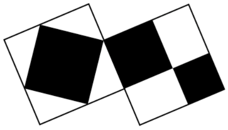
Paperfolding, Automata, and Rational Functions

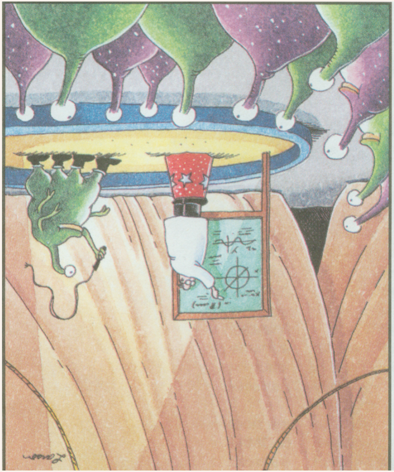
Diagonals and Hadamard products of algebraic power series

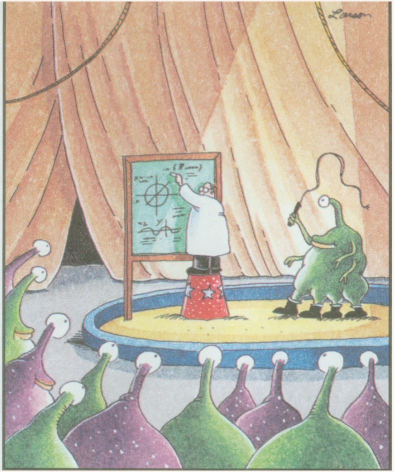
Alf van der Poorten

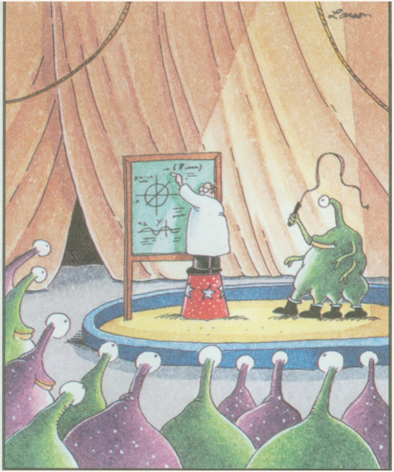
ceNTRe for Number Theory Research, Sydney



08 November, 2007 Laramie







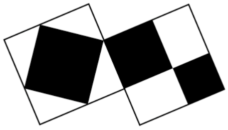
Abducted by an alien circus company, Professor Doyle is forced to write calculus equations in centre ring.

Paperfolding, Automata, and Rational Functions

Diagonals and Hadamard products of algebraic power series

Alf van der Poorten

ceNTRe for Number Theory Research, Sydney



08 November, 2007 Laramie

Paperfolding

Take a rectangular sheet of paper and fold it in half, right half over left. Repeat the operation, and again, and again, and . . . . On unfolding the sheet of paper we see the creases as a sequence of valleys $\longleftarrow 1$ and ridges $\longleftarrow 0$. Then, reading from left to right, after five folds we obtain

$$1$$

We now recall that after one, two, three, four, five folds we saw

1

110

1101100

110110011100100

1101100111001001110110001100100

so we obtain an infinite paperfolding sequence by adding a new middle fold 1 and noting that the second half of the sequence is the reverse mirror image of the first half. This justifies my adding . . . after those thirty-one creases.

Paperfolding

Take a rectangular sheet of paper and fold it in half, right half over left. Repeat the operation, and again, and again, and . . . . On unfolding the sheet of paper we see the creases as a sequence of valleys $\leftarrow 1$ and ridges $\leftarrow 0$. Then, reading from left to right, after five folds we obtain

1 1

We now recall that after one, two, three, four, five folds we saw

1

110

1101100

110110011100100

1101100111001001110110001100100

so we obtain an infinite paperfolding sequence by adding a new middle fold 1 and noting that the second half of the sequence is the reverse mirror image of the first half. This justifies my adding . . . after those thirty-one creases.

Paperfolding

Take a rectangular sheet of paper and fold it in half, right half over left. Repeat the operation, and again, and again, and . . . . On unfolding the sheet of paper we see the creases as a sequence of valleys $\leftarrow 1$ and ridges $\leftarrow 0$. Then, reading from left to right, after five folds we obtain

$$1 \qquad 1 \qquad 0$$

We now recall that after one, two, three, four, five folds we saw

1

110

1101100

110110011100100

1101100111001001110110001100100

so we obtain an infinite paperfolding sequence by adding a new middle fold 1 and noting that the second half of the sequence is the reverse mirror image of the first half. This justifies my adding . . . after those thirty-one creases.

Paperfolding

Take a rectangular sheet of paper and fold it in half, right half over left. Repeat the operation, and again, and again, and . . . . On unfolding the sheet of paper we see the creases as a sequence of valleys $\leftarrow$ 1 and ridges $\leftarrow$ 0. Then, reading from left to right, after five folds we obtain

1 1 1 0

We now recall that after one, two, three, four, five folds we saw

1

110

1101100

110110011100100

1101100111001001110110001100100

so we obtain an infinite paperfolding sequence by adding a new middle fold 1 and noting that the second half of the sequence is the reverse mirror image of the first half. This justifies my adding . . . after those thirty-one creases.

Paperfolding

Take a rectangular sheet of paper and fold it in half, right half over left. Repeat the operation, and again, and again, and . . . . On unfolding the sheet of paper we see the creases as a sequence of valleys $\leftarrow 1$ and ridges $\leftarrow 0$. Then, reading from left to right, after five folds we obtain

1 1 0 1 0

We now recall that after one, two, three, four, five folds we saw

1

110

1101100

110110011100100

1101100111001001110110001100100

so we obtain an infinite paperfolding sequence by adding a new middle fold 1 and noting that the second half of the sequence is the reverse mirror image of the first half. This justifies my adding . . . . after those thirty-one creases.

Paperfolding

Take a rectangular sheet of paper and fold it in half, right half over left. Repeat the operation, and again, and again, and . . . . On unfolding the sheet of paper we see the creases as a sequence of valleys $\leftarrow 1$ and ridges $\leftarrow 0$. Then, reading from left to right, after five folds we obtain

$$1 \quad 1 \quad 0 \quad 1 \quad 1 \quad 0$$

We now recall that after one, two, three, four, five folds we saw

1

110

1101100

110110011100100

1101100111001001110110001100100

so we obtain an infinite paperfolding sequence by adding a new middle fold 1 and noting that the second half of the sequence is the reverse mirror image of the first half. This justifies my adding . . . after those thirty-one creases.

Paperfolding

Take a rectangular sheet of paper and fold it in half, right half over left. Repeat the operation, and again, and again, and . . . . On unfolding the sheet of paper we see the creases as a sequence of valleys $\leftarrow 1$ and ridges $\leftarrow 0$. Then, reading from left to right, after five folds we obtain

$$1 \quad 1 \quad 0 \quad 1 \quad 1 \quad 0 \quad 0$$

We now recall that after one, two, three, four, five folds we saw

1

110

1101100

110110011100100

1101100111001001110110001100100

so we obtain an infinite paperfolding sequence by adding a new middle fold 1 and noting that the second half of the sequence is the reverse mirror image of the first half. This justifies my adding . . . after those thirty-one creases.

Paperfolding

Take a rectangular sheet of paper and fold it in half, right half over left. Repeat the operation, and again, and again, and . . . . On unfolding the sheet of paper we see the creases as a sequence of valleys $\leftarrow 1$ and ridges $\leftarrow 0$. Then, reading from left to right, after five folds we obtain

$$1\ 1\quad 1\quad 0\quad 1\quad 1\quad 0\quad 0$$

We now recall that after one, two, three, four, five folds we saw

1

110

1101100

110110011100100

1101100111001001110110001100100

so we obtain an infinite paperfolding sequence by adding a new middle fold 1 and noting that the second half of the sequence is the reverse mirror image of the first half. This justifies my adding . . . after those thirty-one creases.

Paperfolding

Take a rectangular sheet of paper and fold it in half, right half over left. Repeat the operation, and again, and again, and . . . . On unfolding the sheet of paper we see the creases as a sequence of valleys $\leftarrow 1$ and ridges $\leftarrow 0$. Then, reading from left to right, after five folds we obtain

1 1 0 1 0 1 1 0 0

We now recall that after one, two, three, four, five folds we saw

1

110

1101100

110110011100100

1101100111001001110110001100100

so we obtain an infinite paperfolding sequence by adding a new middle fold 1 and noting that the second half of the sequence is the reverse mirror image of the first half. This justifies my adding . . . after those thirty-one creases.

Paperfolding

Take a rectangular sheet of paper and fold it in half, right half over left. Repeat the operation, and again, and again, and . . . . On unfolding the sheet of paper we see the creases as a sequence of valleys $\leftarrow 1$ and ridges $\leftarrow 0$. Then, reading from left to right, after five folds we obtain

$$1\ 1\ 0\ 1\ 1\ 0\quad 1\quad 1\quad 0\quad 0$$

We now recall that after one, two, three, four, five folds we saw

1

110

1101100

110110011100100

1101100111001001110110001100100

so we obtain an infinite paperfolding sequence by adding a new middle fold 1 and noting that the second half of the sequence is the reverse mirror image of the first half. This justifies my adding . . . after those thirty-one creases.

Paperfolding

Take a rectangular sheet of paper and fold it in half, right half over left. Repeat the operation, and again, and again, and . . . . On unfolding the sheet of paper we see the creases as a sequence of valleys $\leftarrow 1$ and ridges $\leftarrow 0$. Then, reading from left to right, after five folds we obtain

$$1\ 1\ 0\ 1\ 1\ 0\ 0\ 1\quad 1\quad 0\quad 0$$

We now recall that after one, two, three, four, five folds we saw

1

110

1101100

110110011100100

1101100111001001110110001100100

so we obtain an infinite paperfolding sequence by adding a new middle fold 1 and noting that the second half of the sequence is the reverse mirror image of the first half. This justifies my adding . . . after those thirty-one creases.

Paperfolding

Take a rectangular sheet of paper and fold it in half, right half over left. Repeat the operation, and again, and again, and . . . . On unfolding the sheet of paper we see the creases as a sequence of valleys $\leftarrow 1$ and ridges $\leftarrow 0$. Then, reading from left to right, after five folds we obtain

1 1 0 1 1 0 0 1 1 1 0 0

We now recall that after one, two, three, four, five folds we saw

1

110

1101100

110110011100100

1101100111001001110110001100100

so we obtain an infinite paperfolding sequence by adding a new middle fold 1 and noting that the second half of the sequence is the reverse mirror image of the first half. This justifies my adding . . . after those thirty-one creases.

Paperfolding

Take a rectangular sheet of paper and fold it in half, right half over left. Repeat the operation, and again, and again, and . . . . On unfolding the sheet of paper we see the creases as a sequence of valleys $\leftarrow 1$ and ridges $\leftarrow 0$. Then, reading from left to right, after five folds we obtain

$$1\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 0\ 0\quad 0$$

We now recall that after one, two, three, four, five folds we saw

1

110

1101100

110110011100100

1101100111001001110110001100100

so we obtain an infinite paperfolding sequence by adding a new middle fold 1 and noting that the second half of the sequence is the reverse mirror image of the first half. This justifies my adding . . . after those thirty-one creases.

Paperfolding

Take a rectangular sheet of paper and fold it in half, right half over left. Repeat the operation, and again, and again, and . . . . On unfolding the sheet of paper we see the creases as a sequence of valleys $\leftarrow 1$ and ridges $\leftarrow 0$. Then, reading from left to right, after five folds we obtain

$$1\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 0$$

We now recall that after one, two, three, four, five folds we saw

1

110

1101100

110110011100100

1101100111001001110110001100100

so we obtain an infinite paperfolding sequence by adding a new middle fold 1 and noting that the second half of the sequence is the reverse mirror image of the first half. This justifies my adding . . . after those thirty-one creases.

Paperfolding

Take a rectangular sheet of paper and fold it in half, right half over left. Repeat the operation, and again, and again, and . . . . On unfolding the sheet of paper we see the creases as a sequence of valleys $\leftarrow 1$ and ridges $\leftarrow 0$. Then, reading from left to right, after five folds we obtain

$$1\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 0$$

We now recall that after one, two, three, four, five folds we saw

1

110

1101100

110110011100100

1101100111001001110110001100100

so we obtain an infinite paperfolding sequence by adding a new middle fold 1 and noting that the second half of the sequence is the reverse mirror image of the first half. This justifies my adding . . . after those thirty-one creases.

Paperfolding

Take a rectangular sheet of paper and fold it in half, right half over left. Repeat the operation, and again, and again, and . . . . On unfolding the sheet of paper we see the creases as a sequence of valleys $\leftarrow 1$ and ridges $\leftarrow 0$. Then, reading from left to right, after five folds we obtain

$$1101100111001001110110001100100$$

We now recall that after one, two, three, four, five folds we saw

$$1$$

$$110$$

$$1101100$$

$$110110011100100$$

$$1101100111001001110110001100100$$

so we obtain an infinite paperfolding sequence by adding a new middle fold 1 and noting that the second half of the sequence is the reverse mirror image of the first half. This justifies my adding . . . . after those thirty-one creases.

Paperfolding

Take a rectangular sheet of paper and fold it in half, right half over left. Repeat the operation, and again, and again, and . . . . On unfolding the sheet of paper we see the creases as a sequence of valleys $\leftarrow 1$ and ridges $\leftarrow 0$. Then, reading from left to right, after five folds we obtain

1101100111001001110110001100100

We now recall that after one, two, three, four, five folds we saw

1

110

1101100

110110011100100

1101100111001001110110001100100

so we obtain an infinite paperfolding sequence by adding a new middle fold 1 and noting that the second half of the sequence is the reverse mirror image of the first half. This justifies my adding . . . after those thirty-one creases.

Paperfolding

Take a rectangular sheet of paper and fold it in half, right half over left. Repeat the operation, and again, and again, and . . . . On unfolding the sheet of paper we see the creases as a sequence of valleys $\leftarrow 1$ and ridges $\leftarrow 0$. Then, reading from left to right, after five folds we obtain

$$1101100111001001110110001100100$$

We now recall that after one, two, three, four, five folds we saw

$$1$$

$$110$$

$$1101100$$

$$110110011100100$$

$$1101100111001001110110001100100$$

so we obtain an infinite paperfolding sequence by adding a new middle fold 1 and noting that the second half of the sequence is the reverse mirror image of the first half. This justifies my adding . . . after those thirty-one creases.

Paperfolding

Take a rectangular sheet of paper and fold it in half, right half over left. Repeat the operation, and again, and again, and . . . . On unfolding the sheet of paper we see the creases as a sequence of valleys $\leftarrow$ 1 and ridges $\leftarrow$ 0. Then, reading from left to right, after five folds we obtain

1101100111001001110110001100100

We now recall that after one, two, three, four, five folds we saw

1

110

1101100

110110011100100

1101100111001001110110001100100

so we obtain an infinite paperfolding sequence by adding a new middle fold 1 and noting that the second half of the sequence is the reverse mirror image of the first half. This justifies my adding . . . after those thirty-one creases.

Paperfolding

Take a rectangular sheet of paper and fold it in half, right half over left. Repeat the operation, and again, and again, and . . . . On unfolding the sheet of paper we see the creases as a sequence of valleys $\leftarrow 1$ and ridges $\leftarrow 0$. Then, reading from left to right, after five folds we obtain

$$1101100111001001110110001100100$$

We now recall that after one, two, three, four, five folds we saw

$$1$$

$$110$$

$$1101100$$

$$110110011100100$$

$$1101100111001001110110001100100$$

so we obtain an infinite paperfolding sequence by adding a new middle fold 1 and noting that the second half of the sequence is the reverse mirror image of the first half. This justifies my adding . . . after those thirty-one creases.

Paperfolding

Take a rectangular sheet of paper and fold it in half, right half over left. Repeat the operation, and again, and again, and . . . . On unfolding the sheet of paper we see the creases as a sequence of valleys ← 1 and ridges ← 0. Then, reading from left to right, after five folds we obtain

$$1101100111001001110110001100100$$

We now recall that after one, two, three, four, five folds we saw

$$1$$

$$110$$

$$1101100$$

$$110110011100100$$

$$1101100111001001110110001100100$$

so we obtain an infinite paperfolding sequence by adding a new middle fold 1 and noting that the second half of the sequence is the reverse mirror image of the first half. This justifies my adding . . . after those thirty-one creases.

Paperfolding

Take a rectangular sheet of paper and fold it in half, right half over left. Repeat the operation, and again, and again, and . . . . On unfolding the sheet of paper we see the creases as a sequence of valleys $\leftarrow 1$ and ridges $\leftarrow 0$. Then, reading from left to right, after five folds we obtain

$$1101100111001001110110001100100$$

We now recall that after one, two, three, four, five folds we saw

$$1$$

$$110$$

$$1101100$$

$$110110011100100$$

$$1101100111001001110110001100100$$

so we obtain an infinite paperfolding sequence by adding a new middle fold 1 and noting that the second half of the sequence is the reverse mirror image of the first half. This justifies my adding . . . after those thirty-one creases.

Paperfolding

Take a rectangular sheet of paper and fold it in half, right half over left. Repeat the operation, and again, and again, and . . . . On unfolding the sheet of paper we see the creases as a sequence of valleys $\leftarrow 1$ and ridges $\leftarrow 0$. Then, reading from left to right, after five folds we obtain

$$1101100111001001110110001100100$$

We now recall that after one, two, three, four, five folds we saw

$$1$$

$$110$$

$$1101100$$

$$110110011100100$$

$$1101100111001001110110001100100$$

so we obtain an infinite paperfolding sequence by adding a new middle fold 1 and noting that the second half of the sequence is the reverse mirror image of the first half. This justifies my adding . . . after those thirty-one creases.

Paperfolding

Take a rectangular sheet of paper and fold it in half, right half over left. Repeat the operation, and again, and again, and . . . . On unfolding the sheet of paper we see the creases as a sequence of valleys $\leftarrow 1$ and ridges $\leftarrow 0$. Then, reading from left to right, after five folds we obtain

$$1101100111001001110110001100100\ldots$$

We now recall that after one, two, three, four, five folds we saw

$$1$$

$$110$$

$$1101100$$

$$110110011100100$$

$$1101100111001001110110001100100\ldots$$

so we obtain an infinite paperfolding sequence by adding a new middle fold 1 and noting that the second half of the sequence is the reverse mirror image of the first half. This justifies my adding . . . after those thirty-one creases.

A Mahler Functional Equation

Aside. Is the number $0.11011001110010011101100011001001\ldots$ transcendental?

Now consider subtracting the spaced out sequence from the paperfolding sequence:

If we denote the paperfolding sequence by $f_1, f_2, f_3, \ldots$ then we have verified experimentally that the formal power series $F(X) = \sum_{h=1}^{\infty} f_h X^h$ satisfies the functional equation $F(X) - F(X^2) = X/(1 - X^4)$.

Once noticed, we see that this is obvious. Inserting an extra positive fold is to replace $F(X)$ by $F(X^2)$ and to add $X/(1 - X^4)$. However, the infinite paperfolding sequence is invariant under the addition of a positive fold.

A Mahler Functional Equation

Aside. Is the number $0.11011001110010011101100011001001\ldots$ transcendental?

Now consider subtracting the spaced out sequence from the paperfolding sequence:

If we denote the paperfolding sequence by $f_1, f_2, f_3, \ldots$ then we have verified experimentally that the formal power series $F(X) = \sum_{h=1}^{\infty} f_h X^h$ satisfies the functional equation $F(X) - F(X^2) = X/(1 - X^4)$.

Once noticed, we see that this is obvious. Inserting an extra positive fold is to replace $F(X)$ by $F(X^2)$ and to add $X/(1 - X^4)$. However, the infinite paperfolding sequence is invariant under the addition of a positive fold.

A Mahler Functional Equation

Aside. Is the number $0.11011001110010011101100011001001\ldots$ transcendental?

Now consider subtracting the spaced out sequence from the paperfolding sequence:

If we denote the paperfolding sequence by $f_1, f_2, f_3, \ldots$ then we have verified experimentally that the formal power series $F(X) = \sum_{n=1}^{\infty} f_n X^n$ satisfies the functional equation $F(X) - F(X^2) = X/(1 - X^4)$.

Once noticed, we see that this is obvious. Inserting an extra positive fold is to replace $F(X)$ by $F(X^2)$ and to add $X/(1 - X^4)$. However, the infinite paperfolding sequence is invariant under the addition of a positive fold.

A Mahler Functional Equation

Aside. Is the number 0.11011001110010011101100011001001 . . . transcendental?

Now consider subtracting the spaced out sequence from the paperfolding sequence:

If we denote the paperfolding sequence by $f_1, f_2, f_3, \ldots$ then we have verified experimentally that the formal power series $F(X) = \sum_{h=1}^{\infty} f_h X^h$ satisfies the functional equation $F(X) - F(X^2) = X/(1 - X^4)$.

Once noticed, we see that this is obvious. Inserting an extra positive fold is to replace $F(X)$ by $F(X^2)$ and to add $X/(1 - X^4)$. However, the infinite paperfolding sequence is invariant under the addition of a positive fold.

A Mahler Functional Equation

Aside. Is the number 0.11011001110010011101100011001001 . . . transcendental?

Now consider subtracting the spaced out sequence from the paperfolding sequence:

If we denote the paperfolding sequence by $f_1, f_2, f_3, \ldots$ then we have verified experimentally that the formal power series $F(X) = \sum_{h=1}^{\infty} f_h X^h$ satisfies the functional equation $F(X) - F(X^2) = X/(1 - X^4)$.

Once noticed, we see that this is obvious. Inserting an extra positive fold is to replace $F(X)$ by $F(X^2)$ and to add $X/(1 - X^4)$. However, <u>the infinite paperfolding sequence is invariant under the addition of a positive fold.</u>

A Mahler Functional Equation

Aside. Is the number 0.11011001110010011101100011001001 . . . transcendental?

Now consider subtracting the spaced out sequence from the paperfolding sequence:

If we denote the paperfolding sequence by $f_1, f_2, f_3, \ldots$ then we have verified experimentally that the formal power series $F(X) = \sum_{h=1}^{\infty} f_h X^h$ satisfies the functional equation $F(X) - F(X^2) = X/(1 - X^4)$.

Once noticed, we see that this is obvious. Inserting an extra positive fold is to replace $F(X)$ by $F(X^2)$ and to add $X/(1 - X^4)$. However, the infinite paperfolding sequence is invariant under the addition of a positive fold.

A Mahler Functional Equation

Aside. Is the number 0.11011001110010011101100011001001 . . . transcendental?

Now consider subtracting the spaced out sequence from the paperfolding sequence:

If we denote the paperfolding sequence by $f_1, f_2, f_3, \ldots$ then we have verified experimentally that the formal power series $F(X) = \sum_{n=1}^{\infty} f_n X^n$ satisfies the functional equation $F(X) - F(X^2) = X/(1 - X^4)$.

Once noticed, we see that this is obvious. Inserting an extra positive fold is to replace $F(X)$ by $F(X^2)$ and to add $X/(1 - X^4)$. However, the infinite paperfolding sequence is invariant under the addition of a positive fold.

A Mahler Functional Equation

Aside. Is the number 0.11011001110010011101100011001001 . . . transcendental?

Now consider subtracting the spaced out sequence from the paperfolding sequence:

If we denote the paperfolding sequence by $f_1, f_2, f_3, \ldots$ then we have verified experimentally that the formal power series $F(X) = \sum_{h=1}^{\infty} f_h X^h$ satisfies the functional equation $F(X) - F(X^2) = X/(1 - X^4)$.

Once noticed, we see that this is obvious. Inserting an extra positive fold is to replace $F(X)$ by $F(X^2)$ and to add $X/(1 - X^4)$. However, <u>the infinite paperfolding sequence is invariant under the addition of a positive fold</u>.

A Mahler Functional Equation

Aside. Is the number 0.1101100111001001110110001100 1001 ... transcendental?

Now consider subtracting the spaced out sequence from the paperfolding sequence:

1 1 0 1 1 0 0 1 1 1 0 0 1 0 0 1 1 1 0 1 1 0 0 0

If we denote the paperfolding sequence by $f_1, f_2, f_3, \ldots$ then we have verified experimentally that the formal power series $F(X) = \sum_{h=1}^{\infty} f_h X^h$ satisfies the functional equation $F(X) - F(X^2) = X/(1 - X^4)$.

Once noticed, we see that this is obvious. Inserting an extra positive fold is to replace $F(X)$ by $F(X^2)$ and to add $X/(1 - X^4)$. However, the infinite paperfolding sequence is invariant under the addition of a positive fold.

A Mahler Functional Equation

Aside. Is the number 0.11011001110010011101100011001001 . . . transcendental?

Now consider subtracting the spaced out sequence from the paperfolding sequence:

1101100111001001110110001100100111011001110010001 . . .

1 1 0 1 1 0 0 1 1 1 0 0 1 0 0 1 1 1 0 1 1 0 0 0

we get

If we denote the paperfolding sequence by $f_1, f_2, f_3, \ldots$ then we have verified experimentally that the formal power series $F(X) = \sum_{h=1}^{\infty} f_h X^h$ satisfies the functional equation $F(X) - F(X^2) = X/(1 - X^4)$.

Once noticed, we see that this is obvious. Inserting an extra positive fold is to replace $F(X)$ by $F(X^2)$ and to add $X/(1 - X^4)$. However, the infinite paperfolding sequence is invariant under the addition of a positive fold.

A Mahler Functional Equation

Aside. Is the number $0.11011001110010011101100011001001\ldots$ transcendental?

Now consider subtracting the spaced out sequence from the paperfolding sequence:

$$1101100111001001110110001100100111011001110010001\ldots$$
$$1\ \ 1\ \ 0\ \ 1\ \ 1\ \ 0\ \ 0\ \ 1\ \ 1\ \ 1\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 1\ \ 1\ \ 1\ \ 0\ \ 1\ \ 1\ \ 0\ \ 0\ \ 0$$

we get

$$1000100010001000100010001000100010001000100010001\ldots$$

If we denote the paperfolding sequence by $f_1, f_2, f_3, \ldots$ then we have verified experimentally that the formal power series $F(X) = \sum_{h=1}^{\infty} f_h X^h$ satisfies the functional equation $F(X) - F(X^2) = X/(1 - X^4)$.

Once noticed, we see that this is obvious. Inserting an extra positive fold is to replace $F(X)$ by $F(X^2)$ and to add $X/(1 - X^4)$. However, the infinite paperfolding sequence is invariant under the addition of a positive fold.

A Mahler Functional Equation

Aside. Is the number 0.11011001110010011101100011001001 . . . transcendental?

Now consider subtracting the spaced out sequence from the paperfolding sequence:

110110011100100111011000110010011101100111001000 1 . . .

1 1 0 1 1 0 0 1 1 1 0 0 1 0 0 1 1 1 0 1 1 0 0 0

we get

100010001000100010001000100010001000100010001000 1 . . .

If we denote the paperfolding sequence by $f_1, f_2, f_3, \ldots$ then we have verified experimentally that the formal power series $F(X) = \sum_{h=1}^{\infty} f_h X^h$ satisfies the functional equation $F(X) - F(X^2) = X/(1 - X^4)$.

Once noticed, we see that this is obvious. Inserting an extra positive fold is to replace $F(X)$ by $F(X^2)$ and to add $X/(1 - X^4)$. However, the infinite paperfolding sequence is invariant under the addition of a positive fold.

A Mahler Functional Equation

Aside. Is the number 0.1101100111001001110110001100100 1 . . . transcendental?

Now consider subtracting the spaced out sequence from the paperfolding sequence:

11011001110010011101100011001001110110011100100 01 . . .

1 1 0 1 1 0 0 1 1 1 0 0 1 0 0 1 1 1 0 1 1 0 0 0

we get

100010001000100010001000100010001000100010001000 1 . . .

If we denote the paperfolding sequence by $f_1, f_2, f_3, \ldots$ then we have verified experimentally that the formal power series $F(X) = \sum_{h=1}^{\infty} f_h X^h$ satisfies the functional equation $F(X) - F(X^2) = X/(1 - X^4)$.

Once noticed, we see that this is obvious. Inserting an extra positive fold is to replace $F(X)$ by $F(X^2)$ and to add $X/(1 - X^4)$. However, the infinite paperfolding sequence is invariant under the addition of a positive fold.

A Mahler Functional Equation

Aside. Is the number $0.11011001110010011101100011001001\ldots$ transcendental?

