UNIVERSITÄT ZU LÜBECK
INSTITUT FÜR IT-SICHERHEIT

Analysis of the Distribution of Zeros of Polynomials and Their Relevance to Fault Attacks

Analyse der Verteilung von Nullstellen von Polynomen und deren Relevanz für Fault-Angriffe

Masterarbeit

verfasst am
Institut für IT-Sicherheit

im Rahmen des Studiengangs
IT Security
der Universität zu Lübeck

vorgelegt von
Lennart Ostendorf

ausgegeben und betreut von
Prof. Dr. Thomas Eisenbarth
Prof. Dr. Sebastian Berndt

mit Unterstützung von
Paula Arnold, M.Sc.

Lübeck, den 21. März 2025

Eidesstattliche Erklärung

Ich erkläre hiermit an Eides statt, dass ich diese Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

_____

Lennart Ostendorf

Zusammenfassung

Polynome haben eine Vielzahl an Anwendungen, wie zum Beispiel Interpolation oder lokale Approximation von Funktionen. In dieser Arbeit beschränken wir uns auf univariate Polynome über endlichen Körpern. Unser Beitrag ist dabei dreierlei: Zuerst untersuchen wir Polynome hinsichtlich ihrer Nullstellen. Hier betrachten wir verschiedene Varianten, unter anderem die Gesamtzahl von (unterschiedlichen) Nullstellen oder jene mit bestimmten Vielfachheiten an bestimmten Stellen. Wir zählen die Anzahl solcher Polynome und betrachten die entsprechenden Zufallsvariablen bei uniformer Wahl der Polynome. Ferner geben wir statistische Größen wie den Erwartungswert und die Varianz der Nullstellen an, sowie ihr asymptotisches Verhalten. Polynome finden ebenfalls in der Kryptografie Anwendung. Wir verbessern zwei Arbeiten, [BEF+23] und [ABEO24], die Shamir's (polynomielles) Secret Sharing verwenden, um Hardwareschaltkreise gegen kombinierte physikalische Angriffe zu schützen. Bei [BEF+23] verbessern wir eine obere Schranke der Wahrscheinlichkeit, dass ein Angreifer nicht entdeckt wird, der Fehler in einen Schaltkreis fügt. Wir argumentieren, dass unsere Schranke scharf ist, unter der vertretbaren Annahme, dass der Angreifer den Grad eines Faultpolynoms frei wählen kann. Zum Schluss präsentieren wir für den double-sharing Ansatz in [ABEO24] zwei Methoden, die stets erkennen, ob ein Angreifer Fehler hinzufügt. Dies verbessert vorherige Ergebnisse, die dies nur mit einer gewissen Wahrscheinlichkeit detektieren. Überdies stellen wir weitere Ansätze vor, die jedoch für das Szenario in [ABEO24] nicht oder nur partiell verwendbar sind. Näherhin funktionieren sie nur für bestimmte Schaltkreise oder können nicht für kombinierte Angriffe genutzt werden. Letzterem liegt zugrunde, dass kein Schutz gegen passive Angreifer besteht.

Abstract

Polynomials have various applications, such as interpolation or local function approximation. In this thesis, we consider univariate polynomials over finite fields. Our contribution is threefold: Firstly, we investigate polynomials regarding their zeros. We analyze several variants, such as a certain number of (distinct) zeros in total or zeros at specific positions and multiplicities. We count the number of polynomials satisfying these constraints and also consider the corresponding random variables when polynomials are sampled uniformly at random. Furthermore, we provide statistical properties such as the average number and variance of such zeros in polynomials and their asymptotic behavior. Polynomials are also used in cryptography. We improve two papers, [BEF+23] and [ABEO24], which employ Shamir's (polynomial) secret sharing to protect hardware circuits against combined physical attacks. In [BEF+23], we improve an upper bound on the probability that an adversary can fault a circuit without being detected. We argue that our bound is tight under the reasonable assumption that an adversary can choose the degree of a fault polynomial. Lastly, in [ABEO24], we present two methods that always detect an adversary introducing faults into the computation in the double-sharing setting. Moreover, we state further approaches, which, however, either only work with specific circuits or cannot be used for combined attacks. The latter is due to the lack of protection against passive adversaries.

Acknowledgements

Ein besonderer Dank gilt Professor Sebastian Berndt für seine umfassende Betreuung dieser Masterarbeit, die Beantwortung unzähliger Fragen und seine stetige Unterstützung. Ebenso danke ich Paula Arnold für ihre großartige Hilfe, insbesondere für das viele und ausführliche Feedback zu frühen Versionen der Arbeit. Nicht zuletzt danke ich auch Professor Thomas Eisenbarth, der diese Arbeit möglich gemacht hat.

Contents

1 Preliminaries 1

1.1 Algebra 1
1.2 Number Theory 4
1.3 Probability Theory 4
1.4 Generating Functions 6
1.5 Polynomials 9
1.6 Polynomial Secret Sharing 15

2 Introduction 18

2.1 Contributions of This Thesis 19
2.2 Related Work 19
2.3 Structure of This Thesis 21

3 Zeros of Polynomials 22

3.1 The Multiplicity of One Zero 23
3.2 The Multiplicities of Arbitrary Zeros 29
3.3 The Total Multiplicity of Arbitrary Zeros 33
3.4 The Positions of Zeros 38

4 Exact Detection Probabilities of Adversaries in Combined Attacks 42

4.1 Notes on the Original Theorem 44
4.2 Establishing Exact Probabilities 47
4.3 Upper Bounds and Comparison 50

5 Definitive Error Detection in the Double-Sharing Setting 55

5.1 Approach 1: Gadget-Specific Error Propagation 57
5.2 Approach 2: Additive Combination of Multiple Error Propagation 58
5.3 Approach 3: Separate Error Propagation 60
5.4 Approach 4: Indicator-Function-Based Error Detection 64
5.5 Approach 5: Division-Based Truncation of All Lower-Order Terms 66
5.6 Approach 6: Matrix-Based Truncation of All Lower-Order Terms 68

6 Conclusion and Outlook 71

Bibliography 73

1

Preliminaries

In this chapter, we first provide some notation used throughout this thesis. Afterward, we present definitions and concepts from different domains of mathematics, such as abstract algebra and number theory.

We write "$\triangleq$" to denote that equality holds between the left and right sides by definition of one of the sides. We do not use "$\triangleq$" to define the meaning of a symbol or expression. We use ":=" instead.

As usual, we use blackboard bold symbols, such as $\mathbb{R}$, $\mathbb{Z}$, and $\mathbb{P}$, to denote sets of numbers, such as the sets of reals, integers, and primes. We stress that $0 \notin \mathbb{N}$, however, $0 \in \mathbb{N}_0$. To denote that a set $\mathbb{S}$ only includes numbers less than or equal to n, we write $\mathbb{S}^{\leq n}$. Similarly, we write $\mathbb{S}^{\geq n}$ if $\mathbb{S}$ only includes numbers greater than or equal to n. The closed interval $[m, n]$ is assumed to be a subset of $\mathbb{Z}$. If $m = 1$, we abbreviate $[1, n]$ by $[n]$.

Unless otherwise stated, we call *integer sequences* $(a_n) := (a_n)_n := (a_n)_{n=k}^{m}$ simply *sequences*, denoted by parentheses around the sequence terms a_n. We refer to tuples comprising n elements as *n-tuples*. We adopt set-theoretic operations or relations to tuples in a natural manner. Furthermore, 0^n and 1^n denote the n-tuples consisting of 0 and 1, respectively. In the context of vectors, 0^n and 1^n denote the $n \times 1$ column vectors comprising 0 and 1, respectively. Usually, q denotes the cardinality of the finite field $\mathbb{F}_q$ with q elements, where q is a prime power.

We use $[\![\cdot]\!]$ to denote the *Iverson bracket*, which is 1 if the argument, i.e., logical expression, is true and 0 otherwise. For instance, $[\![2 < 3]\!] = 1$ and $[\![0 \in \mathbb{N}]\!] = 0$.

In a mathematical statement, such as a theorem or fact, a citation succeeding the statement's number means that this result is mentioned in said reference, and we did not establish it ourselves. A citation at the beginning of a proof expresses that the entire proof, its methodology, or parts originate from said reference, that is, we restated the proof. In both cases, we usually mention the precise circumstances.

1.1 Algebra

In this section, we briefly discuss algebraic concepts that mainly regard ring theory, such as units or ideals. We use R and $\mathbb{F}$ to denote a ring and field, respectively. We recall both definitions:

Definition 1.1 (Rings). Let R be a set with two associated binary operations $+$ and $\cdot$. We call $R := (R, +, \cdot)$ a *ring* if $(R, +)$ is an Abelian group, $(R, \cdot)$ is a monoid, and distributivity holds.

When the ring forms an Abelian group under multiplication, we refer to the ring as a *field*.

Definition 1.2 (Fields). Let $(R, +, \cdot)$ be a ring. We call $\mathbb{F} := (R, +, \cdot)$ a *field* if $(R, \cdot)$ is an Abelian group.

If the order of $\mathbb{F}_q$ is prime, i.e., if $q \in \mathbb{P}$, we let $\mathbb{F}_q = \mathbb{Z}/q\mathbb{Z}$ denote the field of integers modulo q.

Even if a ring is not a field, some elements $v \in R$ may be invertible. These elements are also referred to as *units*.

Definition 1.3 (Units [Hie24]). Let R be a ring. An element $v \in R$ is called a *unit* if there exists $v' \in R$ such that $vv' = 1$. We denote the subset of units by $R^* \subseteq R$.

The "canonical" unit is the identity element 1 of $(R, \cdot)$, which is also called the *unity*.

The examples we give in this section mainly relate to polynomials because this thesis focuses on polynomials. Thus, we define the ring of all polynomial functions with coefficients from $\mathbb{F}$.

Definition 1.4 (Polynomial Rings over a Field [Hie24]). Let $\mathbb{F}$ be a field. We denote by $\mathbb{F}[x]$ the *polynomial ring* in one variable over $\mathbb{F}$, whose elements we refer to as f such that we write $f(x) = \sum_{k=0}^{n} f_k x^k \in \mathbb{F}[x]$ with $n \in \mathbb{N}_0$ and with coefficients $f_i \in \mathbb{F}$.

As an example of the set of units of a ring, we consider the polynomial ring $\mathbb{F}[x]$.

Example 1.5 ([Hie24]). Let $\mathbb{F}[x]$ be the polynomial ring over $\mathbb{F}$. Then, $\mathbb{F}[x]^*$ consists of all units of the underlying field, i.e., $\mathbb{F}[x]^* = \mathbb{F}^*$, where we consider $\mathbb{F} \subseteq \mathbb{F}[x]$ a subring.

The above example implies that only the "constant" polynomials of degree 0 are invertible. It is justified to call degree-zero polynomials over a field[1] *constants* or *elements of the underlying field* because we may interpret $\mathbb{F}$ as a subring in $\mathbb{F}[x]$ via the injective mapping $\mathbb{F} \to \mathbb{F}[x]$, $a \mapsto a = ax^0$ [Hie24].

The notion of *prime* elements is most prominently known due to prime numbers. According to *Euclid's lemma*, a prime p that divides a product ab also divides a or b. Clearly, this statement does not hold for arbitrary integers. For instance, $4 \mid 2 \cdot 6$ but neither $4 \mid 2$ nor $4 \mid 6$, where $\mid$ denotes the divisibility relation between two integers a and b. Prime elements can be considered in arbitrary (commutative) rings by using Euclid's lemma as the definition. A property similar to primality is *irreducibility*: An irreducible element v can only be written as a product $v = ab$ if a or b is a unit. More precisely, the difference of an element being prime and being irreducible is as follows:

Definition 1.6 (Prime and Irreducible Elements [Hie24]). Let R be a commutative ring, such as a field. An element $v \in R \setminus (R^* \cup \{0\})$ is called

[1] This interpretation does not hold for arbitrary rings.

- *prime* if for all $x, y \in R$, it holds that $v \mid xy$ if, and only if, $v \mid x$ or $v \mid y$.
- *irreducible* if $v = xy$ with $x, y \in R$ implies that $x \in R^*$ or $y \in R^*$.

Every prime element is irreducible, but the converse does not generally hold [Hie24]. Fortunately, equivalence holds if R is a *unique factorization domain (UFD)*, such as a field [Hie24]. Thus, if we consider polynomial rings over fields, a polynomial is prime if, and only if, it is irreducible, and we may use both terms interchangeably.

Fact 1.7 ([Hie24]). The polynomial ring $\mathbb{F}[x]$ is a UFD.

UFDs are rings in which every element has a factorization that is unique up to, e.g., the ordering of terms. For instance, the *fundamental theorem of arithmetic* asserts that the ring $\mathbb{Z}$ is a UFD, that is, all integers (except -1, 0, and 1) have a unique prime factor decomposition. However, as $\mathbb{Z}$ is commutative, the ordering is per se ambiguous. For instance, 6 can be written as $2 \cdot 3$ and $3 \cdot 2$. But, since both products represent the same number, it is justified to disregard the ordering.

Definition 1.8 (Unique Factorization Domains [Hie24]). A domain R is called a *unique factorization domain (UFD)* if every $v \in R \setminus (R^* \cup \{0\})$ has a decomposition $v = \prod_{i=1}^{m} v_i$ with irreducible factors $v_1, \ldots, v_m \in R$ that is unique up to reordering and multiplication by units.

The "multiplication by units" part is usually omitted in the fundamental theorem of arithmetic since it usually only regards positive integers, and the only positive unit of $\mathbb{Z}$ is 1. However, the part is required for polynomial rings, as shown by the following example:

Example 1.9. Let $f(x) = 2x^2 + 2x + 1 \in \mathbb{F}_5[x]$. Then, f factors as $2(2+x)(4+x)$, where 2 is a unit, and $2+x$ and $4+x$ are irreducible. In general, f can be factored as $v(2+x)v'(4+x)$ for all $v, v' \in \mathbb{F}_5$ such that $vv' = 2$, i.e., for all $(v, v') \in \{(1,2), (2,1), (3,4), (4,3)\}$.

Fortunately, we can elude this annoyance by concentrating on *monic* polynomials, i.e., polynomials whose leading coefficient is 1.

Finally, we briefly mention *ideals*. They are subsets of a ring that are closed under addition, closed under multiplication with any ring element, and contain 0.

Definition 1.10 (Ideals [Hie24]). Let $a, b, v \in R$ and let $R' \subseteq R$ such that $a, b \in R'$. We call R' an *ideal* (of R) if $0 \in R'$, $a + b \in R'$, and $av \in R'$.

For instance, $2\mathbb{Z}$, the set of even integers, is an ideal of $\mathbb{Z}$. The ideal of a ring element $v \in R$ is the set comprising all elements that v divides.

Definition 1.11 (Generated Ideals [Hie24]). Let $v \in R$. The *ideal generated by* v, denoted by $\langle v \rangle$, equals $\langle v \rangle = \{ vv' : v' \in R \}$.

For instance, the *unit ideal* $\langle 1 \rangle$ generates the entire ring, i.e., $\langle 1 \rangle = R$, because 1 is the unity of R.

1.2 Number Theory

In this section, we present two number-theoretic concepts, which we use in Section 1.5 to count the number of irreducible polynomials. We first introduce the *Möbius function*.

Definition 1.12 (Möbius Function). The *Möbius function* $\mu\colon \mathbb{N} \to \{-1, 0, 1\}$ is defined as

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n \text{ is the product of } k \text{ distinct primes} \\ 0 & \text{else.} \end{cases}$$

Examples 1.13. $\mu(1) = 1$, $\mu(135) = \mu(3^3 \cdot 5) = 0$, $\mu(165) = \mu(3 \cdot 5 \cdot 11) = (-1)^3 = -1$, and $\mu(2145) = \mu(3 \cdot 5 \cdot 11 \cdot 13) = (-1)^4 = 1$.

In Section 1.5, we state the number of irreducible polynomials over $\mathbb{F}[x]$ of a specific degree. This function is not in a closed form but includes a sum. This sum iterates over all pairs (a, b) such that $ab = n$ for some $n \in \mathbb{N}$. Since $ab = n$ implies that a and b divide n, we can rewrite the sum $\sum_{a,b:ab=n} f(a, b)$ as $\sum_{d:d|n} f(d, n/d)$, or $\sum_{d|n} f(d, n/d)$ for short. Here, $f(\cdot, \cdot)$ denotes the argument of the sum, and $d \in \mathbb{N}$ is simply an alternative notation for a (or b). The divisor sum notation $d \mid n$ is more commonly used, and it is easy to see why both notations are equivalent: Since $ab = n$, $b = n/a$ is a divisor of n and so is a. Thus, a becomes d, and $b = n/a$ becomes n/d.

Example 1.14 ([Apo76]). For all $n \in \mathbb{N}$, it holds that $\sum_{d|n} \mu(d) = [\![n = 1]\!]$.

1.3 Probability Theory

In this section, we recall and present some probability-theoretic concepts that we use throughout this thesis. We usually denote random variables by X, Y, and calligraphic upper-case letters. Recall that a random variable $X\colon D \to R$ is a mathematical function, where D and R denote the domain and range, respectively. We also write $\mathrm{range}(X)$ to denote the latter. Moreover, $\mathrm{supp}(X) \subseteq R$, the *support* of X, comprises all values of X that occur with positive probability. We refer to the expectation and variance of X as $\mathbb{E}[X]$ and $\mathrm{Var}[X]$, respectively. Finally, we use $s \xleftarrow{\$} S$ to denote that $s \in S$ was sampled uniformly at random from the set S.

We present three common discrete probability distributions, their expected value, variance, and an example since we will encounter them in Chapter 3. We begin with the geometric distribution, which models the number of tries before the first success occurs.

Definition 1.15 (Geometric Distribution). A random variable X follows the *geometric distribution* with parameter $p \in (0, 1)$ if $\Pr[X = k] = [\![k \in \mathbb{N}_0]\!]\, p(1-p)^k$. We write this as $X \sim \mathrm{Geo}(p)$.

Intuitively, the probability $\Pr[X = k]$ gives the probability that the first success of identical and independent trials occurs after k failures. We note that k occasionally, but not in this thesis, denotes the total number of tries rather than the number of failures.

Example 1.16. Consider rolling a fair die and let $X \sim \mathrm{Geo}(1/6)$ be the number of rolls *after* one first rolls a six. The probability that the first time happens directly *after* $k = 5$ rolls is $\Pr[X = 5] = 1/6 \cdot (5/6)^5 \approx 6.7\,\%$.

The mean and variance of $X \sim \mathrm{Geo}(p)$ are as follows:

Fact 1.17. Let $X \sim \mathrm{Geo}(p)$. Then, $\mathbb{E}[X] = (1-p)/p$ and $\mathrm{Var}[X] = (1-p)/p^2$.

The next distribution that we consider is the binomial distribution.

Definition 1.18 (Binomial Distribution). A random variable X follows the *binomial distribution* with parameters $n \in \mathbb{N}_0$ and $p \in (0,1)$ if $\Pr[X = k] = [\![k \in \mathbb{N}_0^{\leq n}]\!]\binom{n}{k}p^k(1-p)^{n-k}$. We write this as $X \sim \mathrm{Bin}(n,p)$.

Example 1.19. Consider rolling $n = 10$ fair dice and let $X \sim \mathrm{Bin}(n, 1/6)$ be the number of which show a six. Then, the probability that exactly $k = 4$ dice show a six is precisely $\Pr[X = 4] = \binom{10}{4}(1/6)^4(5/6)^6 \approx 5.4\,\%$.

The mean and variance of $X \sim \mathrm{Bin}(n,p)$ are as follows:

Fact 1.20. Let $X \sim \mathrm{Bin}(n,p)$. Then, $\mathbb{E}[X] = np$ and $\mathrm{Var}[X] = np(1-p)$.

Finally, we consider the negative binomial distribution. This distribution can be seen as a generalization of the geometric distribution because the latter gives the number of tries before the *first* success occurs, and the former gives the number of tries before the r^{th} one occurs.

Definition 1.21 (Negative Binomial Distribution). A random variable X follows the *negative binomial distribution* with parameters $r \in \mathbb{N}_0$ and $p \in (0,1)$, denoted by $X \sim \mathrm{NBin}(r,p)$, if $\Pr[X = n] = [\![n \in \mathbb{N}_0]\!]\binom{n+r-1}{r-1}p^r(1-p)^n$.

We remark that it is also common to consider n as the total number of trials rather than the number of failures. We then had $\Pr[X = n] = \binom{n-1}{r-1}p^r(1-p)^{n-r}$ for $n \in \mathbb{N}_0$.

Example 1.22. Consider rolling a fair die and let $X \sim \mathrm{NBin}(r, 1/6)$ be the number of rolls until one rolls a six for the $r = 3$rd time. The probability that this takes $n = 10$ rolls is $\Pr[X = 10] = \binom{9}{2}(1/6)^3(5/6)^7 \approx 4.7\,\%$.

The mean and variance of $X \sim \mathrm{NBin}(r,p)$ are as follows:

Fact 1.23. Let $X \sim \mathrm{NBin}(r,p)$. Then, $\mathbb{E}[X] = r(1-p)/p$ and $\mathrm{Var}[X] = r(1-p)/p^2$.

To measure the "difference" between two probability distributions, we use the *statistical distance*, that is, half of the L^1 distance between both PMFs.

Definition 1.24 (Statistical Distance). Let X and Y be two random variables defined over a finite domain D. The *total variation distance* Δ, also called *statistical distance*, between X and Y is defined as $\Delta(X,Y) = 1/2 \sum_{s \in D} |\Pr[X = s] - \Pr[Y = s]|$.

The statistical distance between X and Y is 0 if, and only if, the random variables have the same probability distribution. We then write $X \overset{\mathrm{d}}{=} Y$. Given a sequence of random variables $(X_n)_{n \in \mathbb{N}}$, it may be that none of the terms X_n have the same distribution as X; however, it may be that the individual random variables approach X gradually as $n \to \infty$. We then say that $(X_n)_n$ converges to X.

Definition 1.25 (Convergence in Distribution). Let X be a random variable and $(X_n)_{n\in\mathbb{N}}$ be a sequence of random variables such that the X_n and X are defined over a domain D. Also, let F and F_n denote the CDF of X and X_n, respectively. The sequence (X_n) *converges in distribution* to X if $\lim_{n\to\infty} F_n(k) = F(k)$ for all $k \in D$.

1.4 Generating Functions

A generating function stores terms of an (infinite) sequence in its coefficients and can thus be regarded as a "compact" representation of that sequence. Furthermore, it facilitates the derivation of properties of (mathematical) objects, such as moments of random variables or the number of ways to partition a positive integer. We consider the following introductory example about rolling an unfair die four times:

Example 1.26. Assume one has an unfair die whose probability of showing an even number is twice that of an odd number. Thus, the probability of rolling any even number and any odd number is $2/9$ and $1/9$, respectively. Let $X\colon [6]^4 \to [4, 24]$ denote the random variable giving the sum of the pips when rolling the die four times (independently). We are interested in the PMF and the expectation of X. Generating functions allow us to easily "list" the probabilities $\Pr[X = n]$ for all possible sums $n = 4, \dots, n = 24$ as follows: For each outcome o of rolling the die *once*, we create a monomial px^o, where p is the corresponding probability, and x is an indeterminate. Thus, we have

$$\left\{\frac{1}{9}x^1, \frac{2}{9}x^2, \frac{1}{9}x^3, \frac{2}{9}x^4, \frac{1}{9}x^5, \frac{2}{9}x^6\right\}. \tag{1.1}$$

To "list" the PMF of X, we must determine the probabilities $p_n := \Pr[X = n]$ in the set $\{p_4x^4, p_5x^5, \dots, p_{24}x^{24}\}$. Observe that we begin with the fourth power and end with the 24^{th} because we *add* exponents, i.e., individual outcomes. Thus, to determine, say, p_5, we can find all quadruples that sum to 5, namely, all four permutations of $(1, 1, 1, 2)$. The probability of rolling each of the four sequences is $(1/9)^3 \cdot (2/9)^1 = 2/6561$, therefore, $p_5 = 4 \cdot 2/6561 = 8/6561$.

Fortunately, there is an "automatic" way to compute the probabilities p_n *and* all exponents: We form the sum of all monomials corresponding to individual outcomes, that is, of all elements in the set of Equation 1.1. We have $s_1(x) := 1/9x^1 + 2/9x^2 + \cdots + 2/9x^6$. Because individual rolls are independent and due to distributivity, we obtain the sum $s(x) := p_4x^4 + \cdots + p_{24}x^{24}$ that corresponds to the sums by raising $s(x)$ to the fourth power:

$$s(x) = s_1^4(x) = \left(\frac{1}{9}x^1 + \cdots + \frac{2}{9}x^6\right)^4 = \frac{1}{6561}x^4 + \frac{8}{6561}x^5 + \frac{28}{6561}x^6 + \cdots + \frac{16}{6561}x^{24}.$$

We conclude that $p_4 = 1/6561, p_5 = 8/6561, \dots$. Further, we call $s(x) = \sum_{n=4}^{24} p_n x^n$ the *generating function* of $(p_n)_{n=4}^{24}$.

If we intend to extract an individual coefficient, i.e., probability p_n, we could eliminate all monomials except p_nx^n and set $x = 1$ since $p_n1^n = p_n$. Since s is a polynomial (in x), we can differentiate it n times and evaluate $s^{(n)}(x)$ at $x = 0$. The former operation

eliminates all terms below $p_n x^n$ and the latter all terms above. Unfortunately, $s^{(n)}(0) \not\equiv p_n$ because differentiating polynomials not only decreases exponents but also multiplies the coefficients by those. For instance, $[4x^3]' = 3 \cdot 4x^{3-1} = 12x^2 \not\equiv 4x^2$, where $[\cdot]'$ denotes the first derivative. It becomes apparent that $s^{(n)}(0) = p_n(n(n-1)\cdots 1) = p_n \cdot n!$. Thus, $p_n = s^{(n)}(0)/n!$. For instance, $p_5 = s^{(5)}(0)/5! = (320/2187)/5! = 8/6561$.

Finally, we aim to determine the mean $\mathbb{E}[X]$. Since $\mathbb{E}[X] \triangleq \sum_{n=4}^{24} np_n$, we can extract all 21 probabilities using the above derivative method and plug them in the sum, i.e., $\mathbb{E}[X] = \sum_{n=4}^{24} n(s^{(n)}(0)/n!)$. There is, however, an easier way: To determine the terms np_n, we can differentiate s once. Obviously, $s'(x) = 4p_4x^3 + 5p_5x^4 + \cdots + 24p_{24}x^{23}$. To "eliminate" the variable parts $x^3, x^4, \ldots, x^{23}$, we evaluate s' at $x = 1$. Conveniently, $s'(1)$ not only gives us the desired addends of $\sum_{n=4}^{24} np_n$ but the entire sum. We conclude that

$$\mathbb{E}[X] = \sum_{n=4}^{24} np_n = s'(1) = \frac{4}{6561}1^3 + \frac{40}{6561}1^4 + \cdots + \frac{128}{2187}1^{23} = \frac{44}{3}.$$

There are different types of generating functions, most prominently *ordinary* and *exponential* ones. In this thesis, however, we consider only generating functions of the former kind. For instance, $s(x)$ from Example 1.26 is ordinary.

Definition 1.27 (Ordinary Generating Functions). Let $(a_n)_{n\in\mathbb{N}_0}$ be a sequence. The *ordinary generating function* of (a_n) is $A(z) = \sum_{n=0}^{\infty} a_n z^n$.

Evidently, ordinary generating functions are *power series*, where z is merely an *indeterminate* used as an iterator. Henceforth, we use z rather than x to distinguish generating functions from the polynomials we examine in Chapter 3.

The generating function $s(x)$ from Example 1.26 does not feature a "compact" representation because it enumerates all members of (p_n) explicitly and because different die faces appear with different probabilities. A slightly more compact representation is

$$s(x) = \frac{x^4(1 + 2x + x^2 + 2x^3 + x^4 + 2x^5)^4}{6561}.$$

We present two sequences with compact generating functions below:

Example 1.28. Let $a_n = 2^n$ be the number of binary strings of length n. The corresponding generating function is $A(z) = \sum_{n=0}^{\infty} 2^n z^n = 1/(1-2z)$.

Example 1.29 ([GKP94]). Let $b_n = F(n)$ be the n^{th} Fibonacci number. The corresponding generating function is $B(z) = \sum_{n=0}^{\infty} F(n)z^n = z/(1-z-z^2)$.

Certainly, $A(z) = 1/(1-2z)$ and $B(z) = z/(1-z-z^2)$ are more compact representations than $(1, 2, 4, 8, 16, \ldots)$ and $(0, 1, 1, 2, 3, \ldots)$, respectively. However, they "hide" the individual terms $a_n = 2^n$ and $b_n = F(n)$.

Definition 1.30 (Coefficients of Generating Functions). Let $(a_n)_{n\in\mathbb{N}_0}$ be a sequence and $A(z)$ be its corresponding generating function. We denote by $[z^n]A(z)$ the coefficient of z^n in $A(z)$, that is, $[z^n]A(z) = a_n$.

As already mentioned in Example 1.26, setting $z = 0$ eliminates all terms but a_0. Thus, to extract $a_n = [z^n]A(z)$, we shift (a_n) to the left until a_n "becomes independent" of z, that is, a_n becomes $a_0 = a_0 z^0$ (or rather $a_n = a_n z^0$).

Fact 1.31 ([SSB+22]). Let $A(z)$ be a generating function. Then, $[z^n]A'(z) = (n+1)[z^{n+1}]A(z)$.

The above fact states that differentiation shifts terms to the left and multiplies them by their initial index. In this thesis, we assume that the sum of a generating function converges and that all necessary derivatives exist.

Theorem 1.32. *Let (a_n) be a sequence and $A(z)$ the corresponding generating function. It holds that $a_n = A^{(n)}(0)/n!$.*

Proof. Let $A^{(n)}(z) = \sum_{n=0}^{\infty} \hat{a}_n z^n$ be the generating function of the coefficients in $A^{(n)}$. Thus, $\hat{a}_n = [z^n]A^{(n)}(z)$. We aim to show that $a_n = A^{(n)}(0)/n!$. By applying Fact 1.31 recursively n times, we obtain $[z^0]A^{(n)}(z) = n![z^n]A(z)$. Since $[z^n]A(z) \triangleq a_n$, we conclude that $A^{(n)}(0) \triangleq \hat{a}_0 = n! \cdot a_n$. Finally, we can solve $\hat{a}_0 = n! \cdot a_n$ for a_n because the factorial function $n!$ has no zeros. ∎

Example 1.33. Consider again the Fibonacci numbers from Example 1.29. To find $F(3)$, we calculate $B^{(3)}(0) = 6(z^4 + 6z^2 + 4z + 2)/(z^2 + z - 1)^4\big|_{z=0} = 12$. Thus, $F(3) = 12/3! = 2$.

However, calculating the n^{th} derivative of an ordinary generating function, let alone expressing the generating function in a closed form, often is non-trivial.

In Chapter 3, we count polynomials using generating functions, which we express as *products* rather than the "usual" sums $\sum_{n=0}^{\infty} a_n z^n$. This approach closely resembles *Euler products*. In 1737, Euler established the *Euler product formula*, which regards prime numbers and uses the fact that the prime factorization of integers is unique. Without going too deeply into the details, he proved that:

Fact 1.34 ([Apo76]). For all $s \in \mathbb{N}^{\geq 2}$, it holds that $\sum_{n=1}^{\infty} n^{-s} = \prod_{p \in \mathbb{P}} (1 - p^{-s})^{-1}$.

The sum $\sum_{n=1}^{\infty} n^{-s}$ is also known as *Riemann's zeta function*. In the next paragraph, we elaborate on why Fact 1.34 holds because this gives us insight into why we can express generating functions as products. The following explanation, except the part referring to Example 1.26, is from [Mur06].

Again, we stress that every integer $n \geq 1$ uniquely decomposes into a product of primes $n = \prod_{k=1}^{\infty} p_i^{e_i} = 2^{e_1} 3^{e_2} \cdots$, where p_i is the i^{th} prime, and e_i is its multiplicity. We recall that $e_i = 0$ for almost all i holds for every n. In Example 1.26, at the beginning of this section, we obtained the probability that the sum of four die rolls equals a specific total number of pips. To this end, we *multiplied* the *sums* of possible pips. Consider the product over all primes, where each factor consists of the sum of all multiplicities of that prime, i.e., $\prod_p \sum_{k=0}^{\infty} p^k = (2^0 + 2^1 + \dots)(3^0 + 3^1 + \dots) \cdots$. By expanding this infinite product, we observe that each addend represents one distinct integer. For instance, $2^0 3^0 5^0 \cdots = 1$ and $2^3 3^1 5^4 7^0 11^0 13^0 \cdots = 15\,000$. Since $\sum_n n^{-s}$ on the left-hand side considers every integer n, it follows that $\sum_n n^{-s} = \prod_p \sum_{k=0}^{\infty} p^{-sk}$. Finally, the inner sum $\sum_{k=0}^{\infty} p^{-sk} = \sum_{k=0}^{\infty} (p^{-s})^k$ simplifies to $(1 - p^{-s})^{-1}$ because it is a convergent geometric series (as $p^s > 1$).

Euler's product formula demonstrates that products can be used to count the number of ways to assemble the term z^n. We consider a further example regarding values of coins, which can be (almost) directly adapted to count polynomials in Section 1.5 and Chapter 3.

Example 1.35. Assume one has coins of values 1 ct, 2 ct, and 5 ct. The number of coins are $c_1 = 3$, $c_2 = 2$, and $c_5 = 4$. We are interested in the number a_n of different combinations of coins whose combined value is n and aim to use generating functions to determine it. We interpret each of the nine coins as an abstract object. However, since we are only interested in their values, we can equate coins with the same value. To incorporate different quantities of one coin (since all $c_i > 1$), we consider an *enumerator* of a fixed coin of value $i \in \{1, 2, 5\}$. The possible values of coin i, depending on its "multiplicity," are $0, i, 2i, \dots$. The corresponding objects $z^0, z^i, z^{2i}, \dots$ represent the combined coins, where the exponents represent their sums.

To find all sums that are expressible by combining the values of the coins available, we expand the product of the three enumerators $z^{0\cdot1} + z^{1\cdot1} + z^{2\cdot1} + z^{3\cdot1}$, $z^{0\cdot2} + z^{1\cdot2} + z^{2\cdot2}$, and $z^{0\cdot5} + z^{1\cdot5} + z^{2\cdot5} + z^{3\cdot5} + z^{4\cdot5}$. The expanded product is $1z^0 + 1z^1 + 2z^2 + 2z^3 + \cdots + 1z^{26} + 1z^{27}$. For instance, there are two ways to obtain the sum 3: $1 + 1 + 1$ and $1 + 2$. We neglect the ordering of coins just as in other commutative structures.

