On the coefficients of the \(2^n\)-th transformation polynomial for \(j(\omega)\)

by

KURT MAHLER (Canberra, Australia)

In memory of Professor Waclaw Sierpiński

Let \(j(\omega)\) be the modular function of level 1. It is well known that there exists to every integer \(m \geq 2\) an irreducible polynomial

\[ F_m(u, v) = F_m(v, u) \]

with rational integral coefficients such that

\[ F_m(j(m\omega), j(\omega)) = 0 \]

identically in \(\omega\).

As \(m\) increases, the coefficients of \(F_m(u, v)\) soon become extremely large. But how large they do in fact become does not seem to have been studied in the literature.

We shall consider here only the case when

\[ m = 2^n \]

is a power of 2. Let the abbreviation \(F_{(n)}(u, v)\) stand for \(F_{2^n}(u, v)\), and let \(L(F_{(n)})\) be the sum of the absolute values of the coefficients of \(F_{(n)}(u, v)\). It will then be proved that

\[ L(F_{(n)}) \leq 2^{(36n+57)2^n} \quad (n = 1, 2, 3, \ldots). \]

I hope to establish in a later paper an analogous estimate for the general polynomial \(F_m(u, v)\).

1. The following notation will be used.

If \(P(u, v, \ldots)\) is a polynomial with complex coefficients in the indeterminates \(u, v, \ldots\), then \(\partial_u(P)\), \(\partial_v(P)\), \(\ldots\) denote the exact degrees of \(P\) in \(u, v, \ldots\), respectively, and we put

\[ \Delta(P) = \partial_u(P) + \partial_v(P) + \ldots \]

Further \(L(P)\), the length of \(P\), is defined as the sum of the absolute values of the coefficients of \(P\). This length evidently has the properties

\[ L(P + Q) \leq L(P) + L(Q) \quad \text{and} \quad L(PQ) \leq L(P)L(Q), \]

(1)
and it can also be proved (Mahler, [1]) that, if $P$ allows the factorisation

$$ P = P_1 P_2 \ldots P_r, $$

then

$$ L(P_1) L(P_2) \ldots L(P_r) \leq 2^{d(P)} L(P). $$

Next let $\omega = \xi + i\eta$ be a complex variable in the upper halfplane

$$ H: \eta > 0, $$

and let as usual $q$ denote the expression $q = e^{\pi i \omega}$, so that $0 < |q| < 1$. We shall be concerned with the basic modular function

$$ j(\omega) = \left\{ 1 + 240 \sum_{h=1}^{\infty} h^3 \frac{q^{2h}}{1-q^{2h}} \right\} \left\{ q^2 \prod_{h=1}^{\infty} (1-q^{2h})^2 \right\}^{-1} $$

of level 1, and also with the modular function

$$ k(\omega) = 4q^{1/2} \prod_{h=1}^{\infty} \left\{ \frac{1+q^{2h}}{1+q^{2h-1}} \right\}^4 $$

of Legendre and Jacobi of level 4. These two functions are connected by the identity

$$ j(\omega) = 2^8 \frac{(k(\omega)^4 - k(\omega)^2 + 1)^3}{k(\omega)^4 (1-k(\omega)^2)^2}. $$

We shall further make use of Gauss’s formula

$$ k(\omega/2) = \frac{2\sqrt{k(\omega)}}{1+k(\omega)}. $$

2. It is proved in the theory of modular functions that, for every positive integer $n$, there exists an irreducible polynomial

$$ F_{(n)}(u, v) = \sum_{h=0}^{3 \cdot 2^{n-1}} \sum_{k=0}^{3 \cdot 2^{n-1}} F_{hk} u^h v^k $$

symmetric in $u$ and $v$, with integral coefficients, and with the highest terms $u^{3 \cdot 2^{n-1}}$ and $v^{3 \cdot 2^{n-1}}$, such that

$$ F_{(n)}(j(2^n \omega), j(\omega)) = 0 $$

identically in $\omega$.

We shall establish in this note an upper estimate for the length

$$ L(n) = L(F_{(n)}) $$

of the polynomial $F_{(n)}(u, v)$, thus for the quantity

$$ L(n) = \sum_{h=0}^{3 \cdot 2^{n-1}} \sum_{k=0}^{3 \cdot 2^{n-1}} |F_{hk}|. $$
The coefficients of \( F_{(n)} \) become quickly very large, and such an estimate does not seem to have so far been obtained. The proof will depend on the relation (5) between \( j(\omega) \) and \( k(\omega) \) and on Gauss’s formula (6).

