ACTA ARITHMETICA
LXXV.3 (1996)

Minimal multipliers for consecutive Fibonacci numbers

by

K. R. Matthews (Brisbane)

1. Introduction. The Fibonacci and Lucas numbers F_n, L_n (see [2]) are defined by

$$F_1 = F_2 = 1, \quad F_{n+2} = F_{n+1} + F_n, \quad n \ge 1;$$
$$L_1 = 1,\ L_2 = 3, \quad L_{n+2} = L_{n+1} + L_n, \quad n \ge 1.$$

Since

$$F_{n-1}F_n - F_{n-2}F_{n+1} = (-1)^n, \tag{1}$$

it follows that

$$\gcd(F_n, F_{n+1}, \ldots, F_{n+m-1}) = 1 \quad \text{for all } m \ge 2.$$

Consequently, integers $x_1, \ldots, x_m$ exist satisfying

$$x_1F_n + x_2F_{n+1} + \ldots + x_mF_{n+m-1} = 1.$$

We call $(x_1, \ldots, x_m)$ a *multiplier vector*. By equation (1), one such vector is

$$\mathcal{M}_n = ((-1)^nF_{n-1}, (-1)^{n+1}F_{n-2}, 0, \ldots, 0). \tag{2}$$

The problem of finding all multiplier vectors reduces to finding a $\mathbb{Z}$-basis for the lattice Λ of integer vectors $(x_1, \ldots, x_m)$ satisfying

$$x_1F_n + x_2F_{n+1} + \ldots + x_mF_{n+m-1} = 0.$$

It is easy to prove by induction on m that such a lattice basis is given by $\mathcal{M}_{n+2},\ \mathcal{L}_1, \ldots, \mathcal{L}_{m-2}$, where

$$\begin{aligned} \mathcal{L}_1 &= (1, 1, -1, 0, \ldots, 0), \\ \mathcal{L}_2 &= (0, 1, 1, -1, 0, \ldots, 0), \\ &\vdots \\ \mathcal{L}_{m-2} &= (0, \ldots, 0, 1, 1, -1). \end{aligned} \tag{3}$$

Hence the general multiplier vector has the form

$$\mathcal{M}_n + y_1\mathcal{L}_1 + \ldots + y_{m-2}\mathcal{L}_{m-2} + y_{m-1}\mathcal{M}_{n+2},$$

where $y_1, \ldots, y_{m-1}$ are integers.

Table 1. Least multipliers, $m = 4, 5$, $2 \le n \le 20$

n	Least multipliers, $m = 4$			
2	1	0	0	0
3	−1	1	0	0
4	2	−1	0	0
5	−3	1	−1	1
6	4	−3	2	−1
7	−7	4	−3	2
8	11	−7	5	−3
9	−18	12	−7	4
10	30	−18	11	−7
11	−48	30	−18	11
12	78	−48	29	−18
13	−126	77	−48	30
14	203	−126	78	−48
15	−329	203	−126	78
16	532	−329	204	−126
17	−861	533	−329	203
18	1394	−861	532	−329
19	−2255	1394	−861	532
20	3649	−2255	1393	−861

n	Least multipliers, $m = 5$				
2	1	0	0	0	0
3	−1	1	0	0	0
4	2	−1	0	0	0
5	−3	1	−1	1	0
6	4	−3	2	−1	0
7	−7	4	−3	2	0
8	11	−7	4	−4	1
9	−18	12	−6	5	−1
10	29	−19	10	−9	2
11	−47	31	−16	14	−3
12	76	−50	27	−22	4
13	−123	80	−44	37	−7
14	200	−129	70	−59	11
15	−323	209	−114	96	−18
16	523	−338	184	−155	29
17	−846	548	−297	250	−47
18	1368	−887	482	−405	76
19	−2214	1435	−779	655	−123
20	3582	−2322	1260	−1061	200

A recent paper by the author and collaborators [1] contains an algorithm for finding small multipliers based on the LLL lattice basis reduction algorithm. Starting with a short multiplier, we then use the Fincke–Pohst algorithm to determine the shortest multipliers. When applied to the Fibonacci sequence, this experimentally always locates a unique multiplier of least length if $n > 1$. For $m = 2$, it is well known that the extended Euclid's algorithm, applied to coprime positive integers a, b, where b does not divide a, produces a multiplier vector (x_1, x_2) satisfying $|x_1| \le b/2$, $|x_2| \le a/2$, which is consequently the unique least multiplier. With $a = F_{n+1}$, $b = F_n$, $n \ge 3$, this gives the multiplier vector $\mathcal{M}_n$.

However, for $m \ge 3$, the smallest multiplier problem for $F_n, \dots, F_{n+m-1}$ seems to have escaped attention. (Table 1 gives the least multipliers for $m = 4$ and 5, $2 \le n \le 20$.)

