Wach modules and modular forms

Sarah Zerbes

joint with Antonio Lei and David Loeffler

1. Setup

Let p be an odd prime, $\mathbb{Q}_n = \mathbb{Q}(\mu_{p^n})$ and $\mathbb{Q}_{p,n} = \mathbb{Q}_p(\mu_{p^n})$. Let $\mathbb{Q}_\infty = \bigcup \mathbb{Q}_n$ and $\mathbb{Q}_{p,\infty} = \bigcup \mathbb{Q}_{p,n}$. Define the Galois group

$$G = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}_{p,\infty}/\mathbb{Q}_p),$$

which is isomorphic to $\mathbb{Z}_p^\times$ via the cyclotomic character χ. We write $G = \Delta \times \Gamma$, where $\Delta \cong \mathbb{Z}/(p-1)$ and $\Gamma \cong \mathbb{Z}_p$. Choose a topological generator γ of Γ. Let

$$\begin{aligned}\Lambda_{\mathbb{Q}_p}(G) &= \mathbb{Z}_p[[G]] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \\ \mathcal{H}_{\mathbb{Q}_p}(G) &= \mathbb{Q}_p\text{-valued distributions on } G \\ &= \{f(\gamma-1) \mid f(X) \in \mathbb{Q}_p[\Delta][[X]], \quad f \text{ converges for } \mid X \mid < 1\}\end{aligned}$$

Note that under the natural inclusion, the Iwasawa algebra $\Lambda_{\mathbb{Q}_p}(G)$ corresponds to the bounded functions on the open unit p-adic disc.

Let $f = \sum a_n q^n$ be a normalised new eigenform of weight $k \geq 2$, level N such that $p \nmid N$ and character ϵ. Let $K = \mathbb{Q}(f)$ be the coefficient field of f, and fix a prime v of K dividing p.

Simplifying assumptions. (1) ϵ is trivial (which implies in particular that $f = \bar{f}$);
(2) the completion of K at v is $\mathbb{Q}_p$.

Let V_f be the p-adic representation of $\mathcal{G}_\mathbb{Q} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ attached to f (Deligne), and let T_f be a $\mathcal{G}_\mathbb{Q}$-stable lattice in V_f.

Note 1.1. *V_f is a 2-dimensional $\mathbb{Q}_p$-vector space. Moreover, as a representation of $\mathcal{G}_{\mathbb{Q}_p}$, V_f is crystalline, with Hodge-Tate weights $1-k$ and 0.*

1.1. Construction of p-adic L-functions.

Let $F(X) = X^2 - a_p X + p^{k-1}$ be the characteristic polynomial of φ on $\mathbb{D}_{\mathrm{cris}}(V_f)$.

Theorem 1.2. *(Amice-Velu) Let α be a root of $F(X)$ such that $v_p(\alpha) < k-1$. Then there exists $\mathcal{L}_{p,\alpha} \in \mathcal{H}_{\overline{\mathbb{Q}_p}}(G)$ of order $\log_p^{v_p(\alpha)}$ interpolating critical L-values of f and its twists.*

Alternative construction by Kato: Let $H^1_{\mathrm{Iw}}(\mathbb{Q}, T_f) = \varprojlim H^1(\mathbb{Q}_n, T_f)$, where the inverse limit is taken with respect to the corestriction maps, and let $z_{\mathrm{Kato}} \in H^1_{\mathrm{Iw}}(\mathbb{Q}, T_f)$ be Kato's zeta element. Via localisation and twisting, we can consider z_{Kato} as an element in $H^1_{\mathrm{Iw}}(\mathbb{Q}_p, T_f(k-1))$.

For all $\omega \in \mathbb{D}_{\mathrm{cris}}(V_f) \otimes_{\mathbb{Q}_p} \overline{\mathbb{Q}_p}$, Perrin-Riou has constructed a $\Lambda_{\mathbb{Q}_p}(G)$-homomorphism

$$L_\omega : H^1_{\mathrm{Iw}}(\mathbb{Q}_p, T_f(k-1)) \longrightarrow \mathcal{H}_{\overline{\mathbb{Q}_p}}(G).$$

Theorem 1.3. *(Kato) Let α be as above, and let $\omega_\alpha \in \mathbb{D}_{\mathrm{cris}}(V_f) \otimes_{\mathbb{Q}_p} \overline{\mathbb{Q}_p}$ be the φ-eigenvector of α (normalised appropriately). Then*

$$L_{\omega_\alpha}(z_{\mathrm{Kato}}) = \mathcal{L}_{p,\alpha}.$$

1.2. Selmer groups.

Definition 1.4. *For a finite extension L of $\mathbb{Q}$, define the p-Selmer group of f over L as*

$$\mathrm{Sel}(f/L) = \ker\left(H^1(L, V_f/T_f(1)) \longrightarrow \prod_v \frac{H^1(L_v, V_f/T_f(1))}{H^1_f(L_v, v_f/T_f(1))} \right),$$

where the product is taken over all primes v of L, and the $H^1_f(L_v, v_f/T_f(1))$ are the usual local conditions. Here, for a field F, $H^1(F, V_f/T_f(1))$ denotes the Galois cohomology group $H^1(\mathcal{G}_F, V_f/T_f(1))$.

