AN ABSTRACT OF THE THESIS OF

Douglas James Limmer for the degree of Doctor of Philosophy in Mathematics presented on May 7, 1999 Title Measure-Equivalence of Quadratic Forms

Signature redacted for privacy

Abstract approved

Robert O Robson

This paper examines the probability that a random polynomial of specific degree over a field has a specific number of distinct roots in that field Probabilities are found for random quadratic polynomials with respect to various probability measures on the real numbers and p-adic numbers In the process, some properties of the p-adic integer uniform random variable are explored

The measure Witt ring, a generalization of the canonical Witt ring, is introduced as a way to link quadratic forms and measures, and examples are found for various fields and measures Special properties of the Haar measure in connection with the measure Witt ring are explored

Higher-degree polynomials are explored with the aid of numerical methods, and some conjectures are made regarding higher-degree p-adic polynomials Other open questions about measure Witt rings are stated

©Copyright by Douglas James Limmer

May 7, 1999

All rights reserved

Measure-Equivalence of Quadratic Forms

by

Douglas James Limmer

A Thesis

submitted to

Oregon State University

in partial fulfillment of
the requirements for the
degree of

Doctor of Philosophy

Presented May 7, 1999
Commencement June 1999

Doctor of Philosophy thesis of Douglas James Limmer presented on May 7, 1999

APPROVED

Signature redacted for privacy

Major Professor, representing Mathematics

Signature redacted for privacy

Chair of the Department of Mathematics

Signature redacted for privacy

Dean of the Graduate School

I understand that my thesis will become part of the permanent collection of Oregon State University libraries My signature below authorizes release of my thesis to any reader upon request

Signature redacted for privacy

Douglas James Limmer, Author

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

MEASURE-EQUIVALENCE OF QUADRATIC FORMS

1. Introduction

This paper investigates the probability, P_d^k, that a degree d random polynomial has k distinct roots, over a variety of fields and using a variety of probability measures Historically, much work has gone into finding the asymptotic value of this probability, or the expected number of roots, but not much has been done to find exact probabilities We are interested in the exact probabilites

We started by using elementary methods to determine the probability for low-degree polynomials with common fields and probability measures In the p-adic numbers, these methods led to an investigation of p-adic analysis, as well as the properties of p-adic integer random variables, and proved the following theorem

Theorem: Let A, B, and C be independent uniformly-distributed random variables on the p-adic integers (where p is odd) Then, the probability that $Ax^2 + Bx + C$ has two distinct roots is $1/2$

The simplicity of this value, and the fact that the probability is the same for all odd p, led us to investigate the reason that the values are the same Also, it led to a search for a simpler method for finding the probability, which might be generalized to higher-degree polynomials Attempting to find a reason for the probabilities being the same for different fields led to the construction of the measure Witt ring The

measure Witt ring is a modification of the canonical Witt ring, which allows an equivalence of the theory of quadratic forms over different fields

This paper finds the probabilities P_2^k for the field of real numbers for both the uniform probability measure on the interval $[-1, 1]$ and the standard normal probability distribution, and for the uniform distribution on the p-adic integers with p odd In the process, the implicit function theorem for p-adic numbers is presented The measure Witt ring is constructed, and its relation to the canonical Witt ring is shown Examples are also presented for Lebesgue and standard Gaussian measure on the real numbers, and for uniform measure on finite fields and the p-adic numbers Some information on the measure Witt ring for the uniform probability measure on the interval $[-1, 1]$ in the real numbers is also found In the process, the following properties were found

Theorem: For Lebesgue measure on the real numbers, Haar measure on the p-adic numbers with p odd, and uniform measure on finite fields, the measure Witt ring is isomorphic to the canonical Witt ring

Theorem: For a field with Haar measure μ with the property that

$$\mu(A \times B) = \mu(cA \times c^{-1}B)$$

for all non-zero field elements c and all measurable sets A and B in the field, the measure Witt ring is isomorphic to the canonical Witt ring

Theorem: For the standard normal measure on the real numbers, the measure Witt ring is not isomorphic to the canonical Witt ring

The probability P_2^2 for p-adic random quadratic polynomials, and numerical evidence for higher degree polynomials, suggests the following

Conjecture: The probability that a degree d random polynomial with uniformly-distributed p-adic integer coefficients has k roots is the same as the probability that a random d-permutation has k fixed points

2. The P-adic Implicit Function Theorem

For a proof in the next chapter of this thesis, the implicit function theorem is used The real-number version can be stated as follows

Theorem: *The Implicit Function Theorem* Let $\vec{f}$ be a continuously differentiable map from an open set $E \subset \mathbb{R}^{n+m}$ into $\mathbb{R}^n$, such that $\vec{f}(\vec{a}, \vec{b}) = \vec{0}$ for some point $(\vec{a}, \vec{b}) \in E$ Let $A = D\vec{f}(\vec{a}, \vec{b})$ Split A into A_x and A_y by $A_x(\vec{x}) = A(\vec{x}, \vec{0})$ for $\vec{x} \in \mathbb{R}^n$, and $A_y(\vec{y}) = A(\vec{0}, \vec{y})$ for $\vec{y} \in \mathbb{R}^m$ Further assume that A_x is invertible Then there exists open sets $U \subset \mathbb{R}^{n+m}$ and $W \subset \mathbb{R}^n$ with $(\vec{a}, \vec{b}) \in U$ and $\vec{b} \in W$, having the following property

To every $\vec{y} \in W$ there corresponds a unique $\vec{x}$ such that $(\vec{x}, \vec{y}) \in U$ and $\vec{f}(\vec{x}, \vec{y}) = 0$

If this $\vec{x}$ is defined to be $\vec{g}(\vec{y})$, then $\vec{g}$ is a continuously differentiable map of W into $\mathbb{R}^n$, $\vec{g}(\vec{b}) = \vec{a}$, $\vec{f}(\vec{g}(\vec{y}), \vec{y}) = \vec{0}$ $(\vec{y} \in W)$, and $D\vec{g}(\vec{b}) = -(A_x)^{-1}A_y$

This statement of the implicit function theorem appears in [10] as Theorem 9 28 The implicit function theorem also applies in situations other than the real numbers, for instance, an implicit function theorem for real closed fields and semi-algebraic functions appears in [2, §2 9]

This section of the thesis proves the implicit function theorem for the p-adic numbers It follows the proof given in [10] almost exactly

2.1 P-adic Numbers

Let p be an odd prime Define an absolute value on the integers by letting $|n|_p = p^{-k}$ for every integer n, if $n = p^k a$, where a and p are relatively prime Extend this to the rational numbers by letting $|n^{-1}|_p = |n|_p^{-1}$ The p-adic numbers, symbolized by $\mathbb{Q}_p$, are the topological completion of the rational numbers with this

absolute value The closed unit ball around 0, that is, the set of p-adic numbers with absolute value less than or equal to 1, is called the p-adic integers, and symbolized by $\mathbb{Z}_p$

$\mathbb{Z}_p$ can also be seen as an inverse limit

$$\mathbb{Z}/p^1\mathbb{Z} \leftarrow \mathbb{Z}/p^2\mathbb{Z} \leftarrow \mathbb{Z}/p^3\mathbb{Z} \leftarrow$$

is a sequence of groups, with the arrow from $\mathbb{Z}/p^n\mathbb{Z}$ to $\mathbb{Z}/p^{n-1}\mathbb{Z}$ indicates the function which takes $[k]$, an element of $\mathbb{Z}/p^n\mathbb{Z}$, to $[k \pmod{p^{n-1}}]$ in $\mathbb{Z}/p^{n-1}\mathbb{Z}$ $\mathbb{Z}_p$ is the inverse limit of this sequence Later, this will lead to a definition of a measure on the p-adic integers

Any p-adic number β can be uniquely written as $\beta = p^k\alpha$, where α is a p-adic unit, that is, a p-adic integer relatively prime to p $|\alpha|_p = 1$, so $|\beta|_p = p^{-k}$ Also, β can be written uniquely as

$$\beta = \sum_{i=k}^{\infty} b_i p^i$$

where each b_i is in the set $\{0, 1, \quad p-1\}$, and b_k is not zero If β is a p-adic integer, then $k \geq 0$, and β can be written as $\sum_{i=0}^{\infty} b_i p^i$ where b_0 can now be zero Under the inverse limit model, this β gets mapped to $\sum_{i=0}^{n-1} b_i p^i$ in $\mathbb{Z}/p^n\mathbb{Z}$

A p-adic number $\beta = p^k\alpha$ is a square if and only if α is a square and k is even Since p is odd, Hensel's Lemma (See [7, p 16]) shows that a unit α is a square if and only if α is a square modulo p

2.2 *P*-adic Norms and Linear Functions

Let $\vec{x} = (x_1, \quad, x_n) \in \mathbb{Q}_p^n$ Define a norm $|\vec{x}| = \max_{1 \leq i \leq n} |x_i|_p$ This norm, in fact, satisfies the strong triangle inequality

$$\begin{aligned}|\vec{x}+\vec{y}| &= \max_{1\le i\le n} |x_i+y_i|_p \\ &\le \max_{1\le i\le n} (\max\{|x_i|_p, |y_i|_p\}) \\ &= \max(\max_{1\le i\le n} |x_i|_p, \max_{1\le i\le n} |y_i|_p) \\ &= \max(|\vec{x}|, |\vec{y}|)\end{aligned}$$

Note that $|\vec{x}|$ is always of the form p^n for some integer n In particular, statements like $|\vec{x}|\vec{x}$ make sense, since the value of the norm is rational

Let A be a linear function from $\mathbb{Q}_p^n$ to $\mathbb{Q}_p^m$ Define the norm $\|A\|$ to be the supremum of all numbers $|A\vec{x}|$ where $\vec{x}$ ranges over all vectors in $\mathbb{Q}_p^n$ with $|\vec{x}| \le 1$, or $\mathbb{Z}_p^n$ Note that $|A\vec{x}| \le \|A\|\ |\vec{x}|$ for all x, if there is some $\vec{x}$ which is an exception, the unit vector $\vec{y} = |\vec{x}|\vec{x}$ would give a vector of norm 1 with $\|A\| < |A\vec{y}|$

This norm on the set of linear functions from $\mathbb{Q}_p^n$ to $\mathbb{Q}_p^m$, denoted $L(\mathbb{Q}_p^n, \mathbb{Q}_p^m)$, gives a topology, so that terms such as "open set" and "continuous" make sense on this set Denote the set of linear functions from $\mathbb{Q}_p^n$ to itself as $L(\mathbb{Q}_p^n)$

Lemma: If $A \in L(\mathbb{Q}_p^n, \mathbb{Q}_p^m)$, then $\|A\| < \infty$

Proof: Let $\{\vec{e}_1, \quad, \vec{e}_n\}$ be the standard basis for $\mathbb{Q}_p^n$ and suppose $\vec{x} = \sum c_i\vec{e}_i$ with $|\vec{x}| \le 1$, so that $|c_i|_p \le 1$ for all i Then

$$|A\vec{x}| = |\sum c_i A\vec{e}_i| \le \sum |c_i|_p |A\vec{e}_i| \le \sum |A\vec{e}_i| \ \le \infty$$

for all $\vec{x}$ Thus, $\|A\| \le \sum |A\vec{e}_i| < \infty$ □

Theorem: Let Ω be the set of all invertible linear functions in $L(\mathbb{Q}_p^n)$ Then, if $A \in \Omega$, $B \in L(\mathbb{Q}_p^n)$, and $\|B-A\|\ \ \|A^{-1}\| < 1$, then $B \in \Omega$ Also, Ω is open in $L(\mathbb{Q}_p^n)$, and the map $A \to A^{-1}$ is continuous on Ω

Proof: Define α so that $\|A^{-1}\| = 1/\alpha$, and let $\beta = \|B-A\|$ Then $\beta < \alpha$ Let $\vec{x}$ be any vector in $\mathbb{Q}_p^n$ Then

$$\begin{aligned}\alpha|\vec{x}| &= \alpha|A^{-1}A\vec{x}| \\ &\leq \alpha\|A^{-1}\| \ \ |A\vec{x}| \\ &= |A\vec{x}| \\ &\leq |(A-B)\vec{x}| + |B\vec{x}| \\ &\leq \beta|\vec{x}| + |B\vec{x}|,\end{aligned}$$

so that $(\alpha-\beta)|\vec{x}| \leq |B\vec{x}|$ for all $\vec{x}$

Since $\alpha - \beta > 0$, $|B\vec{x}| = 0$ only if $|\vec{x}| = 0$ Thus, B is one-to-one, so B is invertible Since this is true for all B with $\|B - A\| < \alpha$, Ω is open

Since B is invertible, $B^{-1}\vec{y} \in \mathbb{Q}_p^n$ for all $\vec{y}$, so that

$$(\alpha-\beta)|B^{-1}\vec{y}| \leq |B(B^{-1}\vec{y})| = |\vec{y}|$$

for all $\vec{y}$ Thus, $\|B^{-1}\| \leq (\alpha-\beta)^{-1}$ For any two linear transformations C and D,

$$|(DC)\vec{x}| = |D(C\vec{x})| \leq \|D\| \ |C\vec{x}| \leq \|D\| \ \|C\| \ |\vec{x}|,$$

so that $\|DC\| \leq \|D\| \ \|C\|$ Also, for any two linear transformations C and D,

$$D^{-1} - C^{-1} = (D^{-1})(C-D)(C^{-1}),$$

so that for A and B,

$$\|B^{-1} - A^{-1}\| \leq \|B^{-1}\| \ \|A-B\| \ \|A^{-1}\| \leq \frac{\beta}{\alpha(\alpha-\beta)}$$

As $B \to A$, $\beta \to 0$, so that $\|B^{-1} - A^{-1}\| \to 0$ Thus, the inverse map is continuous

□

2.3 *P*-adic Differentiation

One can, as usual, define the derivative of a p-adic function if $f \ \ \mathbb{Q}_p \to \mathbb{Q}_p$ and $x \in \mathbb{Q}_p$, then

$$f'(x) = \lim_{h \to 0} \frac{f(x+h) - f(x)}{h}$$

if the limit exists Thus, $f(x+h) - f(x) = f'(x)h + r(h)$, where the remainder $r(h)$ is 'small', that is, $\lim_{h \to 0} r(h)/h = 0$

Similarly, a multi-variable derivative can be defined if $\vec{f}$ $\mathbb{Q}_p^n \to \mathbb{Q}_p^m$ and $\vec{x} \in \mathbb{Q}_p^n$, and there exists a linear transformation A from $\mathbb{Q}_p^n$ to $\mathbb{Q}_p^m$ such that

$$\lim_{\vec{h} \to 0} \frac{|\vec{f}(\vec{x} + \vec{h}) - \vec{f}(\vec{x}) - A\vec{h}|}{|\vec{h}|} = 0,$$

then $\vec{f}$ is differentiable at $\vec{x}$, and $D\vec{f}(\vec{x}) = A$

If a function $\vec{f}$ is differentiable at a point $\vec{x}$, the above limit can be rewritten as $\vec{f}(\vec{x} + \vec{h}) - \vec{f}(\vec{x}) = D\vec{f}(\vec{x})\vec{h} + \vec{r}(\vec{h})$, where $\lim_{\vec{h} \to 0} |\vec{r}(\vec{h})|/|\vec{h}| = 0$ Note here that $D\vec{f}(\vec{x})$ is a linear transformation, so that $D\vec{f}(\vec{x})\vec{h}$ means the linear tranformation $D\vec{f}(\vec{x})$ applied to the vector $\vec{h}$, and not multiplication

Theorem A: Let E be open and non-empty in $\mathbb{Q}_p^n$, and let $\vec{f}$ $E \to \mathbb{Q}_p^m$ be differentiable in E such that there is a real number M with $\|D\vec{f}(\vec{x})\| \leq M$ for all $\vec{x} \in E$ Then there is an open subset U of E such that

$$|\vec{f}(\vec{b}) - \vec{f}(\vec{a})| \leq M|\vec{b} - \vec{a}|$$

for all $\vec{a} \in U$, $\vec{b} \in U$

Proof: By differentiability, $\vec{f}(\vec{x} + \vec{h}) - \vec{f}(\vec{x}) = D\vec{f}(\vec{x})\vec{h} + \vec{r}(\vec{h})$, with $|\vec{r}(\vec{h})|/|\vec{h}| \to 0$ as $\vec{h} \to 0$ Thus, there exists some $\delta > 0$ such that $|\vec{h}| < \delta$ implies $|\vec{r}(\vec{h})| < M|\vec{h}|$ Choose some point $\vec{a} \in E$ and let U be the intersection of E with the open ball around $\vec{a}$ with radius δ Then, for any points $\vec{a}, \vec{b} \in U$, $|\vec{r}(\vec{b} - \vec{a})| < M|\vec{b} - \vec{a}|$

Let $\vec{x} = \vec{a}$ and $\vec{h} = \vec{b} - \vec{a}$, so that the above becomes $\vec{f}(\vec{b}) - \vec{f}(\vec{a}) = D\vec{f}(\vec{a})(\vec{b} - \vec{a}) + \vec{r}(\vec{b} - \vec{a})$ Take norms of both sides of the inequality to get

$$
\begin{aligned}
|\vec{f}(\vec{b}) - \vec{f}(\vec{a})| &= |D\vec{f}(\vec{a})(\vec{b}-\vec{a}) + \vec{r}(\vec{b}-\vec{a})| \\
&\leq \max(|D\vec{f}(\vec{a})(\vec{b}-\vec{a})|, |\vec{r}(\vec{b}-\vec{a})|) \\
&\leq \max(|D\vec{f}(\vec{a})(\vec{b}-\vec{a})|, M|\vec{b}-\vec{a}|) \\
&\leq \max(\|D\vec{f}(\vec{a})\|\ |\vec{b}-\vec{a}|, M|\vec{b}-\vec{a}|) \\
&\leq M|\vec{b}-\vec{a}|\ \square
\end{aligned}
$$