Now consider subtracting the spaced out sequence from the paperfolding sequence:

$$11011001110010011101100011001001110110011100100001\ldots$$

$$1\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 0\ 1\ 1\ 0\ 0\ 0$$

we get

$$10001000100010001000100010001000100010001000100010001\ldots$$

If we denote the paperfolding sequence by $f_1, f_2, f_3, \ldots$ then we have verified experimentally that the formal power series $F(X) = \sum_{h=1}^{\infty} f_h X^h$ satisfies the functional equation $F(X) - F(X^2) = X/(1 - X^4)$.

Once noticed, we see that this is obvious. Inserting an extra positive fold is to replace $F(X)$ by $F(X^2)$ and to add $X/(1 - X^4)$. However, the infinite paperfolding sequence is invariant under the addition of a positive fold.

A Mahler Functional Equation

Aside. Is the number $0.110110011100100111011000110010 01\ldots$ transcendental?

Now consider subtracting the spaced out sequence from the paperfolding sequence:

$$110110011100100111011000110010011101100111001 0001\ldots$$

$$1\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 0\ 1\ 1\ 0\ 0\ 0$$

we get

$$100010001000100010001000100010001000100010001\ldots$$

If we denote the paperfolding sequence by $f_1, f_2, f_3, \ldots$ then we have verified experimentally that the formal power series $F(X) = \sum_{h=1}^{\infty} f_h X^h$ satisfies the functional equation $F(X) - F(X^2) = X/(1 - X^4)$.

Once noticed, we see that this is obvious. Inserting an extra positive fold is to replace $F(X)$ by $F(X^2)$ and to add $X/(1 - X^4)$. However, the infinite paperfolding sequence is invariant under the addition of a positive fold.

A Mahler Functional Equation

Aside. Is the number 0.110110011100100111011000110010011 ... transcendental?

Now consider subtracting the spaced out sequence from the paperfolding sequence:

110110011100100111011000110010011101100111001000 1 ...

1 1 0 1 1 0 0 1 1 1 0 0 1 0 0 1 1 1 0 1 1 0 0 0

we get

1000100010001000100010001000100010001000100010001 ...

If we denote the paperfolding sequence by $f_1, f_2, f_3, \ldots$ then we have verified experimentally that the formal power series $F(X) = \sum_{h=1}^{\infty} f_h X^h$ satisfies the functional equation $F(X) - F(X^2) = X/(1 - X^4)$.

Once noticed, we see that this is obvious. Inserting an extra positive fold is to replace $F(X)$ by $F(X^2)$ and to add $X/(1 - X^4)$. However, the infinite paperfolding sequence is invariant under the addition of a positive fold.

Regular Binary Substitution

Next, if we pair the sequence

11.01.10.01.11.00.10.01.11.01.10.00.11.00.10.01.
11.01.10.01.11.00.10.00.11.01.10.00.11.00.10.01. . . .

and interpret the pairs as numbers in base 2, we obtain

3.1.2.1.3.0.2.1.3.1.2.0.3.0.2.1.3.1.2.1.3.0.2.0.3.1.2.0.3.0.2.1. . . .

But this is precisely the original sequence warmed up by adding 2 to every second entry:

31.21.30.21.31.20.30.21.31.21.30.20.31.20.30.21.
31.21.30.21.31.20.30.20.31.21.30.20.30.21. . . .

Thus, experimentally at any rate, the new sequence, which I again call (f_n), is invariant under the uniform binary substitution

$$\theta : 0 \mapsto 20,\ 1 \mapsto 21,\ 2 \mapsto 30,\ 3 \mapsto 31.$$

Regular Binary Substitution

Next, if we pair the sequence

$$11.01.10.01.11.00.10.01.11.01.10.00.11.00.10.01.$$
$$11.01.10.01.11.00.10.00.11.01.10.00.11.00.10.01.\ \ldots$$

and interpret the pairs as numbers in base 2, we obtain

$$3.1.2.1.3.0.2.1.3.1.2.0.3.0.2.1.3.1.2.1.3.0.2.0.3.1.2.0.3.0.2.1.\ \ldots$$

But this is precisely the original sequence warmed up by adding 2 to every second entry:

$$31.21.30.21.31.20.30.21.31.21.30.20.31.20.30.21.$$
$$31.21.30.21.31.20.30.20.31.21.30.20.30.21.\ \ldots$$

Thus, experimentally at any rate, the new sequence, which I again call (f_h), is invariant under the uniform binary substitution

$$\theta : 0 \mapsto 20\,,\ 1 \mapsto 21\,,\ 2 \mapsto 30\,,\ 3 \mapsto 31\,.$$

Regular Binary Substitution

Next, if we pair the sequence

$$11.01.10.01.11.00.10.01.11.01.10.00.11.00.10.01.$$
$$11.01.10.01.11.00.10.00.11.01.10.00.11.00.10.01.\ \ldots$$

and interpret the pairs as numbers in base 2, we obtain

$$3.1.2.1.3.0.2.1.3.1.2.0.3.0.2.1.3.1.2.1.3.0.2.0.3.1.2.0.3.0.2.1.\ \ldots$$

But this is precisely the original sequence warmed up by adding 2 to every second entry:

$$31.21.30.21.31.20.30.21.31.21.30.20.31.20.30.21.$$
$$31.21.30.21.31.20.30.20.31.21.30.20.30.21.\ \ldots$$

Thus, experimentally at any rate, the new sequence, which I again call (f_h), is invariant under the uniform binary substitution

$$\theta : 0 \mapsto 20\,,\ 1 \mapsto 21\,,\ 2 \mapsto 30\,,\ 3 \mapsto 31\,.$$

Regular Binary Substitution

Next, if we pair the sequence

$$11.01.10.01.11.00.10.01.11.01.10.00.11.00.10.01.$$
$$11.01.10.01.11.00.10.00.11.01.10.00.11.00.10.01.\ \ldots$$

and interpret the pairs as numbers in base 2, we obtain

$$3.1.2.1.3.0.2.1.3.1.2.0.3.0.2.1.3.1.2.1.3.0.2.0.3.1.2.0.3.0.2.1.\ \ldots$$

But this is precisely the original sequence warmed up by adding 2 to every second entry:

$$31.21.30.21.31.20.30.21.31.21.30.20.31.20.30.21.$$
$$31.21.30.21.31.20.30.20.31.21.30.20.30.21.\ \ldots$$

Thus, experimentally at any rate, the new sequence, which I again call (f_h), is invariant under the uniform binary substitution

$$\theta : 0 \mapsto 20\,,\ 1 \mapsto 21\,,\ 2 \mapsto 30\,,\ 3 \mapsto 31\,.$$

Regular Binary Substitution

Next, if we pair the sequence

$$11.01.10.01.11.00.10.01.11.01.10.00.11.00.10.01.$$
$$11.01.10.01.11.00.10.00.11.01.10.00.11.00.10.01.\ \ldots$$

and interpret the pairs as numbers in base 2, we obtain

$$3.1.2.1.3.0.2.1.3.1.2.0.3.0.2.1.3.1.2.1.3.0.2.0.3.1.2.0.3.0.2.1.\ \ldots$$

But this is precisely the original sequence warmed up by adding 2 to every second entry:

$$31.21.30.21.31.20.30.21.31.21.30.20.31.20.30.21.$$
$$31.21.30.21.31.20.30.20.31.21.30.20.30.21.\ \ldots$$

Thus, experimentally at any rate, the new sequence, which I again call (f_h), is invariant under the uniform binary substitution

$$\theta : 0 \mapsto 20\,,\ 1 \mapsto 21\,,\ 2 \mapsto 30\,,\ 3 \mapsto 31\,.$$

The uniform, or regular, 2-substitution

$$\theta : 0 \mapsto 20\,,\ 1 \mapsto 21\,,\ 2 \mapsto 30\,,\ 3 \mapsto 31\,.$$

provides a transition map τ defined by the transition table:

τ	0	1
s_3	s_3	s_1
s_2	s_3	s_0
s_1	s_2	s_1
s_0	s_2	s_0

The transition table shows how each state s_i responds to the input of a binary digit and makes plain that we are dealing with a finite state automaton; specifically a four-state automaton; s_3 is its initial state.

The automaton provides a map $h \mapsto f_{h+1}$. Consider an input tape containing the digits of h written in base 2. The automaton reads the digits of h successively, disregarding initial zeros because they leave the automaton in state s_3. Finally an output map replaces s_3 or s_1 by 1, and s_2 or s_0 by 0, yielding f_{h+1}.

The uniform, or regular, 2-substitution

$$\theta : 0 \mapsto 20\,,\ 1 \mapsto 21\,,\ 2 \mapsto 30\,,\ 3 \mapsto 31\,.$$

provides a transition map τ defined by the transition table:

τ	0	1
s_3	s_3	s_1
s_2	s_3	s_0
s_1	s_2	s_1
s_0	s_2	s_0

The transition table shows how each state s_i responds to the input of a binary digit and makes plain that we are dealing with a finite state automaton; specifically a four-state automaton; s_3 is its initial state.

The automaton provides a map $h \mapsto f_{h+1}$. Consider an input tape containing the digits of h written in base 2. The automaton reads the digits of h successively, disregarding initial zeros because they leave the automaton in state s_3. Finally an output map replaces s_3 or s_1 by 1, and s_2 or s_0 by 0, yielding f_{h+1}.

The uniform, or regular, 2-substitution

$$\theta : 0 \mapsto 20\,,\ 1 \mapsto 21\,,\ 2 \mapsto 30\,,\ 3 \mapsto 31\,.$$

provides a transition map τ defined by the transition table:

τ	0	1
s_3	s_3	s_1
s_2	s_3	s_0
s_1	s_2	s_1
s_0	s_2	s_0

The transition table shows how each state s_i responds to the input of a binary digit and makes plain that we are dealing with a finite state automaton; specifically a four-state automaton; s_3 is its initial state.

The automaton provides a map $h \mapsto f_{h+1}$. Consider an input tape containing the digits of h written in base 2. The automaton reads the digits of h successively, disregarding initial zeros because they leave the automaton in state s_3. Finally an output map replaces s_3 or s_1 by 1, and s_2 or s_0 by 0, yielding f_{h+1}.

The uniform, or regular, 2-substitution

$$\theta : 0 \mapsto 20\,,\ 1 \mapsto 21\,,\ 2 \mapsto 30\,,\ 3 \mapsto 31\,.$$

provides a transition map τ defined by the transition table:

τ	0	1
s_3	s_3	s_1
s_2	s_3	s_0
s_1	s_2	s_1
s_0	s_2	s_0

The transition table shows how each state s_i responds to the input of a binary digit and makes plain that we are dealing with a finite state automaton; specifically a four-state automaton; s_3 is its initial state.

The automaton provides a map $h \mapsto f_{h+1}$. Consider an input tape containing the digits of h written in base 2. The automaton reads the digits of h successively, disregarding initial zeros because they leave the automaton in state s_3. Finally an output map replaces s_3 or s_1 by 1, and s_2 or s_0 by 0, yielding f_{h+1}.

The uniform, or regular, 2-substitution

$$\theta : 0 \mapsto 20\,,\ 1 \mapsto 21\,,\ 2 \mapsto 30\,,\ 3 \mapsto 31\,.$$

provides a transition map τ defined by the transition table:

τ	0	1
s_3	s_3	s_1
s_2	s_3	s_0
s_1	s_2	s_1
s_0	s_2	s_0

The transition table shows how each state s_i responds to the input of a binary digit and makes plain that we are dealing with a finite state automaton; specifically a four-state automaton; s_3 is its initial state.

The automaton provides a map $h \mapsto f_{h+1}$. Consider an input tape containing the digits of h written in base 2. The automaton reads the digits of h successively, disregarding initial zeros because they leave the automaton in state s_3. Finally an output map replaces s_3 or s_1 by 1, and s_2 or s_0 by 0, yielding f_{h+1}.

The uniform, or regular, 2-substitution

$$\theta : 0 \mapsto 20\,,\ 1 \mapsto 21\,,\ 2 \mapsto 30\,,\ 3 \mapsto 31\,.$$

provides a transition map τ defined by the transition table:

τ	0	1
s_3	s_3	s_1
s_2	s_3	s_0
s_1	s_2	s_1
s_0	s_2	s_0

The transition table shows how each state s_i responds to the input of a binary digit and makes plain that we are dealing with a finite state automaton; specifically a four-state automaton; s_3 is its initial state.

The automaton provides a map $h \mapsto f_{h+1}$. Consider an input tape containing the digits of h written in base 2. The automaton reads the digits of h successively, disregarding initial zeros because they leave the automaton in state s_3. Finally an output map replaces s_3 or s_1 by 1, and s_2 or s_0 by 0, yielding f_{h+1}.

The uniform, or regular, 2-substitution

$$\theta : 0 \mapsto 20\,,\ 1 \mapsto 21\,,\ 2 \mapsto 30\,,\ 3 \mapsto 31\,.$$

provides a transition map τ defined by the transition table:

τ	0	1
s_3	s_3	s_1
s_2	s_3	s_0
s_1	s_2	s_1
s_0	s_2	s_0

The transition table shows how each state s_i responds to the input of a binary digit and makes plain that we are dealing with a finite state automaton; specifically a four-state automaton; s_3 is its initial state.

The automaton provides a map $h \mapsto f_{h+1}$. Consider an input tape containing the digits of h written in base 2. The automaton reads the digits of h successively, disregarding initial zeros because they leave the automaton in state s_3. Finally an output map replaces s_3 or s_1 by 1, and s_2 or s_0 by 0, yielding f_{h+1}.

The uniform, or regular, 2-substitution

$$\theta : 0 \mapsto 20\,,\ 1 \mapsto 21\,,\ 2 \mapsto 30\,,\ 3 \mapsto 31\,.$$

provides a transition map τ defined by the transition table:

τ	0	1
s_3	s_3	s_1
s_2	s_3	s_0
s_1	s_2	s_1
s_0	s_2	s_0

The transition table shows how each state s_i responds to the input of a binary digit and makes plain that we are dealing with a finite state automaton; specifically a four-state automaton; s_3 is its initial state.

The automaton provides a map $h \mapsto f_{h+1}$. Consider an input tape containing the digits of h written in base 2. The automaton reads the digits of h successively, disregarding initial zeros because they leave the automaton in state s_3. Finally an output map replaces s_3 or s_1 by 1, and s_2 or s_0 by 0, yielding f_{h+1}.

The uniform, or regular, 2-substitution

$$\theta : 0 \mapsto 20\,,\ 1 \mapsto 21\,,\ 2 \mapsto 30\,,\ 3 \mapsto 31\,.$$

provides a transition map τ defined by the transition table:

τ	0	1
s_3	s_3	s_1
s_2	s_3	s_0
s_1	s_2	s_1
s_0	s_2	s_0

The transition table shows how each state s_i responds to the input of a binary digit and makes plain that we are dealing with a finite state automaton; specifically a four-state automaton; s_3 is its initial state.

The automaton provides a map $h \mapsto f_{h+1}$. Consider an input tape containing the digits of h written in base 2. The automaton reads the digits of h successively, disregarding initial zeros because they leave the automaton in state s_3. Finally an output map replaces s_3 or s_1 by 1, and s_2 or s_0 by 0, yielding f_{h+1}.

The uniform, or regular, 2-substitution

$$\theta : 0 \mapsto 20\,,\; 1 \mapsto 21\,,\; 2 \mapsto 30\,,\; 3 \mapsto 31\,.$$

provides a transition map τ defined by the transition table:

τ	0	1
s_3	s_3	s_1
s_2	s_3	s_0
s_1	s_2	s_1
s_0	s_2	s_0

The transition table shows how each state s_i responds to the input of a binary digit and makes plain that we are dealing with a finite state automaton; specifically a four-state automaton; s_3 is its initial state.

The automaton provides a map $h \mapsto f_{h+1}$. Consider an input tape containing the digits of h written in base 2. The automaton reads the digits of h successively, disregarding initial zeros because they leave the automaton in state s_3. Finally an output map replaces s_3 or s_1 by 1, and s_2 or s_0 by 0, yielding f_{h+1}.

Characteristic Functions

I found the formation rule by viewing the symbols in pairs as binary integers and noticing that the resulting sequence is self reproducing under the substitution θ. However, let $F_i(X)=\sum_{f_h=i} X^h$ be the characteristic function of each of the symbols $i=0$, 1, 2, and 3. It's not difficult to see from the defining substitution θ, that in fact

$$F_0(X)=F_0(X^2)+F_2(X^2),\quad XF_2(X)=F_0(X^2)+F_1(X^2),$$
$$F_1(X)=F_1(X^2)+F_3(X^2),\quad XF_3(X)=F_2(X^2)+F_3(X^2).$$

Moreover, by definition, $F_0(X)+F_1(X)+F_2(X)+F_3(X)=X/(1-X)$, and of course $F_1(X)+F_3(X)=F(X)$. In this way a trick to 'guess' the Mahler functional equation

$$F(X)=F(X^2)+X/(1-X^4)$$

is replaced by a dull and uninstructive systematic proof.

Mind you, a function $F(X^2)$, more generally $F(X^p)$, seems unnatural. One should wonder how such a function might arise naturally.

Characteristic Functions

I found the formation rule by viewing the symbols in pairs as binary integers and noticing that the resulting sequence is self reproducing under the substitution θ. However, let $F_i(X) = \sum_{f_h=i} X^h$ be the characteristic function of each of the symbols $i = 0$, 1, 2, and 3. It's not difficult to see from the defining substitution θ, that in fact

$$F_0(X) = F_0(X^2) + F_2(X^2), \quad XF_2(X) = F_0(X^2) + F_1(X^2),$$
$$F_1(X) = F_1(X^2) + F_3(X^2), \quad XF_3(X) = F_2(X^2) + F_3(X^2).$$

Moreover, by definition, $F_0(X) + F_1(X) + F_2(X) + F_3(X) = X/(1 - X)$, and of course $F_1(X) + F_3(X) = F(X)$. In this way a trick to 'guess' the Mahler functional equation

$$F(X) = F(X^2) + X/(1 - X^4)$$

is replaced by a dull and uninstructive systematic proof.

Mind you, a function $F(X^2)$, more generally $F(X^p)$, seems unnatural. One should wonder how such a function might arise naturally.

Characteristic Functions

I found the formation rule by viewing the symbols in pairs as binary integers and noticing that the resulting sequence is self reproducing under the substitution θ. However, let $F_i(X) = \sum_{f_h=i} X^h$ be the characteristic function of each of the symbols $i = 0$, 1, 2, and 3. It's not difficult to see from the defining substitution θ, that in fact

$$F_0(X) = F_0(X^2) + F_2(X^2), \quad XF_2(X) = F_0(X^2) + F_1(X^2),$$
$$F_1(X) = F_1(X^2) + F_3(X^2), \quad XF_3(X) = F_2(X^2) + F_3(X^2).$$

Moreover, by definition, $F_0(X) + F_1(X) + F_2(X) + F_3(X) = X/(1 - X)$, and of course $F_1(X) + F_3(X) = F(X)$. In this way a trick to 'guess' the Mahler functional equation

$$F(X) = F(X^2) + X/(1 - X^4)$$

is replaced by a dull and uninstructive systematic proof.

Mind you, a function $F(X^2)$, more generally $F(X^p)$, seems unnatural. One should wonder how such a function might arise naturally.

Characteristic Functions

I found the formation rule by viewing the symbols in pairs as binary integers and noticing that the resulting sequence is self reproducing under the substitution θ. However, let $F_i(X) = \sum_{f_h=i} X^h$ be the characteristic function of each of the symbols $i = 0$, 1, 2, and 3. It's not difficult to see from the defining substitution θ, that in fact

$$F_0(X) = F_0(X^2) + F_2(X^2), \quad XF_2(X) = F_0(X^2) + F_1(X^2),$$
$$F_1(X) = F_1(X^2) + F_3(X^2), \quad XF_3(X) = F_2(X^2) + F_3(X^2).$$

Moreover, by definition, $F_0(X) + F_1(X) + F_2(X) + F_3(X) = X/(1 - X)$, and of course $F_1(X) + F_3(X) = F(X)$. In this way a trick to 'guess' the Mahler functional equation

$$F(X) = F(X^2) + X/(1 - X^4)$$

is replaced by a dull and uninstructive systematic proof.

Mind you, a function $F(X^2)$, more generally $F(X^p)$, seems unnatural. One should wonder how such a function might arise naturally.

Characteristic Functions

I found the formation rule by viewing the symbols in pairs as binary integers and noticing that the resulting sequence is self reproducing under the substitution θ. However, let $F_i(X) = \sum_{f_h=i} X^h$ be the characteristic function of each of the symbols $i = 0$, 1, 2, and 3. It's not difficult to see from the defining substitution θ, that in fact

$$F_0(X) = F_0(X^2) + F_2(X^2), \quad XF_2(X) = F_0(X^2) + F_1(X^2),$$
$$F_1(X) = F_1(X^2) + F_3(X^2), \quad XF_3(X) = F_2(X^2) + F_3(X^2).$$

Moreover, by definition, $F_0(X) + F_1(X) + F_2(X) + F_3(X) = X/(1 - X)$, and of course $F_1(X) + F_3(X) = F(X)$. In this way a trick to 'guess' the Mahler functional equation

$$F(X) = F(X^2) + X/(1 - X^4)$$

is replaced by a dull and uninstructive systematic proof.

Mind you, a function $F(X^2)$, more generally $F(X^p)$, seems unnatural. One should wonder how such a function might arise naturally.

Characteristic Functions

I found the formation rule by viewing the symbols in pairs as binary integers and noticing that the resulting sequence is self reproducing under the substitution θ. However, let $F_i(X) = \sum_{f_h=i} X^h$ be the characteristic function of each of the symbols $i = 0$, 1, 2, and 3. It's not difficult to see from the defining substitution θ, that in fact

$$F_0(X) = F_0(X^2) + F_2(X^2), \quad XF_2(X) = F_0(X^2) + F_1(X^2),$$
$$F_1(X) = F_1(X^2) + F_3(X^2), \quad XF_3(X) = F_2(X^2) + F_3(X^2).$$

Moreover, by definition, $F_0(X) + F_1(X) + F_2(X) + F_3(X) = X/(1 - X)$, and of course $F_1(X) + F_3(X) = F(X)$. In this way a trick to 'guess' the Mahler functional equation

$$F(X) = F(X^2) + X/(1 - X^4)$$

is replaced by a dull and uninstructive systematic proof.

Mind you, a function $F(X^2)$, more generally $F(X^p)$, seems unnatural. One should wonder how such a function might arise naturally.

An Algebraic Equation in Characteristic p

For a prime p, and for G any formal power series with integer coefficients,

$$G(X^p) \equiv (G(X))^p \bmod p\text{; equivalently } G(X^p) = (G(X))^p$$

in the ring $\mathbb{F}_p[[X]]$ of formal power series over the finite field $\mathbb{F}_p$ of p elements. This is plain because the Frobenius map $x \mapsto x^p$ is an additive automorphism (that is: by Fermat's Little Theorem and because all the multinomial coefficients other than those on the diagonal vanish modulo p). Hence the Mahler functional equation

$$(1 - X^4)F(X)^2 - (1 - X^4)F(X) + X = 0$$

for $F = F_1 + F_3$ becomes the equation

$$(1 + X)^4 F^2 + (1 + X)^4 F + X = 0\,,$$

showing that F is an algebraic element over $\mathbb{F}_2[[X]]$.

In general, a linear relation on $1,\ F(X),\ F(X^p),\ \ldots,$ over $\mathbb{Z}[X]$ reduces to an algebraic equation over over $\mathbb{F}_p[X]$ linearly relating $1,\ F,\ F^p,\ \ldots\,.$

An Algebraic Equation in Characteristic p

For a prime p, and for G any formal power series with integer coefficients,

$$G(X^p) \equiv (G(X))^p \bmod p\text{; equivalently } G(X^p) = (G(X))^p$$

in the ring $\mathbb{F}_p[[X]]$ of formal power series over the finite field $\mathbb{F}_p$ of p elements. This is plain because the Frobenius map $x \mapsto x^p$ is an additive automorphism (that is: by Fermat's Little Theorem and because all the multinomial coefficients other than those on the diagonal vanish modulo p). Hence the Mahler functional equation

$$(1 - X^4)F(X)^2 - (1 - X^4)F(X) + X = 0$$

for $F = F_1 + F_3$ becomes the equation

$$(1 + X)^4 F^2 + (1 + X)^4 F + X = 0\,,$$

showing that F is an algebraic element over $\mathbb{F}_2[[X]]$.

In general, a linear relation on $1,\ F(X),\ F(X^p),\ \ldots,$ over $\mathbb{Z}[X]$ reduces to an algebraic equation over over $\mathbb{F}_p[X]$ linearly relating $1,\ F,\ F^p,\ \ldots$.

An Algebraic Equation in Characteristic p

For a prime p, and for G any formal power series with integer coefficients,

$$G(X^p) \equiv (G(X))^p \bmod p; \text{ equivalently } G(X^p) = (G(X))^p$$

in the ring $\mathbb{F}_p[[X]]$ of formal power series over the finite field $\mathbb{F}_p$ of p elements. This is plain because the Frobenius map $x \mapsto x^p$ is an additive automorphism (that is: by Fermat's Little Theorem and because all the multinomial coefficients other than those on the diagonal vanish modulo p). Hence the Mahler functional equation

$$(1 - X^4)F(X)^2 - (1 - X^4)F(X) + X = 0$$

for $F = F_1 + F_3$ becomes the equation

$$(1 + X)^4F^2 + (1 + X)^4F + X = 0\,,$$

showing that F is an algebraic element over $\mathbb{F}_2[[X]]$.

In general, a linear relation on $1,\ F(X),\ F(X^p),\ \dots,$ over $\mathbb{Z}[X]$ reduces to an algebraic equation over over $\mathbb{F}_p[X]$ linearly relating $1,\ F,\ F^p,\ \dots$.

An Algebraic Equation in Characteristic p

For a prime p, and for G any formal power series with integer coefficients,

$$G(X^p) \equiv (G(X))^p \bmod p\text{; equivalently } G(X^p) = (G(X))^p$$

in the ring $\mathbb{F}_p[[X]]$ of formal power series over the finite field $\mathbb{F}_p$ of p elements. This is plain because the Frobenius map $x \mapsto x^p$ is an additive automorphism (that is: by Fermat's Little Theorem and because all the multinomial coefficients other than those on the diagonal vanish modulo p). Hence the Mahler functional equation

$$(1 - X^4)F(X)^2 - (1 - X^4)F(X) + X = 0$$

for $F = F_1 + F_3$ becomes the equation

$$(1 + X)^4 F^2 + (1 + X)^4 F + X = 0\,,$$

showing that F is an algebraic element over $\mathbb{F}_2[[X]]$.

In general, a linear relation on $1,\ F(X),\ F(X^p),\ \ldots,$ over $\mathbb{Z}[X]$ reduces to an algebraic equation over over $\mathbb{F}_p[X]$ linearly relating $1,\ F,\ F^p,\ \ldots$.

An Algebraic Equation in Characteristic p

For a prime p, and for G any formal power series with integer coefficients,

$$G(X^p) \equiv (G(X))^p \bmod p\text{; equivalently } G(X^p) = (G(X))^p$$

in the ring $\mathbb{F}_p[[X]]$ of formal power series over the finite field $\mathbb{F}_p$ of p elements. This is plain because the Frobenius map $x \mapsto x^p$ is an additive automorphism (that is: by Fermat's Little Theorem and because all the multinomial coefficients other than those on the diagonal vanish modulo p). Hence the Mahler functional equation

$$(1 - X^4)F(X)^2 - (1 - X^4)F(X) + X = 0$$

for $F = F_1 + F_3$ becomes the equation

$$(1 + X)^4 F^2 + (1 + X)^4 F + X = 0\,,$$

showing that F is an algebraic element over $\mathbb{F}_2[[X]]$.

In general, a linear relation on 1, $F(X)$, $F(X^p)$, $\ldots$, over $\mathbb{Z}[X]$ reduces to an algebraic equation over over $\mathbb{F}_p[X]$ linearly relating 1, F, F^p, $\ldots$.

An Algebraic Equation in Characteristic p

For a prime p, and for G any formal power series with integer coefficients,

$$G(X^p) \equiv (G(X))^p \bmod p; \text{ equivalently } G(X^p) = (G(X))^p$$

in the ring $\mathbb{F}_p[[X]]$ of formal power series over the finite field $\mathbb{F}_p$ of p elements. This is plain because the Frobenius map $x \mapsto x^p$ is an additive automorphism (that is: by Fermat's Little Theorem and because all the multinomial coefficients other than those on the diagonal vanish modulo p). Hence the Mahler functional equation

$$(1 - X^4)F(X)^2 - (1 - X^4)F(X) + X = 0$$

for $F = F_1 + F_3$ becomes the equation

$$(1 + X)^4 F^2 + (1 + X)^4 F + X = 0\,,$$

showing that F is an algebraic element over $\mathbb{F}_2[[X]]$.

