APPLICATIONS OF CURVES OVER FINITE FIELDS

MICHAEL D. FRIED

ABSTRACT. The area starts with Galois and Gauss. Group theory and exponential sums were the two application areas then. That tradition continues.

- Without Chevalley groups over finite fields there would have been no structure theory of finite simple groups.
- Weil's Riemann Hypothesis for curves over finite fields is a singular event. Many error estimates in combinatorics derive from it.

Research in finite fields requires combinatorial understanding of many examples. This is true in myriad applications: coding theory, exceptional polynomials (and covers), algorithmic applications of elimination of quantifiers, diophantine relations between curves over number fields and their reductions modulo p; probabilistic algorithms over finite fields. Yet, there are powerful general *abstract* tools. Consider two premiere mathematical events from the last twenty-five years:

- Deligne's proof of the general Weil conjectures.
- The classification of finite simple groups.

This conference's papers offer examples of applying such tools to practical researcher specialties. The sections of this preface divide along the basic themes of the conference. The preface makes several connections not appearing directly in the papers. Some papers in the conference refer directly to Bernie Dwork, not only to his papers. This preface (see §4) includes comments giving an overview of his work. It compliments the article of Katz and Tate [24].

1. BEYOND WEIL BOUNDS; CURVES WITH MANY RATIONAL POINTS

Let p be a prime. The word *curve* in this preface always means a one dimensional projective nonsingular algebraic variety. The phrase *variety over a finite field* means the equations have coefficients in a finite field $\mathbb{F}_q$. The usual notation applies: q is p^t with p a prime and $t \geq 1$ an integer. Then, $\mathbb{F}_q$ is the unique fi eld (up to isomorphism) with q elements. For any field K, $\bar{K}$ is its algebraic closure. If X is a curve, let its genus be $g(X) = g$. The curve $\mathbb{P}^1$ is the projective line. If we use a subscript t as in $\mathbb{P}^1_t$, this means t you are given an inhomogenous parameter running over the points on $\mathbb{P}^1$.

The Weil bound estimates the number of points on curves. It offers, however, little for q fixed if the curves have large genus. Applications with g large include explicit constructions of curves arising in coding theory: to compute weight enumerators from Frobenius eigenvalues. It also includes applications to graph theory and various problems involving the decomposition types of polynomials. Persistent preoccupations include exceptional polynomials, Davenport and Schur problems, estimates for Kloosterman sums, Ramanujan graphs. These stipulate a sufficiently

Date: July 21, 1999.

1991 *Mathematics Subject Classification.* Primary 11F32, 11G18, 11R58; Secondary 20B05, 20C25, 20D25, 20E18, 20F34.

NSF #DMS-9622928 and the Alexander von Humboldt Foundation contributed support.

large prime p for the appearance of phenomena that treat the error term in the Weil bound as explicit and small. The error term is roughly $2g\sqrt{q}$ (there are improvements when q is not a square). Assume q fixed and g large. Then, the error overwhelms the main term, $q+1$, in the Weil estimate. This is the naive source for papers on curves over $\mathbb{F}_q$ with genus g large and many rational points.

The paper of Niederreiter and Xing reviews previous results. Two quantities often appear:

- $N_q(g)$, the maximum for $\mathbb{F}_q$ points running over all (finitely many up to isomorphism over $\mathbb{F}_q$) curves of genus g; and
- $A(q) = \limsup_{g\mapsto\infty} \frac{N_q(g)}{g-1}$.

This volume has papers from the people who produced the four now standard approachs. Adding to this, several connect their approach to another.

1.1. **The moduli space approach.** Typically the area refers to modular curves as classical curves rather than as moduli spaces. The moduli space treatment eschews detailed equation information. Rather, each point on such a curve attaches to an object with its own internal structure.

Vlăduț and Drinfeld around 1983 showed $A(q) \le q^{1/2}-1$ for all q. A brief version of a satisfying result for q a square goes like this. Ihara, and Tsfasman-Vlăduț-Zink established a lower bound $A(q) \ge q^{1/2}-1$, so $A(q) = q^{1/2}-1$ for any square q. The brief version, however, doesn't do justice to compelling aspects of the story.

Ihara's contribution went through stages starting in the late 60s. The following definition states a basic principle. Let C_i, $i \in I$ be a *natural* sequence of curves over $\mathbb{F}_q$. The meaning of *natural*, of course, is up to the investigator. Detecting how this sequence contributes to the problem requires knowing the asymptotic behavior of the genus and number o f rational points.

Suppose $q = p^2$ and $(N,p) = 1$. Then, the reduction of the modular curve $X(N)$ (elliptic curves with level N structure) has a model over $\mathbb{F}_{p^2}$. The curve $X(N)$ covers the classical j-line. We know its genus, reduction mod p works well, and there is a set of points of known cardinality on $X(N)$ over $\mathbb{F}_{p^2}$. The ultimate source of being over $\mathbb{F}_p^2$ is a subtlety from th e points lying over j values where the elliptic curves have no p-division points: *supersingular curves*. So, Ihara's example, when $q = p^2$ exhibits these properties.

- The contributing curves forms a natural projective system of moduli spaces.
- Rational points contributing to $A(p^2)$ correspond to *nonordinary* reduction of the object (elliptic curve) they represent.
- A differential (holomorphic except at the cusps) on $X(N)$ has its zeros located at these particular rational points.
- The Frobenius lifts as an explicit correspondence to characteristic 0.

Even if a curve over $\mathbb{F}_q$ contributes significantly to $N_g(q)$, it won't do so for $N_g(q')$ where $q|q'$. So, to extend this result to other square powers of p, Ihara developed similar results for Shimura curves. These are moduli spaces of abelian varieties associated with quaternion algebras. Ihara's paper *Shimura curves over finite fields and their rational points* simplifies the literature on this example. It also reconsiders questions open from the 1970s.