Let $\mathrm{Sel}(f/\mathbb{Q}_\infty) = \varinjlim_n \mathrm{Sel}(f/\mathbb{Q}_n)$ and

$$X(f/\mathbb{Q}_\infty) = \mathrm{Hom}_{\mathrm{cts}}\left(\mathrm{Sel}(f/\mathbb{Q}_\infty), \mathbb{Q}_p/\mathbb{Z}_p\right) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

One can show that $X(f/\mathbb{Q}_\infty)$ is a finitely generated $\Lambda_{\mathbb{Q}_p}(G)$-module.

2. Main conjectures

2.1. **The ordinary case** ($\Leftrightarrow v_p(a_p) = 0$)**.** If f is ordinary at p, then there exists a unique root α of $F(X)$ with $v_p(\alpha) = 0$. The corresponding Amice-Velu p-adic L-function $\mathcal{L}_{p,\alpha}$ is bounded, i.e. an element of $\Lambda_{\mathbb{Q}_p}(G)$.

Theorem 2.1. *(Kato) $X(f/\mathbb{Q}_\infty)$ is a finitely generated torsion $\Lambda_{\mathbb{Q}_p}(G)$-module, and $\mathcal{L}_{p,\alpha} \in \mathrm{char}\big(X(f/\mathbb{Q}_\infty)\big)$.*

Cyclotomic Main Conjecture. We have $\mathrm{char}\big(X(f/\mathbb{Q}_\infty)\big) = (\mathcal{L}_{p,\alpha})$.

Remark 2.2. *A proof of the Main Conjecture has been announced by Skinner-Urban.*

2.2. **The supersingular case** ($\Leftrightarrow v_p(a_p) > 0$)**.** If f is supersingular at p, then there are two problems:
(1) $X(f/\mathbb{Q}_\infty)$ has positive $\Lambda_{\mathbb{Q}_p}(G)$-rank, and
(2) $\mathcal{L}_{p,\alpha_i} \notin \Lambda_{\mathbb{Q}_p}(G)$ for both roots α_1, α_2 of $F(X)$.

2.2.1. *The case $a_p = 0$.*

Theorem 2.3. *(Pollack) There exist two functions $\log_{p,k}^{\pm} \in \mathcal{H}_{\mathbb{Q}_p}(G)$ depending only on p and k, and elements $\mathcal{L}_{p,1}, \mathcal{L}_{p,2} \in \Lambda_{\mathbb{Q}_p}(G)$ such that for $i = 1, 2$ we have*

$$\mathcal{L}_{p,\alpha_i} = \log_{p,k}^{+} \mathcal{L}_{p,1} + \alpha_i \log_{p,k}^{-} \mathcal{L}_{p,2}.$$

Remark 2.4. *(1) The distributions $\log_{p,k}^{\pm}$ can be described explicitly;*
(2) Pollack's theorem gives a joint decomposition of the Amice-Velu p-adic L-functions into a matrix of logarithms and two bounded p-adic L-functions $\mathcal{L}_{p,i}$.

Kobayashi (when f corresponds to an elliptic curve $E/\mathbb{Q}$) and Lei (in the general case) give an arithmetic interpretation of these new p-adic L-functions $\mathcal{L}_{p,i}$ be constructing corresponding Selmer groups $\mathrm{Sel}^i(f/\mathbb{Q}_\infty)$ for $i = 1, 2$:

(1) For $i = 1, 2$, construct $\Lambda(G)$-homomorphisms

$$\mathrm{Col}_i : H^1_{\mathrm{Iw}}(\mathbb{Q}_p, T_f(k-1)) \longrightarrow \Lambda(G);$$

(2) let

$$H^1_{i,f}\big(\mathbb{Q}_{p,n}, V_f/T_f(1)\big) = \text{annihilator of } \big(\ker(\mathrm{Col}_i) \cap H^1(\mathbb{Q}_{p,n}, T_f(k-1))\big)$$

under the Tate pairing.
(3) use the $H^1_{i,f}\big(\mathbb{Q}_{p,n}, V_f/T_f(1)\big)$ instead of the usual local condition $H^1_f\big(\mathbb{Q}_{p,n}, V_f/T_f(1)\big)$ in the definition of $\mathrm{Sel}(f/\mathbb{Q}_n)$.

