

Composition of Quadratic Forms when 2 is NOT invertible

Roland Löttscher

University of Basel

May 29th / Graduate Colloquium

Outline

- 1 Introduction: Quadratic forms and compositions
 - Quadratic forms over rings
 - Composition with quadratic forms
 - Composition with symmetric bilinear forms
- 2 Symmetric bilinear vs. quadratic composition
 - The converse problem
 - First observations
 - The main theorem
- 3 Application to a classical problem

General Setting

We have:

- an arbitrary commutative ring R
- a R -module M
- a quadratic form q on M , that is a map $q: M \rightarrow R$ such that
 - $q(rx) = r^2q(x)$ for all $r \in R, x \in M$,
 - the polar form $b_q: M \times M \rightarrow R$ defined by

$$b_q(x, x') = q(x + x') - q(x) - q(x')$$

is bilinear.

Special role of 2

Note:

We defined $b_q(x, x') = q(x + x') - q(x) - q(x')$

- If $\frac{1}{2} \in R$ then there is a bijection between *quadratic forms* and *symmetric bilinear forms* by:
 - $q \rightsquigarrow b$ where $b(x, x') = \frac{1}{2}(q(x + x') - q(x) - q(x'))$
 - $b \rightsquigarrow q$ where $q(x) = b(x, x)$
- If $\frac{1}{2} \notin R$ then quadratic forms and symmetric bilinear forms are essentially *different* things.

Special role of 2

Note:

We defined $b_q(x, x') = q(x + x') - q(x) - q(x')$

- If $\frac{1}{2} \in R$ then there is a bijection between *quadratic forms* and *symmetric bilinear forms* by:
 - $q \rightsquigarrow b$ where $b(x, x') = \frac{1}{2}(q(x + x') - q(x) - q(x'))$
 - $b \rightsquigarrow q$ where $q(x) = b(x, x)$
- If $\frac{1}{2} \notin R$ then quadratic forms and symmetric bilinear forms are essentially *different* things.

Special role of 2

Note:

We defined $b_q(x, x') = q(x + x') - q(x) - q(x')$

- If $\frac{1}{2} \notin R$ then quadratic forms and symmetric bilinear forms are essentially *different* things.

Example: a symmetric bilinear form not coming from a quadratic form

The bilinear form $b: R^n \times R^n \rightarrow R$, $b(x, x') = \sum x_i x'_i$ is not polar of any quadratic form.

Special role of 2

Note:

We defined $b_q(x, x') = q(x + x') - q(x) - q(x')$

- If $\frac{1}{2} \notin R$ then quadratic forms and symmetric bilinear forms are essentially *different* things.

Example: a symmetric bilinear form not coming from a quadratic form

The bilinear form $b: R^n \times R^n \rightarrow R$, $b(x, x') = \sum x_i x'_i$ is not polar of any quadratic form.

Example: two quadratic forms with the same polar

If $2\mu = 0$, then $q_1, q_2: R^2 \rightarrow R$ defined by $q_1(x) = x_1 x_2$ and $q_2(x) = \mu x_1^2 + x_1 x_2$ both have polar $b(x, x') = x_1 x'_2 + x_2 x'_1$.

Four situations

Let b be a symmetric bilinear form. The following situations are possible:

- **2 is invertible:** $b = b_q$ for some quadratic form q and q is unique.
- **2 is neither invertible, nor a zero divisor:** $b = b_q$ for some q iff $b(x, x) \in 2R, \forall x$; if so then q is unique.
- **2 is a zero divisor, but not equal 0:** $b = b_q$ for some q iff $b(x, x) \in 2R, \forall x$, but q is not unique.
- **2 equals 0:** weird as the previous point, but at least you don't make sign errors.

Four situations

Let b be a symmetric bilinear form. The following situations are possible:

- **2 is invertible:** $b = b_q$ for some quadratic form q and q is unique.
- **2 is neither invertible, nor a zero divisor:** $b = b_q$ for some q iff $b(x, x) \in 2R, \forall x$; if so then q is unique.
- **2 is a zero divisor, but not equal 0:** $b = b_q$ for some q iff $b(x, x) \in 2R, \forall x$, but q is not unique.
- **2 equals 0:** weird as the previous point, but at least you don't make sign errors.