Now, we introduce the distinction between different editions of coins *of the same value*. However, we assume that each edition occurs with equal frequency. For simplicity, we assume that the values 1 ct, 2 ct, and 5 ct have $e_1 = 1$, $e_2 = 2$, and $e_5 = 3$ editions, each with c_1, c_2, and c_3 coins. Hence, there are $\sum_i c_i e_i = 19$ coins in total. Clearly, the value of a coin is independent of its edition. Nevertheless, the sum 3 can now be formed in three ways instead of two because we differentiate between editions, and the 2 ct coins have two. Thus, the three ways are $1+1+1$ and $2+1$ twice. To incorporate this distinction into our generating function, we introduce each enumeration, i.e., factor, as often as there are different editions. As each edition occurs with equal frequency, the product simplifies to

$$\begin{aligned}
&\left(z^{0\cdot1} + z^{1\cdot1} + z^{2\cdot1} + z^{3\cdot1}\right)^{c_1}\left(z^{0\cdot2} + z^{1\cdot2} + z^{2\cdot2}\right)^{c_2}\left(z^{0\cdot5} + z^{1\cdot5} + z^{2\cdot5} + z^{3\cdot5} + z^{4\cdot5}\right)^{c_3} \\
&= 1z^0 + 1z^1 + 3z^2 + 3z^3 + \cdots + 3z^{69} + z^{70} + z^{71} \\
&= \prod_{i\in\{1,2,5\}} \left(\sum_{k=0}^{c_i} z^{ki}\right)^{e_i}.
\end{aligned}$$

We conclude that we can express the generating function $A(z) = \sum_{n=0}^{\infty} a_n z^n = \sum_{n=0}^{71} a_n z^n$ in terms of the product $\prod_{i\in\{1,2,5\}} \left(\sum_{k=0}^{c_i} z^{ki}\right)^{e_i}$ and that $(a_n)_{n=0}^{71} = (1, 1, 3, 3, \dots, 3, 1, 1)$.

1.5 Polynomials

This section provides all the necessary information about polynomials to analyze zeros in Chapter 3 and fault attacks in Chapters 4 and 5.

First and foremost, we draw attention to the difference between *polynomials* and *polynomial functions* because, over finite fields, it can happen that "two different polynomials represent the same function." The following disambiguation is due to [Ogu08]. Roughly speaking, polynomials are the tuples, vectors, or sequences of coefficients of polynomial

functions. More precisely, polynomials (over a field $\mathbb{F}$) are sequences $(f_k)_{k\in\mathbb{N}_0}$ such that $f_k \in \mathbb{F}$ and $f_k = 0$ for almost all k. For each polynomial (f_k), we can define a polynomial function $f\colon \mathbb{F} \to \mathbb{F}$ by letting $f(x) = \sum_{k=0}^{\infty} f_k x^k = \sum_{k=0}^{n} f_k x^k$, where $n = \max\{\, k : f_k \neq 0 \,\}$ is the largest index of a non-zero coefficient. In particular, two *polynomials* are equal if, and only if, they constitute the same coefficient vector. An intuitive notion of equality between *(polynomial) functions* is that they are equal if, and only if, they agree on all members of their domain. More formally, two (polynomial) functions $f, g\colon \mathbb{F} \to \mathbb{F}$ are equal if, and only if, $\forall x \in \mathbb{F} \,.\, f(x) = g(x)$.

Certain fields, such as $\mathbb{R}$, allow reconstructing the polynomial, i.e., coefficients, from the polynomial function. However, in finite fields exist multiple functions that "generate" the same coefficients, i.e., polynomial [Ogu08].

Example 1.36. Let $f(x) = x^3 + 1$ and $g(x) = x + 1$ be two polynomial functions over $\mathbb{F}_2$. Then, $f(0) = 0^3 + 1 = 0 + 1 = g(0)$ and $f(1) = 1^3 + 1 = 1 + 1 = g(1)$. However, the underlying polynomials are $(1, 0, 0, 1, 0, \dots)$ and $(1, 1, 0, \dots)$, respectively.

Although two equal polynomial functions can have different underlying polynomials, in this thesis, we define equality in terms of their polynomials. Thus, we treat f and g from Example 1.36 as different functions.

Remark 1.37 *([Hie24])*. Polynomial functions in the form $f(x) = \sum_{k=0}^{n} f_k x^k$ are, *by definition*, described by the tuple of coefficients $(f_k)_{k=0}^{n}$. Hence, two polynomial functions are equal if, and only if, all their coefficients are equal.

For the remainder of this thesis, we refer to *polynomial functions* as *polynomials*, e.g., we call $f : x \mapsto x^2 + x$ a polynomial. Besides, we allow the sequence of coefficients $(f_k)_{k=0}^{\infty}$ to be truncated to $(f_k)_{k=0}^{n}$ to omit the infinitely many zeros. We also write $\mathrm{coef}(f, k)$ to denote the coefficient f_k of f.

We usually group polynomials according to their *degree* n, the largest index of a non-zero coefficient.

Definition 1.38 (Degree of a Polynomial). Let $f \in \mathbb{F}[x]$ with $f(x) = \sum_{k=0}^{n} f_k x^k$ such that $f_n \neq 0$. The *degree* $\deg$ of f is defined as $\deg(f) = n$. We define the degree of the zero polynomial to be $\deg(0) = -\infty$.

For multivariate polynomials $f(x_1, \dots, x_m)$ in m variables, we consider the *total degree* over all terms, which equals the largest sum of all variables' exponents. For instance, the total degree of $f(x_1, x_2) = x_1^2 x_2^4 + x_1^5 x_2 + x_1^2 x_2^2$ is $\max\{2 + 4, 5 + 1, 2 + 2\} = 6$.

Throughout this thesis, we are particularly interested in the *zeros* of polynomials.

Definition 1.39 (Zeros of a Polynomial). Let $f \in \mathbb{F}[x]$ be a polynomial. We say that $v \in \mathbb{F}$ is a *zero* of f if, and only if, $f(v) = 0$, which is equivalent to $(x - v) \mid f$. The *multiplicity* $s \in \mathbb{N}_0$ of the zero v (w.r.t. f) is the number of how often $(x - v)$ can be factored out.

Zeros denote the positions where (polynomial) functions *vanish*, that is, where they assume the value 0. However, since a zero can occur multiple times, we usually refer to zeros as "the multiset of positions" and to the number of zeros as its cardinality. If we only consider the positions $v \in \mathbb{F}$, we use the term *distinct*.

Example 1.40. Let $f(x) = (x-2)^4(x-3)(x^2+1) \in \mathbb{F}_7[x]$. Then, f has two *distinct* zeros, viz., $x = 2$ and $x = 3$. Further, f has five zeros, four at $x = 2$ and one at $x = 3$.

We remark on the following fact about the limit of the number of zeros of a polynomial:

Fact 1.41 ([Hie24]). Let $f \neq 0$ be a *univariate* polynomial over a *field*. If $\deg(f) = n$, then f has at most n zeros.

If the polynomial is not univariate or not defined over a field, this upper bound does not necessarily hold.

Counterexamples 1.42. Let $f(x_1, x_2) = x_1 - x_2$ be a bivariate polynomial over $\mathbb{F}_3$. Then, f has $3 > 1$ zeros since $f(x_1, x_2) = 0$ if, and only if, $x_1 = x_2$.

Let $f(x) = 3x^3 + 3x^2$ be a univariate polynomial over $\mathbb{Z}/6\mathbb{Z}$. It follows that $f(x) = 0$ for all $6 > 3$ elements in $\mathbb{Z}/6\mathbb{Z}$.

When two polynomials are combined using addition or multiplication, the degrees of the resulting polynomials behave as follows:

Fact 1.43 ([Hie24]). Let f and g be two polynomials over a ring R. In that case, it holds that $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$ with equality if $\deg(f) \neq \deg(g)$. Moreover, $\deg(fg) \leq \deg(f) + \deg(g)$ with equality if R is a UFD, such as a field.

Next, we group polynomials possessing a mutual property, e.g., the same degree, into sets. Recall that q is some prime power.

Definition 1.44 (Set of All Same-Degree Polynomials). Let $n \in \mathbb{N}_0 \cup \{-\infty\}$. We denote by $\mathcal{P}_{n,q}$ the *set of all polynomials of degree* n, i.e., $\mathcal{P}_{n,q} = \{f : f \in \mathbb{F}_q[x] \wedge \deg(f) = n\}$. We write $\mathcal{P}_{\leq n,q}$, to denote the set of all polynomials of degree *at most* n. If q is evident from the context, we simply write $\mathcal{P}_n := \mathcal{P}_{n,q}$ and $\mathcal{P}_{\leq n} := \mathcal{P}_{\leq n,q}$.

Since we define polynomials by their coefficients, we can quickly determine the cardinalities of $\mathcal{P}_n$ and $\mathcal{P}_{\leq n}$.

Theorem 1.45. *For all q and $n \in \mathbb{N}_0$, there are $|\mathcal{P}_{n,q}| = (q-1)q^n$ polynomials of degree n and $|\mathcal{P}_{\leq n,q}| = q^{n+1}$ polynomials of degree at most n, respectively.*

Proof. We count the number of different tuples of coefficients $(f_k)_{k=0}^n$ because we can specify every polynomial $f \in \mathcal{P}_{n,q}$ by its coefficients $(f_k)_{k=0}^n$ as $f(x) = \sum_{k=0}^n f_k x^k$. For all f_k with $k \in [0, n-1]$, there are $|\mathbb{F}_q| = q$ possible values per coefficient because $f_k \in \mathbb{F}_q$. The leading coefficient f_n must not be 0 because $\deg(f)$ is assumed to be n. Thus, there are only $|\mathbb{F}_q \setminus \{0\}| = q-1$ possible values. We conclude that there are $(q-1)^1 q^{|[0,n-1]|} = (q-1)q^n$ different (f_k), i.e., polynomials of degree n. Recall that this equality particularly holds if $n = 0$ since the degree of the zero polynomial is $-\infty \neq 0$.

It remains to determine the cardinality of $\mathcal{P}_{\leq n,q}$. We observe that $\mathcal{P}_{\leq n,q}$ is the union $\mathcal{P}_{\leq n,q} = \mathcal{P}_{-\infty,q} \cup \bigcup_{k=0}^n \mathcal{P}_{k,q}$. In addition, all sets $\mathcal{P}_{k,q}$ and $\mathcal{P}_{k',q}$, where $k \neq k'$, are disjoint because polynomials must differ if their degrees do. We conclude that

$$|\mathcal{P}_{\leq n,q}| = |\{0\}| + \sum_{k=0}^n |\mathcal{P}_{k,q}| = 1 + \sum_{k=0}^n (q-1)q^k = 1 + (q^{n+1} - 1) = q^{n+1}. \qquad \blacksquare$$

For reasons of simplicity, we often consider "normalized" polynomials, that is, polynomials whose leading coefficients are 1. Such *monic* polynomials will be helpful to our analysis of zeros.

Definition 1.46 (Monic Polynomials). Let $f \in \mathcal{P}_{n,q}$. We say that f is *monic* if, and only if, its leading coefficient is 1, i.e., if $f_n = 1$.

We stress that the zero polynomial is not monic. As above, we define the corresponding set comprising all monic polynomials of the same degree.

Definition 1.47 (Set of All Same-Degree Monic Polynomials). Let $n \in \mathbb{N}_0$. We denote by $\mathcal{M}_{n,q}$ the set of all *monic* polynomials of degree n, i.e., $\mathcal{M}_{n,q} = \{f : f \in \mathcal{P}_{n,q} \wedge f_n = 1\}$. We write $\mathcal{M}_{\leq n,q}$, to denote the set of all monic polynomials of degree *at most* n. If q is evident from the context, we simply write $\mathcal{M}_n := \mathcal{M}_{n,q}$ and $\mathcal{M}_{\leq n} := \mathcal{M}_{\leq n,q}$.

It is easy to see that $\mathcal{M}_{n,q} \subsetneq \mathcal{P}_{n,q}$ for all $q > 2$ because, for every $f \in \mathcal{M}_n$, we can replace the leading coefficient $f_n = 1$ with any of the remaining $q - 2$ field elements to obtain a non-monic polynomial of degree n. We establish the cardinalities of $\mathcal{M}_n$ and $\mathcal{M}_{\leq n}$ similarly to Theorem 1.45.

Theorem 1.48. *For all q and $n \in \mathbb{N}_0$, there are $|\mathcal{M}_{n,q}| = q^n$ monic polynomials of degree n and $|\mathcal{M}_{\leq n,q}| = (q^{n+1} - 1)/(q - 1)$ monic polynomials of degree at most n, respectively.*

Proof. Let $f \in \mathcal{M}_{n,q}$. As before, the n coefficients $f_0, \ldots, f_{n-1}$ can assume arbitrary values in $\mathbb{F}_q$. The leading coefficient f_n, however, must be $f_n = 1$ because f is monic. We conclude that $|\mathcal{M}_{n,q}| = 1 \cdot q^{|[0,n-1]|} = q^n$.

Since monic polynomials of different degrees k and k' differ, the sets $\mathcal{M}_{k,q}$ and $\mathcal{M}_{k',q}$ are disjoint. Thus, $|\mathcal{M}_{\leq n,q}| = \sum_{k=0}^{n} |\mathcal{M}_{n,q}| = \sum_{k=0}^{n} q^n = (q^{n+1} - 1)/(q - 1)$. ∎

We deduce that the ratio between the number of polynomials in $\mathcal{P}_n$ and $\mathcal{M}_n$ is $q - 1$.

Corollary 1.49. *For all q and $n \in \mathbb{N}_0$, it holds that $(q - 1)|\mathcal{M}_{n,q}| = |\mathcal{P}_{n,q}|$.*

Proof. Theorems 1.45 and 1.48 state that $|\mathcal{P}_{n,q}| = (q - 1)q^n$ and $|\mathcal{M}_{n,q}| = q^n$, respectively. Since $|\mathcal{M}_{n,q}| > 0$, we deduce that $|\mathcal{P}_{n,q}|/|\mathcal{M}_{n,q}| = (q - 1)$. ∎

To "make" a polynomial $f \neq 0$ monic, one can simply divide $f(x)$ by its leading coefficient f_n. This process is somewhat "injective" in the sense that for every monic polynomial $\hat{f} \in \mathcal{M}_n$ and every non-zero leading coefficient $f_n \in \mathbb{F}_q^*$, there is only one $f \in \mathcal{P}_n$ such that $f_n^{-1} f(x) = \hat{f}(x)$. Thus, it is justified to say that f is converted into its monic form.

Theorem 1.50. *Let $n \in \mathbb{N}_0$. Consider the following function* mon, *which converts polynomials into their monic form:*

$$\text{mon}\colon \mathcal{P}_{n,q} \to \mathcal{M}_{n,q},\ f(x) = \sum_{k=0}^{n} f_k x^k \mapsto f_n^{-1} \sum_{k=0}^{n} f_k x^k = \hat{f}(x).$$

The function mon *is onto but not one-to-one unless $q = 2$. More precisely, it is $(q - 1)$-to-one, i.e., all members of its image have exactly $q - 1$ preimages.*

Proof. We prove both properties individually.

Since the codomain is a subset of the domain and $1^{-1} \in \mathbb{F}_q$, it immediately follows that mon is onto. To prove that mon is $(q-1)$-to-one, fix any $\hat{f} \in \mathcal{M}_n$ and consider the set $\sigma := \sigma_{\hat{f}} := \{ v\hat{f}(x) : v \in \mathbb{F}_q^* \} \subseteq \mathcal{P}_n$, which includes all polynomials with the same monic form $\hat{f}$. Obviously, $|\sigma| = |\mathbb{F}_q^*| = q-1$ as all polynomials in σ differ in their leading coefficient. Hence, $\hat{f}$ has at least $q-1$ preimages. Also, every $f \in \mathcal{P}_n$ that maps to $\hat{f}$ must be in σ because f_n is invertible, i.e., $v = f_n^{-1}$. Thus, $\hat{f}$ has at most $q-1$ preimages, and the claim follows. ∎

As a third and final class of polynomials, we consider *irreducible* polynomials. They become helpful when we count polynomials later. The relationship between irreducible polynomials and polynomials is the same as between primes and integers. In fact, irreducible polynomials are prime elements of $\mathbb{F}[x]$, according to Fact 1.7. The results in Section 1.1 show that every polynomial $f \in \mathbb{F}[x] \setminus (\mathbb{F}[x]^* \cup \{0\})$ has a unique decomposition into irreducible polynomials. The uniqueness is up to the ordering of terms and multiplication of units. This highlights our focus on *monic* polynomials, for which the latter part is no longer required.

Definition 1.51 (Set of All Monic Irreducible Same-Degree Polynomials). Let $n \in \mathbb{N}_0$. We denote by $\mathfrak{I}_{n,q} = \{ f : f \in \mathcal{M}_{n,q} \wedge f \text{ is irreducible} \}$ the set of all *monic and irreducible* polynomials of degree n. If q is evident from the context, we simply write $\mathfrak{I}_n := \mathfrak{I}_{n,q}$.

We remark that $\mathfrak{I}_0 = \emptyset$ because $\mathcal{P}_0 = \mathbb{F}[x]^*$ consists of the units of $\mathbb{F}[x]$. We already know how many (monic) polynomials of degree n exist in $\mathbb{F}[x]$. However, the number of which are also *irreducible* is not apparent. Moreover, whether an irreducible polynomial of degree n exists for all $n \geq 1$ is uncertain.

Fact 1.52 ([Chi09; IBS11]). For all q and $n \in \mathbb{N}$, there are $I_{n,q} := |\mathfrak{I}_{n,q}| = q^n/n \sum_{d|n} \mu(d) q^{1/d}$ *monic irreducible* polynomials of degree n. If q is clear from the context, we write $I_n := I_{n,q}$. Moreover, $\mathfrak{I}_{n,q} \neq \emptyset$, and if n is prime, the function simplifies to $I_{n,q} = (q^n - q)/n$.

We omit the proof of Fact 1.52 because it requires specific number-theoretical background knowledge. Besides, we never use the actual number of monic irreducible polynomials in this thesis except for the following: There are $I_{1,q} = q$ *linear* monic irreducible polynomials of degree 1. Thus, all $|\mathcal{M}_{1,q}| = q$ linear monic polynomials are irreducible.

For our analysis of zeros in Chapter 3, we consider the sequence's generating function $\mathcal{M}(z)$ comprising the cardinalities of $\mathcal{M}_{n,q}$. From Theorem 1.48, it is apparent that $\mathcal{M}(z) = \sum_{n=0}^{\infty} |\mathcal{M}_{n,q}| z^n = \sum_{n=0}^{\infty} q^n z^n$. Since $(q^n z^n)_n = ((qz)^n)_n$ is a geometric sequence, the generating function has the compact representation $\mathcal{M}(z) = 1/(1-qz)$. Similar to Example 1.35, we aim to express $\mathcal{M}(z)$ as a product since this helps us count polynomials with certain zeros in Chapter 3. Although the product form of $\mathcal{M}(z)$ can be found in several papers, e.g., [FGP96; Kno75; Pan04], we thoroughly elaborate on its derivation as it can be modified to count further kinds of polynomials.

Theorem 1.53 ([Pan04]). *Let $\mathcal{M}(z) := \mathcal{M}_q(z)$ denote the generating function of the sequence $(|\mathcal{M}_{n,q}|)_{n=0}^{\infty}$. It holds that $\mathcal{M}_q(z) = \sum_{n=0}^{\infty} q^n z^n = 1/(1-qz) = \prod_{n=1}^{\infty} (1-z^n)^{-I_{n,q}}$.*

Proof ([FGP96; Pan04]). We prove the theorem in three steps, with one step per equation: Firstly, we show that $\mathcal{M}_q(z) = \sum_{n=0}^{\infty} q^n z^n$. Then, we simplify the sum to $1/(1-qz)$. Finally, we argue that $\prod_{n=1}^{\infty}(1-z^n)^{-I_n}$ equals the same sum. For the third step, we use the approach from [Pan04] with additional explanations from [FGP96].

According to Theorem 1.48, $|\mathcal{M}_{n,q}| = q^n$ for all $n \in \mathbb{N}_0$. Therefore, its generating function is $\mathcal{M}(z) = \sum_{n=0}^{\infty} q^n z^n = \sum_{n=0}^{\infty}(qz)^n$, which is a geometric series. Hence, we obtain the simplified form $\sum_{n=0}^{\infty}(qz)^n = 1/(1-qz)$. Strictly speaking, the sum only converges if $|qz| < 1$. However, we recall that since we interpret z as an indeterminate, i.e., formal variable, we avoid such convergence issues.

It remains to prove that $\sum_{n=0}^{\infty} q^n z^n = \prod_{n=1}^{\infty}(1-z^n)^{-I_n}$. To this end, we elaborated in Section 1.4 on why we can express the sum over all integers as a product over all primes in Euler's product formula (Fact 1.34). The gist was that every integer can be uniquely written as a product of primes, which is covered by one addend of the expanded product. The same holds for (monic) polynomials, which we can uniquely write as the product of irreducible polynomials. Recall Example 1.35, the coin example from Section 1.4. We considered each coin as an abstract object and assigned it a value: the coin value. Now, we consider polynomials, where a polynomial's "value" is its degree because we count the number of different polynomials of degree n. The number of coins was limited, whereas each prime could occur arbitrarily often. The latter reflects the situation of polynomials.

Let $\mathcal{F} = \bigcup_{i=1}^{\infty} \mathfrak{I}_{i,q}$ be the family of all monic irreducible polynomials over $\mathbb{F}_q$. As before, we interpret each polynomial $f \in \mathcal{F}$ as an abstract[2] object, where f^i represents the i^{th} power of f. The formal sum $f^0 + f^1 + f^2 + \cdots = \sum_{i=0}^{\infty} f^i$, hence, generates all polynomials being a power of f. Observe that this sum is a geometric series, namely, $\sum_{i=0}^{\infty} f^i = 1/(1-f)$. We conclude that by forming the product $\prod_{f\in\mathcal{F}} 1/(1-f)$ of all formal sums over all $f \in \mathcal{F}$, we generate all monic polynomials (†).

Since we are interested in the value, i.e., degree, of each generated polynomial, we consider the mapping $f \mapsto z^{\deg(f)}$. From (†), it follows that

$$\mathcal{M}(z) = \prod_{f\in\mathcal{F}} \frac{1}{1-z^{\deg(f)}} = \prod_{f\in\mathcal{F}} \left(1-z^{\deg(f)}\right)^{-1}. \tag{1.2}$$

By definition, $\mathcal{F}$ includes every monic irreducible polynomial of every degree $n \in \mathbb{N}$. Thus, we separate the product in Equation 1.2 by degree and thereby replace $\deg(f)$ with that degree:

$$\prod_{f\in\mathcal{F}} \left(1-z^{\deg(f)}\right)^{-1} = \prod_{n=1}^{\infty} \prod_{\substack{f\in\mathcal{F}\\ \deg(f)=n}} \left(1-z^{\deg(f)}\right)^{-1} = \prod_{n=1}^{\infty} \prod_{\substack{f\in\mathcal{F}\\ \deg(f)=n}} (1-z^n)^{-1}. \tag{1.3}$$

Since the argument of the inner product in Equation 1.3 only depends on the degree of f but not f itself, we can simplify the inner product by repeatedly multiplying $(1-z^n)^{-1}$ by itself. Since the number of $f \in \mathcal{F}$ of degree n is precisely I_n, we obtain

$$\mathcal{M}(z) = \prod_{n=1}^{\infty} \prod_{\substack{f\in\mathcal{F}\\ \deg(f)=n}} (1-z^n)^{-1} = \prod_{n=1}^{\infty} \left((1-z^n)^{-1}\right)^{I_n} = \prod_{n=1}^{\infty} (1-z^n)^{-I_n}.$$

[2] We abstain from introducing a different variable for the formal polynomial.

We conclude that $\sum_{n=0}^{\infty} q^n z^n = \prod_{n=1}^{\infty}(1-z^n)^{-I_n}$, which completes the proof. ■

1.6 Polynomial Secret Sharing

In Chapters 4 and 5, we use polynomials to protect the values of wires in circuits from being read and manipulated by an adversary. The values are protected by *secret sharing schemes*.

Polynomial secret sharing schemes provide a way to share a secret s among several parties such that a certain minimum number of parties, say $d+1$, is required to recover the secret. Thus, as soon as at least $d+1$ parties collaborate, they can recover the secret. However, any constellation of at most d parties learns *nothing* about s by combining their *shares*. In what follows, we will consider sharing schemes over a finite field $\mathbb{F}_q$ and refer to the total number of parties by $n \in \mathbb{N}$. We denote the degree of the polynomial that includes the secret by d. We also assume that $d < n < q$.

In 1979, Shamir [Sha79] introduced secret sharing based on polynomials, which is also known as *Shamir's secret sharing*. His idea is to sample a random polynomial $f \in \mathcal{P}_{\leq d,q}$ of degree at most d and to embed the secret by replacing the constant coefficient with it, that is, $f_0 = s$. The polynomial f is then evaluated at n specific and distinct positions $\alpha_1, \dots, \alpha_n \in \mathbb{F} \setminus \{0\}$, where α_i corresponds to party i's position, $i \in [n]$. For instance, the canonical position is $\alpha_i = i$.

Definition 1.54 (Support Points and Nodes). Let $i \in [n]$. In the context of secret sharing, we call the position $\alpha_i \in \mathbb{F} \setminus \{0\}$ of party i his *support point* or *node*. We refer to the n-tuple $\alpha := (\alpha_i)_{i=1}^n$ comprising all n *distinct* nodes as the *tuple* of support points or nodes.

We must exclude $\alpha_i = 0$ because $f(0) = f_0$ is precisely the secret.

Each party i is now given his *share* of the secret, which is the member of the function graph of f at α_i, namely, $(\alpha_i, f(\alpha_i))$. Since it is usually clear what node party i corresponds to, we also treat his share as the function value $f(\alpha_i)$.

Definition 1.55 (Shares). Let $f \in \mathcal{P}_{\leq d,q}$ and let α be an n-tuple of nodes. We call the value $F_i := f(\alpha_i)$ the *share* of party i. Further, we refer to the n-tuple $F := (F_i)_{i=1}^n \triangleq (f(\alpha_i))_{i=1}^n$ as the *n-sharing* of f (w.r.t. α).

Shamir shows that any collection of at least $d+1$ parties, i.e., shares, can recover all coefficients of f, particularly $f_0 = s$. This can be seen by noticing that, given a share $F_i = f(\alpha_i)$, the *linear* equation $\sum_{k=0}^{d} f_k \alpha_i^k \stackrel{!}{=} F_i$ contains $d+1$ unknowns, viz., $f_0, \dots, f_d$. Hence, $d+1$ equations uniquely determine all coefficients, i.e., a polynomial of degree at most d, because f is evaluated at *distinct* positions α_i.

Fact 1.56 ([SB03]). Let $\pi\colon [n] \to [n]$ be a permutation and $(F_{\pi(i)})_{i=1}^{d+1}$ be a $(d+1)$-tuple of shares at nodes $\alpha_{\pi(1)}, \dots, \alpha_{\pi(d+1)}$. Then, there exists a *unique* polynomial $f \in \mathcal{P}_{\leq d}$ such that $f(\alpha_{\pi(i)}) = F_{\pi(i)}$ for all $i \in [d+1]$.

Using more than $d+1$ shares, such as all n, is possible. Although this resembles an overdetermined system of equations, a unique solution still exists because the remaining

$n - d - 1$ equations only provide redundant information. The process of determining a polynomial from the points it "passes through" is called *interpolation*.

Shamir also shows that at most d shares cannot interpolate f. Moreover, the partial information from these shares does not even reveal anything about $f_0 = s$ (in an information-theoretic sense): Since $f(0) = f_0 = s$, we can append this share to the other d. According to Fact 1.56, these $d + 1$ shares uniquely determine a polynomial $f \in \mathcal{P}_{\leq d}$. Clearly, this works for every secret $s \in \mathbb{F}$. Furthermore, since the polynomial underlying the d shares was sampled uniformly at random, each complementary share $f(0) = v$, where $v \in \mathbb{F}$, is equally likely [Sha79].

Fact 1.57 ([Sha79]). Let $s \in \mathbb{F}$, let $f \leftarrow\!\$\ \mathcal{P}_{\leq d,q}$ such that $f_0 = s$, and let F be the n-sharing of f. Any subset $F' \subseteq F$ of at least $d + 1$ shares uniquely determines f, hence, $f_0 = s$. Moreover, for any $\alpha' = (\alpha'_i) \subseteq \alpha$ with $|\alpha'| \leq d$, the corresponding subset $F'' = (F''_i) \subseteq F$ of at most d shares is independent of s, i.e., $\Pr[f_0 = s] = \Pr[f_0 = s \mid \bigwedge_i f(\alpha'_i) = F''_i]$.

By now, it should be apparent that both the coefficients and shares of f are important for secret sharing. Since $\mathbb{F}[x]$ forms a vector space, we can easily switch between the *coefficient view* $(f_i)_{i=0}^{d} = (f_0, \dots, f_d)$ and the *sharing view* $(F_i)_{i=1}^{n} = (f(\alpha_1), \dots, f(\alpha_n))$. Assuming that both tuples are row vectors, we can transform $(f_i)_i$ into $(F_i)_i$ using a matrix $V \in \mathbb{F}^{n\times(d+1)}$ such that

$$
\begin{aligned}
V \cdot (f_i)_i^\intercal = (F_i)_i^\intercal \leftrightarrow & \begin{pmatrix} V_{0,0} & V_{0,1} & \cdots & V_{0,d} \\ V_{1,0} & V_{1,1} & \cdots & V_{1,d} \\ & & \ddots & \\ V_{n-1,0} & V_{n-1,1} & \cdots & V_{n-1,d} \end{pmatrix} \begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_d \end{pmatrix} = \begin{pmatrix} F_1 \\ F_2 \\ \vdots \\ F_n \end{pmatrix} \\
\leftrightarrow & \begin{pmatrix} V_{0,0} \cdot f_0 + V_{0,1} \cdot f_1 + \cdots + V_{0,d} \cdot f_d \\ V_{1,0} \cdot f_0 + V_{1,1} \cdot f_1 + \cdots + V_{1,d} \cdot f_d \\ \vdots \\ V_{n-1,0} \cdot f_0 + V_{n-1,1} \cdot f_1 + \cdots + V_{n-1,d} \cdot f_d \end{pmatrix} = \begin{pmatrix} F_1 \\ F_2 \\ \vdots \\ F_n \end{pmatrix}.
\end{aligned}
$$

Observe that matrix indices are zero-based. From the definition of polynomials in Remark 1.37, we conclude that $V_{i,j} = \alpha_{i+1}^j$. The matrix V is known as the *Vandermonde matrix*.

Definition 1.58 ([Inverse] Vandermonde Matrix). Let $d, n \in \mathbb{N}$ and let α be an n-tuple of shares. The *Vandermonde matrix* $V_d := V_d(\alpha) \in \mathbb{F}^{n\times(d+1)}$ includes the j^{th} power of α_{i+1} in its entry $V_{i,j}$, that is, $V_{i,j} = \alpha_{i+1}^j$. If $d = n - 1$, then $V := V_{n-1}$ is square, and we refer to the entry $V_{i,j}^{-1}$ as $\lambda_{j,i}$.

We implicitly assumed V to be invertible. Since the nodes in α are pairwise disjoint, the well-known determinant $\det(V(\alpha)) = \prod_{i,j>i}(\alpha_j - \alpha_i)$ implies that V^{-1} exists.

Fact 1.59. For all node tuples $\alpha \subseteq \mathbb{F}$, the $n \times n$ Vandermonde matrix $V(\alpha)$ is invertible.

From the n-sharing F, it is possible to individually compute the k^{th} coefficient f_k of f using the k^{th} row of the inverse Vandermonde matrix as $f_k = \sum_{i=1}^{n} \lambda_{i-1,k} F_i$.

In many scenarios, it is desirable to alter s. This includes adding or multiplying it by some value $v \in \mathbb{F}$ or combining it with a secret from another sharing. In a way that resembles *homomorphic encryption*, modifying s is indeed possible without having to reveal,

alter, and then share it again. A framework that realizes the aforementioned functionality is due to Ben-Or, Goldwasser, and Wigderson [BGW88] and is mainly used in the context of *secure multi-party computation (MPC)*.

In Chapters 4 and 5, we use polynomial secret sharing to protect wires in a circuit against manipulation by an adversary by identifying the wire value with the secret. Thus, if the adversary modifies, i.e., *faults*, a wire, he changes one share of the sharing F protecting the actual wire value. If the degree of the polynomial f corresponding to the faulted sharing is greater than d, the sharing is *invalid*, and otherwise remains *valid*. We call the coefficients $f_0, \dots, f_d$ the *lower-order* coefficients of f and $f_{d+1}, f_{d+2}, \dots$ the *higher-order* ones. The following observation states when a faulted sharing is invalid:

Observation 1.60. Let F be an n-sharing of a polynomial f of degree d. If $\omega \in [n-d-1]$ shares change, the degree of the polynomial corresponding to this altered sharing is at least $n-\omega$.

This is because the difference sharing $F_\Delta := F' - F$ includes exactly ω shares that do not vanish. Thus, exactly $n-\omega$ shares are 0, that is, F_Δ has at least $n-\omega$ (distinct) zeros. Accordingly, the corresponding polynomial is either the zero polynomial or its degree is at least $n-\omega$, according to Fact 1.41. The former, however, is not possible since $F_\Delta \neq 0^n$. Since we assumed that $\omega < n-d$, the degrees of f and f_Δ are distinct, and we conclude that $\deg(f') = \max\{\deg(f), \deg(f_\Delta)\} = \deg(f_\Delta) \geq n-\omega$.

Arnold et al. [ABEO24] embed two secrets in *one* polynomial using the lowest and highest coefficients. Embedding two secrets is optimal because placing a non-random value on any intermediate coefficient can restrict the choice of possible polynomials resulting from the corresponding sharing [pon13]. We mention that there are ways to embed multiple secrets, notably more than two, in one polynomial. These schemes are called *packed secret sharing schemes* and were introduced by Franklin and Yung [FY92]. The main difference is that secrets are not embedded as coefficients but as function values. We note that embedding multiple secrets in one polynomial, either using packed or conventional secret sharing, changes the "hide-reconstruct gap": Using a polynomial of degree d in Shamir's classical secret sharing guarantees that any constellation of at most d parties learns nothing about the secret, nevertheless, $d+1$ parties can reconstruct it. Thus, the gap is $(d+1)-d=1$. By embedding multiple, say, σ, secrets, $d+1$ parties still suffice to reconstruct the secrets. However, it is only guaranteed that any constellation of at most $d-\sigma+1$ parties learns nothing about the secrets. This gap of magnitude σ (as opposed to 1) yields an increase of the degree from d to $d+\sigma-1$ if we insist on requiring $d+1$ parties to reconstruct the secrets. For instance, since Arnold et al. embed two secrets, they must increment the degree by 1.

2

Introduction

An important and "nice" class of functions are *polynomial functions* because their properties make them applicable to several areas inside and outside of mathematics. For instance, they are continuous and infinitely often differentiable, i.e., smooth. They can be used to (locally) approximate functions that are otherwise hard to evaluate, e.g., using Taylor expansion. In particular, they are applicable to areas of discrete mathematics such as cryptography and coding theory. There, polynomials are usually regarded from their sharing view, that is, by the values the function assumes at specific nodes. That is because the sharing view enables extracting properties such as the (minimal) number of distinct zeros more easily. Recall that every polynomial of degree (at most) $d - 1$ is uniquely determined by d distinct members of its function graph. Notice that it is possible to embed information in the coefficients of polynomials. In coding theory, *Reed–Solomon* codes embed up to d values in polynomials over a finite field $\mathbb{F}_q$. The corresponding codeword is derived by evaluating the polynomial at $n \leq q$ nodes [RS60]. If k entries of the codeword change, the degree of the altered polynomial is at least $n - k$, which is potentially larger than $d - 1$. This enables error detection (and correction). For these codes, coefficients do not need to remain secret. The situation is different in the case of cryptography. *Shamir's secret sharing* [Sha79] embeds the secret in the constant term of a polynomial to hide and split a secret value into multiple parts. Like Reed–Solomon codes, the polynomial is evaluated at $n < q$ nodes, where each party obtains one function value. Naturally, the polynomial must not be evaluated at position 0 since this value is equal to the secret. If the degree of the polynomial is $d - 1$, then d parties suffice to reconstruct the polynomial and the secret. However, it can be shown that if the remaining $d - 1$ coefficients are sampled uniformly at random, any constitution of at most $d - 1$ parties is not only unable to reconstruct the entire polynomial but neither learns any information about the secret. Thus, secret sharing is particularly suitable for applications requiring confidentiality and tamper protection from individual parties. In this thesis, we employ secret sharing to protect circuits against adversaries that try to learn and modify the values of wires. Zeros provide a further link between a polynomial's coefficients and function values. Although the number and positions of zeros are often not apparent from the coefficients, it was shown that the more consecutive coefficients a polynomial has, all of which are 0, the fewer distinct zeros it can have [Gei15; KW14]. Formulae exist to calculate all zeros for polynomials over the reals (or complex numbers) and of degree at most 4. Never-

theless, the *Abel–Ruffini theorem* states that no *algebraic* solutions exist to solve polynomial equations involving powers greater than 4. Thus, computing the zeros of polynomials specified by their coefficients becomes more complicated. A different approach is to factorize the polynomial. Integers can be uniquely[3] decomposed into their prime factors. An analogous result holds for polynomials over fields. They can be decomposed into a product of irreducible polynomials. Observe that $v \in \mathbb{F}$ is a zero if, and only if, the linear, irreducible factor $x - v$ divides the polynomial. To determine the number of polynomials of degree d with a zero at v, it is possible to divide the polynomial by $x - v$. Thus, it is sufficient to count the number of different quotients. *Generating functions* are a handy tool to enumerate (mathematical) objects, such as polynomials with specific properties. For instance, in probability theory, they ease the computation of the PMF, mean, and variance of random variables. However, compactly storing (structured) information, e.g., the Fibonacci numbers, is also possible. We utilize generating functions to count polynomials with specific zeros.