Remark 2.5. *For the construction of the Coleman maps Col_i, Kobayashi uses the formal group $\hat{E}$ attached to E, and Lei uses $\mathbb{D}_{\mathrm{cris}}(V_f)$ and Perrin-Riou's exponential map.*

Theorem 2.6. *(Kobayashi, Lei) For $i = 1, 2$, $X_i(f/\mathbb{Q}_\infty)$ is a finitely generated torsion $\Lambda_{\mathbb{Q}_p}(G)$-module, and $\mathcal{L}_{p,i} \in \mathrm{char}\big(X_i(f/\mathbb{Q}_\infty)\big)$.*

Cyclotomic Main Conjecture. We have $\mathrm{char}\big(X_i(f/Q_\infty)\big) = (\mathcal{L}_{p,i})$ for $i = 1, 2$.

2.2.2. *The case $a_p \neq 0$.* When $a_p \neq 0$ and f corresponds to an elliptic curve with $E/\mathbb{Q}$ (which implies that $p = 2, 3$), Sprung has generalised Pollack's and Kobayashi's results using $\hat{(E)}$ and explicit calculation.

3. Our approach

Make the following definitions:

$$\begin{aligned} \mathbb{B}^+_{\mathbb{Q}_p} &= \mathbb{Z}_p[[\pi]] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p && \mathbb{Q}_p\text{-valued measures on } \mathbb{Z}_p; \\ \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p} &= \{f \in \mathbb{Q}_p[[\pi]] \mid f \text{ converges for } |\ \pi\ | < 1\} && \mathbb{Q}_p\text{-valued distributions on } \mathbb{Z}_p \end{aligned}$$

Equip both rings with actions of φ and G which are determined by $\varphi(\pi) = (\pi+1)^p - 1$ and $g(\pi) = (\pi+1)^{\chi(g)} - 1$. Then φ is injective, and we can define a left inverse ψ of φ.

Proposition 3.1. *We have isomorphisms $\mathfrak{M}$ of $\Lambda_{\mathbb{Q}_p}(G)$- (resp. $\mathcal{H}_{\mathbb{Q}_p}(G)$-) modules*

$$\begin{aligned} \Lambda_{\mathbb{Q}_p}(G) &\xrightarrow{\cong} \left(\mathbb{B}^+_{\mathbb{Q}_p}\right)^{\psi=0}, \\ \mathcal{H}_{\mathbb{Q}_p}(G) &\xrightarrow{\cong} \left(\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}\right)^{\psi=0} \end{aligned}$$

which are determined by $\mathfrak{M}(g) = (\pi+1)^{\chi(g)}$. We call $\mathfrak{M}$ the Mellin transform.

3.1. Coleman maps for crystalline representations with Hodge-Tate weights ≥ 0.

Definition 3.2. *A Wach module N is a free finitely generated $\mathbb{B}^+_{\mathbb{Q}_p}$-module with commuting actions of G (trivial on $N \mod \pi$) and $\varphi : N[\pi^{-1}] \to N[\varphi(\pi)^{-1}]$ and some additional technical conditions.*

Theorem 3.3. *(Wach, Berger) (1) There is an equivalence of categories*

$$\begin{aligned} \{\textit{crystalline representations of } \mathcal{G}_{\mathbb{Q}_p}\} &\Leftrightarrow \{\textit{Wach modules}\} \\ V &\longrightarrow \mathbb{N}(V); \end{aligned}$$

(2) for any crystalline representation V of $\mathcal{G}_{\mathbb{Q}_p}$, we have a comparison isomorphism

$$\mathbb{N}(V) \otimes_{\mathbb{B}^+_{\mathbb{Q}_p}} \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}[t^{-1}] \cong \mathbb{D}_{\mathrm{cris}}(V) \otimes_{\mathbb{Q}_p} \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}[t^{-1}], \tag{1}$$

where $t = \log(1+\pi)$, which is compatible with the actions of G and φ;
(3) if V is a crystalline representation with Hodge-Tate weights ≤ 0, then φ restrict to $\mathbb{N}(V) \to \mathbb{N}(V)$, and we have an isomorphism of φ-modules

$$\mathbb{D}_{\mathrm{cris}}(V) \cong \mathbb{N}(V) \mod \pi.$$

Remark 3.4. *For any crystalline representation V of $\mathcal{G}_{\mathbb{Q}_p}$, $\mathbb{N}(V)$ is contained in the (φ, G)-module of V.*

