Minimal Rank of Primitively n-Universal Quadratic Forms over Local Fields

Jongheun Yoon
(Joint work with Prof. Byeong-Kweon Oh)

Charles University

Squares in Dortmund, Mar 31 2025

Outline

Introduction

Lower bound for $U_R^*(n)$

Upper bound of $U_R^*(n)$

Classical case

Quadratic forms

Let F be a nonarchimedean local field at the place $\mathfrak{p}$ and let R be the ring of integers in F. We generally assume that $\mathrm{ch}\, F \neq 2$.

- For a positive integer n, a **quadratic form** of rank n is a quadratic homogeneous polynomial

$$f(\mathbf{x}) = f(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} f_{ij} x_i x_j \qquad (f_{ij} = f_{ji} \in F).$$

- To every quadratic form f of rank n, there corresponds a unique symmetric matrix $M_f = (f_{ij}) \in \mathrm{Sym}_n(F)$, called the **(Gram) matrix** of f.
- We call a quadratic form f **nondegenerate** if M_f is nondegenerate.
- We call a quadratic form f **diagonal** if M_f is diagonal.

Integral quadratic forms

Let f be a quadratic form.

- We call f **integral** if f is a polynomial over R.
- We call f **classical** if M_f is a matrix over R.
- Clearly, a classical form is integral.

  The converse is also true if R is nondyadic.
- If R is dyadic, then there exists an integral quadratic form that is not classical, for instance, $f(x, y) = xy$.
- In this talk, we always assume that a quadratic form is nondegenerate and integral, unless stated otherwise.

Representability and universality

Let f and g be (integral) quadratic forms of rank n and m, respectively.

- We say f is **represented** by g if there is a matrix $T \in \mathrm{Mat}_{m,n}(R)$ such that

$$M_f = T^t M_g T.$$

- We say f is **isometric** to g if the above matrix T is invertible (unimodular).
- A (classical) quadratic form g is called n-**universal** if every (classical, respectively) quadratic form of rank n is represented by g.

n-Universal quadratic forms

- In 2023, He, He–Hu, and He–Hu–Xu provided criteria to determine whether a given quadratic form is n-universal.
- Let $U_R(n)$ ($cU_R(n)$) be the minimal rank of n-universal (classical, respectively) quadratic forms over R.

We have $U_R(n) = \begin{cases} 2n & \text{if } 1 \leq n \leq 3, \\ n+3 & \text{if } n \geq 3. \end{cases}$

If R is dyadic, then $cU_R(n) = \begin{cases} 2n+1 & \text{if } 1 \leq n \leq 2, \\ n+3 & \text{if } n \geq 2. \end{cases}$

n-Universality criterion from n-representability

- If a quadratic form f is represented by another form g, then every subform of f is also represented by g.
- There are finitely many quadratic forms of rank n that are "maximal" with respect to a subform relation.
- There are effective criteria to determine whether a given quadratic form is represented by another form.
- Therefore, criteria of n-universality are virtually equivalent to a logical product of criteria of representability for finitely many "maximal" quadratic forms of rank n.

Primitive matrices and primitive vectors

Let m, n be positive integers such that $m \geq n$.

- A matrix $T \in \mathrm{Mat}_{m,n}(R)$ is called **primitive** if it satisfies the following equivalent conditions:
  - (i) We can extend T to an invertible matrix in $GL_m(R)$ by adding suitable $(m-n)$ columns;
  - (ii) There exists a submatrix of T consisting of n rows that is invertible matrix in $GL_n(R)$.
- In particular, a vector $\mathbf{a} = (a_1, \ldots, a_n)$ in R^n is primitive iff (i) there is a basis for R^n containing $\mathbf{a}$, or equivalently, iff (ii) some a_i is a unit in $R^\times$.

Primitive representability and primitive universality

Let m, n be positive integers such that $m \geq n$. Let f and g be quadratic forms of rank n and m, respectively.

- We say that f is **primitively represented** by g if there is a primitive matrix $T \in \mathrm{Mat}_{m,n}(R)$ such that

$$M_f = T^t M_g T.$$

- A (classical) quadratic form g is called **primitively n-universal** if every (classical, respectively) quadratic form of rank n is primitively represented by g.
- Let $U_R^*(n)$ ($cU_R^*(n)$) be the minimal rank of primitively n-universal (classical, respectively) quadratic forms over R.

Previous results

- James(1993) provided criteria to determine whether a quadratic form is primitively represented by another **unimodular** form.
- Budarina(2010) and Earnest–Gunawardana(2021) provided criteria of primitive 1-universality.
- Budarina(2011) provided criteria of primitive 2-universality, for quadratic forms with odd squarefree determinant.