In this paper, we prove that there is a unique multiplier vector of least length if $n \ge 2$, namely $\mathcal{W}_{n,m}$, where

$$\mathcal{W}_{n,m} = (-1)^n \mathcal{V}_{n,m} = (-1)^n (W_{n,1,m}, -W_{n,2,m}, \dots, -W_{n,m,m}), \tag{4}$$

which is defined as follows, using the greatest integer function: Let

$$\mathcal{P}_n = (F_{n-1}, -F_{n-2}, 0, \dots, 0), \tag{5}$$

$$\mathcal{V}_{n,m} = \mathcal{P}_n - G_{n,1,m}\mathcal{L}_1 + G_{n,2,m}\mathcal{L}_2 - \dots + (-1)^m G_{n,m-2,m}\mathcal{L}_{m-2}, \tag{6}$$

where the nonnegative integers $G_{n,1,m}, \dots, G_{n,m-2,m}$ are defined as follows:

Let

$$H_{n,r,m} = \left\lfloor \frac{F_{m-r}(F_{n-2}+F_r)}{F_m} \right\rfloor, \quad 1 \le r \le m.$$

Then for m even,

$$G_{n,r,m} = \begin{cases} H_{n,r,m} & \text{if } 2 \le r \le m-2,\ r \text{ even}, \\ H_{n-1,r+1,m} & \text{if } 1 \le r \le m-3,\ r \text{ odd}, \end{cases} \tag{7}$$

while for m odd,

$$G_{n,r,m} = \begin{cases} H_{n,r,m-1} = G_{n,r,m-1} & \text{if } 2 \le r \le m-3,\ r \text{ even}, \\ H_{n-1,r+1,m+1} = G_{n,r,m+1} & \text{if } 1 \le r \le m-2,\ r \text{ odd}. \end{cases} \tag{8}$$

The definition of $G_{n,r,m}$ extends naturally to $r = -1, 0, m-1, m$:

$$G_{n,-1,m} = F_{n-3}, \quad G_{n,0,m} = F_{n-2}, \quad G_{n,m-1,m} = G_{n,m,m} = 0.$$

Then equations (4)–(6) give

$$W_{n,r,m} = G_{n,r-2,m} + G_{n,r-1,m} - G_{n,r,m}. \tag{9}$$

It was not difficult to identify these multipliers for $2 \le n \le 2m+2$ (see Table 2). It was also not difficult to identify them for m even, n arbitrary, though the initial form of the answer was not elegant. However, it did take some effort to identify the case of m odd, n arbitrary. This was done with the help of the GNUBC 1.03 programming language, which enables one to write simple exact arithmetic number theory programs quickly.

To prove minimality of length, we use the slightly modified lattice basis for Λ,

$$\mathcal{L}_1, \ldots, \mathcal{L}_{m-2}, \mathcal{W}_{n+2,m},$$

which is the one always produced by our LLL-based extended gcd algorithm.

We then have to prove that if $n > 1$,

$$\|x_1\mathcal{L}_1 + \ldots + x_{m-2}\mathcal{L}_{m-2} + x_{m-1}\mathcal{W}_{n+2,m} - \mathcal{W}_{n,m}\|^2 \ge \|\mathcal{W}_{n,m}\|^2$$

for all integers $x_1, \ldots, x_{m-1}$, with equality only if $x_1 = \ldots = x_{m-1} = 0$.

The proof divides naturally into two cases. If x_{m-1} is nonzero, the coefficient of x_{m-1}^2 dominates. For this we need Lemmas 5 and 11.

If $x_{m-1} = 0$, the argument is more delicate and divides into several subcases, again using Lemma 5. The other lemmas play a supporting role for the derivation of Lemmas 5 and 11. In particular, Lemma 2 is important, as congruence properties in Lemma 4 reduce the calculation of the discrepancies for general n to the case $n \le 2m+2$, where everything is quite explicit.

2. Explicit expressions for $W_{n,r,m}$.

For later use in the proof of Lemma 11, we need the following simpler form for $W_{n,1,m}$ in terms of the least integer function:

LEMMA 1.

$$W_{n,1,m} = \begin{cases} \left\lceil \dfrac{F_{n+m-3} - F_{m-2}}{F_m} \right\rceil & \textit{if } m \textit{ is even}, \\ \left\lceil \dfrac{F_{n+m-2} - F_{m-1}}{F_{m+1}} \right\rceil & \textit{if } m \textit{ is odd}. \end{cases}$$

Proof. The identity $F_{n+m-3} = F_m F_{n-1} - F_{m-2} F_{n-3}$ follows from the well known identity

$$F_{a+b} = F_a F_{b+2} - F_{a-2} F_b,$$

with $a = m$ and $b = n - 3$. Consequently, if m is even,

$$\begin{aligned} W_{n,1,m} = F_{n-1} - G_{n,1,m} &= F_{n-1} - \left\lfloor \frac{F_{m-2}(F_{n-3}+1)}{F_m} \right\rfloor \\ &= -\left\lfloor \frac{-F_{n+m-3} + F_{m-2}}{F_m} \right\rfloor = \left\lceil \frac{F_{n+m-3} - F_{m-2}}{F_m} \right\rceil, \end{aligned}$$

and similarly if m is odd.

The $W_{n,r,m}$ with m even and $3 \le n \le 2m+2$ have an especially simple description in terms of Lucas numbers and play a central role in the proof of Lemma 5:

LEMMA 2. (See Table 2, which summarizes (a) and (c).)

