The Probability That a Random Monic *p*-adic Polynomial Splits

Joe Buhler, Daniel Goldstein, David Moews, and Joel Rosenberg

CONTENTS

2000 AMS Subject Classification: Primary 11S05

Keywords: p-adic, polynomial, splits completely

Let R be a complete discrete valuation ring with finite residue field, and let r_n be the probability that a random monic polynomial over R of degree n factors over R into linear factors. We study r_n in detail. Among other things, we show that r_n satisfies an interesting recursion, make a conjecture on the asymptotic behavior of r_n as n goes to infinity, and prove the conjecture in the case that the residue field has two elements.

1. INTRODUCTION

Let R be a complete discrete valuation ring with finite residue field k of cardinality q. Since R is a compact topological group, it has a natural probability measure, and by identifying monic polynomials of degree n over R with n-tuples of elements of R, this gives a natural probability measure on the set of monic polynomials of degree n with coefficients in R. The subset consisting of those monic polynomials of degree n that factor completely into linear factors is closed and therefore measurable.

Define r_n to be the probability that a random monic polynomial f over R of degree n factors over R into linear factors. The first four values of r_n are

$$\begin{aligned}
r_1 &= 1,\\
r_2 &= q/2(q+1),\\
r_3 &= (q^2-q+1)(q-1)q^3/6(q+1)(q^5-1),\\
r_4 &= h(q)(q-1)^4q^6/24(q^2-1)^2(q^5-1)(q^9-1),
\end{aligned}$$

where $h(q) = q^8 - 2q^7 + q^6 + 2q^5 - q^4 + 2q^3 + q^2 - 2q + 1$. For convenience, we set $r_0 = 1$.

As we will see, the values r_n satisfy a remarkable recurrence relation. To express this, it is convenient to define

$$s_n = q^{-(n^2+n)/2} r_n.$$

For $q = 2$ the recurrence can be written

$$r_n = s_0 s_n + s_1 s_{n-1} + \cdots + s_{n-1} s_1 + s_n s_0 \qquad (1\text{–}1)$$

1058-6458/2006 $0.50 per page

(and it is easy to work out that this can be solved for r_n if $n > 1$). For general q the recursion can be expressed in terms of the ordinary generating functions for r_n and s_n:

$$\sum_{n\geq 0} r_n t^n = \Big(\sum_{n\geq 0} s_n t^n\Big)^q. \qquad (1–2)$$

In particular, we note that r_n depends only on the cardinality of the residue field.

Asher Auel [Auel 03], working independently, obtained the same result.

Our further results are related to the asymptotic behavior of r_n as n tends to infinity. Using a formula for r_n in terms of certain labeled trees, we are able to show that r_n decays exponentially in n^2. More precisely, we show that

$$\log_q r_n = -\frac{n^2}{2(q-1)} - \frac{1}{2} n \log_q n + O(n),$$

where the constant implicit in the $O(n)$ depends on q.

The behavior of the $O(n)$ term is interesting; we conjecture that it has the form $W_q(\log_q n) \cdot n + O(1)$, where W_q is a continuous, periodic function of period 1 (and the implied constant depends on q). In the special case $q = 2$ we are able to prove this conjecture by extending the earlier analysis that used the labeled trees formulation of r_n. The graph of W_2 appears as Figure 1.

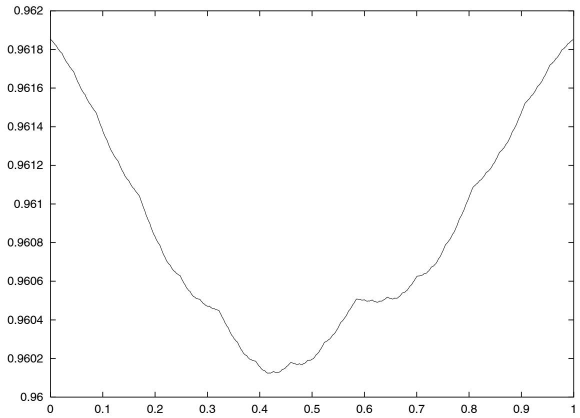

FIGURE 1. Graph of W_2 over its period.

2. PROOF OF THE RECURSION

In this section we prove the recursion (1–2), which we reformulate as the following theorem. For a sequence $d = (d_0, d_1, \ldots, d_{q-1})$ of nonnegative integers, write $|d| = d_0 + d_1 + \cdots + d_{q-1}$ for their sum.

Theorem 2.1. *If $n \geq 0$, then*

$$r_n = \sum_{|d|=n} \prod_{0\leq i\leq q-1} q^{-\binom{d_i+1}{2}} r_{d_i}. \qquad (2–1)$$

Write πR for the maximal ideal of R. For $f \in R[x]$ a monic polynomial of degree n, let $\bar{f}$ denote its reduction mod πR. Since the probability that f reduces to any given monic degree-n polynomial ρ in $k[x]$ is precisely q^{-n}, we have

$$r_n = \sum_{\rho} \mathrm{pr}(f \text{ splits completely} \mid \bar{f} = \rho)\, q^{-n}.$$

A necessary condition for f to split completely in $R[x]$ is that its reduction split completely in $k[x]$, so it is enough to sum over those ρ that split completely in $k[x]$.

Write $\rho = \prod_{\alpha\in k}(x-\alpha)^{d_\alpha}$. Since the polynomials $\rho_\alpha = (x-\alpha)^{d_\alpha}$ are pairwise relatively prime, Hensel's lemma yields the factorization $f = \prod_{\alpha\in k} f_\alpha$, where f_α in $R[x]$ reduces to ρ_α in $k[x]$.

Theorem 2.1 now follows from the following lemma, and the observation that $\binom{d_i+1}{2} = d_i + \binom{d_i}{2}$.

Lemma 2.2.

(i) $\mathrm{pr}(f \text{ splits completely} \mid \bar{f} = \rho)$
$= \prod_{\alpha\in k} \mathrm{pr}(f_\alpha \text{ splits completely} \mid \overline{f_\alpha} = \rho_\alpha)$.

(ii) $\mathrm{pr}(f_\alpha \text{ splits completely} \mid \overline{f_\alpha} = \rho_\alpha) = q^{-\binom{d_\alpha}{2}} r_{d_\alpha}$.

Proof: The first statement follows from Hensel's lemma. Since we could not find the particular version of Hensel's lemma that we need, we state and prove it below as Lemma 2.3.

We prove the second statement for the case $\alpha = 0$. Set $f = f_0$. We have f in $R[x]$ monic with reduction x^n in $k[x]$. Assume for the moment that $f = x^n + c_1 x^{n-1} + \cdots + c_n$ does split completely, say as

$$f = (x - a_1) \cdots (x - a_n).$$

A root of f reduces to a root of $\bar{f}$, so that a_i lies in πR for each i, whence a necessary condition for f to split completely is that c_i lies in $\pi^i R$ for each i. The probability that this condition holds is $q^{-\binom{n}{2}}$, the product of q^{-i} for $0 \leq i \leq n-1$. Set

$$\tilde{f} = f(\pi x)/\pi^n.$$

The necessary condition is met if and only if $\tilde{f}$ has coefficients in R. Conditioned on its being met, $\tilde{f}$ is distributed like a random monic polynomial of degree n, and the result follows because f splits completely if and only if $\tilde{f}$ splits completely.

The proof of the second statement for general α follows from the case $\alpha = 0$ as follows. Let r in R be an element whose image in k is equal to α.

Write $P_n(R)$ for the set of monic polynomials f in $R[x]$ of degree n. Consider the map ψ_r from $P_n(R)$ to itself taking the polynomial $f(x)$ to the polynomial $f(x-r)$.