1.2. **The Drinfeld module approach when q is not a square.** No one has produced a natural sequence of canonical models when q is not a square. No exact values of $A(q)$ are known. Still, Serre introduced the idea of pro viding lower bounds

using the abelian theory of covers. This is class field theory, using data from wild ramification. Serre showed $A(q) \geq c \cdot \log(q)$ with an absolute constant $c > 0$. Zink showed $A(p^3) \geq \frac{2(p^2-1)}{p+2}$ for any prime p.

This approach used Drinfeld modules. Niedderiter and Xing emphasize that Drinfeld modules are explicit, contrasting them with modular curves. This Editor encourages further research separating the Drinfeld module approach from that of Ihara. Especially valuable would would be examples coming from natural projective systems of upper half-plane quotients that are moduli spaces, though they are not modular curves. (The Editor's conference talk discussed Modular Towers —see http://www.math.uci.edu/ñfried/#mt, Papers on Modular Towers [22] —which produce such sequences. Producing, however, an Ihara-type differential with zeros containing the nonordinary points on particular Modular Towers was incomplete at this volume's production time.)

1.3. **More on explicit use of Drinfeld modules.** Hayes in *Distribution of minimal ideals in imaginary quadratic function fields* illustrates how to study class numbers and j-invariants of Drinfeld modules. His examples are abelian covers of hyperelliptic looking curves split over ∞ (formed from $M \in \mathbb{F}_q[x]$ of odd degree). Here, M may not be square-free. The result is an average of class numbers over discriminants. Chen in *Division points of Drinfeld Modules and special values of Weil L-functions* computes values of Weil L -functions of hyperelliptic curves. Thus, he gives degrees of the norm and trace of Drinfeld module j -invariants. These papers show a community growing comfortable with using Drinfeld modules.

1.4. **One curve with many points and fiber products.** Coding theory applications don't explicitly ask for curves with many rational points. Rather, they seek structured *sets* of curves with many rational points. van der Geer and van der Vlugt have used coding theory as a source of problems for finding sets of such curves. *Constructing Curves over Finite Fields with Many Points by Solving Linear Equations* expands their fiber product technique. For some problems their method is more efficient than class field theory.

The process starts with a linear system L of functions on C. For $f \in L$, form the fiber product of these covers of the w-line: $x \in C \mapsto f(x) = w$ and $z \mapsto z^p - z = w$. Call this curve C_f. The divisor giving L has support in rational points on C. (Avoid those for giving reducibility, by assuming $f \neq m^p - m$ for any m in the function field of C.) To assure the resulting fiber product has rational points restrict to the following linear condition. Use only those f with $f(P)$ having 0 trace from $\mathbb{F}_q$ to $\mathbb{F}_p$ for all P in the support of D. Let $f_1, \ldots, f_n$ be a basis of the linear subspace satisfying these conditions. Take C_L the fiber product over all the $f_1, \ldots, f_n$. The result is independent of the basis. The unique nonsingular model of C_L is a covering of C with all rational points in the support of D split completely. The method easily computes the Jacobian and the number of rational points.

This explicitly reproduces many examples from papers of Niederreiter and Xing. There the curves were from narrow ray class fields determined by Drinfeld modules of rank 1 over a curve.

1.5. **Approach from classical curves.** Garcia and Torres *On maximal curves having classical Weierstrass gaps* consider maximal curves over F_{q^2} having classical Weierstrass gaps. *Maximal* means (because the field has square order) it attains the Weil upper bound $q^2 + 1 + 2gq$. For a maximal curve, let P be an $\mathbb{F}_{q^2}$ rational

point. Then, the support of the Frobenius divisor of the linear system $|(q+1)P|$ consists of the Weierstrass points (for the canonical divisor) and the $\mathbb{F}_{q^2}$ points of the curve.

This story resembles achieving maximal groups of automorphisms. Maximal curves often have large automorphism groups, and Jacobians isogenous to products of supersingular elliptic curves (there being but one supersingular curve up to isogeny). There is yet no classification of maximal curves over $\mathbb{F}_{q^2}$ of a given genus.

The genus of a maximal curve over $\mathbb{F}_{q^2}$ satisfies either $g \le (q-1)^2/4$ or $g = (q-1)q/2$. There is one maximal curve (up to $\mathbb{F}_{q^2}$-isomorphism) over $\mathbb{F}_{q^2}$ with $g = (q-1)q/2$. This is the *Hermitian curve* with affine equation $y^q + y = x^{q+1}$. Similarly, if the genus is $(q-1)^2/4$, q, it must be $y^q + y = x^{(q+1)/2}$.

2. Monodromy groups of characteristic p covers

Related to the topic of maximal curves, valid over all finite fields (not just over $\mathbb{F}_{q^2}$), is that of *median value* curves. These curves over $\mathbb{F}_q$ have *exactly* q^t+1 points over $\mathbb{F}_{q^t}$ for *infinitely many* t. Many of these curves do have large automorphism groups and supersingular Jacobians, but most do not. For the relation of these to *exceptional covers* see [21, §3].

Progress in classifying exceptional polynomials (another cryptography connection) came through using monodromy (Galois closure; see §2.1) groups of covers. In characteristic 0 there are especially precise formulations of Riemann's existence theorem (describing covers of curves). In positive characteristic, wild ramification poses difficult elementary problems that have blocked progress.

Example: Müller [27] listed all monodromy groups of polynomial covers over $\mathbb{C}$ (and over $\mathbb{Q}$). Yet, the classification of affine groups arising as *monodromy groups* of exceptional polynomials over a finite field is incomplete. [23, §5-§6] discusses this and details on the genus 0 problem. Exceptional polynomials over $\mathbb{F}_q$ give one-one maps on $\mathbb{F}_{q^t}$ for infinitely many t. The main result of [20] is that excluding a known list, indecomposable exceptional polynomials over $\mathbb{F}_q$ have these properties.

- They have degree p^u for some u.
- Their monodromy group is an affine group acting on $\mathbb{F}_{p^u}$.

