Variables Separated Equations and Finite Simple Groups

2PM, April 6, 2010: Mike Fried, Emeritus UC Irvine [UmSt]

April 7, 2010

1. Algebraic equations in separated variables:
$$\{(x,y)|f(x)-g(y)=0\}.$$

Variables Separated Equations and Finite Simple Groups

2PM, April 6, 2010: Mike Fried, Emeritus UC Irvine [UmSt]

April 7, 2010

1. Algebraic equations in separated variables:
$$\{(x,y)|f(x)-g(y)=0\}.$$
2. Normalize for a projective nonsingular algebraic curve $X_{f,g}$ with two projections to the (Riemann sphere) z-line $\mathbb{P}^1_z=\mathbb{C}\cup\{\infty\}$:
$$\mathrm{pr}_x : X_{f,g}\to\mathbb{P}^1_x \text{ and } \mathrm{pr}_y : X_{f,g}\to\mathbb{P}^1_y;$$
$$f:\mathbb{P}^1_x\to\mathbb{P}^1_z \text{ and } g:\mathbb{P}^1_y\to\mathbb{P}^1_z.$$

We use 2 problems from 60s solved by the *monodromy method*, refers to 2 genus 0 problems related to John Thompson

1. *Davenport's*: Suppose $f, g \in K[x] \setminus K$ has exactly the same ranges on almost all residue fields:
Related in obvious way – $f(x) = g(ax + b)$, a, b constant?
[Sc71], [Fr73].

We use 2 problems from 60s solved by the *monodromy method*, refers to 2 genus 0 problems related to John Thompson

1. *Davenport's*: Suppose $f, g \in K[x] \setminus K$ has exactly the same ranges on almost all residue fields:
Related in obvious way – $f(x) = g(ax + b)$, a, b constant?
[Sc71], [Fr73].
2. *Schinzel's*: Suppose $f(x) - g(y)$ reducible:
Are f, g related in an obvious way?

We use 2 problems from 60s solved by the *monodromy method*, refers to 2 genus 0 problems related to John Thompson

1. *Davenport's*: Suppose $f, g \in K[x] \setminus K$ has exactly the same ranges on almost all residue fields:
   Related in obvious way – $f(x) = g(ax + b)$, a, b constant?
   [Sc71], [Fr73].
2. *Schinzel's*: Suppose $f(x) - g(y)$ reducible:
   Are f, g related in an obvious way?
3. *1st Genus 0 Problem*: What are possible monodromy groups G_f (f a polynomial or rational function)? [Fr05a, §7.2]

We use 2 problems from 60s solved by the *monodromy method*, refers to 2 genus 0 problems related to John Thompson

1. *Davenport's*: Suppose $f, g \in K[x] \setminus K$ has exactly the same ranges on almost all residue fields:
   Related in obvious way – $f(x) = g(ax+b)$, a, b constant?
   [Sc71], [Fr73].
2. *Schinzel's*: Suppose $f(x) - g(y)$ reducible:
   Are f, g related in an obvious way?
3. *1st Genus 0 Problem*: What are possible monodromy groups G_f (f a polynomial or rational function)? [Fr05a, §7.2]
4. *2nd Genus 0 problem*: Relate characters of the Monster simple group and genus 0 modular curves.

Summary

Indecomposability condition: We will assume f is *not* a composition of lower degree polynomials.

1. **Part I**: Davenport and Schinzel Problems

Summary

Indecomposability condition: We will assume f is *not* a composition of lower degree polynomials.

1. **Part I**: Davenport and Schinzel Problems
2. - §I.A. The dihedral group with observations
   - §I.B. Splitting variables
   - §I.C. Introducing Galois groups
   - §I.D. Translating Davenport to Group Theory

Summary

Indecomposability condition: We will assume f is *not* a composition of lower degree polynomials.

1. **Part I**: Davenport and Schinzel Problems
2. - §I.A. The dihedral group with observations
   - §I.B. Splitting variables
   - §I.C. Introducing Galois groups
   - §I.D. Translating Davenport to Group Theory
3. **Part II**: Primitivity, cycles, Simple Group Classification

Summary

Indecomposability condition: We will assume f is *not* a composition of lower degree polynomials.

