Zeta fn. of C (or how to count pts. in C)

- Let $k = \mathbb{F}_q$, for some prime-power $q = p^e$.
- C is a smooth projective curve over k.
- Also, $C \cong C_K$ where K is the fn. field of C.

- Our interest now is in point-counting.
  I.e. for $n \in \mathbb{N}_{>0}$, how well can we estimate

$N_n := |C(\mathbb{F}_{q^n})| :=$ # of $\mathbb{F}_{q^n}$-pts. on C.

▷ $N_n = \#\{P \in C \mid d(P) \text{ divides } n\}$.

Pf: $\cdot$ $P \in GF(q^{d(P)}) \subseteq GF(q^n)$ iff $d(P) \mid n$. $\square$

- Why not study its <u>generating</u> function:

$$G(t) := \sum_{n\geq 1} N_n \cdot t^n \in \mathbb{Z}[[t]]$$

infinite sums allowed unlike $\mathbb{Z}[t]$

- With this as the goal, we define another power-series that's better behaved:

<u>Defn</u>: The <u>zeta fn. of C over k</u> is

$$Z(t) := \sum_{\substack{D\geq 0 \\ \in \mathrm{Div}(C)}} t^{d(D)} \in \mathbb{Z}[[t]].$$

$\triangleright$ $Z(t) = \prod_{P\in C} \left(1-t^{d(P)}\right)^{-1} = \prod_{P\in C}\left(1+t^{d(P)}+t^{2d(P)}+\cdots\right)$

- Eg, $t^{d(P_1)} \cdot t^{d(P_2)} = t^{d(P_1+P_2)}$

$t^{i_1 d(P_1)} \cdot t^{i_2 d(P_2)} = t^{d(i_1P_1 + i_2P_2)}$

[<u>Recall</u>: $d(i_1P_1 + i_2P_2) = i_1 \cdot d(P_1) + i_2 \cdot d(P_2)$.]

- Recall that $d(\cdot)$ does not change up to $\mathrm{Div}_a(C)$.
- We've exact sequence : $0 \to Cl_0(C) \xrightarrow{\subseteq} Cl(C) \xrightarrow{d(\cdot)} \mathbb{Z}$

▷ $\mathrm{img}(d) \trianglelefteq \mathbb{Z} \Rightarrow \exists \delta \in \mathbb{N},\ \mathrm{img}(d) = \langle \delta \rangle_{\mathbb{Z}}$.

▷ $0 \longrightarrow Cl_0(C) \xrightarrow{\subseteq} Cl(C) \xrightarrow{d(\cdot)} \delta\mathbb{Z} \longrightarrow 0$

is exact.

- Define $Cl_d(C)$ to be the set of divisor classes of $\deg = d \in \delta\mathbb{Z}$.
- We expand $Z(t)$ wrt $Cl_d(C)$:

$$\triangleright\ Z(t) = \sum_{D \geq 0} t^{d(D)} = \sum_{d \in \delta\mathbb{Z}} \sum_{\mathcal{D} \in Cl_d(C)} \sum_{D \in \mathcal{D}} t^d .$$

- We now study the two inner-sums.

<u>Lemma 1:</u> $\#\{D \in \mathcal{D} \mid D \geq 0\} = (q^{\ell(\mathcal{D})} - 1)/(q-1)$.

Pf: • Fix a $D \in \mathcal{D}$.

• $\forall\ 0 \leq D' \in \mathcal{D}$, $D' - D = (f)$, for some $f \in K$.

$\Leftrightarrow (f) + D = D' \geq 0 \Leftrightarrow f \in L(D)$.

- For $f, f' \in L(D)$, $(f) = (f') \iff f = c \cdot f'$,
  for some $c \in k^*$.

$\Rightarrow D \; \#\{\text{distinct } 0 \leq D' \in \mathcal{D}\} = \#\{\text{non-similar fns. } f \in L(D)\}$

- Let $L(D) = \langle f_1, \ldots, f_{\ell(\mathcal{D})} \rangle_k$

  $\Rightarrow$ count $= (q^{\ell(\mathcal{D})} - 1)/(q-1)$. $\square$

Lemma 2: $\forall d \in \delta\mathbb{Z}$, $|Cl_d(C)| = |Cl_0(C)| < \infty$.

Pf: • For $\mathcal{D} \in Cl_d(C)$ & $\mathcal{D}' \in Cl_0(C)$ we've the bijection:

$$\begin{aligned} Cl_d(C) &\longrightarrow Cl_0(C) \\ \mathcal{E} &\longmapsto \mathcal{E} + \mathcal{D}' - \mathcal{D} \end{aligned}$$

$\Rightarrow |Cl_d(C)| = |Cl_0(C)|$.

- Why's $|Cl_0(C)| < \infty$?
- Consider $d \in \delta\mathbb{Z}$ s.t. $d \geq g$.
- Let $D \in \mathcal{D} \in Cl_d(C)$. By Riemann's thm.:

$$\ell(D) \geq d(D) + 1 - g \geq 1.$$

$\Rightarrow$ $\exists$ a non-negative divisor in $\mathcal{D}$.

$\Rightarrow |Cl_d(C)| \leq \#\{$ non-equivalent non-negative divisors of $\deg = d\}$.

- Say, pt. $P \in C$ appears in <u>such</u> a divisor D.

$\Rightarrow$ $d(P) \leq d(D) = d$. and $\mathrm{ord}_P(D) \leq d$.

[# such pts. (in $k = \mathbb{F}_q$) is $< \infty$] $\Rightarrow |Cl_d(C)| < \infty$. $\square$

- Defn: Call $|Cl_0(C)|$ the class number of C over k, denoted by $h(C)$.