Four situations

Let b be a symmetric bilinear form. The following situations are possible:

- **2 is invertible:** $b = b_q$ for some quadratic form q and q is unique.
- **2 is neither invertible, nor a zero divisor:** $b = b_q$ for some q iff $b(x, x) \in 2R, \forall x$; if so then q is unique.
- **2 is a zero divisor, but not equal 0:** $b = b_q$ for some q iff $b(x, x) \in 2R, \forall x$, but q is not unique.
- **2 equals 0:** weird as the previous point, but at least you don't make sign errors.

Four situations

Let b be a symmetric bilinear form. The following situations are possible:

- **2 is invertible:** $b = b_q$ for some quadratic form q and q is unique.
- **2 is neither invertible, nor a zero divisor:** $b = b_q$ for some q iff $b(x, x) \in 2R, \forall x$; if so then q is unique.
- **2 is a zero divisor, but not equal 0:** $b = b_q$ for some q iff $b(x, x) \in 2R, \forall x$, but q is not unique.
- **2 equals 0:** weird as the previous point, but at least you don't make sign errors.

Four situations

Let b be a symmetric bilinear form. The following situations are possible:

- **2 is invertible:** $b = b_q$ for some quadratic form q and q is unique.
- **2 is neither invertible, nor a zero divisor:** $b = b_q$ for some q iff $b(x, x) \in 2R, \forall x$; if so then q is unique.
- **2 is a zero divisor, but not equal 0:** $b = b_q$ for some q iff $b(x, x) \in 2R, \forall x$, but q is not unique.
- **2 equals 0:** weird as the previous point, but at least you don't make sign errors.

Definition of Composition

So what is a **composition of quadratic forms**?

Definition

Let $q: M \rightarrow R$ and $p: E \rightarrow R$ be quadratic forms. A bilinear map $\phi: M \times E \rightarrow E$ is called a **quadratic composition** if the following identity holds:

$$p(\phi(x, y)) = q(x)p(y), \quad \text{for all } x \in M, y \in E.$$

More general: A bilinear map $\phi: M \times E \rightarrow N$ satisfying

$$r(\phi(x, y)) = q(x)p(y), \quad \text{for all } x \in M, y \in E,$$

where $r: N \rightarrow R$ is a third quadratic form.

Classical examples

Quaternion multiplication:

$\mathbb{H} \times \mathbb{H} \rightarrow \mathbb{H}$. We have $n(x \cdot y) = n(x)n(y)$, where $n: \mathbb{H} \rightarrow \mathbb{R}$ is the norm of quaternions, $n(x_0 + x_1i + x_2j + x_3ij) = x_0^2 + x_1^2 + x_2^2 + x_3^2$.

More general:

Multiplication in any central simple F -algebra A of dimension 4 (F a field) w. r. t. the reduced norm n_A , e.g. $A = M_2(F)$, $n_A = \det: A \rightarrow F$.

Similarly for Octonions.

Theorem (Hurwitz)

If q is a regular quadratic form on a vector-space V endowed with a composition $\phi: V \times V \rightarrow V$ then $\dim V = 1, 2, 4$ or 8 .

History

Hurwitz' question:

For what values of $m, n \in \mathbb{N}$ does there exist a formula $(x_1^2 + x_2^2 + \dots + x_m^2) \cdot (y_1^2 + y_2^2 + \dots + y_n^2) = (z_1^2 + z_2^2 + \dots + z_n^2)$, where z_1, z_2, \dots, z_n are bilinear forms in the variables $x_1, \dots, x_m; y_1, \dots, y_n$ with coefficients in a field F ?

This corresponds to compositions $F^m \times F^n \rightarrow F^n$ where F^k is furnished with the quadratic form $q_k(\mathbf{x}) = \sum_{i=1}^k x_i^2$.

