

## THE STATISTICS OF CONTINUED FRACTIONS FOR POLYNOMIALS OVER A FINITE FIELD

CHRISTIAN FRIESEN AND DOUG HENSLEY

(Communicated by William W. Adams)

ABSTRACT. Given a finite field  $F$  of order  $q$  and polynomials  $a, b \in F[X]$  of degrees  $m < n$  respectively, there is the continued fraction representation  $b/a = a_1 + 1/(a_2 + 1/(a_3 + \cdots + 1/a_r))$ . Let  $CF(n, k, q)$  denote the number of such pairs for which  $\deg b = n$ ,  $\deg a < n$ , and for  $1 \leq j \leq r$ ,  $\deg a_j \leq k$ . We give both an exact recurrence relation, and an asymptotic analysis, for  $CF(n, k, q)$ . The polynomial associated with the recurrence relation turns out to be of P-V type.

We also study the distribution of  $r$ . Averaged over all  $a$  and  $b$  as above, this presents no difficulties. The average value of  $r$  is  $n(1 - 1/q)$ , and there is full information about the distribution. When  $b$  is fixed and only  $a$  is allowed to vary, we show that this is still the average. Moreover, few pairs give a value of  $r$  that differs from this average by more than  $O(\sqrt{n/q})$ .

### 1. INTRODUCTION

Run the Euclidean algorithm on a random pair of polynomials over a finite field. How many quotient-and-remainder iterations (steps) will it take? What will be the maximal partial quotient degree along the way? How much are these numbers likely to vary from one pair to the next? We have some answers. They involve recurrence relations, Pisot-Vijayaraghavan numbers, and the ubiquitous Gaussian distribution.

Our answers to these counting questions turn out to be a close fit for what is known about the ‘continuous’ case. The usual construction of real numbers as a sum  $\sum_{k=-n}^{\infty} a_k 2^{-k}$ , where  $a_k \in \{0, 1\}$  and  $n$  is an integer, has a natural analog for  $\mathcal{F}_q$ . In [6] Niederreiter works with formal Laurent series of the form  $\sum_{k=-n}^{\infty} a_k x^{-k}$ , where  $a_k \in \mathcal{F}_q$ . In this setting, there are natural analogues to the real-number continued fraction expansion, to the usual measure on  $[0, 1]$ , and so on. For instance, with probability 1, the limit of the average value of the degrees of the first  $n$  continued fraction partial quotients, as  $n \rightarrow \infty$ , is  $q/(q - 1)$ . In this setting, there is also a central limit theorem and a law of the iterated logarithm. The cases Integers,  $\mathcal{F}_q[x]$ , Reals, and Laurent over  $\mathcal{F}_q$ , then, form a ‘square’, and we are looking at the second of these four corners, opposite Reals.

Assume the field has order  $q$  and the polynomials, degree  $n$ . As a consequence of our main theorems, it follows readily that the number of steps will probably be

---

Received by the editors August 20, 1994 and, in revised form, March 27, 1995.  
1991 *Mathematics Subject Classification*. Primary 11A55.

$n(1 - 1/q) + O\left(\sqrt{n(q-1)/q^2}\right)$  and that the largest partial quotient degree will probably be close to  $\log n / \log(q - 1)$ . We hope this whets the reader’s zeal, for we must now establish some terminology.

Let  $\mathcal{F}_q$  be the finite field with  $q$  elements, where  $q$  is a positive power of some prime  $p$ . Let  $\mathcal{F}_q[X]$  be the set of polynomials in the indeterminate  $X$  with coefficients in  $\mathcal{F}_q$ .

Given nonzero polynomials  $a, b \in \mathcal{F}_q[X]$  with  $\deg a > \deg b$  and  $(a, b) = 1$ , there exists a unique sequence  $\bar{a} = (a_1, a_2, \dots, a_r) \in \mathcal{F}_q[X]^r$  of polynomials of positive degree such that

$$\frac{a}{b} = a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots + \frac{1}{a_{r-1} + \frac{1}{a_r}}}}$$

Conversely, given a sequence  $\bar{a}$ , the values of the corresponding  $a$  and  $b$  are determined up to scalar multiplication by an arbitrary nonzero element of  $\mathcal{F}_q$ . We write  $[a_1, a_2, \dots, a_r]$  for this continued fraction expansion, and  $\langle a_1, a_2, \dots, a_r \rangle$  for its numerator. With this notation, the denominator is  $\langle a_2, \dots, a_r \rangle$ . The total degree of such an expansion is defined as the sum of the degrees of the partial quotients  $a_1, a_2, \dots$ , and the length  $r(a, b)$  is the value of  $r$  in the expansion, that is, the number of partial quotients.

The statistics of which we speak include the following, the first few being quite simple, but basic to the more challenging ones:

- (1) The number of relatively prime pairs  $(a, b) \in \mathcal{F}_q[X] \times \mathcal{F}_q[X]$  for which  $1 \leq \deg b < \deg a = n$ .
- (2) The number of continued fraction sequences corresponding to pairs counted in (1) above.
- (3) The distribution of  $r(a, b)$  over all  $(a, b)$  with  $\deg b < \deg a = n$  and with  $a$  and  $b$  relatively prime.
- (4) The distribution of  $\max_{1 \leq j \leq r(a,b)} \deg a_j$  as  $a$  ranges over all polynomials in  $\mathcal{F}_q[X]$  of degree  $n$ , and  $b$ , over all those of degree less than  $n$  and relatively prime to  $a$ .
- (5) For a fixed polynomial  $a \in \mathcal{F}_q[X]$  of degree  $n$ , the distribution of  $r(a, b)$  as  $b$  ranges over nonzero polynomials in  $\mathcal{F}_q[X]$  of degree less than  $n$  and relatively prime to  $a$ .