2.1 Contributions of This Thesis

This thesis contributes to three areas: zeros of univariate polynomials over finite fields and improvements to two papers, [BEF+23] and [ABEO24].

Regarding the zeros of polynomials, we present (parts) of the results established in [IM08] and [KK90] combined as a survey. Together, both papers provide a thorough overview of the distribution of zeros. However, they cover different aspects. We link both topics by showing how the results in [KK90] can be derived from [IM08]. To this end, we generalize the results from the latter. We also restate and prove the fundamental results from [IM08] because the authors provided no proof. Finally, we correct one result from [KK90] regarding the variance of a random variable.

Furthermore, we determine the exact success probability of a (non)-adaptive adversary in [BEF+23]. Previously, the authors established an upper bound; however, the exact value remains undetermined. Ensuing from our probability, we present further upper bounds and compare our results with those from [BEF+23].

The third and final contribution is the improvement of the error detection of the double-sharing framework introduced in [ABEO24]. The original framework allows an adversary to go unnoticed. We present two modifications that eliminate this possibility. Moreover, we argue why one approach cannot work for the framework.

2.2 Related Work

Polynomials are a well-studied subject. The same is true for their zeros. Unless otherwise stated, we assume that (random) polynomials are members of the polynomial ring $\mathbb{F}_q[x]$, where q is a prime power.

In [IM08], Ivchenko and Medvedev analyze what they call the "local structure" of random polynomials f. They decompose f into its irreducible factors and consider their mul-

[3] Up to reordering of factors.

tiplicities. Among other things, they consider the probability that the j^{th} irreducible factor of degree $i \in [n]$ occurs in the decomposition of f with a multiplicity of exactly and at least $s \in [0, n]$, respectively. The authors consider the corresponding probability distribution, mean, variance, and asymptotic behavior for many variants. They specifically address the case $i = 1$, i.e., the linear irreducible polynomials. As mentioned at the beginning of this chapter, these factors contribute the zeros of f. We remark that we use results from this paper in Chapter 3.

Knopfmacher and Knopfmacher [KK90] investigate the number of polynomials of degree n with exactly $k \in [0, n]$ zeros and distinct zeros, respectively. Moreover, they establish the average number and variance in both cases, as well as their asymptotic behavior. The authors employ generating functions to count the number of such polynomials. We use this technique and present their results in Chapter 3. Recall that the number of linear irreducible factors, i.e., factors of degree $i = 1$, of a polynomial is equal to the number of its zeros. In a follow-up paper, Knopfmacher and Knopfmacher [KK93] generalize the results from [KK90] to count the number of polynomials with exactly k (distinct) irreducible factors of degree i.

In 2023, Jain, Moon, and Wu [JMW23] proved that for any fixed q, the average number of distinct zeros of any non-constant multivariate polynomial in m variables is always q^{m-1}. In particular, $m = 1$ implies that for univariate polynomials, the average number is $q^{1-1} = 1$. We mention that this result is known in the univariate case, e.g., due to [KK90], and in the multivariate case, e.g., due to [Sch76]. Nevertheless, the authors use a different approach from the realm of algebraic geometry to prove the result.

Kopparty and Wang [KW14] show that if a polynomial $f \neq 0$ with $\deg(f) \leq q - 2$ has many distinct zeros, it cannot have a long consecutive sequence of zero-coefficients. More precisely, they prove that if $m \in \mathbb{N}$ is the number of positions $v \in \mathbb{F}_q^*$ such that $f(v) \neq 0$, then for no $k \in [0, q - 1 - m]$, all m consecutive coefficients starting at f_k, that is, $f_k, f_{k+1}, \dots, f_{k+m-1}$, are 0. Geil [Gei15] generalizes the above result in two aspects. Firstly, he considers any $k \in [0, q - 2]$ with m consecutive coefficients starting at f_k, i.e., $f_k, f_{(k+1) \bmod (q-1)}, \dots, f_{(k+m-1) \bmod (q-1)}$. For instance, this allows us to consider only the lowest and highest coefficients, f_0 and f_n. By "arranging" the coefficients circularly, it becomes apparent that both are consecutive, although 0 and n are not. An alternative formulation of his theorem is the following: If f takes m different non-zero values (i.e., if f has $q-1-m$ zeros) in $\mathbb{F}_q^*$, then it cannot occur that m consecutive coefficients are all 0. Moreover, Geil states a variant for multivariate polynomials in m variables. However, since this thesis considers univariate polynomials, we omit further details.

Ax [Ax64] shows that for all multivariate polynomials f in m variables of total degree d, the number q^b divides the number of zeros of f. Here, $b \in \mathbb{N}_0$ is the largest number such that $b < m/d$. Unfortunately, this result is trivial for univariate polynomials since $m = 1$ implies that if $d \geq 1$, the variable b is 0. Thus, $q^b = q^0 = 1$, which divides every integer.

The authors of [DNV15] consider zeros of random polynomials over $\mathbb{R}$. Since it is uncertain how to sample coefficients or polynomials uniformly at random from an (uncountably) infinitely "wide" set, different distributions are considered. Do, Nguyen, and Vu sample a random polynomial f of degree n by sampling its i.i.d. coefficients $f_0, \dots, f_n$ according to any distribution that (1) has mean 0, (2) has unit variance, and (3) 0 is not

in its support. Among other things, they consider the case where the f_i are Bernoulli-distributed such that $\Pr[f_i = -1] = 1/2$ and $\Pr[f_i = 1] = 1/2$. Then, they show that the probability that f has at least one double zero is at most $\Theta(n^{-2}) + n^{-\omega(1)}$.

Hwang [Hwa98] considers the random variable Ω_n of the number of irreducible factors of a random polynomial in $\mathcal{M}_n$. He shows that the PMF $\Pr[\Omega_n = s]$, where $s \in \mathbb{N}$, is a convolution if $n \to \infty$ and $n - s \to \infty$. In that case, Ω_n follows a Poisson distribution convoluted with a negative binomial one.

Many works regarding (irreducible) factors of polynomials use generating functions to count polynomials that satisfy specific properties. For instance, Flajolet, Gourdon, and Panario [FGP96] and Panario [Pan04] thereby prove that the number of squarefree[4] polynomials in $\mathcal{M}_n$ of degree at least 2 is $q^n - q^{n-1}$. From this, they deduce that a random polynomial is squarefree with probability $1 - q^{-1}$, which tends to 1 if $q \to \infty$. Thus, an overwhelming number of polynomials decomposes into distinct irreducible polynomials. We recall that in the previous Chapter 1, we used generating functions to count the number of all, monic, and irreducible polynomials of degree n.

We conclude this section by considering fault attacks. Richter-Brockmann, Sasdrich, and Güneysu [RSG23] evaluate common fault attack techniques. Additionally, they propose a generic and unified model to describe adversaries in fault attacks, which is suitable for many different techniques.

2.3 Structure of This Thesis

This thesis comprises three main parts: Chapter 3 concerns zeros of polynomials. We start by analyzing the multiplicity of a zero at one particular position, which enables us to expand our analysis to multiple arbitrary positions. We use these results to focus on the total number of zeros and distinct zeros. In Chapter 4, we improve one result from [BEF+23], which concerns the success probabilities of two kinds of adversaries. We begin by determining the exact number of two polynomials that occur. This way, we establish the exact success probabilities of both adversaries. Afterward, we provide upper bounds on one of the probabilities and compare our result with the original one. Finally, in Chapter 5, we present modifications to the framework from [ABEO24] such that a rigging adversary is always detected instead of only with a certain likelihood. Our first approaches are bound to the current operation used with the framework. Then, we present a universal method. Due to its inefficiency, we present a further method.

[4] A polynomial is *squarefree* if all irreducible factors occur in its decomposition with multiplicity at most 1.

3

Zeros of Polynomials

In this chapter, we analyze polynomials with regard to the distribution of their zeros. Among other things, we consider the number of polynomials of degree $n \in \mathbb{N}_0$ with $k \leq n$ total zeros and distinct zeros each. When choosing a polynomial f from $\mathcal{M}_n$ (or $\mathcal{P}_n$) uniformly at random, the numbers immediately yield the probability that f possesses a given type and number of zeros, e.g., k zeros either in total or distinct. By gaining insight into the number and distribution of different variants of zeros, we aim to provide a foundation for applications that concern polynomials in terms of their zeros or degrees. It is known that for polynomials, the degree and number of zeros are related, e.g., due to Fact 1.41. For instance, a polynomial of degree 4 cannot have more than four zeros (unless it is the zero polynomial). We note that this upper bound holds only for univariate polynomials over a field. However, we restrict ourselves to such polynomials in this chapter. In addition, polynomials can be regarded from their sharing view, i.e., from the values they take at certain positions. In this case, the number and positions of zeros are immediately apparent. In Chapters 4 and 5, we consider polynomials from that sharing view. Although this chapter does not contribute to improving the results in these two chapters, its results may become helpful to further research in their areas, namely, polynomial masking and fault resilience. Notwithstanding the benefit for other applications, we provide an extensive survey regarding the distribution of zeros of polynomials over finite fields. To the best of our knowledge, we are the first to compile the results in such a united manner.

In the first Section 3.1, we start by considering a zero at *one specific* position $v \in \mathbb{F}$ and examine polynomials regarding the multiplicity of that zero. Zeros may occur at other positions, too, but we neglect them. We give the probability distribution of the multiplicity but also state its average and variance. Furthermore, we consider the asymptotic behavior as $n \to \infty$ and find that the distribution has a geometric limit.

In Section 3.2, we expand our analysis of the multiplicity to two and then arbitrary $\ell \in [|\mathbb{F}|]$ zeros at specific positions. As before, we investigate the numbers and probability distributions. Moreover, we consider the restriction that zeros must not occur at positions other than those ℓ.

Afterward, in Section 3.3, we relax the assumptions on specific multiplicities at certain positions and only require these positions to have a combined multiplicity of k. When setting $\ell = q$, we obtain polynomials with exactly k zeros in total. We elaborate on that

number and its probability distribution. Here, we find that the distribution has a negative binomial limit.

Finally, Section 3.4 addresses the case when we consider the positions of zeros but not their multiplicities. For a given collection of positions, we give the number of polynomials with zeros at those positions. We also provide the number when we additionally require that zeros at positions other than those in the collection must not occur. Similarly to the previous Section 3.3, we relax the assumptions of the exact positions and obtain the number of polynomials with exactly k distinct zeros. Again, we go into detail about the distribution and finally ascertain a binomial limit.

Unless otherwise stated, the following holds: We consider polynomials and zeros over $\mathbb{F}_q[x]$ and $\mathbb{F}_q =: \mathbb{F}$, respectively, where q is a prime power. Moreover, we primarily consider *monic* polynomials for convenience. Since $\mathcal{P}_n$ and $\mathcal{M}_n$ differ by a factor of $q-1$, multiplying any number established in a theorem (or suchlike) by $q-1$ yields the number when polynomials in $\mathcal{P}_n$ are considered. When mentioning the term *monic* in parentheses, i.e., "(monic)," we intend to express that the respective matter holds for both monic and non-monic polynomials. We recall that the multiplicity of a zero is the *exact* number of times the zero occurs. Thus, a polynomial with a zero v of multiplicity s implies that $(x-v)^{s+1}$ does not divide the polynomial. In theorems (or suchlike), we use the phrase *such that* to implicitly set the quantity in question to 0 if the subsequent condition is false. For instance, the sentence "For all k, n such that $k \leq n$, the number of polynomials of degree n with k zeros..." implies that if $k > n$, said number is 0.

3.1 The Multiplicity of One Zero

We begin this chapter with the most trivial case, focusing on *one* position and considering polynomials with a zero there (but not necessarily only there). In later sections, we expand our study to multiple positions. Our analysis of multiplicities of individual zeros is influenced by Ivchenko and Medvedev [IM08]. In this paper, the authors analyze the decomposition of polynomials into irreducible factors. For us, the irreducible polynomials of degree 1 are of interest because they correspond to the zeros. The authors state several probabilities regarding zeros at one or multiple individual positions. However, [IM08] does *not* include proofs nor the corresponding number of polynomials that satisfy these constraints. Thus, we use generating functions to count polynomials first. This way, we deduce the probability and prove the statements claimed in [IM08]. Furthermore, we independently determine some results from [IM08].

Firstly, we state the number of polynomials of degree n with a zero of multiplicity s at an arbitrary but fixed position $v \in \mathbb{F}$. We recall that it is still possible for the polynomial to have additional zeros at other positions. For instance, if $v = 1$ and $s = 3$, the polynomial $x^5(x-1)^3$ is feasible nevertheless. We stress that Ivchenko and Medvedev [IM08] determine the corresponding probability (stated below in Corollary 3.2). However, they present no proof. Since it is simple to derive the probability from the number of favorable polynomials, we first determine the latter. To count polynomials, we follow the methodology of Knopfmacher and Knopfmacher [KK90], who use generating functions to prove Theorems 3.19 and 3.28, found in Sections 3.3 and 3.4, respectively. These theorems ad-

dress a polynomial's total number of (distinct) zeros. However, since it is reasonable to begin with examining one zero, we adapt their approach to use it to prove Theorem 3.1 first. Throughout this chapter, we use their methodology in various ways to count polynomials satisfying different constraints on their zeros.

Theorem 3.1. *For all $n, s \in \mathbb{N}_0$ such that $s \leq n$ and for all $v \in \mathbb{F}$, the number of monic polynomials of degree n with a zero at $x = v$ of multiplicity s equals $Z_1(s,n) := Z_{1,v}(s,n) :=$*
$$\begin{cases} q^{n-s} - q^{n-s-1} & \text{if } s \leq n-1 \\ 1 & \text{if } s = n. \end{cases}$$

Proof ([KK90]). Let v be arbitrary but fixed, and let $f \in \mathcal{M}_n$ have a zero at v of multiplicity s. Throughout several proofs in this chapter, we use the fact that we can factorize polynomials over a field into a unique product of irreducible polynomials. This follows because $\mathbb{F}[x]$ is a UFD, according to Fact 1.7. In particular, we can factorize linear terms, which correspond to zeros.

Here, we can write $f = (x-v)^s g$, where g is another polynomial. Factorizing f in that way ensures that f has a zero at $x = v$ of multiplicity *at least* s. So far, the multiplicity does not need to be *exactly* s because g might also include $x - v$ as a factor. Either way, $\deg(g) = n - s$ since $\deg(f) = n$ and s linear factors $x - v$ are fixed. We must ensure that g does not have a zero at v, that is, $g(v) \neq 0$. Thus, we may only consider such g with all zeros being at $x \neq v$. Accordingly, the number of desired polynomials f equals the number of such $g \in \mathcal{M}_{n-s}$.

To determine the number of feasible g, we use generating functions. Knopfmacher and Knopfmacher [KK90] prove Theorem 3.19 using an approach that involves generating functions. We adapt their approach to prove this theorem. In that regard, we recall the proof of Theorem 1.53. As described in the proof of Theorem 1.53, the collection of all monic polynomials is $\prod_{f \in \mathcal{F}} (1-f)^{-1}$, where $\mathcal{F}$ is the family of all monic irreducible polynomials. We are interested in the collection of all monic polynomials *without* zeros at $x = v$. Let G be this multiplicative semigroup generated by all *non-linear* monic irreducible polynomials and the linear ones $x - v'$, where $v' \in \mathbb{F} \setminus \{v\}$. We stress that *generated* is different from *consist of*. Besides, although the identity $1 = 1x^0$ is not irreducible, it is generated by the irreducible polynomials, i.e., $1 \in G$. Thus, G is not only a semigroup but also a monoid. Nevertheless, we call G a semigroup to be consistent with [KK90]. To summarize: A monic polynomial lies in G if, and only if, it has no zero at v.

We call $G(z) = \sum_{n=0}^{\infty} G(n) z^n$ the generating function of $(G(n))_{n \in \mathbb{N}_0}$, where $G(n)$ is the number of polynomials of degree n in G, i.e., $G(n) = |G \cap \mathcal{M}_n|$. The generating function of all monic polynomials is $\mathcal{M}(z) = 1/(1-qz) = \prod_{n=1}^{\infty} (1-z^n)^{-I_n}$, according to Theorem 1.53. Since $\mathcal{M}(z)$ is already known, we try to express $G(z)$ using $\mathcal{M}(z)$. In the product $\prod_{n=1}^{\infty} (1-z^n)^{-I_n}$, the factor at $n = 1$ contributes the linear factors, i.e., zeros. This factor $(1-z^1)^{-I_1} = (1-z)^{-q}$ now becomes $(1-z)^{-(q-1)}$ because polynomials generated by G must not include *one* specific factor, namely, $x - v$. Thus, the number of irreducible polynomials in $\mathcal{F}$ of degree 1 that we regard is $|\mathfrak{I}_1 \setminus \{x - v\}| = I_1 - 1 = q - 1$.

We split the product of $\mathcal{M}(z)$ into $\prod_{n=1}^{\infty} (1-z^n)^{-I_n} = (1-z)^{-q} \prod_{n=2}^{\infty} (1-z^n)^{-I_n}$. This enables us to compare $\mathcal{M}(z)$ with $G(z)$ factor-wise. By the above reasoning, it holds that $G(z) = (1-z)^{-(q-1)} \prod_{n=2}^{\infty} (1-z^n)^{-I_n}$. Consequently, $\mathcal{M}(z)$ and $G(z)$ only differ in the

first factor, which yields the following relation: $\mathcal{M}(z) = (1-z)^{-1}G(z)$, or equivalently, $(1-z)\mathcal{M}(z) = G(z)$. This can be seen because we only need to turn the first factor $(1-z)^{-q}$ into $(1-z)^{-(q-1)}$, which we accomplish by multiplying $(1-z)^{-q}$ by $1-z$.

Next, we use the simple closed form of $\mathcal{M}(z)$, namely, $1/(1-qz)$, to derive one for $G(z)$. We have $G(z) = (1-z)\mathcal{M}(z) = (1-z)\cdot 1/(1-qz) = (1-z)/(1-qz)$.

It remains to find $G(n)$, which is included in $G(z) \triangleq \sum_{n=0}^{\infty} G(n)z^n$. Fortunately, $G(z)$ is the product of two generating functions, $1-z$ and $1/(1-qz)$, each of which we know the generated sequence of: For one thing, $1-z = 1z^0 + (-1)z^1$ is the generating function of the sequence $(1,-1,0,0,\dots)$, and for another, $1/(1-qz) = \sum_{n=0}^{\infty} q^n z^n$. We use the *Cauchy product* to determine the sequence generated by $(1-z)\cdot(1/(1-qz))$, i.e., $G(n)$:

$$G(z) = \frac{1-z}{1-qz} = \sum_{n=0}^{\infty}\left(\sum_{i=0}^{n} q^{n-i}\begin{cases}1 & \text{if } i=0\\ -1 & \text{if } i=1\\ 0 & \text{else}\end{cases}\right)z^n = \sum_{n=0}^{\infty}\left(\begin{cases}q^0 & \text{if } n=0\\ q^n - q^{n-1} & \text{else}\end{cases}\right)z^n.$$

Since $G(z) \triangleq \sum_{n=0}^{\infty} G(n)z^n$, we can see that

$$G(n) = [z^n]G(z) = \begin{cases}q^0 & \text{if } n=0\\ q^n - q^{n-1} & \text{else}\end{cases} = \begin{cases}1 & \text{if } n=0\\ q^n - q^{n-1} & \text{else.}\end{cases}$$

Recall that $\deg(g) = n-s$, so the number of feasible g is $G(n-s)$, which equals

$$G(n-s) = \begin{cases}1 & \text{if } n-s=0\\ q^{n-s} - q^{n-s-1} & \text{else}\end{cases} = \begin{cases}q^{n-s} - q^{n-s-1} & \text{if } s \le n-1\\ 1 & \text{if } s = n.\end{cases}$$

Based on the above reasoning, the number of feasible g equals the number of different f with a zero at v of multiplicity s. Since $G(n-s)$ is said number, the claim follows. ■

We note that since v was chosen arbitrarily, $Z_{1,v}(s,n) = Z_{1,v'}(s,n)$ for all $v, v' \in \mathbb{F}$. This is reflected in the function $Z_{1,v}(s,n)$, which is independent of v.

We use the obtained function $Z_1(s,n)$ to derive the probability that a polynomial has a zero at v of multiplicity s. According to *Laplace's rule*, if we assume a uniform distribution over the polynomials in $\mathcal{M}_n$ (or $\mathcal{P}_n$), the probability in question is given by the number of favorable polynomials, i.e., $Z_1(s,n)$, divided by the number of all polynomials, i.e., $|\mathcal{M}_n|$ or $|\mathcal{P}_n|$. Irrespective of whether or not we restrict ourselves to monic polynomials, the probability remains the same. This is implied by Theorem 1.50 since the process of converting a polynomial into its monic form is independent of its zeros. We recall that Ivchenko and Medvedev give the probability but without proof.

Corollary 3.2 ([IM08]). *For all $n, s \in \mathbb{N}_0$ such that $s \le n$ and for all $v \in \mathbb{F}$, let $\mathcal{Z}_1(n) := \mathcal{Z}_{1,v}(n)$ denote the random variable of the multiplicity of the zero v of a random (monic) polynomial of degree n. Then, the PMF of $\mathcal{Z}_{1,v}(n)$ equals* $\Pr[\mathcal{Z}_{1,v}(n) = s] = \begin{cases}q^{-s} - q^{-s-1} & \text{if } s \le n-1\\ q^{-s} & \text{if } s = n.\end{cases}$

Proof. Due to the uniform distribution, each polynomial $f \in \mathcal{M}_n$ has an equal chance to be chosen. This leads to $\Pr[\mathcal{Z}_{1,v}(n) = s] = Z_1(s,n)/|\mathcal{M}_n| = Z_1(s,n)/q^n$.

Corollary 1.49 states that $|\mathcal{P}_n| = (q-1)|\mathcal{M}_n|$. Accordingly, if $f \in \mathcal{P}_n$, then we have $\Pr[\mathcal{Z}_{1,v}(n) = s] = ((q-1)Z_1(s,n))/|\mathcal{P}_n| = Z_1(s,n)(q-1)/((q-1)q^n) = Z_1(s,n)/q^n$ as before. ■

For our applications, we usually consider polynomials from their sharing view. If a share at node v is zero, we can directly deduce that the polynomial has a zero there. However, we cannot infer anything about the multiplicity of this zero other than that it is *at least* 1. Since the support of $\mathcal{Z}_1(n)$ is $[0,n]$, finding the probability that v is a zero is easy. In fact, the probability is $\Pr[\mathcal{Z}_1(n) \geq 1] = 1 - \Pr[\mathcal{Z}_1(n) = 0]$. Although the probabilities $\Pr[\mathcal{Z}_1(n) \geq 1]$ and $\Pr[\mathcal{Z}_1(n) \geq s]$ (the latter being the "probability variant" of Lemma 3.4) appear in [IM08], we derived them independently as we were unaware that Ivchenko and Medvedev had previously stated them. We use Corollary 3.2 to conclude that the probability is:

Corollary 3.3 ([IM08]). *Let $n \in \mathbb{N}_0$, $v \in \mathbb{F}$, and $f \in \mathcal{P}_n$ (be monic). The probability that v is a zero of f equals $\Pr[\mathcal{Z}_{1,v}(n) \geq 1] = [\![n \geq 1]\!] q^{-1}$. The probability that v is not a zero of f equals $\Pr[\mathcal{Z}_{1,v}(n) = 0] = 1 - [\![n \geq 1]\!] q^{-1}$.*

We omit the proof since the probabilities can be directly obtained from Observation 3.2 using $s = 0$. Nevertheless, we mention that Corollary 3.3 can also be deduced using generating functions in an approach similar to the proof of Theorem 3.1. We recall that in the proof, we needed to ensure that g does not have a zero at v. However, in Corollary 3.3, we only require a multiplicity of *at least* one. Thus, any g (with the proper degree) is feasible, and we only need to count how many polynomials of said degree exist. That number is given in Theorem 1.48.

We state this result below but in a more generalized form since we use it for further applications in later sections.

Lemma 3.4. *Let $n \in \mathbb{N}_0$ and let $v_1, \dots, v_\ell \in \mathbb{F}$ be pairwise distinct. The number of monic polynomials of degree n with zeros at $v_1, \dots, v_\ell$ of multiplicities* at least *$s_1, \dots, s_\ell \in \mathbb{N}_0$, respectively, is q^{n-k}, where $k := \sum_{i=1}^{\ell} s_i \leq n$.*

Proof. Let $f \in \mathcal{M}_n$, and let $v_1, \dots, v_\ell$ be arbitrary but fixed. As before, we write f as the product of the zeros $x - v_1, \dots, x - v_\ell$ and some polynomial g. We factorize out $(x - v_i)^{s_i}$ since the multiplicity of v_i is *at least* s_i. More formally, we write $f = g \prod_{i=1}^{\ell} (x - v_i)^{s_i}$, where g is a polynomial of degree $n - k$. Any g is suitable because it can only add zeros to f. Hence, it cannot decrease but increase the multiplicities of the v_i. We conclude that the number of feasible f is precisely the number of polynomials of degree $n - k$, namely, $|\mathcal{M}_{n-k}| = q^{n-k}$. ■

To prove Corollary 3.3 using Lemma 3.4, as mentioned before, we set $\ell = 1$, $k = 1$, and obtain q^{n-1}. Dividing this number by $|\mathcal{M}_n| = q^n$ yields $q^{-1} = \Pr[\mathcal{Z}_1(n) \geq 1]$.

However, Lemma 3.4 can be used to not only prove the "at least" case but also the "exact" cases in Theorem 3.1 and Corollary 3.2. This is achieved by expressing equality through inequalities as follows: Observe that for all integers s and s', the two propositions $s = s'$ and $s \geq s' \wedge \neg(s \geq s' + 1)$ are equivalent. Hence, some zero v of f has a multiplicity of s if, and only if, v has a multiplicity of at least s but not at least $s + 1$. According to

Lemma 3.4, the number, therefore, is $q^{n-s} - q^{n-(s+1)}$ if $s < n$ and $q^{n-n} - 0 = 1$ if $s = n$. In both cases, it coincides with $Z_1(s, n)$.

For the remainder of this section, we return to the random variable $\mathcal{Z}_1(n)$. To better understand its behavior, we analyze two statistical quantities: its expectation and variance. The former can be found in [IM08], however, without its asymptotic behavior and proof, and equals:

Theorem 3.5 ([IM08]). *The expected value of $\mathcal{Z}_1(n)$ is $\mathbb{E}[\mathcal{Z}_1(n)] = (1 - q^{-n})/(q-1)$. Moreover, the asymptotic expectation equals $\lim_{n\to\infty} \mathbb{E}[\mathcal{Z}_1(n)] = 1/(q-1)$.*

Proof. We use the definition of the expectation, i.e., $\mathbb{E}[\mathcal{Z}_1(n)] \triangleq \sum_{s=0}^{n} s \Pr[\mathcal{Z}_1(n) = s]$. In Corollary 3.2, we established that $\Pr[\mathcal{Z}_1(n) = s]$ distinguishes two cases, $s \leq n-1$ and $s = n$. Thus, we split the sum accordingly and obtain

$$\begin{aligned}
\mathbb{E}[\mathcal{Z}_1(n)] &= \sum_{s=0}^{n-1} s \Pr[\mathcal{Z}_1(n) = s] + \sum_{s=n}^{n} s \Pr[\mathcal{Z}_1(n) = s] \\
&= \sum_{s=0}^{n-1} s(q^{-s} - q^{-s-1}) + nq^{-n} \\
&= \frac{q^{-n}(q^n - nq + n - 1)}{q-1} + nq^{-n} \\
&= \frac{1 - q^{-n}}{q-1}.
\end{aligned} \tag{3.1}$$

It remains to determine the asymptotic expectation. Using the result from Equation 3.1, we obtain $\lim_{n\to\infty} \mathbb{E}[\mathcal{Z}_1(n)] = \lim_{n\to\infty}(1-q^{-n})/(q-1) = (1-0)/(q-1) = 1/(q-1)$. ■

Proceeding from the expectation, we can now calculate the variance.

Theorem 3.6. *The variance of $\mathcal{Z}_1(n)$ is $\mathrm{Var}[\mathcal{Z}_1(n)] = \frac{q^{-2n}(q^{2n+1} - (2n+1)(q-1)q^n - 1)}{(q-1)^2}$. Moreover, the asymptotic variance equals $\lim_{n\to\infty} \mathrm{Var}[\mathcal{Z}_1(n)] = q/(q-1)^2$.*

Proof. It is well known that $\mathrm{Var}[\mathcal{Z}_1(n)] = \mathbb{E}[\mathcal{Z}_1(n)^2] - \mathbb{E}[\mathcal{Z}_1(n)]^2$. Thus, we determine the minuend and subtrahend. Computing $\mathbb{E}[\mathcal{Z}_1(n)]^2$ is straightforward since we already established $\mathbb{E}[\mathcal{Z}_1(n)]$ in Theorem 3.5. The second raw moment $\mathbb{E}[\mathcal{Z}_1(n)^2]$ is established in the same way $\mathbb{E}[\mathcal{Z}_1(n)]$ was, that is, we split the sum. We obtain

$$\begin{aligned}
\mathbb{E}[\mathcal{Z}_1(n)^2] &= \sum_{s=0}^{n-1} s^2 \Pr[\mathcal{Z}_1(n) = s] + n^2 q^{-n} \\
&= \frac{q^{-n}\left((q+1)(q^n-1) - 2n(q-1) - n^2(q-1)^2\right)}{(q-1)^2} + n^2 q^{-n} \\
&= \frac{q^{-n}\left((q+1)(q^n-1) - 2n(q-1)\right)}{(q-1)^2}.
\end{aligned}$$

Combining both values results in

$$\begin{aligned}
\mathrm{Var}[\mathcal{Z}_1(n)] &= \frac{q^{-n}\left((q+1)(q^n-1) - 2n(q-1)\right)}{(q-1)^2} - \left(\frac{1-q^{-n}}{q-1}\right)^2 \\
&= \frac{q^{-2n}\left(q^{2n+1} - (2n+1)(q-1)q^n - 1\right)}{(q-1)^2}.
\end{aligned}$$

To determine the asymptotic variance as n approaches infinity, we observe that the leading term in the parentheses of the above numerator is q^{2n+1}. Thus, we omit the other terms and establish $\lim_{n\to\infty} \operatorname{Var}[\mathcal{Z}_1(n)] = \lim_{n\to\infty}(q^{-2n}(q^{2n+1}+0))/(q-1)^2 = q/(q-1)^2$. ■

The alert reader might have noticed that in the asymptotic case, as n tends to infinity, mean and variance agree with those of $\operatorname{Geo}(1-q^{-1})$. This is not a coincidence since for $s \leq n-1$, the PMF of $\mathcal{Z}_1(n)$ equals $\Pr[\mathcal{Z}_1(n) = s] = q^{-s} - q^{-s-1} = (q^{-1})^s(1-q^{-1})$. This is precisely the PMF of a random variable $X \sim \operatorname{Geo}(1-q^{-1})$ at $X = s$, according to Definition 1.15. Ivchenko and Medvedev state that $\mathcal{Z}_1(n)$ follows the truncated geometric distribution $\operatorname{Geo}(q^{-1})$. However, it is apparent that the truncated PMF of $\mathcal{Z}_1(n)$ corresponds to $\operatorname{Geo}(1-q^{-1})$ and not $\operatorname{Geo}(q^{-1})$.

Observation 3.7 *(Corrected [IM08]).* The random variable $\mathcal{Z}_1(n)$ follows a geometric distribution truncated at $s = n$. More precisely, $\Pr[\mathcal{Z}_1(n) = s] = \Pr[X = s]$ if, and only if, $s \leq n-1$, where $X \sim \operatorname{Geo}(1-q^{-1})$.

Because both PMFs are equal at all support points except $s = n$, it follows that $\mathcal{Z}_1(n)$ has a geometric limit. Let $\mathcal{Z}_1 := \mathcal{Z}_{1,v}$ denote the limit distribution of $\mathcal{Z}_1(n)$ as $n \to \infty$. Informally speaking, this follows because the distribution of $\mathcal{Z}_1(n)$ is a "compressed" variant of the one $\mathcal{Z}_1$ follows, i.e., $\operatorname{Geo}(1-q^{-1})$. More precisely, $\Pr[\mathcal{Z}_1(n) = n] = q^{-n}$ and $\Pr[\mathcal{Z}_1(n) > n] = 0$, but $\mathcal{Z}_1$ has an infinite support with $\Pr[\mathcal{Z}_1 \geq n] = q^{-n}$. In other words, $\mathcal{Z}_1(n)$ "centers all its mass above" $n-1$ at $s = n$, whereas $\mathcal{Z}(n)$ does not.

We will later see that all random variables we consider throughout this chapter have common limit distributions.

Theorem 3.8. *The sequence $(\mathcal{Z}_1(n))_{n\in\mathbb{N}_0}$ converges in distribution to $\mathcal{Z}_1 \sim \operatorname{Geo}(1-q^{-1})$.*

Proof. Let $F_n(s) = \Pr[\mathcal{Z}_1(n) \leq s]$ and $F(s) = \Pr[\mathcal{Z}_1 \leq s]$ denote the CDF of $\mathcal{Z}_1(n)$ and $\mathcal{Z}_1$, respectively. Firstly, we observe that the two CDFs are $F_n(s) = 1 - [\![s \leq n-1]\!]q^{-s-1}$ and $F(s) = 1 - q^{-s-1}$.

To prove convergence in distribution, we need to show that $\lim_{n\to\infty} F_n(s) = F(s)$ for all $s \geq 0$. Since $s \leq n-1$ holds for all s when n approaches infinity, we conclude that $\lim_{n\to\infty} F_n(s) = 1 - 1 \cdot q^{-s-1}$, which coincides with $F(s)$. ■

As mentioned above, the PMFs of $\mathcal{Z}_1(n)$ and $\mathcal{Z}_1$ only disagree if $s \geq n$. However, the probability that any of both random variables takes a value $s \geq n$ is the same, namely, $\Pr[\mathcal{Z}_1(n) \geq n] = \Pr[\mathcal{Z}_1 \geq n] = q^{-n}$. Since q^{-n} is negligible in n, both distributions seem to "approach" each other exponentially fast (in n). Ivchenko and Medvedev [IM08] observed but did not prove that this holds if the notion of closeness is the *statistical distance* between $\mathcal{Z}_1(n)$ and $\mathcal{Z}_1$.

