THE STRUCTURE OF PERIODIC STORAGE SCHEMES

FOR PARALLEL MEMORIES

H.A.G. Wijshoff and J. van Leeuwen

RUU-CS-84-1

January 1984
(July 1984)

Rijksuniversiteit Utrecht

Vakgroep informatica

Budapestlaan 6 3584 CD Utrecht
Corr. adres: Postbus 80.012 3508 TA Utrecht
Telefoon 030-531454
The Netherlands

THE STRUCTURE OF PERIODIC STORAGE SCHEMES FOR PARALLEL MEMORIES

H.A.G. Wijshoff and J. van Leeuwen

Technical Report RUU-CS-84-1
January 1984

Department of Computer Science
University of Utrecht
P.O. Box 80.012, 3508 TA Utrecht
the Netherlands

THE STRUCTURE OF PERIODIC STORAGE SCHEMES FOR PARALLEL MEMORIES

H. A. G. Wijshoff and J. van Leeuwen

Department of Computer Science, University of Utrecht
P.O. Box 80.012, 3508 TA Utrecht, the Netherlands.

Abstract. The use of parallel memories in SIMD-machines requires special data mappings known as "skewing schemes", for storing matrices for the purposes of efficient vector computations. Studies by e.g. Kuck, Lawrie, Shapiro and (recently) the present authors have shown the practicality of skewing schemes and some schemes have explicitly been implemented in e.g. the Burroughs BSP. Linear and periodic skewing schemes are of particular interest, because they have a "regular" structure and can be represented by simple formulae. Yet (periodic) skewing schemes have largely been analysed only for the 2-dimensional case and from the combinatorial point of view. In this paper we will show that periodic skewing schemes have an elegant foundation in the mathematical theory of integral lattices and $\mathbb{Z}$-modules, which will lead to insightful proofs of a number of general properties of periodic skewing schemes in all dimensions.

Keywords and phrases: parallel memories, SIMD machines, skewing schemes, lattices, $\mathbb{Z}$-modules, tables.

1. Introduction. The speed and efficiency of computations by vector- and array-processors heavily depends on a suitable distribution of the data vectors over the available memories. A typical problem arises when a d-dimensional array of size $N \times N \times \cdots \times N$ must be stored into M memory banks in such a way that all vectors of interest (rows, columns, blocks) can be fetched conflict-free in one memory cycle. This means that all ele-

ments of any such vector must be stored in different memory banks, in some way. Data mappings that attempt to achieve this are known as "skewing schemes", and were first introduced in the late nineteen sixties during the design-phase of the ILLIAC IV (see Kuck [4] and Budnik & Kuck [1]). A skewing scheme simply is a mapping s from $\mathbb{Z}_N \times \mathbb{Z}_N \times \cdots \times \mathbb{Z}_N$ (d times) to $\mathbb{Z}_M$, which maps an array element $a[i_1, \cdots, i_d]$ to memory bank $s(i_1, \cdots, i_d)$. We assume that the memory banks are numbered from 0 to $M-1$ and ignore for the moment the assignment of individual addresses within the banks.

Clearly skewing schemes are of practical interest only when they can be represented in a simple and compact manner. Traditionally only "linear" skewing schemes are considered, defined by $s(i_1, \cdots, i_d) = \lambda_1 i_1 + \cdots + \lambda_d i_d \pmod M$ for suitably chosen coefficients $\lambda_1, \cdots, \lambda_d \in \mathbb{Z}$ (see e.g. Budnik & Kuck [1], Lawrie [5], Kuck [4], Hoßfeld & Weidner [2], and Wijshoff & van Leeuwen [12]). More generally, Shapiro [9] defined a skewing scheme to be "periodic", and thus compactly represented, if the skewing scheme can be described by a small-sized table to which all arguments can be reduced by the use of a proper modulus. Wijshoff & van Leeuwen [11] showed that the study of periodic skewing schemes is best approached through the classical theory of integral lattices (as known in e.g. number theory). It is assumed that s is defined on the entire $\mathbb{Z}^d$, to let the theory apply. The connection was exploited to considerably extend the theory of 2-dimensional periodic skewing schemes as begun by Shapiro [9].