(a) *Let* $3 \le n \le m+2$, m *even. If* n *is odd*,

$$W_{n,r,m} = \begin{cases} L_{n-r-2} & \textit{if } r \le n-3, \\ 1 & \textit{if } r = n-2, n-1, \\ 0 & \textit{if } r \ge n. \end{cases}$$

If n *is even*,

$$W_{n,r,m} = \begin{cases} L_{n-r-2} & \textit{if } r \le n-4, \\ 2 & \textit{if } r = n-3, \\ 1 & \textit{if } r = n-2, \\ 0 & \textit{if } r \ge n-1. \end{cases}$$

(b) *Let* $3 \le n \le m+2$, m *odd. Then*

$$W_{n,r,m} = W_{n,r,m-1}, \quad 1 \le r \le m-1, \quad W_{n,m,m} = 0.$$

(c) *Let* $3 + m \le n \le 2m+2$. *Then*

$$W_{n,r,m} = \begin{cases} L_{n-r-2} & \textit{if } r \ne 2m-n+3, \\ L_{n-r-2}+1 & \textit{if } r = 2m-n+3. \end{cases}$$

These formulae follow from explicit expressions below for $G_{n,r,m}$ in terms of the Fibonacci numbers, when m is even:

LEMMA 3. (a) *Let* $3 \le n \le m+2$. *If* r *is even*,

$$G_{n,r,m} = \begin{cases} F_{n-r-2} & \textit{if } r \le n-2, \\ 0 & \textit{if } r \ge n-1. \end{cases}$$

Table 2. The $W_{n,r,m}$, $1 \le n \le 2m+2$, m even

n	$W_{n,1,m}$	$W_{n,2,m}$	$W_{n,3,m}$	$W_{n,4,m}$	$W_{n,5,m}$
1	0	1	0	0	0
2	1	0	0	0	0
3	L_0-1	1	0	0	0
4	L_1+1	L_0-1	0	0	0
5	L_2	L_1	L_0-1	1	0
6	L_3	L_2	L_1+1	L_0-1	0
7	L_4	L_3	L_2	L_1	L_0-1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$m-1$	L_{m-4}	L_{m-5}			
m	L_{m-3}	L_{m-4}			
$m+1$	L_{m-2}	L_{m-3}			
$m+2$	L_{m-1}	L_{m-2}			
$m+3$	L_m	L_{m-1}			
$m+4$	L_{m+1}	L_m			
$m+5$	L_{m+2}	L_{m+1}			
$m+6$	L_{m+3}	L_{m+2}			
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$2m$	L_{2m-3}	L_{2m-4}	$L_{2m-5}+1$		
$2m+1$	L_{2m-2}	$L_{2m-3}+1$	L_{2m-4}		
$2m+2$	$L_{2m-1}+1$	L_{2m-2}	L_{2m-3}		

Table 2 (cont.)

n	$W_{n,6,m}$	$\ldots$	$W_{n,m-3,m}$	$W_{n,m-2,m}$	$W_{n,m-1,m}$	$W_{n,m,m}$
1	0	$\ldots$	0	0	0	0
2	0	$\ldots$	0	0	0	0
3	0	$\ldots$	0	0	0	0
4	0	$\ldots$	0	0	0	0
5	0	$\ldots$	0	0	0	0
6	0	$\ldots$	0	0	0	0
7	1	$\ldots$	0	0	0	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$m-1$		$\ldots$	L_0-1	1	0	0
m		$\ldots$	L_1+1	L_0-1	0	0
$m+1$		$\ldots$	L_2	L_1	L_0-1	1
$m+2$		$\ldots$	L_3	L_2	L_1+1	L_0-1
$m+3$		$\ldots$	L_4	L_3	L_2	L_1+1
$m+4$		$\ldots$	L_5	L_4	L_3+1	L_2
$m+5$		$\ldots$	L_6	L_5+1	L_4	L_3
$m+6$		$\ldots$	L_7+1	L_6	L_5	L_4
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$2m$		$\ldots$	L_{m+1}	L_m	L_{m-1}	L_{m-2}
$2m+1$		$\ldots$	L_{m+2}	L_{m+1}	L_m	L_{m-1}
$2m+2$		$\ldots$	L_{m+3}	L_{m+2}	L_{m+1}	L_m

If r is odd,

$$G_{n,r,m} = \begin{cases} F_{n-r-4} & \text{if } r \le n-3, \\ 0 & \text{if } r \ge n-2. \end{cases}$$

(b) *Let $m+3 \le n \le 2m+2$. If r is even*,

$$G_{n,r,m} = \begin{cases} F_{n-r-2} & \text{if } r \le 2m-n+2, \\ F_{n-r-2} - F_{n-2m+r-2} & \text{if } r \ge 2m-n+3. \end{cases}$$

If r is odd,

$$G_{n,r,m} = \begin{cases} F_{n-r-4} & \text{if } r \le 2m-n+1, \\ F_{n-r-4} - F_{n-2m+r-2} & \text{if } r \ge 2m-n+2. \end{cases}$$

