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

Notations
preliminaries
Cassels-Tate
pairing
(CTP)
Effective

How to
determine
the splitting
fietd of $\eta$
Extra "nice" curves

Himanshu Shukla
Mathematisches Institut, Universität Bayreuth

Rational Points 2022

28 March, 2022

## Notations

```
Computing
    the
Cassels-Tate
    pairing on
    odd-degree
hyperelliptic
    Jacobians
    H. Shukla
Notations
and
preliminaries
Cassels-Tate
pairing
(CTP)
Effective
computation
of CTP
How to
determine
the splitting
field of }
Extra "nice"
- Let \(k\) be a number field with absolute Galois group \(G_{k}\), and let \(C: y^{2}=f(x)\) with \(\operatorname{deg}(f)=2 g+1\) be a hyperelliptic curve of genus \(g\) defined over \(k\) and \(J\) be its Jacobian.
```



``` of points on \(C\) corresponding to the roots \(e_{i}\) of \(f\), and \(T_{0}\) be the point at \(\infty\)
- For a place \(v\) of \(k\), denote the completion of \(k\) at \(v\) by \(k_{v}\).
- \(C^{i}(G, A), Z^{i}(G, A)\) and \(H^{i}(G, A)\) denote continuous icochains, cocycles and cohomology classes associate to a group \(G\) and a \(G\)-module \(A\).
- For \(n \geq 2\), let \(\amalg(J)\) and \(\operatorname{Sel}^{(n)}(J)\) be the Shafarevich-Tate and \(n\)-Selmer groups associated with \(J\).
```

curves

## Notations

Computing the
Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate
pairing
(CTP)
Effective
computation of CTP

How to
determine
the splitting field of $\eta$

■ Let $k$ be a number field with absolute Galois group $G_{k}$, and let $C: y^{2}=f(x)$ with $\operatorname{deg}(f)=2 g+1$ be a hyperelliptic curve of genus $g$ defined over $k$ and $J$ be its Jacobian.
 and $n$-Selmer groups associated with $J$

## Notations

Computing the Cassels-Tate pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate
pairing
(CTP)
Effective
computation of CTP

How to
determine
the splitting field of $\eta$

Extra "nice" curves

■ Let $k$ be a number field with absolute Galois group $G_{k}$, and let $C: y^{2}=f(x)$ with $\operatorname{deg}(f)=2 g+1$ be a hyperelliptic curve of genus $g$ defined over $k$ and $J$ be its Jacobian.

- Let $\Delta:=\left\{T_{i}:=\left(e_{i}, 0\right) \in C: 1 \leq i \leq 2 g+1\right\}$ be the set of points on $C$ corresponding to the roots $e_{i}$ of $f$, and $T_{0}$ be the point at $\infty$.
 and $n$-Selmer groups associated with $J$.


## Notations

Computing the Cassels-Tate pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate
pairing
(CTP)
Effective
computation of CTP

How to
determine
the splitting field of $\eta$

■ Let $k$ be a number field with absolute Galois group $G_{k}$, and let $C: y^{2}=f(x)$ with $\operatorname{deg}(f)=2 g+1$ be a hyperelliptic curve of genus $g$ defined over $k$ and $J$ be its Jacobian.
■ Let $\Delta:=\left\{T_{i}:=\left(e_{i}, 0\right) \in C: 1 \leq i \leq 2 g+1\right\}$ be the set of points on $C$ corresponding to the roots $e_{i}$ of $f$, and $T_{0}$ be the point at $\infty$.
■ For a place $v$ of $k$, denote the completion of $k$ at $v$ by $k_{v}$.
 group $G$ and a $G$-module $A$.

- For $n>2$. let III( $J$ ) and $\operatorname{Sel}^{(n)}(J)$ 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 $\operatorname{deg}(f)=2 g+1$ be a hyperelliptic curve of genus $g$ defined over $k$ and $J$ be its Jacobian.
■ Let $\Delta:=\left\{T_{i}:=\left(e_{i}, 0\right) \in C: 1 \leq i \leq 2 g+1\right\}$ be the set of points on $C$ corresponding to the roots $e_{i}$ of $f$, and $T_{0}$ be the point at $\infty$.
■ For a place $v$ of $k$, denote the completion of $k$ at $v$ by $k_{v}$.
$\square \mathrm{C}^{i}(G, A), \mathrm{Z}^{i}(G, A)$ and $\mathrm{H}^{i}(G, A)$ denote continuous $i-$ cochains, cocycles and cohomology classes associate to a group $G$ and a $G$-module $A$.


## Notations

■ Let $k$ be a number field with absolute Galois group $G_{k}$, and let $C: y^{2}=f(x)$ with $\operatorname{deg}(f)=2 g+1$ be a hyperelliptic curve of genus $g$ defined over $k$ and $J$ be its Jacobian.
■ Let $\Delta:=\left\{T_{i}:=\left(e_{i}, 0\right) \in C: 1 \leq i \leq 2 g+1\right\}$ be the set of points on $C$ corresponding to the roots $e_{i}$ of $f$, and $T_{0}$ be the point at $\infty$.
■ For a place $v$ of $k$, denote the completion of $k$ at $v$ by $k_{v}$.
$\square \mathrm{C}^{i}(G, A), \mathrm{Z}^{i}(G, A)$ 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 $\amalg(J)$ and $\operatorname{Sel}^{(n)}(J)$ be the Shafarevich-Tate and $n$-Selmer groups associated with $J$.


## A quick recall

Computing the
Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations and preliminaries

Cassels-Tate
pairing
(CTP)
Effective
computation of CTP

How to
determine
the splitting field of $\eta$

- We have

$$
\operatorname{Sel}^{(n)}(J):=\operatorname{ker}\left(\mathrm{H}^{1}\left(G_{k}, J[n]\right) \rightarrow \prod_{v} \mathrm{H}^{1}\left(G_{k_{v}}, J\right)\right)
$$

and

$$
\amalg(J):=\operatorname{ker}\left(\mathrm{H}^{1}\left(G_{k}, J\right) \rightarrow \prod_{v} \mathrm{H}^{1}\left(G_{k_{v}}, J\right)\right)
$$

## A quick recall

Computing the
Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate
pairing
(CTP)
Effective
computation of CTP

How to
determine
the splitting
field of $\eta$
Extra "nice" curves

- We have

$$
\operatorname{Sel}^{(n)}(J):=\operatorname{ker}\left(\mathrm{H}^{1}\left(G_{k}, J[n]\right) \rightarrow \prod_{v} \mathrm{H}^{1}\left(G_{k_{v}}, J\right)\right)
$$

and

$$
\amalg(J):=\operatorname{ker}\left(\mathrm{H}^{1}\left(G_{k}, J\right) \rightarrow \prod_{v} \mathrm{H}^{1}\left(G_{k_{v}}, J\right)\right) .
$$