(Note in the real numbers, [10] uses concavity of E to get this result This theorem is the only difference between the p-adic proof of the implicit function theorem and the real version)

The function $\vec{f}$ is said to be continuously differentiable in an open set E if $D\vec{f}$ is a continuous mapping of E into $L(\mathbb{Q}_p^n, \mathbb{Q}_p^m)$ More specifically, $\vec{f}$ is continuously differentiable if for every $\vec{x} \in E$ and $\epsilon > 0$ there exists a $\delta > 0$ such that if $\vec{y} \in E$ and $|\vec{x} - \vec{y}| < \delta$, then $\|D\vec{f}(\vec{x}) - D\vec{f}(\vec{y})\| < \epsilon$

The contraction principle will also be used in the proof of the implicit function theorem The contraction principle says that if X is a complete metric space, and if ϕ is a contraction of X into X, then there exists one and only one $x \in X$ such that $\phi(x) = x$ (A contraction is a map ϕ from X to X such that, for some $c < 1$, $d(\phi(x), \phi(y)) \leq c\, d(x, y)$ for all $x, y \in X$) This theorem is proven as Theorem 9 23 in [10], and since it applies to all (topologically) complete metric spaces, it applies in particular to the p-adic numbers

2.4 The P-adic Inverse Function Theorem

Theorem: *The Inverse Function Theorem* Suppose $\vec{f}$ is continuously differentiable from an open set $E \subset \mathbb{Q}_p^n$ to $\mathbb{Q}_p^n$, $D\vec{f}(\vec{a})$ is invertible for some $\vec{a} \in E$, and $\vec{b} = \vec{f}(\vec{a})$ Then there exist open sets U and V in $\mathbb{Q}_p^n$ such that $\vec{a} \in U$, $\vec{b} \in V$, $\vec{f}$ is

one-to-one on U, and $\vec{f}(U) = V$ Furthermore, if $\vec{g}$ is the inverse of $\vec{f}$, defined in V by $\vec{g}(\vec{f}(\vec{x})) = \vec{x}$, then $\vec{g}$ is continuously differentiable

Proof: Let $A = D\vec{f}(\vec{a})$, and choose c such that $2c\|A^{-1}\| = 1$ Since $D\vec{f}$ is continuous at $\vec{a}$, there is an open ball $D \subset E$, with center $\vec{a}$, such that $\|D\vec{f}(\vec{x}) - A\| < c$ for $\vec{x} \in D$ This means that for all $\vec{x} \in D$, $\|D\vec{f}(\vec{x}) - A\| \ \|A^{-1}\| < c \ \frac{1}{2c} = \frac{1}{2} < 1$ Thus, by a previous theorem (in Section 2 1), $D\vec{f}(\vec{x})$ is invertible for all $\vec{x} \in D$

For every $\vec{y} \in \mathbb{Q}_p^n$, associate a function $\vec{\phi}_y$ defined on $\vec{x} \in E$ by

$$\vec{\phi}_y(\vec{x}) = \vec{x} + A^{-1}(\vec{y} - \vec{f}(\vec{x}))$$

Note that $\vec{f}(\vec{x}) = \vec{y}$ if and only if $\vec{\phi}_y(\vec{x}) = \vec{x}$ Taking the derivative of $\vec{\phi}_y$ gives

$$D\vec{\phi}_y(\vec{x}) = I - A^{-1}D\vec{f}(\vec{x}) = A^{-1}(A - D\vec{f}(\vec{x}))$$

So,

$$\|D\vec{\phi}_y(\vec{x})\| \leq \|A^{-1}\| \ \|A - D\vec{f}(\vec{x})\| < \frac{1}{2c}c = \frac{1}{2}$$

for all $\vec{x} \in B$ Hence,

$$|\vec{\phi}_y(\vec{x}_1) - \vec{\phi}_y(\vec{x}_2)| \leq \frac{1}{2}|\vec{x}_1 - \vec{x}_2|$$

for all $\vec{x}_1, \vec{x}_2$ in some open subset U of D, by Theorem A

If $\vec{x}$ and $\vec{x}_0$ are fixed points of $\vec{\phi}_y$ in U, then

$$|\vec{x} - \vec{x}_0| = |\vec{\phi}_y(\vec{x}) - \vec{\phi}_y(\vec{x}_0)| \leq \frac{1}{2}|\vec{x} - \vec{x}_0|,$$

which implies that $|\vec{x} - \vec{x}_0| = 0$, or $\vec{x} = \vec{x}_0$ Thus, for any $\vec{y}$, there is at most one $\vec{x} \in U$ such that $\vec{f}(\vec{x}) = \vec{y}$ Thus, $\vec{f}$ is one-to-one in U

Define $V = \vec{f}(U)$, and choose $\vec{y}_0 \in V$ Then $\vec{y}_0 = \vec{f}(\vec{x}_0)$ for some $\vec{x}_0 \in U$ by definition of V Let B be an open ball with center at $\vec{x}_0$ and radius $r > 0$, so small that the ball's closure lies in U

Fix $\vec{y}$ such that $|\vec{y} - \vec{y}_0| < cr$ Then, using the definition of $\vec{\phi}_y$,

$$|\vec{\phi}_y(\vec{x}_0) - \vec{x}_0| = |A^{-1}(\vec{y} - \vec{y}_0)| < \|A^{-1}\| cr = \frac{r}{2}$$

If $\vec{x}$ is in the closure of B, then

$$|\vec{\phi}_y(\vec{x}) - \vec{x}_0| \leq |\vec{\phi}_y(\vec{x}) - \vec{\phi}_y(\vec{x}_0)| + |\vec{\phi}_y(\vec{x}_0) - \vec{x}_0| < \frac{1}{2}|\vec{x} - \vec{x}_0| + \frac{r}{2} \leq r$$

Thus, $\vec{\phi}_y(\vec{x}) \in B$, and $\vec{\phi}_y$ is a contraction of the closure of B to itself

Since the closure of B is closed, it is complete The contraction principle says that $\vec{\phi}_y$ has a fixed point $\vec{x}$ in the closure of B For this $\vec{x}$, $\vec{f}(\vec{x}) = \vec{y}$ Thus, $\vec{y} \in V$ In particular, every vector in the open ball centered at $\vec{y}_0$ with radius cr is in V Hence, V is open

Recall that $\vec{g}$ $V \to U$ is the inverse of $\vec{f}$ on U Choose $\vec{y} \in V$, $\vec{y} + \vec{k} \in V$ Then there exists $\vec{x} \in U$, $\vec{x} + \vec{h} \in U$ such that $\vec{y} = \vec{f}(\vec{x})$, $\vec{y} + \vec{k} = \vec{f}(\vec{x} + \vec{h})$ With $\vec{\phi}_y$ defined as above,

$$\vec{\phi}_y(\vec{x} + \vec{h}) - \vec{\phi}_y(\vec{x}) = \vec{h} + A^{-1}[\vec{f}(\vec{x}) - \vec{f}(\vec{x} + \vec{h})] = \vec{h} - A^{-1}\vec{k}$$

Since $|\vec{\phi}_y(\vec{x}_1) - \vec{\phi}_y(\vec{x}_2)| \leq \frac{1}{2}|\vec{x}_1 - \vec{x}_2|$, $|\vec{h} - A^{-1}\vec{k}| \leq \frac{1}{2}|\vec{h}|$ Thus,

$$|\vec{h}| = |\vec{h} - A^{-1}\vec{k} + A^{-1}\vec{k}| \leq \frac{1}{2}|\vec{h}| + |A^{-1}\vec{k}|$$

so that $|A^{-1}\vec{k}| \geq \frac{1}{2}|\vec{h}|$, and

$$|\vec{h}| \leq 2\|A^{-1}\| \, |\vec{k}| = c^{-1}|\vec{k}|$$

Since $\vec{x} \in D$, $D\vec{f}(\vec{x})$ has an inverse Call this inverse T

$$\vec{g}(\vec{y} + \vec{k}) - \vec{g}(\vec{y}) - T\vec{k} = \vec{h} - T\vec{k} = -T[\vec{f}(\vec{x} + \vec{h}) - \vec{f}(\vec{x}) - D\vec{f}(\vec{x})\vec{h}],$$

and $|\vec{k}| \geq c|\vec{h}|$, which gives

$$\frac{|\vec{g}(\vec{y}+\vec{k})-\vec{g}(\vec{y})-T\vec{k}|}{|\vec{k}|} \leq \frac{\|T\|}{c} \quad \frac{|\vec{f}(\vec{x}+\vec{h})-\vec{f}(\vec{x})-D\vec{f}(\vec{x})\vec{h}|}{|\vec{h}|}$$

$|\vec{h}| \leq c^{-1}|\vec{k}|$ also shows that as $\vec{k} \to \vec{0}$, $\vec{h} \to \vec{0}$ as well Thus, as $k \to \vec{0}$, the right hand side of the inequality goes to 0, so that the left hand side does as well Therefore, $D\vec{g}(\vec{y}) = T$, so $\vec{g}$ is differentiable for all $\vec{y} \in V$ Since T is the inverse of $D\vec{f}(\vec{x}) = D\vec{f}(\vec{g}(\vec{y}))$, $D\vec{g}(\vec{y}) = \{D\vec{f}(\vec{g}(\vec{y}))\}^{-1}$ Since $\vec{g}$, $D\vec{f}$, and inverting linear transformations are all continuous functions, $D\vec{g}(\vec{y})$ is continuous, so that $\vec{g}$ is continuously differentiable □

2.5 The P-adic Implicit Function Theorem

Let $\vec{x} = (x_1, \quad , x_n) \in \mathbb{Q}_p^n$ and $\vec{y} = (y_1, \quad , y_m) \in \mathbb{Q}_p^m$ Denote the vector $(x_1, \quad , x_n, y_1, \quad , y_m) \in \mathbb{Q}_p^{n+m}$ as $(\vec{x}, \vec{y})$ Let $A \in L(\mathbb{Q}_p^{n+m}, \mathbb{Q}_p^n)$ A can be split into two linear transformations A_x and A_y as follows

$$A_x(\vec{h}) = A(\vec{h}, \vec{0}), \qquad A_y(\vec{k}) = A(\vec{0}, \vec{k})$$

for any $\vec{h} \in \mathbb{Q}_p^n, \vec{k} \in \mathbb{Q}_p^m$ Then, $A_x \in L(\mathbb{Q}_p^n), A_y \in L(\mathbb{Q}_p^m, \mathbb{Q}_p^n)$, and

$$A(\vec{h}, \vec{k}) = A_x\vec{h} + A_y\vec{k}$$

The implicit function theorem for linear transformations is as follows

Lemma: If $A \in L(\mathbb{Q}_p^{n+m}, \mathbb{Q}_p^n)$, and if A_x is invertible, then there corresponds to every $\vec{k} \in \mathbb{Q}_p^m$ a unique $\vec{h} \in \mathbb{Q}_p^n$ such that $A(\vec{h}, \vec{k}) = 0$ This $\vec{h}$ can be computed by $\vec{h} = -(A_x)^{-1}A_y\vec{k}$

Proof: Since $A(\vec{h}, \vec{k}) = A_x\vec{h} + A_y\vec{k}$, $A(\vec{h}, \vec{k}) = 0$ if and only if $A_x\vec{h} + A_y\vec{k} = 0$, or, when A_x is invertible, $\vec{h} = -(A_x)^{-1}A_y\vec{k}$ □

Theorem: *The Implicit Function Theorem* Let $\vec{f}$ be a continuously differentiable map from an open set $E \subset \mathbb{Q}_p^{n+m}$ to $\mathbb{Q}_p^n$ such that $\vec{f}(\vec{a}, \vec{b}) = \vec{0}$ for some $(\vec{a}, \vec{b}) \in E$ Let $A = D\vec{f}(\vec{a}, \vec{b})$ and assume that A_x is invertible

Then there exist open sets $U \subset \mathbb{Q}_p^{m+n}$ and $W \subset \mathbb{Q}_p^m$, with $(\vec{a}, \vec{b}) \in U$ and $\vec{b} \in W$, such that for every $\vec{y} \in W$ there exists a unique $\vec{x}$ such that $(\vec{x}, \vec{y}) \in U$ and $\vec{f}(\vec{x}, \vec{y}) = \vec{0}$

If this $\vec{x}$ is defined to be $\vec{g}(\vec{y})$, then $\vec{g}$ is a continuously differentiable map from W to $\mathbb{Q}_p^n$, $\vec{g}(\vec{b}) = \vec{a}$, $\vec{f}(\vec{g}(\vec{y}), \vec{y}) = \vec{0}$ for all $\vec{y} \in W$, and $D\vec{g}(\vec{b}) = -(A_x)^{-1} A_y$

Proof: Define $\vec{F}$ by $\vec{F}(\vec{x}, \vec{y}) = (\vec{f}(\vec{x}, \vec{y}), \vec{y})$ for $(\vec{x}, \vec{y}) \in E$ Then $\vec{F}$ is continuously differentiable, and maps E to $\mathbb{Q}_p^{n+m}$ Since $\vec{f}(\vec{a}, \vec{b}) = 0$,

$$\vec{f}(\vec{a} + \vec{h}, \vec{b} + \vec{k}) = A(\vec{h}, \vec{k}) + \vec{r}(\vec{h}, \vec{k}),$$

where $\vec{r}$ is the remainder term in the definition of $D\vec{f}(\vec{a}, \vec{b})$ Since

$$\begin{aligned} \vec{F}(\vec{a} + \vec{h}, \vec{b} + \vec{k}) - \vec{F}(\vec{a}, \vec{b}) &= (\vec{f}(\vec{a} + \vec{h}, \vec{b} + \vec{k}), \vec{k}) \\ &= (A(\vec{h}, \vec{k}), \vec{k}) + (\vec{r}(\vec{h}, \vec{k}), \vec{0}), \end{aligned}$$

$D\vec{F}(\vec{a}, \vec{b})$ is the linear transformation on $\mathbb{Q}_p^{n+m}$ that maps $(\vec{h}, \vec{k})$ to $(A(\vec{h}, \vec{k}), \vec{k})$ If this image vector is $\vec{0}$, then $\vec{k} = \vec{0}$ and $A(\vec{h}, \vec{k}) = \vec{0}$, or $A_x \vec{h} = A(\vec{h}, \vec{0}) = \vec{0}$ Since A_x is invertible, this implies that $\vec{h} = 0$ Thus, the linear transformation $D\vec{F}(\vec{a}, \vec{b})$ is one-to-one, so is invertible

Therefore, the inverse function theorem applies to $\vec{F}$ That means there are open sets U and V in $\mathbb{Q}_p^{n+m}$ with $(\vec{a}, \vec{b}) \in U$, $(\vec{0}, \vec{b}) \in V$, such that $\vec{F}$ is a one-to-one mapping of U onto V

Let W be the set of all $\vec{y} \in \mathbb{Q}_p^m$ such that $(\vec{0}, \vec{y}) \in V$ Note that $\vec{b} \in W$ Since V is open, W is open If $\vec{y} \in W$, then $(\vec{0}, \vec{y}) = \vec{F}(\vec{x}, \vec{y})$ for some $(\vec{x}, \vec{y}) \in U$ By definition of $\vec{F}$, $\vec{f}(\vec{x}, \vec{y}) = \vec{0}$ for this $\vec{x}$ Suppose that, with the same $\vec{y}$, $(\vec{x}', \vec{y}) \in U$ and $\vec{f}(\vec{x}', \vec{y}) = \vec{0}$ Then

$$\vec{F}(\vec{x}', \vec{y}) = (\vec{f}(\vec{x}', \vec{y}), \vec{y}) = (\vec{0}, \vec{y}) = (\vec{f}(\vec{x}, \vec{y}), \vec{y}) = \vec{F}(\vec{x}, \vec{y})$$

Since $\vec{F}$ is one-to-one in U, $\vec{x}' = \vec{x}$, so this $\vec{x}$ is unique

Define $\vec{g}(\vec{y})$, for $\vec{y} \in W$, so that $(\vec{g}(\vec{y}), \vec{y}) \in U$ and $\vec{f}(\vec{g}(\vec{y}), \vec{y}) = \vec{0}$ Then $\vec{F}(\vec{g}(\vec{y}), \vec{y}) = (\vec{0}, \vec{y})$ for all $\vec{y}$ Let $\vec{G}$ be the mapping of V onto U which inverts $\vec{F}$ $\vec{G}$ is continuously differentiable by the inverse function theorem, and

$$(\vec{g}(\vec{y}), \vec{y}) = \vec{G}(\vec{0}, \vec{y})$$

Thus, $\vec{g}$ is continuously differentiable

Let $\vec{\Phi}(\vec{y}) = \vec{G}(\vec{0}, \vec{y}) = (\vec{g}(\vec{y}), \vec{y})$ Then $D\vec{\Phi}(\vec{y})\vec{k} = (D\vec{g}(\vec{y})\vec{k}, \vec{k})$ for all $\vec{y} \in W$, $\vec{k} \in \mathbb{Q}_p^m$ $\vec{f}(\vec{\Phi}(\vec{y})) = \vec{f}(\vec{g}(\vec{y}), \vec{y}) = \vec{0}$ for $\vec{y} \in W$ by definition of $\vec{g}$ The chain rule then gives

$$D\vec{f}(\vec{\Phi}(\vec{y}))D\vec{\Phi}(\vec{y}) = 0$$

(This 0 is the zero linear transformation) When $\vec{y} = \vec{b}$, $\vec{\Phi}(\vec{y}) = (\vec{a}, \vec{b})$ and $D\vec{f}(\vec{\Phi}(\vec{y})) = A$ Thus, $AD\vec{\Phi}(\vec{b}) = 0$ So,

$$A_x D\vec{g}(\vec{b})\vec{k} + A_y\vec{k} = A(D\vec{g}(\vec{b})\vec{k}, \vec{k}) = AD\vec{\Phi}(\vec{b})\vec{k} = \vec{0}$$

for all $\vec{k} \in \mathbb{Q}_p^m$ Therefore, $A_x D\vec{g}(\vec{b}) + A_y = 0$, or $D\vec{g}(\vec{b}) = -(A_x)^{-1}A_y$ $\square$