- So, $Z(t) = \sum_{d \in \mathbb{N}} \sum_{\mathcal{D} \in Cl_d(C)} \sum_{\substack{D \in \mathcal{D} \\ D \geq 0}} t^d$

$$= \sum_{\substack{d \in \mathbb{N}, \\ \mathcal{D} \in Cl_d(C)}} t^d \, \frac{q^{\ell(\mathcal{D})} - 1}{q - 1} \, . \qquad \text{--- } (\alpha)$$

- We know that for $0 \leq D \in \mathcal{D}$:
$\ell(D) - d(D) \leq \ell(0) - d(0) = 1 \Rightarrow \ell(\mathcal{D}) \leq (d+1)$

$$\Rightarrow \quad Z(t) \leq \sum_{d \geq 0} h(C) \cdot (qt)^d \cdot (d+1)$$

<u>Proposition</u>: (i) $Z(t)$ converges for $t \in \mathbb{C}$, if $|t| < q^{-1}$.

(ii) $Z(q^{-s})$ converges for $s \in \mathbb{C}$, if $\mathrm{Re}(s) > 1$.

[<u>Exercise</u>: Prove this.]

$\Rightarrow$ We can view power-series $Z(t)$ also a complex fn. $Z : \mathrm{dom} \longrightarrow \mathbb{C}$ (& has a continuation).

<u>Qn</u>! What's its <u>analytic</u> continuation?

- **Defn:** • We denote $Z(q^{-s})$ by $\underline{\zeta(s,C)}$.
  • **Norm of a divisor** D is

$$\underline{N(D)} := q^{d(D)} \in \mathbb{N}.$$

- **Proposition:** $\zeta(s,C) = \sum_{D \geq 0} N(D)^{-s} = \prod_{P \in C} \left(1 - N(P)^{-s}\right)^{-1}$

& they all converge, if $Re(s) > 1$.

- Ordinary Riemann Zeta fn. is $\zeta(s) := \sum_{n \geq 1} n^{-s}$.

$$= \prod_{\text{prime } p > 1} (1 - p^{-s})^{-1}, \text{ if } Re(s) > 1, s \in \mathbb{C}.$$

The Functional Equation

- We now show that $Z(t)$ is a rational fn.! Further, it has symmetry around $s = \frac{1}{2}$!

Theorem: (i) $Z(t) \in \mathbb{Q}(t)$ [has analytic continuation!]

(ii) $Z(t) = (qt^2)^{g-1} \cdot Z(1/qt)$.

Pf: • By eqn.(α) before, $(q-1) \cdot Z(t) = \sum_{d, \mathcal{D}} (q^{\ell(\mathcal{D})} - 1) \cdot t^d$

$$= \sum_{d, \mathcal{D}} q^{\ell(\mathcal{D})} \cdot t^d - \sum_{d, \mathcal{D}} t^d$$

- Break this further by using genus g, as:

$$\underline{F(t)} := \sum_{\substack{d \geq 2g-2+\delta;\\ \mathcal{D}}} q^{\ell(\mathcal{D})} \cdot t^{d} - \sum_{d,\mathcal{D}} t^{d} \quad , \text{ and}$$

$$\underline{G(t)} := \sum_{\substack{0 \leq d \leq 2g-2;\\ \mathcal{D}}} q^{\ell(\mathcal{D})} \cdot t^{d(\mathcal{D})}.$$

- Recall, for canonical class W, $\ell(W) = g$ & $d(W) = 2g-2$.

$\Rightarrow \quad 2g-2 \in \delta \mathbb{N}$.

- $d(\mathcal{D}) > 2g-2 \Rightarrow \ell(W-\mathcal{D}) = 0. \Rightarrow \ell(\mathcal{D}) = d(\mathcal{D}) + 1 - g.$

$\Rightarrow$ We can sum up $F(t)$ as:

$$F(t) = \sum_{2g-2+\delta \leq d \in \delta\mathbb{N}} h(C) \cdot q^{d+1-g} \cdot t^d \quad - \quad \frac{h(C)}{1-t^\delta}$$

$$= h(C) \cdot q^{1-g} \cdot \sum (qt)^d \quad - \quad \frac{h(C)}{1-t^\delta}$$

$$= h(C) \cdot q^{1-g} \cdot \frac{(q\underline{t})^{2g-2+\delta}}{1-(\underline{qt})^\delta} \quad - \quad \frac{h(C)}{1-t^\delta}$$

- $\Rightarrow$ F & G are in $\mathbb{Q}(t)$ $\Rightarrow$ $Z(t) \in \mathbb{Q}(t)$.

- Let's prove the symmetry under $1/qt$:

$$F((qt)^{-1}) = h(C)\cdot q^{1-g}\cdot \frac{(t^{-1})^{2g-2+\delta}}{1-t^{-\delta}} - \frac{h(C)}{1-(qt)^{-\delta}}$$

$$= (qt^2)^{1-g}\cdot \left\{ \frac{h(C)}{t^{\delta}-1} - \frac{h(C)\cdot(qt)^{\delta}}{(qt)^{\delta}-1}\cdot(qt^2)^{g-1} \right\}$$

$$= (qt^2)^{1-g}\cdot F(t).$$

- The other half is: $G((qt)^{-1}) = \sum_{d\le 2g-2} q^{\ell(D)}\cdot(qt)^{-d}$

$$= \sum_{d,D} q^{d+1-g+\ell(W-D)}\cdot(qt)^{-d} = (qt^2)^{1-g}\cdot\sum_{d,D} q^{\ell(W-D)}\cdot t^{d(W-D)}$$

- $W-D$ can be replaced with D as $d \in [0\ldots \underset{d(W)}{\overset{\shortparallel}{2g-2}}]$.

$$\Rightarrow \quad G((qt)^{-1}) = (qt^2)^{1-g} \cdot G(t).$$

$$\Rightarrow \quad Z((qt)^{-1}) = (qt^2)^{1-g} \cdot Z(t). \qquad \square$$

<u>Corollary 1</u>: $\zeta(1-s, C) = N(w)^{s-\frac{1}{2}} \cdot \zeta(s, C)$.

$\Rightarrow$ mysterious symmetry about the axis: $\mathrm{Re}(s) = \frac{1}{2}$.