In this paper we consider the structure of periodic skewing schemes more generally and show that these schemes have an elegant foundation in the algebraic theory of $\mathbb{Z}$-modules (see e.g. Jacobson [3]). The connection will lead to insightful proofs of a number of crucial, general properties of periodic skewing schemes in all dimensions. We believe this paper provides the correct mathematical understanding of periodic skewing schemes that has been lacking until now. The paper is organised as follows. In section 2 we shall (re-) define periodic skewing schemes and derive some basic facts. Section 3 shows the connection with module-theory, which leads to a useful representation of periodic skewing schemes. In section 4 this representation is applied to derive a number of general properties related to the compact expression of periodic skewing schemes by means of tables and/or arithmetic formulae. It is also shown that when the number of memory banks M is chosen to be square-free, then every periodic skewing scheme is linear.

2. <u>Periodic skewing schemes</u>. The theory of 2-dimensional (periodic) skewing schemes was initialized by Kuck [4], and extended by Shapiro [9] and Wijshoff & van Leeuwen [11]. In this section we redefine the notion of periodic skewing schemes and generalise the theory to arbitrary dimensions using elementary notions from lattice theory (see e.g. Lekkerkerker [6]).

A d-dimensional lattice L^d generated by integral vectors $\vec{x}_1, \cdots, \vec{x}_d$ (the basis of the lattice) is the set of integral linear combinations $\lambda_1\vec{x}_1 + \cdots + \lambda_d\vec{x}_d$. The set $\{v_1\vec{x}_1 + \cdots + v_d\vec{x}_d \mid v_i \in \mathbb{R} \text{ and } 0 \le v_i < 1\}$ is called the fundamental parallelotope of L^d. Its volume is denoted as $\Delta(L^d)$, also called the determinant of L^d. Clearly one has $\Delta(L^d) = |\det(\vec{x}_1 \cdots \vec{x}_d)|$, and it can be shown that $\Delta(L^d)$ is independent of the particular basis chosen for L^d. Points $p = (p_1, \cdots, p_d)$ and $q = (q_1, \cdots, q_d)$ are said to be equivalent modulo L^d, notation: $p \equiv_{L^d} q$, if $p - q \in L^d$.

<u>Fact</u> 2.1 ([6], p. 23) The number of equivalence classes mod L^d is equal to $\Delta(L^d)$.

<u>Definition</u> 2.2. Let G be a finite set (e.g. a finite $\mathbb{Z}$-module) with $|G| = M$. A table t (for G) is any bijective map from G into $\{0, \cdots, M-1\}$

Definition 2.3. Let $s : \mathbb{Z} \times \dots \times \mathbb{Z}$ (d times) $\to \{0, \dots, M-1\}$ be a skewing scheme using M memory banks. The scheme s is called periodic if and only if there exist a d-dimensional lattice L^d, a (surjective) homomorphism $\alpha : \mathbb{Z}^d \to \mathbb{Z}^d/L^d$ with $\mathrm{Ker}(\alpha) = L^d$, and a table t for $\mathbb{Z}^d/L^d$ such that $s = t \circ \alpha$.

L^d is called the underlying lattice of s, and necessarily $\Delta(L^d) = M$. Thus t has exactly M entries. We observe (cf. [11]):

Proposition 2.4. Let s be a periodic skewing scheme with underlying lattice L^d. The number of memory banks used by s is exactly equal to the determinant $\Delta(L^d)$.

The next proposition shows that in the definition of periodicity only the existence of a homomorphism of the desired kind is essential.

Proposition 2.5. Let s be a periodic skewing scheme, $s = t \circ \alpha$. For every (surjective) homomorphism $\alpha' : \mathbb{Z}^d \to \mathbb{Z}^d/L^d$ with $\mathrm{Ker}(\alpha') = L^d$ there exists a table t' such that $s = t' \circ \alpha'$.

Proof.

