EXCEPTIONAL COVERS AND DAVENPORT PAIRS

MICHAEL D. FRIED

This talk is part of a project whose apt title would be *Determining Chow motives from Weil vectors*. Weil vectors refers to the coefficients of a Poincaré series as in the zeta function of a variety over a finite field.

This talk aims to present tools for formulating attractive general problems on determining a virtual variety with zeta function data from an attached Poincaré series. Twenty years ago it might have been too hard to tackle such problems. Several tools, however, including *Galois Stratification* and the *ring of Chow Motives* (over a finite field or a number field), can relate specific work of many combinatorialists and number theorists to general structure theorems. As this is a big topic, this first talk establishes the subject in the most practical way possible.

1. Beginning stages in presenting the topic

Here is a list of focal points for establishing preliminary research directions.

- Illustrating practical examples of relations among Weil vectors.
- Listing mature tools ready for attacking general problems.
- Listing basic research problems going beyond what we presently know.

This talk is heavy on the first item. It uses *Exceptional covers* and *Davenport pairs* as long-standing topics from equations over finite fields.

The sophisticated tools I have in mind are *Galois stratification* from M. Fried, Solving diophantine problems over all residue class fields of a number field ..., *Annals Math.* **104** (1976), 203–233 and Fried-Jarden, Field Arithmetic, *Springer Ergebnisse II* **Vol 11** (1986) Chaps. 24-26; and rings of *Chow Motives* as produced by Manin, and developed more recently by Gillet-Soulé. The model for cooperation between these tools appears in the paper by Denef-Loeser: Definable sets, motives and p-adic integrals, to appear this year in the Journal of the AMS.

This abstract ends with briefly stated future goals that I hope to enhance in further talks. The problems and results of this talk show we have sufficient empirical data to test general difficulties and to formulate general problems.

2. Consider your favorite equation: $F(\boldsymbol{u}, z) = 0$

Example: If you were Dwork, you would have chosen, as do many coding theorists, $z^p - z = H(\boldsymbol{u})$. Throughout q is a power of a prime p. Use $\overline{\mathbb{F}}_q$ for an algebraic closure of the finite field $\mathbb{F}_q$.

Suppose you like to count numbers of solutions $N_{q,t}$ over $\mathbb{F}_{q^t}$, for all t. Maybe, your equation has coefficients in $\mathbb{Z}$. You might be interested in counting solutions $\tilde{N}(q, t, n)$, over $W_{q,t}/p^n$, that lift to the Witt vectors $W_{q,t}$ of $\mathbb{F}_{q^t}$. This gives sets

Date: January 25, 2001.

Presented at Oberwolfach meeting on Finite Fields, Jan. 2001. Travel support for Fried came from NSF #DMS-9970676, funds from Ecole Normal Superier and Max Planck Institute.

$\mathcal{N}_{q,F} = \{N_{q,t}\}_{t=1}^{\infty}$ and $\bar{\mathcal{N}}_{q,t,n} = \{\bar{N}_{q,t,n}\}_{1\le t,1\le n}$. The latter is the problem driving the Denef-Loeser paper. Many famous variants on these problems also produce *Weil vectors* (Poincaré series). Rgard any such collection of counting numbers as a Weil vector attached to a diophantine statement. For simplicity, we concentrate on problems over one finite field $\mathbb{F}_q$.

To use your favorite equation expertise well, you often substitute for z to consider $F(\boldsymbol{u}, h(x)) = 0$. Think $h(x) = z$ with h a polynomial or rational function. Now we make an assumption on pairs of such substitutions from different polynomials h and g. Suppose for $t \in \chi = \chi_{h,g}$ and for each $z \in \mathbb{F}_{q^t}$,

(2.1) $h(x) - z = 0$ has the same number of solutions as does $g(y) - z = 0$.

Then $N_{q,t}(F(\boldsymbol{u}, h)) = N_{q,t}(F(\boldsymbol{u}, g))$ for $t \in \chi$. Let $\chi_{F(\boldsymbol{u},h),F(\boldsymbol{u},g)}$ be the set of t where they are equal. Then, $\chi_{F(\boldsymbol{u},h),F(\boldsymbol{u},g)} \supset \chi_{h,g}$. We'd like to put structure in the counting sets $\mathcal{N}_{q,F}$, etc. so relations as these get automatic recognition. The emphasis is that such relations among Weil vectors don't depend on your choice of *favorite equation*.

My goal is to convince you it is possible to analyze relations like (2.1) and feasible to consider the set $\chi_{h,g}$ with savvy.

