# PARALLEL MEMORIES, PERIODIC SKEWING SCHEMES, AND THE THEORY OF FINITE ABELIAN GROUPS

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

RUU-CS-84-7

August 1984


**Rijksuniversiteit Utrecht**

**Vakgroep informatica**

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

# PARALLEL MEMORIES, PERIODIC SKEWING SCHEMES, AND THE THEORY OF FINITE ABELIAN GROUPS

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

[illegible]

August 1984

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

# PARALLEL MEMORIES, PERIODIC SKEWING SCHEMES, AND THE THEORY OF FINITE ABELIAN GROUPS

J. Tappe*, J. van Leeuwen**, and H.A.G. Wijshoff**

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

Abstract. Current designs of large parallel computers usually include a non-trivial number of separate memory modules that can be accessed independently in parallel. In the engineering literature several schemes (called "skewing schemes") have been proposed for storing the elements of a Nx ... xN (d-fold) matrix in M memory modules such that all M-vectors of interest can be accessed conflict-free, i.e., have elements in distinct memory modules. In [14] it was argued that the general class of periodic skewing schemes is elegantly understood from the viewpoint of classical integer lattice theory. In the present paper we give a detailed account of the more general connection between periodic skewing schemes and the theory of finite abelian groups. As a main result we prove that the periodic skewing schemes can be completely classified into equivalence "types", and a normal form theorem is derived. It is shown that the number of non-equivalent linear skewing schemes using M memory modules is bounded by $O(M^{d-1} \text{loglog } M)$.

* Address: Lehrstuhl B für Mathematik, RWTH Aachen, Templergraben 55, D-5100 Aachen, Fed. Rep. Germany.

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

Keywords and phrases : parallel computers, skewing schemes, conflict-free access, finite abelian groups, automorphisms, normal form, linear skewing schemes.

1. Introduction. The architecture of current and experimental super computers (cf. Hockney & Jesshope [3]) is characterized by having one or more highly pipelined CPU's and a non-trivial number M of memory modules that can be accessed independently in parallel. Since the machines are meant for large scale numeric problem solving, much attention has been given to the problem of storing the elements of an N x .... x N (d-fold) matrix such that all M-vectors of interest can be retrieved conflict-free, i.e., have elements in distinct memory banks. Non-trivial schemes for this task were proposed as early as 1967 in scheduling matrix computations for the ILLIAC IV (Knowles et. al. [4], Kuck [5]), and are commonly referred to as "skewed arrays". Budnik & Kuck [1] and Lawrie [7] formulated simple conditions for skewing schemes to be conflict-free for vectors like rows, columns, and diagonals.

In a fundamental study, Shapiro [9] considerably extended the theoretical understanding of the general skewing problem. In its most general form a skewing scheme is any mapping $s : \mathbb{Z} \times \ldots \times \mathbb{Z}$ (d-fold) $\rightarrow A$, where A is a finite set of M elements ("bank names"). As skewing schemes are required to be readily computable, Shapiro [9] defined a scheme s to be practical ("periodic") if for all $(i_1, \ldots, i_d) \in \mathbb{Z} \times \ldots \times \mathbb{Z}$, $s(i_1 \ldots, i_d)$ can be computed by first reducing the indices according to a suitable modulus and next performing a table look-up. Wijshoff & van Leeuwen [11] generalized this notion and defined a skewing scheme to be "periodic" if and only if there is a lattice $L^d \subseteq \mathbb{Z} \times \ldots \times \mathbb{Z}$ such that $p \equiv_{L^d} q$ precisely when $s(p) = s(q)$ for all $p,q \in Z \times \ldots \times Z$. Up to renaming it means that a periodic skewing scheme is an epimorphism $s : \mathbb{Z}^d \rightarrow A$ with $\mathrm{Ker}(s) = L^d$, which implies that A is isomorphic to $\mathbb{Z}^d / L^d$, a finite abelian group (cf. [11]). In [14] this connection to lattice-theory was exploited to obtain elegant computational characterizations of periodic skewing schemes in all dimensions.

Traditionally, all skewing schemes considered for practical implementation in the engineering literature are "linear", i.e., described by a formula of the type $s(i_1, \ldots, i_d) = \lambda_1 i_1 + \ldots + \lambda_d i_d \pmod M$ for suitably chosen coefficients $\lambda_1, \ldots, \lambda_d \in \mathbb{Z}$. One readily verifies that every linear skewing scheme is periodic. Beside the computational simplicity, there are

mathematical reasons for emphasizing linear skewing schemes. By utilizing Kronecker's version of the Fundamental Theorem for Finite Abelian Groups, Wijshoff & van Leeuwen [14] showed that (i) every d-dimensional periodic skewing scheme corresponds to a d-tuple of linear forms and (ii) a periodic skewing scheme s is linear if and only if $\mathbb{Z}^d/_L d$ is cyclic. If follows that for M prime (a case advocated in studies of conflict-free access, cf. Lawrie [7] and Lawrie & Vora [8]) every periodic skewing scheme using M memory banks is necessarily linear, for the simple reason that a group (viz. $\mathbb{Z}^d/_L d$) with a prime number of elements is necessarily cyclic.

