

# 2-Selmer group of even hyperelliptic curves over function fields

Dao Van Thinh

Department of Mathematics  
National University of Singapore

Pan Asia Number Theory Conference, 2018

# Outline

## Main results

The problem over  $\mathbb{Q}$

The problem over  $\mathbb{F}_q(C)$

# Outline

## Main results

The problem over  $\mathbb{Q}$

The problem over  $\mathbb{F}_q(C)$

## Proof of the main theorem

Vinberg's representation of type  $A_{2n+1}$

Connection to hyperelliptic curves

Canonical reduction theory of  $G$ -bundles

Some computations

# Outline

## Main results

The problem over  $\mathbb{Q}$

The problem over  $\mathbb{F}_q(C)$

## Proof of the main theorem

Vinberg's representation of type  $A_{2n+1}$

Connection to hyperelliptic curves

Canonical reduction theory of  $G$ -bundles

Some computations

## Odd hyperelliptic curve

Theorem (M. Bhargava and B. Gross (2012))

*When all hyperelliptic curves of fixed genus  $n \geq 1$  over  $\mathbb{Q}$  having a rational Weierstrass point are ordered by height, the average size of the 2-Selmer groups of their Jacobians is 3.*

## Odd hyperelliptic curve

### Theorem (M. Bhargava and B. Gross (2012))

*When all hyperelliptic curves of fixed genus  $n \geq 1$  over  $\mathbb{Q}$  having a rational Weierstrass point are ordered by height, the average size of the 2–Selmer groups of their Jacobians is 3.*

### Corollary

*The average rank of of the Mordell-Weil groups of the Jacobians of such curves is at most  $3/2$ .*

## Even hyperelliptic curve

Theorem (A. Shankar and X. Wang (2014))

*When all hyperelliptic curves of fixed genus  $n \geq 2$  over  $\mathbb{Q}$  having a marked rational non-Weierstrass point are ordered by height, the average size of the 2–Selmer groups of their Jacobians is 6.*

## Even hyperelliptic curve

### Theorem (A. Shankar and X. Wang (2014))

*When all hyperelliptic curves of fixed genus  $n \geq 2$  over  $\mathbb{Q}$  having a marked rational non-Weierstrass point are ordered by height, the average size of the 2–Selmer groups of their Jacobians is 6.*

### Corollary

*The average rank of the Mordell-Weil groups of the Jacobians of the above curves is at most  $5/2$ .*



## Even hyperelliptic curve

### Theorem (A. Shankar and X. Wang (2014))

*When all hyperelliptic curves of fixed genus  $n \geq 2$  over  $\mathbb{Q}$  having a marked rational non-Weierstrass point are ordered by height, the average size of the 2-Selmer groups of their Jacobians is 6.*

### Corollary

*The average rank of the Mordell-Weil groups of the Jacobians of the above curves is at most  $5/2$ .*

### Theorem (A. Shankar and X. Wang (2014))

*The proportion of monic even degree hyperelliptic curves having genus  $n \geq 4$  that have exactly two rational points is at least  $1 - (48n + 120)2^{-n}$ .*

# Outline

## Main results

The problem over  $\mathbb{Q}$

The problem over  $\mathbb{F}_q(C)$

## Proof of the main theorem

Vinberg's representation of type  $A_{2n+1}$

Connection to hyperelliptic curves

Canonical reduction theory of  $G$ -bundles

Some computations

## Notation

- $k = \mathbb{F}_q$  with  $(\text{char}(k), 2n + 2) = 1$
- $C$  is a smooth, complete, geometrically connected curve over  $k$
- $K = k(C)$  the function field of  $C$

## Even hyperelliptic curve

An even hyperelliptic curve of genus  $n$  is the smooth projective model of the affine curve defined by

$$H : y^2 = x^{2n+2} + c_2 x^{2n} + \cdots + c_{2n+2},$$

where  $c_i \in K$ , and the tuple  $(c_i)_{2 \leq i \leq 2n+2}$  is unique up to the following identification

$$(c_2, c_3, \dots, c_{2n+2}) \equiv (\lambda^2 \cdot c_2, \lambda^3 c_3, \dots, \lambda^{2n+2} \cdot c_{2n+2}) \quad \lambda \in K^\times.$$