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

$$
0 \rightarrow J(k) / n J(k) \rightarrow \operatorname{Sel}^{(n)}(J) \rightarrow \amalg(J)[n] \rightarrow 0
$$

## Recalling CTP



## Recalling CTP

Computing the Cassels-Tate pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries

Cassels-Tate pairing (CTP)
Effective computation of CTP

How to determine the splitting field of $\eta$

The Cassels-Tate pairing:

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

## which satisfies:

- Anti-symmetric and non-degenerate (on the quotient $\left.\amalg(J)_{n d} \times \amalg(J)_{n d}\right)$.
n Defined first by Cassels for elliptic curves and generalized by Tate to abelian varieties.
- Doonen and Stoll gave the AIbanese-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

Computing the Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries

Cassels-Tate
pairing
(CTP)
Effective computation of CTP

How to determine the splitting field of $\eta$

The Cassels-Tate pairing:

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

## which satisfies:

- Anti-symmetric and non-degenerate (on the quotient $\left.\amalg(J)_{n d} \times \amalg(J)_{n d}\right)$.
■ Defined first by Cassels for elliptic curves and generalized by Tate to abelian varieties.


CTP and showed that it is equivalent to the 2 -other definitions (Weil-nairino and homooenenus snace hased definitions)

- This pairing can be pulled back to the $n$-Selmer group using the $n$-descent seauence


## Recalling CTP

Computing the Cassels-Tate pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations and
preliminaries
Cassels-Tate
pairing (CTP)

Effective computation of CTP

How to
determine
the splitting field of $\eta$

Extra "nice" curves

The Cassels-Tate pairing:

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

which satisfies:

- Anti-symmetric and non-degenerate (on the quotient $\left.\amalg(J)_{n d} \times \amalg(J)_{n d}\right)$.
■ 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

Computing the Cassels-Tate pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate pairing (CTP)

Effective computation of CTP

How to determine the splitting field of $\eta$

The Cassels-Tate pairing:

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

which satisfies:

- Anti-symmetric and non-degenerate (on the quotient $\left.\amalg(J)_{n d} \times \amalg(J)_{n d}\right)$.
- 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



## Albanese-Albanese definition of CTP

Computing the Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate pairing
(CTP)
Effective
computation of CTP

How to
determine
the splitting field of $\eta$

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

## Albanese-Albanese definition of CTP

Computing the Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate pairing
(CTP)
Effective
computation of CTP

How to
determine
the splitting field of $\eta$

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

- $\langle., .\rangle_{1}: \operatorname{Princ}(C) \times \operatorname{Div}^{0}(C) \rightarrow \mathbb{G}_{m}$.

$$
(\operatorname{div}(f), D) \mapsto \prod_{P \in \operatorname{Supp}(D)}\left(f t_{P}^{-v_{P}(f)}(P)\right)^{v_{P}(D)}
$$

## Albanese-Albanese definition of CTP

Computing the
Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate pairing
(CTP)
Effective
computation of CTP

How to
determine
the splitting field of $\eta$

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

- $\langle., .\rangle_{1}: \operatorname{Princ}(C) \times \operatorname{Div}^{0}(C) \rightarrow \mathbb{G}_{m}$.

$$
(\operatorname{div}(f), D) \mapsto \prod_{P \in \operatorname{Supp}(D)}\left(f t_{P}^{-v_{P}(f)}(P)\right)^{v_{P}(D)}
$$

- $\langle., .\rangle_{2}: \operatorname{Div}^{0}(C) \times \operatorname{Princ}(C) \rightarrow \mathbb{G}_{m}$.

$$
(D, \operatorname{div}(f)) \mapsto \prod_{P \in \operatorname{Supp}(D)}(-1)^{v_{P}(f) v_{P}(D)}\left(f t_{P}^{-v_{P}(f)}(P)\right)^{v_{P}(D)} .
$$



## Albanese-Albanese definition of CTP

Computing the Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate pairing
(CTP)
Effective
computation of CTP

How to
determine the splitting field of $\eta$

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

- $\langle., .\rangle_{1}: \operatorname{Princ}(C) \times \operatorname{Div}^{0}(C) \rightarrow \mathbb{G}_{m}$.

$$
(\operatorname{div}(f), D) \mapsto \prod_{P \in \operatorname{Supp}(D)}\left(f t_{P}^{-v_{P}(f)}(P)\right)^{v_{P}(D)}
$$

■ $\langle., .\rangle_{2}: \operatorname{Div}^{0}(C) \times \operatorname{Princ}(C) \rightarrow \mathbb{G}_{m}$.

$$
(D, \operatorname{div}(f)) \mapsto \prod_{P \in \operatorname{Supp}(D)}(-1)^{v_{P}(f) v_{P}(D)}\left(f t_{P}^{-v_{P}(f)}(P)\right)^{v_{P}(D)} .
$$

These pairings agree on the diagonal $\operatorname{Princ}(C) \times \operatorname{Princ}(C)$ (strong Weil reciprocity), and induce cup products $\cup_{1}$ and $\cup_{2}$.

## Global part

Computing the
Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries

Cassels-Tate pairing
(CTP)
Effective
computation of CTP

How to determine the splitting field of $\eta$

Extra "nice" curves

Let $a, a^{\prime} \in \mathrm{H}^{1}\left(G_{k}, J[n]\right)$ and let $\alpha, \alpha^{\prime} \in \mathrm{Z}^{1}\left(G_{k}, J[n]\right)$ represent the classes $a, a^{\prime}$.
Lift $\alpha, \alpha^{\prime}$ to 1 -cochains $\mathfrak{a}, \boldsymbol{a}^{\prime}$ with values in
Using cohomology on the exact sequence:

```
we get a 3-cochain
```

and compatibility of $U_{1}, \cup_{2}$ on the diagonal implies
Since $H^{3}\left(G_{k}, G_{m}\right)=0$, i.e. there exists $\in \in C^{2}\left(G_{k}, \mathbb{G}_{m}\right)$ s.t
Global bottleneck: Finding $\in$ (our Nemo!)

