11:44 a.m. April 2, 2011

Minkowski

Bill Casselman
University of British Columbia
cass@math.ubc.ca

The theory of quadratic forms over $\mathbb{Z}_2$ or over the finite rings $\mathbb{Z}/2^n$ is not treated well in recent literature. At the head of §4 of Chapter 8 in Cassell's book **Rational quadratic forms**, which is where he discusses this topic, the author remarks, "Only the masochist is invited to read the rest of this section." He treats subsequently only the simplest phenomena. There are several other accounts, some complete if obscure and some very sketchy—for example §5 of [Pall:1945] (no proofs and an unmotivated summary); §93 of [O'Meara:1963] (apparently complete but unnecessarily complicated); [Conway:1973] (no proofs, and somewhat vague statements, not improved in [Conway:1995]); and [Miranda-Morrison:1982/2009] (complete, but not simple). This bad press is somewhat puzzling, because the original treatment in Minkowski's prize essay of 1883 is, if interpreted carefully, quite elegant.

The main problem at hand is to classify such forms, and in particular how to tell if two are equivalent. The difficulty is that for $\mathbb{Z}_2$, as opposed to $\mathbb{Z}_p$ with p odd, there is no canonical normal form to which all can be reduced. (Cassels on this matter: "We do not attempt to specify a unique canonical form; that is more for a parliamentary draftsman than a mathematician.") In Minkowski's prize essay a somewhat theoretical criterion for equivalence is demonstrated, but it was written before Hensel had introduced p-adic numbers, and suffers from many annoying technical difficulties. I shall translate Minkowski's treatment into modern terminology, and then approach closer to more recent discussion explaining how to get an explicit algorithm from this account. An important part of Minkowski's treatment also explains how to count the number of points in finite spheres.

Contents

1. Quadratic forms over p-adic integers

I'll call a quadratic form non-degenerate over $\mathbb{Z}_p$ if it is non-degenerate over $\mathbb{Q}_p$. The simplest and most useful theorem about such forms is this:

[strictly-ndg-modp] **Proposition 1.1.** *Two quadratic forms over $\mathbb{Z}_p$ whose reductions modulo p are isomorphic and strictly non-degenerate over $\mathbb{Z}/p$ are isomorphic over $\mathbb{Z}_p$.*

This is a version of Hensel's Lemma. If p is odd, this will give us a canonical form for all non-degenerate quadratic forms over $\mathbb{Z}_p$. The most general result of this kind is that quadratic forms over $\mathbb{Z}_p$ are isomorphic if they are isomorphic modulo p^n for $n \gg 0$—put roughly, two forms are isomorphic if they are close to one another. We'll see this formulated precisely later on.

Proof. The map from $O(Q)$ to $O(Q \mathrm{mod} p$ is surjective.

NOPE!

So we may assume Q_1 and Q_2 are the same modulo p. We want to find $X \equiv_1 0$ such that

$$^{t}(I+X)M_1(I+X) = M_2 \text{ or } {}^{t}XM_1 + M_1X + {}^{t}XM_1X = M_2 - M_1$$

by successive approximations. To start with, we have $M_2 - M_1 \equiv_0 0$. Suppose given X_n such that

0

Suppose (L, Q) to be a quadratic form over $R = \mathbb{Z}_2$ that's non-degenerate over $\mathbb{Q}_2$, with $L = R^n$. As a form over $\mathbb{Q}_2$ it is simply a sum of one-dimensional forms, and in fact the classification of forms over $\mathbb{Q}_2$ is not essentially different from the classification of forms over $\mathbb{Q}_p$ with p odd. But over R the situation is very different. Our goal here will be to classify forms over R up to isomorphism, and to give as well some idea of how to compute the size of spheres.

Let

$$L_n = \{\lambda \in L \,|\, \nabla(\lambda, L) \subseteq p^n R\,.$$

Define

$$L^{\#} = \{\lambda \in L \otimes \mathbb{Q}_2 \,|\, \nabla(\lambda, L) \subseteq \mathbb{Z}_2\}\,.$$

Because Q is assumed non-degenerate over $\mathbb{Q}_2$, the quotient $\mathcal{D} = L^{\#}/L$ is finite. I call $\mathcal{D}$ the **different** of Q and the cardinality $D = |\mathcal{D}|$ its **discriminant**.