Set $f_1 = f - x^n$, so that $\deg(f_1) < n$. We calculate that $f(x-r) = f_1(x-r) + (x-r)^n = (f_1(x-r) + x^n) + (-x^n + (x-r)^n)$. Therefore, the map ψ_r can be written as a composition of the map $f \mapsto f_1(x-r) + x^n$ and the map that adds $-x^n + (x-r)^n$. (The point here is to stay within the space of monic degree-n polynomials.) The former is seen to be upper-triangular by considering the basis of monomials x^i for $0 \le i \le n-1$, and the latter is a translation, so each preserves measure and therefore so does ψ_r. □

Let g be a polynomial in $P_n(k)$. Write P_g for the set of polynomials f in $P_n(R)$ whose reduction $\bar{f}$ is g. As a measurable subset of $P_n(R)$, P_g inherits a topology and a measure from $P_n(R)$. We renormalize the measure so that P_g has total measure 1. Part (1) of Lemma 2.2 now follows from the following lemma:

Lemma 2.3. *Let g and h in $k[x]$ be relatively prime monic polynomials of degree m and n, respectively. The multiplication map*

$$P_g \times P_h \to P_{gh}$$

is a measure-preserving homeomorphism.

The usual version of Hensel's lemma asserts only that the multiplication map is a homeomorphism. The lemma is an immediate consequence of the following, somewhat more general result.

Lemma 2.4. *Let $A = \prod_{1 \le i} a_i$ and $B = \prod_{1 \le i} b_i$ be countable products of finite sets. Normalize counting measure so that each of a_i and b_i has total mass 1, for all i, and give A and B the product measure. Suppose there is a compatible system of bijections ϕ_n between the partial products $A_n = \prod_{1 \le i \le n} a_i$ and $B_n = \prod_{1 \le i \le n} b_i$; that is, for each $n \ge 1$, the map ϕ_n from A_n to B_n is bijective, and for $m \le n$, if y in A_n has x in A_m as initial string, then $\phi_n(y)$ has $\phi_m(x)$ as initial string. Then the map $\phi = \varprojlim \phi_n$ from A to B is a measure-preserving bijection.*

Proof: Certainly ϕ is bijective. Since ϕ takes basic open sets to basic open sets of the same volume, it follows that ϕ preserves measure. □

Here is yet another equivalent formulation of the recursion.

Corollary 2.5. *For $n \ge 0$, we have*

(i) $$\sum_{0 \le j \le n} (n - (q+1)j) r_{n-j} \frac{r_j}{q^{(j^2+j)/2}} = 0.$$

(ii) *If $n \ge 2$, we can solve for r_n:*

$$r_n = \frac{1}{n(-1 + q^{1-n(n+1)/2})} \times \sum_{1 \le j \le n-1} (n - (q+1)j) r_{n-j} r_j q^{-(j^2+j)/2}.$$

In particular, r_n is a rational function of q.

The corollary is proved by logarithmic differentiation. The basic method is due to Euler [Euler 48].

Proof: Let $F = \sum_{n \ge 0} r_n t^n$ and $G = \sum_{n \ge 0} s_n t^n$. Then from the functional equation (1–2), we have $F = G^q$.

Take logarithmic derivatives to get

$$\frac{F'}{F} = q \frac{G'}{G}.$$

Cross-multiply to get

$$F'Gt = qFG't,$$

and equate coefficients of t^n to get

$$\sum_{0 \le j \le n-1} (n-j)\, r_{n-j} s_j = \sum_{1 \le j \le n} q\, r_{n-j} j s_j.$$

There is no harm in including the term $j = n$ in the sum on the left and the term $j = 0$ in the sum on the right, since these terms are zero. Now subtract. This proves the first statement of Corollary 2.5. The second statement follows immediately from the first. □

3. VARIANTS

We consider a version of our question over finite fields and a version for p-adic polynomials that are not necessarily monic.

The first variant we consider is the probability $\bar{r}_n$ that a random monic, degree-n polynomial over a finite field k splits completely. We state some properties that relate r_n and $\bar{r}_n$. Note that $\bar{r}_n$ and r_n depend only on q and n. In fact, we will use the third property in Section 4. Our convention is that $r_0 = \bar{r}_0 = 1$.

1. We have $r_n \le \bar{r}_n$. Indeed, if a monic polynomial f in $R[x]$ splits completely, then $\bar{f}$ splits completely in $k[x]$.

2. We have $\sum_{n\ge 0} \bar{r}_n t^n = (1-t/q)^{-q}$. Indeed, by the result sometimes called the stars and bars theorem, the number of monic degree-n polynomials that split completely is $q^n \bar{r}_n = \binom{n+q-1}{q-1}$. Now use the binomial expansion $(1-t)^{-q} = \sum_{n\ge 0} \binom{-q}{n}(-t)^n$, and the fact that $\binom{-q}{n} = (-1)^n \binom{q-1+n}{n}$.

3. We have $\lim_{q\to\infty} r_n = 1/n! = \lim_{q\to\infty} \bar{r}_n$. The second equality follows from Property 2. For f monic in $R[x]$, the probability that $\bar{f}$ has a repeated root is at most $1/q$. (Proof: The set S of monic polynomials f with constant and linear term in πR has measure $1/q^2$. Hence, if we let ψ_r be as in the proof of Lemma 2.2, the union of the sets $\psi_r(S)$ over a set of lifts r of the elements of k has measure at most $1/q$.) But this tends to zero as $q \to \infty$. This proves the first equality.

The second variant that we consider is for nonmonic p-adic polynomials. The natural probability measure on R gives a probability measure on R^{n+1}, and this set can be identified with the set of all polynomials of degree n with coefficients in R.

Define r_n^{nm} to be the probability that a random polynomial f over R of degree n factors over R into linear factors.

(By definition, f factors over R into linear factors if it can be written in the form $f(x) = (b_1x - a_1)\cdots(b_nx - a_n)$, with a_i, $b_i \in R$.)

The first four values of r_n^{nm} are

$$\begin{aligned}
r_1^{\mathrm{nm}} &= 1,\\
r_2^{\mathrm{nm}} &= 1/2,\\
r_3^{\mathrm{nm}} &= (q^2+1)^2(q-1)/6(q^5-1),\\
r_4^{\mathrm{nm}} &= h^{\mathrm{nm}}(q-1)^2/24(q^5-1)(q^9-1),
\end{aligned}$$

where $h^{\mathrm{nm}} = q^{12} - q^{11} + 4q^{10} + 3q^8 + 4q^7 - q^6 + 4q^5 + 3q^4 + 4q^2 - q + 1$. By convention, we set $r_0^{\mathrm{nm}} = 1$.

The values r_n^{nm} also satisfy a recurrence that can be expressed in terms of the generating function for r_n^{nm} and the generating function for s_n:

$$\sum_{n\ge 0}(1-q^{-n-1}) r_n^{\mathrm{nm}} t^n = \frac{q-1}{q}\Big(\sum_{n\ge 0} s_n t^n\Big)^{q+1}. \qquad (3\text{–}1)$$

The proof is quite similar to the proof of the recurrence for r_n. We merely sketch the details and leave a complete proof to the reader.

By conditioning on the reduction mod πR of f, we see that

$$\begin{aligned}
&\mathrm{pr}(f \text{ splits completely})\\
&\qquad = \sum_{\rho} \mathrm{pr}(f \text{ splits completely} \mid \bar{f} = \rho)\,\mathrm{pr}(\bar{f} = \rho),
\end{aligned}$$

where the sum is over polynomials $\rho \in k[x]$ of degree $\le n$.

