MASSER'S CONJECTURE ON EQUIVALENCE OF INTEGRAL QUADRATIC FORMS

HAN LI

All work is joint with G.A. Margulis.

1. Introduction

We would like to study integral quadratic forms through homogeneous dynamics.

Consider a quadratic form $Q(z) = \sum_{1\leq i,j\leq n} b_i\dot{\gamma} x_i x_j = x^t Bx$ we say $Q(z)$ is *integral* if $B \in \mathbb{Z}^{n\times n}$. Let $A, B \in \mathbb{Z}^{n\times n}$ be symmetric and non singular.

Definition 1. We say A and B are *integrally equivalent*, denoted $A \overset{\mathbb{Z}}{\sim} B$ if there exists $\gamma_0 \in \mathrm{GL}(n,\mathbb{Z})$ such that $A = \gamma_0^t B\gamma_0$.

The main question we want to consider is: Given A, B decide whether $A \overset{\mathbb{Z}}{\sim} B$, and if they are, can we effectively find a γ_0, (i.e. is this possible using only a finite number of operations, or does there exists a procedure that terminates in finite time).

1.1. Massur's Conjecture.

Conjecture 1 (Masser)**.** *For all $n \geq 3$, there exists $c_n, d_n > 0$ satisfying the following properties, if $A = \gamma_0^t B\gamma_0$ with $\gamma_0 \in GL(n,\mathbb{Z})$, then there exists $\gamma \in GL(n,\mathbb{Z})$ such that $A = \gamma^t B\gamma$ and $\|\gamma\| < c_n(\|A\|\cdot\|B\|)^{d_n}$.*

This conjecture provides a *search bound* for the main question, given A and B we can find all the matrices that satisfy the bound, there are only finitely many of these, if we find one that satisfies the equivalence property, then we are done, if not, the conjecture would tell us that we can stop and A and B are not equivalent.

In 1972, Siegel wrote a paper which proved that for each given A, B, there exists a search bound and gave a procedure to find this search bound. Massur and his students then tried to make this explicit. Following Siegel's method, Staurmann was able to show that for $n \geq 2$, $\|\gamma\|, \exp(c_n(\|A\|\cdot\|B\|)^{n^3})$. For $n = 2$ exponential bounds are sharp. Dietmann showed that for $n = 3$, the conjecture is true with $d_3 = 231$. He also managed to prove that for special classes of integral quadratic forms in any variable with $n \geq 4$ you do have polynomial search bounds. The general question still remained open.

Example 1 (Why exponential bounds are sharp for $n = 2$)**.** $x^2 - 631y^2 = 1$, we have the trivial solution $(\pm 1, 0)$, and we have some other non-trivial solutions (u, v). For any of these non-trivial solutions, $|v| > 10^22$. This type of equation should be the only exception to getting polynomial bounds.

2. Main result

Theorem 1 (Li-Margulis)**.** *For all $n \geq 3$, there exists $c_n > 0$ such that if $A = \gamma_0^t B\gamma_0$ with $\gamma_0 \in GL_n(\mathbb{Z})$ then there exists $\gamma \in GL_n(\mathbb{Z})$ such that $A = \gamma^t B\gamma$ and $\|\gamma\| < c_n(\|A\|\cdot\|B\|)^{n_3}$.*

We will prove a simpler version of this theorem. Let $G = \mathrm{SL}(n,\mathbb{R})$, and $\Gamma = \mathrm{SL}(n,\mathbb{Z})$. We know that $\|ab\| \ll \|a\|\cdot\|b\|$ and $\|a^{-1}\| \ll |\det(a)|^{-1}\|a\|^{n-1}$ (Cramer's rule).

Theorem 2 (Li-Margulis)**.** *For all $n \geq 3$, if $A = \gamma_0^t B\gamma_0$ with $\gamma_0 \in \Gamma$, then there exists $\gamma \in \Gamma$ such that $A = \gamma^t B\gamma$ and $\|\gamma\| \ll (\|A\|\cdot\|B\|)^{n_3}$.*

Date: February 02, 2015.

Proof. First we try to show that there exists $g \in G$ that solves, $A = g^t B g$ and we show that $\|g\|$ is small. Then we try to show that there exists an integral solution that is not too far from the real solution, and thus, is also small.

Step 1: Let (p, q) be the signature of A and B, they have the same signature since they are equivalent over the real numbers. Let $X_0 = \begin{pmatrix} I_p & \\ & I_q \end{pmatrix}$. Claim: There exists $g_A \in G$ such that $|\det A|^{-\frac{1}{n}} A = g_A^t X_0 g_A$ and $\|g_A\| \ll \|A\|^{\frac{1}{2}}$. Assume A is a binary form of signature $(1, 1)$, then it can be written in the form

$$k^t \begin{pmatrix} \lambda & \\ & -\mu \end{pmatrix} k = k^t \begin{pmatrix} \sqrt{\lambda} & \\ & \sqrt{\mu} \end{pmatrix} \begin{pmatrix} 1 & \\ & -1 \end{pmatrix} \begin{pmatrix} \sqrt{\lambda} & \\ & \sqrt{\mu} \end{pmatrix} k$$

where k is symmetric, and λ, μ are its eigenvalues with $\lambda\mu = 1$. So $g_A = \begin{pmatrix} \sqrt{\lambda} & \\ & \sqrt{\mu} \end{pmatrix} k$

Similarly, there exists $g_B \in G$ such that $|\det B|^{1\frac{1}{n}} B = g_B^t X_0 g_B$ and $\|g_B\| \ll \|B\|^{\frac{1}{2}}$.

Thus our small real solution is $A = g_A^t (g_B^r)^{-1} B g_B^{-1} g_A$.