The counting arguments needed for (1) through (3) are fairly simple, and may well have appeared somewhere as an exercise. We make no claim to novelty for them. The results we dignify with the appellation ‘theorem’ have to do with statistics (4) and (5). For (4), it turns out that there is a recurrence relation, and an associated  $k \times k$  matrix, both independent of  $n$ , for

$$F(n, k, q) := \#\{(a_1, a_2, \dots, a_r) : r \geq 1, a_j \in \mathcal{F}_q[X] \text{ with } 1 \leq \deg a_j \leq k \ \forall j \leq r, \text{ and } \sum_1^r \deg a_j = n\}.$$

The characteristic polynomial of this matrix is

$$f(z) = f_{k,q}(z) = z^k - (q-1) \sum_{j=0}^{k-1} z^j.$$

Since  $f(z)$  is monic and has integer coefficients, its roots are algebraic integers. The main root of a recursion dominates its asymptotics, and so statistic (4) is basically governed by  $\lambda = \lambda(k, q)$ , the principal root of  $f(z)$ . Let  $C(k, q) := \frac{\lambda-1}{\lambda-k(q-\lambda)}$ . Our first main result is

**Theorem 1.** *For all integers  $q, k > 1$ ,  $\lambda(k, q)$  is a Pisot-Vijayaraghavan number. All but one root of  $f_{k,q}(z) = 0$  lies within the unit circle in the complex plane. The main root  $\lambda(k, q)$  is real and greater than 1. Furthermore,  $\lambda(k, q) \in [q - q^{1-k} + q^{-k} - kq^{1-2k}, q - q^{1-k} + q^{-k})$  and all the roots are distinct.*

*Remark 1.* The case  $q = 2$  of this theorem is found in Chapter 2, Lemma 2.3 of Hua and Wang [3].

*Remark 2.* For  $k = 1$ , the inequality above holds with  $\lambda(1, q) = q - 1$ . For general  $k$  and  $q$  the inequality could be sharpened indefinitely with the same techniques used in our proof, as  $k$  grows. The details are left as an exercise for readers equipped with a diligent computer algebra system.

The results of this analysis of  $\lambda(k, q)$  are then fed into the standard theory of linear recurrences to obtain an estimate for  $F(n, k, q)$ . This gives

**Theorem 2.** *For all prime powers  $q$ , for all positive integers  $k$ , and for all integers  $n > k$ ,*

$$|F(n, k, q) - C(k, q)q^n \lambda^n(k, q)| \leq \frac{2}{3}q^n.$$

*Furthermore, for  $k > 1$ ,  $C(k, q) \in (1 - q^{-1} - kq^{-k}, 1 - q^{-1})$ .*

The remaining statistic is essentially equivalent to the distribution of the length of finite continued fraction sequences of the form  $(a_1, a_2, \dots)$  for which the numerator  $\langle a_1, a_2, \dots \rangle = \alpha a$  for some  $\alpha \in \mathcal{F}_q$ . Were it not for the condition  $\langle a_1, a_2, \dots \rangle = \alpha a$ , this question would reduce to (3). The number of continued fraction sequences with total degree  $n$  and length  $r$ , when  $1 \leq r \leq n$ , is  $\binom{n-1}{r-1}(q-1)^r q^n$ . From the central limit theorem, most of these have  $r$  close to  $1 + (q-1)(n-1)q^{-2}$ , give or take something comparable to the standard deviation  $\text{Sdv} = \sqrt{(n-1)(q-1)/q^2}$ . In more detail, the fraction of those lying outside  $\pm z \text{Sdv}$  is  $\ll \exp(-\frac{1}{2}z^2)$ , over a reasonably wide range of values of  $z$ . Our main result in the last section is that the same sort of estimate holds when attention is restricted to continued fraction sequences for which  $\langle \bar{a} \rangle = \alpha a$ , but with  $\frac{1}{4}$  in place of  $\frac{1}{2}$  above as a coefficient in  $\exp(-\#z^2)$ . The loss of accuracy occurs in the course of arguing to the effect that a continued fraction sequence has a front and back half, (an old idea of Heilbronn [1]) and that neither is likely to have an atypical number of terms. Short runs of random trials have proportionately higher deviations, and we are forced to add the two deviations.

## 2. PRELIMINARIES AND NOTATION

A finite field is determined up to isomorphism by its order, which must be a prime power. Accordingly, let  $\mathcal{F}_q$  denote ‘the’ finite field of order  $q$ , where  $q = p^\#$

is a prime taken to some positive integer power. Let  $\mathcal{F}_q[X]$  denote the set of polynomials in the formal variable  $X$  over  $\mathcal{F}_q$ . Given  $a, b \in \mathcal{F}_q[X]$  with  $(a, b) = 1$  and  $\deg a > \deg b$ , let  $\text{cfx}(a, b)$  denote the sequence  $(a_1, a_2, \dots, a_r)$  of polynomials in  $\mathcal{F}_q[X]$  of positive degree so that  $b/a = 1/(a_1 + (1/(a_2 + (1/a_3 + (1/\dots 1/a_r))))))$ . Let  $[a_1, a_2, \dots, a_r]$  denote this fraction, and  $\langle a_1, a_2, \dots, a_r \rangle$  its denominator. As mentioned before, then  $\langle a_2, \dots, a_r \rangle$  is the numerator, and if  $a = \langle a_1, a_2, \dots, a_r \rangle$  and  $b = \langle a_2, \dots, a_r \rangle$  then  $r(a, b) = r$ . The correspondence between relatively prime pairs  $(a, b)$  with  $\deg a > \deg b$  and sequences  $\bar{a}$  is  $(q - 1)$  to 1. More precisely, if  $\bar{a} = \text{cfx}(a, b)$ , then there exists a unique  $\alpha \neq 0 \in \mathcal{F}_q$  so that  $\alpha a = \langle \bar{a} \rangle$  and  $ab = \langle a_2, \dots, a_r \rangle$ . Let  $\deg \bar{a} = \sum_{j=1}^{r(\bar{a})} \deg a_j = \deg \langle \bar{a} \rangle$ . Let

$$\begin{aligned} CF(n, q) &:= \{ \bar{a} : a_j \in \mathcal{F}_q[X], \deg a_j \geq 1 \text{ for } 1 \leq j \leq r(\bar{a}), \text{ and } \deg \bar{a} = n \}, \\ CFA(a, q) &:= \{ \bar{a} : \bar{a} \in CF(\deg a, q) \text{ and } \langle \bar{a} \rangle = \alpha a, \alpha \neq 0 \in \mathcal{F}_q \}, \\ CFN(n, k, q) &:= \{ \bar{a} \in CF(n, q) : \deg a_j \leq k \text{ for } 1 \leq j \leq r(\bar{a}) \}, \\ CFR(n, r, q) &:= \{ \bar{a} \in CF(n, q) : r(\bar{a}) = r \}, \\ F(n, k, q) &:= \#CFN(n, k, q), \\ F(n, q) &:= F(n, n, q). \end{aligned}$$