In general, a linear relation on 1, $F(X)$, $F(X^p)$, $\ldots$, over $\mathbb{Z}[X]$ reduces to an algebraic equation over over $\mathbb{F}_p[X]$ linearly relating 1, F, F^p, $\ldots$.

An Algebraic Equation in Characteristic p

For a prime p, and for G any formal power series with integer coefficients,

$$G(X^p) \equiv (G(X))^p \bmod p; \text{ equivalently } G(X^p) = (G(X))^p$$

in the ring $\mathbb{F}_p[[X]]$ of formal power series over the finite field $\mathbb{F}_p$ of p elements. This is plain because the Frobenius map $x \mapsto x^p$ is an additive automorphism (that is: by Fermat's Little Theorem and because all the multinomial coefficients other than those on the diagonal vanish modulo p). Hence the Mahler functional equation

$$(1 - X^4)F(X)^2 - (1 - X^4)F(X) + X = 0$$

for $F = F_1 + F_3$ becomes the equation

$$(1 + X)^4 F^2 + (1 + X)^4 F + X = 0\,,$$

showing that F is an algebraic element over $\mathbb{F}_2[[X]]$.

In general, a linear relation on 1, $F(X)$, $F(X^p)$, $\ldots$, over $\mathbb{Z}[X]$ reduces to an algebraic equation over over $\mathbb{F}_p[X]$ linearly relating 1, F, F^p, $\ldots$.

These remarks show that the paperfolding sequence (f_h) is

(i) (an image of) a sequence invariant under the substitution θ and is

(ii) therefore given by $\lim_{h\to\infty}\theta^h(3)$, where $\theta(3) = 31$, $\theta^2(3) = \theta(31) = \theta(3)\theta(1) = 3121, \ldots$.

(iii) It follows that the sequence is 2-automatic, that is there are only finitely many distinct subsequences $\{f_{2^k h+r} \colon k \geq 0,\ 0 \leq r < 2^k\}$; in the present case (f_h) itself, and the purely periodic sequences with period 0, 1, or 10.

(iv) Equivalently the corresponding transition map defines a finite state automaton which maps $h \mapsto f_{h+1}$, or, if one prefers,

(v) the substitution defines a system of Mahler functional equations satisfied by the characteristic function of each state and therefore such an equation satisfied by the paperfolding function.

(vi) Reduction mod 2 of that equation yields an algebraic equation for the paperfolding function over $\mathbb{F}_2(X)$.

These remarks show that the paperfolding sequence (f_h) is

(i) (an image of) a sequence invariant under the substitution θ and is

(ii) therefore given by $\lim_{h\to\infty} \theta^h(3)$, where $\theta(3) = 31$, $\theta^2(3) = \theta(31) = \theta(3)\theta(1) = 3121, \ldots$.

(iii) It follows that the sequence is 2-automatic, that is there are only finitely many distinct subsequences $\{f_{2^k h+r} \colon k \geq 0,\ 0 \leq r < 2^k\}$; in the present case (f_h) itself, and the purely periodic sequences with period 0, 1, or 10.

(iv) Equivalently the corresponding transition map defines a finite state automaton which maps $h \mapsto f_{h+1}$, or, if one prefers,

(v) the substitution defines a system of Mahler functional equations satisfied by the characteristic function of each state and therefore such an equation satisfied by the paperfolding function.

(vi) Reduction mod 2 of that equation yields an algebraic equation for the paperfolding function over $\mathbb{F}_2(X)$.

These remarks show that the paperfolding sequence (f_h) is

(i) (an image of) a sequence invariant under the substitution θ and is

(ii) therefore given by $\lim_{h\to\infty} \theta^h(3)$, where $\theta(3) = 31$, $\theta^2(3) = \theta(31) = \theta(3)\theta(1) = 3121, \dots$.

(iii) It follows that the sequence is 2-automatic, that is there are only finitely many distinct subsequences $\{f_{2^k h+r} \colon k \geq 0,\ 0 \leq r < 2^k\}$; in the present case (f_h) itself, and the purely periodic sequences with period 0, 1, or 10.

(iv) Equivalently the corresponding transition map defines a finite state automaton which maps $h \mapsto f_{h+1}$, or, if one prefers,

(v) the substitution defines a system of Mahler functional equations satisfied by the characteristic function of each state and therefore such an equation satisfied by the paperfolding function.

(vi) Reduction mod 2 of that equation yields an algebraic equation for the paperfolding function over $\mathbb{F}_2(X)$.

These remarks show that the paperfolding sequence (f_h) is

(i) (an image of) a sequence invariant under the substitution θ and is

(ii) therefore given by $\lim_{h\to\infty} \theta^h(3)$, where $\theta(3) = 31$, $\theta^2(3) = \theta(31) = \theta(3)\theta(1) = 3121, \ldots$.

(iii) It follows that the sequence is 2-automatic, that is there are only finitely many distinct subsequences $\{f_{2^k h+r} \colon k \geq 0,\ 0 \leq r < 2^k\}$; in the present case (f_h) itself, and the purely periodic sequences with period 0, 1, or 10.

(iv) Equivalently the corresponding transition map defines a finite state automaton which maps $h \mapsto f_{h+1}$, or, if one prefers,

(v) the substitution defines a system of Mahler functional equations satisfied by the characteristic function of each state and therefore such an equation satisfied by the paperfolding function.

(vi) Reduction mod 2 of that equation yields an algebraic equation for the paperfolding function over $\mathbb{F}_2(X)$.

These remarks show that the paperfolding sequence (f_h) is

(i) (an image of) a sequence invariant under the substitution θ and is

(ii) therefore given by $\lim_{h\to\infty}\theta^h(3)$, where $\theta(3)=31$, $\theta^2(3)=\theta(31)=\theta(3)\theta(1)=3121, \ldots$.

(iii) It follows that the sequence is 2-automatic, that is there are only finitely many distinct subsequences $\{f_{2^k h+r} \colon k\geq 0,\ 0\leq r<2^k\}$; in the present case (f_h) itself, and the purely periodic sequences with period 0, 1, or 10.

(iv) Equivalently the corresponding transition map defines a finite state automaton which maps $h\mapsto f_{h+1}$, or, if one prefers,

(v) the substitution defines a system of Mahler functional equations satisfied by the characteristic function of each state and therefore such an equation satisfied by the paperfolding function.

(vi) Reduction mod 2 of that equation yields an algebraic equation for the paperfolding function over $\mathbb{F}_2(X)$.

The Thue-Morse Sequence

0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	...
0	1	1	0	1	0	0	1	1	0	0	1	0	1	...

The Thue-Morse sequence

$$(s_h)_{h\geq 0} := 0110100110\,0101101001\,0110011010\,0110\ldots\ ,$$

lays compelling claim to being the simplest nontrivial (non-periodic) sequence. It is generated by the rule that $s_h \equiv: s_2(h) \pmod 2$.

Here, $s_p(h)$ denotes the sum of the digits of h written in base p. The function $s_p(h)$ crops up in real life in the following way: It is a cute exercise to confirm that the precise power, $\operatorname{ord}_p h!$, to which a prime p divides $h!$ is $\operatorname{ord}_p h! = \bigl(h - s_p(h)\bigr)/(p-1)$.

More, suppose $a + b = c$ in nonnegative integers a, b, and c. Then $s_2(a) + s_2(b) - s_2(c)$ is both the number of carries required when adding a to b in binary; and is $\operatorname{ord}_2 \binom{a+b}{a}$.

The Thue-Morse Sequence

0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	...
0	1	1	0	1	0	0	1	1	0	0	1	0	1	...

The Thue-Morse sequence

$$(s_h)_{h\geq 0} := 0110100110\,0101101001\,0110011010\,0110\ldots\ ,$$

lays compelling claim to being the simplest nontrivial (non-periodic) sequence. It is generated by the rule that $s_h \equiv: s_2(h) \pmod 2$.

Here, $s_p(h)$ denotes the sum of the digits of h written in base p. The function $s_p(h)$ crops up in real life in the following way: It is a cute exercise to confirm that the precise power, $\operatorname{ord}_p h!$, to which a prime p divides $h!$ is $\operatorname{ord}_p h! = \big(h - s_p(h)\big)/(p-1)$.

More, suppose $a+b=c$ in nonnegative integers a, b, and c. Then $s_2(a)+s_2(b)-s_2(c)$ is both the number of carries required when adding a to b in binary; and is $\operatorname{ord}_2\binom{a+b}{a}$.

The Thue-Morse Sequence

0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	...
0	1	1	0	1	0	0	1	1	0	0	1	0	1	...

The Thue-Morse sequence

$$(s_h)_{h\geq 0} := 0110100110\,0101101001\,0110011010\,0110\ldots\ ,$$

lays compelling claim to being the simplest nontrivial (non-periodic) sequence. It is generated by the rule that $s_h \equiv: s_2(h) \pmod 2$.

Here, $s_p(h)$ denotes the sum of the digits of h written in base p. The function $s_p(h)$ crops up in real life in the following way: It is a cute exercise to confirm that the precise power, $\operatorname{ord}_p h!$, to which a prime p divides $h!$ is $\operatorname{ord}_p h! = \big(h - s_p(h)\big)/(p-1)$.

More, suppose $a+b=c$ in nonnegative integers a, b, and c. Then $s_2(a)+s_2(b)-s_2(c)$ is both the number of carries required when adding a to b in binary; and is $\operatorname{ord}_2\binom{a+b}{a}$.

The Thue-Morse Sequence

0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	...
0	1	1	0	1	0	0	1	1	0	0	1	0	1	...

The Thue-Morse sequence

$$(s_h)_{h\geq 0} := 0110100110\,0101101001\,0110011010\,0110\ldots\ ,$$

lays compelling claim to being the simplest nontrivial (non-periodic) sequence. It is generated by the rule that $s_h \equiv: s_2(h) \pmod 2$.

Here, $s_p(h)$ denotes the sum of the digits of h written in base p. The function $s_p(h)$ crops up in real life in the following way: It is a cute exercise to confirm that the precise power, $\operatorname{ord}_p h!$, to which a prime p divides $h!$ is $\operatorname{ord}_p h! = \big(h - s_p(h)\big)/(p-1)$.

More, suppose $a + b = c$ in nonnegative integers a, b, and c. Then $s_2(a) + s_2(b) - s_2(c)$ is both the number of carries required when adding a to b in binary; and is $\operatorname{ord}_2 \binom{a+b}{a}$.

Euler's Identity and a Functional Equation

Fairly obviously, the sequence (s_h) is invariant under the uniform binary substitution $\theta : 0 \mapsto 01$ and $1 \mapsto 10$. Now recall Euler's identity

$$\prod_{n=0}^{\infty}\left(1 + X^{2^n}\right) = \sum_{h=0}^{\infty} X^h = \frac{1}{1-X}\,,$$

noting it is just a pleasant way of recalling that the nonegative integers each have a unique representation in base 2. It will then also be fairly obvious that

$$T(X) := \prod_{n=0}^{\infty}\left(1 - X^{2^n}\right) = \sum_{h=0}^{\infty}(-1)^{s_h} X^h\,;$$

and that plainly $T(X) = \sum_{h=0}^{\infty}(-1)^{s_h} X^h$ satisfies the Mahler functional equation

$$(1-X)T(X^2) = T(X)\,.$$

Euler's Identity and a Functional Equation

Fairly obviously, the sequence (s_h) is invariant under the uniform binary substitution $\theta : 0 \mapsto 01$ and $1 \mapsto 10$. Now recall Euler's identity

$$\prod_{n=0}^{\infty}\left(1 + X^{2^n}\right) = \sum_{h=0}^{\infty} X^h = \frac{1}{1-X},$$

noting it is just a pleasant way of recalling that the nonegative integers each have a unique representation in base 2. It will then also be fairly obvious that

$$T(X) := \prod_{n=0}^{\infty}\left(1 - X^{2^n}\right) = \sum_{h=0}^{\infty}(-1)^{s_h} X^h;$$

and that plainly $T(X) = \sum_{h=0}^{\infty}(-1)^{s_h} X^h$ satisfies the Mahler functional equation

$$(1-X)T(X^2) = T(X).$$

Euler's Identity and a Functional Equation

Fairly obviously, the sequence (s_h) is invariant under the uniform binary substitution $\theta : 0 \mapsto 01$ and $1 \mapsto 10$. Now recall Euler's identity

$$\prod_{n=0}^{\infty}\left(1 + X^{2^n}\right) = \sum_{h=0}^{\infty} X^h = \frac{1}{1-X},$$

noting it is just a pleasant way of recalling that the nonnegative integers each have a unique representation in base 2. It will then also be fairly obvious that

$$T(X) := \prod_{n=0}^{\infty}\left(1 - X^{2^n}\right) = \sum_{h=0}^{\infty}(-1)^{s_h} X^h;$$

and that plainly $T(X) = \sum_{h=0}^{\infty}(-1)^{s_h} X^h$ satisfies the Mahler functional equation

$$(1-X)T(X^2) = T(X).$$

Euler's Identity and a Functional Equation

Fairly obviously, the sequence (s_h) is invariant under the uniform binary substitution $\theta : 0 \mapsto 01$ and $1 \mapsto 10$. Now recall Euler's identity

$$\prod_{n=0}^{\infty}\left(1+X^{2^n}\right)=\sum_{h=0}^{\infty}X^h=\frac{1}{1-X}\,,$$

noting it is just a pleasant way of recalling that the nonegative integers each have a unique representation in base 2. It will then also be fairly obvious that

$$T(X):=\prod_{n=0}^{\infty}\left(1-X^{2^n}\right)=\sum_{h=0}^{\infty}(-1)^{s_h}X^h\,;$$

and that plainly $T(X)=\sum_{h=0}^{\infty}(-1)^{s_h}X^h$ satisfies the Mahler functional equation

$$(1-X)T(X^2)=T(X)\,.$$

Euler's Identity and a Functional Equation

Fairly obviously, the sequence (s_h) is invariant under the uniform binary substitution $\theta : 0 \mapsto 01$ and $1 \mapsto 10$. Now recall Euler's identity

$$\prod_{n=0}^{\infty}\left(1+X^{2^n}\right)=\sum_{h=0}^{\infty}X^h=\frac{1}{1-X}\,,$$

noting it is just a pleasant way of recalling that the nonegative integers each have a unique representation in base 2. It will then also be fairly obvious that

$$T(X):=\prod_{n=0}^{\infty}\left(1-X^{2^n}\right)=\sum_{h=0}^{\infty}(-1)^{s_h}X^h\,;$$

and that plainly $T(X)=\sum_{h=0}^{\infty}(-1)^{s_h}X^h$ satisfies the Mahler functional equation

$$(1-X)T(X^2)=T(X)\,.$$

An Algebraic Equation

The function $S(X)=\sum_{h=0}^{\infty} s_h X^h$ therefore satisfies

$$(1-X^2)(1-X)S(X^2)-(1-X^2)S(X)+X=0\,.$$

Exercise. Show that for an arbitrary sequence (i_h), with $i_h \in \{0,1\}$, one has $\sum(-1)^{i_h}X^h=(1-X)^{-1}-2\sum i_h X^h$, and hence confirm the “therefore” above.

Hence, reducing modulo 2, we see that over the finite field $\mathbb{F}_2$ we have

$$(1+X)^3S^2+(1+X)^2S+X=0\,,$$

showing that S is quadratic irrational over the field $\mathbb{F}_2(X)$.

An Algebraic Equation

The function $S(X)=\sum_{h=0}^{\infty}s_hX^h$ therefore satisfies

$$(1-X^2)(1-X)S(X^2)-(1-X^2)S(X)+X=0\,.$$

Exercise. Show that for an arbitrary sequence (i_h), with $i_h\in\{0,1\}$, one has $\sum(-1)^{i_h}X^h=(1-X)^{-1}-2\sum i_hX^h\,,$ and hence confirm the "therefore" above.

Hence, reducing modulo 2, we see that over the finite field $\mathbb{F}_2$ we have

$$(1+X)^3S^2+(1+X)^2S+X=0\,,$$

showing that S is quadratic irrational over the field $\mathbb{F}_2(X)$.

An Algebraic Equation

The function $S(X) = \sum_{h=0}^{\infty} s_h X^h$ therefore satisfies

$$(1 - X^2)(1 - X)S(X^2) - (1 - X^2)S(X) + X = 0\,.$$

Exercise. Show that for an arbitrary sequence (i_h), with $i_h \in \{0, 1\}$, one has $\sum (-1)^{i_h} X^h = (1 - X)^{-1} - 2\sum i_h X^h$, and hence confirm the "therefore" above.

Hence, reducing modulo 2, we see that over the finite field $\mathbb{F}_2$ we have

$$(1 + X)^3 S^2 + (1 + X)^2 S + X = 0\,,$$

showing that S is quadratic irrational over the field $\mathbb{F}_2(X)$.

A Counter-example in Analysis

I claim that, whatever the choice of signs $\pm$,

$$\max_{0\le\theta\le 1} \left|\sum_{h=0}^{n-1} \pm e^{2\pi i h\theta}\right| \ge \sqrt{n}.$$

Indeed, by well known orthogonality relations,

$$\int_0^1 \left|\sum_{h=0}^{n-1} \pm e^{2\pi i h\theta}\right|^2 d\theta = n.$$

But what *is* $\min_{\pm} \max_{0\le\theta\le 1} \left|\sum_{h=0}^{n-1} \pm e^{2\pi i h\theta}\right|$?

After suitable statistical incantations, almost surely

$$\min_{\pm} \max_{0\le\theta\le 1} \left|\sum_{h=0}^{n-1} \pm e^{2\pi i h\theta}\right| = O(\sqrt{n}\log\log n).$$

Perhaps the correct question is: What choices $(i_0, \ldots, i_{n-1})$ minimise

$$\max_{0\le\theta\le 1} \left|\sum_{h=0}^{n-1} (-1)^{i_h} e^{2\pi i h\theta}\right| ?$$

A Counter-example in Analysis

I claim that, whatever the choice of signs $\pm$,

$$\max_{0\le\theta\le 1} \left|\sum_{h=0}^{n-1} \pm e^{2\pi i h\theta}\right| \ge \sqrt{n}.$$

Indeed, by well known orthogonality relations,

$$\int_0^1 \left|\sum_{h=0}^{n-1} \pm e^{2\pi i h\theta}\right|^2 d\theta = n.$$

But what is $\min_{\pm} \max_{0\le\theta\le 1} \left|\sum_{h=0}^{n-1} \pm e^{2\pi i h\theta}\right|$?

After suitable statistical incantations, almost surely

$$\min_{\pm} \max_{0\le\theta\le 1} \left|\sum_{h=0}^{n-1} \pm e^{2\pi i h\theta}\right| = O(\sqrt{n}\log\log n).$$

Perhaps the correct question is: What choices $(i_0, \dots, i_{n-1})$ minimise

$$\max_{0\le\theta\le 1} \left|\sum_{h=0}^{n-1} (-1)^{i_h} e^{2\pi i h\theta}\right| ?$$

A Counter-example in Analysis

I claim that, whatever the choice of signs $\pm$,

$$\max_{0\le\theta\le 1} \Big|\sum_{h=0}^{n-1} \pm e^{2\pi i h\theta}\Big| \ge \sqrt{n}.$$

Indeed, by well known orthogonality relations,

$$\int_0^1 \Big|\sum_{h=0}^{n-1} \pm e^{2\pi i h\theta}\Big|^2 \, d\theta = n.$$

But what is $\min_{\pm} \max_{0\le\theta\le 1} \big|\sum_{h=0}^{n-1} \pm e^{2\pi i h\theta}\big|$?

After suitable statistical incantations, almost surely

$$\min_{\pm} \max_{0\le\theta\le 1} \Big|\sum_{h=0}^{n-1} \pm e^{2\pi i h\theta}\Big| = O(\sqrt{n}\log\log n).$$

Perhaps the correct question is: What choices $(i_0, \ldots, i_{n-1})$ minimise

$$\max_{0\le\theta\le 1} \Big|\sum_{h=0}^{n-1} (-1)^{i_h} e^{2\pi i h\theta}\Big| \; ?$$

A Counter-example in Analysis

I claim that, whatever the choice of signs $\pm$,

$$\max_{0\le\theta\le 1} \left| \sum_{h=0}^{n-1} \pm e^{2\pi i h\theta} \right| \ge \sqrt{n}.$$

Indeed, by well known orthogonality relations,

$$\int_0^1 \left| \sum_{h=0}^{n-1} \pm e^{2\pi i h\theta} \right|^2 d\theta = n.$$

But what is $\min_{\pm} \max_{0\le\theta\le 1} \left| \sum_{h=0}^{n-1} \pm e^{2\pi i h\theta} \right|$?

After suitable statistical incantations, almost surely

$$\min_{\pm} \max_{0\le\theta\le 1} \left| \sum_{h=0}^{n-1} \pm e^{2\pi i h\theta} \right| = O(\sqrt{n} \log\log n).$$

Perhaps the correct question is: What choices $(i_0, \ldots, i_{n-1})$ minimise

$$\max_{0\le\theta\le 1} \left| \sum_{h=0}^{n-1} (-1)^{i_h} e^{2\pi i h\theta} \right| ?$$

A Counter-example in Analysis

I claim that, whatever the choice of signs $\pm$,

$$\max_{0\le\theta\le 1} \left|\sum_{h=0}^{n-1} \pm e^{2\pi i h\theta}\right| \ge \sqrt{n}.$$

Indeed, by well known orthogonality relations,

$$\int_0^1 \left|\sum_{h=0}^{n-1} \pm e^{2\pi i h\theta}\right|^2 d\theta = n.$$

But what is $\min_{\pm} \max_{0\le\theta\le 1} \left|\sum_{h=0}^{n-1} \pm e^{2\pi i h\theta}\right|$?

After suitable statistical incantations, almost surely

$$\min_{\pm} \max_{0\le\theta\le 1} \left|\sum_{h=0}^{n-1} \pm e^{2\pi i h\theta}\right| = O(\sqrt{n}\log\log n).$$

Perhaps the correct question is: What choices $(i_0, \dots, i_{n-1})$ minimise

$$\max_{0\le\theta\le 1} \left|\sum_{h=0}^{n-1} (-1)^{i_h} e^{2\pi i h\theta}\right| ?$$

A Counter-example in Analysis

I claim that, whatever the choice of signs $\pm$,

$$\max_{0\le\theta\le 1} \Big|\sum_{h=0}^{n-1} \pm e^{2\pi i h\theta}\Big| \ge \sqrt{n}.$$

Indeed, by well known orthogonality relations,

$$\int_0^1 \Big|\sum_{h=0}^{n-1} \pm e^{2\pi i h\theta}\Big|^2 d\theta = n.$$

But what is $\min_{\pm} \max_{0\le\theta\le 1} |\sum_{h=0}^{n-1} \pm e^{2\pi i h\theta}|$?

After suitable statistical incantations, almost surely

$$\min_{\pm} \max_{0\le\theta\le 1} \Big|\sum_{h=0}^{n-1} \pm e^{2\pi i h\theta}\Big| = O(\sqrt{n}\log\log n).$$

Perhaps the correct question is: What choices $(i_0, \ldots, i_{n-1})$ minimise

$$\max_{0\le\theta\le 1} \Big|\sum_{h=0}^{n-1} (-1)^{i_h} e^{2\pi i h\theta}\Big| \ ?$$

The Shapiro Sequence

Consider, the Shapiro sequence (r_h), which counts mod 2 the number of occurrences of the pair 11 of digits in the binary expansion of h.

0001001000 0111010001 0010111000 1000010010 0001110111 . . .

0 1 0 2 0 1 3 1 0 1 0 2 3 2 0 2 0 1 0 2 0 1 3 1 3 . . .

0001001000 0111010001 0010111000 1000010010 0001110111 . . .

So, the Shapiro sequence is generated by the automaton defined by the transition table given by θ and with output map s_0 and $s_1 \leftarrow 0$, and s_2 and $s_3 \leftarrow 1$. Remarkably

$$\max_{0\le\theta\le1} \Big|\sum_{h=0}^{n-1}(-1)^{r_h}e^{ih\theta}\Big| \le (2+\sqrt{2})\sqrt{n}.$$

The Shapiro Sequence

Consider, the Shapiro sequence (r_h), which counts mod 2 the number of occurrences of the pair 11 of digits in the binary expansion of h.

0001001000 0111010001 0010111000 1000010010 0001110111 ...

0 1 0 2 0 1 3 1 0 1 0 2 3 2 0 2 0 1 0 2 0 1 3 1 3 ...

0001001000 0111010001 0010111000 1000010010 0001110111 ...

So, the Shapiro sequence is generated by the automaton defined by the transition table given by θ and with output map s_0 and $s_1 \leftarrow 0$, and s_2 and $s_3 \leftarrow 1$. Remarkably

$$\max_{0 \le \theta \le 1} \left| \sum_{h=0}^{n-1} (-1)^{r_h} e^{ih\theta} \right| \le (2+\sqrt{2})\sqrt{n}.$$

The Shapiro Sequence

Consider, the Shapiro sequence (r_h), which counts mod 2 the number of occurrences of the pair 11 of digits in the binary expansion of h.

0001001000 0111010001 0010111000 1000010010 0001110111 . . .

0 1 0 2 0 1 3 1 0 1 0 2 3 2 0 2 0 1 0 2 0 1 3 1 3 . . .

0001001000 0111010001 0010111000 1000010010 0001110111 . . .

Here the blue sequence is the result of an ingenious pairing

So, the Shapiro sequence is generated by the automaton defined by the transition table given by θ and with output map s_0 and $s_1 \leftarrow 0$, and s_2 and $s_3 \leftarrow 1$. Remarkably

$$\max_{0\le\theta\le1} \Big|\sum_{h=0}^{n-1}(-1)^{r_h}e^{ih\theta}\Big| \le (2+\sqrt{2})\sqrt{n}.$$

The Shapiro Sequence

Consider, the Shapiro sequence (r_h), which counts mod 2 the number of occurrences of the pair 11 of digits in the binary expansion of h.

$$0001001000\ 0111010001\ 0010111000\ 1000010010\ 0001110111\ldots$$
$$0\ 1\ 0\ 2\ 0\quad 1\ 3\ 1\ 0\ 1\quad 0\ 2\ 3\ 2\ 0\quad 2\ 0\ 1\ 0\ 2\quad 0\ 1\ 3\ 1\ 3\ldots$$
$$0102013101\ 0232020102\ 0131323101\ 3101020131\ 0102320232\ldots$$
$$0001001000\ 0111010001\ 0010111000\ 1000010010\ 0001110111\ldots$$

Here the blue sequence is the result of an ingenious pairing; the brown sequence then recognises that (r_h) is given by the regular binary substitution $\theta : 0 \mapsto 01\,,\ 1 \mapsto 02\,,\ 2 \mapsto 31\,,\ 3 \mapsto 32$.

The intermediate symbols $\{0, 1, 2, 3\}$ represent the four states $\{s_0, s_1, s_2, s_3\}$ of a binary automaton. So, the Shapiro sequence is generated by the automaton defined by the transition table given by θ and with output map s_0 and $s_1 \longleftarrow 0$, and s_2 and $s_3 \longleftarrow 1$. Remarkably

$$\max_{0\le\theta\le1}\Big|\sum_{h=0}^{n-1}(-1)^{r_h}e^{ih\theta}\Big| \le (2+\sqrt{2})\sqrt{n}\,.$$

The Shapiro Sequence

Consider, the Shapiro sequence (r_h), which counts mod 2 the number of occurrences of the pair 11 of digits in the binary expansion of h.

$$\begin{array}{l}
0001001000\ 0111010001\ 0010111000\ 1000010010\ 0001110111\ldots\\
0\ 1\ 0\ 2\ 0\quad 1\ 3\ 1\ 0\ 1\quad 0\ 2\ 3\ 2\ 0\quad 2\ 0\ 1\ 0\ 2\quad 0\ 1\ 3\ 1\ 3\ldots\\
0102013101\ 0232020102\ 0131323101\ 3101020131\ 0102320232\ldots\\
0001001000\ 0111010001\ 0010111000\ 1000010010\ 0001110111\ldots
\end{array}$$

Here the blue sequence is the result of an ingenious pairing; the brown sequence then recognises that (r_h) is given by the regular binary substitution $\theta: 0 \mapsto 01\,, 1 \mapsto 02\,, 2 \mapsto 31\,, 3 \mapsto 32$.