1. **Part I**: Davenport and Schinzel Problems
2. - §I.A. The dihedral group with observations
   - §I.B. Splitting variables
   - §I.C. Introducing Galois groups
   - §I.D. Translating Davenport to Group Theory
3. **Part II**: Primitivity, cycles, Simple Group Classification
4. - §II.A. Translating Primitivity for $f : X \to \mathbb{P}^1_z$
   - §II.B. Further Group translation of Davenport
   - §II.C. Double Transitivity and Difference sets

Summary

Indecomposability condition: We will assume f is *not* a composition of lower degree polynomials.

1. **Part I**: Davenport and Schinzel Problems
2.
   - §I.A. The dihedral group with observations
   - §I.B. Splitting variables
   - §I.C. Introducing Galois groups
   - §I.D. Translating Davenport to Group Theory
3. **Part II**: Primitivity, cycles, Simple Group Classification
4.
   - §II.A. Translating Primitivity for $f : X \to \mathbb{P}^1_z$
   - §II.B. Further Group translation of Davenport
   - §II.C. Double Transitivity and Difference sets
5. **Part III**. What groups give Davenport pairs and how?

Summary

Indecomposability condition: We will assume f is *not* a composition of lower degree polynomials.

1. **Part I**: Davenport and Schinzel Problems
2. - §I.A. The dihedral group with observations
   - §I.B. Splitting variables
   - §I.C. Introducing Galois groups
   - §I.D. Translating Davenport to Group Theory
3. **Part II**: Primitivity, cycles, Simple Group Classification
4. - §II.A. Translating Primitivity for $f : X \to \mathbb{P}^1_z$
   - §II.B. Further Group translation of Davenport
   - §II.C. Double Transitivity and Difference sets
5. **Part III**. What groups give Davenport pairs and how?
6. - §III.A. Projective Linear Groups
   - §III.B. Punchlines on Davenport (f indecomposable)
   - §III.C. From III.B, Hints at the *Genus 0 Problem*

Regard any rational function f in w – degree m – as a cover of a complex sphere by a complex sphere:

$$f : \mathbb{P}^1_w = \mathbb{C}_w \cup \{\infty\} \to \mathbb{P}^1_z = \mathbb{C}_z \cup \{\infty\}.$$

Then, f has finitely many (branch) points, z', over which it *ramifies*: Instead of m distinct values of w, there are fewer. Designate branch points by $\{z_1, \dots, z_r\} = \boldsymbol{z}$.

- *Calculus*: Uses $T_m(\cos(\theta)) = \cos(m\theta)$, with $T_m(w) = z$: mth *Chebychev* polynomial.

Regard any rational function f in w – degree m – as a cover of a complex sphere by a complex sphere:

$$f : \mathbb{P}^1_w = \mathbb{C}_w \cup \{\infty\} \to \mathbb{P}^1_z = \mathbb{C}_z \cup \{\infty\}.$$

Then, f has finitely many (branch) points, z', over which it *ramifies*: Instead of m distinct values of w, there are fewer. Designate branch points by $\{z_1, \dots, z_r\} = \boldsymbol{z}$.

- *Calculus*: Uses $T_m(\cos(\theta)) = \cos(m\theta)$, with $T_m(w) = z$: mth *Chebychev* polynomial.
- *Goal*: Express $\cos(\theta)^m$ as a sum of $\cos(k\theta)$ terms, $0 \le k \le m$. So, we can integrate any polynomial in $\cos(\theta)$.

Regard any rational function f in w – degree m – as a cover of a complex sphere by a complex sphere:

$$f : \mathbb{P}^1_w = \mathbb{C}_w \cup \{\infty\} \to \mathbb{P}^1_z = \mathbb{C}_z \cup \{\infty\}.$$

Then, f has finitely many (branch) points, z', over which it *ramifies*: Instead of m distinct values of w, there are fewer. Designate branch points by $\{z_1, \dots, z_r\} = \boldsymbol{z}$.

- *Calculus*: Uses $T_m(\cos(\theta)) = \cos(m\theta)$, with $T_m(w) = z$: mth *Chebychev* polynomial.
- *Goal*: Express $\cos(\theta)^m$ as a sum of $\cos(k\theta)$ terms, $0 \le k \le m$. So, we can integrate any polynomial in $\cos(\theta)$.
- *Trick*: Induct on m to find $T^*_m(w) = 2T_m(w/2)$ so $T^*_m(u+1/u) = u^m+1/u^m$. Then substitute $u \mapsto e^{2\pi i\theta}$.