(c) *If $n = 1$ or 2, $G_{n,r,m} = 0$ for $1 \le r \le m$.*

Proof. We assume r and m are even, as the case of odd r depends trivially on this case. We start from the following identity, valid for a even:

$$F_{a-r}F_b - F_aF_{b-r} = (-1)^r F_{b-a}F_r. \tag{10}$$

Then

$$F_{m-r}F_{n-2} - F_mF_{n-r-2} = -F_{n-m-2}F_r.$$

Hence

$$\begin{aligned} F_{m-r}(F_{n-2} + F_r) &= F_mF_{n-r-2} + (F_{m-r} - F_{n-m-2})F_r \\ &= F_mF_{n-r-2} + (F_{m-r} + (-1)^n F_{m-n+2})F_r \end{aligned} \tag{11}$$

and

$$G_{n,r,m} = \left\lfloor \frac{F_{m-r}(F_{n-2} + F_r)}{F_m} \right\rfloor = F_{n-r-2} + \left\lfloor \frac{(F_{m-r} - F_{n-m-2})F_r}{F_m} \right\rfloor \tag{12}$$

$$= F_{n-r-2} + \left\lfloor \frac{(F_{m-r} + (-1)^n F_{m-n+2})F_r}{F_m} \right\rfloor. \tag{13}$$

(a) Assume $3 \le n \le m+2$. First suppose $r \le n-2$. Then $m - r \ge m - n + 2 \ge 0$ and hence

$$0 \le F_{m-n+2} \le F_{m-r}$$

and

$$0 \le F_{m-r} + (-1)^n F_{m-n+2} \le 2F_{m-r}.$$

Hence

$$0 \le \frac{(F_{m-r} + (-1)^n F_{m-n+2})F_r}{F_m} \le \frac{2F_{m-r}F_r}{F_m} < 1,$$

as $2F_{m-r}F_r < F_m$ if $2 \le r \le m-2$. Hence

$$\left\lfloor \frac{(F_{m-r} + (-1)^n F_{m-n+2})F_r}{F_m} \right\rfloor = 0$$

and equation (13) gives $G_{n,r,m} = F_{n-r-2}$.

Next suppose $r \geq n-1$. Then

$$0 \leq \frac{F_{m-r}(F_{n-2}+F_r)}{F_m} \leq \frac{F_{m-r}(F_{r-1}+F_r)}{F_m} = \frac{F_{m-r}F_{r+1}}{F_m} < 1,$$

where we have used the inequality $F_aF_b < F_{a+b-1}$ if $2 \leq a, 1 \leq b$. Hence $G_{n,r,m} = 0$.

(b) Assume $m+3 \leq n \leq 2m+2$. First assume $r \leq 2m-n+2$. Then $m-r \geq n-m-2 \geq 0$ and

$$F_{m-r} \geq F_{n-m-2} \geq 0$$

and as seen before, the second integer part is zero in formula (12) and $G_{n,r,m} = F_{n-r-2}$.

Next assume $r \geq 2m-n+3$. Again we use a special case of equation (10):

$$F_{n-m-2}F_r - F_mF_{n-2m+r-2} = (-1)^nF_{m-r}F_{2m-n+2}.$$

This, together with equation (12), gives

$$G_{n,r,m} = F_{n-r-2} - F_{n-2m+r-2} + \left\lfloor \frac{F_{m-r}(F_r+(-1)^{n+1}F_{2m-n+2})}{F_m} \right\rfloor.$$

But $r \geq 2m-n+3$ implies $F_r \geq F_{2m-n+2} \geq 0$ and as before, the integer part vanishes and we have $G_{n,r,m} = F_{n-r-2} - F_{n-2m+r-2}$.

3. The discrepancies $D_{n,r,m}$ and $E_{n,r,m}$

LEMMA 4. *Let* $D_{n,r,m} = W_{n,r-2,m} - W_{n,r-1,m} - W_{n,r,m}$, $3 \leq r \leq m$.

(a) *If* $n = t + 2Nm$, m *even*,

$$F_n = F_t + F_{Nm}L_{Nm+t} \quad \text{and} \quad D_{n,r,m} = D_{t,r,m}.$$

(b) *If* m *is odd*, *then*

$$D_{n,r,m} = \begin{cases} D_{n,r,m-1} & \text{if } r \text{ is even,} \\ D_{n,r,m+1} & \text{if } r \text{ is odd.} \end{cases}$$

Proof. (a) Let $n = t + 2Nm$, m even. Then

$$F_n - F_t = F_{t+2Nm} - F_t = F_{Nm+t+Nm} - F_{Nm+t-Nm} = F_{Nm}L_{Nm+t},$$

as Nm is even. Noting that $F_{Nm} \equiv 0 \pmod{F_m}$, we have from equation (7) and the definition of $H_{n,r,m}$:

$$(14)\quad G_{n,r,m} = \begin{cases} G_{t,r,m} + \dfrac{F_{m-r}F_{Nm}L_{Nm+t}}{F_m} & \text{if } 2 \leq r \leq m-2,\ r \text{ even,} \\ G_{t,r,n} + \dfrac{F_{m-r-1}F_{Nm}L_{Nm+t}}{F_m} & \text{if } 1 \leq r \leq m-3,\ r \text{ odd.} \end{cases}$$

