SAITO-KUROKAWA LIFTS AND APPLICATIONS TO ARITHMETIC

JIM L. BROWN

Abstract. In this short survey paper we present an outline for using the Saito-Kurokawa correspondence to provide evidence for the Bloch-Kato conjecture for modular forms. Specific results will be stated, but the aim is to provide the framework for such results with an aim towards future research.

1. The Bloch-Kato conjecture for modular forms

In this section we will review the Bloch-Kato conjecture for modular forms. The conjecture is presented in the general framework of using L-functions and automorphic data to obtain arithmetic information. As such, we begin by reviewing Dirichlet's class number formula and the Birch Swinnerton-Dyer conjecture in this framework.

Let K be a finite abelian Galois extension of $\mathbb{Q}$. Of particular arithmetic interest is the size of the class group of K, denoted by h_K. In the spirit of the general framework we are trying to establish, we associate automorphic objects to K in the form of the group of characters X of K. Dirichlet's class number formula gives a precise relationship between the special values of the L-functions of these characters and the size of the class group of K. In particular, we have

$$\prod_{\chi \in X} L(1,\chi) = \frac{2^{r_1}(2\pi)^{r_2} R_K}{\omega_K \sqrt{D_K}} h_K$$

where r_1 is the number of real embeddings of K, r_2 the number of pairs of complex embeddings, R_K the regulator of K, ω_K the number of roots of unity in K, and D_K the discriminant of K. Note that for the trivial character in X, we write $L(1,1)$ to denote the residue at $s = 1$ of the L-function, in this case just the Riemann zeta function. One sees that by studying the L-functions of the automorphic data associated to K one can translate this back to the arithmetic data about K that is of interest to us.

Let E be an elliptic curve over $\mathbb{Q}$. The Mordell-Weil theorem gives that the rational points on E are given by

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r$$

where $E(\mathbb{Q})_{\text{tors}}$ is one of 15 possible finite groups and r is the rank of the elliptic curve. Arithmetically, the rank of the elliptic curve is of great interest, as is the

2000 *Mathematics Subject Classification.* Primary 11F33, 11F67; Secondary 11F46, 11F80.
Key words and phrases. modular forms, Saito-Kurokawa lifts, Bloch-Kato conjecture, Selmer groups.

Shafarevich-Tate group $\text{Ш}(E/\mathbb{Q})$ which is defined as follows:

$$\text{Ш}(E/\mathbb{Q}) = \ker\left(\mathrm{H}^1(\mathbb{Q}, E) \to \prod_p \mathrm{H}^1(\mathbb{Q}_p, E)\right)$$

where we use the standard convention that $\mathrm{H}^1(K, E) = \mathrm{H}^1_{\mathrm{cont}}(\mathrm{Gal}(\overline{K}/K), E(\overline{K}))$. The work of Taylor and Wiles ([TW], [W]) and subsequent work of Breuil, Conrad, Diamond and Taylor ([BCDT]) shows that associated to E one has a weight 2 newform f_E so that $L(s, E) = L(s, f_E)$. The Birch and Swinnerton-Dyer conjecture can then be stated as

$$\lim_{s \to 1} \frac{L(s, f_E)}{(s-1)^r \Omega^-_{f_E}} = \left(\frac{2^r R_E \,\mathrm{Tam}(E)}{(\# E(\mathbb{Q})_{\mathrm{tors}})^2}\right) \# \text{Ш}(E/\mathbb{Q})$$

where R_E is the regulator of E, $\Omega^-_{f_E}$ is a period associated to f_E, and $\mathrm{Tam}(E)$ is the Tamagawa factor.

In light of the above framework, one can consider the Bloch-Kato conjecture as a vast generalization of Dirichlet's class number formula and the Birch and Swinnerton-Dyer conjecture to the framework of motives. The reader interested in the general conjecture is directed to the original paper of Bloch and Kato ([BK]). We begin by recalling the definition of the Selmer group. Let E be a finite extension of $\mathbb{Q}_p$, $\mathcal{O}$ the ring of integers of E, and ϖ a uniformizer. Let V be a p-adic Galois representation defined over E and let $T \subset V$ be a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable $\mathcal{O}$-lattice. Set $W = V/T$. Define spaces $\mathrm{H}^1_f(\mathbb{Q}_\ell, V)$ by

$$\mathrm{H}^1_f(\mathbb{Q}_\ell, V) = \begin{cases} \mathrm{H}_{\mathrm{ur}}(\mathbb{Q}_\ell, V) & \ell \neq p \\ \ker(\mathrm{H}^1(\mathbb{Q}_p, V) \to \mathrm{H}^1(\mathbb{Q}_p, V \otimes \mathbb{B}_{\mathrm{crys}})) & \ell = p \end{cases}$$

where

$$\mathrm{H}^1_{\mathrm{ur}}(\mathbb{Q}_\ell, M) = \ker(\mathrm{H}^1(\mathbb{Q}_\ell, M) \to \mathrm{H}^1(I_\ell, M))$$

for any $\mathrm{Gal}(\overline{\mathbb{Q}_\ell}/\mathbb{Q}_\ell)$-module M with I_ℓ the inertia group and $\mathbb{B}_{\mathrm{crys}}$ Fontaine's ring of p-adic periods. The Bloch-Kato groups $\mathrm{H}^1_f(\mathbb{Q}_\ell, W)$ are defined by

$$\mathrm{H}^1_f(\mathbb{Q}_\ell, W) = \mathrm{im}(\mathrm{H}^1_f(\mathbb{Q}_\ell, V) \to \mathrm{H}^1(\mathbb{Q}_\ell, W)).$$

