vakgroep informatica R.U. Utrecht

A LINEARLY CONDITION FOR PERIODIC SKEWING SCHEMES

H.A.G. Wijshoff

J. van Leeuwen

RUU-CS-83-10

June 1983

Rijksuniversiteit Utrecht

Vakgroep informatica

Budapestlaan 6
Postbus 80.012
3508 TA Utrecht
Telefoon 030–531454
The Netherlands

A LINEARLY CONDITION FOR PERIODIC SKEWING SCHEMES

H.A.G. Wijshoff

J. van Leeuwen

Technical Report RUU-CS-83-10

June 1983

Department of Computer Science

University of Utrecht

P.O. Box 80.012

3508 TA Utrecht

the Netherlands

A LINEARITY CONDITION FOR PERIODIC SKEWING SCHEMES

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

Department of Computer Science, University of Utrecht
P.O. Box 80.002, 3508 TA Utrecht, the Netherlands

Abstract. Skewing schemes are mappings that are used for distributing data (e.g. the elements of an $N \times N$ matrix) over a number of memory modules such that certain configurations of data items can be accessed as "vectors", without conflict. In practice only linear and periodic skewing schemes are used, where the former are extremely easy to evaluate but the latter are more flexible and more general. We present necessary and sufficient conditions for a periodic skewing scheme to be equivalent to a linear skewing scheme.

1. Introduction. The speed and efficiency of computations by vector- and array-processors heavily depend on a suitable distribution of the data in local and global memory. A typical problem arises when e.g. an $N \times N$ matrix must be stored into M memory modules ($M \le N$) such that all vectors of interest (rows, columns, blocks, etc) can be accessed conflict-free in one memory cycle. This means that all elements of such a vector must be stored in different memory modules, in some order. Mappings that attempt to achieve this are called skewing schemes, and were first introduced in the late nineteen sixties (see Kuck [3] and Budnik & Kuck [1]). A skewing scheme simply is a mapping s: $\{0..N-1\} \times \{0..N-1\} \to \{0..M-1\}$ mapping an element a_{ij} to memory module $s(i,j)$ with some additional properties. We assume that the memory modules are numbered from 0 to $M-1$.

Definition. A skewing scheme s is linear if there are constants a and b such that $s(i,j) = ai + bj \pmod M$, for all i and j.

Linear skewing schemes are very easy to evaluate and therefore most commonly used in practice. In the literature (see e.g. Lawrie [4]) several conditions on a, b and M have been formulated for s to be conflict-free on rows, columns and diagonals. Very often M is assumed prime. A detailed analysis of linear skewing schemes was given in [7].

More general skewing schemes are of interest only if they too permit a very compact representation. Shapiro [5] defined a skewing scheme to be "periodic" if it can be described by a finite table (to which all arguments are reduced by using a proper modulus). In [6] it was shown that the subject is best approached through the theory of integral lattices (see e.g. Hardy & Wright [2]). To this end we assume that s is defined on the entire $\mathbb{Z}^2$.

<u>Definition</u>. A skewing scheme s is called regular if and only the following property is satisfied for all cells $p, q \in \mathbb{Z}^2$: if $s(p) = s(q)$ then every pair of cells that are in the same relative position as p and q is mapped to equal memory modules.

<u>Definition</u>. A skewing scheme s is periodic if there exist a lattice L and cells $a_0, \ldots, a_{M-1}$ such that $\forall_{0 \le i \le M-1}\ s^{-1}(i) = a_i + L$.

In [6] is shown that regular schemes are periodic, and conversely. It is also shown in [6] that periodic skewing schemes are described by simple arithmetic expressions, although their evaluation is not as immediate as for linear skewing schemes.

It appears that in many cases periodic skewing schemes can still be described by "linear" formulae. In this paper we shall make this precise, and derive necessary and sufficient conditions for a periodic skewing scheme to be "essentially" linear still. The conditions are entirely number-theoretic of nature, involving only the coordinates of the lattice base.

2. Preliminaries. We shall not use any technical results from the theory of linear skewing schemes. The following observation is important and taken from [7].

Proposition 2.1. Every linear skewing scheme is periodic.

Proof.

