Computing the Cassels-Tate pairing on odd-degree hyperelliptic Jacobians

Himanshu Shukla

Mathematisches Institut, Universität Bayreuth

Rational Points 2022

28 March, 2022

Notations

- Let k be a number field with absolute Galois group G_k, and let $C : y^2 = f(x)$ with $\deg(f) = 2g + 1$ be a hyperelliptic curve of genus g defined over k and J be its Jacobian.
- Let $\Delta := \{T_i := (e_i, 0) \in C : 1 \leq i \leq 2g + 1\}$ be the set of points on C corresponding to the roots e_i of f, and T_0 be the point at ∞.
- For a place v of k, denote the completion of k at v by k_v.
- $\mathrm{C}^i(G, A)$, $\mathrm{Z}^i(G, A)$ and $\mathrm{H}^i(G, A)$ denote continuous i-cochains, cocycles and cohomology classes associate to a group G and a G-module A.
- For $n \geq 2$, let $\text{Ш}(J)$ and $\mathrm{Sel}^{(n)}(J)$ be the Shafarevich-Tate and n-Selmer groups associated with J.

Notations

- Let k be a number field with absolute Galois group G_k, and let $C : y^2 = f(x)$ with $\deg(f) = 2g + 1$ be a hyperelliptic curve of genus g defined over k and J be its Jacobian.
- Let $\Delta := \{T_i := (e_i, 0) \in C : 1 \leq i \leq 2g + 1\}$ be the set of points on C corresponding to the roots e_i of f, and T_0 be the point at ∞.
- For a place v of k, denote the completion of k at v by k_v.
- $\mathrm{C}^i(G, A)$, $\mathrm{Z}^i(G, A)$ and $\mathrm{H}^i(G, A)$ denote continuous i-cochains, cocycles and cohomology classes associate to a group G and a G-module A.
- For $n \geq 2$, let $\text{Ш}(J)$ and $\mathrm{Sel}^{(n)}(J)$ be the Shafarevich-Tate and n-Selmer groups associated with J.

Notations

- Let k be a number field with absolute Galois group G_k, and let $C : y^2 = f(x)$ with $\deg(f) = 2g+1$ be a hyperelliptic curve of genus g defined over k and J be its Jacobian.
- Let $\Delta := \{T_i := (e_i, 0) \in C : 1 \leq i \leq 2g+1\}$ be the set of points on C corresponding to the roots e_i of f, and T_0 be the point at ∞.
- For a place v of k, denote the completion of k at v by k_v.
- $\mathrm{C}^i(G, A)$, $\mathrm{Z}^i(G, A)$ and $\mathrm{H}^i(G, A)$ denote continuous i-cochains, cocycles and cohomology classes associate to a group G and a G-module A.
- For $n \geq 2$, let $\text{Ш}(J)$ and $\mathrm{Sel}^{(n)}(J)$ be the Shafarevich-Tate and n-Selmer groups associated with J.

Notations

- Let k be a number field with absolute Galois group G_k, and let $C : y^2 = f(x)$ with $\deg(f) = 2g + 1$ be a hyperelliptic curve of genus g defined over k and J be its Jacobian.
- Let $\Delta := \{T_i := (e_i, 0) \in C : 1 \leq i \leq 2g + 1\}$ be the set of points on C corresponding to the roots e_i of f, and T_0 be the point at ∞.
- For a place v of k, denote the completion of k at v by k_v.
- $\mathrm{C}^i(G, A)$, $\mathrm{Z}^i(G, A)$ and $\mathrm{H}^i(G, A)$ denote continuous i-cochains, cocycles and cohomology classes associate to a group G and a G-module A.
- For $n \geq 2$, let $\text{Ш}(J)$ and $\mathrm{Sel}^{(n)}(J)$ be the Shafarevich-Tate and n-Selmer groups associated with J.

Notations

- Let k be a number field with absolute Galois group G_k, and let $C : y^2 = f(x)$ with $\deg(f) = 2g + 1$ be a hyperelliptic curve of genus g defined over k and J be its Jacobian.
- Let $\Delta := \{T_i := (e_i, 0) \in C : 1 \leq i \leq 2g + 1\}$ be the set of points on C corresponding to the roots e_i of f, and T_0 be the point at ∞.
- For a place v of k, denote the completion of k at v by k_v.
- $\mathrm{C}^i(G, A)$, $\mathrm{Z}^i(G, A)$ and $\mathrm{H}^i(G, A)$ denote continuous i-cochains, cocycles and cohomology classes associate to a group G and a G-module A.
- For $n \geq 2$, let $\text{Ш}(J)$ and $\mathrm{Sel}^{(n)}(J)$ be the Shafarevich-Tate and n-Selmer groups associated with J.

Notations

- Let k be a number field with absolute Galois group G_k, and let $C : y^2 = f(x)$ with $\deg(f) = 2g + 1$ be a hyperelliptic curve of genus g defined over k and J be its Jacobian.
- Let $\Delta := \{T_i := (e_i, 0) \in C : 1 \leq i \leq 2g + 1\}$ be the set of points on C corresponding to the roots e_i of f, and T_0 be the point at ∞.
- For a place v of k, denote the completion of k at v by k_v.
- $\mathrm{C}^i(G, A)$, $\mathrm{Z}^i(G, A)$ and $\mathrm{H}^i(G, A)$ denote continuous i-cochains, cocycles and cohomology classes associate to a group G and a G-module A.
- For $n \geq 2$, let $\text{Ш}(J)$ and $\mathrm{Sel}^{(n)}(J)$ be the Shafarevich-Tate and n-Selmer groups associated with J.

A quick recall

- We have

$$\mathrm{Sel}^{(n)}(J) := \ker\left(\mathrm{H}^1(G_k, J[n]) \to \prod_v \mathrm{H}^1(G_{k_v}, J)\right)$$

and

$$Ш(J) := \ker\left(\mathrm{H}^1(G_k, J) \to \prod_v \mathrm{H}^1(G_{k_v}, J)\right).$$

- For $n \geq 2$, we have the *n-descent exact* sequence:

$$0 \to J(k)/nJ(k) \to \mathrm{Sel}^{(n)}(J) \to Ш(J)[n] \to 0.$$

A quick recall

- We have

$$\mathrm{Sel}^{(n)}(J) := \ker\left(\mathrm{H}^1(G_k, J[n]) \to \prod_v \mathrm{H}^1(G_{k_v}, J)\right)$$

and

$$Ш(J) := \ker\left(\mathrm{H}^1(G_k, J) \to \prod_v \mathrm{H}^1(G_{k_v}, J)\right).$$

- For $n \geq 2$, we have the *n-descent exact* sequence:

$$0 \to J(k)/nJ(k) \to \mathrm{Sel}^{(n)}(J) \to Ш(J)[n] \to 0.$$

Recalling CTP

The Cassels-Tate pairing:

$$\langle \cdot, \cdot \rangle_{\mathrm{CT}} : Ш(J) \times Ш(J) \to \mathbb{Q}/\mathbb{Z}$$

which satisfies:

- Anti-symmetric and non-degenerate (on the quotient $Ш(J)_{nd} \times Ш(J)_{nd}$).
- Defined first by Cassels for elliptic curves and generalized by Tate to abelian varieties.
- Poonen and Stoll gave the Albanese-Albanese definition of CTP and showed that it is equivalent to the 2-other definitions (Weil-pairing and homogeneous space based definitions).
- This pairing can be pulled back to the n-Selmer group using the n-descent sequence.

Recalling CTP

The Cassels-Tate pairing:

$$\langle \cdot, \cdot \rangle_{\mathrm{CT}} : Ш(J) \times Ш(J) \to \mathbb{Q}/\mathbb{Z}$$

which satisfies:

- Anti-symmetric and non-degenerate (on the quotient $Ш(J)_{nd} \times Ш(J)_{nd}$).
- Defined first by Cassels for elliptic curves and generalized by Tate to abelian varieties.
- Poonen and Stoll gave the Albanese-Albanese definition of CTP and showed that it is equivalent to the 2-other definitions (Weil-pairing and homogeneous space based definitions).
- This pairing can be pulled back to the n-Selmer group using the n-descent sequence.

Recalling CTP

The Cassels-Tate pairing:

$$\langle \cdot, \cdot \rangle_{\mathrm{CT}} : Ш(J) \times Ш(J) \to \mathbb{Q}/\mathbb{Z}$$

which satisfies:

- Anti-symmetric and non-degenerate (on the quotient $Ш(J)_{nd} \times Ш(J)_{nd}$).
- Defined first by Cassels for elliptic curves and generalized by Tate to abelian varieties.
- Poonen and Stoll gave the Albanese-Albanese definition of CTP and showed that it is equivalent to the 2-other definitions (Weil-pairing and homogeneous space based definitions).
- This pairing can be pulled back to the n-Selmer group using the n-descent sequence.

