Schwartz-Zippel for multilinear polynomials mod N

Benedikt Bünz*, Ben Fisch†
Stanford University

May 4, 2022

Abstract

We derive a tight upper bound on the probability over $\mathbf{x} = (x_1, \ldots, x_\mu) \in \mathbb{Z}^\mu$ uniformly distributed in $[0, m)^\mu$ that $f(\mathbf{x}) = 0 \bmod N$ for any μ-linear polynomial $f \in \mathbb{Z}[X_1, \ldots, X_\mu]$ co-prime to N. We show that for $N = p_1^{r_1}, ..., p_\ell^{r_\ell}$ this probability is bounded by $\frac{\mu}{m} + \prod_{i=1}^{\ell} I_{\frac{1}{p_i}}(r_i, \mu)$ where I is the regularized beta function. Furthermore, we provide an inverse result that for any target parameter λ bounds the minimum size of N for which the probability that $f(\mathbf{x}) \equiv 0 \bmod N$ is at most $2^{-\lambda} + \frac{\mu}{m}$. For $\mu = 1$ this is simply $N \geq 2^\lambda$. For $\mu \geq 2$, $\log_2(N) \geq 8\mu^2 + \log_2(2\mu) \cdot \lambda$ the probability that $f(\mathbf{x}) \equiv 0 \bmod N$ is bounded by $2^{-\lambda} + \frac{\mu}{m}$. We also present a computational method that derives tighter bounds for specific values of μ and λ. For example, our analysis shows that for $\mu = 20$, $\lambda = 120$ (values typical in cryptography applications), and $\log_2(N) \geq 416$ the probability is bounded by $2^{-120} + \frac{20}{m}$. We provide a table of computational bounds for a large set of μ and λ values.

1 Introduction

The famous DeMillo-Lipton-Schwartz–Zippel (DLSZ) lemma[DL77; Zip79; Sch80][1] states that for any field $\mathbb{F}$, non-empty finite subset $S \subseteq \mathbb{F}$, and non-zero μ-variate polynomial f over $\mathbb{F}$ of total degree d, the number of zeros of f contained in S^μ is bounded by $d \cdot |S|^{\mu-1}$ (or equivalently, the probability that $f(\mathbf{x}) = 0$ for $\mathbf{x}$ sampled uniformly from S^n is bounded by $\frac{d}{|S|}$). For $\mu = 1$ this simply follows from the Fundamental Theorem of Algebra, but for multivariate polynomials, the number of zeros over the whole field could be unbounded. The computational significance of this lemma is that sampling an element from S only takes $n \cdot \log_2(|S|)$ random bits but the probability of randomly sampling a zero of f from S^n is exponentially small in $|S|$. One of its original motivations was an efficient randomized algorithm for polynomial identity testing, but it has since found widespread application in computer science. Polynomial identity testing is the canonical randomized algorithm and is famously hard to derandomize[KI04].

The classical lemma applies more broadly to integral domains, but not to arbitrary commutative rings. As a simple counterexample, over the ring of integers modulo $N = 2p$ the polynomial $f(X) = pX \bmod N$ vanishes on half of the points in $[0, N)$. The lemma has been extended to commutative rings by restricting the set S to special subsets in which the difference of any two elements is not a zero divisor [Bis+15]. For the case of $\mathbb{Z}_N$, this means that the difference of any two elements in S must be co-prime to N. Our present work explores the setting where S is the contiguous interval $[0, m)$ and thus does not satisfy this special condition. Instead, we will restrict the polynomial f to be co-prime with N, thus ruling out polynomials of the form $f(X) = u \cdot g(X)$ where u is a zero-divisor as in the counterexample above.

As a warmup, it is easy to see that any univariate linear polynomial $f(X) = c \cdot X + b$ co-prime to N has at most one root modulo N. If there were two such roots $x_1 \not\equiv x_2 \bmod N$ then $c(x_1 - x_2) \equiv 0 \mod N$ implies c is a zero divisor (i.e., $gcd(c, N) \neq 1$). Furthermore, $c \cdot x_1 \equiv -b \bmod N$ implies $-b = c \cdot x_1 + q \cdot N$ for some $q \in \mathbb{Z}$, and thus, $gcd(c, N)$ also divides b. This would contradict the co-primality of f and N. So for x uniformly distributed in $S = [0, m)$ the probability of $f(x) \equiv 0 \bmod N$ in this case is indeed at most $\frac{1}{|S|}$. Unfortunately, this does not appear to generalize nicely to polynomials of arbitrary degree. As an example, for $N = 2^\lambda$ the polynomial $f(X) = X^\lambda \bmod N$ vanishes on half of the points in $[0, N)$.

On the other hand, we are able to generalize the lemma in a meaningful way to multivariate *linear* polynomials (i.e, at most degree 1 in each variable). It turns out that the probability of sampling a zero from $S^\mu = [0, m)^\mu$ of a μ-linear polynomial can be tightly bounded by $\frac{\mu}{|S|} + \epsilon$, where the error term ϵ is bounded by a product of regularized beta functions. We also formulate an inverse Schwartz-Zippel Lemma for composite showing that for all sufficiently large N this error is negligibly small. In particular, for $\log N \geq 8\mu^2 + (1 + \log \mu)\lambda$ the error term is at most $2^{-\lambda}$, showing that the error decays exponentially. Our technique for deriving this threshold lower bound $t(\lambda, \mu)$ on N for a target λ formulates $t(\lambda, \mu)$ as the objective function of a knapsack problem. We derive an analytical solution by deriving bounds on the regularized beta

*benedikt@cs.stanford.edu
†benafisch@gmail.com

[1] See this blog post for a detailed history of the lemma: `https://rjlipton.wpcomstaging.com/2009/11/30/the-curious-history-of-the-schwartz-zippel-lemma/`

function. We also apply a knapsack approximation algorithm to find tighter values of $t(\lambda, \mu)$ for specific values of μ and λ.

1.1 Applications and Open Problems

We remark on one application of the Multi-Linear Composite Schwartz-Zippel lemma (LCSZ) and its inverse to a problem in cryptography, and postulate other potential cryptographic applications as open problems. Consider a rational multi-linear polynomial $g(X) = \frac{f(X)}{N}$ for $f \in \mathbb{Z}[X]$ and $N \in \mathbb{N}$ coprime with f. The LCSZ gives a bound on the probability that $f(\mathbf{x}) \in \mathbb{Z}$ for a random point $\mathbf{x}$ as in this case $f(\mathbf{x}) \equiv 0 \bmod N$. Furthermore we can use the inverse lemma to show that if $f(\mathbf{x}) \in \mathbb{Z}$ for random point $\mathbf{x}$ then the probability that $N > B$ can be bounded. This application of the inverse LCSZ is an essential component of a new[2] security proof for the polynomial commitment DARK[BFS20]. Additionally, it is conceivable that the inverse LCSZ could be used to strengthen the recent result called Dew[Aru+22], a zero-knowledge proof system with constant proof size and efficient verifier. In particular, the current security proof requires parameters that result in quadratic prover time. There is hope that the security proof can be made to work with tighter parameters and a quasi-linear prover, using the inverse LCSZ.

Further, the LCSZ could potentially also be used to improve other zero-knowledge proof systems for modular arithmetic over rings instead of prime fields. This can have benefits, such as enabling the use of more machine-friendly moduli (e.g., powers-of-two). For example, recent work [Att+22] generalized Bulletproofs and Compressed Σ-Protocols to work for cryptographic commitments to vectors over $\mathbb{Z}_n$ for general n (not strictly prime). Their analysis also deals with multilinear polynomials over rings and uses the generalization of DLSZ [Bis+15] that restricts the sampling domain S to *exceptional sets* (sets whose element differences are not zero-divisors). Since $\mathbb{Z}_n$ does not have large enough exceptional sets, their protocol works over finite extension rings resulting in significantly worse performance in both proof size and computation time than the original versions of these protocols over $\mathbb{Z}_p$ (e.g., by a factor $\lambda \approx 128$ for 128-bit security). Generalizations of Bulletproofs and Compressed Σ-Protocols for lattice-based commitments (e.g., based on the hardness of the Integer SIS problem) encounter similar challenges [ACK21]. The GKR sumcheck protocol [GRK17] also partially relies on the DLSZ for multilinear polynomials. Sumcheck based protocols have similarly been extended to work over rings instead of prime fields using DLSZ with exceptional sets [Che+19; BCS21]. Our new variant (LCSZ) could possibly[3] be used to improve these results (by eliminating the need for exceptional sets) as well as other GKR instantiations[CMT12; Set20; SL20] to integer rings.

1.2 Technical Overview

The regular DLSZ is relatively simple to prove. Consider the special case of a multilinear polynomial over a field. As a base case, a univariate linear polynomial has at most one root over the field. For the induction step, express $f(X_1, ..., X_{n+1}) = g(X_1, ..., X_n) + X_{n+1}h(X_1, ..., X_n)$ for random variables $X_1, \ldots, X_n$. The probability that $h(x_1, ..., x_n) = 0$ over random x_i sampled from S is at most $n/|S|$ by the inductive hypothesis, and if $h(x_1, ..., x_n) = w \neq 0$ and $g(x_1, \ldots, x_n) = u$, then $u + X_{n+1}w$ has at most one root (base case). By the union bound, the overall probability is at most $n/|S|+1/|S|= (n+1)/|S|$.

This simple proof does not work for multilinear polynomials modulo a composite integer. The base case is the same for f coprime to N, which has at most one root. However, in the induction step, it isn't enough that $h(x_1, ..., x_n) \neq 0$ as it still may be a zero divisor, in which case the polynomial $u + X_{n+1}w$ is not necessarily coprime to N and the base case no longer applies. The number of roots depends on $\gcd(u + X_{n+1}w, N)$.

We prove the LCSZ using a modified inductive proof over n. Our analysis takes into account the distribution of $\gcd(u + X_{n+1}w, N)$. For each prime divisor p_i of N, the highest power of p_i that divides $u + X_{n+1}w$ follows a geometric distribution. Using an inductive analysis, we are able to show that the probability $f(x_1, \ldots, x_n) \equiv 0 \bmod p^r$ is bounded by the probability that $\sum_{i=1}^{n} Z_i \geq r$ for *i.i.d.* geometric variables with success parameter $1 - \frac{1}{p}$. This probability is equal to a $I_{\frac{1}{p}}(n, r)$ where I is the regularized beta function. Furthermore, by the Chinese Remainder Theorem this probability is independent for each prime factor of N, and thus, the overall probability can be bounded by a product of regularized beta functions.