Let s be defined by $s(i,j) = ai + bj \pmod{M}$. We shall prove that s is regular, hence periodic. Assume that $s(p) = s(q)$ for some $p = (p_1, p_2)$ and $q = (p_1 + v_1, p_2 + v_2)$. (Here $\vec{v} = (v_1, v_2)$ is the "relative position" of p and q.) It follows that $ap_1 + bp_2 \equiv a(p_1 + v_1) + b(p_2 + v_2) \pmod{M}$, hence that $av_1 + bv_2 \equiv 0 \pmod{M}$. But this is exactly the condition for all pairs of cells in relative position $\vec{v}$ to be mapped to the same bank. Thus s is regular. □

We shall only wish to consider linear schemes $s(i,j) = ai + bj \pmod{M}$ that use all memory modules. Such schemes will be called "proper" and are obtained exactly by requiring that $(a, b, M) = 1$.

WARNING. From now on we shall only consider linear skewing schemes that are proper.

The theory of periodic skewing schemes was developed in [6]. Underlying every periodic skewing scheme there is a lattice L generated by two base vectors $\vec{x}, \vec{y}$ (both $\neq 0$) with $\vec{x} = (x_1, x_2)$ and $\vec{y} = (y_1, y_2)$.

Theorem 2.2 ([6]). Let s be a periodic skewing scheme with underlying lattice L. The number of memory modules used by s is exactly equal to the determinant of L, i.e., $M = \left| \det \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix} \right|$.

By choosing the right base vectors of L we may assume the determinant to be non-negative, i.e., $M = x_1 y_2 - x_2 y_1$.

In the remainder of this section we shall derive the number-theoretic lemmas that we need. The first lemma is well-known but included for the sake of completeness.

Lemma 2.3 Let λ_0, μ_0 be integers satisfying $\lambda_0 u + \mu_0 v = (u,v)$. Then the solutions of the equation $\lambda u + \mu v = k.(u,v)$ are completely characterised by $\lambda = k.\lambda_0 + \tau . v/(u,v)$ and $\mu = k.\mu_0 - \tau . u/(u,v)$, $\tau \in \mathbb{Z}$.

Proof.

$\lambda = k.\lambda_0$ and $\mu = k.\mu_0$ is a special solution of the equation. The difference $\Delta\lambda, \Delta\mu$ between any two solutions must satisfy $\Delta\lambda . u + \Delta\mu . v = 0$. The general solution of $\lambda u + \mu v = 0$ is given by $\lambda = \tau . v/(u,v)$ and $\mu = -\tau . u/(u,v)$, $\tau \in \mathbb{Z}$. The lemma follows. □

Lemma 2.4 Let $(a,b,d) = 1$ and $(c,d) = 1$ and $b \neq 0$. Then there exist m, θ and $k = am + b\theta$ such that $(m,c) = 1$ and $(k,m) = 1$ and $(k,d) = 1$.

Proof.

Take m equal to d "with all factors in common with b removed" (hence m is relatively prime to b) and take θ such that $(\theta, m) = 1$. Because d is relatively prime to c so is m, and we have $(m,c) = 1$. Let $k = am + b\theta$.

Suppose k and m are not relatively prime and have a prime factor f in common. Then $f \mid b\theta$ and, because m (hence f) and θ are relatively prime, necessarily $f \mid b$. But this contradicts that m and b are relatively prime. Hence $(k,m) = 1$.

Next suppose that k and d have a prime factor f in common. If

$f \nmid b$, then $f \mid m$ (by the choice of m) and necessarily $f \mid b\theta$, hence $f \mid \theta$. This contradicts that m and θ are relatively prime. If $f \mid b$, then $f \nmid m$ (by the choice of m) and necessarily $f \mid am$, hence $f \mid a$. But this implies that $f \mid (a,b,d)$, contradicting the assumption that $(a,b,d)=1$. It follows that in both cases a contradiction is reached, and $(k,d)=1$. □

Lemma 2.5 Let u_1, u_2, v_1 and v_2 be integers with $(u_1,u_2,v_1,v_2)=1$ and $\det\begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix} \neq 0$. There exist integers λ and μ such that $(\lambda u_1 + \mu v_1, \lambda u_2 + \mu v_2) = 1$.

Proof.

Clearly the integer linear combinations of u_1 and v_1 and of u_2 and v_2 are multiples of (u_1,v_1) and (u_2,v_2), respectively. Consider the following equations:

$$\begin{aligned} \lambda u_1 + \mu v_1 &= k.(u_1,v_1) \\ \lambda u_2 + \mu v_2 &= m.(u_2,v_2) \end{aligned} \qquad (*)$$

Note that $((u_1,v_1),(u_2,v_2)) = (u_1,u_2,v_1,v_2) = 1$ already by assumption. We will prove the lemma by showing that λ and μ can be chosen such that for the resulting k and m: $(m,(u_1,v_1))=1$ and $(k,m)=1$ and $(k,(u_2,v_2))=1$.