3. Davenport pair and exceptional cover definitions

Use $\mathcal{V}_h(L)$ for the range of the polynomial h on the field L. Let $\chi_{h,g}$ be the characteristic set $\{t \mid \mathcal{V}_h(\mathbb{F}_{q^t}) = \mathcal{V}_g(\mathbb{F}_{q^t})\}$. Don't assume (2.1) holds. Call (h, g) an S(trong)D(avenport)P(air) if $\chi_{h,g} = \mathbb{N}^+$. Call it a DP if $\chi_{h,g}$ is infinite. Recall: $h \in \mathbb{F}_q[x]$ is *exceptional* if the map by h on $\mathbb{F}_{q^t}$ is one-one for infinitely many t. Denote the set of these exceptional t by E_h.

Suppose (h, g) is a DP and h_1 and g_1 are exceptional. The expression $h(h_1)$ denotes the composition of h and h_1. Then, $\chi_{h(h_1),g(g_1)}$ contains $E_{h_1} \cap E_{h_2} \cap \chi_{h,g}$. You have to know something about $E_{h_1}, E_{h_2}, \chi_{h,g}$ to say their intersection is infinite. That is the main emphasis of this talk: Showing we can say such things with considerable understanding and generality. A corollary of Thm. 4.2 says $E_{h_1} \cap E_{h_2} \cap \chi_{h,g}$ is automatically infinite if *indecomposable* h has degree prime to p. Recall: h is indecomposable if it is not a composition of polynomials of lower degree. It is well-known that $(\deg(h), p) = 1$ implies indecomposability of h over $\mathbb{F}_q$ is equivalent to indecomposability over $\bar{\mathbb{F}}_q$.

4. Nature of the characteristic sets for Davenport Pairs

All the characteristic sets used above, like those in $E_{h_1} \cap E_{h_2} \cap \chi_{h,g}$, are unions of *Frobenius progressions*. These are unions of arithmetic progressions with modulus some integer N, where if the progression P_a of positive integers congruent to a is included, so is P_{ak} for each k prime to N.

A corollary of Galois Stratification, which applies to compute characteristic sets, is they are unions of Frobenius progressions in great generality. Computing them, however, is one thing. Finding their refined structure is another.

A work with W. Aitkin and L. Holt, titled *Davenport Pairs over finite fields* (a preprint near completion), considers a question about this structure for DPs. Much of this lecture is an example result. Assume (h, g) is a DP. A piece of geometry about DPs plays an important role in the main result.

Lemma 4.1. *If h is not exceptional over $\mathbb{F}_{q^t}$ and $\chi_{h,g}$ is infinite, then*

$$V_{h,g} = \{(x,y) \in \bar{\mathbb{F}}_q \times \bar{\mathbb{F}}_q \mid h(x) = g(y)\}$$

is reducible over $\mathbb{F}_q^t$ for $t \in \chi_{h,g}$.

Proof. The DP hypothesis already shows the number of points M_t on $V_{h,g}$ is at least q^t. Let N_t be the number of absolutely irreducuble components over $\mathbb{F}_{q^t}$. The regular analog of the Cebotarev density theorem says there are approximately Bq^t (with B a constant independent of t) elements of $\mathcal{V}_h(\mathbb{F}_{q^t})$ achieved with multiplicity 2. Then $M_t \geq q^t(B+1)$. So, either $N_t \geq 2$ or h is one-one. ◻

For $h \in \mathbb{F}_q[x]$, let $x_1, \ldots, x_n$ be the zeros of $h(x) - z$ in some algebraic closure of $\mathbb{F}_q(z)$. An old tradition writes the splitting field of $h(x) - z$ over $\mathbb{F}_q(z)$ as $\Omega_h = \mathbb{F}_q(x_1, \ldots, x_n, z)$. Similarly, $\Omega_g = \mathbb{F}_q(y_1, \ldots, y_m, z)$. Two papers provide the history and tools for considering SDPs:

- The definition field of function fields and a problem in the reducibility of polynomials ..., *Ill. Journal of Math.* **17**, (1973), 128–146.
- Variables Separated Polynomials and Moduli Spaces, No. Theory in Progress, eds. K.Gyory, H.Iwaniec, J.Urbanowicz, proceedings of the Schinzel Festschrift, Summer 1997 Zakopane, Walter de Gruyter, Berlin-New York (Feb. 1999), 169–228. (at www.math.uci.edu$\tilde{\text{m}}$fried/#math).

The controlling factor in distinguishing these with the results with Aitken-Holt is considering DPs. The difference is that between the field $\bar{\mathbb{F}}_q \cap \Omega_h\Omega_g = \hat{\mathbb{F}}_q$ and $\mathbb{F}_q$. Precisely: Consider for each t the elements G_t of $G(\Omega_h\Omega_g/\mathbb{F}_{q^t})$ whose restriction to $\hat{\mathbb{F}}_q$ is the q^t power map. Then, (h,g) is a DP over $\mathbb{F}_{q^t}$ for exactly those t where

(4.1) each element in G_t fixes an element of $x_1, \ldots, x_n$ if and only if it fixes an element of $y_1, \ldots, y_m$.