Remark. There are no known general criteria to determine whether a given form is primitively represented by another form (even locally).

Main question

Let us abbreviate the phrase “primitively n-universal” as PnU.

1. Can we determine the minimal rank $U_R^*(n)$ of PnU quadratic forms?
2. Can we enumerate all PnU quadratic forms of rank $U_R^*(n)$?

Outline

Introduction

Lower bound for $U_R^*(n)$

Upper bound of $U_R^*(n)$

Classical case

PnU implies Witt index $\geq n$

Let g be a quadratic form.

We do not assume that a quadratic form is nondegenerate in this section.

- The **discriminant** dg of g is the square class $(\det M_g)(R^\times)^2$.
- We say that a nondegenerate quadratic form g has **(Witt) index** $\geq n$ if and only if g is isometric over F to a quadratic form with the matrix

$$\left(\begin{array}{c|c} O_n & * \\ \hline * & * \end{array}\right).$$

Clearly, this implies that g has rank $\geq 2n$.

Lemma 1

If g is nondegenerate and primitively n-universal, then g has index $\geq n$.

Representability modulo an ideal

Let m, n be positive integers such that $m \geq n$. Let f and g be quadratic forms of rank n and m, respectively. Let I be an ideal in R.

- We say that f is **(primitively) represented modulo** I by g if there is a (primitive, respectively) matrix $T \in \mathrm{Mat}_{m,n}(R)$ such that

$$M_f - T^t M_g T \in \mathrm{Sym}_n(I).$$

- We say that f is **isometric modulo** I by g if the above matrix T is invertible.

Primitive representability is determined modulo an ideal

Let g be a nondegenerate quadratic form of rank m.

Lemma 2

Let f be a quadratic form of rank n. Let $I = 4\mathfrak{p}(dg)^2R$. If f is primitively represented modulo I by g, then f is primitively represented by g.

(Sketch of proof) The problem of primitive representability of f by g is equivalent to solving a system of $\dfrac{n(n+1)}{2}$ quadratic equations in mn variables. Apply a multivariable version of Hensel's lemma to approximate a solution modulo I to a correct solution.

Proof of Lemma 1

(Proof) Let f be a quadratic form with the matrix O_n and let f' be a nondegenerate quadratic form with the matrix

$$M_{f'} \in \mathrm{Sym}_n(4\mathfrak{p}(dg)^2 R).$$

Since g is PnU, f' is primitively represented by g. This means that f is represented by g modulo $4\mathfrak{p}(dg)^2 R$. Now apply Lemma 2 to f and g to obtain the conclusion.

Consequences of Lemmas

- A primitively n-universal quadratic form has rank $\geq 2n$. Hence,

$$U_p^*(n) \geq 2n.$$

- We may determine in **finite steps** whether a given quadratic form is primitively n-universal, for we only have to check primitive representability modulo some ideal of finitely many quadratic forms of rank n chosen modulo some ideal.

Outline

Introduction

Lower bound for $U_R^*(n)$

Upper bound of $U_R^*(n)$

Classical case

$U_R^*(n) = 2n$ for nondyadic R

- Let $\hat{\mathbb{H}}$ denote the quadratic form $\hat{\mathbb{H}} = \hat{\mathbb{H}}(x, y) = xy$.
- Clearly, every integer is primitively represented by $\hat{\mathbb{H}}$.
- Let R be nondyadic. Then, every quadratic form can be diagonalized.
- Hence, every lattice of rank n is primitively represented by $\hat{\mathbb{H}}^n = \underbrace{\hat{\mathbb{H}} \perp \cdots \perp \hat{\mathbb{H}}}_{n \text{ times}} = x_1 y_1 + \cdots + x_n y_n$.

$U_R^*(n) = 2n$ for dyadic R

- Let R be dyadic. Then, every quadratic form is isometric to a certain "block diagonal" form, which is an orthogonal sum of quadratic forms of rank at most 2.
- Every quadratic form of rank 2 is primitively represented by $\hat{\mathbb{H}} \perp \hat{\mathbb{H}}$, for

$$\begin{pmatrix} \alpha & \frac{1}{2}\beta \\ \frac{1}{2}\beta & \gamma \end{pmatrix} = \begin{pmatrix} 1 & \alpha & & \\ & \beta & 1 & \gamma \end{pmatrix} \begin{pmatrix} 0 & \frac{1}{2} & & \\ \frac{1}{2} & 0 & & \\ & & 0 & \frac{1}{2} \\ & & \frac{1}{2} & 0 \end{pmatrix} \begin{pmatrix} 1 & \\ \alpha & \beta \\ & 1 \\ & \gamma \end{pmatrix}.$$

- Hence, every lattice of rank n is primitively represented by $\hat{\mathbb{H}}^n$.