Theorem 3.9 ([IM08]). *The statistical distance between $\mathcal{Z}_1(n)$ and $\mathcal{Z}_1$ is $\Delta(\mathcal{Z}_1(n), \mathcal{Z}_1) = q^{-n-1}$.*

Proof. Let $\delta(s) = \Pr[\mathcal{Z}_1(n) = s] - \Pr[\mathcal{Z}_1 = s]$. The statistical distance is defined as $\Delta(\mathcal{Z}_1(n), \mathcal{Z}_1) = 1/2 \sum_{s=0}^{\infty} |\delta(s)|$. Following Corollary 3.2, we split the sum into three parts

and obtain

$$\begin{aligned}\sum_{s=0}^{\infty}|\delta(s)| &= \sum_{s=0}^{n-1}|\delta(s)| + |\delta(n)| + \sum_{s=n+1}^{\infty}|\delta(s)| \\ &= \sum_{s=0}^{n-1} 0 + \left|q^{-n} - (q^{-1})^n(1-q^{-1})\right| + \sum_{s=n+1}^{\infty}\Pr[\mathcal{Z}_1 = s] \\ &= 0 + |q^{-n-1}| + q^{-n-1} \\ &= 2q^{-n-1}.\end{aligned}$$

We conclude that $\Delta(\mathcal{Z}_1(n), \mathcal{Z}_1) = 1/2(2q^{-n-1}) = q^{-n-1}$. ■

If the geometric distribution is used to approximate the actual distribution of $\mathcal{Z}_1(n)$, the error is at most q^{-n-1} as Theorem 3.9 implies $|\Pr[\mathcal{Z}_1(n) \in S] - \Pr[\mathcal{Z}_1 \in S]| \leq q^{-n-1}$ for all $S \subseteq [0, \infty)$. The inequality holds in particular if S is a singleton.

3.2 The Multiplicities of Arbitrary Zeros

In this section, we "generalize" our findings from Section 3.1 and consider *two*, later on, $\ell \leq q$, different zeros, $v_1, v_2 \in \mathbb{F}$, with respective multiplicities of s_1 and s_2. We put *generalize* into quotation marks because we now specify the multiplicities of zeros at two (or ℓ) positions. If we neglect part of the zeros, we still need to specify their multiplicities (and positions).

We first inspect the joint probability function $\Pr[\mathcal{Z}_{1,v_1}(n) = s_1 \wedge \mathcal{Z}_{1,v_2}(n) = s_2]$, where $s_1 + s_2 \leq n$. Calculations would become simple if the random variables $\mathcal{Z}_{1,v_1}(n)$ and $\mathcal{Z}_{1,v_2}(n)$ were independent. In that case, the "generalization" is merely the product of both individual PMFs we established in Corollary 3.2. Unfortunately, this is not the case, as demonstrated by the following counterexample:

Counterexample 3.10. Let $s_1 = s_2 = n/2$ and let n be even. Then, the individual probability distributions are $\Pr[\mathcal{Z}_{1,v_1}(n) = s_1] = \Pr[\mathcal{Z}_{1,v_2}(n) = s_2] = q^{-n/2} - q^{-n/2-1}$, and the product equals $(q-1)^2 q^{-n-2}$. However, the joint PMF is $\Pr[\mathcal{Z}_{1,v_1}(n) = s_1 \wedge \mathcal{Z}_{1,v_2}(n) = s_2] = q^{-n}$ since the only possible polynomial is $(x - v_1)^{n/2}(x - v_2)^{n/2}$. Both probabilities are equal if, and only if, $q = 1/2$.

The fact that both random variables are dependent is not surprising because knowing that a factor $(x - v_1)^{s_1}$ divides some polynomial influences the choice of possible s_2 of the factor $(x - v_2)^{s_2}$. For instance, if $s_1 = n - 3$, Fact 1.41 implies that $s_2 \leq 3$ since $s_1 + s_2 \leq n$. In that case, the factor $(x - v_2)^{n-1}$ cannot occur (unless $n \leq 4$).

Since the one-zero case does not trivially expand to multiple zeros, we use generating functions to establish the number of polynomials with two zeros of multiplicities s_1 and s_2, respectively. The approach is similar to Theorem 3.1. For clarity, we denote the pairs, later on, ℓ-tuples, of zeros and multiplicities by $\underline{v} = (v_1, v_2)$ and $\underline{s} = (s_1, s_2)$, respectively.

Theorem 3.11. *For all $n, s_1, s_2 \in \mathbb{N}_0$ such that $s_1 + s_2 \leq n$ and for all $v_1 \neq v_2 \in \mathbb{F}$, the number of monic polynomials of degree n with zeros at v_1 and v_2 of multiplicities s_1 and s_2, respectively, equals*

$$Z_2(\underline{s}, n) := Z_{2,\underline{v}}(\underline{s}, n) := \begin{cases} (q-1)^2 q^{n-(s_1+s_2)-2} & \text{if } s_1 + s_2 \leq n-2 \\ q-2 & \text{if } s_1 + s_2 = n-1 \\ 1 & \text{if } s_1 + s_2 = n. \end{cases}$$

Proof. Let $v_1 \neq v_2$ be arbitrary but fixed, and let $f \in \mathcal{M}_n$ be as required. We adapt the proof of Theorem 3.1 and explicitly consider the *two* factors $(x-v_1)^{s_1}$ and $(x-v_2)^{s_2}$. Then, we can write $f = (x-v_1)^{s_1}(x-v_2)^{s_2} g$, where $\deg(g) = n - (s_1 + s_2)$, and g must not introduce zeros at v_1 or v_2.

Again, we let G be the generating function of this semigroup, which is generated by all non-linear irreducible polynomials and the polynomials $x - v'$, where $v' \in \mathbb{F} \setminus \{v_1, v_2\}$. By comparing $G(z)$ with $\mathcal{M}(z) = \prod_{n=1}^{\infty} (1-z^n)^{-I_n}$, it becomes apparent that we turn the first factor $(1-z)^{-q}$ into $(1-z)^{-(q-2)}$ to exclude $x - v_1$ and $x - v_2$. Thus, $G(z) = (1-z)^2 \mathcal{M}(z)$. The sequence generated by $(1-z)^2 = 1z^0 + (-2)z^1 + 1z^2$ is $(1, -2, 1, 0, 0, \dots)$.

As in the proof of Theorem 3.1, we could do a case distinction to derive $G(n)$. However, since we expand the numbers of zeros to arbitrarily many later, it is unrewarding to expand $(1-z)^3$, $(1-z)^4$, and so forth to extract all coefficients. For this reason, we use a different but unified approach: Notice that $(1-z)^2$ can also be written using the binomial formula and series as $\sum_{n=0}^{2} \binom{2}{n} 1^{2-n} (-z)^n = \sum_{n=0}^{\infty} \binom{2}{n} (-1)^n z^n$. The sequence $\left(\binom{2}{n}(-1)^n\right)_{n=0}^{\infty}$ is precisely $(1, -2, 1, 0, 0, \dots)$.

We know $\mathcal{M}(z) = \sum_{n=0}^{\infty} q^n z^n$ and $(1-z)^2 = \sum_{n=0}^{\infty} \binom{2}{n} (-1)^n z^n$. The Cauchy product yields the generating function of G,

$$G(z) = \frac{(1-z)^2}{1-qz} = \sum_{n=0}^{\infty} \left(\sum_{i=0}^{n} \binom{2}{i} (-1)^i q^{n-i} \right) z^n.$$

If we instead use the case-distinction approach, we can simplify $G(z)$, or rather $G(n)$, further and obtain

$$G(z) = \sum_{n=0}^{\infty} \left(\begin{cases} q^n & \text{if } n = 0 \\ (q-2)q^{n-1} & \text{if } n = 1 \\ (q-1)^2 q^{n-2} & \text{else} \end{cases} \right) z^n.$$

Recall that the number of f with zeros at v_1 and v_2 of multiplicities s_1 and s_2, respectively, equals the number of different suitable g. Since $\deg(g) = n - (s_1 + s_2)$, we conclude that $Z_2(\underline{s}, n)$ equals

$$G(n - (s_1 + s_2)) = [z^{n-(s_1+s_2)}] G(z) = \begin{cases} (q-1)^2 q^{n-(s_1+s_2)-2} & \text{if } s_1 + s_2 \leq n-2 \\ q-2 & \text{if } s_1 + s_2 = n-1 \\ 1 & \text{if } s_1 + s_2 = n. \end{cases}$$

As can be seen, we simplified $(q-2)q^{n-(s_1+s_2)-1}$ to $q-2$ if $s_1 + s_2 = n-1$. ∎

Proceeding from the function $Z_2(\underline{s}, n)$, we can derive the probability that a polynomial has two zeros of certain multiplicities when we assume a uniform distribution over the polynomials in $\mathcal{M}_n$ (or $\mathcal{P}_n$). Again, we establish the probability using Laplace's rule.

Corollary 3.12. *For all $n, s_1, s_2 \in \mathbb{N}_0$ such that $s_1 + s_2 \leq n$ and for all $v_1 \neq v_2 \in \mathbb{F}$, denote by $\mathcal{Z}_2(n) := \mathcal{Z}_{2,\underline{v}}(n)$ the random variable of the multiplicities of the zeros v_1 and v_2 of a random (monic) polynomial of degree n. Then, the PMF of $\mathcal{Z}_{2,\underline{v}}(n)$ equals*

$$\Pr[\mathcal{Z}_{2,\underline{v}}(n) = \underline{s}] = \begin{cases} (q-1)^2 q^{-(s_1+s_2)-2} & \text{if } s_1 + s_2 \leq n-2 \\ (q-2)q^{-n} & \text{if } s_1 + s_2 = n-1 \\ q^{-n} & \text{if } s_1 + s_2 = n. \end{cases}$$

We omit the proofs of Corollary 3.12 and all subsequent PMFs since they are almost identical to the proof of Corollary 3.2: We divide the number of favorable polynomials $\mathcal{Z}_2(\underline{s}, n)$ by the number of all polynomials.

As in the first chapter, we analyze the expectation and variance next. However, the range of $\mathcal{Z}_2(\underline{s}, n)$ is a *pair*, more precisely, $\operatorname{range}(\mathcal{Z}_2(\underline{s}, n)) = [0, n]^2$. Before we try to adapt the definition of expectation to not only work with scalars but also with tuples, we observe that the distribution of $\mathcal{Z}_{2,\underline{v}}(n)$ can be considered the joint distribution of $\mathcal{Z}_{1,v_1}(n)$ and $\mathcal{Z}_{1,v_2}(n)$, i.e., $\Pr[\mathcal{Z}_{2,\underline{v}}(n) = \underline{s}] = \Pr[\mathcal{Z}_{1,v_1}(n) = s_1 \land \mathcal{Z}_{1,v_2}(n) = s_2]$. Thus, it is reasonable to treat $\mathcal{Z}_{2,\underline{v}}(n)$ as a *multivariate* random variable $\mathcal{Z}_{2,\underline{v}}(n) = (\mathcal{Z}_{1,v_1}(n), \mathcal{Z}_{1,v_2}(n))$. Theorems 3.5 and 3.6 then imply the mean and variance, respectively, because they are $\mathbb{E}[\mathcal{Z}_{2,\underline{v}}(n)] = (\mathbb{E}[\mathcal{Z}_1(n)], \mathbb{E}[\mathcal{Z}_1(n)])$ and $\operatorname{Var}[\mathcal{Z}_{2,\underline{v}}(n)] = (\operatorname{Var}[\mathcal{Z}_1(n)], \operatorname{Var}[\mathcal{Z}_1(n)])$.

We move on from considering two zeros and concentrate on $\ell \in [q]$ zeros at $v_1, \dots, v_\ell$ of multiplicities $s_1, \dots, s_\ell$, respectively, for the remainder of this section. During the proof of Theorem 3.11, we saw that the generating function of $(1-z)^2$ cannot only be established by expanding the square of the binomial. Instead, we expressed $(1-z)^2$ using the binomial series $\sum_{n=0}^{\infty} \binom{2}{n}(-1)^n z^n$. Since we now consider ℓ zeros, the binomial $1-z$ is raised to the ℓ^{th} power. The corresponding binomial series is easily deduced, namely, $(1-z)^\ell = \sum_{n=0}^{\infty} \binom{\ell}{n}(-1)^n z^n$. Thereby, we can directly establish the number of such polynomials while following the pattern of Theorems 3.1 and 3.11.

Theorem 3.13. *For all $n, s_1, \dots, s_\ell \in \mathbb{N}_0$, for all pairwise distinct $v_1, \dots, v_\ell \in \mathbb{F}$, and $k = \sum_{i=1}^{\ell} s_i$, the number of monic polynomials of degree n with zeros at $v_1, \dots, v_\ell$ of multiplicities $s_1, \dots, s_\ell$, respectively, equals $Z_\ell(\underline{s}, n) := Z_{\ell,\underline{v}}(\underline{s}, n) := q^{n-k} \sum_{i=0}^{n-k} \binom{\ell}{i}(-1)^i q^{-i}$. Moreover, if $k \leq n - \ell$, the function simplifies to $Z_\ell(\underline{s}, n) = q^{n-k}(1-q^{-1})^\ell$.*

Proof. We follow the approach of the previous Theorems 3.1 and 3.11, which you should be familiar with. In particular, we construct $f \in \mathcal{M}_n$ as $f = g \prod_{i=1}^{\ell} (x - v_i)^{s_i}$. The degree of g is $n - (s_1 + \cdots + s_\ell) \triangleq n - k$.

In order to determine the number of feasible g, we let G be the multiplicative semigroup generated by all non-linear irreducible polynomials and the $q - \ell$ linear ones $x - v'$, where $v' \in \mathbb{F} \setminus \{v_1, \dots, v_\ell\}$. We recall that in this way, we ensure that g does not alter the ℓ predefined multiplicities.

It should now be obvious that the generating function of G is $G(z) = (1-z)^\ell \mathcal{M}(z)$. Since $(1-z)^\ell$ can be expressed as $(1-z)^\ell = \sum_{n=0}^{\infty} \binom{\ell}{n}(-1)^n z^n$, the Cauchy product yields

$$G(z) = \frac{(1-z)^\ell}{1-qz} = \sum_{n=0}^{\infty} \left(\sum_{i=0}^{n} \binom{\ell}{i} (-1)^i q^{n-i} \right) z^n = \sum_{n=0}^{\infty} \left(q^n \sum_{i=0}^{n} \binom{\ell}{i} (-1)^i q^{-i} \right) z^n,$$

from which we can directly read the term $G(n)$.

We conclude that the number of different g and, hence, the number of feasible f equals $G(n-k) = [z^{n-k}]G(z) = q^{n-k} \sum_{i=0}^{n-k} \binom{\ell}{i}(-1)^i q^{-i}$.

It remains to show that if $n - k \geq \ell$, the sum in $G(n-k)$ simplifies to $(1-q^{-1})^\ell$. Here, we observe that if $i > \ell$, the binomial coefficient $\binom{\ell}{i}$ is 0. Hence, the argument of the sum is. Thus, the sum remains unchanged, regardless of whether the upper limit satisfies $n - k > \ell$ or $n - k = \ell$, so we only consider $n - k = \ell$. In that case, the binomial formula is *complete*, and the binomial theorem yields $\sum_{i=0}^{n-k} \binom{\ell}{i}(-1)^i q^{-i} = (1-q^{-1})^\ell$. ■

Unfortunately, there is no simple closed form of the sum if $n-k < \ell$. Simplifications produced by Mathematica [Wol] involve the *Gaussian hypergeometric function* ${}_2F_1$. This function is also defined via a non-trivial sum, including factorials and the *Pochhammer symbol* [Bag09]. A further investigation regarding possible simplifications is beyond the scope of this thesis.

We proceed with giving the PMF regarding the multiplicities $\underline{s}$ of a polynomial chosen uniformly at random. Let $\mathcal{Z}_\ell(n) := \mathcal{Z}_{\ell,\underline{v}}(n)$ denote the random variable of the multiplicities of the zeros $v_1, \dots, v_\ell$ of a random (monic) polynomial of degree n.

Corollary 3.14. *For all $n, s_1, \dots, s_\ell \in \mathbb{N}_0$, for all pairwise distinct $v_1, \dots, v_\ell \in \mathbb{F}$, and $k = \sum_{i=1}^{\ell} s_i$, the PMF of $\mathcal{Z}_{\ell,\underline{v}}(n)$ equals $\Pr[\mathcal{Z}_{\ell,\underline{v}}(n) = \underline{s}] = q^{-k} \sum_{i=0}^{n-k} \binom{\ell}{i}(-1)^i q^{-i}$. Moreover, if $k \leq n - \ell$, the PMF simplifies to $\Pr[\mathcal{Z}_{\ell,\underline{v}}(n) = \underline{s}] = q^{-k}(1-q^{-1})^\ell$.*

So far, this and the previous chapter neglected the multiplicities at the remaining unspecified positions. To conclude this section, we consider a tightened variant of Theorem 3.13, where we additionally require that zeros may *only* occur at the specified positions $v_1, \dots, v_\ell$ in $\underline{v}$. Since the tuples $\underline{v}$ and $\underline{s}$ are ordered, we can use Theorem 3.13 to derive the number of polynomials satisfying this tightened condition: To ensure that the other positions are not zeros, we can include them in $\underline{v}$, e.g., by appending them, and specify their multiplicity in $\underline{s}$ as 0. Thus, the sum of all multiplicities k remains unchanged because we only add 0s, and the desired number is $Z_{q,\underline{v}}(\underline{s}, n)$ (instead of $Z_{\ell,\underline{v}}(\underline{s}, n)$). Note that we claim that the aforementioned function uses the unmodified tuples $\underline{v}$ and $\underline{s}$, which do not include any of the remaining $q - \ell$ values.

Theorem 3.15. *For all $n, s_1, \dots, s_\ell \in \mathbb{N}_0$, for all pairwise distinct $v_1, \dots, v_\ell \in \mathbb{F}$, and $k = \sum_{i=1}^{\ell} s_i$, the number of monic polynomials of degree n with zeros at, and only at, $v_1, \dots, v_\ell$ of multiplicities $s_1, \dots, s_\ell$, respectively, equals $Z_q(\underline{s}, n) = Z_{q,\underline{v}}(\underline{s}, n) = q^{n-k} \sum_{i=0}^{n-k} \binom{q}{i}(-1)^i q^{-i}$. Furthermore, if $k \leq n - q$, the function simplifies to $Z_q(\underline{s}, n) = q^{n-k}(1-q^{-1})^q$.*

Proof. Using the usual technique, we could construct f as $f = g \prod_{i=1}^{\ell} (x - v_i)^{s_i}$ and then consider the number of different g of degree $n - k$ *without* zeros, similar to the proof of Theorem 3.13.

However, we employ a different approach that enables us to derive the number using a function that we already established: To ensure that all other positions $v_{\ell+1}, \dots, v_q \notin \underline{v}$ are not zeros of f, we set their multiplicities $s_{\ell+1}, \dots, s_q$ to 0. We can then append the new positions to $\underline{v}$ and multiplicities to $\underline{s}$, that is, we have $\underline{v}' := (v_1, \dots, v_\ell, v_{\ell+1}, \dots, v_q)$ and $\underline{s}' := (s_1, \dots, s_\ell, 0, \dots, 0)$. Since we covered all possible positions and introduced no new zeros, $k' := \sum_{i=1}^{q} s_i$ equals k. Since $|\underline{v}| = q$ and $k' = k$, Theorem 3.13 implies that the number of different f equals $Z_q(\underline{s}', n) = Z_q(\underline{s}, n)$. ■

We make one final remark regarding the number of *zero-free* polynomials because we can use the previous theorems to directly deduce this number. We call a polynomial f *zero-free* if it has no zeros, i.e., if $\forall v \in \mathbb{F}. f(v) \neq 0$. To find that number, we specify the multiplicities at all positions and set them to 0, i.e., $\underline{s} = 0^q$ for any $\underline{v} \in \mathbb{F}^q$. Thus, we ensure that no linear polynomial $x - v$, where $v \in \mathbb{F}$, occurs in the decomposition of the polynomial since $(x - v)^0 = 1$ (and by defining $0^0 = 1$). Theorems 3.13 and 3.15 give the number of polynomials without zeros. We can use either because we specify all $\ell = q$ possible positions.

Corollary 3.16. *For all $n \in \mathbb{N}_0$, the number of* zero-free *monic polynomials of degree n equals $q^n \sum_{i=0}^{n} \binom{q}{i} (-1)^i q^{-i}$. For $n \geq q$, the function simplifies to $q^n (1 - q^{-1})^q$.*

Proof. We use Theorem 3.15 to show that the actual number is as claimed above. We specify all possible positions using $\underline{v} = (i)_{i \in \mathbb{F}_q}$ and set $\underline{s} = 0^q$. Thus, the sum of all multiplicities equals $k = 0$. In fact, we can use any $\underline{v} \in \mathbb{F}^q$ since the multiplicity at every position specified is the same (namely, 0), and, therefore, there is only one way to permute $\underline{s}$.

Using the values, Theorem 3.15 states that $Z_q(\underline{s}, n) = Z_q(0^q, n)$ equals the number of different polynomials with zeros at, and only at, all possible positions in $\mathbb{F}$ of multiplicity 0. Clearly, this is equivalent to the number of polynomials without zeros.

Finally, we remark that the "only at" part can be omitted because we consider all positions. Thus, Theorem 3.13 also yields the number in question, $Z_\ell(\underline{s}, n) = Z_q(0^q, n)$, because $\ell \triangleq |\underline{v}| = q$. ■

3.3 The Total Multiplicity of Arbitrary Zeros

Up to now, we have considered zeros at specific positions $v_1, \dots, v_\ell$ of *specific* multiplicities $s_1, \dots, s_\ell$, respectively. Since $k = \sum_{i=1}^{\ell} s_i$ represents the total number of zeros at these ℓ positions but with fixed multiplicities, accounting for permutations and replacements of elements in $\underline{s}$ yields the number of monic polynomials for which there exist ℓ possible zeros $v_1, \dots, v_\ell$ of *accumulated* multiplicity k. We recall that v_i is not a zero if its multiplicity is $s_i = 0$, i.e., the factor $x - v_i$ does not occur in the decomposition of the polynomial. The ℓ-tuple $\underline{s} = (s_1, s_2, \dots, s_\ell)$ can be composed arbitrarily as long as its sum equals k. Since each s_i is a non-negative integer, the number of feasible s, therefore, equals the number of ways to represent $k \leq n$ as the sum of ℓ non-negative integers. It is well known that this number is:

Fact 3.17. Let $k \in \mathbb{N}_0$. The number of ℓ-tuples $(s_1, \dots, s_\ell)$ with $s_i \in \mathbb{N}_0$ for all $i \in [\ell]$ satisfying $\sum_{i=1}^{\ell} s_i = k$ equals $\binom{\ell+k-1}{k} = \binom{\ell+k-1}{\ell-1}$.

In Theorem 3.13 of the previous section, we established the number of polynomials with zeros at $\underline{v}$ and exact multiplicities $\underline{s}$. Notice that the function $Z_\ell(\underline{s}, n)$ uses $\underline{s}$ only to derive the value k. Thus, $Z_\ell(\underline{s}, n) = Z_\ell(\underline{s}', n)$ for all $\underline{s}'$ such that $\sum_{s \in \underline{s}'} s = k$. This means that, if S denotes the set of all such $\underline{s}'$, the number of polynomials with zeros in $\underline{v}$ whose multiplicities sum up to k satisfies $\sum_{\underline{s}' \in S} Z_\ell(\underline{s}', n) = |S| \cdot Z_\ell(\underline{s}, n)$. Since the cardinality of S is given by Fact 3.17, we obtain the number of favorable polynomials by combining this fact with Theorem 3.13.

Theorem 3.18. *Let $\underline{s}^{(k)}$ be any $\underline{s}$ with $\sum_{s \in \underline{s}} s = k$. For all $n, k \in \mathbb{N}_0$ and for all pairwise distinct $v_1, \dots, v_\ell \in \mathbb{F}$, the number of monic polynomials of degree n with ℓ possible zeros at $v_1, \dots, v_\ell$ of total multiplicity k equals $\binom{\ell+k-1}{k} Z_\ell(\underline{s}^{(k)}, n) = \binom{\ell+k-1}{k} q^{n-k} \sum_{i=0}^{n-k} \binom{\ell}{i} (-1)^i q^{-i}$. Moreover, if $k \leq n-\ell$, the function simplifies to $\binom{\ell+k-1}{k} q^{n-k} (1-q^{-1})^\ell$.*

Proof. The theorem follows immediately from combining Theorem 3.13 and Fact 3.17. ■

Knopfmacher and Knopfmacher [KK90] examine a special case of the above Theorem 3.18. As there are only $|\mathbb{F}| = q$ positions for zeros to occur, specifying the multiplicities at all q positions implies that the polynomial has not only k zeros at $v_1, \dots, v_q$ but k zeros *in total*. Since Theorem 3.18 takes permutations of $\underline{s}$ into account, we obtain the number of monic polynomials with *exactly* k zeros if $\ell = q$.

Theorem 3.19 ([KK90]). *For all $n, k \in \mathbb{N}_0$, the number of monic polynomials of degree n with exactly k total zeros equals $Z(k, n) := \binom{q+k-1}{k} Z_q(\underline{s}^{(k)}, n) = \binom{q+k-1}{k} q^{n-k} \sum_{i=0}^{n-k} \binom{q}{i} (-1)^i q^{-i}$. Moreover, if $k \leq n-q$, the function simplifies to $Z(k, n) = \binom{q+k-1}{k} q^{n-k} (1-q^{-1})^q$.*

Proof. The theorem follows immediately from Theorem 3.18 because, with $\ell = q$, there are no remaining positions for further zeros to occur in that case. ■

We remark that Knopfmacher and Knopfmacher prove Theorem 3.19 using generating functions. It is not a coincidence that we utilize generating functions to prove several theorems that concern counting polynomials in this chapter. As previously mentioned, e.g., at the beginning of Section 3.1 or in the context of Theorem 3.1, we adapted their proof strategy.

For the remainder of this section, we concentrate on the random variable $\mathcal{Z}(n)$ of the number k of *total* zeros of a (monic) polynomial of degree n chosen uniformly at random. According to Theorem 3.8, $\mathcal{Z}_1(n)$ has a geometric limit. Although this is not the case for $\mathcal{Z}(n)$, it convergences to another common probability distribution: the negative binomial distribution. This observation and the expectation and variance of $\mathcal{Z}(n)$ are examined in [KK90]. Unlike $\mathcal{Z}_\ell(n)$ in the previous chapter, $\mathcal{Z}(n)$ is not a multivariate random variable because its range does not comprise multiplicities at several positions but all feasible integers k, i.e., $\operatorname{range}(\mathcal{Z}(n)) = [0, n]$. Thus, the expectation and variance are scalars.

Corollary 3.20. *For all $n, k \in \mathbb{N}_0$, the PMF of the random variable $\mathcal{Z}(n)$, defined above, equals $\Pr[\mathcal{Z}(n) = k] = \binom{q+k-1}{k} q^{-k} \sum_{i=0}^{n-k} \binom{q}{i} (-1)^i q^{-i}$. Moreover, if $k \leq n-q$, the PMF simplifies to $\Pr[\mathcal{Z}(n) = k] = \binom{q+k-1}{k} q^{-k} (1-q^{-1})^q$.*

In Theorem 3.19 and Corollary 3.20, the sum inside the PMF simplifies to $(1-q^{-1})^q$ if $k \leq n-q$. Note that $q^{-k} = (q^{-1})^k$. Thus, the expression $\binom{q+k-1}{k} q^{-k}(1-q^{-1})^q$ equals the PMF of the negative binomial distribution $\mathrm{NBin}(q, 1-q^{-1})$ evaluated at k, according to Definition 1.21. We further conclude that $Z(n)$ follows a *truncated* negative binomial distribution, which was already observed in [KK90].

Observation 3.21 *([KK90]).* The random variable $Z(n)$ follows a negative binomial distribution truncated at $k = n-q+1$. More precisely, $\Pr[Z(n) = k] = \Pr[X = k]$ if $k \leq n-q$, where $X \sim \mathrm{NBin}(q, 1-q^{-1})$.

Since we consider q fixed, the difference $n-q$ approaches infinity when n does. As a result, the truncation point $n-q+1$ "moves" towards infinity, and the PMFs of $Z(n)$ and $X \sim \mathrm{NBin}(q, 1-q^{-1})$ coincide. Thus, $Z(n)$ has a negative binomial limit. This makes it easy to deduce statistical properties, such as expectation and variance, in the asymptotic case because they have already been analyzed in the context of the negative binomial distribution.

Let Z denote the limit distribution of $Z(n)$ as $n \to \infty$.

Theorem 3.22. *The sequence $(Z(n))_{n \in \mathbb{N}_0}$ converges in distribution to $Z \sim \mathrm{NBin}(q, 1-q^{-1})$.*

Proof. Let $F_n(k)$ and $F(k)$ denote the CDF of $Z(n)$ and Z, respectively, and assume that $Z \sim \mathrm{NBin}(q, 1-q^{-1})$. We need to show that $\lim_{n\to\infty} F_n(k) = F(k)$ holds for all $k \geq 0$.

According to Observation 3.21, the PMFs of $Z(n)$ and Z coincide if $k \leq n-q$. It is apparent that $k \leq n-q$ holds for all k if $n \to \infty$ because q is considered constant. Hence, $\lim_{n\to\infty} \Pr[Z(n) = k] = \Pr[Z = k]$.

We conclude that the CDFs coincide because they comprise the same PMF, that is, $\lim_{n\to\infty} F_n(k) \triangleq \lim_{n\to\infty} \sum_{i=0}^{k} \Pr[Z(n) = i] = \sum_{i=0}^{k} \Pr[Z = i] \triangleq F(k)$. ∎

In addition to the number of polynomials with k zeros in total, Knopfmacher and Knopfmacher also examine the expectation and variance of $Z(n)$. Although the authors give proof of the former, we restate the proof for two reasons: For one thing, their proof of the variance is based on it. Since we elaborate on the variance in greater detail, it is helpful to be familiar with the basis of that proof. For another thing, the original proof in [KK90] is terse, which can make it challenging to comprehend.

We first state the average number of *total* zeros of a polynomial of degree n. Since Z follows a negative binomial distribution, the asymptotic expectation of $Z(n)$ is immediately determined. Furthermore, when q also tends to infinity, the expectation converges to 1. In other words, for large q, we expect polynomials of large degree to have one zero.

Theorem 3.23 ([KK90]). *For all $n \in \mathbb{N}_0$, the expected value of the random variable $Z(n)$ equals $\mathbb{E}[Z(n)] = (q-q^{1-n})/(q-1)$. Moreover, the asymptotic expectation equals $\mathbb{E}[Z] = q/(q-1)$ as $n \to \infty$.*

Proof ([KK90]). Using $Z(k,n)$ from Theorem 3.19 to derive the expectation is tedious because the sum in $Z(k,n)$ is alternating and has no elementary closed form.

Instead, we count the zeros of a polynomial according to their multiplicities. For instance, if the multiplicity of a zero is 3, then the multiplicity is at least 1, at least 2, and at least 3. By counting every "at least" individually but only once, they still add up to the

actual multiplicity $3 \cdot 1 = 3$. The "at least" view allows us to use Lemma 3.4 to count the number of polynomials with a zero at $v \in \mathbb{F}$ of a certain multiplicity. Moreover, as we deal with nested sums, we simplify expressions using associativity and commutativity to switch their order.

Let $f \in \mathcal{M}_n$, let $\zeta(f)$ denote the *total* number of zeros of f, and let $\zeta_i(f)$ be the number of *distinct* zeros of multiplicity at least i. In other words, $\zeta_i(f) = |\{ v \in \mathbb{F} : (x-v)^i \mid f \}|$. By counting the zeros of f according to their multiplicities (as explained above), we notice that ζ can be expressed by ζ_i as $\zeta(f) = \sum_{i=1}^{n} \zeta_i(f)$. Thus, and since every f is chosen with probability q^{-n}, we can expand the expectation as follows:

$$\mathbb{E}[\mathcal{Z}(n)] \triangleq \sum_{f \in \mathcal{M}_n} q^{-n} \zeta(f) = q^{-n} \sum_{f} \zeta(f) = q^{-n} \sum_{f} \sum_{i=1}^{n} \zeta_i(f) = q^{-n} \sum_{i=1}^{n} \sum_{f} \zeta_i(f).$$

Next, we evaluate the sum $\sum_f \zeta_i(f)$. As explained above, $\zeta_i(f)$ is the number of $v \in \mathbb{F}$ such that $(x-v)^i \mid f$. This allows us to write $\zeta_i(f) = \sum_v [\![(x-v)^i \mid f]\!]$. Thus, we can further expand $\sum_f \zeta_i(f)$ to $\sum_f \zeta_i(f) = \sum_f \sum_v [\![(x-v)^i \mid f]\!] = \sum_v \sum_f [\![(x-v)^i \mid f]\!]$.

Hence, we aim to evaluate the inner sum $\sum_f [\![(x-v)^i \mid f]\!]$. Observe that its value is equal to the number of polynomials in $\mathcal{M}_n$ with a zero at v of multiplicity *at least* i. According to Lemma 3.4, this number is precisely q^{n-i}. Hence, $\sum_v \sum_f [\![(x-v)^i \mid f]\!] = \sum_v q^{n-i}$. Furthermore, since v is arbitrary, the sum $\sum_v q^{n-i}$ simplifies to $|\mathbb{F}| \cdot q^{n-i} = q^{n-i+1}$.

We conclude that $\sum_f \zeta_i(f) = \sum_v \sum_f [\![(x-v)^i \mid f]\!] = \sum_v q^{n-i} = q^{n-i+1}$, and the expectation follows immediately:

$$\mathbb{E}[\mathcal{Z}(n)] = q^{-n} \sum_{i=1}^{n} \sum_{f} \zeta_i(f) = q^{-n} \sum_{i=1}^{n} q^{n-i+1} = \frac{q - q^{1-n}}{q-1}.$$

It remains to show that the asymptotic expectation is $q/(q-1)$. Theorem 3.22 states that $\mathcal{Z}(n) \overset{\mathrm{d}}{=} \mathcal{Z} \sim \mathrm{NBin}(q, 1-q^{-1})$ as $n \to \infty$. Thus, the expectation of $\lim_{n\to\infty} \mathbb{E}[\mathcal{Z}(n)]$ and $\mathbb{E}[\mathcal{Z}]$ coincides, where $\mathbb{E}[\mathcal{Z}] = q/(q-1)$, according to Fact 1.23. ■

As mentioned previously, if q approaches infinity in addition to n, the expectation tends to $\lim_{q\to\infty} \mathbb{E}[\mathcal{Z}] = 1$. However, even for small q and n, the average number of zeros of a polynomial is small: We observe that $\mathbb{E}[\mathcal{Z}(n)]$ is monotonically increasing in n. Thus, is it sufficient to consider the asymptotic mean and compute $\max_q(\mathbb{E}[\mathcal{Z}])$ to find $\max_{n,q}(\mathbb{E}[\mathcal{Z}(n)])$. Since $\max_q(\mathbb{E}[\mathcal{Z}]) \triangleq \max_q(q/(q-1)) = 2$, we conclude that the average number of zeros is always at most 2. Although this upper bound is asymptotically tight, there are no n and q such that $\mathbb{E}[\mathcal{Z}(n)] = 2$.