The intermediate symbols $\{0,1,2,3\}$ represent the four states $\{s_0, s_1, s_2, s_3\}$ of a binary automaton. So, the Shapiro sequence is generated by the automaton defined by the transition table given by θ and with output map s_0 and $s_1 \longleftarrow 0$, and s_2 and $s_3 \longleftarrow 1$. Remarkably

$$\max_{0\le\theta\le 1} \Big|\sum_{h=0}^{n-1}(-1)^{r_h}e^{ih\theta}\Big| \le (2+\sqrt{2})\sqrt{n}\,.$$

The Shapiro Sequence

Consider, the Shapiro sequence (r_h), which counts mod 2 the number of occurrences of the pair 11 of digits in the binary expansion of h.

$$
\begin{array}{l}
0001001000\ 0111010001\ 0010111000\ 1000010010\ 0001110111\ldots \\
0\ 1\ 0\ 2\ 0\quad 1\ 3\ 1\ 0\ 1\quad 0\ 2\ 3\ 2\ 0\quad 2\ 0\ 1\ 0\ 2\quad 0\ 1\ 3\ 1\ 3\ldots \\
0102013101\ 0232020102\ 0131323101\ 3101020131\ 0102320232\ldots \\
0001001000\ 0111010001\ 0010111000\ 1000010010\ 0001110111\ldots
\end{array}
$$

Here the blue sequence is the result of an ingenious pairing; the brown sequence then recognises that (r_h) is given by the regular binary substitution $\theta : 0 \mapsto 01\,,\ 1 \mapsto 02\,,\ 2 \mapsto 31\,,\ 3 \mapsto 32$.

The intermediate symbols $\{0, 1, 2, 3\}$ represent the four states $\{s_0, s_1, s_2, s_3\}$ of a binary automaton. So, the Shapiro sequence is generated by the automaton defined by the transition table given by θ and with output map s_0 and $s_1 \leftarrow 0$, and s_2 and $s_3 \leftarrow 1$. Remarkably

$$\max_{0\le\theta\le1} \Big|\sum_{h=0}^{n-1}(-1)^{r_h}e^{ih\theta}\Big| \le (2+\sqrt{2})\sqrt{n}\,.$$

The Shapiro Sequence

Consider, the Shapiro sequence (r_h), which counts mod 2 the number of occurrences of the pair 11 of digits in the binary expansion of h.

$$\begin{array}{l}
0001001000\ 0111010001\ 0010111000\ 1000010010\ 0001110111\ldots\\
0\ 1\ 0\ 2\ 0\quad 1\ 3\ 1\ 0\ 1\quad 0\ 2\ 3\ 2\ 0\quad 2\ 0\ 1\ 0\ 2\quad 0\ 1\ 3\ 1\ 3\ldots\\
0102013101\ 0232020102\ 0131323101\ 3101020131\ 0102320232\ldots\\
0001001000\ 0111010001\ 0010111000\ 1000010010\ 0001110111\ldots
\end{array}$$

Here the blue sequence is the result of an ingenious pairing; the brown sequence then recognises that (r_h) is given by the regular binary substitution $\theta : 0 \mapsto 01\,,\ 1 \mapsto 02\,,\ 2 \mapsto 31\,,\ 3 \mapsto 32$.

The intermediate symbols $\{0, 1, 2, 3\}$ represent the four states $\{s_0, s_1, s_2, s_3\}$ of a binary automaton. So, the Shapiro sequence is generated by the automaton defined by the transition table given by θ and with output map s_0 and $s_1 \leftarrow 0$, and s_2 and $s_3 \leftarrow 1$. Remarkably

$$\max_{0\le\theta\le1} \Big|\sum_{h=0}^{n-1}(-1)^{r_h}e^{ih\theta}\Big| \le (2+\sqrt{2})\sqrt{n}\,.$$

The Shapiro Sequence

Consider, the Shapiro sequence (r_h), which counts mod 2 the number of occurrences of the pair 11 of digits in the binary expansion of h.

0001001000 0111010001 0010111000 1000010010 0001110111 ...

0 1 0 2 0   1 3 1 0 1   0 2 3 2 0   2 0 1 0 2   0 1 3 1 3 ...

0102013101 0232020102 0131323101 3101020131 0102320232 ...

0001001000 0111010001 0010111000 1000010010 0001110111 ...

Here the blue sequence is the result of an ingenious pairing; the brown sequence then recognises that (r_h) is given by the regular binary substitution $\theta : 0 \mapsto 01\,, 1 \mapsto 02\,, 2 \mapsto 31\,, 3 \mapsto 32$.

The intermediate symbols $\{0, 1, 2, 3\}$ represent the four states $\{s_0, s_1, s_2, s_3\}$ of a binary automaton. So, the Shapiro sequence is generated by the automaton defined by the transition table given by θ and with output map s_0 and $s_1 \leftarrow 0$, and s_2 and $s_3 \leftarrow 1$. Remarkably

$$\max_{0 \le \theta \le 1} \Big| \sum_{h=0}^{n-1} (-1)^{r_h} e^{ih\theta} \Big| \le (2 + \sqrt{2})\sqrt{n}\,.$$

The Shapiro Sequence

Consider, the Shapiro sequence (r_h), which counts mod 2 the number of occurrences of the pair 11 of digits in the binary expansion of h.

$$0001001000\ 0111010001\ 0010111000\ 1000010010\ 0001110111\ldots$$

$$0\ 1\ 0\ 2\ 0\quad 1\ 3\ 1\ 0\ 1\quad 0\ 2\ 3\ 2\ 0\quad 2\ 0\ 1\ 0\ 2\quad 0\ 1\ 3\ 1\ 3\ldots$$

$$0102013101\ 0232020102\ 0131323101\ 3101020131\ 0102320232\ldots$$

$$0001001000\ 0111010001\ 0010111000\ 1000010010\ 0001110111\ldots$$

Here the blue sequence is the result of an ingenious pairing; the brown sequence then recognises that (r_h) is given by the regular binary substitution $\theta : 0 \mapsto 01\,,\ 1 \mapsto 02\,,\ 2 \mapsto 31\,,\ 3 \mapsto 32$.

The intermediate symbols $\{0, 1, 2, 3\}$ represent the four states $\{s_0, s_1, s_2, s_3\}$ of a binary automaton. So, the Shapiro sequence is generated by the automaton defined by the transition table given by θ and with output map s_0 and $s_1 \leftarrow 0$, and s_2 and $s_3 \leftarrow 1$. Remarkably

$$\max_{0\le\theta\le1} \Big|\sum_{h=0}^{n-1}(-1)^{r_h}e^{ih\theta}\Big| \le (2+\sqrt{2})\sqrt{n}\,.$$

A Remark on the Shapiro Function

Separating the even and odd placed elements of (r_h), we see that

This same/different rule makes it surprisingly easy to write the sequence from scratch. The second row is (r_{2h}). Remarkably, it coincides with the original sequence, illustrating that $r_h = r_{2h}$. The third row is (r_{2h+1}). With careful attention, we see that $r_{4h} = r_{4h+1}$ but $r_{4h+2} \neq r_{4h+3}$. Setting $P(X) = \sum (-1)^{r_h} X^h$, these observations amount to the functional equation

$$P(X) = P(X^2) + XP(-X^2).$$

By an earlier exercise, and some pain, the function $R(X) = \sum r_h X^h$ satisfies the functional equation

$$2X(1-X^4)R(X^4) + (1-X^4)(1-X)R(X^2) - (1-X^4)R(X) + X^3 = 0.$$

Does the algebraic equation over $\mathbb{F}_2(X)$ already define the function?

A Remark on the Shapiro Function

Separating the even and odd placed elements of (r_h), we see that

This same/different rule makes it surprisingly easy to write the sequence from scratch. The second row is (r_{2h}). Remarkably, it coincides with the original sequence, illustrating that $r_h = r_{2h}$. The third row is (r_{2h+1}). With careful attention, we see that $r_{4h} = r_{4h+1}$ but $r_{4h+2} \neq r_{4h+3}$. Setting $P(X) = \sum (-1)^{r_h} X^h$, these observations amount to the functional equation

$$P(X) = P(X^2) + XP(-X^2).$$

By an earlier exercise, and some pain, the function $R(X) = \sum r_h X^h$ satisfies the functional equation

$$2X(1-X^4)R(X^4) + (1-X^4)(1-X)R(X^2) - (1-X^4)R(X) + X^3 = 0.$$

Does the algebraic equation over $\mathbb{F}_2(X)$ already define the function?

A Remark on the Shapiro Function

Separating the even and odd placed elements of (r_h), we see that

$$0\ 0\ 0\ 1\ 0\quad 0\ 1\ 0\ 0\ 0\quad 0\ 1\ 1\ 1\ 0\quad 1\ 0\ 0\ 0\ 1\quad 0\ 0\ 1\ 0\ 1\quad \ldots$$

This same/different rule makes it surprisingly easy to write the sequence from scratch. The second row is (r_{2h}). Remarkably, it coincides with the original sequence, illustrating that $r_h = r_{2h}$. The third row is (r_{2h+1}). With careful attention, we see that $r_{4h} = r_{4h+1}$ but $r_{4h+2} \neq r_{4h+3}$. Setting $P(X) = \sum (-1)^{r_h} X^h$, these observations amount to the functional equation

$$P(X) = P(X^2) + XP(-X^2)\,.$$

By an earlier exercise, and some pain, the function $R(X) = \sum r_h X^h$ satisfies the functional equation

$$2X(1-X^4)R(X^4) + (1-X^4)(1-X)R(X^2) - (1-X^4)R(X) + X^3 = 0\,.$$

Does the algebraic equation over $\mathbb{F}_2(X)$ already define the function?

A Remark on the Shapiro Function

Separating the even and odd placed elements of (r_h), we see that

$$
\begin{array}{ccccccccccccccccccccccccccccccccccccccccccccccccccc}
0 & & 0 & & 0 & & 1 & & 0 & & 0 & & 1 & & 0 & & 0 & & 0 & & 0 & & 1 & & 1 & & 1 & & 0 & & 1 & & 0 & & 0 & & 0 & & 1 & & 0 & & 0 & & 1 & & 0 & & 1 & & \dots \\
& 0 & & 1 & & 0 & & 0 & & 0 & & 1 & & 1 & & 1 & & 0 & & 1 & & 0 & & 0 & & 1 & & 0 & & 0 & & 0 & & 0 & & 1 & & 0 & & 0 & & 0 & & 1 & & 1 & & 1 & & 1 & \dots
\end{array}
$$

This same/different rule makes it surprisingly easy to write the sequence from scratch. The second row is (r_{2h}). Remarkably, it coincides with the original sequence, illustrating that $r_h = r_{2h}$. The third row is (r_{2h+1}). With careful attention, we see that $r_{4h} = r_{4h+1}$ but $r_{4h+2} \neq r_{4h+3}$. Setting $P(X) = \sum (-1)^{r_h} X^h$, these observations amount to the functional equation

$$P(X) = P(X^2) + XP(-X^2)\,.$$

By an earlier exercise, and some pain, the function $R(X) = \sum r_h X^h$ satisfies the functional equation

$$2X(1-X^4)R(X^4) + (1-X^4)(1-X)R(X^2) - (1-X^4)R(X) + X^3 = 0\,.$$

Does the algebraic equation over $\mathbb{F}_2(X)$ already define the function?

A Remark on the Shapiro Function

Separating the even and odd placed elements of (r_h), we see that

$$0001001000\ 0111010001\ 0010111000\ 1000010010\ 0001110111\ \ldots$$

$$\begin{array}{l} 0\,0\,0\,1\,0\quad 0\,1\,0\,0\,0\quad 0\,1\,1\,1\,0\quad 1\,0\,0\,0\,1\quad 0\,0\,1\,0\,1\ \ldots \\ 0\,1\,0\,0\,0\quad 1\,1\,1\,0\,1\quad 0\,0\,1\,0\,0\quad 0\,0\,1\,0\,0\quad 0\,1\,1\,1\,1\ \ldots \end{array}$$

This same/different rule makes it surprisingly easy to write the sequence from scratch. The second row is (r_{2h}) . Remarkably, it coincides with the original sequence, illustrating that $r_h = r_{2h}$. The third row is (r_{2h+1}) . With careful attention, we see that $r_{4h} = r_{4h+1}$ but $r_{4h+2} \neq r_{4h+3}$. Setting $P(X) = \sum (-1)^{r_h} X^h$, these observations amount to the functional equation

$$P(X) = P(X^2) + XP(-X^2)\,.$$

By an earlier exercise, and some pain, the function $R(X) = \sum r_h X^h$ satisfies the functional equation

$$2X(1-X^4)R(X^4) + (1-X^4)(1-X)R(X^2) - (1-X^4)R(X) + X^3 = 0\,.$$

Does the algebraic equation over $\mathbb{F}_2(X)$ already define the function?

A Remark on the Shapiro Function

Separating the even and odd placed elements of (r_h), we see that

$$0001001000\ 0111010001\ 0010111000\ 1000010010\ 0001110111\ \dots$$

$$\begin{array}{l} 0\,0\,0\,1\,0\;\; 0\,1\,0\,0\,0\;\; 0\,1\,1\,1\,0\;\; 1\,0\,0\,0\,1\;\; 0\,0\,1\,0\,1\;\dots \\ \;0\,1\,0\,0\,0\;\; 1\,1\,1\,0\,1\;\; 0\,0\,1\,0\,0\;\; 0\,0\,1\,0\,0\;\; 0\,1\,1\,1\,1\;\dots \end{array}$$

This same/different rule makes it surprisingly easy to write the sequence from scratch. The second row is (r_{2h}). Remarkably, it coincides with the original sequence, illustrating that $r_h = r_{2h}$. The third row is (r_{2h+1}). With careful attention, we see that $r_{4h} = r_{4h+1}$ but $r_{4h+2} \neq r_{4h+3}$. Setting $P(X) = \sum (-1)^{r_h} X^h$, these observations amount to the functional equation

$$P(X) = P(X^2) + XP(-X^2)\,.$$

By an earlier exercise, and some pain, the function $R(X) = \sum r_h X^h$ satisfies the functional equation

$$2X(1-X^4)R(X^4) + (1-X^4)(1-X)R(X^2) - (1-X^4)R(X) + X^3 = 0\,.$$

Does the algebraic equation over $\mathbb{F}_2(X)$ already define the function?

A Remark on the Shapiro Function

Separating the even and odd placed elements of (r_h), we see that

0001001000 0111010001 0010111000 1000010010 0001110111 ...

0 0 0 1 0   0 1 0 0 0   0 1 1 1 0   1 0 0 0 1   0 0 1 0 1 ...

0 1 0 0 0   1 1 1 0 1   0 0 1 0 0   0 0 1 0 0   0 1 1 1 1 ...

This same/different rule makes it surprisingly easy to write the sequence from scratch. The second row is (r_{2h}) . Remarkably, it coincides with the original sequence, illustrating that $r_h = r_{2h}$. The third row is (r_{2h+1}) . With careful attention, we see that $r_{4h} = r_{4h+1}$ but $r_{4h+2} \neq r_{4h+3}$. Setting $P(X) = \sum (-1)^{r_h} X^h$, these observations amount to the functional equation

$$P(X) = P(X^2) + XP(-X^2)\,.$$

By an earlier exercise, and some pain, the function $R(X) = \sum r_h X^h$ satisfies the functional equation

$$2X(1 - X^4)R(X^4) + (1 - X^4)(1 - X)R(X^2) - (1 - X^4)R(X) + X^3 = 0\,.$$

Does the algebraic equation over $\mathbb{F}_2(X)$ already define the function?

A Remark on the Shapiro Function

Separating the even and odd placed elements of (r_h), we see that

$$0001001000\ 0111010001\ 0010111000\ 1000010010\ 0001110111\ \ldots$$

$$\begin{array}{l} 0\ 0\ 0\ 1\ 0\quad 0\ 1\ 0\ 0\ 0\quad 0\ 1\ 1\ 1\ 0\quad 1\ 0\ 0\ 0\ 1\quad 0\ 0\ 1\ 0\ 1\ \ldots \\ \ 0\ 1\ 0\ 0\ 0\quad 1\ 1\ 1\ 0\ 1\quad 0\ 0\ 1\ 0\ 0\quad 0\ 0\ 1\ 0\ 0\quad 0\ 1\ 1\ 1\ 1\ \ldots \end{array}$$

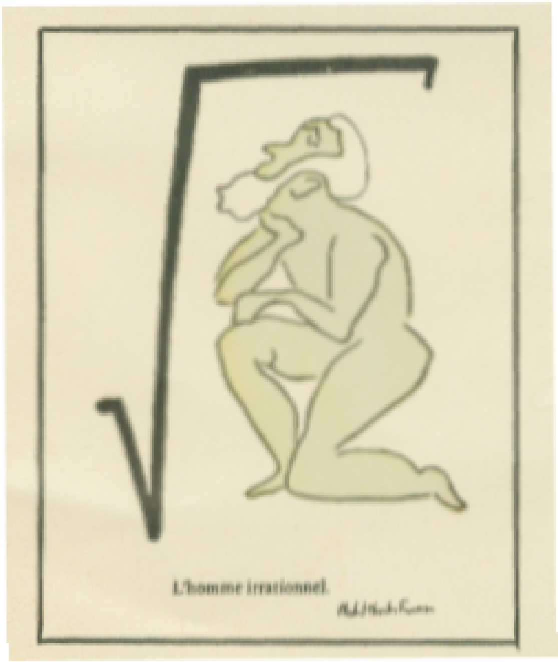
This same/different rule makes it surprisingly easy to write the sequence from scratch. The second row is (r_{2h}) . Remarkably, it coincides with the original sequence, illustrating that $r_h = r_{2h}$. The third row is (r_{2h+1}) . With careful attention, we see that $r_{4h} = r_{4h+1}$ but $r_{4h+2} \neq r_{4h+3}$. Setting $P(X) = \sum (-1)^{r_h} X^h$, these observations amount to the functional equation

$$P(X) = P(X^2) + XP(-X^2)\,.$$

By an earlier exercise, and some pain, the function $R(X) = \sum r_h X^h$ satisfies the functional equation

$$2X(1-X^4)R(X^4) + (1-X^4)(1-X)R(X^2) - (1-X^4)R(X) + X^3 = 0\,.$$

Does the algebraic equation over $\mathbb{F}_2(X)$ already define the function?


L'homme irrationnel

Transcendence of Automatic Numbers

In the eighties, John Loxton and I proved transcendence results on values of Mahler functions giving strong support for the belief that the decimal expansion (more generally the base b expansion) of an irrational algebraic number cannot be generated by a finite automaton.

For instance, it is a theorem that in any base b the paperfolding number $0.1101100111001001110110001 10\ldots$ is transcendental.

In consequence the matter of the transcendence of irrational automatic numbers became known in the trade as the conjecture of Loxton and van der Poorten.

But our results did not cover all cases and had significant exceptions skew to the motivating problem and plainly caused by technical difficulties inherent in our methods.

Fortunately, a much more appropriate argument has now been found by Boris Adamczewski and Yann Bugeaud (Strassbourg).

Transcendence of Automatic Numbers

In the eighties, John Loxton and I proved transcendence results on values of Mahler functions giving strong support for the belief that the decimal expansion (more generally the base b expansion) of an irrational algebraic number cannot be generated by a finite automaton.

For instance, it is a theorem that in any base b the paperfolding number $0.11011001110010011101100011 0\ldots$ is transcendental.

In consequence the matter of the transcendence of irrational automatic numbers became known in the trade as the conjecture of Loxton and van der Poorten.

But our results did not cover all cases and had significant exceptions skew to the motivating problem and plainly caused by technical difficulties inherent in our methods.

Fortunately, a much more appropriate argument has now been found by Boris Adamczewski and Yann Bugeaud (Strassbourg).

Transcendence of Automatic Numbers

In the eighties, John Loxton and I proved transcendence results on values of Mahler functions giving strong support for the belief that the decimal expansion (more generally the base b expansion) of an irrational algebraic number cannot be generated by a finite automaton.

For instance, it is a theorem that in any base b the paperfolding number $0.1101100111001001110110001100\ldots$ is transcendental.

In consequence the matter of the transcendence of irrational automatic numbers became known in the trade as the conjecture of Loxton and van der Poorten.

But our results did not cover all cases and had significant exceptions skew to the motivating problem and plainly caused by technical difficulties inherent in our methods.

Fortunately, a much more appropriate argument has now been found by Boris Adamczewski and Yann Bugeaud (Strassbourg).

Transcendence of Automatic Numbers

In the eighties, John Loxton and I proved transcendence results on values of Mahler functions giving strong support for the belief that the decimal expansion (more generally the base b expansion) of an irrational algebraic number cannot be generated by a finite automaton.

For instance, it is a theorem that in any base b the paperfolding number $0.11011001110010011101100011 0\ldots$ is transcendental.

In consequence the matter of the transcendence of irrational automatic numbers became known in the trade as the conjecture of Loxton and van der Poorten.

But our results did not cover all cases and had significant exceptions skew to the motivating problem and plainly caused by technical difficulties inherent in our methods.

Fortunately, a much more appropriate argument has now been found by Boris Adamczewski and Yann Bugeaud (Strassbourg).

Transcendence of Automatic Numbers

In the eighties, John Loxton and I proved transcendence results on values of Mahler functions giving strong support for the belief that the decimal expansion (more generally the base b expansion) of an irrational algebraic number cannot be generated by a finite automaton.

For instance, it is a theorem that in any base b the paperfolding number $0.11011001110010011101100011 0\ldots$ is transcendental.

In consequence the matter of the transcendence of irrational automatic numbers became known in the trade as the conjecture of Loxton and van der Poorten.

But our results did not cover all cases and had significant exceptions skew to the motivating problem and plainly caused by technical difficulties inherent in our methods.

Fortunately, a much more appropriate argument has now been found by Boris Adamczewski and Yann Bugeaud (Strassbourg).

Transcendence of Automatic Numbers

In the eighties, John Loxton and I proved transcendence results on values of Mahler functions giving strong support for the belief that the decimal expansion (more generally the base b expansion) of an irrational algebraic number cannot be generated by a finite automaton.

For instance, it is a theorem that in any base b the paperfolding number $0.11011001110010011101100011 0\ldots$ is transcendental.

In consequence the matter of the transcendence of irrational automatic numbers became known in the trade as the conjecture of Loxton and van der Poorten.

But our results did not cover all cases and had significant exceptions skew to the motivating problem and plainly caused by technical difficulties inherent in our methods.

Fortunately, a much more appropriate argument has now been found by Boris Adamczewski and Yann Bugeaud (Strassbourg).

Complexity of a Sequence

Given an infinite string, denote by $p(n)$ the number of its distinct subwords of length n. Almost all numbers (in base b) have $p(n) = b^n$; but sequences generated by a finite automaton have only a miserable complexity $p(n) = O(n)$.

Not all that long ago, BORIS ADAMCZEWSKI, YANN BUGEAUD, AND FLORIAN LUCA, 'Sur la complexité des nombres algébriques', *C. R. Acad. Sci. Paris, Ser. I* **336** (2004), applied Schlickewei's p-adic generalisation of Wolfgang Schmidt's subspace theorem (which is itself a multidimensional generalisation of Roth's theorem) to proving that for the base b expansion of an irrational algebraic number

$$\liminf_{n\to\infty} p(n)/n = +\infty.$$

A more detailed paper usefully generalising the earlier announcement: 'On the complexity of algebraic numbers', by BORIS ADAMCZEWSKI AND YANN BUGEAUD, has now appeared in *Annals of Math.*

Complexity of a Sequence

Given an infinite string, denote by $p(n)$ the number of its distinct subwords of length n. Almost all numbers (in base b) have $p(n) = b^n$; but sequences generated by a finite automaton have only a miserable complexity $p(n) = O(n)$.

Not all that long ago, Boris Adamczewski, Yann Bugeaud, and Florian Luca, 'Sur la complexité des nombres algébriques', *C. R. Acad. Sci. Paris, Ser. I* **336** (2004), applied Schlickewei's p-adic generalisation of Wolfgang Schmidt's subspace theorem (which is itself a multidimensional generalisation of Roth's theorem) to proving that for the base b expansion of an irrational algebraic number

$$\liminf_{n\to\infty} p(n)/n = +\infty.$$

A more detailed paper usefully generalising the earlier announcement: 'On the complexity of algebraic numbers', by Boris Adamczewski and Yann Bugeaud, has now appeared in *Annals of Math.*

Complexity of a Sequence

Given an infinite string, denote by $p(n)$ the number of its distinct subwords of length n. Almost all numbers (in base b) have $p(n) = b^n$; but sequences generated by a finite automaton have only a miserable complexity $p(n) = O(n)$.

Not all that long ago, Boris Adamczewski, Yann Bugeaud, and Florian Luca, 'Sur la complexité des nombres algébriques', *C. R. Acad. Sci. Paris, Ser. I* **336** (2004), applied Schlickewei's p-adic generalisation of Wolfgang Schmidt's subspace theorem (which is itself a multidimensional generalisation of Roth's theorem) to proving that for the base b expansion of an irrational algebraic number

$$\liminf_{n\to\infty} p(n)/n = +\infty.$$

A more detailed paper usefully generalising the earlier announcement: 'On the complexity of algebraic numbers', by Boris Adamczewski and Yann Bugeaud, has now appeared in *Annals of Math.*

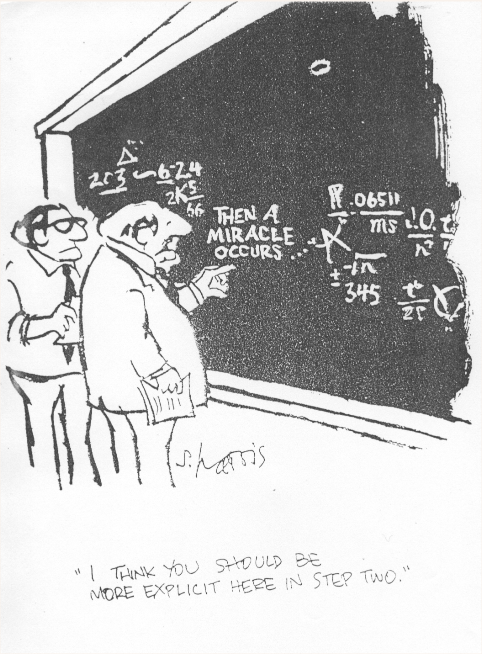
Complexity of a Sequence

Given an infinite string, denote by $p(n)$ the number of its distinct subwords of length n. Almost all numbers (in base b) have $p(n) = b^n$; but sequences generated by a finite automaton have only a miserable complexity $p(n) = O(n)$.

Not all that long ago, BORIS ADAMCZEWSKI, YANN BUGEAUD, AND FLORIAN LUCA, 'Sur la complexité des nombres algébriques', *C. R. Acad. Sci. Paris, Ser. I* **336** (2004), applied Schlickewei's p-adic generalisation of Wolfgang Schmidt's subspace theorem (which is itself a multidimensional generalisation of Roth's theorem) to proving that for the base b expansion of an irrational algebraic number

$$\liminf_{n\to\infty} p(n)/n = +\infty.$$

A more detailed paper usefully generalising the earlier announcement: 'On the complexity of algebraic numbers', by BORIS ADAMCZEWSKI AND YANN BUGEAUD, has now appeared in *Annals of Math.*


THEN A
MIRACLE
OCCURS...
"I THINK YOU SHOULD BE
MORE EXPLICIT HERE IN STEP TWO."

Algebraicity and Automaticity

The phenomena we have just now noticed

1. automaticity
2. in characteristic p
3.
4.

are equivalent.

It is a theorem of Gilles Christol, Teturo Kamae, Michel Mendès France, and Gérard Rauzy that the Taylor coefficients of a power series defined over a finite field of characteristic p provide a p-automatic sequence if and only if the power series represents an algebraic function.

Remarks of Loxton and mine add the identification with Mahler functions in characteristic zero.

Algebraicity and Automaticity

The phenomena we have just now noticed

1. automaticity
2. algebraicity in characteristic p
3.

are equivalent.

It is a theorem of Gilles Christol, Teturo Kamae, Michel Mendès France, and Gérard Rauzy that the Taylor coefficients of a power series defined over a finite field of characteristic p provide a p-automatic sequence if and only if the power series represents an algebraic function.