For example, if $Q = H$ or the norm from K to $\mathbb{Q}_2$, where K is the unique unramified extension of $\mathbb{Q}_2$, then $L^{\#} = L$ and $D = 1$. If $Q = \sum a_i x_i^2$ where a is a unit in $\mathbb{Z}_2$, then $L^{\#} = (1/2)L$ and $D = 2^n$. In general, we can find a basis (λ_i) of $L^{\#}$ such that $(p^{m_i}\lambda_i)$ is a basis of L with $m_{i+1} \ge m_i$. If $m \ge m_n$ then $p^m L^{\#} \subset L$. We have a filtration

$$L \supseteq L \cap pL^{\#} \supseteq L \cap p^2 L^{\#} \supseteq \ldots \supseteq L \cap p^{m_n} L^{\#} = p^{m_n} L^{\#}\,.$$

The exact sequence of quadratic spaces

$$0 \to L \cap pL^{\#} \to L \to L/L \cap pL^{\#} \to 0$$

splits. Let $L_1 = L \cap pL^{\#}$. Then L is the orthogonal sum of a unique non-degenerate form over $\mathbb{Z}_2$ that restricts to one of $L/L \cap pL^{\#}$. The splitting is not canonical, but that doesn't matter. The isomorphism class of the summand is uniquely determined, so it does no harm to assume from now on that $L = L_1$. Under this assumption, every cross term in Q is now divisible by 2. What that means is that every term in ∇ is divisible by 2, is defined in terms of the bilinear form $(1/2)\nabla$. In short, we are in the land in which Gauss, Minkowski, and Cassels feel at home.

The important consequence for us is that we can define $\wedge^m \nabla$ on every $\wedge^m L$. The symmetric matrix M_Q defining Q is now with integral entries, and defines the map ∇ from L to $L^{\#}$, assigned the dual basis. The matrix of $\wedge^m \nabla$ is $\wedge^m M_Q$, so can be explicitly computed. The factors p^{m_i} are those of the matrix M_Q, and the successive factors are the greatest common divisors of the matrices $\wedge^m M_Q$.

The factors $d_k = \prod_{i \le k} p^{m_i}$ are invariants of the form Q, independent of the coordinate system expressing M_Q. If $M = D + S$ then d_k is the gcd of $\wedge^k(D + S)$. For equivalence of quadratic forms the coordinate changes are special, and the gcd e_k of $\wedge^k(D + 2S)$ is also invariant. Define $\sigma_i = e_k/d_k$. Thus $\sigma_k = 1$ or 2. For example, . . .

and if Q is of level 1 then $\sigma = 1$ if $Q = \ldots$ and $\sigma_1 = 2$ if $Q = \ldots$.

[equivalence2] **Proposition 1.2.** *Two non-degenerate quadratic forms of the same dimension over $\mathbb{Z}_2$ are equivalent if and only if (a) the factors σ_k agree; (b) their determinants agree up to unit squares; (c) the volumes of the associated spheres are the same.*

The volume of a sphere is Siegel's limit. Only a finite number presumably involved, since presumably the size of the sphere of size $p^{2n}r$ is easily found from that of size r. I. e./ all modulo some fixed high power of p.

Also, we need the approximation theorem: Q_1 equivalent to Q_2 if close. So if b is a unit then

$$ax^2 + bxy + cy^2 \equiv \begin{cases} x^2 + xy + y^2 & \text{if } a \text{ and } c \text{ are units} \\ xy & \text{otherwise.} \end{cases}$$