## Global part

Computing the
Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate pairing
(CTP)
Effective
computation of CTP

How to
determine
the splitting field of $\eta$

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


## Global part

Computing the Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate pairing (CTP)

Effective computation of CTP

How to
determine
the splitting field of $\eta$

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

$$
0 \rightarrow \operatorname{Princ}(C) \rightarrow \operatorname{Div}^{0}(C) \rightarrow \operatorname{Pic}^{0}(C) \rightarrow 0
$$

we get a 3-cochain:

$$
\eta:=\partial \mathfrak{a} \cup_{1} \mathfrak{a}^{\prime}-\mathfrak{a} \cup_{2} \partial \mathfrak{a}^{\prime}
$$

and compatibility of $U_{1}, \cup_{2}$ on the diagonal implies


Since $H^{3}\left(G_{k}, \mathbb{G}\right)=$ $\square$

Global bottleneck: Finding $\in$ (our Nemo!

## Global part

Computing the Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
preliminaries
Cassels-Tate pairing (CTP)
Effective computation of CTP

How to
determine the splitting field of $\eta$

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

$$
0 \rightarrow \operatorname{Princ}(C) \rightarrow \operatorname{Div}^{0}(C) \rightarrow \operatorname{Pic}^{0}(C) \rightarrow 0
$$

we get a 3-cochain:

$$
\eta:=\partial \mathfrak{a} \cup_{1} \mathfrak{a}^{\prime}-\mathfrak{a} \cup_{2} \partial \mathfrak{a}^{\prime}
$$

and compatibility of $\cup_{1}, \cup_{2}$ on the diagonal implies $\eta \in \mathrm{Z}^{3}\left(G_{k}, \mathbb{G}_{m}\right)$ i.e. a 3 -cocycle

Global bottleneck: Finding $\epsilon$ (our Nemo!

## Global part

Computing the Cassels-Tate pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
preliminaries
Cassels-Tate pairing (CTP)
Effective

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

$$
0 \rightarrow \operatorname{Princ}(C) \rightarrow \operatorname{Div}^{0}(C) \rightarrow \operatorname{Pic}^{0}(C) \rightarrow 0
$$

we get a 3-cochain:

$$
\eta:=\partial \mathfrak{a} \cup_{1} \mathfrak{a}^{\prime}-\mathfrak{a} \cup_{2} \partial \mathfrak{a}^{\prime}
$$

and compatibility of $\cup_{1}, \cup_{2}$ on the diagonal implies $\eta \in \mathrm{Z}^{3}\left(G_{k}, \mathbb{G}_{m}\right)$ i.e. a 3 -cocycle
Since $H^{3}\left(G_{k}, \mathbb{G}_{m}\right)=0$, i.e. there exists $\epsilon \in \mathrm{C}^{2}\left(G_{k}, \mathbb{G}_{m}\right)$ s.t.
$\partial \epsilon=\eta$.
Global bottleneck: Finding $\epsilon$ (our Nemo!

## Global part

Computing the
Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
preliminaries
Cassels-Tate pairing (CTP)
Effective computation of CTP

How to
determine
the splitting field of $\eta$

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

$$
0 \rightarrow \operatorname{Princ}(C) \rightarrow \operatorname{Div}^{0}(C) \rightarrow \operatorname{Pic}^{0}(C) \rightarrow 0
$$

we get a 3-cochain:

$$
\eta:=\partial \mathfrak{a} \cup_{1} \mathfrak{a}^{\prime}-\mathfrak{a} \cup_{2} \partial \mathfrak{a}^{\prime}
$$

and compatibility of $\cup_{1}, \cup_{2}$ on the diagonal implies $\eta \in \mathrm{Z}^{3}\left(G_{k}, \mathbb{G}_{m}\right)$ i.e. a 3 -cocycle Since $H^{3}\left(G_{k}, \mathbb{G}_{m}\right)=0$, i.e. there exists $\epsilon \in \mathrm{C}^{2}\left(G_{k}, \mathbb{G}_{m}\right)$ s.t. $\partial \epsilon=\eta$.
Global bottleneck: Finding $\epsilon$ (our Nemo!)

## Local part



Computing the
Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate pairing
(CTP)
Effective computation of CTP

How to determine the splitting field of $\eta$

Extra "nice" curves

## Local part

Computing the
Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate pairing
(CTP)
Effective
computation of CTP

How to determine the splitting fietd of $\eta$

Let $v$ be a place of $k$. If $a \in \operatorname{Sel}^{(n)}(J)$ then there is a $\beta_{v} \in J\left(\overline{k_{v}}\right)$ such that $\alpha_{v}=\partial \beta_{v}$.

## Local part

Computing the
Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate pairing
(CTP)
Effective
computation of CTP

How to
determine
the splitting field of $\eta$

Let $v$ be a place of $k$. If $a \in \operatorname{Sel}^{(n)}(J)$ then there is a $\beta_{v} \in J\left(\overline{k_{v}}\right)$ such that $\alpha_{v}=\partial \beta_{v}$. Let $\mathfrak{b}_{v} \in \operatorname{Div}^{0}(C)$ represent $\beta$.

## Local part

Computing the
Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

## Notations

and
preliminaries
Cassels-Tate pairing
(CTP)
Effective
computation of CTP

How to
determine
the splitting field of $\eta$

Let $v$ be a place of $k$. If $a \in \operatorname{Sel}^{(n)}(J)$ then there is a $\beta_{v} \in J\left(\overline{k_{v}}\right)$ such that $\alpha_{v}=\partial \beta_{v}$.
Let $\mathfrak{b}_{v} \in \operatorname{Div}^{0}(C)$ represent $\beta$. Then

$$
\gamma_{v}:=\left(\mathfrak{a}_{v}-\partial \mathfrak{b}_{v}\right) \cup_{1} \mathfrak{a}_{v}^{\prime}-\mathfrak{b}_{v} \cup_{2} \partial \mathfrak{a}_{v}^{\prime}-\epsilon_{v}
$$

is a 2-cocycle.