Branch cycles for rational functions

- Select a point $z_0 \in \mathbb{P}^1_z \setminus \boldsymbol{z} \stackrel{\mathrm{def}}{=} U_{\boldsymbol{z}}$. Use *classical generators* of $\pi_1(U_{\boldsymbol{z}}, z_0)$, $P_1, \ldots, P_r$, based at z_0 around $\boldsymbol{z}$.

Branch cycles for rational functions

- Select a point $z_0 \in \mathbb{P}^1_z \setminus \boldsymbol{z} \stackrel{\text{def}}{=} U_{\boldsymbol{z}}$. Use *classical generators* of $\pi_1(U_{\boldsymbol{z}}, z_0)$, $P_1, \ldots, P_r$, based at z_0 around $\boldsymbol{z}$.
- Label points of $\mathbb{P}^1_w$ over z_0 as $\{1', \ldots, m'\}$. Each P_i is a loop around $z_{\tau(i)}$ where τ is a permutation of $\{1, \ldots, r\}$.

Branch cycles for rational functions

- Select a point $z_0 \in \mathbb{P}^1_z \setminus \boldsymbol{z} \stackrel{\text{def}}{=} U_{\boldsymbol{z}}$. Use *classical generators* of $\pi_1(U_{\boldsymbol{z}}, z_0)$, $P_1, \dots, P_r$, based at z_0 around $\boldsymbol{z}$.
- Label points of $\mathbb{P}^1_w$ over z_0 as $\{1', \dots, m'\}$. Each P_i is a loop around $z_{\tau(i)}$ where τ is a permutation of $\{1, \dots, r\}$.
- Restrict f over pullback $U_{\boldsymbol{w}} \subset \mathbb{P}^1_w$ of $U_{\boldsymbol{z}}$ in $\mathbb{P}^1_w$. Unique path lift of P_i, starting at $j' \in \{1', \dots, m'\} \mapsto$ endpoint j''.

  Gives a permutation σ_i of $\{1', \dots, m'\}$.

Branch cycles for rational functions

- Select a point $z_0 \in \mathbb{P}^1_z \setminus \boldsymbol{z} \stackrel{\text{def}}{=} U_{\boldsymbol{z}}$. Use *classical generators* of $\pi_1(U_{\boldsymbol{z}}, z_0)$, $P_1, \ldots, P_r$, based at z_0 around $\boldsymbol{z}$.
- Label points of $\mathbb{P}^1_w$ over z_0 as $\{1', \ldots, m'\}$. Each P_i is a loop around $z_{\tau(i)}$ where τ is a permutation of $\{1, \ldots, r\}$.
- Restrict f over pullback $U_{\boldsymbol{w}} \subset \mathbb{P}^1_w$ of $U_{\boldsymbol{z}}$ in $\mathbb{P}^1_w$. Unique path lift of P_i, starting at $j' \in \{1', \ldots, m'\} \mapsto$ endpoint j''.

  Gives a permutation σ_i of $\{1', \ldots, m'\}$.
- $(\sigma_1, \ldots, \sigma_r) = \boldsymbol{\sigma}$ – *branch cycles* for f – ordered from classical generators emanating in order clockwise from z_0.

Branch cycles for rational functions

- Select a point $z_0 \in \mathbb{P}^1_z \setminus \boldsymbol{z} \stackrel{\text{def}}{=} U_{\boldsymbol{z}}$. Use *classical generators* of $\pi_1(U_{\boldsymbol{z}}, z_0)$, $P_1, \ldots, P_r$, based at z_0 around $\boldsymbol{z}$.
- Label points of $\mathbb{P}^1_w$ over z_0 as $\{1', \ldots, m'\}$. Each P_i is a loop around $z_{\tau(i)}$ where τ is a permutation of $\{1, \ldots, r\}$.
- Restrict f over pullback $U_{\boldsymbol{w}} \subset \mathbb{P}^1_w$ of $U_{\boldsymbol{z}}$ in $\mathbb{P}^1_w$. Unique path lift of P_i, starting at $j' \in \{1', \ldots, m'\} \mapsto$ endpoint j''.
  Gives a permutation σ_i of $\{1', \ldots, m'\}$.
- $(\sigma_1, \ldots, \sigma_r) = \boldsymbol{\sigma}$ – *branch cycles* for f – ordered from classical generators emanating in order clockwise from z_0.
  1. Generation: $\langle \sigma_1, \ldots, \sigma_r \rangle = G_f \le S_m$ is group of smallest Galois cover of $\mathbb{P}^1_z$ over $\mathbb{C}$ factoring through $\mathbb{P}^1_w$.
     Call f a G_f cover (T_m is a dihedral cover).
  2. Conjugacy classes: the σ_i s represent r conjugacy classes **C** in G_f with well-defined multiplicity.
  3. Product-one: $\sigma_1 \cdots \sigma_r = 1$.