2.1. What to expect of monodromy groups from genus 0 covers.

Let $f \in \mathbb{C}(x)$ be a rational function. Denote the Galois (monodromy) group of the splitting field Ω_{f-z} of $f(y) - z$ over $\mathbb{C}(z)$ by G_f. The now complete genus zero problem of Guralnick-Thompson showed the following. Excluding alternating and cyclic groups, only finitely many simple groups occur as composition factors (subquotients) of monodromy groups of rational functions. Contributors to the genus 0 problem include Aschbacher, Frohardt, Guralnick, Magaard, Müller, Neubauer, Thompson and many others. In characteristic p, however, Guralnick found a simple conjecture that has support in papers from this volume.

Conjecture 2.1 (Guralnick)**.** Let $\mathcal{G}_p$ be those simple groups that are composition factors of genus 0 monodromy groups over $\bar{\mathbb{F}}_p$. Then, excluding a finite set, $\mathcal{G}_p$ consists of alternating groups, cyclic groups and Chevalley groups of Lie type over finite fields in $\bar{\mathbb{F}}_p$.

Abhyankar's renown *NICE* papers were the source of Conjecture 2.1. In characteristic 0, Riemann's Existence Theorem offers efficient production of covers from which a check of the genus is transparent. This works in positive characteristic,

for tame covers (ramification indices prime to the characteristic). Wildly ramified covers don't have such a tool. Either producing such covers or showing they don't exist is much harder. For fuller documentation and discussion see [23, §3–§5].

2.2. **Abhyankar's approach.** Abhyankar starts with polynomials having built in Frobenius linearity. A separable projective q-polynomial of q-prodegree m over a field $\mathbb{F}_q(z)$ has the form

$$M(x) = M(x,z) = \sum_{i=0}^{m} a_i x^{\langle m-i\rangle}, \quad a_i \in \mathbb{F}_q(z),\ a_0 \neq 0, \quad a_m \neq 0 \text{ and } \langle j\rangle = \langle j\rangle_q = 1 + q + q^2 + \ldots + q^j. \tag{2.1}$$

There is a related polynomial $F(x)$ from the formula

$$M(x^{q-1})x = F(x) = \sum_{i=0}^{m+1} a_i x^{q^i}. \tag{2.2}$$

The splitting field over $\bar{\mathbb{F}}_q(z)$ of $M(x)$ in (2.1) has group a subgroup of $\mathrm{PGL}_m(\mathbb{F}_q)$. Further, the permutation representation on zeros of $M(x)$ is (permutation) equivalent to $\mathrm{PGL}_m(\mathbb{F}_q)$ acting on points of m-dimensional projective space over $\mathbb{F}_q$. Specializing the a_i s and adjusting the exponents produces other Chevalley groups.

Abhyankar and Loomis in *Twice more nice equations for nice groups* produce this list of monodromy groups with $m > 2$.

- projective symplectic isometry groups and (vectorial) symplectic isometry groups $\mathrm{Sp}(2m, q)$
- projective symplectic similitude groups $\mathrm{PGSp}(2m, q)$ and the (vectorial) symplectic similitude groups $\mathrm{GSp}(2m, q)$)

One sees here Abhyankar's *mantra* (his name!). It illustrates how combinatorially changing exponents in polynomial expressions relates distinct Chevalley group series. It doesn't, however, explain it.

2.3. **Reflection on classical invariant theory.** Under the title *Linearized Algebra and Finite Groups of Lie Type: I: Linear and Symplectic Groups* Elkies includes reflections on why Abhyankar's mantra works. He starts with "linearized algebra," the systematic study of q-linearized polynomials. The idea is to devolve classical invariant theory from their study. This paper concentrates on linear and symplectic groups, showing that in each case the monodromy groups have associated Deligne-Lusztig varieties.

Elkies emphasizes that Deligne-Lusztig varieties come with a finite group of Lie type *and* an element w of the associated Weyl group. This extra structure, comes with the production of differential analogues of these varieties. This structure, he suggests, may be what lies behind Abhyankar's intuitions. Later papers will give analogous constructions for unitary, orthogonal, and more exotic groups G. Elkies' paper also contains a compendium of group notation useful for those not finite groups theorists.

2.4. **Reduction** mod p **and field of moduli of covers.** Debes (with his student Deschamps) has general conjectures relating these topics:

- Hilbert's irreducibility theorem,
- fields of definition of covers, and
- various refined embedding problems.

These put different formulations of the regular version of the Inverse Galois Problem over *any* field under one conjecture of Black: Any Galois extension of a field K is a specialization from a regular Galois extension $L/K(t)$. These clean formulations require K to be arbitrary. This motivates the papers of Debes and Emsalem in this volume. Here, non-Galois covers initiate the process of going to the Galois closure. This produces a constant field extension that is part of the formulation.

2.5. **Refined abelian covers.** Debes in *Regular Realization of Abelian Groups with Controlled ramification* considers an arbitrary field K, a finite subset $D \subset \mathbb{P}^1(\bar{K})$ and a finite abelian group A. He shows there is an extension $F/K(T)$, regular over K, with group A and F unramified over each element of D. Harbater's patching method requires such covers for its inductive use of cyclic groups generating a given group. Getting a totally split place is necessary for completing the construction. Starting with a finite field, finding such an extension with at least one unramified point $t_0 \in \mathbb{P}^1(K)$ adds an extra difficulty not in the literature.

2.6. **Good reduction of covers.** Emsalem in *On Reduction of Covers of Arithmetic Surfaces* refines a renown Grothendieck theorem. It considers curve covers over Spec of a discrete valuation henselian ring R with quotient field K. The paper connects covers with good reduction to those having a model over the *field of moduli* M of the cover. It generalizes a theorem of Debes-Harbater for G-covers of the Riemann sphere.

Let M^{ur} be the maximal unramified algebraic extension of M. Emsalem shows the prime of R being *bad* is the only obstruction to having a model over M^{ur}. Bad primes are those where one of these events happen.

- Either the base curve of the cover has bad reduction, or
- two points of the branch locus meet, or
- the ramified prime divides the order of the geometric monodromy group.