Define a mapping $\psi : \mathbb{Z}^d/L^d \to \mathbb{Z}^d/L^d$ as follows. For every $y \in \mathbb{Z}^d/L^d$ and x such that $\alpha'(x) = y$ let $\psi(y) = \alpha(x)$. Because $\mathrm{Ker}(\alpha') = \mathrm{Ker}(\alpha)$ the value of $\psi(y)$ is well-defined and independent of the particular x with $\alpha'(x) = y$. It is easily verified that ψ is an automorphism of $\mathbb{Z}^d/L^d$ and that $\psi \circ \alpha' = \alpha$. Hence $s = t \circ \alpha = t' \circ \alpha'$ with $t' = t \circ \psi$. □

It follows that in definition 2.3 we may always assume α to be the natural homomorphism from $\mathbb{Z}^d$ into $\mathbb{Z}^d/L^d$.

Proposition 2.6. A skewing scheme s is periodic if and only if there exist a lattice L^d and $a_0, \dots, a_{M-1} \in \mathbb{Z}^d$ (where $M = \Delta(L^d)$) such that for all $0 \leq i \leq M-1$: $s^{-1}(i) = a_i + L^d$.

The following notion has proved useful in the theory (see e.g. [11]) and provides yet another characterisation of periodicity.

Definition 2.7 A skewing scheme s is called regular if and only if the following property is satisfied for all $p, q \in \mathbb{Z}^d$: if $s(p) = s(q)$ then every pair of points $\in \mathbb{Z}^d$ that are in the same relative position as p and q is (also) mapped to equal memory banks.

Lemma 2.8. A skewing scheme s is periodic if and only if it is regular.

Proof.

$\Rightarrow$. By proposition 2.6.

$\Leftarrow$. (See [11].) Let any vector $\vec{v}$ that is the relative position of two cells p and q with $s(p) = s(q)$ be called a period of s. The crucial fact to observe is that the periods of s form a discrete group in $\mathbb{Z}^d$, and hence form a lattice L^d (see e.g. Weyl [10], p. 142). This lattice is the underlying lattice for s in the sense of definition 2.3 (or use proposition 2.6). $\square$

3. A representation of periodic skewing schemes. We will now argue that for every periodic skewing scheme $s : \mathbb{Z}^d \rightarrow \{0, \cdots, M-1\}$ there are a homomorphism α and a table t such that $s = t \circ \alpha$ and α can be expressed as a direct product of linear forms.

Definition 3.1 A fundamental domain F of a d-dimensional lattice L^d is any (viz. compact) domain $\subseteq \mathbb{Z}^d$ such that (i) no two points of F are equivalent mod L^d, and (ii) every point $p \in \mathbb{Z}^d$ is equivalent mod L^d to a point of F. (Thus F has exactly one point from every equivalence class mod L^d and $|F| = \Delta(L^d)$.)

Given a fundamental domain $F \subseteq \mathbb{Z}^d$, let $\delta_F : \mathbb{Z}^d \to F$ be defined such that for all $p \in \mathbb{Z}^d$ $\delta_F(p)$ is the unique $q \in F$ with $p \equiv_{L^d} q$. Any fundamental domain F can be regarded as an embedding of $\mathbb{Z}^d/L^d$ into $\mathbb{Z}^d$ and thus inherits the structure of a finite $\mathbb{Z}$-module, with $\oplus$ and $\odot$ defined by $p \oplus q = \delta_F(p+q)$ and $\lambda \odot p = \delta_F(\lambda p)$. With this structure δ_F is a homomorphism, with $\mathrm{Ker}(\delta_F) = L^d$. A natural fundamental domain would be the set of (integral) points inside the fundamental parallelotope.

<u>Proposition</u> 3.2. Every fundamental domain F of L^d is (module-) isomorphic to $\mathbb{Z}^d/L^d$.

<u>Proposition</u> 3.3. Let s be a periodic skewing scheme with underlying lattice L^d, and let F be a fundamental domain of L^d. There is a table t for F such that $s = t \circ \delta_F$.

<u>Proof</u>.

