Scientific Research Publishing

Advances in Pure Mathematics, 2022, 12, 70-79
https://www.scirp.org/journal/apm
ISSN Online: 2160-0384
ISSN Print: 2160-0368

Factorization Patterns in $\mathbb{F}_q[x]$

Thomas Beatty, Nicole Legge

Department of Mathematics, Florida Gulf Coast University, Fort Myers, USA
Email: tbeatty@fgcu.edu, nlegge@fgcu.edu

How to cite this paper: Beatty, T. and Legge, N. (2022) Factorization Patterns in $\mathbb{F}_q[x]$. *Advances in Pure Mathematics*, **12**, 70-79.
https://doi.org/10.4236/apm.2022.122006

Received: January 6, 2022
Accepted: February 12, 2022
Published: February 15, 2022

Abstract

The finite field $\mathbb{F}_q$ has q elements, where $q = p^k$ for prime p and $k \in \mathbb{N}$. Then $\mathbb{F}_q[x]$ is a unique factorization domain and its polynomials can be bijectively associated with their unique (up to order) factorizations into irreducibles. Such a factorization for a polynomial of degree n can be viewed as conforming to a specific template if we agree that factors with higher degree will be written before those with lower degree, and factors of equal degree can be written in any order. For example, a polynomial $f(x)$ of degree n may factor into irreducibles and be written as $(a)(b)(c)$, where $\deg a \geq \deg b \geq \deg c$. Clearly, the various partitions of n correspond to the templates available for these canonical factorizations and we identify the templates with the possible partitions. So if $f(x)$ is itself irreducible over $\mathbb{F}_q$, it would belong to the template $[n]$, and if $f(x)$ split over $\mathbb{F}_q$, it would belong to the template $[1,1,\cdots,1]$. Our goal is to calculate the cardinalities of the sets of polynomials corresponding to available templates for general q and n. With this information, we characterize the associated probabilities that a randomly selected member of $\mathbb{F}_q[x]$ belongs to a given template. Software to facilitate the investigation of various cases is available upon request from the authors.

Keywords

Finite Field, Factorization, Polynomial, Degree, Irreducible, Splitting, Partition, Probability

1. Introduction

Our purpose is to develop probability estimates for factorization of polynomials over finite fields. In particular, we will explore the fine structure of patterns in which the irreducible factors appear. Since a polynomial ring over a field is a unique factorization domain, each polynomial has a representation as a product

of irreducibles which is unique up to order of factors. To organize our combinatorial perspective, we may tighten up the uniqueness modulo order by imposing an additional minor condition on the degrees of the factors... higher degrees written before lower degrees, and equal degrees written interchangeably. Then any canonical factorization is unique up to the order of factors [1] [2] [3] of the same degree. Each factorization in this manner corresponds to a partition of the degree n of the factored polynomial belonging to $\mathbb{F}_q[x]$. The possible partitions of n induce in a natural way an equivalence relation on the family of irreducible factorizations for a given degree. The equivalence classes can be identified as templates for factorization, and the fact that they are mutually disjoint allows us to take a combinatorial approach to the problem of counting them. Our task is to present a method for enumerating these templates for general q and n, implement the method for selected small n, and use this data to calculate the probability that a randomly selected element of $\mathbb{F}_q[x]$ with specified degree belongs to a particular template. These will include, of course, both the probabilities for splitting and for being irreducible.

Some notation will help. For $q=p^k$ with p prime and $k\in\mathbb{N}$, the number of elements in $\mathbb{F}_q[x]$ of degree n will be denoted by $N(q,n)$. The number of elements in $\mathbb{F}_q[x]$ of degree n which are themselves irreducible will be denoted by $I(q,n)$. The number of elements in $\mathbb{F}_q[x]$ of degree n which are reducible will be denoted by $R(q,n)$. So $N(q,n)=I(q,n)+R(q,n)$. The classical probability that a random element of $\mathbb{F}_q[x]$ with degree n can be factored is $\pi(q,n)=\dfrac{R(q,n)}{N(q,n)}$, and its complement is $\bar{\pi}(q,n)=\dfrac{I(q,n)}{N(q,n)}$. A partition $\lambda\vdash n$ defines a factorization template for a polynomial of degree n as follows. If $\lambda=[i_1,\cdots,i_r]$, where $j<m$ implies $i_j\geq i_m$ and $\sum_{j=1}^{r} i_j=n$, the polynomials belonging to the λ-template class all factor into r irreducibles, arranged from left to right in order of weakly decreasing degree i_j. The number of elements in $\mathbb{F}_q[x]$ of degree n which belong to λ will be denoted by $N(q,n,\lambda)$. For example, the number of cubics over $\mathbb{F}_9$ that factor into linear times a quadratic factor would be $N(9,3,[2,1])$. The probability that a random element of $\mathbb{F}_q[x]$ of degree n belongs to the template λ is then $\beta(q,n,\lambda)=\dfrac{N(q,n,\lambda)}{N(q,n)}$. Note that $\beta(q,n,[1,1,\cdots,1])$ is the probability that the random polynomial splits over $\mathbb{F}_q$, and $N(q,n,[n])=I(q,n)$, so $\beta(q,n,[n])=\bar{\pi}(q,n)$ by definition, and we will consider $[n]$ an improper or trivial "factorization" template.