This result requires care in stating the equivalence between covers. Several kinds of covers appear in applications depending on what extra data the equivalence preserves. Emsalem's paper assumes fixed maps to the base curve X for *mere* covers. He assumes fixed isomorphisms of the automorphism group with a fixed group G for Galois (G-)covers.

The field of moduli of such an equivalence class of covers is intrinsic to the equivalence class. It is easy to describe. Let S be a complete listing of all objects in the equivalence class over $\bar{K}$. Then, the absolute Galois group G_K maps S to another equivalence class for the (same or related) moduli problem. The subgroup H_S stabilizing S has fixed field K_S, the field of moduli of S.

If the moduli problem is *fine*, the field of moduli will automatically be a field of definition (of some element of S). Still, in many problems the moduli problem is not fine. Thus, it is serious to decide if a model for the problem exists over the field of moduli. It is a habit to write $Y \to X$ as if a particular cover were given with its equations. In practice, it is Riemann's existence theorem that tells of such a cover existing. Emsalem uses a moduli space approach. So coordinates of a point on a Hurwitz space generate the field of moduli for the equivalence class S. One recurring problem is to characterize points whose corresponding equivalence classes contain an element over the (possibly unknown) field of moduli.

A result of Beckmann gives one property: *only* bad primes ramify in the field of moduli of a (G)-cover. For more general equivalence classes of covers, use G and $\hat{G}$

for the respective geometric and arithmetic monodromy groups of the cover. Then, inertia groups of good primes are in the centralizer $Z_{\hat{G}}$ of G in $\hat{G}$.

2.7. **Explicit computation of monodromy groups over finite fields.** Adleman and Huang in *On Function Field Sieve Method for Discrete Logarithms* remind us of changes wrought in this decade in our ability to compute quantities. They apply to function fields a sieve method for discrete logarithms over finite fields. This is an analog of the sieve method for number fields. That applied to factoring integers. Theirs runs asymptotically faster than the previously known algorithms for finite fields $\mathbb{F}_{p^u}$ when $\log^2 p \ll u$.

Abhyankar's computations for monodromy groups are often a recognition problem along the following lines. His polynomial monodromy groups are identifiably subgroups of a particular Chevalley group. This comes through the algebraic form of his mantra manipulations. He wants, then, to know if they are the full target group. Available is much information from the classification of finite simple groups. Thus, resolving his problem often comes to deciding orbit lengths of a subgroup stabilizing integers of the representation. Ultimately that factorization problem applies to an explicit polynomial in several variables. Factorization problems appear throughout Abhyankar's papers. Some aspects of his mantra intuit how a change of exponents in a polynomial (in two variables) affects the factorization problem after eliminating one (or two) roots.

The problem, however, that Adleman and Ming treat is of finding a descrete log. I review that. Let x be a generator for the multiplicative group of $\mathbb{F}_{p^u}$. The discrete logarithm problem is to compute, for non-zero $h \in \mathbb{F}_{p^u}$, the fewest non-negative integer e giving $x^e = h$: $e = \log_x h$. The logarithm function maps the multiplicative group of $\mathbb{F}_{p^u}$ to the additive group of $\mathbb{Z}/(p^u - 1)$. Though the additive group structure is extremely simple, computing the log-function is difficult because this isomorphism is not explicit. Recall: Confidence in many cryptographic security processes depends on the discrete logarithm being *hard* to compute.

Their paper gives a computer scientist's view. For example, the number field sieve applies (in polynomial run-time) to $\mathbb{F}_{p^u}$ with $u \ll (\log p)^{1/2}$. By contrast, the function field sieve applies to finite fields $\mathbb{F}_{p^u}$ when $u \gg (\log p)^2$. It is an open (computer scientist) question to find an algorithm of comparable time complexity for u between $(\log p)^{1/2}$ and $(\log p)^2$.

Now consider an adherent of monodromy group calculations. It is likely a function of the adherent's age if he or she would relish connecting directly to the Adleman-Huang method. It should not bring to mind (even if intended with great sympathy) the old folk song, "John Henry was a steel-driving man." Our mathematical era features acute specialization of technique. Yet, researchers express constant surprise at the smooth accomplishments possible by joining techniques from one area to another. (The last sentence of §4.3 is a common mathematical refrain.) There is much to be in a quandry over. Only a few readily take to new techniques, yet so many expect others to understand their specializations.

3. Zeta functions and trace formulas

Directly interpreting properties of varieties over finite fields is still a growth area. For example, did you know the zeta function neatly encodes the p-rank of a curve over $\mathbb{F}_q$? Suppose $\sum_{i=0}^{2g} c_i T^i$ is the characteristic polynomial for the Frobenius acting on the Tate module of a curve. Recall: The symmetry of the Weil pairing

implies $c_i q^{g-i} = c_{2g-i}$. The rank of p-torsion is the maximal i with $c_i \neq 0 \bmod p$ [29]. So, for families of curves (and varieties) there is a p-adic stratification of the parameter space from mod p properties of the zeta function. On the largest piece of the stratification, roots of the zeta function have p-adic analytic continuations. Their p-adic absolute values here are constant. This inspired investigations of Dwork around the name of *unit roots*.

3.1. **Unit root L-functions.** Wan in *Dwork's Conjecture* discusses an example, and then conjecture, of Dwork. In the last 25 years this example has informed most investigations into p-adic deformation of cohomology, including Grothendieck's crystalline cohomology. It started with Dwork's unit root conjecture for K-3 surfaces represented by degree four hypersurfaces in $\mathbb{P}^3$.

Dwork wrote a p-adic matrix lifting the Frobenius with its action on a collection of convergent power series. The model for it was a similar p-adic Frobenius lifting on the Legendre family of elliptic curves over the λ-line (see §4.3). This started with their p-adic analogs of periods, through classical functions when E_λ is isomorphic to a p-adic analytic torus (Tate curve). In this case, after slight base extension, E_λ looks like $K^*/\langle q^{\mathbb{Z}}\rangle$. Then, periods appear as a projective system of p^n-th roots of q and as p^n-th roots of 1. The p-adic liftings of the Frobenius then act on p-adic solutions of the hypergeometric differential equation.