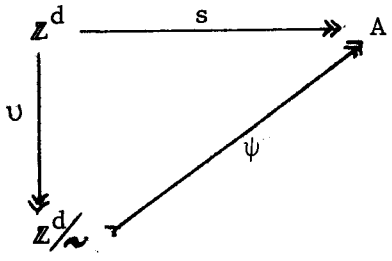
In this paper we further extend the theory of periodic skewing schemes, by exploiting the close connections to the classical theory of finite abelian groups. In section 2 we present basic definitions and give a (re-)appraisal of some observations of Lawrie ([7]) in the group-theoretic setting. In section 3 we explicate the connection between periodic skewing schemes and finite abelian groups. In section 4 we show that the periodic skewing schemes can be completely classified into equivalence "types", and a normal form theorem is derived. The results heavily rely on the characterization of the automorphisms of finite abelian groups. In section 5 it is shown that the number of non-equivalent linear skewing schemes using M memory banks is bounded by $O(M^{d-1}\text{loglog } M)$, thus generalizing an observation of [13] for the case d=2.

The mathematical background for this paper is available from advanced texts on algebra (e.g. Goldhaber & Ehrlich [2]) or group theory (viz. Kurosh [6]). Throughout this paper we use the following notations :

| | |
|---|---|
| s | a skewing scheme, |
| $(i_1 \ldots, i_d)$ | an element of $\mathbb{Z}^d$, |
| M | the number of memory banks utilized, |
| A | a finite abelian group of M elements, |
| Aut(A) | the group of automorphisms of A, |
| $\oplus$ | the direct sum (of abelian groups), |
| $\otimes$ | the direct product (of automorphism groups), |
| $\twoheadrightarrow$ | a surjection (e.g. an epimorphism), |
| $\rightarrowtail\!\!\!\!\twoheadrightarrow$ | a bijection (e.g. an isomorphism), |
| $\circ$ | composition of mappings, |
| $\cong$ | isomorphism. |

2. Skewing schemes and conflict-free access. A general d-dimensional skewing scheme is defined to be any surjective mapping $s : \mathbb{Z}^d \twoheadrightarrow A$, where A is a finite set of M elements. The elements of A denote the M parallel memories that are

available for storing data. Let "~" denote the equivalence relation on $\mathbb{Z}^d$ defined such that for all $p,q \in \mathbb{Z}^d$ : $p \sim q$ iff $s(p) = s(q)$. Since A is finite, the equivalence ~ is necessarily of finite index. Let $\mathbb{Z}^d/\sim$ denote the set of equivalence classes of ~ and $\upsilon : \mathbb{Z}^d \twoheadrightarrow \mathbb{Z}^d/\sim$ the natural projection. It follows that there must exist a bijection $\psi$ such that the following diagram commutes :




The following definition formalizes the corresponding notion in Shapiro [9] and Wijshoff & van Leeuwen [12].

Definition. A skewing scheme $s : \mathbb{Z}^d \twoheadrightarrow A$ is called periodic if and only if ~ is a congruence relation with respect to the free abelian group structure of $\mathbb{Z}^d$.

If s is periodic, then $A \cong \mathbb{Z}^d/\sim$ and (hence) A is identified with a finite abelian factor group of $\mathbb{Z}^d$ with (necessarily) d generators. Conversely every epimorphism $s : \mathbb{Z}^d \twoheadrightarrow A$ with A a finite abelian group is seen to be a periodic skewing scheme.

Skewing schemes are usually called equivalent (cf. [13]) if they differ merely by the naming of the memory banks. More precisely, $s_1 : \mathbb{Z}^d \twoheadrightarrow A_1$ and $s_2 : \mathbb{Z}^d \twoheadrightarrow A_2$ are equivalent if and only if there is a bijection $\varphi : A_1 \twoheadrightarrow A_2$ such that $\varphi \circ s_1 = s_2$.

Proposition 2.1. Let $s_1 : \mathbb{Z}^d \twoheadrightarrow A_1$ and $s_2 : \mathbb{Z}^d \twoheadrightarrow A_2$ be periodic skewing schemes, where $A_1$ and $A_2$ are finite abelian groups, and let $\varphi : A_1 \twoheadrightarrow A_2$ be a bijection such that $\varphi \circ s_1 = s_2$. Then $\varphi$ is an isomorphism of abelian groups.

The observation in proposition 2.1 leads to the following "program" for classifying the periodic skewing schemes $s : \mathbb{Z}^d \twoheadrightarrow A$, with A a finite abelian group. First let A run through the isomorphism types of all finite abelian groups with d generators. Next, for each such A consider the action of the automorphism group Aut(A) on the set of all epimorphisms (read : periodic

skewing schemes) $s : \mathbb{Z}^d \twoheadrightarrow A$ defined by $\alpha(s) = \alpha \circ s$, for $\alpha \in \mathrm{Aut}(A)$. The orbits of this action precisely correspond to the equivalence classes of periodic skewing schemes.