Finally, we provide the variance of the number of *total* zeros. As n and q tend to infinity, the variance again converges to 1. Besides, the asymptotic case is once again implied by $\mathcal{Z} \sim \mathrm{NBin}(q, 1-q^{-1})$. Thus, we focus on $\mathcal{Z}(n)$. We remark that Knopfmacher and Knopfmacher [KK90] state the variance, but it is incorrect. This is due to a mistake in splitting a sum inside their proof. Below, we state the correct variance and further details in the proof, whose structure we adopt from [KK90].

Theorem 3.24 ([KK90]). *For all $n \in \mathbb{N}_0$, the variance of $\mathcal{Z}(n)$ is* $\mathrm{Var}[\mathcal{Z}(n)] = \frac{q(q-q^{1-2n}-(q^2-1)nq^{-n})}{(q-1)^2}$. *Moreover, the asymptotic variance equals* $\mathrm{Var}[\mathcal{Z}] = (q/(q-1))^2$ *as* $n \to \infty$.

Proof ([KK90]). The reader should be roughly familiar with the proof of Theorem 3.23 and the proof on pages 4–5 of [KK90]. Nevertheless, we also outline the latter proof. We recall that the functions N^* and N_i in [KK90] correspond to ζ and ζ_i, respectively. Furthermore, we format equations from [KK90] in parentheses and a sans-serif letterform and underline the number, e.g., (3.5).

Let $f \in \mathcal{M}_n$. The variance satisfies $\mathrm{Var}[Z(n)] = \mathbb{E}[Z(n)^2] - \mathbb{E}[Z(n)]^2$. Hence, it suffices to compute $\mathbb{E}[Z(n)^2] = q^{-n} \sum_f \zeta(f)^2$. We recall that $\zeta(f) = \sum_{i=1}^n \zeta_i(f)$, which implies that $\sum_f \zeta(f)^2 = \sum_f (\sum_{i=1}^n \zeta_i(f))^2$. The authors expand the inner sum to

$$\left(\sum_{i=1}^{n} \zeta_i(f)\right)^2 = \sum_{i=1}^{n} \zeta_i(f)^2 + 2 \sum_{i=1}^{n} \sum_{j=i+1}^{n} \zeta_i(f)\zeta_j(f). \tag{3.2}$$

To determine $\sum_{i=1}^n \sum_{j=i+1}^n \zeta_i(f)\zeta_j(f)$, the authors distinguish two cases, $i+j \leq n$ and $i+j > n$. This way, they establish two separate formulae, in (3.3) and (3.4), respectively. In equation (3.6), they split the sum[5] $\sum_{j=i+1}^n$ into two parts, $\sum_{j=i+1}^{n-i}$ and $\sum_{j=n-i+1}^n$, to plug in these deduced formulae. However, it is possible for the latter sum to "start" before the former. This happens if $n-i+1 < i+1$ (i.e., if $i > n/2$). In that case, the former sum is empty. But more importantly, besides the indices $i+1, i+2, \dots, n$, the sum(s) additionally consider $i, i-1, \dots, n-i+1$.

Fortunately, there is a simple remedy for this problem: We adjust the bounds of the sums to $\sum_{j=i+1}^{\max\{n-i,i\}}$ and $\sum_{j=\max\{n-i,i\}+1}^{n}$. Using Mathematica [Wol], we obtain the following results[6]: The correct equation (3.6) is

$$\begin{aligned} q^{-n} \sum_f \sum_{j=i+1}^{n} \zeta_i(f)\zeta_j(f) &= \frac{(1-q)q^{-\max\{i,n-i\}-i+1} + q^{1-i} + q^{2-2i} - q^{1-2i} - q^{1-n}}{q-1} \\ &= \begin{cases} \dfrac{q(q^{-i} - q^{-n})}{q-1} & \text{if } 2i \geq n \\ \dfrac{q(-q^{-2i} + q^{-i} + q^{1-2i} - q^{1-n})}{q-1} & \text{else.} \end{cases} \end{aligned}$$

We infer the correct variance by plugging the correct equation (3.6) in the residual parts of the proof in [KK90]. Summing over all i yields equation (3.7):

$$\begin{aligned} q^{-n} \sum_f \sum_{i=1}^{n} \sum_{j=i+1}^{n} \zeta_i(f)\zeta_j(f) &= \frac{(1-q)q^{3-2\lceil n/2 \rceil} + nq^{1-n} - 2q^{2-n} + 2q^2}{(q-1)^2(q+1)} \\ &\quad + \frac{q^{4-n} - (1+n)q^{3-n}}{(q-1)^2(q+1)} - \left\lceil \frac{n}{2} \right\rceil q^{1-n}. \end{aligned} \tag{3.3}$$

Recall that the inner sum in the second raw moment $\mathbb{E}[Z(n)^2] = q^{-n} \sum_f (\sum_{i=1}^n \zeta_i(f))^2$ is split according to Equation 3.2. There, the single sum is established in (3.5), and we

[5] For the sake of clarity, we omit the arguments of the sums.
[6] We attached the Mathematica notebook with the performed computations to the CD.

computed the double sum in Equation 3.3. Hence, combining both results yields the correct second raw moment

$$\begin{aligned}\mathbb{E}[\mathcal{Z}(n)^2] &= q^{-n}\sum_{f}\sum_{i=1}^{n}\zeta_i(f)^2 + 2q^{-n}\sum_{f}\sum_{i=1}^{n}\sum_{j=i+1}^{n}\zeta_i(f)\zeta_j(f)\\ &= \frac{q^{1-n}\left(1-2n(q-1)+q(2(q+q^n)-5)\right)}{(q-1)^2}\\ &\quad + \frac{q\left((1-q)q^{-2\lfloor n/2\rfloor} - 2q^{2-2\lceil n/2\rceil} - 2q^{-n}(q^2-1)\lceil n/2\rceil\right)}{(q+1)(q-1)}.\end{aligned}$$

We finally obtain the variance

$$\begin{aligned}\operatorname{Var}[\mathcal{Z}(n)] &= \frac{q^2-q^{2-2n}}{(q-1)^2} - \frac{(q^2-1)(2n-2q+1)q^{1-n}}{(q-1)^2(q+1)}\\ &\quad - \frac{q\left(2q^{2-2\lceil n/2\rceil}+(q-1)q^{-2\lfloor n/2\rfloor}\right)}{(q-1)(q+1)} - 2q^{1-n}\left\lceil\frac{n}{2}\right\rceil\end{aligned}$$

by combining the second raw moment and the squared expectation from Theorem 3.23.

To eliminate the floor and ceiling functions, we distinguish whether n is even or odd. Let $m \in \mathbb{Z}$ such that either $n = 2m$ or $n = 2m+1$. The variance simplifies to

$$\begin{aligned}\operatorname{Var}[\mathcal{Z}(n)] &= \begin{cases}\dfrac{q(q-q^{1-4m}-2mq^{2-2m}+2mq^{-2m})}{(q-1)^2} & \text{if } n = 2m\\[2ex] \dfrac{q^{-4m}\left((1+2m)q^{2m}-1-(1+2m)q^{2+2m}+q^{2+4m}\right)}{(q-1)^2} & \text{if } n = 2m+1\end{cases}\\ &\overset{(\dagger)}{=} \frac{q\left(q-q^{1-2n}-(q^2-1)nq^{-n}\right)}{(q-1)^2}.\end{aligned}$$

It can be seen that $(\dagger)$ holds by substituting n with $2m$ and $2m+1$ each.

Finally, the asymptotic variance $\lim_{n\to\infty}\operatorname{Var}[\mathcal{Z}(n)] = \operatorname{Var}[\mathcal{Z}]$ agrees with [KK90]. Fact 1.23 and Theorem 3.22 imply that $\operatorname{Var}[\mathcal{Z}] = (q/(q-1))^2$. ■

Notice that $\operatorname{Var}[\mathcal{Z}] = \mathbb{E}[\mathcal{Z}]^2$. It follows that if q and n approach infinity, the variance also tends to $\mathbb{E}[\mathcal{Z}]^2 = 1^2 = 1$. Regarding an upper bound on the variance for all q and n, it can be shown that $\operatorname{Var}[\mathcal{Z}(n)]$ is monotonically increasing in n. Thus, the asymptotic variance implies that $\operatorname{Var}[\mathcal{Z}(n)] \leq \max_q(\mathbb{E}[\mathcal{Z}]^2) = 2^2 = 4$ is an asymptotically tight upper bound for all q and n.

3.4 The Positions of Zeros

In this final section, we analyze the number of (monic) polynomials in terms of their *distinct* zeros. Thus, we neglect multiplicities and only count the number of positions with zeros. For instance, the polynomial $x^5(x-1)^3$ has *two* distinct zeros, viz., $x = 0$ and $x = 1$. Recall that some position v is a zero of a polynomial f if the term $x - v$ occurs in the decomposition of f. This, on the other hand, is the case if the multiplicity of v is *at*

least 1. Thus, we can use the results from Section 3.3 to derive formulae that only count positions.

The structure of this section is (more or less) identical to Section 3.3: We start by counting distinct zeros in different ways. Then, we analyze the random variable of the number of distinct zeros, where we consider its asymptotic behavior, expectation, and variance. We remark that these quantities are also stated in [KK90].

Lemma 3.4 provides the number of polynomials with zeros at $\underline{v}$ with multiplicities of *at least* $\underline{s}$. Using $\underline{s} = 1^\ell$, we count polynomials with zeros at $\underline{v}$ and obtain the equivalent of Theorem 3.13:

Theorem 3.25. *For all $n, \ell \in \mathbb{N}_0$ such that $\ell \leq n$ and for all pairwise distinct $v_1, \dots, v_\ell \in \mathbb{F}$, the number of monic polynomials of degree n with zeros at $v_1, \dots, v_\ell$ equals $q^{n-\ell}$.*

Proof. The theorem follows immediately from Lemma 3.4 with $\underline{s} = 1^\ell$. ■

At the end of Section 3.2, we imposed the restriction that zeros may occur *only* at the ℓ positions $v_1, \dots, v_\ell$. The number of such polynomials can be found in Theorem 3.15. To prove that theorem, we suggested counting the number of different polynomials g of degree $n - k$ that are zero-free. This ensures that the remaining positions are not zeros and that the multiplicities of the zeros at $\underline{v}$ do not increase. Since we neglect multiplicities in this chapter, we must only ensure the former, i.e., that no zeros are introduced at positions that are not in $\underline{v}$. Thus, g can have zeros but only at positions in $\underline{v}$.

Theorem 3.26. *For all $n, \ell \in \mathbb{N}_0$ and for all pairwise distinct positions $v_1, \dots, v_\ell \in \mathbb{F}$, the number of all monic polynomials of degree n with zeros at,* and only at, *the ℓ positions $v_1, \dots, v_\ell$ equals $Z^*_\ell(n) := Z^*_{\ell,\underline{v}}(n) := q^{n-\ell} \sum_{i=0}^{n-\ell} \binom{q-\ell}{i} (-1)^i q^{-i}$. Moreover, if $n \geq q$, the function simplifies to $Z^*_\ell(n) = q^{n-\ell}(1 - q^{-1})^{q-\ell}$.*

Proof. Let $v_1, \dots, v_\ell$ be arbitrary but fixed, and let $f \in \mathcal{M}_n$ have zeros at, and only at, the ℓ specified positions. We use generating functions and proceed similarly to previous proofs, such as Theorem 3.13.

To ensure that f has zeros in $\underline{v}$, we construct $f = g \prod_{i=1}^{\ell} (x - v_i)$, where $\deg(g) = n - \ell$. To ensure that f does not have zeros at the remaining $q - \ell$ positions, g must have zeros that are only in $\underline{v}$.

Let G denote the multiplicative semigroup generated by all non-linear irreducible polynomials and the ℓ linear ones $x - v'$, where $v' \in \underline{v}$. As before, we modify $(1-z)^{-q}$ from $\mathcal{M}(z)$ to disregard all positions not in $\underline{v}$. Since there are q positions in total, we obtain

$$G(z) = (1 - z)^{q-\ell} \mathcal{M}(z) = \sum_{n=0}^{\infty} \left(\sum_{i=0}^{n} \binom{q - \ell}{i} (-1)^i q^{n-i} \right) z^n.$$

We conclude that the number of different g and, hence, the number of feasible f equals $G(n - \ell) = [z^{n-\ell}]G(z) = q^{n-\ell} \sum_{i=0}^{n-\ell} \binom{q-\ell}{i} (-1)^i q^{-i}$.

If $n - \ell \geq q - \ell$, that is, if $n \geq q$, the binomial formula is complete, and the sum simplifies to $\sum_{i=0}^{n-\ell} \binom{q-\ell}{i} (-1)^i q^{-i} = (1 - q^{-1})^{q-\ell}$. ■

At the beginning of Section 3.3, we relaxed Theorem 3.13 by neglecting the actual multiplicities of the zeros at $v_1, \dots, v_\ell$. For the remainder of that section, we only required that

the sum of all multiplicities at $\underline{v}$ equals some predetermined value k. By specifying all q positions in $\underline{v}$, we covered all multiplicities. Thus, we obtained Theorem 3.19, which states the number of polynomials with k zeros *in total*. Since we disregard multiplicities in this section, we do not need to exhaust all q multiplicities to obtain the number of polynomials with a total of ℓ *distinct* zeros. We solely need to count how many ways exist to select $\ell \leq q$ positions. Selecting positions is simpler than selecting multiplicities because the former are pairwise distinct.

Fact 3.27. Let $\ell, q \in \mathbb{N}_0$. The number of ways to choose ℓ distinct elements from a set with q elements disregarding their order equals $\binom{q}{\ell}$.

Since we count polynomials with a certain *total* number of distinct zeros, we henceforth use variable k instead of ℓ to be consistent with the previous Section 3.3, such as in Theorem 3.19.

By combining Theorem 3.26 and Fact 3.27, we obtain the "distinct" variant of Theorem 3.19. This theorem appears in [KK90] and is therein proven using generating functions, similar to Theorem 3.19.

Theorem 3.28 ([KK90]). *For all $n, k \in \mathbb{N}_0$ such that $k \leq n$, the number of monic polynomials of degree n with exactly k* distinct *zeros is $Z^*(k,n) := \binom{q}{k} Z_k^*(n) = \binom{q}{k} q^{n-k} \sum_{i=0}^{n-k} \binom{q-k}{i} (-1)^i q^{-i}$. Moreover, if $n \geq q$, the function simplifies to $Z^*(k,n) = \binom{q}{k} q^{n-k} (1-q^{-1})^{q-k}$.*

Proof. The theorem directly follows from combining Theorem 3.26 and Fact 3.27. ■

We mention that in Theorem 3.28, $Z^*(k,n)$ can be defined through $Z_k^*(n)$, although no positions in $\underline{v}$ are specified. This is because Z_k^* only uses them to derive the quantity $|\underline{v}| = \ell$, which we explicitly state in Z^*, namely, in the first argument.

The remainder of this section is dedicated to the random variable $\mathcal{Z}^*(n)$ concerning the number of *distinct* zeros. As in the previous section, we analyze its asymptotic behavior. We determine that $\mathcal{Z}^*(n)$ has a binomial limit. Besides, both its mean and variance are independent of n, with the expectation equaling 1 regardless of n (unless $n = 0$).

Firstly, we consider the probability of obtaining a polynomial with a certain number of distinct zeros:

Corollary 3.29. *For all $n, k \in \mathbb{N}_0$ such that $k \leq n$, let $\mathcal{Z}^*(n)$ denote the random variable of the number of* distinct *zeros of a random (monic) polynomial of degree n. Then, the PMF of $\mathcal{Z}^*(n)$ equals $\Pr[\mathcal{Z}^*(n) = k] = \binom{q}{k} q^{-k} \sum_{i=0}^{n-k} \binom{q-k}{i} (-1)^i q^{-i}$. Moreover, if $n \geq q$, the PMF simplifies to $\Pr[\mathcal{Z}^*(n) = k] = \binom{q}{k} q^{-k} (1-q^{-1})^{q-k}$.*

Unlike previous PMFs, the PMF of $\mathcal{Z}^*(n)$ takes its simplified form independently of k. Moreover, $\binom{q}{k} q^{-k} (1-q^{-1})^{q-k} = \binom{q}{k} (q^{-1})^k (1-q^{-1})^{q-k}$ is the PMF of the binomial distribution $\mathrm{Bin}(q, q^{-1})$, according to Definition 1.18. Thus, $\mathcal{Z}^*(n)$ follows a binomial distribution for *almost all* n (if we consider q fixed), which Knopfmacher and Knopfmacher [KK90] also observed.

Observation 3.30 *([KK90]).* The random variable $\mathcal{Z}^*(n)$ follows the binomial distribution $\mathrm{Bin}(q, q^{-1})$ if $n \geq q$.

Since $\mathcal{Z}^*(n)$ follows $\mathrm{Bin}(q, q^{-1})$ for almost all n, it follows this distribution in particular for all sufficiently large n. More precisely, the sequence $(\mathcal{Z}^*(n))_{n\in\mathbb{N}^{\geq q}}$ coincides with $(X)_{n\in\mathbb{N}^{\geq q}}$, where $X \sim \mathrm{Bin}(q, q^{-1})$. Hence, we conclude that $\mathcal{Z}^*(n)$ has a binomial limit.

Let $\mathcal{Z}^*$ denote the limit distribution of $\mathcal{Z}^*(n)$ as n approaches infinity.

Theorem 3.31. *The sequence $(\mathcal{Z}^*(n))_{n\in\mathbb{N}_0}$ converges in distribution to $\mathcal{Z}^* \sim \mathrm{Bin}(q, q^{-1})$.*

Proof. Let $F_n(k)$ and $F(k)$ denote the CDF of $\mathcal{Z}^*(n)$ and $\mathcal{Z}^*$, respectively. Also, assume that $\mathcal{Z}^* \sim \mathrm{Bin}(q, q^{-1})$ and that q is arbitrary but fixed. It is particularly easy to show that $\lim_{n\to\infty} F_n(k) = F(k)$ for all $k \geq 0$ because the PMFs of $\mathcal{Z}^*(n)$ and $\mathcal{Z}^*$ coincide for all $n \geq q$. Hence, $F_n(k) = F(k)$ for all $n \geq q$, and the claim follows. ■

We conclude this section and chapter with the expectation and variance of $\mathcal{Z}^*(n)$. Knopfmacher and Knopfmacher state these values in [KK90]. However, they give no proof because their results follow from more general ones determined by Schmidt [Sch76]. Schmidt examines the zeros of *multivariate* polynomials over finite fields. His results on the expectation and variance concern polynomials in $m \in \mathbb{N}$ variables, however, only of a positive (total) degree. Thus, we remark that if $n = 0$, the expectation is 0 because all units have the same number of zeros, namely, 0. Since all polynomials have that same number of zeros, the variance is 0, too. Furthermore, it is also 0 if $n = 1$ because each linear polynomial $x - v$ has exactly one zero, namely, v.

Theorem 3.32 ([KK90]). *For all $n \in \mathbb{N}_0$, the expected value of $\mathcal{Z}^*(n)$ is $\mathbb{E}[\mathcal{Z}^*(n)] = [\![n \geq 1]\!]$.*

Proof ([Sch76]). If $n = 0$, the expectation is 0 because all units are zero-free. The remaining case, $n \geq 1$, is proven in [Sch76] for polynomials in m variables. Schmidt determines that the expectation is q^{m-1}. Since we consider univariate polynomials in this thesis, we set $m = 1$ and obtain $\mathbb{E}[\mathcal{Z}^*(n)] = q^{1-1} = 1$. ■

Because the expected value is the same for all but one n, its asymptotic behavior is $\mathbb{E}[\mathcal{Z}^*] = 1$, and we do not explicitly state it in Theorem 3.32. This result also follows from the expectation of $\mathrm{Bin}(q, q^{-1})$, which is $qq^{-1} = 1$ [KK90].

The variance $\mathrm{Var}[\mathcal{Z}^*(n)]$ is not constant but only depends on q. As mentioned above, if $n \leq 1$, the variance is 0. We note that Schmidt does not consider the case $n = 1$ separately, although the formula provided in [Sch76] only holds if $n \geq 2$.

Theorem 3.33 ([KK90]). *For all $n \in \mathbb{N}_0$, the variance of the random variable $\mathcal{Z}^*(n)$ is equal to $\mathrm{Var}[\mathcal{Z}^*(n)] = [\![n \geq 2]\!](1 - q^{-1})$.*

Proof ([Sch76]). If $n = 0$, all polynomials are zero-free. Likewise, all polynomials have exactly one zero if $n = 1$. Thus, the variance is 0 in both cases. The remaining case, $n \geq 2$, is proven in [Sch76] for multivariate polynomials in m variables. Schmidt determines that the variance is $q^{m-1} - q^{m-2}$, which simplifies to $q^{1-1} - q^{1-2} = 1 - q^{-1}$ in our case $m = 1$. ■

Once again, the asymptotic variance $\mathrm{Var}[\mathcal{Z}^*]$ can be directly obtained from the distribution $\mathrm{Bin}(q, q^{-1})$ [KK90]. When q tends to infinity, the (asymptotic) variance converges to $\lim_{q\to\infty}(1 - q^{-1}) = 1$. Since $\mathrm{Var}[\mathcal{Z}^*(n)]$ is monotonically increasing in q, an asymptotically tight upper bound on the variance is 1 for all n and q.

4

Exact Detection Probabilities of Adversaries in Combined Attacks

In this chapter, we address the work by Berndt et al. [BEF+23] and improve a result therein about the probability that an adversary is not detected when introducing faults. Countermeasures based on polynomial sharing have proven useful to protect against fault and leakage attacks in cryptographic implementations, e.g., [CPR13; SFES18]. Recall that we introduced polynomial sharing in Section 1.6 of Chapter 1. Berndt et al. [BEF+23] propose a framework that addresses *combined* attacks, i.e., attacks both *passive* and *active*. In passive attacks, an adversary only observes side-channel information about the computation, e.g., by probing wires. In active attacks, on the other hand, an adversary alters (values in) the computation, e.g., by inserting faults [BEF+23]. Furthermore, the framework from Berndt et al. addresses *adaptive* attacks, i.e., attacks introducing faults based on previously conducted probing. Their work improves many previous ones, which only considered non-adaptive adversaries. The authors establish security notions applicable to adaptive adversaries and present new compilers that reduce the required randomness and number of shares.

Given an arithmetic circuit over $\mathbb{F} := \mathbb{F}_q$, Berndt et al.'s approach replaces gates with so-called *gadgets*, which use *encodings* of a field element rather than the actual element itself. For instance, a gate computing usual addition has two input wires and one output wire, where the value of the output wire is the sum of both values corresponding to the input wires. The corresponding gadget takes two sharings as input and outputs a sharing such that its secret equals the sum of the secrets of both input sharings. We usually use the term *sharing* instead of encoding. An adversary probing an intermediate wire then solely obtains a *share* of the protected value. In addition, him actively faulting a wire, i.e., a share, likely renders the underlying sharing invalid due to the degree of the polynomial being too high. More precisely, Berndt et al. focus on the *detection* of errors rather than their *correction*. They consider n-sharings of polynomials of degree $d < n$, and call a sharing *invalid* if, and only if, the degree of its underlying polynomial is greater than d. Thus, The authors must ensure that errors do not vanish. To be consistent with [BEF+23], we consider n-sharings of polynomials of degree $d < n$, and we adopt their definition of (in)valid sharings. An adversary can introduce up to $e \in \mathbb{N}_0$ errors. Berndt et al. show that $n = d + e + 1$ shares are necessary and sufficient to protect circuits against combined

attacks. Thus, they assume that $n \geq d + e + 1$ throughout the paper, which we adopt.

As already mentioned above, we improve a result in [BEF+23], stated in Fact 4.2, about the probability that an adversary is not detected when introducing faults, in other words, that he remains undetected if the degree of the polynomial corresponding to the output of a gadget is at most d, although the secret is incorrect. We state the improved version in Theorem 4.18. We assume that the reader is (roughly) familiar with the paper [BEF+23] or with its concepts. The proof of Fact 4.2 should be known, however, we sketch it at the beginning of Section 4.1.

For the sake of convenience, we first restate the authors' definition of fault robustness.

Definition 4.1 (e-f-robust [ABEO24; BEF+23]). A gadget G with two input sharings and one output sharing is *e-fault-robust* with respect to a class of faults $\mathcal{F}$ if for any valid encodings $x := (x_i)_{i\in[n]}$ and $x' := (x'_i)_{i\in[n]}$, the output $y := (y_i)_{i\in[n]} \leftarrow G(x, x')$ is also valid. Further, it holds for any fault vectors $v := (v_i)_{i\in[n]}$, $v' := (v'_i)_{i\in[n]}$, and $T \in \mathsf{A}(\mathcal{F})$ with $|T| \leq e$ and $(y_i + w_i + w'_i)_{i\in[n]} \leftarrow T[G](x + v, x' + v')$, that there are numbers t_1 and t_2 with $t_1 + t_2 \leq |T|$ such that

1. $\mathrm{weight}(w) \in [0, t_1] \cup [|\mathrm{weight}(v + v') - t_1|, \mathrm{weight}(v + v') + t_1]$, where weight gives the number of non-zero elements of a vector;
2. and $(w'_i)_{i\in[n]}$ is the zero vector or produced by the following random experiment: A polynomial $p' \in \mathcal{P}_{\leq n-t_2}$ is chosen such that the coefficients $p'_{d+1}, p'_{d+2}, \ldots, p'_{n-t_2}$ are chosen uniformly at random from $\mathbb{F}$. Then, $(w'_i)_{i\in[n]} := (p'(\alpha_i))_{i\in[n]}$.

We interpret the fault vectors as n-sharings and thus associate the sharings w and w' with the polynomials p and p', respectively, at pairwise distinct nodes $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$.

We may interpret adding faults v and v' to the inputs x and x', respectively, as well as inside the gadget (except for gates corresponding to non-linear operations) as faulting the output sharing y of G by adding the fault vector w. This is due to the "linear" nature of polynomial sharing. Since faults at the inputs of the gadget and inside the gadget can cancel out each other, it can happen that $\mathrm{weight}(w) \in [|\mathrm{weight}(v + v') - t_1|, \mathrm{weight}(v + v') + t_1]$. The absolute value of the left endpoint is needed because there may be more faults at the inputs than inside the gadget *and* vice versa. The second fault vector w' corresponds to faults introduced at non-constant, i.e., binary, multiplication gates. By definition of polynomial multiplication, the higher-order coefficients $p_{d+1}, p_{d+2}, \ldots$ of the product polynomial p are each a combination of the lower-order coefficients of $x^0, \ldots, x^d$ of both factor polynomials. Since the adversary cannot probe all these lower-order coefficients, the higher-order coefficients of p are essentially random[7] from the view of an adversary.

Berndt et al. [BEF+23] establish upper bounds on the probability that an adversary generates a valid sharing of an invalid value, i.e., the adversary is not detected when introducing faults. Their theorem is as follows:

Fact 4.2 (Theorem 4 in [BEF+23]). If a circuit is e-fault-robust, the probability that $s \leq e$ faults can produce a valid encoding of an invalid value is at most q^{s-e-1} in the case of non-adaptive attackers and $q^{s-e}(d + e + 1)^{t_1}$ for all $t_1 \leq s$ in the case of adaptive attackers.

[7] The product of two random polynomials in $\mathcal{P}_d$ is *not* random over $\mathcal{P}_{2d}$.

Throughout this chapter, we refer to Fact 4.2 as Theorem 4 (formatted in sans-serif and without chapter number).

In Section 4.1, we mention that three quantities established in the proof of Theorem 4 are not exact but upper (or lower) bounds. Thus, we establish the exact figures.

In Section 4.2, we improve the authors' theorem by stating the *exact* probabilities in both the non-adaptive and adaptive cases. Regarding the latter case, although our formula gives the exact probability, it is not in closed form. This stems from the fact that it includes the PMF of a random variable that is a priori difficult to analyze.

Finally, in Section 4.3, we provide several upper bounds on the probability in the adaptive case, e.g., by replacing $t_1 + t_2$ with s since $t_1 + t_2 \leq s$. These formulae include fewer terms than the exact formula, and they are in a closed form. This facilitates using them in other applications where the exact probability is not required. We also argue that one of the given upper bounds is tight. Furthermore, we present an improved version of Theorem 4 in Theorem 4.18. Lastly, we compare the improved theorem with the original one and conclude that our upper bound yields a proper improvement over theirs.

4.1 Notes on the Original Theorem

Before we improve Theorem 4, we first remark that three quantities stated by Berndt et al. in the proof of Theorem 4 are upper or lower bounds rather than exact figures. Furthermore, one upper bound was derived incorrectly. Nevertheless, this upper bound and the entire Theorem 4 are still valid.

We first sketch the proof of Theorem 4. Berndt et al. establish the upper bound q^{s-e-1} in the case of non-adaptive adversaries by computing the probability that all higher-order coefficients of p' are 0, which they state as q^{s-e-1}. In Lemma 4.10, we prove that the exact probability is $q^{d+t_2-n} \leq q^{s-e-1}$. In the adaptive case, it can occur that the higher-order coefficients of p and p' cancel out each other when both polynomials are added. The authors compute the probability of that happening by comparing the number of different p with the number of different p'. They state the number of the former and the latter as $\binom{n}{t_1}q^{t_1}$ and q^{e-t_2}, respectively. These numbers are upper bounds and lower bounds, respectively. Then, they divide the former by the latter to determine the probability $q^{t_1+t_2-e}n^{t_1}$ that some p matching the polynomial p' exists such that the higher-order coefficients of $p + p'$ vanish. Finally, the term $q^{s-e}(d + e + 1)^{t_1}$ is used to bound $q^{t_1+t_2-e}n^{t_1}$ from above, which, however, does not hold: We consider both factors, $q^{t_1+t_2-e}$ and n^{t_1}. Regarding the former, bounding $q^{t_1+t_2-e}$ by q^{s-e} from above is valid because $t_1 + t_2 \leq s$. Regarding the latter, substituting n with $d + e + 1$, however, yields a *lower* bound since $n \geq d + e + 1$. That is, $(d + e + 1)^{t_1} \leq n^{t_1}$. The upper bound on the first factor $q^{t_1+t_2-e} \leq q^{s-e}$ cannot compensate for this because if $t_1 + t_2 = s$, the upper bound is tight, although n can still be larger than $d + e + 1$.

Nevertheless, one may wonder if the final bound $q^{s-e}(d+e+1)^{t_1}$ yields a feasible upper bound on the *actual* probability. In Remark 4.17, we answer in the affirmative, hence, Theorem 4 is valid.

We further elaborate on the exact numbers of different p and p'. Firstly, we regard the number of possible polynomials p'. We recall that p' is the polynomial defining the

sharing w', which captures faults introduced at multiplication gates or other non-linear ones. In the proof, the authors give this number as q^{e-t_2}, which we conceive as an exact figure since the authors say that "the number of different polynomials possible for $[p']$ is q^{e-t_2}." We emphasize that this number is only a loose lower bound. We also recall that $n \geq d + e + 1$, where $d + e + 1$ is the minimum number of shares required to protect against adversaries who can probe d wires and fault e wires.

Lemma 4.3. *The number of different polynomials p' equals $q^{n-t_2+1} > q^{e-t_2}$.*

Proof. By construction, p' is a polynomial of degree at most $n - t_2$ with random higher-order coefficients $p'_{d+1}, \ldots, p'_{n-t_2}$. Theorem 1.45 states that $|\mathcal{P}_{\leq n-t_2}| = q^{n-t_2+1}$. Thus, there are q^{n-t_2+1} different p', regardless of whether the higher-order coefficients are randomly sampled. Since $n > d + e$, we obtain the lower bound $q^{n-t_2+1} > q^{(d+e)-t_2+1}$. We conclude that q^{e-t_2} is a loose lower bound because $d + e - t_2 + 1 > e - t_2$. ■

We turn to polynomial p, which corresponds to the sharing w combining the input faults and the faults at linear gates inside the gadget. The authors specify the number of different p as $\binom{n}{t_1}q^{t_1}$, which we also understand as an exact figure. Since the authors do no elaborate on the derivation of the formula, we *suppose* that by using the term q^{t_1} (which equals $|\mathbb{F}|^{q_1}$) rather than $(q-1)^{t_1}$ (which equals $|\mathbb{F} \setminus \{0\}|^{t_1}$), they account for the fact that *at most* t_1 faults occur. This allows them to introduce no faults at certain selected shares. In particular, $\binom{n}{t_1}q^{t_1}$ counts the number of ways of choosing t_1 shares from n possible ones to add t_1 (vanishing) faults from $\mathbb{F}$ there. Thus, the formula $\binom{n}{t_1}q^{t_1}$ sometimes counts the "same" faulting twice, namely, when no faults occur at two different chosen shares.

Example 4.4. Let $t_1 = 2$ and consider the two pairs of chosen nodes $(\alpha_1, \alpha_2) = (1, 2)$, as well as $(\alpha'_1, \alpha'_2) = (1, 3)$. The only non-zero fault, say, ε, occurs at node $\alpha_1 = \alpha'_1 = 1$. Since no fault is introduced at nodes 2 and 3, both faultings constitute the same fault vector, namely, $(\varepsilon, 0, \ldots, 0)$. The formula distinguishes them because we chose different nodes.

The formula counts twice as soon as we can introduce no fault at a node in the chosen node vector. The formula counting the exact number of different p should count the *actual* number of faults. Remember that *at most* t_1 shares are faulted. The exact formula, therefore, is:

Observation 4.5. For all $n, t_1 \in \mathbb{N}_0$, the number of ways to introduce at most t_1 faults into an n-sharing is $\sum_{i=0}^{t_1} \binom{n}{i}(q-1)^i$.

The summand $\binom{n}{i}$ counts the number of ways of choosing the i fault nodes, i.e., i elements from α. The term $(q-1)^i$ counts the number of ways to fault i nodes. We stress that we introduce *exactly* i faults since the value 0 is prohibited.

However, as the authors establish an *upper* bound and $\binom{n}{t_1}q^{t_1}$ overestimates the actual number of different p, as shown below, this turns out not to be a problem, and Theorem 4 remains valid.

Theorem 4.6. *For all $q \in \mathbb{N}^{\geq 2}$, $n \in [0, q]$, and $t_1 \in [0, n]$, the formula $\binom{n}{t_1}q^{t_1}$ provides an upper bound on the number of different p, i.e., $\sum_{i=0}^{t_1} \binom{n}{i}(q-1)^i \leq \binom{n}{t_1}q^{t_1}$ holds.*

Proof. We prove the claim by showing that for every combination considered by the left-hand side of the inequality, a corresponding one exists considered by the right-hand side.

Let $\alpha = (\alpha_j)_{j\in[n]} \in \mathbb{F}^n$ be the vector of nodes, let $\rho = (\rho_j)_{j\in[i]} \subseteq \alpha$ be the vector of nodes where a fault occurs, and denote by $\varepsilon := (\varepsilon_j)_{j\in[i]} \in (\mathbb{F} \setminus \{0\})^i$ the fault vector comprising the fault values at the i nodes in ρ. We stress that the number of faults need not be exactly t_1 but rather is between 0 and t_1. Let $\pi = \{\langle\rho_1, \varepsilon_1\rangle, \dots, \langle\rho_i, \varepsilon_i\rangle\}$ be the set of node-value fault pairs, considered by the sum on the left-hand side. Likewise, let $\pi' = \{\langle\rho'_1, \varepsilon'_1\rangle, \dots, \langle\rho'_{t_1}, \varepsilon'_{t_1}\rangle\}$ be the set of node-value pairs that corresponds to *possible* faults, considered by the formula on the right-hand side, where $\rho' = (\rho'_j)_{j\in[t_1]}$ and $\varepsilon' \in \mathbb{F}^{t_1}$. Furthermore, let Π and Π' be the sets of possible π and π', respectively.