Classification

Lemma 3

A quadratic form of rank 4 is primitively 2-universal if and only if it is isometric to $\hat{\mathbb{H}}^2$.

Lemma 4

Let R be nondyadic and $2 \le n \le 4$. A quadratic form of rank $2n$ is primitively n-universal if and only if it is n-universal and isometric to $\hat{\mathbb{H}}^n$ over F.

- $n = 3$: $\hat{\mathbb{H}}^3$ or $\hat{\mathbb{H}}^2 \perp \pi\hat{\mathbb{H}}$.
- $n = 4$: $\hat{\mathbb{H}}^3 \perp \langle -1, \pi^{2a} \rangle$, $\hat{\mathbb{H}}^3 \perp \langle -\pi, \pi^{2a+1} \rangle$, $\hat{\mathbb{H}}^2 \perp \langle -1 \rangle \perp \pi\hat{\mathbb{H}} \perp \langle \pi^{2a+2} \rangle$ (π is a uniformizer, a is a nonnegative integer).

Outline

Introduction

Lower bound for $U_R^*(n)$

Upper bound of $U_R^*(n)$

Classical case

Classical universality

In this section, we let R be dyadic.

- If $n = 1$, then the problem of (primitive) n-universality for classical quadratic forms is nothing more than a subset of that for integral quadratic forms.
- However, if $n \geq 2$, they become **distinct problems** that may be answered separately, for classical lattices only represent classical lattices.

$Q^*(\langle 1, -1\rangle)$

- Hereafter, we assume that R is 2-**adic**. i.e., 2 is unramified.
- For α_1, . . . , $\alpha_n \in R$, we mean by $\langle \alpha_1, \ldots, \alpha_n\rangle$ the quadratic form $\alpha_1 x_1^2 + \cdots + \alpha_n x_n^2$.
- For a quadratic form f of rank n, we mean by $Q(f)$ ($Q^*(f)$) the set of all $f(v)$, where v runs over all (primitive, respectively) vectors in R^n.

Lemma 5

Let $f = \langle 1, -1\rangle$. Then,

$$Q(f) = R^\times \cup 4R, \qquad Q^*(f) = \begin{cases} Q(f) & \text{if } R \neq \mathbb{Z}_2, \\ R^\times \cup 8R & \text{if } R = \mathbb{Z}_2. \end{cases}$$

Proof of Lemma 5

(Proof) Define $g(x, y) = x(x + 2y)$. Since $\langle 1, -1\rangle \cong \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, we have

$$Q(L) = \left\{ g(x, y) \mid (x, y) \in R^2 \right\},$$

$$Q^*(L) = \left\{ g(x, y) \mid (x, y) \in R^2 \text{ is primitive} \right\}.$$

If x is a unit in R, then so is $g(x, y)$. If x is even, then $4 \mid g(x, y)$. Hence, $Q(L) \subseteq R^\times \cup 4R$.

Let ϵ be any unit. Then, there exists a unit η such that $\eta^2 = \epsilon - 2\alpha$ for some $\alpha \in R$; hence, $g(\eta, \eta^{-1}\alpha) = \epsilon$. For a nonnegative integer a, $g(2^{a+2}, \epsilon - 2^{a+1}) = 2^{a+3}\epsilon$. Hence, $R^\times \cup 8R \subseteq Q^*(L)$.

Proof of Lemma 5 (cont'd)

Suppose that $R = \mathbb{Z}_2$. In this case, it remains to show that $Q^*(L) \cap 4R^\times = \varnothing$.
Assume that $g(x, y) \in Q^*(L) \cap 4R^\times$. Since x must be even, we have $y \in R^\times$.
Since $y \equiv 1 \pmod 2$, we have $8 \mid g(x, y)$, which is absurd.
Now, suppose that $R \neq \mathbb{Z}_2$. In this case, it remains to show that $4R^\times \subseteq Q^*(L)$.
Let $\epsilon \in R^\times$. There exists a unit η such that $\eta^2 \not\equiv \epsilon \pmod 2$. Then,
$g(2\eta, \eta^{-1}\epsilon - \eta) = 4\epsilon$.