Remarks of Loxton and mine add the identification with Mahler functions in characteristic zero.

Algebraicity and Automaticity

The phenomena we have just now noticed

1. automaticity
2. algebraicity in characteristic p
3. Mahler functional equation
4. regular p-substitutions

are equivalent.

It is a theorem of Gilles Christol, Teturo Kamae, Michel Mendès France, and Gérard Rauzy that the Taylor coefficients of a power series defined over a finite field of characteristic p provide a p-automatic sequence if and only if the power series represents an algebraic function.

Remarks of Loxton and mine add the identification with Mahler functions in characteristic zero.

Algebraicity and Automaticity

The phenomena we have just now noticed

1. automaticity
2. algebraicity in characteristic p
3. Mahler functional equation
4. regular p-substitutions

are equivalent.

It is a theorem of Gilles Christol, Teturo Kamae, Michel Mendès France, and Gérard Rauzy that the Taylor coefficients of a power series defined over a finite field of characteristic p provide a p-automatic sequence if and only if the power series represents an algebraic function.

Remarks of Loxton and mine add the identification with Mahler functions in characteristic zero.

Algebraicity and Automaticity

The phenomena we have just now noticed

1. automaticity
2. algebraicity in characteristic p
3. Mahler functional equation
4. regular p-substitutions

are equivalent.

It is a theorem of Giles Christol, Teturo Kamae, Michel Mendès France, and Gérard Rauzy that the Taylor coefficients of a power series defined over a finite field of characteristic p provide a p-automatic sequence if and only if the power series represents an algebraic function.

Remarks of Loxton and mine add the identification with Mahler functions in characteristic zero.

Algebraicity and Automaticity

The phenomena we have just now noticed

1. automaticity
2. algebraicity in characteristic p
3. Mahler functional equation
4. regular p-substitutions

are equivalent.

It is a theorem of Giles Christol, Teturo Kamae, Michel Mendès France, and Gérard Rauzy that the Taylor coefficients of a power series defined over a finite field of characteristic p provide a p-automatic sequence if and only if the power series represents an algebraic function.

Remarks of Loxton and mine add the identification with Mahler functions in characteristic zero.

Algebraicity and Automaticity

The phenomena we have just now noticed

1. automaticity
2. algebraicity in characteristic p
3. Mahler functional equation
4. regular p-substitutions

are equivalent.

It is a theorem of Giles Christol, Teturo Kamae, Michel Mendès France, and Gérard Rauzy that the Taylor coefficients of a power series defined over a finite field of characteristic p provide a p-automatic sequence if and only if the power series represents an algebraic function.

Remarks of Loxton and mine add the identification with Mahler functions in characteristic zero.

Algebraicity and Automaticity

The phenomena we have just now noticed

1. automaticity
2. algebraicity in characteristic p
3. Mahler functional equation
4. regular p-substitutions

are equivalent.

It is a theorem of Giles Christol, Teturo Kamae, Michel Mendès France, and Gérard Rauzy that the Taylor coefficients of a power series defined over a finite field of characteristic p provide a p-automatic sequence if and only if the power series represents an algebraic function.

Remarks of Loxton and mine add the identification with Mahler functions in characteristic zero.

Algebraicity and Automaticity

The phenomena we have just now noticed

1. automaticity
2. algebraicity in characteristic p
3. Mahler functional equation
4. regular p-substitutions

are equivalent.

It is a theorem of Giles Christol, Teturo Kamae, Michel Mendès France, and Gérard Rauzy that the Taylor coefficients of a power series defined over a finite field of characteristic p provide a p-automatic sequence if and only if the power series represents an algebraic function.

Remarks of Loxton and mine add the identification with Mahler functions in characteristic zero.

Comments on the Proof

The best proof (in my opinion) is due to Jan Denef and Leonard Lipshitz and relies on studying formal power series in many variables with coefficients from a finite field, say $\mathbb{F}_p$.

Given polynomials P and Q in just two variable x and y, and with $Q(0,0) \neq 0$, suppose one were forced to look at the series expansion

$$P(x,y)/Q(x,y) = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} a_{nm} x^n y^m.$$

It is arguably natural to recoil in fright and to insist on following a suggestion of Furstenberg to study just its diagonal $\sum_{n=0}^{\infty} a_{nn} x^n$.

It turns out to be not hard to prove that the complete diagonal of a rational function in two variables always is an algebraic function.

Comments on the Proof

The best proof (in my opinion) is due to Jan Denef and Leonard Lipshitz and relies on studying formal power series in many variables with coefficients from a finite field, say $\mathbb{F}_p$.

Given polynomials P and Q in just two variable x and y, and with $Q(0,0) \neq 0$, suppose one were forced to look at the series expansion

$$P(x,y)/Q(x,y) = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} a_{nm} x^n y^m.$$

It is arguably natural to recoil in fright and to insist on following a suggestion of Furstenberg to study just its diagonal $\sum_{n=0}^{\infty} a_{nn} x^n$.

It turns out to be not hard to prove that the complete diagonal of a rational function in two variables always is an algebraic function.

Comments on the Proof

The best proof (in my opinion) is due to Jan Denef and Leonard Lipshitz and relies on studying formal power series in many variables with coefficients from a finite field, say $\mathbb{F}_p$.

Given polynomials P and Q in just two variable x and y, and with $Q(0,0) \neq 0$, suppose one were forced to look at the series expansion

$$P(x,y)/Q(x,y) = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} a_{nm} x^n y^m.$$

It is arguably natural to recoil in fright and to insist on following a suggestion of Furstenberg to study just its diagonal $\sum_{n=0}^{\infty} a_{nn} x^n$.

It turns out to be not hard to prove that the complete diagonal of a rational function in two variables always is an algebraic function.

Comments on the Proof

The best proof (in my opinion) is due to Jan Denef and Leonard Lipshitz and relies on studying formal power series in many variables with coefficients from a finite field, say $\mathbb{F}_p$.

Given polynomials P and Q in just two variable x and y, and with $Q(0,0) \neq 0$, suppose one were forced to look at the series expansion

$$P(x,y)/Q(x,y) = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} a_{nm} x^n y^m.$$

It is arguably natural to recoil in fright and to insist on following a suggestion of Furstenberg to study just its diagonal $\sum_{n=0}^{\infty} a_{nn} x^n$.

It turns out to be not hard to prove that the complete diagonal of a rational function in two variables always is an algebraic function.

Comments on the Proof

The best proof (in my opinion) is due to Jan Denef and Leonard Lipshitz and relies on studying formal power series in many variables with coefficients from a finite field, say $\mathbb{F}_p$.

Given polynomials P and Q in just two variable x and y, and with $Q(0,0) \neq 0$, suppose one were forced to look at the series expansion

$$P(x,y)/Q(x,y) = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} a_{nm} x^n y^m.$$

It is arguably natural to recoil in fright and to insist on following a suggestion of Furstenberg to study just its diagonal $\sum_{n=0}^{\infty} a_{nn} x^n$.

It turns out to be not hard to prove that the complete diagonal of a rational function in two variables always is an algebraic function.

But for expansions over the complex numbers $\mathbb{C}$, the complete diagonal of a power series of a rational function in more than two variables is in general not algebraic.

It is a beautiful fact that it is, however, a G-function, a power series inter alia satisfying a linear differential equation with polynomial coefficients.

However, for expansions over a finite field, say $\mathbb{F}_p$, diagonals of a rational function always are algebraic. Conversely, every algebraic power series in n variables is a diagonal of a rational function in at most $2n$ variables.

More, the Taylor coefficients of such an algebraic power series are readily shown to satisfy congruence conditions which amount to the sequence plainly being generated by a p-automaton. I might remark that those congruences also were noticed independently by Pierre Deligne, some years after the CKMR proof. Indeed, Denef and Lipshitz tell me they developed their arguments after giving up on trying to understand Deligne's proof.

But for expansions over the complex numbers $\mathbb{C}$, the complete diagonal of a power series of a rational function in more than two variables is in general not algebraic.

It is a beautiful fact that it is, however, a G-function, a power series inter alia satisfying a linear differential equation with polynomial coefficients.

However, for expansions over a finite field, say $\mathbb{F}_p$, diagonals of a rational function always are algebraic. Conversely, every algebraic power series in n variables is a diagonal of a rational function in at most $2n$ variables.

More, the Taylor coefficients of such an algebraic power series are readily shown to satisfy congruence conditions which amount to the sequence plainly being generated by a p-automaton. I might remark that those congruences also were noticed independently by Pierre Deligne, some years after the CKMR proof. Indeed, Denef and Lipshitz tell me they developed their arguments after giving up on trying to understand Deligne's proof.

But for expansions over the complex numbers $\mathbb{C}$, the complete diagonal of a power series of a rational function in more than two variables is in general not algebraic.

It is a beautiful fact that it is, however, a G-function, a power series inter alia satisfying a linear differential equation with polynomial coefficients.

However, for expansions over a finite field, say $\mathbb{F}_p$, diagonals of a rational function always are algebraic. Conversely, every algebraic power series in n variables is a diagonal of a rational function in at most $2n$ variables.

More, the Taylor coefficients of such an algebraic power series are readily shown to satisfy congruence conditions which amount to the sequence plainly being generated by a p-automaton. I might remark that those congruences also were noticed independently by Pierre Deligne, some years after the CKMR proof. Indeed, Denef and Lipshitz tell me they developed their arguments after giving up on trying to understand Deligne's proof.

But for expansions over the complex numbers $\mathbb{C}$, the complete diagonal of a power series of a rational function in more than two variables is in general not algebraic.

It is a beautiful fact that it is, however, a G-function, a power series inter alia satisfying a linear differential equation with polynomial coefficients.

However, for expansions over a finite field, say $\mathbb{F}_p$, diagonals of a rational function always are algebraic. Conversely, every algebraic power series in n variables is a diagonal of a rational function in at most $2n$ variables.

More, the Taylor coefficients of such an algebraic power series are readily shown to satisfy congruence conditions which amount to the sequence plainly being generated by a p-automaton. I might remark that those congruences also were noticed independently by Pierre Deligne, some years after the CKMR proof. Indeed, Denef and Lipshitz tell me they developed their arguments after giving up on trying to understand Deligne's proof.

But for expansions over the complex numbers $\mathbb{C}$, the complete diagonal of a power series of a rational function in more than two variables is in general not algebraic.

It is a beautiful fact that it is, however, a G-function, a power series inter alia satisfying a linear differential equation with polynomial coefficients.

However, for expansions over a finite field, say $\mathbb{F}_p$, diagonals of a rational function always are algebraic. Conversely, every algebraic power series in n variables is a diagonal of a rational function in at most $2n$ variables.

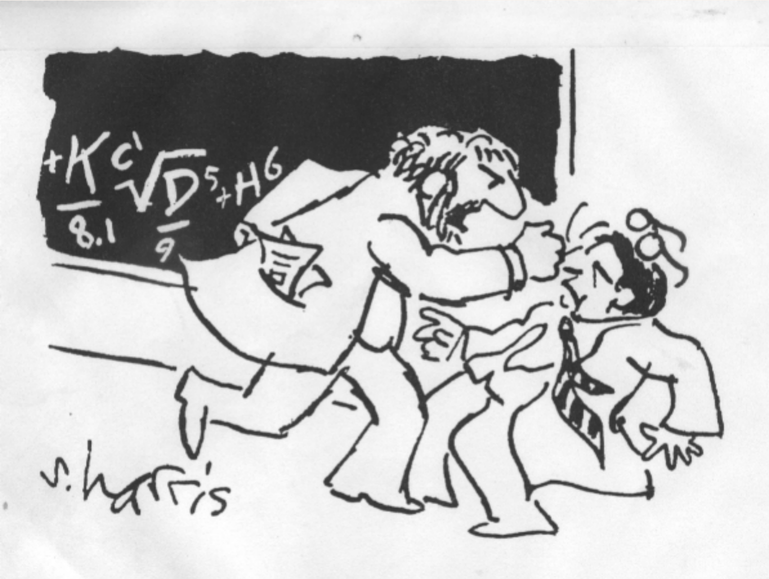
More, the Taylor coefficients of such an algebraic power series are readily shown to satisfy congruence conditions which amount to the sequence plainly being generated by a p-automaton. I might remark that those congruences also were noticed independently by Pierre Deligne, some years after the CKMR proof. Indeed, Denef and Lipshitz tell me they developed their arguments after giving up on trying to understand Deligne's proof.

But for expansions over the complex numbers $\mathbb{C}$, the complete diagonal of a power series of a rational function in more than two variables is in general not algebraic.

It is a beautiful fact that it is, however, a G-function, a power series inter alia satisfying a linear differential equation with polynomial coefficients.

However, for expansions over a finite field, say $\mathbb{F}_p$, diagonals of a rational function always are algebraic. Conversely, every algebraic power series in n variables is a diagonal of a rational function in at most $2n$ variables.

More, the Taylor coefficients of such an algebraic power series are readily shown to satisfy congruence conditions which amount to the sequence plainly being generated by a p-automaton. I might remark that those congruences also were noticed independently by Pierre Deligne, some years after the CKMR proof. Indeed, Denef and Lipshitz tell me they developed their arguments after giving up on trying to understand Deligne's proof.



"You want proof? I'll give you proof!"

Power Series in Several Variables

$R[[x]]$ is the ring of formal power series in $x = (x_1, \ldots, x_n)$.

I write a series $f(x) \in R[[x]]$ as $f(x) = \sum a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n} = \sum a_\nu x^\nu$ where $\nu = (\nu_1, \ldots, \nu_n)$ is a multi-index and $x^\nu = x_1^{\nu_1} \cdots x_n^{\nu_n}$.

Below, R is usually the finite field $\mathbb{F}_p$ of p elements or the ring of p-adic integers $\mathbb{Z}_p$.

One says that $f(x) \in R[[x]]$ is *algebraic* if it is algebraic over the quotient field of the polynomial ring $R[x]$. I say that $f(x) \in \mathbb{Z}_p[[x]]$ is *algebraic* mod p^s if there is an algebraic $g(x) \in \mathbb{Z}_p[[x]]$ with $f \equiv g$ mod p^s.

Given $f(x, y) = \sum a_{ij} x^i y^j$ it is natural to refer to the series $I_{xy} f = \sum a_{ii} x^i$ as its *diagonal*.

Given $f(x) = \sum a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}$ we define its diagonal $I_{12} f$ by $I_{12} f = \sum a_{i_1 i_1 i_3 \cdots i_n} x_1^{i_1} x_3^{i_3} \cdots x_n^{i_n}$; generally, for $k \neq l$, the other I_{kl} are defined correspondingly. By a diagonal we mean any composition of the I_{kl} s. The complete diagonal is $If = \sum a_{ii \cdots i} x_1^i$.

Power Series in Several Variables

$R[[x]]$ is the ring of formal power series in $x = (x_1, \dots, x_n)$.

I write a series $f(x) \in R[[x]]$ as $f(x) = \sum a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n} = \sum a_\nu x^\nu$ where $\nu = (\nu_1, \dots, \nu_n)$ is a multi-index and $x^\nu = x_1^{\nu_1} \cdots x_n^{\nu_n}$.

Below, R is usually the finite field $\mathbb{F}_p$ of p elements or the ring of p-adic integers $\mathbb{Z}_p$.

One says that $f(x) \in R[[x]]$ is *algebraic* if it is algebraic over the quotient field of the polynomial ring $R[x]$. I say that $f(x) \in \mathbb{Z}_p[[x]]$ is *algebraic* mod p^s if there is an algebraic $g(x) \in \mathbb{Z}_p[[x]]$ with $f \equiv g$ mod p^s.

Given $f(x, y) = \sum a_{ij} x^i y^j$ it is natural to refer to the series $I_{xy} f = \sum a_{ii} x^i$ as its *diagonal*.

Given $f(x) = \sum a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}$ we define its diagonal $I_{12} f$ by $I_{12} f = \sum a_{i_1 i_1 i_3 \cdots i_n} x_1^{i_1} x_3^{i_3} \cdots x_n^{i_n}$; generally, for $k \neq l$, the other I_{kl} are defined correspondingly. By a diagonal we mean any composition of the I_{kl} s. The complete diagonal is $If = \sum a_{ii \cdots i} x_1^i$.

Power Series in Several Variables

$R[[x]]$ is the ring of formal power series in $x = (x_1, \dots, x_n)$.

I write a series $f(x) \in R[[x]]$ as $f(x) = \sum a_{i_1 \dots i_n} x_1^{i_1} \cdots x_n^{i_n} = \sum a_\nu x^\nu$ where $\nu = (\nu_1, \dots, \nu_n)$ is a multi-index and $x^\nu = x_1^{\nu_1} \cdots x_n^{\nu_n}$.

Below, R is usually the finite field $\mathbb{F}_p$ of p elements or the ring of p-adic integers $\mathbb{Z}_p$.

One says that $f(x) \in R[[x]]$ is *algebraic* if it is algebraic over the quotient field of the polynomial ring $R[x]$. I say that $f(x) \in \mathbb{Z}_p[[x]]$ is *algebraic* mod p^s if there is an algebraic $g(x) \in \mathbb{Z}_p[[x]]$ with $f \equiv g$ mod p^s.

Given $f(x, y) = \sum a_{ij} x^i y^j$ it is natural to refer to the series $I_{xy} f = \sum a_{ii} x^i$ as its *diagonal*.

Given $f(x) = \sum a_{i_1 \dots i_n} x_1^{i_1} \cdots x_n^{i_n}$ we define its diagonal $I_{12} f$ by $I_{12} f = \sum a_{i_1 i_1 i_3 \dots i_n} x_1^{i_1} x_3^{i_3} \cdots x_n^{i_n}$; generally, for $k \neq l$, the other I_{kl} are defined correspondingly. By a diagonal we mean any composition of the I_{kl}s. The complete diagonal is $If = \sum a_{ii \dots i} x_1^i$.

Power Series in Several Variables

$R[[x]]$ is the ring of formal power series in $x = (x_1, \ldots, x_n)$.

I write a series $f(x) \in R[[x]]$ as $f(x) = \sum a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n} = \sum a_\nu x^\nu$ where $\nu = (\nu_1, \ldots, \nu_n)$ is a multi-index and $x^\nu = x_1^{\nu_1} \cdots x_n^{\nu_n}$.

Below, R is usually the finite field $\mathbb{F}_p$ of p elements or the ring of p-adic integers $\mathbb{Z}_p$.

One says that $f(x) \in R[[x]]$ is *algebraic* if it is algebraic over the quotient field of the polynomial ring $R[x]$. I say that $f(x) \in \mathbb{Z}_p[[x]]$ is *algebraic* mod p^s if there is an algebraic $g(x) \in \mathbb{Z}_p[[x]]$ with $f \equiv g$ mod p^s.

Given $f(x, y) = \sum a_{ij} x^i y^j$ it is natural to refer to the series $I_{xy} f = \sum a_{ii} x^i$ as its *diagonal*.

Given $f(x) = \sum a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}$ we define its diagonal $I_{12} f$ by

$I_{12} f = \sum a_{i_1 i_1 i_3 \cdots i_n} x_1^{i_1} x_3^{i_3} \cdots x_n^{i_n}$; generally, for $k \neq l$, the other I_{kl} are defined correspondingly. By a diagonal we mean any composition of the I_{kl} s. The complete diagonal is $If = \sum a_{ii \cdots i} x_1^i$.

Power Series in Several Variables

$R[[x]]$ is the ring of formal power series in $x = (x_1, \ldots, x_n)$.

I write a series $f(x) \in R[[x]]$ as $f(x) = \sum a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n} = \sum a_\nu x^\nu$ where $\nu = (\nu_1, \ldots, \nu_n)$ is a multi-index and $x^\nu = x_1^{\nu_1} \cdots x_n^{\nu_n}$.

Below, R is usually the finite field $\mathbb{F}_p$ of p elements or the ring of p-adic integers $\mathbb{Z}_p$.

One says that $f(x) \in R[[x]]$ is *algebraic* if it is algebraic over the quotient field of the polynomial ring $R[x]$. I say that $f(x) \in \mathbb{Z}_p[[x]]$ is *algebraic* mod p^s if there is an algebraic $g(x) \in \mathbb{Z}_p[[x]]$ with $f \equiv g$ mod p^s.

Given $f(x, y) = \sum a_{ij} x^i y^j$ it is natural to refer to the series $I_{xy} f = \sum a_{ii} x^i$ as its *diagonal*.

Given $f(x) = \sum a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}$ we define its diagonal $I_{12} f$ by

$I_{12} f = \sum a_{i_1 i_1 i_3 \cdots i_n} x_1^{i_1} x_3^{i_3} \cdots x_n^{i_n}$; generally, for $k \neq l$, the other I_{kl} are defined correspondingly. By a diagonal we mean any composition of the I_{kl} s. The complete diagonal is $If = \sum a_{ii \cdots i} x_1^i$.

Power Series in Several Variables

$R[[x]]$ is the ring of formal power series in $x = (x_1, \ldots, x_n)$.

I write a series $f(x) \in R[[x]]$ as $f(x) = \sum a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n} = \sum a_\nu x^\nu$ where $\nu = (\nu_1, \ldots, \nu_n)$ is a multi-index and $x^\nu = x_1^{\nu_1} \cdots x_n^{\nu_n}$.

Below, R is usually the finite field $\mathbb{F}_p$ of p elements or the ring of p-adic integers $\mathbb{Z}_p$.

One says that $f(x) \in R[[x]]$ is *algebraic* if it is algebraic over the quotient field of the polynomial ring $R[x]$. I say that $f(x) \in \mathbb{Z}_p[[x]]$ is *algebraic* mod p^s if there is an algebraic $g(x) \in \mathbb{Z}_p[[x]]$ with $f \equiv g$ mod p^s.

Given $f(x, y) = \sum a_{ij} x^i y^j$ it is natural to refer to the series $I_{xy} f = \sum a_{ii} x^i$ as its *diagonal*.

Given $f(x) = \sum a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}$ we define its diagonal $I_{12} f$ by $I_{12} f = \sum a_{i_1 i_1 i_3 \cdots i_n} x_1^{i_1} x_3^{i_3} \cdots x_n^{i_n}$; generally, for $k \neq l$, the other I_{kl} are defined correspondingly. By a diagonal we mean any composition of the I_{kl} s. The complete diagonal is $If = \sum a_{ii \cdots i} x_1^i$.

Power Series in Several Variables

$R[[x]]$ is the ring of formal power series in $x = (x_1, \ldots, x_n)$.

I write a series $f(x) \in R[[x]]$ as $f(x) = \sum a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n} = \sum a_\nu x^\nu$ where $\nu = (\nu_1, \ldots, \nu_n)$ is a multi-index and $x^\nu = x_1^{\nu_1} \cdots x_n^{\nu_n}$.

Below, R is usually the finite field $\mathbb{F}_p$ of p elements or the ring of p-adic integers $\mathbb{Z}_p$.

One says that $f(x) \in R[[x]]$ is *algebraic* if it is algebraic over the quotient field of the polynomial ring $R[x]$. I say that $f(x) \in \mathbb{Z}_p[[x]]$ is *algebraic* mod p^s if there is an algebraic $g(x) \in \mathbb{Z}_p[[x]]$ with $f \equiv g$ mod p^s.

Given $f(x, y) = \sum a_{ij} x^i y^j$ it is natural to refer to the series $I_{xy} f = \sum a_{ii} x^i$ as its *diagonal*.

Given $f(x) = \sum a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}$ we define its diagonal $I_{12} f$ by $I_{12} f = \sum a_{i_1 i_1 i_3 \cdots i_n} x_1^{i_1} x_3^{i_3} \cdots x_n^{i_n}$; generally, for $k \neq l$, the other I_{kl} are defined correspondingly. By a diagonal we mean any composition of the I_{kl} s. The complete diagonal is $If = \sum a_{ii \cdots i} x_1^i$.

Power Series in Several Variables

$R[[x]]$ is the ring of formal power series in $x = (x_1, \dots, x_n)$.

I write a series $f(x) \in R[[x]]$ as $f(x) = \sum a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n} = \sum a_\nu x^\nu$ where $\nu = (\nu_1, \dots, \nu_n)$ is a multi-index and $x^\nu = x_1^{\nu_1} \cdots x_n^{\nu_n}$.

Below, R is usually the finite field $\mathbb{F}_p$ of p elements or the ring of p-adic integers $\mathbb{Z}_p$.

One says that $f(x) \in R[[x]]$ is *algebraic* if it is algebraic over the quotient field of the polynomial ring $R[x]$. I say that $f(x) \in \mathbb{Z}_p[[x]]$ is *algebraic* mod p^s if there is an algebraic $g(x) \in \mathbb{Z}_p[[x]]$ with $f \equiv g$ mod p^s.

Given $f(x, y) = \sum a_{ij} x^i y^j$ it is natural to refer to the series $I_{xy} f = \sum a_{ii} x^i$ as its *diagonal*.

Given $f(x) = \sum a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}$ we define its diagonal $I_{12} f$ by $I_{12} f = \sum a_{i_1 i_1 i_3 \cdots i_n} x_1^{i_1} x_3^{i_3} \cdots x_n^{i_n}$; generally, for $k \neq l$, the other I_{kl} are defined correspondingly. By a diagonal we mean any composition of the I_{kl} s. The complete diagonal is $If = \sum a_{ii \cdots i} x_1^i$.

Power Series in Several Variables

$R[[x]]$ is the ring of formal power series in $x = (x_1, \dots, x_n)$.

I write a series $f(x) \in R[[x]]$ as $f(x) = \sum a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n} = \sum a_\nu x^\nu$ where $\nu = (\nu_1, \dots, \nu_n)$ is a multi-index and $x^\nu = x_1^{\nu_1} \cdots x_n^{\nu_n}$.

Below, R is usually the finite field $\mathbb{F}_p$ of p elements or the ring of p-adic integers $\mathbb{Z}_p$.

One says that $f(x) \in R[[x]]$ is *algebraic* if it is algebraic over the quotient field of the polynomial ring $R[x]$. I say that $f(x) \in \mathbb{Z}_p[[x]]$ is *algebraic* mod p^s if there is an algebraic $g(x) \in \mathbb{Z}_p[[x]]$ with $f \equiv g$ mod p^s.

Given $f(x, y) = \sum a_{ij} x^i y^j$ it is natural to refer to the series $I_{xy} f = \sum a_{ii} x^i$ as its *diagonal*.

Given $f(x) = \sum a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}$ we define its diagonal $I_{12} f$ by $I_{12} f = \sum a_{i_1 i_1 i_3 \cdots i_n} x_1^{i_1} x_3^{i_3} \cdots x_n^{i_n}$; generally, for $k \neq l$, the other I_{kl} are defined correspondingly. By a diagonal we mean any composition of the I_{kl} s. The complete diagonal is $If = \sum a_{ii \cdots i} x_1^i$.

Power Series in Several Variables

$R[[x]]$ is the ring of formal power series in $x = (x_1, \dots, x_n)$.

I write a series $f(x) \in R[[x]]$ as $f(x) = \sum a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n} = \sum a_\nu x^\nu$ where $\nu = (\nu_1, \dots, \nu_n)$ is a multi-index and $x^\nu = x_1^{\nu_1} \cdots x_n^{\nu_n}$.

Below, R is usually the finite field $\mathbb{F}_p$ of p elements or the ring of p-adic integers $\mathbb{Z}_p$.

One says that $f(x) \in R[[x]]$ is *algebraic* if it is algebraic over the quotient field of the polynomial ring $R[x]$. I say that $f(x) \in \mathbb{Z}_p[[x]]$ is *algebraic* mod p^s if there is an algebraic $g(x) \in \mathbb{Z}_p[[x]]$ with $f \equiv g$ mod p^s.

Given $f(x, y) = \sum a_{ij} x^i y^j$ it is natural to refer to the series $I_{xy} f = \sum a_{ii} x^i$ as its *diagonal*.

Given $f(x) = \sum a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}$ we define its diagonal $I_{12} f$ by $I_{12} f = \sum a_{i_1 i_1 i_3 \cdots i_n} x_1^{i_1} x_3^{i_3} \cdots x_n^{i_n}$; generally, for $k \neq l$, the other I_{kl} are defined correspondingly. By a diagonal we mean any composition of the I_{kl} s. The complete diagonal is $If = \sum a_{ii \cdots i} x_1^i$.