For special families Dwork investigated p-adic meromorphic continuation of his unit root L-function. Dwork's conjecture considers a continuous p-adic Galois representation ρ *coming from algebraic geometry* (see §4.3) over a finite field of characteristic p. It suggests the L-function $L(\rho, T)$ is p-adic meromorphic. For a geometrically connected algebraic variety X defined over $\mathbb{F}_q$, let $\pi_1^{\rm ar}(X)$ denote the arithmetic fundamental group of X.

Let R be the ring of integers in a finite extension of the p-adic rational numbers $\mathbb{Q}_p$. To come from algebraic geometry means ρ is the homomorphism arising from the local p-adic variation of some kind of cohomology (or system of differential forms). It produces a continuous p-adic representation

$$\rho:\ \pi_1^{\rm ar}(X) \longrightarrow {\rm GL}_n(R).$$

This latter is the exact analog of an older notion over $\mathbb{C}$ called a *flat connection*.

Let X_0 be the closed points of X over $\mathbb{F}_q$ and ${\rm Fr}_x$ the Frobenius conjugacy class at x in $\pi_1^{\rm ar}(X)$. The L-function of ρ is an infinite Euler product:

$$L(\rho, T) = \prod_{x \in X_0} \frac{1}{\det\left(I - T^{\deg(x)}\rho({\rm Fr}_x)\right)}.$$

The L-function $L(\rho, T)$ is a formal power series with coefficients in R. So it is trivially p-adic analytic in the open unit disk $|T|_p < 1$.

Suppose ρ has finite image. Then, the general Dwork-Grothendieck Theorem says $L(\rho, T)$ is a rational function. Deligne's Riemann hypothesis for varieties over finite fields, says the zeroes and poles of $L(\rho, T)$ have complex absolute values that are (known) integral powers of $\sqrt{q}$. The number of zeroes and poles of $L(\rho, T)$ has an explicit bound from a theorem of Bombieri-Sperber. Yet, p-adic absolute values of the zeroes and poles of $L(\rho, T)$ are still mysterious. The topic of p-adic absolute values has its roots in an old Chevalley Theorem: A homogenous form of degree d in $d+1$ variables has a nontrivial zero over $\mathbb{F}_q$ for every q.

Wan explains modern expections when the image of ρ is infinite. Most acute is this. Only under special circumstances for ρ can we expect a rational L-function. The key definition is that of *overconvergence*, a concept arising from Dwork-Monsky trace formula.

3.2. **Zeta functions of complete intersections.** Let $Z(V/k,t)$ be the zeta function of an algebraic variety. Since it is a rational function there are several possible degrees, including the maximum degrees of the numerator and denominator (see §3.1). This calls for taking the gcd of the two polynomials. Adolphson and Sperber in *The degree of the Zeta function of a complete intersection* investigate the *difference* of the degrees (the degree at ∞), or the negative of the Euler characteristic of any Weil cohomology. This does not use the gcd. They compute this when V is a sufficiently general toric, affine, or projective complete intersection. In particular, this gives the number of solutions of a suitably general system of n polynomial equations in n unknowns over a finite field as a mixed Minkowski volume. Exponential sums count points on V. This paper expresses $Z(V/k,t)$ from L-functions of exponential sums. The degrees of these L-functions appear in a previous work of Adolphson and Sperber. This paper shows how to compute the degree of $\deg Z(V/k,t)$ as a Minkowski mixed volumes.

A similar formula holds for Euler characteristics of singular cohomology for general toric complete intersections over $\mathbb{C}$ (results of Kouchnirenko, Bernshtein and Khovanskii). The Adolphson-Sperber result requires a stronger hypothesis. Comparing their hypothesis with that for singular cohomology is a significant topic in the paper. Especially important is the result that their hypothesis is satisfied by "generic" Laurent polynomials $f_1, \ldots, f_r$ excluding finitely many characteristics.

3.3. **Properties of a modular curve quotient.** Leprévost in *The Modular Points of a Genus* 2 *Quotient of* $X_0(67)$ studies the quotient $X(67)$ of $X_0(67)$ by its Fricke involution. Each point on $X_0(67)$ corresponds to an isogeny $E \to E'$ of elliptic curves of degree 67. The Fricke involution sends this point to the equivalence class of the dual isogeny $E' \to E$. The paper applies Selberg's trace formula to obtain an equation of $X(67)$ over $\mathbb{Q}$. It then proves the Jacobian of $X(67)$ is an absolutely simple abelian subvariety of $J_0(67)$. It gives a modular interpretation of 10 rational points of small height on $X(67)(\mathbb{Q})$, the *modular points* of $X(67)(\mathbb{Q})$.

3.4. **Appearance of rank 1 representations in L-functions for higher dimensional representations.** Chai and Li in *Function Fields: Arithmetic and Applications* construct automorphic L-functions for GL_n over a function field by taking suitable products of automorphic L-functions for GL_1. The Kloosterman conjecture over a function field is a consequence. Suppose an idele class character η of a function field K over a finite field F with q elements is not principal. Then its associated L-function $L(s,\eta)$ (see §3.1) is a polynomial in q^{-s} with character sums as coefficients. Also, $L(s,\eta)$ is a factor of the zeta function of a finite abelian extension H of K. So, it encodes arithmetic of curve underlying H.

On the other hand, an automorphic L-function $L(s)$ of GL_n over K has an Euler product over the places of K. The factor at almost all places v is the reciprocal of a polynomial in Nv^{-s} with degree n. The paper characterizes when the local factors of $L(s)$ are L-functions of idele class characters (for homomorphisms of the absolute Galois group of K into GL_1). It systematically constructs automorphic

L-functions $L(s)$ by taking products of appropriate L-functions of GL_1. The Hasse-Weil zeta function of an elliptic curve over K is a special case of this construction. By taking $K = F(t)$ and $f(x) = x+t/x$ they prove the Kloosterman conjecture over a function field. The paper explains the connection of the Kloosterman conjecture to Ramanujan graphs.

