Presentation Speech Draft

Shubin Xue

Good [morning/afternoon/evening], everyone. I am Shubin Xue from Beijing Institute of Technology. Today, It's my pleasure to present my talk on Classification of Quadratic Forms over $\mathbb{Q}$.

My presentation will be divided into two main parts:

First, I will discuss the primary motivations and standard approaches to this problem.

Second, I will show the classification of quadratic forms over the field $\mathbb{Q}$.

The third part is an appendix about the proof of the Hasse-Minkowski theorem.

Before we begin, let me outline some notation:

- K will denote an arbitrary field.
- X, Y, Z are used as variables.
- $\left(\frac{a}{p}\right)$ is the Legendre symbol.
- We will often denote by the same letter an element and its class modulo.

Now, let us begin with the first part.

What is a quadratic form? What is a quadratic space?

Let V be a vector space over a field K. A function $Q : V \to K$ is called a quadratic form if it satisfies the following two conditions.

$Q(\lambda v) = \lambda^2 Q(v)$, $B_Q(u, v)$ is a symmetric bilinear form on V.

A quadratic space is such a pair (V, Q).

Define the scalar product $x \cdot y$ as half of $B_Q(x, y)$, noting that $Q(x) = x \cdot x$.

Given a basis of V, the quadratic form Q corresponds to a matrix A. An element x in this basis, we can directly compute $Q(x)$.

This shows that $Q(x)$ is a quadratic form in the usual sense.

Let us consider a simpler quadratic form: the sum of $X_i X_j$. And the pair (K^n, f) is a quadratic space.

If f is a quadratic form in n variables and g is a quadratic form in m variables, we denote by $f \oplus g$ the quadratic form in $n + m$ variables given by their direct sum.

When we change the basis of the space V, the corresponding matrix A transforms as $A' = PAP^T$.

We know that two quadratic forms are equivalent if and only if their matrices are congruent (denoted as $f \sim g$), and any symmetric matrix can be diagonalized by a congruence transformation. This means we have reduced the discussion to

$$\sum_{i=1}^{n} a_i X_i^2$$

We also note that $\det(A) = \det(PAP^T)$, which means that $\det A$ is an invariant in the quotient group modulo squares, called the discriminant. Denoted by $d(Q)$ or d.

Next, let us review the classification of quadratic forms over $\mathbb{R}$ and $\mathbb{F}_q$:

Sylvester's Law of Inertia tells us that any non-degenerate quadratic form over $\mathbb{R}$ can be diagonalized by a congruence transformation and reduced to a form where all diagonal entries are ± 1. Therefore, quadratic forms over $\mathbb{R}$ are completely classified by their rank and signature. Both rank and signature are invariants.

We can observe some general ideas:

First, the rank is always an invariant, so our classification can be reduced to non-degenerate quadratic forms of rank n.

Second, two quadratic forms are equivalent if their coefficients differ by a square element.

This tells us that it suffices to understand how the elements of $K^\times/(K^\times)^2$ are distributed along the diagonal to classify quadratic forms.

Here are some examples for common fields:

- For $\mathbb{C}$, every element is a square, so classification is determined by rank alone.
- For $\mathbb{R}$, $\mathbb{R}^\times/(\mathbb{R}^\times)^2 = \{\pm 1\}$, so we need to consider the signature.
- For $\mathbb{F}_q$, $\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^2 = \{1, a\}$, where a is a non-square.

From the above discussion, we have seen that the diagonal elements provide a **coarse** classification, but unfortunately, this is not a complete classification.

Consider a rank 2 non-degenerate quadratic form over $\mathbb{F}_q$ where a is a non-square, we have $f_1 = aX^2 + aY^2 \sim f_2 = X^2 + Y^2$.

Do a change of basis: $X = sX' + tY'$ and $Y = tX' - sY'$. If we require $aX'^2 + aY'^2 = X^2 + Y^2$, then $s^2 + t^2 = a$.