Recalling CTP

The Cassels-Tate pairing:

$$\langle \cdot, \cdot \rangle_{\mathrm{CT}} : Ш(J) \times Ш(J) \to \mathbb{Q}/\mathbb{Z}$$

which satisfies:

- Anti-symmetric and non-degenerate (on the quotient $Ш(J)_{nd} \times Ш(J)_{nd}$).
- Defined first by Cassels for elliptic curves and generalized by Tate to abelian varieties.
- Poonen and Stoll gave the Albanese-Albanese definition of CTP and showed that it is equivalent to the 2-other definitions (Weil-pairing and homogeneous space based definitions).
- This pairing can be pulled back to the n-Selmer group using the n-descent sequence.

Recalling CTP

The Cassels-Tate pairing:

$$\langle \cdot, \cdot \rangle_{\mathrm{CT}} : Ш(J) \times Ш(J) \to \mathbb{Q}/\mathbb{Z}$$

which satisfies:

- Anti-symmetric and non-degenerate (on the quotient $Ш(J)_{nd} \times Ш(J)_{nd}$).
- Defined first by Cassels for elliptic curves and generalized by Tate to abelian varieties.
- Poonen and Stoll gave the Albanese-Albanese definition of CTP and showed that it is equivalent to the 2-other definitions (Weil-pairing and homogeneous space based definitions).
- This pairing can be pulled back to the n-Selmer group using the n-descent sequence.

Albanese-Albanese definition of CTP

Choose uniformizers t_P, for $P \in C$ Galois-equivariantly. There are two evaluation based Galois-equivariant pairings:

- $\langle ., . \rangle_1 : \mathrm{Princ}(C) \times \mathrm{Div}^0(C) \to \mathbb{G}_m$.

$$(\mathrm{div}(f), D) \mapsto \prod_{P \in \mathrm{Supp}(D)} (f t_P^{-v_P(f)}(P))^{v_P(D)}.$$

- $\langle ., . \rangle_2 : \mathrm{Div}^0(C) \times \mathrm{Princ}(C) \to \mathbb{G}_m$.

$$(D, \mathrm{div}(f)) \mapsto \prod_{P \in \mathrm{Supp}(D)} (-1)^{v_P(f) v_P(D)} (f t_P^{-v_P(f)}(P))^{v_P(D)}.$$

These pairings agree on the diagonal $\mathrm{Princ}(C) \times \mathrm{Princ}(C)$ (strong Weil reciprocity), and induce cup products $\cup_1$ and $\cup_2$.

Albanese-Albanese definition of CTP

Choose uniformizers t_P, for $P \in C$ Galois-equivariantly. There are two evaluation based Galois-equivariant pairings:

- $\langle ., . \rangle_1 : \mathrm{Princ}(C) \times \mathrm{Div}^0(C) \to \mathbb{G}_m$.

$$(\mathrm{div}(f), D) \mapsto \prod_{P \in \mathrm{Supp}(D)} (f t_P^{-v_P(f)}(P))^{v_P(D)}.$$

- $\langle ., . \rangle_2 : \mathrm{Div}^0(C) \times \mathrm{Princ}(C) \to \mathbb{G}_m$.

$$(D, \mathrm{div}(f)) \mapsto \prod_{P \in \mathrm{Supp}(D)} (-1)^{v_P(f) v_P(D)} (f t_P^{-v_P(f)}(P))^{v_P(D)}.$$

These pairings agree on the diagonal $\mathrm{Princ}(C) \times \mathrm{Princ}(C)$ (strong Weil reciprocity), and induce cup products $\cup_1$ and $\cup_2$.

Albanese-Albanese definition of CTP

Choose uniformizers t_P, for $P \in C$ Galois-equivariantly. There are two evaluation based Galois-equivariant pairings:

- $\langle .,. \rangle_1 : \mathrm{Princ}(C) \times \mathrm{Div}^0(C) \to \mathbb{G}_m$.

$$(\mathrm{div}(f), D) \mapsto \prod_{P \in \mathrm{Supp}(D)} (ft_P^{-v_P(f)}(P))^{v_p(D)}.$$

- $\langle .,. \rangle_2 : \mathrm{Div}^0(C) \times \mathrm{Princ}(C) \to \mathbb{G}_m$.

$$(D, \mathrm{div}(f)) \mapsto \prod_{P \in \mathrm{Supp}(D)} (-1)^{v_P(f)v_P(D)}(ft_P^{-v_P(f)}(P))^{v_p(D)}.$$

These pairings agree on the diagonal $\mathrm{Princ}(C) \times \mathrm{Princ}(C)$ (strong Weil reciprocity), and induce cup products $\cup_1$ and $\cup_2$.

Albanese-Albanese definition of CTP

Choose uniformizers t_P, for $P \in C$ Galois-equivariantly. There are two evaluation based Galois-equivariant pairings:

- $\langle .,. \rangle_1 : \mathrm{Princ}(C) \times \mathrm{Div}^0(C) \to \mathbb{G}_m$.

$$(\mathrm{div}(f), D) \mapsto \prod_{P \in \mathrm{Supp}(D)} (f t_P^{-v_P(f)}(P))^{v_p(D)}.$$

- $\langle .,. \rangle_2 : \mathrm{Div}^0(C) \times \mathrm{Princ}(C) \to \mathbb{G}_m$.

$$(D, \mathrm{div}(f)) \mapsto \prod_{P \in \mathrm{Supp}(D)} (-1)^{v_P(f) v_P(D)} (f t_P^{-v_P(f)}(P))^{v_p(D)}.$$

These pairings agree on the diagonal $\mathrm{Princ}(C) \times \mathrm{Princ}(C)$ (strong Weil reciprocity), and induce cup products $\cup_1$ and $\cup_2$.

Albanese-Albanese definition of CTP

Choose uniformizers t_P, for $P \in C$ Galois-equivariantly. There are two evaluation based Galois-equivariant pairings:

- $\langle .,. \rangle_1 : \mathrm{Princ}(C) \times \mathrm{Div}^0(C) \to \mathbb{G}_m$.

$$(\mathrm{div}(f), D) \mapsto \prod_{P \in \mathrm{Supp}(D)} (f t_P^{-v_P(f)}(P))^{v_p(D)}.$$

- $\langle .,. \rangle_2 : \mathrm{Div}^0(C) \times \mathrm{Princ}(C) \to \mathbb{G}_m$.

$$(D, \mathrm{div}(f)) \mapsto \prod_{P \in \mathrm{Supp}(D)} (-1)^{v_P(f) v_P(D)} (f t_P^{-v_P(f)}(P))^{v_p(D)}.$$

These pairings agree on the diagonal $\mathrm{Princ}(C) \times \mathrm{Princ}(C)$ (strong Weil reciprocity), and induce cup products $\cup_1$ and $\cup_2$.

Global part

Let $a, a' \in \mathrm{H}^1(G_k, J[n])$ and let $\alpha, \alpha' \in \mathrm{Z}^1(G_k, J[n])$ represent the classes a, a'.

Lift α, α' to 1-cochains $\mathfrak{a}$, $\mathfrak{a}'$ with values in $\mathrm{Div}^0(C)$.

Using cohomology on the exact sequence:

$$0 \to \mathrm{Princ}(C) \to \mathrm{Div}^0(C) \to \mathrm{Pic}^0(C) \to 0,$$

we get a 3-cochain:

$$\eta := \partial\mathfrak{a} \cup_1 \mathfrak{a}' - \mathfrak{a} \cup_2 \partial\mathfrak{a}',$$

and compatibility of $\cup_1$, $\cup_2$ on the diagonal implies $\eta \in \mathrm{Z}^3(G_k, \mathbb{G}_m)$ i.e. a 3-cocycle

Since $\mathrm{H}^3(G_k, \mathbb{G}_m) = 0$, i.e. there exists $\epsilon \in \mathrm{C}^2(G_k, \mathbb{G}_m)$ s.t. $\partial\epsilon = \eta$.

Global bottleneck: Finding ϵ (our *Nemo*!)

Global part

Let $a, a' \in \mathrm{H}^1(G_k, J[n])$ and let $\alpha, \alpha' \in \mathrm{Z}^1(G_k, J[n])$ represent the classes a, a'.