Inverse LCSZ While the LCSZ gives a tight bound on the probability for particular values of N, μ, and m, cryptographic applications require finding concrete parameters such that the probability is exponentially small in a security parameter λ. This is easy for the standard DLSZ, as it simply states that when sampling from sets of size $d \cdot 2^\lambda$ the probability is at most $\frac{d}{2^\lambda}$. The LCSZ does not have such a simple form so we need to explicitly find an inverse formulation. Concretely, we want to find a value N^* such that for all $N \geq N^*$ the probability that $f(X_1, \ldots, X_n) \equiv 0 \bmod N$ is bounded by $2^{-\lambda}$.

To do this we first derive simple and useful bounds for the regularized beta function.

[2]There was a gap in the original analysis [Blo+21].

[3]A key challenge for applying LCSZ to these applications would be showing that the polynomials are co-prime with the modulus.

Bounds on regularized beta function We show the following three useful facts about $I_{\frac{1}{p}}(n, r)$

- $I_{\frac{1}{p}}(r, \mu) \leq \left(\frac{n}{p}\right)^r$ for $p \geq 2\mu$
- $I_{\frac{1}{p}}(r, \mu) \leq \frac{r^n}{p^r}$ for $r \geq 2\mu$
- $\log(I_{1/p}(r-1, \mu)) - \log(I_{1/p}(r, \mu))$ is non-increasing in r for any $p > \mu$ and for $r = 1$ in p.

Knapsack Formulation We then formulate finding N^* as an optimization problem. N^* is the maximum value of N such that the probability of $f(\mathbf{x}) \equiv 0 \bmod N$ is greater than $2^{-\lambda}$. For any N let $S(N)$ denote the set of pairs (p, r) where p is a prime divisor of N with multiplicity r. Taking the logarithm of both the objective and the constraint yields a knapsack-like constraint maximization [roblem where the objective is $\log(N^*) = \sum_{(p_i, r_i) \in S(N^*)} r_i \cdot \log(p_i)$ and the constraint is $\sum_{(p_i, r_i) \in S(N^*)} - \log(I_{\frac{1}{p_i}}(r, \mu)) \leq \lambda$. Using the bounds on $I_{\frac{1}{p_i}}$ and several transformations of the problem we show that any optimal solution to this problem must be bounded by $t = 8\mu^2 + \log_2(2\mu)\lambda$, which in turn implies that $N^* \leq 2^t$.

Tighter computational solution We further show that a simple greedy knapsack algorithm computes an upper bound to the knapsack problem. The algorithm uses the fact that $\frac{\log(p)}{\log(I_{1/p}(r-1,\mu)) - \log(I_{1/p}(r,\mu))}$ the so-called marginal density of each item is non increasing over certain regions. Adding the densest items to the knapsack computes an upper bound to the objective. We run the algorithm on a large number of values for μ and λ and report the result.

2 Main theorem statement

Theorem 1 (Multilinear Composite Schwartz-Zippel (LCSZ)). *Let $N = \prod_{i=1}^{\ell} p_i^{r_i}$ for distinct primes $p_1, ..., p_\ell$. Let f be any μ-linear integer polynomial co-prime to N. For any integer $m > 1$ and $\mathbf{x}$ sampled uniformly from $[0, m)^\mu$:*

$$\mathbb{P}_{\mathbf{x} \leftarrow [0,m)^\mu}[f(\mathbf{x}) \equiv 0 \bmod N] \leq \frac{\mu}{m} + \prod_{i=1}^{\ell} I_{\frac{1}{p_i}}(r_i, \mu)$$

where $I_{\frac{1}{p}}(r, \mu) = (1 - \frac{1}{p})^\mu \sum_{j=r}^{\infty} \binom{\mu+r-1}{r} \left(\frac{1}{p}\right)^j$ is the regularized beta function.

Remark 1. *The regularized beta function characterizes the tail distribution of the sum of independent geometric random variables. If $Y = \sum_{i=1}^{\mu} Z_i$ where each Z_i is an independent geometric random variable with parameter ϵ then $P[Y \geq r] = I_{1-\epsilon}(r, \mu)$. Y is a negative binomial variable with parameters ϵ, μ.*

Remark 2. *For $m \gg \mu$ the theorem is nearly tight for all N. Setting $f(\mathbf{x}) = \prod_{i=1}^{\mu} x_i$ and $m = N$ gives $P_{\mathbf{x} \leftarrow [0,m)^\mu}[f(\mathbf{x}) \equiv 0 \bmod N] = \mathbb{P}_{\mathbf{x} \leftarrow [0,N)^\mu}[f(\mathbf{x}) \equiv 0 \bmod N] = \prod_{i=1}^{\ell} I_{\frac{1}{p_i}}(r_i, \mu)$*

Remark 3. *$1 - e^{-\mu/p_i} \leq I_{\frac{1}{p_i}}(1, \mu) = 1 - (1 - \frac{1}{p_i})^\mu \leq \frac{\mu}{p_i}$. Hence, for square-free N the probability in Theorem 1 is upper bounded by $\frac{\mu}{m} + \frac{\mu^\ell}{N}$, but for $\ell > 1$ this is a loose upper bound unless $\mu \ll p_i$ for all $p_i | N$. For $\ell = 1$ (i.e., prime N), Theorem 1 coincides with the Schwartz-Zippel lemma.*

Remark 4. *$I_{\frac{1}{p_i}}(r_i, 1) = \left(\frac{1}{p_i}\right)^{r_i}$. Hence, for $\mu = 1$, the bound in Theorem 1 is $\frac{1}{N} + \frac{\mu}{m}$.*

Proof. We begin by introducing some notations.

- For a polynomial $f \in \mathbb{Z}[X_1, ..., X_\mu]$ let $\vec{f}$ denote the coefficients of f and let $\mathsf{cont}(f)$ denote the greatest integer divisor of f, i.e. the *content*.
- $\vec{\beta} = (\beta_1, ..., \beta_\mu) \in [0, m)^\mu$ is a random variable distributed uniformly over $[0, m)^\mu$. For any $i \geq 1$, let $\vec{\beta}_i = (\beta_1, ..., \beta_i)$, let $f_0 = f$, and let $f_i(\vec{\beta}_i) := f(\beta_1, \ldots, \beta_i, X_{i+1}, \ldots, X_\mu)$.
- Given the random variable $\vec{\beta}$ distributed uniformly over $[0, m)^\mu$, define for each $j \in [1, \ell]$ and $i \in [1, \mu]$ the random variable $Y_{j,i}$ (as a function of $\vec{\beta}$) representing the multiplicity of p_j in $\mathsf{cont}(f_i(\vec{\beta}_i))$). Naturally, we set $Y_{j,0} = 0$ for all j because $\forall_j f_0 \neq 0 \bmod p_j$. (**Note:** $Y_{j,i}$ are *not* independent). For any $i \in [\mu]$ the event that $\forall_j Y_{j,i} \geq r_j$ is equivalent to the event that $f_i(\vec{\beta}_i) = 0 \bmod N$ and the event that $\forall_j Y_{j,i} = r_i$ is equivalent to $\mathsf{cont}(f_i(\vec{\beta}_i)) = N$. The event $\forall_j Y_{j,\mu} \geq r_j$ is thus equivalent to $f(\vec{\beta}) = 0 \bmod N$.
- Let $\{Z_{j,i}\}$ for $i \in [\mu]$ and $j \in [\ell]$ be a set of independent random variables, where $Z_{j,i}$ is geometric with parameter $1 - \frac{1}{p_j}$.

From the CCDF (complementary CDF) of geometric random variables we have that $P[Z_{j,i} \geq k] = (\frac{1}{p_j})^k$. Setting $Z_j := \sum_{i=1}^{\mu} Z_{j,i}$, from the CCDF of the negative binomial distribution (i.e., tail distribution of the sum of independent geometric random variables) it follows that $\forall_j P[Z_j \geq r] = I_{\frac{1}{p_j}}(r, \mu)$.

Next, we establish an important subclaim:

Claim 1. *For any $i \geq 2$ and $\vec{k}, \vec{k}' \in \mathbb{N}^\ell$ where $\forall_j k_j \geq 0$:*

$$P[\forall_j Y_{j,i} \geq k_j + k'_j | \forall_j Y_{j,i-1} = k'_j] \leq \frac{1}{m} + P[\forall_j Z_{j,i} \geq k_j]$$

Furthermore, for all $i \geq 1$, $P[\forall_j Y_{j,i} \geq Y_{j,i-1} + k_j] \leq \frac{1}{m} + P[\forall_j Z_{j,i} \geq k_j]$.

Proof. Since the order of the variables does not matter, w.l.o.g. assume that $\forall_{j \in [1,\ell']} k_j \geq 1$ and $\forall_{j > \ell'} k_j = 0$. Let $N^* = \prod_{j=1}^{\ell'} p_j^{k_j}$ and $N' = \prod_{j=1}^{\ell'} p_j^{k'_j}$. For any $i \geq 2$ and any $\mathbf{x} \in [0, m)^{i-1}$, in the event that $\vec{\beta}_{i-1} = \mathbf{x}$ and $\forall j\ Y_{j,i-1} = k'_j$, then by definition $f_{i-1}(\mathbf{x}) \equiv 0 \bmod N'$ and $\forall_j f_{i-1}(\mathbf{x})/N' \not\equiv 0 \bmod p_j$. In case $i = 1$, we have that $\forall_j Y_{j,0} = 0$, $N' = 1$, and $\forall_j f_0 = f \neq 0 \bmod p_j$. Thus, for all $i \geq 1$, conditioned on the events that $\vec{\beta}_{i-1} = \mathbf{x}$ and $\forall j\ Y_{j,i-1} = k'_j$, there exist multilinear $\mu - i$ variate polynomials h_i, g_i such that $f_{i-1}(\mathbf{x})/N' = h_i(X_{i+1}, \ldots, X_\mu) + X_i \cdot g_i(X_{i+1}, \ldots, X_\mu)$ where for all j at least one of h_i or g_i is nonzero modulo p_j.

Furthermore, for any $i \geq 1$, conditioned on the events $\forall j\ Y_{j,i-1} = k'_j$ and $\vec{\beta}_{i-1} = \mathbf{x}$, the event that $\forall_j Y_{j,i} \geq k_j + k'_j$ is equivalent to the event that $h_i + \beta_i g_i \equiv 0 \bmod N^*$.