2. Monics Are Sufficient

Our life will be made easier in the sequel if we can work with monic polynomials instead of fully general ones. If $f(x)\in\mathbb{F}_q[x]$ has degree n, then certainly its leading coefficient, say α_n, is nonzero. It follows that $\alpha_n^{-1}f(x)=\hat{f}(x)$ is monic of degree n, and any factorization of $f(x)$ can be expressed as α_n times a factorization of $\hat{f}(x)$. None of the template structure is changed by this and our

study of the possible patterns will not be affected. The probabilities that we calculate are based on ratios of cardinalities of sets of monic polynomials. Any such ratio will be the same for the corresponding general polynomials since the number of nonzero choices $(q-1)$ for leading coefficient will appear in both the numerator and denominator and hence cancel. From this point on, all polynomials will be assumed to be monic.

3. Irreducibles in $\mathbb{F}_q[x]$

A great help in enumerating the various templates is a formula originally due to Gauss, which extends to values of q which are prime powers. The number of irreducible polynomials of degee n over $\mathbb{F}_q$ is given by $I(q,n)=\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)q^d$. Here $\mu(k)$ is the Möbius function and d is any divisor of the degree n. Recall $\mu:\mathbb{N}\to\{-1,0,1\}$ is defined by $\mu(1)=1$, $\mu(p_1\cdots p_m)$ for a product of distinct primes p_i is 1 if m is even and -1 if it is odd, and finally $\mu(j)=0$ for any other $j\in\mathbb{N}$. This formula may be derived using Möbius inversion or more transparently using the Inclusion/Exclusion Principle [4]. For example, $I(3,5)=\frac{1}{5}\sum_{d|n}\mu\left(\frac{5}{d}\right)3^d=\frac{1}{5}\left[\mu(5)3^1+\mu(1)3^5\right]=48$. It is worth noting that if n itself is prime and $q=p^k$, then $I(q,n)=\frac{1}{n}\left[\mu(1)q^n+\mu(n)q^1\right]=\frac{1}{n}\left[p^{kn}-p^k\right]$. It is also apparent that the numbers $I(q,n)$, given immediately by the extended Gauss formula, can in principle be recovered for a fixed q and any n by an obvious bootstrapping argument starting with degree $n=2$.

4. Motivating Example

Before we explore the general method, let us illustrate the approach by determining the populations and corresponding probabilities for all the factorization templates of quartics over $\mathbb{F}_q[x]$. First, the total number of quartics $N(q,4)=q^4$, and the Gauss formula for $n=4$ yields $I(q,4)=\frac{1}{4}\left(\mu(1)q^4+\mu(2)q^2+\mu(4)q\right)=\frac{1}{4}\left(q^4-q^2\right)$. There are four non-trivial templates: $[1,1,1,1]$, $[2,1,1]$, $[2,2]$, and $[3,1]$. For the splitting template $[1,1,1,1]$, corresponding to the factorization $(x-r_1)(x-r_2)(x-r_3)(x-r_4)$, there are four zeroes to be selected *with replacement* from q field values available. This yields $N(q,4,[1,1,1,1])=\left(\!\!\binom{q}{4}\!\!\right)=\binom{q+3}{4}=\frac{q^4+6q^3+11q^2+6q}{24}$ possibilities including all various configurations of multiple zeroes. For the $[2,1,1]$ template, corresponding to the factorization $P_2(x)(x-r_1)(x-r_2)$, where $P_2(x)$ is an irreducible quadratic, there are $I(q,2)=\frac{q^2-q}{2}$ possibilities from the Gauss formula for $n=2$. Also there are $\left(\!\!\binom{q}{2}\!\!\right)=\binom{q+1}{2}=\frac{q^2+q}{2}$ possibilities for selecting