## Minimal integral model

Fix the data  $(c_2, c_3, \dots, c_{2n+2})$ , we define the minimal integral model of  $H$  as follows: for each point  $v \in |C|$ , we can choose an integer  $n_v$  which is the smallest integer satisfying that: the tuple

$$(\varpi_v^{2n_v} c_2, \varpi_v^{3n_v} c_3, \dots, \varpi_v^{(2n+2)n_v} c_{2n+2})$$

has coordinates in  $\mathcal{O}_{K_v}$ . Given  $(n_v)_{v \in |C|}$ , we define the invertible sheaf  $\mathcal{L}_H \subset K$  whose sections over a Zariski open  $U \subset C$  are given by

$$\mathcal{L}_H(U) = K \cap \left( \prod_{v \in U} \varpi_v^{-n_v} \mathcal{O}_{K_v} \right).$$

Then  $c_i \in H^0(C, \mathcal{L}_H^{\otimes i})$  for all  $2 \leq i \leq 2n+2$ . Furthermore, the stratum  $(\mathcal{L}_H, \underline{c})$  is minimal in the sense that there is no proper subsheaf  $\mathcal{M}$  of  $\mathcal{L}_H$  such that  $c_i \in H^0(C, \mathcal{M}^{\otimes i})$  for all  $i$ .

# Height of hyperelliptic curves

## Definition

The height of the hyperelliptic curve  $H$  is defined to be the degree of the associated line bundle  $\mathcal{L}_H$ .

## Height of hyperelliptic curves

### Definition

The height of the hyperelliptic curve  $H$  is defined to be the degree of the associated line bundle  $\mathcal{L}_H$ .

We are going to consider the following family of hyperelliptic curves:

### Definition

An even hyperelliptic curve  $H$  with an associated minimal data  $(\mathcal{L}_H, \underline{c})$  is called to be **transversal** if the discriminant  $\Delta(\underline{c}) \in H^0(C, \mathcal{L}_H^{\otimes (2n+1)(2n+2)})$  is square-free.

## Main theorem

Denote  $\mathcal{A}_{\leq d}^{trans}$  to be the set of all transversal even hyperelliptic curves of height less than or equal to  $d$ .



## Main theorem

Denote  $\mathcal{A}_{\leq d}^{trans}$  to be the set of all transversal even hyperelliptic curves of height less than or equal to  $d$ .

### Theorem

*When all transversal even hyperelliptic curves of genus  $n \geq 2$  over  $K$  are ordered by height, the average size of the 2–Selmer group of their Jacobians is 6. Equivalently,*

$$\lim_{d \rightarrow \infty} \frac{\sum_{H \in \mathcal{A}_{\leq d}^{trans}} \frac{|Sel_2(H)|}{|Aut(H, \infty)|}}{\sum_{H \in \mathcal{A}_{\leq d}^{trans}} \frac{1}{|Aut(H, \infty)|}} = 6.$$

## Notation

- $\mathcal{H}$ : the minimal integral model of  $H$
- $\mathcal{J}_H$  and  $\mathcal{J}_{\mathcal{H}}$  are Jacobian group schemes associated to  $H$  and  $\mathcal{H}$  respectively.
- Observe that  $\mathcal{J}_H$  is the generic fiber of  $\mathcal{J}_{\mathcal{H}}$ .

## Restatement of the main theorem

### Lemma

If  $H$  is transversal, then  $\mathcal{J}_{\mathcal{H}}$  is the Néron model of  $\mathcal{J}_H$ .  
Furthermore,

$$|\mathrm{Sel}_2(\mathcal{J}_H)| = |H^1(C, \mathcal{J}_{\mathcal{H}}[2])|.$$

The main theorem is equivalent to:

$$\lim_{d \rightarrow \infty} \frac{\sum_{H \in \mathcal{A}_{\leq d}^{\mathrm{trans}}} \frac{|H^1(C, \mathcal{J}_{\mathcal{H}}[2])|}{|Aut(H, \infty)|}}{\sum_{H \in \mathcal{A}_{\leq d}^{\mathrm{trans}}} \frac{1}{|Aut(H, \infty)|}} = 6.$$

# Outline

## Main results

The problem over  $\mathbb{Q}$

The problem over  $\mathbb{F}_q(C)$

## Proof of the main theorem

Vinberg's representation of type  $A_{2n+1}$

Connection to hyperelliptic curves

Canonical reduction theory of  $G$ -bundles

Some computations

Let  $(U, Q)$  be the split quadratic space over  $k$  of dimension  $2n + 2$  and discriminant 1. Then for any linear operator  $T : U \rightarrow U$ , we defined its adjoint  $T^*$  by the following equation:

$$\langle Tv, w \rangle_Q = \langle v, T^*w \rangle_Q, \quad \forall v, w \in U.$$

where  $\langle v, w \rangle_Q = Q(v + w) - Q(v) - Q(w)$  denotes the bilinear form associated to  $Q$ . The Vinberg's representation we are going to study is the conjugate action of

$$G := PSO(U) = \{g \in GL(U) | gg^* = I, \det(g) = 1\} / \mu_2$$

on

$$V = \{T : U \rightarrow U | T = T^*, \text{trace}(T) = 0\} \cong \text{Sym}_0^2(U).$$