Theorem 4.2. *Suppose* $(\deg(h), p) = 1$ *and h is indecomposable and not exceptional. Then, $g = g_1(g_2(y))$, a composition over $\mathbb{F}_q$ with* $\deg(h) = \deg(g_1)$ *and* $\chi_{h,g_1} = \mathbb{N}^+$. *Also,* (2.1) *holds for (h, g_1).*

A brief survey of ingredients. Find g_2 (and therefore g_1) as given by $\Omega_h \cap \mathbb{F}_{q^t}(y_1) = \mathbb{F}_{q^t}(g_2(y_1))$. So $\Omega_h = \Omega_{g_1}$ and (h, g_1) is a DP. Replace g_1 by g. This gives two permutation representations T_h and T_g of $G(\Omega_h) = \hat{G}$. Let $n = \deg(h)$ (again, it is prime to p). Ramification over ∞ gives σ_∞, an n-cycle in both representations. This shows the degrees of h and g are equal.

A basic Lemma is in the paper, On a conjecture of Schur, *Mich. Math. Journal* **17** (1970), 41–55. It says if T_h and T_g are inequivalent, with h indecomposable, then T_h is double transitive. Consider the permutation representation of $G_{t,h} = G(\omega_h/\mathbb{F}_{q^t}(z))$ on the pairs $(x_i, y_j) \mapsto (i,j)$. The number of orbits equals the classical inner product of the permutation representations. We know this is at least two, with $T_h = \mathbf{1} \oplus V$ and V an irreducible module for the $G_{t,h}$ action. To be at least two requires $T_g = \mathbf{1} \oplus V$. The representations are equivalent and (2.1) holds.

Suppose $P = \{1, i_2, \ldots, i_k\}$ is the $G(x_1)$ orbit on y_1. If u translates of this contain 1, then $(n-1)u = k(k-1)$. So the two factors have different degrees and must be over $\mathbb{F}_q$: (h, g_1) is an SDP. The critical point: Though we did our analysis over $\mathbb{F}_{q^t}$, we now know the factorization of $h(x) - g(y)$ is actually over $\mathbb{F}_q$. The equivalence of representations holds over $\mathbb{F}_q$. ◻

5. Nontrivial examples of Davenport pairs

Under the indecomposable and prime to p assumption, we know much about the SDPs (h,g). From the classification of finite simple groups —as in the Schinzel vol. paper —we have the following. Their geometric monodromy group must be between $\mathrm{PGL}_w(\mathbb{F}_r)$ and $\mathrm{PSL}_w(\mathbb{F}_r)$ for some finite field $\mathbb{F}_r$ and integer w (excluding $w = 11$ which comes from an Hadamard design). Further, except for $w = 11$, the representations are respectively on points and hyperplanes. The Schinzel vol. paper uses examples of Anhyankar to find infinitely many SDPs over every finite field $\mathbb{F}_r$.

6. Future goals

Generalizing definitions of SDPs, DPs and Exceptional polynomials apply to a general curve cover or even covers of varieties of higher dimension. As in Denef-Loeser, any Galois stratification maps into the ring of Chow Motives over $\mathbb{F}_q$.

Problem 6.1. Figure what general exceptional covers and Davenport pairs generate of all relations in the ring of Chow Motives over $\mathbb{F}_q$.

This imprecise question will get refinement in later talks and papers.

Consider exactly what to do about finding the nature of the image of the Grothendieck group on smooth schemes. The paper, Global construction of general exceptional covers, with motivation for applications to coding, *G.L. Mullen an P.J. Shiue, Finite Fields: Theory, applications and algorithms, Cont. Math.* **168** (1994), 69–100 has two goals related to this talk.

- It produces general exceptional covers in great abundance over any finite field, based only on an equivalent group theory condition.
- It poses (in §3) the relation between general exceptional covers and *median value curves*.

A median value curve is one with exactly $q^t + 1$ points over $\mathbb{F}_{q^t}$ for infinitely many t. One proposition shows, for any (projective, nonsingular) curve, the values of t where it has median value form a union of Frobenius progressions. That same diophantine approximation argument works in great generality.

Proposition 6.2. *Let X be a Chow motive over $\mathbb{F}_q$ with underlying space in the image of the Grothendieck group of projective nonsingular varieties over $\mathbb{F}_q$. Then, the set of t, χ_X, where its Weil vector is 0 is a union of Frobenius progressions.*

Galois stratification reverts analysis to a Cebotarev density theorem type result. You can pull back any Galois stratification over a cover of the underlying manifold under the equivalences the papers above (including Denef-Loeser) use.

Problem 6.3. Does de Jong's covering replacement for resolution of singularities suffice to replace the lack of resolution of singularities in positive characteristic? In particular, can we apply Galois stratification to remove in Prop. 6.2 the hypothesis that its underlying virtual space is a virtual smooth projective scheme?

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