two zeroes with replacement. The number of total selections for the $[2,1,1]$ template is then $\frac{q^4-q^2}{4}$. Moving to the $[2,2]$ template, we re-use the multiset formula for two factors, but now instead of q choices among field values we have $I(q,2)$ choices among the available quadratic irreducibles. This gives $\left(\!\!\binom{I(q,2)}{2}\!\!\right)=\frac{\left[I(q,2)\right]^2+I(q,2)}{2}=\frac{q^4-2q^3+3q^2-2q}{8}$ choices for the two irreducible quadratics, again with replacement. Being able to use the same multiset formulas repeatedly will save a lot of work for the higher degree cases. Finally, the $[3,1]$ template is the easiest to enumerate. Again by the Gauss formula there are $I(q,3)=\frac{1}{3}\left(q^3-q\right)$ choices for the irreducible cubic and q choices for the linear term, giving $\frac{q^4-q^2}{3}$ possibilities for this template. Summarizing:

1) $N(q,4)=q^4$
2) $I(q,4)=N(q,4,[4])=\frac{1}{4}\left(q^4-q^2\right)$
3) $N(q,4,[1,1,1,1])=\frac{q^4+6q^3+11q^2+6q}{24}$
4) $N(q,4,[2,1,1])=\frac{q^4-q^2}{4}$
5) $N(q,4,[2,2])=\frac{q^4-2q^3+3q^2-2q}{8}$
6) $N(q,4,[3,1])=\frac{1}{3}\left(q^4-q^2\right)$

We verify $\sum_{\lambda\vdash 4}N(q,4,\lambda)=N(q,4)$, and after computing the corresponding probability ratios, we have shown:

Proposition 1

If $f(x)\in\mathbb{F}_q[x]$ and $\deg f=4$, then: $\pi(q,4)=\frac{3}{4}+\frac{1}{4q^2}$,

$\overline{\pi}(q,4)=\frac{1}{4}-\frac{1}{4q^2}$, $\beta(q,4,[1,1,1,1])=\frac{1}{24}+\frac{1}{4q}+\frac{11}{24q^2}+\frac{1}{4q^3}$,

$\beta(q,4,[2,1,1])=\frac{1}{4}-\frac{1}{4q^2}$, $\beta(q,4,[2,2])=\frac{1}{8}-\frac{1}{4q}+\frac{3}{8q^2}-\frac{1}{4q^3}$,

$\beta(q,4,[3,1])=\frac{1}{3}-\frac{1}{3q^2}$.

Proof. Divide the template enumerations by q^4. Done. ■

5. General Case

All of the complications typical of the general case are on display in the preceding quartic example. We have seen that the Gauss formula gives a straightforward way to obtain $I(q,n)$. The multiset number counts up the ways a polynomial could split, and the multiset number applied to the various $I(q,n)$ in

place of q gives the number of ways a multiplicity of irreducible factors of common degree can appear in a factorization template.

Consider the family of polynomials of degree n in $\mathbb{F}_q[x]$. Suppose $f(x)$ belongs to this family and $f(x)=\prod_{j=1}^{r} g_j(x)$, where the $g_j(x)$ are written in order of (weakly) decreasing degree from left to right. We say $f(x)$ conforms to the template λ if $\lambda=[i_1,\cdots,i_j,\cdots,i_r]$ is a partition of n and $i_j=\deg g_j(x)$. In general, there will be repeated degrees among the $g_j(x)$ corresponding to repeated parts i_j in the partition of n. Let $\{\delta_1,\cdots,\delta_t\}$ be the set of *distinct* degrees of the factors of $f(x)$, and let m_k be the multiplicity of each δ_k, so that $\sum_{k=1}^{t} m_k\delta_k=n$. For example, if $\lambda=[3,2,2,2,1,1]$, $\delta_1=3$, $\delta_2=2$, and $\delta_3=1$, then $m_1=1$, $m_2=3$, and $m_1=2$.