Linear skewing schemes have traditionally played a central role in all applications of skewed matrix storage (see e.g. [4], [5], [7]).

Definition. A skewing scheme $s : \mathbb{Z}^d \twoheadrightarrow A$ is called linear if and only if $A \cong \mathbb{Z}_M$ and for all $(i_1, \ldots, i_d) \in \mathbb{Z}^d : s(i_1, \ldots, i_d) = \lambda_1 i_1 + \ldots + \lambda_d i_d \pmod{M}$, for suitably chosen and fixed constants $\lambda_1, \ldots, \lambda_d \in \mathbb{Z}$.

One readily verifies that every linear skewing scheme is periodic.

Proposition 2.2. ([14]) A periodic skewing scheme $s : \mathbb{Z}^d \twoheadrightarrow A$ is linear if and only is A is a cyclic finite abelian group.

Skewing schemes are designed such that desired collections ("vectors") of at most M elements each can be retrieved conflict-free from the parallel memories. In several studies of conflict-free access it has been suggested to choose M prime (see Lawrie [7], Lawrie & Vora [8], Wijshoff & van Leeuwen [13]). This choice severely limits the type of skewing scheme that one can use, in view of the following fact.

Proposition 2.3. ([14]) If M is square-free (e.g. a prime), then every periodic skewing scheme using M memory banks is necessarily linear.

Proof.

Every finite abelian group of square-free order is necessarily cyclic. Now apply proposition 2.2. □

Although we shall not study the property of conflict-free access in much detail here, a further observation is of interest. The rows, columns, and diagonals of a $N \times \ldots \times N$ (d-fold) matrix are easily parametrized into the form $p+\lambda q$ for fixed $p,q \in \mathbb{Z}^d$ and $\lambda \in \{0, .., N-1\}$, and a periodic skewing scheme $s : \mathbb{Z}^d \twoheadrightarrow A$ will map the elements to banks $s(p)+\lambda s(q)$ (where the latter "+" denotes addition in A). This led Lawrie [7] to the paradigm of an "ordered" vector, which now takes the following form.

Definition. Let A be a finite abelian group. A $\gamma$-ordered k-vector ($\gamma \in A$, $k \geq 1$) is any vector of k elements whose $i^{th}$ logical element is mapped to bank $\delta + i\gamma$, for a suitable $\delta \in A$ and $0 \leq i < k$.

Thus rows, columns, and diagonals are all $\gamma$-ordered k-vectors for suitable $\gamma$ and k, when a periodic skewing scheme is used. Lawrie's main observation was that a $\gamma$-ordered k-vector with $\gamma \in \mathbb{Z}_M$ can be accessed conflict-free if and only if $M \geq k \cdot \gcd(\gamma, M)$ (see [7], [12], [13]). The result is easily understood in the present framework. Let $\mathrm{ord}(\gamma)$ denote the order of $\gamma$ in A, an abelian group of M elements.

Proposition 2.4. A $\gamma$-ordered k-vector ($\gamma \in A, k \geq 1$) can be accessed conflict-free if and only if $\mathrm{ord}(\gamma) \geq k$.

Proof.

Conflict-freeness means that $\delta + i\gamma \neq \delta + j\gamma$ for $i \neq j$, $0 \leq i, j \leq k$. It is equivalent to the condition that $i\gamma \neq 0$ for $i = 1, \ldots, k-1$ and hence to $\mathrm{ord}(\gamma) \geq k$. □

Note that when A is cyclic, the order of an element $\gamma$ ($\gamma \in \mathbb{Z}_M$ generator of A) is simply $M/\gcd(\gamma, M)$ and Lawrie's result follows. The following observation leads perhaps to the most compelling reason for the restriction to linear skewing schemes in practice.

Theorem 2.5. Let s be a periodic skewing scheme using M memory banks, and suppose s yields conflict-free access to some $\gamma$-ordered k-vector for $k > M/2$. Then s is linear.

Proof.

By proposition 2.4 we have $\mathrm{ord}(\gamma) > M/2$ and hence $\mathrm{ord}(\gamma) \mid M$ because $\mathrm{ord}(\gamma) \mid M$ by elementary group theory, if follows that $\mathrm{ord}(\gamma) = M$. Thus $\gamma$ is a generator of A, and A is cyclic. The result now follows from proposition 2.2. □

We conclude that if we want a periodic skewing scheme to be conflict-free on even a single row (or column or diagonal) of a Mx ... xM matrix, then the skewing scheme is necessarily linear. See Wijshoff & van Leeuwen [13] for a further analysis of this case.

3. The classification of periodic skewing schemes. In order to work out the program for classifying the periodic skewing schemes as suggested in section 2, we have to delve deeply into the structure theory of finite abelian groups. First we review the (known) facts concerning the isomorphism types of finite abelian groups, which will enable us to derive the connection between periodic skewing schemes and d-tuples of linear forms rather directly (cf. Wijshoff & van Leeuwen [14]). Next we derive a characterization

of Aut(A). The results will be used in section 4 to prove a normal form theorem for periodic skewing schemes, thus completing the classification effort.