By proposition 3.2 there is an isomorphism $\varphi : F \to \mathbb{Z}^d/L^d$, hence $\varphi \circ \delta_F$ is a (surjective) homomorphism : $\mathbb{Z}^d \to \mathbb{Z}^d/L^d$ with $\mathrm{Ker}(\varphi \circ \delta_F) = L^d$. By proposition 2.5 there exists a table t' such that $s = t' \circ (\varphi \circ \delta_F)$. Take $t = t' \circ \varphi$. □

Next we show that for a suitable basis L^d has a fundamental domain that is "box-like", i.e., a polytope spanned by vectors along the coordinate axes. (See [11] for the more special situation in the 2-dim case.) Let A be a $d \times d$ matrix with integer coefficients. For $1 \le k \le d$ define the k^{th} determinantal divisor d_k of A by

$$d_k = \begin{cases} 0 & \text{, if all } k \times k \text{ determinantal minors of } A \text{ are } 0 \\ \text{the gcd of all } k \times k \text{ determinantal minors of } A & \text{, otherwise} \end{cases}$$

and let

$$s_k = \frac{d_k}{d_{k-1}}$$

(where for consistency we define $d_0 = 1$ and $\frac{0}{0} \equiv 0$). The coefficients s_k are known as the invariant factors of A.

<u>Fact</u> 3.4 ([7], p.28). The coefficients s_k $(1 \leq k \leq d)$ are integers and $s_1 | s_2 | \cdots | s_d$.

<u>Theorem</u> 3.5 ([7], p.36). Let L^d be a d-dimensional lattice in $\mathbb{Z}^d$, with basis $\{\vec{x}_1, \cdots, \vec{x}_d\}$ (with respect to the standard basis of unit vectors in $\mathbb{Z}^d$). There exists a basis $\mathcal{U} = \{\vec{u}_1, \cdots, \vec{u}_d\}$ of $\mathbb{Z}^d$ such that $\{s_1 \vec{u}_1, \cdots, s_d \vec{u}_d\}$ is a basis of L^d, where s_1 through s_d are the invariant factors of the matrix $A = (\vec{x}_1 \cdots \vec{x}_d)$.

Note that $|\det(\vec{u}_1 \cdots \vec{u}_d)| = 1$ and that all s_k are non-zero (in the case of the theorem). Use the notation $(\cdot\cdot, \cdots, \cdot\cdot)_{\mathcal{U}}$ to denote any coordinated vector with respect to $\mathcal{U}$.

<u>Lemma</u> 3.6. The domain $F^* = \{(\lambda_1, \cdots, \lambda_d)_{\mathcal{U}} \mid \lambda_k \in \mathbb{Z}_{s_k} \text{ for } 1 \leq k \leq d\}$ is a fundamental domain of L^d, where $\mathcal{U}$ and s_1 through s_d are as defined in the preceding theorem. Furthermore, the homomorphism $\delta_{F^*} : \mathbb{Z}^d \to F^*$ is given by $\delta_{F^*}((i_1, \cdots, i_d)_{\mathcal{U}}) = (i_1 \bmod s_1, \cdots, i_d \bmod s_d)_{\mathcal{U}}$.

<u>Proof</u>

Clearly F^* contains no two distinct points that differ by an integer linear combination of the base-vectors $s_1\vec{u}_1, \cdots, s_d\vec{u}_d$ of L^d. Thus $p \not\equiv_{L^d} q$ for any distinct $p, q \in F^*$. Let $\delta : \mathbb{Z}^d \to F^*$ be the homomorphism defined in the lemma. For every $(i_1, \cdots, i_d)_{\mathcal{U}} \in \mathbb{Z}^d$ there are integers l_1 through l_d such that $(i_1, \cdots, i_d)_{\mathcal{U}} - (i_1 \bmod s_1, \cdots, i_d \bmod s_d)_{\mathcal{U}} =$ $= (l_1 s_1, \cdots, l_d s_d)_{\mathcal{U}}$ and hence for every $p \in \mathbb{Z}^d$: $p - \delta(p) \in L^d$, or: $p \equiv_{L^d} \delta(p)$. It follows that all equivalence classes mod L^d are uniquely represented in F^* (hence F^* is a fundamental domain) and $\delta = \delta_{F^*}$. $\square$

Use $\sigma(x)$ to denote the order of any element x of a (finite) $\mathbb{Z}$-module

The following fact is well-known in the theory of finitely generated modules over any principal ideal domain (e.g. [3], chapter 3).