Lemma 1

Let $f(x)\in\mathbb{F}_q[x]$ with $\deg f(x)=n$ and $f(x)=\prod_{j=1}^{r} g_j(x)$ with the preceding setup. If m_k is the multiplicity of the degree δ_k, then the number of canonical factorizations of $f(x)$ conforming to the template $\lambda=[i_1,\cdots,i_j,\cdots,i_r]$ is $N(q,n,\lambda)=\prod_{k=1}^{t}\left(\!\!\binom{I(q,\delta_k)}{m_k}\!\!\right)$.

Proof. The multiset number $\left(\!\!\binom{I(q,\delta_k)}{m_k}\!\!\right)$ is the number of ways a set of m_k irreducible factors of degree δ_k can be chosen with replacement from the $I(q,\delta_k)$ irreducible polynomials of degree δ_k available to fill the corresponding positions in the template. The choices for each δ_k are mutually independent, so the product over all t distinct degrees that occur in the template gives the total number of possible configurations overall, namely $N(q,n,\lambda)=\prod_{k=1}^{t}\left(\!\!\binom{I(q,\delta_k)}{m_k}\!\!\right)$. ■

So for each partition of the degree n: 1) we identify the distinct parts that appear in each partition (these are the distinct degrees that appear in the template), 2) find their multiplicity, and 3) compute the product in the lemma. We can now state the final result.

Proposition 2

The probability that a randomly selected polynomial $f(x)$ of degree n over $\mathbb{F}_q$

1) cannot be factored is $\bar{\pi}(q,n)=\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)q^{d-n}$.

2) can be factored is $\pi(q,n)=1-\bar{\pi}(q,n)$.

3) can be factored as $\prod_{j=1}^{r} g_j(x)$, where $\deg g_j(x)=i_j$ belongs to the partition $\lambda=[i_1,\cdots,i_j,\cdots,i_r]$ of n, is $\beta(q,n,\lambda)=\frac{1}{q^n}\prod_{k=1}^{t}\left(\!\!\binom{I(q,\delta_k)}{m_k}\!\!\right)$.

Proof. 1) The number $N(q,n)$ of (monic) polynomials over $\mathbb{F}_q$ is q^n. The number $I(q,n)$ of irreducible polynomials over $\mathbb{F}_q$ is $\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)q^d$. So

$\overline{\pi}(q,n)=\dfrac{I(q,n)}{N(q,n)}=\dfrac{1}{n}\sum_{d\mid n}\mu\left(\dfrac{n}{d}\right)q^{d-n}$.

2) Complementary probability.

3) The number $N(q,n,\lambda)$ of factorizations of $f(x)$ conforming to the template λ is $N(q,n,\lambda)=\prod_{k=1}^{t}\left(\binom{I(q,\delta_k)}{m_k}\right)$ by the Lemma, hence

$\beta(q,n,\lambda)=\dfrac{1}{q^n}\prod_{k=1}^{t}\left(\binom{I(q,\delta_k)}{m_k}\right)$. ■

6. Low Degree Cases

We now establish probability formulas for $n=2$ and $n=3$ (see $n=4$ above), and derive the multiset formulas up to $n=9$ to allow the determination of $\beta(q,n,\lambda)$ for specific $\lambda\vdash 10$. Since there are 42 partitions of 10, anything more than a "surgical" calculation for a particular λ or two seems impractical.

Proposition 3

1) If $f(x)\in\mathbb{F}_q[x]$ with $\deg f(x)=2$, then $\pi(q,2)=\beta(q,2,[1,1])=\dfrac{1}{2}+\dfrac{1}{2q}$ and $\overline{\pi}(q,2)=\beta(q,2,[2])=\dfrac{1}{2}-\dfrac{1}{2q}$.

2) If $f(x)\in\mathbb{F}_q[x]$ with $\deg f(x)=3$, then $\pi(q,3)=\dfrac{2}{3}+\dfrac{1}{3q^2}$, $\overline{\pi}(q,3)=\dfrac{1}{3}-\dfrac{1}{3q^2}$, $\beta(q,3,[1,1,1])=\dfrac{1}{6}+\dfrac{1}{2q}+\dfrac{1}{3q^2}$, and $\beta(q,3,[2,1])=\dfrac{1}{2}-\dfrac{1}{2q}$.

Proof. 1) From Proposition 2, $\overline{\pi}(q,2)=\dfrac{1}{2}\sum_{d\mid 2}\mu\left(\dfrac{2}{d}\right)q^{d-2}=\dfrac{1}{2}-\dfrac{1}{2q}$. Now the only non-trivial template is $[1,1]$, so

$\pi(q,2)=\beta(q,2,[1,1])=1-\overline{\pi}(q,2)=\dfrac{1}{2}+\dfrac{1}{2q}$.