## Local part

Computing the
Cassels-Tate
pairing on
odd-degree
hyperelliptic
Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate pairing
(CTP)
Effective
computation
of CTP
How to
determine
the splitting field of $\eta$

Let $v$ be a place of $k$. If $a \in \operatorname{Sel}^{(n)}(J)$ then there is a $\beta_{v} \in J\left(\overline{k_{v}}\right)$ such that $\alpha_{v}=\partial \beta_{v}$.
Let $\mathfrak{b}_{v} \in \operatorname{Div}^{0}(C)$ represent $\beta$. Then

$$
\gamma_{v}:=\left(\mathfrak{a}_{v}-\partial \mathfrak{b}_{v}\right) \cup_{1} \mathfrak{a}_{v}^{\prime}-\mathfrak{b}_{v} \cup_{2} \partial \mathfrak{a}_{v}^{\prime}-\epsilon_{v}
$$

is a 2-cocycle.
We have $\left[\gamma_{v}\right] \in \operatorname{Br}\left(k_{v}\right)$ and the CTP is defined as:

## Definition 1

$$
\left\langle a, a^{\prime}\right\rangle_{\mathrm{CT}}:=\sum_{v} \operatorname{inv}_{v}\left(\left[\gamma_{v}\right]\right) .
$$

## Local part

Computing the Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
preliminaries
Cassels-Tate pairing
(CTP)
Effective
computation
of CTP
How to
determine
the splitting field of $\eta$

Let $v$ be a place of $k$. If $a \in \operatorname{Sel}^{(n)}(J)$ then there is a $\beta_{v} \in J\left(\overline{k_{v}}\right)$ such that $\alpha_{v}=\partial \beta_{v}$.
Let $\mathfrak{b}_{v} \in \operatorname{Div}^{0}(C)$ represent $\beta$. Then

$$
\gamma_{v}:=\left(\mathfrak{a}_{v}-\partial \mathfrak{b}_{v}\right) \cup_{1} \mathfrak{a}_{v}^{\prime}-\mathfrak{b}_{v} \cup_{2} \partial \mathfrak{a}_{v}^{\prime}-\epsilon_{v}
$$

is a 2-cocycle.
We have $\left[\gamma_{v}\right] \in \operatorname{Br}\left(k_{v}\right)$ and the CTP is defined as:

## Definition 1

$$
\left\langle a, a^{\prime}\right\rangle_{\mathrm{CT}}:=\sum_{v} \operatorname{inv}_{v}\left(\left[\gamma_{v}\right]\right) .
$$

Local bottleneck: Computing $\operatorname{inv}_{v}\left(\left[\gamma_{v}\right]\right)$

## Local part

Computing the Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
preliminaries
Cassels-Tate pairing (CTP)

Effective computation of CTP

How to determine the splitting field of $\eta$

Let $v$ be a place of $k$. If $a \in \operatorname{Sel}^{(n)}(J)$ then there is a $\beta_{v} \in J\left(\overline{k_{v}}\right)$ such that $\alpha_{v}=\partial \beta_{v}$.
Let $\mathfrak{b}_{v} \in \operatorname{Div}^{0}(C)$ represent $\beta$. Then

$$
\gamma_{v}:=\left(\mathfrak{a}_{v}-\partial \mathfrak{b}_{v}\right) \cup_{1} \mathfrak{a}_{v}^{\prime}-\mathfrak{b}_{v} \cup_{2} \partial \mathfrak{a}_{v}^{\prime}-\epsilon_{v}
$$

is a 2-cocycle.
We have $\left[\gamma_{v}\right] \in \operatorname{Br}\left(k_{v}\right)$ and the CTP is defined as:

## Definition 1

$$
\left\langle a, a^{\prime}\right\rangle_{\mathrm{CT}}:=\sum_{v} \operatorname{inv}_{v}\left(\left[\gamma_{v}\right]\right) .
$$

Local bottleneck: Computing $\operatorname{inv}_{v}\left(\left[\gamma_{v}\right]\right)$ (generically solvable!).

## Previous works

Computing the
Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate pairing
(CTP)
Effective computation of CTP

How to determine the splitting fietd of $\eta$

■ Previous works have mainly focused on elliptic curves:


## Previous works

Computing the Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate
pairing (CTP)

Effective computation of CTP

How to
determine
the splitting field of $\eta$

■ Previous works have mainly focused on elliptic curves:

| Authors | Domain |
| :---: | :---: |
| Cassels | $\mathrm{Sel}^{(2)}(E) \times \operatorname{Sel}^{(2)}(E)$ |
| Swinnerton-Dyer | $\operatorname{Sel}^{\left(2^{m \prime}\right)}(E) \times \operatorname{Sel}^{(2)}(E)$ |
| van Beek \& Fisher | $\mathrm{Sel}^{(\phi)}(E) \times \mathrm{Sel}^{(\phi)}(E)$ <br> $\operatorname{deg}(\phi)$ is odd prime |
| Fischer \& Newton | $\mathrm{Sel}^{(3)}(E) \times \operatorname{Sel}^{(3)}(E)$ |

- 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

H. Shukla

## Notations

and
preliminaries
Cassels-Tate
pairing
(CTP)
Effective computation of CTP

How to
determine the splitting field of $\eta$

■ Previous works have mainly focused on elliptic curves:

| Authors | Domain |
| :---: | :---: |
| Cassels | $\mathrm{Sel}^{(2)}(E) \times \operatorname{Sel}^{(2)}(E)$ |
| Swinnerton-Dyer | $\operatorname{Sel}^{\left(2^{m \prime}\right)}(E) \times \operatorname{Sel}^{(2)}(E)$ |
| van Beek \& Fisher | $\mathrm{Sel}^{(\phi)}(E) \times \mathrm{Sel}^{(\phi)}(E)$ <br> $\operatorname{deg}(\phi)$ is odd prime |
| Fischer \& Newton | $\mathrm{Sel}^{(3)}(E) \times \operatorname{Sel}^{(3)}(E)$ |

■ For 2-Selmer groups of genus 2 Jacobians, Jiali Yan has an algorithm (assuming some conditions).

## Previous works

H. Shukla

## Notations

and
preliminaries
Cassels-Tate
pairing
(CTP)
Effective computation of CTP

How to
determine
the splitting field of $\eta$

Extra "nice" curves

■ Previous works have mainly focused on elliptic curves:

| Authors | Domain |
| :---: | :---: |
| Cassels | $\operatorname{Sel}^{(2)}(E) \times \operatorname{Sel}^{(2)}(E)$ |
| Swinnerton-Dyer | $\operatorname{Sel}^{\left(2^{m}\right)}(E) \times \operatorname{Sel}^{(2)}(E)$ |
| van Beek \& Fisher | $\mathrm{Sel}^{(\phi)}(E) \times \operatorname{Sel}^{(\phi)}(E)$ <br> $\operatorname{deg}(\phi)$ is odd prime |
| Fischer \& Newton | $\operatorname{Sel}^{(3)}(E) \times \operatorname{Sel}^{(3)}(E)$ |

■ 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 $\epsilon$

Computing the
Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate pairing
(CTP)
Effective computation of CTP