Corollary 3.7. Let L^d be a d-dimensional lattice in $\mathbb{Z}^d$. $\mathbb{Z}^d/L^d$, or any fundamental domain of L^d, is (module-) isomorphic to a direct sum of d finite cyclic $\mathbb{Z}$-modules $\langle z_1 \rangle \oplus \cdots \oplus \langle z_d \rangle$ where $\sigma(z_k) = s_k$ for $1 \le k \le d$, and s_1 through s_d are as in the preceding theorem.
Proof.
Immediate from proposition 3.2 and lemma 3.6. □

Another way of phrasing corollary 3.7 is to say that $\mathbb{Z}^d/L^d$, or any fundamental domain of L^d, is (module-) isomorphic to the block B_{L^d} defined as

$$B_{L^d} = \{0, \cdots, s_1 - 1\} \oplus \{0, \cdots, s_2 - 1\} \oplus \cdots \oplus \{0, \cdots, s_d - 1\}.$$

Using this we can finally derive the main result concerning the proper representation of periodic skewing schemes.

Theorem 3.8 Let s be a periodic skewing scheme and L^d its underlying lattice. There exist a (surjective) homomorphism $\alpha : \mathbb{Z}^d \to B_{L^d}$ and a table t for B_{L^d} such that $s = t \circ \alpha$ and α is given by an expression of the type $\alpha((i_1, \cdots, i_d)) = (L_1(\vec{i}) \bmod s_1, \cdots, L_d(\vec{i}) \bmod s_d)$, where $L_k(\vec{i}) \equiv \lambda_{k1} i_1 + \cdots + \lambda_{kd} i_d$ is an integer linear form for $1 \le k \le d$ and B_{L^d} and s_1 through s_d are defined as before.
Proof.
Let $U = \{\vec{u}_1, \cdots, \vec{u}_d\}$ be a basis for $\mathbb{Z}^d$ as implied by theorem 3.5. The matrix $(\vec{u}_1 \cdots \vec{u}_d)$ is unimodular and (hence) the mapping $\beta \equiv (\vec{u}_1 \cdots \vec{u}_d)^{-1}$ representing the linear transformation from standard coordinates to U-coordinates in $\mathbb{Z}^d$ is again described by an integral matrix. Because $\mathbb{Z}^d/L^d$, F^*, and B_{L^d} are all fundamental domains of L^d (cf. lemma 3.6 and corollary 3.7) there are isomorphisms φ, ψ (cf. proposition 3.2) with $\varphi : F^* \to \mathbb{Z}^d/L^d$ and $\psi : F^* \to B_{L^d}$ (where ψ is

the natural isomorphism). Defining $\alpha' = \varphi \circ \delta_{F^*} \circ \beta$ we observe that $\alpha' : \mathbb{Z}^d \to \mathbb{Z}^d/L^d$ is a homomorphism with $\mathrm{Ker}(\alpha') = L^d$, and hence by proposition 2.5 there exists a table t' for $\mathbb{Z}^d/L^d$ such that $s = t' \circ \alpha'$. Now let $\alpha = \psi \circ \delta_{F^*} \circ \beta$ and $t = t' \circ \varphi \circ \psi^{-1}$. Then $\alpha : \mathbb{Z}^d \to B_{L^d}$ is again a homomorphism, t is a table for B_{L^d}, and $t \circ \alpha = t' \circ \varphi \circ \psi^{-1} \circ \psi \circ \delta_{F^*} \circ \beta = t' \circ \alpha' = s$. Furthermore α can be expressed as stated. (The k^{th} coordinate expression of $\beta(\vec{i})$ provides the $L_k(\vec{i})$, and the $\psi \circ \delta_{F^*}$ the reduction mod s_k.) □

4. Applications to the theory of (periodic) skewing schemes. We show that various general and practical properties of periodic skewing schemes, often stated only for the 2-dimensional case, hold and have elegant proofs for all dimensions. The characterisation derived in theorem 3.8 will be crucial here.

The particular "naming" (numbering) of the memory banks is of no importance for the property of conflict-free access to vectors, but it is perhaps for a simple arithmetic expression of the periodic skewing scheme. The following definition and results make this precise.