Theorem (Hurwitz' solution for $F = \mathbb{C}$)

Such a composition exists iff $m \leq \rho(n)$ where $\rho: \mathbb{N} \rightarrow \mathbb{N}$ is given as $\rho(n) = 8a + 2^b$ for $n = n_0 \cdot 2^{4a+b}$ with n_0 odd and $0 \leq b < 4$.

First Conclusion

Let $\phi : M \times E \rightarrow E$ be a quadratic composition. Then we have:

- $\rho(\phi(x, y)) = q(x)\rho(y)$ (1)
- $\rho(\phi(x, y')) = q(x)\rho(y')$ (2)
- $\rho(\phi(x, y) + \phi(x, y')) = q(x)\rho(y + y')$ (3)
- Subtracting (1) and (2) from (3) gives:

$$b_p(\phi(x, y), \phi(x, y')) = q(x)b_p(y, y').$$

First Conclusion

Let $\phi : M \times E \rightarrow E$ be a quadratic composition. Then we have:

- $p(\phi(x, y)) = q(x)p(y)$ (1)
- $p(\phi(x, y')) = q(x)p(y')$ (2)
- $p(\phi(x, y) + \phi(x, y')) = q(x)p(y + y')$ (3)
- Subtracting (1) and (2) from (3) gives:

$$b_p(\phi(x, y), \phi(x, y')) = q(x)b_p(y, y').$$

First Conclusion

Let $\phi : M \times E \rightarrow E$ be a quadratic composition. Then we have:

- $p(\phi(x, y)) = q(x)p(y)$ (1)
- $p(\phi(x, y')) = q(x)p(y')$ (2)
- $p(\phi(x, y) + \phi(x, y')) = q(x)p(y + y')$ (3)
- Subtracting (1) and (2) from (3) gives:

$$b_p(\phi(x, y), \phi(x, y')) = q(x)b_p(y, y').$$

First Conclusion

Let $\phi : M \times E \rightarrow E$ be a quadratic composition. Then we have:

- $p(\phi(x, y)) = q(x)p(y)$ (1)
- $p(\phi(x, y')) = q(x)p(y')$ (2)
- $p(\phi(x, y) + \phi(x, y')) = q(x)p(y + y')$ (3)
- Subtracting (1) and (2) from (3) gives:

$$b_p(\phi(x, y), \phi(x, y')) = q(x)b_p(y, y').$$

Symmetric bilinear composition

Definition

Let $q: M \rightarrow R$ be a quadratic form and $b: E \times E \rightarrow R$ be a (symmetric) bilinear form.

A bilinear map $\phi: M \times E \rightarrow E$ is called a **(symmetric) bilinear composition** if the identity

$$b(\phi(x, y), \phi(x, y')) = q(x)b(y, y'), \quad x \in M, y, y' \in E$$

holds.

We observed: A composition $\phi: M \times E \rightarrow E$ of quadratic forms $q: M \rightarrow R$ and $p: E \rightarrow R$ induces a composition of q with the polar form b_p of p .

Outline

- 1 Introduction: Quadratic forms and compositions
 - Quadratic forms over rings
 - Composition with quadratic forms
 - Composition with symmetric bilinear forms
- 2 Symmetric bilinear vs. quadratic composition
 - The converse problem
 - First observations
 - The main theorem
- 3 Application to a classical problem

Formulation of the problem

The problem:

Given a composition $\phi : M \times E \rightarrow E$ of a quadratic form $q : M \rightarrow R$ with a symmetric bilinear form $b : E \times E \rightarrow R$, is it possible to find a quadratic form p with polar b such that $p(\phi(x, y)) = q(x)p(y)$??

Subsequent questions:

- If yes, how to find such a p ?
- If no, what conditions could ensure that there exists a p ?