For each index $t \in [1, 2^{\mu-i}]$ let $h_i[t]$ and $g_i[t]$ denote the tth coefficients of h_i and g_i respectively (i.e., the coefficients on the tth monomial in a canonical ordering of the $2^{\mu-i}$ monomials over the $\mu - i$ variables $X_{i+1}, ..., X_\mu$). Given that for every $j \in [\ell']$ the polynomial $h_i + X_i \cdot g_i$ is non-zero modulo p_j, for each $j \in [\ell']$ there exists at least one index t_j for which the univariate linear polynomial $h_i[t_j] + X_i g_i[t_j]$ is non-zero modulo p_j. We now have that:

$$P[\forall_j Y_{j,i} \geq k_j + k'_j | \vec{\beta}_{i-1} = \mathbf{x} \wedge \forall_j Y_{j,i-1} = k'_j] = P[\forall_j\ h_i + \beta_i \cdot g_i \equiv 0 \bmod p_j^{k_j}] \tag{1}$$

$$\leq P[\forall_j\ h_i[t_j] + \beta_i \cdot g_i[t_j] \equiv 0 \bmod p_j^{k_j}] \tag{2}$$

For each t_j there is *at most* one solution to the equation $h_i[t_j] + X_i \cdot g_i[t_j] \equiv 0 \bmod\ p_j$. Consequently, by CRT, there is at most one integer solution $x^* \in [0, N^*)$ to the system of equations $\forall_j h_i[t_j] + X_i \cdot g_i[t_j] \equiv \bmod p_j$[4]. Therefore, if $m \leq N^*$, then the probability in line (2) above is bounded by $1/m$.

However, we must also consider the case that $m > N^*$. Let E denote the event that the system of equations $\forall_j\ h_i[t_j] + \beta_i \cdot g_i[t_j] \equiv 0 \bmod p_j^{k_j}$ from line (2) is satisfied. There is at most one integer equivalence class modulo N^* satisfying this system of equations and the random variable β_i is uniformly distributed over $[0, m)$ for some $m > N^*$. Let U denote the event that $\beta_i \in [0, m - m \bmod N^*)$ and let $\bar{U}$ denote the event that $\beta_i \in [m - m \bmod N^*, m)$. Conditioned on U, β_i is uniformly distributed modulo N^*, and thus $P[E|U] \leq 1/N^*$. Conditioned on $\bar{U}$, β_i is uniformly distributed over the set $[m - m \bmod N^*, m)$. As this set is a contiguous interval of less than N^* integers it contains at most one solution to the systems of equations, and thus, $P[E|\bar{U}] \leq 1/(m \bmod N^*)$. Therefore:

$$P[E] = P[E|U] \cdot P[U] + P[E|\bar{U}] \cdot P[\bar{U}] \tag{3}$$

$$\leq \frac{1}{N^*} \cdot (1 - \frac{m \bmod N^*}{m}) + \frac{1}{m \bmod N^*} \cdot \frac{m \bmod N^*}{m} \tag{4}$$

$$\leq \frac{1}{N^*} + \frac{1}{m} \tag{5}$$

We also have that:

$$P[\forall_{j \in [\ell]} Z_{j,i} \geq k_j] = \prod_{j=1}^{\ell'} P[Z_{j,i} \geq k_j] = \prod_{j=1}^{\ell'} \left(\frac{1}{p_j}\right)^{k_j} = \frac{1}{N^*}$$

Thus, putting it all together, for any $i \geq 1$ and any $\mathbf{x} \in [0, m)^{i-1}$:

$$P[\forall_j Y_{j,i} \geq k_j + k'_j | \vec{\beta}_{i-1} = \mathbf{x} \wedge \forall_j Y_{j,i-1} = k'_j] \leq \frac{1}{m} + \frac{1}{N^*} = \frac{1}{m} + P[\forall_j Z_{j,i} \geq k_j]$$

Since the probability bound is independent of $\mathbf{x}$, this implies:

$$P[\forall_j Y_{j,i} \geq k_j + k'_j | \forall_j Y_{j,i-1} = k'_j] \leq \frac{1}{m} + P[\forall_j Z_{j,i} \geq k_j]$$

Consequently, for any $i \geq 2$ and $\vec{k} \in \mathbb{N}^\ell$ where $\forall_j k_j > 0$:

$$P[\forall_j Y_{j,i} \geq Y_{j,i-1} + k_j] \leq \max_{\vec{k}'} P[\forall_j Y_{j,i} \geq k_j + k'_j | \forall_j Y_{j,i-1} = k'_j] \leq \frac{1}{m} + P[\forall_j Z_{j,i} \geq k_j]$$

Similarly, for $i = 1$ and $\vec{k} \in \mathbb{N}^\ell$ where $\forall_j k_j > 0$:

$$P[\forall_j Y_{j,i} \geq k_j] \leq \frac{1}{m} + P[\forall_j Z_{j,i} \geq k_j]$$

□

[4]This is where the proof falls apart for higher degree polynomials. For example if the polynomial is quadratic in each variable then there could be up to 2^ℓ solutions where ℓ is the number of prime factors.

We now prove the full theorem by induction over $i \in [1, \mu]$. Specifically, we will prove the following inductive hypothesis for $i \in [1, \mu]$:

$$P[f_i(\vec{\beta_i}) = 0 \bmod N] = P[\forall_j Y_{j,i} \geq r_j] \leq \frac{i}{m} + \prod_{j=1}^{\ell} P[\sum_{k=1}^{i} Z_{j,k} \geq r_j]$$

Setting $i = \mu$ this is equivalent to the theorem statement.

Base Case: The base case follows directly from the subclaim for the case $i = 1$.

$$P[\forall_j Y_{j,1} \geq r_j] \leq \frac{1}{m} + P[\forall_j Z_{j,1} \geq r_j] = \frac{1}{m} + \prod_{j=1}^{\ell} P[Z_{j,1} \geq r_j]$$

Induction Step: Assume the inductive hypothesis holds for some $1 \leq i < \mu$, i.e.:

$$P[\forall_j Y_{j,i} \geq r_j] \leq \frac{i}{m} + \prod_{j=1}^{\ell} P[\sum_{k=1}^{i} Z_{j,k} \geq r_j]$$

We will show this implies the hypothesis holds for $i + 1$:

$$\begin{aligned}
&P[\forall_j Y_{j,i+1} \geq r_j] = \sum_{\vec{k} \in \mathbb{N}^\ell} P[\forall_j Y_{j,i+1} - Y_{j,i} \geq r_j - k_j | \forall_j Y_{j,i} = k_j] \cdot P[\forall_j Y_{j,i} = k_j] \\
&\leq \sum_{\vec{k}} (P[\forall_j Z_{j,i+1} \geq r_j - k_j] + \frac{1}{m}) \cdot P[\forall_j Y_{j,i} = k_j] \quad \textbf{(by subclaim)} \\
&= \frac{1}{m} + \sum_{\vec{k}} P[\forall_j Z_{j,i+1} \geq r_j - k_j] \cdot P[\forall_j Y_{j,i} = k_j] \\
&= \frac{1}{m} + \sum_{\vec{\Delta} \in \mathbb{Z}^\ell : \forall_j \Delta_j \leq r_j} P[\forall_j Z_{j,i+1} \geq \Delta_j] \cdot P[\forall_j Y_{j,i} = r_j - \Delta_j] \quad \textbf{(change of variables)} \\
&= \frac{1}{m} + \sum_{\vec{\Delta} \in \mathbb{Z}^\ell : \forall_j \Delta_j \leq r_j} \sum_{\vec{k} \in \mathbb{N}^\ell} P[\forall_j Z_{j,i+1} = \Delta_j + k_j] \cdot P[\forall_j Y_{j,i} = r_j - \Delta_j] \\
&= \frac{1}{m} + \sum_{\vec{\Delta'} \in \mathbb{N}^\ell} P[\forall_j Z_{j,i+1} = \Delta'_j] \cdot \sum_{\vec{k} \in \mathbb{N}^\ell} P[\forall_j Y_{j,i} = r_j - (\Delta'_j - k_j)] \quad \textbf{(c.o.v.)} \\
&= \frac{1}{m} + \sum_{\vec{\Delta'} \in \mathbb{N}^\ell} P[\forall_j Z_{j,i+1} = \Delta'_j] \cdot P[\forall_j Y_{j,i} \geq r_j - \Delta'_j] \\
&\leq \frac{1}{m} + \sum_{\vec{\Delta'}} P[\forall_j Z_{j,i+1} = \Delta'_j] \cdot (P[\forall_j \sum_{i'=1}^{i} Z_{j,i'} \geq r_j - \Delta'_j] + \frac{i}{m}) \quad \textbf{(inductive hyp.)} \\
&= \frac{i+1}{m} + \sum_{\vec{\Delta'}} P[\forall_j Z_{j,i+1} = \Delta'_j] \cdot P[\forall_j \sum_{k=1}^{i} Z_{j,k} \geq r_j - \Delta'_j] \\
&= \frac{i+1}{m} + P[\forall_j \sum_{k=1}^{i} Z_{j,k} \geq r_j - Z_{j,i+1}] \quad \textbf{(independence of variables)} \\
&= \frac{i+1}{m} + \prod_{j=1}^{\ell} P[\sum_{k=1}^{i+1} Z_{j,k} \geq k_j] \quad \textbf{(independence of variables)}
\end{aligned}$$

□

3 Bounds on the Regularized Beta Function

The regularized incomplete beta function is defined for $k, \mu \in \mathbb{N}$ as:

$$I_\epsilon(k, \mu) = (1 - \epsilon)^\mu \sum_{j=k}^{\infty} \binom{\mu + j - 1}{j} \epsilon^j$$

Special values are $I_\epsilon(k, 1) = \epsilon^k$, which matches the tail distribution of a geometric variable with parameter $1 - \epsilon$, and $I_\epsilon(1, \mu) = 1 - (1 - \epsilon)^\mu$, which is the probability that at least one of μ geometric variables of parameter $1 - \epsilon$ is positive.