How to determine the splitting field of $\eta$

Extra "nice" curves

One can compute $\epsilon$ if a splitting field of $\eta$ is known! For a cochain $x \in \mathrm{C}^{1}\left(G_{k}, M\right)$, let $\operatorname{fod}(x)$ be the field of definition of $x$, i.e. minimal field extension $L$ s.t. $x=\inf (y)$ for some $y \in \mathrm{C}^{i}(\operatorname{Gal}(L / k), M(L))$. Let $\prod \mathrm{H}^{2}\left(G_{k}, J[n]\right)$ Proposition 2

- For $\sigma, \tau, \tau^{\prime} \in G_{k}, \epsilon(\sigma, \tau)=\epsilon\left(\sigma, \tau^{\prime}\right)$ if $\left.\tau\right|_{K^{\prime}}=\left.\tau^{\prime}\right|_{K^{\prime}}$, where $K^{\prime}:=\operatorname{fod}\left(\alpha^{\prime}\right)$


## Existence of a nice $\epsilon$

Computing the
Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate
pairing
(CTP)
Effective

How to determine the splitting field of $\eta$

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

## Existence of a nice $\epsilon$

Computing the
Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate
pairing
(CTP)
Effective
computation of CTP

How to determine the splitting field of $\eta$

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

$$
\operatorname{loc}^{2}(J[n]): \mathrm{H}^{2}\left(G_{k}, J[n]\right) \rightarrow \prod_{v} \mathrm{H}^{2}\left(G_{k}, J[n]\right)
$$

## Existence of a nice $\epsilon$

Computing the Cassels-Tate pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations and
preliminaries
Cassels-Tate
pairing
(CTP)
Effective
computation of CTP

How to determine the splitting field of $\eta$

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

$$
\operatorname{loc}^{2}(J[n]): \mathrm{H}^{2}\left(G_{k}, J[n]\right) \rightarrow \prod_{v} \mathrm{H}^{2}\left(G_{k}, J[n]\right)
$$

## Proposition 2

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

## Existence of a nice $\epsilon$

Computing the Cassels-Tate pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations and
preliminaries
Cassels-Tate
pairing
(CTP)
Effective
computation of CTP

How to determine the splitting field of $\eta$

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

$$
\operatorname{loc}^{2}(J[n]): \mathrm{H}^{2}\left(G_{k}, J[n]\right) \rightarrow \prod_{v} \mathrm{H}^{2}\left(G_{k}, J[n]\right)
$$

## Proposition 2

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

- For $\sigma, \tau, \tau^{\prime} \in G_{k}, \epsilon(\sigma, \tau)=\epsilon\left(\sigma, \tau^{\prime}\right)$ if $\left.\tau\right|_{K^{\prime}}=\left.\tau^{\prime}\right|_{K^{\prime}}$, where $K^{\prime}:=\operatorname{fod}\left(\alpha^{\prime}\right)$.


## Existence of a nice $\epsilon$

Computing the Cassels-Tate pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations and preliminaries

Cassels-Tate pairing
(CTP)
Effective computation of CTP

How to determine the splitting field of $\eta$

Extra "nice" curves

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

$$
\operatorname{loc}^{2}(J[n]): \mathrm{H}^{2}\left(G_{k}, J[n]\right) \rightarrow \prod_{v} \mathrm{H}^{2}\left(G_{k}, J[n]\right)
$$

## Proposition 2

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

■ For $\sigma, \tau, \tau^{\prime} \in G_{k}, \epsilon(\sigma, \tau)=\epsilon\left(\sigma, \tau^{\prime}\right)$ if $\left.\tau\right|_{K^{\prime}}=\tau_{K^{\prime}}$, where $K^{\prime}:=\operatorname{fod}\left(\alpha^{\prime}\right)$.

- $\epsilon(\sigma, \tau)=1$ if $\left.\tau\right|_{K^{\prime}}=i d$.


## Sketch of proof of proposition 2

Computing the
Cassels-Tate
pairing on
odd-degree
hyperelliptic
Jacobians
H. Shukla
to show: if $a \in \operatorname{Sel}^{(n)}(J)$, then $\delta(a)=0$, where
$\delta: \mathrm{H}^{1}\left(G_{k}, J[n]\right) \rightarrow \mathrm{H}^{2}\left(G_{k}, J[n]\right)$.
How to determine the splitting field of $\eta$

■ Use cohomology on commutative diagram:


Cassels-Tate
pairing (CTP)

Effective computation of CTP
Notations
and
preliminaries

## Sketch of proof of proposition 2

pairing on
odd-degree
hyperelliptic
Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate
pairing
(CTP)
Effective
computation
of CTP
How to determine the splitting field of $\eta$

■ Use cohomology on commutative diagram:

to show: if $a \in \operatorname{Sel}^{(n)}(J)$, then $\delta(a)=0$, where
$\delta: \mathrm{H}^{1}\left(G_{k}, J[n]\right) \rightarrow \mathrm{H}^{2}\left(G_{k}, J[n]\right)$.
■ 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 $\eta$

Computing the Cassels-Tate pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
preliminaries
Cassels-Tate
pairing
(CTP)
Effective

How to determine the splitting field of $\eta$

## Lemma 3

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

- $K \cap K^{\prime}=k$.

■ $\left[K^{\prime}: k\right]=2$.
Then $\eta$ splits in $K K^{\prime}$, i.e. its field of definition.

## Splitting field of $\eta$

## Lemma 3

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

- $K \cap K^{\prime}=k$.

■ $\left[K^{\prime}: k\right]=2$.
Then $\eta$ splits in $K K^{\prime}$, i.e. its field of definition.

## Remark 4

The proof of the above lemma constructs $\epsilon$ explicitly.
 directly) to determine a splitting field of $\eta$ even for $n=2$.

## Splitting field of $\eta$

## Lemma 3

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

- $K \cap K^{\prime}=k$.

■ $\left[K^{\prime}: k\right]=2$.
Then $\eta$ splits in $K K^{\prime}$, i.e. its field of definition.

## Remark 4

The proof of the above lemma constructs $\epsilon$ explicitly.
Since $k(J[n]) \subset K \cap K^{\prime}$, lemma 3 cannot be applied (at least directly) to determine a splitting field of $\eta$ even for $n=2$.