Note that s^2 and $a - t^2$ each have $(q+1)/2$ possible values, totaling $q+1$ values, but the finite field has only q elements. By the pigeonhole principle, the equation has a nontrivial solution.

Fortunately, their discriminant can serve as an invariant for classifying quadratic forms.

Just now, we dealt with the question of whether a certain quadratic equation has a solution, and this inspires us to make some generalizations:

We define the Hilbert symbol of a and b as follows: if the equation has a nontrivial solution, the symbol is 1; otherwise, it is -1. It is not hard to see that if you change a or b by multiplying by a square, the value of the Hilbert symbol does not change. Thus, you can think of it as a map on $K^\times/(K^\times)^2$.

From now on, let's always assume $K = \mathbb{Q}_p$. Let's take a look at the Hilbert symbol over the p-adic field $\mathbb{Q}_p$.

I will just give the explicit algorithm for the Hilbert symbol here, the details are tedious and not interesting, but what you should notice from this formula is that the Hilbert symbol is a symmetric, non-degenerate bilinear form.

Let $\mathbb{V}$ be the set of all primes together with ∞, and let $Q_\infty = \mathbb{R}$. $(a, b)_v$ denotes the Hilbert symbol of their images in Q_v for all $v \in \mathbb{V}$.

Without going into details, there's a multiplication formula: for any a and b, the Hilbert symbol $(a, b)_v$ equals 1 for all but finitely many v, and the product over all v is 1.

The Hilbert symbol already works for rank 2, so now we need to generalize it to higher rank cases: let $\varepsilon(f)$ be the product of the Hilbert symbols of the diagonal entries; this is called the Hasse invariant of f.

Let's summarize what we have so far:

We have reduced the problem to non-degenerate diagonal quadratic forms of rank n, and we have the discriminant $d(f)$ and the Hasse invariant $\varepsilon(f)$.

For the induction proof coming up, it's helpful to work out how these invariants change when we remove a variable:

Suppose $f = a_1X_1^2 \oplus f_1$, $d(f)$ is the product of the a_i. You can factor it as a_1 times $(a_2 \cdots a_n)$, so that's just a_1 times $d(f_1)$.The Hasse invariant $\varepsilon(f)$ is the product of all Hilbert symbols (a_i, a_j). By the bilinearity of the Hilbert symbol, this simplifies to $\varepsilon(f_1) \cdot (a_1, a_1 d(f_1))$.

So, under what conditions can we split a quadratic form into a direct sum of two quadratic forms? The set of numbers represented by the quadratic form will be the key to this question.

If there exists a nonzero element $v \in V$ such that $f(v) = a$, we say that f represents a.

For an element a in K, f represents a if and only if - $f \sim g \oplus aZ^2$ - $f \oplus -aZ^2$ represents 0.

Item 3 means that to check whether a can be represented by f, it suffices to consider whether $f \oplus -aZ^2$ can represent 0.

Item 2 means that if f can represent a, we can decompose f as $aZ^2 \oplus g$, where g has rank one less than f.

In other words, item 2 allows us to successfully reduce the problem of decomposing a quadratic form to the problem of when a quadratic form represents a, while item 3 tells us that the question of whether a quadratic form represents a can be reduced to whether it represents 0.

This involves a lot of tedious casework, so we will omit all details due to time constraints.

f represents 0 if and only if:

For rank 2, $d = -1$.

For rank 3, the Hilbert symbol of -1 and $-d$ equals the Hasse invariant.

For rank 4, either $d \neq -1$, or $d = 1$ and the Hasse invariant is the Hilbert symbol of -1 and -1.

For rank ≥ 5, it always holds.

Applying this theorem to $f_a = f \oplus -aZ^2$, we can directly obtain the condition for f to represent a, which will not be repeated here. However, you should notice that the representation numbers of a quadratic form are completely determined by its rank, discriminant, and Hasse invariant.

At the end of the first part, let me mention some results here without going into details.