<u>Corollary 2</u>: • The poles of $Z(t)$ are given by the roots of $(1-t^\delta)(1-q^\delta t^\delta)$; and are <u>simple</u>.

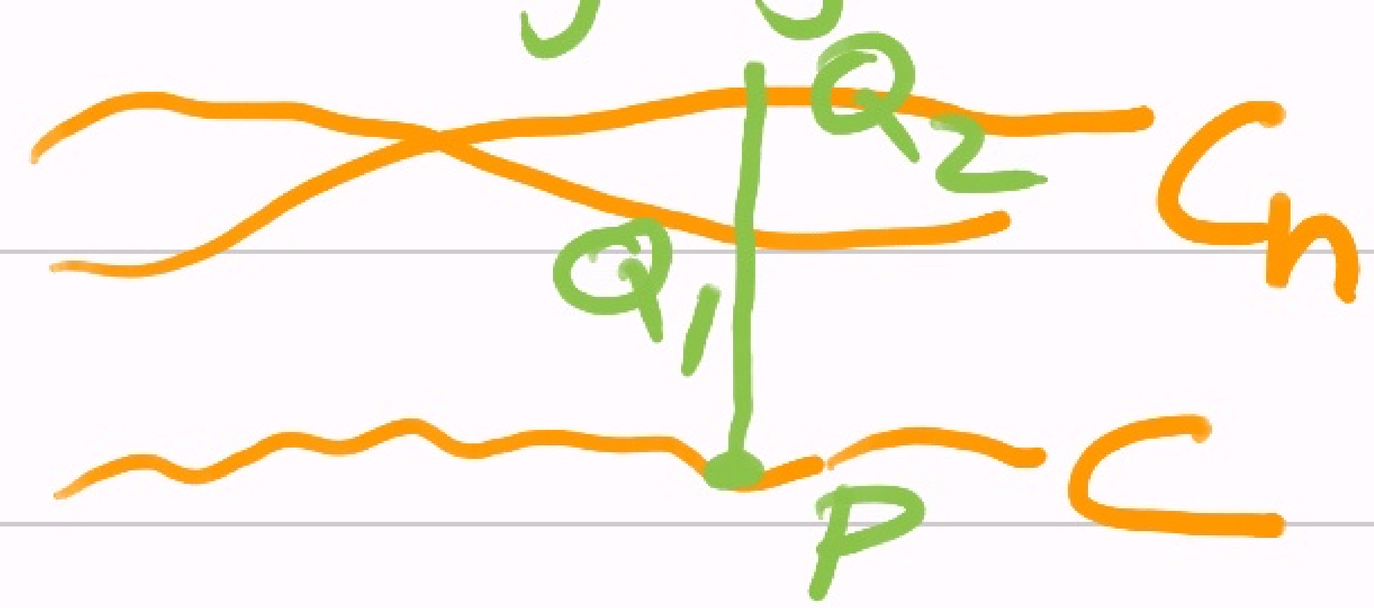
• The <u>residue</u> of $(q-1)Z(t)$ is $h(C)/\delta$, at $t=1$.

– **Qn:** How does $Z(t)$ change as k changes?

Theorem (Base change): Let C_n be the curve obtained from C by extending $k = \mathbb{F}_q$ to $k' =: \mathbb{F}_{q^n}$. Then,

$$Z(t^n, C_n) = \prod_{\eta^n = 1} Z(\eta t, C) .$$

Pf: • By Euler product, it suffices to compare the two sides for a pt. $P \in C$ (& its conjugates in C_n).



• Let's fix $P \in C$.

- Let $\mathfrak{m}_P \lhd R_P$ be the dvr data.
- $k_P := R_P / \mathfrak{m}_P$ is a finite extn. of $k = \mathbb{F}_q$.
- $\Rightarrow$ $k_P \cong k[T]/\langle f \rangle$, where $f(T)$ is an irreducible polynomial in $k[T]$.

- Over $k' = \mathbb{F}_{q^n}$, $f(T)$ splits into e irreducible factors, say $f(T) = f_1 \cdots f_e$.

  ▷ f_i's are coprime over k'; equi-degree & $e = \gcd(n, d(P))$.

[Eg. $x^6 - \alpha$ over $\mathbb{F}_q$ splits over $\mathbb{F}_{q^2}$ into $(x^3 \pm \sqrt{\alpha})$.]

$\Rightarrow$ pt. P gives e pts. $Q_1, \ldots, Q_e \in C_n$ s.t.

$$d(P) = \sum d(Q_i) = e \cdot d(Q_1).$$

- Thus, the contribution in $Z(t^n, c_n)$ corresponding to P is : $\prod_{1\le i\le e} (1 - t^{n\cdot d(P)/e})^{-1}$.

Claim: $(1 - t^{n\cdot d(P)/e})^e = \prod_{\eta^n=1} (1 - (\eta t)^{d(P)})$.

Pf:
- Let $n' := n/e$, $d' := d(P)/e$. [$(n', d') = 1$.]
- RHS (in Clm.) $= \prod_\eta (1 - \eta^{ed'} \cdot t^{d(P)})$

So, as η runs over $1^{1/n}$, η^e runs over $1^{1/n'}$ with e repetitions. $\Rightarrow$ $\eta^{ed'}$ runs over $1^{1/n'}$ with e repetitions.

$$\Rightarrow \text{RHS} = \Big(\prod_{\eta' \text{ is in } 1^{1/n'}} (1-\eta' t^{d(P)})\Big)^e = (1-t^{n'\cdot d(P)})^e$$

$$= (1-t^{n\cdot d(P)/e})^e = \text{LHS}. \qquad \square$$

- Going back to $Z(\cdot)$: the contribution of P in $Z(t^n, c^n)$ is $= \prod_{\eta} (1-(\eta t)^{d(P)})^{-1}$.

$$\Rightarrow Z(t^n, c^n) = \prod_{\eta} Z(\eta t, c). \qquad \square$$

Corollary (Two poles): $S = 1$.

