A COMPUTATIONAL APPROACH TO CALCULATING COEFFICIENTS FOR TWISTS OF SIEGEL PARAMODULAR FORMS

BEAU HORENBERGER AND KERP BROGGLI

ABSTRACT. This paper details the methodologies and proofs involved in calculating the coefficients for twists of Siegel paramodular forms. We will discuss the algorithmic method as well as the proofs used to increase efficiency of the algorithm. The format will be broken in to the cases of the twist theorem, and then into algorithm and proof sections.

1. SCRATCH WORK (FOR COPYPASTA)

The modular group, Γ, is the group of integral linear fractional transformations of the complex upper half plane (complex numbers with complex parts greater than or equal to zero) onto itself. We consider these transformations as matrices, M, with mappings as follows:

$$M = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$$

where $\alpha\delta - \gamma\beta = 1$

$$z \mapsto \frac{\alpha z + \beta}{\gamma z + \delta}$$

The operation on these transformations is composition. Note that this set of matrices is isomorphic to $SL(2, \mathbb{Z})$. For references on the modular group, see [?].

A modular form of weight k is a function f on the upper-half plane, H, satisfying three conditions:

(1) f is holomorphic (and thus infinitely differentiable) on H
(2) $\forall z \in H$ and for all matrices in $SL(2, \mathbb{Z})$,

$$f\left(\frac{\alpha z + \beta}{\gamma z + \delta}\right) = (cz + d)^k f(z)$$

(3) f is holomorphic as $z \to i\infty$

Siegel modular forms are essentially multivariable modular forms, and they are conjecturally related to algebraic structures. Where modular forms map from the upper-half plane to the upper-half plane, Siegel modular forms map from the Siegel upper-half space,

$$\mathcal{H}_g = \{\tau \in M_{g \times g}(\mathbb{C}) | \tau^T = \tau, Im(\tau) \text{ positive definite}\}$$

to a complex vector space. These forms have Fourier expansions as well,

$$F(Z) = \sum_{S \in A(N)^+} a(S)e^{2\pi i tr(SZ)}$$

for $Z \in \mathcal{H}_2$. Note the index of the sum is $A(N)^+$, the set of all 2×2 matrices S of the form

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \quad \alpha \in N\mathbb{Z}, \quad \gamma \in \mathbb{Z}, \quad \beta \in \frac{1}{2}\mathbb{Z}, \quad \alpha > 0, \text{and } \alpha\gamma - \beta^2 > 0$$

And N is the paramodular level of F.

2. GENERAL METHODS

The methodology for creating this algorithm centers on the available data. Through LMFDB, we have collections of coefficients for Siegel modular forms.

$$F(Z) = \sum_{S \in A(N)^+} a(S)e^{2\pi i tr(SZ)}$$

Thus, we are interested in taking this data, picking an arbitrary prime p, and using these to discover coefficients for the respective twist,

$$T_\chi(F)(Z) = \sum_{S' \in A(Np^4)^+} W(\chi)a_\chi(S')e^{2\pi i tr(S'Z)}$$

Dr. Johnson-Leung's paper describes methods for taking some quantity of $a(S)$ coefficients from the original form and calculating a $a_\chi(S')$ for the twisted form. In order to make this algorithmic, our general goal is to take all $a(S)$ from the available data for a particular form and determine which subsets of these can generate some $a_\chi(S')$ given a prime p. Then, we generate S' and its respective $a_\chi(S')$ from the data using the methods in Dr. J's paper.

3. NOTATION

3.1. $A(N)^+$ is the set of all 2×2 matrices S

$$S = \begin{bmatrix} \alpha & \beta \\ \beta & \gamma \end{bmatrix}, \quad \alpha \in N\mathbb{Z}, \quad \gamma \in \mathbb{Z}, \quad \beta \in \frac{1}{2}\mathbb{Z}, \quad \alpha > 0, \quad \det\begin{bmatrix} \alpha & \beta \\ \beta & \gamma \end{bmatrix} = \alpha\gamma - \beta^2 > 0$$

3.2. For S and A 2×2 matrices with A invertible,
$S[A] := A^t S A$
$S[A]^{-1} := A^{-t} S A^{-1}$

4. QUESTIONS

4.1. Is S[A] Well Defined. If we let $A = \begin{bmatrix} 1 & -bp^{-1} \\ & p \end{bmatrix}$, we would like to know if $S, T \in A(N)^+$ and S is properly equivalent to T, is S[A] properly equivalent to T[A]? It is also important to explore if this holds under gamma equivalency as well.

