* New York: Springer-Verlag, 1992.

[19] Alain Darte, "Regular partitioning for synthesizing fixed-size systolic arrays," LIP, Ecole Normale Superieure de Lyon, France, Tech. Rep. 91-10, 1991; also in *Integration, The VLSI J.,* vol. 12, pp. 293-304, Dec. 1991.

[20] Richard Pinch, personal communication.

[21] Pierre Boulet and José A.B. Fortes, "Experimental evaluation of affine scheduling for matrix multiplication on the Maspar architecture," LIP, Ecole Normale Superieure de Lyon, France, Tech. Rep. 93-34, Oct. 1993.

8 Appendix

Definition A.1 (module): Let R be a ring. A *module (over R or R-moclule)* consists of an abelian group M together with an operation of external multiplication of each element of M by each element of R on the left such that for all p, q $\in M$ and $\alpha, \beta \in$ R, the following conditions are satisfied:

1. $(\alpha\bar{p}) \in$ M,
2. $\alpha(\bar{p} + \bar{q}) = \alpha\bar{p} + \alpha\bar{q}$,
3. $(\alpha + \beta)\bar{p} = \alpha\bar{p} + \beta\bar{q}$,
4. $(\alpha\beta)\bar{p} = \alpha(\beta\bar{p})$.

Lemma A.1: Let S^0 be the set of points equivalent to zero under a modular function $T_{\bar{m}}$ with $|T| = 1$. Let $S^0 = \{p \in Z^n | T_{\bar{m}}(\bar{p}) = \bar{0}\}$. Then, S^0 is a finitely generated module (over Z).

(Proof)

0. It is necessary to prove that S^0 is an abelian group under the vector addition(componentwise addition of two vectors.) Let p, q $\in S^0$, then

$$T_{\bar{m}}(\bar{p}) = T_{\bar{m}}(\bar{q}) = \bar{0}. \tag{49}$$

Thus', we have

$$(T\bar{p})_i = \text{aim; } \textit{for} \text{ some } a_i \in Z, \tag{50}$$

and

$$(T\bar{q})_i = \beta_i m_i \ \textit{for some} \ \beta_i \in Z, \tag{51}$$

where $(T\bar{q})_i$ and $(T\bar{q})_i$ represents the i^{th} entry of the vector $T\bar{p}$ and $T\bar{q}$, respectively. Thus, we have

$$(T(\bar{p} + \bar{q}))_i = (\alpha_i + \beta_i)m_i. \tag{52}$$

Hence,

$$T_{\bar{m}}(\bar{p} + \text{q}) = 0. \tag{53}$$

Therefore, $\bar{p} + \bar{q} \in S^0$. We also have $0 \in S^0$ which can be the identity of the vector addition. In addition, for any p, we have

$$\bar{p} + \bar{0} = \bar{0} + \bar{p} = \bar{p}. \tag{54}$$

Finally, it is necessary to prove that $-\bar{p} \in S^0$ for any p $\in S^0$. Since

$$(T(-\bar{p}))_i = (-T\bar{p})_i = -\alpha_i m_i, \tag{55}$$

we have

$$(-T\bar{p})_{mod\ \bar{m}} = \bar{0}. \tag{56}$$

Therefore, $-\bar{p} \in S^0$.

1. For any a $\in Z$, we have

$$T_{\bar{m}}(\alpha\bar{p}) = (T\alpha\bar{p})_{mod\ \bar{m}} = (\alpha T\bar{p})_{mod\ \bar{m}} = \bar{0}. \tag{57}$$

Therefore, $\alpha\bar{p} \in S^0$.

Conditions 2,3, and 4 are obviously true.

Let G = $T^{-1}\Theta$. Then, any point p such that $(T\bar{p})_{mod\,\bar{m}} = 0$ can be a (integer) linear combination of G. □

Lemma 1:

(Proof) (→) Suppose that $T_{\bar{b}}$ is injective, but there exists $\bar{p} \in \hat{J}$ such that $T_{\bar{b}}(\bar{p}) = 0$ and p ≠ $\bar{0}$. Consider a new point $\bar{p'}$ such that

$$\begin{aligned} p_i' &= \quad p_i \quad\quad if\ \ 0 \le p_i < b_i \\ p_i' &= \ p_i + b_i - 1 \quad if\ \ -b_i < p_i < 0 \end{aligned}$$

Then, $0 \le p_i' < b_i$ for all i. Thus, $\bar{p'}$ is an element of the index set J. Let $\bar{q} = \bar{p'} - \bar{p}$. Then, we obtain

$$\begin{aligned} q_i &= \quad 0 \quad\quad if\ \ 0 \le p_i < b_i \\ q_i &= \ b_i - 1 \quad if\ \ -b_i < p_i < 0 \end{aligned}$$

Thus, we have

$$\bar{0} \le \bar{q} < \bar{b}. \tag{58}$$

Therefore, $\bar{q}$ is also an element of the index set **J**.