I.B: Splitting variables

- Separated variables $\Rightarrow$ introduce z:
  $f(x) - z = 0$ and $g(y) - z = 0$. Express by covers:

I.B: Splitting variables

- Separated variables $\Rightarrow$ introduce z:
  $f(x) - z = 0$ and $g(y) - z = 0$. Express by covers:
- $f : \mathbb{P}^1_x \rightarrow \mathbb{P}^1_z$ and $g : \mathbb{P}^1_y \rightarrow \mathbb{P}^1_z$ (added ∞; degrees m and n).
  Note: Problem not changed by replacing (f, g) by
  $(\alpha \circ f \circ \beta, \alpha \circ g \circ \gamma)$ with α, β, γ affine transformations.

- Separated variables $\Rightarrow$ introduce z: $f(x) - z = 0$ and $g(y) - z = 0$. Express by covers:
- $f : \mathbb{P}^1_x \to \mathbb{P}^1_z$ and $g : \mathbb{P}^1_y \to \mathbb{P}^1_z$ (added ∞; degrees m and n). Note: Problem not changed by replacing (f, g) by $(\alpha \circ f \circ \beta, \alpha \circ g \circ \gamma)$ with α, β, γ affine transformations.
- Fiber product denoted $\mathbb{P}^1_x \times_{\mathbb{P}^1_z} \mathbb{P}^1_y$:

$$\{(x', y') \mid f(x') = g(y')\}.$$

  But this will have singularities. We want non-singular (*normalization*) of set-theoretic fiber product.

1. Galois closure covers $\hat{f} : \hat{X}_f \longrightarrow \mathbb{P}^1_z$ (resp. $\hat{g} : \hat{X}_g \longrightarrow \mathbb{P}^1_z$): connected component of m-fold (resp. n-fold) fiber product of f (resp. g), minus *fat diagonal*.

I.C: More on *Galois closure of f*

1. Galois closure covers $\hat{f}: \hat{X}_f \to \mathbb{P}^1_z$ (resp. $\hat{g}: \hat{X}_g \to \mathbb{P}^1_z$): connected component of m-fold (resp. n-fold) fiber product of f (resp. g), minus *fat diagonal*.
2. S_m permutes coordinates: G_f is subgroup of S_m fixing $\hat{X}_f$; Denote the permutation representation by T_f.

I.C: More on *Galois closure of f*

1. Galois closure covers $\hat{f} : \hat{X}_f \to \mathbb{P}^1_z$ (resp. $\hat{g} : \hat{X}_g \to \mathbb{P}^1_z$): connected component of m-fold (resp. n-fold) fiber product of f (resp. g), minus *fat diagonal*.
2. S_m permutes coordinates: G_f is subgroup of S_m fixing $\hat{X}_f$; Denote the permutation representation by T_f.
3. *Combine Galois closures*: Fiber product of $\hat{f}$ and $\hat{g}$ over the maximal cover $Z \to \mathbb{P}^1_z$ through which they both factor:

$$G_{f,g} = G_f \times_{G(Z/\mathbb{P}^1_z)} G_g.$$

Projects to G_f and G_g, inducing reps. T_f and T_g.

As expected, particular problems require an expert to *translate*:
Use *C(hebotarev) D(ensity) T(heorem)*$^+$.

Theorem (Strong Davenport)

Equivalent to (f, g) *a Davenport pair:* $\forall\ \sigma \in G_{f,g}$,
$T_f(\sigma)$ *fixes an integer* $\Leftrightarrow$ $T_g(\sigma)$ *fixes an integer.*

The $+$ above CDT: Usual rough result is here precise.