First we consider the term with $\rho = 0$. It is straightforward that the probability that $\bar{f} = 0$ (or any given polynomial of degree $\le n$) is q^{-n-1}. If $\bar{f} = 0$, then f/π is distributed randomly and splits if and only if f does. Hence, the contribution from the $\rho = 0$ term is $q^{-n-1} r_n^{\mathrm{nm}}$.

Otherwise, the degree of ρ is $n-j$ for some $0 \le j \le n$. The probability that $\deg \bar{f} = n-j$ is equal to $(q-1)/q^{j+1}$. By Hensel's lemma, f has a factor $f^{\inf}$ which has the same degree as ρ, has reduction ρ modulo πR, and yields a quotient $f_{\inf} := f/f^{\inf}$ which has constant term 1. Then $f_{\inf}$ has degree $n-j$ and the quotient $f_{\inf}$ has degree no more than j and reduction $\overline{f_{\inf}} = 1$.

By an analogue of Lemma 2.3, we have

$$\begin{aligned}
&\mathrm{pr}(f \text{ splits completely})\\
&\quad = \mathrm{pr}(f^{\inf} \text{ splits completely})\mathrm{pr}(f_{\inf} \text{ splits completely}).
\end{aligned}$$

The first term on the right is equal to r_{n-j}. By replacing $f_{\inf}$ with $x^j f_{\inf}(1/x)$, it can be shown that the second term on the right is equal to the probability that f splits completely given that f is monic of degree j and $\bar{f} = x^j$, which equals $q^j s_j$ by Lemma 2.2 (ii).

Thus, we have

$$r_n^{\mathrm{nm}} = \sum_{0\le j\le n} \frac{q-1}{q} r_{n-j} s_j + \frac{r_n^{\mathrm{nm}}}{q^{n+1}}. \qquad (3\text{–}2)$$

This identity, for all n, is tantamount to the single power series identity

$$\sum_{n\ge 0}(1-q^{-n-1}) r_n^{\mathrm{nm}} t^n = \frac{q-1}{q}\Big(\sum_{n\ge 0} r_n t^n\Big)\Big(\sum_{n\ge 0} s_n t^n\Big).$$

From this and the functional equation (1–2), we get the desired recursion (3–1). We see, in particular, that r_n^{nm} is a rational function of q for each n.

4. GENERATING FUNCTIONS

In this section we regard q as a variable, and let $(r_n) = (r_n(q))$ be the sequence of rational functions defined by $r_0 = r_1 = 1$, and

$$\sum_{n\ge 0} r_n t^n = \Big(\sum_{n\ge 0} \frac{r_n}{q^{\binom{n+1}{2}}} t^n\Big)^q \qquad (4\text{–}1)$$

if $n \geq 2$. Thus, if we plug in a prime power for q we recover the r_n's with their previous meaning.

We note some properties of these rational functions.

Lemma 4.1.

(i) *The degree of the numerator of* r_n *is the degree of the denominator, and* $\lim_{q\to\infty} r_n(q) = 1/n!$.

(ii) r_n *vanishes at* 0 *to order* $\binom{n}{2}$.

(iii) *The only poles of* r_n *are at roots of unity.*

(iv) $r_n(q) = r_n(1/q)q^{\binom{n}{2}}$.

Proof of Properties (i)–(iv)*:* Property (i) follows from Property 3 in Section 3.

To prove (iv), let $R_n = R_n(q) = q^{\binom{n}{2}} r_n(1/q)$. Replace q by $1/q$ in the recursion (4–1) and raise to the qth power to get

$$\Big(\sum_{n\geq 0} R_n q^{-\binom{n}{2}} t^n\Big)^q = \sum_{n\geq 0} R_n q^n t^n.$$

Replacing t by t/q gives (4–1), with r_n replaced by R_n. Since r_n and R_n satisfy the same recursion, and have the same values for $n = 0$ and $n = 1$, it follows that $r_n = R_n$ for all n, as desired.

To prove (iii), note that the formula in Corollary 2.5 (ii) can be written, after some juggling, as

$$n\left(1 - q^{\binom{n+1}{2}-1}\right) r_n \\ = q^{\binom{n+1}{2}-1} \sum_{0<j<n} (n-(q+1)j) r_{n-j} r_j q^{-\binom{j+1}{2}}.$$

An easy induction argument then shows that the only poles of the rational functions r_n are at roots of unity, as desired.

Property (ii) is an immediate consequence of (i) and (iv). This finishes the proof of Properties (i)–(iv). □

5. ASYMPTOTICS

Let $q \geq 2$ be an integer. In Theorem 5.1 of this section we give the first two terms in the asymptotic expansion of $\log_q r_n$. (The first term is quadratic in n and the second is of order $n \log_q n$.) In Section 6, we make a conjecture for the third term. Theorem 6.2 proves this conjecture for $q = 2$; in this case we have a remarkably precise result:

$$\log_2 r_n = -\frac{n^2}{2} - \frac{n}{2}\log_2 n + W_2(\log_2 n)n + O(1), \quad (5\text{–}1)$$

where $W_2(x)$ is continuous and periodic of period 1, and has only small-magnitude fluctuations.

After we discovered this, we found that this remarkable sort of oscillatory behavior has been observed in other contexts, for example by Li and Pomerance [Li and Pomerance 01], who studied primitive roots; Gordon, Schilling, and Waterman, who studied long head runs [Gordon et al. 86]; and Kirschenhofer and Prodinger [Kirschenhofer and Prodinger 96], who studied the number of winners in a geometrically distributed sample. In our case, we have no closed-form expression for W_2, but its graph is given in Figure 1.

The proofs of Theorems 5.1 and 6.2 rely on a formula for r_n in terms of certain labeled trees.

Theorem 5.1. *If* $q \geq 2$ *is an integer, then*

$$\log_q r_n = -\frac{n^2}{2(q-1)} - \frac{1}{2} n \log_q n + O(n), \quad (5\text{–}2)$$

for all $n \geq 1$*, where the implied constant depends on* q.

Proof: The proof of Theorem 5.1 is as follows. In the proof of the exact formula for r_n, we looked at a certain infinite tree whose branching was given by the factorization of a polynomial mod the maximal ideal πR of R, mod $\pi^2 R$, etc. In a modification of this method, we use finite trees instead. Lemma 5.6 expresses $r_n/q^{\binom{n+1}{2}}$ as the sum of a certain function H over labeled q-trees (defined below) with n leaves. By Lemma 5.3, we will see that for any fixed q, the logarithm of the number of labeled q-trees is $O(n)$. We will therefore have

$$\gamma_n \leq -\binom{n+1}{2} + \log_q r_n \leq \gamma_n + O(n),$$

where γ_n is the maximum value of $\log_q H$.

In Lemmas 5.10 and 5.12 we will calculate γ_n, as follows. In Lemma 5.12 we calculate H evaluated at a particular q-tree that we call the *well-balanced* q*-tree.* In Lemma 5.10 we show that the function H is maximized at the well-balanced q-tree. This will complete the proof of the theorem. □

5.1 q-Trees

A rooted tree is a connected acyclic graph with a distinguished vertex (the root). We can direct the edges of a rooted tree in a unique way, by directing them away from the root. The root has in-degree 0; all other vertices have in-degree 1. The edges emanating from a vertex go to distinct vertices, called the *children* of v. A vertex with no children is a *leaf* vertex.

A *q-tree* is a rooted tree in which the number of out-edges from each vertex is at most q, and is not 1 (i.e., there is branching at each vertex that is not a leaf).

For v a vertex of the q-tree T, we write T_v for the full subtree whose vertices are v and all its descendants. This is a q-tree.