The Selmer group of W is given by

$$\mathrm{H}^1_f(\mathbb{Q}, W) = \ker\left(\mathrm{H}^1(\mathbb{Q}, W) \to \bigoplus_\ell \frac{\mathrm{H}^1(\mathbb{Q}_\ell, W)}{\mathrm{H}^1_f(\mathbb{Q}_\ell, W)}\right),$$

i.e., it consists of cocycles in $\mathrm{H}^1(\mathbb{Q}, W)$ that when restricted to the decomposition group at ℓ lie in $\mathrm{H}^1_f(\mathbb{Q}_\ell, W)$ for each prime ℓ. When working with modular forms of level greater then 1, it is often necessary to work with a larger Selmer group where we do not require any conditions at the primes dividing the level. Suppose f is of level is N and set $\Sigma = \{\ell \mid N\}$. The relevant Selmer group is then

$$\mathrm{H}^{1,\Sigma}_f(\mathbb{Q}, W) = \ker\left(\mathrm{H}^1(\mathbb{Q}, W) \to \bigoplus_{\ell \notin \Sigma} \frac{\mathrm{H}^1(\mathbb{Q}_\ell, W)}{\mathrm{H}^1_f(\mathbb{Q}_\ell, W)}\right).$$

We are now in a position to state the Bloch-Kato conjecture for modular forms. For each prime p, let V_p be the p-adic Galois representation arising from a weight $2k-2$ newform f. Let T_p be a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable lattice and $W_p = V_p/T_p$. We denote the j^{th} Tate-twist of V_p by $V_p(j)$ and similarly for W_p. Let π_* be the natural map $\mathrm{H}^1(\mathbb{Q}, V_p(j)) \to \mathrm{H}^1(\mathbb{Q}, W_p(j))$. The Shafarevich-Tate group is defined to be

$$Ш(j) = \bigoplus_\ell \mathrm{H}^1_f(\mathbb{Q}, W_\ell(j))/\pi_* \mathrm{H}^1_f(\mathbb{Q}, V_\ell(j)).$$

Define the set of "global points" by

$$\Gamma_\mathbb{Q}(j) = \bigoplus_\ell \mathrm{H}^0(\mathbb{Q}, W_\ell(j)).$$

One should think of these as the analogue of the rational torsion points on an elliptic curve.

Conjecture 1.1. (Bloch-Kato) With the notation as above, one has

$$L_{\mathrm{alg}}(k, f) = \frac{(\prod_\ell c_\ell(k))}{\#\Gamma_\mathbb{Q}(k)\#\Gamma_\mathbb{Q}(k-2)} \# Ш(1-k)$$

where $c_p(j)$ are "Tamagawa factors" and we define

$$L_{\mathrm{alg}}(k, f) := \frac{L(k, f)}{\pi^k \Omega_f^\pm}$$

and the period $\Omega_f^\pm$ is chosen based on the parity of k.

Remark 1.2. 1. It is known that away from the central critical value the Selmer group is finite ([K], Theorem 14.2). Therefore we can identify the p-part of the Selmer group with the p-part of the Shafarevich-Tate group.
2. If $T_\ell/\varpi T_\ell$ is irreducible, then $\mathrm{H}^0(\mathbb{Q}, W_\ell(j)) = 0$.
3. The Tamagawa factors are integers. See ([BK], Section 5) for definitions and discussion.

The results we aim to prove are of the form that if $\varpi | L_{\mathrm{alg}}(k, f)$ and ϖ does not divide some other product of special values of normalized L-functions, then one has $p | \# \mathrm{H}^{1,\Sigma}_f(\mathbb{Q}, W_p(1-k))$.

2. Ribet's proof of the converse of Herbrand's Theorem

In 1976 Ribet published a short paper using modular forms and Galois representations to prove the converse of Herbrand's theorem ([R]). This work was subsequently generalized by Wiles in his proof of the main conjecture of Iwasawa theory for totally real fields. We briefly outline this argument here as it provides a framework for recent work on the Bloch-Kato conjecture; for example see [Kl] or [SU] for applications other then those described in this paper.

Theorem 2.1. *Let p be a fixed odd prime and $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{Q}}_p^\times$ an even primitive Dirichlet character of order prime to p, $\chi \neq \omega^{-2}$. Suppose $\chi\omega \mid_{I_p} \neq 1$ as a character into $\mathbb{F}_p^\times$ where I_p denotes the inertia group at p. Set $\psi = \chi\omega$ and $F = \mathbb{Q}^\psi$. If $L(-1, \chi)$ is not a unit in $\overline{\mathbb{Q}}_p$, then $A_F^{\psi^{-1}} = A_F \otimes_{\mathbb{Z}_p[\Delta]} \mathbb{F}_p(\psi^{-1}) \neq 0$ where $\Delta = \mathrm{Gal}(F/\mathbb{Q})$ and we write $\mathbb{F}_p(\psi^{-1})$ to denote $\mathbb{F}_p$ with an action of Δ by ψ^{-1}.*

To prove the theorem, one constructs a nontrivial unramified abelian p-extension of F on which Δ acts by ψ^{-1}. This is accomplished by constructing an appropriate Galois representation.