- If conclusion reduced mod prime $\boldsymbol{p}$ holds, then ranges of f and g mod $\boldsymbol{p}$ are the same [DL63], [Fr05b, Princ. 3.1], [Mc67].

As expected, particular problems require an expert to *translate*:
Use *C(hebotarev) D(ensity) T(heorem)*$^+$.

Theorem (Strong Davenport)

Equivalent to (f, g) *a Davenport pair:* $\forall\ \sigma \in G_{f,g}$*,*
$T_f(\sigma)$ *fixes an integer* $\Leftrightarrow$ $T_g(\sigma)$ *fixes an integer.*

The $+$ above CDT: Usual rough result is here precise.

- If conclusion reduced mod prime $\boldsymbol{p}$ holds, then ranges of f and g mod $\boldsymbol{p}$ are the same [DL63], [Fr05b, Princ. 3.1], [Mc67].
- Actual Davenport pairs have equality in the ranges without exception, (you might expect only near equality).

I.D: Translating Davenport to Group Theory
Start of *monodromy method*

As expected, particular problems require an expert to *translate*:
Use *C(hebotarev) D(ensity) T(heorem)*$^+$.

Theorem (Strong Davenport)

Equivalent to (f, g) *a Davenport pair:* $\forall\ \sigma \in G_{f,g}$,
$T_f(\sigma)$ *fixes an integer* $\Leftrightarrow$ $T_g(\sigma)$ *fixes an integer.*

The $+$ above CDT: Usual rough result is here precise.

- If conclusion reduced mod prime $\boldsymbol{p}$ holds, then ranges of f and g mod $\boldsymbol{p}$ are the same [DL63], [Fr05b, Princ. 3.1], [Mc67].
- Actual Davenport pairs have equality in the ranges without exception, (you might expect only near equality).
- Natural pairs come with equality of ranges for all primes.

Capturing Davenport with Group Theory

1. *Group Problem* P_1: What groups (permutation pairs) give such a $G_{f,g}$? How does this relate to *simple group* classification?

Capturing Davenport with Group Theory

1. *Group Problem* P_1: What groups (permutation pairs) give such a $G_{f,g}$? How does this relate to *simple group* classification?
2. *Converse Problem* P_2: Even answering P_1, from whence polynomials (f, g) satisfying Davenport?

Capturing Davenport with Group Theory

1. *Group Problem* P_1: What groups (permutation pairs) give such a $G_{f,g}$? How does this relate to *simple group* classification?
2. *Converse Problem* P_2: Even answering P_1, from whence polynomials (f, g) satisfying Davenport?
3. Our hypothesis: f indecomposable $\Leftrightarrow$ G_f is primitive.

Capturing Davenport with Group Theory

1. *Group Problem P_1*: What groups (permutation pairs) give such a $G_{f,g}$? How does this relate to *simple group* classification?
2. *Converse Problem P_2*: Even answering P_1, from whence polynomials (f, g) satisfying Davenport?
3. Our hypothesis: f indecomposable $\Leftrightarrow$ G_f is primitive.
   - *Primitive*: No group properly between G_f and $G_f(1) = \{\sigma \in G_f \mid T_f(\sigma)(1) = 1\}$.
   - *Doubly Transitive*: $G_f(1)$ transitive on $\{2, \ldots, m\}$ $\Longrightarrow$ primitive.

Primitive group template of 5 patterns: 4 from (*almost*) simple groups; rest from *affine groups* [A-O-S85], [FGS93, §13]. Classifying Doubly transitive groups is easier.

If group is *not* primitive, even the classification isn't helpful.

- G_f primitive $\Leftrightarrow$ f factors through no proper cover.

Primitive group template of 5 patterns: 4 from (*almost*) simple groups; rest from *affine groups* [A-O-S85], [FGS93, §13]. Classifying Doubly transitive groups is easier.

If group is *not* primitive, even the classification isn't helpful.

- G_f primitive $\Leftrightarrow$ f factors through no proper cover.
- G_f doubly transitive $\Leftrightarrow$ $X \times_{\mathbb{P}^1_z} X$ has exactly two irreducible components (one the diagonal).

Primitive group template of 5 patterns: 4 from (*almost*) simple groups; rest from *affine groups* [A-O-S85], [FGS93, §13]. Classifying Doubly transitive groups is easier.

If group is *not* primitive, even the classification isn't helpful.

