DESCRIPTIONS OF PROMYS 2011 RESEARCH PROJECTS ON BINARY QUADRATIC FORMS

JONATHAN HANKE

1. Brief project descriptions

A **binary quadratic form** is a polynomial Q of the form $Q := Q(x, y) := ax^2+bxy+cy^2$ where the coefficients a, b, c are numbers in our fixed number system R (e.g. $\mathbb{Z}$ or $\mathbb{Z}[\sqrt{2}]$). Quadratic forms arise in many areas of number theory, with binary quadratic forms being among the oldest and most important. At PROMYS, one question we study is what numbers can be written as $Q(x, y)$ for some choices of x and y (e.g. when $Q(x, y) = x^2+y^2$).

In the quadratic formula, we first learn about the **discriminant** $\Delta_Q := b^2 - 4ac$ of $Q(x, y)$. It turns out that this is an **invariant** of Q, meaning that if we perform an invertible linear change of variables to get some quadratic form Q' (i.e. $x := a_1x' + a_2y'$ and $y := b_1x' + b_2y'$ for some $a_1, a_2, b_1, b_2 \in R$ and this can be undone by a similar substitution) then $\Delta_{Q'} = \Delta_Q$.

One of the most classical questions about binary quadratic forms is to know how many of them there are of a given discriminant (up to invertible linear change of variables). This question was first asked by Gauss, who made extensive tables of **positive definite** binary quadratic forms, meaning those where both $a > 0$ and $c > 0$. He used these tables to conjecture that there are only 9 discriminants having exactly one positive definite binary quadratic form, and it turns out that this can be reinterpreted as saying that there are only 9 quadratic fields $\mathbb{Q}(\sqrt{d})$ with $d < 0$ whose integers have unique prime factorization. To perform this counting, Gauss defined a notion of a "reduced" quadratic form and showed that by an invertible linear change of variables we can always exchange a quadratic form for a unique reduced one, and then he counted these reduced forms. This circle of ideas goes by the name of **"reduction theory"**.

The following two projects focus on trying to understand the reduction theory of binary quadratic forms over the integers and over the number system $\mathbb{Z}[\sqrt{2}]$.

1) Reduction by Conway Topographs – Recently a new approach to reduction theory of binary quadratic forms over $\mathbb{Z}$ has been introduced by John Conway that can be computed purely pictorally in terms of a certain branching tree in the plane (called a **topograph**) associated to a binary quadratic form Q that illustrates what happens to Q as we perform (all) invertible linear changes of variables. The important structures in this picture are referred to somewhat whimsically as "lakes", "rivers", "valleys", but these simple pictures carry a lot of information and can be used to prove some very important theorems about binary quadratic forms.

For our purposes, we would like to use these pictures to give a "reduction theory" for binary quadratic forms. This project will focus on working with Conway topographs to see why they work so effectively to understand binary quadratic forms over $\mathbb{Z}$, and then to try to generalize these topographs toinderstand binary quadratic forms over $\mathbb{Z}[\sqrt{2}]$. This will involve a careful study of the kinds of invertible linear changes of variables are possible over $\mathbb{Z}[\sqrt{2}]$, and how closely related these different kinds of changes of variables can be. This will involve generalzing Conway's notions of "superbases" and "lax bases" (defined over $\mathbb{Z}$) to $\mathbb{Z}[\sqrt{2}]$.

The primary reference for this project is Chapter 1 of Conway's book [1, pp1-26].

2) Reduction by Voronoi Domains – There is a more systematic way of establishing a "reduction theory" for quadratic forms due to Voronoi that is known to produce a definition of reduced quadratic forms quite generally in terms of a system of inequalities on the coefficients a, b, c of a quadratic form Q. This is similar to the definition of reduced form $0 \leq |b| \leq a \leq c$ used by Gauss, but this approach makes use of certain notions of "perpendicular" (i.e. inner products) in higher dimensional (vector) spaces, and some related ideas about vectors and matrices that are part of the subject of "linear algebra". Once these ideas are understood, this theory should give a very explicit notion of reduced forms in terms of a system of inequalities. It would be interesting to know what these look like, and to try to use them to make a table of all (totally positive definite) quadratic forms of any given discriminant.

The primary reference for this project is Chapter 3.1 of [2, pp45-54].

For both of these projects, having a good notion of "reduced form" should allow one to make a conjecture similar to Gauss's for which discriminants have only one (totally) positive definite binary quadratic form up to invertible linear change of variables, but for $\mathbb{Z}[\sqrt{2}]$ instead of $\mathbb{Z}$.