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

Computing the
Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

## Notations

and
preliminaries
Cassels-Tate
pairing
(CTP)
Effective computation of CTP

How to determine the splitting field of $\eta$

## We have:

$$
H^{1}\left(G_{k}, J[2]\right) \simeq \operatorname{ker}\left(N: L^{\times} /\left(L^{\times}\right)^{2} \rightarrow k^{\times} /\left(k^{\times}\right)^{2}\right)
$$

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

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

Computing the
Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

## Notations

and
preliminaries
Cassels-Tate
pairing
(CTP)
Effective computation of CTP

How to determine the splitting field of $\eta$

We have:

$$
H^{1}\left(G_{k}, J[2]\right) \simeq \operatorname{ker}\left(N: L^{\times} /\left(L^{\times}\right)^{2} \rightarrow k^{\times} /\left(k^{\times}\right)^{2}\right),
$$

where $L:=k[x] /(f(x))$. and $N: L^{\times} \rightarrow k^{\times}$is the norm map.
■ Let $T_{i}$ be the representative of $i^{\text {th }}$ orbit of $\Delta$.


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

Computing the
Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

## Notations

and
preliminaries
Cassels-Tate
pairing (CTP)

Effective computation of CTP

How to determine the splitting field of $\eta$

We have:

$$
H^{1}\left(G_{k}, J[2]\right) \simeq \operatorname{ker}\left(N: L^{\times} /\left(L^{\times}\right)^{2} \rightarrow k^{\times} /\left(k^{\times}\right)^{2}\right)
$$

where $L:=k[x] /(f(x))$. and $N: L^{\times} \rightarrow k^{\times}$is the norm map.
■ Let $T_{i}$ be the representative of $i^{\text {th }}$ orbit of $\Delta$.

- For $1 \leq j \leq 2 g+1$ choose $d_{j}^{\prime} \in k\left(T_{j}\right)^{\times}$such that $\left(d_{1}^{\prime}, d_{2}^{\prime}, \ldots, d_{2 g+1}^{\prime}\right)$ represents $\alpha^{\prime}$.


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

Computing the
Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate
pairing (CTP)

Effective computation of CTP

How to determine the splitting field of $\eta$

We have:

$$
H^{1}\left(G_{k}, J[2]\right) \simeq \operatorname{ker}\left(N: L^{\times} /\left(L^{\times}\right)^{2} \rightarrow k^{\times} /\left(k^{\times}\right)^{2}\right),
$$

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

- Let $T_{i}$ be the representative of $i^{\text {th }}$ orbit of $\Delta$.
- For $1 \leq j \leq 2 g+1$ choose $d_{j}^{\prime} \in k\left(T_{j}\right)^{\times}$such that $\left(d_{1}^{\prime}, d_{2}^{\prime}, \ldots, d_{2 g+1}^{\prime}\right)$ represents $\alpha^{\prime}$.
- $d_{j}^{\prime} \mathrm{s}$ satisfy the condition: for $1 \leq n, m \leq 2 g+1$, $d_{m}^{\prime}$ and $d_{n}^{\prime}$ are conjugates if $T_{n}$ and $T_{m}$ are.


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

Computing the Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

## Notations

and
preliminaries
Cassels-Tate
pairing (CTP)
Effective computation of CTP

How to determine the splitting field of $\eta$

We have:

$$
H^{1}\left(G_{k}, J[2]\right) \simeq \operatorname{ker}\left(N: L^{\times} /\left(L^{\times}\right)^{2} \rightarrow k^{\times} /\left(k^{\times}\right)^{2}\right)
$$

where $L:=k[x] /(f(x))$. and $N: L^{\times} \rightarrow k^{\times}$is the norm map.
■ Let $T_{i}$ be the representative of $i^{\text {th }}$ orbit of $\Delta$.
■ For $1 \leq j \leq 2 g+1$ choose $d_{j}^{\prime} \in k\left(T_{j}\right)^{\times}$such that $\left(d_{1}^{\prime}, d_{2}^{\prime}, \ldots, d_{2 g+1}^{\prime}\right)$ represents $\alpha^{\prime}$.
■ $d_{j}^{\prime}$ s satisfy the condition: for $1 \leq n, m \leq 2 g+1$, $d_{m}^{\prime}$ and $d_{n}^{\prime}$ are conjugates if $T_{n}$ and $T_{m}$ are.
First, note that $\operatorname{loc}^{2}(J[2])$ is injective (consequence of Poitou-Tate duality).

Computing
the
Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate pairing
(CTP)
Effective
computation of CTP

How to determine the splitting field of $\eta$

Extra "nice" curves

■ We choose (we can) $\mathfrak{a}^{\prime}$ to be where
 enough to trivialize 3-cocycles Now $\left[k\left(T_{i}\right)\left(\sqrt{d_{i}^{\prime}}\right): k\left(T_{i}\right)\right]=2$ and values of $t_{i}^{\prime}$ are defined over $k\left(T_{i}\right)$. Use lemma 3 to find $\epsilon_{i}$ s s.t

## Computing

the
Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate pairing
(CTP)
Effective
computation of CTP

How to determine the splitting field of $\eta$

Extra "nice" curves

■ We choose (we can) $\mathfrak{a}^{\prime}$ to be $\sum_{\text {orbits }} \operatorname{cor}_{G_{k\left(T_{i}\right)}}^{G_{k}} \mathfrak{t}_{i}^{\prime}$, where $t_{i}^{\prime} \in C^{1}\left(G_{k}\left(T_{i}\right),\left\langle\left(T_{i}\right)-\left(T_{0}\right)\right\rangle\right)$ is given by:

$$
t_{i}^{\prime}(\sigma):=\left\{\begin{array}{l}0 \\ \left.\left(T_{i}\right)-\left(T_{0}\right) \quad \sigma\left(\sqrt{d_{i}^{\prime}}\right)=-\sqrt{d_{i}^{\prime \prime}}\right)=\sqrt{d_{i}^{\prime \prime}}\end{array}\right.
$$

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

Computing
the
Cassels-Tate
pairing on
odd-degree
hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate
pairing
(CTP)
Effective computation of CTP

How to determine the splitting field of $\eta$

- We choose (we can) $\mathfrak{a}^{\prime}$ to be $\sum_{\text {orbits }} \operatorname{cor}_{G_{k\left(T_{i}\right)}}^{G_{k}} \mathfrak{t}_{i}^{\prime}$, where $\mathfrak{t}_{i}^{\prime} \in \mathrm{C}^{1}\left(G_{k\left(T_{i}\right)},\left\langle\left(T_{i}\right)-\left(T_{0}\right)\right\rangle\right)$ is given by:

$$
\mathfrak{t}_{i}^{\prime}(\sigma):=\left\{\begin{array}{lr}
0 & \sigma\left(\sqrt{d_{i}^{\prime}}\right)=\sqrt{d_{i}^{\prime}} \\
\left(T_{i}\right)-\left(T_{0}\right) & \sigma\left(\sqrt{d_{i}^{\prime}}\right)=-\sqrt{d_{i}^{\prime}}
\end{array}\right.
$$

$$
\begin{aligned}
& \text { The identity } x \cup \operatorname{cor}(y)=\operatorname{cor}( \\
& \text { enough to trivialize } 3 \text {-cocycles }
\end{aligned}
$$