3. Put

\[ j(2^h \omega) = j_h \quad \text{and} \quad k(2^h \omega) = k_h \quad (h = 0, 1, 2, \ldots). \]

Firstly, by (5),

\[ 2^8 (k_0^4 - k_0^2 + 1)^3 - j_0 k_0^4 (1 - k_0^2)^2 = 0, \]

or, say,

\[ f_{(0)}(j_0, k_0) = 0, \tag{10} \]

where \( f_{(0)}(u, v) \) is the polynomial

\[ f_{(0)}(u, v) = 2^8 (v^4 - v^2 + 1)^3 - uv^4 (1 - v^2)^2. \tag{11} \]

By (6), the consecutive function values \( k_0, k_1, k_2, \ldots \) are connected by the recursive formulae

\[ k_n = 2 (k_{n+1})^{1/2} (k_{n+1} + 1)^{-1} \quad (n = 0, 1, 2, \ldots). \tag{12} \]

Let us therefore define a sequence of polynomials \( \{f_{(n)}(u, v)\} \) by the formulae

\[ f_{(n+1)}(u, v) = \begin{cases} 2^{-4} (1 + v)^{1/2} f_{(0)} \left( u, \frac{2 \sqrt{v}}{1 + v} \right) & \text{for } n = 0, \\ 2^{-2} (1 + v)^{1/2} f_{(1)} \left( u, \frac{2 \sqrt{v}}{1 + v} \right) & \text{for } n = 1, \\ (1 + v)^{20/v^{(n)}} f_{(n)} \left( u, \frac{2 \sqrt{v}}{1 + v} \right) f_{(n)} \left( u, -\frac{2 \sqrt{v}}{1 + v} \right) & \text{for } n \geq 2. \end{cases} \tag{13} \]

Then

\[ f_{(1)}(u, v) = 2^4 (v^4 + 14v^2 + 1)^3 - uv^2 (1 - v^2)^2, \]

\[ f_{(2)}(u, v) = 4 (v^4 + 60v^3 + 134v^2 + 60v + 1)^3 - uv(v + 1)^2 (v - 1)^8. \tag{14} \]

Generally, for all \( n \geq 2 \), \( f_{(n)}(u, v) \) becomes a polynomial in \( u \) and \( v \) with rational integral coefficients, of the form

\[ f_{(n)}(u, v) = \sum_{h=0}^{2n-2} \sum_{k=0}^{2n-2} f_{hk}^{(n)} u^h v^k \tag{15} \]

and, naturally, with the property that

\[ f_{(n)}(j_0, k_n) = 0. \tag{16} \]
4. Put
\begin{equation}
A_{(n)} = L(f_{(n)}) \quad (n = 0, 1, 2, \ldots).
\end{equation}
Thus, by (11) and (14),
\begin{equation}
A_{(0)} = 2^8 3^3 + 2^2, \quad A_{(1)} = 2^6 + 2^2, \quad A_{(2)} = 2^{26} + 2^{47}.
\end{equation}
We shall now determine a recursive inequality for $A_{(n)}$ and by means of it an upper estimate for this quantity.

