Southwestern Center for Arithmetical Algebraic Geometry
1998 Arizona Winter School Workshop
13–18 March 1998 in Tucson, Arizona
Diophantine Geometry Related to the ABC Conjecture

STUDENT PRESENTATION

STUDENTS:	**FACULTY:**
Sang Yook An	Minhyong Kim
Seog Young Kim	Barry Mazur
David Marshall	William McCallum
Susan Marshall	Dinesh Thakur
Alexander Perlis	

Theorem:

Assuming the ABC, Szpiro, and B&SD conjectures, all semistable elliptic curves of fixed rank have

$$|\text{Ш}| \ll N^{3/4+\varepsilon}.$$

From:

Dorian Goldfeld and Lucien Szpiro, *Bounds for the order of the Tate–Shafarevich group*, Compositio Mathematica **97**, 1995, pp. 71–87.

ASSUMPTIONS

ABC Conjecture
For all $A, B, C \in \mathbf{Z}$ with $\mathrm{GCD}(A, B, C) = 1$ and $A + B = C$,

$$\mathrm{SUP}\left(|A|, |B|, |C|\right) \ll N_0(ABC)^{1+\varepsilon},$$

where N_0 is the conductor of the product ABC:

$$N_0(ABC) = \prod_{p|ABC} p.$$

Szpiro's Conjecture
For all elliptic curves $E/\mathbf{Q}$,

$$|\mathcal{D}| \ll N^{6+\varepsilon},$$

where $\mathcal{D}$ is the minimal discriminant of E, and N is the conductor of E.

Remark
The above conjectures are equivalent. We will make use of both formulations.

ASSUMPTIONS

Birch & Swinnerton-Dyer Conjecture

Let $L(s) \equiv L$-series of E, and $r \equiv \text{RANK}(E)$. Then

$$\operatorname*{ORD}_{s=1} L(s) = r,$$

and

$$\left.\frac{L(s)}{(s-1)^r}\right|_{s=1} = \frac{2^r \cdot |\text{Ш}| \cdot \Omega \cdot R \cdot \prod_{p|N} c_p}{|E(\mathbf{Q})_{\text{TOR}}|^2},$$

where Ω is the real period, R is the regulator, and the c_p are the local periods (Tamagawa numbers).

THEOREM

Assuming the previous three conjectures, we have:

For all semistable elliptic curves *of fixed rank* r,

$$|Ш| \ll N^{3/4+\varepsilon}.$$

Precise statement:

For each rank r and each $\varepsilon > 0$, there exists a constant $C_{r,\varepsilon} > 0$ so that, for all semistable elliptic curves of rank r, we have

$$|Ш| < C_{r,\varepsilon} \cdot N^{3/4+\varepsilon}.$$

OVERVIEW OF PROOF

Rearranging B&SD gives:

$$|\text{Ш}| = \left.\frac{L(s)}{(s-1)^r}\right|_{s=1} \cdot \frac{|E(\mathbf{Q})_{\mathsf{TOR}}|^2}{2^r\,\Omega\,R\,\prod_{p|N} c_p} \ll N^{3/4+\varepsilon}$$

(rank fixed)

Thus, to bound $|\text{Ш}|$, we seek bounds for:

- $\left.\frac{L(s)}{(s-1)^r}\right|_{s=1} \ll N^{1/4+\varepsilon}$, to be shown

- $|E(\mathbf{Q})_{\mathsf{TOR}}|^2 \leq 144$, by Mazur's theorem

- $\frac{1}{\Omega} \ll N^{1/2+\varepsilon}$, to be shown

- $\frac{1}{R} \ll C_r$ (constant depending on r),
  to be shown

- $\frac{1}{\prod_{p|N} c_p} \leq 1$, since each $c_p = \left|\frac{E(\mathbf{Q}_p)}{E_0(\mathbf{Q}_p)}\right| \geq 1$

OVERVIEW OF PROOF

Rearranging B&SD gives:

$$|\text{Ш}| = \left.\frac{L(s)}{(s-1)^r}\right|_{s=1} \cdot \frac{|E(\mathbf{Q})_{\text{TOR}}|^2}{2^r\,\Omega\,R\,\prod_{p|N} c_p}$$

Thus, to bound $|\text{Ш}|$, we seek bounds for:

- $\left.\dfrac{L(s)}{(s-1)^r}\right|_{s=1}$
- $|E(\mathbf{Q})_{\text{TOR}}|^2$
- $\dfrac{1}{\Omega}$
- $\dfrac{1}{R}$
- $\dfrac{1}{\prod_{p|N} c_p}$

≤ 144, by Mazur's theorem

≤ 1, since each $c_p = \left| \frac{E(\mathbf{Q}_p)}{E_0(\mathbf{Q}_p)} \right| \geq 1$

$\ll N^{1/4+\varepsilon}$, to be shown

$\ll N^{1/2+\varepsilon}$, to be shown

$\ll C_r$ (constant depending on r),
to be shown

$\ll N^{3/4+\varepsilon}$

(rank fixed)

Establishing $\left.\frac{L(s)}{(s-1)^r}\right|_{s=1} \ll N^{1/4+\varepsilon}$

Recall, for $\Re(s) > 3/2$, and semistable E:

$$L(s) = \prod_{p|N} \frac{1}{1 \pm p^{-s}} \prod_{p\nmid N} \frac{1}{1 - a_p\, p^{-s} + p^{1-2s}},$$

where $a_p = (1+p) - \#E_p(\mathbf{F}_p)$.

To bound $\left.\frac{L(s)}{(s-1)^r}\right|_{s=1}$, we proceed indirectly. As usual, set

$$\Lambda(s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(s),$$

so that $\Lambda(2-s) = \pm\Lambda(s)$.

We have the bounds:

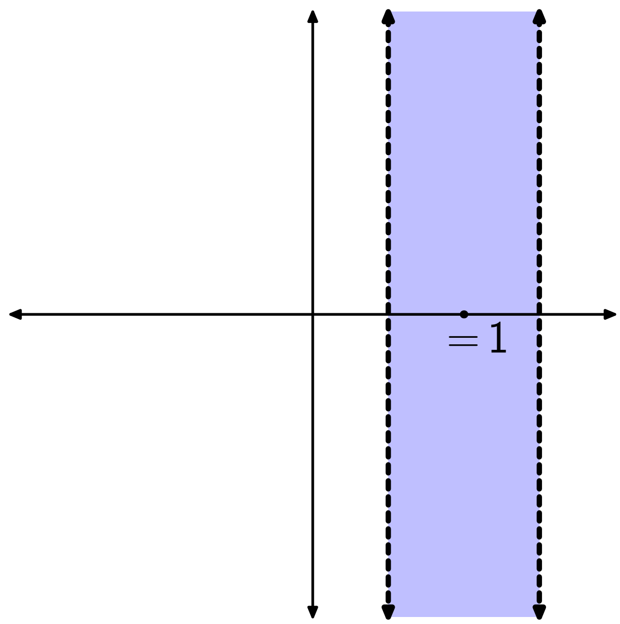
- $\left|\frac{\Lambda(s)}{(s-1)^r}\right| \ll N^{3/4+\varepsilon}$ for $\Re(s) = 3/2+\varepsilon$.

- $\left|\frac{\Lambda(s)}{(s-1)^r}\right| \ll N^{3/4+\varepsilon}$ for $\Re(s) = 1/2-\varepsilon$.

Establishing $\left.\frac{L(s)}{(s-1)^r}\right|_{s=1} \ll N^{1/4+\varepsilon}$

Now we will transfer these bounds to the strip

$$1/2-\varepsilon \le \Re(s) \le 3/2+\varepsilon.$$



By a generalized maximum modulus principle, it is sufficient to show, throughout the strip,

$$\left|\frac{\Lambda(s)}{(s-1)^r}\right| \text{ is bounded (by } \textit{something}\text{).}$$

Establishing $\left.\frac{L(s)}{(s-1)^r}\right|_{s=1} \ll N^{1/4+\varepsilon}$

Obtaining an arbitrary bound on $\left|\frac{\Lambda(s)}{(s-1)^r}\right|$:

- Some upper bound on $\Lambda(s)$:

  $$\Lambda(s) = N^{s/2}\underbrace{(2\pi)^{-s}\Gamma(s)L(s)}_{\substack{\text{Mellin transform of} \\ \text{the weight 2 cusp} \\ \text{form } \sum a_n q^n}} \quad \text{(semistable)}$$

- Some lower bound on $(s-1)^r$:
  B&SD implies that $\frac{\Lambda(s)}{(s-1)^r}$ does not blow up at $s = 1$.