**Lemma 2.1.**  $\#CFR(n, r, q) = \binom{n-1}{r-1} (q - 1)^r q^n$  for  $n \geq r \geq 1$ .

*Proof.* There are  $(q - 1)q^j$  polynomials in  $\mathcal{F}_q[X]$  of degree  $j$ . Thus for any degree sequence  $\bar{j} = j_1, j_2, \dots, j_r$  specifying the degree of each  $a_j$  of an  $\bar{a} \in CFR(n, r, q)$ , there are  $(q - 1)^r q^n$  polynomials in  $CFR(n, r, q)$  matching that degree sequence. The number of sequences  $\bar{j}$  of  $r$  positive integers summing to  $n$ , though, is equal to the number of subsets of  $\{1, 2, \dots, n - 1\}$  with  $r - 1$  elements via the correspondence  $(j_1, j_2, \dots, j_r) \rightarrow \{j_1, j_1 + j_2, \dots, j_1 + j_2 + \dots + j_r\}$ . A similar result is proved in a paper by Knopfmacher [4].

If we sum  $CFR(n, r, q)$  over all possible values of  $r$  we obtain

$$F(n, q) = \sum_{r=1}^n \#CFR(n, r, q) = \sum_{r=1}^n \binom{n-1}{r-1} (q - 1)^r q^n = (q - 1)q^{2n-1}$$

thus proving the

**Corollary 2.2.**  $F(n, q) = (q - 1)q^{2n-1}$  for all  $n \geq 1$ .

**Lemma 2.3.**

$$F(n, k, q) = (q - 1) \sum_{i=1}^k q^i F(n - i, k, q) \quad \text{for } n > k.$$

*Proof.* We separate off the first partial quotient of degree 1, 2, ..., or  $k$  and recognize that there are  $(q - 1)q^i$  polynomials of degree  $i$  possible for the first partial quotient and  $F(n - i, k, q)$  possible continuations giving

$$F(n, k, q) = \sum_{i=1}^k (q - 1)q^i F(n - i, k, q),$$

as required.

## 3. CONTINUED FRACTIONS WITH BOUNDED PARTIAL QUOTIENT DEGREES

In this section we fix  $k$  and  $q$ . Unless specifically noted, quantities in the text should be deemed to have these as implicit parameters. The recurrence relation of Lemma 2.3 implies that

$$\begin{pmatrix} q^{-(n+1)}F(n+1, k, q) \\ q^{-(n+2)}F(n+2, k, q) \\ \cdots \\ \cdots \\ q^{-(n+k)}F(n+k, k, q) \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 \\ q-1 & q-1 & q-1 & \cdots & q-1 \end{pmatrix} \begin{pmatrix} q^{-n}F(n, k, q) \\ q^{-(n+1)}F(n+1, k, q) \\ \cdots \\ \cdots \\ q^{-(n+k-1)}F(n+k-1, k, q) \end{pmatrix}$$

The above  $k$ -by- $k$  matrix, which we shall denote by  $M$  has as characteristic polynomial  $f(z) = z^k - (q-1)(z^{k-1} + z^{k-2} + \cdots + z + 1)$ . This polynomial, regardless of whether or not the integer  $q > 1$  is a prime or prime power, has for its main zero a Pisot-Vijayaraghavan number. This is an algebraic integer  $\lambda > 1$  so that all algebraic conjugates of  $\lambda$  have absolute value less than 1. Equivalently, the fractional part of  $\lambda^k$  tends to zero exponentially with  $k$ . This, of course, is very good news for our estimates of  $F(n, k, q)$ . We thank the referee for pointing out that the special case  $q = 2$  is described by Hua and Wang [3].

We preface our proof of the general case of Theorem 1 by first disposing of the special case  $k = 2$ . It is a straightforward calculation to show that  $f(z)$  evaluated at the left endpoint is  $-4q^{-3} + 5q^{-4} - 4q^{-5} + 4q^{-6} < 0$  and that at the right endpoint  $f(z) = 2q^{-2} - 2q^{-3} + q^{-4} > 0$  from which we conclude that  $\lambda$  belongs to the interval under consideration.

For the remainder of the argument we shall take  $k > 2$ . We start by showing that there is a real root in the desired interval. Since  $z > 1$  on the interval we will multiply  $f(z)$  by  $(z-1)$  to arrive at  $(z-1)f(z) = q-1 - (q-z)z^k$  and it will suffice to show that  $q-1 - (q-z)z^k$  has opposite signs at the interval endpoints. Let  $z = q - q^{-k+1} + q^{-k} - kq^{-2k+1} = q(1 - q^{-k} + q^{-k-1} - kq^{-2k})$ . Then  $z^k = q^k(1 - q^{-k} + q^{-k-1} - kq^{-2k})^k$ . Now

$$\begin{aligned} (1 - q^{-k} + q^{-k-1} - kq^{-2k})^k &= \sum_{i=0}^k \binom{k}{i} (-1)^i (q^{-k} + q^{-k-1} - kq^{-2k})^i \\ &= \sum_{i=0}^k \binom{k}{i} (-1)^i q^{-ki} (1 - q^{-1} + kq^{-k})^i. \end{aligned}$$