Let already $n \geq 2$. By (13) and (15),
\begin{align*}
f_{(n+1)}(u, v) &= (1+v)^{2 \cdot 12 \cdot 2^{n-2}} \times \\
&\left\{ \sum_{h=0}^{2^{n-2}} \sum_{k=0}^{2^{n-2}} f_{hk}^{(n)} u^h \left( \frac{2 \sqrt{v}}{1+v} \right)^k \right\} \left\{ \sum_{h=0}^{2^{n-2}} \sum_{k=0}^{2^{n-2}} f_{hk}^{(n)} u^h \left( \frac{-2 \sqrt{v}}{1+v} \right)^k \right\}.
\end{align*}
Here, for both signs $\varepsilon = +1$ and $\varepsilon = -1$,
\begin{align*}
(1+v)^{12 \cdot 2^{n-2}} &\sum_{h=0}^{2^{n-2}} \sum_{k=0}^{2^{n-2}} f_{hk}^{(n)} u^h \left( \frac{2 \sqrt{v}}{1+v} \right)^k = \sum_{h=0}^{2^{n-2}} \sum_{l=0}^{2^{n-2}} f_{h,2l}^{(n)} u^h 2^{2l} v^l (1+v)^{12 \cdot 2^{n-2} - 2l} + \\
+ \varepsilon \sqrt{v} &\sum_{h=0}^{2^{n-2}} \sum_{l=0}^{2^{n-2}} f_{h,2l+1}^{(n)} u^h 2^{2l+1} v^l (1+v)^{12 \cdot 2^{n-2} - 2l-1}.
\end{align*}
Hence $f_{(n+1)}$ has the rational form
\begin{align*}
f_{(n+1)}(u, v) &= \left\{ \sum_{h=0}^{2^{n-2}} \sum_{l=0}^{2^{n-2}} f_{h,2l}^{(n)} u^h 2^{2l} v^l (1+v)^{12 \cdot 2^{n-2} - 2l} \right\}^2 - \\
&\left[ \varepsilon \sqrt{v} \sum_{h=0}^{2^{n-2}} \sum_{l=0}^{2^{n-2}} f_{h,2l+1}^{(n)} u^h 2^{2l+1} v^l (1+v)^{12 \cdot 2^{n-2} - 2l-1} \right]^2.
\end{align*}
Now
\begin{equation}
L(2^k (1+v)^{12 \cdot 2^{n-2}}) = 2^{12 \cdot 2^{n-2}} \quad (k = 0, 1, \ldots, 12 \cdot 2^{n-2}).
\end{equation}
It follows therefore that
\begin{equation}
A_{(n+1)} \leq 2^{2 \cdot 12 \cdot 2^{n-2}} \left\{ \left( \sum_{h=0}^{2^{n-2}} \sum_{l=0}^{2^{n-2}} |f_{h,2l}^{(n)}|^2 \right)^2 + \left( \sum_{h=0}^{2^{n-2}} \sum_{l=0}^{2^{n-2}} |f_{h,2l+1}^{(n)}|^2 \right)^2 \right\},
\end{equation}
whence evidently
\begin{equation}
A_{(n+1)} \leq 2^{24 \cdot 2^{n-2}} A_{(n)}^2 \quad \text{for} \quad n \geq 2.
\end{equation}
On applying this inequality repeatedly, we find easily that
\begin{equation}
A_{(n)} \leq 2^{12(n-2)2^{n-2}} A_{(2)}^{2^{n-2}} \quad \text{for} \quad n \geq 2.
\end{equation}
Here, by (18),
\begin{equation}
A_{(2)} < 2^{28},
\end{equation}
and therefore
\[ A(n) < 2^{(3n+1)2^n} \quad \text{for} \quad n \geq 2. \]

This estimate is not valid when \( n = 0 \) and \( n = 1 \). It would have some interest to decide whether there exists a positive constant \( C \) such that
\[ A(n) \leq 2^{C \cdot 2^n} \]
for all sufficiently large \( n \).

5. Let again \( n \geq 2 \). Put
\[ a_k^{(n)}(u) = \sum_{k=0}^{12 \cdot 2^{n-2}} f_k^{(n)} u^k \quad (k = 0, 1, \ldots, 12 \cdot 2^{n-2}), \]
so that, by (15),
\[ f_{(n)}(u, v) = \sum_{k=0}^{12 \cdot 2^{n-2}} a_k^{(n)}(u) v^k. \]

Here the \( a_k^{(n)}(u) \) are polynomials in \( u \) with rational integral coefficients, where the inequality (20) implies that
\[ \sum_{k=0}^{12 \cdot 2^{n-2}} L(a_k^{(n)}) < 2^{(3n+1)2^n}. \]

Both \( a_0^{(n)}(u) \) and \( a_{12 \cdot 2^{n-2}}^{(n)}(u) \) can be determined explicitly, as follows. Firstly, by (11) and (14),
\[ a_0^{(0)}(u) = 2^8, \quad a_0^{(1)}(u) = 2^4, \quad a_0^{(2)}(u) = 4, \]
while by (13),
\[ a_0^{(n+1)}(u) = f_{(n+1)}(u, 0) = f_{(n)}(u, 0)^2 = a_0^{(n)}(u)^2. \]

It follows therefore that, for all \( n \geq 2 \),
\[ a_0^{(n)}(u) = 2^{2^{n-1}}, \]
hence that \( a_0^{(n)}(u) \) is for all \( n \) independent of \( u \).

Next \( f_{(n)}(u, v) \) is reciprocal with respect to the variable \( v \),
\[ v^{\delta_{\varepsilon(f_{(n)})(u)}} f_{(n)} \left( u, \frac{1}{v} \right) = f_{(n)}(u, v), \]
whence also
\[ a_k^{(n)}(u) = a_{12 \cdot 2^{n-2}}^{(n)}(u) \quad (k = 0, 1, \ldots, 12 \cdot 2^{n-2}). \]
For all three polynomials \(f_{(0)}, f_{(1)}, \) and \(f_{(2)}\) are reciprocal; and if \(n \geq 2\) and \(f_{(n)}\) is reciprocal, then the same is true for \(f_{(n+1)}\) because, by (13),

\[
v^{12 \cdot 2^n - 1} f_{(n+1)} \left( u, \frac{1}{v} \right)
\]

\[
= v^{12 \cdot 2^n - 1} \left( 1 + (1/v) \right)^{12 \cdot 2^n - 1} f_{(n)} \left( u, \frac{2v^{-1/2}}{1 + v^{-1}} \right)
\]

\[
= (1 + v)^{12 \cdot 2^n - 1} f_{(n)} \left( u, \frac{2Vv}{1 + v} \right) f_{(n)} \left( u, -\frac{2Vv}{1 + v} \right) = f_{(n+1)}(u, v).
\]