A *labeled q-tree* is a q-tree together with a labeling of its edges with elements of the set $S = \{0, 1, \dots, q-1\}$ so that the out-edges emanating from each vertex have distinct labels.

Example 5.2. We list the q-trees with at most three leaves.

(i) The tree τ_1 with one vertex and no edges is the unique q-tree with one leaf. In all other q-trees, a vertex is a leaf if and only if it has total degree 1.

(ii) The tree τ_2 with three vertices, a root with two leaf children, is the unique q-tree with two leaves. There are $\binom{q}{2}$ ways of labeling this q-tree.

(iii) There are two q-trees with three leaves (one if $q = 2$). One, call it τ_{3a}, has a root with three leaf children (if $q > 2$). The other, τ_{3b}, has a root with two children v and w, with v a leaf and $T_w = \tau_2$. There are $\binom{q}{3}$ ways of labeling τ_{3a}, and $q(q-1)\binom{q}{2}$ ways of labeling τ_{3b}.

Lemma 5.3. *The number of labeled q-trees with l leaves is $\leq (2q+1)^{5l-3}$.*

Proof. Let Σ be the set of $2q+1$ symbols: the parentheses $(_i$ and $)_i$ for $0 \leq i \leq q-1$, plus a dot. We construct for every labeled q-tree a distinct string of at most $5l-4$ of these symbols, thus constructing an injective map from the set of labeled q-trees with l leaves to $\cup_{0\leq i\leq 5l-4}\Sigma^i$.

We proceed by induction on l. For $l = 1$, the tree τ_1 corresponds to the dot.

Assume $l \geq 2$, and let T be a labeled q-tree with l leaves. Let the root of T have j children. For each child v of the root of T, bracket the sequence corresponding to the subtree T_v with the symbols $(_i$ and $)_i$, where $i \in S$ is the label of the edge from the root to the vertex v. By the induction hypothesis, this uses at most $5l - 4j + 2j = 5l - 2j \leq 5l - 4$ symbols.

The number of labeled q-trees with l leaves is therefore not more than

$$\sum_{0\leq i\leq 5l-4} (2q+1)^i = (2q)^{-1}((2q+1)^{5l-3}-1) \leq (2q+1)^{5l-3}.$$

5.2 A q-Tree Recursion

Group the r_n terms in (2–1) to get

$$r_n = \frac{q}{q^{\binom{n+1}{2}}} r_n + \sum\nolimits'_{|b|=n} \prod_{0\leq i\leq q-1} \frac{r_{b_i}}{q^{\binom{b_i+1}{2}}},$$

where $\sum'$ is the sum over b such that $b_i > 0$ for at least two values of i. Rewriting this in terms of $s_n = q^{-\binom{n+1}{2}} r_n$, we have

$$q^{\binom{n+1}{2}} s_n = q s_n + \sum\nolimits'_{|b|=n} \prod_{0\leq i\leq q-1} s_{b_i}.$$

For $n \geq 2$, set

$$\beta_n = 1/(q^{\binom{n+1}{2}} - q). \tag{5–3}$$

Set $\beta_1 = 1/q$. We have proved the following.

Lemma 5.4. *Assume $n \geq 2$. Then*

$$s_n = \beta_n \sum\nolimits'_{|b|=n} \prod_{0\leq i\leq q-1} s_{b_i}. \tag{5–4}$$

Remark 5.5. We can decompose a q-tree into its root, plus a subtree T_v for each child v of the root of T. This decomposition underlies Lemma 5.3, and will allow us to interpret Lemma 5.4 as a recursion on labeled q-trees.

Write $\ell(v)$ for the number of leaves of the tree T_v. As an easy application of the decomposition in Remark 5.5, we have the following. Let T be a q-tree with more than one vertex. Then the root of T is not a leaf, and the number of leaves of T equals $\sum \ell(v)$, where the sum is over the set of children v of the root of the tree T.

We can now interpret the recursion for s_n in terms of labeled q-trees.

Lemma 5.6. *We have*

$$s_n = \sum_T \prod_{v\in T} \beta_{\ell(v)},$$

where the sum is over labeled q-trees T with n leaves, and the product is over all vertices v of the tree T.

Proof: For $n = 1$, this follows by our choice of β_1. The general case follows by Remark 5.5 and Lemma 5.4. □

We shall write $H(T)$ for $\prod_{v\in T} \beta_{\ell(v)}$.

5.3 The Well-Balanced q-Tree

Lemma 5.7. *We have*

(i) $\log_q \beta_n = -\binom{n+1}{2} + o(1)$ *as* $n \to \infty$.

(ii) *The sequence* $(\beta_n/\beta_{n-1})_{n=2}^{\infty}$ *is monotone decreasing.*

Proof: Part (i) is clear since $\beta_n q^{\binom{n+1}{2}}$ tends to 1 as $n \to \infty$.

In order to prove (ii) it suffices to show that $1/\beta_n^2 \leq 1/(\beta_{n-1}\beta_{n+1})$ for all $n \geq 2$.

First consider the case $n = 2$. We have $1/\beta_2^2 = (q^3 - q)^2 \leq (q^3 - q)(q^3 + q) = q^6 - q^2 \leq q(q^6 - q)$, and this last quantity is equal to $1/\beta_1\beta_3$.

Next suppose $n \geq 3$. Then $1/\beta_n^2 = (q^{\binom{n+1}{2}} - q)^2$, and we have,

$$\begin{aligned}(q^{\binom{n+1}{2}} - q)^2 &\leq (q^{\binom{n+1}{2}} - q)(q^{\binom{n+1}{2}} + q)\\ &= q^{n^2+n} - q^2\\ &\leq (q^{\binom{n}{2}-1} + q)(q^{\binom{n+2}{2}} - q).\end{aligned}$$

Call this product AB. The last inequality follows since $\binom{n}{2} - 1$ is less than $\binom{n+2}{2}$ and their sum is $n^2 + n$.

Since $2 \leq q$, we have $2 \leq q(q-1)$, which implies that $2q \leq q^j(q-1)$ for any $j \geq 2$. Rearranging terms gives $q^j + q \leq q^{j+1} - q$, which implies (taking $j = \binom{n}{2} - 1 \geq \binom{3}{2} - 1 = 2$) that $A \leq 1/\beta_{n-1}$. Since $B = 1/\beta_{n+1}$, the lemma is proved. □

Let $n \geq 1$ be an integer. We are interested in q-tuples of nonnegative integers that sum to n, and such that any two entries differ by at most one. We remark that such a q-tuple i exists: write $n = qx+y$ with $0 \leq y \leq q$ (we allow either $y = 0$ or $y = q$); now take $i_1 = \cdots = i_y = x+1$ and $i_{y+1} = \cdots = i_q = x$. Moreover, if such a q-tuple contained a value less than x (respectively larger than $x+1$), all values would be at most x (respectively at least $x+1$), and the sum would be too small (respectively too large). Thus all values are x or $x+1$, and the number of each must be $q - y$ (respectively y). Hence the q-tuple is unique up to order.

Lemma 5.8. *Let* $n \geq 1$ *be an integer. There is a unique* q*-tree* $T = T(n)$ *with* n *leaves such that for every vertex* v *of* T*:*

(i) *If* $\ell(v) < q$ *then all children of* v *are leaves.*

(ii) *If* $\ell(v) \geq q$ *then* v *has* q *children and, for any two children* w *and* w' *of* v, $\ell(w)$ *and* $\ell(w')$ *differ by at most* 1.

Proof: If $n = 1$, then T is the unique q-tree with one (leaf) vertex. If $1 < n < q$, then T is the unique q-tree with $n+1$ vertices that consists of a root with n children all of which are leaves.