Now, for  $k > 2$  the above binomial series has terms of diminishing size and alternating sign and we conclude that

$$(1 - q^{-k} + q^{-k-1} - kq^{-2k})^k > 1 - \binom{k}{1} q^{-k} (1 - q^{-1} + kq^{-k})$$

from which it follows that

$$\begin{aligned} (q - z)z^k &> (q^{-k+1} - q^{-k} + kq^{-2k+1})q^k(1 - kq^{-k}(1 - q^{-1} + kq^{-k})) \\ &= (q - 1 + kq^{-k+1})(1 - kq^{-k}(1 - q^{-1} + kq^{-k})) \\ &= q - 1 + 2kq^{-k} - kq^{-k-1} - 2k^2q^{-2k+1} + 2k^2q^{-2k} - k^3q^{-3k+1} \\ &> q - 1 \end{aligned}$$

where we have used  $k > 2$  to obtain the final inequality. From this we see that  $f(z)$  is negative at  $z = q - q^{-k+1} + q^{-k} - kq^{-2k+1}$ . At the upper end-point

$$z = q - q^{-k+1} + q^{-k}$$

and we have

$$\begin{aligned} q - 1 - (q - z)z^k &= q - 1 - (q^{-k+1} - q^{-k})q^k(1 - q^{-k} + q^{-k-1})^k \\ &= q - 1 - (q - 1)(1 - q^{-k} + q^{-k-1})^k \\ &> 0 \end{aligned}$$

from which we conclude that  $f(z)$  is positive at the upper endpoint and therefore the root  $\lambda$  lies in the desired interval.

The proof that  $\lambda$  is a PV number for any integer  $q > 1$  can be generalized from the argument given in section 2.4 of “Applications of Number Theory to Numerical Analysis” [3] and we shall finish our proof of Theorem 1 by showing that the roots of  $f$  are distinct.

Let  $g(z) = (z - 1)f(z)$ . Assume that  $\lambda_i$  is a multiple root of  $f$  satisfying  $|\lambda_i| < 1$ . Then it is a multiple root of  $g$  and therefore also a root of  $g'$ , giving  $(k + 1)\lambda_i^k - qk\lambda_i^{k-1} = 0$ . Since  $\lambda_i \neq 0$  this gives us  $\lambda_i = \frac{qk}{k+1}$ . However,  $q \geq 2$  and  $k > 1$  result in the contradiction that  $|\lambda_i| > 1$ . Therefore the roots with absolute value less than 1 are distinct and, since there is only one root,  $\lambda$ , with absolute value greater than 1, we conclude that all roots of  $f$  are distinct. This completes the proof of Theorem 1, and we turn to the proof of Theorem 2.

*Proof.* From Corollary 2.2 and the matrix relation involving the  $F(n, k, q)$  we arrive at the following equation:

$$\begin{pmatrix} q^{-n}F(n, k, q) \\ q^{-(n+1)}F(n + 1, k, q) \\ \dots \\ \dots \\ q^{-(n+k-1)}F(n + k - 1, k, q) \end{pmatrix} = M^{n-1} \begin{pmatrix} (q - 1) \\ (q - 1)q \\ (q - 1)q^2 \\ \dots \\ (q - 1)q^{k-1} \end{pmatrix}.$$

From Theorem 1 we see that the eigenvalues of the matrix  $M$  are all distinct and we denote them  $\lambda_1, \lambda_2, \dots, \lambda_k$ . Let  $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k$  be the associated eigenvectors,  $\mathbf{v}_i = \sum_{j=1}^k \lambda_i^{j-1} \mathbf{e}_j$ . If we denote by  $D$  the diagonal matrix with  $\lambda_i$  as the  $i^{\text{th}}$  diagonal element and if we denote by  $B$  the matrix whose  $j^{\text{th}}$  column is  $\mathbf{v}_j$ , then we can

rewrite the above equation as

$$\begin{pmatrix} q^{-n}F(n, k, q) \\ q^{-(n+1)}F(n+1, k, q) \\ \dots \\ \dots \\ q^{-(n+1-k)}F(n+k-1, k, q) \end{pmatrix} = (q-1)BD^{n-1}B^{-1} \begin{pmatrix} 1 \\ q \\ q^2 \\ \dots \\ q^{k-1} \end{pmatrix}.$$

To aid in the computation above we define the polynomials  $h_j(x)$ , for  $j = 1, 2, \dots, k$  via  $\sum_{j=1}^k h_j(x)\mathbf{e}_j = B^{-1} \sum_{j=1}^k x^{j-1}\mathbf{e}_j$ . Then, recalling that each element of the first row of  $B$  is 1 and that the elements of  $D^{n-1}$  are just  $\lambda_i^{n-1}$  on the diagonal, we obtain

$$q^{-n}F(n, k, q) = (q-1)(\lambda_1^{n-1}h_1(q) + \lambda_2^{n-1}h_2(q) + \dots + \lambda_k^{n-1}h_k(q))$$

as one of the equations given by the matrix identity above. When  $x = \lambda_i$  we have  $\sum_{j=1}^k h_j(\lambda_i)\mathbf{e}_j = B^{-1}\mathbf{v}_i = \mathbf{e}_i$ . This determines  $h_j(x)$  for the  $k$  distinct values of  $x = \lambda_1, \dots, \lambda_k$  and since the degree of  $h_i$  is at most  $k-1$  we conclude that

$$h_j(x) = \prod_{i \neq j} \frac{x - \lambda_i}{\lambda_j - \lambda_i} = \frac{f(x)}{(x - \lambda_j)f'(\lambda_j)}$$

where the expression on the far right is valid for all  $x$  except  $x = \lambda_j$ .

We now have the result

$$q^{-n}F(n, k, q) = (q-1) \sum_{j=1}^k \lambda_j^{n-1} \frac{f(q)}{(q - \lambda_j)f'(\lambda_j)}.$$

To evaluate  $f'(\lambda_j)$  we differentiate  $(z-1)f(z)$  to obtain  $f(z) + (z-1)f'(z) = [(z-1)f(z)]' = (k+1)z^k - qkz^{k-1}$ . We set  $z = \lambda_j$  and multiply the expression by  $\lambda_j$  to arrive at

$$\lambda_j(\lambda_j - 1)f'(\lambda_j) = \lambda_j^k((k+1)\lambda_j - qk).$$

At this stage we recall that  $\lambda_j^k = \frac{q-1}{q-\lambda_j}$  and that  $f(q) = 1$  to achieve the desired result

$$q^{-n}F(n, k, q) = (q-1) \sum_{j=1}^k \lambda_j^{n-1} \frac{\lambda_j(\lambda_j - 1)}{(q-1)((k+1)\lambda_j - qk)} = \sum_{j=1}^k \lambda_j^n \frac{\lambda_j - 1}{\lambda_j - k(q - \lambda_j)}.$$

We now separate the positive real eigenvalue (which we designate by  $\lambda = \lambda_1$  from here on) from the ones with absolute value less than 1 and we need only show that the remaining eigenvalues contribute an amount with absolute value less than  $2/3$ . We write the error term as  $\epsilon(n, k, q) = \sum_{j=2}^k \frac{\lambda_j - 1}{\lambda_j - k(q - \lambda_j)} \lambda_j^n$ .