Pf:

- The fn. eqn. calculation gives us:

$$Z(t,c) = \frac{L(t)}{(1-t^\delta)\cdot(1-(qt)^\delta)}$$

where $L(t) \in \mathbb{Z}[t]$.

- Let's "change base" to $n := \delta$.

$$\Rightarrow \quad Z(t^\delta, c_\delta) = \prod_{\eta^\delta=1} Z(\eta t, c) = \prod_{\eta^\delta=1} \frac{L(\eta t)}{(1-t^\delta)(1-(qt)^\delta)}$$

$$= \frac{L(t^\delta)}{(1-t^\delta)^\delta\cdot(1-(qt)^\delta)^\delta}.$$

- On the other hand, $Z(t, C_\delta) =: \dfrac{L'(t)}{(1-t^{\delta'})\cdot(1-(qt)^{\delta'})}$

$\Rightarrow Z(t^\delta, C_\delta) = \dfrac{L'(t^\delta)}{(1-t^{\delta\delta'})\cdot(1-q^{\delta'}\cdot t^{\delta\delta'})}$.

which has only simple poles.

$\Rightarrow$ The two expressions imply $\delta = 1$. $\square$

- Note that $L(0) = Z(0) = 1$.
- Also, $(q-1)\cdot Z(t)\cdot(t-1)\,\big|_{t=1} = h(C)$ [as $\delta=1$].

$\Rightarrow (q-1)\cdot \dfrac{L(t)}{qt-1}\Big|_{t=1} = h(C) \Rightarrow L(1) = h(C)$.

Theorem (L-fn.): (i) We've an exact sequence
$$0 \longrightarrow Cl_0(C) \xrightarrow{\subseteq} Cl(C) \xrightarrow{d(\cdot)} \mathbb{Z} \longrightarrow 0.$$
(ii) $Z(t,C) = L(t)/(1-t)(1-qt)$

where $L(t) \in \mathbb{Z}[t]$ has $\deg = 2g$ &
$$L(t) = (qt^2)^g \cdot L(1/qt).$$
(iii) $L(0) = 1$ & $L(1) = h(C)$.

Qn: • Can we compute $D \in d^{-1}(1)$?
• Can we compute $L(t)$ efficiently, given C/k?

Consequences to counting pts.

- Euler product: $Z = Z(t,C) = \prod_{P \in C} (1 - t^{d(P)})^{-1}$.

- Idea: Use dlog (log-derivative operator). $\left[d\log f = \frac{f'}{f} \right]$

$$\Rightarrow \quad d\log Z = \sum_{P \in C} d\log (1 - t^{d(P)})^{-1}$$

$$= \sum_{P \in C} \frac{d(P) \cdot t^{d(P)-1}}{(1 - t^{d(P)})} = t^{-1} \cdot \sum_{P \in C} d(P) \cdot \sum_{n \geq 1} t^{n \cdot d(P)}$$

$$= t^{-1} \cdot \sum_{m \geq 1} t^m \cdot \sum_{P \in C : d(P) | m} d(P) = t^{-1} \cdot \sum_{m \geq 1} N_m \cdot t^m$$

$N_m = \# C(\mathbb{F}_{q^m})$

$\Rightarrow$ Definite integration $\int_0^t$ gives:

<u>Proposition:</u> • $\log Z(t) = \left(\sum_{m \geq 1} N_m \cdot \frac{t^m}{m} \right)$.

• $Z(t) = \exp\left(\sum_{m \geq 1} N_m \cdot \frac{t^m}{m} \right)$.

- Now, use $Z(t) = \dfrac{L(t)}{(1-t)(1-qt)} =: \dfrac{\prod_{i=1}^{2g} (1 - \overset{\in \mathbb{C}}{\alpha_i} t)}{(1-t)(1-qt)}$

[$\because$ $L(0) = 1$, roots of L are <u>units</u>.]

• Plugging in the first formula above, we get:

$$\Rightarrow \sum_{i=1}^{2g} \log(1-\alpha_i t) - \log(1-t) - \log(1-qt) = \sum_{m\geq 1} N_m \cdot \frac{t^m}{m}.$$

$$\Rightarrow \forall m \geq 1, \quad N_m = q^m + 1 - \sum_{i=1}^{2g} \alpha_i^m \;\; = |\mathbb{P}_1(\mathbb{F}_{q^m})| + \text{error}$$

▷ $\sum_{i=1}^{2g} \alpha_i^m$ is viewed as the <u>error-term</u>.

<u>Qn.</u> How big can the error be?

— By fn. symmetry we get: $(1-\alpha_i t) \mapsto 1-(\alpha_i/qt) \swarrow (1-\alpha_j t)$

▷ We can label α_i's s.t. $\alpha_i \cdot \alpha_{i+g} = q$, $\forall i \in [g]$.

The Riemann Hypothesis (RH)

- RH conjectures a strong symmetry, namely $|\alpha_i|$ are equal, $\forall i \in [2g]$.
  $\Rightarrow |\alpha_i| = \sqrt{q} = q^{1/2}$

- In terms of $\zeta(s, C) = Z(q^{-s}, C)$, it means that the zeros of ζ are on the line $Re(s) = 1/2$ [just like the original unproved RH!]

▷ It means: $|N_n - (q^n+1)| = |\sum_{i\in[2g]} \alpha_i^n| \leq 2g \cdot q^{n/2}$.

▷ RH ⟹ # $\mathbb{F}_q$-pts. on a curve (smooth projective) are in the range $q+1 \pm 2g.\sqrt{q}$.

- We'll prove RH by doing a sequence of reductions, and finally using the $L(D)$-sheaf.

<u>Proposition</u> (base-change): RH is true for $Z(t,C)$ iff RH is true for $Z(t,C_n)$, for $n>1$.

<u>Pf</u>: • We know $Z(t,C) \mid Z(t^n, C_n) = \prod_{\eta^n=1} Z(\eta t, C)$.

• We've: $(1-\beta t) \mid Z(t, C_n) \iff (1-\beta^{1/n} t)$ is a factor of $Z(t^n, C_n)$.

