Geometry via point counting

Asher Auel

Department of Mathematics
Yale University

CCR-Princeton
Wednesday 29 March 2017

Linear algebra problem

Problem. Compute the number of k-dim subspaces of $\mathbb{F}_q^n$

Linear algebra problem

Problem. Compute the number of k-dim subspaces of $\mathbb{F}_q^n$

Case $k = 1$

$$\frac{q^n - 1}{q - 1} = 1 + q + q^2 + \cdots + q^{n-1}$$

$$\#\mathbb{P}^{n-1}(\mathbb{F}_q) = 1 + q + q^2 + \cdots + q^{n-1}$$

Projective space $\mathbb{P}^{n-1}$ over $\mathbb{F}_q$

Linear algebra problem

Problem. Compute the number of k-dim subspaces of $\mathbb{F}_q^n$

General case. Transitive action of $\mathrm{GL}_n(\mathbb{F}_q)$ with stabilizer

$$\begin{pmatrix} \mathrm{GL}_k(\mathbb{F}_q) & M_{k\times(n-k)}(\mathbb{F}_q) \\ 0 & \mathrm{GL}_{n-k}(\mathbb{F}_q) \end{pmatrix}$$

Orbit-stabilizer theorem gives

$$\frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{|\mathrm{GL}_k(\mathbb{F}_q)||\mathrm{GL}_{n-k}(\mathbb{F}_q)||M_{k\times(n-k)}(\mathbb{F}_q)|}$$

$$\frac{(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})}{(q^k-1)\cdots(q^k-q^{k-1})\,(q^{n-k}-1)\cdots(q^{n-k}-q^{n-k-1})\,q^{k(n-k)}}$$

Linear algebra problem

Problem. Compute the number of k-dim subspaces of $\mathbb{F}_q^n$

$$\#G(k,n)(\mathbb{F}_q) = \frac{(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})}$$

$$= \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}$$

$$= \binom{n}{k}_q \qquad q\text{-binomial coefficient}$$

Grassmannian $G(k,n)$ over $\mathbb{F}_q$

Linear algebra problem

Problem. Compute the number of k-dim subspaces of $\mathbb{F}_q^n$

$$\binom{n}{k}_q = \sum_{i=0}^{k(n-k)} \lambda_{n,k}(i)\, q^i$$

$\lambda_{n,k}(i)$ number of partitions of i into at most $n-k$ parts of size at most k

$$\begin{aligned}
\#G(1,n)(\mathbb{F}_q) &= 1 + q + \cdots + q^{n-1} \\
\#G(2,4)(\mathbb{F}_q) &= 1 + q + 2q^2 + q^3 + q^4 \\
\#G(2,5)(\mathbb{F}_q) &= 1 + q + 2q^2 + 2q^3 + 2q^4 + q^5 + q^6 \\
\#G(2,6)(\mathbb{F}_q) &= 1 + q + 2q^2 + 2q^3 + 3q^4 + 2q^5 + 2q^6 + q^7 + q^8
\end{aligned}$$

Topology

$G(k, n)$ complex Grassmannian manifold, dimension $k(n - k)$

$b_i = \text{rk}\, H^i(G(k, n), \mathbb{Z})$ ith Betti number

Theorem (Schubert 1874). $H^i(G(k, n), \mathbb{Z})$ is free abelian group generated by Schubert classes for i even and is 0 for i odd

Topology

$G(k,n)$ complex Grassmannian manifold, dimension $k(n-k)$

$b_i = \operatorname{rk} H^i(G(k,n),\mathbb{Z})$ ith Betti number

Theorem (Schubert 1874). $H^i(G(k,n),\mathbb{Z})$ is free abelian group generated by Schubert classes for i even and is 0 for i odd

Poincaré polynomial $P_X(t) = \sum_{i=0}^{2\dim(X)} (-1)^i b_i\, t^i$

$$\begin{aligned}
P_{G(1,n)}(t) &= 1 + t^2 + \cdots + t^{2(n-1)} \\
P_{G(2,4)}(t) &= 1 + t^2 + 2t^4 + t^6 + t^8 \\
P_{G(2,5)}(t) &= 1 + t^2 + 2t^4 + 2t^6 + 2t^8 + t^{10} + t^{12} \\
P_{G(2,6)}(t) &= 1 + t^2 + 2t^4 + 2t^6 + 3t^8 + 2t^{10} + 2t^{12} + t^{14} + t^{16}
\end{aligned}$$

Topology

$G(k,n)$ complex Grassmannian manifold, dimension $k(n-k)$

$b_i = \operatorname{rk} H^i(G(k,n),\mathbb{Z})$ ith Betti number

Theorem (Schubert 1874). $H^i(G(k,n),\mathbb{Z})$ is free abelian group generated by Schubert classes for i even and is 0 for i odd