Recall that there exists an Eisenstein series $E_{1,\chi}(z) \in M_2(N, \chi)$ with constant term $\frac{L(-1,\chi)}{2}$ and ℓ^{th} Fourier coefficient given by $c_E(\ell) = 1 + \chi(\ell)\ell$. The first step in Ribet's argument is to produce a cuspidal eigenform f so that the eigenvalues of f are congruent to those of $E_{1,\chi}(z)$ modulo a prime ϖ that divides $L(-1, \chi)$. Note that modulo ϖ the Eisenstein series is a semi-cusp form, i.e., it is a modular form with a constant term of 0 in the Fourier expansion about the cusp infinity. One can show that there is a modular form $g \in M_2(M, \chi)$ with constant term 1 for some M with $N \mid M$ by studying the geometry of the modular curve $X_1(p)$. In fact, one can choose M so that $\text{ord}_p(M) \leq 1$ and if $\ell | M$ with $\ell \nmid Np$, then $\chi(\text{Frob}_\ell) \not\equiv \ell^{-2}$ modulo any prime above p. One then sets $h = E_{1,\chi}(z) - \frac{L(-1,\chi)}{2} g$. The modular form h is congruent to $E_{1,\chi}(z)$ modulo ϖ and is in fact a semi-cusp form. Note that h is not necessarily an eigenform, it is only an eigenform modulo ϖ. One then applies the Deligne-Serre lifting lemma to obtain a semi-cusp form f' that is an eigenform and congruent to $E_{1,\chi}(z)$ modulo ϖ. A short argument then yields an ordinary cusp form f that is an eigenform and congruent to $E_{1,\chi}(z)$ modulo ϖ. It may be of interest to note that this can be phrased in terms of the Eisenstein ideal if one wishes. If $I = \langle T_\ell - 1 - \chi(\ell)\ell \rangle \subset \mathbb{T}_{\mathcal{O}}^{(M)}$ is the Eisenstein ideal, then equivalently one has the following isomorphism

$$\mathbb{T}_{\mathcal{O}}^{(M)}/I \xrightarrow{\sim} \mathcal{O}/(L(-1, \chi)).$$

One would be interested in the statement in this language if one wanted to formulate the results on the Bloch-Kato conjecture in terms of the CAP-ideal (see [Kl]). We will not pursue such a formulation here so only mention the Eisenstein ideal in passing.

The reason we are interested in such a congruence is because of what it tells us about the residual Galois representation of f. Let $\overline{\rho}_f : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\mathbb{F})$ be the residual representation obtained upon composing ρ_f with the natural map $\mathcal{O} \twoheadrightarrow \mathbb{F} = \mathcal{O}/\varpi$. Observe that the congruence to $E_{1,\chi}(z)$ modulo ϖ gives $\text{trace}(\overline{\rho}_f(\text{Frob}_\ell)) = \overline{a_f(\ell)} \equiv 1 + \chi(\ell)\ell (\text{mod}\, \varpi)$, i.e., $\overline{\rho}_f^{\text{ss}} = 1 \oplus \psi$ where $\psi = \chi\omega$. Using the fact that f is ordinary at p so that we have

$$\rho_f|_{D_p} \simeq \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}$$

where χ_2 is unramified at p and satisfies $\chi_2(\text{Frob}_p)$ is the unit root of $x^2 - a_f(p)x + \chi(p)p^{k-1}$, one shows that in fact

$$\overline{\rho}_f \simeq \begin{pmatrix} 1 & * \\ 0 & \psi \end{pmatrix}$$

and is non-split. One knows that $\overline{\rho}_f$ is unramified away from pM because f has level M. Some relatively straight-forward calculations with tame inertia allow one to conclude that $\overline{\rho}_f$ is unramified everywhere. Thus, if one defines $h : \text{Gal}(\overline{\mathbb{Q}}/F) \to \mathbb{F}$ by $h(\sigma) = *(\sigma)$ then one can show that the splitting field $\mathbb{Q}^h$ of h is the extension we seek.

In the following sections we will see how this type of argument can be adapted to our situation.

3. Saito-Kurokawa Lifts

In the previous section we outlined Ribet's proof of the converse of Herbrand's theorem. The main point of the argument was to produce a cuspidal eigenform congruent to an Eisenstein series. The reason for this was that the particularly simple form of the Galois representation of the Eisenstein series could be used to deduce information about the residual Galois representation of f. In order to apply Ribet's argument to our situation we need to find a suitable substitute for the Eisenstein series used in Ribet's argument. The substitute we seek is a Saito-Kurokawa lift. One begins with a cusp form f on $\mathrm{SL}_2(\mathbb{Z})$ and associates a cusp form F_f on $\mathrm{Sp}_4(\mathbb{Z})$. In the language of automorphic forms, F_f is a CAP form (cuspidal associated to parabolic). What this means is that F_f is a cusp form that has the same Hecke eigenvalues almost everywhere as the Eisenstein series obtained by inducing the cuspidal automorphic representation π_f of GL_2 viewed on the Siegel parabolic to an automorphic representation on GSp_4. For the details of this construction in the language of automorphic representations one should consult ([PS]). We will be interested in the classical description of the Saito-Kurokawa correspondence as described in ([EZ], [MRV], [MR], [Z]). As this correspondence is well-known and the references listed provide all the details of the construction, we content ourselves here with stating the facts we will need.