Diagonals and Hadamard Products

The *Hadamard product* of series $f(x) = \sum a_\nu x^\nu$ and $g(x) = \sum b_\nu x^\nu$ is the student product

$$f * g(x) = \sum a_\nu b_\nu x^\nu .$$

Diagonals and Hadamard products are connected by:

$$f * g(x) = I_{1,n+1} \dots I_{n,2n} f(x_1, \dots, x_n) g(x_{n+1}, \dots, x_{2n}) ;$$

$$I_{12} f = f * \left(\frac{1}{1 - x_1 x_2} \prod_{j=3}^{n} \frac{1}{1 - x_j}\right) .$$

If a ring of power series is closed under one of the two operations of taking diagonals or Hadamard products then it is closed under the other operation. Over $\mathbb{C}$, the diagonal is also given by the integral

$$I_{12} f(t, x_3, \dots, x_n) = \frac{1}{2\pi i} \oint_{x_1 x_2 = t} f(x_1, \dots, x_n) \frac{dx_1 \wedge dx_2}{dt}$$

$$= \frac{1}{2\pi i} \oint_{|y| = \epsilon} f(t/y, y, x_3, \dots, x_n) dy/y .$$

Diagonals and Hadamard Products

The *Hadamard product* of series $f(x) = \sum a_\nu x^\nu$ and $g(x) = \sum b_\nu x^\nu$ is the student product

$$f * g(x) = \sum a_\nu b_\nu x^\nu .$$

Diagonals and Hadamard products are connected by:

$$f * g(x) = I_{1,n+1} \dots I_{n,2n} f(x_1, \dots, x_n) g(x_{n+1}, \dots, x_{2n}) ;$$

$$I_{12} f = f * \Big(\frac{1}{1 - x_1 x_2} \prod_{j=3}^{n} \frac{1}{1 - x_j}\Big) .$$

If a ring of power series is closed under one of the two operations of taking diagonals or Hadamard products then it is closed under the other operation. Over $\mathbb{C}$, the diagonal is also given by the integral

$$I_{12} f(t, x_3, \dots, x_n) = \frac{1}{2\pi i} \oint_{x_1 x_2 = t} f(x_1, \dots, x_n) \frac{dx_1 \wedge dx_2}{dt}$$

$$= \frac{1}{2\pi i} \oint_{|y| = \epsilon} f(t/y, y, x_3, \dots, x_n) dy/y .$$

Diagonals and Hadamard Products

The *Hadamard product* of series $f(x) = \sum a_\nu x^\nu$ and $g(x) = \sum b_\nu x^\nu$ is the student product

$$f * g(x) = \sum a_\nu b_\nu x^\nu \,.$$

Diagonals and Hadamard products are connected by:

$$f * g(x) = I_{1,n+1} \ldots I_{n,2n} f(x_1, \ldots, x_n) g(x_{n+1}, \ldots, x_{2n})\,;$$

$$I_{12} f = f * \Big(\frac{1}{1 - x_1 x_2} \prod_{j=3}^{n} \frac{1}{1 - x_j}\Big)\,.$$

If a ring of power series is closed under one of the two operations of taking diagonals or Hadamard products then it is closed under the other operation. Over $\mathbb{C}$, the diagonal is also given by the integral

$$I_{12} f(t, x_3, \ldots, x_n) = \frac{1}{2\pi i} \oint_{x_1 x_2 = t} f(x_1, \ldots, x_n) \frac{dx_1 \wedge dx_2}{dt}$$

$$= \frac{1}{2\pi i} \oint_{|y| = \epsilon} f(t/y, y, x_3, \ldots, x_n)\, dy/y \,.$$

Diagonals and Hadamard Products

The *Hadamard product* of series $f(x) = \sum a_\nu x^\nu$ and $g(x) = \sum b_\nu x^\nu$ is the student product

$$f * g(x) = \sum a_\nu b_\nu x^\nu \, .$$

Diagonals and Hadamard products are connected by:

$$f * g(x) = I_{1,n+1} \ldots I_{n,2n} f(x_1, \ldots, x_n) g(x_{n+1}, \ldots, x_{2n}) \, ;$$

$$I_{12} f = f * \Big(\frac{1}{1 - x_1 x_2} \prod_{j=3}^{n} \frac{1}{1 - x_j}\Big) \, .$$

If a ring of power series is closed under one of the two operations of taking diagonals or Hadamard products then it is closed under the other operation. Over $\mathbb{C}$, the diagonal is also given by the integral

$$I_{12} f(t, x_3, \ldots, x_n) = \frac{1}{2\pi i} \oint_{x_1 x_2 = t} f(x_1, \ldots, x_n) \frac{dx_1 \wedge dx_2}{dt}$$

$$= \frac{1}{2\pi i} \oint_{|y| = \epsilon} f(t/y, y, x_3, \ldots, x_n) dy/y \, .$$

Diagonals and Hadamard Products

The *Hadamard product* of series $f(x) = \sum a_\nu x^\nu$ and $g(x) = \sum b_\nu x^\nu$ is the student product

$$f * g(x) = \sum a_\nu b_\nu x^\nu \,.$$

Diagonals and Hadamard products are connected by:

$$f * g(x) = I_{1,n+1} \dots I_{n,2n} f(x_1, \dots, x_n) g(x_{n+1}, \dots, x_{2n})\,;$$

$$I_{12} f = f * \left(\frac{1}{1 - x_1 x_2} \prod_{j=3}^{n} \frac{1}{1 - x_j}\right) .$$

If a ring of power series is closed under one of the two operations of taking diagonals or Hadamard products then it is closed under the other operation. Over $\mathbb{C}$, the diagonal is also given by the integral

$$\begin{aligned} I_{12} f(t, x_3, \dots, x_n) &= \frac{1}{2\pi i} \oint_{x_1 x_2 = t} f(x_1, \dots, x_n) \frac{dx_1 \wedge dx_2}{dt} \\ &= \frac{1}{2\pi i} \oint_{|y| = \epsilon} f(t/y, y, x_3, \dots, x_n) dy/y \,. \end{aligned}$$

A Theorem of Furstenberg

It follows that the diagonal of a rational function $f(x, y)$ of two variables is an algebraic function. Indeed,

$$(If)(t) = \frac{1}{2\pi i} \oint_{|y|=\epsilon} f(t/y, y)\frac{dy}{y} = \frac{1}{2\pi i} \oint_{|y|=\epsilon} \frac{P(t, y)}{Q(t, y)} dy \, .$$

Writing $Q(t, y) = \prod \big(y - y_i(t)\big)$, where the $y_i(t)$ are algebraic, and evaluating the integral by residues verifies the claim.

In fact, every algebraic power series of one variable is the diagonal of a rational power series of two variables and, indeed, every algebraic power series in n variables is the diagonal of a rational power series in $2n$ variables.

Below I sketch a proof showing that every diagonal of a rational function defined over a finite field is algebraic. However, in characteristic zero diagonals of rational functions in more than two variables do not generally yield algebraic functions.

A Theorem of Furstenberg

It follows that the diagonal of a rational function $f(x, y)$ of two variables is an algebraic function. Indeed,

$$(If)(t) = \frac{1}{2\pi i} \oint_{|y|=\epsilon} f(t/y, y)\frac{dy}{y} = \frac{1}{2\pi i} \oint_{|y|=\epsilon} \frac{P(t, y)}{Q(t, y)} dy \,.$$

Writing $Q(t, y) = \prod (y - y_i(t))$, where the $y_i(t)$ are algebraic, and evaluating the integral by residues verifies the claim.

In fact, every algebraic power series of one variable is the diagonal of a rational power series of two variables and, indeed, every algebraic power series in n variables is the diagonal of a rational power series in $2n$ variables.

Below I sketch a proof showing that every diagonal of a rational function defined over a finite field is algebraic. However, in characteristic zero diagonals of rational functions in more than two variables do not generally yield algebraic functions.

A Theorem of Furstenberg

It follows that the diagonal of a rational function $f(x,y)$ of two variables is an algebraic function. Indeed,

$$(If)(t) = \frac{1}{2\pi i} \oint_{|y|=\epsilon} f(t/y, y)\frac{dy}{y} = \frac{1}{2\pi i} \oint_{|y|=\epsilon} \frac{P(t,y)}{Q(t,y)} dy\,.$$

Writing $Q(t,y) = \prod \big(y - y_i(t)\big)$, where the $y_i(t)$ are algebraic, and evaluating the integral by residues verifies the claim.

In fact, every algebraic power series of one variable is the diagonal of a rational power series of two variables and, indeed, every algebraic power series in n variables is the diagonal of a rational power series in $2n$ variables.

Below I sketch a proof showing that every diagonal of a rational function defined over a finite field is algebraic. However, in characteristic zero diagonals of rational functions in more than two variables do not generally yield algebraic functions.

A Theorem of Furstenberg

It follows that the diagonal of a rational function $f(x,y)$ of two variables is an algebraic function. Indeed,

$$(If)(t) = \frac{1}{2\pi i}\oint_{|y|=\epsilon} f(t/y,y)\frac{dy}{y} = \frac{1}{2\pi i}\oint_{|y|=\epsilon} \frac{P(t,y)}{Q(t,y)}dy\,.$$

Writing $Q(t,y) = \prod\big(y - y_i(t)\big)$, where the $y_i(t)$ are algebraic, and evaluating the integral by residues verifies the claim.

In fact, every algebraic power series of one variable is the diagonal of a rational power series of two variables and, indeed, every algebraic power series in n variables is the diagonal of a rational power series in $2n$ variables.

Below I sketch a proof showing that every diagonal of a rational function defined over a finite field is algebraic. However, in characteristic zero diagonals of rational functions in more than two variables do not generally yield algebraic functions.

A Theorem of Furstenberg

It follows that the diagonal of a rational function $f(x, y)$ of two variables is an algebraic function. Indeed,

$$(If)(t) = \frac{1}{2\pi i} \oint_{|y|=\epsilon} f(t/y, y) \frac{dy}{y} = \frac{1}{2\pi i} \oint_{|y|=\epsilon} \frac{P(t, y)}{Q(t, y)} dy\,.$$

Writing $Q(t, y) = \prod \big(y - y_i(t)\big)$, where the $y_i(t)$ are algebraic, and evaluating the integral by residues verifies the claim.

In fact, every algebraic power series of one variable is the diagonal of a rational power series of two variables and, indeed, every algebraic power series in n variables is the diagonal of a rational power series in $2n$ variables.

Below I sketch a proof showing that <u>every diagonal of a rational function defined over a finite field is algebraic</u>. However, in characteristic zero diagonals of rational functions in more than two variables do not generally yield algebraic functions.

A Theorem of Furstenberg

It follows that the diagonal of a rational function $f(x, y)$ of two variables is an algebraic function. Indeed,

$$(If)(t) = \frac{1}{2\pi i} \oint_{|y|=\epsilon} f(t/y, y)\frac{dy}{y} = \frac{1}{2\pi i} \oint_{|y|=\epsilon} \frac{P(t, y)}{Q(t, y)} dy\,.$$

Writing $Q(t, y) = \prod \big(y - y_i(t)\big)$, where the $y_i(t)$ are algebraic, and evaluating the integral by residues verifies the claim.

In fact, every algebraic power series of one variable is the diagonal of a rational power series of two variables and, indeed, every algebraic power series in n variables is the diagonal of a rational power series in $2n$ variables.

Below I sketch a proof showing that <u>every diagonal of a rational function defined over a finite field is algebraic</u>. However, in characteristic zero diagonals of rational functions in more than two variables do not generally yield algebraic functions.

As said, in characteristic zero, neither diagonals, nor Hadamard products, preserve algebraicity. For the latter, the standard example is

$$(1-4X)^{-1/2} = \sum \binom{2h}{h} X^h; \quad \text{but} \quad \sum \binom{2h}{h}^2 X^h$$

is not algebraic. The first remark is just the useful identity

$$\binom{2h}{h} = (-4)^h \binom{-1/2}{h}$$

Facts such as this are of interest to logicians. Then, introductory calculus shows the latter series is given by the integral

$$\frac{2}{\pi}\int_0^{\pi/2} \frac{dt}{\sqrt{(1-16X\sin^2 t)}}.$$

This is a complete elliptic integral well known not to represent an algebraic function.

As said, in characteristic zero, neither diagonals, nor Hadamard products, preserve algebraicity. For the latter, the standard example is

$$(1-4X)^{-1/2} = \sum \binom{2h}{h} X^h; \quad \text{but} \quad \sum \binom{2h}{h}^2 X^h$$

is not algebraic. The first remark is just the useful identity

$$\binom{2h}{h} = (-4)^h \binom{-1/2}{h}$$

Facts such as this are of interest to logicians.Then, introductory calculus shows the latter series is given by the integral

$$\frac{2}{\pi}\int_0^{\pi/2} \frac{dt}{\sqrt{(1-16X\sin^2 t)}}\,.$$

This is a complete elliptic integral well known not to represent an algebraic function.

As said, in characteristic zero, neither diagonals, nor Hadamard products, preserve algebraicity. For the latter, the standard example is

$$(1-4X)^{-1/2} = \sum \binom{2h}{h} X^h; \quad \text{but} \quad \sum \binom{2h}{h}^2 X^h$$

is not algebraic. The first remark is just the useful identity

$$\binom{2h}{h} = (-4)^h \binom{-1/2}{h}$$

Facts such as this are of interest to logicians. Then, introductory calculus shows the latter series is given by the integral

$$\frac{2}{\pi}\int_0^{\pi/2} \frac{dt}{\sqrt{(1-16X\sin^2 t)}}.$$

This is a complete elliptic integral well known not to represent an algebraic function.

As said, in characteristic zero, neither diagonals, nor Hadamard products, preserve algebraicity. For the latter, the standard example is

$$(1-4X)^{-1/2} = \sum \binom{2h}{h} X^h \,; \quad \text{but} \quad \sum \binom{2h}{h}^2 X^h$$

is not algebraic. The first remark is just the useful identity

$$\binom{2h}{h} = (-4)^h \binom{-1/2}{h}$$

Facts such as this are of interest to logicians.Then, introductory calculus shows the latter series is given by the integral

$$\frac{2}{\pi} \int_0^{\pi/2} \frac{dt}{\sqrt{(1-16X\sin^2 t)}} \,.$$

This is a complete elliptic integral well known not to represent an algebraic function.

As said, in characteristic zero, neither diagonals, nor Hadamard products, preserve algebraicity. For the latter, the standard example is

$$(1-4X)^{-1/2}=\sum\binom{2h}{h}X^h; \quad \text{but} \quad \sum\binom{2h}{h}^2X^h$$

is not algebraic. The first remark is just the useful identity

$$\binom{2h}{h}=(-4)^h\binom{-1/2}{h}$$

Facts such as this are of interest to logicians.Then, introductory calculus shows the latter series is given by the integral

$$\frac{2}{\pi}\int_0^{\pi/2}\frac{dt}{\sqrt{(1-16X\sin^2 t)}}\,.$$

This is a complete elliptic integral well known not to represent an algebraic function.

A Beautiful Transcendence Argument

For general odd k the question of the transcendence of the Hadamard powers

$$F_k(X) = \sum \binom{2h}{h}^k X^h$$

had long been open, until delightfully settled by a remark of Sharif and Woodcock.

On the one hand, one views F_k as defined over $\mathbb{F}_p$, so that certainly $F_k^p = F_k$ and plainly F_k has degree dividing $p-1$. However, it is easy to see that given any lower bound r there are infinitely many odd primes p so that $p-1$ is divisible only by 1, 2, and primes greater than r.

Exercise. One also confirms fairly readily that F_k is neither rational nor of degree 2 over $\mathbb{F}_p$ for infinitely many p.

On the other hand, if F_k defined over $\mathbb{Q}$ were algebraic, say of degree r, then obviously its reduction mod p also is algebraic of degree at most r.

A Beautiful Transcendence Argument

For general odd k the question of the transcendence of the Hadamard powers

$$F_k(X) = \sum \binom{2h}{h}^k X^h$$

had long been open, until delightfully settled by a remark of Sharif and Woodcock.

On the one hand, one views F_k as defined over $\mathbb{F}_p$, so that certainly $F_k^p = F_k$ and plainly F_k has degree dividing $p-1$. However, it is easy to see that given any lower bound r there are infinitely many odd primes p so that $p-1$ is divisible only by 1, 2, and primes greater than r.

Exercise. One also confirms fairly readily that F_k is neither rational nor of degree 2 over $\mathbb{F}_p$ for infinitely many p.

On the other hand, if F_k defined over $\mathbb{Q}$ were algebraic, say of degree r, then obviously its reduction mod p also is algebraic of degree at most r.

A Beautiful Transcendence Argument

For general odd k the question of the transcendence of the Hadamard powers

$$F_k(X) = \sum \binom{2h}{h}^k X^h$$

had long been open, until delightfully settled by a remark of Sharif and Woodcock.

On the one hand, one views F_k as defined over $\mathbb{F}_p$, so that certainly $F_k^p = F_k$ and plainly F_k has degree dividing $p-1$. However, it is easy to see that given any lower bound r there are infinitely many odd primes p so that $p-1$ is divisible only by 1, 2, and primes greater than r.

Exercise. One also confirms fairly readily that F_k is neither rational nor of degree 2 over $\mathbb{F}_p$ for infinitely many p.

On the other hand, if F_k defined over $\mathbb{Q}$ were algebraic, say of degree r, then obviously its reduction mod p also is algebraic of degree at most r.

A Beautiful Transcendence Argument

For general odd k the question of the transcendence of the Hadamard powers

$$F_k(X) = \sum \binom{2h}{h}^k X^h$$

had long been open, until delightfully settled by a remark of Sharif and Woodcock.

On the one hand, one views F_k as defined over $\mathbb{F}_p$, so that certainly $F_k^p = F_k$ and plainly F_k has degree dividing $p-1$. However, it is easy to see that given any lower bound r there are infinitely many odd primes p so that $p-1$ is divisible only by 1, 2, and primes greater than r.

Exercise. One also confirms fairly readily that F_k is neither rational nor of degree 2 over $\mathbb{F}_p$ for infinitely many p.

On the other hand, if F_k defined over $\mathbb{Q}$ were algebraic, say of degree r, then obviously its reduction mod p also is algebraic of degree at most r.

A Beautiful Transcendence Argument

For general odd k the question of the transcendence of the Hadamard powers

$$F_k(X) = \sum \binom{2h}{h}^k X^h$$

had long been open, until delightfully settled by a remark of Sharif and Woodcock.

On the one hand, one views F_k as defined over $\mathbb{F}_p$, so that certainly $F_k^p = F_k$ and plainly F_k has degree dividing $p-1$. However, it is easy to see that given any lower bound r there are infinitely many odd primes p so that $p-1$ is divisible only by 1, 2, and primes greater than r.

Exercise. One also confirms fairly readily that F_k is neither rational nor of degree 2 over $\mathbb{F}_p$ for infinitely many p.

On the other hand, if F_k defined over $\mathbb{Q}$ were algebraic, say of degree r, then obviously its reduction mod p also is algebraic of degree at most r.

Breaking Up in Characteristic p

The following breaking up procedure is fundamental below:

$\{x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n} : \alpha \in S\}$ is a basis for $\mathbb{F}_p[[x]]$ over $\big(\mathbb{F}_p[[x]]\big)^p$.

Hence if $y(x) \in \mathbb{F}_p[[x]]$ and $S = \{0, 1, \ldots, p-1\}^n$ then, for $\alpha \in S$, there are unique $y_\alpha(x) \in \mathbb{F}_p[[x]]$ such that $y(x) = \sum_{\alpha \in S} x^\alpha y_\alpha^p(x)$.

If $y(x) \in \mathbb{F}_p[[x]]$ is algebraic then y satisfies an equation of the shape

$$\sum_{i=r}^{s} f_i(x) y^{p^i} = 0 ,$$

with r , $s \in \mathbb{N}$, the $f_i \in \mathbb{F}_p[x]$ and $f_r \neq 0$. In fact, we may take $r = 0$, for if $r > 0$ then writing $f_i = \sum_\alpha x^\alpha f_{i\alpha}^p$ we get that

$$\sum_\alpha x^\alpha \Big(\sum_{i=r}^{s} f_{i\alpha}(x) y^{p^{i-1}}\Big)^p = 0 .$$

Hence $\sum_{i=r-1}^{s-1} f_{i+1,\alpha}(x) y^{p^i} = 0$ and some $f_{r\alpha} \neq 0$.

Breaking Up in Characteristic p

The following breaking up procedure is fundamental below:

$\{x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n} : \alpha \in S\}$ is a basis for $\mathbb{F}_p[[x]]$ over $\left(\mathbb{F}_p[[x]]\right)^p$.

Hence if $y(x) \in \mathbb{F}_p[[x]]$ and $S = \{0, 1, \ldots, p-1\}^n$ then, for $\alpha \in S$, there are unique $y_\alpha(x) \in \mathbb{F}_p[[x]]$ such that $y(x) = \sum_{\alpha \in S} x^\alpha y_\alpha^p(x)$.

If $y(x) \in \mathbb{F}_p[[x]]$ is algebraic then y satisfies an equation of the shape

$$\sum_{i=r}^{s} f_i(x) y^{p^i} = 0 \,,$$

with r , $s \in \mathbb{N}$, the $f_i \in \mathbb{F}_p[x]$ and $f_r \neq 0$. In fact, we may take $r = 0$, for if $r > 0$ then writing $f_i = \sum_\alpha x^\alpha f_{i\alpha}^p$ we get that

$$\sum_\alpha x^\alpha \Big(\sum_{i=r}^{s} f_{i\alpha}(x) y^{p^{i-1}}\Big)^p = 0 \,.$$

Hence $\sum_{i=r-1}^{s-1} f_{i+1,\alpha}(x) y^{p^i} = 0$ and some $f_{r\alpha} \neq 0$.

Breaking Up in Characteristic p

The following breaking up procedure is fundamental below:

$\{x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n} : \alpha \in S\}$ is a basis for $\mathbb{F}_p[[x]]$ over $\left(\mathbb{F}_p[[x]]\right)^p$.

Hence if $y(x) \in \mathbb{F}_p[[x]]$ and $S = \{0, 1, \ldots, p-1\}^n$ then, for $\alpha \in S$, there are unique $y_\alpha(x) \in \mathbb{F}_p[[x]]$ such that $y(x) = \sum_{\alpha \in S} x^\alpha y_\alpha^p(x)$.

If $y(x) \in \mathbb{F}_p[[x]]$ is algebraic then y satisfies an equation of the shape

$$\sum_{i=r}^{s} f_i(x) y^{p^i} = 0 ,$$

with r , $s \in \mathbb{N}$, the $f_i \in \mathbb{F}_p[x]$ and $f_r \neq 0$. In fact, we may take $r = 0$, for if $r > 0$ then writing $f_i = \sum_\alpha x^\alpha f_{i\alpha}^p$ we get that

$$\sum_\alpha x^\alpha \Big(\sum_{i=r}^{s} f_{i\alpha}(x) y^{p^{i-1}}\Big)^p = 0 .$$

Hence $\sum_{i=r-1}^{s-1} f_{i+1,\alpha}(x) y^{p^i} = 0$ and some $f_{r\alpha} \neq 0$.

Breaking Up in Characteristic p

The following breaking up procedure is fundamental below:

$\{x^\alpha = x_1^{\alpha_1}\cdots x_n^{\alpha_n} : \alpha \in S\}$ is a basis for $\mathbb{F}_p[[x]]$ over $\left(\mathbb{F}_p[[x]]\right)^p$.

Hence if $y(x) \in \mathbb{F}_p[[x]]$ and $S = \{0, 1, \ldots, p-1\}^n$ then, for $\alpha \in S$, there are unique $y_\alpha(x) \in \mathbb{F}_p[[x]]$ such that $y(x) = \sum_{\alpha\in S} x^\alpha y_\alpha^p(x)$.

If $y(x) \in \mathbb{F}_p[[x]]$ is algebraic then y satisfies an equation of the shape

$$\sum_{i=r}^{s} f_i(x) y^{p^i} = 0 ,$$

with r , $s \in \mathbb{N}$, the $f_i \in \mathbb{F}_p[x]$ and $f_r \neq 0$. In fact, we may take $r = 0$, for if $r > 0$ then writing $f_i = \sum_\alpha x^\alpha f_{i\alpha}^p$ we get that

$$\sum_\alpha x^\alpha \Big(\sum_{i=r}^{s} f_{i\alpha}(x) y^{p^{i-1}}\Big)^p = 0 .$$

Hence $\sum_{i=r-1}^{s-1} f_{i+1,\alpha}(x) y^{p^i} = 0$ and some $f_{r\alpha} \neq 0$.

Breaking Up in Characteristic p

The following breaking up procedure is fundamental below:

$\{x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n} : \alpha \in S\}$ is a basis for $\mathbb{F}_p[[x]]$ over $\left(\mathbb{F}_p[[x]]\right)^p$.

Hence if $y(x) \in \mathbb{F}_p[[x]]$ and $S = \{0, 1, \ldots, p-1\}^n$ then, for $\alpha \in S$, there are unique $y_\alpha(x) \in \mathbb{F}_p[[x]]$ such that $y(x) = \sum_{\alpha \in S} x^\alpha y_\alpha^p(x)$.

If $y(x) \in \mathbb{F}_p[[x]]$ is algebraic then y satisfies an equation of the shape

$$\sum_{i=r}^{s} f_i(x) y^{p^i} = 0 \,,$$

with r , $s \in \mathbb{N}$, the $f_i \in \mathbb{F}_p[x]$ and $f_r \neq 0$. In fact, we may take $r = 0$, for if $r > 0$ then writing $f_i = \sum_\alpha x^\alpha f_{i\alpha}^p$ we get that

$$\sum_\alpha x^\alpha \Big(\sum_{i=r}^{s} f_{i\alpha}(x) y^{p^{i-1}}\Big)^p = 0 \,.$$

Hence $\sum_{i=r-1}^{s-1} f_{i+1,\alpha}(x) y^{p^i} = 0$ and some $f_{r\alpha} \neq 0$.

Breaking Up in Characteristic p

The following breaking up procedure is fundamental below:

$\{x^\alpha = x_1^{\alpha_1}\cdots x_n^{\alpha_n} : \alpha \in S\}$ is a basis for $\mathbb{F}_p[[x]]$ over $\big(\mathbb{F}_p[[x]]\big)^p$.

Hence if $y(x) \in \mathbb{F}_p[[x]]$ and $S = \{0, 1, \ldots, p-1\}^n$ then, for $\alpha \in S$, there are unique $y_\alpha(x) \in \mathbb{F}_p[[x]]$ such that $y(x) = \sum_{\alpha\in S} x^\alpha y_\alpha^p(x)$.

If $y(x) \in \mathbb{F}_p[[x]]$ is algebraic then y satisfies an equation of the shape

$$\sum_{i=r}^{s} f_i(x) y^{p^i} = 0\,,$$

with r , $s \in \mathbb{N}$, the $f_i \in \mathbb{F}_p[x]$ and $f_r \neq 0$. In fact, we may take $r = 0$, for if $r > 0$ then writing $f_i = \sum_\alpha x^\alpha f_{i\alpha}^p$ we get that

$$\sum_\alpha x^\alpha \Big(\sum_{i=r}^{s} f_{i\alpha}(x) y^{p^{i-1}}\Big)^p = 0\,.$$

Hence $\sum_{i=r-1}^{s-1} f_{i+1,\alpha}(x) y^{p^i} = 0$ and some $f_{r\alpha} \neq 0$.

Algebraic power series in characteristic p

Thus if $y \in \mathbb{F}_p[[x]]$ is algebraic, y satisfies an equation of the shape

$$f(x)y = \sum_{i=1}^{s} f_i(x)y^{p^i} = L\big(y^p, \ldots, y^{p^s}\big) ,$$

where L is linear with coefficients polynomials in x . After multiplying by f^{p-1} , breaking up y and the coefficients of L, and then taking p-th roots, we get equations

$$f(x)y_{\alpha_1} = L_{\alpha_1}\big(y, y^p, \ldots, y^{p^{s-1}}\big) .$$

Now multiplying by f^{p-1} and substituting for $f(x)y$ on the right yields

$$f^p y_{\alpha_1} = L_{\alpha_1}(f^{p-2}L(y^p, \ldots, y^{p^s}), f^{p-1}y^p, \ldots, f^{p-1}y^{p^{s-1}}) ,$$

which again is linear in y^p ,..., y^{p^s} . This brings us back, more or less, to the start and shows that iterating the process described leads to equations of the shape

$$f(x)y_{\alpha_1\ldots\alpha_e} = L_{\alpha_1\ldots\alpha_e}\big(y, y^p, \ldots, y^{p^{s-1}}\big) .$$

If, during this procedure, we keep track of the (multi-) degree in x of $L_{\alpha_1\ldots\alpha_e}$ we see that degree remains bounded.

