THE MESIROV–SWEET PROPERTY OVER $\mathbb{F}_2$ UP TO DEGREE 33, WITH TWO QUOTIENTS OF DEGREE TWO UP TO DEGREE 28

DAVID NIEDBALA GIRAUDIN

ABSTRACT. For a monic polynomial $g \in \mathbb{F}_2[T]$ of degree d, the conjecture of Mesirov and Sweet asserts that there is $f \in \mathbb{F}_2[T]$, coprime to g with $\deg f < d$, such that every partial quotient of the continued fraction of f/g has degree at most 2. We check by exhaustive computation that this holds for every g of degree at most 33. We also check that for every g of degree at most 28 one can choose f so that all partial quotients are linear except at most two, which have degree 2. The computations combine exhaustive enumeration of fixed degree patterns, explicit certificates for the polynomials not reached by the patterns, and two separately written enumeration programs whose outputs coincide bit for bit. All programs are provided.

hexagon:2611.00220v1

1. STATEMENTS

For $a_1, \dots, a_r \in \mathbb{F}_2[T]$ let $K(a_1, \dots, a_r)$ denote the continuant, so that

$$[0; a_1, \dots, a_r] = \frac{K(a_2, \dots, a_r)}{K(a_1, \dots, a_r)} \quad \text{in lowest terms.}$$

Every pair (f, g) with g monic, $\gcd(f, g) = 1$ and $\deg f < \deg g$ arises from exactly one sequence of non-constant quotients, and $\deg g = \sum_i \deg a_i$.

Conjecture 1 (Mesirov–Sweet [2]; [1, Conj. 3.6])**.** *For every monic $g \in \mathbb{F}_2[T]$ of degree $d \geq 1$ there is f with $\gcd(f, g) = 1$, $\deg f < d$, such that all partial quotients of f/g have degree ≤ 2.*

The bound 2 cannot be lowered: $T^2 + T$ has no admissible f with linear quotients only. For irreducible g Mesirov and Sweet proved that all quotients can be taken linear [2]; for general g the best known bound grows like $\log d$ [3]. For an admissible g let $k(g)$ be the least number of quotients of degree 2 among the f of Conjecture 1.

Theorem 1 (verified by computation)**.** *Conjecture 1 holds for every monic $g \in \mathbb{F}_2[T]$ with $1 \leq \deg g \leq 33$.*

Theorem 2 (verified by computation)**.** *For every monic $g \in \mathbb{F}_2[T]$ with $1 \leq \deg g \leq 28$ one has $k(g) \leq 2$.*

Theorem 2 gives Theorem 1 for $d \leq 28$; the degrees $29 \leq d \leq 33$ are treated separately. Table 2 records the number of g with $k(g) = 2$.

2. METHOD

Cells. A *cell* is a finite sequence $\pi = (e_1, \dots, e_r)$ with $e_i \in \{1, 2\}$ and $\sum e_i = d$. Since every polynomial of degree e over $\mathbb{F}_2$ is monic, the cell carries exactly $\prod_i 2^{e_i} = 2^d$ quotient sequences, and we write $I_\pi \subseteq \mathbb{F}_2[T]$ for the set of their continuants. The pure cell $(1, \dots, 1)$ is the one of Mesirov and Sweet; $k(g) \leq j$ if and only if g lies in I_π for some cell with at most j entries equal to 2.

Date: November 7, 2026.

Two enumerations. Program A runs through each cell depth first, appending quotients on the right and updating the pair $(K(a_1,\dots,a_i), K(a_1,\dots,a_{i-1}))$. Program B was written separately: it runs through the same sequences in a different order (the first quotient varies fastest) and evaluates the continuants by the recurrence in the opposite direction. Both mark the images in a bitmap indexed by the d low coefficients of g.

Certificates. For the g outside the union of the cells, an explicit f is produced and then checked by a third program, which runs the Euclidean algorithm on (g, f) from scratch and verifies $\deg g = d$, $\deg f < d$, that every quotient has degree 1 or 2 (and, for Theorem 2, that at most two have degree 2), and that the last non-zero remainder is 1.

Search for certificates. For g outside the union of the cells, f is searched for by a meet-in-the-middle procedure resting on two classical identities: for $1 \le j < r$,

$$K(a_1,\dots,a_r) = K(a_1,\dots,a_j)\,K(a_{j+1},\dots,a_r) + K(a_1,\dots,a_{j-1})\,K(a_{j+2},\dots,a_r),$$