Hence, noting that $Z = (F_{Nm}L_{Nm+t})/F_m$ is an integer, we verify that with r even, equations (7) and (9) give

$$\begin{aligned} W_{n,r,m} &= W_{t,r,m} + F_{m-r+2}Z, \\ W_{n,r-1,m} &= W_{t,r,m} - F_{m-r}Z + 2F_{m-r+2}Z, \\ W_{n,r-2,m} &= W_{t,r,m} + F_{m-r+4}Z. \end{aligned}$$

Hence

$$\begin{aligned} D_{n,r,m} - D_{t,r,m} &= (F_{m-r+4} - (-F_{m-r} + 2F_{m-r+2}) - F_{m-r+2})Z \\ &= (F_{m-r} + F_{m-r+4} - 3F_{m-r+2})Z \\ &= (F_{m-r} + F_{m-r+3} - 2F_{m-r+2})Z \\ &= (F_{m-r} + F_{m-r+1} - F_{m-r+2})Z = 0. \end{aligned}$$

Similarly for r odd.

(b) Let m be odd. Then if r is even, equations (8) and (9) give

$$\begin{aligned} W_{n,r,m} &= G_{n,r-2,m-1} + G_{n,r-1,m+1} - G_{n,r,m-1}, \\ W_{n,r-1,m} &= G_{n,r-3,m+1} + G_{n,r-2,m-1} - G_{n,r-1,m+1}, \\ W_{n,r-2,m} &= G_{n,r-4,m-1} + G_{n,r-3,m+1} - G_{n,r-2,m-1}, \end{aligned}$$

and consequently

$$D_{n,r,m} = 3G_{n,r-2,m-1} - G_{n,r,m-1} - G_{n,r-4,m-1} = D_{n,r,m-1}.$$

Similarly when r is odd, we find $D_{n,r,m} = D_{n,r,m+1}$.

LEMMA 5. *For each n, we have $W_{n,r-2,m} = W_{n,r-1,m} + W_{n,r,m}$, with at most three exceptional r, which satisfy $|D_{n,r,m}| = 1$.*

Proof. If m is even, Lemma 4(a) reduces the problem to the range $1 \le n \le 2m$, where it is evidently true, by virtue of the explicit formulae for $W_{n,r,m}$ given in Lemma 2. We also observe that if m is even, then for n even, there are at most 2 odd r and one even r for which $|D_{n,r,m}| = 1$. Then Lemma 4(b) gives the result when n is even. Similarly for n odd.

As a corollary, we have

LEMMA 6. *For fixed $n > 1$ and $m \ge 3$,*

$$W_{n,r-1,m} \ge W_{n,r,m} \quad \text{if } 2 \le r \le m.$$

Proof. This is clear when $n \le m + 2$, while for $n \ge m + 3$, it is a consequence of the inequalities $W_{n,m,m} \ge 1$, $W_{n,m-1,m} \ge W_{n,m,m}$ and

$$W_{n,r-2,m} \ge W_{n,r-1,m} + W_{n,r,m} - 1, \quad 3 \le r \le m.$$

We will need an alternative $\mathbb{Z}$-basis for the lattice Λ.

LEMMA 7. *The vectors $\mathcal{L}_1, \ldots, \mathcal{L}_{m-2}, \mathcal{W}_{n+2,m}$ form a $\mathbb{Z}$-basis for Λ.*

P r o o f. This is a consequence of the identity

$$\mathcal{W}_{n+2,m} = \mathcal{M}_{n+2} + (-1)^n \sum_{i=1}^{m-2} (-1)^i G_{n+2,i,m} \mathcal{L}_i,$$

which follows from equations (4)–(6).

LEMMA 8. *Let* $E_{n,r,m} = G_{n+2,r,m} - G_{n+1,r,m} - G_{n,r,m}$, *where* m *is even.*

(a) *If* $n \equiv t \pmod{2m}$, *then* $E_{n,r,m} = E_{t,r,m}$.

(b) *If* $n = 1, 2, m+1$ *or* $m+2$, *then* $E_{n,r,m} = 0$ *for* $1 \le r \le m$. *If* $3 \le n \le m$ *and* n *is even*,

$$E_{n,r,m} = \begin{cases} 1 & \textit{if } r = n-3, \\ 0 & \textit{otherwise.} \end{cases}$$

If $3 \le n \le m$ *and* n *is odd*,

$$E_{n,r,m} = \begin{cases} 1 & \textit{if } r = n-1, \\ 0 & \textit{otherwise.} \end{cases}$$

If $m+3 \le n \le 2m+2$,

$$E_{n,r,m} = \begin{cases} -1 & \textit{if } r = n-2-m, \\ 0 & \textit{otherwise.} \end{cases}$$

P r o o f. (a) follows from equation (14), while (b) follows from the explicit form of $G_{n,r,m}$ given in Lemma 3.