- Thus, RH for $C_n \Rightarrow |\beta| = q^{n/2}$
  $\Rightarrow |\beta^{1/n}| = \sqrt{q}$
  $\Rightarrow$ All roots of $Z(t,C)$ satisfy $|\alpha| = \sqrt{q}$
  $\Rightarrow$ RH for C.
- Conversely, assume RH for $Z(t,C)$.
- As, $(1-\alpha t) \mid Z(t,c) \Rightarrow (1-\alpha\eta t) \mid Z(\eta t, c)$
- We deduce, $\prod_\eta (1-\alpha\eta t) \mid Z(t^n, C_n)$ are the only factors.
  $\Rightarrow (1-\alpha^n t^n) \mid Z(t^n, C_n) \Rightarrow (1-\alpha^n t) \mid Z(t, C_n)$
  $\Rightarrow |\alpha^n| = q^{n/2} \Rightarrow$ RH for C_n.

$\square$

- **Proposition:** TFAE:

(i) RH for $Z(t, C)$. [i.e. $|\alpha| = q^{1/2}$.]

(ii) $|N_d - (q^d+1)| \leq A + B \cdot q^{d/2}$, for some constants $A, B, N \in \mathbb{N}$ & all multiples d of N.

(independent of d)

Proof: • (i) $\Rightarrow$ (ii): We've proved already ($\forall d$).

• (ii) $\Rightarrow$ (i): • Replace the base field $\mathbb{F}_q$ by $\mathbb{F}_{q^N}$. & rename $\mathbb{F}_{q'}$.

$\Rightarrow \mathbb{F}_{q'} \subseteq \mathbb{F}_{q'^d}$, as we vary d.

• Hypothesis-(ii) $\Rightarrow \left| \sum_{i \in [2g]} \alpha_i^d \right| \leq A + B q^{d/2}$, $\forall d \equiv_N 0$.

• We've $\prod_{i=1}^{2g} \alpha_i = \prod_{i=1}^{g} (\alpha_i \cdot \alpha_{i+g}) = q^g$ (by symmetry)

$\Rightarrow$ It suffices to show: $\forall i$, $|\alpha_i'| \leq \sqrt{q}$, where

- Recall $L(t) =: \prod_{i \in [2g]} (1 - \alpha_i' t)$

α_i''s come from $L(t, C_N) =: L(t)$

$\triangleright$ $\alpha_i' = \alpha_i^N$.

$$\Rightarrow \log 1/L(t) = \sum_{d \geq 1} \Big(\sum_{i \in [2g]} \alpha_i'^{\,d} \Big) \cdot \frac{t^d}{d}$$

$$\Rightarrow \left| \log 1/L(t) \right| \leq \sum_{d \geq 1} \left(A + B \cdot q'^{\,d/2} \right) \cdot \frac{|t|^d}{d}$$

$$\leq A \cdot \log 1/(1 - |t|) + B \cdot \log 1/(1 - |t\sqrt{q'}|) .$$

$\Rightarrow$ LHS converges, for $t \in \mathbb{C}$, if $|t| < 1/\sqrt{q'}$.

$\Rightarrow$ Zeros of $L(t)$ are $\geq 1/\sqrt{q'}$, in norm.

$\Rightarrow \quad |\alpha_i'^{-1}| \geq 1/\sqrt{q'} \quad \Rightarrow \quad |\alpha_i'| \leq \sqrt{q'}$.

$\Rightarrow \ \forall i \in [2g], \quad |\alpha_i'| = \sqrt{q'}$.

$\Rightarrow$ RH for $Z(t, C_N)$ holds.

$\Rightarrow$ " " $Z(t, C)$ holds. $\square$

- Next reduction that we need is to make the cover $C \longrightarrow \mathbb{P}^1$; $k(x_1)[x_2]/\langle F \rangle \supseteq k(x_1)$ Galois ;

$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \|$

i.e. we want $k(C)$ to have all roots of F wrt x_2 (think of x_1 fixed in $\overline{k}$).

Move to the Galois cover of C

- Eg. Let C (in affine patch $x_0=1$) be
$$x_2^3 - x_2 - x_1^2 = 0 \quad \text{over } k = \mathbb{F}_q.$$

$$\Rightarrow k(C) =: K = k(x_1)[x_2] / \langle \underbrace{x_2^3 - x_2 - x_1^2}_{=: F(x_1, x_2)} \rangle$$
is a deg $=3$ extn. of $k(x_1) = k(\mathbb{P}^1)$
which may not be a splitting field, over $k(x_1)$.

- We correct this by moving to the splitting field K' of $x_2^3 - x_2 - x_1^2$ over $k(x_1)$.

▷ $[K' : k(x_1)] = 3 \times 2 = 6.$

– $\underbrace{K' \supset K}_{2} \underbrace{\supset k(x_1)}_{\deg = 3} \supset k = \mathbb{F}_q$

▷ K'/K & $K'/k(x_1)$ are <u>Galois</u> extensions.
(i.e. they're <u>separable</u> & <u>normal</u>.)

– Let <u>C'</u> be the curve defined by K' (as it's a trdeg $= 1$ field over k).

▷ $C' \longrightarrow C \longrightarrow \mathbb{P}^1$ is called the <u>Galois cover</u> of C.

$$\begin{tikzcd}
P_0, P_1, P_2, \dots \in C' \arrow[d] & k(x_1)[x_2, y_2]/\langle - \rangle \\
P_0 \in C \arrow[d] & k(x_1)[x_2]/\langle - \rangle \arrow[u, "\subseteq"'] \\
\mathbb{P}^1 & k(x_1) \arrow[u, "\subseteq"']
\end{tikzcd}$$

$\rightsquigarrow$ eg. $\langle x_2^3 - x_2 - x_1 \rangle$

$\rightsquigarrow \left\langle x_2^3 - x_2 - x_1, \ \dfrac{y_2^3 - y_2 - x_1}{y_2 - x_2} \right\rangle$

$\Rightarrow$ $P_0 := (x_1, x_2)$, $P_1 := (x_1, y_2)$ & $P_2 := (x_1, -x_2 - y_2)$ are the <u>three</u> roots for x_2, given x_1.