For $n \geq q$, we define $T = T(n)$ by induction on n. Write $n = qx + y$ with $0 \leq y \leq q - 1$ as in the remarks preceding this lemma. Applying property (ii) above at the root of T, we see that if T exists, its root must have children $v_1, \ldots, v_q$ such that $\ell(v_1) = \cdots = \ell(v_y) = x+1$ and $\ell(v_{y+1}) = \cdots = \ell(v_q) = x$. It now follows from the induction hypothesis that each T_{v_i} must equal $T(\ell(v_i))$. This gives a unique candidate for T, namely the q-tree whose root has precisely q children, and such that $T_w = T(x+1)$ for y of these children w and $T_w = T(x)$ for the remaining $q - y$ children w. It is easy to see that this does indeed satisfy Properties (i) and (ii). □

We call a q-tree *well-balanced* if it satisfies the two conditions of the lemma. For T the well-balanced q-tree with $n \geq 1$ leaves, write $\nu_n = \prod_{v \in T} \beta_{\ell(v)}$. Set $\nu_0 = 1$.

Lemma 5.9.

(i) $\nu_1 = 1/q$.

(ii) *If* $n \geq 2$ *and we write* $n = qx + y$, $0 \leq y \leq q$, *then*

$$\nu_n = \beta_n \nu_x^{q-y} \nu_{x+1}^{y}.$$

(iii) *The sequence* $(\nu_i/\nu_{i-1})_{i=1}^{\infty}$ *is monotone decreasing.*

Proof: (i) is obvious, and (ii) follows immediately from the defining properties of the well-balanced q-tree and the remarks preceding Lemma 5.8. We now prove that for all n, the sequence $(\nu_i/\nu_{i-1})_{i=1}^{n}$ is monotone decreasing; this will prove (iii). We proceed by induction on n. If $n \leq 3$, the result follows from Example 5.2, so assume that $n \geq 4$. We need to show that $\nu_{n-1}/\nu_{n-2} \geq \nu_n/\nu_{n-1}$.

For any $2 \leq m \leq n-1$, write $m = qx + y$ with $0 \leq y \leq q-1$ (note that we do not allow $y = q$). By (ii), $\nu_m = \beta_m \nu_x^{q-y} \nu_{x+1}^{y}$.

Next we calculate ν_{m+1}. We have $m+1 = qx + (y+1)$, with $y + 1 \leq q$, so (ii) gives $\nu_{m+1} = \beta_{m+1} \nu_x^{q-y-1} \nu_{x+1}^{y+1}$, whence $\nu_{m+1}/\nu_m = \frac{\beta_{m+1}}{\beta_m} \frac{\nu_{x+1}}{\nu_x}$.

We apply this to $m = n-2$ and $m = n-1$. The desired result now follows from Lemma 5.7(ii), after possibly using the induction hypothesis. □

If $n > 0$, let γ_n be the largest tree contribution $H(T) = \prod_{v \in T} \beta_{\ell(v)}$ among q-trees T with n leaves. Set $\gamma_0 = 1$.

Lemma 5.10. *For all* $n \geq 0$, $\gamma_n = \nu_n$.

Proof: We proceed by induction on n. For $n = 0$ and $n = 1$, the result is obvious.

Assume $n > 1$. The contribution from a tree with n leaves is at most $\beta_n \gamma_{i_1} \cdots \gamma_{i_q}$, where $i_1, \dots, i_q$ are nonnegative integers that sum to n, at least two of which are positive. Since at least two i_z's are positive, we have $i_1, \dots, i_q \le n-1$, so by the induction hypothesis, $\gamma_{i_z} = \nu_{i_z}$ for all z. It therefore follows that the contribution is no more than

$$\beta_n \nu_{i_1} \cdots \nu_{i_q}. \tag{5–5}$$

Now by Lemma 5.9(iii),

$$\nu_{i-1}\nu_j \le \nu_i \nu_{j-1} \text{ if } 1 \le i \le j. \tag{5–6}$$

Let $n = qx + y$ with $0 \le y \le q$. It follows from the inequality (5–6) that the quantity (5–5) is maximized when $|i_z - i_{z'}| \le 1$ for all $1 \le z, z' \le q$, when, by the remarks preceding Lemma 5.8, it equals $\beta_n \nu_x^{q-y} \nu_{x+1}^y$. By Lemma 5.9(ii), this equals ν_n, so we are done. □

Lemma 5.11. *Let T be the well-balanced q-tree with n leaves, let $k \ge 0$, and let $n = q^k x + y$, $0 \le y < q^k$. Then:*

(i) *If $n < q^{k-1}$, there are no vertices at distance k from the root of T.*

(ii) *If $q^{k-1} \le n < 2q^{k-1}$, there are $2(n - q^{k-1})$ vertices at distance k from the root of T, each of which is a leaf.*

(iii) *If $2q^{k-1} \le n < q^k$, there are n vertices at distance k from the root of T, each of which is a leaf.*

(iv) *If $n \ge q^k$, there are q^k vertices v' at distance k from the root of T, y with $\ell(v') = x + 1$ and $q^k - y$ with $\ell(v') = x$.*

Proof: We prove the lemma by induction on k. If $k = 0$, these results are clear. Otherwise, we proceed as follows: To prove the first claim, suppose that $n < q^{k-1}$. Then by the induction hypothesis, all the vertices at distance $k-1$ from the root of T are leaves, and therefore there are no vertices at distance k from the root, as desired.

If $q^{k-1} \le n < 2q^{k-1}$, then by the induction hypothesis, there are q^{k-1} vertices v' at distance $k-1$ from the root, $2q^{k-1} - n$ of which are leaves and $n - q^{k-1}$ of which satisfy $\ell(v') = 2$, i.e., have 2 children, both leaves; this gives a total of $2(n - q^{k-1})$ vertices at distance k from the root, all leaves, which is the second claim.

If $2q^{k-1} \le n < q^k$, then write $n = q^{k-1}x' + y'$, $2 \le x' \le q - 1$, $0 \le y' < q^{k-1}$. By the induction hypothesis, there are q^{k-1} vertices v' at distance $k-1$ from the root, y' of which satisfy $\ell(v') = x' + 1$, and $q^{k-1} - y'$ of which satisfy $\ell(v') = x'$. By the properties of the well-balanced q-tree, the vertices v' for which $\ell(v') = x'$ must have x' children, all leaves. Similarly, the vertices v' for which $\ell(v') = x' + 1$ must have $x' + 1$ children, all leaves. This gives n vertices at distance k from the root, all leaves. This proves the third claim.

Finally, if $n \ge q^k$, write $y = y_0 q^{k-1} + y_1$, $0 \le y_0 < q$, $0 \le y_1 < q^{k-1}$. We then have $n = q^{k-1}(qx + y_0) + y_1$. By the induction hypothesis, therefore, there are q^{k-1} vertices v' at distance $k-1$ from the root, $q^{k-1} - y_1$ of which satisfy $\ell(v') = qx + y_0$. Since $x \ge 1$, we have $qx + y_0 \ge q$, so each of these vertices will, by the properties of the well-balanced q-tree, have y_0 children v'' satisfying $\ell(v'') = x + 1$ and $q - y_0$ children v'' satisfying $\ell(v'') = x$. Similarly, y_1 of the vertices at distance $k-1$ from the root will satisfy $\ell(v') = qx + y_0 + 1$ and will have $y_0 + 1$ children v'' satisfying $\ell(v'') = x + 1$ and $q - y_0 - 1$ children v'' satisfying $\ell(v'') = x$. This gives a total of $y_0(q^{k-1} - y_1) + (y_0 + 1)y_1 = q^{k-1}y_0 + y_1 = y$ vertices v'' at distance k from the root with $\ell(v'') = x + 1$ and $(q - y_0)(q^{k-1} - y_1) + (q - y_0 - 1)y_1 = (q - y_0)q^{k-1} - y_1 = q^k - y$ vertices v'' at distance k from the root with $\ell(v'') = x$, as desired. This proves the final claim. □

5.4 The Largest Tree Contribution

We wish to estimate the contribution from the well-balanced q-tree. By the previous subsection, the well-balanced q-tree gives the largest contribution to the sum $s_n = \sum \prod_{v \in T} \beta_{\ell(v)}$.