Step 2: Translate the problem into dynamical terms. Claim: $H g_A \Gamma = H g_B \Gamma \subseteq G$ where $H = \{h \in G \mid h^t X_0 h = X_0\} = \mathrm{SO}(p, q)$. Proof: $g_A^t X_0 g_A = \gamma_0^t g_B^t X_0 g_B \gamma_0 \Rightarrow g_b \gamma_0 g_A^{-1} \in H \Rightarrow H g_B \gamma_0 g_A^{-1} = H \Rightarrow H g_B \Gamma = H g_A \Gamma$. View $g_A\Gamma, g_B\Gamma \in G/\Gamma$, $H g_A \Gamma = H g_B \Gamma \subseteq G/\Gamma$. Recall that H acts on G/Γ by left translations. The claim says that $g_A\Gamma$ and $g_B\Gamma$ lie on the same orbit of H because they are integrally equivalent. Therefore there exists $h \in H$ such that $h g_A \Gamma = g_B \Gamma$. Take $\gamma = g_B^{-1} h g_A \in Gamma$ and $A = \gamma^t B \gamma$. We now want to find what the smallest element h is that would translate one element to the other. As long as we can find a polynomial bound for h, we are done.

Step 3: We have that the orbit $H g_A \Gamma = H/\Gamma_A$, if A is integral then Γ_A is a lattice in H. For example $H = \mathrm{SO}(1, 2)$, Γ_A a Fuchsian group. Fix Haar measure (H, vol), this induces a Haar measure on the quotient $(H g_A \Gamma, \mathrm{vol})$. The total measure $V = \mathrm{vol}(H g_A \Gamma) = \mathrm{covol}(\Gamma_A)$ in H.

The theorem will then follow from the following two dynamical results. □

Theorem 3. *There exists $h \in H$ such that $h g_A \Gamma = g_B \Gamma$ and $\|h\| \ll [V(\|g_A\| \cdot \|g_B\|)^*]^{13/5}$ where $* = n\left(1 + \frac{\dim H}{2}\right)$.*

Theorem 4. $V \ll |\det A|^{\frac{\dim G - \dim H}{n}}$

Proof of Thm. 3. Recall that our orbit $H g_A \Gamma$ is a homogeneous manifold. We want to know what is the smallest element that moves the point $g_A\Gamma$ to $g_B\Gamma$. Define the following flow

$$a_t = \begin{pmatrix} \cosh t & & \sinh t \\ & I_{n-2} & \\ \sinh t & & \cosh t \end{pmatrix}.$$

Consider a cube in $H g_A \Gamma$, under a_t the cube will become very thing and very long. Take a ball, v_A, containing $g_A\Gamma$ and a ball, v_B, $g_B\Gamma$. Translate v_A by a_t, when t is large, $a_t v_A \cap v_B \neq \emptyset$. We want to know what balls v_A, v_B do we choose, and at what time t does this happen? To answer this question we use quantitative mixing.

Theorem 5. *For all $\varphi, \psi \in C_c^\infty(H g_A \Gamma)$, we have*

$$|\langle a_t \varphi, \psi \rangle - \int \varphi \, d\mu \int \psi \, d\mu| \ll e^{-\frac{5}{13}t} \|\varphi\|_{sob} \|\psi\|_{sob}$$

where $\mu = \frac{1}{V} vol$ and $\|\varphi\|_{sob} = \|\varphi\|_{L^2(\mu)} + \sum_{\mathcal{D}} \|\mathcal{D}\varphi\|_{L^2(\mu)}$.

To apply this theorem, we take φ and ψ with $\mathrm{supp}(\varphi) \subseteq v_A$ and $\mathrm{supp}(\psi) \subseteq v_B$, such that $\int \varphi \, \mathrm{d}\mu = \frac{1}{V}$, $\int \psi \, \mathrm{d}\mu = \frac{1}{V}$, $\|\varphi\|_{\mathrm{sob}} \ll \frac{1}{\sqrt{v}} \|g_A\|^*$, and $\|\psi\|_{\mathrm{sob}} \ll \frac{1}{V} \|g_B\|^*$. If $\langle a_t \varphi, \psi \rangle \neq 0$ then $\mathrm{supp}(a_t \varphi) \cap \mathrm{supp}(\psi) \neq \emptyset$. This implies that $a_t v_A \cap v_B \neq \emptyset$. We want to know at what time t this happens. The critical point happens when

$$\int \varphi \, \mathrm{d}\mu \int \psi \, \mathrm{d}\mu = e^{-\frac{5}{13}t} \|\varphi\|_{\mathrm{sob}} \|\psi\|_{\mathrm{sob}}$$

so

$$\frac{1}{V^2} = e^{-\frac{5}{13}t}\frac{1}{V}(\|g_A\|\|g_B\|)^*$$

rearranging, we get

$$e^t = [V(\|g_A\|\|g_B\|)^*]^{\frac{13}{5}}$$

□

To prove Thm 5, we fix $\mathrm{SO}(1,2) \subseteq \mathrm{SO}(p,q)$, by the Buger-Sarnak restriction principle, we are still looking at an automorphic form. We have to be a little careful though. For example if you have $x_1^2 + \cdots x_p^2 - y_1^2 - \cdots - y_q^2$, we look at $\mathrm{SO}(1,2) \curvearrowright \mathrm{SO}(p,q)/\Gamma_A$, when you change the quadratic form the structure gets twisted and it might not be a $\mathbb{Q}$ subgroup. The Witt extension theorem says that if we look at the set $\{V \subseteq \mathbb{R}^n \mid \dim = 3, Q_0|_V \text{ has signature } (1,2)\}$ then the $\mathrm{SO}(p,q)$ action on this space is transitive.