Definition 4.1. Let s and r be d-dimensional (periodic) skewing schemes using an equal number of memory banks M. We say that s and r are equivalent, notation: $s \equiv r$, if and only if there exists a bijective map $\varphi : \{0, \ldots, M-1\} \to \{0, \cdots, M-1\}$ such that $s = \varphi \circ r$.

(Compare definition 2.3, and note that $\equiv$ is indeed an equivalence relation on skewing schemes.) The definition expresses that two skewing schemes are equivalent if and only if they are "equal" except for a change of table.

Proposition 4.2. Let s and r be d-dimensional periodic skewing schemes using an equal number of memory banks M and underlying lattices L_s^d and L_r^d, respectively. Then $s \equiv r$ if and only if $L_s^d = L_r^d$.

Proof.

$\Rightarrow$. Immediately from the characterisation given in proposition 2.6.

$\Leftarrow$. Let $s = t_s \circ \alpha_s$ and $r = t_r \circ \alpha_r$, as suggested by theorem 3.8. If $L_s^d = L_r^d$ (which determine the α's) then $\alpha_s = \alpha_r$. Consequently s and r are equivalent, using $\varphi = t_s \circ t_r^{-1}$. □

Proposition 4.3. Let $s = t \circ \alpha$ be a periodic skewing scheme, with α a (surjective) map : $\mathbb{Z}^d \to G$ for some finite set G and t a table for G. For every table t' of G and skewing scheme $s' = t' \circ \alpha$, $s \equiv s'$.

Theorem 4.4. Let s be a periodic skewing scheme and L^d its underlying lattice. Then s is equivalent to a periodic skewing scheme s' defined by an expression of the type $s'(\vec{i}) = \sum_1^d s_1 \cdots s_{k-1} \cdot (L_k(\vec{i}) \bmod s_k)$ for $\vec{i} \in \mathbb{Z}^d$, where L_1 through L_d are integer linear forms and s_1 through s_d are integer factors determined by L^d as defined in section 3.

Proof.

By theorem 3.8 we know that $s = t \circ \alpha$, for a (surjective) homomorphism $\alpha : \mathbb{Z}^d \to B_{L^d}$ as expressed in the theorem and a table t of B_{L^d}. Define a table t' of B_{L^d} by $t'((b_1, \dots, b_d)) = \sum_1^d s_1 \cdots s_{k-1} \cdot b_k$. (This is indeed a bijective map : $B_{L^d} \to \{0, \dots, M-1\}$ as $0 \le b_k < s_k$ and $s_1 \cdots s_d = \Delta(L_d) = M$.) By proposition 4.3 follows that s must be equivalent to $s' = t' \circ \alpha$, and s' is expressed as in the theorem. □

The theorem shows that every periodic skewing scheme is equivalent to a scheme that is described by a simple arithmetic expression that can be evaluated fast. Explicit formulae for general 2-dimensional periodic skewing schemes can be found in [11].

Corollary 4.5 Let s be a periodic skewing scheme and L^d its underlying lattice. Then s is equivalent to a periodic skewing scheme s' defined by $s'(\vec{i}) = \sum_1^d d_{k-1} \cdot (L_k(\vec{i}) \bmod s_k)$, where L_1 through L_d are integer linear expressions and d_1 through d_d and s_1 through s_d are the determinantal divisors and invariant factors (respectively) of the lattice basis.

Definition 4.6. A skewing scheme $s : \mathbb{Z}^d \to \{0, \cdots, M-1\}$ is called linear if and only if there are integer constants $\lambda_1, \cdots, \lambda_d$ with $\gcd(\lambda_1, \cdots, \lambda_d, M) = 1$ such that $s(\vec{i}) = \lambda_1 \cdot i_1 + \cdots + \lambda_d \cdot i_d \pmod M$.

(The condition on the gcd guarantees that s uses all its memory banks.) Linear skewing schemes are very simple and therefore most commonly used in practice. In the literature (e.g. Lawrie [5], Shapiro [8], Wijshoff & van Leeuwen [12]) several conditions on $\lambda_1, \cdots, \lambda_d$ and M have been formulated in order for a linear skewing scheme to be conflict-free for rows, columns, and/or diagonals. Very often M is assumed to be prime, to simplify the conditions of conflict-free access. A detailed analysis was given in [12].

