The Probability that Random Polynomials Are Relatively r-Prime

Kent E. Morrison
Department of Mathematics
California Polytechnic State University
San Luis Obispo, CA 93407
kmorriso@calpoly.edu

Zhou Dong [*]
Department of Mathematics
University of Illinois
Urbana, IL 61801
zhoudong@math.uiuc.edu

October 4, 2004

Abstract

We find the generating function for the number of k-tuples of monic polynomials of degree n over $\mathbf{F}_q$ that are relatively r-prime, meaning they have no common factor that is an rth power. A corollary is the probability that k monic polynomials of degree n are relatively r-prime, which we express in terms of a zeta function for the polynomial ring. This gives an analogue of Benkoski's result concerning the density of k-tuples of relatively r-prime integers. Special cases include that of pairs of relatively prime polynomials ($k = 2$ and $r = 1$) and square-free polynomials ($k = 1$ and $r = 2$). We also generalize to the broader context of prefabs and their generating functions.

In this paper we consider for polynomials over a finite field the analogues of classical results in probabilistic number theory going back to 1874 when Mertens [9] proved that the probability that two positive integers are relatively prime is s $6/\pi^2$ or $1/\zeta(2)$. This result was extended by D. N. Lehmer [8] in 1900 to show that the probability that k positive integers are relatively

[*] Partially supported by NSF Grant DMS-0097392

prime is $1/\zeta(k)$. In 1885 Gegenbauer [4] proved that $1/\zeta(r)$ is the probability that a positive integer is not divisible by an rth power, where $r \geq 2$ is a fixed integer. More recently, in 1976 Benkoski [2] unified these results by proving that the probability that k positive integers do not have a common rth power factor is $1/\zeta(kr)$. As a guide to the history of this material and for related results we recommend Hardy and Wright [5] and Kac [7]. Short, accessible proofs of Lehmer's result and of Gegenbauer's result for $r = 2$ (the square-free probability) are in papers of Nymann [10] and [11]. A readable and heuristic approach at the student level is in a fairly recent article of Jones [6].

The main result of this paper are two analogues of Benkoski's theorem for polynomials over a finite field and proved with combinatorial techniques. Similar results are in the literature, but it does not appear that the unified analogue of Benkoski's theorem has been published. Then we show how the first analogue fits into the wider context of prefabs.

Let q be a prime power and let $\mathbf{F}_q$ be the finite field of order q. We consider polynomials with coefficients in $\mathbf{F}_q$. For an integer $r \geq 1$ we say that polynomials $f_1, \ldots, f_k$ are **relatively r-prime** if they have no common factor of the form h^r, where $\deg h > 0$. When $r = 1$, this is the usual notion of being relatively prime.

Theorem 1 *Let c_n be the number of k-tuples of monic polynomials of degree n that are relatively r-prime. Let $C(t) = \sum_{n\geq 0} c_n t^n$ be the ordinary power series generating function of the c_n. Then*

$$C(t) = \frac{1 - qt^r}{1 - q^k t}$$

and

$$c_n = \begin{cases} q^{kn} & 0 \leq n \leq r-1 \\ q^{kn} - q^{kn-kr+1} & n \geq r \end{cases} .$$

Proof Partition the q^{kn} k-tuples $(f_1, \ldots, f_k)$ into subsets according to the degree i of the monic polynomial h where h^r is the greatest common rth power divisor. Then $(f_1/h^r, \ldots, f_k/h^r)$ is a tuple with no common rth power divisors. There are c_{n-ir} such k-tuples. Therefore,

$$q^{kn} = \sum_{i\geq 0} q^i c_{n-ir}.$$

We construct the generating function and change indices by letting $j =$

$n - ir$:

$$\begin{aligned}\sum_{n\geq 0} q^{kn} t^n &= \sum_{n\geq 0}\sum_{i\geq 0} q^k c_{n-ir} t^n \\ &= \sum_{n\geq 0}\sum_{i\geq 0} q^k t^{ir} c_{n-ir} t^{n-ir} \\ &= \sum_{j\geq 0}\sum_{i\geq 0} q^k t^{ir} c_j t^j \\ &= \sum_{j\geq 0} c_j t^j \sum_{i\geq 0} q^i t^{ir}\end{aligned}$$

From this we see that

$$\sum_{n\geq 0} c_n t^n = (1 - qt^r) \sum_{n\geq 0} q^{kn} t^n.$$

Comparing the coefficients of t^n gives the formula for the c_n. Sum the geometric series on the right to see that

$$C(t) = \frac{1 - qt^r}{1 - q^k t}.$$

□

Corollary 2 *The probability that k monic polynomials of degree n are relatively r-prime is*

$$1 - \frac{1}{q^{kr-1}}.$$

□

This probability is, of course, also the asymptotic probability as $n \to \infty$ and should be seen as the polynomial analogue of $1/\zeta(kr)$ in Benkoski's theorem. We will see that it is indeed the reciprocal of the value at $s = kr$ of the zeta function of the polynomial ring $\mathbf{F}_q[x]$. This zeta function is defined by

$$\zeta_q(s) = \sum_{\mathfrak{a}} \frac{1}{(\mathrm{N}\mathfrak{a})^s},$$

where the sum is over all ideals of $\mathbf{F}_q[t]$ and $\mathrm{N}\mathfrak{a}$, the norm of the ideal $\mathfrak{a}$, is the order of the residue ring $\mathbf{F}_q[t]/\mathfrak{a}$. Every ideal is principal and generated by a unique monic polynomial. There are q^n monic polynomials of degree n and hence q^n ideals of norm q^n. Therefore,

$$\begin{aligned}\zeta_q(s) &= \sum_{n\geq 0} \frac{q^n}{q^{ns}} \\ &= \frac{1}{1-q^{1-s}}.\end{aligned}$$

Thus, from Corollary 2 the probability that k polynomials are relatively r-prime is given by

$$\frac{1}{\zeta_q(kr)} = 1 - \frac{1}{q^{kr-1}}.$$

There is an alternative polynomial analogue for which we consider k-tuples of polynomials of degree less than or equal to n. In some sense this may be more like the integer case in which the density of a subset of $\mathbf{N}^k$ is defined by counting those tuples less than or equal to n. On the other hand, the limit probability as $n \to \infty$ remains the same even though the number of relatively r-prime k-tuples changes.