Theorem 3.5. *(Fontaine, Berger) Let V be crystalline with Hodge-Tate weights ≥ 0, and assume that V has no quotient isomorphic to $\mathbb{Q}_p$. Then $H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V) \cong \mathbb{N}(V)^{\psi=1}$.*

Theorem 3.6. *(LLZ, Berger) Let N be a Wach module, and let $n_1, \ldots, n_d$ be a $\mathbb{B}^+_{\mathbb{Q}_p}$-basis of N. Let $\varphi^*(N)$ be the $\mathbb{B}^+_{\mathbb{Q}_p}$-span of $\varphi(N)$. Then $\left(\varphi^*(N)\right)^{\psi=0}$ is a free $\Lambda_{\mathbb{Q}_p}(G)$-module of rank d, and a basis is given by $(1+\pi)\varphi(n_1), \ldots, (1+\pi)\varphi(n_d)$.*

Remark 3.7. *For every $x \in \left(\varphi^*(N)\right)^{\psi=0}$ there exist unique $x_1, \ldots, x_d \in (\mathbb{B}^+_{\mathbb{Q}_p})^{\psi=0}$ such that $x = x_1\varphi(n_1) + \cdots + x_d\varphi(n_d)$.*

Definition 3.8. *(Coleman maps) Let V be a crystalline representation of dimension d with Hodge-Tate weights ≥ 0, and assume that V has no quotient isomorphic to $\mathbb{Q}_p$. Fix a basis $n_1, \ldots, n_d$ of $\mathbb{N}(V)$. For $1 \leq i \leq d$, define*

$$\mathrm{Col}_i : H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V) \cong \mathbb{N}(V)^{\psi=1} \xrightarrow{1-\varphi} \left(\varphi^*\mathbb{N}(V)\right)^{\psi=0} \cong \Lambda_{\mathbb{Q}_p}(G)^{\oplus d} \xrightarrow{\mathrm{pr}_i} \Lambda_{\mathbb{Q}_p}(G).$$

Note that the Coleman maps are $\Lambda_{\mathbb{Q}_p}(G)$-homomorphisms.

3.2. **The special case $V = V_f(k-1)$ for f ordinary or supersingular.** Recall that the Hodge-Tate weights of V_f are $1-k$ and 0, so

$$\mathbb{D}_{\mathrm{cris}}(V_f) \cong \mathbb{N}(V_f) \mod \pi. \tag{2}$$

Choose the following basis for $\mathbb{D}_{\mathrm{cris}}(V_f)$:

- if f is supersingular, let $v_1' \in \mathrm{Fil}^{k-1}\mathbb{D}_{\mathrm{cris}}(V_f)$ and $v_2' = \varphi(v_1)$;
- if f is ordinary, let v_i' be the φ-eigenvector basis of $\mathbb{D}_{\mathrm{cris}}(V_f)$.

Let n_1', n_2' be a basis of $\mathbb{N}(V_f)$ lifting v_1', v_2' under (2). Let

$$v_i = v_i' \otimes e_{k-1}t^{1-k},$$
$$n_i = n_i' \otimes e_{k-1}\pi^{1-k},$$

which are bases of $\mathbb{D}_{\mathrm{cris}}(V)$ and $\mathbb{N}(V)$, respectively. Here, e_{k-1} is the basis of the $k-1$st cyclotomic twist.

Let $M \in M_2\big(\varphi(\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p})\big)$ be the matrix such that $\begin{pmatrix}\varphi(n_1)\\ \varphi(n_2)\end{pmatrix} = M\begin{pmatrix}v_1\\ v_2\end{pmatrix}$; note that M exists by Berger's comparison isomorphism (1). Moreover, let $\underline{M} = \mathfrak{M}^{-1}\big((1+\pi)M\big) \in M_2\big(\mathcal{H}_{\mathbb{Q}_p}(G)\big)$, where $\mathfrak{M}^{-1}$ is applied entry-wise.