Need a Lemma about

$${}^t(I + X)M_1(I + X) = M_2$$

or

$$\begin{bmatrix} 1+a & c \\ b & 1+d \end{bmatrix} \begin{bmatrix} A & B/2 \\ B/1 & C \end{bmatrix} \begin{bmatrix} 1+a & b \\ c & 1+d \end{bmatrix} = M_1 + {}^tXM_1 + M_1X + {}^tXM_1X\,.$$

so we are reduced to solving

$${}^tXM_1 + M_1X = M_2$$

or

$$\begin{aligned} &\begin{bmatrix} a & c \\ b & d \end{bmatrix} \begin{bmatrix} A & B/2 \\ B/2 & C \end{bmatrix} + \begin{bmatrix} A & B/2 \\ B/2 & C \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \\ &\quad= \begin{bmatrix} aA + cB/2 & aB/2 + cC \\ bA + dB/2 & bB/2 + dC \end{bmatrix} + \begin{bmatrix} aA + cB/2 & bA + dB/2 \\ aB/2 + cC & bB/2 + dC \end{bmatrix} \\ &\quad= \begin{bmatrix} 2aA + cB & bA + (a+d)B/2 + cC \\ bA + (a+d)B/2 + cC & bB + 2dC \end{bmatrix} \\ &\quad= M_2 - M_1\,. \end{aligned}$$

If $M_1 \equiv_n M_2$, we look for $X \equiv_n 0$ such that $(I + {}^tX)M_1(I + X) \equiv_{n+1} M_2$ so we get an equation

$$\begin{bmatrix} 2a\varpi^n A + c\varpi^n B & b\varpi^n A + (a+d)\varpi^n B/2 + c\varpi^n C \\ b\varpi^n A + (a+d)\varpi^n B/2 + c\varpi^n C & b\varpi^n B + 2d\varpi^n C \end{bmatrix} = M_2 - M_1 = \varpi^n M$$

or

$$\begin{bmatrix} cB & bA + (a+d)B/2 + cC \\ bA + (a+d)B/2 + cC & bB \end{bmatrix} = M$$

which can always be solved, since B is a unit.

Relations from [Miranda-Morrison:2009].

How to prove the Proposition, how to calculate what is needed? See [O'Meara:1963].

$$(L_1 \oplus L_2)^\# = L_1^\# \oplus L_2^\#$$

If Q is irreducible, then $Q = ax^2$ with a a unit or $Q = 2N$ or $Q = 2H$, then $L^\# = (1/2)L$.

The quotient $L^\#/L$ is a sum of copies of $\mathbb{Z}/2$ if and only if Q is an orthogonal sum of copies of ax^2 ($a \equiv 1, 3, 5$, or 7 modulo 8), N, and H.

General $\mathbb{F}_q$ is OK, because $x \mapsto x^2$ is an automorphism.

Suppose $Ax^2 + Bxy = Cy^2$ is non-degenerate over F with $B \neq 0$. Since $x \mapsto x^2$ is onto, we may write $B = \beta^2$, then set $x = x_*/\beta$, $y = y_*/\beta$, getting a new form with $B = 1$. So now we have $Ax^2 + xy + Cy^2$. There are two cases: this factors over F, or it does not. Or: in the first case some non-trivial zero, in the second not. Claim: in the first case, equivalent to xy, in the second to $N_{K/F}$.

2. References

1. J. W. S. Cassels, **Rational quadratic forms**, Academic Press, 1978. Reprinted by Dover in 2008.

§4 of Chapter 8 is about canonical forms over $\mathbb{Z}_2$.

2. J. H. Conway and N. J. A. Sloane, **Sphere packings, lattices and groups**, Springer-Verlag, 1993.

§7 of Chapter 15 is about forms over p-adic integers.

3. Richard Elman, Nikita Karpenko, and Alexander Merjurjev, **The algebraic and geometric theory of quadratic forms**, A. M. S., 2008.

4. Yoshiyuki Kitaoka, **Arithmetic quadratic forms**, Cambridge University Press, 1993.

5. Hermann Minkowski, 'Grundlagen für eine Theorie quadratischen Formen mit ganzahligen Koeffizienten', in **Gesammelte Abhandlungen**, 3–145.

6. Rick Miranda and David R. Morrison, **Embeddings of integral quadratic forms**, preprint, 2009. Available on the Internet.

7. O. T. O'Meara, 'Local characterization of integral quadratic forms by Gauss sums', *American Journal of Mathematics* **79** (1957), 687–709.

8. O. T. O'Meara, **Introduction to quadratic forms**, Springer-Verlag, 1963.

§93 is about quadratic forms over dyadic fields.

9. Gordon Pall, 'The arithmetical invariants of quadratic forms', *Bulletin of the A. M. S.* **51** (1945), 185–197.