LEMMA 9. *Let* $E_{n,m} = \mathcal{W}_{n+2,m} + \mathcal{W}_{n+1,m} - \mathcal{W}_{n,m}$. *Then*

$$E_{n,m} = (0, \ldots, 0) \textit{ or } \pm \mathcal{L}_i \quad \textit{for some } i. \tag{15}$$

P r o o f. By equations (4)–(6),

$$\begin{aligned} E_{n,m} &= (-1)^n (\mathcal{V}_{n+2,m} - \mathcal{V}_{n+1,m} - \mathcal{V}_{n,m}) \\ &= (-1)^n \sum_{r=1}^{m-2} (-1)^r E_{n,r,m} \mathcal{L}_r. \end{aligned}$$

If m is even, Lemma 8 gives the result directly, while if m is odd, we see from equation (8) that

$$E_{n,r,m} = \begin{cases} E_{n,r,m-1} & \text{if } 2 \le r \le m-3,\ r \text{ even}, \\ E_{n-1,r+1,m+1} & \text{if } 1 \le r \le m-2,\ r \text{ is odd}. \end{cases}$$

Then Lemma 8, with m replaced by $m-1$ and $m+1$, respectively, gives the result.

As a corollary, we have

LEMMA 10. *For fixed* r *and* m,

$$W_{n+1,r,m} \ge W_{n,r,m}.$$

Proof. If $n \le m$, the result follows from Lemma 2. If $n \ge m+1$, m even, or $n \ge m+2$, m odd, we have $W_{n,r,m} \ge 1$ and equation (15) gives

$$W_{n+2,r,m} \ge W_{n+1,r,m} + W_{n,r,m} - 1,$$

which gives the desired result. The remaining cases are simple exercises.

4. A size estimate for $\|\mathcal{W}_{n+2,m}\|$

LEMMA 11. *If* $n \ge 5$,

$$\|\mathcal{W}_{n+2,m}\|^2 > 2\mathcal{W}_{n+2,m} \cdot \mathcal{W}_{n,m} + 18. \tag{16}$$

Proof. $\mathcal{W}_{n+2,m} - \mathcal{W}_{n,m} - \mathcal{W}_{n+1,m} = 0$ or $\tau_i \mathcal{L}_i$, where $\tau_i = \pm 1$. Hence

$$\begin{aligned}&\|\mathcal{W}_{n+2,m}\|^2 - 2\mathcal{W}_{n+2,m} \cdot \mathcal{W}_{n,m} + \|\mathcal{W}_{n,m}\|^2 \\ &\qquad \ge \|\mathcal{W}_{n+1,m}\|^2 - 2\mathcal{W}_{n+1,m} \cdot \mathcal{L}_i + \|\mathcal{L}_i\|^2 \ge \|\mathcal{W}_{n+1,m}\|^2 - 3.\end{aligned}$$

Hence the desired inequality will follow if we can prove

$$\|\mathcal{W}_{n+1}\|^2 > \|\mathcal{W}_n\|^2 + 21. \tag{17}$$

But $W_{n+1,r,m} \ge W_{n,r,m} \ge 0$ and from Lemma 1, it is easy to prove that

$$W_{n+1,1,m} > W_{n,1,m} + 3$$

if $n \ge 7$. Then because $W_{n,1,m} \ge 2$ if $n \ge 4$, inequality (17) follows if $n \ge 7$.

Cases $n = 5$ and 6 of inequality (16) can be verified using the following identities:

$$\begin{aligned} W_{5,m} &= (-3, 1, -1, 1, 0, 0, \ldots), & W_{6,m} &= (4, -3, 2, -1, 0, 0, \ldots), \\ W_{7,m} &= (-7, 4, -3, 1, -1, 1, \ldots), & W_{8,m} &= (11, -7, 4, -3, 2, -1, \ldots), \end{aligned}$$

if $m \ge 6$. Also

$$\begin{aligned} W_{5,5} &= (-3, 1, -1, 1, 0), & W_{6,5} &= (4, -3, 2, -1, 0), \\ W_{7,5} &= (-7, 4, -3, 2, 0), & W_{8,5} &= (11, -7, 4, -4, 1), \\ W_{5,4} &= (-3, 1, -1, 1), & W_{6,4} &= (4, -3, 2, -1), \\ W_{7,4} &= (-7, 4, -3, 2), & W_{8,4} &= (11, -7, 5, -3), \\ W_{5,3} &= (-3, 2, 0), & W_{6,3} &= (4, -4, 1), \\ W_{7,3} &= (-7, 6, -1), & W_{8,3} &= (11, -10, 2). \end{aligned}$$

5. The proof of minimality

THEOREM. *For all integers* $x_1, \ldots, x_{m-1}$,

$$\|x_1\mathcal{L}_1 + \ldots + x_{m-2}\mathcal{L}_{m-2} + x_{m-1}\mathcal{W}_{n+2,m} - \mathcal{W}_{n,m}\|^2 \ge \|\mathcal{W}_{n,m}\|^2, \tag{18}$$

with equality only if $x_1 = \ldots = x_{m-1} = 0$.