4.2. Also, a weaker but still computationally important question is when S is equivalent to T, does $a(S[A]) = a(T[A])$? Surely, if we had Question 4.1 this would follow since equivalent forms give index equal coefficients.

5. Case 1

Our approach to Case 1 revolved around limiting the conditions under which coefficients for a Siegel modular form collected in the LMFDB database might correlate to coefficients in a twist of that Siegel modular form. Particularly, case one has the form

$$a_\chi(S') = p^{1-k}\chi(2\beta) \sum_{b \in (\mathbb{Z}/p\mathbb{Z})} \chi(b)a(S'[\begin{bmatrix} 1 & -bp^{-1} \\ 0 & p \end{bmatrix}])$$

where $a_\chi(S')$ with $S' = \begin{bmatrix} \alpha & \beta \\ \beta & \gamma \end{bmatrix}$ and $p \nmid 2\beta$ and $p^4|\alpha$

Since we have values of S for the parent Siegel modular form, we will determine the new coefficient using

$$\sum_{b \in (\mathbb{Z}/p\mathbb{Z})} \chi(b)a(S'[\begin{bmatrix} 1 & -bp^{-1} \\ 0 & p \end{bmatrix}]$$

. Specifically, we calculate the inverse of the Bonnie operator, $S[X]$, given our values of S and an arbitrary $b \in (\mathbb{Z}/p\mathbb{Z})$. This returns a respective S' that would use our S. Formally,

$$(S[\begin{bmatrix} 1 & -bp^{-1} \\ 0 & p \end{bmatrix}]^{-1}) = \begin{bmatrix} x & (bx+py)/p^2 \\ (bx+py)/p^2 & (b^2x+2bpy+p^2z)/p^4 \end{bmatrix} = S'$$

$$\text{for } S = \begin{bmatrix} x & y \\ y & z \end{bmatrix}]$$

So, one of the most important questions is when a given S will correspond to an S' with integer values. This is the primary motivation for the methods to follow, which limit the S values that could possibly be used in case 1 based on divisibility conditions for S' to be integer-valued. Once all of the candidate S values are paired with their respective S' values for a given b, we can finally calculate $a_\chi(S') = p^{1-k}\chi(2\beta) \sum_{b \in (\mathbb{Z}/p\mathbb{Z})} \chi(b)a(S'[\begin{bmatrix} 1 & -bp^{-1} \\ 0 & p \end{bmatrix}])$ for any S' which has an S for each value of b.

5.1. Proofs.

5.1.1. *Properties of $P^1(\mathbb{Z}/n\mathbb{Z})$.*
$([a], [b]) \not\sim ([x], 1)$ for some $[x] \in \mathbb{Z}/n\mathbb{Z} \iff [b]$ is not invertible
$([a], 1) \sim (1, [b]) \implies [a]^{-1} = [b]$
$([a], 1) \sim ([b], 1) \iff [a] \equiv [b]$
$([a].[b]) \sim ([b], [a])$

3

5.1.2. $[\Gamma : \Gamma_0(n)] = n \cdot \prod_{p|n}\left(1 + \frac{1}{p}\right).$

First we will show that $\Gamma : \Gamma_0(n) \cong P^1(\mathbb{Z}/n\mathbb{Z})$ blah blah blah

5.1.3. Let $n \in \mathbb{Z}$, write the prime factorization of n as $p_1^{k_1} p_2^{k_2}...p_m^{k_m}$ where $k_i \in \mathbb{N}$ for $1 \le i \le m$ and $p_i = p_j$ implies $i = j$.