First case

- Assume that 2 is not a zero divisor and $b = b_p$ is polar of a quadratic form.
- We have $b(\phi(x, y), \phi(x, y')) = q(x)b(y, y')$.
- Take $y = y'$. $b(\phi(x, y), \phi(x, y)) = q(x)b(y, y)$.
- Thus $2p(\phi(x, y)) = 2q(x)p(y)$. **Cancel 2!**
- Hence ϕ is induced by a quadratic composition.
- So what if 2 IS a zero divisor?

First case

- Assume that 2 is not a zero divisor and $b = b_p$ is polar of a quadratic form.
- We have $b(\phi(x, y), \phi(x, y')) = q(x)b(y, y')$.
- Take $y = y'$. $b(\phi(x, y), \phi(x, y)) = q(x)b(y, y)$.
- Thus $2p(\phi(x, y)) = 2q(x)p(y)$. Cancel $2!$
- Hence ϕ is induced by a quadratic composition.
- So what if 2 IS a zero divisor?

First case

- Assume that 2 is not a zero divisor and $b = b_p$ is polar of a quadratic form.
- We have $b(\phi(x, y), \phi(x, y')) = q(x)b(y, y')$.
- Take $y = y'$. $b(\phi(x, y), \phi(x, y)) = q(x)b(y, y)$.
- Thus $2p(\phi(x, y)) = 2q(x)p(y)$. Cancel $2!$
- Hence ϕ is induced by a quadratic composition.
- So what if 2 IS a zero divisor?

First case

- Assume that 2 is not a zero divisor and $b = b_p$ is polar of a quadratic form.
- We have $b(\phi(x, y), \phi(x, y')) = q(x)b(y, y')$.
- Take $y = y'$. $b(\phi(x, y), \phi(x, y)) = q(x)b(y, y)$.
- Thus $2p(\phi(x, y)) = 2q(x)p(y)$. **Cancel 2!**
- Hence ϕ is induced by a quadratic composition.
- So what if 2 IS a zero divisor?

First case

- Assume that 2 is not a zero divisor and $b = b_p$ is polar of a quadratic form.
- We have $b(\phi(x, y), \phi(x, y')) = q(x)b(y, y')$.
- Take $y = y'$. $b(\phi(x, y), \phi(x, y)) = q(x)b(y, y)$.
- Thus $2p(\phi(x, y)) = 2q(x)p(y)$. **Cancel 2!**
- Hence ϕ is induced by a quadratic composition.
- So what if 2 IS a zero divisor?

First case

- Assume that 2 is not a zero divisor and $b = b_p$ is polar of a quadratic form.
- We have $b(\phi(x, y), \phi(x, y')) = q(x)b(y, y')$.
- Take $y = y'$. $b(\phi(x, y), \phi(x, y)) = q(x)b(y, y)$.
- Thus $2p(\phi(x, y)) = 2q(x)p(y)$. **Cancel 2!**
- Hence ϕ is induced by a quadratic composition.
- So what if 2 IS a zero divisor?

Interpretation

For $x \in M$ consider the map $\phi_x: E \rightarrow E$, $\phi_x(y) = \phi(x, y)$.

- The formula $p(\phi(x, y)) = q(x)p(y)$ means that ϕ_x is a **similitude of (E, p)** of norm $q(x)$.
- The formula $b(\phi(x, y'), \phi(x, y')) = q(x)b(y, y')$ means that ϕ_x is a **similitude of (E, b)** of norm $q(x)$.
- In general: **$\text{Sim}(E, p) \subsetneq \text{Sim}(E, b_p)$** .

Example:

$p: F^2 \rightarrow F$, $p(y) = y_1 y_2$, $\text{char } F = 2$. Then $O(F^2, p) = \left\{ \begin{pmatrix} x & y \\ u & v \end{pmatrix} \in \text{Sl}_2(F) \mid xu = vy = 0 \right\} \subsetneq \text{Sl}_2(F) = O(F^2, b_p)$.