Proposition 4.7. Every linear skewing scheme is periodic.

Proof.

Let s be defined by $s(\vec{i}) = \lambda_1 \cdot i_1 + \cdots + \lambda_d \cdot i_d \pmod M$. We show that s is regular, hence periodic by lemma 2.8. Assume that $s(p) = s(q)$ for two points $p = (p_1, \cdots, p_d)$ and $q = (q_1, \cdots, q_d)$, and let $\vec{v} = q - p$ be the "relative position" of p and q. By substituting in the expression for s it follows that $\lambda_1 \cdot v_1 + \cdots + \lambda_d \cdot v_d \equiv 0 \pmod M$. But this is precisely the condition for all pairs of points in relative position $\vec{v}$ to be mapped to equal banks, i.e., to have the same s-value. Thus s is regular. $\square$

Whereas linear skewing schemes have the advantage of being very simple and easy to evaluate, it can be argued that periodic skewing schemes in general give a greater flexibility for achieving some type of conflict-free access. Nevertheless we show that for M prime (more generally: M square-free) the full power of periodic skewing schemes can be obtained using just the linear schemes. This is interesting because in a number of machines the number of memory banks M was specifically chosen to be prime. We begin by deriving a general condition for linearity.

<u>Theorem</u> 4.8. Let s be a periodic skewing scheme and L^d its underlying lattice with basis $\{\vec{x}_1, \cdots, \vec{x}_d\}$. Then s is equivalent to a linear skewing scheme if and only if $d_k = 1$ for $1 \le k \le d-1$ (equivalently: $s_k = 1$ for $1 \le k \le d-1$, where d_k (s_k) is the k^{th} determinantal divisor (invariant factor) of the matrix $A = (\vec{x}_1 \cdots \vec{x}_d)$.

<u>Proof</u>.

$\Rightarrow$. Let s be equivalent to a linear skewing scheme, thus $s = \varphi \circ s'$ for a bijective map $\varphi : \{0, \cdots, M-1\} \to \{0, \cdots, M-1\}$ and $s'(\vec{i}) = \lambda_1 i_1 + \cdots + i_d \lambda_d$ (mod M) for some integers $\lambda_1, \cdots, \lambda_d$ with $\gcd(\lambda_1, \cdots, \lambda_d, M) = 1$. From elementary number theory follows that there exists an $\vec{i}^* \in \mathbb{Z}^d$ with $s'(\vec{i}^*) = 1$. Thus $\{ s'(\mu . \vec{i}^*) \mid 0 \le \mu < M\} = \{0, \cdots, M-1\}$ and (hence) $\{ s(\mu \vec{i}^*) \mid 0 \le \mu < M\} = \{0, \cdots, M-1\}$. It follows that $F = \{\mu . \vec{i}^* \mid 0 \le \mu < M\}$ is a fundamental domain of L^d. By corollary 3.7 F is isomorphic to a direct sum of cyclic modules $\langle z_1 \rangle \oplus \cdots \oplus \langle z_d \rangle$ with $\sigma(z_k) = s_k$ for $1 \le k \le d$. Because F is generated by one vector all but one of the modules must be trivial. Because $s_1 | s_2 | \cdots | s_d$ (fact 3.4) it follows that necessarily $s_1 = \cdots = s_{d-1} = 1$, or equivalently $d_1 = \cdots = d_{d-1} = 1$.

$\Leftarrow$. Let $d_k = 1$ for $1 \le k \le d-1$, or equivalently $s_k = 1$ for $1 \le k \le d-1$. It follows in particular that $d_d = s_d = \Delta(L^d) = M$. From corollary 4.5 it follows immediately that s is equivalent to a skewing scheme s' of the type $s'(\vec{i}) = L_d(\vec{i})$ (mod M), by substitution. Clearly s' is linear

□

<u>Corollary</u> 4.9. Let s be a periodic skewing scheme and L^d its underlying lattice. Then s is equivalent to a linear skewing scheme if and only if $\mathbb{Z}^d/L^d$, or any fundamental domain of L^d, is cyclic.