## GIT quotient

For each  $T \in V$ , denote  $f_T(x)$  be the characteristic polynomial of  $T$ :

$$f_T(x) = x^{2n+2} + c_2(T)x^{2n} + \cdots + c_{2n+1}(T)x + c_{2n+2}(T).$$

Then

$$V//G \cong \operatorname{Spec}(k[c_2, c_3, \dots, c_{2n+2}]) = S.$$

We denote the projection map by  $\pi : V \rightarrow S$ .

## Regular locus

Set

$$\begin{aligned} V^{reg}(\bar{k}) &= \{T \in V(\bar{k}) \mid |\text{Stab}_{G(\bar{k})}(T)| \text{ is finite}\} \\ &= \{T \in V(\bar{k}) \mid f_T(x) \text{ is its minimal polynomial}\} \end{aligned}$$

## Regular locus

Set

$$V^{reg}(\bar{k}) = \{T \in V(\bar{k}) \mid |\text{Stab}_{G(\bar{k})}(T)| \text{ is finite}\}$$

$$= \{T \in V(\bar{k}) \mid f_T(x) \text{ is its minimal polynomial}\}$$

$\implies$  for any field extension  $k \subset F$  and  $T \in V^{reg}(F)$ ,

$$\text{Stab}_G(T) \cong (\text{Res}_{L/F} \mu_2)_{N=1} / \mu_2,$$

where  $L = F[x]/(f_T(x))$ .



## Stabilizer group scheme over $S$

### Theorem

*There exists a unique group scheme  $I_S$  over  $S$  equipped with an isomorphism  $\pi^* I_S \rightarrow \text{Stab}_G$  over  $V^{\text{reg}}$ . This isomorphism is  $G$ -equivariant, thus, as a corollary, there is a  $\mathbb{G}_m$ -equivariant isomorphism of stacks  $[BI_S] \cong [V^{\text{reg}}/G]$ , where  $BI_S$  is the relative classifying stack of  $I_S$  over  $S$ .*

# Outline

## Main results

The problem over  $\mathbb{Q}$

The problem over  $\mathbb{F}_q(C)$

## Proof of the main theorem

Vinberg's representation of type  $A_{2n+1}$

Connection to hyperelliptic curves

Canonical reduction theory of  $G$ -bundles

Some computations

## The generalized Jacobian group scheme

For each  $\underline{c} = (c_2, c_3, \dots, c_{2n+2}) \in S$ , the associated polynomial

$$f_{\underline{c}}(x) = x^{2n+2} + c_2 x^{2n} + \dots + c_{2n+1} x + c_{2n+2}$$

defines an even hyperelliptic curve  $y^2 = f_{\underline{c}}(x)$  (we allow singular hyperelliptic curves)

## The generalized Jacobian group scheme

For each  $\underline{c} = (c_2, c_3, \dots, c_{2n+2}) \in S$ , the associated polynomial

$$f_{\underline{c}}(x) = x^{2n+2} + c_2 x^{2n} + \dots + c_{2n+1} x + c_{2n+2}$$

defines an even hyperelliptic curve  $y^2 = f_{\underline{c}}(x)$  (we allow singular hyperelliptic curves)  $\implies$  a group scheme  $\mathcal{J}_S$  which represents the (generalized) Jacobian functor.

## The generalized Jacobian group scheme

For each  $\underline{c} = (c_2, c_3, \dots, c_{2n+2}) \in S$ , the associated polynomial

$$f_{\underline{c}}(x) = x^{2n+2} + c_2 x^{2n} + \dots + c_{2n+1} x + c_{2n+2}$$

defines an even hyperelliptic curve  $y^2 = f_{\underline{c}}(x)$  (we allow singular hyperelliptic curves)  $\implies$  a group scheme  $\mathcal{J}_S$  which represents the (generalized) Jacobian functor.