Let $f \in S_{2k-2}^{\mathrm{new}}(\Gamma_0(N))$ be a newform with Fourier coefficients in some ring $\mathcal{O}$. The Saito-Kurokawa lift is constructed as a series of lifts: first lifting f to a half-integer weight form in Kohnen's $+$-space, then lifting this form to a Jacobi form, finally lifting the Jacobi form to a Siegel cuspidal eigenform we denote by F_f. The form F_f lies in the Maass space, denoted by $\mathcal{S}_k^{*,\mathrm{new}}(\Gamma_0^4(N))$. The precise result is as follows.

Theorem 3.1. *([MRV], Theorem 8) The space $\mathcal{S}_k^{*,\mathrm{new}}(\Gamma_0^4(N))$ is isomorphic to the space $S_{2k-2}^{\mathrm{new}}(\Gamma_0(N))$ for N odd and square-free. Given a newform $f \in S_{2k-2}^{\mathrm{new}}(\Gamma_0(N))$, the corresponding $F_f \in \mathcal{S}_k^{*,\mathrm{new}}(\Gamma_0^4(N))$ has modified Spinor L-function satisfying*

$$L^*_{\mathrm{spin}}(s,F) = \zeta(s-k+1)\zeta(s-k+2)L(s,f) \tag{1}$$

where the modified Spinor L-function is defined by

$$L^*_{\mathrm{spin}}(s,F) = \left(\prod_{p\mid N}[(1-p^{k-1-s})(1-p^{k-2-s})]^{-1}\right) L_{\mathrm{spin}}(s,F).$$

We will be interested in the arithmetic properties of this correspondence, so we will need the following result as well.

Corollary 3.2. *([B5], Corollary 2.7) If f has Fourier coefficients in $\mathcal{O}$, there is a normalization of the Saito-Kurokawa lift so that F_f has Fourier coefficients in $\mathcal{O}$. In particular, if $\mathcal{O}$ is a discrete valuation ring, F_f has a Fourier coefficient in $\mathcal{O}^\times$.*

There are two other main results we will need about Saito-Kurokawa lifts. The first is the calculation of the inner product $\langle F_f, F_f\rangle$ in terms of $\langle f, f\rangle$. We will need this result as one of the main steps in our argument is to produce a congruence between a Saito-Kurokawa lift and a Siegel eigenform that is not a CAP form. This is the analogous step to Ribet's construction of a cuspidal eigenform congruent to to the Eisenstein series $E_{1,\chi}(z)$. In the case of level 1 this inner product calculation is a well-known result, see for example [F] or [KS]. For the case of square-free level $N > 1$ the result is as follows.

Theorem 3.3. *([B2], Theorem 1.1) Let $N = p_1 \dots p_n$ with the p_i odd distinct primes, $f \in S_{2k-2}^{new}(\Gamma_0(N))$ a newform, and $F_f \in \mathcal{S}_k^{*,new}(\Gamma_0^4(N))$ the Siegel modular form associated to f via the Saito-Kurokawa correspondence. Let D be a fundamental discriminant with $(-1)^{k-1}D > 0$, $\gcd(N, D) = 1$, χ_D the associated quadratic character, and $c_g(|D|) \neq 0$ where the c_g are the Fourier coefficients of the half-integral weight modular form associated to f via the Saito-Kurokawa correspondence. Then one has*

$$\langle F_f, F_f \rangle = \mathcal{B}_{k,N} \frac{|c_g(|D|)|^2 L(k,f)}{\pi |D|^{k-3/2} L(k-1, f, \chi_D)} \langle f, f \rangle \tag{2}$$

where

$$\mathcal{B}_{k,N} = \frac{N^k (k-1) \prod_{i=1}^n \left(p_i^{2m_i-2}(p_i^4+1)\right)}{2^{n+3}\, 3\, [\mathrm{Sp}_4(\mathbb{Z}) : \Gamma_0^4(N)]\, [\Gamma_0(N) : \Gamma_0(4N)]}.$$

One should note here that this calculation really only relies on the explicit nature of the Saito-Kurokawa correspondence and contains no deep results. It is possible to calculate such inner products in other similar situations. For example, the corresponding statement in terms of unitary groups and Hermitian modular forms can be found in [Kl]. In the symplectic case, more generally one can calculate a similar relation for the Ikaeda lift F_f on $\mathrm{Sp}_{2n}(\mathbb{Z})$ where in this case the relation is between $\langle F_f, F_f \rangle$ and $\langle f, f \rangle^n$. This result is given in [CK] where the explicit formula is not worked out, but the foundations for such a calculation are set.

Finally, to complete the analogy with the Eisenstein series as used by Ribet we should have a particularly simple form for the 4-dimensional Galois representation associated to F_f (see Theorem 5.1). This is in fact the case and follows from the factorization of the Spinor L-function of F_f. We have $\rho_{F_f} = \varepsilon^{k-2} \oplus \rho_f \oplus \varepsilon^{k-1}$ where ε is the p-adic cyclotomic character and ρ_f is the p-adic Galois representation associated to f. Comparing this with the fact that $\rho_{E_{1,\chi}} = 1 \oplus \chi\omega$ we see that the Saito-Kurokawa lift is a suitable replacement for the Eisenstein series in our situation.

4. Congruences

In this section we will give a general outline for producing congruences between Saito-Kurokawa lifts and cuspidal Siegel eigenforms that are not CAP forms. These congruences rely on being able to calculate certain inner products of pullbacks of Eisenstein series and Saito-Kurokawa lifts. We will stick to giving a general outline of the argument. We outline the method in much greater generality then it is known to work for, thereby providing an outline for future research. For a detailed treatment of such an argument in the cases it is known to work the reader can consult [B3], [B4], or [B5].