- G_f primitive $\Leftrightarrow$ f factors through no proper cover.
- G_f doubly transitive $\Leftrightarrow$ $X \times_{\mathbb{P}^1_z} X$ has exactly two irreducible components (one the diagonal).
- Doubly Transitive $\Leftrightarrow (f(x) - f(y)/(x - y)$ *irreducible*.

Key Observations:

1. Degree m poly. *branch cycles* include an m-cycle σ_∞ at ∞.

Key Observations:

1. Degree m poly. *branch cycles* include an m-cycle σ_∞ at ∞.
2. If T_f *primitive*, then T_f *doubly transitive* unless f is (*Möbius equivalent to*: modulo linear fractional compositions) Chebychev or cyclic ($x \mapsto x^n$) [Fr70].

Key Observations:

1. Degree m poly. *branch cycles* include an m-cycle σ_∞ at ∞.
2. If T_f *primitive*, then T_f *doubly transitive* unless f is (*Möbius equivalent to*: modulo linear fractional compositions) Chebychev or cyclic ($x \mapsto x^n$) [Fr70].
3. Representation Thm: For (f, g) a Davenport pair:

II.B: Further Group translation of Davenport

Key Observations:

1. Degree m poly. *branch cycles* include an m-cycle σ_∞ at ∞.
2. If T_f *primitive*, then T_f *doubly transitive* unless f is (*Möbius equivalent to*: modulo linear fractional compositions) Chebychev or cyclic ($x \mapsto x^n$) [Fr70].
3. Representation Thm: For (f, g) a Davenport pair:
   - $\deg(f) = \deg(g)$, $\hat{X}_f = \hat{X}_g$, so $G_f = G_g$; and
   - $T_f = T_g$ as group representations, but not as permutation representations.

Proof of Degree Equality

- Get branch cycle σ_∞ in $G_{f,g}$ with $T_f(\sigma_\infty)$ (resp. $T_g(\sigma_\infty)$) an m-cycle (resp. n-cycle).

Proof of Degree Equality

- Get branch cycle σ_∞ in $G_{f,g}$ with $T_f(\sigma_\infty)$ (resp. $T_g(\sigma_\infty)$) an m-cycle (resp. n-cycle).
- Suppose $(m, n) = d < m$. Consider $\sigma' = \sigma_\infty^m$.

Proof of Degree Equality

- Get branch cycle σ_∞ in $G_{f,g}$ with $T_f(\sigma_\infty)$ (resp. $T_g(\sigma_\infty)$) an m-cycle (resp. n-cycle).
- Suppose $(m, n) = d < m$. Consider $\sigma' = \sigma_\infty^m$.
- Then $T_f(\sigma')$ fixes all integers; $T_g(\sigma')$ moves each integer.

Proof of Degree Equality

- Get branch cycle σ_∞ in $G_{f,g}$ with $T_f(\sigma_\infty)$ (resp. $T_g(\sigma_\infty)$) an m-cycle (resp. n-cycle).
- Suppose $(m,n) = d < m$. Consider $\sigma' = \sigma_\infty^m$.
- Then $T_f(\sigma')$ fixes all integers; $T_g(\sigma')$ moves each integer.
- This contradicts Strong Dav. Thm.

Proof of Degree Equality

- Get branch cycle σ_∞ in $G_{f,g}$ with $T_f(\sigma_\infty)$ (resp. $T_g(\sigma_\infty)$) an m-cycle (resp. n-cycle).
- Suppose $(m,n) = d < m$. Consider $\sigma' = \sigma_\infty^m$.
- Then $T_f(\sigma')$ fixes all integers; $T_g(\sigma')$ moves each integer.
- This contradicts Strong Dav. Thm.
- A fancier version of this gives $\hat{X}_f = \hat{X}_g$ and $G_f = G_g$.

Consider zeros $\{x_i\}_{i=1}^n$ of $f(x) - z$. Equality of Galois closures $\implies$ these are functions of zeros $\{y_i\}_{i=1}^n$ of $g(y) - z$ (and vice-versa).

- Normalize numbering: σ_∞ cycles x_is and y_is.

Consider zeros $\{x_i\}_{i=1}^n$ of $f(x) - z$. Equality of Galois closures $\implies$ these are functions of zeros $\{y_i\}_{i=1}^n$ of $g(y) - z$ (and vice-versa).

- Normalize numbering: σ_∞ cycles x_is and y_is.