Witt's theorem tells us that an injective metric-preserving map from a subspace of a quadratic space to another quadratic space can be extended to an metric-preserving map of the whole space.

If we consider two isomorphic subspaces U and W of the same quadratic space V, Witt's theorem allows us to extend the isomorphism to an automorphism of V. By restricting this automorphism to the orthogonal complement, we obtain an isomorphism on the complement.

Therefore, we have Witt's cancellation theorem: if two quadratic forms are equivalent and one direct summand is equivalent, then the other direct summand is also equivalent.

Next, let's move on to the second part: quadratic forms over $\mathbb{Q}_p$ and $\mathbb{Q}$.

Let's start with the discussion over $\mathbb{Q}_p$.

Non-degenerate quadratic forms of rank n over $\mathbb{Q}_p$ are completely classified by their Hasse invariant and discriminant.

If f and g have the same discriminant d and ε, then they can both represent some a. Thus, f can be decomposed as $f_1 \oplus aZ^2$, and similarly for g.

A direct calculation shows that f_1 and g_1 have the same invariants. By induction on the rank, $f_1 \sim g_1$, so $f \sim g$.

However, the invariants d and ε cannot be chosen arbitrarily; they must satisfy certain constraints. At the same time, we can also prove that for any invariants satisfying these constraints, there always exists a quadratic form with those invariants.

For $n = 1$, it's clear that the Hilbert symbol must be 1, while d is unrestricted.

For $n = 2$, by the properties of the Hilbert symbol, if $d = -1$ then ε must be 1. In both cases, we can construct $f = aX^2 + adY^2$ to match the invariants.

For $n = 3$, we can always first choose any $a \neq d$, then by the $n = 2$ case above, construct g with $d(g) = ad$, $\varepsilon(g) = \varepsilon(a, -d)$. Then $f = g \oplus aZ^2$ works.

For $n > 3$, simply take $g(X_1, X_2, X_3)$ satisfying the conditions, and then add X_i^2 terms as needed.

Finally, let us address the core question of today: the classification of quadratic forms over $\mathbb{Q}$.

The Hasse-Minkowski theorem tells us that a quadratic form f represents 0 over $\mathbb{Q}$ if and only if it represents 0 over $\mathbb{R}$ and over all $\mathbb{Q}_p$.

The Hasse-Minkowski theorem is essential for today's topic, so I have included its proof in the appendix as the third part. If you are interested, feel free to discuss it with me after the presentation.

With the help of the Hasse-Minkowski theorem, we can completely classify quadratic forms over $\mathbb{Q}$.

Non-degenerate quadratic forms of rank n over $\mathbb{Q}$ are equivalent if and only if they are equivalent over all completions $\mathbb{Q}_v$.

Necessity of this result is clear, so we only need to consider sufficiency.

If f and g are equivalent over all $\mathbb{Q}_v$, then by the Hasse-Minkowski theorem, there exists an a that can be represented over $\mathbb{Q}$. Thus, we can decompose $f \sim f_1 \oplus aZ^2$ and $g \sim g_1 \oplus aZ^2$. We have $f \sim g$ over all $\mathbb{Q}_v$, and clearly $aZ^2 \sim aZ^2$. By Witt's cancellation theorem, we know that $f_1 \sim g_1$ over all $\mathbb{Q}_v$. By induction, $f_1 \sim g_1$ over $\mathbb{Q}$. Hence, $f \sim g$ over $\mathbb{Q}$.

Of course, the selection of invariants here will be subject to even greater restrictions, including both local and global constraints.

First, the Hilbert symbol must satisfy the global property: the product formula.

Second, the invariants must satisfy the restrictions we discussed for $\mathbb{Q}_p$.

Finally, the invariants must satisfy the restrictions over $\mathbb{R}$: signature, d_∞, and ε_∞.

I think I'll stop here. This completes the classification of quadratic forms over $\mathbb{Q}$. Thank you.