One begins by defining a Siegel Eisenstein series E on some symplectic space $\mathrm{Sp}_{2m}(\mathbb{Z})$ with the Eisenstein series normalized to have p-integral Fourier coefficients. The specific Eisenstein series and symplectic space vary depending on the application. The important part is that one must be able to form the pullback of this Eisenstein series to some product of the symplectic groups $\mathrm{Sp}_2(\mathbb{Z})$ and $\mathrm{Sp}_4(\mathbb{Z})$. We need at least one copy of $\mathrm{Sp}_4(\mathbb{Z})$ to occur since we are interested in Saito-Kurokawa lifts. If one wanted to work with Ikaeda lifts, one would want copies of $\mathrm{Sp}_2(\mathbb{Z})$ and $\mathrm{Sp}_{2n}(\mathbb{Z})$ instead.

Suppose we have such a pullback. Write our pullback as $E(Z_1, Z_2, \ldots, Z_r)$ for $Z_i \in \mathfrak{h}^{n_i}$ where $\mathfrak{h}^{n_i}$ is the Siegel upper half-space on which $\mathrm{Sp}_{2n_i}(\mathbb{Z})$ acts and we have $2n_1+2n_2+\cdots+2n_r = 2m$. For simplicity assume that $n_1 = 2$ so that the first factor will correspond to $\mathrm{Sp}_4(\mathbb{Z})$. For example, the two cases in which we will state concrete results are the case of the space $\mathrm{Sp}_8(\mathbb{Z})$ pulled back to $\mathrm{Sp}_4(\mathbb{Z}) \times \mathrm{Sp}_4(\mathbb{Z})$ and the space $\mathrm{Sp}_{10}(\mathbb{Z})$ pulled back to $\mathrm{Sp}_4(\mathbb{Z}) \times \mathrm{Sp}_4(\mathbb{Z}) \times \mathrm{Sp}_2(\mathbb{Z})$. The important and difficult (at least from the author's point of view) step is now to calculate the inner product of $E(Z_1, \ldots, Z_r)$ with particular forms of our choosing on $\mathrm{Sp}_{2n_i}(\mathbb{Z})$. For the factors of $\mathrm{Sp}_4(\mathbb{Z})$, we choose our particular form to be F_f. For the factors of $\mathrm{Sp}_2(\mathbb{Z})$, any newform will do as we will ultimately allow this form to vary. Write $F^{(i)}$ for our "particular" form at the ith place. One hopes to obtain a relationship of the form

$$\langle \cdots \langle E(Z_1, \ldots, Z_r), F^{(1)}(Z_1)\rangle \cdots \rangle F^{(r)}(Z_r)\rangle = \mathcal{C} \prod L\text{-fctns} \prod \text{periods} \tag{3}$$

where $\mathcal{C}$ is an explicitly determined constant and the product over periods is a product containing terms of the form $\langle F^{(i)}, F^{(i)}\rangle$ for some of the i. For example, using the inner product given in [Shim95] for $\mathrm{Sp}_4(\mathbb{Z}) \times \mathrm{Sp}_4(\mathbb{Z})$ one obtains

$$\langle\langle E(Z_1, Z_2), F_f(Z_1)\rangle F_f(Z_2)\rangle = \mathcal{C} \cdot L(3-k, \chi) L(1, f, \chi) L(2, f, \chi) \langle F_f, F_f\rangle$$

where χ is a character that is used in the definition of E and f is of weight $2k-2$. One should note that Shimura's formula is true for $\mathrm{Sp}_{2n}(\mathbb{Z}) \times \mathrm{Sp}_{2n}(\mathbb{Z})$ so a similar statement holds for Ikaeda lifts. The product of L-functions that occur will play an important role in our divisibility conditions needed to ensure our congruence exists.

Choose an orthogonal basis $F_1 = F_f, F_2, \ldots, F_s$ of weight k Siegel forms on $\mathrm{Sp}_4(\mathbb{Z})$ and an orthogonal basis $g_1, \ldots, g_t$ of weight k elliptic modular forms on $\mathrm{Sp}_2(\mathbb{Z})$ with g_1 being a newform. For each Z_j, write $H_{i_j}^{(j)}$ for the i_jth basis element. Thus, if Z_j corresponds to $\mathrm{Sp}_4(\mathbb{Z})$ then $H_{i_j}^{(j)} = F_{i_j}$ and if Z_j corresponds to $\mathrm{Sp}_2(\mathbb{Z})$ then $H_{i_j}^{(j)} = g_{i_j}$. We can expand $E(Z_1, \ldots, Z_r)$ in terms of these bases:

$$E(Z_1, \ldots, Z_r) = \sum_{i_1, \ldots, i_r} c_{i_1, \ldots, i_r} H_{i_1}^{(1)}(Z_1) \cdots H_{i_r}^{(r)}(Z_r). \tag{4}$$

For example, in the case of $\mathrm{Sp}_4(\mathbb{Z}) \times \mathrm{Sp}_4(\mathbb{Z}) \times \mathrm{Sp}_2(\mathbb{Z})$ we write

$$E(Z_1, Z_2, Z_3) = \sum_{i_1, i_2, i_3} c_{i_1, i_2, i_3} F_{i_1}(Z_1) F_{i_2}(Z_2) g_{i_3}(Z_3).$$

In order to ensure the congruence we construct does not produce a congruence betwween F_f and another Saito-Kurokawa lift, it is necessary to kill all the other Saito-Kurokawa lifts that occur in the above expansion. This is accomplished by constructing an appropriate Hecke operator and then applying it to the expansion in equation (4). We omit the details and assume hereafter that this has been performed. For the details of such a construction see [B3] or [B5].