By the maximum modulus principle the function  $\frac{z-1}{z-k(q-z)}$ , on the region  $|z| \leq 1$ , assumes its maximum on the boundary. A straightforward calculation

verifies that  $\left| \frac{\omega - 1}{\omega - \alpha} \right| \leq \frac{2}{\alpha + 1}$  for any  $|\omega| = 1$  and real  $\alpha > 1$ . We conclude that, for any of the roots with norm less than 1 we have

$$\left| \frac{\lambda_j - 1}{\lambda_j - k(q - \lambda_j)} \right| = \frac{1}{k + 1} \left| \frac{\lambda_j - 1}{\lambda_j - \frac{kq}{k+1}} \right| < \frac{1}{k + 1} \left( \frac{2}{\frac{kq}{k+1} + 1} \right) = \frac{2}{k(q + 1) + 1}.$$

Using the previous inequality gives us the desired bound on the error term

$$|\epsilon(n, k, q)| \leq (k - 1) \frac{2}{k(q + 1) + 1} < \frac{2}{3}.$$

Finally we wish to show that  $C(k, q)$  is in the interval  $(1 - q^{-1} - kq^{-k}, 1 - q^{-1})$ . We start by writing  $\lambda = q - \delta$  with  $\delta \in [q^{-k+1} - q^{-k}, q^{-k+1} - q^{-k} + kq^{-2k+1}]$  and obtain

$$\begin{aligned} C(k, q) - \frac{q - 1}{q} &= \frac{q - \delta - 1}{(k + 1)(q - \delta) - kq} - \frac{q - 1}{q} \\ &= \frac{q^2 - q\delta - q - (q^2 - q - kq\delta + k\delta - q\delta + \delta)}{q(q - k\delta - \delta)} \\ &= \frac{(kq - k + 1)\delta}{q(q - k\delta - \delta)} = \frac{(k - \frac{k+1}{q})\delta}{(q - k\delta - \delta)}. \end{aligned}$$

Combining the last line above with the bounds for  $\delta$  gives  $0 < C(k, q) - (q - 1)/q < kq^{-k}$  for  $k > 1$ , as required.

#### 4. THE DISTRIBUTION OF $r(a, b)$ WITH FIXED $a$

Fix  $a \in \mathcal{F}_q[X]$  with  $\deg a = n$ . The distribution of  $r(a, b)$ , for  $a$  fixed, is identical to that of  $r(\bar{a})$  over  $\bar{a}$  so that  $\langle \bar{a} \rangle = \alpha a$  for some  $\alpha \neq 0 \in \mathcal{F}_q$ , because of the  $(q - 1)$  to 1 correspondence between continued fraction sequences and pairs  $(a, b)$ . We state and prove Theorem 3 in the setting of these sequences.

**Theorem 3.** *Given a fixed polynomial  $a \in \mathcal{F}_q[X]$  of degree  $n$ , the number of  $\bar{a} \in CFA(a, q)$  for which  $|r(\bar{a}) - n(1 - 1/q)| > z\sqrt{n(q - 1)/q^2}$  is  $\ll q^n \exp(-\frac{1}{4}z^2)$  uniformly in  $n \geq 6q$  and in  $0 \leq z \leq \frac{1}{2}(n(q - 1)/q^2)^{1/6}$ .*

*Remark.* For most  $a \in \mathcal{F}_q[X]$  of degree  $n$ , the number  $\phi(a)$  of polynomials of degree less than  $n$  and relatively prime to  $a$  is comparable to  $q^n$ . In the worst case, from the point of view of the relative error in Theorem 3,  $a$  would be the product of many irreducible polynomials over  $\mathcal{F}_q$  of small degree. It is well known that the number of such polynomials of degree  $d$  is about  $d^{-1}q^d$ , and a short calculation shows that  $q^{-n}\phi(a) \gg \log q / \log n$ . If in Theorem 3,  $z \ll \sqrt{\log(\log n / \log q)}$ , the estimate of the theorem could, in certain cases, be weaker than that to be had from the trivial observation that there can be no more polynomials  $b$  relatively prime to  $a$  with atypical  $r(a, b)$  than there are polynomials relatively prime to  $a$  altogether. The real shortcoming of this theorem is that in all probability it holds even with  $1/2$  in place of  $1/4$ .

We begin the proof of Theorem 3 with a lemma about large deviations in Bernoulli trials (coin tosses) with an unfair coin. Let  $X_{m,\theta}$  denote a random variable corresponding to the number of heads out of  $m$  tosses of a coin which comes up tails with probability  $\theta$  and heads with probability  $1 - \theta$ . That is,  $\text{prob}[X_{m,\theta} = k] = \binom{m}{k}\theta^k(1 - \theta)^{m-k}$ .

**Lemma 3.1.** *prob* $[|X_{m,\theta} - m(1 - \theta)| > z\sqrt{m\theta(1 - \theta)}] \ll \exp(-\frac{1}{2}z^2)$  uniformly in  $0 < \theta < 1/2, m > \theta^{-1}(1 - \theta)^{-1}$  and  $0 \leq z \leq (m\theta(1 - \theta))^{1/6}$ .