Set

$$\mathcal{J}_{V^{reg}} := \mathcal{J}_S \times_S V^{reg}$$

# Stabilizer group scheme and Jacobian

## Theorem

*There exists a canonical  $G$ –equivariant isomorphism over  $V^{\text{reg}}$  between the stabilizer scheme  $\text{Stab}_G$  and  $\mathcal{J}_{V^{\text{reg}}}[2]$ .*

# Stabilizer group scheme and Jacobian

## Theorem

*There exists a canonical  $G$ –equivariant isomorphism over  $V^{\text{reg}}$  between the stabilizer scheme  $\text{Stab}_G$  and  $\mathcal{J}_{V^{\text{reg}}}[2]$ .*

## Corollary

*The above isomorphism induces an isomorphism over  $S$  from  $I_S$  to  $\mathcal{J}_S[2]$ .*

$\implies$  an isomorphism between stacks

$$B\mathcal{J}_S[2] \cong [V^{\text{reg}}/G]$$

## An interpretation of $H^1(C, \mathcal{J}_{\mathcal{H}}[2])$

- Hyperelliptic curve  $H \leftrightarrow (\mathcal{L}_H, \underline{c})$ ,  $\underline{c} \in S(K)$



## An interpretation of $H^1(C, \mathcal{J}_{\mathcal{H}}[2])$

- Hyperelliptic curve  $H \leftrightarrow (\mathcal{L}_H, \underline{c})$ ,  $\underline{c} \in S(K)$

$$\leftrightarrow \alpha_H : C \rightarrow [S/\mathbb{G}_m]$$

## An interpretation of $H^1(C, \mathcal{J}_{\mathcal{H}}[2])$

- Hyperelliptic curve  $H \leftrightarrow (\mathcal{L}_H, \underline{c})$ ,  $\underline{c} \in S(K)$

$$\leftrightarrow \alpha_H : C \rightarrow [S/\mathbb{G}_m]$$

Set  $\mathcal{A} = \text{Hom}(C, [S/\mathbb{G}_m])$

## An interpretation of $H^1(C, \mathcal{J}_{\mathcal{H}}[2])$

- Hyperelliptic curve  $H \leftrightarrow (\mathcal{L}_H, \underline{c})$ ,  $\underline{c} \in S(K)$

$$\leftrightarrow \alpha_H : C \rightarrow [S/\mathbb{G}_m]$$

Set  $\mathcal{A} = \text{Hom}(C, [S/\mathbb{G}_m])$

- Set  $\mathcal{M} = \text{Hom}(C, [B\mathcal{J}_S[2]/\mathbb{G}_m])$

## An interpretation of $H^1(C, \mathcal{J}_{\mathcal{H}}[2])$

- Hyperelliptic curve  $H \leftrightarrow (\mathcal{L}_H, \underline{c})$ ,  $\underline{c} \in S(K)$

$$\leftrightarrow \alpha_H : C \rightarrow [S/\mathbb{G}_m]$$

Set  $\mathcal{A} = \text{Hom}(C, [S/\mathbb{G}_m])$

- Set  $\mathcal{M} = \text{Hom}(C, [B\mathcal{J}_S[2]/\mathbb{G}_m])$

$$\implies \text{a base map } b : \mathcal{M} \rightarrow \mathcal{A}$$

## An interpretation of $H^1(C, \mathcal{J}_{\mathcal{H}}[2])$

- Hyperelliptic curve  $H \leftrightarrow (\mathcal{L}_H, \underline{c}), \quad \underline{c} \in S(K)$

$$\leftrightarrow \alpha_H : C \rightarrow [S/\mathbb{G}_m]$$

Set  $\mathcal{A} = \text{Hom}(C, [S/\mathbb{G}_m])$

- Set  $\mathcal{M} = \text{Hom}(C, [B\mathcal{J}_S[2]/\mathbb{G}_m])$

$$\implies \text{a base map } b : \mathcal{M} \rightarrow \mathcal{A}$$

$$\implies H^1(C, \mathcal{J}_{\mathcal{H}}[2]) = b^{-1}(\alpha_H)$$

## Counting points on stacks

We also have a commutative diagram:

$$\begin{array}{ccc}
 \mathcal{M} & \xrightarrow{b} & \mathcal{A} \\
 \searrow \pi_{\mathcal{M}} & & \swarrow \pi_{\mathcal{A}} \\
 & \text{Hom}(C, B\mathbb{G}_m) &
 \end{array}$$

## Counting points on stacks

We also have a commutative diagram:

$$\begin{array}{ccc}
 \mathcal{M} & \xrightarrow{b} & \mathcal{A} \\
 \searrow \pi_{\mathcal{M}} & & \swarrow \pi_{\mathcal{A}} \\
 & \text{Hom}(C, B\mathbb{G}_m) &
 \end{array}$$

$\implies$  for any line bundle  $\mathcal{F}$  over  $C$ ,

$$|\mathcal{M}_{\mathcal{F}}(k)| = \sum_{H \in \mathcal{A}_{\mathcal{F}}(k)} |H^1(C, \mathcal{J}_{\mathcal{H}}[2])|.$$

Now it is enough to prove that

$$\lim_{\deg(\mathcal{F}) \rightarrow \infty} \frac{|\mathcal{M}_{\mathcal{F}}^{trans}(k)|}{|\mathcal{A}_{\mathcal{F}}^{trans}(k)|} = 6,$$

where  $\mathcal{M}_{\mathcal{F}}^{trans} = b^{-1}(\mathcal{A}_{\mathcal{F}}^{trans})$ .