Algebraic power series in characteristic p

Thus if $y \in \mathbb{F}_p[[x]]$ is algebraic, y satisfies an equation of the shape

$$f(x)y = \sum_{i=1}^{s} f_i(x) y^{p^i} = L\left(y^p, \ldots, y^{p^s}\right),$$

where L is linear with coefficients polynomials in x . After multiplying by f^{p-1} , breaking up y and the coefficients of L, and then taking p-th roots, we get equations

$$f(x)y_{\alpha_1} = L_{\alpha_1}\left(y, y^p, \ldots, y^{p^{s-1}}\right).$$

Now multiplying by f^{p-1} and substituting for $f(x)y$ on the right yields

$$f^p y_{\alpha_1} = L_{\alpha_1}(f^{p-2}L(y^p, \ldots, y^{p^s}), f^{p-1}y^p, \ldots, f^{p-1}y^{p^{s-1}}),$$

which again is linear in y^p ,…, y^{p^s} . This brings us back, more or less, to the start and shows that iterating the process described leads to equations of the shape

$$f(x)y_{\alpha_1\ldots\alpha_e} = L_{\alpha_1\ldots\alpha_e}\left(y, y^p, \ldots, y^{p^{s-1}}\right).$$

If, during this procedure, we keep track of the (multi-) degree in x of $L_{\alpha_1\ldots\alpha_e}$ we see that degree remains bounded.

Algebraic power series in characteristic p

Thus if $y \in \mathbb{F}_p[[x]]$ is algebraic, y satisfies an equation of the shape

$$f(x)y = \sum_{i=1}^{s} f_i(x)y^{p^i} = L\big(y^p, \ldots, y^{p^s}\big) ,$$

where L is linear with coefficients polynomials in x . After multiplying by f^{p-1} , breaking up y and the coefficients of L, and then taking p-th roots, we get equations

$$f(x)y_{\alpha_1} = L_{\alpha_1}\big(y, y^p, \ldots, y^{p^{s-1}}\big) .$$

Now multiplying by f^{p-1} and substituting for $f(x)y$ on the right yields

$$f^p y_{\alpha_1} = L_{\alpha_1}(f^{p-2}L(y^p, \ldots, y^{p^s}), f^{p-1}y^p, \ldots, f^{p-1}y^{p^{s-1}}) ,$$

which again is linear in y^p ,. . . , y^{p^s} . This brings us back, more or less, to the start and shows that iterating the process described leads to equations of the shape

$$f(x)y_{\alpha_1\ldots\alpha_e} = L_{\alpha_1\ldots\alpha_e}\big(y, y^p, \ldots, y^{p^{s-1}}\big) .$$

If, during this procedure, we keep track of the (multi-) degree in x of $L_{\alpha_1\ldots\alpha_e}$ we see that degree remains bounded.

Algebraic power series in characteristic p

Thus if $y \in \mathbb{F}_p[[x]]$ is algebraic, y satisfies an equation of the shape

$$f(x)y = \sum_{i=1}^{s} f_i(x)y^{p^i} = L\left(y^p, \ldots, y^{p^s}\right),$$

where L is linear with coefficients polynomials in x. After multiplying by f^{p-1}, breaking up y and the coefficients of L, and then taking p-th roots, we get equations

$$f(x)y_{\alpha_1} = L_{\alpha_1}\left(y, y^p, \ldots, y^{p^{s-1}}\right).$$

Now multiplying by f^{p-1} and substituting for $f(x)y$ on the right yields

$$f^p y_{\alpha_1} = L_{\alpha_1}(f^{p-2}L(y^p, \ldots, y^{p^s}), f^{p-1}y^p, \ldots, f^{p-1}y^{p^{s-1}}),$$

which again is linear in y^p ,..., y^{p^s}. This brings us back, more or less, to the start and shows that iterating the process described leads to equations of the shape

$$f(x)y_{\alpha_1\ldots\alpha_e} = L_{\alpha_1\ldots\alpha_e}\left(y, y^p, \ldots, y^{p^{s-1}}\right).$$

If, during this procedure, we keep track of the (multi-) degree in x of $L_{\alpha_1\ldots\alpha_e}$ we see that degree remains bounded.

Algebraic power series in characteristic p

Thus if $y \in \mathbb{F}_p[[x]]$ is algebraic, y satisfies an equation of the shape

$$f(x)y = \sum_{i=1}^{s} f_i(x)y^{p^i} = L\big(y^p, \ldots, y^{p^s}\big) ,$$

where L is linear with coefficients polynomials in x . After multiplying by f^{p-1} , breaking up y and the coefficients of L, and then taking p-th roots, we get equations

$$f(x)y_{\alpha_1} = L_{\alpha_1}\big(y, y^p, \ldots, y^{p^{s-1}}\big) .$$

Now multiplying by f^{p-1} and substituting for $f(x)y$ on the right yields

$$f^p y_{\alpha_1} = L_{\alpha_1}(f^{p-2}L(y^p, \ldots, y^{p^s}), f^{p-1}y^p, \ldots, f^{p-1}y^{p^{s-1}}) ,$$

which again is linear in y^p ,..., y^{p^s} . This brings us back, more or less, to the start and shows that iterating the process described leads to equations of the shape

$$f(x)y_{\alpha_1\ldots\alpha_e} = L_{\alpha_1\ldots\alpha_e}\big(y, y^p, \ldots, y^{p^{s-1}}\big) .$$

If, during this procedure, we keep track of the (multi-) degree in x of $L_{\alpha_1\ldots\alpha_e}$ we see that degree remains bounded.

Algebraic power series in characteristic p

Thus if $y \in \mathbb{F}_p[[x]]$ is algebraic, y satisfies an equation of the shape

$$f(x)y = \sum_{i=1}^{s} f_i(x)y^{p^i} = L\big(y^p, \ldots, y^{p^s}\big) ,$$

where L is linear with coefficients polynomials in x . After multiplying by f^{p-1} , breaking up y and the coefficients of L, and then taking p-th roots, we get equations

$$f(x)y_{\alpha_1} = L_{\alpha_1}\big(y, y^p, \ldots, y^{p^{s-1}}\big) .$$

Now multiplying by f^{p-1} and substituting for $f(x)y$ on the right yields

$$f^p y_{\alpha_1} = L_{\alpha_1}(f^{p-2}L(y^p, \ldots, y^{p^s}), f^{p-1}y^p, \ldots, f^{p-1}y^{p^{s-1}}) ,$$

which again is linear in y^p ,..., y^{p^s} . This brings us back, more or less, to the start and shows that iterating the process described leads to equations of the shape

$$f(x)y_{\alpha_1\ldots\alpha_e} = L_{\alpha_1\ldots\alpha_e}\big(y, y^p, \ldots, y^{p^{s-1}}\big) .$$

If, during this procedure, we keep track of the (multi-) degree in x of $L_{\alpha_1\ldots\alpha_e}$ we see that degree remains bounded.

Hence, since $\mathbb{F}_p$ is finite, there are only a finite number of distinct $y_{\alpha_1\ldots\alpha_e}$ and we have a result of Christol, Kamae, Mendès France, and Rauzy, here proved by the elegant independent methods of Jan Denef and Leonard Lipshitz.

Theorem. If $y = \sum a_\nu x^\nu$ is algebraic then

(F) there is an e such that for every $(\alpha_1, \ldots, \alpha_e) \in S^e$ there is an $e' < e$ and a $(\beta_1, \ldots, \beta_{e'}) \in S^{e'}$ such that
$$y_{\alpha_1\ldots\alpha_e} = y_{\beta_1\ldots\beta_{e'}} ;$$

(A) equivalently, there is an e such that for all $j = (j_1, \ldots, j_n)$ with the $j_i < p^e$ there is an $e' < e$ and a $j' = (j'_1, \ldots, j'_n)$ with the $j'_i < p^{e'}$ such that
$$a_{p^e\nu+j} = a_{p^{e'}\nu+j'} \text{ for all } \nu .$$

Conversely, if y satisfies (F) then taking $y_{\beta_1\ldots\beta_{e'}}$ and breaking it up $e - e'$ times, we see that the $y_{\alpha_1\ldots\alpha_e}$ satisfy a system of the form
$$y_{\alpha_1\ldots\alpha_e} = \sum x^\gamma y_{\beta_1\ldots\beta_e}^{p^{e-e'}} .$$
By an easy lemma it follows that the $y_{\alpha_1\ldots\alpha_e}$, and hence y, must be algebraic.

Hence, since $\mathbb{F}_p$ is finite, there are only a finite number of distinct $y_{\alpha_1\dots\alpha_e}$ and we have a result of Christol, Kamae, Mendès France, and Rauzy, here proved by the elegant independent methods of Jan Denef and Leonard Lipshitz.

Theorem. If $y = \sum a_\nu x^\nu$ is algebraic then

(F) there is an e such that for every $(\alpha_1, \dots, \alpha_e) \in S^e$ there is an $e' < e$ and a $(\beta_1, \dots, \beta_{e'}) \in S^{e'}$ such that

$$y_{\alpha_1\dots\alpha_e} = y_{\beta_1\dots\beta_{e'}} \,;$$

(A) equivalently, there is an e such that for all $j = (j_1, \dots, j_n)$ with the $j_i < p^e$ there is an $e' < e$ and a $j' = (j'_1, \dots, j'_n)$ with the $j'_i < p^{e'}$ such that

$$a_{p^e\nu+j} = a_{p^{e'}\nu+j'} \text{ for all } \nu \,.$$

Conversely, if y satisfies (F) then taking $y_{\beta_1\dots\beta_{e'}}$ and breaking it up $e - e'$ times, we see that the $y_{\alpha_1\dots\alpha_e}$ satisfy a system of the form

$$y_{\alpha_1\dots\alpha_e} = \sum x^\gamma y_{\beta_1\dots\beta_e}^{p^{e-e'}} \,.$$

By an easy lemma it follows that the $y_{\alpha_1\dots\alpha_e}$, and hence y, must be algebraic.

Hence, since $\mathbb{F}_p$ is finite, there are only a finite number of distinct $y_{\alpha_1\dots\alpha_e}$ and we have a result of Christol, Kamae, Mendès France, and Rauzy, here proved by the elegant independent methods of Jan Denef and Leonard Lipshitz.

Theorem. If $y = \sum a_\nu x^\nu$ is algebraic then

(F) there is an e such that for every $(\alpha_1, \dots, \alpha_e) \in S^e$ there is an $e' < e$ and a $(\beta_1, \dots, \beta_{e'}) \in S^{e'}$ such that
$$y_{\alpha_1\dots\alpha_e} = y_{\beta_1\dots\beta_{e'}} \, ;$$

(A) equivalently, there is an e such that for all $j = (j_1, \dots, j_n)$ with the $j_i < p^e$ there is an $e' < e$ and a $j' = (j'_1, \dots, j'_n)$ with the $j'_i < p^{e'}$ such that
$$a_{p^e\nu+j} = a_{p^{e'}\nu+j'} \text{ for all } \nu \, .$$

Conversely, if y satisfies (F) then taking $y_{\beta_1\dots\beta_{e'}}$ and breaking it up $e - e'$ times, we see that the $y_{\alpha_1\dots\alpha_e}$ satisfy a system of the form
$$y_{\alpha_1\dots\alpha_e} = \sum x^\gamma y_{\beta_1\dots\beta_e}^{p^{e-e'}} \, .$$
By an easy lemma it follows that the $y_{\alpha_1\dots\alpha_e}$, and hence y, must be algebraic.

Suppose the series $\sum a_\nu x^\nu$ is generated by a finite automaton $\mathcal{M}$.

Choose e so large that every state that $\mathcal{M}$ enters in the course of any computation is entered in a computation of length less than e. Then the a_ν satisfy version (A) of the Theorem.

Conversely, if the a_ν satisfy (A) one can construct a finite automaton $\mathcal{M}$ that generates $\sum a_\nu x^\nu$.

$\mathcal{M}$ will be equipped with a table detailing the identifications (A) and an output list of the values of the a_j for $j = (j_1, \ldots, j_n)$ with the $j_i < p^e$.

The automaton $\mathcal{M}$ computes as follows: It reads e digits from each tape. Then it uses the table (A) to replace those e digits by e' digits. It reads a further $e - e'$ digits and iterates. At each stage it outputs the appropriate value from its output list.

Suppose the series $\sum a_\nu x^\nu$ is generated by a finite automaton $\mathcal{M}$.

Choose e so large that every state that $\mathcal{M}$ enters in the course of any computation is entered in a computation of length less than e. Then the a_ν satisfy version (A) of the Theorem.

Conversely, if the a_ν satisfy (A) one can construct a finite automaton $\mathcal{M}$ that generates $\sum a_\nu x^\nu$.

$\mathcal{M}$ will be equipped with a table detailing the identifications (A) and an output list of the values of the a_j for $j = (j_1, \ldots, j_n)$ with the $j_i < p^e$.

The automaton $\mathcal{M}$ computes as follows: It reads e digits from each tape. Then it uses the table (A) to replace those e digits by e' digits. It reads a further $e - e'$ digits and iterates. At each stage it outputs the appropriate value from its output list.

Suppose the series $\sum a_\nu x^\nu$ is generated by a finite automaton $\mathcal{M}$.

Choose e so large that every state that $\mathcal{M}$ enters in the course of any computation is entered in a computation of length less than e . Then the a_ν satisfy version (A) of the Theorem.

Conversely, if the a_ν satisfy (A) one can construct a finite automaton $\mathcal{M}$ that generates $\sum a_\nu x^\nu$.

$\mathcal{M}$ will be equipped with a table detailing the identifications (A) and an output list of the values of the a_j for $j = (j_1, \ldots, j_n)$ with the $j_i < p^e$.

The automaton $\mathcal{M}$ computes as follows: It reads e digits from each tape. Then it uses the table (A) to replace those e digits by e' digits. It reads a further $e - e'$ digits and iterates. At each stage it outputs the appropriate value from its output list.

Suppose the series $\sum a_\nu x^\nu$ is generated by a finite automaton $\mathcal{M}$.

Choose e so large that every state that $\mathcal{M}$ enters in the course of any computation is entered in a computation of length less than e . Then the a_ν satisfy version (A) of the Theorem.

Conversely, if the a_ν satisfy (A) one can construct a finite automaton $\mathcal{M}$ that generates $\sum a_\nu x^\nu$.

$\mathcal{M}$ will be equipped with a table detailing the identifications (A) and an output list of the values of the a_j for $j = (j_1, \ldots, j_n)$ with the $j_i < p^e$.

The automaton $\mathcal{M}$ computes as follows: It reads e digits from each tape. Then it uses the table (A) to replace those e digits by e' digits. It reads a further $e - e'$ digits and iterates. At each stage it outputs the appropriate value from its output list.

Suppose the series $\sum a_\nu x^\nu$ is generated by a finite automaton $\mathcal{M}$.

Choose e so large that every state that $\mathcal{M}$ enters in the course of any computation is entered in a computation of length less than e . Then the a_ν satisfy version (A) of the Theorem.

Conversely, if the a_ν satisfy (A) one can construct a finite automaton $\mathcal{M}$ that generates $\sum a_\nu x^\nu$.

$\mathcal{M}$ will be equipped with a table detailing the identifications (A) and an output list of the values of the a_j for $j = (j_1, \ldots, j_n)$ with the $j_i < p^e$.

The automaton $\mathcal{M}$ computes as follows: It reads e digits from each tape. Then it uses the table (A) to replace those e digits by e' digits. It reads a further $e - e'$ digits and iterates. At each stage it outputs the appropriate value from its output list.

Suppose the series $\sum a_\nu x^\nu$ is generated by a finite automaton $\mathcal{M}$.

Choose e so large that every state that $\mathcal{M}$ enters in the course of any computation is entered in a computation of length less than e . Then the a_ν satisfy version (A) of the Theorem.

Conversely, if the a_ν satisfy (A) one can construct a finite automaton $\mathcal{M}$ that generates $\sum a_\nu x^\nu$.

$\mathcal{M}$ will be equipped with a table detailing the identifications (A) and an output list of the values of the a_j for $j = (j_1, \ldots, j_n)$ with the $j_i < p^e$.

The automaton $\mathcal{M}$ computes as follows: It reads e digits from each tape. Then it uses the table (A) to replace those e digits by e' digits. It reads a further $e - e'$ digits and iterates. At each stage it outputs the appropriate value from its output list.

Suppose the series $\sum a_\nu x^\nu$ is generated by a finite automaton $\mathcal{M}$.

Choose e so large that every state that $\mathcal{M}$ enters in the course of any computation is entered in a computation of length less than e. Then the a_ν satisfy version (A) of the Theorem.

Conversely, if the a_ν satisfy (A) one can construct a finite automaton $\mathcal{M}$ that generates $\sum a_\nu x^\nu$.

$\mathcal{M}$ will be equipped with a table detailing the identifications (A) and an output list of the values of the a_j for $j = (j_1, \ldots, j_n)$ with the $j_i < p^e$.

The automaton $\mathcal{M}$ computes as follows: It reads e digits from each tape. Then it uses the table (A) to replace those e digits by e' digits. It reads a further $e - e'$ digits and iterates. At each stage it outputs the appropriate value from its output list.

Suppose the series $\sum a_\nu x^\nu$ is generated by a finite automaton $\mathcal{M}$.

Choose e so large that every state that $\mathcal{M}$ enters in the course of any computation is entered in a computation of length less than e . Then the a_ν satisfy version (A) of the Theorem.

Conversely, if the a_ν satisfy (A) one can construct a finite automaton $\mathcal{M}$ that generates $\sum a_\nu x^\nu$.

$\mathcal{M}$ will be equipped with a table detailing the identifications (A) and an output list of the values of the a_j for $j = (j_1, \dots, j_n)$ with the $j_i < p^e$.

The automaton $\mathcal{M}$ computes as follows: It reads e digits from each tape. Then it uses the table (A) to replace those e digits by e' digits. It reads a further $e - e'$ digits and iterates. At each stage it outputs the appropriate value from its output list.

So we have:

Theorem. $\sum a_\nu x^\nu \in \mathbb{F}_p[[x]]$ is algebraic if and only if it is generated by a finite automaton.

Corollary. And so: Let f, $g \in \mathbb{F}_p[[x]]$ be algebraic. Then

(i) Every diagonal of f is algebraic, as is every off-diagonal.

(ii) The Hadamard product $f * g$ is algebraic.

(iii) Irrelevance of symbols: Each characteristic series $f^{(i)} = \sum_{a_\nu = i} x^\nu$ is algebraic.

We have already noted that the situation in characteristic zero is very different.

Indeed, in characteristic zero there is a theorem of Polyá –Carleson by which a power series with integer coefficients and radius of convergence 1 is either rational or has the unit circle as a natural boundary. Thus the Mahler functions mentioned here all are transcendental functions.

So we have:

Theorem. $\sum a_\nu x^\nu \in \mathbb{F}_p[[x]]$ is algebraic if and only if it is generated by a finite automaton.

Corollary. And so: Let f, $g \in \mathbb{F}_p[[x]]$ be algebraic. Then

(i) Every diagonal of f is algebraic, as is every off-diagonal.

(ii) The Hadamard product $f * g$ is algebraic.

(iii) Irrelevance of symbols: Each characteristic series $f^{(i)} = \sum_{a_\nu = i} x^\nu$ is algebraic.

We have already noted that the situation in characteristic zero is very different.

Indeed, in characteristic zero there is a theorem of Pólya –Carleson by which a power series with integer coefficients and radius of convergence 1 is either rational or has the unit circle as a natural boundary. Thus the Mahler functions mentioned here all are transcendental functions.

So we have:

Theorem. $\sum a_\nu x^\nu \in \mathbb{F}_p[[x]]$ is algebraic if and only if it is generated by a finite automaton.

Corollary. And so: Let f, $g \in \mathbb{F}_p[[x]]$ be algebraic. Then

(i) Every diagonal of f is algebraic, as is every off-diagonal.

(ii) The Hadamard product $f * g$ is algebraic.

(iii) Irrelevance of symbols: Each characteristic series $f^{(i)} = \sum_{a_\nu = i} x^\nu$ is algebraic.

We have already noted that the situation in characteristic zero is very different.

Indeed, in characteristic zero there is a theorem of Pólya–Carlson by which a power series with integer coefficients and radius of convergence 1 is either rational or has the unit circle as a natural boundary. Thus the Mahler functions mentioned here all are transcendental functions.

So we have:

Theorem. $\sum a_\nu x^\nu \in \mathbb{F}_p[[x]]$ is algebraic if and only if it is generated by a finite automaton.

Corollary. And so: Let f, $g \in \mathbb{F}_p[[x]]$ be algebraic. Then

(i) Every diagonal of f is algebraic, as is every off-diagonal.

(ii) The Hadamard product $f * g$ is algebraic.

(iii) Irrelevance of symbols: Each characteristic series $f^{(i)} = \sum_{a_\nu = i} x^\nu$ is algebraic.

We have already noted that the situation in characteristic zero is very different.

Indeed, in characteristic zero there is a theorem of Polyá–Carleson by which a power series with integer coefficients and radius of convergence 1 is either rational or has the unit circle as a natural boundary. Thus the Mahler functions mentioned here all are transcendental functions.

So we have:

Theorem. $\sum a_\nu x^\nu \in \mathbb{F}_p[[x]]$ is algebraic if and only if it is generated by a finite automaton.

Corollary. And so: Let $f, g \in \mathbb{F}_p[[x]]$ be algebraic. Then

(i) Every diagonal of f is algebraic, as is every off-diagonal.

(ii) The Hadamard product $f * g$ is algebraic.

(iii) Irrelevance of symbols: Each characteristic series $f^{(i)} = \sum_{a_\nu = i} x^\nu$ is algebraic.

We have already noted that the situation in characteristic zero is very different.

Indeed, in characteristic zero there is a theorem of Polyá –Carleson by which a power series with integer coefficients and radius of convergence 1 is either rational or has the unit circle as a natural boundary. Thus the Mahler functions mentioned here all are transcendental functions.

So we have:

Theorem. $\sum a_\nu x^\nu \in \mathbb{F}_p[[x]]$ is algebraic if and only if it is generated by a finite automaton.

Corollary. And so: Let f, $g \in \mathbb{F}_p[[x]]$ be algebraic. Then

(i) Every diagonal of f is algebraic, as is every off-diagonal.

(ii) The Hadamard product $f * g$ is algebraic.

(iii) Irrelevance of symbols: Each characteristic series $f^{(i)} = \sum_{a_\nu = i} x^\nu$ is algebraic.

We have already noted that the situation in characteristic zero is very different.

Indeed, in characteristic zero there is a theorem of Polyá –Carleson by which a power series with integer coefficients and radius of convergence 1 is either rational or has the unit circle as a natural boundary. Thus the Mahler functions mentioned here all are transcendental functions.

So we have:

Theorem. $\sum a_\nu x^\nu \in \mathbb{F}_p[[x]]$ is algebraic if and only if it is generated by a finite automaton.

Corollary. And so: Let $f, g \in \mathbb{F}_p[[x]]$ be algebraic. Then

(i) Every diagonal of f is algebraic, as is every off-diagonal.

(ii) The Hadamard product $f * g$ is algebraic.

(iii) Irrelevance of symbols: Each characteristic series $f^{(i)} = \sum_{a_\nu = i} x^\nu$ is algebraic.

We have already noted that the situation in characteristic zero is very different.

Indeed, in characteristic zero there is a theorem of Polyá –Carleson by which a power series with integer coefficients and radius of convergence 1 is either rational or has the unit circle as a natural boundary. Thus the Mahler functions mentioned here all are transcendental functions.

So we have:

Theorem. $\sum a_\nu x^\nu \in \mathbb{F}_p[[x]]$ is algebraic if and only if it is generated by a finite automaton.

Corollary. And so: Let $f, g \in \mathbb{F}_p[[x]]$ be algebraic. Then

(i) Every diagonal of f is algebraic, as is every off-diagonal.

(ii) The Hadamard product $f * g$ is algebraic.

(iii) Irrelevance of symbols: Each characteristic series $f^{(i)} = \sum_{a_\nu = i} x^\nu$ is algebraic.

We have already noted that the situation in characteristic zero is very different.

Indeed, in characteristic zero there is a theorem of Polyá –Carleson by which a power series with integer coefficients and radius of convergence 1 is either rational or has the unit circle as a natural boundary. Thus the Mahler functions mentioned here all are transcendental functions.

So we have:

Theorem. $\sum a_\nu x^\nu \in \mathbb{F}_p[[x]]$ is algebraic if and only if it is generated by a finite automaton.

Corollary. And so: Let $f, g \in \mathbb{F}_p[[x]]$ be algebraic. Then

(i) Every diagonal of f is algebraic, as is every off-diagonal.

(ii) The Hadamard product $f * g$ is algebraic.

(iii) Irrelevance of symbols: Each characteristic series $f^{(i)} = \sum_{a_\nu = i} x^\nu$ is algebraic.

We have already noted that the situation in characteristic zero is very different.

Indeed, in characteristic zero there is a theorem of Polyá –Carleson by which a power series with integer coefficients and radius of convergence 1 is either rational or has the unit circle as a natural boundary. Thus the Mahler functions mentioned here all are transcendental functions.

The Lifting Theorem

Looking carefully, one sees that every algebraic power series in $\mathbb{F}_p[[x]]$ is the reduction of an algebraic power series in $\mathbb{Z}_p[[x]]$.

Conversely there is an surprising lifting theorem (Loxton and vdP) whereby every algebraic power series in $\mathbb{F}_p[[x]]$ is found to lift to a series in $\mathbb{Z}[[x]]$ which is a solution of a system of functional equations.

Note the example of the Shapiro sequence, where

$$2X(1-X^4)R(X^4)+(1-X^4)(1-X)R(X^2)-(1-X^4)R(X)+X^3=0\,,$$

in characteristic zero, is the lifting of

$$(1+X)^5R^2+(1+X)^4R+X^3=0$$

in characteristic two.

By a theorem of Cobham, a sequence generated by both an r and an s automaton is rational if r and s are multiplicatively independent. It follows that a non-rational formal power series, such as R, that makes sense in any characteristic is algebraic in at most one interpretation and transcendental in all others.

The Lifting Theorem

Looking carefully, one sees that every algebraic power series in $\mathbb{F}_p[[x]]$ is the reduction of an algebraic power series in $\mathbb{Z}_p[[x]]$.

Conversely there is an surprising lifting theorem (Loxton and vdP) whereby every algebraic power series in $\mathbb{F}_p[[x]]$ is found to lift to a series in $\mathbb{Z}[[x]]$ which is a solution of a system of functional equations.

Note the example of the Shapiro sequence, where

$$2X(1-X^4)R(X^4)+(1-X^4)(1-X)R(X^2)-(1-X^4)R(X)+X^3=0\,,$$

in characteristic zero, is the lifting of

$$(1+X)^5R^2+(1+X)^4R+X^3=0$$

in characteristic two.

By a theorem of Cobham, a sequence generated by both an r and an s automaton is rational if r and s are multiplicatively independent. It follows that a non-rational formal power series, such as R, that makes sense in any characteristic is algebraic in at most one interpretation and transcendental in all others.

The Lifting Theorem

Looking carefully, one sees that every algebraic power series in $\mathbb{F}_p[[x]]$ is the reduction of an algebraic power series in $\mathbb{Z}_p[[x]]$.

Conversely there is an surprising lifting theorem (Loxton and vdP) whereby every algebraic power series in $\mathbb{F}_p[[x]]$ is found to lift to a series in $\mathbb{Z}[[x]]$ which is a solution of a system of functional equations.

Note the example of the Shapiro sequence, where

$$2X(1-X^4)R(X^4)+(1-X^4)(1-X)R(X^2)-(1-X^4)R(X)+X^3=0\,,$$

in characteristic zero, is the lifting of

$$(1+X)^5R^2+(1+X)^4R+X^3=0$$

in characteristic two.

By a theorem of Cobham, a sequence generated by both an r and an s automaton is rational if r and s are multiplicatively independent. It follows that a non-rational formal power series, such as R, that makes sense in any characteristic is algebraic in at most one interpretation and transcendental in all others.

The Lifting Theorem

Looking carefully, one sees that every algebraic power series in $\mathbb{F}_p[[x]]$ is the reduction of an algebraic power series in $\mathbb{Z}_p[[x]]$.

Conversely there is an surprising lifting theorem (Loxton and vdP) whereby every algebraic power series in $\mathbb{F}_p[[x]]$ is found to lift to a series in $\mathbb{Z}[[x]]$ which is a solution of a system of functional equations.