*Proof.* Consider the measures  $\mu_{c,\theta} := \theta e^{c(1-\theta)}\delta(\theta - 1) + (1 - \theta)e^{-c\theta}\delta(\theta)$ , and  $M_{c,\theta,m} := (\mu_{c,\theta})^{*m}$ . Let  $M(c, \theta, m) := (\theta e^{c(1-\theta)} + (1 - \theta)e^{-c\theta})^m$ . Let  $\bar{M}_{c,\theta,m}$  denote the normalized version of  $M$ , that is,  $(1/M(c, \theta, m)) \cdot M$ . Then

$$\begin{aligned} &\text{prob} \left[ X_{\theta,m} - m(1 - \theta) < -z\sqrt{m\theta(1 - \theta)} \right] \\ &= \int_{-\infty}^{-z\sqrt{m\theta(1-\theta)}} e^{ct} M(c, \theta, m) d\bar{M}_{c,\theta,m}(t) \\ &< M(c, \theta, m) e^{-cz\sqrt{m\theta(1-\theta)}}. \end{aligned}$$

Now  $M(c, \theta, m) = e^{-cm\theta}(1 - \theta + e^c\theta)^m$ , and if we take  $c := z/\sqrt{m\theta(1 - \theta)}$ , then  $M(c, \theta, m) = \exp\left(-z\sqrt{\frac{m\theta}{1-\theta}}\right) \cdot \exp\left(m \log\left(1 - \theta + \theta e^{z/\sqrt{m\theta(1-\theta)}}\right)\right)$ . Expanding the log of the second factor here in a series gives

$$m \left( \frac{\theta z}{\sqrt{m\theta(1 - \theta)}} + \frac{1}{2} \frac{\theta z^2}{m\theta(1 - \theta)} + O(1/m) - \frac{1}{2} \frac{\theta^2 z^2}{m\theta(1 - \theta)} + \text{junk} \right)$$

and on simplification we obtain one side of the lemma. The other one goes the same way.

Let  $Y_{m,q}$  be a random variable with  $\text{prob}[Y = k] := \binom{m}{k}(1 - 1/q)^k q^{k-m}$ . Then the corollary reads

**Corollary 3.2.**

$$\text{prob} \left[ |Y_{m,q} - m(1 - 1/q)| > z\sqrt{\frac{m(q - 1)}{q^2}} \right] \ll \exp\left(-\frac{1}{2}z^2\right),$$

uniformly in  $q \geq 2, m \geq q^2/(q - 1)$ , and  $0 \leq z \leq (m(q - 1)/q^2)^{1/6}$ .

We now turn to the proof of Theorem 3 proper. In the context of this proof, by the distribution of  $r(\bar{a})$ , we mean the list or vector telling, for each integer  $r$ , how often that  $r$  occurred amongst  $\bar{a}$  so that  $\langle \bar{a} \rangle = a$ . (Dividing by  $\phi(a)$  can wait.)

Let  $\rho(\bar{a})$  denote that  $r$  so that  $\sum_{j=1}^r \text{deg } a_j \leq \frac{1}{2}n < \sum_{j=1}^{r+1} \text{deg } a_j$ . Let  $m(\bar{a}) := \sum_{j=1}^{\rho(\bar{a})} \text{deg } a_j$ . Then clearly  $m(\bar{a}) \leq \frac{1}{2}n$  for all  $\bar{a}$  with  $\langle \bar{a} \rangle = a$ , and the distribution of  $\rho(\bar{a})$  over all  $\bar{a}$  such that  $\langle \bar{a} \rangle = a$  is the sum, from  $m = 1$  to  $\lfloor n/2 \rfloor$ , of that distribution taken over those  $\bar{a}$  so that  $m(\bar{a}) = m$ .

On the other hand, for fixed  $m$  and for  $\bar{a}$  so that  $m(\bar{a}) = m$ , the number of such sequences is the sum, over all ‘first halves’  $(a_1, a_2, \dots, a_r)$  so that  $\sum_{j=1}^r \text{deg } a_j = m$ , of the number of continuations  $(a_{r+1}, a_{r+2}, \dots, a_s)$  such that  $\langle \bar{a} \rangle = a$  and  $\rho(\bar{a}) = r$ . For given  $(a_1, a_2, \dots, a_r)$ , let  $u = \langle a_1, a_2, \dots, a_{r-1} \rangle$  and  $v = \langle a_1, a_2, \dots, a_r \rangle$ . The number of such extensions is then bounded above by the number of  $\hat{u}, \hat{v}$  such that  $u\hat{u} + v\hat{v} = a$  and  $\text{deg } \hat{v} - \text{deg } \hat{u} + \text{deg } v > n/2$ . (This is an upper bound only, because some choices of  $\hat{u}$  and  $\hat{v}$  may fail to be coprime, resulting in a continuation  $(a_{r+1}, a_{r+2}, \dots, a_s)$  with total degree less than  $\text{deg}(\hat{v})$ .)

The number of such pairs  $(\hat{u}, \hat{v})$ , though, is exactly  $q^{\lfloor n/2 \rfloor - m}$ . As this is independent of  $r$ , we conclude that the distribution in question is bounded above, as a list,

by

$$\begin{aligned} & \sum_{\{\bar{a}: m(\bar{a}) \leq n/2\}} \sum_{r=1}^m q^{[n/2]-m(\bar{a})} \delta(r) \chi(r(\bar{a}) = r) \\ &= \sum_{m=1}^{[n/2]} q^{[n/2]-m} \delta(r) \# \left\{ (a_1, \dots, a_r) \text{ s.t. } \sum_1^r \deg a_j = m \right\} \\ &= \sum_{m=1}^{[n/2]} q^{[n/2]-m} \sum_{r=1}^m (q-1)^r q^m \binom{m-1}{r-1} \delta(r) \\ &= (q-1) q^{[n/2]} \sum_{m=0}^{[n/2]-1} Y(m, q), \end{aligned}$$

where  $Y(m, q)$  is the probability measure for  $Y_{m,q}$  and where  $\delta(r)$  denotes the unit point mass at  $r$ .

