Parallel Hankel-based Integer GCD

Sidi Mohamed SEDJELMACI

LIPN CNRS UMR 7030,
Université Paris-Nord
Av. J.-B. Clment, 93430 Villetaneuse, France.
E-mail: sms @lipn.univ-paris13.fr

1 Notation and basic results

Let $u \geq v \geq 1$ be two odd integers, where $2^{n-1} < v < 2^n$ with $n \geq 2$ and $v = \sum_{i=0}^{n-1} v_i 2^i$ the binary expansion of v. We consider the sequence $(a) = (a_k)_k$ defined by $a_k = (2^k u) \bmod v$, for any integer $k \geq 0$, or equivalently by $a_{k+1} = 2a_k \bmod v$ with $a_0 = u \bmod v$. Our starting point is the following observation.

Lemma 1: Let $v \geq 1$ be an integer of n bits, i.e.: $2^{n-1} < v < 2^n$ with $n \geq 2$ and $v = \sum_{i=0}^{n-1} v_i 2^i$. Then for any integer a_0, such that $0 < a_0 < v$, and the associated sequence $(a) = (a_i)_i$ defined by $a_{i+1} = 2a_i \bmod v$, for $i \geq 0$, we have

$$i) \qquad \sum_{i=0}^{n-1} v_i\, a_i \equiv 0 \bmod v.$$

$$ii)\ \forall k \geq 0\,, \quad \sum_{i=0}^{n-1} v_i\, a_{i+k} \equiv 0 \bmod v.$$

Proof: Since $vu \equiv 0 \bmod v$, then

$$vu = \sum_{i=0}^{n-1} v_i\, 2^i\, u \equiv \sum_{i=0}^{n-1} v_i\, a_i \equiv 0 \bmod v\,,$$

hence $i)$. For $ii)$, just consider $2^k vu$ instead of vu, for $k > 0$.

Example: If $(u, v) = (246, 177)$ and $a_0 = u \bmod v = 69$, then $n = 8$ and the sequence a is

$$a = \{\, 69, 138, 99, 21, 42, 84, 168, 159, \cdots \}\,.$$

Since $v = 177 = 2^7 + 2^5 + 2^4 + 1$, then

$$a_7 + a_5 + a_4 + a_0 = 159 + 84 + 42 + 69 = 354 \equiv 0 \bmod 177\,.$$

Note that it si not necessary to take $a_0 = u \bmod v$, any other choice of a_0 such that $0 < a_0 < v$ yields the relation modulo v: $a_7 + a_5 + a_4 + a_0 \equiv 0 \bmod v$.

Lemma 1 shows that for a fixed v and for any $0 \leq a_0 < v$, we obtain a set of linear recurrence modulo v. However, it is not always the smaller linear recurrence modulo v. Let $d = \gcd(u, v)$, $M = v/d$. If $d > 1$ then $0 < M < v$ and let $M = \sum_{i=0}^{p-1} m_i 2^i$, with $2 \leq p < n$. Then

$$Mu = \frac{v}{d}\, u = \frac{u}{d}\, v \equiv 0 \bmod v\,,$$

and as in Lemma 1, we obtain

$$\forall k \geq 0\,, \quad \sum_{i=0}^{p-1} m_i\, a_{i+k} \equiv 0 \bmod v\,,$$

which is a smaller linear recurrence modulo v. In the previous example, $\gcd(246, 177) = 3$ and $M = v/3 = 59 = 2^5 + 2^4 + 2^3 + 2 + 1$, so

$$a_5 + a_4 + a_3 + a_1 + a_0 = 84 + 42 + 21 + 138 + 69 = 354 \equiv 0 \bmod 177\,,$$

which a smaller linear recurrence modulo v, since its order is $p = 6$, which less than $n = 8$.

There is another important observation:

It is worth to note that, once v and $0 < a_0 < v$ are fixed, together with their associated sequence (a), then for any $k \geq 0$, the remainder $r_k = ku \bmod v$, can be expressed as linear combination of the finite set of n special remainders a_i. For this purpose the set $\{\, a_0, a_1, \ldots, a_{n-1} \,\}$ will be called a *basis of remainders* for v.

Example: If $v = 177$, then $n = 8$. We have $a_0 = u \bmod v = 69$ and the sequence a is

$$a = \{\, 69, 138, 99, 21, 42, 84, 168, 159, \cdots \}\,,$$

but only the first 8 a_i's, i.e.: $a_0, a_1, \ldots, a_7$ are enough to represent <u>all</u> the remainders.