3. Roots of Random Polynomials

A random polynomial of degree d is a polynomial of the form $A_d x^d + A_{d-1}x^{d-1} + \quad + A_2 x^2 + A_1 x + A_0$, where each A_i is a random variable over some field $\mathbb{F}$ For this thesis, each A_i will be independent and usually identically distributed over $\mathbb{F}$ In addition, the probability that A_i is x will be zero for all x in $\mathbb{F}$ (Later in the thesis, finite fields will be considered, but not in conjunction with random polynomials) With this condition, A_d is almost never zero, so that the random polynomial is almost always of degree d Denote the probability of this degree d random polynomial having k distinct roots in $\mathbb{F}$ as P_d^k This thesis will concentrate on $\mathbb{F} = \mathbb{R}$ or $\mathbb{F} = \mathbb{Q}_p$, with their appropriate norms, but much of this can be extended to other fields

In order to prove that this polynomial will almost never have multiple roots, other work must be done first

Lemma: Let $\mathbb{F}$ be either $\mathbb{R}$ or $\mathbb{Q}_p$ Let μ be a measure on $\mathbb{F}$ such that the measure of a ball of radius ϵ goes to zero as ϵ goes to zero, and compact sets have finite measure Let $f \quad \mathbb{F}^n \to \mathbb{F}$ be continuous The graph $G = \{(\vec{x}, f(\vec{x})) \quad \vec{x} \in \mathbb{F}^n\}$ has measure zero

Proof: For every positive integer m, let K_m be the closed ball of radius m centered at 0 Each K_m is compact, and for all m, $K_m \subset K_{m+1}$ and $\lim K_m = \mathbb{F}^n$ Choose some positive integer m Since f is continuous, f restricted to K_m is uniformly continuous So, choose an $\epsilon > 0$ Then there exists $\delta > 0$ such that, for all $\vec{x}, \vec{y} \in \mathbb{F}^n$, $|\vec{x} - \vec{y}| < \delta$ implies $|f(\vec{x}) - f(\vec{y})| < \epsilon$ There is a finite collection of open balls $B_1, \quad , B_k$ of radius at most δ which covers all of K_m The graph of f on K_m is the union of the graphs of f on all B_i On each B_i, $f(B_i)$ is contained in an open ball of radius ϵ So, the measure of the graph of f on the union of B_i is at

most the measure of K_m times the max of the measures of B_i, which goes to zero as ϵ goes to zero Since K_m has finite measure, and ϵ was chosen arbitrarily, this means that the measure of the graph of f on K_m is zero Since $\lim K_m = \mathbb{F}$, the measure of the graph on all of $\mathbb{F}$ is zero $\square$

Theorem: Let f be a polynomial from $\mathbb{F}^n$ to $\mathbb{F}$, with $\mathbb{F}$ and a measure on $\mathbb{F}$ defined as in the lemma The set $Z(f) = \{\vec{x} \in \mathbb{F}^n | f(\vec{x}) = 0\}$ has measure zero

Proof: Induct on n if $n = 1$, then f is a single variable polynomial Then $Z(f)$ is a finite set, and finite sets have measure zero Otherwise, assume the theorem is true for polynomials with less than n variables

Single out one of the variables, and look at f as a function from $\mathbb{F} \times \mathbb{F}^{n-1}$ to $\mathbb{F}$ Denote that variable as y, and the derivative of the function f with respect to that variable as f_y $Z(f) = \{(y, \vec{x}) | f(y, \vec{x}) = 0\}$ Let

$$Z_1(f) = \{(y, \vec{x}) | f(y, \vec{x}) = 0, f_y(y, \vec{x}) \neq 0\}$$

Let $Z_2(f) = Z(f) \backslash Z_1(f)$ Let d be the degree of y in the polynomial f, so that $f(y, \vec{x}) = f_d(\vec{x})y^d + \quad + f_1(\vec{x})y + f_0(\vec{x})$ Note that $Z_2(f) \subset Z(f_y)$ By the Implicit Function Theorem, for every point in $Z_1(f)$ there are open sets U, W, and a function g such that $f(y, \vec{x}) = 0$ and $(y, \vec{x}) \in U$ if and only if $g(\vec{x}) = y$ $Z_1(f)$ is the union of the graphs of all such g in all such U The collection of all U has a countable subcover, so that the set $Z_1(f)$ is composed of a countable collection of graphs of functions Each graph has measure zero, so the union must have measure zero, so $Z_1(f)$ has measure zero

Induct on d if $d = 1$, then $f = f_1(\vec{x})y + f_0(\vec{x})$ and $f_y = f_1(\vec{x})$ f_y has less than n variables, so by the inductive hypothesis, $Z(f_y)$ has measure zero, so that $Z_2(f)$, a subset of $Z(f_y)$, has measure zero Since both $Z_1(f)$ and $Z_2(f)$ have measure zero, so does $Z(f)$

Assume that the theorem is true for polynomials with the degree of y less than d The derivative f_y has a y-degree of less than d, so $Z(f_y)$ has measure zero Again, since $Z_2(f)$ is a subset of $Z(f_y)$, $Z_2(f)$ also has measure zero Since both $Z_1(f)$ and $Z_2(f)$ have measure zero, $Z(f)$ has measure zero

Therefore, by induction, $Z(f)$ has measure zero $\square$

Theorem: Let $\mathbb{F}$ be $\mathbb{R}$ or $\mathbb{Q}_p$ Let $A_0, A_1, \quad, A_d$ be independent random variables on the field $\mathbb{F}$ such that for all i, the probability that A_i is in a ball of radius ϵ approaches zero as ϵ approaches zero Then the random polynomial $A_d x^d + A_{d-1}x^{d-1} + \quad + A_2 x^2 + A_1 x + A_0$ almost always has distinct roots

Proof: (The first paragraph of this proof is adapted from parts of [3, §14 6]) The discriminant D of a polynomial with roots $\alpha_1, \alpha_2, \quad, \alpha_d$ in an algebraic closure of $\mathbb{F}$ is

$$D = \prod_{1 \le i < j \le d} (\alpha_i - \alpha_j)^2$$

which is zero if and only if two of the roots are the same The coefficients of the polynomial $a(x-\alpha_1)(x-\alpha_2) \quad (x-\alpha_d)$ are determined by the elementary symmetric functions of the roots, that is, if

$$s_1 = \sum_{i=1}^{d} \alpha_i$$
$$s_2 = \sum_{1 \le i < j \le d} \alpha_i \alpha_j$$

$$s_d = \prod_{j=1}^{d} \alpha_j,$$

then $a(x-\alpha_1)(x-\alpha_2) \quad (x-\alpha_d) = a(x^d - s_1 x^{d-1} + s_2 x^{d-2} + \quad + (-1)^d s_d)$ The discriminant D can be written as a polynomial in s_i, that is, a polynomial in the coefficients of the original polynomial

The original polynomial has multiple roots if and only if the discriminant is zero The set of zeroes of a polynomial has measure zero, so the probability that the discriminant is zero is zero, so that the probability that the original polynomial has multiple roots is zero □

The probability P_d^k that a random degree d polynomial over the field $\mathbb{F}$ has k distinct roots in $\mathbb{F}$ will be found for some specific fields and random distributions For this part of the thesis, quadratic polynomials are considered, so $d = 2$

Three independent random variables A, B, and C, all of them almost never zero, are used to create the random polynomial $r(x) = Ax^2 + Bx + C = A(x^2 + B/Ax + C/A)$ Since this polynomial will almost never have a multiple root, only P_2^2 need be found, then $P_2^0 = 1 - P_2^2$ The polynomial has two distinct roots if and only if the discriminant D is a square in $\mathbb{F}$ [3, pp 524-526] Call the two roots α_1 and α_2

$$\begin{aligned} D &= (\alpha_1 - \alpha_2)^2 \\ &= \alpha_1^2 - 2\alpha_1\alpha_2 + \alpha_2^2 \\ &= (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 \\ &= (s_1)^2 - 4s_2 \\ &= (-B/A)^2 - 4(C/A) \\ &= (B^2 - 4AC)/A^2 \end{aligned}$$

This is a square in $\mathbb{F}$ if and only if $B^2 - 4AC$ is a square in $\mathbb{F}$ So, $Ax^2 + Bx + C$ has two distinct roots if and only if $B^2 - 4AC$ has a (non-zero) square root in $\mathbb{F}$

3.1 Real Numbers

In the real numbers, $B^2 - 4AC$ has a square root if and only if $B^2 - 4AC$ is positive. So, $P_2^2 = P(B^2 - 4AC > 0) = P(B^2 - 4AC \geq 0)$. This probability will be found for two probability distributions.

3.1.1 Uniform Distribution

Let A, B, and C be independent random variables, uniformly distributed over the interval $[-1, 1]$, the unit disc in the real numbers. This distribution is proportional to the standard Lebesgue measure on the reals, so the probability $P(B^2 - 4AC \geq 0)$ can be found by integration.

$$P(B^2 - 4AC \geq 0) = \frac{\int_{B^2-4AC\geq 0} d\vec{x}}{\int_{(A,B,C)\in[-1,1]^3} d\vec{x}}$$

Let B range over the whole interval [-1,1]. If the determinant is zero, then $C = B^2/4A$. If A is positive, and $C < B^2/4A$, then the discriminant is positive. If A is negative, and $C > B^2/4A$, then the discriminant is also positive. So, A can range over any value in [-1,1], and C ranges over [-1,min$\{1, B^2/4A\}$] if A is positive, and [max$\{B^2/4A, -1\}$,1] if A is negative. If $|A| < B^2/4$, then use either 1 or -1 as the bound for C. Otherwise, use $B^2/4A$.

Symmetry can simplify this region. $B^2 = (-B)^2$, so by doubling the result, B need only range over $[0, 1]$. Also, the range [-1,min$\{1, B^2/4A\}$] has the same length as [max$\{B^2/4A, -1\}$,1]. Thus, by doubling the result again, A also need only range over $[0, 1]$. This gives

$$
\begin{aligned}
P_2^2 &= \frac{\int_{B^2-4AC\geq 0}\, d\vec{x}}{\int_{(A,B,C)\in[-1,1]^3}\, d\vec{x}} \\
&= \frac{4\int_0^1\int_0^{B^2/4}\int_{-1}^1 dCdAdB + 4\int_0^1\int_{B^2/4}^1\int_{-1}^{B^2/4A} dCdAdB}{8} \\
&= \frac{1}{2}\left(\int_0^1\int_0^{B^2/4} 2\; dAdB + \int_0^1\int_{B^2/4}^1 \frac{B^2}{4A} + 1\; dAdB\right) \\
&= \frac{1}{2}\left(2\int_0^1 \frac{B^2}{4}dB + \int_0^1 A + \frac{B^2\ln A}{4}\Big|_{B^2/4}^1 dB\right) \\
&= \frac{1}{2}\left(\frac{1}{6} + \int_0^1 1 - \left(\frac{B^2}{4} + \frac{B^2\ln\left(B^2/4\right)}{4}\right)dB\right) \\
&= \frac{1}{2}\left(\frac{1}{6} + \frac{1}{4}\int_0^1 4 - B^2 - B^2\ln\left(B^2/4\right)dB\right) \\
&= \frac{1}{2}\left(\frac{1}{6} + \frac{1}{4}\int_0^1 4 - B^2 - B^2\;\; 2\ln\left(B/2\right)dB\right) \\
&= \frac{1}{2}\left(\frac{1}{6} + \frac{1}{4}\int_0^1 4 - B^2 - B^2\;\; 2\left(\ln B - \ln 2\right)dB\right) \\
&= \frac{1}{2}\left(\frac{1}{6} + \frac{1}{4}\int_0^1 4 + \left(2\ln 2 - 1\right)B^2 - 2B^2\ln B dB\right) \\
&= \frac{1}{2}\left(\frac{1}{6} + \frac{1}{4}\left(4B + \left(2\ln 2 - 1\right)\frac{B^3}{3} - 2(\frac{B^3\ln B}{3} - \frac{B^3}{9})\right)\Big|_0^1\right) \\
&= \frac{1}{2}\left(\frac{1}{6} + \frac{1}{4}\left(4 + \frac{2\ln 2 - 1}{3} - 2(0 - \frac{1}{9})\right)\right) \\
&= \frac{1}{2}\left(\frac{1}{6} + \frac{1}{36}\left(36 + 6\ln 2 - 3 + 2\right)\right) \\
&= \frac{1}{72}\left(6 + \left(35 + 6\ln 2\right)\right) \\
&= \frac{41 + 6\ln 2}{72} \approx 0\;6272
\end{aligned}
$$

3 1 2 Gaussian Distribution

An analysis similar to the above for the Gaussian distribution on the real numbers is possible, but previous work done with Gaussian distributions makes it unnecessary The Kac formula is a well-known formula for finding E, the expected number of roots of a real random polynomial with Gaussian coefficients See [4] for

one way of finding the Kac formula For quadratics, $E = 2\ P_2^2 + 1\ P_2^1 + 0\ P_2^0 = 2\ P_2^2$ since these random polynomials almost never have a double root So, $P_2^2 = E/2$ and $P_2^0 = 1 - P_2^2$

The Kac formula gives us an integral for E for a degree d polynomial

$$E = \frac{4}{\pi} \int_0^1 \sqrt{\frac{1}{(1-t^2)^2} - \frac{(d+1)^2 t^{2d}}{(1-t^{2d+2})^2}}\, dt$$

which evaluates numerically, for $d = 2$, to $E \approx 1\ 2970$ Thus, the probability that a random quadratic polynomial with Gaussian coefficients has two distinct roots is 0 6485

3.2 *P*-adic Random Variables

On every locally compact group, there is a unique (up to a constant) measure which is translation-invariant, or 'uniform', called the Haar measure [5, §57-60] As in the case with the real numbers, this uniform measure cannot be used as a probability measure on all of $\mathbb{Q}_p$, so a suitable subset will be chosen The subset used here is the unit disk in $\mathbb{Q}_p$ the p-adic integers

There is an alternate way of looking at this probability measure Every p-adic integer can be written in its canonical sum form

$$\sum_{n=0}^{\infty} a_n p^n$$

where a_n is in the set $\{0, 1, 2, \quad p-1\}$ Now, create a random variable by letting each a_n be an independent random variable uniformly distributed over the set $\{0, 1, 2, \quad p-1\}$ This random variable is translation-invariant, as seen below, and the total measure of $\mathbb{Z}_p$ is 1, so this must be the probability Haar measure on $\mathbb{Z}_p$

Lemma: For all non-negative integers n, let A_n be an independent random variable uniformly distributed over the set $\{0, 1, \quad, p-1\}$ Define a random variable

A over the p-adic integers as

$$A = \sum_{k=0}^{\infty} A_k p^k$$

The random variable A is uniformly distributed on the p-adic integers, that is, it is translation-invariant ($P(A \in E) = P(A \in n + E)$ for Borel sets E and p-adic integers n) and every open set has positive probability This determines a Haar measure on the p-adic integers ($\mu(E) = P(A \in E)$)

Proof: A basic open set in the p-adic integers looks like $a + p^n\mathbb{Z}_p$, where $\mathbb{Z}_p$ is the set of p-adic integers, n is a non-negative (rational) integer, and a is some p-adic integer The elements $A = \sum_{k=0}^{\infty} A_k p^k$ will be in this set if and only if $A \equiv a \pmod{p^n}$ Write $a = \sum_{k=0}^{\infty} a_k p^k$ Then A is in $a + p^n\mathbb{Z}_p$ if and only if $\sum_{k=0}^{\infty} A_k p^k \equiv \sum_{k=0}^{\infty} a_k p^k \pmod{p^n}$, or $\sum_{k=0}^{n-1} A_k p^k = \sum_{k=0}^{n-1} a_k p^k$, or $A_k = a_k$ for all $k \in \{0, 1, \quad n-1\}$ $P(A_k = a_k) = 1/p$ for all k, so $P(A \in a + p^n\mathbb{Z}_p) = 1/p^n$ Thus, every basic open set has positive probability, so all open sets have positive probability Also, the probability of the basic open set $a + p^n\mathbb{Z}_p$ is independent of a, so the probability is translation-invariant for open sets, and thus for all Borel sets

□

This uniform measure on $\mathbb{Z}_p$ is also the limit of the uniform probability measures on $\mathbb{Z}/p^n\mathbb{Z}$, which can be seen as follows

Proposition: Let S be a measurable set in the p-adic integers, and let the set S_n be the image of S in $\mathbb{Z}/p^n\mathbb{Z}$ under the functions defined by the inverse limit, that is, if $s = \sum_{k=0}^{\infty} s_k p^k$ is in S, then $\sum_{k=0}^{n-1} s_k p^k$ is in S_n Let μ be the uniform probability measure on the p-adic integers, and let μ_n be the uniform probability measure on $\mathbb{Z}/p^n\mathbb{Z}$ Then, $\mu(S) = \lim_{n\to\infty} \mu_n(S_n)$

Proof: Let S be a basic open set in $\mathbb{Z}_p$ Then $S = a + p^k\mathbb{Z}_p$ for some p-adic integer a and some non-negative integer k $\mu(a + p^k\mathbb{Z}_p) = p^{-k}$ If $n \leq k$, then the set