From $T_{\bar{b}}(\bar{p}) = 0$, we obtain

$$T_{\bar{b}}(\bar{p} + \bar{q}) = (T(\bar{p} + \bar{q}))_{(mod\ \bar{b})} = T_{\bar{b}}(\bar{q}), \tag{59}$$

and

$$T_{\bar{b}}(\bar{p'}) = T_{\bar{b}}(\bar{q}) \tag{60}$$

This contradicts to the assumption that $T_{\bar{b}}$ is injective.

(←) Suppose that $T_{\bar{b}}$ is not injective. Then, there exist two index points $\bar{p}$ and q such that $T_{\bar{b}}(\bar{p}) = T_{\bar{b}}(\bar{q})$. Thus, we have

$$\bar{0} = T_{\bar{b}}(\bar{p}) - T_{\bar{b}}(\bar{q}) = (T\bar{p})_{(mod\ \bar{b})} - (T\bar{q})_{(mod\ \bar{b})} = (T\bar{p} - T\bar{q})_{(mod\ \bar{b})} = T_{\bar{b}}(\bar{p} - \bar{q}). \tag{61}$$

Let $\bar{r}$ = p − q. Then, we have

$$-b_i < r_i < b_i, i = 1, \cdots, n. \tag{62}$$

Thus, $\bar{r}$ is an element of the set $\hat{J}$. This contradicts the assumption. □

Lemma 2:

(Proof) (←) It suffices to show that for any vector g $\in S^0$, there exists $\bar{\alpha} \in Z^n$ such that

$$\bar{g} = G'\bar{\alpha}. \tag{63}$$

Since G is a generator matrix, there exists $\bar{\beta} \in Z^n$ such that

$$\bar{g} = G\bar{\beta}. \tag{64}$$

Let $\bar{\alpha} = U^{-1}\bar{\beta}$, then we have

$$\bar{g} = GUU^{-1}\bar{\beta}, \tag{65}$$

and

$$\bar{g} = G'\bar{\alpha}. \tag{66}$$

(→) Since G and G' are generator matrices, there exist V, $V' \in Z^{n\times n}$ such that

$$G' = \mathrm{GV} \text{ and } \mathrm{G} = G'V'. \tag{67}$$

Hence, $V' = V^{-1}$. Therefore, $|V'| = |V| = \pm 1$, i.e. unimodular. □

Lemma 3:

(Proof) This proof is similar to the proof of Theorem 1 in [19].

Suppose that the linear inequality,

$$-\bar{b} < \sum_i \alpha_i \bar{g}_i < \bar{b} \tag{68}$$

has only a trivial solution, i.e. all $\alpha_i's$ are equal to zero. Then, this implies that there does not exist any point equivalent to zero in $\hat{J} = \{\bar{p} \in Z^n | -b < \bar{p} < \bar{b}\}$ except $\bar{p} = 0$. Hence, $T_{\bar{b}}$ is injective. Therefore, it suffices to show that if there is an $a;$ that satisfies Eq. 68, then $\alpha_i = 0$. Eq. 68 can be divided into n inequalities:

$$\begin{aligned} -b_1 &< \textstyle\sum_{i=1}^n \alpha_i g_{1i} < b_1 \\ -b_2 &< \textstyle\sum_{i=1}^n \alpha_i g_{2i} < b_2 \\ &\vdots \\ -b_n &< \textstyle\sum_{i=1}^n \alpha_i g_{ni} < b_n \end{aligned} \tag{69}$$

Consider the last inequality:

$$-b_n < \sum_{i=1}^{n} \alpha_i g_{ni} < b_n. \tag{70}$$

Since

$$g_{ni} = 0 \ \ if \ \ i < n, \tag{71}$$

Inequality 70 becomes

$$-b_n < \alpha_n g_{nn} < b_n. \tag{72}$$

Sinct: $g_{nn} = b_n$, α_n should be equal to zero. Thus, the following '$n-1$' inequalities remain:

$$\begin{array}{rcl} -b_1 & < \sum_{i=1}^{n-1} \alpha_i g_{1i} < & b_1 \\ -b_2 & < \sum_{i=1}^{n-1} \alpha_i g_{2i} < & b_2 \\ \vdots & \vdots & \vdots \\ -b_{n-1} & < \sum_{i=1}^{n-1} \alpha_i g_{(n-1)i} < & b_{n-1}. \end{array} \tag{73}$$

These inequalities are exactly the same form as those of Eq. 69. Therefore, we obtain $\alpha_{n-1} = 0$ from the last inequality and reduce the last inequality to get '$n-2$' inequalities. By similar steps, it is possible to conclude that all $\alpha_i's$ are zero. □

Lemma 4:

(Proof) See proof of Theorem 4 in [19].