Let λ_1, μ_1, λ_2 and μ_2 be chosen such that $\lambda_1 u_1 + \mu_1 v_1 = (u_1,v_1)$ and $\lambda_2 u_2 + \mu_2 v_2 = (u_2,v_2)$. By lemma 2.3 the solutions to $(*)$ are completely characterised as follows:

$$\begin{aligned} \lambda &= k.\lambda_1 + r.\,{}^{v_1}/_{(u_1,v_1)} = m.\lambda_2 + \theta.\,{}^{v_2}/_{(u_2,v_2)} \\ \mu &= k.\mu_1 - r.\,{}^{u_1}/_{(u_1,v_1)} = m.\mu_2 - \theta.\,{}^{u_2}/_{(u_2,v_2)} \end{aligned} \qquad (**)$$

(for all choices of r and θ, given k and m). Rewrite these equations in matrix form, and define the matrix A as indicated:

$$\underbrace{\begin{bmatrix} \lambda_1 & {}^{v_1}/_{(u_1,v_1)} \\ \mu_1 & -{}^{u_1}/_{(u_1,v_1)} \end{bmatrix}}_{A} \begin{bmatrix} k \\ r \end{bmatrix} = \begin{bmatrix} \lambda_2 & {}^{v_2}/_{(u_2,v_2)} \\ \mu_2 & -{}^{u_2}/_{(u_2,v_2)} \end{bmatrix} \begin{bmatrix} m \\ \theta \end{bmatrix}$$

Claim 2.5.1 $\det(A) = -1$.

Proof.

$\det(A) = -\lambda_1 u_1/(u_1,v_1) - \mu_1 v_1/(u_1,v_1) = -1$ (by the definition of λ_1 and μ_1).

It follows that A has an integer inverse, and one easily verifies that

$$\begin{bmatrix} k \\ r \end{bmatrix} = \begin{bmatrix} u_1/(u_1,v_1) & v_1/(u_1,v_1) \\ \mu_1 & -\lambda_1 \end{bmatrix} \begin{bmatrix} \lambda_2 & v_2/(u_2,v_2) \\ \mu_2 & -u_2/(u_2,v_2) \end{bmatrix} \begin{bmatrix} m \\ \theta \end{bmatrix} =$$

$$= \begin{bmatrix} (\lambda_2 u_1 + \mu_2 v_1)/(u_1,v_1) & (u_1 v_2 - u_2 v_1)/(u_1,v_1)(u_2,v_2) \\ \mu_1\lambda_2 - \mu_2\lambda_1 & (\mu_1 v_2 - \lambda_1 u_2)/(u_2,v_2) \end{bmatrix} \begin{bmatrix} m \\ \theta \end{bmatrix}.$$

Writing $a = (\lambda_2 u_1 + \mu_2 v_1)/(u_1,v_1)$ and $b = (u_1 v_2 - u_2 v_1)/(u_1,v_1)(u_2,v_2)$ we obtain that $k = am + b\theta$. Note that $b \neq 0$. Let $c = (u_1,v_1)$ and $d = (u_2,v_2)$. Note that $(c,d) = 1$.

Claim 2.5.2 $(a,b,d) = 1$.

Proof.

We need two useful equalities that follow after direct substitution of the expressions for a and b:

$$\begin{aligned} u_2/(u_2,v_2) \cdot a + \mu_2 \cdot b &= u_1/(u_1,v_1) \\ v_2/(u_2,v_2) \cdot a - \lambda_2 \cdot b &= v_1/(u_1,v_1) \end{aligned} \qquad (***)$$

Suppose that a, b and d are not relatively prime and have a prime factor f in common. Because $f \mid d$ it follows that $f \mid u_2$ and $f \mid v_2$. But from $(***)$ we conclude that also $f \mid u_1$ and $f \mid v_1$. This contradicts the assumption that $(u_1, u_2, v_1, v_2) = 1$. Hence $(a,b,d) = 1$.

Now apply lemma 2.4 to conclude that there exist m and θ and $k = am + b\theta$ such that $(m,c) = 1$ and $(k,m) = 1$ and $(k,d) = 1$, as required for the proof of the lemma. The choice of m and θ translates into the proper λ and μ by (**). □

Lemma 2.5 has an interesting interpretation in terms of integral lattices. Let L be generated by the vectors $\vec{u} = (u_1, u_2)$ and $\vec{v} = (v_1, v_2)$ with $(u_1, u_2, v_1, v_2) = 1$ and $\det(L) \neq 0$. Then L contains points $p = (p_1, p_2)$ with p_1 and p_2 relatively prime.