We show that for every π, there exists a corresponding π' that represents the same faulting by giving an injective mapping $\varphi\colon \Pi \to \Pi', \pi \mapsto \pi'$. The mapping constructs π' from π by "faulting" the remaining $t_1 - i$ positions with 0. More precisely,

$$\begin{aligned}\varphi(\pi) &\triangleq \varphi(\{\langle\rho_1, \varepsilon_1\rangle, \dots, \langle\rho_i, \varepsilon_i\rangle\})\\ &\triangleq \{\langle\rho_1, \varepsilon_1\rangle, \dots, \langle\rho_i, \varepsilon_i\rangle, \langle\rho'_{i+1}, \varepsilon'_{i+1}\rangle, \dots, \langle\rho'_{t_1}, \varepsilon'_{t_1}\rangle\}\\ &:= \{\langle\rho_1, \varepsilon_1\rangle, \dots, \langle\rho_i, \varepsilon_i\rangle, \langle\bar\rho_1, 0\rangle, \dots, \langle\bar\rho_{t_1-i}, 0\rangle\},\end{aligned}$$

where $(\bar\rho)_{i\in[n-i]} = \alpha \setminus \rho$. The function φ is one-to-one because none of the $\varepsilon_j \in \varepsilon$ is 0. Thus, the original set π can be recovered by removing the $t_1 - i$ appended pairs $\langle\bar\rho_1, 0\rangle, \dots, \langle\bar\rho_{t_1-i}, 0\rangle$ from $\varphi(\pi)$. From the injectivity of φ, we conclude that $|\Pi| \le |\Pi'|$. Since $|\Pi| = \sum_{i=0}^{t_1} \binom{n}{i}(q-1)^i$ and $|\Pi'| = \binom{n}{t_1}q^{t_1}$, the claim follows. ∎

It follows that, once the adversary introduces faults but not at *every* node, that is, $t_1 \in [n-1]$, there is a combination that the formula $\binom{n}{t_1}q^{t_1}$ counts twice. This implies that the inequality in Theorem 4.6 is tight if, and only if, $t_1 = 0$ or $t_1 = n$, where the latter case cannot occur since $t_1 < n$.

Corollary 4.7. *Equality between* $\sum_{i=0}^{t_1} \binom{n}{i}(q-1)^i$ *and* $\binom{n}{t_1}q^{t_1}$ *holds if, and only if,* $t_1 = 0$ *or* $t_1 = n$.

Proof. We consider all three cases, viz., $t_1 = 0$, $t_1 = n$, and $t_1 \in [n-1]$, separately, and we begin with $t_1 = 0$.

If $t_1 = 0$, we have $\sum_{i=0}^{0} \binom{n}{i}(q-1)^i = \binom{n}{0}(q-1)^0 = 1 = \binom{n}{0}q^0$.

Likewise, if $t_1 = n$, the binomial formula, which the sum represents, is complete, and we obtain $\sum_{i=0}^{n} \binom{n}{i}(q-1)^i = \sum_{i=0}^{n} \binom{n}{i}(q-1)^i 1^{n-i} = ((q-1)+1)^n = q^n = \binom{n}{n}q^n$.

Finally, if $t_1 \in [n-1]$, then according to Example 4.4, we can always choose two different nodes (since $t_1 < n$) and not fault there. They count as two combinations, nevertheless. More precisely and by referring to the proof of Theorem 4.6, for all $i \in [0, t_1 - 1]$, we do not fault at the remaining $t_1 - i$ nodes $\rho'_{i+1}, \dots, \rho'_{t_1}$, i.e., we set all $\varepsilon'_{i+1}, \dots, \varepsilon'_{t_1}$ to 0. Since $t_1 < n$, there exists a node $\alpha_j \in \alpha$ which is neither in ρ nor in ρ'. Hence, replacing any of the remaining nodes with α_j, say, ρ'_{t_1}, yields a different combination because ρ' changed. However, since $\varepsilon'_{t_1} = 0$, substituting α_j for ρ'_{t_1} leaves the faulting unchanged. ∎

Finally, to obtain an upper bound on the probability in the adaptive case, Berndt et al. divide the number of different p by the number of different p'. We note that there are cases with more p than p', hence, the bound can exceed 1. In general, there are sometimes more p than p' and vice versa.

Example 4.8. Let $q = 23$, $t_1 = 14$, $t_2 = 4$, and $d = 1$. With $n = t_1 + t_2 + d + 1 = 20$, we have more p than p', namely, $\sum_{i=0}^{t_1} \binom{n}{i}(q-1)^i \approx 2.65 \cdot 10^{23} > 1.41 \cdot 10^{23} \approx q^{n-t_2+1}$, whereas with $n = q - 1 = 22$, we have less p than p', namely, approximately $2.14 \cdot 10^{24} < 7.46 \cdot 10^{25}$.

4.2 Establishing Exact Probabilities

In this section, we improve Theorem 4 by providing exact probabilities rather than upper bounds in case the adversary is not adaptive and when he is. We first consider the case where the adversary is non-adaptive. As the authors have already observed, either p or p' may be assumed to be zero in this case. We give the exact probabilities, first if p' is zero and then if p is.

If p' is zero, an adversary introducing faults into the computation is always detected.

Fact 4.9 ([BEF+23]). If the adversary is non-adaptive and $p' = 0$, the output sharing is always invalid or $p = 0$.

Since we use the reason why Fact 4.9 holds later on, we recall it: If at most t_1 faults occur, p has at least $n - t_1 > d$ zeros or $p = 0$. The former implies $\deg(p) \geq n - t_1 > d$, according to Fact 1.41. Then, the sharing is invalid. The latter, however, implies that no fault occurred.

Next, we consider the second case, that is, if $p = 0$ instead. In this case, the sharing may be valid but only if p' is also zero. Berndt et al. give an upper bound on the probability that p' is zero, namely, q^{s-e-1}. Here, $e \geq t_1 + t_2$ is an upper bound on the number of faults an adversary can introduce, and $s \geq t_1 + t_2$ equals the actual number of introduced faults. We determine the exact probability that p' is zero below by adapting the proof from [BEF+23]:

Lemma 4.10. *If the adversary is non-adaptive and $p = 0$, the probability that the output sharing is valid is $q^{d+t_2-n} \leq q^{s-e-1}$.*

Proof ([BEF+23]). By construction, we can write p' as $p'(x) = \sum_{k=0}^{n-t_2} p'_k x^k$. Recall that the output sharing is valid if, and only if, $\deg(p') \leq d$ because we assumed that $p = 0$. Further, the higher-order coefficients of p' are randomly sampled. Thus, p' is valid if, and only if, $\bigwedge_{k=d+1}^{n-t_2}(p'_k = 0)$. Since all coefficients are sampled uniformly and independently, the probability that p' is valid is $\Pr[\bigwedge_{k=d+1}^{n-t_2}(p'_k = 0)] = \prod_{k=d+1}^{n-t_2} q^{-1} = q^{d+t_2-n}$.

Finally, we show that q^{s-e-1} yields an upper bound. Since $n \geq d + e + 1$ and $t_2 \leq s$, we deduce that $q^{d+t_2-n} \leq q^{d+s-(d+e+1)} = q^{s-e-1}$. ∎

We have completed analyzing the non-adaptive case and now turn to the more sophisticated one where the adversary is adaptive. To simplify computations, we henceforth assume that p is invalid, i.e., $\deg(p) > d$. This is reasonable because otherwise, i.e., if $\deg(p) \leq d$, the polynomial p must be zero, which is implied by Observation 1.60 since at most s faults ensure that $\deg(p) \geq n - s > d$. But if $p = 0$, an *adaptive* adversary can only use p' to generate an invalid output sharing. Recall that p' corresponds to faults at multiplication gates. However, the higher-order coefficients of p' are randomly produced, according to Definition 4.1. Thus, whether p' is invalid is independent of the

faults that the adversary introduces. This means he cannot exploit having probed wires beforehand and may thus be considered non-adaptive. In other words, the case $p = 0$ reduces to that of a non-adaptive adversary, in which case Lemma 4.10 gives the probability of him not being detected.

Before we determine the probability of an adaptive adversary not being detected, we state the part of the PMF of $\deg(p')$ (treated as a random variable) that is relevant for us as it will be of use in various places throughout the remainder of this chapter. According to Definition 4.1, we can only give the exact PMF when $\deg(p') \geq d + 1$ because only the higher-order coefficients of p' are random. Fortunately, this range coincides with the relevant part.

Lemma 4.11. *For all $i \in [d+1, n-t_2]$, the probability that the degree of p' equals i is precisely* $\Pr[\deg(p') = i] = (q-1)q^{i+t_2-n-1}$. *Moreover,* $\Pr[\deg(p') > n - t_2] = 0$.

Proof. Let $i = \deg(p')$ and recall that we have $p'(x) = \sum_{k=0}^{n-t_2} p'_k x^k$ by construction. It immediately follows that $\deg(p') > n - t_2$ is impossible.

Thus, assume that $i \in [d+1, n-t_2]$. The degree of p' is i if, and only if, the coefficient p'_i does not vanish, but all coefficients above it do, i.e., $p'_i \neq 0$ and $\bigwedge_{k=i+1}^{n-t_2}(p'_k = 0)$. Since the higher-order coefficients are uniformly and independently, the former happens with probability $(q-1)/q$ and the latter with probability $q^{-((n-t_2)-(i+1)+1)} = q^{i+t_2-n}$. Finally, due to the p'_k being independent, the probability that both events occur is the *product* of the two previous probabilities, namely, $(q-1)/q \cdot q^{i+t_2-n} = (q-1)q^{i+t_2-n-1}$. ∎

We are now ready to give the probability of an adaptive adversary not being detected. For the sake of clarity, we let $p^+ = p + p'$, $\delta = \deg(p)$, $\delta' = \deg(p')$, and $\delta^+ = \deg(p^+)$. We mention that d is the degree of a regular, valid polynomial used to share a wire value. Since the adversary can only probe d wires, choosing d as the degree is optimal.

Theorem 4.12. *If the adversary is adaptive, the probability that the output sharing is valid equals*

$$\frac{q^{d+t_2-2n}(q^{t_1+1} - q^{t_2})}{q-1} \sum_{i=n-t_1}^{n-t_2} q^i \Pr[\deg(p) = i]. \tag{4.1}$$

Proof. First, recall that $\delta' > d$ does not necessarily hold, whereas we may always assume that $\delta > d$ holds. It should be clear that the adversary is not detected if, and only if, $\delta^+ \leq d$. Since we add p and p', it may happen that their higher-order terms cancel out each other, that is, $\delta^+ \leq d$, although $\delta > d$ or $\delta' > d$. Otherwise, if $\delta^+ > d$, an adaptive adversary is always detected. Fortunately, $\delta^+ \leq d$ can only happen if $\delta = \delta'$, according to Fact 1.43. Using this observation, we analyze both cases separately and combine them later using the *law of total probability*. More precisely, we separate the probability of interest $\Pr[\delta^+ \leq d]$ into

$$\Pr[\delta^+ \leq d] = \Pr[\delta^+ \leq d \mid \delta = \delta'] \Pr[\delta = \delta'] + \Pr[\delta^+ \leq d \mid \delta \neq \delta'] \Pr[\delta \neq \delta'].$$

We begin with the easy case where $\delta \neq \delta'$. Then, the adversary cannot go unnoticed since at least one of the higher-order coefficients $p^+_{d+1}, p^+_{d+2}, \ldots$ does not vanish. This is implied by Fact 1.43. More precisely, δ^+ is *exactly* $\max\{\delta, \delta'\} \geq \delta$ if $\delta \neq \delta'$ and, therefore, $\delta^+ \geq \delta \geq n - t_1 > (d+e) - e = d$. We conclude that $\Pr[\delta^+ \leq d \mid \delta \neq \delta'] = 0$.

It remains to regard the case $\delta = \delta'$, where we need to compute $\Pr[\delta^+ \leq d \mid \delta = \delta']$ and $\Pr[\delta = \delta']$. To evaluate probabilities regarding $\delta = \delta'$, we evaluate the joint PMF $\Pr[\delta = i \wedge \delta' = i]$ over the common domain of δ and δ'. Since both random variables are finite, it is sufficient to consider i in the set $\operatorname{supp}(\delta) \cap \operatorname{supp}(\delta')$. Berndt et al. have already ascertained that equality can only occur in case $n - t_1 \leq n - t_2$, i.e., if $t_1 \geq t_2$, because $\delta \geq n - t_1$ but $\delta' \leq n - t_2$. We, hence, only consider $i \in [n - t_1, n - t_2] \subseteq [d + 1, n - t_2]$. The conditional probability of δ^+ being at most d equals

$$\begin{aligned}
\Pr[\delta^+ \leq d \mid \delta = \delta'] &= \sum_{i=n-t_1}^{n-t_2} \Pr[\delta^+ \leq d \mid \delta = i \wedge \delta' = i] \\
&\overset{(\dagger)}{=} \sum_{i=n-t_1}^{n-t_2} \Pr\left[\bigwedge_{j=d+1}^{i} (p'_j = -p_j) \;\middle|\; p_i, p'_i \neq 0 \right] \\
&\overset{(\ddagger)}{=} \sum_{i=n-t_1}^{n-t_2} \left(\frac{1}{q-1} \prod_{j=d+1}^{i-1} q^{-1} \right) \\
&= [\![t_1 \geq t_2]\!] \frac{q^{d+1-n}(q^{t_1+1} - q^{t_2})}{(q-1)^2}.
\end{aligned} \tag{4.2}$$

The second equality (†) holds since to achieve $\delta^+ \leq d$, all coefficients $p^+_{d+1}, \ldots, p^+_i$ must vanish. Because $p^+_j \triangleq p_j + p'_j$, this requires $p'_j = -p_j$. Moreover, the third equality (‡) holds because the higher-order coefficients of p' are chosen independently (of p). The probability that $p'_j = -p_j$ equals q^{-1} if $j < i$. In case of $j = i$, the probability is $1/(q-1)$ since we assume $p_i, p'_i \neq 0$.

Now that we have calculated $\Pr[\delta^+ \leq d \mid \delta = \delta']$, it remains to establish $\Pr[\delta = \delta']$. Again, we evaluate the joint PMF. We use the fact that δ and δ' are independent if $\delta' > d$ and that we already obtained the PMF of δ' when $\delta' \in [d + 1, n - t_2]$ in Lemma 4.11:

$$\begin{aligned}
\Pr[\delta = \delta'] &= \sum_{i=n-t_1}^{n-t_2} \Pr[\delta = i \wedge \delta' = i] \\
&= \sum_{i=n-t_1}^{n-t_2} \Pr[\delta = i] \Pr[\delta' = i] \\
&= \sum_{i=n-t_1}^{n-t_2} \Pr[\delta = i](q-1)q^{i+t_2-n-1} \\
&= (q-1)q^{t_2-n-1} \sum_{i=n-t_1}^{n-t_2} q^i \Pr[\delta = i].
\end{aligned}$$

Because p depends on the adversary's fault strategy, specifying the distribution of δ is difficult. For that reason, we provide universal upper bounds and argue that one bound is tight in the next Section 4.3.

Finally, we can combine all results and obtain the desired probability:

$$\begin{aligned}\Pr[\delta^+ \le d] &= \Pr[\delta^+ \le d \mid \delta = \delta'] \Pr[\delta = \delta'] + \Pr[\delta^+ \le d \mid \delta \neq \delta'] \Pr[\delta \neq \delta'] \\ &= \Pr[\delta^+ \le d \mid \delta = \delta'] \Pr[\delta = \delta'] + 0 \\ &= \left([\![t_1 \ge t_2]\!] \frac{q^{d+1-n}(q^{t_1+1} - q^{t_2})}{(q-1)^2} \right) \left((q-1) q^{t_2-n-1} \sum_{i=n-t_1}^{n-t_2} q^i \Pr[\delta = i] \right) \\ &= \frac{q^{d+t_2-2n}(q^{t_1+1} - q^{t_2})}{q-1} \sum_{i=n-t_1}^{n-t_2} q^i \Pr[\delta = i],\end{aligned}$$

where in the last row, we may omit the $[\![t_1 \ge t_2]\!]$ bracket due to the present sum. ■

4.3 Upper Bounds and Comparison

In Theorem 4.12 of the previous Section 4.2, we determined the exact probability that an adaptive adversary is not detected. In the established Equation 4.1, we could not simplify the sum $\sum_{i=n-t_1}^{n-t_2} q^i \Pr[\delta = i]$ because the distribution of δ depends on the adversary. Thus, we present an upper bound on the aforementioned equation that holds regardless of the adversary's strategy. The following estimation comes in useful:

Observation 4.13. For all $q \in \mathbb{N}$, $a, b \in \mathbb{N}_0$ such that $a \le b$, and random variables X such that $[0, b]$ is a subset of its codomain, $\sum_{i=a}^{b} q^i \Pr[X = i] \le \sum_{i=a}^{b} q^b \Pr[X = i] \le q^b$ holds.

Applying Observation 4.13 to Equation 4.1 yields a universal upper estimate.

Theorem 4.14. *If the adversary is adaptive, the probability that the output sharing is valid is at most*

$$\begin{aligned}\Pr[\delta^+ \le d] &\le \frac{q^{d+t_2-2n}(q^{t_1+1} - q^{t_2})}{q-1} q^{n-t_2} \sum_{i=n-t_1}^{n-t_2} \Pr[\delta = i] \\ &\le [\![t_1 \ge t_2]\!] \frac{q^{d+t_2-2n}(q^{t_1+1} - q^{t_2})}{q-1} q^{n-t_2} \cdot 1 \\ &= [\![t_1 \ge t_2]\!] \frac{q^{d-n}(q^{t_1+1} - q^{t_2})}{q-1} =: I.\end{aligned} \tag{4.3}$$

Proof. We omit all $[\![t_1 \ge t_2]\!]$ brackets because the chain of inequalities holds regardless. The two inequalities in Equation 4.3 hold due to Observation 4.13, which implies that the sum in Equation 4.1 can be bounded from above by

$$\sum_{i=n-t_1}^{n-t_2} q^i \Pr[\delta = i] \le \sum_{i=n-t_1}^{n-t_2} q^{n-t_2} \Pr[\delta = i] = q^{n-t_2} \sum_{i=n-t_1}^{n-t_2} \Pr[\delta = i] \le q^{n-t_2}.$$

Thus, replacing the sum by either $q^{n-t_2} \sum_{i=n-t_1}^{n-t_2} \Pr[\delta = i]$ or q^{n-t_2} yields the claimed chain of inequalities. ■

With the universal upper bound I established, the question arises whether it is tight. In the following, we argue that I is tight because an adversary is always able to choose a polynomial p of suitable degree. Naturally, the greater the degree, the more likely it is that a randomly chosen p' is of said degree because $i < i'$ implies $|\mathcal{P}_i| < |\mathcal{P}_{i'}|$, but the less likely it is that all necessary coefficients of p and p' cancel out so that $\delta^+ \leq d$. Hence, an adversary *controlling* p would certainly try to find the best trade-off, i.e., he would choose a p with $\delta = \operatorname{argmax}_i(\Pr[\delta' = i \wedge \delta^+ \leq d \mid \delta = i])$. In fact, his choice is not restricted at all because the probability is the same for all possible δ. This is intuitively clear because an increase of δ' by 1 requires an additional coefficient to cancel out to achieve $\delta^+ \leq d$. Thus, the initial probability is multiplied by q^{-1}. However, if the degree δ' increases by 1, there is one coefficient less between p'_{i+1} and p'_{n-t_2} that must vanish in order that p' assumes that degree. Since each coefficient vanishes with probability q^{-1} as well, both probabilities cancel out.

Lemma 4.15. *For all $i \in [n - t_1, n - t_2]$, the probability $\Pr[\delta' = i \wedge \delta^+ \leq d \mid \delta = i]$ is the same, namely, q^{d+t_2-n}.*

Proof. To be able to use expressions that we have already determined, we first rewrite the term $\Pr[\delta' = i \wedge \delta^+ \leq d \mid \delta = i]$ by applying the definition of conditional probability:

$$\begin{aligned}\Pr[\delta' = i \wedge \delta^+ \leq d \mid \delta = i] &\triangleq \Pr[\delta^+ \leq d \mid \delta = i \wedge \delta' = i] \Pr[\delta' = i \mid \delta = i] \\ &= \Pr[\delta^+ \leq d \mid \delta = i \wedge \delta' = i] \Pr[\delta' = i].\end{aligned}$$

The second equality holds because δ and δ' are independent when $i \geq d + 1$. Fortunately, both factors are known, the former from Equation 4.2 and the latter from Lemma 4.11. We recall that $\Pr[\delta^+ \leq d \mid \delta = i \wedge \delta' = i] = q^{d+1-i}/(q-1)$ and $\Pr[\delta' = i] = (q-1)q^{i+t_2-n-1}$. We conclude that

$$\Pr[\delta' = i \wedge \delta^+ \leq d \mid \delta = i] = \frac{q^{d+1-i}}{q-1}\left((q-1)q^{i+t_2-n-1}\right) = q^{d+t_2-n},$$

which is independent of i. ∎

It is reasonable to assume that the adversary knows t_1 and t_2. Consequently, the upper bound $\Pr[\delta^+ \leq d] \leq I$ in Equation 4.3 is tight *if* the adversary can choose δ ad libitum, i.e., choose p such that $\delta \in [n - t_1, n - t_2]$. In that case, $\Pr[\delta \in [n - t_1, n - t_2]] = 1$, and so is the sum $\sum_{i=n-t_1}^{n-t_2} \Pr[\delta = i]$ in Equation 4.3. In other words, this is the best strategy the adversary can pursue since the event $\delta^+ \leq d$ then only depends on the higher-order coefficients of p', which he cannot control. We recall that δ depends on the number of faults the adversary introduces into the computation. Consider the following example: If the adversary introduces $\gamma = 4$ faults using w, then δ is *at least* $n - 4$ because w has at least $n-\gamma = n-4$ (distinct) zeros. However, it is uncertain that a suitable p exists *for every* degree between $n - 4$ and $n - 1$. For instance, if t_2 happens to be 3, the adversary must be able to choose p such that $\delta \leq n - t_2 = n - 3$, whereas it may be that w, including the $\gamma = 4$ faults, corresponds to a polynomial of degree $n-1$. Nevertheless, the adversary can always construct a sharing w with exactly $\gamma \geq 1$ faults that corresponds to a polynomial of degree $i \in [n-\gamma, n-1]$ for all i, i.e., he can choose a p with $\delta \in [n-t_1, n-t_2]$. To prove this

claim, we construct a polynomial of degree i whose n-sharing includes precisely γ faults, that is, γ non-zero entries. The adversary can efficiently construct the polynomial and evaluate it at all n nodes in α to obtain the sharing w, according to which he introduces the γ faults.

We show that for any degree $i \in [n-\gamma, n-1]$, there is a polynomial of degree i with exactly $n-\gamma$ distinct zeros at the nodes in α, i.e., with exactly γ faults.

Theorem 4.16. *For all $\gamma \in \mathbb{N}^{\leq n}$ and for all $i \in [n-\gamma, n-1]$, there is a polynomial p of degree i such that the corresponding n-sharing $w = (p(\alpha_i))_{i\in[n]}$ satisfies* $\mathrm{weight}(w) = \gamma$.

Proof. We construct p according to the requirements made to w. For the sake of simplicity, let $w_1, \dots, w_\gamma$ be the faults in w, that is, its non-zero elements. Thus, $w_{\gamma+1}, \dots, w_n$ vanish, which implies that $\alpha_{\gamma+1}, \dots, \alpha_n$ are zeros of p. As previously done throughout Chapter 3, this observation lets us construct p as $p = g\prod_{j=\gamma+1}^{n}(x-\alpha_j)$. This construction guarantees (until now) that w has at least $n-\gamma$ vanishing entries, viz., $w_{\gamma+1}, \dots, w_n$. Thus, we must define g in a way that guarantees that the remaining γ entries are non-zero, that is, g must not introduce zeros there. Furthermore, since $\deg(p) = i$ and the degree of the split product $\prod_{j=\gamma+1}^{n}(x-\alpha_j)$ is $n-(\gamma+1)+1 = n-\gamma$, the degree of g must be $i-(n-\gamma)$. There are several options to define g so that both of the above-mentioned requirements are satisfied. For instance, $g(x) = (x-v)^{i-n+\gamma}$ is feasible for any $v \in \mathbb{F} \setminus \{\alpha_1, \dots, \alpha_\gamma\}$ because it only introduces a zero where p already is or that is not in α. Since $\gamma < q$, $\mathbb{F} \setminus \{\alpha_1, \dots, \alpha_\gamma\} \neq \emptyset$ and, hence, such v always exists. ∎

In Section 4.1, we raised the following question concerning the final upper bound in the proof of Theorem 4: Does the final upper bound $q^{s-e}(d+e+1)^{t_1}$ yield a feasible bound on the *actual* success probability of an adaptive adversary, stated in Equation 4.1, although it does not on $q^{t_1+t_2-e}n^{t_1}$? Now that we have established I, we can answer in the affirmative:

Remark 4.17. The final bound $q^{s-e}(d+e+1)^{t_1}$ in Theorem 4 is feasible because it is at least as great as I. To see why, we first bound I from above by dropping its denominator, which yields $I \leq q^{d-n}(q^{t_1+1} - q^{t_2})$. Substituting n and q^{t_2} with $d+e+1$ and 0, respectively, further yields $q^{d-n}(q^{t_1+1} - q^{t_2}) \leq q^{-e-1}(q^{t_1+1} - 0) = q^{t_1-e}$. It remains for us to show that $q^{t_1-e} \leq q^{s-e}(d+e+1)^{t_1}$. Note that $(d+e+1)^{t_1} \geq 1$. Thus, the previous inequality holds since already $q^{t_1-e} \leq q^{s-e}\cdot 1$ holds. Finally, we remark that the slightly different final bound $q^{t_1+t_2-e}(d+e+1)^{t_1}$ is feasible too.

We present further upper bounds on I from Equation 4.3 and, accordingly, also on $\Pr[\delta^+ \leq d]$ because simpler expressions suffice for certain applications. We use the pre-existing inequalities $0 \leq t_2 \leq t_1 \leq s \leq e < n$ and $t_1 + t_2 \leq s$ to bound the numerator of I further from above. The established chain of inequalities is displayed in Figure 4.1. We omit further bounds regarding the denominator $q-1$ of I and simply note that dropping it yields a feasible upper bound.

In Section 4.2, we established exact formulae for the probability of an adversary remaining undetected in the non-adaptive and adaptive cases. For the latter, we also provided upper bounds and argued that I in Equation 4.3 is tight. Thus, we are ready to present our improved version of Theorem 4.

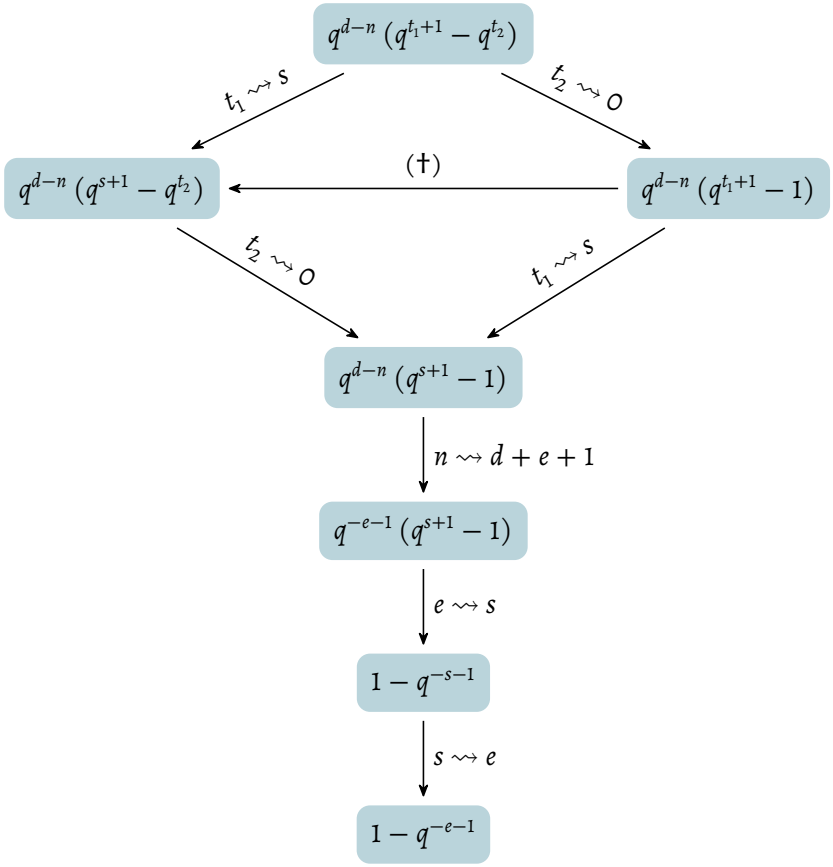

Figure 4.1: The chain of inequalities of the denominator of I in Equation 4.3. An arrow pointing from A to B means that $A \leq B$. A squiggly arrow $a \rightsquigarrow b$ denotes substituting a with b. Inequality (†) holds because $q^{s+1} - q^{t_2} \geq q^{t_1+t_2+1} - q^{t_2}$ and $q^{t_1+t_2+1} - q^{t_2} \geq q^{t_1+1} - 1$ is equivalent to $(q^{t_1+1} - 1)(q^{t_2} - 1) \geq 0$, where both factors are non-negative.

Theorem 4.18 (Improved Theorem 4 in [BEF+23]). *If a circuit is e-fault-robust, the probability that $s \leq e$ faults can produce a valid encoding of an invalid value is at most $q^{d+t_2-n} \leq q^{s-e-1}$ in the case of non-adaptive attackers and*

$$\frac{q^{d+t_2-2n}(q^{t_1+1}-q^{t_2})}{q-1}\sum_{i=n-t_1}^{n-t_2} q^i \Pr[\deg(p)=i] \overset{(\dagger)}{\leq} \frac{q^{d-n}(q^{t_1+1}-q^{t_2})}{q-1} \leq q^{-e-1}(q^{t_1+1}-1)$$

for all $t_1, t_2 \leq s$ in the case of adaptive attackers. Moreover, the first inequality $(\dagger)$ is tight.

Proof. The theorem follows immediately from combining Fact 4.9, Lemma 4.10, Theorems 4.12 and 4.14, and Lemma 4.15. The last inequality holds since $n > d + e$ and $t_2 \geq 0$. ■

Finally, we compare our upper bound I against the original one established by Berndt et al. We recall that the authors' *final* upper bound is $q^{s-e}(d+e+1)^{t_1}$ and that it is valid, according to Remark 4.17. We even use $t_1 + t_2$ instead of s, that is, we compare our bound with $q^{t_1+t_2-e}(d+e+1)^{t_1}$.

Theorem 4.19. *The upper bound I is at least $(q-1)(d+e+1)^{t_1}$ times as good as the original one $q^{s-e}(d+e+1)^{t_1}$ in Theorem 4.*

Proof. Let $\mu = d+e+1$. Since $t_1+t_2 \leq s$, we have $q^{t_1+t_2-e}\mu^{t_1} \leq q^{s-e}\mu^{t_1}$. Thus, it is sufficient to consider the quotient of I and $q^{t_1+t_2-e}\mu^{t_1}$ and bound it from below:

$$\begin{aligned}
q^{t_1+t_2-e}\mu^{t_1} \Big/ \frac{q^{d-n}(q^{t_1+1}-q^{t_2})}{q-1} &= \frac{(q-1)q^{n+t_1+t_2-d-e}\mu^{t_1}}{q^{t_1+1}-q^{t_2}} \\
&\geq \frac{(q-1)q^{(d+e+1)+t_1+t_2-d-e}\mu^{t_1}}{q^{t_1+1}-q^{t_2}} \\
&= \frac{(q-1)q^{t_1+t_2+1}\mu^{t_1}}{q^{t_1+1}-q^{t_2}} \\
&\overset{(\dagger)}{\geq} \frac{(q-1)q^{t_1+0+1}\mu^{t_1}}{q^{t_1+1}-q^{0}} \\
&\geq \frac{(q-1)q^{t_1+1}\mu^{t_1}}{q^{t_1+1}-0} \\
&= (q-1)\mu^{t_1}.
\end{aligned}$$

Thus, $q^{t_1+t_2-e}\mu^{t_1}$ is at least $(q-1)\mu^{t_1}$ times as large as I. The inequality $(\dagger)$ holds because it is equivalent to $q^{2t_1+2}(q^{t_2}-1)/((q^{t_1+1}-1)(q^{t_2}-q^{t_1+1})) \leq 0$ and all four factors but $q^{t_2}-q^{t_1+1}$ are non-negative. This implies the left-hand side is non-positive. ■

We note that Theorem 4.19 continues to hold if $\mu = d+e+1$ is replaced by n. Thus, I is at least $(q-1)n^{t_1}$ times as good as $q^{t_1+t_2-e}n^{t_1} \leq q^{s-e}n^{t_1}$.

Our upper bound I demonstrates a proper improvement for all $q > 2$ since both ratios $(q-1)\mu^{t_1}$ are strictly greater than 1. If $q = 2$, then $n \leq 1$ and $e, d \leq 0$, i.e., the adversary cannot introduce faults. Thus, it is justified to say that our upper bound *always* yields a proper improvement.

5

Definitive Error Detection in the Double-Sharing Setting

In a follow-up paper, Arnold et al. [ABEO24] modify the framework proposed by Berndt et al. [BEF+23], which we covered in Chapter 4, to work with two secrets per sharing albeit considering only additive faults and non-adaptive adversaries.

We assume familiarity with the concepts used in [ABEO24] (and [BEF+23]). To recall the definition of fault-robustness, see Definition 4.1 on page 43. We remark that e and s are henceforth called σ and ω, respectively. We again denote by d and n the degree of a sharing polynomial and the number of parties, respectively. Throughout this chapter, we refer to a polynomial of degree *at most* d simply as a polynomial of degree d. Furthermore, the higher-order coefficients usually denote the coefficients of $x^{n-\sigma}, \dots, x^{n-1}$. Concerning the (input) polynomials f and g, we call the corresponding sharings $F := (F_i)_{i\in[0,n-1]}$ and $G := (G_i)_{i\in[0,n-1]}$ and their four secrets: s_0, s_1, s'_0, and s'_1. We embed the first secret in the lowest-degree coefficient and the second in the highest coefficient, where $s_{(\cdot)}$ and $s'_{(\cdot)}$ correspond to f and g, respectively, i.e., $s_0 = f_0$, $s_1 = f_d$, $s'_0 = g_0$, and $s'_1 = g_d$. Indices of sharings and parties are zero-based to be consistent with [ABEO24].

As observed by the authors, share-wise operations on f and g, i.e., linear ones, continue to function with double sharings. In particular, we have $\mathrm{coef}(af + bg, 0) = as_0 + bs'_0$ and $\mathrm{coef}(af + bg, d) = as_1 + bs'_1$, where $a, b \in \mathbb{F}$ are constants. Hence, we focus on non-linear operations.

In order to support different operations, as well as the combination and reordering of secrets, Arnold et al. introduce so-called (φ_0, φ_1)-*gadgets*. These gadgets operate on F and G and return a sharing $Q := (Q_i)_{i\in[0,n-1]}$ of a polynomial q of degree d such that $q_0 = \varphi_0(s_0, s_1, s'_0, s'_1)$ and $q_d = \varphi_1(s_0, s_1, s'_0, s'_1)$. Inside the φ-gadgets, the authors utilize ℓ-*functions* to set the coefficients q_0 and q_d, where $\ell_{i,j}^{(\varphi_0,\varphi_1)}(F_i, G_i)$ is the share of party i for party j of the polynomial $\varphi_0(s_0, s_1, s'_0, s'_1) + \varphi_1(s_0, s_1, s'_0, s'_1)x^d$. Recall that coefficients of, say, f, can be expressed using the inverse Vandermonde matrix as $f_k = \sum_{i=0}^{n-1} \lambda_{i,k} F_i$. In order to add f_k to x^m, i.e., to obtain the polynomial $f_k x^m$, party i can multiply its share of f_k by α_i^m. Due to distributivity, the sharing $\left(\sum_{i=0}^{n-1} \lambda_{i,k} F_i \alpha_j^m\right)_{j\in[0,n-1]}$ corresponds to $f_k x^m$.