Let A be an arbitrary finite abelian group of M elements, and let $M = p_1^{e_1} \ldots p_r^{e_r}$ (the factorization of M into distinct primes). A has a unique decomposition as a direct sum $A = A_1 \oplus \ldots \oplus A_r$, where the $A_i$ are abelian p-groups of coprime order. (In fact, for $1 \leq i \leq r$, $A_i$ is the Sylow subgroup of order $p_i^{e_i}$.) For $1 \leq i \leq r$, let $\pi_i : A \twoheadrightarrow A_i$ be the implied projection morphism. For a periodic skewing scheme (or: epimorphism) $s : \mathbb{Z}^d \twoheadrightarrow A$, let $s_i = \pi_i \circ s$.

Proposition 3.1. The mapping $s \mapsto (s_1, \ldots, s_r)$ is a bijection between the set of all periodic schemes $s : \mathbb{Z}^d \twoheadrightarrow A$ and the set of all r-tuples $(t_1, \ldots, t_r)$ of periodic skewing schemes $t_i : \mathbb{Z}^d \twoheadrightarrow A_i$ $(1 \leq i \leq r)$.

We also note that $\mathrm{Aut}(A) = \mathrm{Aut}(A_1) \otimes \ldots \otimes \mathrm{Aut}(A_r)$ and that, consequently, two periodic skewing schemes s and s' are conjugate under Aut(A) if and only if the corresponding $s_i$ and $s_i'$ are conjugate under $\mathrm{Aut}(A_i)$ for $1 \leq i \leq r$. This shows that the classification of periodic skewing schemes $s : \mathbb{Z}^d \twoheadrightarrow A$ reduces to the case where A can be assumed to be a finite abelian p-group.

To complete the description we note that a finite abelian p-group can be uniquely decomposed as the direct sum of cyclic p-groups. Hence $A_i \cong \mathbb{Z}_{p_i^{e_{i1}}} \oplus \ldots \oplus \mathbb{Z}_{p_1^{e_{id}}}$ for suitable $e_{i1} \geq \ldots \geq e_{id} \geq 0$ with $e_{i1} + \ldots + e_{id} = e_i$ and $1 \leq i \leq r$, and assuming that A is a d-generator group. (The $p_i^{e_{i1}}, \ldots, p_i^{e_{id}}$ are known as the invariants of the abelian p-group.) For $1 \leq i \leq d$, let $f_j = p_1^{e_{1j}} \ldots p_r^{e_{rj}}$ denote the "invariant factors" of A. Observe that $f_{j+1} \mid f_j$ for $1 \leq j < d$ and by the Chinese Remainder Theorem one also has $\mathbb{Z}_{f_j} \cong \mathbb{Z}_{p_1^{e_{ij}}} \oplus \ldots \oplus \mathbb{Z}_{p_r^{e_{rj}}}$. It follows that $A \cong \mathbb{Z}_{f_1} \oplus \ldots \oplus \mathbb{Z}_{f_d}$, a direct sum of cyclic groups.

Theorem 3.2. ([14]) Every periodic skewing scheme $s : \mathbb{Z}^d \twoheadrightarrow A$ can be uniquely represented by a d-tuple $(L_1 \bmod f_1, \ldots, L_d \bmod f_d)$, where $L_1$ through $L_d$ are integer linear forms and $f_1$ through $f_d$ are the invariant factors of A.

Proof.

s uniquely corresponds to the d-tuple $(\bar{s}_1, \ldots, \bar{s}_d)$, where $\bar{s}_j = \pi_j \circ s$ and $\pi_j : A \twoheadrightarrow \mathbb{Z}_{f_j}$ are the projections corresponding to the composition above $(1 \leq j \leq d)$. By proposition 2.2 every $\bar{s}_j$ is a linear skewing scheme. □

Note that the component expressions for s are build up, using the Chinese Remainder Theorem, from the (linear) expressions corresponding to the projected skewing schemes: $\mathbb{Z}^d \twoheadrightarrow \mathbb{Z}_{p_k^{e_{kj}}}$ $(1 \leq k \leq r,\ 1 \leq j \leq d)$, which are all linear skewing schemes by proposition 2.2.

Restricting to the case of finite abelian p-groups A, assume that $A \cong \mathbb{Z}_{p^{e_1}} \oplus \ldots \oplus \mathbb{Z}_{p^{e_m}}$ for suitable $e_1 \geq \ldots \geq e_m > 0$ and $m \leq d$. For classifying the periodic skewing schemes in A's isomorphism type, we need a precise understanding of the action of Aut(A). Write the elements $\alpha$ of A as vectors $\alpha = (\alpha_1, \ldots, \alpha_m)^T$, where $\alpha_i$ is the residue of $\alpha$ in $\mathbb{Z}_{p^{e_i}}$ $(1 \leq i \leq m)$. A general result due to Shoda [10] (Satz 1) is the following.