Define $\pi : P^1(\mathbb{Z}/n\mathbb{Z}) \to P^1(\mathbb{Z}/p_1^{k_1}\mathbb{Z}) \times P^1(\mathbb{Z}/p_2^{k_2}\mathbb{Z}) \times ... \times P^1(\mathbb{Z}/p_m^{k_m}\mathbb{Z})$

by $\pi(([a]_n, [b]_n)) = [([a]_{p_1^{k_1}}, [b]_{p_1^{k_1}}), ([a]_{p_2^{k_2}}, [b]_{p_2^{k_2}}), ..., ([a]_{p_m^{k_m}}, [b]_{p_m^{k_m}})]$

Well defined

let $([a], [b]) \in P^1(\mathbb{Z}/n\mathbb{Z})$. Then for $\lambda \in (\mathbb{Z}/n\mathbb{Z})^\times$ $([a],[b]) \sim \lambda([a],[b])$.

$\pi(([a], [b])) = [([a]_{p_1^{k_1}}, [b]_{p_1^{k_1}}), ([a]_{p_2^{k_2}}, [b]_{p_2^{k_2}}), ..., ([a]_{p_m^{k_m}}, [b]_{p_m^{k_m}})]$

$\pi(\lambda([a], [b])) = [([\lambda a]_{p_1^{k_1}}, [\lambda b]_{p_1^{k_1}}), ([\lambda a]_{p_2^{k_2}}, [\lambda b]_{p_2^{k_2}}), ..., ([\lambda a]_{p_m^{k_m}}, [\lambda b]_{p_m^{k_m}})]$

$\pi(\lambda([a], [b])) = [\lambda([a]_{p_1^{k_1}}, [b]_{p_1^{k_1}}), \lambda([a]_{p_2^{k_2}}, [b]_{p_2^{k_2}}), ..., \lambda([a]_{p_m^{k_m}}, [b]_{p_m^{k_m}})]$

So $\pi(([a], [b])) \sim \pi(\lambda([a], [b]))$

Well Defined part 2 eclectic boogaloo

Let $([a], [b]) \in P^1(\mathbb{Z}/n\mathbb{Z})$ and suppose $[a] = [c]$ and $[b] = [d]$. Then they remain equal under change of modulus in π since $p_i^{k_i}|n$ for $1 \le i \le m$

1-1

spose $\pi(a, b) = \pi(c, d)$, by uniqueness in chinese remainder thm (a,b)=(c,d).

onto

spose we got some element of the direct product business. then by chinese remaineder thm we have and element in $(Z/nZ)^2$ call it (r,s). if gcd of r and s is not 1 then it does not divide n.

certainly if it did, it would be divisible by some power of a prime dividing n say $(p_j)^{(}f)$ where it doesnt maximally divide n (otherwise would send to (0,0) for that modululs). when sent to the modulus of $p_j^{k_j}$

5.1.4.

Claim:

Let S be a binary quadratic form such that $S = \begin{bmatrix} x & y \\ y & z \end{bmatrix}$ with discriminant D

such that $p^4|x$ and $p \nmid 2(bx+py)/p^2$, $S' = (S[\begin{bmatrix} 1 & -bp^{-1} \\ 0 & p \end{bmatrix}]^{-1}) = \begin{bmatrix} x & (bx + py)/p^2 \\ (bx + py)/p^2 & (b^2x + 2bpy + p^2z)/p^4 \end{bmatrix}.$

Then S' is integer-valued $\implies p^2||D$ and $p \nmid z$

Proof:

Assume S' is integer-valued. There are three parts to this proof: proving $p||y$, proving $p \nmid z$, and then proving from these and that $p^4|x$ that it follows $p^2||D$. First, since S' is integer-valued, $p^2|(bx + py)$. Since $p^4|x$, we say $x = qp^4$. Then $p^2|bqp^4 + py$, so $p|bqp^3 + y$. It follows that $p|y$. Next, since $p \nmid \beta = 2((bx + py)/p^2)$, it follows by the same logic as above (since $p > 2$) that $p \nmid y/p$, and then $p|y \implies p||y$.

Next, we show $p \nmid z$. Since $p^4|(b^2x + 2bpy + p^2z)$, we substitute $x = qp^4$ and $y = rp$. Then $p^4|(b^2qp^4 + 2bp^2r + p^2z) \implies p^2|b^2qp^2 + 2br + z$. Then, this implies $p^2|2br + z$. but since

4

$p \nmid b, 2, r$, this can only be true if $p \nmid z$.