Establishing $\left.\frac{L(s)}{(s-1)^r}\right|_{s=1} \ll N^{1/4+\varepsilon}$

Thus our bounds transfer to give

$$\left|\frac{\Lambda(s)}{(s-1)^r}\right| \ll N^{3/4} + \varepsilon$$

for $1/2 - \varepsilon \leq \Re(s) \leq 3/2 + \varepsilon$.

In particular, substituting $s = 1$ gives

$$N^{1/2}(2\pi)^{-1}\Gamma(1) \left.\frac{L(s)}{(s-1)^r}\right|_{s=1} \ll N^{3/4+\varepsilon},$$

so that

$$\left.\frac{L(s)}{(s-1)^r}\right|_{s=1} \ll N^{1/4+\varepsilon}.$$

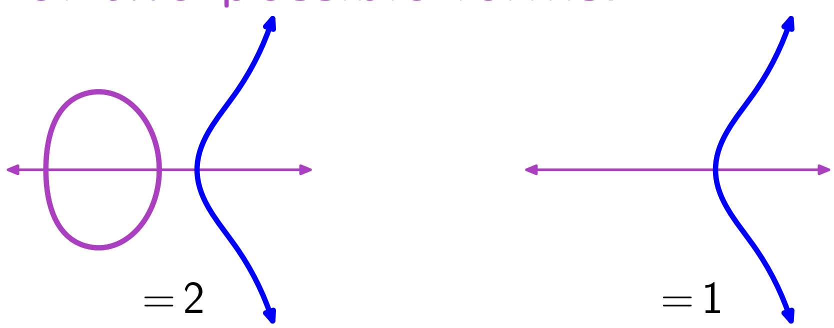
Establishing $\frac{1}{\Omega} \ll N^{1/2+\varepsilon}$

Recall that the real period is

$$\Omega = \int_{E(\mathbf{R})} |\omega| \, ,$$

where ω is the associated invariant differential.

Upon choosing a Weierstrass equation, $E(\mathbf{R})$ has one of two possible forms:



Let γ denote the infinite component, and let δ denote the number of components. The integral along either component is the same; thus

$$\Omega = \delta \int_{\gamma} |\omega| \, .$$

Establishing $\frac{1}{\Omega} \ll N^{1/2+\varepsilon}$

Starting with a global minimal equation

$$Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6,$$

we have $$\omega = \frac{\mathrm{d}X}{2Y + a_1 X + a_3}.$$

The usual transformations (see Tate's article or Silverman's book) give the convenient form:

$$\begin{aligned} y^2 &= x^3 - 27c_4 x - 54c_6 \\ \omega &= \frac{3\mathrm{d}x}{y}. \end{aligned}$$

Furthermore (we'll need this later):

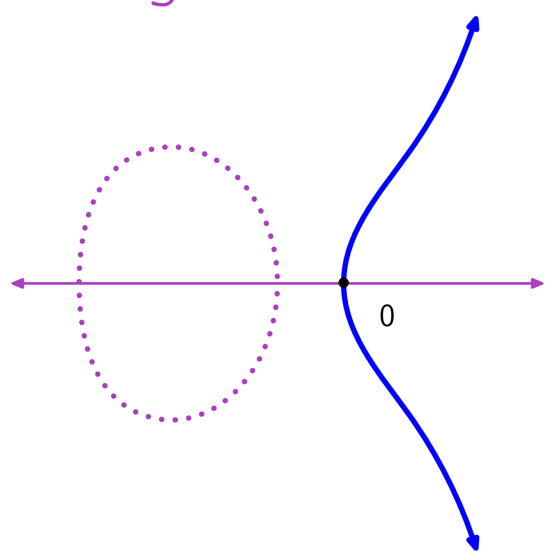
$$\begin{aligned} 1728\mathcal{D} &= {c_4}^3 - {c_6}^2, \\ \mathrm{GCD}(c_4, \mathcal{D}) &= 1. \qquad \leftarrow \text{semistable} \end{aligned}$$

Establishing $\frac{1}{\Omega} \ll N^{1/2+\varepsilon}$

Then $\Omega = \delta \int_\gamma |\omega|$ becomes

$$\Omega = \delta \int_\gamma \left| \frac{3\,\mathrm{d}x}{y} \right| = 2\delta \int_{r_0}^{\infty} \frac{3\,\mathrm{d}x}{\sqrt{x^3 - 27c_4x^2 - 54c_6}},$$

where r_0 is the largest real root of the cubic.