$2n \leq cU_R^*(n) \leq 2n+1$

- Let $\mathbb{H}$ denote the quadratic form $\mathbb{H} = \mathbb{H}(x,y) = 2xy$.
- For every unit ϵ in R, $\mathbb{H} \perp \langle \epsilon \rangle \cong \langle 1, -1, \epsilon \rangle$.
- Hence, if R, then every quadratic form of rank n is primitively represented by $\mathbb{H}^n \perp \langle \epsilon \rangle$ for any unit ϵ in R.
- Hence, we have to determine between $cU_R^*(n) = 2n$ or $2n+1$.
- Since $cU_R^*(2) \geq cU_R(2) = 5$, we have $cU_R^*(2) = 5$.

Even unimodular quadratic forms

- Let $\Delta = 1 - 4\rho$ be a fixed nonsquare unit in R such that $\rho \in R^\times$.
- Let $\mathbb{A}$ denote the quadratic form $\mathbb{A} = \mathbb{A}(x, y) = 2x^2 + 2xy + 2\rho y^2$.
- If f is an even unimodular quadratic form of rank 2, then either $f \cong \mathbb{H}$ or $f \cong \mathbb{A}$.
- If f is a unimodular quadratic form of rank 3, then either $f \cong \mathbb{H} \perp \langle -dL \rangle$ or $f \cong \mathbb{A} \perp \langle -\Delta \cdot df \rangle$.
- For any $\epsilon \in R^\times$, $\mathbb{H} \perp \langle 2\epsilon \rangle \cong \mathbb{A} \perp \langle 2\Delta \cdot \epsilon \rangle$.
- We have $\mathbb{H} \perp \mathbb{H} \cong \mathbb{A} \perp \mathbb{A}$.

Improper modular quadratic forms

Let α be an integer in R.

- Scalings of $\mathbb{H}$ and $\mathbb{A}$ by α are denoted by

$$\alpha\mathbb{H} = 2\alpha xy \quad \text{and} \quad \alpha\mathbb{A} = 2\alpha x^2 + 2\alpha xy + 2\alpha\rho y^2.$$

- If 2α is primitively represented by a quadratic form h, then $\alpha\mathbb{H}$ and $\alpha\mathbb{A}$ are primitively represented by $\mathbb{H} \perp h$.
- If a quadratic form h has nonzero index, then $\alpha\mathbb{H}$ is primitively represented by $\mathbb{H} \perp h$ for any $\alpha \in R$.

$cU_R^*(n) = 2n$ for $n \geq 3$ when $R \neq \mathbb{Z}_2$

Lemma

Let $n \geq 3$ and $R \neq \mathbb{Z}_2$ be unramified dyadic. Then, the quadratic form $\mathbb{H}^{n-1} \perp \langle 1, -1 \rangle$ is primitively n-universal. In particular, $cU_R^*(n) = 2n$.

(Proof) Let ℓ be any lattice of rank n. By Lemma 2, ℓ is primitively represented by the given form unless ℓ is an orthogonal sum of even unimodular and proper 2-modular components.

Suppose so. If $\mathfrak{s}\ell = R$, then ℓ is orthogonally split by $\mathbb{H}$. Otherwise, ℓ is proper 2-modular. Then, ℓ is orthogonally split by $2\mathbb{H}$ or $2\mathbb{A}$.

Since $\mathbb{H}$, $2\mathbb{H}$, and $2\mathbb{A}$ are primitively represented by $\mathbb{H} \perp \langle 1, -1 \rangle$, we are done.

$cU^*_{\mathbb{Z}_2}(3) = 7$

- Hereafter, we assume that $R = \mathbb{Z}_2$.
- If there exists a P3U classical quadratic form of rank 6, then it must be a 3U quadratic form that is isometric to $\mathbb{H}^3$ over F.
- Hence, every P3U classical quadratic form of rank 6 is isometric to a unit scaling of one of the following six quadratic forms:

(A) $\mathbb{H}^2 \perp \langle 1, -1 \rangle$ (B) $\mathbb{H}^2 \perp \langle -1, 4 \rangle$ (C) $\mathbb{H} \perp \langle 1, -1, 2, -2 \rangle$

(D) $\mathbb{H} \perp \langle 1, -1, -2, 8 \rangle$ (E) $\mathbb{H} \perp \langle -1, 2, -2, 4 \rangle$ (F) $\mathbb{H} \perp \langle -1, -2, 4, 8 \rangle$

Lemma

No classical quadratic form of rank 6 over $\mathbb{Z}_2$ is primitively 3-universal.