Poincaré polynomial $P_X(t) = \sum_{i=0}^{2\dim(X)} (-1)^i b_i\, t^i$

$$\begin{aligned}
P_{G(1,n)}(t) &= 1 + t^2 + \cdots + t^{2(n-1)}\\
P_{G(2,4)}(t) &= 1 + t^2 + 2t^4 + t^6 + t^8\\
P_{G(2,5)}(t) &= 1 + t^2 + 2t^4 + 2t^6 + 2t^8 + t^{10} + t^{12}\\
P_{G(2,6)}(t) &= 1 + t^2 + 2t^4 + 2t^6 + 3t^8 + 2t^{10} + 2t^{12} + t^{14} + t^{16}
\end{aligned}$$

$$P_{G(k,n)}(q^{1/2}) = \#G(k,n)(\mathbb{F}_q)$$

Elliptic curves I

Theorem (Tate 1966). Two elliptic curves over $\mathbb{F}_q$ are isogenous if and only if they have the same number of rational points.

Use this as a test for when two elliptic curves defined over a number field are not isogenous

Elliptic curves I

Theorem (Tate 1966). Two elliptic curves over $\mathbb{F}_q$ are isogenous if and only if they have the same number of rational points.

Use this as a test for when two elliptic curves defined over a number field are not isogenous

$$E : y^2 + xy + y = x^3 - 460x - 3830$$
$$E' : y^2 + xy + y = x^3 - x^2 - 213x - 1257$$

E and E' have conductor 26 and no torsion points over $\mathbb{Q}$

$$\#E(\mathbb{F}_2) = 4, \#E'(\mathbb{F}_2) = 2$$

Elliptic curves I

Theorem (Tate 1966). Two elliptic curves over $\mathbb{F}_q$ are isogenous if and only if they have the same number of rational points.

Use this as a test for when two elliptic curves defined over a number field are not isogenous

$$E : y^2 + xy + y = x^3 - 460x - 3830$$
$$E' : y^2 + xy + y = x^3 - x^2 - 213x - 1257$$

E and E' have conductor 26 and no torsion points over $\mathbb{Q}$

$$\#E(\mathbb{F}_2) = 4, \#E'(\mathbb{F}_2) = 2$$

$$\#E(\mathbb{F}_3) = 3, \#E'(\mathbb{F}_3) = 7$$

Elliptic curves II*

$E/\mathbb{Q}$ elliptic curve

$$L(E,s) = \prod_p L_p(E,s)^{-1}$$

Local factors in terms of $\#E(\mathbb{F}_p)$

$$L_p(E,s) = 1 - a_p p^{-s} + p^{1-2s} \quad p \text{ is a prime of good reduction}$$

Fourier coefficiant $a_p = p + 1 - \#E(\mathbb{F}_p)$

Conjecture (Birch–Swinnerton-Dyer 1965).

$$\mathrm{ord}_{s=1} L(s,E) = \mathrm{rk}\, E(\mathbb{Q})$$

Weil conjectures

X smooth projective variety of dimension n over $\mathbb{Z}_p$

$$\zeta(X,s) = \exp\left(\sum_{m=1}^{\infty} \frac{\#X(\mathbb{F}_{q^m})}{m} q^{-ms}\right)$$

Conjecture (Weil 1949) [Dwork, Grothendieck, Deligne]

1. (Rationality) $\zeta(X,s)$ is a rational function in $T = q^{-s}$

$$\zeta(X,s) = \frac{P_1(T)\cdots P_{2n-1}(T)}{P_0(T)\cdots P_{2n}(T)}$$

2. (Betti numbers) $\deg P_i(T) = b_i(X(\mathbb{C}))$
3. (Functional equation) $E = \sum_{i=0}^{2n}(-1)^i\, b_i(X(\mathbb{C}))$

$$\zeta(X, n-s) = \pm q^{(\frac{n}{2}-s)E}\,\zeta(X,s)$$

4. (Riemann hypoth) $|\alpha_{ij}| = q^{i/2}$ if $P_i(T) = \prod_j (1-\alpha_{ij}T)$

Weil conjectures

X smooth projective variety of dimension n over $\mathbb{Z}_p$

$$\zeta(X,s) = \frac{P_1(T)\cdots P_{2n-1}(T)}{P_0(T)\cdots P_{2n}(T)}$$

Grothendieck's proof of Betti numbers

$$P_i(T) = \det\big(I - \Phi^* T \mid H^i_{\text{ét}}(\overline{X}_0, \mathbb{Q}_\ell)\big)$$

Characteristic polynomial of Frobenius $\Phi : \overline{X}_0 \to \overline{X}_0$ acting on ℓ-adic cohomology of the special fiber over $\overline{\mathbb{F}}_q$

Lefschetz trace formula

$$\# X(\mathbb{F}_{q^m}) = \sum_{i=0}^{2n} (-1)^i \operatorname{Tr}\big(\Phi^{m*} \mid H^i_{\text{ét}}(\overline{X}_0, \mathbb{Q}_\ell)\big)$$