Lemma 5:

(Proof)

Since $\mathbf{I} = TT^{-1}$, we have the following n × n equations:

$$\sum_{\mathrm{k}} t_{ik} t_{kj}^{-1} = \delta_{ij} \ \text{ for } \ 1 \le i, j \le n. \tag{74}$$

Let $\{i_1, i_2, \cdots, i_n\}$ be the set of integers such that

$$i_j \in \mathrm{I}, \ \text{ for } \ j = 1, \cdots, n, \ \ i_k \succ i_l \ \text{ if } \ \mathrm{k} > l. \tag{75}$$

Then, $i_n \succ i_j$ for all $j \neq$ n. Consider the following n equations:

$$\sum_{k} t_{i_n k} t_{kj}^{-1} = \delta_{i_n j} \ \ for \ \ 1 \le j \le n. \tag{76}$$

Since

$$i_n \succ \mathrm{j} \quad \textit{for all } j \neq i_n, \tag{77}$$

Eq. 76 becomes

$$\sum_k t_{i_n k} t^{-1}_{kj} = t_{i_n i_n} t^{-1}_{i_n j} = \delta_{i_n j} \quad \textit{for } 1 \leq j \leq n. \tag{78}$$

For $j = i_n$, Eq. 78 becomes

$$t_{i_n i_n} t^{-1}_{i_n i_n} = \delta_{i_n i_n} = 1. \tag{79}$$

Since $t_{i_n i_n} = \pm 1$, we obtain $t^{-1}_{i_n i_n} = \pm 1$. For $\mathrm{j} \# i_n$, Eq. 78 becomes

$$t_{i_n i_n} t^{-1}_{i_n j} = \delta_{i_n j} = 0. \tag{80}$$

Thus, we have $t^{-1}_{i_n j} = 0$ for $\mathrm{j} \neq i_n$.

Consider the following n equations:

$$\sum_k t_{i_{n-1} k} t^{-1}_{kj} = \delta_{i_{n-1} j} \quad \textit{for } 1 \leq j \leq n. \tag{81}$$

Since $i_{n-1} \succ \mathrm{k}$ for all $\mathrm{k} \neq i_n, i_{n-1}$, we have

$$\sum_k t_{i_n k} t^{-1}_{kj} = t_{i_{n-1} i_n} t^{-1}_{i_n j} + t_{i_{n-1} i_{n-1}} t^{-1}_{i_{n-1} j} \tag{82}$$

$$= t_{i_{n-1} i_n} t^{-1}_{i_n j} + t^{-1}_{i_{n-1} j}. \tag{83}$$

For $j = i_{n-1}$, Eq. 81 becomes

$$t_{i_{n-1} i_n} t^{-1}_{i_n i_{n-1}} + t^{-1}_{i_{n-1} i_{n-1}} = \delta_{i_{n-1} i_{n-1}} = 1. \tag{84}$$

Since $t^{-1}_{i_n i_{n-1}} = 0$, we have $t^{-1}_{i_{n-1} i_{n-1}} = \pm 1$. For $j \neq i_n$ and $\neq i_{n-1}$, Eq. 81 becomes

$$t_{i_{n-1} i_n} t^{-1}_{i_n j} + t^{-1}_{i_{n-1} j} = \delta_{i_{n-1} j} = 0. \tag{85}$$

Sincr: $t^{-1}_{i_n j} = 0$ for $\mathrm{j} \neq i_n, i_{n-1}$, we have $t^{-1}_{i_{n-1} j} = 0$ for $\mathrm{j} \neq i_n, i_{n-1}$.

The remaining equations will be proved by induction.

Suppose that the conditions **3** and 4 are satisfied by $t_{i,j}$ for all $i \in \{i_n, \cdots, i_{m+1}\}$. Now, consider the following n equations:

$$\sum_k t_{i_m k} t^{-1}_{kj} = \delta_{i_m j} \quad \textit{for } 1 \leq j \leq n. \tag{86}$$

Since $t_{i_m i_m} = 1$ and $t_{i_m k} = 0$ if $i_m \succ$ k,

$$\sum_k t_{i_m k} t^{-1}_{kj} = t_{i_m i_m} t^{-1}_{i_m j} + \sum_{k \succ i_m} t_{i_m k} t^{-1}_{kj} \tag{87}$$

$$= t^{-1}_{i_m j} + \sum_{k \succ i_m} t_{i_m k} t^{-1}_{kj}. \tag{88}$$

For $j = i_m$, *Eq.* 86 becomes

$$t^{-1}_{i_m i_m} + \sum_{k \succ i_m} t_{i_m k} t^{-1}_{k i_m} = \delta_{i_m i_m} = 1. \tag{89}$$

Since $t^{-1}_{k i_m} = 0$ for k $\succ i_m$, we have $t^{-1}_{i_m i_m} = \pm 1$. For j such that $i_m \succ j$, **Eq. 86** becomes

$$t^{-1}_{i_m j} + \sum_{k \succ i_m} t_{i_m k} t^{-1}_{kj} = \delta_{i_m j} = 0. \tag{90}$$

Since $t^{-1}_{kj} = 0$ for k $\succ i_m \succ j$, we have $t^{-1}_{i_m j} = 0$ for j, $i_m \succ j$. □

Lemma 6:

(Proof) Let t^{-1}_{ij} be the $(i,j)^{th}$ entry of the inverse of the transformation matrix T. Claim that $G = T^{-1}\Theta H$ for $H = \mathbf{I}$ (i.e. $G = T^{-1}\Theta$) be the generator matrix that satisfies the cond tions of Lemma 4. To prove the claim, it suffices to prove the following facts:

1. $3H \in Z^{nXn}$ *such that* $TG = OH$, (91)
2. *for any g such that* $T\bar{g} = Oh$ *for* $h \in Z^n$, *3* $\bar{\alpha}$ *such that* $\bar{g} = G\bar{\alpha}$, *(92)*
3. *G satisfies two conditions in Lemma 4.* (93)

(1) Since $G = T^{-1}\Theta$, we have

$$TG = TT^{-1}\Theta = \Theta. \tag{94}$$

(2) Since $T = \Theta G^{-1}$, we have

$$T\bar{g} = \Theta G^{-1}\bar{g} = \Theta\bar{h}. \tag{95}$$

Therefore, we have

$$\bar{g} = G\Theta^{-1}\Theta\bar{h} = G\bar{h}. \tag{96}$$

(3) Consider a matrix $U = \begin{pmatrix} t_{11} & 0 & \cdots & 0 \\ 0 & t_{22} & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & t_{nn} \end{pmatrix}$. Since $t_{ii} = \pm 1$ for all $i = 1, \cdots, n$, U is a unimodular matrix. Let $G' = GU$. Let g_{ij}, g'_{ij} and θ_{ij} be the $(i,j)^{th}$ entries of the

matrices G, G' and O, respectively. Then, we have

$$g'_{ij} = g_{ij}t_{jj} = (\sum_k t_{ik}^{-1}\theta_{kj})t_{jj} = t_{ij}^{-1}b_j t_{jj}. \tag{97}$$

Lemma 5 shows that T^{-1} satisfies the following equations:

$$t_{ii}^{-1} = \pm 1 = t_{ii}, \tag{98}$$

$$t_{ij}^{-1} = 0, \ if \ i \succ j. \tag{99}$$

For $i = j$, we have

$$g'_{ii} = b_i, \ \ for \ \ a22 \ \ i, \ \ i = 1, \cdots, n. \tag{100}$$

For $i \succ j$, we have

$$g'_{ij} = t_{ij}^{-1}b_j = 0 \ \ if \ \ i \succ j. \tag{101}$$

Thus, G satisfies two conditions in Lemma 4. Therefore, 1,2, and 3, are all satisfied. □

Lemma A.2: Let $J_{\bar{b}}$ be a rectangular index set with a boundary vector $\bar{b}$. Let $T_{\bar{b}}$ be a modular function of the index set $J_{\bar{b}}$. Let G be the generator matrix. Let $\{I_i\}$ be a partition of the set $\{1, 2, \cdots, n)$ and $\succ$ be an arbitrary order of the set $\{1, 2, \cdots, n)$. $T_{\bar{b}}$ is injective if G satisfies the following equations:

1. $|G^{i,i}| = b_i^{|I_i|}$, all elements of $G^{i,i}$ are either 0 or multiples of b_i,
2. $G^{i,j} = 0$ if $i \succ j$.

(Proof) Without loss of generality, it is assumed that i $\succ$ j if $i >$ j. Then, it suffices to show that the following inequalities have only a trivial solution:

$$\begin{array}{lll} -b_1 & < \sum_{i=1}^n \alpha_i g_{1i} < & b_1 \\ -b_2 & < \sum_{i=1}^n \alpha_i g_{2i} < & b_2 \\ \vdots & \vdots & \vdots \\ -b_n & < \sum_{i=1}^n \alpha_i g_{ni} < & b_n \end{array} \tag{102}$$

Consider the last inequality:

$$-b_n < \sum_{i=1}^{n} \alpha_i g_{ni} < b_n. \tag{103}$$

Assume that there exists m partitions of the set $\{1, 2, \cdots, \mathrm{n}\}$ and $\mathrm{n} \in I_n$.
(Case 1: $|I_n| = 1$) We have $I_n = \{n\}$. Thus, $G^{n,n} = [g_{nn}]$ and $g_{nj} \in G^{n,j}$ for all $j \neq \mathrm{n}$. Moreover, we have

$$\mathrm{n} \succ \mathbf{j}, \textit{ for all } j \notin I_n. \tag{104}$$

Thus, $G^{n,j} = 0$ for all $j \notin I_n$. Since $g_{nj} \in G^{n,j}$ for all $j \neq n$, condition 2 shows that $g_{nj} = 0$ for all $\mathbf{j} \neq n$. Therefore, Eq. 102 becomes

$$-b_n < \alpha_n g_{nn} < b_n. \tag{105}$$

Sinct: $G^{n,n} = [g_{nn}]$ and $|G^{n,n}| = b_n$, we have $g_{nn} = b_n$. Therefore, $\alpha_n = 0$. Hence, we obtain '$n - 1$' equations which are exactly the same form as Eq. 102.