It follows now from (24) and (26) that also

\[
a_{12 \cdot 2^n - 2}^{(n)}(u) = 2^{2n-1} \quad \text{if} \quad n \geq 2.
\]

The term of \(f_{(n)}\) of highest degree in \(v\) has thus for \(n \geq 2\) the form

\[
2^{2n-1} v^{12 \cdot 2^n - 2}
\]

and so is independent of \(u\).

6. The functions

\[
j_0 = j(\omega) \quad \text{and} \quad k_n = k(2^n \omega)
\]

are connected by the equation

\[
f_{(n)}(j_0, k_n) = 0.
\]

It follows further, from (5), on replacing \(\omega\) by \(2^n \omega\), that

\[
j_n = j(2^n \omega) \quad \text{and} \quad k_n = k(2^n \omega)
\]

satisfy the equation

\[
f_{(0)}(j_n, k_n) = 0.
\]

Denote therefore by

\[
R_{(n)} = R_{(n)}(j_0, j_n)
\]

the resultant relative to \(v\) of the two polynomials

\[
f_{(n)}(j_0, v) = \sum_{k=0}^{12 \cdot 2^n - 2} a_{k}^{(n)}(j_0) v^{k}
\]

and

\[
f_{(0)}(j_n, v) = 2^{5}(v^4 - v^2 + 1)^3 - j_n v^4 (1 - v^2)^2.
\]

This resultant is a polynomial in \(j_0\) and \(j_n\) which does not vanish identically. For the coefficients of the highest powers

\[
v^{12 \cdot 2^n - 2} \quad \text{and} \quad v^{12}
\]
of \( v \) that occur in these two polynomials are never zero; and whatever the value of \( v \), it is always possible to find a value of \( j_n \) such that

\[ f_{(0)}(j_n, v) \neq 0. \]

As usual, \( R_{(n)} \) can be written as a determinant. For this purpose, let

\[ f_{(0)}(j_n, v) = \sum_{k=0}^{12} b_k(j_n) v^k, \]

so that evidently

\[
\begin{align*}
  b_0(j_n) &= b_{12}(j_n) = 2^8, \\
  b_2(j_n) &= b_{10}(j_n) = -3 \cdot 2^8, \\
  b_3(j_n) &= b_8(j_n) = 6 \cdot 2^3 - j_n, \\
  b_6(j_n) &= -7 \cdot 2^8 + 2 j_n; \\
  b_1(j_n) &= b_3(j_n) = b_5(j_n) = b_7(j_n) = b_9(j_n) = b_{11}(j_n) = 0.
\end{align*}
\]

Further

\[ \sum_{k=0}^{12} L(b_k) = 2^8 3^3 + 2^2. \]

The resultant \( R_{(n)} \) takes now the explicit form

\[
R_{(n)}(j_0, j_n) = \begin{vmatrix}
  a_{N}^{(n)}(j_0) & a_{N-1}^{(n)}(j_0) & \cdots & a_0^{(n)}(j_0) & 0 & \cdots & 0 \\
  0 & a_{N}^{(n)}(j_0) & \cdots & a_1^{(n)}(j_0) & a_0^{(n)}(j_0) & \cdots & 0 \\
  \vdots & \vdots & \ddots & \vdots & \ddots & \ddots & \vdots \\
  0 & 0 & \cdots & a_{N}^{(n)}(j_0) & a_{N-1}^{(n)}(j_0) & \cdots & a_0^{(n)}(j_0) \\
  b_{12}(j_n) & b_{11}(j_n) & \cdots & b_0(j_n) & 0 & \cdots & 0 \\
  0 & b_{12}(j_n) & \cdots & b_1(j_n) & b_0(j_n) & 0 & \cdots \\
  \vdots & \vdots & \ddots & \vdots & \ddots & \ddots & \vdots \\
  0 & 0 & \cdots & b_{12}(j_n) & b_{11}(j_n) & \cdots & b_0(j_n)
\end{vmatrix}
\]

where \( N \) stands for the abbreviation

\[ N = 12 \cdot 2^{n-2}. \]