Lift α, α' to 1-cochains $\mathfrak{a}$, $\mathfrak{a}'$ with values in $\mathrm{Div}^0(C)$.

Using cohomology on the exact sequence:

$$0 \to \mathrm{Princ}(C) \to \mathrm{Div}^0(C) \to \mathrm{Pic}^0(C) \to 0,$$

we get a 3-cochain:

$$\eta := \partial\mathfrak{a} \cup_1 \mathfrak{a}' - \mathfrak{a} \cup_2 \partial\mathfrak{a}',$$

and compatibility of $\cup_1$, $\cup_2$ on the diagonal implies $\eta \in \mathrm{Z}^3(G_k, \mathbb{G}_m)$ i.e. a 3-cocycle

Since $\mathrm{H}^3(G_k, \mathbb{G}_m) = 0$, i.e. there exists $\epsilon \in \mathrm{C}^2(G_k, \mathbb{G}_m)$ s.t. $\partial\epsilon = \eta$.

Global bottleneck: Finding ϵ (our *Nemo*!)

Global part

Let $a, a' \in \mathrm{H}^1(G_k, J[n])$ and let $\alpha, \alpha' \in \mathrm{Z}^1(G_k, J[n])$ represent the classes a, a'.
Lift α, α' to 1-cochains $\mathfrak{a}$, $\mathfrak{a}'$ with values in $\mathrm{Div}^0(C)$.
Using cohomology on the exact sequence:

$$0 \to \mathrm{Princ}(C) \to \mathrm{Div}^0(C) \to \mathrm{Pic}^0(C) \to 0,$$

we get a 3-cochain:

$$\eta := \partial\mathfrak{a} \cup_1 \mathfrak{a}' - \mathfrak{a} \cup_2 \partial\mathfrak{a}',$$

and compatibility of $\cup_1$, $\cup_2$ on the diagonal implies $\eta \in \mathrm{Z}^3(G_k, \mathbb{G}_m)$ i.e. a 3-cocycle
Since $\mathrm{H}^3(G_k, \mathbb{G}_m) = 0$, i.e. there exists $\epsilon \in \mathrm{C}^2(G_k, \mathbb{G}_m)$ s.t. $\partial\epsilon = \eta$.
Global bottleneck: Finding ϵ (our *Nemo*!)

Global part

Let $a, a' \in \mathrm{H}^1(G_k, J[n])$ and let $\alpha, \alpha' \in \mathrm{Z}^1(G_k, J[n])$ represent the classes a, a'.
Lift α, α' to 1-cochains $\mathfrak{a}$, $\mathfrak{a}'$ with values in $\mathrm{Div}^0(C)$.
Using cohomology on the exact sequence:

$$0 \to \mathrm{Princ}(C) \to \mathrm{Div}^0(C) \to \mathrm{Pic}^0(C) \to 0,$$

we get a 3-cochain:

$$\eta := \partial\mathfrak{a} \cup_1 \mathfrak{a}' - \mathfrak{a} \cup_2 \partial\mathfrak{a}',$$

and compatibility of $\cup_1$, $\cup_2$ on the diagonal implies $\eta \in \mathrm{Z}^3(G_k, \mathbb{G}_m)$ i.e. a 3-cocycle
Since $\mathrm{H}^3(G_k, \mathbb{G}_m) = 0$, i.e. there exists $\epsilon \in \mathrm{C}^2(G_k, \mathbb{G}_m)$ s.t. $\partial\epsilon = \eta$.
Global bottleneck: Finding ϵ (our *Nemo*!)

Global part

Let $a, a' \in \mathrm{H}^1(G_k, J[n])$ and let $\alpha, \alpha' \in \mathrm{Z}^1(G_k, J[n])$ represent the classes a, a'.
Lift α, α' to 1-cochains $\mathfrak{a}$, $\mathfrak{a}'$ with values in $\mathrm{Div}^0(C)$.
Using cohomology on the exact sequence:

$$0 \to \mathrm{Princ}(C) \to \mathrm{Div}^0(C) \to \mathrm{Pic}^0(C) \to 0,$$

we get a 3-cochain:

$$\eta := \partial\mathfrak{a} \cup_1 \mathfrak{a}' - \mathfrak{a} \cup_2 \partial\mathfrak{a}',$$

and compatibility of $\cup_1$, $\cup_2$ on the diagonal implies $\eta \in \mathrm{Z}^3(G_k, \mathbb{G}_m)$ i.e. a 3-cocycle
Since $\mathrm{H}^3(G_k, \mathbb{G}_m) = 0$, i.e. there exists $\epsilon \in \mathrm{C}^2(G_k, \mathbb{G}_m)$ s.t. $\partial\epsilon = \eta$.
Global bottleneck: Finding ϵ (our *Nemo*!)

Global part

Let $a, a' \in \mathrm{H}^1(G_k, J[n])$ and let $\alpha, \alpha' \in \mathrm{Z}^1(G_k, J[n])$ represent the classes a, a'.

Lift α, α' to 1-cochains $\mathfrak{a}$, $\mathfrak{a}'$ with values in $\mathrm{Div}^0(C)$.

Using cohomology on the exact sequence:

$$0 \to \mathrm{Princ}(C) \to \mathrm{Div}^0(C) \to \mathrm{Pic}^0(C) \to 0,$$

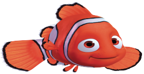
we get a 3-cochain:

$$\eta := \partial\mathfrak{a} \cup_1 \mathfrak{a}' - \mathfrak{a} \cup_2 \partial\mathfrak{a}',$$

and compatibility of $\cup_1$, $\cup_2$ on the diagonal implies $\eta \in \mathrm{Z}^3(G_k, \mathbb{G}_m)$ i.e. a 3-cocycle

Since $\mathrm{H}^3(G_k, \mathbb{G}_m) = 0$, i.e. there exists $\epsilon \in \mathrm{C}^2(G_k, \mathbb{G}_m)$ s.t. $\partial\epsilon = \eta$.

Global bottleneck: Finding ϵ (our *Nemo*!)



Local part

Let v be a place of k. If $a \in \mathrm{Sel}^{(n)}(J)$ then there is a $\beta_v \in J(\overline{k_v})$ such that $\alpha_v = \partial\beta_v$.
Let $\mathfrak{b}_v \in \mathrm{Div}^0(C)$ represent β. Then

$$\gamma_v := (\mathfrak{a}_v - \partial\mathfrak{b}_v) \cup_1 \mathfrak{a}'_v - \mathfrak{b}_v \cup_2 \partial\mathfrak{a}'_v - \epsilon_v$$

is a 2-cocycle.
We have $[\gamma_v] \in \mathrm{Br}\,(k_v)$ and the CTP is defined as:

Definition 1

$$\langle a, a' \rangle_{\mathrm{CT}} := \sum_v \mathrm{inv}_v([\gamma_v]).$$

Local bottleneck: Computing $\mathrm{inv}_v([\gamma_v])$ (generically solvable!).

Local part

Let v be a place of k. If $a \in \mathrm{Sel}^{(n)}(J)$ then there is a $\beta_v \in J(\overline{k_v})$ such that $\alpha_v = \partial\beta_v$.

Let $\mathfrak{b}_v \in \mathrm{Div}^0(C)$ represent β. Then

$$\gamma_v := (\mathfrak{a}_v - \partial\mathfrak{b}_v) \cup_1 \mathfrak{a}'_v - \mathfrak{b}_v \cup_2 \partial\mathfrak{a}'_v - \epsilon_v$$

is a 2-cocycle.

We have $[\gamma_v] \in \mathrm{Br}(k_v)$ and the CTP is defined as:

Definition 1

$$\langle a, a' \rangle_{\mathrm{CT}} := \sum_v \mathrm{inv}_v([\gamma_v]).$$

Local bottleneck: Computing $\mathrm{inv}_v([\gamma_v])$ (generically solvable!).

Local part

Let v be a place of k. If $a \in \mathrm{Sel}^{(n)}(J)$ then there is a $\beta_v \in J(\overline{k_v})$ such that $\alpha_v = \partial\beta_v$.
Let $\mathfrak{b}_v \in \mathrm{Div}^0(C)$ represent β. Then

$$\gamma_v := (\mathfrak{a}_v - \partial\mathfrak{b}_v) \cup_1 \mathfrak{a}'_v - \mathfrak{b}_v \cup_2 \partial\mathfrak{a}'_v - \epsilon_v$$

is a 2-cocycle.
We have $[\gamma_v] \in \mathrm{Br}(k_v)$ and the CTP is defined as:

Definition 1

$$\langle a, a' \rangle_{\mathrm{CT}} := \sum_v \mathrm{inv}_v([\gamma_v]).$$

Local bottleneck: Computing $\mathrm{inv}_v([\gamma_v])$ (generically solvable!).