S_n is just a single element $a \in \mathbb{Z}/p^n\mathbb{Z}$ out of a possible p^n elements, so $\mu_n(S_n) = p^{-n}$ If $n > k$, then

$$S_n = a \pmod{p^n} + p^k(\mathbb{Z}/p^n\mathbb{Z}),$$

which has p^{n-k} elements, so that $\mu_n(S_n) = p^{n-k}/p^n = p^{-k}$ Therefore, for basic measurable sets, $\mu(S) = \lim_{n\to\infty} \mu_n(S_n)$ Since it holds for basic sets, it must hold for all measurable sets □

This random variable has some properties which may seem surprising from the point of view of real random variables These properties, however, are based on properties of the uniform random variable on $\mathbb{Z}/n\mathbb{Z}$

Lemma: Let X be a uniform random variable on $\mathbb{Z}/n\mathbb{Z}$, Y be any random variable on $\mathbb{Z}/n\mathbb{Z}$, and Z be any random variable on the units of $\mathbb{Z}/n\mathbb{Z}$, with X, Y, and Z independent Then $P(Y + ZX = k) = P(X = k)$ for all k in $\mathbb{Z}/n\mathbb{Z}$

Proof:

$$\begin{aligned}
P(Y + ZX = k) &= \sum_{j=0}^{n-1} P(Y = j)P(ZX = k - j) \\
&= \sum_{j=0}^{n-1} P(Y = j) \sum_{i=0}^{n-1} P(Z = i)P(X = \frac{k-j}{i}) \\
&= \sum_{j=0}^{n-1} P(Y = j) \sum_{i=0}^{n-1} P(Z = i)\frac{1}{n} \\
&= \frac{1}{n} \sum_{j=0}^{n-1} P(Y = j) \sum_{i=0}^{n-1} P(Z = i) \\
&= \frac{1}{n} \quad 1 \quad 1 \\
&= P(X = k)
\end{aligned}$$

Note that in the above equations, if i is not a unit, then $P(Z = i) = 0$ Looking at this lemma on $\mathbb{Z}/p^n\mathbb{Z}$, and letting n go to infinity, gives the following corollary

Corollary: Let X be a uniform random variable on $\mathbb{Z}_p$, Y be any random variable on $\mathbb{Z}_p$, and Z be any random variable on the units of $\mathbb{Z}_p$ with X, Y, and Z independent Then $P(Y + ZX \in S) = P(X \in S)$ for all measurable sets S in $\mathbb{Z}_p$

The uniform random variable on the p-adic integers can also be split into two independent pieces, one involving the units, and the other involving the power of p which exactly divides the p-adic integer

Lemma: Let A be a random variable uniformly distributed over the p-adic integer Let $\hat{A}$ be a random variable uniformly distributed over the p-adic units, that is,

$$\hat{A} = \sum_{k=0}^{\infty} A_k p^k,$$

where A_0 is uniformly distributed over the set $\{1, 2, \quad , p-1\}$ and for all positive integers k, A_k is uniformly distributed over the set $\{0, 1, \quad , p-1\}$ Let J be a random variable, independent from $\hat{A}$, distributed over the non-negative (rational) integers such that

$$P(J = j) = \frac{p-1}{p} p^{-j}$$

Then $A = p^J \hat{A}$, that is, $P(A \in E) = P(p^J \hat{A} \in E)$

Proof: Without loss of generality, the lemma need only be proven for basic open sets So, if $P(p^J \hat{A} \in a + p^n \mathbb{Z}_p) = P(A \in a + p^n \mathbb{Z}_p) = 1/p^n$, then the lemma is true a is a p-adic integer, so $a = p^m \alpha$ for some non-negative integer m and some p-adic integer unit α If $m \geq n$, then $p^J \hat{A} \in p^m \alpha + p^n \mathbb{Z}_p$ if and only if $J \geq n$

$$\begin{aligned} P(J \geq n) &= 1 - P(J < n) \\ &= 1 - \sum_{j=0}^{n-1} \frac{p-1}{p} \; p^{-j} \\ &= 1 - \frac{p-1}{p} \sum_{j=0}^{n-1} p^{-j} \\ &= 1 - \frac{p-1}{p} \frac{1-p^{-n}}{1-p^{-1}} \\ &= 1 - (p-1) \frac{1-p^{-n}}{p-1} \\ &= 1 - (1-p^{-n}) \\ &= p^{-n} \end{aligned}$$

Let $m < n$ Then $p^J \hat{A} \in p^m \alpha + p^n \mathbb{Z}_p$ if and only if $J = m$ and $\hat{A} \equiv \alpha \pmod{p^{n-m}}$ Recall that $P(J = m) = [(p-1)/p] \cdot p^{-m}$ Let $\alpha = \sum_{k=0}^{\infty} \alpha_k p^k$ Then $\hat{A} \equiv \alpha \pmod{p^{n-m}}$ if and only if $A_k = \alpha_k$ for all $k \in \{0, 1, \quad , n-m-1\}$ $P(A_0 = \alpha_0) = 1/(p-1)$ $P(A_k = \alpha_k) = 1/p$ for all $k \in \{1, 2, \quad , n-m-1\}$ So, $P(\hat{A} \equiv \alpha \pmod{p^{n-m}}) = 1/(p-1) \; (1/p)^{n-m-1}$ Thus,

$$P(p^J \hat{A} \in p^m \alpha + p^n \mathbb{Z}_p) = \frac{p-1}{p} \; p^{-m} \; \frac{1}{p-1} \; (\frac{1}{p})^{n-m-1} = p^{-n}$$

So, in every case, $P(p^J \hat{A} \in a + p^n \mathbb{Z}_p) = 1/p^n = P(A \in a + p^n \mathbb{Z}_p)$ Therefore, $A = p^J \hat{A}$ □

The previous properties can be used to find probabilities for uniformly-distributed p-adic random variables, and the related quadratic random polynomials Recall that p is an odd prime

Lemma: Let A be a uniformly distributed random variable over the p-adic integers Then

$$P(A \text{ is a square}) = \frac{p}{2(p+1)}$$

Proof: A is a square if and only if $A = p^J \hat{A}$, where J and $\hat{A}$ are distributed as in the last lemma in the previous section, and J is even and $\hat{A}$ is a unit square

Since $\hat{A}$ is uniformly distributed over the units in $\mathbb{Z}_p$, and $\hat{A}$ is a square if and only if it is a square modulo p (due to Hensel's Lemma), and half of the units modulo p are square, $P(\hat{A}$ is a square$) = 1/2$

$$\begin{aligned} P(J \text{ is even}) &= \sum_{j \text{ even}} P(J = j) \\ &= \sum_{j=0}^{\infty} P(J = 2j) \\ &= \sum_{j=0}^{\infty} \frac{1}{p^{2j}} \frac{p-1}{p} \\ &= \frac{p-1}{p} \sum_{j=0}^{\infty} (p^{-2})^j \\ &= \frac{p-1}{p} \frac{1}{1-p^{-2}} \\ &= \frac{p-1}{p} \frac{p^2}{p^2-1} \\ &= \frac{p}{p+1} \end{aligned}$$

So,

$$P(A \text{ is a square}) = \frac{1}{2} \frac{p}{p+1} \quad \square$$

Proposition: Let A be any random variable over the units in $\mathbb{Z}_p$, B be any random variable over $\mathbb{Z}_p$, and C be uniformly distributed over $\mathbb{Z}_p$ with A, B, and C independent Then

$$P(Ax^2 + Bx + C \text{ has two distinct roots}) = P(C \text{ is a square}) = \frac{p}{2(p+1)}$$

Proof: $Ax^2 + Bx + C$ has two distinct roots if and only if $B^2 - 4AC$ is a non-zero square A is a unit in $\mathbb{Z}_p$, and, since p is odd, so is -4 Thus, $B^2 - 4AC$ has the same distribution as C In particular, the probability that $B^2 - 4AC$ is a non-zero square is the same as the probability that C is a non-zero square $P(C = 0) = 0$, so $P(C$ is a non-zero square$) = p/[2(p+1)]$ $\square$

Corollary: Let B and C be independent, uniformly distributed random variables over the p-adic integers Then, the probability that the monic polynomial $x^2 + Bx + C$ has two distinct roots is $p/[2(p+1)]$

Proof: The random variable A with $P(A = 1) = 1$ is a random variable over the units in the p-adic integers, so the above proposition applies □

The same technique, however, cannot be applied to random polynomials where the first coefficient is not a unit

Theorem: Let A, B, and C be independent, uniformly distributed random variables over the p-adic integers Then, the probability that $B^2 - 4AC$ is a non-zero p-adic square is $1/2$ Therefore, the probability that the quadratic polynomial $Ax^2 + Bx + C$ has two distinct roots is also $1/2$

Proof: By the second lemma, the three independent random variables A, B, and C can be rewritten as six independent random variables $\hat{A}$, $\hat{B}$, $\hat{C}$, J, K, and L, where $A = p^J\hat{A}$, $B = p^K\hat{B}$, and $C = p^L\hat{C}$ So, the probability that $B^2 - 4AC$ is a square is the same as the probability that $p^{2K}\hat{B}^2 - 4p^{J+L}\hat{A}\hat{C}$ is a square Split this into three cases, depending on J, K, and L

Case 1: $2K < J + L$

If $2K < J + L$, then $p^{2K}\hat{B}^2 - 4p^{J+L}\hat{A}\hat{C} = p^{2K}(\hat{B}^2 - 4p^{J+L-2K}\hat{A}\hat{C})$ This will be a p-adic square if and only if $2K$ is even, and $\hat{B}^2 - 4p^{J+L-2K}\hat{A}\hat{C}$ is a square modulo p Since $\hat{B}^2 - 4p^{J+L-2K}\hat{A}\hat{C} \equiv \hat{B}^2 \pmod{p}$, $\hat{B}^2 - 4p^{J+L-2K}\hat{A}\hat{C}$ is always a square modulo p Clearly, $2K$ is even

Case 2: $2K = J + L$

If $2K = J + L$, then $p^{2K}\hat{B}^2 - 4p^{J+L}\hat{A}\hat{C} = p^{2K}(\hat{B}^2 - 4\hat{A}\hat{C})$ This will be a p-adic square if and only if $2K$ is even and $\hat{B}^2 - 4\hat{A}\hat{C}$ is a p-adic square ($\hat{B}^2 - 4\hat{A}\hat{C}$ may not be a p-adic unit) $2K$ is always even Let

$$p_1 = P(\hat{B}^2 - 4\hat{A}\hat{C} \text{ is a non-zero square})$$

Case 3: $2K > J + L$

If $2K > J + L$, then $p^{2K}\hat{B}^2 - 4p^{J+L}\hat{A}\hat{C} = p^{J+L}(p^{2K-J-L}\hat{B}^2 - 4\hat{A}\hat{C})$ This will be a p-adic square if and only if $J+L$ is even and $p^{2K-J-L}\hat{B}^2 - 4\hat{A}\hat{C}$ is a square modulo p The latter is true if and only if $-\hat{A}\hat{C}$ is a square modulo p

Since $\hat{A}$ and $\hat{C}$ are units, their product can never be 0 modulo p Also, half of the numbers in $\{1, \quad p-1\}$ are squares modulo p $-\hat{A} \equiv A_0 \pmod{p}$ and $\hat{C} \equiv C_0 \pmod{p}$, with A_0 and C_0 uniformly distributed over the above set There are $(p-1)^2$ possible choices for A_0 and C_0 (together) Let s be one of the $(p-1)/2$ squares modulo p If $A_0C_0 = s$, then $C_0 = s/A_0$ So, for any particular choice of A_0, there are $(p-1)/2$ choices for C_0 (namely, s/A_0) which make A_0C_0 equal to a square modulo p Thus, out of the $(p-1)^2$ choices for A_0 and C_0, $(p-1)^2/2$ of them result in the product being a square, so $P(-\hat{A}\hat{C}$ is a square$) = 1/2$

Let q_1 be the probability that $2K < J + L$, q_2 be the probability that $2K = J + L$, and q_3 be the probability that $2K > J + L$ and $J + L$ is even Then, $P(B^2 - 4AC$ is a square$) = q_1 \quad 1 + q_2 \quad p_1 + q_3 \quad 1/2$

If $K = 0$, $J = 0$, and $L = 0$, then $2K = J + L$ If $K = 0$ and at least one of J and L is positive, then $2K < J + L$ Let $K > 0$ If $J > 2K$, or if $J = 2K$ and L is positive, then $2K < J+L$ If $J = 2K$ and $L = 0$, then $2K = J+L$ Let $J < 2K$ $2K = J + L$ if $L = 2K - J$ If $L < 2K - J$, then $2K > J + L$ If $L > 2K - J$, then $2K < J + L$

The following table separates the possible values of J, K, and L into nine categories In each category, either $2K < J + L$, $2K = J + L$, or $2K > J + L$

$K=0$	$J=0$	$L=0$	R_1
		$L=1 \quad \infty$	R_2
	$J=1 \quad \infty$	$L=0 \quad \infty$	R_3
$K=1 \quad \infty$	$J=0 \quad 2K-1$	$L=0 \quad 2K-J-1$	R_4
		$L=2K-J$	R_5
		$L=2K-J+1 \quad \infty$	R_6
	$J=2K$	$L=0$	R_7
		$L=1 \quad \infty$	R_8
	$J=2K+1 \quad \infty$	$L=0 \quad \infty$	R_9

$$q_2 = P(2K = J + L) = R_1 + R_5 + R_7$$

$$q_1 = P(2K < J + L) = R_2 + R_3 + R_6 + R_8 + R_9 = 1 - q_2 - R_4$$

q_3 uses the values for J, K, and L in R_4, but further requires that $J + L$ be even Finding R_1, R_5, and R_7 will determine q_2 Then, finding R_4 will determine q_1 Finding q_3 will be similar to finding R_4

The following sums give the above values

$$R_1 = P(K = 0) \quad P(J = 0) \quad P(L = 0)$$

$$R_5 = \sum_{k=1}^{\infty} \sum_{j=0}^{2k-1} [l = 2k - j] P(K = k) \quad P(J = j) \quad P(L = l)$$

$$R_7 = \sum_{k=1}^{\infty} [j = 2k][l = 0] P(K = k) \quad P(J = j) \quad P(L = l)$$

$$R_4 = \sum_{k=1}^{\infty} \sum_{j=0}^{2k-1} \sum_{l=0}^{2k-j-1} P(K = k) \quad P(J = j) \quad P(L = l)$$

$$q_3 = \sum_{k=1}^{\infty} \sum_{j=0}^{2k-1} \sum_{l=0}^{2k-j-1} P(K = k) \quad P(J = j) \quad P(L = l) \quad 1_{j+l \text{ even}}$$

where $1_{j+l \text{ even}}$ is 1 if $j+l$ is even, and 0 if $j+l$ is odd

The geometric series will be used often in the following computations, as will a similar series (here, $a < 1$)

$$\begin{aligned}
\sum_{k=0}^{\infty} a^k &= \frac{1}{1-a} \\
\sum_{k=1}^{\infty} a^k &= \frac{1}{1-a} - 1 \\
&= \frac{a}{1-a} \\
\sum_{k=1}^{\infty} k a^k &= \sum_{k=0}^{\infty} k a^k \\
&= \sum_{k=0}^{\infty} k a^{k-1} a \\
&= a \sum_{k=0}^{\infty} k a^{k-1} \\
&= a \sum_{k=0}^{\infty} \frac{d}{da} a^k \\
&= a \frac{d}{da} \sum_{k=0}^{\infty} a^k \\
&= a \frac{d}{da} \frac{1}{1-a} \\
&= a \frac{1}{(1-a)^2}
\end{aligned}$$

In particular, for $a = p^{-n}$,

$$\begin{aligned}
\sum_{k=0}^{\infty}\left(p^{-n}\right)^k &= \frac{1}{1-p^{-n}} \\
&= \frac{p^n}{p^n-1}, \\
\sum_{k=1}^{\infty}\left(p^{-n}\right)^k &= \frac{p^{-n}}{1-p^{-n}} \\
&= \frac{1}{p^n-1}, \\
\sum_{k=1}^{\infty} k\left(p^{-n}\right)^k &= \sum_{k=0}^{\infty} k\left(p^{-n}\right)^k \\
&= p^{-n}\frac{1}{(1-p^{-n})^2} \\
&= \frac{p^n}{(p^n-1)^2}
\end{aligned}$$

$$\begin{aligned}
R_1 &= P(K=0)\cdot P(J=0)\quad P(L=0) \\
&= \frac{p-1}{p}p^0\quad \frac{p-1}{p}p^0\quad \frac{p-1}{p}p^0 \\
&= \frac{(p-1)^3}{p^3}
\end{aligned}$$

$$\begin{aligned}
R_5 &= \sum_{k=1}^{\infty}\sum_{j=0}^{2k-1}[l=2k-j]P(K=k)\quad P(J=j)\quad P(L=l) \\
&= \sum_{k=1}^{\infty}\sum_{j=0}^{2k-1}[l=2k-j]\frac{p-1}{p}p^{-k}\quad \frac{p-1}{p}p^{-j}\frac{p-1}{p}p^{-l} \\
&= \frac{(p-1)^3}{p^3}\sum_{k=1}^{\infty}\sum_{j=0}^{2k-1}p^{-k}p^{-j}p^{-(2k-j)} \\
&= \frac{(p-1)^3}{p^3}\sum_{k=1}^{\infty}\sum_{j=0}^{2k-1}p^{-3k} \\
&= \frac{(p-1)^3}{p^3}\sum_{k=1}^{\infty}2k\left(p^{-3}\right)^k \\
&= 2\frac{(p-1)^3}{p^3}\frac{p^3}{(p^3-1)^2} \\
&= 2\frac{p-1}{(p^2+p+1)^2}
\end{aligned}$$

$$
\begin{aligned}
R_7 &= \sum_{k=1}^{\infty} [\jmath = 2k][l = 0] P(K = k) \quad P(J = \jmath) \quad P(L = l) \\
&= \sum_{k=1}^{\infty} \frac{p-1}{p} p^{-k} \quad \frac{p-1}{p} p^{-2k} \quad \frac{p-1}{p} p^{0} \\
&= \frac{(p-1)^3}{p^3} \sum_{k=1}^{\infty} \left(p^{-3}\right)^k \\
&= \frac{(p-1)^3}{p^3} \frac{1}{p^3-1} \\
&= \frac{(p-1)^2}{p^3(p^2+p+1)}
\end{aligned}
$$