Another way to express this is that the number of sequences  $\bar{a}$  such that  $\langle \bar{a} \rangle = a$  and  $\rho(\bar{a}) = r$  is bounded above by  $(q-1)q^{[n/2]} \sum_{m=0}^{[n/2]-1} q^m \text{prob}[Y_{m,q} = r]$ . The main step in the proof of Theorem 3 is to show that

$$\sum_{m=0}^{[n/2]-1} q^m \text{prob} \left[ \left| Y_{m,q} - \frac{n(q-1)}{q^2} \right| > z \sqrt{\frac{n(q-1)}{q^2}} \right] \ll q^{[n/2]-1} \exp(-z^2).$$

Now clearly

$$\begin{aligned} & \text{prob} \left[ \left| Y_{m,q} - \frac{1}{2} n(1-1/q) \right| > z \sqrt{n(q-1)/q^2} \right] \\ & \leq \text{prob} \left[ \left| Y_{m,q} - m(1-1/q) \right| > z \sqrt{n(q-1)/q^2} - (n/2 - m)(1-1/q) \right]. \end{aligned}$$

Put  $\zeta(m, n) := z \sqrt{n/m} - (n/2 - m) \sqrt{(q-1)/m}$ . Then

$$z \sqrt{n(q-1)/q^2} - (n/2 - m)(1-1/q) = \zeta(m, n) \sqrt{m(q-1)/q^2},$$

so that the last probability above is equal to

$$\text{prob} \left[ \left| Y_{m,q} - m(1-1/q) \right| > \zeta(m, n) \sqrt{m(q-1)/q^2} \right].$$

For our lemma to apply, we need  $\zeta(m, n) \leq (m(q-1)/q^2)^{1/6}$  and  $(m(q-1)/q^2)^{1/6} \geq 1$ . We do not need to call on the lemma for all  $m$  in the sum, though. When  $m < [n/2] - 1 - z^2/\log q$ , there is no need for subtlety, since  $\sum_{m=0}^{[n/2]-1-z^2/\log q} q^m \ll q^{[n/2]-1} \exp(-z^2)$ . We now contrive hypotheses on  $z, n$  and  $q$  to ensure that  $\zeta(m, n) \leq (m(q-1)/q^2)^{1/6}$  and  $(m(q-1)/q^2)^{1/6} > 1$  whenever  $m \geq [n/2] - 1 - z^2/\log q$ . These will eventually tie in with the announced theorem by substitution. We require the following:

- (1)  $n(q-1) \geq 3q^2$ ;
- (2)  $1 \leq z \leq (n(q-1)/q^2)^{1/6} \leq \sqrt{([n/2] - 1 - n/3) \log q}$ ;
- (3)  $n \geq 56$ .

Algebra will confirm that the requirements on  $m$  are then met. First, we claim that if  $[n/2] - 1 - z^2/\log q \leq m < n/2$  then  $\zeta(m, n) > 0$ . Equivalently,  $0 \leq n/2 - m \leq 3/2 + z^2/\log q \Rightarrow z^2 n \geq (3/2 + z^2/\log q)^2 (q-1)$ . Now  $z \leq (n(q-1)/q^2)^{1/6} \Leftrightarrow n \geq 64q^2 z^6 / (q-1)$  so we just need to show that  $64q^2 z^8 / (q-1) \geq (3/2 + z^2/\log q)^2 (q-1)$ . But this is true since  $8z^4 \geq 3/2 + z^2/\log q$  for  $z \geq 1$  and  $q \geq 2$ .

Next, we claim that under these circumstances, if  $[n/2] - 1 - z^2/\log q \leq m < n/2$  then  $m(q - 1) \geq q^2$ . For the proof, first observe that  $[n/2] - 1 - z^2/\log q > n/3$  because for  $n \geq 56$  and  $q \geq 2$ ,  $n/2 - 3/2 - (n(q - 1)/q^2)^{1/5} \geq n/3$  since  $n/6 \geq 3/2 + n^{1/3}$ . But now  $m \geq n/3$  and  $n(q - 1) \geq 3q^2$  so  $m(q - 1) \geq q^2$  as claimed.

Finally, we claim that if  $n/3 \leq m \leq n/2$  and  $z \leq (1/2)(n(q - 1)/q^2)^{1/6}$  then  $\zeta(m, n) \leq (m(q - 1)/q^2)^{1/6}$ . In view of the previous estimates, this will show that the lemma applies to  $m, q$  and  $\zeta(m, n)$ . Proving this claim takes a bit of calculus. We begin by putting  $m = \theta n$  with  $1/3 \leq \theta \leq 1/2$ . Then the estimate to be proved is that if  $z \leq (1/2)(n(q - 1)/q^2)^{1/6}$  then

$$z\sqrt{\theta} - \left(\frac{1}{2} - \theta\right)n\sqrt{\frac{q-1}{\theta n}} \leq n^{1/6}\theta^{1/6}(q-1)^{1/6}q^{-1/3}$$

and to show this it is sufficient to show that  $1/2 - (1/2 - \theta)\theta^{-1/2}q^{1/3}(q - 1)^{1/3}n^{1/3} \leq \theta^{1/6}$ . In this last inequality, the worst case is clearly  $q = 2$ , when it reduces to  $1/2 - (1/2 - \theta)\theta^{-1/2}2^{1/3}n^{1/3} \leq \theta^{1/6}$ . Now the worst case with respect to  $n$  is when  $n$  is small, i. e.  $n = 56$ . We are now down to showing that for  $1/3 \leq \theta \leq 1/2$ ,  $1/2 - (1/2 - \theta)\theta^{-1/2}112^{1/3} \leq \theta^{1/6}$ . The derivative of the left side here is  $\theta^{-1/2}112^{1/3} + \dots$ , while the derivative of the right side is  $(1/6)\theta^{-5/6}$ . The left derivative is larger, so the worst case in this final inequality is when  $\theta = 1/2$ , when it is obviously true.

Thus it is legitimate to invoke the lemma! We have

$$\begin{aligned} & \sum_{m=0}^{[n/2]-1} q^m \text{prob}[|Y_{m,q} - (1/2)n(1 - 1/q)| > z\sqrt{n(q-1)/q^2}] \\ & \leq \sum_{m=0}^{\hat{n}} q^m \\ & + \sum_{\hat{n} \leq m \leq [n/2]-1} q^m \text{prob}[|Y_{m,q} - m(1 - 1/q)| > \zeta(m, n)(m(q-1)/q^2)^{1/6}] \end{aligned}$$

where  $\hat{n} = [n/2] - 1 - z^2/\log q$ .