(Case 2: $|I_n| > 1$) Let $I_n = \{\mathrm{i}; i_2, \cdots, i_{|I_n|}\}$. Consider the following $|I_n|$ equations:

$$\begin{array}{lll} -b_n & < \sum_{i=1}^{n} \alpha_i g_{i_1 i} < & b_n \\ -b_n & < \sum_{i=1}^{n} \alpha_i g_{i_2 i} < & b_n \\ \vdots & \vdots & \vdots \\ -b_n & < \sum_{i=1}^{n} \alpha_i g_{i_{|I_n|} i} < & b_n \end{array} \tag{106}$$

For any $I_j \neq I_n$, we have $I_n \succ I_j$. Thus, condition 2 shows $g_{ij} = 0$ if $j \notin I_n$. Thus, Eq. 102 becomes

$$\begin{array}{lll} -b_n & < \sum_{i \in I_n} \alpha_i g_{i_1 i} < & b_n \\ -b_n & < \sum_{i \in I_n} \alpha_i g_{i_2 i} < & b_n \\ \vdots & \vdots & \vdots \\ -b_n & < \sum_{i \in I_n} \alpha_i g_{i_{|I_n|} i} < & b_n \end{array} \tag{107}$$

These equations can be combined into a new equation in a matrix form as follows:

$$-\bar{1} b_n < G^{n,n} \bar{\alpha}^n < \bar{1} b_n \tag{108}$$

where $\bar{\alpha}^n = (a;, \cdots, \alpha_{i_{|I_n|}})^T$. Since every element in $G^{n,n}$ is a multiple of b_m, $6''$ should be $\bar{0}$. Therefore, $|I_n|$ equations are removed from Eq. 102.

For both cases, there exist less equations which are exactly in the same form as Eq. 102. Hence, it is possible to proceed this step until all α_i's become zero. □

Lemma *A.3:* Let $\{I_i\}$ be a partition of the set $\{1, 2, \cdots, n\}$. Let T be an n x n matrix which satisfies

$$1. \quad |T^{i,i}| = \pm 1, \tag{109}$$

$$2. \quad T^{i,j} = 0, \ if \ i \succ j. \tag{110}$$

Then, T^{-1} satisfies

$$3. \quad |T^{-i,i}| = \pm 1, \tag{111}$$

$$4. \quad T^{-i,j} = 0, \ if \ i \succ j. \tag{112}$$

where $T^{-i,j} = (T^{-1})^{i,j}$.

(Proof) Without loss of generality, it is assumed that i $\succ j$ if i $> j$. As Lemma 5, we have n x n equations:

$$\sum t_{ik} t_{kj}^{-1} = \delta_{ij} \quad for \ \ 1 \leq i, j \leq n. \tag{113}$$

Consider the following n equations:

$$\sum t_{nk} t_{kj}^{-1} = \delta_{nj} \quad for \ \ 1 \leq j \leq n. \tag{114}$$

Let $n \in I_i$.

(Case 1: $|I_n| = 1$) From condition 1 and 2,

$$t_{nn} = \pm 1, \tag{115}$$

$$t_{nj} = 0, \quad for \ \ j \neq n. \tag{116}$$

Eq. 114 becomes

$$t_{nn} t_{nj}^{-1} = \delta_{nj} \quad for \ \ 1 \leq j \leq n. \tag{117}$$

Thus, we have

$$t_{nn}^{-1} = \pm 1, \tag{118}$$

$$t_{nj}^{-1} = 0, \quad for \ \ j \neq n. \tag{119}$$

Therefore, condition 3 and 4 are satisfied.

(Case 2: $|I_n| > 1$) Consider the following $|I_n|$ x $|I_n|$ equations:

$$\sum t_{ik} t_{kj}^{-1} = \delta_{ij} \quad for \ \ i, j \in I_n. \tag{120}$$

Since n $\succ$ j for all j $\notin I_n$, condition 2 says that

$$T^{n,k} = 0 \text{ ifk } \notin I_n. \tag{121}$$

Therefore, Eq. 120 becomes

$$\sum_{k \in I_n} t_{ik} t_{kj}^{-1} = \delta_{ij} \text{ for } i, \mathrm{j} \in I_n. \tag{122}$$

In a matrix form, Eq. 122 can be rewritten as follows:

$$T^{n,n} T^{-n,n} = I. \tag{123}$$

Therefore, $T^{-m,m} = (T^{m,m})^{-1}$. Hence, condition **3** is satisfied.

Consider the following equations:

$$\sum t_{ik} t_{kj}^{-1} = \delta_{ij} \text{ for } i \in I_n, \ \mathrm{j} \in \mathbf{I} \quad \mathrm{n} \succ \mathrm{m}. \tag{124}$$

From condition 2, $t_{ik} = 0$ if k $\notin$ I,. Thus, Eq. 124 becomes

$$\sum_{k \in I_n} t_{ik} t_{kj}^{-1} = \delta_{ij} \ for \ i \in I_n, \ j \in I_m, \ n \succ m. \tag{125}$$

In a matrix form, Eq. 125 can be rewritten as follows:

$$T^{n,n} \bar{t}_j^{-1} = \bar{0}, \tag{126}$$

where $\bar{t}_j^{-1} = [t_{kj}^{-1} | k \in I_n]^T$ for j $\in I_m$, n $\succ m$. Since $T^{n,n}$ is non-singular, $\bar{t}_j^{-1} = 0$. Therefore, condition 4 is satisfied.