Theorem 3.9. *(LLZ) For $i = 1, 2$, the following diagram is commutative:*

$$\begin{array}{ccccc}
\mathbb{N}(V)^{\psi=1} & \xrightarrow{h^1_{\mathbb{Q}_p,\mathrm{Iw}}} & H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V) & & \\
\downarrow{\scriptstyle 1-\varphi} & & \downarrow{\scriptstyle (\mathrm{Col}_1,\mathrm{Col}_2)} & & \\
(\varphi^*\mathbb{N}(V))^{\psi=0} & \xrightarrow{\cong} & \Lambda_{\mathbb{Q}_p}(G_\infty)^{\oplus 2} & & \\
\downarrow{\scriptstyle M} & & \downarrow{\scriptstyle \underline{M}} & \searrow{\scriptstyle L_{v_i}} & \\
\big((\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p})^{\psi=0}\big)^{\oplus 2} & \xrightarrow{\mathfrak{M}^{-1}} & \mathcal{H}(G_\infty)^{\oplus 2} & & \\
\downarrow{\scriptstyle \mathrm{pr}_i} & & \downarrow{\scriptstyle \mathrm{pr}_i} & & \\
(\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p})^{\psi=0} & \xrightarrow{\mathfrak{M}^{-1}} & \mathcal{H}(G_\infty). & &
\end{array}$$

Definition 3.10. *For $i = 1, 2$, let $\mathcal{L}_{p,i} = \mathrm{Col}_i(z_{\mathrm{Kato}}) \in \Lambda_{\mathbb{Q}_p}(G)$.*

Corollary 3.11. *If f is supersingular, we have*

$$\begin{pmatrix}\mathcal{L}_{p,\alpha_1}\\ \mathcal{L}_{p,\alpha_2}\end{pmatrix} = A\underline{M}\begin{pmatrix}\mathcal{L}_{p,1}\\ \mathcal{L}_{p,2}\end{pmatrix},$$

where A is the change-of-basis matrix from v_1, v_2 to the basis of φ-eigenvectors.

Corollary 3.12. *As a special case, we recover the decompositions of Pollack and Sprung (when $p = 3$).*

Define the following assumptions:
(A) f is supsersingular, $k \geq 3$ or $a_p = 0$;
(A') f is ordinary, V_f is not locally split at p and $k \geq 3$.

Theorem 3.13. *(LLZ) If either f is supersingular or (A') holds,*
(1) $\mathcal{L}_{p,i} \neq 0$ for $i = 1, 2$;
(2) we have explicit interpolation formulae for the $\mathcal{L}_{p,i}$ at the characters of conductor 1 or p of G;
(3) if f is supersingular, $\mathcal{L}_{p,\alpha_i}$ has infinitely many zeros for $i = 1, 2$.

Remark 3.14. *The values of the $\mathcal{L}_{p,i}$ at the characters of conductor 1 or p of G do not depend on the choice of the basis n_1, n_2 of $\mathbb{N}(V)$ lifting v_1, v_2.*

As in Section 2.2.1, we use the Coleman maps to define Selmer groups $\mathrm{Sel}^i(f/\mathbb{Q}_\infty)$.

Remarks 3.15. *(1) We recover the $\pm$-Selmer groups of Kobayashi and Sprung (when $p = 3$).*

(2) We get a second Selmer group when f is ordinary.

Theorem 3.16. *(LLZ) Assume that either (A) or (A') is satisfied. Then $X_i(f/\mathbb{Q}_\infty)$ is a finitely generated torsion $\Lambda_{\mathbb{Q}_p}(G)$-module for $i = 1, 2$, and*

$$\mathcal{L}_{p,i}^{\eta} \in \mathrm{char}\big(\mathrm{X_i(f/\mathbb{Q}_\infty)^\eta}\big),$$

where $\eta = \begin{cases} \text{any character } \Delta \to \mathbb{Z}_p^\times & \text{if } i = 1 \\ \text{trivial character} & \text{if } i = 2 \end{cases}$.

Moreover, if the map $\mathcal{G}_{\mathbb{Q}} \to \mathrm{GL_2(T_f)}$ is surjective, then Kato's Main Conjecture (with $\mathbb{Q}_p$-coefficients) is equivalent to

$$\mathrm{char}\big(X_i(f/\mathbb{Q}_\infty)\big) = \mathrm{char}\left(\mathrm{image(Col_i)}/(\mathcal{L}_{\mathrm{p,i}})\right)$$

for **either** $i = 1$ *or* 2.

Remarks 3.17. *(1) If f is supersingular and a_p satisfies some additional conditions, Berger-Li-Zhu have constructed an explicit basis of $\mathbb{N}(V)$. Using this basis, we can show that Col_1 is surjective, so Kato's Main Conjecture is equivalent to*

$$\mathrm{char}\big(X_1(f/\mathbb{Q}_\infty)\big) = \big(\mathcal{L}_{p,1}\big).$$

(2) In joint work with Antonio Lei, we give a general description of the image of Col_i using Perrin-Riou's p-adic regulator.

(3) We do not know whether Theorem 3.16 holds when we work with $\mathbb{Z}_p$-coefficients and $a_p \neq 0$.