P r o o f. Inequality (18) is equivalent to

$$\|x_1\mathcal{L}_1 + \ldots + x_{m-2}\mathcal{L}_{m-2} + \mathcal{W}_{n+2,m}x_{m-1}\|^2 - 2\sum_{i=1}^{m-2}\mathcal{L}_i\cdot\mathcal{W}_{n,m}\,x_i - 2\mathcal{W}_{n+2}\cdot\mathcal{W}_{n,m}\,x_{m-1} \ge 0. \tag{19}$$

The left hand side of this inequality expands to

$$\sum_{i=1}^{m-2}\sum_{j=1}^{m-2}\mathcal{L}_i\cdot\mathcal{L}_j\,x_ix_j + \|\mathcal{W}_{n+2,m}\|^2x_{m-1}^2 + 2\sum_{i=1}^{m-2}\mathcal{L}_i\cdot\mathcal{W}_{n+2,m}\,x_ix_{m-1}.$$

Now $\varepsilon_i = \mathcal{L}_i\cdot\mathcal{W}_{n,m} = (-1)^nD_{n,i+2,m}$. But by Lemma 5, $D_{n,r,m} = 0$ for $3 \le r \le m$, with at most three exceptional r, in which case $D_{n,r,m} = \pm1$. Also $\eta_i = \mathcal{L}_i\cdot\mathcal{W}_{n+2,m} = 0$, with at most three exceptions.

Also

$$\mathcal{L}_i\cdot\mathcal{L}_j = \begin{cases} 3 & \text{if } i=j,\\ 0 & \text{if } j=i+1,\\ -1 & \text{if } j=i+2,\\ 0 & \text{if } j\ge i+3.\end{cases}$$

Substituting all this in the expanded form of inequality (19) gives the equivalent inequality

$$Q = Q_1 + Ax_{m-1}^2 - 2Bx_{m-1} + 2\sum_{i=1}^{m-2}\eta_ix_ix_{m-1} - 2\sum_{i=1}^{m-2}\varepsilon_ix_i \ge 0, \tag{20}$$

where $A = \|\mathcal{W}_{n+2,m}\|^2$, $B = \mathcal{W}_{n+2,m}\cdot\mathcal{W}_{n,m}$ and

$$Q_1 = 3\sum_{i=1}^{m-2}x_i^2 - 2\sum_{i=1}^{m-4}x_ix_{i+2}.$$

Now let $x_1,\ldots,x_{m-2}$ be integers, not all zero. We prove $Q > 0$.

C a s e 1: x_{m-1} nonzero. The coefficient of x_{m-1}^2 dominates. For completing the square gives the equivalent inequality

$$Q = Q_2 + \Big(A - \sum_{i=1}^{m-2}\eta_i^2\Big)x_{m-1}^2 - 2\Big(B - \sum_{i=1}^{m-2}\varepsilon_i\eta_i\Big)x_{m-1} + \sum_{i=1}^{m-2}(x_i - \varepsilon_i + \eta_ix_{m-1})^2 - \sum_{i=1}^{m-2}\varepsilon_i^2 \ge 0, \tag{21}$$

where $Q_2 \ge 0$. Here

$$Q_2 = \begin{cases} 2x_1^2 & \text{if } m=3,\\ 2x_1^2+2x_2^2 & \text{if } m=4,\\ (x_1-x_3)^2+x_1^2+2x_2^2+x_3^2 & \text{if } m=5,\\ T+x_1^2+x_2^2+x_{m-3}^2+x_{m-2}^2 & \text{if } m\ge 6,\end{cases}$$

where

$$T = \sum_{i=1}^{m-4} (x_i - x_{i+2})^2. \tag{22}$$

But

$$\sum_{i=1}^{m-2} \varepsilon_i^2 \le 3, \qquad \sum_{i=1}^{m-2} \eta_i^2 \le 3, \qquad \Big|\sum_{i=1}^{m-2} \varepsilon_i \eta_i\Big| \le 6.$$

Hence inequality (21) holds with strict inequality, if we can prove

$$(A-3)x_{m-1}^2 - 3 > 2(B+6)|x_{m-1}|.$$

This will be true if $A > 2B + 18$ and this follows from Lemma 11 if $n \ge 5$.

Finally, only the case $n = 4$ needs any thought and this is straightforward, as $\mathcal{W}_{2,m} = (2, -1, 0, 0, \ldots, 0)$, $\mathcal{W}_{4,m} = (4, -3, 2, -1, \ldots, 0)$, if $m \ge 4$.

Case 2: $x_{m-1} = 0$. The argument is more delicate. We start by assuming $m \ge 6$. Then $Q = T + S_0 - U$, where

$$S_0 = 2x_1^2 + 2x_2^2 + x_3^2 + \ldots + x_{m-4}^2 + 2x_{m-3}^2 + 2x_{m-2}^2$$

and

$$U = 2\sum_{i=1}^{m-2} \varepsilon_i x_i.$$

In what follows, we make use of the inequalities

$$x(x \pm 1) \ge 0, \quad x(x \pm 2) \ge -1 \quad \text{if } x \in \mathbb{Z}.$$

Clearly we need only consider $T \le 3$.