2) Likewise, $\overline{\pi}(q,3)=\dfrac{1}{3}\sum_{d\mid 3}\mu\left(\dfrac{3}{d}\right)q^{d-3}=\dfrac{1}{3}-\dfrac{1}{3q^2}$, and it follows that $\pi(q,3)=1-\left(\dfrac{1}{3}-\dfrac{1}{3q^2}\right)=\dfrac{2}{3}+\dfrac{1}{3q^2}$. There are two proper templates: $[1,1,1]$ and $[2,1]$. Now $N(q,3,[1,1,1])=\left(\binom{q}{3}\right)=\dfrac{q^3}{6}+\dfrac{q^2}{2}+\dfrac{q}{3}$, so $\beta(q,3,[1,1,1])=\dfrac{N(q,3,[1,1,1])}{N(q,3)}=\dfrac{1}{q^3}\left(\dfrac{q^3}{6}+\dfrac{q^2}{2}+\dfrac{q}{3}\right)=\dfrac{1}{6}+\dfrac{1}{2q}+\dfrac{1}{3q^2}$. Also, using $I(q,2)=q^2\overline{\pi}(q,2)$ from the quadratic case,

$N(q,3,[2,1])=\left(\dfrac{1}{2}\left(q^2-q\right)\right)(q)=\dfrac{1}{2}q^3-\dfrac{1}{2}q^2$, so $\beta(q,3,[2,1])=\dfrac{1}{2}-\dfrac{1}{2q}$. ■

Observe from Propositions 1 and 3 that most of the probability that $f(x)$ factors at all seems to come from templates that are heavy with high degree factors. The flip side of this is that as n increases for a fixed q the probability of

$f(x)$ splitting or at least factoring into low degree pieces becomes smaller. We comment on this more fully in the Epilogue.

7. Computational Aids

Following are several computational aids for higher degree cases.

Enumerators for Multiple Factors of Same Degree

In the notation of Lemma 1 suppose there are exactly m_k irreducible polynomials of degree δ_k in a particular factorization of $f(x) \in \mathbb{F}_q[x]$. As noted in the Lemma, the pool of polynomials available to make m_k such selections is $I(q,\delta_k)$. It follows that there are $\left(\!\!\binom{I(q,\delta_k)}{m_k}\!\!\right)$ ways to do this. To simplify the entries, let us denote $I(q,\delta_k)$ by x.

$$m_k = 2 \qquad \left(\!\!\binom{x}{2}\!\!\right) = \frac{1}{2}x^2 + \frac{1}{2}x$$

$$m_k = 3 \qquad \left(\!\!\binom{x}{3}\!\!\right) = \frac{1}{6}x^3 + \frac{1}{2}x^2 + \frac{1}{3}x$$

$$m_k = 4 \qquad \left(\!\!\binom{x}{4}\!\!\right) = \frac{1}{24}x^4 + \frac{1}{4}x^3 + \frac{11}{24}x^2 + \frac{1}{4}x$$

$$m_k = 5 \qquad \left(\!\!\binom{x}{5}\!\!\right) = \frac{1}{120}x^5 + \frac{1}{12}x^4 + \frac{7}{24}x^3 + \frac{5}{12}x^2 + \frac{1}{5}x$$

$$m_k = 6 \qquad \left(\!\!\binom{x}{6}\!\!\right) = \frac{1}{720}x^6 + \frac{1}{48}x^5 + \frac{17}{144}x^4 + \frac{5}{16}x^3 + \frac{137}{360}x^2 + \frac{1}{6}x$$

$$m_k = 7 \qquad \left(\!\!\binom{x}{7}\!\!\right) = \frac{1}{5040}x^7 + \frac{1}{240}x^6 + \frac{5}{144}x^5 + \frac{7}{48}x^4 + \frac{29}{90}x^3 + \frac{7}{20}x^2 + \frac{1}{7}x$$

$$m_k = 8 \qquad \left(\!\!\binom{x}{8}\!\!\right) = \frac{1}{40320}x^8 + \frac{1}{1440}x^7 + \frac{23}{2880}x^6 + \frac{7}{144}x^5 + \frac{967}{5760}x^4 + \frac{469}{1440}x^3 + \frac{363}{1120}x^2 + \frac{1}{8}x$$

$$m_k = 9 \qquad \left(\!\!\binom{x}{9}\!\!\right) = \frac{1}{362880}x^9 + \frac{1}{10080}x^8 + \frac{13}{8640}x^7 + \frac{1}{80}x^6 + \frac{1069}{17280}x^5 + \frac{89}{480}x^4 \frac{29531}{90720}x^3 + \frac{761}{2520}x^2 + \frac{1}{9}x$$