Note the example of the Shapiro sequence, where

$$2X(1-X^4)R(X^4)+(1-X^4)(1-X)R(X^2)-(1-X^4)R(X)+X^3=0\,,$$

in characteristic zero, is the lifting of

$$(1+X)^5R^2+(1+X)^4R+X^3=0$$

in characteristic two.

By a theorem of Cobham, a sequence generated by both an r and an s automaton is rational if r and s are multiplicatively independent. It follows that a non-rational formal power series, such as R, that makes sense in any characteristic is algebraic in at most one interpretation and transcendental in all others.

The Lifting Theorem

Looking carefully, one sees that every algebraic power series in $\mathbb{F}_p[[x]]$ is the reduction of an algebraic power series in $\mathbb{Z}_p[[x]]$.

Conversely there is an surprising lifting theorem (Loxton and vdP) whereby every algebraic power series in $\mathbb{F}_p[[x]]$ is found to lift to a series in $\mathbb{Z}[[x]]$ which is a solution of a system of functional equations.

Note the example of the Shapiro sequence, where

$$2X(1-X^4)R(X^4)+(1-X^4)(1-X)R(X^2)-(1-X^4)R(X)+X^3=0\,,$$

in characteristic zero, is the lifting of

$$(1+X)^5R^2+(1+X)^4R+X^3=0$$

in characteristic two.

By a theorem of Cobham, a sequence generated by both an r and an s automaton is rational if r and s are multiplicatively independent. It follows that a non-rational formal power series, such as R, that makes sense in any characteristic is algebraic in at most one interpretation and transcendental in all others.

The Lifting Theorem

Looking carefully, one sees that every algebraic power series in $\mathbb{F}_p[[x]]$ is the reduction of an algebraic power series in $\mathbb{Z}_p[[x]]$.

Conversely there is an surprising lifting theorem (Loxton and vdP) whereby every algebraic power series in $\mathbb{F}_p[[x]]$ is found to lift to a series in $\mathbb{Z}[[x]]$ which is a solution of a system of functional equations.

Note the example of the Shapiro sequence, where

$$2X(1-X^4)R(X^4)+(1-X^4)(1-X)R(X^2)-(1-X^4)R(X)+X^3=0\,,$$

in characteristic zero, is the lifting of

$$(1+X)^5R^2+(1+X)^4R+X^3=0$$

in characteristic two.

By a theorem of Cobham, a sequence generated by both an r and an s automaton is rational if r and s are multiplicatively independent. It follows that a non-rational formal power series, such as R, that makes sense in any characteristic is algebraic in at most one interpretation and transcendental in all others.

Diagonals of Rational Functions

Now consider the class of power series in $\mathbb{Q}[[x]]$ which occur as the diagonals of rational functions $f(x) = P(x)/Q(x)$ with $Q(\underline{0}) \neq 0$.

Every algebraic power series is the diagonal of a rational power series, and every such diagonal is algebraic mod p^s for all s and almost all p.

The complete diagonals of rational power series have many other interesting properties:

Theorem. If $f(x_1)$ is the diagonal of a rational power series over $\mathbb{Q}$

(i) f has positive radius of convergence r_p at every place p of $\mathbb{Q}$ and $r_p = 1$ for almost all p .

(ii) for almost all p the function f is bounded on the disc $D_p(1^-) = \{t \in \mathbb{C}_p : |t| < 1\}$, where $\mathbb{C}_p$ is the completion of the algebraic closure of the p-adic rationals $\mathbb{Q}_p$ and, for almost all p , $\sup\{|f(t)| : t \in D_p(1^-)\} = 1$.

(iii) f satisfies a linear differential equation over $\mathbb{Q}[x_1]$; and

(iv) this equation is a Picard-Fuchs equation.

Diagonals of Rational Functions

Now consider the class of power series in $\mathbb{Q}[[x]]$ which occur as the diagonals of rational functions $f(x) = P(x)/Q(x)$ with $Q(\underline{0}) \neq 0$.

Every algebraic power series is the diagonal of a rational power series, and every such diagonal is algebraic mod p^s for all s and almost all p.

The complete diagonals of rational power series have many other interesting properties:

Theorem. If $f(x_1)$ is the diagonal of a rational power series over $\mathbb{Q}$

(i) f has positive radius of convergence r_p at every place p of $\mathbb{Q}$ and $r_p = 1$ for almost all p .

(ii) for almost all p the function f is bounded on the disc $D_p(1^-) = \{t \in \mathbb{C}_p : |t| < 1\}$, where $\mathbb{C}_p$ is the completion of the algebraic closure of the p-adic rationals $\mathbb{Q}_p$ and, for almost all p , $\sup\{|f(t)| : t \in D_p(1^-)\} = 1$.

(iii) f satisfies a linear differential equation over $\mathbb{Q}[x_1]$; and

(iv) this equation is a Picard-Fuchs equation.

Diagonals of Rational Functions

Now consider the class of power series in $\mathbb{Q}[[x]]$ which occur as the diagonals of rational functions $f(x) = P(x)/Q(x)$ with $Q(\underline{0}) \neq 0$.

Every algebraic power series is the diagonal of a rational power series, and every such diagonal is algebraic mod p^s for all s and almost all p.

The complete diagonals of rational power series have many other interesting properties:

Theorem. If $f(x_1)$ is the diagonal of a rational power series over $\mathbb{Q}$

(i) f has positive radius of convergence r_p at every place p of $\mathbb{Q}$ and $r_p = 1$ for almost all p .

(ii) for almost all p the function f is bounded on the disc $D_p(1^-) = \{t \in \mathbb{C}_p : |t| < 1\}$, where $\mathbb{C}_p$ is the completion of the algebraic closure of the p-adic rationals $\mathbb{Q}_p$ and, for almost all p , $\sup\{|f(t)| : t \in D_p(1^-)\} = 1$.

(iii) f satisfies a linear differential equation over $\mathbb{Q}[x_1]$; and

(iv) this equation is a Picard-Fuchs equation.

Diagonals of Rational Functions

Now consider the class of power series in $\mathbb{Q}[[x]]$ which occur as the diagonals of rational functions $f(x) = P(x)/Q(x)$ with $Q(\underline{0}) \neq 0$.

Every algebraic power series is the diagonal of a rational power series, and every such diagonal is algebraic mod p^s for all s and almost all p.

The complete diagonals of rational power series have many other interesting properties:

Theorem. If $f(x_1)$ is the diagonal of a rational power series over $\mathbb{Q}$

(i) f has positive radius of convergence r_p at every place p of $\mathbb{Q}$ and $r_p = 1$ for almost all p .

(ii) for almost all p the function f is bounded on the disc $D_p(1^-) = \{t \in \mathbb{C}_p : |t| < 1\}$, where $\mathbb{C}_p$ is the completion of the algebraic closure of the p-adic rationals $\mathbb{Q}_p$ and, for almost all p , $\sup\{|f(t)| : t \in D_p(1^-)\} = 1$.

(iii) f satisfies a linear differential equation over $\mathbb{Q}[x_1]$; and

(iv) this equation is a Picard-Fuchs equation.

Diagonals of Rational Functions

Now consider the class of power series in $\mathbb{Q}[[x]]$ which occur as the diagonals of rational functions $f(x) = P(x)/Q(x)$ with $Q(\underline{0}) \neq 0$.

Every algebraic power series is the diagonal of a rational power series, and every such diagonal is algebraic mod p^s for all s and almost all p.

The complete diagonals of rational power series have many other interesting properties:

Theorem. If $f(x_1)$ is the diagonal of a rational power series over $\mathbb{Q}$

(i) f has positive radius of convergence r_p at every place p of $\mathbb{Q}$ and $r_p = 1$ for almost all p .

(ii) for almost all p the function f is bounded on the disc $D_p(1^-) = \{t \in \mathbb{C}_p : |t| < 1\}$, where $\mathbb{C}_p$ is the completion of the algebraic closure of the p-adic rationals $\mathbb{Q}_p$ and, for almost all p , $\sup\{|f(t)| : t \in D_p(1^-)\} = 1$.

(iii) f satisfies a linear differential equation over $\mathbb{Q}[x_1]$; and

(iv) this equation is a Picard-Fuchs equation.

Diagonals of Rational Functions

Now consider the class of power series in $\mathbb{Q}[[x]]$ which occur as the diagonals of rational functions $f(x) = P(x)/Q(x)$ with $Q(\underline{0}) \neq 0$.

Every algebraic power series is the diagonal of a rational power series, and every such diagonal is algebraic mod p^s for all s and almost all p.

The complete diagonals of rational power series have many other interesting properties:

Theorem. If $f(x_1)$ is the diagonal of a rational power series over $\mathbb{Q}$

(i) f has positive radius of convergence r_p at every place p of $\mathbb{Q}$ and $r_p = 1$ for almost all p .

(ii) for almost all p the function f is bounded on the disc $D_p(1^-) = \{t \in \mathbb{C}_p : |t| < 1\}$, where $\mathbb{C}_p$ is the completion of the algebraic closure of the p-adic rationals $\mathbb{Q}_p$ and, for almost all p , $\sup\{|f(t)| : t \in D_p(1^-)\} = 1$.

(iii) f satisfies a linear differential equation over $\mathbb{Q}[x_1]$; and

(iv) this equation is a Picard-Fuchs equation.

Diagonals of Rational Functions

Now consider the class of power series in $\mathbb{Q}[[x]]$ which occur as the diagonals of rational functions $f(x) = P(x)/Q(x)$ with $Q(\underline{0}) \neq 0$.

Every algebraic power series is the diagonal of a rational power series, and every such diagonal is algebraic mod p^s for all s and almost all p.

The complete diagonals of rational power series have many other interesting properties:

Theorem. If $f(x_1)$ is the diagonal of a rational power series over $\mathbb{Q}$

(i) f has positive radius of convergence r_p at every place p of $\mathbb{Q}$ and $r_p = 1$ for almost all p .

(ii) for almost all p the function f is bounded on the disc $D_p(1^-) = \{t \in \mathbb{C}_p : |t| < 1\}$, where $\mathbb{C}_p$ is the completion of the algebraic closure of the p-adic rationals $\mathbb{Q}_p$ and, for almost all p , $\sup\{|f(t)| : t \in D_p(1^-)\} = 1$.

(iii) f satisfies a linear differential equation over $\mathbb{Q}[x_1]$; and

(iv) this equation is a Picard-Fuchs equation.

Diagonals of Rational Functions

Now consider the class of power series in $\mathbb{Q}[[x]]$ which occur as the diagonals of rational functions $f(x) = P(x)/Q(x)$ with $Q(\underline{0}) \neq 0$.

Every algebraic power series is the diagonal of a rational power series, and every such diagonal is algebraic mod p^s for all s and almost all p.

The complete diagonals of rational power series have many other interesting properties:

Theorem. If $f(x_1)$ is the diagonal of a rational power series over $\mathbb{Q}$

(i) f has positive radius of convergence r_p at every place p of $\mathbb{Q}$ and $r_p = 1$ for almost all p .

(ii) for almost all p the function f is bounded on the disc $D_p(1^-) = \{t \in \mathbb{C}_p : |t| < 1\}$, where $\mathbb{C}_p$ is the completion of the algebraic closure of the p-adic rationals $\mathbb{Q}_p$ and, for almost all p , $\sup\{|f(t)| : t \in D_p(1^-)\} = 1$.

(iii) f satisfies a linear differential equation over $\mathbb{Q}[x_1]$; and

(iv) this equation is a Picard-Fuchs equation.

Diagonals of Rational Functions

Now consider the class of power series in $\mathbb{Q}[[x]]$ which occur as the diagonals of rational functions $f(x) = P(x)/Q(x)$ with $Q(\underline{0}) \neq 0$.

Every algebraic power series is the diagonal of a rational power series, and every such diagonal is algebraic mod p^s for all s and almost all p.

The complete diagonals of rational power series have many other interesting properties:

Theorem. If $f(x_1)$ is the diagonal of a rational power series over $\mathbb{Q}$

(i) f has positive radius of convergence r_p at every place p of $\mathbb{Q}$ and $r_p = 1$ for almost all p .

(ii) for almost all p the function f is bounded on the disc $D_p(1^-) = \{t \in \mathbb{C}_p : |t| < 1\}$, where $\mathbb{C}_p$ is the completion of the algebraic closure of the p-adic rationals $\mathbb{Q}_p$ and, for almost all p , $\sup\{|f(t)| : t \in D_p(1^-)\} = 1$.

(iii) f satisfies a linear differential equation over $\mathbb{Q}[x_1]$; and

(iv) this equation is a Picard-Fuchs equation.

Whilst (i) and (ii) are reasonably straightforward, (iii) and (iv) are more difficult and are proved by Deligne using resolution of singularities. Dwork has given a proof which avoids resolution.

An elementary proof of (iii) and its generalisations is given by Lipshitz: Leonard argues so as to show D-finiteness is retained under the taking of diagonals: roughly speaking, the vector space generated by the partial derivatives of an algebraic power series remains finite dimensional. I conclude by mentioning Grothendieck's Conjecture: If a linear homogeneous differential equation with coefficients from $\mathbb{Q}[x_1]$, and of order n, has, for almost all p, n independent solutions in $\mathbb{F}_p[[x_1]]$ then all its solutions are algebraic.

This has been proved in a number of special cases (for example, for Picard-Fuchs equations) by Katz. Some results have also been obtained by elementary methods by Honda.

Whilst (i) and (ii) are reasonably straightforward, (iii) and (iv) are more difficult and are proved by Deligne using resolution of singularities. Dwork has given a proof which avoids resolution.
An elementary proof of (iii) and its generalisations is given by Lipshitz: Leonard argues so as to show D-finiteness is retained under the taking of diagonals: roughly speaking, the vector space generated by the partial derivatives of an algebraic power series remains finite dimensional. I conclude by mentioning Grothendieck's Conjecture: If a linear homogeneous differential equation with coefficients from $\mathbb{Q}[x_1]$, and of order n , has, for almost all p , n independent solutions in $\mathbb{F}_p[[x_1]]$ then all its solutions are algebraic.

This has been proved in a number of special cases (for example, for Picard-Fuchs equations) by Katz. Some results have also been obtained by elementary methods by Honda.

Whilst (i) and (ii) are reasonably straightforward, (iii) and (iv) are more difficult and are proved by Deligne using resolution of singularities. Dwork has given a proof which avoids resolution.

An elementary proof of (iii) and its generalisations is given by Lipshitz: Leonard argues so as to show D-finiteness is retained under the taking of diagonals: roughly speaking, the vector space generated by the partial derivatives of an algebraic power series remains finite dimensional. I conclude by mentioning Grothendieck's Conjecture: If a linear homogeneous differential equation with coefficients from $\mathbb{Q}[x_1]$, and of order n, has, for almost all p, n independent solutions in $\mathbb{F}_p[[x_1]]$ then all its solutions are algebraic.

This has been proved in a number of special cases (for example, for Picard-Fuchs equations) by Katz. Some results have also been obtained by elementary methods by Honda.

References

MICHEL DEKKING, MICHEL MENDÈS FRANCE, and AJvdP, 'FOLDS!', The Mathematical Intelligencer **4** (1982), 130–138; II: 'Symmetry disturbed', *ibid.* 173–181; III: 'More morphisms', *ibid.* 190–195;

LEONARD LIPSHITZ and AJvdP, 'Rational functions, diagonals, automata and arithmetic', in Number Theory (First Conference of the Canadian Number Theory Association, Banff 1988) (Walter de Gruyter Berlin New York, 1990), 339–358; see `http://www-centre.ics.mq.edu.au/alfpapers/a084.pdf`.

JEAN-PAUL ALLOUCHE and JEFFREY SHALLIT, Automatic Sequences, Cambridge UP, 2003.

Essentially the present talk can be found on my website.

References

Michel Dekking, Michel Mendès France, and AJvdP, 'FOLDS!', The Mathematical Intelligencer **4** (1982), 130–138; II: 'Symmetry disturbed', *ibid.* 173–181; III: 'More morphisms', *ibid.* 190–195;

Leonard Lipshitz and AJvdP, 'Rational functions, diagonals, automata and arithmetic', in Number Theory (First Conference of the Canadian Number Theory Association, Banff 1988) (Walter de Gruyter Berlin New York, 1990), 339–358; see
`http://www-centre.ics.mq.edu.au/alfpapers/a084.pdf`.

Jean-Paul Allouche and Jeffrey Shallit, Automatic Sequences, Cambridge UP, 2003.

Essentially the present talk can be found on my website.

References

Michel Dekking, Michel Mendès France, and AJvdP, 'FOLDS!', The Mathematical Intelligencer **4** (1982), 130–138; II: 'Symmetry disturbed', *ibid.* 173–181; III: 'More morphisms', *ibid.* 190–195;

Leonard Lipshitz and AJvdP, 'Rational functions, diagonals, automata and arithmetic', in Number Theory (First Conference of the Canadian Number Theory Association, Banff 1988) (Walter de Gruyter Berlin New York, 1990), 339–358; see `http://www-centre.ics.mq.edu.au/alfpapers/a084.pdf`.

Jean-Paul Allouche and Jeffrey Shallit, Automatic Sequences, Cambridge UP, 2003.

Essentially the present talk can be found on my website.

References

Michel Dekking, Michel Mendès France, and AJvdP, 'FOLDS!', The Mathematical Intelligencer **4** (1982), 130–138; II: 'Symmetry disturbed', *ibid.* 173–181; III: 'More morphisms', *ibid.* 190–195;

Leonard Lipshitz and AJvdP, 'Rational functions, diagonals, automata and arithmetic', in Number Theory (First Conference of the Canadian Number Theory Association, Banff 1988) (Walter de Gruyter Berlin New York, 1990), 339–358; see `http://www-centre.ics.mq.edu.au/alfpapers/a084.pdf`.

Jean-Paul Allouche and Jeffrey Shallit, Automatic Sequences, Cambridge UP, 2003.

Essentially the present talk can be found on my website.

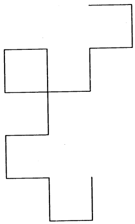
JURASSIC PARK

A NOVEL BY

MICHAEL CRICHTON

ALFRED A. KNOPF *New York*

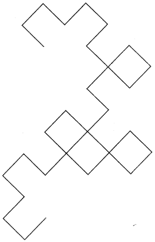
FIRST ITERATION



"At the earliest drawings of the fractal curve, few clues to the underlying mathematical structure will be seen."

IAN MALCOLM

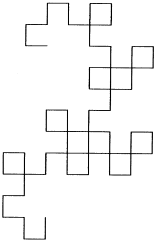
SECOND ITERATION



"With subsequent drawings of the fractal curve, sudden changes may appear."

IAN MALCOLM

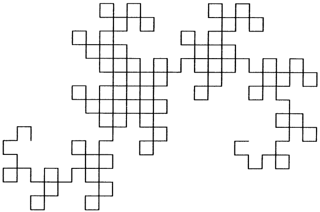
THIRD ITERATION



"Details emerge more clearly as the fractal curve is redrawn."

IAN MALCOLM

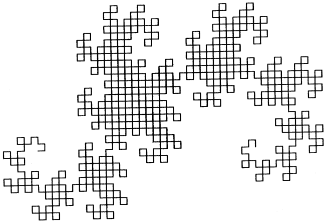
FOURTH ITERATION



"Inevitably, underlying instabilities begin to appear."

IAN MALCOLM

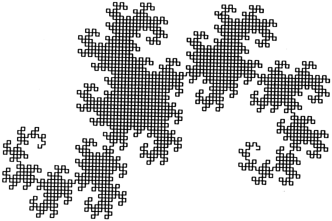
FIFTH ITERATION



"Flaws in the system will now become severe."

IAN MALCOLM

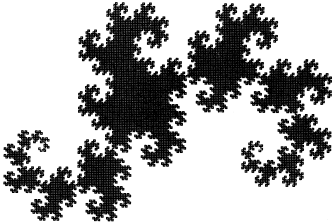
SIXTH ITERATION



"System recovery may prove impossible."

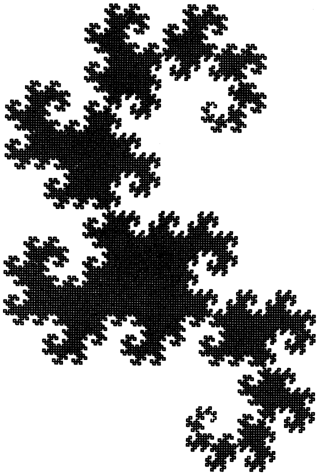
IAN MALCOLM

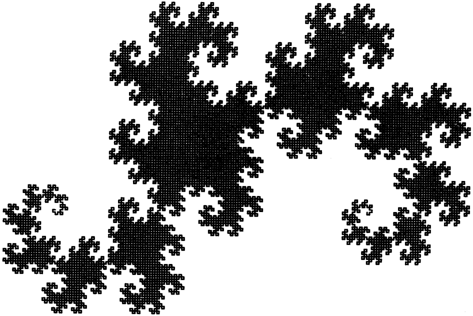
SEVENTH ITERATION

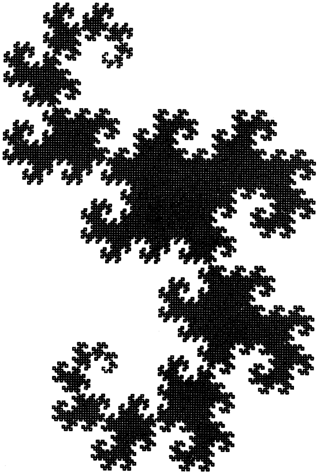


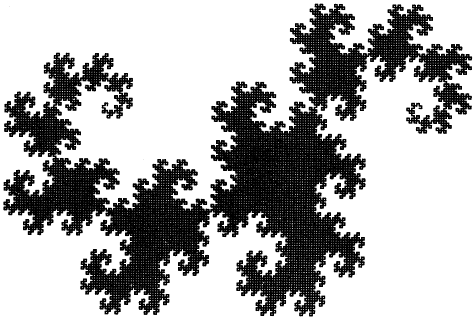
"Increasingly, the mathematics will demand the courage to face its implications."

IAN MALCOLM









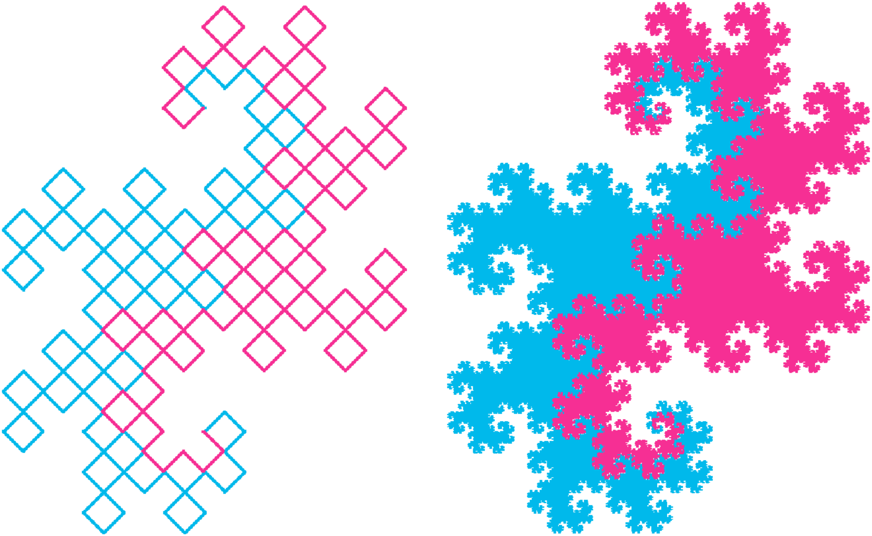


Plate 5

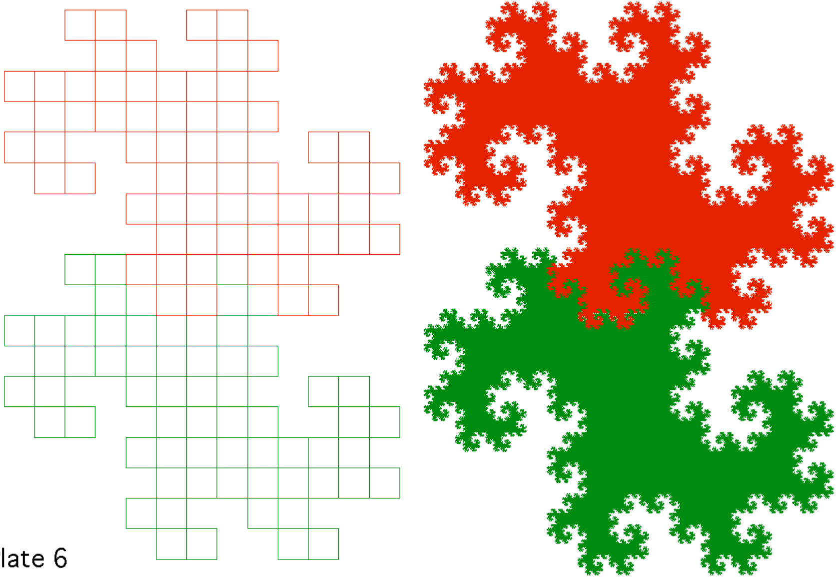


Plate 6

References

MICHEL DEKKING, MICHEL MENDÈS FRANCE, and AJvdP, 'FOLDS!', The Mathematical Intelligencer **4** (1982), 130–138; II: 'Symmetry disturbed', *ibid.* 173–181; III: 'More morphisms', *ibid.* 190–195;

LEONARD LIPSHITZ and AJvdP, 'Rational functions, diagonals, automata and arithmetic', in Number Theory (First Conference of the Canadian Number Theory Association, Banff 1988) (Walter de Gruyter Berlin New York, 1990), 339–358; see http://www-centre.ics.mq.edu.au/alfpapers/a084.pdf.

JEAN-PAUL ALLOUCHE and JEFFREY SHALLIT, Automatic Sequences, Cambridge UP, 2003.

Essentially the present talk can be found on my website at http://www.maths.mq.edu.au/~alf/automata.pdf

References

MICHEL DEKKING, MICHEL MENDÈS FRANCE, and AJvdP, 'FOLDS!', The Mathematical Intelligencer **4** (1982), 130–138; II: 'Symmetry disturbed', *ibid.* 173–181; III: 'More morphisms', *ibid.* 190–195;

LEONARD LIPSHITZ and AJvdP, 'Rational functions, diagonals, automata and arithmetic', in Number Theory (First Conference of the Canadian Number Theory Association, Banff 1988) (Walter de Gruyter Berlin New York, 1990), 339–358; see
`http://www-centre.ics.mq.edu.au/alfpapers/a084.pdf`.

JEAN-PAUL ALLOUCHE and JEFFREY SHALLIT, Automatic Sequences, Cambridge UP, 2003.

Essentially the present talk can be found on my website at
`http://www.maths.mq.edu.au/~alf/automata.pdf`

References

MICHEL DEKKING, MICHEL MENDÈS FRANCE, and AJvdP, 'FOLDS!', The Mathematical Intelligencer **4** (1982), 130–138; II: 'Symmetry disturbed', *ibid.* 173–181; III: 'More morphisms', *ibid.* 190–195;

LEONARD LIPSHITZ and AJvdP, 'Rational functions, diagonals, automata and arithmetic', in Number Theory (First Conference of the Canadian Number Theory Association, Banff 1988) (Walter de Gruyter Berlin New York, 1990), 339–358; see `http://www-centre.ics.mq.edu.au/alfpapers/a084.pdf`.

JEAN-PAUL ALLOUCHE and JEFFREY SHALLIT, Automatic Sequences, Cambridge UP, 2003.

Essentially the present talk can be found on my website at `http://www.maths.mq.edu.au/~alf/automata.pdf`

References

MICHEL DEKKING, MICHEL MENDÈS FRANCE, and AJvdP, 'FOLDS!', The Mathematical Intelligencer **4** (1982), 130–138; II: 'Symmetry disturbed', *ibid.* 173–181; III: 'More morphisms', *ibid.* 190–195;

LEONARD LIPSHITZ and AJvdP, 'Rational functions, diagonals, automata and arithmetic', in Number Theory (First Conference of the Canadian Number Theory Association, Banff 1988) (Walter de Gruyter Berlin New York, 1990), 339–358; see `http://www-centre.ics.mq.edu.au/alfpapers/a084.pdf`.

JEAN-PAUL ALLOUCHE and JEFFREY SHALLIT, Automatic Sequences, Cambridge UP, 2003.

Essentially the present talk can be found on my website at `http://www.maths.mq.edu.au/~alf/automata.pdf`