## Another interpretation of $\mathcal{M}_{\mathcal{F}}(k)$

From the isomorphism:

$$[B\mathcal{J}_S[2]/\mathbb{G}_m] \cong [V^{reg}/(G \times \mathbb{G}_m)]$$

$$\implies \mathcal{M} \cong \text{Hom}(C, [V^{reg}/(G \times \mathbb{G}_m)]).$$

## Another interpretation of $\mathcal{M}_{\mathcal{F}}(k)$

From the isomorphism:

$$[B\mathcal{I}S[2]/\mathbb{G}_m] \cong [V^{reg}/(G \times \mathbb{G}_m)]$$

$$\implies \mathcal{M} \cong \text{Hom}(C, [V^{reg}/(G \times \mathbb{G}_m)]).$$

$\implies$  a  $k$ -point of  $\mathcal{M}_{\mathcal{F}}$  is a pair  $(\mathcal{E}, s)$ , where  $\mathcal{E}$  is a principal  $G$ -bundle, and  $s$  is a section of

$$V^{reg}(\mathcal{E}, \mathcal{F}) = (V^{reg} \times^G \mathcal{E}) \otimes \mathcal{F}$$

# Outline

## Main results

The problem over  $\mathbb{Q}$

The problem over  $\mathbb{F}_q(C)$

## Proof of the main theorem

Vinberg's representation of type  $A_{2n+1}$

Connection to hyperelliptic curves

Canonical reduction theory of  $G$ -bundles

Some computations

As algebraic groups over  $k$ :

$$G = \mathrm{PSO}(U) \cong \mathrm{GSO}(U)/\mathbb{G}_m,$$

where  $\mathbb{G}_m$  denotes the center of  $\mathrm{GSO}(U)$ .

$\implies G$ –bundles  $\leftrightarrow \mathrm{GSO}(U)/\mathbb{G}_m$ –bundles.

Moreover, any  $\mathrm{GSO}(U)/\mathbb{G}_m$ –bundle can be lifted to a  $\mathrm{GSO}(U)$ –bundle uniquely up to tensor twist by a line bundle.

## Canonical reduction of $\mathrm{GSO}(2n+2)$ –bundles

Let  $\mathcal{E}$  be a  $\mathrm{GSO}(2n+2)$ –bundle. Then there exists uniquely a parabolic subgroup  $P \subset \mathrm{GSO}(U)$  with Levi quotient  $L$  and the associated  $P$ –bundle  $\mathcal{E}_P$  such that

1. We have an isomorphism  $\mathcal{E} \cong \mathcal{E}_P(\mathrm{GSO}(U))$ , where  $\mathcal{E}_P(\mathrm{GSO}(U))$  is the quotient  $(\mathcal{E}_P \times \mathrm{GSO}(U))/P$  with the following action of  $P$  on  $\mathcal{E}_P \times \mathrm{GSO}(U)$  : for any  $h \in P$ ,  $e \in \mathcal{E}_P$ , and  $g \in \mathrm{GSO}(U)$  then  $h.(e, g) = (h.e, h^{-1}g)$ .

## Canonical reduction of $\mathrm{GSO}(2n+2)$ –bundles

Let  $\mathcal{E}$  be a  $\mathrm{GSO}(2n+2)$ –bundle. Then there exists uniquely a parabolic subgroup  $P \subset \mathrm{GSO}(U)$  with Levi quotient  $L$  and the associated  $P$ –bundle  $\mathcal{E}_P$  such that

1. We have an isomorphism  $\mathcal{E} \cong \mathcal{E}_P(\mathrm{GSO}(U))$ , where  $\mathcal{E}_P(\mathrm{GSO}(U))$  is the quotient  $(\mathcal{E}_P \times \mathrm{GSO}(U))/P$  with the following action of  $P$  on  $\mathcal{E}_P \times \mathrm{GSO}(U)$  : for any  $h \in P$ ,  $e \in \mathcal{E}_P$ , and  $g \in \mathrm{GSO}(U)$  then  $h.(e, g) = (h.e, h^{-1}g)$ .
2. The Levi bundle  $\mathcal{E}_L$  associated, by extension of structure group, to  $\mathcal{E}_P$  for the projection  $P \rightarrow L$  is semi-stable.