The remained equations will be proved by an induction. Suppose that the condition **3** and 4 are satisfied by t_{ij}^{-1}, i $\in \cup_{l' \succ l} I_{l'}$. Now, consider the following equations:

$$\sum t_{lk} t_{kj}^{-1} = \delta_{ij} \text{ for } 1 \leq \mathrm{j} \leq n. \tag{127}$$

(Case 1: $|I_l| = 1$)
From condition 1 and 2, Eq. 127 becomes

$$t_{lj}^{-1} + \sum_{k \in \cup_{l' \succ l} I_{l'}} t_{lk} t_{kj}^{-1} = \delta_{lj}. \tag{128}$$

(condition 3:) Suppose that $j = l$. We have $t_{kl}^{-1} = 0$ for $k \in \cup_{l' \succ l} I_{l'}$. Hence, Eq. 128 becomes

$$t_{ll}^{-1} = \delta_{ll} = 1. \tag{129}$$

Hence, condition 3 is satisfied.
(condition 4:) Consider t_{lj}^{-1} for $j \in \mathbf{I}_m$, $l \succ m$. We have $t_{kl}^{-1} = 0$ for $k \in \cup_{l' \succ l} I_{l'}$. Hence, Eq. 128 becomes

$$t_{lj}^{-1} = \delta_{lj} = 0. \tag{130}$$

Hence, we have

$$t_{lj}^{-1} = 0 \quad for \quad j \bullet I_m, \quad l \succ m. \tag{131}$$

Thus, condition 4 is satisfied.

(Case 2: $|I_l| > 1$)
(condition 3:)
Consider the following $|I_l|$ x $|I_l|$ equations:

$$\sum t_{ik} t_{kj}^{-1} = \delta_{ij} \quad for \quad i, j \in I_l. \tag{132}$$

From condition 2, we have

$$\sum_{k \in I_l} t_{ik} t_{kj}^{-1} + \sum_{k \in \cup_{l' \succ l} I_{l'}} t_{ik} t_{kj}^{-1} = \delta_{ij} \quad for \quad i, j \in I_l. \tag{133}$$

We have $t_{kj}^{-1} = 0$ for $k \in \cup_{l' \succ l} I_{l'}$, $j \in I_l$. Therefore, Eq. 132 becomes:

$$\sum_{k \in I_l} t_{ik} t_{kj}^{-1} = \delta_{ij} \quad for \quad i, j \in I_l. \tag{134}$$

In a matrix form, Eq. 134 can be rewritten as follows:

$$T^{l,l} T^{-l,l} = I. \tag{135}$$

Therefore, $T^{-l,l} = (T^{l,l})^{-1}$. Hence, From Eq. 130 and 135, condition 3 is satisfied.

(condition 4:) Consider the following equations:

$$\sum t_{ik} t_{kj}^{-1} = \delta_{ij} \quad for \quad i \in I_l, \quad j \in \mathbf{I}_m \quad l \succ m. \tag{136}$$

From condition *2*, it becomes

$$\sum_{k\in I_l} t_{ik}t^{-1}_{kj} + \sum_{k\in \cup_{l'\succ l} I_{l'}} t_{ik}t^{-1}_{kj} = \delta_{ij} \quad for \quad i \in I_l, \quad j \in I_m, \quad l \succ m. \tag{137}$$

Since $l \succ$ I $\succ$ m, for k $\in \cup_{l'\succ l} I_{l'}$, $j \in I_m$, $l \succ$ m, we have $t^{-1}_{kj} = 0$. Therefore, Eq. *137* becomes:

$$\sum_{k\in I_l} t_{ik}t^{-1}_{kj} = \delta_{ij} \quad for \quad i \in I_l, \quad j \in I_m, \quad l \succ \text{m}. \tag{138}$$

In a matrix form, Eq. *138* can be rewritten as follows:

$$T^l \bar{t}^{-1}_j = \bar{0}, \tag{139}$$

where $\bar{t}^{-1}_j = [t^{-1}_{kj} | k \in I_l]^T$ for $j \in I_m$, $1 \succ$ m. Since T^l is non-singular, we have $\bar{t}^{-1}_j = \bar{0}$. Therefore, condition *4* is satisfied.