Case 2(a): $T = 0$. Then $Q = S_0 - U$ and $x_1 = x_3 = \ldots,\quad x_2 = x_4 = \ldots$ Hence one of x_1, x_2 must be nonzero and one of x_{m-3}, x_{m-2} must be nonzero. Then a consideration of the possible terms in U shows that

$$Q = S_0 - U = 2x_1^2 + 2x_2^2 + x_3^2 + \ldots + x_{m-4}^2 + 2x_{m-3}^2 + 2x_{m-2}^2 - U \ge 1.$$

Case 2(b): $T = 1$. Then $Q = 1 + S_0 - U$ and there exists i such that

$$|x_i - x_{i+2}| = 1, \quad \text{while} \quad x_j = x_{j+2} \text{ if } j \ne i.$$

A consideration of the possible terms in U shows that $S_0 - U \ge 0$ and hence $Q = 1 + S_0 - U \ge 1$.

Case 2(c): $T = 2$. Then $Q = 2 + S_0 - U$. If one of $x_1, x_2, x_{m-3}, x_{m-2}$ is nonzero, then $S_0 \ge 2$ and $Q \ge 1$. Suppose $x_1 = x_2 = x_{m-3} = x_{m-2} = 0$. Then

$$S_0 = x_3^2 + \ldots + x_{m-4}^2.$$

If at least two of the variables are nonzero, then $S_0 \ge 2$ and $Q = 2 + S_0 - U \ge 1$. If precisely one variable x_k has nonzero coefficient, then

$S_0 = x_k^2$. If $|x_k| \geq 2$, we are done. However, if $|x_k| = 1$, then nonzero terms in U can contribute at most $x_k^2 \pm 2x_k \geq -1$ to $S_0 - U$ and we have $Q = 2 + S_0 - U \geq 1$.

Case 2(d). $T = 3$. Then $Q = 3 + S_0 - U \geq 0$. Moreover, $Q = 0$ implies $S_0 - U = -3$ and there exist indices I, J, K satisfying $3 \leq I < J < K \leq m-4$ with

$$x_I = \varepsilon_I = \pm 1, \quad x_J = \varepsilon_J = \pm 1, \quad x_K = \varepsilon_K = \pm 1,$$

while $x_i = 0$ if $i \neq I, J, K$. A consideration of cases shows this would in turn imply $T \geq 4$.

Finally, there remain the cases $m = 3, 4, 5$.

- $m = 3$: Here $x_1^2 > 0$ and

$$Q = 3x_1^2 - 2\varepsilon_1 x_1 = x_1^2 - 2x_1(x_1 - \varepsilon_1) > 0.$$

- $m = 4$: Here $x_1^2 + x_2^2 > 0$ and

$$\begin{aligned} Q &= 3x_1^2 + 3x_2^2 - 2\varepsilon_1 x_1 - 2\varepsilon_2 x_2 \\ &= x_1^2 + x_2^2 + 2x_1(x_1 - \varepsilon_1) + 2x_2(x_2 - \varepsilon_2) > 0. \end{aligned}$$

- $m = 5$: Here $x_1^2 + x_2^2 + x_3^2 > 0$ and

$$\begin{aligned} Q &= (x_1 - x_3)^2 + 2x_1^2 + 3x_2^2 + 2x_3^2 - 2\varepsilon_1 x_1 - 2\varepsilon_2 x_2 - 2\varepsilon_3 x_3 \\ &= (x_1 - x_3)^2 + x_2^2 + 2x_1(x_1 - \varepsilon_1) + 2x_2(x_2 - \varepsilon_2) + 2x_3(x_3 - \varepsilon_3) \geq 0. \end{aligned}$$

Moreover, equality implies $x_1 = x_3 = \varepsilon_1 = \varepsilon_3$ and $x_2 = 0$. Then

$$\begin{aligned} 0 = \varepsilon_1 - \varepsilon_3 &= (\mathcal{L}_1 - \mathcal{L}_3) \cdot \mathcal{W}_{n,5} \\ &= (1, 1, -2, -1, -1) \cdot \mathcal{W}_{n,5} \\ &= (-1)^n (W_{n,1,5} - W_{n,2,5} + 2W_{n,3,5} + W_{n,4,5} - W_{n,1,5}). \end{aligned}$$

But Lemma 6 implies $W_{n,r-1,5} \geq W_{n,r,5}$ if $n > 1$, $r \geq 2$. Also Lemma 10 gives $W_{n,3,5} \geq W_{5,3,5} = 1$ if $n \geq 5$. Hence we get a contradiction if $n \geq 5$. Also we cannot have $n < 5$, as $(\varepsilon_1, \varepsilon_3) = (1, 0), (0, 0), (1, 0)$ for $n = 2, 3, 4$, respectively.

Acknowledgements. In conclusion, the author wishes to thank Dr. George Havas for suggesting that the LLL-based extended gcd algorithm be applied to the Fibonacci numbers.

Calculations were performed using the GNUBC 1.03 exact arithmetic calculator program, together with a number theory calculator program called CALC, written by the author.

The author is grateful to the referee for painstaking efforts and for suggesting that the paper be revised to improve its readability.

References

[1] G. Havas, B. S. Majewski and K. R. Matthews, *Extended gcd algorithms*, to appear.
[2] V. E. Hoggatt Jr., *Fibonacci and Lucas Numbers*, Houghton Mifflin, Boston, 1969.

Department of Mathematics
University of Queensland
Brisbane, Australia Q4072
E-mail: krm@axiom.maths.uq.oz.au

Received on 8.3.1995
and in revised form on 16.10.1995 (2752)