Lemma 1. *$I_\epsilon(k, \mu) \leq (\epsilon\mu)^k$ for all $\mu, k \in \mathbb{N}$ and $\epsilon \in (0, 1)$ where $\epsilon\mu \leq 1/2$.*

Proof. For $k = 0$ the statement holds because $I_\epsilon(0, \mu) = 1$. For $\mu = 1$ we have $I_\epsilon(k, 1) = \epsilon^k$. It remains to prove the inequality for $\mu \geq 2$ and $k \geq 1$. We will use the following ordinary generating function identity for binomial coefficients:

$$\sum_{j=0}^{\infty} \binom{a + j}{a} x^j = \frac{1}{(1 - x)^{a+1}}$$

This allows us to write $I_\epsilon(k, \mu)$ as:

$$I_\epsilon(k,\mu) = (1-\epsilon)^\mu \cdot \left(\sum_{j=0}^{\infty} \binom{\mu+j-1}{j} \epsilon^j - \sum_{j=0}^{k-1} \binom{\mu+j-1}{j} \epsilon^j \right)$$

$$= (1-\epsilon)^\mu \cdot (\frac{1}{(1-\epsilon)^\mu} - \sum_{j=0}^{k-1} \binom{\mu+j-1}{j} \epsilon^j) = 1 - (1-\epsilon)^\mu \sum_{j=0}^{k-1} \binom{\mu+j-1}{j} \epsilon^j$$

Using the geometric series identity $(\epsilon\mu)^k = 1 - (1-\epsilon\mu) \cdot \sum_{j=0}^{k-1} (\epsilon\mu)^j$, we obtain:

$$(\epsilon\mu)^k - I_\epsilon(k,\mu) = \sum_{j=0}^{k-1} (1-\epsilon)^\mu \cdot \binom{\mu+j-1}{j} \epsilon^j - (1-\epsilon\mu)(\epsilon\mu)^j$$

$$= \sum_{j=0}^{k-1} ((1-\epsilon)^\mu \cdot \binom{\mu+j-1}{j} - (1-\epsilon\mu)\mu^j)\epsilon^j$$

Let $\Phi_{\epsilon,\mu}(k) = (\epsilon\mu)^k - I_\epsilon(k,\mu)$ so that the goal is to show $\Phi_{\epsilon,\mu}(k) \geq 0$ for $k, \mu \in \mathbb{N}$ where $\mu \geq 2$ and $\epsilon\mu \leq 1/2$. Observe that:

$$\Phi_{\epsilon,\mu}(1) = \epsilon\mu - 1 + (1-\epsilon)^\mu = (1-\epsilon)^\mu - (1-\epsilon\mu) \geq 0$$

$$\lim_{k\to\infty} \Phi_{\epsilon,\mu}(k) = 0$$

Thus, it suffices to show that $\Phi_{\epsilon,\mu}(k)$ is non-increasing on the interval $k \in [2,\infty)$ when $\epsilon\mu \leq 1/2$ as this implies that $\Phi_{\epsilon,\mu}(k) \geq 0$ for all $k \geq 1$, $\mu \geq 2$, and $\epsilon\mu \leq 1/2$. Moreover, we can easily show this by showing that for all $\mu, j \geq 2$ and $\epsilon\mu \leq 1/2$:

$$(1-\epsilon)^\mu \cdot \binom{\mu+j-1}{j} \leq (1-\epsilon\mu) \cdot \mu^j$$

Letting $R(\mu,j) = \frac{\binom{\mu+j-1}{j}}{\mu^j}$, observe that:

$$R(\mu,j) = \frac{\binom{\mu+j-1}{j}}{\mu^j} = \frac{\prod_{i=0}^{j-1}(\mu+i)}{j!\ \mu^j} = \prod_{i=0}^{j-1} \frac{\mu+i}{\mu\cdot(i+1)}$$

Since $\mu + i \leq \mu \cdot (i+1)$ for all $\mu \geq 2$ and $i \geq 0$, it follows that $R(\mu,j) \leq R(\mu,2) = \frac{1}{2} \cdot (1+\frac{1}{\mu})$ for $j \geq 2$. Furthermore, for $\epsilon \in (0, 1/\mu)$:

$$\frac{d}{d\epsilon} \frac{(1-\epsilon)^\mu}{1-\epsilon\mu} = \frac{(\mu-1)\epsilon\mu(1-\epsilon)^{\mu-1}}{(1-\epsilon\mu)^2} \geq 0$$

Thus, for $\epsilon \in (0, \frac{1}{2\mu}]$ and $\mu \geq 2$:

$$\frac{(1-\epsilon)^\mu}{(1-\epsilon\mu)} \cdot R(\mu,j) \leq \frac{(1-\frac{1}{2\mu})^\mu}{1/2} \cdot R(\mu,2) \leq \frac{(1+\frac{1}{\mu})}{\sqrt{e}} \leq e^{\frac{1}{\mu}-1/2} \leq 1$$

This completes the proof. □

Lemma 2. *$I_\epsilon(k,\mu) \leq \epsilon^k \cdot k^\mu$ for $k \geq 2\mu$ and $\epsilon \leq 1/2$.*

This is tighter than Bound 1 for larger k, i.e. when $k^\mu < \mu^k$.

Proof. Similar to the analysis in Bound 1, define $\Psi_{\epsilon,\mu}(k) = \epsilon^k k^\mu - I_\epsilon(k,\mu)$ so that:

$$\Psi_{\epsilon,\mu}(k) = \epsilon^k k^\mu - 1 + (1-\epsilon)^\mu \sum_{j=0}^{k-1} \binom{\mu+j-1}{j} \epsilon^j$$

Bound 2 holds iff $\Psi_{\epsilon,\mu}(k) \geq 0$ for all $k \geq 2\mu$ and $\epsilon \leq 1/2$. For $\mu = 1$ we have $I_\epsilon(k,1) = \epsilon^k$ so

$$\Psi_{\epsilon,1}(k) = \epsilon^k \cdot k - \epsilon^k \geq 0$$

Furthermore, $\lim_{k\to\infty} \Psi_{\epsilon,\mu}(k) = 0$. Thus, it suffices to show that $\Psi_{\epsilon,\mu}$ is non-increasing on the interval $[2\mu,\infty)$ for $\mu \geq 2$ and $\epsilon \leq 1/2$.

Observe that:

$$\Psi_{\epsilon,\mu}(k+1) - \Psi_{\epsilon,\mu}(k) = \epsilon^{k+1}(k+1)^\mu - \epsilon^k k^\mu + (1-\epsilon)^\mu \binom{\mu+k-1}{k} \epsilon^k$$

$$= \epsilon^k \left[\epsilon(k+1)^\mu - k^\mu + (1-\epsilon)^\mu \binom{\mu+k-1}{k} \right]$$

Defining:

$$\Delta_\epsilon(k,\mu) := (1-\epsilon)^\mu \frac{\binom{\mu+k-1}{k}}{k^\mu} + \epsilon(1+\frac{1}{k})^\mu$$

$\Psi_{\epsilon,\mu}(k)$ is non-increasing on $k \in [2\mu, \infty]$ iff $\Delta_\epsilon(k,\mu) \le 1$ for all $k \ge 2\mu$. We will prove this for $\mu \ge 2$ and $\epsilon \le 1/2$. Using the inequality $(1+\frac{1}{k})^\mu \le \sqrt{e}$ for $k \ge 2\mu$:

$$\Delta_\epsilon(2\mu,\mu) \le (1-\epsilon)^\mu \frac{\binom{3n-1}{2\mu}}{(2\mu)^\mu} + \epsilon\sqrt{e}$$

The right hand side is decreasing as $\mu \to \infty$ and thus for $\mu \ge 2$ and $\epsilon \le 1/2$:

$$\Delta_\epsilon(2\mu,\mu) \le (1-\epsilon)^2 \cdot \frac{\binom{5}{4}}{4^2} + \epsilon\sqrt{e} = (1-\epsilon)^2 \cdot \frac{5}{16} + \epsilon\sqrt{e} \ < 1$$

To see why this is less than 1 for $\epsilon \le 1/2$, note that $\frac{d}{d\epsilon}(1-\epsilon)^2 \cdot c_1 + \epsilon \cdot c_2 = 2c_1\epsilon + c_2 - 2c_1$ is positive when $\epsilon \ge 0$ and $c_2 \ge 2c_1$, and $\sqrt{e} > \frac{5}{8}$. Thus, on the interval $\epsilon \in [0, \frac{1}{2}]$, $(1-\epsilon)^2\frac{5}{16} + \epsilon\sqrt{e} \le \frac{1}{4} \cdot \frac{5}{16} + \frac{1}{2}\sqrt{e} = 0.902...$

Finally, since $\Delta_\epsilon(k,\mu)$ is decreasing as $k \to \infty$:

$$\forall_{k \ge 2\mu, \mu \ge 2, \epsilon \le 1/2} \ \Delta_\epsilon(k,\mu) \le \Delta_\epsilon(2\mu,\mu) < 1$$

□

Corollary 1. *For any prime p and any positive integer μ*

$$P[\sum_{i=1}^{\mu} X_i \ge r] = I_{\frac{1}{p}}(r,\mu) \le \begin{cases} \frac{r^\mu}{p^r} \text{ if } r \ge 2\mu \\ (\frac{\mu}{p})^r \text{ if } p \ge 2\mu \\ 1 \text{ otherwise} \end{cases}$$

, where X_i are independent geometric variables with parameter $(\frac{1}{p})$ and $P[X_i \ge r] = \left(\frac{1}{p}\right)^r$

4 Inverse LCSZ (for cryptographers)

Theorem 1 (LCSZ) bounds the probability $\mathbb{P}_{\mathbf{x} \leftarrow [0,m)^\mu}[f(\mathbf{x} \equiv 0 \bmod N]$ for given values of μ, N, and m, which has the form $\frac{\mu}{m} + \delta_{N,\mu}$. In the case that N is prime, $\delta_{N,\mu} = \frac{\mu}{N}$, which agrees with the standard Schwartz-Zippel lemma applied to μ-linear polynomials. The term $\delta_{N,\mu}$ for composite N, which is dependent on both μ and the factorization of N, has a complicated closed form expression in terms of a product of regularized beta functions.

Motivated by applications to cryptography, this section analyzes the inverse: for a given $\mu, \lambda \in \mathbb{N}$ what size threshold $t(\lambda,\mu) \in \mathbb{N}$ is sufficient such that $\delta_{N,\mu} \le 2^{-\lambda}$ for all $N \ge t(\lambda,\mu)$? (Cryptographers often need to know how to choose parameters in order to achieve a target probability bound). In other words:

$$t(\lambda,\mu) := \sup\{N \in \mathbb{N} : \prod_{(p,r) \in S(N)} I_{\frac{1}{p}}(r,\mu) \ge 2^{-\lambda}\} \qquad (t(\lambda,\mu) \text{ def})$$

For $\mu = 1$, since $I_{1/p}(r,1) = \frac{1}{p^r}$ and $\prod_{(p,r)\in S(N)} I_{\frac{1}{p}}(r,\mu) = \frac{1}{N}$, it is easy to see that $t(\lambda,\mu) = 2^\lambda$. For $\mu \ge 2$, the value of $t(\lambda,\mu)$ (or even an upper bound) is not nearly as easy to derive. For the rest of this section we will focus on this $\mu \ge 2$ case. We will analytically derive an upper bound to $t(\lambda,\mu)$, showing that $\log t(\lambda,\mu) \in O(\mu^{2+\epsilon} + \frac{\lambda}{\epsilon})$ for any $\epsilon \ge \log_\mu(2)$.