Therefore, conditions *3*, and r are satisfied. □

Lemma 7:

(Proof) Let t^{-1}_{ij} be the $(i,j)^{th}$ entry of the inverse of the transformation matrix T. Claim that G = $T^{-1}\Theta$ be the generator matrix which satisfies the conditions in Lemma *A.2*. To prove the claim, it suffices to prove the following facts:

1. $\exists H \in \text{Z}^{\text{nXn}}$ *such that* TG = OH, (140)
2. *for any* $\bar{g}$ *such that* $T\bar{g}$ = Oh *for* h $\in$ Z^{n}, 3 $\bar{\alpha}$ *such that* $\bar{g} = G\bar{\alpha}$, *(141)*
3. G *satisfies three conditions in* Lemma *A.2.* (142)

The proofs of *(1)* and *(2)* are same as for *(1)* and *(2)* in Lemma 6.

(3) Consider *a* matrix $U = [u_{ij}]$ such that

$$u_{ii} = 1 \ or \ -1, \tag{143}$$

$$u_{ij} = 0 \ if \ i \neq j, \tag{144}$$

$$|U^{i,i}| = |T^{i,i}| \tag{145}$$

Then, U is a unimodular matrix. Let $G' = GU$. Let g_{ij},g'_{ij} and θ_{ij} be the $(i,j)^{th}$ entries of the matrices G, G' and Θ, respectively. Lemma **A.3** shows that T^{-1} satisfies the following equations:

$$|T^{-i,i}| = 1, \tag{146}$$

$$T^{-i,j} = 0, \ if \ i \succ j. \tag{147}$$

(Case 1: $|I_i| = 1$)
(condition 1:)

$$(G')^{i,i} = g'_{ii} = t_{ii}g_{ii} = t_{ii}(\sum t_{ik}^{-1}\theta_{ki}) = t_{ii}t_{ii}^{-1}b_i = b_i. \tag{148}$$

Therefore, condition 1 is satisfied.
(condition 2:)
Consider $g_{ij}, j \in I_l, i \succ l$. We have

$$g_{ij} = \sum t_{ik}^{-1}\theta_{kj} = t_{ij}^{-1}b_j. \tag{149}$$

Since $t_{ij}^{-1} = 0$, we have $g_{ij} = 0$. Since $g'_{ij} = g_{ij}$ or $g'_{ij} = -g_{ij}$, we obtain $g'_{ij} = 0$ for $j \in I_l, i \succ$ l. Thus, condition 2 is satisfied.

(Case 2: $|I_i| > 1$)
(contlition 1:) Consider the following $|I_i|$ x $|I_i|$ equations:

$$g_{ij} = \sum t_{ik}^{-1}\theta_{kj} = t_{ij}^{-1}b_j - t_{ij}^{-1}b_i, \ \ i,j \in I_i. \tag{150}$$

Here, all $g_{ij} \in G^{i,i}$ are multiples of b_i. Moreover,

$$|G^{i,i}| = |T^{-i,i}|b_i^{|I_i|}. \tag{151}$$

Hence, $g'_{ij} \in (G')^{i,i}$ are also multiples of b_i. In addition,

$$|(G')^{i,i}| = |G^{i,i}||U^{i,i}| = |T^{-i,i}|b_i^{|I_i|}|T^{i,i}| = b_i^{|I_i|}. \tag{152}$$

Therefore, condition 1 is again satisfied.

(contlition **3:**)
Consider the following equations:

$$g_{ij} = \sum t_{ik}^{-1}\theta_{kj} = t_{ij}^{-1}b_j, \ \ i \in I_i, \ \ j \in I_m, \ \ l \succ m. \tag{153}$$

From Eq. 147, we have $g_{ij} = 0$. Hence, $g'_{ij} = 0$. Therefore, condition 3 in Lemma A.2 is satisfied. □

Corollary 2:

(Proof) Since all entries of b are same, there is only one partition, I_1 which is equal to $\mathbf{I} = \{1, 2, \cdots, n)$. Thus, $T^{1,1} = \mathrm{T}$. Since T is unimodular, $|T^{1,1}| = \pm 1$. Therefore, Lemma 7 shows that $T_{\bar{b}}$ is injective. □

Lemma A.4: [20] Let $J_{\bar{b}}$ be a rectangular index set with a boundary vector $\bar{b}$. Suppose that all entries of the vector b are same, i.e. $b_i = \beta$ for all $i, 1 \leq \mathrm{i} \leq n$. Let $T_{\bar{b}}$ be a modular function of the index set $J_{\bar{b}}$. Then $T_{\bar{b}}$ is a modular transformation if and only if the determinant of T is relatively prime with β.

(Proof) (+) Let T' denote the adjugate matrix (transpose of matrix of cofactors) of T. Then $\mathrm{TT}' = \mathrm{T}'\mathrm{T} = dI$ where I is the n x n identity matrix and $\mathrm{d} = det(T)$. So

$$T'(T\bar{j})_{mod\,\bar{\beta}} = (T'T\bar{j})_{mod\,\bar{\beta}} = (d\bar{j})_{mod\,\bar{\beta}},$$

where $\bar{\beta} = (\beta, \beta, \cdots, \beta)$. If d has no factor in common with b, then the equation du+ bv = 1 is soluble in integer u and v by Euclid's algorithm, so $du_{mod\,\beta} = 1$. Then

$$(uT'T\bar{j})_{mod\,\bar{\beta}} = \bar{j}.$$

Hence, the map $uT'_{mod\,\bar{\beta}}()$ is the inverse of the map $T_{mod\,\bar{\beta}}$. Hence, $T_{mod\,\bar{\beta}}$ is one-to-one.