▷ Let F be the Frob_q & σ be the Galois automorphism of $k(C')$ over $k(C)$.

$\Rightarrow$ $P_0^\sigma = P_0$, $P_1^\sigma = P_2$, $P_2^\sigma = P_1$.

eg. Fix (x_1, x_2) in $\mathbb{F}_q^2$ s.t. $x_2^3 - x_2 - x_1$ has only <u>one</u> root in $\mathbb{F}_q^2$. The other two roots are in $\mathbb{F}_q \times \mathbb{F}_{q^2}$.

$\Rightarrow$ $F(P_0) = P_0$, $F(P_1) = P_2$, $F(P_2) = P_1$.

$\Rightarrow$ P_1, P_2 are conjugates over $\mathbb{F}_{q^2}$, via F.

$\triangleright$ $P_1 = P_2$ for some $x_1 \in \mathbb{F}_q$ $\Longleftrightarrow$ x_1 is a zero of $\mathrm{Res}_{x_2}(f(x_1, x_2), \partial_{x_2} f)$.

$\Rightarrow$ Thus, $P_1 = P_2$ happens for $\leq (\deg f)^2$ many x_1's.

- <u>Defn</u>: Let $G(K(C')/K(C))$ be the group of $K(C)$-automorphisms of $K' := K(C')$.

<u>Proposition</u>: Let C be a smooth projective curve over k & let C' be a Galois cover.

$$\Rightarrow \quad |G(k(C')/k(C))| = [k(C'):k(C)].$$

<u>Pf</u>: • $k(C')/k(C)$ is a finite Galois extension.

• $\exists\, \alpha$, $k(C') = k(C)(\alpha)$. [Primitive element]

$\Rightarrow$ $\deg(\text{minpoly}_\alpha) = [k(C'):k(C)]$.

& $k(C')$ is the splitting-field of minpoly_α, & so it has all its conjugates.

$$\Rightarrow \quad G(k(C')/k(C)) = \#\text{conjugates}$$

$$= [k(C'):k(C)].$$

$\square$

▷ $\forall\, \sigma \in G(k(C')/k(C))$, σ can be seen to act on pts. $P' \in C'$ via its action on $k(C')$.

Pf: – Say, pt. $P' = (x_1, x_2)$

– $\sigma(x_1)$ & $\sigma(x_2)$ can be seen as fns. in $k(C')$. Use them to define $\sigma(P')$.

– Qn: What about poles of $\sigma(x_2)$? □

▷ q-th Frobenius $F : k(C') \to k(C')$; $f(x_1, x_2) \mapsto f(x_1^q, x_2^q)$

$C' \to C'$; $(\alpha, \beta) \mapsto (\alpha^{q^{-1}}, \beta^{q^{-1}})$.

▷ F is injective. (k-monomorphism)

- Eg. $F: \overbrace{(x_1-\alpha)}^{=:f} \mapsto (x_1^q-\alpha) = (x_1-\alpha^{q^{-1}})^q$, $\alpha \in \overline{\mathbb{F}_q}$.

So, $\mathrm{ord}_{F\alpha} F(x_1-\alpha) = q \cdot \mathrm{ord}_\alpha(x_1-\alpha)$.

" $\mathrm{ord}_{\alpha^{q^{-1}}}(x_1^q-\alpha) = \mathrm{ord}_{\alpha^{q^{-1}}}(x_1-\alpha^{q^{-1}})^q = q \cdot \mathrm{ord}_\alpha(f)$.

▷ The k-pts. on C are exactly $\{P \in C \mid F(P) = P\}$, i.e. the fixed-pts. of F.

- Let's relate the k-pts. of C with those of C'.

- Defn: For $\sigma \in G = G(k(C')/k(C))$, define
$\underline{N_1(C', \sigma)} := \{P \in C' \mid \sigma^{-1} \circ F(P) = P\}$.

- Eg. $N_1(C) = N_1(C, 1)$.

Proposition (Avg. over G): $N_1(C) = |G|^{-1} \cdot \sum_{\sigma \in G} N_1(C', \sigma) + O_\delta(1)$, where $\delta :=$ deg of f defining C.

Pf: • Let $\varphi : C' \to C$ be the Galois cover.

• For $P \in C$, let the distinct pts. in C', above P, be $\varphi^{-1}(P) := \{Q_1, Q_2, \to Q_r\}$.

▷ $F(Q_i) \in \varphi^{-1}(P)$.

▷ $1 \leq r \leq |G|$.

Qn: Why's $r < |G|$? • It happens only when P has repeated conjugates, i.e. P ramifies in C'.

▷ Ramified pts. $P \in C$ are $\leq \delta^2 \leq O_\delta(1)$.

- For unramified k-point $P \in C$,

$$r = |\varphi^{-1}(P)| = \#\{Q \in C' \cap \varphi^{-1}(P) \mid \exists \sigma \in G,\ \sigma^{-1} \circ F(Q) = Q\}$$
$$= |G|.$$

$\triangleright$ If $Q' \in C'$ satisfies $\sigma^{-1} \circ F(Q') = Q'$, for some σ, then $\varphi(Q') \in C$ is a k-pt.