According to the Langlands philosophy, L-functions of complex automorphic representations of GL_n over a function field K should be a motive attached to an ℓ-adic representations of $Gal(\bar{K}/K)$. This is known only for GL_2 from Drinfeld. By class field theory, L-functions of GL_1 over K are also L-functions of degree one representations of $Gal(\bar{K}/K)$. So, this paper contributes to Langlands' philosophy by taking advantage of motivic thinking.

3.5. **Eigenvalues of a Laplacian.** Chung has many papers on graphs generated by relations over finite fields. *Spanning trees in subgraphs of lattices* considers the combinatorial Laplacian of a graph and an induced subgraph of a graph.

The classical *Matrix-tree Theorem* says the number of spanning trees of a graph is proportional to the product of nonzero eigenvalues of the combinatorial Laplacian. This paper relates the zeta function of a graph to the heat kernel and the spanning trees of the graph.

Applications arise from induced subgraphs of a lattice graph. Let S be a connected induced subgraph of a 2-dimensional lattice graph. It shows the number of spanning trees $\tau(S)$ satisfies

$$ce^{c_1\ |S|-c_2|\partial S|} \le \tau(S) \le c'e^{c_1\ |S|+c_3\ |\partial S|^2/|S|} \tag{3.1}$$

with constants c_1, c_2 and c_3 depending only on the host graph (independent of S).

3.6. **Average values of Zeta functions and elliptic surfaces.** Rosen in *Average Rank for Elliptic Curves and a Conjecture of Nagao* discusses work with Silverman on the average rank problem for elliptic curves. Consider a proper map $\pi : E \to \mathbb{P}^1_t$ over $\mathbb{Q}$. Assume all but finitely fibers $E_t = \pi^{-1}(t)$ are elliptic curves.

Their E is a desingularization of an elliptic surface defined by the equation

$$y^2 + a_1(T)xy + a_3(T)y = x^3 + a_2(T)x^2 + a_4(T)x + a_6(T)$$

with the $a_i(T) \in \mathbb{Z}[T]$ and discriminant $\Delta(T) \neq 0$.

For $t \in \mathbb{Z}$ and $\Delta(t) \neq 0$,

$$E_t: \quad y^2 + a_1(t)xy + a_3(t)y = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t)$$

is an elliptic curve over $\mathbb{Q}$. For each prime p, let $E_t^{(p)}$ be the reduction of E_t at p. If p does not divide $\Delta(t)$, set

$$a_p(E_t) = p + 1 - \#E_t^{(p)}(\mathbb{F}_p).$$

Otherwise define $a_p(E_t)$ to be 0.

Note: $a_p(E_t)$ only depends on the congruence class of t modulo p. Following Nagao they define the average value as $A_p(E) = \frac{1}{p}\sum_{t=1}^{p} a_p(E_t)$.

Nagao conjectured how $A_p(E)$ relates to the rank of the group of $\mathbb{Q}$ sections $\sigma : \mathbb{P}^1 \to E$ to π. The Rosen-Silverman analytic version considers $F(E/\mathbb{Q}, s) = \sum_p -A_p(E)\log(p)p^{-s}$. By a theorem of Deligne, the numbers $A_p(E)$ are bounded. So, the Dirichlet series $F(E/\mathbb{Q}, s)$ converges for $\Re(s) > 1$. They conjecture

$$\lim_{s\to 1^+}(s-1)F(E/\mathbb{Q}, s) = \mathrm{rank}E(\mathbb{Q}(T)).$$

In particular, Nagoa's conjecture follows from a case of Tate's conjecture relating the rank of groups of algebraic cycles to the poles of certain L-series.

4. A short dedication to the work of Bernard Dwork

Bernie was a complicated man. No simple view of him can encapsulate all his moods. One consistent aspect was a strong loyalty to his students and mentors. Michael Rosen alludes to this from his association with Ken Ireland at Brown (§4.1). Bernie's students reciprocated that loyalty, by being ever aware of their mathematical and personal debt to him. Alan Adolphson gives a clear illustration in §4.3. Bernie worked often by accumulated evidence from a deep example, rather than general theory. Returning to examples that motivated him still works for young researchers. Daqing Wan's paper (see §3.1) illustrates that. So does the statement from Pierre Debes (§4.2). Debes did not know Bernie well, except for being present when Bernie spent two weeks at UC Irvine just before he died.

4.1. **Michael Rosen: Dwork's relation to his students.** Bernie Dwork was Ken Ireland's thesis advisor. Ken's thesis appeared in the Amer. J. Math. 1966: On the Zeta Function of an Algebraic Variety. Ken died suddenly in 1992. Thereafter Bernie inquired often after the well being of his widow, Noel Ireland, and his family. Even at Seattle, when he was so very ill, he sought me out to ask about Ken's family.

4.2. **Pierre Debes: Dwork's role in G-Functions.** B. Dwork has renown contributions to the theory of G-functions and G-modules. [Editor: See the comment at the end of §4.3.]

The definition G-function starts with power series in x having coefficients in a number field and satisfying a linear differential equation with coefficients in $\bar{\mathbb{Q}}(x)$. The key G function property is that for some N, N^m bound the the mth coefficient denominator. Algebraic functions are typical G-functions.

Siegel started investigations into the arithmetic of G-function values. For one, G-functions have properties resembling the conclusions of Hilbert's irreducibility theorem applied to algebraic functions. Applying Siegel's method requires refined p-adic estimates for determinantal quantities in values of functions (and their derivatives). The Dwork-Robba theorem is such a tool. It was a major ingredient in Bombieri's completion of Siegel's program.

Generalizing G-functions is a notion of G-module (or G-operator). First it is a module with an underlying differential operator (having coefficients in $\bar{\mathbb{Q}}(x)$). The key defining property is that the module has a basis of G-function solutions $\mathbf{y} = (y_1, \ldots, y_d)$, expanded in power series around a generic point. To be precise requires a *size* of modules. Several proposed sizes have produced corresponding definitions of G-operators. Some of these sizes give equivalent modules. There remain open problems about other possible definitions. Dwork persistently contributed to the analysis of these proposed definitions.