3. <u>A linearity condition</u>. A periodic skewing scheme s is not completely characterised by its underlying integral lattice L although all its essential properties concerning conflict-free access to data vectors are. Two periodic skewing schemes that have the same underlying lattice differ only in the names they use, i.e., they are identical after a suitable renaming of the memory modules.

<u>Definition</u>. A periodic skewing scheme s is called linear if and only if there exists a periodic skewing scheme equivalent to s (i.e., with the same underlying lattice) that is linear.

(Thus by proposition 2.1 a periodic skewing scheme is called linear if and only if it is equivalent to a linear skewing scheme.) Note that we only consider skewing schemes that use all memory modules. The main result of this paper can be stated as follows.

<u>Theorem</u> 3.1 Let s be a periodic skewing scheme, with its underlying lattice generated by $\vec{x} = (x_1, x_2)$ and $\vec{y} = (y_1, y_2)$. Then s is linear if and only if $(x_1, x_2, y_1, y_2) = 1$.

The proof requires another technical step first.

<u>Lemma</u> 3.2 Let s be a periodic skewing scheme using M memory mo-

dules, and let its underlying lattice L be generated by $\vec{x} = (x_1, x_2)$ and $\vec{y} = (y_1, y_2)$. Then s is linear if and only if there exist integers λ and μ such that $(\lambda x_1 + \mu y_1, \lambda x_2 + \mu y_2, M) = 1$.

Proof.

By theorem 2.2 M must equal the absolute value of the determinant of L. It is no restriction to let $M = x_1 y_2 - x_2 y_1$. (Otherwise replace $\vec{y}$ by $-\vec{y}$ below, and the resulting μ by $-\mu$.)

Assume first that s is linear. Thus $s(i,j) = ai + bj \pmod M$ for some a and b with $(a, b, M) = 1$. (The latter condition holds because s uses all memory modules, cf. section 2.) L necessarily is the set of all points mapped to module 0. Because $s(b, -a) = 0 \pmod M$ it follows that $(b, -a) \in L$ and (hence) that there are integers λ and μ such that $b = \lambda x_1 + \mu y_1$ and $-a = \lambda x_2 + \mu y_2$. For these λ and μ we thus have $(\lambda x_1 + \mu y_1, \lambda x_2 + \mu y_2, M) = 1$.

Conversely, assume that λ and μ exist that satisfy the condition $(\lambda x_1 + \mu y_1, \lambda x_2 + \mu y_2, M) = 1$. Write $a = -(\lambda x_2 + \mu y_2)$ and $b = \lambda x_1 + \mu y_1$ and consider the (proper) linear skewing scheme t defined by $t(i,j) = ai + bj \pmod M$. We show that t is periodic with lattice L. To this end we first show that t is "constant" on every coset $p + L$ (which implies that all periods of L are periods of t). Write $p = (p_1, p_2)$ and observe the following for every λ' and μ':

$$
\begin{aligned}
t(p_1 + \lambda' x_1 + \mu' y_1, p_2 + \lambda' x_2 + \mu' y_2) &= \\
&= ap_1 + bp_2 - (\lambda x_2 + \mu y_2)(\lambda' x_1 + \mu' y_1) + (\lambda x_1 + \mu y_1)(\lambda' x_2 + \mu' y_2) \equiv \\
&\equiv ap_1 + bp_2 + (\lambda \mu' - \lambda' \mu)(x_1 y_2 - x_2 y_1) \equiv \\
&\equiv ap_1 + bp_2 \pmod M = \\
&= t(p_1, p_2)
\end{aligned}
$$

Next we show that every period of t belongs to L. Let $p = (p_1, p_2)$ and $q = (q_1, q_2)$ be such that $t(p_1, p_2) = t(q_1, q_2)$. It follows that $ap_1 + bp_2 \equiv aq_1 + bq_2 \pmod M$, hence that $a(p_1 - q_1) + b(p_2 - q_2) \equiv 0 \pmod M$. From elementary number theory we know that the general solution of the equation $au + bv \equiv 0 \pmod M$ is given by $u = r \cdot b/(a,b) + \varepsilon \cdot M$ and $v =$

$= -r \cdot {}^{a}/_{(a,b)} + \delta \cdot M$ when $(a,b,M) = 1$, with r and ε and δ arbitrary integers (This follows indirectly from lemma 2.3 because we want to solve every equation $au + bv = k \cdot (a,b)$ with $M | k(a,b)$ which, because M and (a,b) are relatively prime, is equivalent to requiring k to be an arbitrary multiple of M.)