Local part

Let v be a place of k. If $a \in \mathrm{Sel}^{(n)}(J)$ then there is a $\beta_v \in J(\overline{k_v})$ such that $\alpha_v = \partial\beta_v$.
Let $\mathfrak{b}_v \in \mathrm{Div}^0(C)$ represent β. Then

$$\gamma_v := (\mathfrak{a}_v - \partial\mathfrak{b}_v) \cup_1 \mathfrak{a}'_v - \mathfrak{b}_v \cup_2 \partial\mathfrak{a}'_v - \epsilon_v$$

is a 2-cocycle.
We have $[\gamma_v] \in \mathrm{Br}(k_v)$ and the CTP is defined as:

Definition 1

$$\langle a, a' \rangle_{\mathrm{CT}} := \sum_v \mathrm{inv}_v([\gamma_v]).$$

Local bottleneck: Computing $\mathrm{inv}_v([\gamma_v])$ (generically solvable!).

Local part

Let v be a place of k. If $a \in \mathrm{Sel}^{(n)}(J)$ then there is a $\beta_v \in J(\overline{k_v})$ such that $\alpha_v = \partial\beta_v$.
Let $\mathfrak{b}_v \in \mathrm{Div}^0(C)$ represent β. Then

$$\gamma_v := (\mathfrak{a}_v - \partial\mathfrak{b}_v) \cup_1 \mathfrak{a}'_v - \mathfrak{b}_v \cup_2 \partial\mathfrak{a}'_v - \epsilon_v$$

is a 2-cocycle.
We have $[\gamma_v] \in \mathrm{Br}(k_v)$ and the CTP is defined as:

Definition 1

$$\langle a, a' \rangle_{\mathrm{CT}} := \sum_v \mathrm{inv}_v([\gamma_v]).$$

Local bottleneck: Computing $\mathrm{inv}_v([\gamma_v])$ (generically solvable!).

Local part

Let v be a place of k. If $a \in \mathrm{Sel}^{(n)}(J)$ then there is a $\beta_v \in J(\overline{k_v})$ such that $\alpha_v = \partial\beta_v$.
Let $\mathfrak{b}_v \in \mathrm{Div}^0(C)$ represent β. Then

$$\gamma_v := (\mathfrak{a}_v - \partial\mathfrak{b}_v) \cup_1 \mathfrak{a}'_v - \mathfrak{b}_v \cup_2 \partial\mathfrak{a}'_v - \epsilon_v$$

is a 2-cocycle.
We have $[\gamma_v] \in \mathrm{Br}(k_v)$ and the CTP is defined as:

Definition 1

$$\langle a, a' \rangle_{\mathrm{CT}} := \sum_v \mathrm{inv}_v([\gamma_v]).$$

Local bottleneck: Computing $\mathrm{inv}_v([\gamma_v])$ (generically solvable!).

Local part

Let v be a place of k. If $a \in \mathrm{Sel}^{(n)}(J)$ then there is a $\beta_v \in J(\overline{k_v})$ such that $\alpha_v = \partial\beta_v$.
Let $\mathfrak{b}_v \in \mathrm{Div}^0(C)$ represent β. Then

$$\gamma_v := (\mathfrak{a}_v - \partial\mathfrak{b}_v) \cup_1 \mathfrak{a}'_v - \mathfrak{b}_v \cup_2 \partial\mathfrak{a}'_v - \epsilon_v$$

is a 2-cocycle.
We have $[\gamma_v] \in \mathrm{Br}(k_v)$ and the CTP is defined as:

Definition 1

$$\langle a, a' \rangle_{\mathrm{CT}} := \sum_v \mathrm{inv}_v([\gamma_v]).$$

Local bottleneck: Computing $\mathrm{inv}_v([\gamma_v])$ (generically solvable!).

Previous works

- Previous works have mainly focused on elliptic curves:

Authors	Domain
Cassels	$\mathrm{Sel}^{(2)}(E) \times \mathrm{Sel}^{(2)}(E)$
Swinnerton-Dyer	$\mathrm{Sel}^{(2^m)}(E) \times \mathrm{Sel}^{(2)}(E)$
van Beek & Fisher	$\mathrm{Sel}^{(\phi)}(E) \times \mathrm{Sel}^{(\phi)}(E)$ deg(ϕ) is odd prime
Fischer & Newton	$\mathrm{Sel}^{(3)}(E) \times \mathrm{Sel}^{(3)}(E)$

- For 2-Selmer groups of genus 2 Jacobians, Jiali Yan has an algorithm (assuming some conditions).
- We handle the case of 2-Selmer groups of odd-degree hyperelliptic Jacobians completely!

Previous works

- Previous works have mainly focused on elliptic curves:

Authors	Domain
Cassels	$\mathrm{Sel}^{(2)}(E) \times \mathrm{Sel}^{(2)}(E)$
Swinnerton-Dyer	$\mathrm{Sel}^{(2^m)}(E) \times \mathrm{Sel}^{(2)}(E)$
van Beek & Fisher	$\mathrm{Sel}^{(\phi)}(E) \times \mathrm{Sel}^{(\phi)}(E)$ $\deg(\phi)$ is odd prime
Fischer & Newton	$\mathrm{Sel}^{(3)}(E) \times \mathrm{Sel}^{(3)}(E)$

- For 2-Selmer groups of genus 2 Jacobians, Jiali Yan has an algorithm (assuming some conditions).
- We handle the case of 2-Selmer groups of odd-degree hyperelliptic Jacobians completely!

Previous works

- Previous works have mainly focused on elliptic curves:

Authors	Domain
Cassels	$\mathrm{Sel}^{(2)}(E) \times \mathrm{Sel}^{(2)}(E)$
Swinnerton-Dyer	$\mathrm{Sel}^{(2^m)}(E) \times \mathrm{Sel}^{(2)}(E)$
van Beek & Fisher	$\mathrm{Sel}^{(\phi)}(E) \times \mathrm{Sel}^{(\phi)}(E)$ $\deg(\phi)$ is odd prime
Fischer & Newton	$\mathrm{Sel}^{(3)}(E) \times \mathrm{Sel}^{(3)}(E)$

- For 2-Selmer groups of genus 2 Jacobians, Jiali Yan has an algorithm (assuming some conditions).
- We handle the case of 2-Selmer groups of odd-degree hyperelliptic Jacobians completely!

Previous works

- Previous works have mainly focused on elliptic curves:

Authors	Domain
Cassels	$\mathrm{Sel}^{(2)}(E) \times \mathrm{Sel}^{(2)}(E)$
Swinnerton-Dyer	$\mathrm{Sel}^{(2^m)}(E) \times \mathrm{Sel}^{(2)}(E)$
van Beek & Fisher	$\mathrm{Sel}^{(\phi)}(E) \times \mathrm{Sel}^{(\phi)}(E)$ $\deg(\phi)$ is odd prime
Fischer & Newton	$\mathrm{Sel}^{(3)}(E) \times \mathrm{Sel}^{(3)}(E)$

- For 2-Selmer groups of genus 2 Jacobians, Jiali Yan has an algorithm (assuming some conditions).
- We handle the case of 2-Selmer groups of odd-degree hyperelliptic Jacobians completely!

Existence of a nice ϵ

One can compute ϵ if a splitting field of η is known!