Knowing how to compute Ω, we now show how to bound $1/\Omega$:

$$\frac{1}{\Omega} \underset{\substack{\uparrow \\ \text{Calculus}}}{\ll} \mathrm{SUP}\left(|c_4|^{1/4}, |c_6|^{1/6}\right) \underset{\substack{\uparrow \\ \text{ABC}}}{\ll} N^{1/2+\varepsilon}.$$

Calculus: $\frac{1}{\Omega} \ll \text{SUP}\left(|c_4|^{1/4}, |c_6|^{1/6}\right)$

We must study

$$\Omega = 2\delta \int_{r_0}^{\infty} \frac{3\,\mathrm{d}x}{\sqrt{x^3 - 27c_4x - 54c_6}}.$$

We will consider two cases based on the value

$$k = |c_4| \,/\, |c_6|^{2/3}.$$

If $|c_6|^2 \geq |c_4|^3$, i.e., if $0 < k \leq 1$, then write the integral in the form

$$\frac{1}{|c_6|^{1/2}} \int_{r_0}^{\infty} \frac{3\,\mathrm{d}x}{\sqrt{\left(\frac{x}{|c_6|^{1/3}}\right)^3 \pm 27\left(\frac{|c_4|}{|c_6|^{2/3}}\right)\left(\frac{x}{|c_6|^{1/3}}\right) \pm 54}}.$$

The substitution $u = x/\,|c_6|^{1/3}$ gives

$$\frac{1}{|c_6|^{1/6}} \int_{\underset{\substack{\uparrow \\ \text{largest real root of } u^3 \pm 27ku \pm 54}}{r(k)}}^{\infty} \frac{3\,\mathrm{d}u}{\sqrt{u^3 \pm 27ku \pm 54}}.$$

Calculus: $\frac{1}{\Omega} \ll \text{SUP}\left(|c_4|^{1/4}, |c_6|^{1/6}\right)$

Three observations:

- The integral

$$\frac{1}{|c_6|^{1/6}} \int_{r(k)}^{\infty} \frac{3\,\mathrm{d}u}{\sqrt{u^3 \pm 27ku \pm 54}}$$

  converges when $u^3 \pm 27ku \pm 54$ has distinct roots, i.e., when $k \neq 1$.

- The integral goes to ∞ as $k \to 1$, which is okay since we seek a lower bound.

- The integral is continuous in k for $k \in [0, 1-\varepsilon]$.

Calculus: $\frac{1}{\Omega} \ll \mathrm{SUP}\left(|c_4|^{1/4}, |c_6|^{1/6}\right)$

Hence a lower bound must exist for the integral, so that

$$\frac{1}{|c_6|^{1/6}} \ll \Omega.$$

The other case, $|c_6|^2 \leq |c_4|^3$, similarly gives

$$\frac{1}{|c_4|^{1/4}} \ll \Omega.$$

Combining the two cases gives

$$\frac{1}{\Omega} \ll \mathrm{SUP}\left(|c_4|^{1/4}, |c_6|^{1/6}\right).$$

ABC: $\mathrm{SUP}\left(|c_4|^{1/4}, |c_6|^{1/6}\right) \ll N^{1/2+\varepsilon}$.

Recall

$$\begin{aligned} \mathrm{GCD}(c_4, \mathcal{D}) &= 1, \\ {c_4}^3 - {c_6}^2 &= 1728\mathcal{D}. \end{aligned}$$

Let $d = \mathrm{GCD}({c_4}^3, 1728)$. Applying ABC to

$$\frac{{c_4}^3}{d} - \frac{{c_6}^2}{d} = \frac{1728\mathcal{D}}{d}.$$

gives

$$\begin{aligned} \mathrm{SUP}\left(\frac{|c_4|^3}{d}, \frac{|c_6|^2}{d}\right) &\ll N_0\left(\frac{{c_4}^3{c_6}^2 1728\mathcal{D}}{d^3}\right)^{1+\varepsilon} \\ &\ll N_0\left(c_4 c_6 2 \cdot 3 \cdot \mathcal{D}\right)^{1+\varepsilon} \\ &\ll |c_4|^{1+\varepsilon}\, |c_6|^{1+\varepsilon}\, N_0(\mathcal{D})^{1+\varepsilon} \\ &= |c_4|^{1+\varepsilon}\, |c_6|^{1+\varepsilon}\, N^{1+\varepsilon}. \end{aligned}$$

Absorb the d's into the "$\ll$" constant:

$$\mathrm{SUP}\left(|c_4|^3, |c_6|^2\right) \ll |c_4|^{1+\varepsilon}\, |c_6|^{1+\varepsilon}\, N^{1+\varepsilon}.$$

ABC: $\text{SUP}\left(|c_4|^{1/4}, |c_6|^{1/6}\right) \ll N^{1/2+\varepsilon}$.