Theorem S. The automorphisms of A can be represented by $m \times m$ matrices $\chi = (x_{ij})$ with columns that are generators of A and $p^{e_i - e_j} \mid x_{ij}$ for $i \leq j$.

The action of $\chi$ on A and the composition of two automorphisms are derived from the usual matrix-vector and matrix-matrix product. A matrix $\chi$ represents a proper automorphism of A if and only if $\det \chi \not\equiv 0 \pmod{p}$.

Theorem 3.3. Let $A \cong \mathbb{Z}_{p^{e_1}} \oplus \ldots \oplus \mathbb{Z}_{p^{e_m}}$ be a finite abelian p-group, with $e_1 \geq \ldots \geq e_m > 0$. Aut(A) is generated by all automorphisms ("matrices") $\chi$ having one of the following forms :

(a) $\chi$ interchanges the $i^{th}$ and $j^{th}$ component of elements, for fixed i and j with $e_i = e_j$.

(b) $\chi$ multiplies a single (fixed) component of elements by a (fixed) integer $\not\equiv 0$ modulo p.

(c) $\chi$ adds an integer multiple of the $j^{th}$ component to the $i^{th}$ component of elements, using a (fixed) integer multiplier divisible by $\lceil p^{e_i - e_j} \rceil$.

Proof.

One easily verifies that the mappings $\chi$ of the form (a), (b), and (c) are automorphisms of A. Consider any automorphism of A and view it, using theorem S, as a matrix $\chi = (x_{ij})$ with $p^{e_i - e_j} \mid x_{ij}$ for $i \leq j$ and $\det \chi \not\equiv 0 \pmod{p}$. By repeated premultiplication with matrices of type (a), (b), and (c) one can transform $\chi$ into the identity matrix, by following a suitable version of the Gauss-Jordan algorithm. Thus the automorphisms of type (a), (b), and (c) generate Aut(A). □

4. A normal form for (general) periodic skewing schemes. Let $s : \mathbb{Z}^d \twoheadrightarrow A$ be any d-dimensional periodic skewing scheme. By proposition 3.1 we may assume

that A is a finite abelian p-group, and (hence)
$A \cong \mathbb{Z}_{p^{e_1}} \oplus \ldots \oplus \mathbb{Z}_{p^{e_m}}$ for suitable $e_1 \geq \ldots \geq e_m > 0$ and $m \leq d$. As $\mathbb{Z}^d$ is a free abelian group (of rank d), the homomorphisms from $\mathbb{Z}^d$ to A uniquely correspond to the mxd matrices $T = (t_{ij})$ with $t_{ij} \in \mathbb{Z}_{p^{e_i}}$ whose columns can be regarded as the elements of A that are the images of the standard basis of $\mathbb{Z}^d$. A matrix T of this form represents a periodic skewing scheme (an epimorphism) if and only if the columns of T generate A. To obtain a classification of the periodic skewing schemes $s : \mathbb{Z}^d \twoheadrightarrow A$, we must classify the matrices T modulo the action of the automorphisms of A as described in theorem S. The normal forms will be suitable representatives from the resulting equivalence classes.

For the analysis we have to delve into the subgroup structure of the component p-groups $\mathbb{Z}_{p^e}$ of A. A cyclic p-group $\mathbb{Z}_{p^e}$ has precisely e+1 subgroups, which are all cyclic p-groups and form a "tower" (or: a composition series). In fact, it are precisely the subgroups $p^k.\mathbb{Z}_{p^e}$ (generated by $p^k$) for k=0,1, ..., e. For $i \leq j$, let $C_{ij}$ be a fixed system of coset representations of $p^{e_i-e_j}.\mathbb{Z}_{p^{e_i}}$ in $\mathbb{Z}_{p^{e_i}}$ and let $\tilde{C}_{ij}$ be a fixed system of coset representatives of $p^{e_i-e_j}\,\mathbb{Z}_{p^{e_i}}$ in $p.\mathbb{Z}_{p^{e_i}}$. One may take $C_{ij} = \{ 0,1,2, \ldots, p^{e_i-e_j-1} \}$ and, provided $e_i > e_j$, $\tilde{C}_{ij} = \{ 0,p,2p, \ldots, p^{e_i-e_j-p} \}$. If $e_i = e_j$ we let $\tilde{C}_{ij} = \{0\}$. Hence $|C_{ij}| = p^{e_i-e_j}$ and $|\tilde{C}_{ij}| = \lceil p^{e_i-e_j-1} \rceil$.

Let $s : \mathbb{Z}^d \twoheadrightarrow A$ be a periodic skewing scheme, and T the matrix representing s. Denote the $j^{th}$ column of T by $T_j$ $(i \leq j \leq d)$.

Definition. s is said to have normal form if the following properties hold :

(i) there are column indices $j_1, \ldots, j_m$ (written such that $j_k < j_l$ whenever $e_k = e_l$ and $k < l$) such that $T_{j_k} = (x_1, \ldots, x_{k-1}, 1, 0, \ldots, 0)^T$, with $x_i \in C_{ik}$ if $j_i < j_k$ and $x_i \in \tilde{C}_{ik}$ if $j_i > j_k$ for $1 \leq i < k$.