Let v run over places of a number field containing the coefficients of the involved power series. Consider the v-adic radius of convergence r_v of $\mathbf{y}$ (at generic points), for each place v. Bombieri proposed that the operators would be of arithmetic type $\sum_v \max(0, -\log(r_v))$ finite. A strengthened condition is that all but finitely many radii r_v equal 1. There is also the notion of *globally nilpotent operators* studied by Katz: the p-curvatures should be nilpotent for all but finitely many primes p. Galochkin introduced another definition using iterates of the differential operator.

Finally there are the operators coming from the geometry (see §4.3). Although appearing classically, it is difficult to find a precise definition in the literature for this. In his book on G-functions, Y. André defines them as iterate extensions of sub-quotients of Gauss-Manin connexions attached to algebraic varieties. That is, the definition is *motivic*.

The Bombieri-André Theorem says the Bombieri and Galochkin notions coincide. The Dwork-Robba theorem revealed a basic tool. Dwork recently improved on this equivalence by involving p-curvatures. Based on Katz, the Bombieri-Galochkin operators are proved globally nilpotent in the weak form (for v of density 1). The strong form (for almost all v) is still open.

Grothendieck's conjecture from 30 years ago is that globally nilpotent in the weak sense implies the differential equations come from geometry (see §3.1). From this, all preceding notions actually coincide. This phrasing appears in the literature as the Bombieri-Dwork conjecture.

Bernie Dwork visited UC Irvine in January 1998. One from his two talks was on G-operators. He gave examples (involving the hypergeometric differential equation) of explicitly computing the (Bombieri) size of the operator. He mentioned the significance of Chudnovsky's theorem. This says it is sufficient for an operator to be a G-operator (in the sense of Bombieri and/or Galochkin) if there is a solution $(y_1, \dots, y_d)$ whose entries have these properties.

- They are G-functions with coefficients in $\bar{\mathbb{Q}}$.
- They are linearly independent over $\bar{\mathbb{Q}}(x)$.

This result and all others from the theory of G-functions and G-operators appear in the book Dwork wrote with G. Gerotto and F. Sullivan. [Editor: See Conjecture 4.1 for continuation of this topic.]

4.3. **Alan Adolphson: Dwork's final conjecture.** Perhaps because of his early training as an engineer, Bernie respected how differential equations capture mathematical behavior. His most celebrated result was the rationality of the zeta function of an algebraic variety. For this he received the Cole Prize in 1962. Still, his greatest influence may be in the application of differential equations to problems in number theory. His ideas are too too broad for this exposition. I only discuss those influencing my work.

To my knowledge, differential equations first appear in Bernie's work in [9]. Proving the rationality of an algebraic varieties zeta function involved constructing a Frobenius operator on certain spaces of p-adic power series satisfying growth conditions. Bernie did not associate cohomology spaces to the variety as expected by the Weil Conjectures. In [9], he constructed a complex whose terms were spaces of p-adic power series and whose boundary maps came from differential operators on those spaces. The Frobenius action on that complex, and hence on its cohomology, gives the zeta function.

An immediate problem arose. Even for smooth varieties, no one knew if the cohomology of this complex was finite dimensional. This gave a basic question. Given a differential operator on a space of p-adic analytic functions, is its cokernel finite-dimensional? Finiteness of the kernel is usually easy. So the question is to determine if the differential operator has finite index (= $\dim \text{kernel} - \dim \text{cokernel}$). This has motivated much research, including part of my thesis [1]. Robba studied this extensively (see his bibliography in [16]). Recently, Christol and Mebkhout [6, 7, 8] have made progress. I understand de Jong's use of resolution of singularities

in characteristic p implies finite-dimensionality of Dwork's cohomology. I haven't, however, seen the details.

Bernie describes a more subtle application of p-adic differential equations in [10]. Suppose a variable λ with values in a finite field of characteristic p parametrizes a smooth family. Dwork's p-adic cohomology spaces then depend on lifting the family to characteristic 0. So the cohomology classes depend analytically on the lifted parameter. Differentiating Dwork's cohomology classes with respect to the (lifting of) the parameter produces a differential equation satisfied by the cohomology classes. Dwork recognized this as the p-adic analogue of the classical Fuchs-Picard differential equation for the corresponding family over $\mathbb{C}$. For example, consider the family $y^2 = x(x-1)(x-\lambda)$. Dwork's p-adic cohomology classes (2nd kind differentials) satisfy the classical Gaussian hypergeometric differential equation

$$\lambda(1-\lambda)z'' + (1-2\lambda)z' - \tfrac{1}{4}z = 0.$$

The λ here, however, is a p-adic variable.

Bernie was able to identify his cohomology spaces with solution spaces of p-adic differential equations [11]. The action of Frobenius on the cohomology spaces then induces an F-crystal structure on the solution space of a differential equation. Thus, these solutions have radius of convergence one. (Determining p-adic radius of convergence is difficult. Usual results on analytic continuation in the complex case fail p-adically.) This allowed him to analytically continue certain ratios of solutions to a larger p-adic domain. The result gave explicit formulas for eigenvalues of Frobenius as special values of these analytically continued ratios.

Much of my thesis [2] depended on [11] and the related [12]. Specifically, I used the relation (of Ihara [25], worked out by Morita [26] for the principal congruence subgroup of level two) between Hecke polynomials and the eigenvalues of Frobenius on H^1 of elliptic curves over a finite field. Applying Dwork's explicit formulas for these eigenvalues, I constructed a p-adic cohomology space with a Frobenius action having a Hecke polynomial as its characteristic polynomial. This gave p-adic information about eigenvalues of Hecke operators. Robba[28] carried out a similar analysis for eigenvalues of Frobenius on H^1 of Kloosterman sums. From this I gave a p-adic proof of the equidistribution of angles of Kloosterman sums[3].