Refined setting

- R arbitrary commutative ring
- M, E finitely generated projective R -modules of constant rank
- (M, q) and (E, b) are “spaces”, i. e.
 - $b: E \times E \rightarrow R$ regular symmetric bilinear form.
 - $q: M \rightarrow R$ regular or semi-regular (if $\text{rk } M$ is odd) quadratic form.
- $\phi: M \times E \rightarrow E$ a composition of the quadratic space (M, q) with the symmetric bilinear space (E, b) , written
$$\phi: (M, q) \times (E, b) \rightarrow (E, b)$$

A first observation

Let $\phi : (M, q) \times (E, b) \rightarrow (E, b)$ be a composition.

Proposition (Uniqueness)

If $\text{rk } M \geq 2$ and ϕ comes from a composition with a quadratic form p , then p is unique!

More generally: If $\text{rk } M \geq 2$ there exists at most one pair of quadratic forms $p, p' : E \rightarrow R$ with polar b such that $p'(\phi(x, y)) = q(x)p(y)$

Proof.

- Assume $b_q(z, z') = 1$ for some $z, z' \in M$. Linearize $p'(\phi(x, y)) = q(x)p(y)$ in x :
- $b(\phi(z, y), \phi(z', y)) = b_q(z, z')p(y) = p(y)$, hence p is unique.
- For $q(x) \in R^\times$ the map ϕ_x is surjective, hence p' is unique.



A second observation

(M, q) quadratic space, (E, b) symmetric bilinear space.

Let $\phi: M \times E \rightarrow E$ be some bilinear map.

Let $\phi^\sigma: M \times E \rightarrow E$ be the bilinear map defined by

$$\phi^\sigma(x, y) = \sigma_b(\phi_x)(y).$$

Proposition

The following statements are equivalent:

- $\phi: (M, q) \times (E, b) \rightarrow (E, b)$ is a composition.
- The equation $\phi_x^\sigma \phi_x = q(x)\text{id}_E$ holds for all $x \in M$.
- The equation $\phi_x \phi_x^\sigma = q(x)\text{id}_E$ holds for all $x \in M$.
- $\phi^\sigma: (M, q) \times (E, b) \rightarrow (E, b)$ is a composition.

Refutation of the converse

A counterexample

Assume $\exists \mu \in R$ with $2\mu = 0, \mu \neq 0$. Let $(M, q) = (R^4, q_H)$,
 $q_H(x) = x_1x_2 + x_3x_4$ and b be the symmetric bilinear form on $E = R^4$
defined by $b(y, y') = y_1y'_4 + y_4y'_1 - y_2y'_3 - y_3y'_2 + \mu(y_1y'_2 + y_2y'_1)$.
The bilinear map $\phi : M \times E \rightarrow E$ given by

$$\phi(x, y) = \begin{pmatrix} x_1y_1 + x_3y_2 \\ x_2y_2 - x_4y_1 \\ x_1y_3 + x_3y_4 \\ x_2y_4 - x_4y_3 \end{pmatrix}$$

is a composition of (M, q) with (E, b) , but there is **no** quadratic form p
with polar b such that $p(\phi(x, y)) = q(x)p(y)$ for all $x \in M, y \in E$.

Rank 6 Theorem

Let $\phi : (M, q) \times (E, b) \rightarrow (E, b)$ be a composition.

Theorem (Rank 6 Theorem)

*If $\text{rk } M \geq 6$, there exist unique quadratic forms p, p^σ on E both with polar b such that $p^\sigma(\phi(x, y)) = q(x)p(y)$ for all $x \in M, y \in E$.
Moreover $p(\phi^\sigma(x, y)) = q(x)p^\sigma(y)$ for all $x \in M, y \in E$.*

Remark: p and p^σ are locally given as

$$p(y) = b(\phi_z(y), \phi_{z'}(y))$$

$$p^\sigma(y) = b(\phi_z^\sigma(y), \phi_{z'}^\sigma(y))$$

for some $z, z' \in M$ satisfying $b_q(z, z') = 1$.

Sketch of the proof

Proof.