(←) Suppose that d has a prime factor p in common with β. Let p = (p, p, ···, p). Claim that $T_{mod\,\bar{p}}$ is not injective, and so it cannot be injective $T_{mod\,\bar{\beta}}$. Since $\det(T)_{mod\,p} = 0$, so T is not invertible over the field of p elements, and so there is a non-zero vector $\bar{j}'$ such that $(T\bar{j}')_{mod\,p} = 0$. Hence $T_{\bar{p}}$ is not injective □

Lemma A.5: Let $J_{\bar{b}}$ be a rectangular index set with a boundary vector $\bar{b}$. Let $T_{\bar{m}}$ be a modular function of the index set $J_{\bar{b}}$. Let $\succ$ be an arbitrarily order on the set $\{1, 2, \cdots, n)$. $T_{\bar{m}}$ is a modular transformation if its transformation matrix T satisfies the following equations:

1. $(t_{ii}, b_i) = 1$,

2. $t_{ij} = 0$ if $i \succ j$,

where $(t_{i;}, b_{i;}) = 1$ means that t_{ii} and b_i are relatively prime.

(Proof) Decompose the transformation matrix T into DT' where

$$D = \begin{pmatrix} t_{11} & 0 & \cdots & 0 \\ 0 & t_{22} & \cdots & 0 \\ \vdots & & & 0 \\ 0 & \cdots & 0 & t_{nn} \end{pmatrix},$$

and

$$\begin{aligned} t'_{ii} &= 1 \quad \text{for } i = 1, \cdots, n \\ t'_{ij} &= t_{ij} \quad i \neq j. \end{aligned}$$

Since T' satisfies the conditions in Theorem 1, $T'_{mod\, \bar{b}}$ is one-to-one. Hence, $T'_{mod\, \bar{b}}(\bar{j}) = \bar{0}$ if and only if $\bar{j} = 0$. Let $\bar{j}' = T'\bar{j}$ then

$$T_{mod\, \bar{b}}(\bar{j}) = DT'_{mod\, \bar{b}}(\bar{j}) = D_{mod\, \bar{b}}(\bar{j}') = (t_{11}j'_1, t_{22}j'_2, \cdots, t_{nn}j'_n).$$

Since $T'_{mod\, \bar{b}}$ is one-to-one, there exists i such that $(j'_i)_{mod\, b_i} \neq 0$. Since t_{ii} is relative prime with b_i, $(t_{ii}j'_i)_{mod\, b_i} \neq 0$. Thus, $D_{mod\, \bar{b}}(\bar{j}')$ is not equal to 0. Hence, $T_{mod\, \bar{b}}(\bar{j})$ is one-to-one

Lemma ***A.6:*** Let $J_{\bar{b}}$ be a rectangular index set with a boundary vector $\bar{b}$. Let $T_{\bar{m}}$ be a modular transformation of the index set $J_{\bar{b}}$. Let $\{I_{i;}\}$ be a partition of the set $\{1, 2, \cdots, n\}$ and $\succ$ be an arbitrary order of the set $\{1, 2, \cdots, n\}$. $T_{\bar{m}}$ is a modular transformation if its transformation matrix satisfies

1. $(|T^i|, b_i) = 1$,

2. $T^{i,j} = 0$, if $i \in I_i$, $i \succ j$.

(Proof) Decompose the transformation matrix T into DT' where

$$\begin{aligned} D^i &= T^i \\ D^{ij} &= 0 \text{ if } i \neq j. \end{aligned}$$

and

$$\begin{aligned} T'^i &= I^i \\ T'^{i,j} &= T^{i,j} \text{ if } i \neq j \end{aligned}$$

where I^i is the identity matrix with the same number of entries as T^i. Since T' satisfies the conditions in Lemma 7, $T'_{mod\ \bar{b}}$ is one-to-one. Hence, $T'_{mod\ \bar{b}}(\bar{j}) = \bar{0}$ if and only if $\bar{j} = 0$. Let $\bar{j}' = T'\bar{j}$ then

$$T_{mod\ \bar{b}}(\bar{j}) = DT'_{mod\ \bar{b}}(\bar{j}) = D_{mod\ \bar{b}}(\bar{j}').$$

Since $T'_{mod\ \bar{b}}$ is one-to-one, there exists i such that $(j'_i)_{mod\ b_i} \neq 0$. Since $det(T^i)$ is relative prime with b_i, Lemma **A.2** shows that there exists $i' \in \mathbf{I}$; such that the i'^{th} entry of $D_{mod\ \bar{b}}(\bar{j}')$ is not equal to 0. Therefore, $D_{mod\ \bar{b}}(\bar{j}')$ is not equal to 0. Hence, $T_{mod\ \bar{b}}(\bar{j})$ is one-to-one □