There are two cases to consider.
If $|c_6|^2 \le |c_4|^3$, then our inequality

$$\text{SUP}\left(|c_4|^3, |c_6|^2\right) \ll |c_4|^{1+\varepsilon} |c_6|^{1+\varepsilon} N^{1+\varepsilon}$$

becomes $|c_4|^3 \ll |c_4|^{5/2+5/2\varepsilon} N^{1+\varepsilon}$.

Thus $\qquad |c_4|^{1/2-5/2\varepsilon} \ll N^{1+\varepsilon}$,

or simply $\qquad |c_4|^{1/2} \ll N^{1+\varepsilon}$,

so that $\qquad |c_4|^{1/4} \ll N^{1/2+\varepsilon}$.

The other case, $|c_4|^3 \le |c_6|^2$, similarly gives

$$|c_6|^{1/6} \ll N^{1/2+\varepsilon}.$$

Combining the cases gives

$$\text{SUP}\left(|c_4|^{1/4}, |c_6|^{1/6}\right) \ll N^{1/2+\varepsilon}.$$

PROGRESS REPORT

Rearranging B&SD gives:

$$|\text{Ш}| = \left.\frac{L(s)}{(s-1)^r}\right|_{s=1} \cdot \frac{|E(\mathbf{Q})_{\text{TOR}}|^2}{2^r\, \Omega\, R\, \prod_{p|N} c_p} \ll N^{3/4+\varepsilon}$$

(rank fixed)

Thus, to bound $|\text{Ш}|$, we seek bounds for:

- $\left.\dfrac{L(s)}{(s-1)^r}\right|_{s=1} \ll N^{1/4+\varepsilon}$, DONE

- $|E(\mathbf{Q})_{\text{TOR}}|^2 \leq 144$, by Mazur's theorem

- $\dfrac{1}{\Omega} \ll N^{1/2+\varepsilon}$, DONE

- $\dfrac{1}{R} \ll C_r$ (constant depending on r),
  TO BE SHOWN

- $\dfrac{1}{\prod_{p|N} c_p} \leq 1$, since each $c_p = \left|\dfrac{E(\mathbf{Q}_p)}{E_0(\mathbf{Q}_p)}\right| \geq 1$

Establishing $\frac{1}{R} \ll C_r$

Recall that the regulator is

$$R = \mathsf{DET}\left[\left\langle P_i, P_j \right\rangle\right],$$

where $\langle \cdot, \cdot \rangle$ is the canonical height pairing, and $\{P_i\}$ is a basis for $E(\mathbf{Q})/E(\mathbf{Q})_{\mathsf{TOR}}$.

Viewing the free $\mathbf{Z}$-module $E(\mathbf{Q})/E(\mathbf{Q})_{\mathsf{TOR}}$ as a lattice (of rank r) inside the $\mathbf{R}$-vectorspace

$$\frac{E(\mathbf{Q})}{E(\mathbf{Q})_{\mathsf{TOR}}} \bigotimes_{\mathbf{Z}} \mathbf{R} \qquad \text{(of dimension } r\text{)},$$

the regulator is simply

$$R = \mathsf{COVOL}(\mathsf{lattice})^2,$$

where volume is measured with respect to the length

$$\ell(P) = \sqrt{\langle P, P \rangle}.$$

Establishing $\frac{1}{R} \ll C_r$

Among all nonzero lattice points, let h_0 be the minimal canonical height. Three results will help us bound $1/R$:

- Minkowski's Theorem from the geometry of numbers will give us:
$$\frac{1}{R} \ll c_r \left(\frac{1}{h_0}\right)^r.$$

- Hindry–Silverman will give us:
$$\frac{1}{h_0} \ll \text{something involving } \mathcal{S}.$$

- Szpiro's conjecture will give us:
$$\mathcal{S} \le 6 + \varepsilon + c_\varepsilon.$$

Establishing $\frac{1}{R} \ll c_r \left(\frac{1}{h_0}\right)^r$

Theorem (Minkowski)
Let B_n denote the ball of radius n. If

$$\mathrm{VOL}(B_n) \geq 2^r\,\mathrm{COVOL}(\text{lattice}),$$

then B_n contains a nonzero lattice point. In particular, the minimal nonzero length ℓ_0 satisfies $\ell_0 \leq n$.