Enumerators for Irreducible Polynomials over $\mathbb{F}_q$ by Degree

Here are the expressions for $I(q,\delta_k)$ with $1 \le \delta_k \le 9$ via the Gauss formula $I(q,\delta_k) = \frac{1}{\delta_k}\sum_{d|\delta_k} \mu\left(\frac{\delta_k}{d}\right) q^d$. These should be substituted as appropriate for x in the above.

1) $I(q,1) = q$

2) $I(q,2) = \frac{1}{2}\left(q^2 - q\right)$

3) $I(q,3) = \frac{1}{3}\left(q^3 - q\right)$

4) $I(q,4)=\frac{1}{4}\left(q^4-q^2\right)$

5) $I(q,5)=\frac{1}{5}\left(q^5-q\right)$

6) $I(q,6)=\frac{1}{6}\left(q^6-q^3-q^2+q\right)$

7) $I(q,7)=\frac{1}{7}\left(q^7-q\right)$

8) $I(q,8)=\frac{1}{8}\left(q^8-q^4\right)$

9) $I(q,9)=\frac{1}{9}\left(q^9-q^3\right)$

8. A Higher Degree Example

To illustrate the types of questions that can be answered with the machinery we have developed, consider the following. Suppose we are given a random $f(x)\in\mathbb{F}_q[x]$ with $\deg f(x)=7$.

1) What is the probability that $f(x)$ splits?

2) What is the probability that it has three irreducible quadratic factors?

3) If it has an irreducible quintic factor, what is the probability that it also has a zero in $\mathbb{F}_q$?

Solutions:

1) $N(q,7)=q^7$. Also $\left(\!\!\binom{I(q,1)}{7}\!\!\right)=\frac{1}{5040}q^7+\frac{1}{240}q^6+\frac{5}{144}q^5+\frac{7}{48}q^4+\frac{29}{90}q^3+\frac{7}{20}q^2+\frac{1}{7}q$. Then the splitting probability is

$$\beta(q,7,[1,1,1,1,1,1,1])=\frac{1}{5040}+\frac{1}{240q}+\frac{5}{144q^2}+\frac{7}{48q^3}+\frac{29}{90q^4}+\frac{7}{20q^5}+\frac{1}{7q^6},$$

which is miniscule.

2) If $f(x)$ has three irreducible quadratic factors, then the remaining factor

$$\beta(q,7,[2,2,2,1])=\left(\frac{1}{q^7}\right)\left(\!\!\binom{I(q,2)}{3}\!\!\right)\left(\!\!\binom{I(q,1)}{1}\!\!\right)$$

must be linear. So $=\left(\frac{1}{q^7}\right)\left(\frac{1}{6}\left(\frac{q^2-q}{2}\right)^3+\frac{1}{2}\left(\frac{q^2-q}{2}\right)^2+\frac{1}{3}\left(\frac{q^2-q}{2}\right)\right)(q)$.

$$=\frac{1}{48}-\frac{1}{16q}+\frac{3}{16q^2}-\frac{13}{48q^3}+\frac{7}{24q^4}-\frac{1}{6q^5}$$

For perspective, this would be $\frac{1}{64}$ for $q=2$. The only irreducible quadratic over $\mathbb{F}_2$ is x^2+x+1, so in this case $f(x)$ would have to be either $x\left(x^2+x+1\right)^3$ or $(x-1)\left(x^2+x+1\right)^3$. Since there are $2^7=128$ possible seventh degree polynomials over $\mathbb{F}_2$, and $\frac{2}{128}=\frac{1}{64}$, we have a hands-on confirmation of our re-

sult.