The proof of Theorem 5.1 will follow from the following lemma.

Lemma 5.12. *Let T be the well-balanced q-tree. Set $\nu_n = \prod_{v \in T} \beta_{\ell(v)}$. Then*

$$\log_q \nu_n = -\frac{n^2}{2(1 - q^{-1})} - \frac{n \log_q n}{2} + O(n). \tag{5–7}$$

Proof: We first treat the contribution η to ν_n from vertices at distance more than $\log_q n$ from the root. By Lemma 5.11 (i)–(iii), there are $O(n)$ such vertices, and each contributes a factor of $\beta_1 = 1/q$ to $\nu_n = \prod_v \beta_{\ell(v)}$. Thus $\log_q \eta = O(n)$.

Let k be an integer such that $1 \le q^k \le n$. Write ω_k for the contribution to ν_n from the vertices at distance k from the root.

Write $n = q^k x + y$, with $0 \leq y \leq q^k - 1$. By Lemma 5.11 (iv), we have $\omega_k = \beta_x^{q^k - y} \beta_{x+1}^y$, so that,

$$\begin{aligned} \log_q \omega_k &= (q^k - y) \log_q \beta_x + y \log_q \beta_{x+1} \\ &= -(q^k - y) \binom{x+1}{2} - y \binom{x+2}{2} + O(q^k) \\ &= A + O(q^k), \quad \text{say}, \end{aligned}$$

by Lemma 5.7 (i). Next we calculate

$$\begin{aligned} A &= -\frac{x+1}{2}((q^k - y)x + y(x+2)) \\ &= -\frac{x+1}{2}(n+y) \\ &= -\frac{1}{2}\left(n + y + \frac{n-y}{q^k}(n+y)\right) \\ &= -\frac{1}{2}\left(\frac{n^2}{q^k} + n\right) + O(q^k), \end{aligned}$$

since $y = O(q^k)$. Now sum over k such that $1 \leq q^k \leq n$. Note that $\sum_k q^k$ is $O(n)$. Finally, we complete the proof of the lemma by noting that

$$\begin{aligned} \log_q \nu_n &= \sum_{1 \leq q^k \leq n} \log_q \omega_k + \log_q \eta \qquad (5\text{–}8) \\ &= -\frac{n^2}{2(1-q^{-1})} - \frac{n \log_q n}{2} + O(n). \end{aligned}$$

Theorem 5.1 is now proved. □

6. THE THIRD TERM

Let $q \geq 2$ be an integer. It seems natural to us to make the following conjecture concerning the third term in the asymptotic expansion of $\log_q r_n$.

Conjecture 6.1. *There is a continuous function W_q with period 1 such that*

$$\log_q r_n = -\frac{n^2}{2(q-1)} - \frac{1}{2} n \log_q n + W_q(\log_q n) n + O(1)$$

for all $n \geq 1$, where the implied constant depends on q.

If $q = 2$ then we are able to prove this.

Theorem 6.2. *Conjecture 6.1 is true for $q = 2$.*

We can rewrite Lemma 5.9 (ii) as

$$\log_q \nu_n = \log_q \beta_n + (q-y) \log_q \nu_x + y \log_q \nu_{x+1}, \quad (6\text{–}1)$$

where $n \geq 2$, $n = qx + y$, $0 \leq y \leq q$.

Empirically, we have observed that a similar recursion appears to hold for $\log_q s_n$. This is because the main contribution in (5–4) comes when all the b_i's differ by at most 1. For $q = 2$, we can prove this.

Lemma 6.3. *If $q = 2$ and $n \geq 2$, then $s_{n+1} s_{n-1} \leq \frac{1}{2} s_n^2$.*

Proof: Set

$$R_n = \frac{s_{n+1} s_{n-1}}{s_n^2} \qquad \text{for } n \geq 2. \qquad (6\text{–}2)$$

We have $s_1 = \frac{1}{2}$, and taking $q = 2$ in (5–4), we get, for $n \geq 2$,

$$s_n = \beta_n (s_1 s_{n-1} + s_2 s_{n-2} + \cdots + s_{n-1} s_1). \qquad (6\text{–}3)$$

Here, since $q = 2$, we have $\beta_n = 1/\big(2^{\binom{n+1}{2}} - 2\big)$.

We see from this by direct calculation that to three decimal places, $R_2 = 0.194, R_3 = 0.217$, $R_4 = 0.216$, and $R_5 = 0.230$. We see that $R_n \leq \frac{1}{2}$ for $2 \leq n \leq 5$. We will prove by induction on n that $R_n \leq \frac{1}{2}$ for all $n \geq 6$. It will be convenient to treat the cases of even and odd n separately.

Let $n = 2m$, so that $m \geq 3$. We see that

$$A_m := \frac{s_1 s_{2m-1} + \cdots + s_{2m-1} s_1}{s_m^2} \geq 1 + 2R_m \qquad (6\text{–}4)$$

by taking only the middle three terms.

On the other hand, if $2 \leq k \leq m$,

$$\begin{aligned} B_k &:= \frac{s_1 s_{2k} + \cdots + s_{2k} s_1}{s_k s_{k+1}} \qquad (6\text{–}5) \\ &= 2 + 2R_k R_{k+1} + 2R_{k-1} R_k^2 R_{k+1}^2 R_{k+2} + \cdots \\ &\quad + 2R_2 R_3^2 \cdots R_k^{k-1} R_{k+1}^{k-1} \cdots R_{2k-2}^2 R_{2k-1} \\ &\leq 2 + 2 \cdot \left(\frac{1}{2}\right)^2 + 2 \cdot \left(\frac{1}{2}\right)^6 + \cdots \leq 2.6, \end{aligned}$$

where the first inequality is by the induction hypothesis, and the second inequality is a calculation.

By definition, $R_n = R_{2m} = s_{2m+1} s_{2m-1} / s_{2m}^2$. By the recursion for s, we have

$$R_{2m} = \xi_{2m} R_m \frac{B_m B_{m-1}}{A_m^2}, \qquad (6\text{–}6)$$

where it is convenient to define $\xi_k = \beta_{k+1} \beta_{k-1} / {\beta_k}^2$.

Lemma 6.4. *If $k \geq 6$, then $\xi_k \leq 0.5001$.*

Proof: By definition,

$$\begin{aligned} \xi_k &= \frac{\beta_{k+1} \beta_{k-1}}{\beta_k^2} \\ &= \frac{(2^{(k^2+k)/2} - 2)^2}{(2^{(k^2+3k+2)/2} - 2)(2^{(k^2-k)/2} - 2)}. \end{aligned}$$

Divide numerator and denominator by 2^{k^2+k+1}. The new numerator is less than $\frac{1}{2}$. The new denominator is at least $1-2\cdot 2^{-(k(k-1)-2)/2} \geq 1-2\cdot 2^{-14}$. Therefore, $\xi_k \leq \frac{1}{2}(1-2^{-13})^{-1} \leq 0.5001$. □

Using the inequalities from Lemma 6.4, (6–4), and (6–5) in (6–6), we get

$$R_{2m} \leq 0.5001 \cdot (2.6)^2 \cdot \frac{R_m}{(1+2R_m)^2}.$$

However, by the induction hypothesis, $0 \leq R_m \leq \frac{1}{2}$, and since the function $x/(1+2x)^2$ is increasing on $[0, \frac{1}{2}]$, $R_m/(1+2R_m)^2 \leq \frac{1}{8}$. Since $0.5001\cdot(2.6)^2\cdot\frac{1}{8} \leq 0.423 \leq \frac{1}{2}$, $R_{2m} \leq \frac{1}{2}$, as desired.