2. Background Information

Quadratic forms and Quadratic lattices – A useful perspective for studying binary quadratic forms up to invertible linear change of variables is given by "quadratic lattices". We say that L is a **(binary) quadratic lattice** which is the fixed lattice $\mathbb{Z}^2$ in the plane $\mathbb{R}^2$ where we label each of the lattice points $(x, y) \in \mathbb{Z}^2$ with the numbers $Q(x, y)$ given by evaluating the quadratic form at that point. Conversely we can recover the quadratic form $Q(x, y) = ax^2 + bxy + cy^2$ from L by noticing that $a = Q(1, 0)$, $c = Q(0, 1)$, and $Q(1, 1) = a + b + c$. (Because of this, when talking about L we will often refer to the values at various points in terms of Q even though the quadratic form may not be explicitly given as a polynomial.)

From the perspective of vectors we can think of this description of Q in terms of L as coming from a way of expressing every vector $\vec{v} \in L$ in terms of an x-direction $\vec{e}_1 := (1, 0)$ and a y-direction $\vec{e}_2 := (0, 1)$, since we can any $\vec{v} := (x, y) \in L$ as

$$\vec{v} = (x, y) = (x, 0) + (0, y) = x\vec{e}_1 + y\vec{e}_2, \tag{1}$$

and that $Q(\vec{v}) = Q(x, y) = Q(x\vec{e}_1 + y\vec{e}_2)$. Since this description of L in terms of two given vectors is what is really important here, we say that a pair of vectors $\mathcal{B} := \{\vec{v}_1, \vec{v}_2\}$ is a **basis** for $\mathbb{Z}^2$ if $\vec{v}_1, \vec{v}_2 \in \mathbb{Z}^2$ and every $\vec{v} \in \mathbb{Z}^2$ can be expressed uniquely as an $\mathbb{Z}$-linear combination of these two vectors (which is exactly what equation (1) says). For any basis $\mathcal{B}$ of the quadratic lattice L, we can associate a quadratic form $Q_{\mathcal{B}}(x, y)$ by the description

$$Q_{\mathcal{B}}(x, y) := Q(x\vec{v}_1 + y\vec{v}_2),$$

and we can solve for the coefficients of $Q_{\mathcal{B}}(x, y) = ax^2 + bxy + cy^2$ in terms of the values of Q at $\vec{v}_1, \vec{v}_2$, and $\vec{v}_1 + \vec{v}_2$ (i.e. $a = Q(\vec{v}_1), c = Q(\vec{v}_2)$, and $b = Q(\vec{v}_1 + \vec{v}_2)$).

The real advantage of looking at (binary) quadratic lattices is that they keep track of equivalent quadratic forms. To see this, suppose that we have a linear change of variables

$$x := a_1x' + a_2y' \qquad y := b_1x' + b_2y'$$

which can be written in matrix language as

$$\vec{v} := \begin{bmatrix} x \\ y \end{bmatrix} = \underbrace{\begin{bmatrix} a_1 & a_2 \\ b_1 & b_2 \end{bmatrix}}_{A:=} \underbrace{\begin{bmatrix} x' \\ y' \end{bmatrix}}_{\vec{v}\,':=} = A\vec{v}\,'.$$

These matrices (and the matrices A^{-1} of their inverse transformation) have integer coefficients, and it is interesting to see how this linear transformation affects our description of the quadratic lattice L. Suppose we have a quadratic form $Q_{\mathcal{B}}$ associated to some basis $\mathcal{B}$ (which could be our standard basis $\{\vec{e}_1, \vec{e}_2\}$). Then one can show that the linear transformation A will carry $Q_{\mathcal{B}}$ to another quadratic form $Q_{\mathcal{B}'}$ where $\mathcal{B} = A\mathcal{B}' := \{A\vec{v}_1', A\vec{v}_2'\}$, or equivalently $\mathcal{B}' := A^{-1}\mathcal{B}$.

Saying this more concisely, from this perspective we see that quadratic forms equivalent to Q are given exactly as quadratic forms $Q_{\mathcal{B}}$ associated to different choices of basis for the quadratic lattice L. Therefore,

Lemma 2.1. *A quadratic form $Q(x, y)$ is a quadratic lattice L, together with a choice of basis $\mathcal{B}$ for L. Equivalent quadratic forms arise from different choices of basis on a fixed quadratic lattice.*

Superbases and Lax objects – For the project on Conway topographs, it is important to understand a more elementary way of passing between various bases $\mathcal{B}$. As we have seen, we can get from one basis to another by an invertible linear change of variables, but this doesn't really give us a good way of saying which bases are close to each other. Conway's approach to this way of moving between different bases is to say which bases are "adjacent" to each other, more or less. More precisely, to simplify the picture he thinks of vectors where he doesn't distinguish between a vector $\vec{v}$ and its negative $-\vec{v}$, and any object where we identify vectors with their negatives is called a **lax** object. So for instance we can talk about a vector $\vec{v}$, or a **lax vector** $\pm\vec{v}$. In this spirit, he doesn't consider bases but instead considers **lax bases** of the form $\{\pm\vec{v}_1, \pm\vec{v}_2\}$ where $\{\vec{v}_1, \vec{v}_2\}$ is a basis. Notice that a lax basis is not really that different from a basis because any choice of signs in a lax basis will give a basis.