Weil conjectures

X smooth projective variety of dimension n over $\mathbb{Z}_p$

Lefschetz trace formula

$$\#X(\mathbb{F}_{q^m}) = \sum_{i=0}^{2n} (-1)^i \operatorname{Tr}\big(\Phi^{m*} \mid H^i_{\text{ét}}(\overline{X}_0, \mathbb{Q}_\ell)\big)$$

Example. E elliptic curve over $\mathbb{Z}_p$

$$\zeta(E, s) = \frac{1 - a_p T + pT^2}{(1-T)(1-pT)}$$

$H^1_{\text{ét}}(\overline{E}, \mathbb{Q}_\ell) = T_\ell(E) \otimes \mathbb{Q}_\ell$ Tate module
$a_p = 1 - \#E(\mathbb{F}_p) + p$ Frobenius trace
Corollary is Tate's isogeny theorem

Weil conjectures

X smooth projective variety of dimension n over $\mathbb{Z}_p$

Lefschetz trace formula

$$\#X(\mathbb{F}_{q^m}) = \sum_{i=0}^{2n} (-1)^i \operatorname{Tr}\big(\Phi^{m*} \mid H^i_{\text{ét}}(\overline{X}_0, \mathbb{Q}_\ell)\big)$$

Example. $G(k,n)$ Grassmannian over $\mathbb{Z}_p$

$$\zeta(G(k,n),s) = \prod_{i=0}^{k(n-k)} (1 - q^i T)^{-\lambda_{n,k}(i)}$$

Corollary

$$\#G(k,n)(\mathbb{F}_q) = P_{G(k,n)}(q^{1/2})$$

Quartic K3 surfaces

$X \subset \mathbb{P}^3_{\mathbb{C}}$ smooth quartic hypersurface, e.g.,

$$x^4 + y^4 + z^4 + w^4 = 0$$

X is a K3 surface: $\omega_X = \mathscr{O}_X$ and $H^1(X, \mathscr{O}_X) = 0$

$$\begin{array}{ccccc} & & 1 & & \\ & 0 & & 0 & \\ 1 & & 20 & & 1 \\ & 0 & & 0 & \\ & & 1 & & \end{array}$$

Néron–Severi group
$\mathrm{NS}(X) \subset H^2(X, \mathbb{Z})$
free lattice of rank $\rho(X)$
$1 \leq \rho(X) \leq 20$

Quartic K3 surfaces

$X \subset \mathbb{P}^3_{\mathbb{C}}$ smooth quartic hypersurface, e.g.,

$$x^4 + y^4 + z^4 + w^4 = 0$$

X is a K3 surface: $\omega_X = \mathscr{O}_X$ and $H^1(X, \mathscr{O}_X) = 0$

$$\begin{matrix} & & & 1 & & & \\ & & 0 & & 0 & & \\ & 1 & & 20 & & 1 & \\ & & 0 & & 0 & & \\ & & & 1 & & & \end{matrix}$$

Néron–Severi group
$\mathrm{NS}(X) \subset H^2(X, \mathbb{Z})$
free lattice of rank $\rho(X)$
$1 \le \rho(X) \le 20$

$\rho(X) = 1$ for a “very general” X

Challenge (Mumford). Write down any example with $\rho(X) = 1$.

Quartic K3 surfaces

Theorem (van Luijk 2007). First explicit example of quartic K3 surface X with $\rho(X) = 1$

Idea: A random enough choice of coefficients will suffice, the real challenge is verifying that $\rho(X) = 1$

Quartic K3 surfaces

Theorem (van Luijk 2007). First explicit example of quartic K3 surface X with $\rho(X) = 1$

Idea: A random enough choice of coefficients will suffice, the real challenge is verifying that $\rho(X) = 1$

X K3 surface over $\mathbb{Z}_p$

$$\zeta(X, s) = \frac{P_2(T)}{(1 - T)(1 - q^2 T)}$$

$P_2(T) = \Psi(T) P_{\mathrm{tr}}(T)$
$\Psi(T)$ product of cyclotomic polynomials, coming from $\mathrm{NS}(\overline{X}_0)$

Conclusion $\rho(X_{\mathbb{C}}) \leq$ number of root of unity roots of $P_2(T)$

Quartic K3 surfaces

Theorem (van Luijk 2007). First explicit example of quartic K3 surface X with $\rho(X) = 1$

To compute $P_2(T)$ = characteristic poly of Φ^* on $H^2_{\text{ét}}(\overline{X}_0, \mathbb{Q}_\ell))$

- Newton's formulas $\Longrightarrow$
  can deduce $P_2(T)$ from $\mathrm{Tr}(\Phi^{m*})$ for $m = 1, \ldots, 22$
- Lefschetz trace formula $\Longrightarrow$
  $\#X(\mathbb{F}_{q^m}) = 1 + \mathrm{Tr}(\Phi^{m*}) + q^2$
- Functional equation $\Longrightarrow$
  only need to count $\#X(\mathbb{F}_{q^m})$ for $m = 1, \ldots, 11$