- 1 Assume R is local and 2 is not invertible. Choose elements $z, z' \in M$ with $b_q(z, z') = 1$.
- 2 $N = Rz \oplus Rz'$ is a regular subspace and $(M, q) \simeq N \perp N^\perp$.
- 3 Calculation shows that $p^\sigma(\phi(x, y)) = q(x)p(y)$ for all $y \in E$ and for $x \in N \cup N^\perp$.
- 4 Write $x = c + d$ where $c \in N, d \in N^\perp$.
By (3) it suffices to show

$$b(\phi_c y, \phi_d y) = 0, \text{ for all } y \in E.$$

- 5 We need a Lemma!



The decisive lemma

Lemma

Let $\phi : (M, q) \times (E, b) \rightarrow (E, b)$ be a composition. Then for $u, v, c, d \in M$ and $y \in E$ the following identity holds:

$$\begin{aligned} b_q(u, v)b(\phi_c y, \phi_d y) + b_q(u, c)b(\phi_v y, \phi_d y) + b_q(v, c)b(\phi_u y, \phi_d y) \\ = b_q(c, d)b(\phi_u y, \phi_v y) + b_q(v, d)b(\phi_u y, \phi_c y) + b_q(u, d)b(\phi_v y, \phi_c y) \end{aligned}$$

In particular, if $b_q(u, c) = b_q(v, c) = b_q(v, d) = b_q(u, d) = 0$, then:

$$b_q(u, v)b(\phi_c y, \phi_d y) = b_q(c, d)b(\phi_u y, \phi_v y).$$

We need $u, v \in \{c, d\}^\perp$ satisfying $b_q(u, v) = 1$.

Outline

- 1 Introduction: Quadratic forms and compositions
 - Quadratic forms over rings
 - Composition with quadratic forms
 - Composition with symmetric bilinear forms
- 2 Symmetric bilinear vs. quadratic composition
 - The converse problem
 - First observations
 - The main theorem
- 3 Application to a classical problem

Ranks of compositions

Theorem (Züger)

The smallest rank of a symmetric bilinear space (E, b) for which there exists a composition $\phi : (M, q) \times (E, b) \rightarrow (E, b)$ with $\text{rk } M = m$ is given by $\pi(m)$ if $2 \neq 0$ in R , and by $\pi'(m)$ if $2 = 0$ in R , respectively.

| b | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|-----------|------------|----------|------------|------------|------------|------------|------------|------------|
| $\pi(m)$ | 2^{4a-1} | 2^{4a} | 2^{4a+1} | 2^{4a+2} | 2^{4a+2} | 2^{4a+3} | 2^{4a+3} | 2^{4a+3} |
| $\pi'(m)$ | 2^{4a-1} | 2^{4a} | 2^{4a+1} | 2^{4a+1} | 2^{4a+1} | 2^{4a+2} | 2^{4a+3} | 2^{4a+3} |

where $m = 8a + b \in \mathbb{N}$ with $a, b \in \mathbb{N}_0$ and $0 \leq b < 8$.

Application of the rank 6 theorem

Theorem (L)

The smallest rank $\gamma(m)$ of a quadratic space (E, p) for which there exists a composition $\phi : (M, q) \times (E, p) \rightarrow (E, p)$ with $\text{rk } M = m$ is $\pi(m)$ if $2 \neq 0$, and $\pi'(m)$ if $2 = 0$, respectively, with the exceptions: $\gamma(3) = 4, \gamma(4) = 4, \gamma(5) = 8$.

Remarks:

- The above theorem generalizes a result of Elduque (1999) for fields of characteristic 2.
- The function γ is a reformulation of the Hurwitz-Radon function.

Summary

- Symmetric bilinear compositions and quadratic compositions $\phi: M \times E \rightarrow E$ coincide for $\text{rk } M \geq 6$ and are different for $\text{rk } M < 6$ if 2 is a zero divisor.
- The minimal ranks of spaces (E, ρ) admitting a composition with a quadratic space (M, q) of fixed rank depend only on whether $+1 = -1$ or not.

| |
|----------|
| ∞ |
| ... |
| 7 |
| 6 |
| 5 |
| 4 |
| 3 |
| 2 |
| 1 |