and, in characteristic 2, $K(a_1,\dots,a_j)K(a_2,\dots,a_{j-1}) + K(a_1,\dots,a_{j-1})K(a_2,\dots,a_j) = 1$. Fix a cut degree c ($c = 17$ for $d = 33$, $c = \lfloor d/2 \rfloor$ for $29 \le d \le 32$) and a random sample of 2^{20} prefixes $(a_1,\dots,a_j)$ with $\sum_{i\le j} \deg a_i = c$ and all degrees in $\{1, 2\}$. For each prefix put $q = K(a_1,\dots,a_j)$, $q' = K(a_1,\dots,a_{j-1})$, $\rho = K(a_2,\dots,a_j)$, $\rho' = K(a_2,\dots,a_{j-1})$. The second identity gives $q'\rho \equiv 1 \pmod q$, so a suffix with $V = K(a_{j+2},\dots,a_r)$ of degree $< c$ must be $V = g\rho \bmod q$, and then $U = K(a_{j+1},\dots,a_r) = (g - q'V)/q$. The candidate is kept when $\deg U = d - c$ and the Euclidean algorithm on (U, V) produces quotients of degree 1 or 2 only and ends with 1; then $f = \rho U + \rho' V$. If the sample fails, all prefixes at the cuts c and $c+1$ are tried. Certificates are accepted only after the independent check described above, so the search needs no correctness argument of its own.

3. Results

Theorem 1. For each $d \in \{29,\dots,33\}$ ten cells with four entries equal to 2 were drawn at random (they are listed in the ancillary files). Table 1 gives the size of the complement of their union and the outcome of the certificate search. Programs A and B produced identical bitmaps for every d, and every certificate passed the independent check. Together with Theorem 2, this gives Conjecture 1 for every $d \le 33$.

d	not reached by the cells	share	fallback searches	certificates rejected	A=B
29	2 015 190	0.375%	0	0	yes
30	4 020 219	0.374%	0	0	yes
31	8 051 860	0.375%	0	0	yes
32	16 187 206	0.377%	0	0	yes
33	32 430 306	0.378%	0	0	yes

Table 1. Ten random cells with four entries 2 per degree; every g outside their union received a certificate.

Theorem 2. For $d \le 5$ every g has $k(g) \le 1$. For $6 \le d \le 28$, program A covers all 2^d polynomials with the cells having at most two entries equal to 2. The set $L_1(d)$ of polynomials not reached by the cells with at most one entry equal to 2 was computed by A and by B, with identical results, and B produced for each $g \in L_1(d)$ an f with exactly two quotients of degree 2, accepted by the independent check. Since $|L_1(d)| = \#\{g : k(g) = 2\}$, the counts in Table 2 are exact.

Remark 1. The share of g with $k(g) = 2$ decreases for $12 \le d \le 28$, from 0.0269 to 0.0065, and the ratio $\#\{g : k(g) = 2\}$ between consecutive even degrees is close to 3.27 for $22 \le d \le 28$.

Question. Is $k(g) \le 2$ for every monic $g \in \mathbb{F}_2[T]$? An affirmative answer implies Conjecture 1.

d	$\#\{g : k(g) = 2\}$	share	d	$\#\{g : k(g) = 2\}$	share
1	0	0.0000	15	756	0.0231
2	0	0.0000	16	1 364	0.0208
3	0	0.0000	17	2 524	0.0193
4	0	0.0000	18	4 582	0.0175
5	0	0.0000	19	8 322	0.0159
6	3	0.0469	20	14 974	0.0143
7	4	0.0312	21	27 440	0.0131
8	4	0.0156	22	50 069	0.0119
9	16	0.0312	23	90 076	0.0107
10	19	0.0186	24	163 599	0.0098
11	48	0.0234	25	295 916	0.0088
12	110	0.0269	26	535 199	0.0080
13	216	0.0264	27	967 956	0.0072
14	419	0.0256	28	1 748 470	0.0065

TABLE 2. Number of monic g of degree d with $k(g) = 2$; all other g have $k(g) \leq 1$.

4. Ancillary files

The folder `anc` contains: `c_sources.py`, which writes out the C sources of programs A and B, of the certificate search, of the checker and of the small-degree enumeration, together with the run scripts and a description of the file formats; the cell lists `cells_d29.csv`, ..., `cells_d33.csv`; the logs of the runs; and `verif_ms_f2.py` (Python with numpy only), which repeats the exhaustive computation of the counts $\#\{g : k(g) = j\}$, $j = 0, 1, 2$, in degree 18, 20 or 22 (according to a memory budget set in the file) and checks the samples `certs_d28_two_insertions.csv` and `certs_d33_sample.csv` of 10^5 certificates each, together with a control on corrupted certificates. Polynomials are written as integers whose binary digits are their coefficients.

References

[1] A. G. B. Lauder, *Continued fractions and sequences*, PhD thesis, University of London, 1999.

[2] J. P. Mesirov and M. M. Sweet, Continued fraction expansions of rational expressions with irreducible denominators in characteristic 2, *J. Number Theory* **27** (1987), 144–148.

[3] H. Niederreiter, Rational functions with partial quotients of small degree in their continued fraction expansion, *Monatsh. Math.* **103** (1987), 269–288.

ORCID 0009-0009-1526-1178