## Canonical reduction of $\mathrm{GSO}(2n+2)$ –bundles

Let  $\mathcal{E}$  be a  $\mathrm{GSO}(2n+2)$ –bundle. Then there exists uniquely a parabolic subgroup  $P \subset \mathrm{GSO}(U)$  with Levi quotient  $L$  and the associated  $P$ –bundle  $\mathcal{E}_P$  such that

1. We have an isomorphism  $\mathcal{E} \cong \mathcal{E}_P(\mathrm{GSO}(U))$ , where  $\mathcal{E}_P(\mathrm{GSO}(U))$  is the quotient  $(\mathcal{E}_P \times \mathrm{GSO}(U))/P$  with the following action of  $P$  on  $\mathcal{E}_P \times \mathrm{GSO}(U)$  : for any  $h \in P$ ,  $e \in \mathcal{E}_P$ , and  $g \in \mathrm{GSO}(U)$  then  $h.(e, g) = (h.e, h^{-1}g)$ .
2. The Levi bundle  $\mathcal{E}_L$  associated, by extension of structure group, to  $\mathcal{E}_P$  for the projection  $P \rightarrow L$  is semi-stable.
3. For every non-trivial character  $\chi$  of  $P$  which is a non-negative linear combination of simple roots with respect to some Borel subgroup contained in  $P$ , the line bundle  $\chi_*\mathcal{E}_P$  on  $C$  has positive degree.

Assume that the Levi subgroup

$$L = \mathrm{GL}_{n_1} \times \mathrm{GL}_{n_2} \times \cdots \times \mathrm{GL}_{n_t} \times \mathrm{GSO}(2h).$$

$\implies$  a flag of isotropic subspaces

$$0 = V_0 \subset V_1 \subset \cdots \subset V_t \subset V_t^* \subset \cdots \subset V_1^* \subset U,$$

where  $\dim(V_i/V_{i-1}) = n_i$  for  $1 \leq i \leq t$ , and  $\dim(V_t^*/V_t) = 2h$ .

$\implies$  a filtration of the vector bundle  $\mathcal{E} \times^{\mathrm{GSO}(U)} U$ :

$$0 \subset \mathcal{E}_P \times^P V_1 \subset \cdots \subset \mathcal{E}_P \times^P V_t \subset \mathcal{E}_P \times^P V_t^* \subset \cdots \subset \mathcal{E}_P \times^P V_1^*$$

satisfying that the quotient bundles

$$X_i = \mathcal{E}_P \times^P V_i / (\mathcal{E}_P \times^P V_{i-1}), \quad 1 \leq i \leq t$$

and

$$X_{t+1} = (\mathcal{E}_P \times^P V_t^*) / (\mathcal{E}_P \times^P V_t)$$

are semistable.



Moreover,

$$(\mathcal{E}_P \times^P V_{i-1}^*)/(\mathcal{E}_P \times^P V_i^*) \cong X_i^\vee \otimes \mathcal{L}$$

and

$$X_{t+1} \cong X_{t+1}^\vee \otimes \mathcal{L}.$$

Denote the slope of  $X_i$  by  $\mu_i$ , then the "canonical conditions" imply that:

$$\begin{aligned} \mu_1 &> \mu_2 > \cdots > \mu_t > \mu_{t+1} = d/2 \text{ if } h > 0, \\ \mu_1 &> \mu_2 > \cdots > \mu_t \quad \text{and} \quad \mu_{t-1} + \mu_t > d \text{ if } h = 0. \end{aligned}$$

# Semistable filtration of $(\mathcal{E} \times^{\mathrm{GSO}(U)} V)$

we obtain the following "matrix filtration" of  $\mathrm{Sym}_0^2(\mathcal{E}) \otimes \mathcal{L}^\vee$ :