Examples 5.1. We provide three instantiations of $\varphi = (\varphi_0, \varphi_1)$-functions together with their corresponding ℓ-functions. Further can be found in [ABEO24] on page 18.

1. $\varphi = (s_0 + s_0', 0)$: The ℓ-function is $\ell_{i,j}^{(\varphi_0,\varphi_1)}(F_i, G_i) = \lambda_{i,0}F_i + \lambda_{i,0}G_i$. Since s_0 and s_0' are the secrets at the constant terms f_0 and g_0, we extract them using $\lambda_{(\cdot),0}$ and add them.
2. $\varphi = (0, s_0 + s_0')$: The ℓ-function is $\ell_{i,j}^{(\varphi_0,\varphi_1)}(F_i, G_i) = (\lambda_{i,0}F_i + \lambda_{i,0}G_i)\alpha_j^d$. Multiplying by α_j^d adds the coefficient to q_d instead of q_0. Since $\alpha_j^0 = 1$, the term is omitted for φ_0.
3. $\varphi = (s_0 + s_1', 3s_1s_1')$: The ℓ-function is $\ell_{i,j}^{(\varphi_0,\varphi_1)}(F_i, G_i) = (\lambda_{i,0}F_i + \lambda_{i,d}G_i) + (3\lambda_{i,2d}(F_iG_i)\alpha_j^d)$. The coefficient $s_1s_1' = f_dg_d$ is at position $2d$ in fg. Due to linearity, we multiply by 3.

The sharing Q corresponds to a polynomial of degree d because ℓ-functions contribute only to coefficients q_0 and q_d, which in turn are added to random polynomials of degree d generated by ZEnc. More precisely, with $q(x) = \sum_{k=0}^{d} q_k x^k$, the coefficients of q are $q_0 = \varphi_0(s_0, s_1, s_0', s_1')$, $q_d = \varphi_1(s_0, s_1, s_0', s_1')$, and $q_k = \sum_{i=0}^{n-1} z_k^{(i)}$ for all $k \in [d-1]$, where $z^{(i)}$ is the polynomial corresponding to the ZEnc-sharing computed by party i during the execution of the φ-gadget.

The degree of q always being d implies that an adversary faulting F or G is never detected because the detection mechanism requires the degree of q to exceed d. To restrain the adversary from going unnoticed, the authors add an *error propagation polynomial* ρ to q. Its construction should guarantee that $q' := q + \rho$ equals q if no fault occurred (i.e., $\rho = 0$) and that otherwise, $\deg(q') > d$. They define ρ via the n-sharing that includes all σ higher-order coefficients of $f'g'$, namely, $(\mathrm{coef}(f'g', n-1), \dots, \mathrm{coef}(f'g', n-\sigma), 0, \dots, 0)$. To add ρ to q, the *error propagation term* $E_{i,j}F_i'G_i'$ is added to the ℓ-function during the computation, where $E_{i,j} = [\![j < \sigma]\!]\lambda_{i,n-j-1}$. Since f and g are polynomials of degree d, the degree of fg is $2d$, according to Fact 1.43. If $n > 2d + \sigma$, the *higher-order* terms at positions $n-\sigma, \dots, n-1$ all vanish if, and only if, f' and g' are valid. Here, $f' = f + \zeta^f$ and $g' = g + \zeta^g$ include the "potential" fault polynomials ζ^f and ζ^g, respectively.

As already noticed in [ABEO24], a fault pair (Z_i^F, Z_i^G) exists for each pair (F_i, G_i) of input shares such that $F_i'G_i' = F_iG_i$ because ρ uses the product $f'g'$. This means that all higher-order terms of $f'g'$ may vanish despite the adversary introducing faults. Suppose the φ-gadget computes a multiplication, such as (s_0s_0', s_1s_1'). In that case, the faulting is *ineffective* since $F_i'G_i' = F_iG_i$ implies $f'g' = fg$. Unfortunately, the faults can remain effective when the gadget uses different operations. An estimate calculated by the authors shows that due to the adversary being non-adaptive, the probability of him "guessing" the correct faults to remain unnoticed is at most $|\mathbb{F}|^{-\omega}$.

In the following, we present several approaches to mitigate the adversary's success probability of going undetected. Although not all approaches are suitable, we include them as they might be of independent use, e.g., in domains different from secret sharing and MPC.

We begin in Section 5.1 by using different error propagation terms depending on the operation the ℓ-function performs. However, it remains unclear how to deal with ℓ-functions that compute multiple operations.

In Section 5.2, we combine different error terms using addition to enable combining different operations. We ascertain that adding two error terms does not protect the operations but their sum. We ask whether there is an operation with no vanishing errors. However, we can only show that two generic operations *do* have vanishing errors. Combining the error terms differently, e.g., using multiplication, fails too.

Since combining error terms seems to fail, we consider the higher-order terms of f'

and g' separately in Section 5.3. We modify the φ-gadget by introducing two additional sharings, Q^f and Q^g. These include the higher-order coefficients of f' and g', respectively. By comparing the degrees of the polynomials corresponding to Q^f and Q^g with d, we *always* manage to detect whether f' or g' are invalid.

We present an alternative approach in Section 5.4, where we check the vector consisting of all higher-order coefficients of f' and g' for non-zero entries. We describe two strategies: On the one hand, parties randomize f' and g' before exchanging shares of both polynomials. This enables each party to reconstruct all higher-order terms without revealing the secrets. On the other hand, the higher-order coefficients are normalized and subtracted from 1 first. The corresponding polynomials can be multiplied when parties re-share the adjusted coefficients separately. Due to the aforementioned preprocessing, the embedded secret equals the product of the altered coefficients, which is 1 if, and only if, all higher-order terms are zero. However, it is tedious to re-share and combine all σ coefficients. It can even be undesirable to reconstruct polynomials.

In the attempt we pursue in Section 5.5, we try to truncate all lower-order terms using polynomial division. When dividing f' and g' by $x^{n-\sigma}$, all coefficients below $f'_{n-\sigma}$ and $g'_{n-\sigma}$, respectively, vanish. That way, any information about the secrets embedded in f and g is removed, and the parties can exchange shares directly. However, the framework we use to compute the division privately cannot function under standard secret sharing requirements since it allows parties to learn additional shares.

Finally, we present a working technique to truncate lower-order terms in Section 5.6. We utilize the Vandermonde matrix to transform a sharing of a polynomial into its coefficient vector. Using modified identity matrices allows us to alter the coefficient vector, particularly to zero the lower-order coefficients. Finally, the altered coefficient vector is transformed back so parties can obtain their new shares.

5.1 Approach 1: Gadget-Specific Error Propagation

We start with the idea of using distinct error propagation terms depending on the operation the φ-gadget performs. For instance, if the gadget performs a multiplication, such as $(\varphi_0, \varphi_1) = (s_1 s'_1, s_0 s'_0)$, the multiplicative error propagation originally proposed by Arnold et al. can be used. Likewise, if the gadget performs an addition, such as $(\varphi_0, \varphi_1) = (s_0 + s'_1, s_1 + s'_0)$, we can use the additive error propagation term $E_{i,j}(F_i + G_i)$ instead.

However, it is unclear how to choose the correct error term if different operations are combined. Consider, for instance, the gadget $(s_0 + s'_0, s_1 s'_1)$ with its corresponding ℓ-function $\lambda_{i,0}(F_i + G_i) + \lambda_{i,2d} F_i G_i \alpha_j^d$. The error terms corresponding to the polynomials $f + g$ and fg are $E_{i,j}(F_i + G_i)$ and $E_{i,j} F_i G_i$, respectively. We present one solution in the next Section 5.2.

Another drawback is that this approach is not unified, meaning that the error term must be adapted for distinct ℓ-functions. Besides, one has to manually fabricate new error terms for new ℓ-functions.

5.2 Approach 2: Additive Combination of Multiple Error Propagation

The approach presented in the previous Section 5.1 lacks composability. We assume the gadget combines the coefficients using different operations, such as addition and multiplication, and we now try combining the error terms corresponding to these operations. We consider the naïve approach to protect the combination by first computing both error terms and then merging them in an adequate way. In the case of addition, we have $E_{i,j}(F_i + G_i)$, whereas for multiplication, we have $E_{i,j}(F_iG_i)$. Since the original approach in [ABEO24] adds the error term to the ℓ-function, we proceed to do so with both terms. Accordingly, we obtain $\ell_{i,j}^{(\varphi_0,\varphi_1)}(F_i, G_i) + E_{i,j}(F_i + G_i) + E_{i,j}(F_iG_i)$, with distributivity implying $E_{i,j}(F_i + G_i) + E_{i,j}(F_iG_i) = E_{i,j}(F_i + G_i + F_iG_i)$. Thus, the added error terms protect the polynomial $f + g + fg$ rather than $f + g$ and fg. In order for the higher-order terms of $f' + g' + f'g'$ to be 0, we require

$$(F_i + Z_i^F) + (G_i + Z_i^G) + (F_i + Z_i^F)(G_i + Z_i^G) = F_i + G_i + F_iG_i.$$

Equality holds if, e.g.,

$$Z_i^G = -\frac{(G_i + 1)Z_i^F}{F_i + 1 + Z_i^F}. \tag{5.1}$$

It is easy to see that choosing faults Z_i^F and Z_i^G such that Equation 5.1 holds does not render the fault on either $f' + g'$ or $f'g'$ ineffective. Consequently, both coefficients q_0 and q_d are incorrect, although $\deg(q') \leq d$.

It is natural to ask whether some algebraic operation $\diamond$ on f and g exists such that the higher-order coefficients of $f' \diamond g'$ are 0 if, and only if, the adversary introduces no faults into the computation, e.g., if $f' \diamond g' = f \diamond g$. We call such an operation *perfect*, i.e., if for all strategies that the adversary can use to fault f and g, the function $f' \diamond g'$ is invalid. Such operation must also be computable using sharings of f and g. To this end, with faulted shares $F_i' = F_i + Z_i^F$ and $G_i' = G_i + Z_i^G$, we can treat the original shares F_i and G_i as constants (or parameters) and the faults Z_i^F and Z_i^G as variables. We follow the approach to achieve $(F_i + Z_i^F) \diamond (G_i + Z_i^G) \stackrel{!}{=} F_i \diamond G_i$. By subtracting the right-hand side from the left-hand side, it becomes clear that we are interested in the non-trivial zeros of the bivariate function

$$\beta_\diamond := \beta_{\diamond,F_i,G_i} \colon (Z_i^F, Z_i^G) \mapsto ((F_i + Z_i^F) \diamond (G_i + Z_i^G)) - (F_i \diamond G_i).$$

If we proved that for every appropriate $\beta_\diamond$, i.e., operation $\diamond$, a non-trivial zero exists, this would imply that no perfect $\diamond$ exists. As we assume the underlying field to be arbitrary, a non-trivial zero must exist for all $\mathbb{F}_q$. However, requiring a non-trivial zero to exist for *some* field $\mathbb{F}_q$ could also suffice, depending on the scenario. In any case, the choice of possible $\beta_\diamond$ depends on the operations applicable to polynomials that can also be computed with sharings.

In what follows, we assume $\diamond$ is a composition of only addition, multiplication, and squaring. Thus, $\beta_\diamond$ is a polynomial. We recall that given a share F_i of f, it is possible to locally transform F_i into a share of the "linear" transformation $af + b$. We already know

the operations addition and multiplication are not perfect because non-vanishing faults exist for both operations if the gadget performs a different one. Consequently, neither is squaring because it can be reduced[8] to multiplication. It follows that neither of the above is perfect when f and g are transformed "linearly" beforehand. Since we assume $n > 2d$, we cannot square f or g *and* multiply the result by the respective other polynomial. We can, however, add the resulting polynomials.

We now consider two "generic" operations and state vanishing faults for each. In this way, we show that many operations are unsuitable for $\diamond$. Let $a_1, a_2 \in \mathbb{F}^*$, $b_1, b_2 \in \mathbb{F}$, and $c_1, c_2 \in \{1, 2\}$. The $c_{(\cdot)}$ serve as exponents. We restrict ourselves to the two values in $\{1, 2\}$ because, on the one hand, a value greater than two can cause the parties to no longer be able to reconstruct the polynomial. On the other hand, if $c_{(\cdot)} = 0$, a constant value is added because the addend is 1 or $a_2 + b_2$, depending on the operation.

1. The operation $(a_1 f + b_1)^{c_1} + (a_2 g + b_2)^{c_2}$ has the vanishing faults

$$c_1 = 1, c_2 = 2: \quad Z_i^F = -\frac{a_2 Z_i^G (2(a_2 G_i + b_2) + a_2 Z_i^G)}{a_1} \ \wedge \ Z_i^G \neq 0$$
$$c_1 = 2, c_2 = 2: \quad Z_i^F = 0 \ \wedge \ Z_i^G = -\frac{2(a_2 G_i + b_2)}{a_2} \ \wedge \ a_2 G_i + b_2 \neq 0.$$

   Note that Z_i^F and Z_i^G can be swapped by substituting a_2, b_2, and G_i with a_1, b_1, and F_i, respectively.
2. The operation $(a_1 f^{c_1} + b_1) + (a_2 g^{c_2} + b_2)$ has the vanishing faults

$$c_1 = 1, c_2 = 2: \quad Z_i^F = -\frac{a_2 Z_i^G (2G_i + Z_i^G)}{a_1} \ \wedge \ Z_i^G \neq 0$$
$$c_1 = 2, c_2 = 2: \quad Z_i^F = -2F_i \ \wedge \ Z_i^G \in \{0, -2G_i\}.$$

We omit the case $c_1 = 2 \wedge c_2 = 1$ due to commutativity.

Unfortunately, due to a shortage of time, we are not able to show (or refute) that all appropriate bivariate polynomials $\beta_\diamond$ have non-trivial zeros over all (or some) fields $\mathbb{F}_q$. However, we mention the following fact for *univariate* polynomials, which perhaps also applies to bivariate polynomials in some related way:

Fact 5.2 ([Hie24]). For all $\mathbb{F}_q$ and for all non-constant irreducible univariate polynomials p over $\mathbb{F}_q$, there exists an extension field such that p has a zero in it, namely, $\mathbb{F}_q[x]/\langle p\rangle$ with zero $x + \langle p\rangle$, where $\langle p\rangle$ denotes the ideal generated by p. Moreover, there exists exactly[9] one extension field in which p splits, namely, $\mathbb{F}_{q^{\deg(p)}}$.

We may assume irreducibility since if p is reducible, it has two non-trivial factors. According to the zero-product property, it is sufficient to examine these factors instead.

The above fact implies that the splitting field is different from $\mathbb{F}_q$ unless $\deg(p) = 1$, in which case p is linear and obviously splits over $\mathbb{F}$. Regarding the mentioned extension field, Definition 1.11 implies that the ideal $\langle p\rangle$ equals the product of all $p' \in \mathbb{F}[x]$ by p.

[8] Use the non-trivial fault $Z_i^F = -2F_i$.
[9] Up to isomorphism.

Hence, $x + \langle p \rangle \notin \mathbb{F}_q$ is not a suitable zero either. We stress that the above does not necessarily have to hold for bivariate polynomials.

For the remainder of this section, we consider two alternative methods of combining multiple error terms.

As additively combining both error terms, say, $E_{i,j}\varepsilon_1$ and $E_{i,j}\varepsilon_2$, is only one option, we now consider multiplying them. We then need to use $\sqrt{E_{i,j}}$ instead of $E_{i,j}$. The product of both error terms equals $\left(\sqrt{E_{i,j}}\varepsilon_1\right)\left(\sqrt{E_{i,j}}\varepsilon_2\right) = E_{i,j}\varepsilon_1\varepsilon_2$. As can be seen, the error terms are multiplied instead of being added. If we continue to use the previous two error terms, $\varepsilon_1 = F_i + G_i$ and $\varepsilon_2 = F_iG_i$, the polynomial corresponding to $\varepsilon_1\varepsilon_2$ is $f^2g + fg^2$. Since the degree of f and g is likely to be exactly d, the degree of the combined polynomial can exceed $2d$, so parties cannot reconstruct the secrets. Because it is reasonable that one involved operation is multiplication-like, this approach does not work.

Finally, we multiply the error terms by the ℓ-function instead of adding them. Regardless of the operation $\circ$ used to combine the error terms with (e.g., $\circ \in \{+, \cdot\}$), the multiplication yields $Q_j(1 + E_{i,j}(\varepsilon_1 \circ \varepsilon_2)) = Q_j + Q_jE_{i,j}(\varepsilon_1 \circ \varepsilon_2)$. The share Q_j remains unaltered if no fault is introduced since $Q_jE_{i,j} \cdot 0 = 0$. However, the contrary does not need to hold because $Q_j = 0$ causes the product to vanish. Thus, this approach does not work either.

5.3 Approach 3: Separate Error Propagation

In this section, we present a comparison-based approach that *always* detects if the adversary faults F or G and returns an (in)valid sharing accordingly. Unlike Section 5.2, we no longer combine error propagation terms but evaluate them separately. We modify the original φ-gadget proposed by Arnold et al. [ABEO24]. More precisely, each party holds three shares instead of one *during* computation: The first share corresponds to the unmodified sharing Q, and the remaining two include the error terms. Instead of adding $E_{i,j}F_iG_i$ to Q_j, parties add the error terms, e.g., $E_{i,j}(F_i + G_i)$ and $E_{i,j}F_iG_i$, to the last two shares separately and reconstruct the underlying polynomials. We thereby ascertain if all higher-order terms vanish.

If we use the above example error functions $F_i + G_i$ and F_iG_i, which correspond to $f + g$ and fg, respectively, it is again possible for the adversary to choose vanishing faults, namely, $Z_i^F = G_i - F_i$ and $Z_i^G = F_i - G_i$. It is, hence, essential to use error terms corresponding either to the two operations of the φ-gadget since this renders faults ineffective or to operations such that higher-order terms cannot vanish.

We pursue the latter approach because it is independent of the underlying ℓ-function and avoids the drawback of the approach in Section 5.1, namely, the approach not being unified. Let Q_j continue to be the j^{th} share of the unmodified output sharing Q without any error propagation. Also, recall that $\tilde{Q}_i$ is party i's sharing of a random polynomial generated by ZEnc. The share for party j is denoted by $\tilde{Q}_{i,j}$. The j^{th} shares of the other two sharings, say, Q^f and Q^g, consist of the sum of n ZEnc shares and the $(n-1-j)^{\text{th}}$

higher-order coefficients of f' and g', respectively. In particular, it holds that

$$Q_j^f = \sum_{i=0}^{n-1} (\tilde{Q}_{i,j}^f + E_{i,j} F_i') = \sum_{i=0}^{n-1} \tilde{Q}_{i,j}^f + \begin{cases} f'_{n-j-1} & \text{if } j \in [0, \sigma-1] \\ 0 & \text{else,} \end{cases}$$

$$Q_j^g = \sum_{i=0}^{n-1} (\tilde{Q}_{i,j}^g + E_{i,j} G_i') = \sum_{i=0}^{n-1} \tilde{Q}_{i,j}^g + \begin{cases} g'_{n-j-1} & \text{if } j \in [0, \sigma-1] \\ 0 & \text{else.} \end{cases}$$

As can be seen, we do not add the ℓ-function to either Q_j^f or Q_j^g since this saves ij additions and makes no difference to the error detection. The updated φ-gadget from [ABEO24] is presented in Algorithm 5.1. Our changes are as follows: In lines 4 and 5, we initialize

Algorithm 5.1 (φ_0, φ_1)-Gadget With Guaranteed Fault Detection

Input: Degree-d shares of s_0, s_1 as F and shares of s_0', s_1' as G.
Output: Degree-d shares of $q_0 = \varphi_0(s_0, s_1, s_0', s_1'), q_d = \varphi_1(s_0, s_1, s_0', s_1')$ as Q.

1: initialize Q_j, Q_j^f, Q_j^g
2: **for** $i = 0$ **to** $n-1$ **do**
3: $\quad (\tilde{Q}_{i,0}, \dots, \tilde{Q}_{i,n-1}) \leftarrow \mathsf{ZEnc}_n^d$
4: $\quad (\tilde{Q}_{i,0}^f, \dots, \tilde{Q}_{i,n-1}^f) \leftarrow \mathsf{ZEnc}_n^d$
5: $\quad (\tilde{Q}_{i,0}^g, \dots, \tilde{Q}_{i,n-1}^g) \leftarrow \mathsf{ZEnc}_n^d$
6: $\quad$ **for** $j = 0$ **to** $n-1$ **do**
7: $\quad\quad Q_j \leftarrow Q_j + \tilde{Q}_{i,j} + \ell_{i,j}^{(\varphi_0,\varphi_1)}(F_i, G_i)$
8: $\quad\quad Q_j^f \leftarrow Q_j^f + \tilde{Q}_{i,j}^f + E_{i,j} F_i$
9: $\quad\quad Q_j^g \leftarrow Q_j^g + \tilde{Q}_{i,j}^g + E_{i,j} G_i$
10: reconstruct $\hat{f}$ from Q^f and $\hat{g}$ from Q^g
11: **if** $\deg(\hat{f}) > d$ or $\deg(\hat{g}) > d$ **then**
12: $\quad p \leftarrow\!\!\$\ \mathcal{P}_{\leq n-1} \setminus \mathcal{P}_{\leq n-\sigma-1}$
13: $\quad P \leftarrow (p(\alpha_i))_{i \in [0,n-1]}$
14: $\quad$ **return** $(P_0, \dots, P_{n-1})$
15: **return** $(Q_0, \dots, Q_{n-1})$

random sharings to protect the shares F_i and G_i in Q_j^f and Q_j^g, respectively. The sharings may correspond to any random polynomials of degree d and need not necessarily originate from ZEnc. In lines 8 and 9, we add the error propagation terms to Q_j^f and Q_j^g. Once each party i has obtained its shares Q_i^f and Q_i^g, parties exchange them to reconstruct the corresponding polynomials $\hat{f}$ and $\hat{g}$ in line 10. The polynomials do not include sensitive information because Q_j^f and Q_j^g only include information from random polynomials and the coefficients of ζ^f and ζ^g. Then, in line 11, the parties validate if the degrees of $\hat{f}$ or $\hat{g}$ exceed d, i.e., if $\hat{f}$ or $\hat{g}$ is invalid. We later argue that this is the case if, and only if, the adversary introduced faults. If both polynomials are valid, the original sharing Q is returned. Otherwise, parties sample a random polynomial p of degree at least $n - \sigma$ and return the sharing P corresponding to p in lines 12–14.

We must now prove that the sharing returned by Algorithm 5.1 is valid and includes

the correct secrets if no faults were introduced. Otherwise, the output sharing must be invalid. In any case, no information about the secrets may be deduced.

Observation 5.3. After leaving the first (outer) for-loop, i.e., when line 10 is reached, it holds that $Q^\chi = (\sum_{i=0}^{n-1} \tilde{Q}^\chi_{i,0}, \dots, \sum_{i=0}^{n-1} \tilde{Q}^\chi_{i,n-1}) + (\chi'_{n-1}, \dots, \chi'_{n-\sigma}, 0, \dots, 0)$, where $\chi \in \{f, g\}$.

We prove the aforementioned claims in three steps: In Lemma 5.4, we show that the sharing returned by Algorithm 5.1 is valid if, and only if, the adversary introduced no faults. The only-if part is equivalent to saying that f' and g' are valid. Then, in Lemma 5.5, we prove that if the returned sharing is valid, the secrets embedded in the corresponding polynomial are correct, i.e., as specified by φ_0 and φ_1. It remains to show that parties do not learn sensitive information about the secrets (or shares of F and G) during the computation or by the returned sharing. We show this in Lemma 5.6.

Lemma 5.4. *Algorithm 5.1 returns a valid sharing if, and only if, f' and g' are valid.*

Proof. Recall that f' and g' are valid if, and only if, $f' = f$ and $g' = g$, respectively. Also, the unmodified output sharing Q corresponds to a polynomial of degree d because it remains as originally specified in [ABEO24]. Thus, the output sharing can only be invalid if a sharing different from Q is returned. This only happens in line 14. We show that line 14 is reached if, and only if, the adversary faults F or G, in which case f' or g' becomes invalid. Thus, the returned sharing is valid if, and only if, $f' = f$ and $g' = g$, i.e., if no faults were introduced.

Line 14 is reached if, and only if, $\hat{f}$ or $\hat{g}$ is invalid. W.l.o.g., we only consider $\hat{f}$: According to Observation 5.3, $\hat{f}$ is the sum of n polynomials of degree d and the polynomial, say, u^f, corresponding to the higher-order coefficients of f'. Thus, the sharing U^f corresponding to the latter polynomial u^f equals $U^f = (f'_{n-1}, \dots, f'_{n-\sigma}, 0, \dots, 0)$. Since $n > d + \sigma$, the sharing U^f is zero if, and only if, the adversary did not fault any F_i (i.e., $F' = F$ or $f' = f$). This implies that the degree of $\hat{f}$ is d if no fault was introduced and, otherwise, is at least $n - \sigma$. Since the if-condition in line 11 uses d as the degree threshold, we conclude that line 14 is reached if, and only if, $f' \neq f$ or $g' \neq g$.

We already argued above that Q corresponds to a valid polynomial. Thus, it remains to show that P does not. The sharing P corresponds to the random polynomial chosen in line 12, whose degree is at least $n - \sigma$ by specification. Accordingly, P corresponds to an invalid polynomial since $d < n - \sigma$. ■

Next, we show that any valid sharing returned by Algorithm 5.1 includes the correct secrets. Roughly speaking, this is implied by [ABEO24] because we do not alter the specification of Q in our modified algorithm.

Lemma 5.5. *If Algorithm 5.1 returns a valid sharing Q, the embedded secrets corresponding to the polynomial of Q are as specified by φ_0 and φ_1, i.e., $q_0 = \varphi_0(s_0, s_1, s'_0, s'_1)$ and $q_d = \varphi_1(s_0, s_1, s'_0, s'_1)$.*

Proof. According to Lemma 5.4, the output sharing is valid if, and only if, the adversary did not introduce faults. This is equivalent to Algorithm 5.1 returning Q and not P. We know Q is returned since we assume that the output sharing is valid. Its shares Q_j are composed of the operation in line 7 and are not altered afterward. The operation in line 7 is identical to the one in the original φ-gadget from [ABEO24]. The claim follows since Arnold et al. proved the correctness of the original φ-gadget. ■

Through the two previous lemmata, we showed the correctness of Algorithm 5.1 and that it always detects if the adversary faulted F or G. It is left to show that the modifications we introduced in Algorithm 5.1 do not allow an adversary to extract sensitive information. To this end, we argue that the original gadget from Arnold et al. is secure and that our modifications mainly consist of computing three, instead of one, ℓ-functions.

Lemma 5.6. *From and during the computation of Algorithm 5.1, an adversary can only deduce information about the secrets, F, or G, that he can already deduce from the original φ-gadget in [ABEO24].*

Proof. We show that, for one thing, parties do not exchange data from which sensitive information can be deduced, and for another thing, that the output sharing reveals nothing sensitive.

Regarding the former, we analyze all places where the sensitive shares F_i and G_i are used. As can be seen, the shares are used only for Q_j, Q_j^f, and Q_j^g in lines 7–9. Note that no party i sends the result of the ℓ-function, $E_{i,j}F_i$, or $E_{i,j}G_i$ directly and individually to party j. Instead, they add $\tilde{Q}_{i,j}$, $\tilde{Q}_{i,j}^f$, and $\tilde{Q}_{i,j}^g$ to them, respectively, beforehand. Observe that the terms $E_{i,j}F_i$ and $E_{i,j}G_i$ can be interpreted as ℓ-functions. Because the Q_j reveal no sensitive information about F_i or G_i, as shown in [ABEO24], neither do $\tilde{Q}_{i,j}^f$ and $\tilde{Q}_{i,j}^g$. We stress that this no longer holds if we use *the same* "masking" shares in lines 3–5.

Next, we show that neither $\hat{f}$ nor $\hat{g}$ includes sensitive information. As before, we only analyze $\hat{f}$: According to Observation 5.3, $\hat{f}$ corresponds to the sum of the n random polynomials specified by $\tilde{Q}_0^f, \dots, \tilde{Q}_{n-1}^f$ and the polynomial specified by the sharing $(f'_{n-1}, \dots, f'_{n-\sigma}, 0, \dots, 0)$. Since $d < n - \sigma$, the higher-order terms of f' equal those of ζ^f. Thus, $(f'_{n-1}, \dots, f'_{n-\sigma}, 0, \dots, 0) = (\zeta^f_{n-1}, \dots, \zeta^f_{n-\sigma}, 0, \dots, 0)$. Neither ζ^f nor any of the $\tilde{Q}_i^f$ include any information about f: The error polynomial ζ^f is independent of f since it corresponds to the sharing of faults added to F by the adversary, who is non-adaptive. Also, $\tilde{Q}_i^f$ is generated using ZEnc, which, by definition, samples a random polynomial without constant term from $\mathcal{P}_{\leq d-2}$. This procedure is independent of f and the secrets.

Finally, we argue that no output sharing reveals sensitive information. According to [ABEO24], the original sharing Q does not. Neither does P because it corresponds to a random polynomial. ■

We have proven all the necessary facts above. Thus, we can state the complete theorem that combines all three results.

Theorem 5.7. *The sharing returned by Algorithm 5.1 is valid if, and only if, the adversary introduces no faults into the computation. Further, any valid output sharing is correct, i.e., it embeds the secrets specified by φ_0 and φ_1. Moreover, the adversary learns nothing about the secrets embedded in f and g, neither during the computation nor from the output sharing.*

Proof. The theorem follows immediately from combining Lemmata 5.4, 5.5, and 5.6. ■

We remark that instead of replacing Q with P in case a fault occurs, we initially considered returning a modified Q as follows: If $\hat{f}_{n-i-1} \neq 0$ or $\hat{g}_{n-i-1} \neq 0$, where $i \in [0, \sigma-1]$, we add a random non-zero value to Q_i. Since at least one, but at most σ higher-order terms do not vanish, between one and σ entries in Q are modified. Thus, the modified

sharing Q' corresponds to a polynomial of degree at least $n-\sigma$, which is invalid. The problem with this approach is that if the adversary faults, say, F, such that only one higher-order coefficient of f' is non-zero, we replace only one share, e.g., Q_0. If the adversary subsequently faults the modified share Q'_0, the probability that he reverts to the original value of Q'_0 is q^{-1}. If the adversary were adaptive, the probability would increase to $1/(q-1)$ since he knows that $Q_0 \neq Q'_0$ by probing Q'_0. In any case, he turns Q' into a valid sharing with incorrect secrets. He might also deduce further information about Q since Q'_0 is not distributed uniformly over $\mathbb{F}$.

There are, of course, more alternatives to replace Q with an invalid Q' in case a fault occurs. For instance, we can return $Q + (1, 0, \dots, 0)$, Q^f in case $\deg(\hat{f}) > d$, or Q^g in case $\deg(\hat{g}) > d$. However, we strongly advise against using these alternatives because each enables the adversary to trivially transform the output sharing Q' back into a valid one. In general, the adversary can take advantage of such "deterministic" invalid sharings in subsequent computations because the higher-order terms of the corresponding output polynomial are no longer random, let alone uniformly distributed. This is not the case for the original multiplicative error term $E_{i,j}F_iG_i$ of [ABEO24] since the higher-order terms of the product $f'g'$ are indeed random from the view of an adversary (see Chapter 4 on page 43).

5.4 Approach 4: Indicator-Function-Based Error Detection

Although we presented an always-detecting solution in the previous Section 5.3, we elaborate on further ways to detect invalid sharings, e.g., when it is undesirable or impossible to reconstruct polynomials during the computation of the φ-gadget.

Let $C = (f'_{n-\sigma}, \dots, f'_{n-1}, g'_{n-\sigma}, \dots, g'_{n-1})$ be the vector consisting of the higher-order coefficients of f' and g'. The idea is to compare C with the zero vector $0^{2\sigma}$ to ascertain if all higher-order coefficients are 0 [ABO24]. More precisely, we aim to *privately* compute the predicate $\tau(C) := [\![C \neq 0^{2\sigma}]\!]$, which is 0 if all coefficients are zero and, say, 1 otherwise.

If the coefficients in C were Boolean, τ would precisely represent the logical OR function, that is, $\tau(C) = \bigvee_{c \in C} c \equiv \neg \bigwedge_{c \in C} \neg c$. As we use arithmetic circuits and values over some finite field $\mathbb{F}_q$, associating the Boolean constants $\bot$ and $\top$ with $0, 1 \in \mathbb{F}_2$ allows evaluating Boolean circuits by arithmetical ones as follows: Evaluate $\neg a$ and $a \wedge b$ by computing $1 - a$ and ab, respectively. Using this minimal functionally complete set consisting of negation and conjunction, we need not reduce results over $\mathbb{F}_q$.

Hence, it seems prudent to compute τ by

$$1 - \prod_{c \in C} (1 - c) = 1 - \prod_{k=n-\sigma}^{n-1} \left((1 - f'_k)(1 - g'_k) \right). \tag{5.2}$$

Unfortunately, if $q > 2$, the result in Equation 5.2 does not need to equal $\tau(C)$ because the values $c \in C$ can be different from 0 and 1. This causes $\tau(C)$ to be 0, even though f' or g' is invalid: If all c are equal to 0, the result is 0, as expected since $1 - \prod_c (1-0) = 1 - 1 = 0$. If there exists $c \neq 0$, the product should be 0 (or at least take a value different from 1). However, this is not always the case:

Counterexample 5.8. Let all c be 2. Then[10], $\prod_c (1-c) = \prod_c (-1) = (-1)^{|\mathcal{C}|} = 1$ since $|\mathcal{C}| = 2\sigma$ is even.

To circumvent this problem, we can *normalize* the coefficients in $\mathcal{C}$. To normalize an element $v \in \mathbb{F}_q$, i.e., compute $\operatorname{sgn}(v) := [\![v \neq 0]\!]$, *Fermat's little theorem* gives a possible way if q is prime.

Theorem 5.9. *Let $\eta(v) = v^{q-1} \bmod q$ and assume that $q \in \mathbb{P}$. For all $v \in \mathbb{F}_q$, it holds that $\eta(v) = \operatorname{sgn}(v)$.*

Proof. If $v = 0$, we have $\eta(v) = 0^{q-1} = 0 = \operatorname{sgn}(0)$ as $q > 1$. Since q is prime, it holds that $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. Accordingly, q and every $v \neq 0$ are coprime. Fermat's little theorem implies $v^{q-1} \equiv 1 \pmod q$, i.e., $\eta(v) = 1 = \operatorname{sgn}(v)$. ∎

Consequently, we are able to compute τ as follows:

$$\tau(\mathcal{C}) = 1 - \prod_{c \in \mathcal{C}} (1 - \eta(c)) = 1 - \prod_{k=n-\sigma}^{n-1} \left((1 - {f'_k}^{q-1})(1 - {g'_k}^{q-1}) \right). \tag{5.3}$$

For finite fields in general, field elements can be raised to the power of $\lambda(q)$, where λ is the *Carmichael function*. For the remainder of this section, we use $q-1$ instead of $\lambda(q)$.