Theorem 2 (Inverse LCSZ)**.** *For all $\mu \ge 2$, $\epsilon \ge \log_\mu(2)$, and all N such that*

$$\log N \ge 4\mu^{2+\epsilon} + (1 + \frac{1}{\epsilon}) \cdot \lambda$$

we have that for any μ-linear polynomial f that is coprime with N

$$\mathbb{P}_{x \leftarrow [0,m)^\mu}[f(x) \equiv 0 \bmod N] \le 2^{-\lambda} + \frac{\mu}{m}$$

By setting $\epsilon = \log_\mu(2)$ we get:

Corollary 2. *For all N such that*

$$\log N \ge 8\mu^2 + \log_2(2\mu) \cdot \lambda$$

we have that for any n-linear polynomial f that is coprime with N

$$P_{x \leftarrow [0,m)^\mu}[f(x) \equiv 0 \bmod N] \le 2^{-\lambda} + \frac{\mu}{m}$$

4.1 Proof of Inverse LCSZ (Theorem 2)

By Theorem 1 (CSZ) we have that for $N = \prod_i p_i^{r_i}$:

$$\mathbb{P}_{\mathbf{x} \leftarrow [0,m)^\mu}[f(\mathbf{x}) \equiv 0 \bmod N] \le \prod_i I_{\frac{1}{p_i}}(r_i,\mu) + \frac{\mu}{m}.$$

For $\mu = 1$ and $\log_2(N) \ge \lambda$, Theorem 1 shows that $\mathbb{P}_{x \leftarrow [0,m)}[f(x) \equiv 0 \bmod N] \le 2^{-\lambda} + \frac{1}{m}$. This is derived by substituting $I_{1/p}(r,1) = \frac{1}{p^r}$, which gives $\mathbb{P}_{x \leftarrow [0,m)}[f(x) \equiv 0 \bmod N] \le \frac{1}{N} + \frac{1}{m}$. The case $\mu \ge 2$ is more complicated. This is the focus of the rest of the proof..

For a given $N \in \mathbb{N}$, let $S(N)$ denote the set of pairs (p, r) where p is a prime divisor of N and r is its multiplicity, i.e. $N = \prod_{(p,r)\in S} p^r$. Define:

$$t(\lambda, \mu) := \sup\{N \in \mathbb{N} : \prod_{(p,r)\in S(N)} I_{\frac{1}{p}}(r, \mu) \geq 2^{-\lambda}\} \qquad (t(\lambda,\mu) \text{ def})$$

It follows from Theorem 1 (CSZ) that if $N \geq t(\lambda, \mu)$ then

$$\mathbb{P}_{\mathbf{x}\leftarrow[0,m)^\mu}[f(\mathbf{x}) \equiv 0 \bmod N] \leq 2^{-\lambda} + \frac{\mu}{m}.$$

Assuming $t(\lambda, \mu) < \infty$, we obtain the following constrained maximization problem:

$$\log_2 t(\lambda, \mu) := \max_{N\in\mathbb{N}} \log_2 N \text{ subject to } \sum_{(p,r)\in S(N)} -\log_2 I_{\frac{1}{p}}(r, \mu) \leq \lambda.$$

(Constrained Maximization 1)

In order to derive an upper bound on $\log_2 t(\lambda, \mu)$, we construct a sequence of modified maximization problems, each of which is an upper bound to the prior. The last in this sequence is a knapsack problem for which we analytically derive an upper bound.

Definition 1. *Let* $\mathsf{val}(p, r) := r \log_2 p$ *and let* $\mathsf{weight}_\mu(p, r) = -\log_2 I_{\frac{1}{p}}(r, \mu)$. *Additionally, for all* $\epsilon \geq \log_\mu(2)$, *let:*

$$\mathsf{weight}_{\mu,\epsilon}(p, r) := \begin{cases} r \cdot (\log_2(p) - \log_2(\mu)) \text{ if } p \geq \mu^{1+\epsilon} \\ r \cdot \log_2(p) - \mu \cdot \log_2(r) \text{ if } p < \mu^{1+\epsilon} \wedge r > 2(1+\epsilon)\frac{\mu \ln \mu}{\ln p} \\ 0 \text{ otherwise} \end{cases}$$

Claim 2. *For any prime* p *and* $r \in \mathbb{N}$, *if* $\epsilon \geq \log_\mu(2)$ *then* $\mathsf{weight}_\mu(p, r) \leq \mathsf{weight}_{\mu,\epsilon}(p, r)$.

Proof. If $\epsilon \geq \log_\mu(2)$ then $\mu^{1+\epsilon} \geq 2\mu$ and the claim follows from Corollary 1 (to Lemma 1 and Lemma 2). □

Claim 3. *For any prime* p, $\mathsf{weight}_{\mu,\epsilon}(p, r)$ *is non-decreasing over* $r \geq 1$ *and increasing for* $r > 2(1+\epsilon)\frac{\mu \log \mu}{\log p}$.

Proof. We first show that the function $\mathsf{weight}_{\mu,\epsilon}(p, r)$ is non-decreasing in r in each of the three cases, which comprise three subdivisions of the plane $\mathsf{Primes} \times \mathbb{N}$, which we denote S_A, S_B, and S_C respectively. S_A contains all (p, r) where $p \geq \mu^{1+\epsilon}$, in which case $\frac{d}{dr}\mathsf{weight}_{\mu,\epsilon}(p, r) = \log_2(p) - \log_2(\mu) > 0$. S_B contains all (p, r) where $r > 2(1+\epsilon)\frac{\mu \ln \mu}{\ln p}$ and $p < \mu^{1+\epsilon}$, in which case $\frac{d}{dr}\mathsf{weight}_{\mu,\epsilon}(p, r) = \log_2(p) - \frac{\mu}{r \ln 2}$, and $\log_2(p) - \frac{\mu}{r \ln 2} \geq \log_2 p - \frac{1}{2 \ln 2} > 0$. The weight function is constant at 0 for all remaining pairs, which comprise set S_C.

It remains to show that $\mathsf{weight}_{\mu,\epsilon}(p, r)$ increases in r across the boundary between S_B and S_C, for which it suffices to show that the weight is positive for all $(p, r) \in S_B$. Suppose, towards contradiction, that $r \log_2 p \leq \mu \log_2 r$ and $r > 2(1+\epsilon)\frac{\mu \log_2 \mu}{\log_2 p}$. This would imply that both $\frac{r}{\log_2 r} \leq \frac{\mu}{\log_2 p}$ and $\frac{r}{2(1+\epsilon)\log \mu} > \frac{\mu}{\log_2 p}$, which implies that $\log_2 r > 2(1+\epsilon)\log \mu$. Since $\frac{r}{\log_2 r}$ is monotonic increasing in r, this in turn implies that $\frac{r}{\log_2 r} > \frac{\mu^2}{4 \log_2 \mu} \geq \mu$ for all $\mu \geq 1$. Finally, the implication that $\frac{r}{\log_2 r} > \mu$ contradicts the assumption that $r \log_2 p \leq \mu \log_2 r$.

□

The first modified maximization problem is:

$$\max_{N\in\mathbb{N}} \sum_{(p,r)\in S(N)} \mathsf{val}(p, r) \text{ subject to } \sum_{(p,r)\in S(N)} \mathsf{weight}_{\mu,\epsilon}(p, r) \leq \lambda$$

(Constrained Maximization 2)

Claim 4. *Eq.* (Constrained Maximization 2) *is an upper bound to Eq.* (Constrained Maximization 1) *for any* μ *and* $\epsilon \geq \log_\mu(2)$*:*

Proof. For any $N \in \mathbb{N}$, by definition $\sum_{(p,r)\in S(N)} \mathsf{val}(p, r) = \log_2 N$. Thus the only difference between the two maximization problems are the constraints. Furthermore, if $\epsilon \geq \log_\mu(2)$ then, by Claim 2, Eq. (Constrained Maximization 2) is simply a relaxation of the constraints in Eq. (Constrained Maximization 1). □

Let Primes denote the infinite set of prime numbers.

Definition 2 (Marginal Value/Weight)**.** *Using* $\mathsf{val}(p, r)$ *and* $\mathsf{weight}(p, r)$ *as defined in Definition 1,* $r \geq 1$ *and* $p \in \mathsf{Primes}$, *let* $\Delta\mathsf{val}(p, r) := \mathsf{val}(p, r) - \mathsf{val}(p, r-1) = \log_2 p$ *and* $\Delta\mathsf{val}(p, 0) := \mathsf{val}(p, 0) = 0$. *Similarly, for* $r \geq 1$ *let* $\Delta\mathsf{weight}_{\mu,\epsilon}(p, r) := \mathsf{weight}_{\mu,\epsilon}(p, r) - \mathsf{weight}_{\mu,\epsilon}(p, r-1)$ *and* $\Delta\mathsf{weight}_{\mu,\epsilon}(p, 0) := \mathsf{weight}_{\mu,\epsilon}(p, 0) = 1$.

By Claim 3, $\Delta\mathsf{weight}_{\mu,\epsilon}(p, r)$ is non-negative for all prime p and $r \in \mathbb{N}$, and positive for $r > 2(1+\epsilon)\frac{\mu \log \mu}{\log p}$. The following knapsack problem gives an upper bound to Eq. (Constrained Maximization 2) :

$$\max_{S\subseteq\mathsf{Primes}\times\mathbb{N}} \sum_{(p,r)\in S} \Delta\mathsf{val}(p, r) \text{ subject to } \sum_{(p,r)\in S} \Delta\mathsf{weight}_{\mu,\epsilon}(p, r) \leq \lambda. \qquad \text{(Knapsack Problem)}$$

Claim 5. *Eq.* (Knapsack Problem) *is an upper bound to Eq.* (Constrained Maximization 2).