(ii) for every column index $j \notin \{ j_1, \ldots, j_m \}$ and corresponding column $T_j = (x_1, \ldots, x_m)^T$ one has $x_i \in \mathbb{Z}_{p^{e_i}}$ if $j_i < j$ and $x_i \in p.\mathbb{Z}_{p^{e_i}}$ $j_i > j$, for $1 \leq i \leq m$.

In the definition the columns $j_1, \ldots, j_m$ are called the basis columns of s (or: of T), and the remaining columns are called the non-basis columns of s. For every k $(1 \leq k \leq m)$ the index $j_k$ refers to the left-most column of T having a generator of $\mathbb{Z}_{p^{e_k}}$ in its $k^{th}$ component. (Hence, trivially, the basis columns of T generate A.)

Theorem 4.1. (Normal Form Theorem)

(i) Every periodic skewing scheme $s : \mathbb{Z}^d \to A$ is equivalent to a periodic skewing scheme that has normal form.

(ii) Different periodic skewing schemes in normal form are not equivalent.

Proof.

(By proposition 2.1 two periodic skewing schemes $s_{1,2} : \mathbb{Z}^d \to A$ are equivalent if and only if $s_1$ and $s_2$ are conjugate under the action of Aut(A).)

(i) Let $s : \mathbb{Z}^d \to A$ be an arbitrary periodic skewing scheme, and T the $m \times d$ matrix representing s. We show that s can be transformed to normal form by a step-wise procedure, using the action of suitably chosen automorphisms of type (a), (b) and (c) (cf. theorem 3.3).

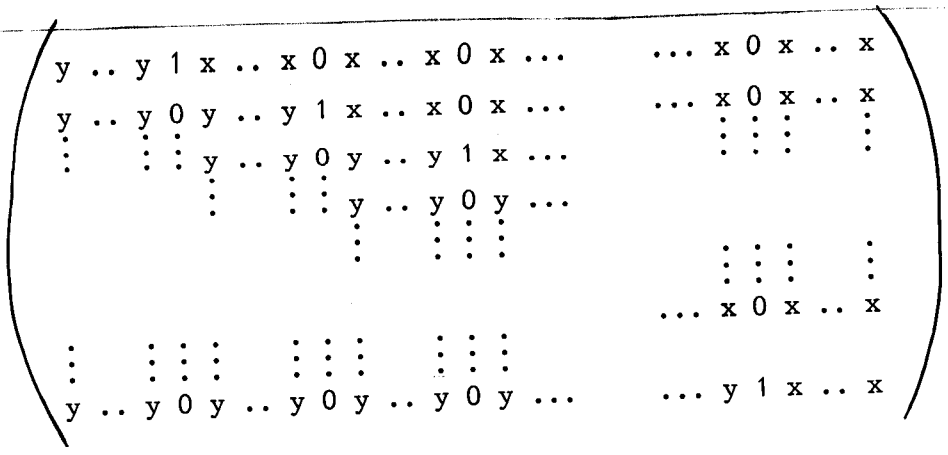
As the columns of T generate A, there must be a column of maximal order in A. Choose $j_1$ to be the index of the leftmost column of this kind, necessarily containing a generator of $\mathbb{Z}_p e_1$ among its components. Use operations of type (a) and (b) to obtain an entry 1 in the first position of the column, and use operations of type (c) to make the lower entries vanish. Proceeding inductively, assume that we have obtained columns $j_1, \ldots, j_k$ as required in the normal form. Let $k < m$. Because the columns of T generate A and observing the structure of the columns $j_1, \ldots, j_k$, there must be a leftmost column $j_{k+1}$ in T which has an entry in one of the components $k+1, k+2, \ldots$ which generates $\mathbb{Z}_p e_{k+1}$. Use operations of type (a), (b), and (c) as before to obtain an entry 1 in position k+1 of the column and zeroes below it. (Note that these operations do not affect the structure of the columns $j_1, \ldots, j_k$ because they are zero in all positions $\geq k+1$.) As for the upper entries of column $j_{k+1}$, we observe the following. Let $x_i$ be the entry in position i, for some $i < k+1$. Suppose that $x_i \notin p\mathbb{Z}_p e_i$, i.e., $x_i$ is a generator of $\mathbb{Z}_p e_i$, but $j_i > j_{k+1}$. This contradicts the choice of $j_i$. Hence we can use operations of type (c) in order to change the upper entries into coset representatives of the desired characteristic. (Note that again the structure of the columns $j_1, \ldots, j_k$ is not affected by these operations.) By continuing this process T is transformed to normal form.

(ii) Let $s,s' : \mathbb{Z}^d \to A$ be different periodic skewing schemes and $T,T'$ the corresponding matrices, and suppose that both s and s' have normal form. We show that s and s' cannot be conjugate under the action of Aut(A).