Theorem 3 *Let e_n be the number of relatively r-prime k-tuples $(f_1, \ldots, f_k)$ of polynomials of degree less than or equal to n, and let $E(t) = \sum e_n t^n$. Then*

$$E(t) = (1 - qt^r)\left(\frac{q^k}{1-q^k t} - \frac{1}{1-t}\right)$$

and

$$e_n = \begin{cases} q^{k(n+1)} - 1 & 0 \leq n \leq r-1 \\ q^{k(n+1)} - q^{k(n+1-r)+1} + q - 1 & n \geq r \end{cases}.$$

Proof There are $q^{k(n+1)}$ k-tuples $(f_1, \ldots, f_k)$, where $\deg f_i \leq n$. Setting aside $(0, 0, \ldots, 0)$, we partition the remaining $q^{k(n+1)} - 1$ non-zero k-tuples, just as before, into subsets according to the degree of the greatest common rth power factor. Then

$$q^{k(n+1)} = 1 + \sum_{i\geq 0} q^i e_{n-ir}.$$

Now we proceed as in the proof of Theorem 1 to see that

$$\sum_{n\geq 0} e_n t^n = (1 - qt^r) \sum_{n\geq 0} \left(q^{k(n+1)} - 1\right) t^n.$$

Compare the coefficients of t^n to derive the formula for e_n and sum the geometric series to derive the closed form for $E(t)$. □

Corollary 4 *The probability that k random polynomials are relatively r-prime is*

$$\frac{1}{\zeta_q(kr) =}1-\frac{1}{q^{kr-1}}.$$

Proof This probability is the limit

$$\lim_{n\to\infty}\frac{e_n}{q^{k(n+1)}},$$

and its value follows immediately from the theorem. □

The monic polynomials over a finite field are an example of a **prefab** [1, 12]. We will consider a prefab $\mathcal{P}$ having a_n objects of order n and associated generating function $A(t)=\sum_{n\geq 0}a_nt^n$. For the prefab of monic polynomials over $\mathbf{F}_q$, the order of a polynomial is its degree, $a_n=q^n$, and $A(t)=(1-qt)-1$. To put Theorem 1 into the context of prefabs we consider k-tuples of objects of order n, the number of which is ${a_n}^k$. Let

$$A^{[k]}(t)=\sum_{n\geq 0}{a_n}^kt^n$$

be the associated generating function. Now let c_n be the number of k-tuples of objects of order n having no common constituent that is repeated r times in each element of the tuple. Then, just as for polynomials, we have

$${a_n}^k=\sum_{i\geq 0}a_ic_{n-ir}.$$

Therefore

$$\sum_{n\geq 0}{a_n}^kt^n=\sum_{n\geq 0}\sum_{0\leq i\leq n}a_it^{ir}c_{n-ir}t^{n-ir},$$

and so we see that $A^{[k]}(t)=A(t^r)C(t)$, which leads to the prefab generalization of Theorem 1

$$C(t)=\frac{A^{[k]}(t)}{A(t^r)}.$$

For the case $r=1$, that is for relatively prime tuples in prefabs, this was derived in [3]. Now Theorem 1 follows from this equation because for polynomials $A^{[k]}(t)=(1-q^kt)^{-1}$ and $A(t^r)=(1-qt^r)^{-1}$.

References

[1] E. A. Bender and J. R. Goldman, Enumerative uses of generating functions, Indiana Univ. Math. J. **20** (1970/1971), 753–765.

[2] S. J. Benkoski, The probability that k positive integers are relatively r-prime, *J. Number Theory* **8** (1976) 218–223.

[3] S. Corteel, C. D. Savage, H. S. Wilf, and D. Zeilberger, A pentagonal number sieve, *J. Combin. Theory Ser. A* **82** (1998) 186–192.

[4] L. Gegenbauer, Asymptotische Gesetze der Zahlentheorie, *Denkshcriften Akad. Wien* **49** (1885) 37–80.

[5] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, fifth edition. Oxford Univ. Press, Oxford, 1979.

[6] G. A. Jones, $6/\pi^2$, *Mathematics Magazine* **66** (1993) 290–298.

[7] M. Kac, *Statistical Independence in Probability, Analysis and Number Theory.* Carus Monographs, no. 12. Mathematical Association of America, Washington, D.C., 1959.

[8] D. N. Lehmer, Asymptotic evaluation of certain totient sums. *Amer. J. Math.* **22** (1900) 293–335.

[9] F. Mertens, Über einige asymptotische Gesetze der Zahlentheorie, *J. Reine Angew. Math.* **77** (1874) 289–338.

[10] J. E. Nymann, On the probability that k positive integers are relatively prime. J. Number Theory **4** (1972) 469–473.

[11] J. E. Nymann, A note concerning the square-free integers. *Amer. Math. Monthly* **79** (1972) 63–65.

[12] H. S. Wilf, *Generatingfunctionology*, Second edition, Academic Press, Boston, MA, 1994.