Proof. Le S^* denote argmax of Eq. (Knapsack Problem) with $v^* = \sum_{(p,r)\in S^*} \Delta\mathsf{val}(p,r)$ and suppose (towards contradiction) that there exists $N \in \mathbb{N}$ such that $\sum_{(p,r)\in S(N)} \mathsf{weight}_{\mu,\epsilon}(p,r) \leq \lambda$ and $\sum_{(p,r)\in S(N)} \mathsf{val}(p,r) > v^*$. Consider the set S', which includes $S(N)$ and adds for each $(p,r) \in S(N)$ the pairs (p,j) for each $j \leq r$, i.e:

$$S' = \bigcup_{(p,r)\in S(N)} \bigcup_{j=0}^{r} \{(p,j)\}$$

Observe that:

$$\sum_{(p,r)\in S'} \Delta\mathsf{val}(p,r) = \sum_{(p,r)\in S(N)} \sum_{j=0}^{r} \Delta\mathsf{val}(p,j) = \sum_{(p,r)\in S(N)} \mathsf{val}(p,r) > v^*$$

$$\sum_{(p,r)\in S'} \Delta\mathsf{weight}_{\mu,\epsilon}(p,r) = \sum_{(p,r)\in S(N)} \sum_{j=0}^{r} \Delta\mathsf{weight}_{\mu,\epsilon}(p,j) = \sum_{(p,r)\in S(N)} \mathsf{weight}_{\mu,\epsilon}(p,r) \leq \lambda$$

This is a contradiction to the assumption that v^* is the solution to Eq. (Knapsack Problem). □

Finally, we prove a series of claims that will enable us to derive an upper bound on Eq. (Knapsack Problem). First, we define:

Definition 3 (Density)**.** $\mathsf{density}_{\mu,\epsilon}(p,r) = \frac{\Delta\mathsf{val}(p,r)}{\Delta\mathsf{weight}_{\mu,\epsilon}(p,r)}$ *where* $\Delta\mathsf{val}(p,r)$ *and* $\Delta\mathsf{weight}(p,r)$ *are defined in Definition 2.*

Claim 6. *For all* $S \subseteq \mathit{Primes} \times \mathbb{N}$*:*

$$\sum_{(p,r)\in S} \Delta\mathsf{val}(p,r) \leq \sum_{(p,r)\in S} \Delta\mathsf{weight}(p,r) \cdot \max_{(p,r)\in S} \{\mathsf{density}_{\mu,\epsilon}(p,r)\}$$

Proof.

$$\begin{aligned}\sum_{(p,r)\in S} \Delta\mathsf{weight}(p,r) \cdot \max_{(p,r)\in S} \{\mathsf{density}_{\mu,\epsilon}(p,r)\} &\geq \sum_{(p,r)\in S} \mathsf{weight}_{\mu}(p,r) \cdot \mathsf{density}_{\mu,\epsilon}(p,r) \\ &= \sum_{(p,r)\in S} \mathsf{val}(p,r)\end{aligned}$$

□

Claim 7. *If* $\mu \geq 2$*,* $\epsilon \geq \log_\mu(2)$*,* $r \geq 1$*, and* $p \geq \mu^{1+\epsilon}$ *then* $\mathsf{density}_{\mu,\epsilon}(p,r) \leq 1 + \frac{1}{\epsilon}$

Proof. If $\epsilon \geq \log_\mu(2)$ and $p \geq \mu^{1+\epsilon}$ then $p \geq 2\mu$, and thus:

$$\mathsf{density}_{\mu,\epsilon}(p,r) = \frac{\Delta\mathsf{val}(p,r)}{\Delta\mathsf{weight}_{\mu,\epsilon}(p,r)} = \frac{\log p}{\log_2(p) - \log_2(\mu)}$$

Furthermore, $p \geq \mu^{1+\epsilon}$ implies that:

$$\log_2(p) - \log_2(\mu) \geq \log_2(p) - \frac{1}{1+\epsilon}\log_2(p) = \log_2(p) \cdot \frac{\epsilon}{1+\epsilon}$$

Thus $\mathsf{density}_{\mu,\epsilon}(p,r) \leq \frac{\log_2(p)}{\log_2(p)\cdot\frac{\epsilon}{1+\epsilon}} = 1 + \frac{1}{\epsilon}$ □

Claim 8. *If* $\mu \geq 2$*,* $\epsilon \geq \log_\mu(2)$*,* $r > 2(1+\epsilon)\cdot\frac{\mu\cdot\ln\mu}{\ln p}$*, and* $p < \mu^{1+\epsilon}$ *then* $\mathsf{density}_{\mu,\epsilon}(p,r) \leq 1 + \frac{1}{\epsilon}$

Proof. Since $p < \mu^{1+\epsilon}$, the conditions on r imply $r > 2(1+\epsilon)\frac{\mu\ln\mu}{\ln p} > 2\mu$ and thus:

$$\mathsf{density}_{\mu,\epsilon}(p,r) = \frac{\Delta\mathsf{val}(p,r)}{\Delta\mathsf{weight}_{\mu,\epsilon}(p,r)} = \frac{\ln p}{\ln p + \mu\ln\frac{r-1}{r}} = \frac{1}{1 - \frac{\mu}{\ln p}\ln\frac{r}{r-1}}$$

$\mathsf{density}_{\mu,\epsilon}(p,r)$ is non-negative because $\Delta\mathsf{val}(p,r)$ is non-negative and $\Delta\mathsf{weight}(p,r)$ is positive over $r > 2(1+\epsilon)\frac{\mu\log\mu}{\log p}$. Thus, for p and r satisfying these conditions, it must be the case that $0 \leq \frac{\mu}{\ln p}\ln\frac{r}{r-1} < 1$. Furthermore, this term is decreasing (approaching zero) as r increases, which shows that for r and p subject to these conditions $\mathsf{density}_{\mu,\epsilon}(p,r)$ is also decreasing in r. Combining this with the fact that $\ln\frac{r}{r-1} = \ln(1+\frac{1}{r-1}) \leq \frac{1}{r-1}$:

$$\mathsf{density}_{\mu,\epsilon}(p,r) \leq \mathsf{density}_{\mu,\epsilon}(p, 2(1+\epsilon)\frac{\mu\ln\mu}{\ln p} + 1) \leq \frac{1}{1 - \frac{\mu}{\ln p}\frac{\ln p}{2(1+\epsilon)\mu\ln\mu}} = \frac{1}{1 - \frac{1}{2(1+\epsilon)\ln\mu}} \leq 1 + \frac{1}{\epsilon}$$

□

Claim 9. *For $\alpha \in \mathbb{R}$ let $\mathsf{Primes}(\alpha)$ denote the set of prime numbers strictly less than α. For $\mu \in \mathbb{N}$ and $\epsilon \in (0,1)$ define:*

$$B_{\mu,\epsilon} := \{(p,r) : p \in \mathsf{Primes}(\mu^{1+\epsilon}), r \leq 2(1+\epsilon)\frac{\mu \ln \mu}{\ln p}\}$$

Then :

$$\sum_{(p,r)\in B_{\mu,\epsilon}} \Delta\mathsf{val}(p,r) \leq 4\mu^{2+\epsilon}$$

Proof. Let $\pi(X)$ denote the prime counting function. We use the fact that $\pi(x) \leq 1.3 \cdot \frac{x}{\ln(x)}$ for all $x > 1$ [RS62].

$$\sum_{(p,r)\in B_{\mu,\epsilon}} \Delta\mathsf{val}(p,r) = \sum_{p\in\mathsf{Primes}(\mu^{1+\epsilon})} \sum_{r=0}^{\lfloor 2(1+\epsilon)\frac{\mu\ln\mu}{\ln p}\rfloor} \log p = \sum_{\mathsf{Primes}(\mu^{1+\epsilon})} 2(1+\epsilon)\mu \log_2 \mu$$
$$\leq 1.3 \cdot \frac{\mu^{1+\epsilon}}{\ln(\mu^{1+\epsilon})} \cdot \frac{2\cdot(1+\epsilon)\mu\ln(\mu)}{\ln(2)} \leq 4\mu^{2+\epsilon}$$

□

Putting together these claims, we obtain the bound:

Claim 10. *For all $\mu \geq 2$, $\epsilon \geq \log_\mu(2)$ and $S \subseteq \mathsf{Primes} \times \mathbb{N}$:*

$$\sum_{(p,r)\in S} \Delta\mathsf{val}(p,r) \leq 4n^{2+\epsilon} + \sum_{(p,r)\in S} \Delta\mathsf{weight}_{\mu,\epsilon}(p,r)\cdot(1+\frac{1}{\epsilon})$$

Proof. Partition S into disjoint sets S_1 and S_2 such that S_2 contains all the pairs $(p,r) \in S$ for which either $p \geq \mu^{1+\epsilon}$ or $r > 2(1+\epsilon)\frac{\mu\ln\mu}{\ln p}$, and S_1 contains the remaining pairs. $S_1 \subseteq B_{\mu,\epsilon}$ from Claim 9 and thus $\sum_{(p,r)\in S_1} \Delta\mathsf{val}(p,r) \leq 4\mu^{2+\epsilon}$. Furthermore, by Claim 7, if $(p,r) \in S_2$ then $\mathsf{density}_{\mu,\epsilon}(p,r) \leq 1 + \frac{1}{\epsilon}$ and by Claim 6:

$$\sum_{(p,r)\in S_2} \Delta\mathsf{val}(p,r) \leq \sum_{(p,r)\in S_2} \Delta\mathsf{weight}_{\mu,\epsilon}(p,r)\cdot(1+\frac{1}{\epsilon})$$

Putting everything together:

$$\sum_{(p,r)\in S} \Delta\mathsf{val}(p,r) = \sum_{(p,r)\in S_1} \Delta\mathsf{val}(p,r) + \sum_{(p,r)\in S_2} \Delta\mathsf{val}(p,r) \leq 4n^{2+\epsilon} + \sum_{(p,r)\in S} \Delta\mathsf{weight}_{\mu,\epsilon}(p,r)\cdot(1+\frac{1}{\epsilon})$$

□

Finally, we can conclude from Claim 10 that for any $S \in \mathsf{Primes}\times\mathbb{N}$, $\mu \geq 2$, and $\epsilon \geq \log_\mu(2)$, if $\sum_{(p,r)\in S} \Delta\mathsf{weight}_{\mu,\epsilon}(p,r) \leq \lambda$, i.e., if S satisfies the constraints of Eq. (Knapsack Problem) then:

$$\sum_{(p,r)\in S} \Delta\mathsf{weight}_{\mu,\epsilon}(p,r) \leq 4n^{2+\epsilon} + \lambda\cdot(1+\frac{1}{\epsilon})$$

The right hand side of the equation is therefore an upper bound for the solution to Eq. (Knapsack Problem), and consequently (by Claim 12 and Claim 5), an upper bound for the solution $t(\lambda,\mu)$ to Eq. (Constrained Maximization 1) when $\mu \geq 2$. In conclusion, for any $N \in \mathbb{N}$, $\mu \geq 2$, and $\epsilon \geq \log_\mu(2)$, if $\log_2 N \geq 4n^{2+\epsilon} + \lambda\cdot(1+\frac{1}{\epsilon})$ then $\log_2 N \geq t(\lambda,\mu)$ and:

$$\mathbb{P}_{\mathbf{x}\leftarrow[0,m)^\mu}[f(\mathbf{x}) \equiv 0 \bmod N] \leq 2^{-\lambda} + \frac{\mu}{m}$$

4.2 Computational Inverse LCSZ

Theorem 2 provides an analytical upper bound on $t(\lambda,\mu)$ for any $\mu,\lambda \in \mathbb{N}$. However, the analytical bound does not appear to be tight for $\mu \geq 2$ (for $\mu = 1$ it is tight). This next section provides an algorithm to derive an upper bound on $t(\lambda,\mu)$ for any specific values of λ,μ. The algorithm gives tighter bounds than Theorem 2 for a table of tested values (Table 1). This is useful in practice, e.g. for deriving concrete cryptographic security parameters in cryptographic protocols that rely on LCSZ.