For a cochain $x \in \mathrm{C}^1(G_k, M)$, let $\mathrm{fod}(x)$ be the field of definition of x, i.e. minimal field extension L s.t. $x = \inf(y)$ for some $y \in \mathrm{C}^i(\mathrm{Gal}(L/k), M(L))$. Let

$$\mathrm{loc}^2(J[n]) : \mathrm{H}^2(G_k, J[n]) \to \prod_v \mathrm{H}^2(G_k, J[n]).$$

Proposition 2

If $\mathrm{loc}^2(J[n])$ is injective, then there is a 2-cochain ϵ s.t. $\partial\epsilon = \eta$ satisfying:

- *For $\sigma, \tau, \tau' \in G_k$, $\epsilon(\sigma,\tau) = \epsilon(\sigma,\tau')$ if $\tau\big|_{K'} = \tau'\big|_{K'}$, where $K' := \mathrm{fod}(\alpha')$.*
- *$\epsilon(\sigma,\tau) = 1$ if $\tau\big|_{K'} = id$.*

Existence of a nice ϵ

One can compute ϵ if a splitting field of η is known!
For a cochain $x \in \mathrm{C}^1(G_k, M)$, let $\mathrm{fod}(x)$ be the field of definition of x, i.e. minimal field extension L s.t. $x = \inf(y)$ for some $y \in \mathrm{C}^i(\mathrm{Gal}(L/k), M(L))$. Let

$$\mathrm{loc}^2(J[n]) : \mathrm{H}^2(G_k, J[n]) \to \prod_v \mathrm{H}^2(G_k, J[n]).$$

Proposition 2

If $\mathrm{loc}^2(J[n])$ is injective, then there is a 2-cochain ϵ s.t. $\partial\epsilon = \eta$ satisfying:

- *For $\sigma, \tau, \tau' \in G_k$, $\epsilon(\sigma,\tau) = \epsilon(\sigma,\tau')$ if $\tau\big|_{K'} = \tau'\big|_{K'}$, where $K' := \mathrm{fod}(\alpha')$.*
- *$\epsilon(\sigma,\tau) = 1$ if $\tau\big|_{K'} = id$.*

Existence of a nice ϵ

One can compute ϵ if a splitting field of η is known!
For a cochain $x \in \mathrm{C}^1(G_k, M)$, let $\mathrm{fod}(x)$ be the field of definition of x, i.e. minimal field extension L s.t. $x = \inf(y)$ for some $y \in \mathrm{C}^i(\mathrm{Gal}(L/k), M(L))$. Let

$$\mathrm{loc}^2(J[n]) : \mathrm{H}^2(G_k, J[n]) \to \prod_v \mathrm{H}^2(G_k, J[n]).$$

Proposition 2

If $\mathrm{loc}^2(J[n])$ is injective, then there is a 2-cochain ϵ s.t. $\partial\epsilon = \eta$ satisfying:

- *For $\sigma, \tau, \tau' \in G_k$, $\epsilon(\sigma, \tau) = \epsilon(\sigma, \tau')$ if $\tau\big|_{K'} = \tau'\big|_{K'}$, where $K' := \mathrm{fod}(\alpha')$.*
- *$\epsilon(\sigma, \tau) = 1$ if $\tau\big|_{K'} = id$.*

Existence of a nice ϵ

One can compute ϵ if a splitting field of η is known!
For a cochain $x \in \mathrm{C}^1(G_k, M)$, let $\mathrm{fod}(x)$ be the field of definition of x, i.e. minimal field extension L s.t. $x = \inf(y)$ for some $y \in \mathrm{C}^i(\mathrm{Gal}(L/k), M(L))$. Let

$$\mathrm{loc}^2(J[n]) : \mathrm{H}^2(G_k, J[n]) \to \prod_v \mathrm{H}^2(G_k, J[n]).$$

Proposition 2

If $\mathrm{loc}^2(J[n])$ is injective, then there is a 2-cochain ϵ s.t. $\partial\epsilon = \eta$ satisfying:

- *For $\sigma, \tau, \tau' \in G_k$, $\epsilon(\sigma,\tau) = \epsilon(\sigma,\tau')$ if $\tau\big|_{K'} = \tau'\big|_{K'}$, where $K' := \mathrm{fod}(\alpha')$.*
- *$\epsilon(\sigma,\tau) = 1$ if $\tau\big|_{K'} = id$.*

Existence of a nice ϵ

One can compute ϵ if a splitting field of η is known!
For a cochain $x \in \mathrm{C}^1(G_k, M)$, let $\mathrm{fod}(x)$ be the field of definition of x, i.e. minimal field extension L s.t. $x = \inf(y)$ for some $y \in \mathrm{C}^i(\mathrm{Gal}(L/k), M(L))$. Let

$$\mathrm{loc}^2(J[n]) : \mathrm{H}^2(G_k, J[n]) \to \prod_v \mathrm{H}^2(G_k, J[n]).$$

Proposition 2

If $\mathrm{loc}^2(J[n])$ is injective, then there is a 2-cochain ϵ s.t. $\partial\epsilon = \eta$ satisfying:

- *For $\sigma, \tau, \tau' \in G_k$, $\epsilon(\sigma,\tau) = \epsilon(\sigma,\tau')$ if $\tau\big|_{K'} = \tau'\big|_{K'}$, where $K' := \mathrm{fod}(\alpha')$.*
- *$\epsilon(\sigma,\tau) = 1$ if $\tau\big|_{K'} = id$.*

Existence of a nice ϵ

One can compute ϵ if a splitting field of η is known!
For a cochain $x \in \mathrm{C}^1(G_k, M)$, let $\mathrm{fod}(x)$ be the field of definition of x, i.e. minimal field extension L s.t. $x = \inf(y)$ for some $y \in \mathrm{C}^i(\mathrm{Gal}(L/k), M(L))$. Let

$$\mathrm{loc}^2(J[n]) : \mathrm{H}^2(G_k, J[n]) \to \prod_v \mathrm{H}^2(G_k, J[n]).$$

Proposition 2

If $\mathrm{loc}^2(J[n])$ is injective, then there is a 2-cochain ϵ s.t. $\partial\epsilon = \eta$ satisfying:

- *For $\sigma, \tau, \tau' \in G_k$, $\epsilon(\sigma, \tau) = \epsilon(\sigma, \tau')$ if $\tau\big|_{K'} = \tau'\big|_{K'}$, where $K' := \mathrm{fod}(\alpha')$.*
- *$\epsilon(\sigma, \tau) = 1$ if $\tau\big|_{K'} = id$.*

Sketch of proof of proposition 2

- Use cohomology on commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & J[n] & \longrightarrow & J[n^2] & \xrightarrow{[n]} & J[n] & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & J[n] & \longrightarrow & J & \xrightarrow{[n]} & J & \longrightarrow & 0. \end{array} \tag{4.1}$$

to show: if $a \in \mathrm{Sel}^{(n)}(J)$, then $\delta(a) = 0$, where $\delta : \mathrm{H}^1(G_k, J[n]) \to \mathrm{H}^2(G_k, J[n])$.

- Expressing the Weil pairing in terms of $\langle \cdot, \cdot \rangle_1$ and $\langle \cdot, \cdot \rangle_2$, plus some identities of cup-product imply the proposition.

Sketch of proof of proposition 2

- Use cohomology on commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & J[n] & \longrightarrow & J[n^2] & \xrightarrow{[n]} & J[n] & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & J[n] & \longrightarrow & J & \xrightarrow{[n]} & J & \longrightarrow & 0. \end{array} \tag{4.1}$$

to show: if $a \in \mathrm{Sel}^{(n)}(J)$, then $\delta(a) = 0$, where $\delta : \mathrm{H}^1(G_k, J[n]) \to \mathrm{H}^2(G_k, J[n])$.

- Expressing the Weil pairing in terms of $\langle \cdot, \cdot \rangle_1$ and $\langle \cdot, \cdot \rangle_2$, plus some identities of cup-product imply the proposition.

Splitting field of η

Lemma 3

Let $K := \mathrm{fod}(\alpha)$, $K' := \mathrm{fod}(\alpha')$ and assume that α' takes values defined over k. If $\mathrm{loc}^2(J[n])$ is injective, and one of the following is satisfied:

- $K \cap K' = k$.
- $[K' : k] = 2$.

Then η splits in KK', i.e. its field of definition.

Remark 4

The proof of the above lemma constructs ϵ explicitly.

Since $k(J[n]) \subset K \cap K'$, lemma 3 cannot be applied (at least directly) to determine a splitting field of η even for $n = 2$.

Splitting field of η

Lemma 3

Let $K := \mathrm{fod}(\alpha)$, $K' := \mathrm{fod}(\alpha')$ and assume that α' takes values defined over k. If $\mathrm{loc}^2(J[n])$ is injective, and one of the following is satisfied:

- $K \cap K' = k$.
- $[K' : k] = 2$.

Then η splits in KK', i.e. its field of definition.

Remark 4

The proof of the above lemma constructs ϵ explicitly.

Since $k(J[n]) \subset K \cap K'$, lemma 3 cannot be applied (at least directly) to determine a splitting field of η even for $n = 2$.

Splitting field of η

Lemma 3

Let $K := \mathrm{fod}(\alpha)$, $K' := \mathrm{fod}(\alpha')$ and assume that α' takes values defined over k. If $\mathrm{loc}^2(J[n])$ is injective, and one of the following is satisfied:

- $K \cap K' = k$.
- $[K' : k] = 2$.

Then η splits in KK', i.e. its field of definition.

Remark 4

The proof of the above lemma constructs ϵ explicitly.