Computing the

- We choose (we can) $\mathfrak{a}^{\prime}$ to be $\sum_{\text {orbits }} \operatorname{cor}_{G_{k\left(T_{i}\right)}}^{G_{k}} \mathfrak{t}^{\prime}$, where $\mathfrak{t}_{i}^{\prime} \in \mathrm{C}^{1}\left(G_{k\left(T_{i}\right)},\left\langle\left(T_{i}\right)-\left(T_{0}\right)\right\rangle\right)$ is given by:

$$
\mathfrak{t}_{i}^{\prime}(\sigma):=\left\{\begin{array}{lr}
0 & \sigma\left(\sqrt{d_{i}^{\prime}}\right)=\sqrt{d_{i}^{\prime}} \\
\left(T_{i}\right)-\left(T_{0}\right) & \sigma\left(\sqrt{d_{i}^{\prime}}\right)=-\sqrt{d_{i}^{\prime}}
\end{array}\right.
$$

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

$$
\eta_{i}:=\partial \operatorname{res}(\mathfrak{a}) \cup_{1} \mathfrak{t}_{i}^{\prime}-\operatorname{res}(\mathfrak{a}) \cup_{2} \partial \mathfrak{t}_{i}^{\prime} \in \mathrm{Z}^{3}\left(G_{k\left(T_{i}\right)}, \mathbb{G}_{m}\right)
$$

Computing the

- We choose (we can) $\mathfrak{a}^{\prime}$ to be $\sum_{\text {orbits }} \operatorname{cor}_{G_{k\left(T_{i}\right)}}^{G_{k}} \mathfrak{t}^{\prime}$, where $\mathfrak{t}_{i}^{\prime} \in \mathrm{C}^{1}\left(G_{k\left(T_{i}\right)},\left\langle\left(T_{i}\right)-\left(T_{0}\right)\right\rangle\right)$ is given by:

$$
\mathfrak{t}_{i}^{\prime}(\sigma):=\left\{\begin{array}{lr}
0 & \sigma\left(\sqrt{d_{i}^{\prime}}\right)=\sqrt{d_{i}^{\prime}} \\
\left(T_{i}\right)-\left(T_{0}\right) & \sigma\left(\sqrt{d_{i}^{\prime}}\right)=-\sqrt{d_{i}^{\prime}}
\end{array}\right.
$$

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

$$
\eta_{i}:=\partial \operatorname{res}(\mathfrak{a}) \cup_{1} \mathfrak{t}_{i}^{\prime}-\operatorname{res}(\mathfrak{a}) \cup_{2} \partial \mathfrak{t}_{i}^{\prime} \in \mathrm{Z}^{3}\left(G_{k\left(T_{i}\right)}, \mathbb{G}_{m}\right)
$$

Now $\left[k\left(T_{i}\right)\left(\sqrt{d_{i}^{\prime}}\right): k\left(T_{i}\right)\right]=2$ and values of $\mathfrak{t}_{i}^{\prime}$ are defined over $k\left(T_{i}\right)$. Use lemma 3 to find $\epsilon_{i}$ s s.t. $\partial \epsilon_{i}=\eta_{i}$ !

## Form of the CTP

## Computing the

Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate pairing
(CTP)
Effective computation of CTP

How to determine the splitting field of $\eta$

Extra "nice" curves

## A similar trick for the local part gives

## Theorem 5 <br> Cassels-Tate pairing on 2-Selmer groups of odd-degree

 hyperelliptic Jacobians takes the following form. where $\delta_{v, i} \in k_{v}\left(T_{i}\right)^{\times}$and $(\cdot, \cdot) k_{k_{v}}\left(T_{i}\right)$ is the Hilbert's symbol.
## Remark 6

- Finding the local point witnessing local triviality of $\alpha$


## Form of the CTP

Computing the Cassels-Tate pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate
pairing
(CTP)
Effective

How to determine the splitting field of $\eta$

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:

$$
(-1)^{2\left\langle a, a^{a^{\prime}}\right\rangle_{\mathrm{CT}}}=\prod_{v} \prod_{G_{k_{v}} \text {-orbits }}\left(\delta_{v, i}, d_{i}^{\prime}\right)_{k_{v}\left(T_{i}\right)},
$$

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

## Remark 6

Finding the local point witnessing local triviality of $\alpha$

## Form of the CTP

Computing the Cassels-Tate pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate
pairing
(CTP)
Effective
computation of CTP

How to determine the splitting field of $\eta$

Extra "nice" curves

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:

$$
(-1)^{2\left\langle a, a^{\prime}\right\rangle_{\mathrm{CT}}}=\prod_{v} \prod_{G_{k v} \text {-orbits }}\left(\delta_{v, i}, d_{i}^{\prime}\right)_{k_{v}\left(T_{i}\right)},
$$

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

## Remark 6

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

## Form of the CTP

Computing the Cassels-Tate pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate
pairing
(CTP)
Effective
computation of CTP

How to determine the splitting field of $\eta$

Extra "nice" curves

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:

$$
(-1)^{2\left\langle a, a^{a^{\prime}}\right\rangle_{\mathrm{CT}}}=\prod_{v} \prod_{G_{k_{v}} \text {-orbits }}\left(\delta_{v, i}, d_{i}^{\prime}\right)_{k_{v}\left(T_{i}\right)},
$$

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

## Remark 6

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

- Finding the local point witnessing local triviality of $\alpha$.


## Form of the CTP

Computing the Cassels-Tate pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate
pairing
(CTP)
Effective computation of CTP

How to determine the splitting field of $\eta$

Extra "nice" curves

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:

$$
(-1)^{2\left\langle a, a^{\prime}\right\rangle_{\mathrm{CT}}}=\prod_{v} \prod_{G_{k v} \text {-orbits }}\left(\delta_{v, i}, d_{i}^{\prime}\right)_{k_{v}\left(T_{i}\right)},
$$

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

## Remark 6

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

- Finding the local point witnessing local triviality of $\alpha$.
- Solving a Hilbert 90 problem.


## Some remarks!

Computing the
Cassels-Tate
pairing on
odd-degree
hyperelliptic
Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate pairing
(CTP)
Effective computation of CTP

How to determine the splitting field of $\eta$

Extra "nice" curves

■ Constructing $\epsilon$ in the proof of lemma 3 requires:


## Some remarks!

Computing the Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate pairing (CTP)
Effective computation of CTP

How to determine the splitting field of $\eta$

■ Constructing $\epsilon$ in the proof of lemma 3 requires:
■ Trivializing some explicitly given 2-cocycles that represent trivial class in $\operatorname{Br}(k)$ (hard part).