The condition in theorem 4.8 takes a particularly simple form for $d=2$, as shown initially in [14] by a direct number-theoretic argument.

Corollary 4.10. Let s be a 2-dimensional periodic skewing scheme, and L^2 its underlying lattice with base-vectors $\vec{x}=(x_1,x_2)$ and $\vec{y}=(y_1,y_2)$. Then s is equivalent to a linear scheme if and only if $\gcd(x_1,x_2,y_1,y_2) = 1$.

Proof.

Immediately from theorem 4.8, using that $d_1 = \gcd(x_1,x_2,y_1,y_2)$ by definition. □

Corollary 4.11. Let the number of memory banks M be prime. Then every periodic skewing scheme $s: \mathbb{Z}^d \to \{0,\dots,M-1\}$ (using M banks) is equivalent to a linear scheme.

Proof.

By fact 2.1 $\mathbb{Z}^d/L^d$ has $\Delta(L^d) = M$ elements and thus is necessarily cyclic (M prime). By corollary 4.9 every periodic skewing scheme will (thus) be equivalent to a linear scheme. (Alternatively, it is straightforward from divisibility arguments that the d_k must be 1 for $1 \le k \le d-1$ when M is prime.) □

Corollary 4.12. Let M be square-free, i.e., not divisible by the square of a prime). Then every periodic skewing scheme $s: \mathbb{Z}^d \to \{0,\dots,M-1\}$ (using M banks) is equivalent to a linear scheme.

Proof.

Let M be square-free, and suppose there was a periodic skewing schem that was not equivalent to a linear scheme. By theorem 4.8 there must be a k with $1 \le k \le d-1$ such that $s_k > 1$. Let p be a prime factor of s_k. By fact 3.4 it follows that $p \mid s_d$, and (hence) $p^2 \mid s_1 \cdots s_d = \Delta(L^d) = M$. Contradiction. □

5. Conclusion. We have shown that the concepts and results of the practical theory of periodic skewing schemes are best understood and easily derived from (known) concepts and results in lattice- and module-theory.

6. References.

[1] Budnik, P., and D.J. Kuck, The organisation and use of parallel memories, IEEE Trans. Comput. C-20 (1971) 1566-1569.

[2] Hoßfeld, F., and P. Weidner, Parallele Algorithmen, Inf. Spektr. 6 (1983) 142-154.

[3] Jacobson, N., Basic algebra I, W.H. Freeman, San Francisco, 1974.

[4] Kuck, D.J., ILLIAC IV software and application programming, IEEE Trans. Comput. C-17 (1968) 758-770.

[5] Lawrie, D.H., Access and alignment in an array processor, IEEE Trans. Comput. C-24 (1975) 1145-1155.

[6] Lekkerkerker, C.G., Geometry of numbers, Wolters-Noordhoff / North-Holland Publ. Comp., Amsterdam, 1969.

[7] Newman, M., Integral matrices, Ser. Pure Appl. Math vol 45, Academic Press, New York, 1972.

[8] Shapiro, H.D., Storage schemes in parallel memories, 1975 Sagamore Conf. Parall. Proc., 1975, pp. 159-166.

[9] Shapiro, H.D., Theoretical limitations on the use of parallel memories, IEEE Trans. Comput. C-27 (197) 421-428.

[10] Weyl, H., Algebraic theory of numbers, Ann. Math. Stud. 1, Princeton Univ. Press, Princeton, 1940.

[11] Wijshoff, H.A.G., and J. van Leeuwen, Periodic storage schemes with a minimum number of memory banks, Techn. Rep. RUU-CS-83-4, Dept of Computer Science, University of Utrecht, Utrecht, 1983.

[12] Wijshoff, H.A.G., and J. van Leeuwen, On linear skewing schemes and d-ordered vectors, Techn. Rep. RUU-CS-83-7, Dept of Computer

Science, University of Utrecht, Utrecht, 1983.

[14] Wijshoff, H.A.G., and J. van Leeuwen, A linearity condition for periodic storage skewing schemes, Techn. Rep. RUU-CS-83-10, Dept of Computer Science, University of Utrecht, Utrecht, 1983.