The probability q_2 can now be computed

$$
\begin{aligned}
q_2 &= \frac{(p-1)^3}{p^3} + 2\frac{p-1}{(p^2+p+1)^2} + \frac{(p-1)^2}{p^3(p^2+p+1)} \\
&= \frac{(p-1)^3(p^2+p+1)^2 + 2(p-1)p^3 + (p-1)^2(p^2+p+1)}{p^3(p^2+p+1)^2} \\
&= \frac{(p-1)(p^3-1)^2 + 2(p-1)p^3 + (p-1)(p^3-1)}{p^3(p^2+p+1)^2} \\
&= \frac{(p-1)(p^6 - 2p^3 + 1 + 2p^3 + p^3 - 1)}{p^3(p^2+p+1)^2} \\
&= \frac{(p-1)(p^6+p^3)}{p^3(p^2+p+1)^2} \\
&= \frac{(p-1)(p^3+1)}{(p^2+p+1)^2}
\end{aligned}
$$

$$
\begin{aligned}
R_4 &= \sum_{k=1}^{\infty}\sum_{j=0}^{2k-1}\sum_{l=0}^{2k-j-1} P(K=k)\;\; P(J=j)\;\; P(L=l) \\
&= \sum_{k=1}^{\infty}\sum_{j=0}^{2k-1}\sum_{l=0}^{2k-j-1} \frac{p-1}{p}p^{-k}\;\; \frac{p-1}{p}p^{-j}\;\; \frac{p-1}{p}p^{-l} \\
&= \frac{(p-1)^3}{p^3}\sum_{k=1}^{\infty}\left(p^{-k}\sum_{j=0}^{2k-1}\left(p^{-j}\sum_{l=0}^{2k-j-1}\left(p^{-1}\right)^l\right)\right) \\
&= \frac{(p-1)^3}{p^3}\sum_{k=1}^{\infty}\left(p^{-k}\sum_{j=0}^{2k-1}p^{-j}\frac{1-p^{-(2k-j)}}{1-p^{-1}}\right) \\
&= \frac{(p-1)^3}{p^3}\frac{1}{1-p^{-1}}\sum_{k=1}^{\infty}\left(p^{-k}\sum_{j=0}^{2k-1}\left(p^{-j}-p^{-2k}\right)\right) \\
&= \frac{(p-1)^3}{p^3}\frac{p}{p-1}\sum_{k=1}^{\infty}p^{-k}\left(\frac{1-p^{-2k}}{1-p^{-1}}-2kp^{-2k}\right) \\
&= \frac{(p-1)^2}{p^2}\sum_{k=1}^{\infty}\frac{p}{p-1}\left(p^{-k}-p^{-3k}\right)-2k\left(p^{-3}\right)^k \\
&= \frac{(p-1)^2}{p^2}\sum_{k=1}^{\infty}\frac{p}{p-1}\left(p^{-k}-p^{-3k}\right)-\frac{(p-1)^2}{p^2}\sum_{k=1}^{\infty}2k\left(p^{-3}\right)^k \\
&= \frac{(p-1)}{p}\sum_{k=1}^{\infty}\left(p^{-k}-p^{-3k}\right)-2\frac{(p-1)^2}{p^2}\sum_{k=1}^{\infty}k\left(p^{-3}\right)^k \\
&= \frac{(p-1)}{p}\left(\frac{p}{p-1}-\frac{p^3}{p^3-1}\right)-2\frac{(p-1)^2}{p^2}\frac{p^3}{(p^3-1)^2} \\
&= 1-\frac{p^2}{p^2+p+1}-2\frac{p}{(p^2+p+1)^2} \\
&= \frac{(p^2+p+1)^2-p^2(p^2+p+1)-2p}{(p^2+p+1)^2} \\
&= \frac{p^3+2p^2+1}{(p^2+p+1)^2}
\end{aligned}
$$

The probability q_1 can now be computed

$$
\begin{aligned}
q_1 &= 1 - q_2 - R_4 \\
&= 1 - \frac{(p-1)(p^3+1)}{(p^2+p+1)^2} - \frac{p^3+2p^2+1}{(p^2+p+1)^2} \\
&= \frac{(p^2+p+1)^2 - (p-1)(p^3+1) - (p^3+2p^2+1)}{(p^2+p+1)^2} \\
&= \frac{p^4+2p^3+3p^2+2p+1-(p^4-p^3+p-1)-(p^3+2p^2+1)}{(p^2+p+1)^2} \\
&= \frac{2p^3+p^2+p+1}{(p^2+p+1)^2}
\end{aligned}
$$

$$
\begin{aligned}
q_3 &= \sum_{k=1}^{\infty} \sum_{j=0}^{2k-1} \sum_{l=0}^{2k-j-1} P(K=k)\ \ P(J=j)\ \ P(L=l)\ \ 1_{j+l \text{ even}} \\
&= \sum_{k=1}^{\infty} \sum_{j=0}^{2k-1} \sum_{l=0}^{2k-j-1} P(K=k)\ \ P(J=j)\ \ P(L=l)\ \ 1_{j,l \text{ even}} \\
&\quad + \sum_{k=1}^{\infty} \sum_{j=0}^{2k-1} \sum_{l=0}^{2k-j-1} P(K=k)\ \ P(J=j)\ \ P(L=l)\ \ 1_{j,l \text{ odd}}
\end{aligned}
$$

Split this into two different sums

$$
a_3 = \sum_{k=1}^{\infty} \sum_{j=0}^{2k-1} \sum_{l=0}^{2k-j-1} P(K=k)\ \ P(J=j)\ \ P(L=l)\ \ 1_{j,l \text{ even}}
$$

and

$$
b_3 = \sum_{k=1}^{\infty} \sum_{j=0}^{2k-1} \sum_{l=0}^{2k-j-1} P(K=k)\ \ P(J=j)\ \ P(L=l)\ \ 1_{j,l \text{ odd}}
$$

so that $q_3 = a_3 + b_3$

$$
a_3 = \sum_{k=1}^{\infty} \sum_{j=0}^{2k-1} \sum_{l=0}^{2k-j-1} P(K=k)\ \ P(J=j)\ \ P(L=l)\ \ 1_{j,l \text{ even}}
$$

Since j must be even, it runs from 0 to $2k-2$ Similarly, l runs from 0 to $2k-j-2$

Let $j = 2j'$ and $l = 2l'$ to get

$$
a_3 = \sum_{k=1}^{\infty} \sum_{j'=0}^{k-1} \sum_{l'=0}^{k-j'-1} P(K=k)\ \ P(J=2j')\ \ P(L=2l')
$$

and then get rid of the primes to solve for a_3

$$
\begin{aligned}
a_3 &= \sum_{k=1}^{\infty}\sum_{j=0}^{k-1}\sum_{l=0}^{k-j-1} P(K=k)\;\; P(J=2j)\;\; P(L=2l) \\
&= \sum_{k=1}^{\infty}\sum_{j=0}^{k-1}\sum_{l=0}^{k-j-1} \frac{(p-1)^3}{p^3} p^{-k} p^{-2j} p^{-2l} \\
&= \frac{(p-1)^3}{p^3}\sum_{k=1}^{\infty} p^{-k}\left(\sum_{j=0}^{k-1} p^{-2j}\left(\sum_{l=0}^{k-j-1} p^{-2l}\right)\right) \\
&= \frac{(p-1)^3}{p^3}\sum_{k=1}^{\infty} p^{-k}\left(\sum_{j=0}^{k-1} p^{-2j}\frac{1-p^{-2(k-j)}}{1-p^{-2}}\right) \\
&= \frac{(p-1)^3}{p^3}\frac{p^2}{p^2-1}\sum_{k=1}^{\infty} p^{-k}\left(\sum_{j=0}^{k-1} p^{-2j} - p^{-2k}\right) \\
&= \frac{(p-1)^2}{p(p+1)}\sum_{k=1}^{\infty} p^{-k}\left(\frac{1-p^{-2k}}{1-p^{-2}} - kp^{-2k}\right) \\
&= \frac{(p-1)^2}{p(p+1)}\left(\sum_{k=1}^{\infty}\frac{p^{-k}-p^{-3k}}{1-p^{-2}} - \sum_{k=1}^{\infty} kp^{-3k}\right) \\
&= \frac{(p-1)^2}{p(p+1)}\left(\frac{p^2}{p^2-1}\sum_{k=1}^{\infty}\left(p^{-k}-p^{-3k}\right) - \frac{p^3}{(p^3-1)^2}\right) \\
&= \frac{(p-1)^2}{p(p+1)}\left(\frac{p^2}{p^2-1}\left(\frac{1}{p-1}-\frac{1}{p^3-1}\right) - \frac{p^3}{(p^3-1)^2}\right) \\
&= \frac{p(p-1)}{(p+1)^2}\left(\frac{p^2+p+1}{p^3-1}-\frac{1}{p^3-1}\right) - \frac{p^2}{(p+1)(p^2+p+1)^2} \\
&= \frac{p(p-1)}{(p+1)^2}\frac{p^2+p}{p^3-1} - \frac{p^2}{(p+1)(p^2+p+1)^2} \\
&= \frac{p^2}{(p+1)(p^2+p+1)} - \frac{p^2}{(p+1)(p^2+p+1)^2} \\
&= \frac{p^2(p^2+p+1)}{(p+1)(p^2+p+1)^2} - \frac{p^2}{(p+1)(p^2+p+1)^2} \\
&= \frac{p^2(p^2+p)}{(p+1)(p^2+p+1)^2} \\
&= \frac{p^3}{(p^2+p+1)^2}
\end{aligned}
$$

$$
b_3 = \sum_{k=1}^{\infty}\sum_{j=0}^{2k-1}\sum_{l=0}^{2k-j-1} P(K=k)\;\; P(J=j)\;\; P(L=l)\;\; 1_{j,l \text{ odd}}
$$

Since j and l must be odd, j must be between 1 and $2k-1$, and l must be between 1 and $2k-j-2$ Let $j = 2j'+1$ and $l = 2l'+1$ to find that j' is between 0 and $k-1$, and l' is between 0 and $k-j'-2$ Dropping primes gives

$$\begin{aligned}
b_3 &= \sum_{k=1}^{\infty}\sum_{j=0}^{k-1}\sum_{l=0}^{k-j-2} P(K=k)\ \ P(J=2j+1)\ \ P(L=2l+1) \\
&= \sum_{k=1}^{\infty}\sum_{j=0}^{k-1}\sum_{l=0}^{k-j-2} \frac{(p-1)^3}{p^3} p^{-k} p^{-2j-1} p^{-2l-1} \\
&= \frac{(p-1)^3}{p^5}\sum_{k=1}^{\infty} p^{-k}\left(\sum_{j=0}^{k-1} p^{-2j}\left(\sum_{l=0}^{k-j-2} p^{-2l}\right)\right) \\
&= \frac{1}{p^2}\frac{(p-1)^3}{p^3}\sum_{k=1}^{\infty} p^{-k}\left(\sum_{j=0}^{k-1} p^{-2j}\left(\sum_{l=0}^{k-j-1} p^{-2l}\right)\right) - \\
&\quad \frac{1}{p^2}\frac{(p-1)^3}{p^3}\sum_{k=1}^{\infty} p^{-k}\left(\sum_{j=0}^{k-1} p^{-2j}\left([l=k-j-1]p^{-2l}\right)\right) \\
&= \frac{1}{p^2}\left(a_3 - \frac{(p-1)^3}{p^3}\sum_{k=1}^{\infty} p^{-k}\left(\sum_{j=0}^{k-1} p^{-2j}\left(p^{-2(k-j-1)}\right)\right)\right) \\
&= \frac{1}{p^2}\left(\frac{p^3}{(p^2+p+1)^2} - \frac{(p-1)^3}{p^3}\sum_{k=1}^{\infty} p^{-k}\left(\sum_{j=0}^{k-1} p^{-2k+2}\right)\right) \\
&= \frac{p}{(p^2+p+1)^2} - \frac{(p-1)^3}{p^3}\sum_{k=1}^{\infty} p^{-k}\left(\sum_{j=0}^{k-1} p^{-2k}\right) \\
&= \frac{p}{(p^2+p+1)^2} - \frac{(p-1)^3}{p^3}\sum_{k=1}^{\infty} p^{-k}\left(kp^{-2k}\right) \\
&= \frac{p}{(p^2+p+1)^2} - \frac{(p-1)^3}{p^3}\sum_{k=1}^{\infty} kp^{-3k} \\
&= \frac{p}{(p^2+p+1)^2} - \frac{(p-1)^3}{p^3}\frac{p^3}{(p^3-1)^2} \\
&= \frac{p}{(p^2+p+1)^2} - \frac{p-1}{(p^2+p+1)^2} \\
&= \frac{1}{(p^2+p+1)^2}
\end{aligned}$$

Thus,

$$q_3 = a_3 + b_3 = \frac{p^3}{(p^2+p+1)} + \frac{1}{(p^2+p+1)^2} = \frac{p^3+1}{(p^2+p+1)^2}$$

$p_1 = P(\hat{B}^2 - 4\hat{A}\hat{C}$ is a non-zero square) Denote the unit p-adic integers by $\mathbb{Z}_p$ Let $f(A,B,C) = B^2 - 4AC$ Then,

$$p_1 = \mu(\{(A,B,C)|A,B,C \in \mathbb{Z}_p \text{ and } f(A,B,C) \text{ is a non-zero square}\}),$$

or $p_1 = \mu((\mathbb{Z}_p)^3 \cap f^{-1}(S))$, where S is the set of non-zero p-adic integer squares Since S is open, and f is continuous, and $\mathbb{Z}_p$ is open, p_1 is the measure of an open set In particular,

$$p_1 = \lim_{n\to\infty} P(\hat{B}^2 - 4\hat{A}\hat{C} \text{ is a non-zero square modulo } p^n)$$

And, since open sets are measurable, the limit has to exist, so

$$p_1 = \lim_{n\to\infty} P(\hat{B}^2 - 4\hat{A}\hat{C} \text{ is a non-zero square modulo } p^{2n})$$

Let $\hat{A}$, $\hat{B}$, and $\hat{C}$ be units in $\mathbb{Z}/p^{2n}\mathbb{Z}$ Let S_1 be the set of unit squares in $\mathbb{Z}/p^{2n}\mathbb{Z}$, and let S_2 be the set of non-unit non-zero squares in $\mathbb{Z}/p^{2n}\mathbb{Z}$

$$\begin{aligned}
p_2 &= P(\hat{B}^2 - 4\hat{A}\hat{C} \text{ is a square modulo } p^{2n}) \\
&= \sum_{k\in S_1\cup S_2} P(\hat{B}^2 - 4\hat{A}\hat{C} = k) \\
&= \sum_{k\in S_1} P(\hat{B}^2 - 4\hat{A}\hat{C} = k) + \sum_{k\in S_2} P(\hat{B}^2 - 4\hat{A}\hat{C} = k) \\
&= \sum_{k\in S_1} P\left(\hat{C} = \frac{\hat{B}^2 - k}{4\hat{A}}\right) + \sum_{k\in S_2} P\left(\hat{C} = \frac{\hat{B}^2 - k}{4\hat{A}}\right)
\end{aligned}$$

Given k, $\hat{A}$, and $\hat{B}$, there is at most one choice for $\hat{C}$ Since $4\hat{A}$ is a unit, the only way there can be no choices for $\hat{C}$ is if $\hat{B}^2 - k$ has a factor of p, since $\hat{C}$ must be a unit If k is divisible by p, $\hat{B}^2 - k$ will not be, and $\hat{B}$ can be any unit Suppose k is not divisible by p There is some j such that $k = j^2 = (-j)^2$, or $\hat{B}^2 - k = \hat{B}^2 - j^2 = (\hat{B}+j)(\hat{B}-j)$ p divides $\hat{B}^2 - k$ if and only if p divides at least one of $\hat{B}+j$ or $\hat{B}-j$ So, p divides $\hat{B}^2 - k$ if and only if $B \equiv \pm j \pmod{p}$