The coefficient $c_{1,1,\ldots,1}$ is the coefficient that "controls" the congruence we seek to establish. Suppose that we are able to write $c_{1,1,\ldots 1} = \varpi^{-1} \cdot \mathcal{A}$ for ϖ a uniformizer of some finite extension $\mathcal{O}$ of $\mathbb{Z}_p$ and $\mathcal{A} \in \mathcal{O}^{\times}$. Multiplying equation (4) through by ϖ and using that E has p-integral Fourier coefficients and a little work we obtain a congruence modulo ϖ of the form

$$\mathcal{A} H_1^{(1)}(Z_1) \cdots H_1^{(r)}(Z_r) \equiv -\sum_{i_1 > 1} \varpi c_{i_1, \ldots, i_r} H_{i_1}^{(1)}(Z_1) \cdots H_{i_r}^{(r)}(Z_r) (\operatorname{mod} \varpi).$$

For $j > 1$, we expand the Z_j terms in their Fourier expansions and equate the appropriate Fourier coefficients to obtain a congruence

$$F_f(Z_1) \equiv \sum_{i>1} c_i' F_i(Z_1) (\mathrm{mod}\, \varpi).$$

Thus, it only remains to study the coefficient $c_{1,1,\dots,1}$. To do this we combine equation (3) with equation (4). Using these equations and the fact that Z_1 corresponds to $\mathrm{Sp}_4(\mathbb{Z})$, we will obtain a $\langle F_f, F_f \rangle$ in the denominator of $c_{1,1,\dots,1}$. Thus, we can apply Theorem 3.3 to replace $\langle F_f, F_f \rangle$ and obtain $L(k, f)$ in the denominator of $c_{1,1,\dots,1}$. The rest of $c_{1,1,\dots,1}$ will consist of things that are p-units and then the rest of the L-functions coming from equation (3) and the L-function $L(k-1, f, \chi_D)$ from Theorem 3.3. The periods occurring are used to normalize the L-functions. Thus, we obtain statements of the form that if $\varpi | L_{\mathrm{alg}}(k, f)$ and ϖ does not divide some product of L-functions, then there is a congruence between F_f and a Siegel modular form G that is not a Saito-Kurokawa lift. In order to make G into a cuspidal eigenform some more work is required, but we omit the details. One should also note that we assume $\overline{\rho}_f$ is irreducible and so one cannot have F_f congruent to a CAP form that is not a Saito-Kurokawa lift because of the shapes of the corresponding Galois representations.

We now list two specific results as an illustration of theorems proven in this manner.

Theorem 4.1. *(*[B3]*, Theorem 6.5) Let $k > 3$ be an even integer and p a prime so that $p > 2k - 2$. Let $f \in S_{2k-2}(\mathrm{SL}_2(\mathbb{Z}), \mathcal{O})$ be a newform with real Fourier coefficients and F_f the Saito-Kurokawa lift of f. Suppose that $\overline{\rho}_f$ is irreducible and f is ordinary at p. If there exists an integer $M > 1$, a fundamental discriminant D so that $(-1)^{k-1} D > 0$, $\chi_D(-1) = -1$, $p \nmid MD[\mathrm{Sp}_4(\mathbb{Z}) : \Gamma_0^4(M)]$, and a Dirichlet character χ of conductor M so that*

$$\varpi^m \mid L_{\mathrm{alg}}(k, f)$$

with $m \geq 1$ and

$$\varpi^n \parallel L(3-k, \chi) L_{\mathrm{alg}}(k-1, f, \chi_D) L_{\mathrm{alg}}(1, f, \chi) L_{\mathrm{alg}}(2, f, \chi)$$

with $n < m$, then there exists a cuspidal Siegel eigenform G on $\mathrm{Sp}_4(\mathbb{Z})$ of weight k that is not a CAP form so that $F_f \equiv G (\mathrm{mod}\, \varpi)$ where the congruence is a congruence of eigenvalues.

Theorem 4.2. *(*[B4]*) Let $k \in 2\mathbb{Z}$, $k > 6$ and let $p > 2k+3$ be a regular prime. Let $f \in S_{2k-2}(\mathrm{SL}_2(\mathbb{Z}))$ and $h \in S_k(\Gamma_0(M))$ be newforms with F_f the Saito-Kurokawa lift of f. Assume further that f is ordinary at p. If*

$$\varpi^m \mid L_{\mathrm{alg}}(k, f)$$

and

$$\varpi^n \| L_{\mathrm{alg}}(2k-4, f) L_{\mathrm{alg}}(2k-3, F_f \otimes h)$$

with $n < m$, then then there exists a cuspidal Siegel eigenform G on $\mathrm{Sp}_4(\mathbb{Z})$ of weight k that is not a CAP form so that $F_f \equiv G (\mathrm{mod}\, \varpi)$ where the congruence is a congruence of eigenvalues. Note that $L_{\mathrm{alg}}(s, F_f \otimes h)$ is a convolution L-function.

Note the essential difference in the two theorems is the L-function we want our prime ϖ to “miss”. In the first theorem we have the freedom to move a character χ around to try and cause ϖ to miss the L-values. The second theorem allows us to move a modular form around instead, providing more freedom and hopefully more instances where the L-values are "missed" by ϖ. It should also be mentioned that Theorem 4.2 will appear in [B4] only in the case of h having level 1. The general case is still work in progress and will appear in a future paper.