If $k = 900$, then $900 \equiv 15 \bmod 177$. We obtain $r_{900} = r_{15}$ and

$$r_{900} = r_{15} \equiv a_3 + a_2 + a_1 + a_0 \bmod v \quad \text{since} \quad 15 = 2^3 + 2^2 + 2 + 1\,.$$

As a matter of fact we have $15\, u \bmod v = 3690 \bmod 177 = 150$ and $21 + 99 + 138 + 69 = 327 \equiv 150 \bmod 177$, as expected.

The aim of this paper is: For a given pair of positive integers (v, a_0) and their associated sequence (a) satisfying a linear recurrence modulo v of order $n > 2$, find a smaller linear recurrence modulo v (if any) of order $2 \leq p < n$, i.e.: Find an integer $2 \leq p \leq n - 1$, such that

$$\sum_{i=0}^{p-1} c_i\, a_i \equiv 0 \bmod v \;\;, \;\; \mathrm{c_i} \in \{\, 0, 1 \,\}\,, \quad \text{with} \quad 2 \leq p < n.$$

If such integer p exists then $\gcd(u, v) > 1$ and if $M = \sum_{i=0}^{p-1} c_i\, 2^i$, then $M = \lambda\, v/d\, < v$, for some integer $0 < \lambda < d$, and most of the time $v/M = \gcd(v, a_0)$.

2 Hankel Matrices

Let $(a) = (a_i)_{i\geq 0}$ be a sequence of integers. The Hankel matrix $H_k(a)$ of order n associated to the sequence (a) is defined by $H_n(a) = (a_{ij})$ with $a_{ij} = a_{i+j-2}$, for $1 \leq i\,, j \leq n$ i.e.:

$$H_n = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_1 & a_2 & \cdots & a_n \\ \vdots & \vdots & \vdots & \vdots \\ a_{n-1} & a_n & \cdots & a_{2n-1} \end{pmatrix}.$$

It is well know that Hankel matrices is a useful tool to detect linear recurrence relation from a given sequence (a). Similarly, one can consider Hankel matrices associated to the sequence (a), since we have :

$$\begin{cases} v_0a_0 + v_1a_1 + \cdots + v_{n-1}a_{n-1} \equiv 0 \bmod v \\ v_0a_1 + v_1a_2 + \cdots + v_{n-1}a_n \equiv 0 \bmod v \\ \vdots \\ v_0a_{n-1} + v_1a_n \cdots + v_{n-1}a_{2n-1} \equiv 0 \bmod v. \end{cases}$$

However the main difficulty is that we do not have equalities but only equalities modulo v, i.e.: equality in the ring $A = Z/vZ$.

The advantage of this approach is that there is a link with Hankel matrices and it is well known that all the matrix operations can be achieved in $O(\log^2 n)$ parallel time with a polynomial of processors.

Proposition: If $h_k = \det(H_k)$, for $k \geq 2$, then there exists some integer s_k such that

$$1)\ h_k = (-v)^{k-1}\, s_k$$

$$2)\ \gcd(v, a_0) \mid s_k\,.$$

Proof: For all $i \geq 1$, we have $a_i - 2a_{i-1} \equiv 0 \bmod v$ and let's define the integer λ_i by $\lambda_i = (a_i - 2a_{i-1})/v$. We have $\lambda_i = 0$ if $a_{i-1} < v/2$ and $\lambda_i = -1$ if $a_{i-1} > v/2$. Let L_i be the i-th row of the matrix $H_k(a)$, then replacing the row L_i by $L_i - 2L_{i-1}$ gives arow of $(-\lambda_{i+j}\, v)_j$, for $0 \leq j \leq n-1$. Then, for $i \geq 2$, each element of the i-th row is a multiple of $-v$, so $h_k = \det(H_k) = (-v)^{k-1}s_k$, for some integer s_k and 1) is proved.
2) Let $d = \gcd(v, a_0)$. The first row of the the matrix is formed by $a_0, a_1, \cdots, a_{k-1}$, so its determinant s_k is a linear combination of the a_i's, namely $s_k = \sum_{i=0}^{k-1} c_i\, a_i$, for some integers $c_0, c_1, \cdots, c_{k-1}$. Moreover, $a_i \equiv 0 \bmod d$, for each $0 \leq i \leq k-1$, then $d = \gcd(v, r_1) \mid s_k$.

Corollary:

1) If there exists an index j such that a_j is small enough say the bit-size of v is reduced by at least $\log^{2+\epsilon} n$, for $\epsilon > 0$, then we return a_j. The whole parallel complexity for computing $d = \gcd(v, a_0)$ will be $n/\log^2 n$ which is better then the best known upper bound $n/\log n$.