Finally, we use these conditions on $D = (2y)^2 - 4xz$. Since $p|y$ and $p^4|x$, we have $p^2|(2y)^2 - 4xz$. But $p^2||(2y)^2$, so it follows $p^2||D$ $\qquad\square$

Claim:

Let S be a binary quadratic form such that $S = \begin{bmatrix} x & y \\ y & z \end{bmatrix}$ with discriminant D such that $p^4|x$, $p||y$, and $p \nmid z$. Then there exists a binary quadratic form $\begin{bmatrix} x' & y' \\ y' & z' \end{bmatrix}$ with discriminant D such that $p||y'$, $p \nmid z'$, and $x' = p^n$ for some $n \in \mathbb{N}$.

Proof:

Suppose we have a binary quadratic form $S = \begin{bmatrix} x & y \\ y & z \end{bmatrix}$ with discriminant D such that $p^4|x$, $p||y$, and $p \nmid z$. Then $D = y^2 - 4xz$. If $x = p^n$, we are done. Otherwise, let $x = p^n * c$, where $p^n||x$. Then $D = y^2 - 4p^n cz$. Now let $y' = y$, $x' = p^n$, and $z' = cz$. Then we have $p||y'$, $p \nmid z'$, and $x' = p^n$, as desired. $\qquad\square$

5.2. Algorithm. For Case 1, the algorithm is as follows:

Algorithm 1 Coefficient Calculator

1: **procedure** CALCCOEFFICIENTS
2:     $ParentData \leftarrow$ Coefficients and Reduced BQF's Sorted by Discriminant D
3:     $Solutions = []$
4:     **for** $D \in ParentData$ **do**
5:         **if** $p^2||D$ **then**
6:             $x \leftarrow p^4$
7:             **for** $b : 1 \leq b < p$ **do**
8:                 **for** $y : 1 \leq y < i$ **do**
9:                     **if** $p \nmid y$ **and** $(-4x)|(D - (yp)^2)$ **then**
10:                         $z = (D - (yp)^2)/(-4x)$
11:                         **if** $p \nmid z$ **then**
12:                             S' $\leftarrow$ InverseBonney$((x, yp, z), b)$
13:                             $OldCoeff \leftarrow ParentData.D.$Reduce$(x, yp, z).Coeff$
14:                             **if** S' not in $Solutions$ **then**
15:                                 $Solutions \leftarrow S'$
16:                             **if** $OldCoeff$ not in $Solutions.S'$ **then**
17:                               $Solutions.S' \leftarrow ((x, yp, z), OldCoeff, b)$
18:     **for** $S' \in Solutions$ **do**
19:         **if** len$(Solutions.S') == p$-1 **then**
20:             CalcCoeff$(Solutions.S')$

TO DO: Define reduction function, InverseBonney,and CalcCoeff function ADAPT AL-GORITHM TO INCORPORATE PROOF 2 WHERE $x = p^n$. Search a range of values of n?

5.3. Questions about Case 1. For the given sample data, the above conditions do not seem exact to the extent of creating a terminating algorithm. Particularly, three discriminants satisfy the above conditions : -99, -72, and -36. However, only -99 and -72 have successfully generated coefficients. How can we tighten the conditions to ensure we only search for representatives in cases where there will be enough?

There are two particular routes for exploration that I am considering: limiting the possible discriminants further by checking conditions for when the resulting BQF will have an integer-valued discriminant, and exploring the conditions under which a discriminant D has a BQF $ax^2 + bxy + cy^2$ where $p^4 \nmid a$. The former seems likely to yield no new information, while the latter seems particularly difficult. With regards to the latter, one might be inclined to reference David A. Cox's Lemma 2.5 in Binary Quadratic Forms, but this relies on the Legendre and its generalizations, all of which depend on the condition $p^2 \nmid D$, which is exactly not the case.

NOTE: Experimentation has lead me to believe D=-36 cannot represent forms where $p^4 | a$, which is good news.

QUESTION:

If a discriminant D has a form $ax^2 + bxy + cy^2$ where $p^4 | a$, does D have a form where $p^4 || a$? This would aid the efficiency of calculations greatly.

ANSWER:

It seems $p^4 || a$ may be too tight, but there does exist a form where $a = p^n$, which is more convenient.

References

[Van] Van Der Geer, G. *Siegel Modular Forms*, Retrieved from https://https://arxiv.org/pdf/math/0605346.pdf