Theorem (Double Transitivity)

T_f doubly transitive $\implies$ this much stronger conclusion:

$$x_1 = y_1 + y_{\alpha_2} + \cdots + y_{\alpha_k}, 2 \le k \le (n-1)/2 :$$

The representation space is the same for x s and y s.
Write $R_1 = \{1, \alpha_2, \ldots, \alpha_k\} \mod n$.

Difference Set Argument

Theorem (Multiplier)

1

- *Different set: Among nonzero differences from* R_1*, each integer* $\{1, \ldots, n-1\}$ *occurs* $u = k(k-1)/(n-1)$ *times.*

Difference Set Argument

Theorem (Multiplier)

1.
- *Different set: Among nonzero differences from R_1, each integer $\{1, \ldots, n-1\}$ occurs $u = k(k-1)/(n-1)$ times.*
- *The expression for y_is in x_js gives the different set (up to translation) $-R_1$.*

2. Acting by σ_∞ – translating subscripts – gives collections R_i, $i = 1, \ldots, n$.

Difference Set Argument

Theorem (Multiplier)

1.
   - *Different set: Among nonzero differences from R_1, each integer $\{1, \ldots, n-1\}$ occurs $u = k(k-1)/(n-1)$ times.*
   - *The expression for y_is in x_js gives the different set (up to translation) $-R_1$.*

2. Acting by σ_∞ – translating subscripts – gives collections R_i, $i = 1, \ldots, n$.
3. # times $u \mod n$ appears as a (nonzero) difference from R_1 equals # times $\{1, u+1\}$ appears in the union of the R_is. (Normalize u as a difference to have 1st integer "1.")

Difference Set Argument

Theorem (Multiplier)

1. - *Different set: Among nonzero differences from R_1, each integer $\{1, \ldots, n-1\}$ occurs $u = k(k-1)/(n-1)$ times.*
   - *The expression for y_is in x_js gives the different set (up to translation) $-R_1$.*
2. Acting by σ_∞ – translating subscripts – gives collections R_i, $i = 1, \ldots, n$.
3. # times $u \mod n$ appears as a (nonzero) difference from R_1 equals # times $\{1, u+1\}$ appears in the union of the R_is. (Normalize u as a difference to have 1st integer "1.")
4. T_f doubly transitive $\Leftrightarrow$ $G_f(1)$ transitive on $\{2, \ldots, n\}$: # of appearances of $\{1, u+1\}$ in $\cup_i R_i$ independent of u.

Finite field $\mathbb{F}_q$ (with $q = p^t$, p prime). For $v \geq 2$, $\mathbb{F}_{q^{v+1}}$ is a dimension $v+1$ vector space over $\mathbb{F}_q$.

- $\mathrm{PGL}_{v+1}(\mathbb{F}_q) = \mathrm{GL}_{v+1}(\mathbb{F}_q)/(\mathbb{F}_q)^*$ acts on lines through origin: on the $n = (q^{v+1} - 1)(q - 1)$ points of projective v-space.

Finite field $\mathbb{F}_q$ (with $q = p^t$, p prime). For $v \geq 2$, $\mathbb{F}_{q^{v+1}}$ is a dimension $v+1$ vector space over $\mathbb{F}_q$.

- $\mathrm{PGL}_{v+1}(\mathbb{F}_q) = \mathrm{GL}_{v+1}(\mathbb{F}_q)/(\mathbb{F}_q)^*$ acts on lines through origin: on the $n = (q^{v+1} - 1)(q - 1)$ points of projective v-space.
- Brumer-McLaughlin-Misera-Feit-Thompson-Guralnick-Saxl-Müller interactions story told in [UMSt]: Using group theory vs how to study groups. I now outline these points.

Finite field $\mathbb{F}_q$ (with $q = p^t$, p prime). For $v \geq 2$, $\mathbb{F}_{q^{v+1}}$ is a dimension $v+1$ vector space over $\mathbb{F}_q$.

- $\mathrm{PGL}_{v+1}(\mathbb{F}_q) = \mathrm{GL}_{v+1}(\mathbb{F}_q)/(\mathbb{F}_q)^*$ acts on lines through origin: on the $n = (q^{v+1} - 1)(q - 1)$ points of projective v-space.
- Brumer-McLaughlin-Misera-Feit-Thompson-Guralnick-Saxl-Müller interactions story told in [UMSt]: Using group theory vs how to study groups. I now outline these points.
  1. What groups arise as G_f with (f, g) a D(avenport)P(air).