As shown in the prior section, $t(\lambda,\mu)$ is upper bounded by a solution to a knapsack problem, Eq. (Knapsack Problem), over the infinite set of items $\mathsf{Primes}\times\mathbb{N}$. There is a simple well-known greedy algorithm that returns an upper bound to the optimal value for the knapsack problem over a *finite* set of items. This algorithm greedily adds items to the knapsack in order of decreasing density until the knapsack overflows the weight bound, and returns the total value of the added items at this point. Over an infinite set of items, it is not generally possible to sort by decreasing density. However, by leveraging monotonicity properties of the density function in our case, we are able to adapt the greedy approximation algorithm to work for Eq. (Knapsack Problem). In particular, we are able to enumerate over pairs in $\mathsf{Primes}\times\mathbb{N}$ in an order of non-increasing density.

Claim 11. *Let A and B be any pair of discrete strictly ordered sets which contain minimum elements $a_0 \in A$ and $b_0 \in B$. Let $a+$ denote the next element of A after a and likewise $b+$ the next element of B after b. If $f : A \times B \to \mathbb{R}^+$ is monotonically non-increasing over pairs (a, b_0) as $a \in A$ increases, and for any fixed a, monotonically non-increasing over pairs (a, b) as $b \in B$ increases, then the following algorithm enumerates the pairs $(a, b) \in A \times B$ in order of decreasing $f(a, b)$. The algorithm initializes the set $C = \{(a_0, b_0)\}$ and also a variable max_A to keep track of the highest order element in A seen so far. At each iteration, it removes a pair $(a, b) \in C$ of lowest $f(a, b)$ value and appends (a, b) to the output enumeration list. Before proceeding to the next iteration, it adds $(a, b+)$ to C, and if $a = \mathsf{max}_A$ then it also adds $(a+, b_0)$ to C and updates $\mathsf{max}_A := a+$.*

Proof. Suppose, towards contradiction, that the algorithm appends (a, b) to the output list, and there exists at least one pair (a', b') not yet in the list at this iteration such that $f(a', b') > f(a, b)$. If $b' \neq b_0$ and (a', b_0) appeared in the output list already, then each (a', b^*) for $b^* \in [b_0, b']$ would also have been added to C and removed before (a, b) because $f(a', b^*) \geq f(a', b') > f(a, b)$. This would be a contradiction, so it remains to consider the case that $b' = b_0$, i..e. that (a', b_0) did not appear in the list and $f(a', b_0) > f(a, b)$.

First, this implies that $a' > a$. Otherwise, If $a' \leq a$, then (a', b_0) would have been added to C before (a, b) and thus removed before (a, b). Second, $b \neq b_0$ and $f(a, b) < f(a, b_0)$, as otherwise this would imply that $f(a', b_0) > f(a, b) \geq f(a, b_0)$, contradicting the monotonicity property. Thus (a, b_0) must already appear in the output list because it is added to C before (a, b) and removed before (a, b). Furthermore, for all $a^* \in [a, a']$, $f(a^*, b_0) \geq f(a', b_0) > f(a, b)$, thus each such pair (a^*, b_0) would have been added and removed before (a, b). This is a contradiction. □

We use the enumeration algorithm of Claim 11 to implement the greedy algorithm that obtains an upper bound to a generic knapsack problem over the infinite set of items $\mathsf{Primes} \times \mathbb{N}$:

$$\max_{S \subseteq \mathsf{Primes} \times \mathbb{N}} \sum_{(p,r) \in S} \mathsf{val}(p, r) \text{ subject to } \sum_{(p,r) \in S} \mathsf{weight}(p, r) \leq \lambda. \quad \text{(Generic Knapsack Problem)}$$

for any $\mathsf{val}, \mathsf{weight} : \mathsf{Primes} \times \mathbb{N} \to \mathbb{R}^+$ where $\mathsf{density}(p, r) = \frac{\mathsf{val}(p,r)}{\mathsf{weight}(p,r)}$ is monotonic non-increasing over r for any fixed p, and also over p for fixed $r = 1$. This is presented below as Algorithm 1.

Algorithm 1 Greedy algorithm that returns an upper bound to Eq. (Constrained Maximization 2)

Input $\mu \in \mathbb{N}, \lambda \in \mathbb{N}$

1. Initialize a max heap H that stores tuples $(p, r, d) \in \mathbb{P} \times \mathbb{Z} \times \mathbb{R}$ and sorts them by the third value.
2. Initialize $w \leftarrow 0$ and $v \leftarrow 0$.
3. Push $(\mathsf{density}(2, 1), 2, 1)$ onto the heap and set $\mathsf{pmax} = 2$.
4. While $w < \lambda$
5. (a) Pop (p, r, d) from H.
   (b) Push $(p, r + 1, (\mathsf{density}(p, r + 1))$ onto H
   (c) Set $v \leftarrow v + \mathsf{val}(p, r)$
   (d) Set $w \leftarrow w + \mathsf{weight}(p, r)$
   (e) If $p = \mathsf{pmax}$ then set $\mathsf{pmax} \leftarrow \mathsf{next\_prime}(p)$ and push $(\mathsf{density}(\mathsf{pmax}, 1), \mathsf{pmax}, 1)$ onto H
6. Output v

Moreover, we will show that the density function defined in terms of $\mathsf{val}(p, r) = \log p$, $\mathsf{weight}(p, 1) = -\log I_{1/p}(1, \mu)$, and $\mathsf{weight}(p, r) = \log I_{1/p}(r - 1,) - \log I_{1/p}(r, \mu)$ for $r > 1$ satisfies this monotonicity property. The density function in Eq. (Knapsack Problem) also has this monotonicity property, but we are able to obtain a tighter bound on Eq. (Constrained Maximization 1) by defining regularized beta function directly instead of the simpler form upper bounds on the regularized beta function that were more useful for deriving the analytical result in Theorem 2.

Claim 12. *Eq.* (Generic Knapsack Problem) *with* $\mathsf{density}(p, r) = \frac{\mathsf{val}(p,r)}{\mathsf{weight}(p,r)}$, $\mathsf{val}(p, r) = \log p$, *and* $\mathsf{weight}(p, r) = \log I_{1/p}(r - 1, \mu) - \log I_{1/p}(r, \mu)$ *is an upper bound to Eq.* (Constrained Maximization 1).

Proof. The analysis is the same as in Claim 5, replacing $\Delta\mathsf{weight}_{\mu,\epsilon}$ with the weights defined here. □

Claim 13. *For $p \in \mathbb{P}, r \in \mathbb{N}$ and $\mu \geq 2 \in \mathbb{N}$ let* $\mathsf{density}(p, r) = \frac{\mathsf{val}(p,r)}{\mathsf{weight}(p,r)}$ *where* $\mathsf{val}(p, r) = \log p$, *and* $\mathsf{weight}(p, r) = \log I_{1/p}(r - 1, \mu) - \log I_{1/p}(r, \mu)$ *for $r \geq 1$. Then* $\mathsf{density}(p, r)$ *is decreasing in r and* $\mathsf{density}(p, 1)$ *is non-increasing in p.*

Proof. **Part 1: $\mathsf{density}(p,r)$ is decreasing in r**

$\mathsf{density}(p,r) = \frac{\log p}{\mathsf{weight}(p,r)}$ is decreasing in r iff $\mathsf{weight}(p,r)$ is increasing in r.

$$\mathsf{weight}(p,r) = -\log I_{1/p}(r,\mu) + \log I_{1/p}(r-1,\mu) = \log \frac{I_{1/p}(r-1,\mu)}{I_{1/p}(r,\mu)}$$

is decreasing in r if $\frac{I_{1/p}(r-1,\mu)}{I_{1/p}(r,\mu)}$ is decreasing in r. This is the case if for all r

$$\frac{I_{1/p}(r,\mu)}{I_{1/p}(r+1,\mu)} - \frac{I_{1/p}(r-1,\mu)}{I_{1/p}(r,\mu)} > 0$$

. Which is equivalent to showing that

$$I_{1/p}(r,\mu)\cdot I_{1/p}(r,\mu) - I_{1/p}(r-1,\mu)\cdot I_{1/p}(r-1,\mu) > 0 \tag{6}$$

The regularized beta function $I_x(a,b)$ is log convave for all $b > 1$ as shown in [Kar15]. This implies that for $b > 1$ and all $\alpha, \beta > 0$ $I_x(a+\alpha,b)\cdot I_x(a+\beta,b) - I_x(a,b)\cdot I_x(a+\alpha+\beta,b) > 0$. Setting $a = r-1, b = \mu, \alpha = 1, \beta = 1$ this shows that Eq. (6) holds and weight is incresing in r, and $\mathsf{density}$ is decreasing in r for all $\mu > 1$.