2) Similarly, if s_k is small enough say the bit-size of v is reduced by at least $\log^{2+\epsilon} n$, for $\epsilon > 0$, then we return such s_k since $d \,|\, s_k$.

3) If $s_{k+1} = 0$ and $s_k \neq 0$, then there exists a linear recurrence of order k, i.e.: $\sum_{i=0}^{k-1} \alpha_i \, a_i = 0$. Let $M = \sum_{i=0}^{k-1} \alpha_i \, 2^i$. If M is even then $M := M/2^t$ such that M is odd. Then $M = \lambda v/d$ and v and a_0 are not coprime, i.e.: $d = \gcd(v, a_0) > 1$.

4) If k is the smallest index such that $h_{k+1} = 0$ and $h_k \neq 0$ for some $k \geq 2$, then there exists a linear recurrence for the the sequence (a). i.e.: $m_0 a_0 + m_1 a_1 + \cdots m_{k-1} a_{k-1} = 0$. So let $M = \sum_{i=0}^{k-1} c_i \, 2^i$. If $2 \leq k < n$, then $M = \lambda v/d$ and v and a_0 are not coprime, i.e.: $d = \gcd(v, a_0) > 1$.

2.1 Some examples:

Recall that $\det(H_k) = h_k(a) = (-v)^{k-1} s_k$ and we only compute the determinant s_k of the matrix S_k where all the factor $-v$ are removed from each j-th row, $2 \leq j \leq k$.

Example 1:
With $(v, a_0) = (13, 5)$, we have $n = 4$ and $d = \gcd(v, a_0) = 1$, we obtain the sequence of remainders $a = \{5, 10, 7, 1, 2, 4, 8, 3, 6, 12, 11, 9, 3, \cdots\}$ and respectively
$s_3 = -2$, $s_4 = 1$, $s_5 = 0$, so by the previous Corollary, $d \,|\, s_4$ and $d = 1$:

$$s_3 = \det S_3 = \begin{pmatrix} 5 & 10 & 7 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix} = -2$$

$$s_4 = \det S_4 = \begin{pmatrix} 5 & 10 & 7 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} = 1$$

$$s_5 = \det S_5 = \begin{pmatrix} 5 & 10 & 7 & 1 & 2 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} = 0\,.$$

Example 2:

For $(v, a_0) = (289, 65)$, we have $n = 4$ and $d = \gcd(v, a_0) = 1$. We obtain the sequence $a = \{\,65, 130, 260, 231, 173, 57, 114, 228, 167, 45, 90, 180, 71, 142, 184, \cdots\}$ and obtain $s_4 = 36$, $s_5 = 29$, $s_6 = -5$, $s_7 = -1$ and $s_8 = 1$:

$$s_4 = \det S_4 = \begin{pmatrix} 65 & 130 & 260 & 231 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} = 36$$

$$s_5 = \det S_5 = \begin{pmatrix} 65 & 130 & 260 & 231 & 173 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix} = 29$$

$$s_6 = \det S_6 = \begin{pmatrix} 65 & 130 & 260 & 231 & 173 & 57 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix} = -5$$

$$s_7 = \det S_7 = \begin{pmatrix} 65 & 130 & 260 & 231 & 173 & 57 & 114 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} = -1$$

$$s_8 = \det S_8 = \begin{pmatrix} 5 & 130 & 260 & 231 & 173 & 57 & 114 & 228 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} = 1$$

Example 3**:**

With $(v, a_0) = (299, 65)$, we have $n = 9$ and $d = \gcd(v, a_0) = 13$, we obtain the sequence of remainders $a = \{65, 130, 260, 221, 143, 286, 273, 247, 195, 91, \cdots\}$ and respectively $s_4 = -39$, $s_5 = 0$, $s_6 = 39$, $s_7 = -26$ and $s_8 = 0$:

$$s_4 = \det S_4 = \begin{pmatrix} 65 & 130 & 260 & 221 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix} = -39$$

$$s_5 = \det S_5 = \begin{pmatrix} 65 & 130 & 260 & 221 & 143 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \end{pmatrix} = -104$$

$$s_6 = \det S_6 = \begin{pmatrix} 65 & 130 & 260 & 221 & 143 & 286 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix} = 39$$

$$s_7 = \det S_7 = \begin{pmatrix} 65 & 130 & 260 & 221 & 143 & 286 & 273 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 \end{pmatrix} = -26$$

$$s_8 = \det S_8 = \begin{pmatrix} 65 & 130 & 260 & 221 & 143 & 286 & 273 & 247 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} = 0\,.$$

Note that $M = v/(\gcd(v, a_0) = 299/13 = 23$ and $d \,|\, (s_7/2) = -13$.