An element of $\mathbb{Z}/p^{2n}\mathbb{Z}$ is a unit if and only if it is not divisible by p, so there are p^{2n-1} units in $\mathbb{Z}/p^{2n}\mathbb{Z}$, or $(p-1)p^{2n-1}$ non-units in $\mathbb{Z}/p^{2n}\mathbb{Z}$. For $\hat{C} = \frac{\hat{B}^2-k}{4\hat{A}}$ to be valid, $\hat{A}$ can be any of these units and $\hat{C}$ can only be one of these units. If k is not a unit, then $\hat{B}$ can be any unit, but if k is a unit, then $\hat{B} \neq \pm j \pmod{p}$, so $\hat{B}$ can only be one of $(p-3)p^{2n-1}$ of the units. So, the probability becomes

$$\begin{aligned}
p_2 &= \sum_{k\in S_1} P\left(\hat{C} = \frac{\hat{B}^2-k}{4\hat{A}}\right) + \sum_{k\in S_2} P\left(\hat{C} = \frac{\hat{B}^2-k}{4\hat{A}}\right) \\
&= \sum_{k\in S_1} \frac{(p-1)p^{2n-1}}{(p-1)p^{2n-1}} \frac{(p-3)p^{2n-1}}{(p-1)p^{2n-1}} \frac{1}{(p-1)p^{2n-1}} \\
&\quad + \sum_{k\in S_2} \frac{(p-1)p^{2n-1}}{(p-1)p^{2n-1}} \frac{(p-1)p^{2n-1}}{(p-1)p^{2n-1}} \frac{1}{(p-1)p^{2n-1}} \\
&= \sum_{k\in S_1} \frac{p-3}{(p-1)^2p^{2n-1}} + \sum_{k\in S_2} \frac{1}{(p-1)p^{2n-1}} \\
&= |S_1| \quad \frac{p-3}{(p-1)^2p^{2n-1}} + |S_2| \quad \frac{1}{(p-1)p^{2n-1}}
\end{aligned}$$

where $|S_i|$ is the cardinality of the set S_i. For k to be a unit square, it must be a square modulo p. Thus, half of the units are squares, and $|S_1| = (p-1)p^{2n-1}/2$. If k is a non-unit square, it must be divisible by an even power of p. In addition, if k is divisible by p^{2j}, then $k = p^{2j}\alpha$, where α is a unit square modulo p^{2n-2j}. There are $(p-1)p^{2n-2j-1}/2$ possibilities for α. So, the number of non-unit squares is

$$\begin{aligned}
|S_2| &= \sum_{j=1}^{n-1} \frac{(p-1)p^{2n-2j-1}}{2} \\
&= \frac{p-1}{2p} \sum_{j=1}^{n-1} \left(p^2\right)^{n-j} \\
&= \frac{p-1}{2p} \sum_{i=1}^{n-1} \left(p^2\right)^{i} \\
&= \frac{p-1}{2p} \left(\frac{p^{2n}-1}{p^2-1} - 1\right) \\
&= \frac{p-1}{2p} \frac{p^{2n}-p^2}{p^2-1} \\
&= \frac{p^{2n-1}-p}{2(p+1)}
\end{aligned}$$

Thus,

$$\begin{aligned} p_2 &= |S_1| \quad \frac{p-3}{(p-1)^2 p^{2n-1}} + |S_2| \quad \frac{1}{(p-1)p^{2n-1}} \\ &= \frac{(p-1)p^{2n-1}}{2} \quad \frac{p-3}{(p-1)^2 p^{2n-1}} + \frac{p^{2n-1}-p}{2(p+1)} \quad \frac{1}{(p-1)p^{2n-1}} \\ &= \frac{p-3}{2(p-1)} + \frac{1-p^{2-2n}}{2(p^2-1)} \end{aligned}$$

Therefore,

$$\begin{aligned} p_1 &= \lim_{n\to\infty} \frac{p-3}{2(p-1)} + \frac{1-p^{2-2n}}{2(p^2-1)} \\ &= \lim_{n\to\infty} \frac{(p-3)(p+1)}{2(p^2-1)} + \frac{1}{2(p^2-1)} - \frac{p^2}{2(p^2-1)p^{2n}} \\ &= \lim_{n\to\infty} \frac{p^2-2p-3+1}{2(p^2-1)} - \frac{p^2}{2(p^2-1)}\frac{1}{p^{2n}} \\ &= \frac{p^2-2p-2}{2(p^2-1)} - \lim_{n\to\infty} \frac{p^2}{2(p^2-1)}\frac{1}{p^{2n}} \\ &= \frac{p^2-2p-2}{2(p^2-1)} \end{aligned}$$

Finally,

$$
\begin{aligned}
P(B^2-4AC \text{ is a square}) &= q_1 \quad 1+q_2 \quad p_1+q_3 \quad 1/2 \\
&= \frac{2p^3+p^2+p+1}{(p^2+p+1)^2} \\
&\quad + \frac{(p-1)(p^3+1)}{(p^2+p+1)^2} \quad \frac{p^2-2p-2}{2(p^2-1)} \\
&\quad + \frac{p^3+1}{2(p^2+p+1)^2} \\
&= \frac{2(p+1)(2p^3+p^2+p+1)}{2(p+1)(p^2+p+1)^2} \\
&\quad + \frac{(p^3+1)(p^2-2p-2)}{2(p+1)(p^2+p+1)^2} \\
&\quad + \frac{(p+1)(p^3+1)}{2(p+1)(p^2+p+1)^2} \\
&= \frac{4p^4+6p^3+4p^2+4p+2}{2(p+1)(p^2+p+1)^2} \\
&\quad + \frac{p^5-2p^4-2p^3+p^2-2p-2}{2(p+1)(p^2+p+1)^2} \\
&\quad + \frac{p^4+p^3+p+1}{2(p+1)(p^2+p+1)^2} \\
&= \frac{p^5+3p^4+5p^3+5p^2+3p+1}{2(p+1)(p^4+2p^3+3p^2+2p+1)} \\
&= \frac{p^5+3p^4+5p^3+5p^2+3p+1}{2(p^5+3p^4+5p^3+5p^2+3p+1)} \\
&= \frac{1}{2}
\end{aligned}
$$

4. The Measure Witt Ring

The previous section found the probability that a random quadratic form has two distinct roots for various fields and measures In the p-adic case, that probability was $1/2$, no matter what odd prime p is chosen There may be a way to explain why these probabilities are the same, and perhaps to determine how probabilites for other fields might compare With all of the fields and measures in question, the key is the probability that the quadratic form $b^2 - 4ac$ is a square in the field The Witt ring is a mathematical object which tells when, in some sense, the theory of quadratic forms is the same over two different fields A version of this, the measure Witt ring, may help explain when two fields with measures have, in some sense, the same theory of measure and quadratic forms together

4.1 Equivalence of Quadratic Forms

Two quadratic forms q and r over a field $\mathbb{F}$ are said to be equivalent if there is a linear transformation T such that $q(\vec{x}) = r(T\vec{x})$ A similar definition can be used for measure equivalence

Definition: Let $\mathbb{F}$ be a field Let q and r be quadratic forms from $\mathbb{F}^n$ to $\mathbb{F}$, and let μ be a measure on $\mathbb{F}$ Call the resulting product measures μ_n Then q and r are **equivalent with respect to** μ, or **μ-equivalent**, if $q(\vec{x}) = r(T\vec{x})$ for some invertible linear transformation T which preserves μ, that is, $\mu_n(A) = \mu_n(T^{-1}(A))$ for all measurable sets A When the measure is understood, q and r are called **measure equivalent**

This definition gives

$$\begin{aligned}\mu_n(q^{-1}(A)) &= \mu_n((r \circ T)^{-1}(A)) \\ &= \mu_n((T^{-1} \circ r^{-1})(A)) \\ &= \mu_n(T^{-1}(r^{-1}(A))) \\ &= \mu_n(r^{-1}(A))\end{aligned}$$

provided $q^{-1}(A)$ and $r^{-1}(A)$ are measurable This matches with the definition of measure equivalence for general functions However, with some measures it is possible that $\mu_n(q^{-1}(A)) = \mu_n(r^{-1}(A))$, but there is no invertible linear transformation T such that $q(\vec{x}) = r(T\vec{x})$ For instance, if q is a real two-dimensional hyperbolic quadratic form (that is, $q = ax^2 + bxy + cy^2$ and $b^2 - 4ac > 0$), and A is an interval, then $\mu_2(q^{-1}(A))$ is always infinite, where μ is Lebesgue measure If q and r are real two-dimensional hyperbolic quadratic forms whose matrices have different determinants, then any linear transformation T which makes the two equivalent must have a determinant other than 1 or -1 However, as will be seen later, the only Lebesgue measure-preserving linear transformations are the ones with determinant 1 or -1 Thus, even though $q^{-1}(A)$ and $r^{-1}(A)$ are always the same (infinite), there is no measure-preserving linear transformation T such that $q(\vec{x}) = r(T\vec{x})$

4.2 The Witt Ring

The Witt ring is a mathematical object which determines when the theory of quadratic forms is the same for two different fields More precisely, if two fields have isomorphic Witt rings (with operations symbolized by + and), then there is a function ϕ from the quadratic forms of one field to another, such that, given quadratic forms q, r, and s, then $q = r + s$ implies $\phi(q) = \phi(r) + \phi(s)$ and $q = r \ \ s$ implies $\phi(q) = \phi(r) \ \ \phi(s)$ [6, p 58]

The measure Witt ring is a slight modification of the Witt ring The measure Witt ring uses measure-preserving linear transformations where the Witt ring any invertible linear transformations to define equivalence classes Since all invertible linear transformations are measure preserving if the measure is the zero measure, the canonical Witt ring is a special case of the measure Witt ring

4.3 Measure-Preserving Linear Transformations

In the construction of the measure Witt ring, it is useful to know which invertible linear transformations are measure preserving Given a measure μ on the field $\mathbb{F}$, the measure on $\mathbb{F}^n$ is determined by the product measure The identity linear transformation I is always measure preserving, for a measurable set U, $I^{-1}(U) = U$, so $\mu(I^{-1}(U)) = \mu(U)$ If an invertible linear transformation T is measure preserving, then its inverse will also be measure preserving, $\mu((T^{-1})^{-1}(U)) = \mu(T(U))$, and since T is measure preserving, $\mu(T(U)) = \mu(T^{-1}(T(U)) = \mu(U)$ Also, since the measure on $\mathbb{F}^n$ is the product measure, a linear transformation which switches coordinates of a vector (for example, $T(x, y, z) = (y, x, z)$) with respect to the standard basis is also measure preserving Note that if μ is the zero measure, all invertible linear transformations are measure-preserving

4 3 1 Real Measures

The relation between Lebesgue measure and integration leads to a relatively simple determination of whether or not a linear transformation is measure preserving for some measures on the real numbers Let μ be Lebesgue measure on the real numbers Suppose that ν is a real measure such that $\nu(A) = \int_A f(x)d\mu$, where f is a continuous function If ν is a finite signed measure which is absolutely continuous

with respect to μ, then the Radon-Nikodym theorem allows us to find an f with $|f|$ integrable [1, p 238]

A linear transformation is ν-preserving if, for all measurable sets A, $\nu(A) = \nu(T^{-1}(A))$ (Here, μ and ν also represent their product measures in $\mathbb{R}^n$) Equivalently, $\int_A f(\vec{x})d\mu = \int_{T^{-1}(A)} f(\vec{x})d\mu = \int_A f(T^{-1}(\vec{x}))|J(T^{-1})|d\mu$, where $J(T^{-1})$ is the Jacobian of the linear transformation T^{-1}, which is the determinant of T^{-1} Let Δ be the determinant of T Then, T is a ν-preserving linear transformation if and only if $\int_A f(\vec{x})d\mu = 1/|\Delta| \int_A f(T^{-1}(\vec{x}))d\mu$ for all measurable A By the Fundamental Theorem of Calculus, this requires that $f(\vec{x}) = 1/|\Delta| f(T^{-1}(\vec{x}))$ for all vectors $\vec{x}$ Therefore, T is ν-preserving if and only if $f(\vec{x}) = 1/|\Delta| f(T^{-1}(\vec{x}))$ for all vectors $\vec{x}$

4 3 2 Haar Measures

If μ is a Haar measure, then μ is translation-invariant (that is, $\mu(A) = \mu(x + A)$ for all $x \in F$ and measurable A) This lets us narrow down which linear transformations are measure-preserving The following transformation is measure preserving for Haar measures

Theorem: Suppose T is a transformation from $X \times Y$ into itself, with X and Y one-dimensional vector spaces over F, such that $T(x, y) = (x, y + kx)$, with k some fixed scalar in F Let μ be a Haar measure on F Then, T is μ-preserving

Proof: (This proof is based on one given in [5, p 258]) By definition of T, $T^{-1}(x, y) = (x, y - kx)$ Let E be a measurable subset of $X \times Y$ For any set A in $X \times Y$, and $x \in X$, define A_x to be the set of all $y \in Y$ such that $(x, y) \in A$ Let $y \in (T^{-1}(E))_x$, that is, $(x, y) \in (T^{-1}(E))$ Then, $(x, y + kx)$ must be in E, or, $y \in E_x - kx$ Similarly, if $y \in E_x - kx$, then $y + kx$ is in E, or $(x, y + kx)$ is

in E, so that $(x, y + kx - kx) = (x, y) \in T^{-1}(E)$, or $y \in (T^{-1}(E))_x$ Therefore, $(T^{-1}(E))_x = E_x - kx$

Then,

$$(\mu \times \mu)(T^{-1}(E)) = \int \mu((T^{-1}(E))_x)d\mu = \int \mu(E_x - kx)d\mu = \int \mu(E_x)d\mu = \mu(E)$$

So, T is μ-preserving □

Thus, if a matrix (representing a linear transformation) is measure preserving, then we can rearrange rows, and add rows to one another, to find another measure preserving matrix Similarly, we can multiply any invertible matrix by measure-preserving matrices to get a diagonal matrix Either both the diagonal matrix and the original matrix are measure preserving, or neither are

4.4 Construction of the Measure Witt Ring

The following construction is adapted from the construction of the Witt ring in [8]

Let $\mathbb{F}$ be a field, and μ be a measure on that field Use the product measure as a measure on $\mathbb{F}^n$ Each quadratic form f on $\mathbb{F}$ maps $\mathbb{F}^n$ to itself for some integer n The integer n is the dimension of the form f, and f is called an n-dimensional form Each quadratic form f can be represented uniquely by a symmetric matrix M_f, such that $f(\vec{x}) = (\vec{x})^t \ M_f \ \vec{x}$, where the symbol t represents transposition A quadratic form f is regular if M_f is invertible Then, two quadratic forms f and g are equivalent if and only if $f(\vec{x}) = g(T\vec{x})$ for some invertible linear transformation T, or, $M_f = T^t \ M_g \ T$ This is an equivalence relation on the set of regular quadratic forms Call this set of equivalence classes $M(\mathbb{F}, \mu)$

Definition: The **orthogonal sum** of two quadratic forms $q \quad \mathbb{F}^n \to \mathbb{F}$ and $r \quad \mathbb{F}^m \to \mathbb{F}$ is $q \oplus r \quad \mathbb{F}^n \times \mathbb{F}^m \to \mathbb{F}$, where $(q \oplus r)(\vec{x}, \vec{y}) = q(\vec{x}) + r(\vec{y})$ in $\mathbb{F}$

This operation is well-defined, if $q_1(\vec{x}) = q(T\vec{x})$, then

$$(q_1 \oplus r)(\vec{x}, \vec{y}) = q_1(\vec{x}) + r(\vec{y}) = q(T\vec{x}) + r(\vec{y}) = (q \oplus r)(T\vec{x}, \vec{y}) = (q \oplus r)((T \oplus I)(\vec{x}, \vec{y}))$$

Also, the orthogonal sum is commutative here, $(q \oplus r)(\vec{x}, \vec{y}) = (r \oplus q)(\vec{y}, \vec{x})$, and the linear function which switches coordinates is measure preserving

Definition: The **tensor product** of two quadratic forms $q \quad \mathbb{F}^m \to \mathbb{F}$ and $r \quad \mathbb{F}^m \to \mathbb{F}$ is $q \otimes r \quad \mathbb{F}^{mm} \to \mathbb{F}$, where $(q \otimes r)(\vec{x} \otimes \vec{y}) = q(\vec{x}) \quad r(\vec{y})$ in $\mathbb{F}$ The matrix of $q \otimes r$ will be the Kronecker product of the matrices of q and r This holds in equivalence classes also

Under the operations $\oplus$ and $\otimes$, $M(\mathbb{F}, \mu)$ is a semi-ring Cancellation holds in a semi-group if $q \oplus q_1 = q \oplus q_2$ implies $q_1 = q_2$ If cancellation does not hold in $M(\mathbb{F}, \mu)$, then combine equivalence classes so that q_1 is equivalent to q_2 if $q \oplus q_1 = q \oplus q_2$ for some quadratic form q, cancellation then does hold

The following Grothendieck construction generates a group from a cancellation semi-group Define a relation on $M(\mathbb{F}, \mu) \times M(\mathbb{F}, \mu)$ by

$$(x, y) \simeq (x', y') \Longleftrightarrow x \oplus y' = x' \oplus y \in M(\mathbb{F})$$

Since $x \oplus y = x \oplus y$, $(x, y) \simeq (x, y)$ And if $(x, y) \simeq (x', y')$, then $x \oplus y' = x' \oplus y$, or $x' \oplus y = x \oplus y'$, or $(x', y') \simeq (x, y)$ If $(x, y) \simeq (x', y')$ and $(x', y') \simeq (x'', y'')$, then $x \oplus y' = x' \oplus y$ and $x' \oplus y'' = x'' \oplus y'$ Since the operation $\oplus$ is commutative,

$$x \oplus y'' \oplus y' = x \oplus y' \oplus y'' = x' \oplus y \oplus y'' = y \oplus x' \oplus y'' = y \oplus x'' \oplus y'$$

By cancellation, $x \oplus y'' = x'' \oplus y$, and the relation is transitive Therefore, this is an equivalence relation Let $\mathrm{Groth}(M(\mathbb{F}, \mu))$ be the set of equivalence classes of $M(\mathbb{F}, \mu) \times M(\mathbb{F}, \mu)$ under this relation Addition and multiplication on $M(\mathbb{F}, \mu)$ induce addition and multiplication on $\mathrm{Groth}(M(\mathbb{F}, \mu))$, making this a ring This is

called the Witt-Grothendieck ring, and is denoted by $\hat{W}(\mathbb{F}, \mu)$ Since $x \oplus 0 = 0 \oplus x$, $(x, x) \simeq (0, 0)$, so that $(x, 0) + (0, x) = (0, 0)$, or $(0, x) = -(x, 0)$ The element $(x, 0)$ is often denoted x