- 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!

Computing the Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate pairing (CTP)
Effective computation of CTP

How to determine the splitting field of $\eta$

■ Constructing $\epsilon$ in the proof of lemma 3 requires:

- Trivializing some explicitly given 2-cocycles that represent trivial class in $\operatorname{Br}(k)$ (hard part).
- Solving some Hilbert 90 problems explicitly (easy part).


## Some remarks!

Computing the Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate pairing (CTP)
Effective computation of CTP

How to determine the splitting field of $\eta$

■ Constructing $\epsilon$ in the proof of lemma 3 requires:

- Trivializing some explicitly given 2 -cocycles that represent trivial class in $\operatorname{Br}(k)$ (hard part).
■ Solving some Hilbert 90 problems explicitly (easy part).
- Gluing the above information carefully.


## Some remarks!

Computing the Cassels-Tate
pairing on
odd-degree
hyperelliptic
Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate
pairing
(CTP)
Effective
computation of CTP

How to determine the splitting field of $\eta$

■ Constructing $\epsilon$ in the proof of lemma 3 requires:

- Trivializing some explicitly given 2-cocycles that represent trivial class in $\operatorname{Br}(k)$ (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!

Computing the Cassels-Tate pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations

■ Constructing $\epsilon$ in the proof of lemma 3 requires:

- Trivializing some explicitly given 2-cocycles that represent trivial class in $\operatorname{Br}(k)$ (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

## Computing

 theCassels-Tate
pairing on odd-degree hyperelliptic Jacobians

Notations
and

Cassels-Tate pairing

Effective computation of CTP

How to determine the splitting field of $\eta$

Extra "nice" curves

## Definition 7

## If $\alpha$ is good, then we can explicitly write $\epsilon_{i}$ such that $\partial \epsilon_{i}=\eta_{i}$

For a fixed i, the values of $\epsilon_{i}$ are combinations of pijs where $p_{i j}:=\sqrt{d_{i}} u^{*}+\sqrt{d_{j}} v^{*}$, and $u^{*}, v^{*}$ satisfies $C_{i j}$
Trivializing quaternion algebras corresponding to $C_{i j}$ is probably simpler!

## Good curves

Computing the
Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate
pairing (CTP)

Effective computation of CTP

How to determine the splitting field of $\eta$

Extra "nice" curves

## Definition 7

Recall $e_{i} s$ are the roots of $f$.

- An $\alpha=\left(d_{1}, \ldots, d_{2 g+1}\right) \in \operatorname{Sel}^{(2)}(J)$ with $d_{i} \in k\left(e_{i}\right)^{\times}$is said to be good if for each $j$, the conics

$$
C_{i j}: d_{i} u^{2}-d_{j} v^{2}+e_{i}-e_{j}=0 \text { has a solution over } k\left(e_{i}, e_{j}\right) .
$$

## Good curves

Computing the
Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate
pairing
(CTP)
Effective
computation of CTP

How to determine the splitting field of $\eta$

Extra "nice" curves

## Definition 7

Recall $e_{i} s$ are the roots of $f$.

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

If $\alpha$ is good, then we can explicitly write $\epsilon_{i}$ such that $\partial \epsilon_{i}=\eta_{i}$
$\square$


Trivializing quaternion simoler!

## Good curves

H. Shukla

Notations
preliminaries
Cassels-Tate
pairing
(CTP)
Effective computation of CTP

How to
determine
the splitting field of $\eta$

Extra "nice" curves

## Definition 7

Recall $e_{i} s$ are the roots of $f$.

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

If $\alpha$ is good, then we can explicitly write $\epsilon_{i}$ such that $\partial \epsilon_{i}=\eta_{i}$.
For a fixed $i$, the values of $\epsilon_{i}$ are combinations of $p_{i j}$ s where


Trivializing quaternion algebras corresponding to $C_{i j}$ is probably simnler!

## Good curves

H. Shukla

Notations

How to

## Definition 7

Recall $e_{i} s$ are the roots of $f$.

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

If $\alpha$ is good, then we can explicitly write $\epsilon_{i}$ such that $\partial \epsilon_{i}=\eta_{i}$.
For a fixed $i$, the values of $\epsilon_{i}$ are combinations of $p_{i j} \mathrm{~s}$ where $p_{i j}:=\sqrt{d_{i}} u^{*}+\sqrt{d_{j}} v^{*}$, and $u^{*}, v^{*}$ satisfies $C_{i j}$.

## Good curves

H. Shukla

Notations

How to

## Definition 7

Recall $e_{i} s$ are the roots of $f$.

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

If $\alpha$ is good, then we can explicitly write $\epsilon_{i}$ such that $\partial \epsilon_{i}=\eta_{i}$.
For a fixed $i$, the values of $\epsilon_{i}$ are combinations of $p_{i j} \mathrm{~s}$ where $p_{i j}:=\sqrt{d_{i}} u^{*}+\sqrt{d_{j}} v^{*}$, and $u^{*}, v^{*}$ satisfies $C_{i j}$.
Trivializing quaternion algebras corresponding to $C_{i j}$ is probably simpler!

## Some statistics on good curves

```
Computing
    the
Cassels-Tate
    pairing on
    odd-degree
hyperelliptic
    Jacobians
    H. Shukla
Notations
and
preliminaries
Cassels-Tate
pairing
(CTP)
Effective
computation
of CTP
How to
determine
the splitting
field of \eta
Extra "nice"
curves
```


## Some statistics on good curves

Computing the
Cassels-Tate
pairing on odd-degree hyperelliptic Jacobians
H. Shukla

Notations
and
preliminaries
Cassels-Tate pairing
(CTP)
Effective

How to determine the splitting fietd of $\eta$

Extra "nice" curves

## Some statistics on good curves

Computing the

■ Hope: Most of the curves are good.

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


## Computing the <br> Cassels-Tate <br> pairing on odd-degree hyperelliptic Jacobians <br> H. Shukla <br> Notations <br> and <br> preliminaries <br> Questions?

Cassels-Tate pairing (CTP)

Effective computation of CTP

How to determine the splitting field of $\eta$

Extra "nice" curves

## Computing the <br> Cassels-Tate <br> pairing on odd-degree hyperelliptic Jacobians <br> H. Shukla <br> Notations and <br> preliminaries <br> Thank You!