5. Galois representations and Selmer groups

This final section deals with the problem of using an eigenvalue congruence of the form $F_f \equiv G(\operatorname{mod} \varpi)$ between a Saito-Kurokawa lift and a cuspidal Siegel eigenform that is not a CAP form to produce nontrivial p-torsion elements in an appropriate Selmer group. We begin with the following result stating the existence of the desired Galois representations.

Theorem 5.1. *([SU], Theorem 3.1.3) Let $F \in \mathcal{S}_k(\Gamma_0^4(N))$ be an eigenform, K_F the number field generated by the Hecke eigenvalues of F, and $\mathfrak{p}$ a prime of K_F over p. There exists a finite extension E of the completion $K_{F,\mathfrak{p}}$ of K_F at $\mathfrak{p}$ and a continuous semi-simple Galois representation*

$$\rho_{F,\mathfrak{p}} : \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}_4(E)$$

unramified at all primes $\ell \nmid pN$ and so that for all $\ell \nmid pN$, we have

$$\det(X \cdot I - \rho_{F,\mathfrak{p}}(\operatorname{Frob}_\ell)) = L_{\mathrm{spin}}^{(\ell)}(X).$$

We also need the following result.

Theorem 5.2. *([Falt], [U]) Let F be as in Theorem 5.1 with p a prime not dividing the level of F. The restriction of $\rho_{F,\mathfrak{p}}$ to the decomposition group D_p is crystalline at p. In addition if $p > 2k-2$ then $\rho_{F,\mathfrak{p}}$ is short.*

Recall that in section 3 it was stated that for F_f a Saito-Kurokawa lift, the Galois representation associated to F_f is of the form

$$\rho_{F_f,\mathfrak{p}} = \begin{pmatrix} \varepsilon^{k-2} & & \\ & \rho_{f,\mathfrak{p}} & \\ & & \varepsilon^{k-1} \end{pmatrix}$$

where ε is the p^{th} cyclotomic character. This fact along with the eigenvalue congruence $F_f \equiv G(\operatorname{mod} \varpi)$ allows one to deduce that

$$\overline{\rho}_{G,\mathfrak{p}}^{\mathrm{ss}} = \overline{\rho}_{F_f,\mathfrak{p}} = \begin{pmatrix} \omega^{k-2} & & \\ & \overline{\rho}_{f,\mathfrak{p}} & \\ & & \omega^{k-1} \end{pmatrix}$$

where we use ω to denote the reduction of ε modulo ϖ. The goal is to use this result on the semi-simplification of $\overline{\rho}_{G,\mathfrak{p}}$ to deduce the form of $\overline{\rho}_{G,\mathfrak{p}}$. In particular, simple matrix calculations allow one to conclude that there is a $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable lattice so that one has

$$\overline{\rho}_{G,\mathfrak{p}} = \begin{pmatrix} \omega^{k-2} & *_1 & *_2 \\ *_3 & \overline{\rho}_{f,\mathfrak{p}} & *_4 \\ & & \omega^{k-1} \end{pmatrix}$$

where either $*_1$ or $*_3$ is zero. For the details of these calculations one can consult [B1].

In analogy with Ribet's result, we would like to show that $*_4$ gives a non-zero class in the Selmer group $\mathrm{H}_f^{1,\Sigma}(\mathbb{Q}, W_{f,\mathfrak{p}}(1-k))$. We first need the following result.

The proof of this proposition is a direct generalization of the corresponding result in [R].

Proposition 5.3. *Let $\rho_{G,\mathfrak{p}}$ be such that it does not have a sub-quotient of dimension 1 and $\overline{\rho}_{G,\mathfrak{p}}^{\mathrm{ss}} = \omega^{k-2} \oplus \overline{\rho}_{f,\mathfrak{p}} \oplus \omega^{k-1}$. Then there exists a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable $\mathcal{O}$-lattice in V_G having an $\mathcal{O}$-basis such that the corresponding representation $\rho = \rho_{G,\mathfrak{p}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_4(\mathcal{O})$ has reduction of the form*

$$\overline{\rho}_{G,\mathfrak{p}} = \begin{pmatrix} \omega^{k-2} & *_1 & *_2 \\ *_3 & \overline{\rho}_{f,\mathfrak{p}} & *_4 \\ & & \omega^{k-1} \end{pmatrix} \tag{5}$$

and such that there is no matrix of the form

$$U = \begin{pmatrix} 1 & & & n_1 \\ & 1 & & n_2 \\ & & 1 & n_3 \\ & & & 1 \end{pmatrix} \in \mathrm{GL}_4(\mathcal{O}) \tag{6}$$

such that $\rho' = U\rho U^{-1}$ has reduction of type (5) with $*_2 = *_4 = 0$.