Let $j_1, \ldots, j_m$ and $j'_1, \ldots, j'_m$ be the indixes of the basis columns of T and T', respectively. Suppose that the two sequences are not equal, i.e., let $j_1 = j'_1, \ldots, j_{i-1} = j'_{i-1}$ but $j_i \neq j'_i$ for some $1 \leq i \leq m$. Without loss of generality, let $j_i < j'_i$. By the structure of the basis columns it follows that $T_{j_1}, \ldots, T_{j_i}$ generate a subgroup of A whose order is greater than the order of the subgroup generated by $T'_{j_1}, \ldots, T'_{j_i}$. In this case T and T' cannot be conjugate under Aut(A). Suppose next that the two index sequences are equal, i.e., $j_i = j'_i$ for every $1 \leq i \leq m$. We show that any automorphism $\chi \in$ Aut(A) that maps the basis $T_{j_1}, \ldots, T_{j_m}$ (of A) onto the basis $T'_{j_1}, \ldots, T'_{j_m}$ (of A) must be the identity. Clearly $T_{j_1}$ and $T'_{j_1} = \chi(T_{j_1})$ coincide, as both are equal to the first unit vector. Proceeding inductively, assume that $T_{j_i}$ and $T'_{j_i} = \chi(T_{j_i})$ coincide for $i = 1, \ldots, k$. Let $k < m$. By order considerations we have $T'_{j_{k+1}} = \chi(T_{j_{k+1}})$. Because of the structure of the basis columns, there exist integer coefficients $x_i (1 \leq i \leq k)$ such that $T_{j_{k+1}} = u_{k+1} + \sum_1^k x_i T_{j_i}$ (where $u_{k+1}$ is the $(k+1)^{st}$ unit vector). It follows that $\chi(T_{j_{k+1}}) = \chi(u_{k+1}) + \sum_1^k x_i \chi(T_{j_i}) = \chi(u_{k+1}) + \sum_1^k x_i T_{j_i}$ and (hence) $T'_{j_{k+1}} - T_{j_{k+1}} = \chi(u_{k+1}) - u_{k+1}$. By theorem S (applied to $\chi$) we conclude that the coset representatives in the upper diagonal positions of $T'_{j_{k+1}}$ and $T_{j_{k+1}}$ necessarily coincide. Thus $T_{j_{k+1}}$ and $T'_{j_{k+1}} = \chi(T_{j_{k+1}})$ coincide as complete vectors. By induction we conclude that $\chi$ must be the identity. This contradicts that s and s' are different. □

We conclude from theorem 4.1 that every periodic skewing scheme can be transfored to a unique (equivalent) normal form.

The existence of unique normal forms is intrumental for counting the number of "essentially different", i.e., non-equivalent, periodic skewing schemes. As an example, we count the number of non-equivalent periodic skewing schemes $s : \mathbb{Z}^d \to A$ where the underlying p-group A has the form $A \cong \mathbb{Z}_{p^e} \oplus \ldots \oplus \mathbb{Z}_{p^e}$ (m summands). One verifies that the normal forms are mxd matrices of the following form :



where the basis columns (unit vectors in this case) occur in m selected positions $j_1, \ldots, j_m$ and the x's and y's denote arbitrary elements of $\mathbb{Z}_p e$ and $p\mathbb{Z}_p e$, respectively. Every matrix (in normal form) represents a unique equivalence class of periodic skewing schemes, and conversely. The number of different normal forms is seen to be

$$\sum_{j_o < j_1 < .. < j_m < j_{m+1}} \prod_{i=o}^{m} p^{(j_{i+1}-j_i-1)(i.e + (m-i)(e-1))}$$

where $j_0 = 0$ and $j_{m+1} = d+1$ are fixed and the summation ranges over all choices of $j_1,\ldots,j_m$. Further manipulation shows this number to be equal to

$$p^{(d-m)(m-1)(e+1) + \frac{1}{2}m(m-1)+d} \sum_{o < j_1 < \ldots < j_m < d+1} \frac{1}{p^{j_1+ \ldots +j_m}}.$$

5. The number of non-equivalent linear skewing schemes. In section 2 we argued that all periodic skewing schemes of practical use in supercomputer computations are likely to be linear. Indeed, the engineering literature on the subject has largely focussed on the analysis of linear skewing schemes for the purposes of d-dimensional array storage. In a recent study Wijshoff & van Leeuwen [13] showed that the number of non-equivalent linear skewing schemes in the usual 2-dimensional case is surprisingly small and bounded by O(M loglog M), where M is the number of memory banks being used. In this section we apply our results on normal forms to obtain a precise expression for the number of non-equivalent linear skewing schemes in the general case and a feasible procedure for enumerating these schemes.