The hyperbolic quadratic form, $\mathbb{H}(x, y) = x^2 - y^2$, is equivalent to the sum of a quadratic form with matrix [1] and a quadratic form with matrix $[-1]$ If $[1] \oplus [-1]$ is made equivalent to 0 by taking the quotient by the ideal generated by $\mathbb{H}$, then $-[1] = [-1]$, and an element (x, y) in $\hat{W}(\mathbb{F}, \mu)$ is equivalent to $(x, 0) + (0, y) = (x, 0) - (y, 0) = x - y$ This brings the equivalence class representatives back into $M(\mathbb{F}, \mu)$ Taking the quotient of $\hat{W}(\mathbb{F}, \mu)$ by the ideal in $\hat{W}(\mathbb{F}, \mu)$ generated by $\mathbb{H}$ gives $\hat{W}(\mathbb{F}, \mu) / < \mathbb{H} >$ This is the **measure Witt ring** of $\mathbb{F}$ and μ, and is denoted $W(\mathbb{F}, \mu)$

In order to find Witt rings, it is useful to use diagonalization Every symmetric matrix is equivalent to some diagonal matrix, that is, if M is symmetric, there is some invertible matrix T such that $T^t M T$ is diagonal There is no guarantee, however, that T will be measure preserving If a matrix is measure equivalent to some diagonal matrix, that matrix is equivalent to a sum of one-dimensional matrices Then, the corresponding quadratic form is equivalent to the sum of one-dimensional quadratic forms Also, the Kroenecker product of diagonal matrices is simple to find

4.5 Examples

Using the zero measure μ_0, every invertible linear transformation is a measure-preserving linear transformation Thus, the measure Witt ring $W(\mathbb{F}, \mu_0)$ will be the same as the canonical Witt ring, symbolized $W(\mathbb{F})$ In the canonical Witt ring, cancellation holds if the characteristic of the field is not 2 See Theorem

1 6 in [6], attributed to Witt Also, the ideal generated by $\mathbb{H}$ is simply $\mathbb{Z}$ $\mathbb{H}$ in the canonical Witt ring

4 5 1 Real, Zero Measure

Lemma: Every one-dimensional real quadratic form is equivalent to a one-dimensional form whose matrix is either $[-1]$, $[1]$, or $[0]$

Proof: Let $[a]$ be the matrix for the one-dimensional form If $a = 0$, then $[a]$ is equivalent to $[0]$ So, suppose $a \neq 0$ Then $[1/\sqrt{|a|}]$ is an invertible linear transformation (its inverse is $[\sqrt{|a|}]$) which is its own transpose So, $[a]$ is equivalent to $[1/\sqrt{|a|}]$ $[a]$ $[1/\sqrt{|a|}] = [a/|a|] = [\text{sign } a]$ □

Since only regular forms are used in the construction of the Witt ring, the $[0]$ term will never appear, if a quadratic form had a $[0]$ term, its resulting matrix would not be invertible So, every regular quadratic form is equivalent to the sum of $[1]$ and $[-1]$ terms Finding the Witt-Grothendieck ring gives additional possible terms of the form $-[1]$ and $-[-1]$ Taking the quotient gives $-[1] = [-1]$ (and $-[-1] = [1]$), so all terms are again of the form $[1]$ and $[-1]$, and $[1] \oplus [-1] = 0$

Everything in $W(\mathbb{R})$, therefore, is the sum of terms of the form $[1]$ and $[-1]$ Any such sum can be reduced to a sum of all $[1]$ terms, or all $[-1]$ terms, or a sum of no terms $W(\mathbb{R})$ is isomorphic to $\mathbb{Z}$, which can be seen by sending the sum of n $[1]$ terms to the integer n, the sum of n $[-1]$ terms to the integer $-n$, and the sum of no terms to zero

4 5 2 Finite Field, Zero Measure

Let $F = \mathbb{F}_q$, the finite field of $q = p^m$ elements, with p odd Let F^* denote the units in F, that is, all non-zero elements of F Half of the elements of F^* are squares

So, we can work in a way similar to the real numbers, in that all forms are (still) diagonalizable, and, by the argument in the lemma, every one-dimensional form is equivalent to a form whose matrix is either $[1]$ or $[s]$, where s is some representative non-square in F^* Again, since the matrix for each form is invertible, no zero terms will appear So, the only possible non-equivalent two-dimensional forms are $[1]\oplus[1]$, $[1]\oplus[s]$, and $[s]\oplus[s]$ There are two possible cases either -1 is a square, or it is not

If -1 is a square (that is, if $p \equiv 1 \pmod 4$), then the form $[-1]$ is equivalent to the form $[1]$ In particular, $[1]\oplus[1] = [1]\oplus[-1] = 0$ and $[s]\oplus[s] = [s]\oplus[-s] = 0$ So, the only possible form with two terms not equivalent to 0 is $[1]\oplus[s]$ If we add any one-dimensional form to this, we get cancellation, and so we can never get a form with three terms The only (non-equivalent) forms in the ring are 0, $[1]$, $[s]$, and $[1]\oplus[s]$ This is ring-isomorphic to the group algebra $\mathbb{Z}_2[\mathbb{Z}_2]$, where here $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$

Suppose -1 is not a square Then $[s]$ is equivalent to $[-1]$, so that

$$[1]\oplus[s] = [1]\oplus[-1] = 0$$

Look at the sets $(F^*)^2$ and $1+(F^*)^2$ These two sets have the same cardinality, and are not equal, since 1 is not in $1+(F^*)^2$ So, there is some element in $1+(F^*)^2$ which is not in $(F^*)^2$ This element cannot be 0, since $0 = 1 + \text{-}1$ is not in $1+(F^*)^2$ Let this non-square element be s, so that s is the sum of two squares, that is, $s = 1+k^2$ for some $k \in F^*$ The following matrix multiplication

$$\begin{bmatrix} 1 & k \\ -k & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & -k \\ k & 1 \end{bmatrix} = \begin{bmatrix} 1 & k \\ -k & 1 \end{bmatrix}\begin{bmatrix} 1 & -k \\ k & 1 \end{bmatrix} = \begin{bmatrix} 1+k^2 & 0 \\ 0 & 1+(-k)^2 \end{bmatrix} = \begin{bmatrix} s & 0 \\ 0 & s \end{bmatrix}$$

says that $[1]\oplus[1]$ is equivalent to $[s]\oplus[s]$ In particular, $[1]\oplus[1]$ is equivalent to $[-1]\oplus[-1]$, or that $[1]\oplus[1]\oplus[1]\oplus[1] = 0$ in the Witt ring Thus, in the Witt ring, at most three $[1]$ terms can be added together $[-1]$ is equivalent to $[1]\oplus[1]\oplus[1]$, so any

$[-1]$ terms can be converted to $[1]$ terms Therefore, the only non-equivalent forms in the Witt ring are 0, $[1]$, $2[1]$, and $3[1]$, which makes the Witt ring isomorphic to the ring $\mathbb{Z}/4\mathbb{Z}$

4 5 3 P-adic, Zero Measure

Let p be an odd prime All quadratic forms are still equivalent to diagonal forms Also, as in the other cases, $[a]$ is equivalent to $[c^2 \quad a]$ for all non-zero c

Every element in $\mathbb{Q}_p$, can be written as $p^m\alpha$, where m is some integer, and α is a p-adic unit Since $[p^2 \quad a]$ is equivalent to $[a]$, every one-dimensional form $[p^m\alpha]$ is equivalent to $[p^\epsilon\alpha]$, where ϵ is either 0 or 1, depending on whether m is even or odd Set up two functions as follows $d_1(\alpha) = a$, $d_1(p\alpha) = 0$, $d_2(\alpha) = 0$, $d_2(p\alpha) = a$, where α is a p-adic unit, and a is the first p-adic 'digit' of α, that is, if $\alpha = \sum_{n=0}^{\infty} a_n p^n$, then $a = a_0$ These d_i are homomorphisms from the equivalence classes of one-dimensional forms on $\mathbb{Q}_p$ to the equivalence classes of one-dimensional forms on $\mathbb{F}_p$ The two functions induce an isomorphism from $W(\mathbb{F}_p) \oplus W(\mathbb{F}_p)$ to $W(\mathbb{Q}_p)$ Therefore, if $p \equiv 1 \mod 4$, then $W(\mathbb{Q}_p)$ is isomorphic to $\mathbb{Z}_2[\mathbb{Z}_2] \oplus \mathbb{Z}_2[\mathbb{Z}_2]$, and if $p \equiv 3 \mod 4$, then $W(\mathbb{Q}_p)$ is isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$

4 5 4 Finite Field, Uniform Measure

The measure Witt ring of finite fields with a uniform measure is easy to find

Theorem: Let $\mathbb{F}$ be a finite field, and μ the uniform probability measure on $\mathbb{F}$, that is, $\mu(\{a\}) = 1/|\mathbb{F}|$ for all $a \in \mathbb{F}$, where $|\mathbb{F}|$ is the cardinality of $\mathbb{F}$ Then $W(\mathbb{F}, \mu) = W(\mathbb{F})$

Proof: In order to determine the measure Witt ring, the invertible measure-preserving linear transformations must be found The measure of a set S in $\mathbb{F}$ is

equal to $|S|/|\mathbb{F}|$, that is, it is based solely on the number of elements in the set S If T is any invertible linear transformation, then T is one-to-one and onto, so that $|A| = |T(A)| = |T^{-1}(A)|$ Therefore, all invertible linear transformations are measure preserving This means the set of equivalent quadratic forms in the measure Witt ring and the canonical Witt ring are the same, and the resulting rings must be the same □

Every uniform measure is proportional to the uniform probability measure, so the same linear transformations are measure preserving Thus, the measure Witt rings will be the same Therefore, for all uniform measures on finite fields, $W(\mathbb{F}, \mu) = W(\mathbb{F})$

4 5 5 Real, Lebesgue Measure

Let μ_L be Lebesgue measure on the real numbers The relationship between (standard) integration and Lebesgue measure is very useful here $\mu_L(A) = \int_A d\vec{x}$ So, in this case, the density function for the measure is just the function $f(\vec{x}) = 1$, and we get that T is measure-preserving if and only if $f(\vec{x}) = 1/|\Delta| f(T^{-1}(\vec{x}))$, or in this case $1 = 1/|\Delta|$ 1, or $|\Delta| = 1$ Thus, any linear transformation whose determinant is ± 1 preserves Lebesgue measure

Or, we can look at Lebesgue measure as a Haar measure In this case, not only do we have that each matrix (representing a linear transformation) is measure-equivalent to a diagonal matrix, but Lebesgue measure has the property that $\mu(c\ A) = |c|\mu(A)$ for c a constant, which lets us multiply one row of the matrix by c, and another by $1/c$, and keep the measure the same By multiplying rows of the diagonal matrix by appropriate values, we can make any matrix measure-equivalent to a diagonal matrix with ones on the diagonal, except for the determinant (modulo

sign) in (say) the first diagonal entry This matrix is only measure preserving if all of the entries are ± 1, that is, if the determinant of the matrix is ± 1

The standard quadratic form theory tells us that, given the matrix M of a quadratic form, there exists some invertible matrix T such that T^tMT is diagonal Define the matrix R to be the same as T, but with the entries in the first row divided by the determinant of T Then R is measure preserving, and R^tMR is also a diagonal matrix Thus, every matrix is still equivalent to the sum of one-dimensional matrices

Lemma: (Lebesgue Cancellation) Let q, q_1, and q_2 be real quadratic forms, with corresponding matrices M, M_1, and M_2, respectively If $q \oplus q_1$ is Lebesgue measure-equivalent to $q \oplus q_2$, then q_1 is measure-equivalent to q_2

Proof: Since $q \oplus q_1$ is equivalent to $q \oplus q_2$, we know that there is some matrix T with determinant ± 1 such that

$$T^t \begin{bmatrix} M & 0 \\ 0 & M_1 \end{bmatrix} T = \begin{bmatrix} M & 0 \\ 0 & M_2 \end{bmatrix}$$

Since T is an invertible matrix, $q \oplus q_1$ and $q \oplus q_2$ are equivalent in the non-measure-preserving case, so there is some matrix S such that $S^tM_1S = M_2$ Thus,

$$\begin{bmatrix} I & 0 \\ 0 & S^t \end{bmatrix} \begin{bmatrix} M & 0 \\ 0 & M_1 \end{bmatrix} \begin{bmatrix} I & 0 \\ 0 & S \end{bmatrix} = \begin{bmatrix} M & 0 \\ 0 & M_2 \end{bmatrix},$$

or

$$T^t \begin{bmatrix} M & 0 \\ 0 & M_1 \end{bmatrix} T = \begin{bmatrix} I & 0 \\ 0 & S^t \end{bmatrix} \begin{bmatrix} M & 0 \\ 0 & M_1 \end{bmatrix} \begin{bmatrix} I & 0 \\ 0 & S \end{bmatrix}$$

Taking determinants of both sides gives

$$(\det T)^2 \det M \det M_1 = (\det S)^2 \det M \det M_1,$$

or $(\det T)^2 = (\det S)^2$ Since $\det T = \pm 1$, $\det S$ must be ± 1, so that S is measure preserving, and q_1 and q_2 are equivalent under the measure $\square$

Theorem: $W(\mathbb{R}, \mu_L) = W(\mathbb{R}) = \mathbb{Z}$

Proof: By the above lemma, cancellation holds, and the semi-ring of equivalence classes can be made into a ring by the Grothendieck construction Then, in order to get the measure Witt ring for the reals and Lebesgue measure, take the quotient of this ring by the ideal generated by the hyperbolic form Since

$$\left[a\right] \otimes \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & -a \end{bmatrix},$$

this ideal contains sums of matrices of the form $[a] \oplus [-a]$ However, in the measure Witt ring, the following computation holds

$$\begin{bmatrix} \frac{1+a}{2a} & \frac{1-a}{2} \\ \frac{1-a}{2a} & \frac{1+a}{2} \end{bmatrix} \begin{bmatrix} a^2 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \frac{1+a}{2a} & \frac{1-a}{2a} \\ \frac{1-a}{2} & \frac{1+a}{2} \end{bmatrix} = \begin{bmatrix} \frac{1+a}{2a} & \frac{1-a}{2} \\ \frac{1-a}{2a} & \frac{1+a}{2} \end{bmatrix} \begin{bmatrix} \frac{a(1+a)}{2} & \frac{a(1-a)}{2} \\ \frac{a-1}{2} & \frac{-(1+a)}{2} \end{bmatrix} =$$

$$\begin{bmatrix} \frac{(1+a)^2}{4} - \frac{(1-a)^2}{4} & \frac{(1+a)(1-a)}{4} - \frac{(1+a)(1-a)}{4} \\ \frac{(1+a)(1-a)}{4} - \frac{(1+a)(1-a)}{4} & \frac{(1-a)^2}{4} - \frac{(1+a)^2}{4} \end{bmatrix} =$$

$$\begin{bmatrix} \frac{1+2a+a^2-(1-2a+a^2)}{4} & 0 \\ 0 & \frac{1-2a+a^2-(1+2a+a^2)}{4} \end{bmatrix} =$$

$$\begin{bmatrix} a & 0 \\ 0 & -a \end{bmatrix}$$

The matrix $\begin{bmatrix} \frac{1+a}{2a} & \frac{1-a}{2a} \\ \frac{1-a}{2} & \frac{1+a}{2} \end{bmatrix}$ has determinant

$$(1+a)^2/4a - (1-a)^2/4a = ((1+2a+a^2) - (1-2a-a^2))/4a = 4a/4a = 1,$$

so it is measure preserving Thus, the matrix $[a^2] \oplus [-1]$ is equivalent to $[a] \oplus [-a]$, which is in the ideal generated by the hyperbolic form Thus, in the measure Witt ring, $[a^2] \oplus [-1] = 0$, or $[a^2] = [1]$ So, all one-dimensional regular quadratic forms are equivalent to $[1]$ or $[-1]$, and the same cancellations occur as in the regular real number case Therefore, the measure Witt ring for Lebesgue measure on the real numbers is the same as the regular Witt ring for the real numbers, or $W(\mathbb{R}, \mu_L) = W(\mathbb{R}) = \mathbb{Z}$ □

4 5 6 Real, Gaussian Measure

Let μ_G be the Gaussian measure on the real numbers There is a relationship between Gaussian measure and Lebesgue measure, namely, that

$$\mu_G(A) = \int_A \mu_G = \int_A (2\pi)^{-n/2} e^{-|\vec{x}|/2} d\mu_L,$$

where n is the dimension of the space, and $|\vec{x}|$ is the standard norm of a vector in real space The distribution function of the measure is $f(\vec{x}) = (2\pi)^{-n/2} e^{-|\vec{x}|/2}$ The linear transformation T is measure preserving if and only if $f(\vec{x}) = f(T^{-1}(\vec{x}))$ for all $\vec{x}$, or, $(2\pi)^{-n/2} e^{-|\vec{x}|/2} = (2\pi)^{-n/2} e^{-|T^{-1}(\vec{x})|/2}$ for all $\vec{x}$, or $|\vec{x}| = |T^{-1}(\vec{x})|$ for all $\vec{x}$ These are exactly the orthogonal matrices, so orthogonal matrices are the measure-preserving matrices for Gaussian measure

If M is a symmetric matrix, then there is some orthogonal matrix T such that $T^t M T$ is diagonal, so all quadratic forms in this setting are equivalent to a

form with a diagonal matrix The entries on the diagonal of this matrix are the eigenvalues of the matrix M with appropriate multiplicity

Let the symbol $\equiv$ stand for 'orthogonal equivalence', that is, matrices $A \equiv B$ if there is some orthogonal matrix T such that $T^tAT = T^{-1}AT = B$ Let quadratic forms $q \equiv r$ if their corresponding matrices are equivalent This is the same as equivalence under standard Gaussian measure In particular, for symmetric matrices, $A \equiv B$ if and only if A and B have the same eigenvalues with the same multiplicity, since they can be diagonalized to the same diagonal matrix