Since $k(J[n]) \subset K \cap K'$, lemma 3 cannot be applied (at least directly) to determine a splitting field of η even for $n = 2$.

Making lemma 3 useful when $n = 2$ (survival instinct!)

We have:

$$H^1(G_k, J[2]) \simeq \ker\left(N : L^\times/(L^\times)^2 \to k^\times/(k^\times)^2\right),$$

where $L := k[x]/(f(x))$. and $N : L^\times \to k^\times$ is the norm map.

- Let T_i be the representative of i^{th} orbit of Δ.
- For $1 \leq j \leq 2g+1$ choose $d'_j \in k(T_j)^\times$ such that $(d'_1, d'_2, \ldots, d'_{2g+1})$ represents α'.
- d'_js satisfy the condition: for $1 \leq n, m \leq 2g+1$, d'_m and d'_n are conjugates if T_n and T_m are.

First, note that $\mathrm{loc}^2(J[2])$ is injective (consequence of Poitou-Tate duality).

Making lemma 3 useful when $n = 2$ (survival instinct!)

We have:

$$H^1(G_k, J[2]) \simeq \ker\left(N : L^\times/(L^\times)^2 \to k^\times/(k^\times)^2\right),$$

where $L := k[x]/(f(x))$. and $N : L^\times \to k^\times$ is the norm map.

- Let T_i be the representative of i^{th} orbit of Δ.
- For $1 \leq j \leq 2g+1$ choose $d'_j \in k(T_j)^\times$ such that $(d'_1, d'_2, \ldots, d'_{2g+1})$ represents α'.
- d'_js satisfy the condition: for $1 \leq n, m \leq 2g+1$, d'_m and d'_n are conjugates if T_n and T_m are.

First, note that $\mathrm{loc}^2(J[2])$ is injective (consequence of Poitou-Tate duality).

Making lemma 3 useful when $n = 2$ (survival instinct!)

We have:

$$H^1(G_k, J[2]) \simeq \ker \left(N : L^\times/(L^\times)^2 \to k^\times/(k^\times)^2 \right),$$

where $L := k[x]/(f(x))$. and $N : L^\times \to k^\times$ is the norm map.

- Let T_i be the representative of i^{th} orbit of Δ.
- For $1 \le j \le 2g+1$ choose $d'_j \in k(T_j)^\times$ such that $(d'_1, d'_2, \ldots, d'_{2g+1})$ represents α'.
- d'_js satisfy the condition: for $1 \le n, m \le 2g+1$, d'_m and d'_n are conjugates if T_n and T_m are.

First, note that $\text{loc}^2(J[2])$ is injective (consequence of Poitou-Tate duality).

Making lemma 3 useful when $n = 2$ (survival instinct!)

We have:

$$H^1(G_k, J[2]) \simeq \ker\left(N : L^\times/(L^\times)^2 \to k^\times/(k^\times)^2\right),$$

where $L := k[x]/(f(x))$. and $N : L^\times \to k^\times$ is the norm map.

- Let T_i be the representative of i^{th} orbit of Δ.
- For $1 \leq j \leq 2g+1$ choose $d'_j \in k(T_j)^\times$ such that $(d'_1, d'_2, \ldots, d'_{2g+1})$ represents α'.
- d'_js satisfy the condition: for $1 \leq n, m \leq 2g+1$, d'_m and d'_n are conjugates if T_n and T_m are.

First, note that $\mathrm{loc}^2(J[2])$ is injective (consequence of Poitou-Tate duality).

Making lemma 3 useful when $n = 2$ (survival instinct!)

We have:

$$H^1(G_k, J[2]) \simeq \ker\left(N : L^\times/(L^\times)^2 \to k^\times/(k^\times)^2\right),$$

where $L := k[x]/(f(x))$. and $N : L^\times \to k^\times$ is the norm map.

- Let T_i be the representative of i^{th} orbit of Δ.
- For $1 \leq j \leq 2g+1$ choose $d'_j \in k(T_j)^\times$ such that $(d'_1, d'_2, \ldots, d'_{2g+1})$ represents α'.
- d'_js satisfy the condition: for $1 \leq n, m \leq 2g+1$, d'_m and d'_n are conjugates if T_n and T_m are.

First, note that $\mathrm{loc}^2(J[2])$ is injective (consequence of Poitou-Tate duality).

- We choose (we can) $\mathfrak{a}'$ to be $\sum_{\text{orbits}} \operatorname{cor}_{G_{k(T_i)}}^{G_k} \mathfrak{t}_i'$, where $\mathfrak{t}_i' \in C^1(G_{k(T_i)}, \langle (T_i) - (T_0) \rangle)$ is given by:

$$\mathfrak{t}_i'(\sigma) := \begin{cases} 0 & \sigma(\sqrt{d_i'}) = \sqrt{d_i'} \\ (T_i) - (T_0) & \sigma(\sqrt{d_i'}) = -\sqrt{d_i'}, \end{cases}$$

- The identity $x \cup \operatorname{cor}(y) = \operatorname{cor}(\operatorname{res}(x) \cup y)$ implies that it is enough to trivialize 3-cocycles

$$\eta_i := \partial \operatorname{res}(\mathfrak{a}) \cup_1 \mathfrak{t}_i' - \operatorname{res}(\mathfrak{a}) \cup_2 \partial \mathfrak{t}_i' \in Z^3(G_{k(T_i)}, \mathbb{G}_m).$$

Now $[k(T_i)(\sqrt{d_i'}) : k(T_i)] = 2$ and values of $\mathfrak{t}_i'$ are defined over $k(T_i)$. Use lemma 3 to find ϵ_is s.t. $\partial \epsilon_i = \eta_i$!

- We choose (we can) $\mathfrak{a}'$ to be $\sum_{\text{orbits}} \operatorname{cor}^{G_k}_{G_{k(T_i)}} \mathfrak{t}'_i$, where $\mathfrak{t}'_i \in \mathrm{C}^1(G_{k(T_i)}, \langle (T_i) - (T_0) \rangle)$ is given by:

$$\mathfrak{t}'_i(\sigma) := \begin{cases} 0 & \sigma(\sqrt{d'_i}) = \sqrt{d'_i} \\ (T_i) - (T_0) & \sigma(\sqrt{d'_i}) = -\sqrt{d'_i}, \end{cases}$$

- The identity $x \cup \operatorname{cor}(y) = \operatorname{cor}(\operatorname{res}(x) \cup y)$ implies that it is enough to trivialize 3-cocycles

$$\eta_i := \partial \operatorname{res}(\mathfrak{a}) \cup_1 \mathfrak{t}'_i - \operatorname{res}(\mathfrak{a}) \cup_2 \partial \mathfrak{t}'_i \in \mathrm{Z}^3(G_{k(T_i)}, \mathbb{G}_m).$$

Now $[k(T_i)(\sqrt{d'_i}) : k(T_i)] = 2$ and values of $\mathfrak{t}'_i$ are defined over $k(T_i)$. Use lemma 3 to find ϵ_is s.t. $\partial \epsilon_i = \eta_i$!

- We choose (we can) $\mathfrak{a}'$ to be $\sum_{\text{orbits}} \mathrm{cor}^{G_k}_{G_{k(T_i)}} \mathfrak{t}'_i$, where $\mathfrak{t}'_i \in \mathrm{C}^1(G_{k(T_i)}, \langle (T_i) - (T_0) \rangle)$ is given by:

$$\mathfrak{t}'_i(\sigma) := \begin{cases} 0 & \sigma(\sqrt{d'_i}) = \sqrt{d'_i} \\ (T_i) - (T_0) & \sigma(\sqrt{d'_i}) = -\sqrt{d'_i}, \end{cases}$$

- The identity $x \cup \mathrm{cor}(y) = \mathrm{cor}(\mathrm{res}(x) \cup y)$ implies that it is enough to trivialize 3-cocycles

$$\eta_i := \partial \mathrm{res}(\mathfrak{a}) \cup_1 \mathfrak{t}'_i - \mathrm{res}(\mathfrak{a}) \cup_2 \partial \mathfrak{t}'_i \in \mathrm{Z}^3(G_{k(T_i)}, \mathbb{G}_m).$$

Now $[k(T_i)(\sqrt{d'_i}) : k(T_i)] = 2$ and values of $\mathfrak{t}'_i$ are defined over $k(T_i)$. Use lemma 3 to find ϵ_is s.t. $\partial \epsilon_i = \eta_i$!