To connect two bases, Conway defines a **(lax) superbasis** as a triple of lax vectors $\{\pm\vec{v}_1, \pm\vec{v}_2, \pm\vec{v}_3\}$ where every pair of lax vectors forms a lax basis for $\mathbb{Z}^2$. His main observation about how superbases and bases are related is what allows one to draw the topograph picture:

Theorem 2.2. *Every superbase contains exactly three lax bases, and every lax basis* $\mathcal{B} = \{\pm\vec{v}_1, \pm\vec{v}_2\}$ *appears in exactly two superbases*

$$\mathcal{S}_+ := \{\pm\vec{v}_1, \pm\vec{v}_2, \pm(\vec{v}_1 + \vec{v}_2)\} \quad \textit{and} \quad \mathcal{S}_- := \{\pm\vec{v}_1, \pm\vec{v}_2, \pm(\vec{v}_1 - \vec{v}_2)\}.$$

Conway describes the geometry of lax bases and superbases by an infinitely branching tree in the plane (but we don't draw the whole thing – we only draw the part we are interested in at any given moment!). He represents the superbases as vertices (points), and he joins two points by an edge if they share a lax basis. From Theorem 2.2 we can see that at most one edge joins any two vertices, and each vertex has exactly three edges coming out of it. By organizing the three edges properly, one can label the regions in the plane that do not cross the topograph with (lax) vectors $\vec{v}$ appearing in the lax bases that the region borders.

The connection to quadratic forms comes by relabelling the regions above (labelled by $\pm v$) by the value $Q(\pm_v)$, which does not depend on the choice of $\pm$. Once any three regions touching a given superbasis are labelled by their values, then one can quickly work out the values of regions adjacent to any two known regions. By moving to an edge on the topograph where the values in adjaecnt regions are minimal, we can define a "reduced" positive definite quadratic form equivalent to the given one, and by studying the possible labellings of regions around a minimal edge one can enumerate all positive definite quadratic forms of a give discriminant.

Warmup Questions:

(1) What is the relation between the topograph and the discriminant of the associated quadratic form?
(2) Suppose that the values of all regions adjacent to a superbasis are known. What is the rule that allows us to fill in the values of unknown region adjacent to any adjacent superbasis?
(3) What is the reduced form associated to $109x^2 + 140xy + 45y^2$?

Perfect forms – The Voronoi theory of reduction is related to Conway's topographs, but takes a somewhat different approach that does not assume anything about the structure of bases for $\mathbb{Z}^2$. Instead it is based on the theory of "perfect" quadratic forms (which has no relation to perfect numbers!) that are a particularly symmetric kind of quadratic forms. We say that a quadratic form $Q(x, y)$ is **perfect** if it is uniquely determined (up to equivalence) by the length of its shortest vector (i.e. the minimal non-zero value). Over $\mathbb{Z}$, there is a unique perfect form of minimal length 1 (up to equivalence). This form is determined by its three minimal lax vectors, and can be written as $x^2 + xy + y^2$ if we take these minimal vectors to be $\vec{e}_1, \vec{e}_2$, and $\vec{e}_1 + \vec{e}_2$. In general, one can check the existence of a perfect form with any given set of minimal vectors by solving a system of linear equations.

The geometry of perfect forms and their relation to the space of positive definite quadratic forms is given in [2, Section 3.1.3, p47].

Once a perfect for is known, one can use it to look for other perfect forms "adjacent" to it in a way very similar to what was done for the Conway topograph. We do this by fixing all but one of the minimal (lax) vectors, and varying the remaining one to obtain a new perfect form. It is a theorem of Voronoi that there are only finitely many perfect forms (up to equivalence, and for a given dimension), and this algorithm allows one to enumerate all of them. This enumeration is the key to writing down explicit inequalities giving an explicit reduction theory, and is described in [2, Section 3.1.8, pp53-4].

Warmup Questions:

(1) Show that $x^2 + xy + y^2$ is the unique binary quadratic form with minimal vectors $\vec{e}_1, \vec{e}_2$, and $\vec{e}_1 + \vec{e}_2$ having length 1.
(2) Use Conway's topograph to show that there is a unique perfect binary quadratic form of any given minimum $m > 0$ up to equivalence.
(3) Can you find a perfect quadratic form in 3 variables?

References

[1] John H. Conway. *The sensual (quadratic) form*, volume 26 of *Carus Mathematical Monographs*. Mathematical Association of America, Washington, DC, 1997. With the assistance of Francis Y. C. Fung.
[2] Achill Schürmann. Computational geometry of positive definite quadratic forms – theory, algorithms, applications, http://fma2.math.uni-magdeburg.de/ achill/public/habil.pdf, 2008.