Claim 3.2.1 $(a,b) = (\lambda, \mu)$

Proof

First suppose that λ or μ is zero, say $\mu = 0$. (The case $\lambda = 0$ is similar.) Then $a = -\lambda x_2$ and $b = \lambda x_1$, and $(a,b) = \lambda \cdot (-x_2, x_1)$. If $\lambda = 0$ then the claim is trivially true. Otherwise we show that x_1 and x_2 must be relatively prime. For suppose they are not and have a prime factor f in common. Then $f | a$ and $f | b$ and $f | (x_1 y_2 - x_2 y_1)$, i.e., $f | M$ contradicting that $(a,b,M) = 1$. Thus $(-x_2, x_1) = 1$, and $(a,b) = \lambda = (\lambda, 0)$.

Next suppose that both λ and μ are non-zero. Obviously $(\lambda,\mu) | (a,b)$ and we may as well consider the problem as if λ and μ are relatively prime. (Otherwise apply the argument below to $a' := {}^{a}/_{(\lambda,\mu)}$ and $b' = {}^{b}/_{(\lambda,\mu)}$.) We claim that under this assumption $(a,b) = 1$. For suppose that a and b have a prime factor f in common. One easily verifies that $\mu y_1 \cdot a + \mu y_2 \cdot b = \lambda\mu(x_1 y_2 - x_2 y_1) = \lambda \mu M$ and thus $f | \lambda\mu M$. Now f cannot be a divisor of M because $(a,b,M) = 1$. It also cannot be a divisor of both λ and μ, because λ and μ are assumed relatively prime. Thus $f | \lambda$ but $f \nmid \mu$. (The case $f \nmid \lambda$ and $f | \mu$ is handled analogously.) Since f divides a and b it follows that $f | \mu y_2$ and $f | \mu y_1$, hence that $f | y_2$ and $f | y_1$. But then we also have $f | (x_1 y_2 - x_2 y_1)$, i.e., $f | M$ contradicting that $(a,b,M) = 1$. Thus $(a,b) = 1$

It follows from the claim that $\lambda' = {}^{\lambda}/_{(a,b)}$ and $\mu' = {}^{\mu}/_{(a,b)}$ are both integers.

We conclude that for the equation $a(p_1-q_1)+b(p_2-q_2)\equiv 0 \pmod M$ to hold there must exist integers τ, ε and δ such that

$$p_1-q_1 = \tau(\lambda' x_1+\mu' y_1) + \varepsilon M$$
$$p_2-q_2 = \tau(\lambda' x_2+\mu' y_2) + \delta M.$$

Using again that $M = x_1y_2 - x_2y_1$ we can rewrite this to

$$p_1-q_1 = (\tau\lambda' - \delta y_1 + \varepsilon y_2)x_1 + (\tau\mu' + \delta x_1 - \varepsilon x_2)y_1$$
$$p_2-q_2 = (\tau\lambda' - \delta y_1 + \varepsilon y_2)x_2 + (\tau\mu' + \delta x_1 - \varepsilon x_2)y_2,$$

which shows that $\vec{p}-\vec{q} \in L$, or $p \in q+L$. Thus t has no other periods than those of L, and t and s are equivalent. In particular s is linear. □

We can now put all ingredients together and give a proof of the main theorem.

Theorem 3.1 (recapitulated) s is linear if and only if $(x_1, x_2, y_1, y_2)=1$

Proof.

Let s be periodic as assumed. Suppose s is linear. By lemma 3.2 there are integers λ and μ such that $(\lambda x_1+\mu y_1, \lambda x_2+\mu y_2, M)=1$. Suppose that x_1, x_2, y_1 and y_2 have a prime factor f in common. It follows that $f \mid \lambda x_1+\mu y_1$ and $f \mid \lambda x_2+\mu y_2$ and $f \mid (x_1y_2 - x_2y_1)$, i.e., $f \mid M$ contradicting the relative primality. Hence $(x_1, x_2, y_1, y_2)=1$.

Conversely, let the basis of L be such that $(x_1, x_2, y_1, y_2)=1$. By lemma 2.5 there exist integers λ and μ such that we even have $(\lambda x_1+\mu y_1, \lambda x_2+\mu y_2)=1$. By lemma 3.2 s is linear. □

We conclude that linearity is a property of periodic skewing schemes that is completely characterised by theorem 3.1 and easily tested by inspecting only the coordinates of an arbitrary basis of the underlying lattice.

4. References

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

[2] Hardy, G.H., and E.M. Wright, An introduction to the theory of numbers, 5th ed., Clarendon Press, Oxford, 1979 (1st ed. 1938)

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

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

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

[6] 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.

[7] 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