- We choose (we can) $\mathfrak{a}'$ to be $\sum_{\text{orbits}} \operatorname{cor}^{G_k}_{G_{k(T_i)}} \mathfrak{t}'_i$, where $\mathfrak{t}'_i \in \mathrm{C}^1(G_{k(T_i)}, \langle (T_i) - (T_0) \rangle)$ is given by:

$$\mathfrak{t}'_i(\sigma) := \begin{cases} 0 & \sigma(\sqrt{d'_i}) = \sqrt{d'_i} \\ (T_i) - (T_0) & \sigma(\sqrt{d'_i}) = -\sqrt{d'_i}, \end{cases}$$

- The identity $x \cup \operatorname{cor}(y) = \operatorname{cor}(\operatorname{res}(x) \cup y)$ implies that it is enough to trivialize 3-cocycles

$$\eta_i := \partial \operatorname{res}(\mathfrak{a}) \cup_1 \mathfrak{t}'_i - \operatorname{res}(\mathfrak{a}) \cup_2 \partial \mathfrak{t}'_i \in \mathrm{Z}^3(G_{k(T_i)}, \mathbb{G}_m).$$

Now $[k(T_i)(\sqrt{d'_i}) : k(T_i)] = 2$ and values of $\mathfrak{t}'_i$ are defined over $k(T_i)$. Use lemma 3 to find ϵ_is s.t. $\partial \epsilon_i = \eta_i$!

- We choose (we can) $\mathfrak{a}'$ to be $\sum_{\text{orbits}} \mathrm{cor}_{G_{k(T_i)}}^{G_k} \mathfrak{t}_i'$, where $\mathfrak{t}_i' \in \mathrm{C}^1(G_{k(T_i)}, \langle (T_i) - (T_0) \rangle)$ is given by:

$$\mathfrak{t}_i'(\sigma) := \begin{cases} 0 & \sigma(\sqrt{d_i'}) = \sqrt{d_i'} \\ (T_i) - (T_0) & \sigma(\sqrt{d_i'}) = -\sqrt{d_i'}, \end{cases}$$

- The identity $x \cup \mathrm{cor}(y) = \mathrm{cor}(\mathrm{res}(x) \cup y)$ implies that it is enough to trivialize 3-cocycles

$$\eta_i := \partial \mathrm{res}(\mathfrak{a}) \cup_1 \mathfrak{t}_i' - \mathrm{res}(\mathfrak{a}) \cup_2 \partial \mathfrak{t}_i' \in \mathrm{Z}^3(G_{k(T_i)}, \mathbb{G}_m).$$

Now $[k(T_i)(\sqrt{d_i'}) : k(T_i)] = 2$ and values of $\mathfrak{t}_i'$ are defined over $k(T_i)$. Use lemma 3 to find ϵ_is s.t. $\partial \epsilon_i = \eta_i$!

Form of the CTP

A similar trick for the local part gives

Theorem 5

Cassels-Tate pairing on 2-Selmer groups of odd-degree hyperelliptic Jacobians takes the following form:

$$(-1)^{2\langle a,a'\rangle_{\mathrm{CT}}} = \prod_{v} \prod_{G_{k_v}\text{-orbits}} (\delta_{v,i}, d_i')_{k_v(T_i)},$$

where $\delta_{v,i} \in k_v(T_i)^\times$ and $(\cdot,\cdot)_{k_v(T_i)}$ is the Hilbert's symbol.

Remark 6

Obtaining $\delta_{v,i}$ once we have the trivializers ϵ_i of η_i reduces to

- Finding the local point witnessing local triviality of α.
- Solving a Hilbert 90 problem.

Form of the CTP

A similar trick for the local part gives

Theorem 5

Cassels-Tate pairing on 2-Selmer groups of odd-degree hyperelliptic Jacobians takes the following form:

$$(-1)^{2\langle a,a'\rangle_{\mathrm{CT}}} = \prod_{v} \prod_{G_{k_v}\text{-orbits}} (\delta_{v,i}, d_i')_{k_v(T_i)},$$

where $\delta_{v,i} \in k_v(T_i)^\times$ and $(\cdot,\cdot)_{k_v(T_i)}$ is the Hilbert's symbol.

Remark 6

Obtaining $\delta_{v,i}$ once we have the trivializers ϵ_i of η_i reduces to

- Finding the local point witnessing local triviality of α.
- Solving a Hilbert 90 problem.

Form of the CTP

A similar trick for the local part gives

Theorem 5

Cassels-Tate pairing on 2-Selmer groups of odd-degree hyperelliptic Jacobians takes the following form:

$$(-1)^{2\langle a,a'\rangle_{\mathrm{CT}}} = \prod_{v} \prod_{G_{k_v}\text{-orbits}} (\delta_{v,i}, d_i')_{k_v(T_i)},$$

where $\delta_{v,i} \in k_v(T_i)^\times$ and $(\cdot,\cdot)_{k_v(T_i)}$ is the Hilbert's symbol.

Remark 6

Obtaining $\delta_{v,i}$ once we have the trivializers ϵ_i of η_i reduces to

- Finding the local point witnessing local triviality of α.
- Solving a Hilbert 90 problem.

Form of the CTP

A similar trick for the local part gives

Theorem 5

Cassels-Tate pairing on 2-Selmer groups of odd-degree hyperelliptic Jacobians takes the following form:

$$(-1)^{2\langle a,a'\rangle_{\mathrm{CT}}} = \prod_{v} \prod_{G_{k_v}\text{-orbits}} (\delta_{v,i}, d_i')_{k_v(T_i)},$$

where $\delta_{v,i} \in k_v(T_i)^\times$ *and* $(\cdot,\cdot)_{k_v(T_i)}$ *is the Hilbert's symbol.*

Remark 6

Obtaining $\delta_{v,i}$ once we have the trivializers ϵ_i of η_i reduces to

- Finding the local point witnessing local triviality of α.
- Solving a Hilbert 90 problem.

Form of the CTP

A similar trick for the local part gives

Theorem 5

Cassels-Tate pairing on 2-Selmer groups of odd-degree hyperelliptic Jacobians takes the following form:

$$(-1)^{2\langle a,a'\rangle_{\mathrm{CT}}} = \prod_{v} \prod_{G_{k_v}\text{-orbits}} (\delta_{v,i}, d_i')_{k_v(T_i)},$$

where $\delta_{v,i} \in k_v(T_i)^\times$ and $(\cdot,\cdot)_{k_v(T_i)}$ is the Hilbert's symbol.

Remark 6

Obtaining $\delta_{v,i}$ once we have the trivializers ϵ_i of η_i reduces to

- Finding the local point witnessing local triviality of α.
- Solving a Hilbert 90 problem.

Some remarks!

- Constructing ϵ in the proof of lemma 3 requires:
  - Trivializing some explicitly given 2-cocycles that represent trivial class in $\mathrm{Br}(k)$ (hard part).
  - Solving some Hilbert 90 problems explicitly (easy part).
  - Gluing the above information carefully.
- If C is an elliptic curve then the formula obtained by Cassels has exactly the same form as in theorem 5.
- If f splits over k and $g = 2$, then the above form reduces to the form of the formula obtained by Jiali Yan in her PhD thesis.

Some remarks!

- Constructing ϵ in the proof of lemma 3 requires:
  - Trivializing some explicitly given 2-cocycles that represent trivial class in $\mathrm{Br}(k)$ (hard part).
  - Solving some Hilbert 90 problems explicitly (easy part).
  - Gluing the above information carefully.
- If C is an elliptic curve then the formula obtained by Cassels has exactly the same form as in theorem 5.
- If f splits over k and $g = 2$, then the above form reduces to the form of the formula obtained by Jiali Yan in her PhD thesis.

Some remarks!

- Constructing ϵ in the proof of lemma 3 requires:
  - Trivializing some explicitly given 2-cocycles that represent trivial class in $\mathrm{Br}(k)$ (hard part).
  - Solving some Hilbert 90 problems explicitly (easy part).
  - Gluing the above information carefully.
- If C is an elliptic curve then the formula obtained by Cassels has exactly the same form as in theorem 5.
- If f splits over k and $g = 2$, then the above form reduces to the form of the formula obtained by Jiali Yan in her PhD thesis.

Some remarks!

- Constructing ϵ in the proof of lemma 3 requires:
  - Trivializing some explicitly given 2-cocycles that represent trivial class in $\mathrm{Br}(k)$ (hard part).
  - Solving some Hilbert 90 problems explicitly (easy part).
  - Gluing the above information carefully.
- If C is an elliptic curve then the formula obtained by Cassels has exactly the same form as in theorem 5.
- If f splits over k and $g = 2$, then the above form reduces to the form of the formula obtained by Jiali Yan in her PhD thesis.