We split into two cases, $*_3 = 0$ and $*_1 = 0$. Suppose $*_3 = 0$. We wish to show that the quotient extension

$$\begin{pmatrix} \overline{\rho}_{f,\mathfrak{p}} & *_4 \\ 0 & \omega^{k-1} \end{pmatrix} \tag{7}$$

is not split. Suppose it is split. Then by Proposition 5.3 we know that the extension

$$\begin{pmatrix} \omega^{k-2} & *_2 \\ 0 & \omega^{k-1} \end{pmatrix} \tag{8}$$

cannot be split as well. One can then use class field theory and some arguments in tame inertia to show that this gives a non-trivial quotient of the ω^{-1}-isotypical piece of the p-part of the class group of $\mathbb{Q}(\zeta_p)$. However, this is impossible by Herbrand's theorem. Thus we have that the quotient extension (7) is non-split. A similar argument deals with the case of $*_1 = 0$. The properties of the Galois representation $\rho_{G,\mathfrak{p}}$ and the fact that $p > 2k-2$ so that $\rho_{G,\mathfrak{p}}$ is crystalline and short at p give that $*_4$ gives a non-trivial p-torsion element in $\mathrm{H}_f^{1,\Sigma}(\mathbb{Q}, W_{f,\mathfrak{p}}(1-k))$. Thus, we have the following theorem.

Theorem 5.4. *Let $f \in S_{2k-2}(\Gamma_0(N))$ be a newform with F_f the Saito-Kurokawa lift of f. If there is a non-CAP cuspidal Siegel eigenform G so that $F_f \equiv G (\mathrm{mod}\, \varpi)$, then $\mathrm{H}_f^{1,\Sigma}(\mathbb{Q}, W_{f,\mathfrak{p}}(1-k))$ is non-trivial and $p \mid \#\,\mathrm{H}_f^{1,\Sigma}(\mathbb{Q}, W_{f,\mathfrak{p}}(1-k))$.*

The main point to notice here is that the input to these Galois representation arguments is an eigenvalue congruence $F_f \equiv G (\mathrm{mod}\, \varpi)$. Once one knows such a congruence, the arguments given produce the non-trivial p-torsion element in the Selmer group regardless of how one achieved such a congruence. The hope is that by looking at more general inner product formulas as in the outline given in section 4 one can produce congruences with conditions that are easier to satisfy.

References

[BK] S. Bloch and K. Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift, Vol. 1, edited by P. Cartier, et al., Birkhäuser, 1990.

[BCDT] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc. 14(4), 843-939(electronic) (2001).

[B1] J. Brown, *Saito-Kurokawa lifts, L-values for* GL_2*, and congruences between Siegel modular forms*, PhD Thesis, University of Michigan, Ann Arbor, (2005).

[B2] J. Brown, *An inner product relation on Saito-Kurokawa lifts*, to appear The Ramanujan Journal of Math.

[B3] J. Brown, *Saito-Kurokawa lifts and applications to the Bloch-Kato conjecture*, to appear Compositio Math.

[B4] J. Brown, *L-functions on* $\mathrm{GSp}(4) \times \mathrm{GL}(2)$ *and the Bloch-Kato conjecture*, submitted.

[B5] J. Brown, *Saito-Kurokawa lifts of square-free level and non-vanishing of Selmer groups*, in preparation.

[CK] Y. Choie and W. Kohnen, *On the Petersson norm of certain Siegel modular forms*, RAMA 7, 45-48 (2003).

[EZ] M. Eichler and D. Zagier, *The theory of Jacobi forms*, Prog. in Math. 55, Birkhauser, Boston (1985).

[Falt] G. Faltings, *Crystalline Cohomology and Galois Representations*, Algebraic Analysis, Geometry and Number Theory, Proceedings of JAMI Inaugural Conference, John Hopkins Univ. Press, 1989.

[F] M. Furusawa, *On Petersson norms for some liftings*, Math. Ann. 267, 543-548 (1984).

[K] K. Kato, *p-adic Hodge Theory and Values of Zeta Functions of Modular Forms*, Asterique 295, 117-290 (2004).

[Kl] K. Klosin, *Congruences among automorphic forms on the unitary group* $U(2,2)$, PhD Thesis, University of Michigan, Ann Arbor (2006).

[KS] W. Kohnen and N.P. Skoruppa, *A certain Dirichlet series attached to Siegel modular forms of degree two*, Invent. Math. 95, 541-558 (1989).

[MRV] M. Manickam, B. Ramakrishnan, and T. C. Vasudevan, *On Saito-Kurokawa descent for congruence subgroups*, Manuscripta Math. 81 (1993), 161-182.

[MR] M. Manickham and B. Ramakrishnan, *On Saito-Kurokawa correspondence of degree two for arbitrary level*, J. Ram. Math. Soc. 17 (2002), no. 3, 149-160.

[PS] I.I. Piatetski-Shapiro, *On the Saito-Kurokawa lifting*, Invent. Math. 71, 309-338 (1983).

[R] K. Ribet, *A modular construction of unramified p-extensions of* $\mathbb{Q}(\mu_p)$, Invent. Math. 34, 151-162 (1976).

[Shim95] G. Shimura, *Eisenstein series and zeta functions on symplectic groups*, Invent. Math. 119, 539-584 (1995).

[SU] C. Skinner and E. Urban, *Sur les déformations p-adiques de certaines représentations automorphes*, JIMJ, to appear.

[U] E. Urban, *Sur les Représentations p-adiques Associées aux Représentations Cuspidales de* $\mathrm{GSp}_{4/\mathbb{Q}}$, Astrisque 302, 151–176 (2005).

[TW] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) 141 (3), 553-572 (1995).

[W] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) 141 (3), 443-551 (1995).

[Z] D. Zagier, *Sur la conjecture de Saito-Kurokawa*, Sé Delange-Pisot-Poitou 1979/80, Progress in Math. 12, Boston-Basel-Stuttgart, 371-394 (1980).

E-mail address: `jimlb@math.ohio-state.edu`

Department of Mathematics, The Ohio State University, Columbus, OH 43210