$$\begin{array}{ccccccc}
 \mathrm{Sym}^2(X_1) \otimes \mathcal{L}^\vee & X_1 \otimes X_2 \otimes \mathcal{L}^\vee & \cdots & X_1 \otimes X_t \otimes \mathcal{L}^\vee & X_1 \otimes X_{t+1}^\vee & X_1 \otimes X_t^\vee & \cdots & X_1 \otimes X_1^\vee \\
 X_2 \otimes X_1 \otimes \mathcal{L}^\vee & \mathrm{Sym}^2(X_2) \otimes \mathcal{L}^\vee & \cdots & X_2 \otimes X_t \otimes \mathcal{L}^\vee & X_2 \otimes X_{t+1}^\vee & X_2 \otimes X_t^\vee & \cdots & X_2 \otimes X_1^\vee \\
 \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\
 X_t \otimes X_1 \otimes \mathcal{L}^\vee & X_t \otimes X_2 \otimes \mathcal{L}^\vee & \cdots & \mathrm{Sym}^2(X_t) \otimes \mathcal{L}^\vee & X_t \otimes X_{t+1}^\vee & X_t \otimes X_t^\vee & \cdots & X_t \otimes X_1^\vee \\
 X_{t+1}^\vee \otimes X_1 & X_{t+1}^\vee \otimes X_2 & \cdots & X_{t+1}^\vee \otimes X_t & \mathrm{Sym}_0^2(X_{t+1}) \otimes \mathcal{L}^\vee & X_{t+1}^\vee \otimes X_t^\vee & \cdots & X_{t+1}^\vee \otimes X_1^\vee \\
 X_t^\vee \otimes X_1 & X_t^\vee \otimes X_2 & \cdots & X_t^\vee \otimes X_t & X_t^\vee \otimes X_{t+1} & \mathrm{Sym}^2(X_t^\vee) \otimes \mathcal{L} & \cdots & X_t^\vee \otimes X_1^\vee \otimes \mathcal{L} \\
 \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\
 X_2^\vee \otimes X_1 & X_2^\vee \otimes X_2 & \cdots & X_2^\vee \otimes X_t & X_2^\vee \otimes X_{t+1} & X_2^\vee \otimes X_t^\vee \otimes \mathcal{L} & \cdots & X_2^\vee \otimes X_1^\vee \otimes \mathcal{L} \\
 X_1^\vee \otimes X_1 & X_1^\vee \otimes X_2 & \cdots & X_1^\vee \otimes X_t & X_1^\vee \otimes X_{t+1} & X_1^\vee \otimes X_t^\vee \otimes \mathcal{L} & \cdots & \mathrm{Sym}^2(X_1^\vee) \otimes \mathcal{L}
 \end{array}$$

# Outline

## Main results

The problem over  $\mathbb{Q}$

The problem over  $\mathbb{F}_q(C)$

## Proof of the main theorem

Vinberg's representation of type  $A_{2n+1}$

Connection to hyperelliptic curves

Canonical reduction theory of  $G$ -bundles

Some computations

## The case $P=B$ the Borel subgroup

The main contributors to the average

$$\lim_{\deg(\mathcal{F}) \rightarrow \infty} \frac{|\mathcal{M}_{\mathcal{F},B}^{trans}(k)|}{|\mathcal{A}_{\mathcal{F}}^{trans}|}$$

are

$$\mathcal{E} = X_1 \oplus \cdots \oplus X_{n+1} \oplus (X_{n+1}^{\vee} \otimes \mathcal{L}) \oplus \cdots \oplus (X_1^{\vee} \otimes \mathcal{L})$$

## The case $P=B$ the Borel subgroup

The main contributors to the average

$$\lim_{\deg(\mathcal{F}) \rightarrow \infty} \frac{|\mathcal{M}_{\mathcal{F},B}^{trans}(k)|}{|\mathcal{A}_{\mathcal{F}}^{trans}|}$$

are

$$\mathcal{E} = X_1 \oplus \cdots \oplus X_{n+1} \oplus (X_{n+1}^\vee \otimes \mathcal{L}) \oplus \cdots \oplus (X_1^\vee \otimes \mathcal{L})$$

satisfying that

$$\mu_i = \mu_{i+1} + f \quad \forall \quad 1 \leq i \leq n,$$

where  $f = \deg(\mathcal{F})$ ,  $\mu_i = \deg(X_i)$ .

## Case 1: $2\mu_{n+1} - d = f$

For any  $(\mathcal{E}, s) \in \mathcal{M}_{\mathcal{F}}^{trans}$ , where  $s$  is a section of

$$(V \times^{\mathrm{GSO}(U)} \mathcal{E}) \otimes \mathcal{F} = \mathrm{Sym}_0^2(\mathcal{E}) \otimes \mathcal{L}^{\vee} \otimes \mathcal{F},$$

## Case 1: $2\mu_{n+1} - d = f$

For any  $(\mathcal{E}, s) \in \mathcal{M}_{\mathcal{F}}^{trans}$ , where  $s$  is a section of

$$(V \times^{\mathrm{GSO}(U)} \mathcal{E}) \otimes \mathcal{F} = \mathrm{Sym}_0^2(\mathcal{E}) \otimes \mathcal{L}^\vee \otimes \mathcal{F},$$

then  $s$  is of the following form:

$$\begin{pmatrix} * & * & \cdots & * & * & * \\ x_1 & * & \cdots & * & * & * \\ 0 & x_2 & \cdots & * & * & * \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & x_2 & * & * \\ 0 & 0 & \cdots & 0 & x_1 & * \end{pmatrix}$$

where  $x_i \in k^*$ .