Some remarks!

- Constructing ϵ in the proof of lemma 3 requires:
  - Trivializing some explicitly given 2-cocycles that represent trivial class in $\mathrm{Br}(k)$ (hard part).
  - Solving some Hilbert 90 problems explicitly (easy part).
  - Gluing the above information carefully.
- If C is an elliptic curve then the formula obtained by Cassels has exactly the same form as in theorem 5.
- If f splits over k and $g = 2$, then the above form reduces to the form of the formula obtained by Jiali Yan in her PhD thesis.

Some remarks!

- Constructing ϵ in the proof of lemma 3 requires:
  - Trivializing some explicitly given 2-cocycles that represent trivial class in $\mathrm{Br}(k)$ (hard part).
  - Solving some Hilbert 90 problems explicitly (easy part).
  - Gluing the above information carefully.

- If C is an elliptic curve then the formula obtained by Cassels has exactly the same form as in theorem 5.
- If f splits over k and $g = 2$, then the above form reduces to the form of the formula obtained by Jiali Yan in her PhD thesis.

Good curves

Definition 7

Recall e_is are the roots of f.

- An $\alpha = (d_1, \ldots, d_{2g+1}) \in \mathrm{Sel}^{(2)}(J)$ with $d_i \in k(e_i)^\times$ is said to be good if for each j, the conics $C_{ij} : d_i u^2 - d_j v^2 + e_i - e_j = 0$ has a solution over $k(e_i, e_j)$.
- A curve C is good if the subgroup generated by good elements is at most of index 2.

If α is good, then we can explicitly write ϵ_i such that $\partial \epsilon_i = \eta_i$.

For a fixed i, the values of ϵ_i are combinations of p_{ij}s where $p_{ij} := \sqrt{d_i} u^* + \sqrt{d_j} v^*$, and u^*, v^* satisfies C_{ij}.
Trivializing quaternion algebras corresponding to C_{ij} is probably simpler!

Good curves

Definition 7

Recall e_is are the roots of f.

- An $\alpha = (d_1, \dots, d_{2g+1}) \in \mathrm{Sel}^{(2)}(J)$ with $d_i \in k(e_i)^\times$ is said to be good if for each j, the conics $C_{ij} : d_i u^2 - d_j v^2 + e_i - e_j = 0$ has a solution over $k(e_i, e_j)$.
- A curve C is good if the subgroup generated by good elements is at most of index 2.

If α is good, then we can explicitly write ϵ_i such that $\partial \epsilon_i = \eta_i$.

For a fixed i, the values of ϵ_i are combinations of p_{ij}s where $p_{ij} := \sqrt{d_i} u^* + \sqrt{d_j} v^*$, and u^*, v^* satisfies C_{ij}.
Trivializing quaternion algebras corresponding to C_{ij} is probably simpler!

Good curves

Definition 7

Recall e_is are the roots of f.

- An $\alpha = (d_1, \ldots, d_{2g+1}) \in \mathrm{Sel}^{(2)}(J)$ with $d_i \in k(e_i)^\times$ is said to be good if for each j, the conics $C_{ij} : d_i u^2 - d_j v^2 + e_i - e_j = 0$ has a solution over $k(e_i, e_j)$.
- A curve C is good if the subgroup generated by good elements is at most of index 2.

If α is good, then we can explicitly write ϵ_i such that $\partial \epsilon_i = \eta_i$.

For a fixed i, the values of ϵ_i are combinations of p_{ij}s where $p_{ij} := \sqrt{d_i} u^* + \sqrt{d_j} v^*$, and u^*, v^* satisfies C_{ij}.
Trivializing quaternion algebras corresponding to C_{ij} is probably simpler!

Good curves

Definition 7

Recall e_is are the roots of f.

- An $\alpha = (d_1, \ldots, d_{2g+1}) \in \mathrm{Sel}^{(2)}(J)$ with $d_i \in k(e_i)^\times$ is said to be good if for each j, the conics $C_{ij} : d_i u^2 - d_j v^2 + e_i - e_j = 0$ has a solution over $k(e_i, e_j)$.
- A curve C is good if the subgroup generated by good elements is at most of index 2.

If α is good, then we can explicitly write ϵ_i such that $\partial \epsilon_i = \eta_i$.

For a fixed i, the values of ϵ_i are combinations of p_{ij}s where $p_{ij} := \sqrt{d_i} u^* + \sqrt{d_j} v^*$, and u^*, v^* satisfies C_{ij}.
Trivializing quaternion algebras corresponding to C_{ij} is probably simpler!

Good curves

Definition 7

Recall e_is are the roots of f.

- An $\alpha = (d_1, \ldots, d_{2g+1}) \in \mathrm{Sel}^{(2)}(J)$ with $d_i \in k(e_i)^\times$ is said to be good if for each j, the conics $C_{ij} : d_i u^2 - d_j v^2 + e_i - e_j = 0$ has a solution over $k(e_i, e_j)$.
- A curve C is good if the subgroup generated by good elements is at most of index 2.

If α is good, then we can explicitly write ϵ_i such that $\partial\epsilon_i = \eta_i$.

For a fixed i, the values of ϵ_i are combinations of p_{ij}s where $p_{ij} := \sqrt{d_i}u^* + \sqrt{d_j}v^*$, and u^*, v^* satisfies C_{ij}.

Trivializing quaternion algebras corresponding to C_{ij} is probably simpler!

Good curves

Definition 7

Recall e_is are the roots of f.

- An $\alpha = (d_1, \ldots, d_{2g+1}) \in \mathrm{Sel}^{(2)}(J)$ with $d_i \in k(e_i)^\times$ is said to be good if for each j, the conics $C_{ij} : d_i u^2 - d_j v^2 + e_i - e_j = 0$ has a solution over $k(e_i, e_j)$.
- A curve C is good if the subgroup generated by good elements is at most of index 2.

If α is good, then we can explicitly write ϵ_i such that $\partial\epsilon_i = \eta_i$.

For a fixed i, the values of ϵ_i are combinations of p_{ij}s where $p_{ij} := \sqrt{d_i}u^* + \sqrt{d_j}v^*$, and u^*, v^* satisfies C_{ij}.
Trivializing quaternion algebras corresponding to C_{ij} is probably simpler!

Some statistics on good curves

- Hope: Most of the curves are good.
- $\mathrm{rk}_{\mathbb{F}_2}\mathrm{Sel}^{(2)}(J) \geq 2$, $r_{an}(J) = 0$: 1207 curves on LMFDB, all good.
- $\mathrm{rk}_{\mathbb{F}_2}\mathrm{Sel}^{(2)}(J) \geq 2$, $r_{an}(J) = 1$: 538 curves on LMFDB, all good.
- $\mathrm{rk}_{\mathbb{F}_2}\mathrm{Sel}^{(2)}(J) \geq 4$, $r_{an}(J) \geq 2$: 4 curves on LMFDB, all good.
- $x^5 + A$, $0 < A < 1000$, and A is prime: 168 curves, all good.

Some statistics on good curves

- Hope: Most of the curves are good.
- $\mathrm{rk}_{\mathbb{F}_2}\mathrm{Sel}^{(2)}(J) \geq 2$, $r_{an}(J) = 0$: 1207 curves on LMFDB, all good.
- $\mathrm{rk}_{\mathbb{F}_2}\mathrm{Sel}^{(2)}(J) \geq 2$, $r_{an}(J) = 1$: 538 curves on LMFDB, all good.
- $\mathrm{rk}_{\mathbb{F}_2}\mathrm{Sel}^{(2)}(J) \geq 4$, $r_{an}(J) \geq 2$: 4 curves on LMFDB, all good.
- $x^5 + A$, $0 < A < 1000$, and A is prime: 168 curves, all good.

Some statistics on good curves

- Hope: Most of the curves are good.
- $\mathrm{rk}_{\mathbb{F}_2}\mathrm{Sel}^{(2)}(J) \geq 2$, $r_{an}(J) = 0$: 1207 curves on LMFDB, all good.
- $\mathrm{rk}_{\mathbb{F}_2}\mathrm{Sel}^{(2)}(J) \geq 2$, $r_{an}(J) = 1$: 538 curves on LMFDB, all good.
- $\mathrm{rk}_{\mathbb{F}_2}\mathrm{Sel}^{(2)}(J) \geq 4$, $r_{an}(J) \geq 2$: 4 curves on LMFDB, all good.
- $x^5 + A$, $0 < A < 1000$, and A is prime: 168 curves, all good.

Questions?

Thank You!