Corollary
Since $\mathrm{VOL}(B_n) = n^r\,\mathrm{VOL}(B_1)$, the theorem requires

$$n^r \geq 2^r\,\mathrm{COVOL}(\text{lattice})/\,\mathrm{VOL}(B_1),$$

and gives ${\ell_0}^r \leq n^r$. In particular, the possibility

$$n^r = 2^r\,\mathrm{COVOL}(\text{lattice})/\,\mathrm{VOL}(B_1)$$

gives us the *unconditional conclusion*

$$\ell_0 \leq 2^r\,\mathrm{COVOL}(\text{lattice})/\,\mathrm{VOL}(B_1).$$

Establishing $\frac{1}{R} \ll c_r \left(\frac{1}{h_0}\right)^r$

The corollary gave,

$$\ell_0 \leq 2^r \,\mathsf{COVOL(lattice)} / \mathsf{VOL}(B_1),$$

which for us becomes

$$\ell_0{}^r \leq 2^r \sqrt{R} / \mathsf{VOL}(B_1).$$

Length and canonical height satisfy the identity $\ell(P)^2 = 2\hat{h}(P)$; in particular, $\ell_0{}^2 = 2h_0$. Thus we have

$$(2h_0)^r \leq 2^{2r} R / \mathsf{VOL}(B_1)^2,$$

so that

$$\frac{1}{R} \leq \frac{2^r / \mathsf{VOL}(B_1)^2}{h_0{}^r}.$$

In short, we have established

$$\frac{1}{R} \ll c_r \left(\frac{1}{h_0}\right)^r.$$

Establishing $\frac{1}{R} \ll C_r$

Theorem (Hindry–Silverman)
Letting $\mathcal{S} = \mathsf{LOG}\,|\mathcal{D}|\,/\,\mathsf{LOG}\,N$ denote the "Szpiro number", we have

$$\frac{1}{h_0} \leq \frac{(20\mathcal{S})^8 10^{1.1+4\mathcal{S}}}{\mathsf{LOG}\,|\mathcal{D}|}.$$

Conjecture (Szpiro)
We have $|\mathcal{D}| \ll N^{6+\varepsilon}$. Hence we have

$$\mathsf{LOG}\,|\mathcal{D}| \leq c_\varepsilon + (6+\varepsilon)\,\mathsf{LOG}\,N,$$

or

$$\mathcal{S} = \frac{\mathsf{LOG}\,|\mathcal{D}|}{\mathsf{LOG}\,N} \leq 6 + \varepsilon + \frac{c_\varepsilon}{\mathsf{LOG}\,N} \leq 6 + \varepsilon + c_\varepsilon.$$

Establishing $\frac{1}{R} \ll C_r$

Now combine the pieces:

$$
\begin{aligned}
\frac{1}{R} &\ll c_r \frac{1}{{h_0}^r} \\
&\leq c_r \frac{(20\mathcal{S})^{8r} 10^{1.1r+4r\mathcal{S}}}{(\mathsf{LOG}\,|\mathcal{D}|)^r} \\
&\leq c_r \frac{(20(6+\varepsilon+c_\varepsilon))^{8r} 10^{1.1r+4r(6+\varepsilon+c_\varepsilon)}}{(\mathsf{LOG}\,|\mathcal{D}|)^r}
\end{aligned}
$$

Since $|\mathcal{D}|$ is always at least 3, we know

$$\frac{1}{\mathsf{LOG}\,|\mathcal{D}|} < 1,$$

and thus we may conclude

$$\frac{1}{R} \ll C_r.$$

THANKS

- To Barry Mazur and Minhyong Kim, for suggesting this material.

- To Minhyong Kim, Dinesh Thakur, Kirti Joshi, and Bill McCallum, for answering all our questions.

These slides were last modified in March 1999. The most recent version is available for anonymous retrieval from the website:

`www.math.arizona.edu/~aprl`

Send comments and corrections to Alex Perlis:

`aprl@math.arizona.edu`