Lemma: (Orthogonal Cancellation) Let q, q_1, and q_2 be real quadratic forms such that $q \oplus q_1 \equiv q \oplus q_2$, where $\equiv$ is the above orthogonal equivalence Then $q_1 \equiv q_2$

Proof: Let M, M_1, and M_2 be the symmetric matrices for the quadratic forms q, q_1, and q_2, respectively These forms are equivalent to diagonal forms d, d_1, and d_2 with corresponding *diagonal* matrices D, D_1, and D_2 The entries in D are the eigenvalues of M, and similarly for D_i and M_i $(i \in \{1,2\})$ $d \oplus d_1 \equiv q \oplus q_1 \equiv q \oplus q_2 \equiv d \oplus d_2$ In terms of matrices, we get that $D \oplus D_1 \equiv D \oplus D_2$, where

$$A \oplus B = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}$$

In particular, $D \oplus D_1$ has the same eigenvalues as $D \oplus D_2$, but the eigenvalues of a diagonal matrix are its diagonal entries, so it must be that D_1 and D_2 have the same eigenvalues By the following proposition, $D_1 \equiv D_2$, which means $d_1 \equiv d_2$, or $q_1 \equiv q_2$ $\square$

Proposition: Two diagonal matrices are orthogonally equivalent if and only if their diagonal entries are the same, including multiplicity

Proof: The diagonal entries in a diagonal matrix are the eigenvalues of the matrix If the eigenvalues of two matrices are different, then the matrices cannot

be equivalent So, in order for two diagonal matrices to be equivalent, their entries must be the same, including multiplicity

Given a diagonal matrix, its entries can be rearranged freely using orthogonal matrices, as follows let D be a diagonal n by n matrix Let e_i be the ith standard basis element for the real numbers, that is, the vector with a one in the ith position, and zeros in all other positions Let σ be the permutation of the entries in the diagonal matrix that is desired, that is, if the first entry in D is to become the fourth, then let $\sigma(1) = 4$ Construct the orthogonal matrix T where the ith row of T is $e_{\sigma^{-1}(i)}$ The resulting matrix $T^t DT$ will be the diagonal matrix appropriately arranged So, if two matrices have the same entries, including multiplicity, then the matrices are equivalent □

Theorem: $W(\mathbb{R}, \mu_G)$ is isomorphic to the group ring $\mathbb{Z}[\mathbb{R}^+]$, where $\mathbb{R}^+$ is the multiplicative group of positive real numbers

Proof: From what has already been done, all matrices are equivalent to diagonal matrices, and cancellation applies The Grothendieck construction can again be used to form a ring The only other equivalences obtained in the construction of the measure Witt ring are those found by setting all multiples of the hyperbolic form to zero This allows additive inverses to cancel, that is, $[x] \oplus [-x] = 0$, or $[-x] = -[x]$, for all real numbers x Treating diagonal matrices as sums of one-dimensional matrices, each non-zero element of the measure Witt ring can be written as

$$\sum_{n=1}^{m} \epsilon_n [r_n],$$

where $r_n \in \mathbb{R}^+$ and ϵ_n is ± 1, and m is some positive integer The only sums equivalent to a given sum are those found by commuting the elements (due to the proposition), and cancelling additive inverses (by the measure Witt ring construc-

tion) Thus, every element can be written as

$$\sum_{n=1}^{j} k_n[r_n],$$

where $k_n \in \mathbb{Z}$ is the number of instances of $[r_n]$ in the original sum, minus the number of instances of $-[r_n]$, and j is the appropriate integer Each of these is unique, that is, two of these sums are equivalent if and only if one is a reordering of the terms of another So, as a set, $W(\mathbb{R}, \mu_G)$ can be written as the set of all formal sums as above, with $k_n \in \mathbb{Z}$ and $r_n \in \mathbb{R}^+$ This set is the same as the set of elements in the group ring $\mathbb{Z}[\mathbb{R}^+]$

Addition of two of these formal sums is componentwise, that is,

$$k_1[r] + k_2[r] + k_3[s] = (k_1 + k_2)[r] + k_3[s],$$

which matches the addition in the group ring

Multiplication in $W(\mathbb{R}, \mu_G)$ comes from the tensor product, where $[r] \otimes [s] = [rs]$ and $([r] + [s]) \otimes [t] = [rt] + [st]$ This gives

$$m[r] \otimes n[s] = \sum_{i=1}^{m} [r] \otimes \sum_{j=1}^{n} [s] = \sum_{i=1}^{m} \sum_{j=1}^{n} [rs] = (mn)[rs]$$

which matches the multiplication in the group ring

Therefore, $W(\mathbb{R}, \mu_G)$ is isomorphic to the group ring $\mathbb{Z}[\mathbb{R}^+]$ □

4 5 7 Real, Uniform Measure on $[-1, 1]$

With this measure, the linear transformation $T \quad \mathbb{R}^n \to \mathbb{R}^n$ is measure preserving if and only if $f(\vec{x}) = 1/|\Delta| f(T^{-1}(\vec{x}))$ for all vectors $\vec{x}$, where Δ is the determinant of T, and f is the function which is 1 on the square $[-1, 1]^n$ and 0 everywhere else If $\vec{x}$ is sufficiently small, then both $\vec{x}$ and $T^{-1}(\vec{x})$ are in the $[-1, 1]$ square, so that $|\Delta|$ must be 1 Thus, for T to be measure preserving, $f(\vec{x}) = f(T^{-1}(\vec{x}))$ must

be true for all $\vec{x}$ In other words, every vector in the square must stay in the square, and every vector outside the square must stay outside the square

The only invertible linear transformations which fit these criteria are the symmetries of the square In particular, in $\mathbb{R}^2$, there are only eight such linear transformations Checking all of these linear transformations against the quadratic form with matrix $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ shows that the above quadratic form is not diagonalizable The above quadratic form was not chosen with any special property, most quadratic forms won't be diagonalizable This makes the resulting measure Witt ring very difficult to find

4 5 8 P-adic, Haar Measure

Let μ_H be the measure previously used on the p-adic numbers, that is, the Haar measure with $\mu_H(\mathbb{Z}_p) = 1$ Following the same procedure as in the real Lebesgue case, every quadratic form is equivalent to a diagonal form However, the measure on the p-adic numbers has the property that $\mu_H(\alpha A) = \mu_H(A)$ if α is a p-adic unit Also, $\mu_H(p^n A) = p^{-n}\mu_H(A)$ So, if $c = p^n\gamma$ is a non-zero p-adic number, where γ is a unit and n is the appropriate power of p, then $\mu_H(cA)$ $\mu_H(c^{-1}B) = \mu_H(p^n\gamma A)$ $\mu_H(p^{-n}\gamma^{-1}B) = p^{-n}\mu_H(A)$ $p^n\mu_H(B) = \mu_H(A)$ $\mu_H(B)$ In other words, multiplying by $[c] \oplus [c^{-1}]$ is measure preserving Thus, every diagonal matrix is measure-equivalent to a matrix with all ones on the diagonal, except for the determinant of the matrix in the first entry Thus, if multiplication by the determinant is measure-preserving, then the entire matrix is measure-preserving In particular, if the determinant is a p-adic integer unit, then the matrix is measure-preserving

Theorem: $W(\mathbb{Q}_p, \mu_H) = W(\mathbb{Q}_p)$

Proof: The matrix used in the real Lebesgue case is still measure preserving, since it has determinant 1, and the same argument used there can be used here to get that, in this measure Witt ring, $[a^2] = [1]$ This is the same property that the canonical p-adic Witt ring has, so this measure Witt ring is constructed in the same way as the canonical p-adic Witt ring Therefore, the measure Witt ring for the p-adic numbers and the Haar measure is the same as that for the canonical Witt ring, or $W(\mathbb{Q}_p, \mu_H) = W(\mathbb{Q}_p)$ □

In both the case of the real numbers with Lebesgue measure, and the p-adic numbers with Haar measure, the measure Witt ring is the same as the canonical Witt ring In these measure Witt rings $[a^2]$ is equivalent to $[1]$, so it has the same structure as the canonical Witt ring That equivalence came from $\mu(A \times B) = \mu(cA \times c^{-1}B)$, and that all matrices of quadratic forms were equivalent to diagonal matrices If these hold true for some measure on some field, then that measure Witt ring will be the same as the canonical Witt ring for that field In particular, for Haar measure, the diagonalization property already holds This gives the following theorem

Theorem: If a field $\mathbb{F}$ has a Haar measure μ such that

$$\mu(A \times B) = \mu(cA \times c^{-1}B)$$

for all measurable sets A and B in $\mathbb{F}$, and $c \in \mathbb{F}$, then $W(\mathbb{F}, \mu) = W(\mathbb{F})$

4.6 Abstract Witt Rings

According to [6, p 30], for an abelian group G with exponent 2, "[a] *Witt ring for* G is a ring $R \neq 0$ together with an isomorphism $\mathbb{Z}[G]/K \to R$, where the ideal K fulfils the following condition

$$\chi(K) = 0 \text{ or } \chi(K) = 2^{n(\chi)}\mathbb{Z} \text{ with } n(\chi) \geq 0$$

for every character χ of G All these rings R are called *abstract Witt rings*"

In most of the examples computed above, the measure Witt ring is identical to the canonical Witt ring, and therefore is an abstract Witt ring In the case of $W(\mathbb{R}, \mu_G)$, the measure Witt ring is not an abstract Witt ring, but it has the form of one if you allow $G = \mathbb{R}^+$ and $K = 0$ The case of the uniform measure on the interval [-1,1] in the reals was too complicated to find, it is unclear whether or not it is an abstract Witt ring However, due to the gaussian case, not all measure Witt rings are abstract Witt rings by the above definition

4.7 Measure Witt Rings and Probability

Unfortunately, the measure Witt ring, by itself, doesn't completely determine when the probability of two random quadratic polynomials having two roots will be the same for two different fields and measures While the measure Witt rings $W(\mathbb{Q}_p, \mu)$ and $W(\mathbb{Q}_q, \nu)$ were the same with μ and ν the respective Haar measures, and with p and q equivalent modulo 4, they are not the same if the two primes are different modulo 4 Thus, even if two isomorphic measure Witt rings implied that the corresponding probabilites would be the same, it wouldn't explain why the probabilities are the same when the primes are different modulo 4 Something else is necessary to link all of the p-adic fields together

5. Conclusion

5.1 What Has Been Done

The concept of a measure Witt ring has been defined It gives a connection between the quadratic forms of a field and a measure on that field It has been determined that the canonical Witt ring and this measure Witt ring are the same for several fields with translation-invariant measure For Haar measure, if inverse elements affect the measure appropriately (that is, if $\mu(A \times B) = \mu(cA \times c^{-1}B)$), then the two rings will always be the same

It has also been shown that the measure Witt ring is not always the same as the canonical Witt ring, the measure Witt ring of the real numbers with the standard Gaussian distribution is an example of that The probability of certain events regarding quadratic forms does not determine the measure Witt ring, two events can have the same probability, but the measure Witt rings may be different, as was seen in the p-adic case

With regard to the probability of an n-degree polynomial having k distinct roots, some answers have been found For real numbers and Lebesgue measure, with $n < 4$, these probabilities can be found by integrating, perhaps numerically The integral for $n = 3$ is difficult to resolve, it is perhaps easier to use Monte Carlo methods to determine the probability Using this method P_3^3 has been estimated at 0 2178, and since real cubic polynomials must have at least one root, this gives $P_3^1 \approx 0\ 7822$ With Gaussian measure, using the Kac formula and the fact that all cubic reals have at least one root gives $P_3^3 \approx 0\ 246380$ and $P_3^1 \approx 0\ 753620$

For $n = 4$, the integral method is even more difficult, as another condition (other than sign of the determinant) is needed to distinguish a polynomial with 4 roots from one with 0 roots This has been attempted, with different random

variables for coefficients, in [9], which uses monic polynomials and non-uniform distributions for the coefficients Since polynomials with degree greater than 4 are not solvable algebraically, this method cannot be extended to higher degrees

In the p-adic numbers, numerical evidence suggests that a similarly simple probability holds true for polynomials For each of the primes 3, 5, and 7, 24,000 cubic p-adic polynomials were generated, where the coefficients were uniformly distributed in $\mathbb{Z}/n\mathbb{Z}$, with $n = p^{10}$ The number of roots of each polynomial was found Below is a table with the results

p	0 roots	1 root	2 roots	3 roots
3	6539	14120	9	3332
5	6869	13660	0	3471
7	7136	13249	0	3615

These results suggest that the probability a random cubic polynomial has no roots is 1/3, the probability that it has one root is 1/2, the probability that it has two roots is zero, and the probability it has 3 roots is 1/6 This is the same as the proportion of a permutation in S_3 has zero, one, two, or three fixed points, respectively

It may be that, as p get larger, these probabilities approach the exact rational values, but are not exactly equal to them However, the rational value of the quadratic case, and the result giving 3-adic cubics with two roots (which happens with probability zero), suggests that imprecision in the numerical method can also explain the difference between the numeric results and the conjecture, so that the values are exact Extending this conjecture to higher-degree polynomials gives

Conjecture: The probability that a degree d random polynomial with uniformly-distributed p-adic integer coefficients has k roots is the same as the probability that a random d-permutation has k fixed points

5.2 Future Work

More work needs to be done on the relationships between measure Witt rings If two measure Witt rings are isomorphic, there should be some sort of relationship between the measures While it isn't true that equal probabilities implies isomorphic measure Witt rings, the converse may be true It may be that if $W(F_1, \mu)$ and $W(F_2, \nu)$ are isomorphic, then appropriate probabilities are equal Or, certain properties of the measures may be the same Comparing two measure Witts rings generated using the same field but different measures may be more likely to lead to these results

Similar to the above, it may be true that a measure μ has a certain property if the measure Witt ring has some appropriate ring property That way, information about the measure may be found by examining the measure Witt ring For instance, one theorem which may come out of this work is the following if the measure Witt ring is isomorphic to the canonical Witt ring, then the measure is translation-invariant This seems likely, and is supported by the examples computed so far

Another question to be examined is whether or not the measure Witt ring with Haar measure is always equivalent to the canonical Witt ring This depends on what happens with the measure under 'multiplication by inverse elements' that is, it requires that $\mu(cA \times c^{-1}B) = \mu(A \times B)$ for all non-zero c in the field It seems somewhat unlikely that this holds for all fields with Haar measure, but which fields have this property is a question which should be explored

The work on measure Witt rings led to a study of measure-preserving linear transformations In writing this thesis, very few references were found regarding the general question of which linear transformations perserved which measures This is another field of study which I feel requires more attention

Regarding the question of the probability that a random polynomial has a certain number of roots, no general answer was found The simple answer found for p-adic quadratic polynomials, and the simple answer suggested by numerical methods for higher degree polynomals, suggests that there is a simpler proof than what was used here

Work on the probability question was done for two measures on the real numbers, but the answers found only went up to degree 3, and the method could only be used for low-degree polynomials Some way to find more exact probabilities may be able to be found for higher degree polynomials In particular, it may be possible to use the method outlined at the beginning of [4] to find not only the expected number of real zeroes of a real random polynomial, but the exact probabilities for the different number of roots as well

As was commented on before, not all of the measure Witt rings found were abstract Witt rings However, all had the same general form as an abstract Witt ring The definition of the measure Witt ring can be extended to include any equivalence class of linear transformations, not only the equivalence class of measure-preserving linear transformations Probably all these "Witt rings" are of the same general form as abstract Witt rings, and that should be explored Also, it should be determined whether all abstract Witt rings can be obtained using measure Witt rings

Only the real numbers and the p-adic numbers were studied in this thesis Other fields, and other measures on the given fields, deserve more study Also, as

more probabilities over more fields and measures are found, a clearer picture of the general problem may develop, and a more general theory may be found

BIBLIOGRAPHY

[1] Charalambos Alıprantıs and Owen Burkınshaw, *Prıncıples of Real Analysıs*, Academıc Press, Inc , San Dıego, CA 1990

[2] Jacek Bochnak, Mıchel Coste, and Marıe-Françoıse Roy, *Real Algebraıc Geometry*, Sprınger-Verlag, Berlın 1998

[3] Davıd S Dummıt and Rıchard M Foote, *Abstract Algebra*, Prentıce Hall, Englewood Clıffs, NJ 1991

[4] Alan Edelman and Erıc Kostlan, "How many zeros of a random polynomıal are real?", *Bulletın (New Serıes) of the Amerıcan Mathematıcal Socıety*, vol 32, no 1, pp 1–37, January 1995

[5] Paul R Halmos, *Measure Theory*, Sprınger-Verlag Graduate Texts ın Mathematıcs 18, New York, NY, 1974

[6] Manfred Knebusch and Manfred Kolster, "Wıttrınge", *Der Regensburger Trıchter*, vol 14, 1971-1972

[7] Neal Koblıtz, *p-adıc Numbers, p-adıc Analysıs, and Zeta-Functıons*, Second Edıtıon, Sprınger-Verlag Graduate Texts ın Mathematıcs 58, New York, NY, 1984

[8] T Y Lam, *The Algebraıc Theory of Quadratıc Forms*, W A Benjamın, Inc , Readıng, MS, 1973

[9] Hung C Lı, "The exact probabılıty that the roots of quadratıc, cubıc, and quartıc equatıons are all real ıf the equatıon coefficıents are random", *Communıcatıons ın Statıstıcs Theory and Methods*, vol 17, no 2, pp 395-409, 1988

[10] Walter Rudın, *Prıncıples of Mathematıcal Analysıs*, McGraw-Hıll, Inc , New York, NY, 1976