The case of n odd is slightly more difficult. Let $n = 2m+1$, where again $m \geq 3$. We have

$$B_m = \frac{s_1 s_{2m} + \cdots + s_{2m}s_1}{s_m s_{m+1}} \geq 2 + 2R_m R_{m+1} \qquad (6\text{–}7)$$

by taking only the middle four terms.

On the other hand, if $2 \leq k \leq m+1$,

$$\begin{aligned} A_k &= \frac{s_1 s_{2k-1} + \cdots + s_{2k-1}s_1}{s_k^2} \qquad (6\text{–}8)\\ &= 1 + 2R_k + 2R_{k-1}R_k^2 R_{k+1} + \cdots \\ &\quad + 2R_2 \cdots R_k^{k-1} \cdots R_{2k-2} \\ &\leq b + 2R_k, \end{aligned}$$

where $b = 1 + 2\sum_{i\geq 2} 2^{-i^2}$, and we have used the induction hypothesis again. By a calculation, $b \leq 1.13$.

Combining the recursion for s with the inequalities (6–7) and (6–8) yields

$$\begin{aligned} &R_{2m+1} \qquad (6\text{–}9)\\ &\quad = \xi_{2m+1}\frac{A_m A_{m+1}}{B_m^2} \\ &\quad \leq \frac{1}{4}\xi_{2m+1}\frac{(2R_m+b)(2R_{m+1}+b)}{1+2R_m R_{m+1}} \\ &\quad = \frac{1}{4}\xi_{2m+1} \\ &\qquad \times \left(b^2 + \frac{2b(R_m+R_{m+1}) + (4-2b^2)R_m R_{m+1}}{1+2R_m R_{m+1}}\right). \end{aligned}$$

Clearly, $\frac{R_m+R_{m+1}}{1+2R_mR_{m+1}} \leq R_m + R_{m+1} \leq 1$, by the induction hypothesis. Also, $\frac{R_mR_{m+1}}{1+2R_mR_{m+1}} \leq \frac{1}{6}$. (Indeed, the function $g(x) = \frac{x}{1+2x}$ is increasing on the interval $[0, \frac{1}{4}]$, so its maximum value is $g(\frac{1}{4}) = \frac{1}{6}$.) These remarks, together with Lemma 6.4, (6–9), and the upper bound on b, imply

$$\begin{aligned} R_{2m+1} &\leq 0.25 \cdot 0.5001 \cdot \left(b^2 + 2b + \frac{4-2b^2}{6}\right) \\ &\leq 0.473 \leq \frac{1}{2}. \end{aligned}$$

This concludes the proof of the lemma. □

Theorem 6.5. *Suppose that $q = 2$. Then if $n \geq 2$, $n = qx + y$, and $0 \leq y \leq q$, we have*

$$\frac{1}{s_x^{q-y}s_{x+1}^y}\sum_{|b|=n}{}' \prod_{0\leq i\leq q-1} s_{b_i} \leq 3. \qquad (6\text{–}10)$$

Proof: This is obvious if n is 2 or 3. Otherwise, if $n = 2m$ is even, then by (6–8) and Lemma 6.3,

$$\sum_{j+k=n,\ j,\,k>0} s_j s_k = A_m s_m^2 \leq (1.13 + 2R_m)s_m^2 \leq 3s_m^2.$$

If $n = 2m+1$ is odd, then by (6–5),

$$\sum_{j+k=n,\ j,\,k>0} s_j s_k = B_m s_m s_{m+1} \leq 2.6 s_m s_{m+1}.$$

This completes the proof. □

We have proved the case $q = 2$ of the following conjecture.

Conjecture 6.6. *If $q \geq 2$ is an integer, then*

$$\log_q s_n = \log_q \beta_n + (q-y)\log_q s_x + y\log_q s_{x+1} + O(1)$$

where $n \geq 2$, $n = qx+y$, $0 \leq y \leq q$.

The next section is devoted to the proof of the following lemma:

Lemma 6.7. *For each integer $q \geq 2$, Conjecture 6.6 implies Conjecture 6.1.*

Since we have just seen that Conjecture 6.6 is true for $q = 2$, it will follow that Conjecture 6.1 is also true for $q = 2$, completing the proof of Theorem 6.2.

7. A RECURSION

Lemma 7.1. *Fix q and some constant $\bar{C}$, and for nonnegative integers n, set*

$$w_n = \begin{cases} -\frac{n^2}{2(1-q^{-1})} - \frac{1}{2}n\log_q n, & \textit{if } n > 0, \\ 0, & \textit{if } n = 0. \end{cases}$$

Then there is some constant C' such that if $a_1, \ldots, a_q$ satisfy $a_1 + \cdots + a_q = n \geq 1$, and for $i = 1, \ldots, q$, we have $|a_i - n/q| < \bar{C}$, then

$$|w_n - \log_q \beta_n - (w_{a_1} + \cdots + w_{a_q})| < C'. \tag{7–1}$$

Proof: Write $a_i = n/q + \epsilon_i$. It will suffice to prove (7–1) for large n. Take n large enough so that $|\epsilon_i| < \bar{C} < n/2q$. Now

$$\begin{aligned} w_{a_i} &= -\frac{(n/q + \epsilon_i)^2}{2\,(1 - q^{-1})} - \frac{1}{2}\left(\frac{n}{q} + \epsilon_i\right)\log_q\left(\frac{n}{q} + \epsilon_i\right) \\ &= -\frac{n^2}{2\,(q^2 - q)} - \epsilon_i\frac{n/q}{1 - q^{-1}} - \frac{\epsilon_i^2}{2\,(1 - q^{-1})} \\ &\quad - \frac{1}{2}\left(\frac{n}{q} + \epsilon_i\right)\log_q\frac{n}{q} \\ &\quad - \frac{1}{2}\left(\frac{n}{q} + \epsilon_i\right)\log_q\left(1 + \frac{\epsilon_i}{n/q}\right). \end{aligned}$$

Summing over i, we get

$$\begin{aligned} \sum_{1 \leq i \leq q} w_{a_i} = -\frac{n^2}{2(q - 1)} - \frac{1}{2}n(-1 + \log_q n) \\ - \sum_{1 \leq i \leq q}\frac{\epsilon_i^2}{2(1 - q^{-1})} \\ + \frac{1}{2}\left(\frac{n}{q} + \epsilon_i\right)\log_q\left(1 + \frac{\epsilon_i}{n/q}\right). \end{aligned} \tag{7–2}$$

By looking at the power series for $\log(1+x)$, we find that $|\log_q(1 + \chi)| \leq 4|\chi|$, if $|\chi| < \frac{1}{2}$. By our assumption on n, $|\epsilon_i|/(n/q) < \frac{1}{2}$, so $|\log_q(1 + \epsilon_i/(n/q))| \leq 4|\epsilon_i|/(n/q)$. It follows that the absolute value of the sum on the right-hand side of (7–2) is bounded, say by C'', so

$$\left|-\frac{n^2}{2(q - 1)} + \frac{1}{2}n - \frac{1}{2}n\log_q n - (w_{a_1} + \cdots + w_{a_q})\right| \leq C''.$$

The result now follows from the definition of w_n and Lemma 5.7 (i). □

If we assume that Conjecture 6.6 is true and set $\Omega_n = -w_n + \log_q s_n$, we can rewrite

$$\log_q s_n = \log_q \beta_n + (q - y)\log_q s_x + y\log_q s_{x+1} + O(1)$$

as the recursion

$$\Omega_n = (q - y)\Omega_x + y\Omega_{x+1} + \epsilon_n \tag{7–3}$$

for $n \geq 2$, where $n = qx + y$ and $0 \leq y \leq q$. Since $s_0 = 1$ and $w_0 = 0$, we also have

$$\Omega_0 = 0. \tag{7–4}$$

In the following theorem, we show how to solve this recursion if ϵ_n does not grow too rapidly with n. In our case, Lemma 7.1 implies that $\epsilon_n = O(1)$, so it will suffice to take $\kappa = 0$.