$cU^*_{\mathbb{Z}_2}(4) = 9$

- If there exists a P4U classical quadratic form of rank 8, then it must be a 4U quadratic form that is isometric to $\mathbb{H}^4$ over F.
- Hence, every P4U classical quadratic form of rank 8 is isometric to a unit scaling of one of the following seven family of forms ($a \geq 0$):

(A) $\mathbb{H}^3 \perp \langle -1, 2^{2a} \rangle$

(B) $\mathbb{H}^2 \perp \langle 1, -1, -2, 2^{2a+1} \rangle$

(C) $\mathbb{H}^2 \perp \langle -1, -1, 4, 2^{2a+2} \rangle$

(D) $\mathbb{H}^2 \perp \langle -1, 2, -2, 2^{2a+2} \rangle$

(E) $\mathbb{H}^2 \perp \langle -1, -2, 4, 2^{2a+3} \rangle$

(F) $\mathbb{H}^2 \perp \langle -1, -2, 8, 2^{2a+4} \rangle$

(G) $\mathbb{H}^2 \perp \langle -1, 2, -8, 2^{2a+4} \rangle$

Lemma

No classical quadratic form of rank 8 over $\mathbb{Z}_2$ is primitively 4-universal.

Sketch of proof

Claim

$\mathbb{A} \perp 2^{2a+1}\mathbb{A}$ is not primitively represented by $\mathbb{H}^3 \perp \langle -1, 2^{2a} \rangle$.

(Sketch of Proof) Let M be a lattice such that $M \cong \mathbb{H} \perp \langle 5, 5, 5, 2^{2a} \rangle$ in $e_1, \ldots, e_6$. It suffices to show that $2^{2a+1}\mathbb{A}$ is not primitively represented by M. Suppose if possible that there exist z, $w \in M$ such that $\mathbb{Z}_2[z, w]$ is primitive, $Q(z) = Q(w) = 2^{2a+2}$, and $B(z, w) = 2^{2a+1}$. We may assume that $z \in \mathbb{H}$. Hence, if we write $w = \sum_1^6 w_i e_i$, then $\mathbb{Z}_2[z, w]$ is primitive iff (w_3, w_4, w_5, w_6) is primitive, and $2w_1 w_2 \equiv 0 \pmod{2^{2a+3}}$. However, no integer congruent to 2^{2a+2} modulo 2^{2a+3} is primitively represented by $\langle 5, 5, 5, 2^{2a} \rangle$. This is absurd.

$U^*_{\mathbb{Z}_2}(n) = 2n$ for $n \geq 5$

- Every classical quadratic form of rank 4 except $\mathbb{A} \perp 2\mathbb{A}$ is primitively represented by $\mathbb{H}^3 \perp \langle -1, 1 \rangle$.
- Using the above fact, it can be proven that $\mathbb{H}^4 \perp \langle -1, 1 \rangle$ and $\mathbb{H}^5 \perp \langle -1, 1 \rangle$ are P5U and P6U, respectively.
- By induction on n, $\mathbb{H}^{n-1} \perp \langle -1, 1 \rangle$ is classically PnU for all $n \geq 5$.

Main Theorem

Theorem(Oh–Y. 2024+)

We have $U_R^*(n) = 2n$.

If $R \neq \mathbb{Z}_2$ is 2-adic, then $cU_R^*(n) = \begin{cases} 2n+1 & \text{if } 1 \leq n \leq 2, \\ 2n & \text{if } n \geq 3. \end{cases}$

If $R = \mathbb{Z}_2$, then $cU_{\mathbb{Z}_2}^*(n) = \begin{cases} 2n+1 & \text{if } 1 \leq n \leq 4, \\ 2n & \text{if } n \geq 5. \end{cases}$

Summary of minimal ranks

	R		$R \neq \mathbb{Z}_2$ 2-adic		$\mathbb{Z}_2$		$\mathbb{Z}$, pos. def.	
n	$U_R(n)$	$U_R^*(n)$	$cU_R(n)$	$cU_R^*(n)$	$cU_{\mathbb{Z}_2}(n)$	$cU_{\mathbb{Z}_2}^*(n)$	$cU_{\mathbb{Z}}(n)^\dagger$	$cU_{\mathbb{Z}}^*(n)$
1	2	2	3	3	3	3	4	4
2	4	4	5	5	5	5	5	6
3	6	6	6	6	6	7	6	7
4	7	8	7	8	7	9	7	
5	8	10	8	10	8	10	8	
6	9	12	9	12	9	12	13	
$\vdots$	$\vdots$		$\vdots$		$\vdots$		$\vdots$	

† Oh(1999)

Thanks for your attention!