We apply now the following trivial estimate for the length of a determinant. Let

\[ p_{hk}(u, v) \quad (h, k = 1, 2, \ldots, m) \]

be arbitrary polynomials with complex coefficients in any two indeterminates \( u \) and \( v \), and let \( D(u, v) \) be the determinant

\[
D = \begin{vmatrix}
  p_{11} & p_{12} & \cdots & p_{1m} \\
  p_{21} & p_{22} & \cdots & p_{2m} \\
  \vdots & \vdots & \cdots & \vdots \\
  p_{m1} & p_{m2} & \cdots & p_{mm}
\end{vmatrix}
\]
It is then evident from the definition of a determinant that

\[ L(D) \leq \prod_{h=1}^{m} (L(p_{h1}) + L(p_{h2}) + \ldots + L(p_{hm})). \]

On applying this inequality to the determinant for \( R_{(n)} \) and making use of the estimates (23) and (31), noting that

\[ 2^8 \cdot 3^3 + 2^2 < 2^{13}, \]

we find that

\[ L(R_{(n)}) < 2^{12(3n+1)2^n}(2^8 \cdot 3^3 + 2^2)^{12 \cdot 2^{n-2}} \]

and hence that

(33) \[ L(R_{(n)}) < 2^{(36n+51)2^n}. \]

In the determinant for \( R_{(n)} \), the elements \( a_k^{(n)}(j_0) \) are polynomials in \( j_0 \) at most of degree \( 2^{n-2} \), while the elements \( b_k(j_n) \) are polynomials in \( j_n \) at most of degree 1, where all these polynomials have rational integral coefficients. Therefore \( R_{(n)}(j_0, j_n) \) is a polynomial with rational integral coefficients in \( j_0 \) and \( j_n \), at most of degree \( 12 \cdot 2^{n-2} \) in \( j_0 \) and at most of degree \( 12 \cdot 2^{n-2} \) in \( j_n \). Hence, in the notation of § 1,

(34) \[ A(R_{(n)}) \leq 24 \cdot 2^{n-2}. \]

7. The two equations (28) and (29) can only hold if

\[ R_{(n)}(j_0, j_n) = 0. \]

On the other hand, \( j_0 \) and \( j_n \) are also connected by the transformation equation

\[ F_{(n)}(j_0, j_n) = 0, \]

and it is known that the polynomial \( F_{(n)}(u, v) \) is irreducible. Hence the polynomial \( R_{(n)}(u, v) \) necessarily is divisible by \( F_{(n)}(u, v) \). The latter polynomial is primitive because its highest coefficients are equal to 1. Therefore \( R_{(n)} \) allows a factorisation

\[ R_{(n)}(u, v) = F_{(n)}(u, v)G_{(n)}(u, v) \]

where \( G_{(n)} \) denotes a further polynomial in \( u \) and \( v \) with rational integral coefficients. Therefore

(35) \[ L(G_{(n)}) \geq 1. \]

The inequality (2) implies then that

\[ L(F_{(n)}) \leq L(F_{(n)})L(G_{(n)}) \leq 2^{A(R_{(n)})}L(R_{(n)}), \]
hence, by (33) and (35),

$$L(F_{(n)}) \leq 2^{24} 2^{n-2} \cdot 2^{(36n+51)2^n}.$$ 

Thus we arrive finally at the following result.

**Theorem.** For every positive integer $n$, the length $L(F_{(n)})$ of the $2^n$th transformation polynomial $F_{(n)}(u, v)$ satisfies the inequality

$$L(F_{(n)}) \leq 2^{(36n+57)2^n}.$$ 

(36)

Actually, our proof gave this estimate only for $n \geq 2$. It remains, however, true also for $n = 1$ because the explicit expression for $F_{(1)}(u, v)$ shows that

$$L(F_{(1)}) < 2^{48}.$$ 

It would be valuable if it could be proved that $L(F_{(n)})$ satisfies a stronger inequality

$$L(F_{(n)}) \leq 2^{C \cdot 2^n}$$

where $C$ denotes any absolute positive constant. For such a result would enable one to prove that

$$j\left(\frac{\log q}{\pi i}\right)$$

is transcendental for all algebraic numbers $q$ satisfying

$$0 < |q| < 1.$$ 

It is, as yet, unknown whether this statement is in fact true.

**References**


DEPARTMENT OF MATHEMATICS
INSTITUTE OF ADVANCED STUDIES
AUSTRALIAN NATIONAL UNIVERSITY
Canberra, ACT. 2600, Australia

Received on 12. 2. 1971