Recall: The phrase, *arises in algebraic geometry* applied to a differential equation means the differential equation is the Picard-Fuchs equation using the Gauss-Manin connection on a smooth family of algebraic varieties. [Editor: Check the motivic comments in §4.2 and §3.1.] That is, it comes from differentiating differential forms representing cohomology classes with respect to the variables of the parameter space. Over $\mathbb{C}$ it is classical these differential equations have regular singular points.

In characteristic p, however, exponential sums on a variety appear. In 1974 Bernie found a new behavior in the differential equation describing variation of p-adic cohomology in the family of Kloosterman sums. He showed it is the p-adic analogue of the classical Bessel equation [13]. In particular, it has an irregular singularity, the first such example. Later, Sperber and I [4, 5] extended many of these results on Kloosterman sums to *twisted* (involving multiplicative *and* additive characters) Kloosterman sums.

Bernie continued working on p-adic differential equations, producing three books [14, 15, 19] (the latter joint with Gerotto and Sullivan). One question dominated his later work. It was to give a p-adic characterization of those differential equations

coming from geometry. [17, 18] were written after the onset of his illness. The solutions of such differential equations are all G-functions, and all known G-functions are solutions of such differential equations.

Conjecture 4.1 (Dwork)**.** There is a G-function characterization of the equations arising from geometry.

[19] gives an introduction to this question while covering many topics in the theory of p-adic differential equations. It is fascinating that disparate mathematical ideas produce such beautiful and fruitful interactions.

References

[1] A. Adolphson, An index theorem for p-adic differential operators, Trans. Amer. Math. Soc. **216**(1976), 279–293
[2] ———, A p-adic theory of Hecke polynomials, Duke Math. J. **43**(1976), 115–145
[3] ———, On the distribution of angles of Kloosterman sums, J. reine angew. Math. **395**(1989), 214–220
[4] A. Adolphson and S. Sperber, Twisted Kloosterman sums and p-adic Bessel functions, Amer. J. Math. **106**(1984), 549–591
[5] ———, Twisted Kloosterman sums and p-adic Bessel functions II: Newton polygons and analytic continuation, Amer. J. Math. **109**(1987), 723–764
[6] G. Christol and Z. Mebkhout, Sur le théorème de l'indice des équations différentielles p-adiques I, Ann. Inst. Fourier **43**(1993), 1545–1574
[7] ———, Sur le théorème de l'indice des équations différentielles p-adiques II, Ann. of Math. **146**(1997), 345–410
[8] ———, Sur le théorème de l'indice des équations différentielles p-adiques III, to appear
[9] B. Dwork, On the zeta function of a hypersurface, Publ. Math. I. H. E. S. **12**(1962), 5–68
[10] ———, On the zeta function of a hypersurface II, Ann. of Math. **80**(1964), 227–299
[11] ———, p-Adic cycles, Publ. Math. I. H. E. S **37**(1969), 27–115
[12] ———, On Hecke polynomials, Inv. Math. **12**(1971), 249–256
[13] ———, Bessel functions as p-adic functions of the argument, Duke Math. J. **41**(1974), 711–738
[14] ———, *Lectures on p-adic differential equations*, Grundlehren der mathematischen Wissenschaften no. 253, Springer-Verlag, 1982
[15] ———, *Generalized hypergeometric functions*, Oxford University Press, 1990
[16] ———, Work of Philippe Robba, in p-adic Analysis, Lecture Notes in Math. no. 1454, 1–10, Springer-Verlag, 1990
[17] ———, On the size of differential modules, Duke Math. J. **96**(1999), 225–239
[18] ———, Cohomology of singular hypersurfaces, Pacific J. Math., to appear
[19] B. Dwork, G. Gerotto, and F. Sullivan, *An Introduction to G-functions*, Princeton University Press, 1994
[20] M. Fried, R. Guralnick and J. Saxl, *Schur covers and Carlitz's conjecture*, Israel J. **82** (1993), 157–225.
[21] M. Fried, *Global construction of general exceptional covers, with motivation for applications to encoding*, Cont. Math., vol. 168, pp. 69–100, AMS, Rhode Island, Editors G.L. Mullen an P.J. Shiue, 1994, Finite Fields: Theory, applications and algorithms.
[22] ———, *Introduction to modular towers: Generalizing the relation between dihedral groups and modular curves*, Proceedings AMS-NSF Summer Conference, vol. 186, 1995, Cont. Math series, Recent Developments in the Inverse Galois Problem, pp. 111–171, http://www.math.uci.edu/~mfried/#mt.
[23] ———, *Separated variables polynomials and moduli spaces*, Number Theory in Progress (Berlin-New York) (J. Urbanowicz K. Gyory, H. Iwaniec, ed.), Walter de Gruyter, Berlin-New York (Feb. 1999), Proceedings of the Schinzel Festschrift, Summer 1997, pp. 169–228, http://www.math.uci.edu/~mfried/#math.
[24] N. Katz and J. Tate, *B. Dwork 1923–1998*, Notices of the AMS **46, 3**, 338–343.
[25] Y. Ihara, Hecke polynomials as congruence zeta functions in the elliptic modular case, Ann. of Math. **85**(1967), 267–295

[26] Y. Morita, Hecke polynomials of modular groups and congruence zeta functions of fibre varieties, J. Math. Soc. Japan **21**(1969), 617–637
[27] P. Müller, *Primitive monodromy groups of polynomials*, Proceedings of the Recent developments in the Inverse Galois Problem conference, vol. 186, 1995, AMS Cont. Math series, pp. 385–401.
[28] P. Robba, Symmetric powers of the p-adic Bessel equation, J. reine angew. Math. **366** (1986), 194–220
[29] H. Stichtentoth, Die Hasse-Witt Invariante eines Kongruenzfunktionenkörpers, Arch. Math. **33** (1979), 357–360.

UC Irvine, Irvine, CA 92697, USA
E-mail address: mfriedmath.uci.edu