- Thus, any $Q' \in C'$ contributing to $\sum_{\sigma \in G} N_1(C', \sigma)$ <u>either</u> has $\varphi(Q') \in C$ ramified, <u>or</u> " " unramified.

$$\Rightarrow \sum_{\sigma \in G} N_1(C', \sigma) = |G| \cdot N_1(C) + |G| \cdot O_g(1) \qquad \square$$

- This averaging over G, allows us to connect $N_1(C)$ to $N_1(\mathbb{P}^1)$ tightly.
- We first prove RH for Galois extn.

$$\text{Galois}\left\{\begin{array}{l} \left.\begin{array}{c} C' \\ \downarrow \\ C \end{array}\right\}\text{Galois} \\ \;\;\downarrow \\ \;\mathbb{P}^1 \end{array}\right.$$

<u>Theorem</u> (RH) (Weil 1930s, Bombieri-Stepanov 1960s): Let $C \to \mathbb{P}^1$ be a Galois cover over $\mathbb{F}_q =: k$. Assume $q =: p^\alpha$ with even α & $q > (g+1)^4$, where $g =$ genus of C/k. Then, $\forall \sigma \in Aut(C/\mathbb{P}^1)$,

$$N_1(C,\sigma) \leq q+1+(2g+1)\sqrt{q}.$$

(Think of $C/\mathbb{F}_q$ as defined $\mathbb{F}_p \subseteq \mathbb{F}_{q'} \subseteq \mathbb{F}_q$, & then go to $\mathbb{F}_q$ large enough.)

- Let's see why it implies RH:

- Let C_0/k be a curve with fn. field $K_0 = k(C_0)$. Let $K := K_0 \cdot \bar{k}$ be the fn. field over $\overline{\mathbb{F}_q} = \overline{\mathbb{F}_p}$.
- Let C be the curve corresponding to fn. field K.
- Let $K' \supseteq K$ be the <u>smallest</u> Galois extn. defining the Galois cover $C' \to C$.
- Let $H := G(K'/K)$. By the avg. proposition:

$$N_1(C) = |H|^{-1} \cdot \sum_{h \in H} N_1(C', h) + O_g(1). \quad ---(i)$$

$$G\left\{\begin{array}{c} \left.\begin{array}{c} C' \\ \downarrow \\ C \end{array}\right\} H \\ \downarrow \\ \mathbb{P}^1 \end{array}\right.$$

- Let $G := G(K'/\bar{k}(x)) \geq H$. By the avg. proposition:

$$q+1 = N_1(\mathbb{P}^1) = |G|^{-1} \cdot \sum_{\sigma\in G} N_1(C',\sigma) + O_\delta(1)^{\leq O(\delta^2)}.$$

$\Rightarrow$ (By the Thm.) $\forall \sigma \in G$, $N_1(C',\sigma) = q+1+O(\underbrace{\delta^2+g\sqrt{q}}_{\text{(by Thm.)}})$.

(by (i)) $\underset{N_1(C_0)=}{\Rightarrow}$ $N_1(C) = q+1+O(\delta^2+g\sqrt{q})$.

$\Rightarrow$ RH for C_0 (over all fields). $\square$

- Let's now prove the RH-Theorem.

<u>Idea:</u> · Use $L(aP)$-sheaf & the actions of $\sigma \in G(C/\mathbb{P}^1)$, q-th-Frob F & p-th-Frob F_{abs} on it.

Proof: • In the pf we work with $k := \overline{\mathbb{F}_q}$ & the corresponding fn. field K.

• If $N_1(C,\sigma) = 0$ then we're done! Else, pick a pt. $P \in C$ s.t. $\sigma^{-1} \circ F(P) = P$. It's degree $d(P) = 1$.

• Pick $a \in \mathbb{N}$ "large" enough $(a > 2g-2)$ and define $\underline{L_a} := L(aP)$, $\underline{l_a} := \ell(aP)$.

[Riemann-Roch] $\Rightarrow$ $l_a = a + 1 - g$.

• Define $\varphi := \sigma^{-1} \circ F : C \to C$. $L_a^{\varphi} \leftarrow L_a : \varphi$

• Define its pull-back as $\underline{L_a^{\varphi}} := \{ f \circ \varphi \mid f \in L_a \}$

▷ For $Q \in C$ & $f \in L_a$, $(f \circ \varphi) = q \cdot \varphi^{-1}((f))$.

• $\mathrm{ord}_Q(f \circ \varphi) = \mathrm{ord}_Q(f'^q) = q \cdot \mathrm{ord}_Q(f') = q \cdot \mathrm{ord}_{\varphi(Q)}(f)$.

$\Rightarrow$ We get a sequence of tr. maps:

$$\begin{array}{ccccc} L_a & \xrightarrow[\sim]{\varphi} & L_a^{\varphi} & \hookrightarrow & L_{aq} \\ f & \longmapsto & f\circ\varphi & \longmapsto & g_1 \end{array} \quad \text{---(i)}$$

$(f)+aP \geq 0$ $\qquad$ $(f\circ\varphi)+qaP \geq 0$

$\qquad\qquad$ & $\varphi(P)=P$.

- Let's repeat this with F_{abs}^{μ} (for $\mu \geq 1$), for a "large" enough $b \in \mathbb{N}$:

$$L_b^{p,\mu} := \{ f\circ F_{abs}^{\mu} \mid f \in L_b \}.$$

$$\begin{array}{ccccc} L_b & \xrightarrow[\sim]{F_{abs}^{\mu}} & L_b^{p,\mu} & \hookrightarrow & L_{bp^{\mu}} \\ f & \longmapsto & f\circ F_{abs}^{\mu} & \longmapsto & g_2 \end{array} \quad \text{---(ii)}$$

- Now, we take the <u>tensor product</u> of the two sequences:

<u>Claim 1</u> (Mult. map): If $bp^\mu < q$ then the multiplication map $L_b^{p,\mu} \otimes_k L_a^p \xrightarrow{\sim} L_b^{p,\mu} \cdot L_a^p \hookrightarrow L_{bp^\mu + aq}$

$g_2 \otimes g_1 \longmapsto g_2 \cdot g_1 \longmapsto g_3$

gives an <u>injection</u>.

Pf: • L_a has a tower of k-subspaces:

$$k = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_{a-1} \subseteq L_a.$$

$$\Rightarrow \quad L_a \cong \bigoplus_{0 \le i \le a} L_i / L_{i-1}.$$

& $\dim L_i / L_{i-1} \le d(P) = 1.$

$\Rightarrow \exists$ k-basis $\{f_1, f_2, \to f_r\}$, $r \leq a$, of L_a s.t. $\forall i$, $v_p(f_i) < v_p(f_{i+1})$.