In section 2 we defined a linear skewing scheme to be any epimorphism $s: \mathbb{Z}^d \longrightarrow \mathbb{Z}_M$. Let $M = p_1^{e_1} \ldots p_r^{e_r}$ (the factorization of M into distinct primes). By the Chinese Remainder Theorem $\mathbb{Z}_M$ can be decomposed as a direct sum $\mathbb{Z}_M = \mathbb{Z}_{p_1^{e_1}} \oplus \ldots \oplus \mathbb{Z}_{p_r^{e_r}}$. Every (projected) linear skewing scheme $s_i = \pi_i \circ s : \mathbb{Z}^d \longrightarrow \mathbb{Z}_{p_i^{e_i}}$ can be described by a 1 x d matrix $T_i$ whose (single) row contains at least one component that is a generator of $\mathbb{Z}_{p_i^{e_i}}$. Observe that the results of section 4 apply (use m=1, a direct approach is given in [11]). It follows that the non-equivalent $s_i$'s can be enumerated by simply enumerating the normal forms, which are described as the 1 x d matrices of the type $(y_1, \ldots, y_{j-1}, 1, x_{j+1}, \ldots, x_d)$ with $1 \leq j \leq d$, $x_k \in \mathbb{Z}_{p_i^{e_i}}$ $(j+1 \leq k \leq d)$, and $y_l \in p_i.\mathbb{Z}_{p_i^{e_i}}$ $(1 \leq l \leq j-1)$. According to proposition 3.1 and the arguments in section 3, the combinations of normal forms for the $s_i$ $(1 \leq i \leq r)$ precisely characterize the equivalence classes of linear skewing schemes s. The enumeration of the non-equivalent linear skewing schemes now follows by a trivial algorithm.

Theorem 5.1. The number of non-equivalent linear skewing schemes $s : \mathbb{Z}^d \longrightarrow \mathbb{Z}_M$ is bounded by $M^{d-1} . \prod_{i=1}^{r} \frac{p_i}{p_i - 1}$.

Proof.

There are precisely $\sum_{j=1}^{d} p_i^{(d-1)e_i - j + 1} = (p_i^{e_i})^{d-1} \sum_{j=1}^{d} 1/p_i^{j-1} =$ $(p_i^{e_i})^{d-1} . \frac{1 - 1/p_i^d}{1 - 1/p_i}$ different normal forms for every $s_i$ $(1 \leq i \leq r)$.

The number of non-equivalent linear skewing schemes is thus given by

$$\prod_{i=1}^{r} (p_i^{e_i})^{d-1} . \frac{1 - 1/p_i^d}{1 - 1/p_i} = M^{d-1} . \prod_{i=1}^{r} \frac{1 - 1/p_i^d}{1 - 1/p_i} < M^{d-1} \prod_{i=1}^{r} \frac{p_i}{p_i - 1} \quad . \; \square$$

Corollary 5.2. The number of non-equivalent linear skewing schemes $s : \mathbb{Z}^d \longrightarrow \mathbb{Z}_M$ is bounded by $O(M^{d-1} \log \log M)$.

Proof.

Let $q_1, \ldots, q_r$ be the first r primes. From number theory it is known that there are constants $c_1$ and $c_2$ such that $\prod_{1}^{r} \frac{q_i}{q_i - 1} \leq c_1 . \log q_r$ and $q_r \leq c_2 . r \log r$. It follows that $\prod_{i=1}^{r} \frac{p_i}{p_i - 1} \leq \prod_{i=1}^{r} \frac{q_i}{q_i - 1} = O(\log r)$. Clearly $r \leq \log M$, and the result follows by substitution in the bound of theorem 5.1. $\square$

## 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] Goldhaber, J.K., and G. Ehrlich, Algebra, the MacMillan Comp., Toronto, 1970.

[ 3] Hockney, R.W., and C.R. Jesshope, Parallel computers, Hilger, Bristol, 1981.

[ 4] Knowles, M., B. Okawa, Y. Muroaka, and R. Wilhelmson, Matrix operations on ILLIAC IV, Report 222, Dept. of Computer Science, University of Illinois, Urbana, Ill., 1967.

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

[ 6] Kurosh, A.G., The theory of groups, vol. I, translated from the Russian and edited by K.A.Hirsch, Chelsea Publ. Comp., New York, NY, 1956.

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

[ 8] Lawrie, D.H., and C.R. Vora, The prime memory system for array access, IEEE Trans. Comput. C-31 (1982) 435-442.

[ 9] Shapiro, H.D., Theoretical limitations on the efficient use of parallel memories, IEEE Trans. Comput. C-27 (1978) 421-428.

[10] Shoda, K., Über die Automorphismen einer endlichen Abelschen Gruppe, Math. Ann. 100 (1928) 674-686.

[11] Tappe, J., Algebraische Hilfsmittel zur Organisation paralleler Speicher, Informatik-Kolloquium über Parallelverarbeitung, Lessach, 1984.

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

[13] Wijshoff, H.A.G., and J. van Leeuwen, On linear skewing schemes and d-ordered vectors, Techn. Report RUU-CS-83-7, Dept. of Computer Science, University of Utrecht, Utrecht, 1983.

[14] Wijshoff, H.A.G., and J. van Leeuwen, The structure of periodic skewing schemes for parallel memories, Techn. Report RUU-CS-84-1, Dept. of Computer Science, University of Utrecht, Utrecht, 1984. (Revised version to appear in IEEE Trans. Comput.)