To analyze the last sum here we start by asking the reader to verify that for  $m$  in the sum,  $\zeta(m, n)$  is increasing as a function of  $m$ . The effect of this is to cause  $\exp(-(1/2)\zeta(m, n))$  to be decreasing in  $m$ . However,  $q^m$  is increasing in  $m$ , and we claim, more strongly, to the extent that the final term in this sum is  $\gg$  the whole sum. To prove this claim we need an upper bound on  $(\partial/\partial m)((1/2)(\zeta(m, n))^2) = \zeta(m, n)\partial\zeta/\partial m$ . Now  $\zeta(m, n) \leq z\sqrt{2}$ , and  $(\partial\zeta/\partial m) = -(1/2)zm^{-3/2}\sqrt{n} + (1/2)(n/2 - m)m^{-3/2}\sqrt{q-1} + \sqrt{(q-1)/m}$ .

This simplifies to

$$m^{-3/2} \left( (1/2)n^{1/2} + mn^{-1/2} - z(q-1)^{-1/2} \right) (n(q-1))^{1/2}$$

which is  $< m^{-3/2}((1/2)n^{1/2} + mn^{-1/2})(n(q-1))^{1/2} < 3^{3/2}n^{-1/2}(q-1)^{1/2}$ . For  $q \geq 2$  though, this is less than  $\log q$  by a margin of at least  $1/10$  because  $6\sqrt{(q-1)/n} \geq \log q$  because  $n \geq 36(q-1)/\log^2 q$  for  $n \geq 56$ . This establishes the claim that the sum in question is dominated by its last term.

In this last term, we have

$$\zeta([n/2] - 1, m) \geq \zeta(n/2 - 3/2, n) = z\sqrt{\frac{2}{(1 - 3/2n)}} - \frac{3}{2}\sqrt{\frac{2(q-1)}{(n-3)}}.$$

Therefore,  $\zeta^2([n/2] - 1, n) \geq 2z^2 - 6z\sqrt{(q-1)/n}$ , so that

$$\exp\left(-\frac{1}{2}\zeta^2([n/2] - 1, n)\right) \leq \exp\left(-z^2 + 3z\sqrt{\frac{q-1}{n}}\right).$$

But  $3z\sqrt{(q-1)/n} < 3$  here, so this all is  $\ll \exp(-z^2)$ .

That is, we have shown that if conditions (1), (2) and (3) hold, then

$$\begin{aligned} &\sum_{m=0}^{[n/2]-1} q^m \text{prob}[|Y_{m,q} - (1/2)n(1 - 1/q)| > z\sqrt{n(q-1)/q^2}] \\ &\ll q^{[n/2]-1} \exp(-z^2). \end{aligned}$$

From this it follows immediately that under the same hypotheses on  $z, n$  and  $q$ ,

$$\begin{aligned} &\# \left\{ \bar{a} = (a_1, a_2, \dots) : |\rho(\bar{a}) - n(1 - 1/q)| > z\sqrt{\frac{n(q-1)}{q^2}} \right. \\ &\quad \left. \text{and } \prod_1^{s(\bar{a})} \begin{pmatrix} 0 & 1 \\ 1 & a_j \end{pmatrix} = \begin{pmatrix} \# & \# \\ \# & a \end{pmatrix} \right\} \ll q^n \exp(-z^2). \end{aligned}$$

Of course, by symmetry, the same holds with regard to  $\bar{a}$  reversed. (Call this  $\bar{a}'$  say.)

Since  $\rho(\bar{a}) + \rho(\bar{a}') = r$  or  $r - 1$  according as  $\rho(\bar{a}) = n/2$  or not, we have the following nearly-conclusive state of affairs:

If  $\bar{a}$  had neither

$$|\rho(\bar{a}) - (1/2)n(1 - 1/q)| > z\sqrt{n(q-1)/q^2}$$

nor

$$|\rho(\bar{a}') - (1/2)n(1 - 1/q)| > z\sqrt{n(q-1)/q^2},$$

then

$$|r(\bar{a}) - n(1 - 1/q)| \leq 1 + 2z\sqrt{n(q-1)/q^2}.$$

Hence

$$\begin{aligned} &\# \left\{ \bar{a} : |s(\bar{a}) - n(1 - 1/q)| > 1 + 2z\sqrt{\frac{n(q-1)}{q^2}} \right. \\ &\quad \left. \text{and } \prod_1^{r(\bar{a})} \begin{pmatrix} 0 & 1 \\ 1 & a_j \end{pmatrix} = \begin{pmatrix} \# & \# \\ \# & a \end{pmatrix} \right\} \ll q^n \exp(-z^2). \end{aligned}$$

Putting  $w := q/\sqrt{n(q-1)} + 2z$  gives the theorem.

## REFERENCES

- [1] H. Heilbronn, *On the average length of a class of finite continued fractions*, Number Theory and Analysis, Plenum Press, New York, 1969, pp. (87–96). MR **41**:3406
- [2] D. Hensley, *The largest digit in the continued fraction expansion of a rational number*, Pacific Jour. Math. **151** (1991), 237–255. MR **92i**:11009
- [3] L. K. Hua and Y. Wang, *Applications of Number Theory to Numerical Analysis*, Springer, Berlin, 1981. MR **83g**:10034
- [4] A. Knopfmacher, *The length of the continued fraction expansion for a class of rational functions in  $\mathcal{F}_q(X)$* , Proc. Edinburgh Math. Soc. **34** (1991), 7–17. MR **92c**:11144
- [5] H. Niederreiter, *Rational functions with partial quotients of small degree in their continued fraction expansion*, Monatshefte Math. **103** (1987), 269–288. MR **88h**:12002
- [6] H. Niederreiter, *The probabilistic theory of linear complexity*, Advances in Cryptology-EURO-CRYPT '88, Lecture Notes in Computer Science, vol. 330, Springer, Berlin, 1988. MR **90d**:11138

DEPARTMENT OF MATHEMATICS, OHIO STATE UNIVERSITY, MARION CAMPUS, MARION, OHIO 43302

*E-mail address:* `friesen.4@osu.edu`

DEPARTMENT OF MATHEMATICS, TEXAS A& M UNIVERSITY, COLLEGE STATION, TEXAS 77843

*E-mail address:* `doug.hensley@math.tamu.edu`