However, how to *efficiently* evaluate τ remains unclear because we assume we know f'_k and g'_k in Equation 5.3. The obvious way is that parties interactively obtain these coefficients and thereby construct $\mathcal{C}$. But in this case, they can simply check if $\mathcal{C} = 0$, need not evaluate τ, and save computing several multiplications and exponentiations. Suppose the coefficients are obtained by exchanging $\lambda_{i,k} F_i$ and $\lambda_{i,k} G_i$ (or directly using F_i and G_i). In that case, it is necessary to re-randomize the sharings beforehand to erase the secrets, e.g., by adding random polynomials of degree d. We described this approach in Algorithm 5.1 in the previous Section 5.3.

We now consider evaluating τ using the parties' shares F_i and G_i such that the value $\tau(\mathcal{C})$ is embedded in one of the secrets of some polynomial. This enables the parties to recover $\tau(\mathcal{C})$ by reconstructing said coefficient.

According to Equation 5.3, parties first need to attain shares of ${f'_k}^{q-1}$ and ${g'_k}^{q-1}$. We mention that parties cannot simply raise their shares to the power of $q-1$ as this does not result in the coefficients being raised to said power. Using repeated multiplication, e.g., exponentiation by squaring, to obtain shares of ${f'}^{q-1}$ and ${g'}^{q-1}$ does not work either because multiplying invalid polynomials can lead to a degree overflow and a consequential loss of information. Even if no overflow occurs, the higher-order terms are "garbled" and, due to (several) degree reductions, not preserved either. Hence, parties must first re-share f'_k and g'_k to raise them to a higher power.

Assume $f'_k = s_0$ and $g'_k = s_1$ have been re-shared in one polynomial with the corresponding sharing $D^{(k)} := (D_i^{(k)})_{i \in [0, n-1]}$. Using exponentiation by squaring, the sharing of a polynomial that includes the normalized coefficients ${f'_k}^{q-1}$ and ${g'_k}^{q-1}$ can be computed using the ℓ-functions $(s_0^2, s_1^2) = ({f'_k}^2, {g'_k}^2)$ and $(s_0 f'_k, s_1 g'_k)$ on $D^{(k)}$ repeatedly.

Let $\overline{D}^{(k)}$ denote the sharing that embeds the normalized coefficients $s_0 = {f'_k}^{q-1}$ and $s_1 = {g'_k}^{q-1}$. Before parties can compute the product of all σ normalized higher-order

[10] Recall that $-1 \equiv q - 1 \pmod q$.

coefficients, they must transform s_0 and s_1 into $1 - s_0$ and $1 - s_1$. This can be accomplished by negating shares and adding 1. Negating the shares $\overline{D}_i^{(k)}$ negates the secrets because the underlying polynomial is negated. To add 1 to $-s_0$ and $-s_1$, respectively, parties add $\alpha_i^0 = 1$ and α_i^d to their shares. Thus, they apply the mapping $\overline{D}_i^{(k)} \mapsto 1 + \alpha_i^d - \overline{D}_i^{(k)}$.

Now that parties possess shares of the polynomial embedding the transformed normalized coefficients, they can compute the product in Equation 5.3. It then holds that $s_0 = \prod_k (1 - {f'_k}^{q-1})$ and $s_1 = \prod_k (1 - {g'_k}^{q-1})$.

Finally, it is left to subtract the negated products from 1. Additionally, we merge the products into one secret, in our case, into the first. To this end, we employ the ℓ-function $(1 - s_0 s_1, 0)$. The coefficient of the constant term equals $\tau(C)$, which parties can reconstruct. Alternatively, instead of adding the secret to the constant term, it can be added to any higher-order term, e.g., at position $n - \sigma$. In this case, the polynomial is valid if, and only if, $C = 0^{2\sigma}$, i.e., if the adversary introduced no faults.

Due to the computationally expensive operations that accompany computing τ, such as re-sharing all σ higher-order coefficients, we present more efficient approaches in Sections 5.5 and 5.6.

5.5 Approach 5: Division-Based Truncation of All Lower-Order Terms

The approach we pursue in this section and the following Section 5.6 is to truncate all but the higher-order terms of f' and g'. We then know that a polynomial is valid if, and only if, it is the zero polynomial (i.e., corresponds to the zero sharing).

In this section, we attempt to use polynomial division to privately compute the quotients $f' \div x^{n-\sigma}$ and $g' \div x^{n-\sigma}$, which include no lower-order terms. Here, $\div$ denotes polynomial division with remainder. Thus, the quotient of two polynomials remains a polynomial. A division by $x^{n-\sigma}$ "shifts" the coefficients by $n - \sigma$ positions to the left non-circularly. The resulting polynomials are, hence, of degree $(n-1) - (n-\sigma) = \sigma - 1 < n$. After performing the division, parties can exchange their shares and reconstruct both polynomials to see if they equal the zero polynomial. This can also be deduced directly from the sharing because only the zero sharing corresponds to the zero polynomial. However, our approach to computing polynomial division cannot work in the general context of MPC since it allows a party to learn further shares. We will elaborate on that later on.

Firstly, we show that the quotient polynomials are zero if, and only if, the adversary did not introduce faults. This follows from observing that the quotient comprises precisely the higher-order terms.

Theorem 5.10. *The polynomials $f' \div x^{n-\sigma}$ and $g' \div x^{n-\sigma}$ are zero if, and only if, f' and g' are valid, respectively.*

Proof. W.l.o.g., we consider f'. If f' is valid, its degree is d. Then, $f' \div x^{n-\sigma} = 0$ since $d < n - \sigma$. If f' is invalid, there exists $k \in [0, \sigma - 1]$ such that $f'_{n-\sigma+k} \neq 0$. This coefficient is shifted to position $(n - \sigma + k) - (n - \sigma) = k \geq 0$ and, hence, $f' \div x^{n-\sigma}$ cannot be zero. ∎

Next, we prove that it is safe for parties to exchange shares of the truncated polynomials. The truncated polynomials reveal nothing about the lower-order terms since all

coefficients less than or equal to d are removed, and the higher-order terms are independent of f and g.

Theorem 5.11. *The polynomials $f' \div x^{n-\sigma}$ and $g' \div x^{n-\sigma}$ include no information about the secrets embedded in f and g, respectively.*

Proof. W.l.o.g., we consider f'. Recall that $f' = f + \zeta^f$ and that the degree of f is d, whereas the degree of ζ^f is at least $n - \sigma$ (or $\zeta^f = 0$). Since all higher-order terms of f are 0, it holds that

$$f'_k \triangleq \operatorname{coef}(f + \zeta^f, k) = \begin{cases} f_k + \zeta^f_k & \text{if } k \in [0, d] \\ \zeta^f_k & \text{if } k \in [d+1, n-1]. \end{cases}$$

Because $d < n - \sigma$ and a division by $x^{n-\sigma}$ eliminates all coefficients less than $n - \sigma$, every coefficient of f vanishes. It follows that $f'(x) \div x^{n-\sigma} = \sum_{k=0}^{\sigma-1} \zeta^f_{k+(n-\sigma)} x^k$. We conclude that as ζ^f is independent of the secrets embedded in f, so is $f' \div x^{n-\sigma}$. ■

In order to privately compute polynomial division, we planned on using the approach by Mohassel and Franklin [MF06], which does not require interaction. They use the fact that for any polynomial p of degree δ, the polynomial $x^\delta p(1/x)$ corresponds to p with reversed coefficients. For instance, if $p(x) = 1+2x+3x^2$, then $x^2 p(1/x) = 3+2x+1x^2$. With reversed coefficients, the authors are able to truncate all higher-order terms of p by reducing the reversed polynomial modulo $x^{n-\sigma}$, which removes all but the *lowest* $n - \sigma$ terms. It, therefore, holds that the coefficients removed in $p(x) \div x^{n-\sigma}$ and $x^\delta p(1/x) \bmod x^{n-\sigma}$ are the same. Finally, they reverse the reduced polynomial once more to return the coefficients to their initial order. We can, however, omit this last step because we are only interested in whether or not the reduced polynomial is zero. We remark that since the exact degrees of f' and g' (and especially of f and g) are unknown, it is possible to use $\delta = n - 1$ instead of $\delta = \deg(f')$ and $\delta = \deg(g')$.

Mohassel and Franklin assume the so-called *shared-coefficients model*, where coefficients are shared *individually*. Both previously mentioned operations can be computed privately and without interaction (i.e., *locally*) in said model.

Fact 5.12 ([MF06]). Given a share of a polynomial p of degree δ, it is possible to locally obtain shares of the polynomials $x^\delta p(1/x)$ and $x^\delta p(1/x) \bmod x^\delta$, respectively, in the shared-coefficients model.

We now argue that this approach cannot work for MPC-related applications when we assume the "standard" secret-sharing model as described in Fact 1.57. First of all, reversing coefficients becomes trivial if parties can interact with each other and do not have to use polynomial division. For instance, they employ the anti-diagonal matrix in the approach described in Section 5.6. On the other hand, the local case is more complicated. If we assume x^δ to be publicly known, the obvious approach is trying to transform a share of $p(x)$ into one for $p(1/x)$ and then multiply by the share of x^δ, namely, α_i^δ. This, however, cannot work as it allows a party to learn a further share and, hence, less than d parties suffice to reconstruct the polynomial [ABO24]. More precisely, party i possessing its share $p(\alpha_i)$ then learns the share $p(\alpha_i^{-1})$, which corresponds to a different node if $\alpha_i \neq 1$.

Furthermore, a party must not even obtain a share of the completely reversed polynomial $x^\delta p(1/x)$ because it again enables them to deduce the second share $p(\alpha_i^{-1})$ as follows: To transform the reversed polynomial $x^\delta p(1/x)$ back to $p(1/x)$, we multiply by $x^{-\delta}$. We stress that we may consider $x^{-\delta}$ a polynomial since $x^{-\delta} \equiv x^{\phi(q)-\delta} \pmod{x^q - x}$ and $\phi(q) - \delta \in \mathbb{N}_0$, where ϕ denotes *Euler's totient function*. According to Fermat's little theorem, party i's share of $x^{-\delta}$ is $\alpha_i^{-\delta} \equiv \alpha_i^{\phi(q)-\delta}$, where both terms belong to the same residue class. Although we consider n-sharings, the degree of $x^{\phi(q)-\delta}$ may exceed $n-1$ because we do not want to reconstruct the polynomial or its coefficients—the polynomial is already known. We only demand that α_i^δ and the share in question, say, s, cancel, that is, $s \cdot \alpha_i^\delta p(\alpha_i^{-1}) = p(\alpha_i^{-1})$. A feasible s is $s \equiv \alpha_i^{-\delta}$, which holds for all $\alpha_i \in \alpha$ when using $x^{-\delta}$. Note that instead of using $x^{-\delta}$, it is also possible to use the polynomial corresponding to the n-sharing $(\alpha_i^{-\delta})_{i\in[0,n-1]}$ because the values of both functions coincide at all nodes $\alpha_i \in \alpha$.

Below, we illustrate the approach using an example.

Example 5.13. Let $q = 11$, $n = 5$, $\delta = n - 1 = 4$, $\alpha = [n]$, and consider the polynomial p with $p(x) = 3 + 6x + 4x^2$. Since $x^{-\delta} \equiv x^6$, the sharings are

$$\begin{aligned} p(x)&\colon (2,9,2,3,1), & p(1/x)&\colon (2,7,3,2,7),\\ x^\delta p(1/x)&\colon (2,2,1,6,8), & x^{-\delta}&\colon (1,9,3,4,5). \end{aligned}$$

Multiplying the sharing of $x^\delta p(1/x)$ by the one of $x^{-\delta}$ componentwise yields $(2,7,3,2,7)$, the sharing of $p(1/x)$. The polynomial corresponding to the n-sharing of x^6 is $7 + 3x + 10x^2 + 6x^3 + 8x^4$, and of course, its sharing coincides with $(\alpha_i^6)_{i\in[0,n-1]} \triangleq (i^6)_{i\in[n]}$.

We conclude that any approach, whether division-based or reduction-based, must produce shares corresponding to the final truncated polynomial to be usable in our context of secret sharing or for MPC. However, the approach described above works in the context of side-channel attacks where the adversary can only probe a fixed number of shares or for applications where the secret need not remain confidential, such as Reed–Solomon codes in coding theory. In these scenarios, two parties, i and j, simply "swap" their shares α_i and $\alpha_j = \alpha_i^{-1}$, or each party i possesses both α_i and α_i^{-1} [ABO24].

5.6 Approach 6: Matrix-Based Truncation of All Lower-Order Terms

In this last section, we pursue the same goal as in the previous section: We intend to truncate all lower-order terms to determine if the corresponding polynomial is zero. In contrast to Section 5.5, this approach is usable for MPC applications, and we utilize matrices instead of polynomial division. More precisely, we employ the Vandermonde matrix to switch between the coefficient view and the sharing view of polynomials. Recall that the lower-order coefficients of a polynomial p refer to $p_0, \dots, p_d$, and the higher-order ones refer to $p_{n-\sigma}, \dots, p_{n-1}$. Although it is sufficient to truncate the lower-order coefficients, we truncate all but the higher-order ones. The arguments in this section hold regardless, and changing the matrices to truncate only the lower-order terms is straightforward.

Let $\lfloor_i$ and $\rceil_i$ denote the identity matrix $I := I_n$ of size n with its first i rows and all but its first $i+1$ rows set to zero, respectively. That is,

$$\mathrm{row}(\lfloor_i, j) = \begin{cases} \mathrm{row}(I,j) & \text{if } j \geq i \\ 0^{1\times n} & \text{else,} \end{cases} \qquad \mathrm{row}(\rceil_i, j) = \begin{cases} \mathrm{row}(I,j) & \text{if } j \leq i \\ 0^{1\times n} & \text{else,} \end{cases}$$

where $\mathrm{row}(A,j)$ denotes the j^{th} row of matrix A. Moreover, let $\pi_{i,j}$ be the permutation matrix formed by swapping rows i and j of I. We recall that matrix indices are zero-based.

Example 5.14. Let $n = 5$. Then,

$$\lfloor_2 = \begin{pmatrix} 0&0&0&0&0\\ 0&0&0&0&0\\ 0&0&1&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1 \end{pmatrix}, \quad \rceil_1 = \begin{pmatrix} 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&0&0&0\\ 0&0&0&0&0\\ 0&0&0&0&0 \end{pmatrix}, \quad \pi_{0,1} = \begin{pmatrix} 0&1&0&0&0\\ 1&0&0&0&0\\ 0&0&1&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1 \end{pmatrix}.$$

In order to remove all but the higher-order terms like in Section 5.5, we employ the method described by Asharov and Lindell [AL11], which they use to perform the degree-reduction step in case of a multiplication gate in the protocol of [BGW88].

Fact 5.15 ([AL11]). For given n, $d < n/2$, and interpolation nodes $\alpha_0, \dots, \alpha_{n-1}$, there exists a *constant* matrix A such that for all polynomials p of degree $2d$ with $p(x) = \sum_{k=0}^{2d} p_k x^k$ and corresponding truncation $p'(x) = \sum_{k=0}^{d} p_k x^k$, it holds that $A \cdot (p(\alpha_0), \dots, p(\alpha_{n-1}))^\intercal = (p'(\alpha_0), \dots, p'(\alpha_{n-1}))^\intercal$. The matrix A is precisely $A = V\rceil_d V^{-1}$.

The matrix A is *constant* because it is independent of the shares $p(\alpha_0), \dots, p(\alpha_{n-1})$ and changes only if n, d, or α change. In other words, A is public. We briefly explain why the above method works: Multiplying the sharing $(p(\alpha_i))_{i\in[0,n-1]}^\intercal$ by V^{-1} transforms the sharing vector into the coefficient vector $(p_k)_{k\in[0,n-1]}^\intercal$ of p. The matrix $\rceil_d$ truncates all but its first $d+1$ elements, effectively zeroing the coefficients $p_{d+1}, \dots, p_{2d}$ in p. Finally, V transforms the coefficient vector back into the sharing corresponding to p'. Since A is constant and matrices describe linear transformations, parties can *privately* compute a sharing of the truncated polynomial p', as shown in [AL11]. The method also works in the double-sharing setting if the coefficients p_d and p_{2d} are swapped beforehand using $\pi_{d,2d}$. The matrix A then equals $V\rceil_d \pi_{d,2d} V^{-1}$.

Modifying I differently, that is, using matrices other than $\rceil_d$ and $\rceil_d \pi_{d,2d}$, enables manipulating p in further ways. In particular, we can remove all but the higher-order terms using $\lfloor_{n-\sigma}$ (or only the lower-order terms using $\lfloor_{d+1}$).

Theorem 5.16. *For given σ, n, and interpolation nodes $\alpha_0, \dots, \alpha_{n-1}$, there exists a* constant *matrix A' such that for all polynomials p of degree $n-1$ with $p(x) = \sum_{k=0}^{n-1} p_k x^k$ and corresponding truncation $p''(x) = \sum_{k=n-\sigma}^{n-1} p_k x^k$, it holds that $A' \cdot (p(\alpha_0), \dots, p(\alpha_{n-1}))^\intercal = (p''(\alpha_0), \dots, p''(\alpha_{n-1}))^\intercal$. The matrix A' is precisely $A' = V\lfloor_{n-\sigma} V^{-1}$.*

Proof. It is evident that $A' = V\lfloor_{n-\sigma} V^{-1}$ sets all coefficients $p_0, \dots, p_{n-\sigma-1}$ to 0 and leaves the higher-order ones untouched. Thus, the claim follows. ∎

After applying the transformation described in Theorem 5.16, parties can compare their shares with 0 to verify if all higher-order terms of p are 0 since those are the ones p'' precisely comprises.

Observation 5.17. All higher-order terms of p are 0 if, and only if, p'' is the zero polynomial, that is, if, and only if, $V\lfloor_{n-\sigma}V^{-1}(p(\alpha_0),\dots,p(\alpha_{n-1}))^\intercal \triangleq (p''(\alpha_0),\dots,p''(\alpha_{n-1}))^\intercal = 0^n$.

For our purposes, i.e., to detect whether the adversary introduced faults, parties privately compute the transformation described in Theorem 5.16, once for f' and once for g'. Afterward, they exchange shares or notify each other if one of their shares is not 0.

In fact, if $n > 2\sigma$, we can store all higher-order terms of f' and g' in one polynomial, say, h, and save checking one sharing. For instance, we put the coefficients of g' in $h_{n-\sigma},\dots,h_{n-1}$ and shift the higher-order coefficients of f' to the left by σ positions to put them in $h_{n-2\sigma},\dots,h_{n-1-\sigma}$. In that case, h is as follows:

$$\begin{aligned} h(x) &= \sum_{k=n-\sigma}^{n-1} f'_k x^{k-\sigma} + \sum_{k=n-\sigma}^{n-1} g'_k x^k \\ &= f'_{n-\sigma}x^{n-2\sigma} + \cdots + f'_{n-1}x^{n-\sigma-1} + g'_{n-\sigma}x^{n-\sigma} + \cdots + g'_{n-1}x^{n-1}. \end{aligned}$$

As before, $h = 0$ holds if, and only if, f' and g' are valid. Computing a sharing H of h from sharings F' and G' can be accomplished using permutation matrices, as they allow *permuting* the coefficients of f':

$$H^\intercal = \left(V \left(\prod_{i=n-\sigma}^{n-1} \pi_{i,i-\sigma} \right) \lfloor_{n-\sigma} V^{-1} \right) \cdot F'^\intercal + (V\lfloor_{n-\sigma}V^{-1}) \cdot G'^\intercal.$$

Observe that both matrices, which $F'^\intercal$ and $G'^\intercal$ are multiplied by, are again constant.

We finally mention that if $n > 2\sigma$ cannot be guaranteed or the overhead is undesirable, yet only one sharing is available, we can combine the higher-order coefficients of f' and g' pairwise, e.g., using subtraction. In this case, we consider the polynomial $\sum_{k=n-\sigma}^{n-1}(f'_k - g'_k)x^k = (f'_{n-\sigma} - g'_{n-\sigma})x^{n-\sigma} + \cdots + (f'_{n-1} - g'_{n-1})x^{n-1}$. However, we are then again faced with the problem of coefficients f'_k and g'_k potentially canceling out each other.

6

Conclusion and Outlook

In this thesis, we investigated univariate polynomials over finite fields regarding their zeros and improved results from [BEF+23] and [ABEO24]. These improvements concern the probability of an adversary successfully faulting a circuit without being noticed.

In Chapter 3, we considered the zeros of polynomials from several perspectives. We began by counting the number of polynomials in $\mathcal{M}_n$ with a zero at one specific position $v \in \mathbb{F}$ of multiplicity $s \leq n$. Here, we used the generating-function approach from [KK90] to derive the desired number. We stated the corresponding random variable $\mathcal{Z}_{1,v}(n)$, which gives the multiplicity of the zero v of a polynomial chosen uniformly at random from $\mathcal{M}_n$ or $\mathcal{P}_n$. The random variable $\mathcal{Z}_1(n)$ follows the geometric distribution $\mathrm{Geo}(1-q^{-1})$, truncated at $s = n$. Thus, $\mathcal{Z}_1(n)$ has a geometric limit. Furthermore, we proved that the statistical distance $\Delta(\mathcal{Z}_1(n), \mathcal{Z}_1) = q^{-n-1}$ is negligible in n, and we derived the expectation and variance of $\mathcal{Z}_1(n)$. Their asymptotic behavior is implied by $\mathrm{Geo}(1-q^{-1})$. We proceeded to consider two, then ℓ, positions $\underline{v}$ with zeros of multiplicities $\underline{s}$. Again, we established the number of such polynomials. We observed that the random variable $\mathcal{Z}_{\ell,\underline{v}}(n)$ is multivariate and comprises the ℓ random variables from the single-position case, i.e., $\mathcal{Z}_{\ell,\underline{v}}(n) = (\mathcal{Z}_{1,v_1}(n), \dots, \mathcal{Z}_{1,v_\ell}(n))$. Hence, the expectation and variance directly follow. Additionally, we considered the more restrictive case where zeros may only occur at positions in $\underline{v}$, which allowed us to derive the number of zero-free polynomials. We advanced to disregard the exact multiplicities $\underline{s}$ and, henceforth, only required that ℓ positions, either $\underline{v}$ or any other, have a combined multiplicity of $k = \sum_{s\in\underline{s}} s$. As before, we derived the number of favorable polynomials. From this, we inferred the number of polynomials with k zeros in total. The corresponding random variable $\mathcal{Z}(n)$ follows the negative binomial distribution $\mathrm{NBin}(q, 1-q^{-1})$ truncated at $k = n-q+1$. The asymptotic expectation and variance are, hence, directly established. When n and q approach infinity, polynomials have one zero on average and a variance of the same. Finally, we disregarded the multiplicities and focused only on the positions $\underline{v}$ with zeros. Since a zero occurs if, and only if, its multiplicity is at least 1, we were able to use our previous results to count all feasible polynomials. The random variable $\mathcal{Z}^*(n)$ follows the binomial distribution $\mathrm{Bin}(q, q^{-1})$ for all $n \geq q$ and, hence, has a binomial limit. The mean number of distinct zeros is 1 (unless $n = 0$), and its variance depends on q but not n. When q tends to infinity, the variance converges to 1. In the future, it is worthwhile to further analyze and simplify the similar alternating sums of the functions Z_ℓ, Z, and Z^*, such as

$\sum_{i=0}^{n-k} \binom{q}{i} (-1)^i q^{-i}$. That way, properties like lower or upper bounds can be derived more easily. Furthermore, the analysis of zeros can be expanded to multivariate polynomials or those over more general (finite) rings. We recall that in either case, Fact 1.41 no longer holds, that is, the number of zeros can exceed a polynomial's degree. These results can be used to improve applications that do not (necessarily) work over fields.

In Chapter 4, we first established the exact number of different polynomials p and p'. Then, we improved the upper bounds in Theorem 4 from [BEF+23] by providing exact probabilities in case the adversary is either non-adaptive or adaptive. The former probability is in closed form, whereas the latter contains parts of the unknown PMF of δ. Thus, we provided an upper bound that holds unconditionally. Further, we argued that said upper bound is tight since the adversary can choose p such that the relevant parts of the PMF add up to 1. Using known inequalities such as $t_1 \leq s$ and $e < n$, we presented further upper bounds in Figure 4.1. Finally, we compared our upper bound with the original one from [BEF+23] and concluded that ours is at least $(q-1)(d+e+1)^{t_1} > 1$ times as good.

In Chapter 5, we improved the error detection of the double-sharing framework from [ABEO24]. Since the original error propagation term, which protects the polynomial fg, allows an adversary to remain unnoticed when non-linear operations are used, we considered using different terms. Initially, we used different error terms depending on the operation the ℓ-function performs. However, this yields a non-unified method since the error propagation must be adapted to match the ℓ-function. Thus, we considered combining multiple terms by adding them. We found that this protects the sum of the polynomials rather than both polynomials individually. We considered the error terms protecting $f+g$ and fg, whose sum protects $f+g+fg$. In that case, we showed that the adversary still can introduce non-vanishing faults. However, we could neither show nor refute that there is a single polynomial such that the adversary can only introduce vanishing faults. Since the higher-order terms of f' and g' cannot vanish if considered individually, we adapted the φ-gadget in [ABEO24] by adding two further sharings, Q^f and Q^g, besides Q. Our modified φ-gadget in Algorithm 5.1, hence, always detects if an adversary introduces faults and returns an (in)valid sharing accordingly. We further considered three potential alternative methods that provide always-detecting error detection. Firstly, we privately combined all higher-order coefficients of f' and g' in one coefficient of a polynomial such that the combination is 0 if, and only if, all higher-order coefficients are 0. The remaining methods aim to truncate all but the higher-order terms of f' and g' using either polynomial division or matrix multiplication. The framework from [MF06], which we intended to use to perform polynomial division, does not work for secret-sharing-related applications since it allows parties to learn additional shares. Hence, we adapted the matrix-based approach described in [AL11] and, thereby, established a second working method that always detects a faulting adversary. Future research should pursue determining more efficient methods for error detection. In that regard, Algorithm 5.1 could be further improved, e.g., to shed the need to interpolate two polynomials (line 11). Moreover, in Section 5.2, we could neither prove nor refute whether there is a meaningful bivariate polynomial without vanishing faults, i.e., non-trivial zeros, for all or some finite fields. By "meaningful," we refer to a polynomial corresponding to an operation computable by an ℓ-function. Resolving this open question shows whether or not a universal error term exists that protects all operations.

Bibliography

[ABEO24] Arnold, P., Berndt, S., Eisenbarth, T., and Orlt, M. *Polynomial sharings on two secrets: Buy one, get one free*. Cryptology ePrint Archive, Paper 2024/1025. 2024. URL: https://eprint.iacr.org/2024/1025.

[ABO24] Arnold, P., Berndt, S., and Ostendorf, L. Private Communication. 2024.

[AL11] Asharov, G. and Lindell, Y. *A Full Proof of the BGW Protocol for Perfectly-Secure Multiparty Computation*. Cryptology ePrint Archive, Paper 2011/136. 2011. URL: https://eprint.iacr.org/2011/136.

[Apo76] Apostol, T. M. *Introduction to Analytic Number Theory*. Undergraduate Texts in Mathematics. Springer New York, NY, 1976. ISBN: 978-1-4757-5579-4. DOI: 10.1007/978-1-4757-5579-4.

[Ax64] Ax, J. Zeroes of Polynomials Over Finite Fields. In: *American Journal of Mathematics* 86(2):255–261, 1964. DOI: 10.2307/2373163.

[Bag09] Bagdasaryan, A. *A Note on the 2F1 Hypergeometric Function*. 2009. arXiv: 0912.0917 [math.CA]. URL: https://arxiv.org/abs/0912.0917.

[BEF+23] Berndt, S., Eisenbarth, T., Faust, S., Gourjon, M., Orlt, M., and Seker, O. *Combined Fault and Leakage Resilience: Composability, Constructions and Compiler*. Cryptology ePrint Archive, Paper 2023/1143. 2023. URL: https://eprint.iacr.org/2023/1143.

[BGW88] Ben-Or, M., Goldwasser, S., and Wigderson, A. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In: *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*. STOC '88. Association for Computing Machinery, 1988, pp. 1–10. DOI: 10.1145/62212.62213.

[Chi09] Childs, L. N. *A Concrete Introduction to Higher Algebra*. Undergraduate Texts in Mathematics. Springer New York, NY, 2009. ISBN: 978-0-387-74725-5. DOI: 10.1007/978-0-387-74725-5.

[CPR13] Coron, J.-S., Prouff, E., and Roche, T. On the Use of Shamir's Secret Sharing against Side-Channel Analysis. In: *Smart Card Research and Advanced Applications*. Springer Berlin Heidelberg, 2013, pp. 77–90. DOI: 10.1007/978-3-642-37288-9_6.

[DNV15] Do, Y., Nguyen, H., and Vu, V. Real roots of random polynomials: expectation and repulsion. In: *Proceedings of the London Mathematical Society* 111(6):1231–1260, 2015. DOI: 10.1112/plms/pdv055.

[FGP96] Flajolet, P., Gourdon, X., and Panario, D. Random Polynomials and Polynomial Factorization. In: *Automata, Languages and Programming, 23rd International Colloquium, ICALP96, Paderborn, Germany, 8-12 July 1996, Proceedings*.

Vol. 1099. Lecture Notes in Computer Science. Springer, 1996, pp. 232–243. DOI: 10.1007/3-540-61440-0_131.

[FY92] Franklin, M. and Yung, M. Communication complexity of secure computation (extended abstract). In: *Proceedings of the Twenty-Fourth Annual ACM Symposium on Theory of Computing*. STOC '92. Association for Computing Machinery, 1992, pp. 699–710. DOI: 10.1145/129712.129780.

[Gei15] Geil, O. Roots and coefficients of multivariate polynomials over finite fields. In: *Finite Fields and Their Applications* 34:36–44, 2015. ISSN: 1071-5797. DOI: doi.org/10.1016/j.ffa.2015.01.001.

[GKP94] Graham, R. L., Knuth, D. E., and Patashnik, O. *Concrete Mathematics: A Foundation for Computer Science, 2nd Ed*. Addison-Wesley, 1994. ISBN: 978-0-201-55802-9.

[Hie24] Hien, M. *Abstract Algebra*. Mathematics Study Resources. Springer Berlin, Heidelberg, 2024. ISBN: 978-3-66267974-6. DOI: 10.1007/978-3-662-67974-6.

[Hwa98] Hwang, H. A Poisson * Negative Binomial Convolution Law for Random Polynomials over Finite Fields. In: *Random Struct. Algorithms* 13(1):17–47, 1998. DOI: 10.1002/(SICI)1098-2418(199808)13:1\<17::AID-RSA2\>3.0.CO;2-V.

[IBS11] IBS *Number of monic irreducible polynomials of prime degree p over finite fields*. 2011. URL: https://math.stackexchange.com/a/40875 (visited on 03/08/2025).

[IM08] Ivchenko, G. I. and Medvedev, Y. I. Random polynomials over a finite field. In: *Discrete Mathematics and Applications* 18:1–23, 2008. DOI: 10.1515/DMA.2008.001.

[JMW23] Jain, R., Moon, H., and Wu, P. *Distribution of the number of zeros of polynomials over a finite field*. 2023. arXiv: 2308.14580 [math.PR]. URL: https://arxiv.org/abs/2308.14580.

[KK90] Knopfmacher, A. and Knopfmacher, J. Counting polynomials with a given number of zeros in a finite field. In: *Linear and Multilinear Algebra* 26(4):287–292, 1990. DOI: 10.1080/03081089008817985.

[KK93] Knopfmacher, A. and Knopfmacher, J. Counting irreducible factors of polynomials over a finite field. In: *Discrete Mathematics* 112(1):103–118, 1993. DOI: 10.1016/0012-365X(93)90227-K.

[Kno75] Chapter 3 Enumeration Problems. In: *Abstract Analytic Number Theory*. Ed. by J. Knopfmacher. Vol. 12. North-Holland Mathematical Library. Elsevier, 1975, pp. 54–72. DOI: 10.1016/S0924-6509(08)70319-2.

[KW14] Kopparty, S. and Wang, Q. Roots and coefficients of polynomials over finite fields. In: *Finite Fields and Their Applications* 29:198–201, 2014. ISSN: 1071-5797. DOI: 10.1016/j.ffa.2014.04.002.

[MF06] Mohassel, P. and Franklin, M. K. Efficient Polynomial Operations in the Shared-Coefficients Setting. In: *Public Key Cryptography - PKC 2006, 9th International Conference on Theory and Practice of Public-Key Cryptography*. Vol. 3958. Lecture Notes in Computer Science. Springer, 2006, pp. 44–57. DOI: 10.1007/11745853_4.

[Mur06] Murphy, T. *2006 Course 4281 Prime Numbers*. https://www.maths.tcd.ie/pub/Maths/Courseware/428/Primes-II.pdf. Online; accessed 05-03-2025. 2006.

[Ogu08] Ogus, A. *Polynomials and polynomial functions*. https://math.berkeley.edu/~ogus/Math_110--008/Supplements/polynomials.pdf. Online; accessed 06-03-2025. 2008.

[Pan04] Panario, D. What Do Random Polynomials over Finite Fields Look Like? In: *Finite Fields and Applications*. Springer Berlin Heidelberg, 2004, pp. 89–108. ISBN: 978-3-540-24633-6. DOI: 10.1007/978-3-540-24633-6_8.

[pon13] poncho *Coefficients in Shamir's Secret Sharing Scheme*. 2013. URL: https://crypto.stackexchange.com/a/12553/85194 (visited on 02/01/2025).

[RS60] Reed, I. S. and Solomon, G. Polynomial Codes Over Certain Finite Fields. In: *Journal of the Society for Industrial and Applied Mathematics* 8(2):300–304, 1960. DOI: 10.1137/0108018.

[RSG23] Richter-Brockmann, J., Sasdrich, P., and Güneysu, T. Revisiting Fault Adversary Models – Hardware Faults in Theory and Practice. In: *IEEE Transactions on Computers* 72(2):572–585, 2023. DOI: 10.1109/TC.2022.3164259.

[SB03] Stoer, J. and Bulirsch, R. *Introduction to Numerical Analysis*. Texts in Applied Mathematics. Springer New York, NY, 2003. ISBN: 978-0-387-21738-3. DOI: 10.1007/978-0-387-21738-3.

[Sch76] Schmidt, W. M. *Equations over Finite Fields*. Lecture Notes in Mathematics. Springer Berlin, Heidelberg, 1976. ISBN: 978-3-54038123-5. DOI: 10.1007/BFb0080437.

[SFES18] Seker, O., Fernandez-Rubio, A., Eisenbarth, T., and Steinwandt, R. Extending Glitch-Free Multiparty Protocols to Resist Fault Injection Attacks. In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2018(3):394–430, 2018. DOI: 10.13154/tches.v2018.i3.394-430.

[Sha79] Shamir, A. How to share a secret. In: *Commun. ACM* 22(11):612–613, 1979. DOI: 10.1145/359168.359176.

[SSB+22] Shapiro, L., Sprugnoli, R., Barry, P., Cheon, G., He, T., Merlini, D., and Wang, W. *The Riordan Group and Applications*. Springer Monographs in Mathematics. Springer Cham, 2022. ISBN: 978-3-03094151-2. DOI: 10.1007/978-3-030-94151-2.

[Tan23] Tantau, T. *The TikZ and PGF Packages. Manual for version 3.1.10*. Jan. 13, 2023. URL: https://github.com/pgf-tikz/pgf/.

[Wol] Wolfram Research, Inc. *Mathematica*. Version 14.2. Champaign, IL, 2024. URL: https://www.wolfram.com/mathematica.