Part 2: $\mathsf{density}(p,1)$ is non-increasing in p.

$$\mathsf{density}(p,1) = \frac{\log p}{\mathsf{weight}(p,1)} = \frac{\ln p}{-\ln(1-(1-p^{-1})^{\mu})}$$

The derivative $\frac{d}{dp}\mathsf{density}(p,1)$ is non-negative iff:

$$-p^{-1}\cdot\ln(1-(1-p^{-1})^{\mu}) - \frac{\ln p\cdot\mu(1-p^{-1})^{\mu-1}\cdot p^{-2}}{1-(1-p^{-1})^{\mu}} \geq 0$$

Equivalently:

$$-\ln(1-(1-p^{-1})^{\mu}) - \frac{\ln p\cdot\mu(1-p^{-1})^{\mu-1}p^{-1}}{1-(1-p^{-1})^{\mu}} \geq 0$$

Set $x = 1-\frac{1}{p}$, which increases over the range $(1/2,1)$ as p increases in the range $[2,\infty)$. The requisite inequality for $x \in (1/2,1)$ becomes:

$$-\ln(1-x^{\mu}) + \frac{\ln(1-x)\cdot\mu\cdot x^{\mu-1}(1-x)}{1-x^{\mu}} \geq 0$$

which, rearranging terms, holds true iff for $x \in (1/2,1)$:

$$\frac{\ln(1-x^{\mu})(1-x^{\mu})}{\ln(1-x)(1-x)x^{\mu-1}} \leq \mu$$

In fact we can show this inequality holds true over all $x \in (0,1)$. Using the inequalities $\ln(1-x^{\mu}) \leq -x^{\mu}$ and $-\ln(1-x) \geq x$ we obtain:

$$\frac{\ln(1-x^{\mu})(1-x^{\mu})}{\ln(1-x)(1-x)x^{\mu-1}} \leq \frac{x^{\mu}(1-x^{\mu})}{x(1-x)x^{\mu-1}} = \frac{1-x^{\mu}}{1-x} \leq \mu$$

□

Theorem 3 (Computational bound)**.** *Let k be the output of algorithm Algorithm 1 on input λ,μ. Then for all $m \in \mathbb{N}$, all $N \geq 2^k$ and all μ-linear polynomials f, coprime with N, $\log_2 N \geq t(\lambda,\mu)$ and*

$$P_{\mathbf{x}\leftarrow[0,m)^{\mu}}[f(\mathbf{x}) \equiv 0 \bmod N] \leq 2^{-\lambda} + \frac{\mu}{m}$$

Proof. Algorithm 1 is a greedy enumeration algorithm over pairs (p,r) following the enumeration strategy in Claim 11. By Claim 13, $\mathsf{density}$ satisfies the monotonicity conditions required for Claim 11 and thus the enumeration algorithm enumerates pairs in order of non-increasing density. Thus, the algorithm outputs an upper bound to Eq. (Generic Knapsack Problem) with density $\mathsf{density}(p,r) = \frac{\mathsf{val}(p,r)}{\mathsf{weight}(p,r)}$, $\mathsf{val}(p,r) = \log p$, and $\mathsf{weight}(p,r) = \log I_{1/p}(r-1,\mu) - \log I_{1/p}(r,\mu)$. By Claim 12 this is an upper bound to Eq. (Constrained Maximization 1) which in turn by Theorem 1 gives a bound on $\log_2 t(\lambda,\mu)$. □

4.3 Computational Results

Using Algorithm 1 we computed analytical bounds for all $\mu \in (1,50)$ for different values of λ. The precise bound for $\mu = 20$ and $\lambda = 120$ is

$$\begin{aligned}2^v = {} & 2^{36}\cdot 3^{20}\cdot 5^{11}\cdot 7^8\cdot 11^5\cdot 13^5\cdot 17^4\cdot 19^3\cdot 23^3\cdot 29^2\cdot 31^2\cdot 37^2\cdot 41^2\cdot 43^2\cdot 47^2\cdot 53^2\cdot 59\cdot 61\cdot 67\\ & \cdot 71\cdot 73\cdot 79\cdot 83\cdot 89\cdot 97\cdot 101\cdot 103\cdot 107\cdot 109\cdot 113\cdot 127\cdot 131\cdot 137\cdot 139\cdot 149\cdot 151\cdot 157\cdot 163\end{aligned}$$

Other results are presented in their logarithmic form in Table 1. The results are significantly tighter than the analytical Theorem 2. For $n = 20$ and $\lambda = 120$ the analytical theorem gives a value for $\log_2(N)$ of 3839 vs the computational which is 416. We also provide the open-source Python implementation of the algorithm on Github[5].

[5] `https://github.com/bbuenz/Composite-Schwartz-Zippel`

μ	$\lambda = 40$	$\lambda = 100$	$\lambda = 120$	$\lambda = 240$
1	40	100	120	240
2	57	130	156	290
3	67	148	175	328
4	79	169	197	359
5	86	187	212	386
6	97	200	234	415
7	107	214	244	435
8	113	227	260	459
9	122	237	277	483
10	133	252	289	500
11	139	263	301	523
12	148	276	315	540
13	152	291	331	565
14	160	304	344	576
15	168	314	354	600
16	178	323	366	616
17	186	335	381	634
18	193	347	391	653
19	198	356	407	664
20	207	368	416	679
21	216	378	429	695
22	222	389	437	718
23	228	402	448	732
24	233	411	464	749
25	241	420	472	758
26	248	432	481	772
27	256	438	492	792
28	264	452	506	806
29	275	460	516	820
30	278	469	527	831
50	419	662	736	1105

Table 1: Computationally determined values of $t(\lambda, \mu)$ such that for all $N \geq t(\lambda, \mu)$, $\mathbb{P}_{\mathbf{x} \leftarrow [0,m)^\mu}[f(\mathbf{x}) \equiv 0 \bmod N] \leq 2^{-\lambda} + \frac{\mu}{m}$ for different μ and different λ

References

[ACK21] Thomas Attema, Ronald Cramer, and Lisa Kohl. *A Compressed Σ-Protocol Theory for Lattices*. Cryptology ePrint Archive, Report 2021/307. https://ia.cr/2021/307. 2021.

[Aru+22] Arasu Arun et al. "Dew: Transparent Constant-sized zkSNARKs". In: *IACR Cryptol. ePrint Arch.* (2022), p. 419. URL: https://eprint.iacr.org/2022/419.

[Att+22] Thomas Attema et al. "Vector Commitments over Rings and Compressed Σ-Protocols". In: *IACR Cryptol. ePrint Arch.* (2022), p. 181. URL: https://eprint.iacr.org/2022/181.

[BCS21] Jonathan Bootle, Alessandro Chiesa, and Katerina Sotiraki. "Sumcheck Arguments and Their Applications". In: *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part I*. Ed. by Tal Malkin and Chris Peikert. Vol. 12825. Lecture Notes in Computer Science. Springer, 2021, pp. 742–773. DOI: 10.1007/978-3-030-84242-0_26. URL: https://doi.org/10.1007/978-3-030-84242-0_26.

[BFS20] Benedikt Bünz, Ben Fisch, and Alan Szepieniec. "Transparent SNARKs from DARK compilers". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2020, pp. 677–706.

[Bis+15] Anurag Bishnoi et al. *On zeros of a polynomial in a finite grid*. 2015. DOI: 10.48550/ARXIV.1508.06020. URL: https://arxiv.org/abs/1508.06020.

[Blo+21] Alexander R. Block et al. “Time- and Space-Efficient Arguments from Groups of Unknown Order”. In: *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part IV*. Ed. by Tal Malkin and Chris Peikert. Vol. 12828. Lecture Notes in Computer Science. Springer, 2021, pp. 123–152. DOI: 10.1007/978-3-030-84259-8_5. URL: https://doi.org/10.1007/978-3-030-84259-8_5.

[Che+19] Shuo Chen et al. *Verifiable Computing for Approximate Computation*. Cryptology ePrint Archive, Report 2019/762. https://ia.cr/2019/762. 2019.

[CMT12] Graham Cormode, Michael Mitzenmacher, and Justin Thaler. “Practical verified computation with streaming interactive proofs”. In: *Innovations in Theoretical Computer Science 2012, Cambridge, MA, USA, January 8-10, 2012*. Ed. by Shafi Goldwasser. ACM, 2012, pp. 90–112. DOI: 10.1145/2090236.2090245. URL: https://doi.org/10.1145/2090236.2090245.

[DL77] Richard A DeMillo and Richard J Lipton. *A Probabilistic Remark on Algebraic Program Testing*. Tech. rep. GEORGIA INST OF TECH ATLANTA SCHOOL OF INFORMATION and COMPUTER SCIENCE, 1977.

[GRK17] Shafi Goldwasser, Guy N. Rothblum, and Yael Tauman Kalai. “Delegating Computation: Interactive Proofs for Muggles”. In: *Electron. Colloquium Comput. Complex.* (2017), p. 108. URL: https://eccc.weizmann.ac.il/report/2017/108.

[Kar15] Dmitrii Karp. *Normalized incomplete beta function: log-concavity in parameters and other properties*. 2015. DOI: 10.48550/ARXIV.1509.05120. URL: https://arxiv.org/abs/1509.05120.

[KI04] Valentine Kabanets and Russell Impagliazzo. “Derandomizing Polynomial Identity Tests Means Proving Circuit Lower Bounds”. In: *Comput. Complex.* 13.1-2 (2004), pp. 1–46. DOI: 10.1007/s00037-004-0182-6. URL: https://doi.org/10.1007/s00037-004-0182-6.

[RS62] J Barkley Rosser and Lowell Schoenfeld. “Approximate formulas for some functions of prime numbers”. In: *Illinois Journal of Mathematics* 6.1 (1962), pp. 64–94.

[Sch80] Jacob T Schwartz. “Fast probabilistic algorithms for verification of polynomial identities”. In: *Journal of the ACM (JACM)* 27.4 (1980), pp. 701–717.

[Set20] Srinath T. V. Setty. “Spartan: Efficient and General-Purpose zkSNARKs Without Trusted Setup”. In: *Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part III*. Ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12172. Lecture Notes in Computer Science. Springer, 2020, pp. 704–737. DOI: 10.1007/978-3-030-56877-1_25. URL: https://doi.org/10.1007/978-3-030-56877-1_25.

[SL20] Srinath T. V. Setty and Jonathan Lee. “Quarks: Quadruple-efficient transparent zkSNARKs”. In: *IACR Cryptol. ePrint Arch.* (2020), p. 1275. URL: https://eprint.iacr.org/2020/1275.

[Zip79] Richard Zippel. “Probabilistic algorithms for sparse polynomials”. In: *International symposium on symbolic and algebraic manipulation*. Springer. 1979, pp. 216–226.