[eg. $L_i / L_{i-1} = L(iP)/L((i-1)P) \ni g_1$ $\Rightarrow v_p(g_1) <$
$L_{i+1}/L_i = L((i+1)P)/L(iP) \ni g_2$ $v_p(g_2)$.]

- Now, write any element G in $L_b^{p,\mu} \cdot L_a^{\varphi}$ as:
$$G =: \sum_{i \in [r]} (s_i \circ F_{abs}^{p,\mu}) \cdot (f_i \circ \varphi), \quad s_i \in L_b.$$

- **Qn:** When is $G = 0$?
  - Let s_h is the first $s_i \neq 0$.
  - Apply v_p on the equation:

$$-(g_h \circ F_{abs}^{p,\mu}) \cdot (f_h \circ \varphi) = \sum_{h<i\leq n} (g_i \circ F_{abs}^{p,\mu}) \cdot (f_i \circ \varphi).$$

$$\Rightarrow \quad p^{\mu} \cdot v_p(g_h) + q \cdot v_p(f_h) \geq \min_{i>h} \left(p^{\mu} \cdot v_p(g_i) + q \cdot v_p(f_i) \right)$$

$$\geq p^{\mu} \cdot (-b) + q \cdot v_p(f_i) \quad , \forall i>h.$$

$$\Rightarrow \quad p^{\mu} \cdot v_p(g_h) \geq -p^{\mu} b + q \cdot (v_p(f_i) - v_p(f_h))$$

$$\geq q - p^{\mu} b > 0.$$

$\Rightarrow \quad g_h|_p = 0 \quad \Rightarrow g_h = 0. \quad \Rightarrow$ a contradiction!

$\Rightarrow \quad G \neq 0 \quad \Rightarrow$ it's an injection. $\square$

— Claim 1, now, gives us a k-lin. map τ s.t.

$$
\begin{tikzcd}
L_{bp^\mu+aq} & L_b^{p,\mu}\cdot L_a^{p} \arrow[l, hook'] \arrow[r, "\tau"] & L_b^{p,\mu}\cdot L_a \arrow[r, hook] & L_{bp^\mu+a} \\
& L_b^{p,\mu}\otimes_k L_a^{p} \arrow[u, "\wr", "\text{(Claim 1)}"'] & L_b^{p,\mu}\otimes_k L_a \arrow[l] \arrow[u, "\text{(mult.)}"'] &
\end{tikzcd}
$$

is a commutative diagram.

▷ τ (or mult.) map may not be injective.

(as, "$-bp^\mu+q>0$" is unavailable in the pf. of Clm.1); So, we use $\ker(\tau)$ as:

▷ $bp^\mu<q$ & $l_b\cdot l_a>l_{bp^\mu+a} \Rightarrow \exists\, G\neq 0,\ \tau(G)=0.$

- Let $G =: \sum_{i \in [t]} (s_i \circ F_{abs}^{p,\mu}) \cdot (f_i \circ \varphi) \neq 0$ s.t.

$$\tau(G) = \sum_i (s_i \circ F_{abs}^{p,\mu}) \cdot f_i = 0.$$

▷ G is a p^μ-th power. ($\because q > p^\mu$)

▷ $\forall P \neq Q \in C$ s.t. $\varphi(Q) = Q$, $G|_Q = \tau(G)|_Q = 0$.

($\because f_i \circ \varphi(Q) = f_i(Q)$)

(& $\tau(G)$ is zero polynomial)

- Thus, we can count Q's as:

▷ $p^\mu \cdot (N_1(C,\sigma) - 1) \leq d((G)_0) = d((G)_\infty)$

$\leq bp^\mu + aq.$

$\Rightarrow N_1(C,\sigma) \leq 1 + b + aqp^{-\mu}.$

– We can fix a, b, μ by parameter chasing.
(Take $a, b \geq 2g$, to allow Riemann–Roch.)

Claim 2: Take $\mu := \alpha/2$ ($p^\mu := \sqrt{q}$), $a := \sqrt{q} + 2g$
& $b := g + 1 + \lfloor g\sqrt{q}/(g+1) \rfloor$. Then,

(i) $bp^\mu < q$,

(ii) $l_b l_a > l_{bp^\mu + a}$, and

(iii) $b + 1 + aqp^{-\mu} < q + 1 + (2g+1)\sqrt{q}$.

Pf: (i) $b = \left(g + 1 + \lfloor g\sqrt{q}/(g+1) \rfloor + \sqrt{q}/(g+1)\right) - \sqrt{q}/(g+1)$

$\leq \left(g + 1 + \sqrt{q}\right) - \sqrt{q}/(g+1) < \sqrt{q}$ [$\because \sqrt{q} > (g+1)^2$]

$\Rightarrow bp^\mu < \sqrt{q} \cdot \sqrt{q} = q$.

(ii) $\ell_b \ell_a \overset{\text{RR-thm}}{=} (b+1-g)(a+1-g) > (bp^{\mu} + a+1-g)$

iff $(b-g)(a+1-g) > bp^{\mu}$

iff $b(a+1-g-p^{\mu}) > g(a+1-g)$

iff $b(1+g) > g(1+g+\sqrt{q})$ [$\because a = \sqrt{q}+2g$]

iff $b > g + \dfrac{g\cdot\sqrt{q}}{g+1}$; which holds!

(iii) $b + a\sqrt{q} + 1 = g+1+\lfloor g\sqrt{q}/(g+1)\rfloor + \sqrt{q}(2g+\sqrt{q}) + 1$

$\leq g+1+\dfrac{g\sqrt{q}}{g+1} + 2g\sqrt{q} + \underbrace{q+1}$

$< q+1+(2g+1)\sqrt{q}$. [$\because \sqrt{q} > (g+1)^2$] $\square$

$\Rightarrow$ The RH for $N_1(C,\sigma)$. $\square$