3) The templates that admit a quintic are $[5,2]$ and $[5,1,1]$. We need to parse the details of these two templates to compute a conditional probability. First, $N(q,7,[5,2]) = (I(q,5))(I(q,2)) = \left(\frac{q^5-q}{5}\right)\left(\frac{q^2-q}{2}\right) = \frac{q^7-q^6-q^3+q^2}{10}$. Next, $N(q,7,[5,1,1]) = (I(q,5))\left(\binom{q}{2}\right) = \left(\frac{q^5-q}{5}\right)\left(\frac{q^2+q}{2}\right) = \frac{q^7+q^6-q^3-q^2}{10}$. Now the total number of configurations featuring a quintic is $N(q,7,[5,2]) + N(q,7,[5,1,1]) = \frac{q^7-q^3}{5}$. It follows that the conditional probability of $f(x)$ having a zero, given that it has an irreducible quintic factor, is $\frac{N(q,7,[5,1,1])}{N(q,7,[5,1,1]) + N(q,7,[5,2])} = \frac{1}{2} + \frac{1}{2q}$. This should not be surprising, since once the quintic "has occurred" in the factorization, the remaining situation is that of factoring the residual degree available, which parallels the derivation in Proposition 3(1) exactly.

9. Epilogue

We can easily draw several conclusions regarding the limit behavior of three important probability estimates.

Proposition 4

Suppose $f(x) \in \mathbb{F}_q[x]$ and $\deg f(x) = n$. Then:

1) $\lim_{q\to\infty} \bar{\pi}(q,n) = \frac{1}{n}$ and $\lim_{q\to\infty} \pi(q,n) = \frac{n-1}{n}$.

2) $\lim_{q\to\infty} \beta(q,n,[1,1,\cdots,1]) = \frac{1}{n!}$.

Proof. 1) $N(q,n) = q^n$. By the Gauss formula, $I(q,n) = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$. Then $\bar{\pi}(q,n) = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) q^{d-n}$. Now $d-n<0$ unless $d=n$, in which case the term contributes $\frac{1}{n}\mu(1) = \frac{1}{n}$ to the sum. For all other divisors of n, since $\left|\mu\left(\frac{n}{d}\right) q^{d-n}\right|$ is at most $O\left(\frac{1}{q^{n/2}}\right)$, and $\lim_{q\to\infty} \frac{1}{q^{n/2}} = 0$, we have $\lim_{q\to\infty} \bar{\pi}(q,n) = \frac{1}{n}$. It follows that $\lim_{q\to\infty} \pi(q,n) = \frac{n-1}{n}$.

2)

$$R(q,n,[1,1,\cdots,1]) = \left(\binom{q}{n}\right) = \binom{q+n-1}{n} = \frac{1}{n!}\prod_{k=0}^{n-1}(q+k) = \frac{1}{n!}\left(q^n + O\left(q^{n-1}\right)\right).$$

Hence $\beta(q,n,[1,1,\cdots,1]) = \frac{1}{n!} + O\left(\frac{1}{q}\right)$ and since $\lim_{q\to\infty} \frac{1}{q} = 0$, the result follows. ■

The result in (1) is dramatically different from that of factoring over $\mathbb{Z}$,

which becomes less and less likely as the absolute bound on coefficients increases [5]. If q is very large, it may seem that the chances for a proper factorization of $f(x)$ would be about as slim as if the factorization were to be done over $\mathbb{Z}$. This is not the case, moreover, it becomes even more counterintuitive as q approaches infinity and the likelihood of factorability approaches 1. The companion result in (2) shows that the chance a randomly selected polynomial splits over $\mathbb{F}_q$ degrades very rapidly as degree and field cardinality grow.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Dummit, D.S. and Foote, R.M. (2003) Abstract Algebra. 3rd Edition, John Wiley and Sons, Inc., Hoboken, NJ.

[2] Gallian, J.A. (2010) Contemporary Abstract Algebra. 7th Edition, Brooks-Cole/Cengage Learning, Belmont, CA.

[3] Hungerford, T.W. (1974) Algebra. Springer Verlag, Berlin. https://doi.org/10.1007/978-1-4612-6101-8_4

[4] Chebolu, S.K. and Mináč, J. (2011) Counting Irreducible Polynomials over Finite Fields Using the Inclusion-Exclusion Principle. *Mathematics Magazine*, **84**, 369-371. https://doi.org/10.4169/math.mag.84.5.369

[5] Beatty, T. and von Linden, G. (2020) On Conditional Probabilities of Factoring Quadratics. *Advances in Pure Mathematics*, **10**, 114-124. https://doi.org/10.4236/apm.2020.103008