Theorem 7.2. *If $(\Omega_n)_{n \geq 0}$ satisfies (7–3) and (7–4), and $\epsilon_n = O(n^\kappa)$ for $0 \leq \kappa < 1$, then there exists a continuous function $\bar{W}$ with period 1 such that*

$$\Omega_n = \bar{W}(\log_q n)n + O(n^\kappa).$$

Proof: Let $n \geq 1$. It is clear from (7–3) and (7–4) that if we set $\epsilon_1 = \Omega_1$, and let T be the well-balanced q-tree with n leaves, then Ω_n is the sum of $\epsilon_{\ell(v)}$ over all vertices v of T. Write $\lfloor z \rfloor$ for the largest integer that is no more than z and $\{z\}$ for $z - \lfloor z \rfloor$. Now define $X(m)$ by

$$X(m) = \begin{cases} 0, & m < q^{-1}; \\ 2\epsilon_1\left(m - q^{-1}\right), & q^{-1} \leq m < 2q^{-1}; \\ \epsilon_1 m, & 2q^{-1} \leq m < 1; \\ \epsilon_{1+\lfloor m \rfloor}\{m\} + \epsilon_{\lfloor m \rfloor}(1 - \{m\}), & 1 \leq m. \end{cases}$$

Observe that X is continuous and that $X(m) = O(m^\kappa)$. Now Lemma 5.11 implies that the contribution to Ω_n from vertices at distance k from the root of T is $q^k X(n/q^k)$, so

$$\Omega_n = \sum_{k \geq 0} q^k X\left(\frac{n}{q^k}\right).$$

Note that the summand is zero for $k > Z := \lfloor \log_q n \rfloor + 1$. Now

$$\begin{aligned} \frac{\Omega_n}{n} &= \sum_{0 \leq k \leq Z}\frac{X(n/q^k)}{n/q^k} \\ &= \sum_{-Z \leq k \leq 0}\frac{X(nq^k)}{nq^k} \\ &= \sum_{k \geq -Z}\frac{X(nq^k)}{nq^k} + O(n^{\kappa - 1}), \end{aligned} \tag{7–5}$$

since $X(m)/m = O\left(m^{\kappa-1}\right)$.

Set

$$\bar{W}(m) = \sum_{k \geq -1-\lfloor m \rfloor}\frac{X(q^{m+k})}{q^{m+k}}, \tag{7–6}$$

or equivalently,

$$\bar{W}(m) = \zeta(\{m\}), \qquad \zeta(x) = \sum_{k \geq -1}\frac{X(q^{x+k})}{q^{x+k}}. \tag{7–7}$$

It is now clear from (7–5) and (7–6) that $\Omega_n = \bar{W}(\log_q n)n + O(n^\kappa)$. However, from (7–7), $X(m)/m = O(m^{\kappa-1})$, and the continuity of X, we see that on $[0,1]$, ζ is a sum of continuous functions that are uniformly bounded by a convergent series. Therefore ζ is continuous on $[0,1]$. The continuity of $\bar{W}$ now follows from the continuity of ζ on $[0,1]$ and the fact that since $X(q^{-1}) = 0$, $\zeta(0) = \zeta(1)$. This concludes the proof. □

Lemma 6.7 is now proved.

8. FURTHER THOUGHTS

The recursion (2–1) for r_n as a function of q is well-defined for any complex number q that isn't a root of unity. Curiously, the asymptotic behavior of $r_n(q)$ for nonintegers q is radically different from its behavior for integers q. It can be shown (we omit the proof) by singularity analysis, using the functional equation (1–2), that for $|q| \geq 3$ a noninteger there are nonzero constants A and B such that

$$r_n(q) \sim AB^n/n^{q+1},$$

so that $r_n(q)$ decreases much more slowly with n for nonintegers q than for integers q.

It seems natural to wonder whether for real noninteger q, the combinatorially defined $r_n(q)$ have a probabilistic interpretation. This appears not to be the case: experimentally we have observed that if $q > 2$ is a real noninteger then the quantity B is real and negative, so that $r_n(q)$ oscillates in sign (for n large). Of course, even a single negative value means that it is not possible to interpret $r_n(q)$ as a probability.

We mention some open questions for further research.

1. Zeros of the numerator. Let N_n be the numerator of r_n. Is it true that N_n has no zeros on the negative real axis?
2. Zeros of G. Let $q \geq 2$ be an integer. Is it true that the zeros of the function $G = \sum_{n\geq 0} s_n t^n$ are all real and negative?

We remark that the zeros $|z_0| \leq |z_1| \leq \cdots$ of G completely determine G as follows. Because $G(t)$ is an entire function of order zero, i.e., for all $\alpha > 0$, $|G(z)| = o\left(e^{|z|^\alpha}\right)$ as $|z| \to \infty$, it is equal up to a constant factor to the Weierstrass product $\prod_{i\geq 0}\left(1 - \frac{t}{z_i}\right)$. But then $G(t)$ equals this product since $G(0) = 1$.

3. Asymptotics. Prove Conjectures 6.1 and 6.6 concerning the asymptotics of the third term for $q > 2$ an integer.

REFERENCES

[Auel 03] Asher N. Auel. "Volumes of Integer Polynomials over Local Fields." B.A. thesis, Reed College, 2003.

[Euler 48] Leonhard Euler. *Introductio in Analysin Infinitorum 1* (1748), §76.

[Gordon et al. 86] L. Gordon, M. Schilling, and M. Waterman. "An Extreme Value Theory for Long Head Runs." *Probab. Theory Relat. Fields* 72:2 (1986), 279–287.

[Kirschenhofer and Prodinger 96] P. Kirschenhofer and H. Prodinger. "The Number of Winners in a Discrete Geometrically Distributed Sample." *Ann. Appl. Probab.* 6:2 (1996), 687–694.

[Li and Pomerance 01] S. Li and C. Pomerance. "Primitive Roots: A Survey." In *Number Theoretic Methods: Future Trends. Proc. China–Japan Seminar on Number Theory, Iizuka, Japan, 2001*, Dev. Math., 8, S. Kanemitsu and C. Jia, eds., pp. 219–231, Dordrecht, Kluwer Acad. Publ., 2002.

Joe Buhler, Center for Communications Research, 4320 Westerra Court, San Diego, CA 92121
(buhler@ccrwest.org).

Daniel Goldstein, Center for Communications Research, 4320 Westerra Court, San Diego, CA 92121
(dgoldste@ccrwest.org).

David Moews, Center for Communications Research, 4320 Westerra Court, San Diego, CA 92121
(dmoews@ccrwest.org).

Joel Rosenberg, Center for Communications Research, 4320 Westerra Court, San Diego, CA 92121
(joelr@ccrwest.org).

Received March 18, 2004; accepted November 3, 2005.