$$\xrightarrow{g \cdot s \cdot g^*} \begin{pmatrix} 0 & 0 & \cdots & 0 & * & * \\ 1 & 0 & \cdots & * & * & * \\ 0 & 1 & \cdots & * & * & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{pmatrix}, \text{ for some } g \in \text{GSO}(U)(K)$$



$$\xrightarrow{g \cdot s \cdot g^*} \begin{pmatrix} 0 & 0 & \cdots & 0 & * & * \\ 1 & 0 & \cdots & * & * & * \\ 0 & 1 & \cdots & * & * & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{pmatrix}, \text{ for some } g \in \text{GSO}(U)(K)$$

The Kostant section  $\kappa_1$

$$\xrightarrow{g \cdot s \cdot g^*} \begin{pmatrix} 0 & 0 & \cdots & 0 & * & * \\ 1 & 0 & \cdots & * & * & * \\ 0 & 1 & \cdots & * & * & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{pmatrix}, \text{ for some } g \in \text{GSO}(U)(K)$$

The Kostant section  $\kappa_1$

$\implies$  This case contributes 1 to the average.

## Case 2: $-2\mu_{n+1} + d = f$

Any section  $s$  is of the form:

$$\begin{pmatrix} * & \cdots & * & * & * & \cdots & * & * \\ x_1 & \cdots & * & * & * & \cdots & * & * \\ \vdots & \ddots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & \cdots & x_n & * & x_{n+1} & \cdots & * & * \\ 0 & \cdots & 0 & * & * & \cdots & * & * \\ 0 & \cdots & 0 & 0 & x_n & \cdots & * & * \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & x_1 & * \end{pmatrix}$$

where  $x_i \in k^\times$ .

[illegible]

[illegible]

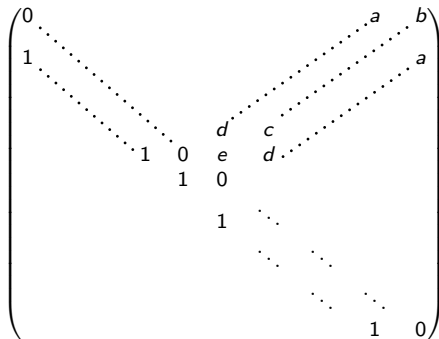
### The Kostant section $\kappa_2$

[illegible]

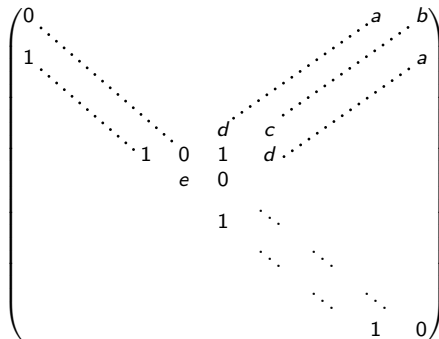
### The Kostant section $\kappa_2$

⇒ This case contributes 1 to the average.

## The case $P=B$ the Borel subgroup

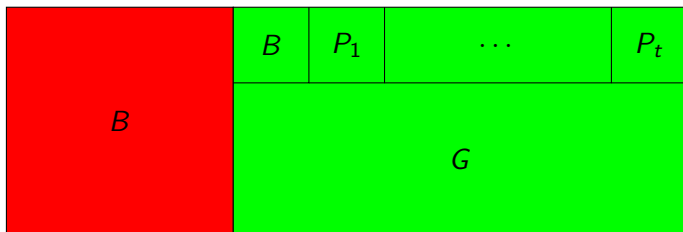


The Kostant section  $\kappa_1$



The Kostant section  $\kappa_2$

## The whole picture



$$\text{Vol}(\text{red}) = 2$$

$$\text{Vol}(\text{green}) = 4 = \tau(G)$$



# Summary

- $6 = \text{the number of Kostant sections} + \tau(G).$

## Summary

- $6 =$  the number of Kostant sections  $+ \tau(G)$ .
- By a similar method, we also can give an upperbound for the average in general case (remove the transversal condition) if we assume  $\text{char}(k)$  is big enough.

## Summary

- $6 =$  the number of Kostant sections  $+ \tau(G)$ .
- By a similar method, we also can give an upperbound for the average in general case (remove the transversal condition) if we assume  $\text{char}(k)$  is big enough.
- The method that was used here, is partially similar to the method in the paper "Average size of 2-Selmer groups of elliptic curves over function fields" of Q.P. Ho, V.B. Le Hung, and B.C. Ngo.

# Thank you!