Part III: What groups give Davenport pairs and how?
§III.A: Projective Linear Groups

Finite field $\mathbb{F}_q$ (with $q = p^t$, p prime). For $v \geq 2$, $\mathbb{F}_{q^{v+1}}$ is a dimension $v + 1$ vector space over $\mathbb{F}_q$.

- $\mathrm{PGL}_{v+1}(\mathbb{F}_q) = \mathrm{GL}_{v+1}(\mathbb{F}_q)/(\mathbb{F}_q)^*$ acts on lines through origin: on the $n = (q^{v+1} - 1)(q - 1)$ points of projective v-space.
- Brumer-McLaughlin-Misera-Feit-Thompson-Guralnick-Saxl-Müller interactions story told in [UMSt]: Using group theory vs how to study groups. I now outline these points.
    1. What groups arise as G_f with (f, g) a D(avenport)P(air).
    2. From those, how to produce all Davenport pairs.

Finite field $\mathbb{F}_q$ (with $q = p^t$, p prime). For $v \geq 2$, $\mathbb{F}_{q^{v+1}}$ is a dimension $v+1$ vector space over $\mathbb{F}_q$.

- $\mathrm{PGL}_{v+1}(\mathbb{F}_q) = \mathrm{GL}_{v+1}(\mathbb{F}_q)/(\mathbb{F}_q)^*$ acts on lines through origin: on the $n = (q^{v+1} - 1)(q-1)$ points of projective v-space.
- Brumer-McLaughlin-Misera-Feit-Thompson-Guralnick-Saxl-Müller interactions story told in [UMSt]: Using group theory vs how to study groups. I now outline these points.
  1. What groups arise as G_f with (f,g) a D(avenport)P(air).
  2. From those, how to produce all Davenport pairs.
  3. Genus 0 Problem–Thompson Conjecture: From Davenport and related: Only composition factors of $f : \mathbb{P}^1_w \to \mathbb{P}^1_z$ monodromy, A_n s and $\mathbb{Z}/p$ s, excluding finitely many exceptions.

Finite field $\mathbb{F}_q$ (with $q = p^t$, p prime). For $v \geq 2$, $\mathbb{F}_{q^{v+1}}$ is a dimension $v + 1$ vector space over $\mathbb{F}_q$.

- $\mathrm{PGL}_{v+1}(\mathbb{F}_q) = \mathrm{GL}_{v+1}(\mathbb{F}_q)/(\mathbb{F}_q)^*$ acts on lines through origin: on the $n = (q^{v+1} - 1)(q - 1)$ points of projective v-space.
- Brumer-McLaughlin-Misera-Feit-Thompson-Guralnick-Saxl-Müller interactions story told in [UMSt]: Using group theory vs how to study groups. I now outline these points.
  1. What groups arise as G_f with (f, g) a D(avenport)P(air).
  2. From those, how to produce all Davenport pairs.
  3. Genus 0 Problem–Thompson Conjecture: From Davenport and related: Only composition factors of $f : \mathbb{P}^1_w \to \mathbb{P}^1_z$ monodromy, A_n s and $\mathbb{Z}/p$ s, excluding finitely many exceptions.
  4. Guralnick conjecture: Precise on actual monodromy of primitive Rational function [Fr05a, §7.2.3].

Why projective Linear Groups arise

1. $\mathrm{PGL}_{v+1}(\mathbb{F}_q)$ has two (inequivalent) doubly transitive *permutation* representations: On points and on hyperplanes.

Why projective Linear Groups arise

1. $\mathrm{PGL}_{v+1}(\mathbb{F}_q)$ has two (inequivalent) doubly transitive *permutation* representations: On points and on hyperplanes.
2. An incidence matrix conjugates between them: They are equivalent as group representations.

Why projective Linear Groups arise

1. $\mathrm{PGL}_{v+1}(\mathbb{F}_q)$ has two (inequivalent) doubly transitive *permutation* representations: On points and on hyperplanes.
2. An incidence matrix conjugates between them: They are equivalent as group representations.
3. Euler's Thm. gives a cyclic generator, γ_q, of $\mathbb{F}^*_{q^{v+1}}$. Multiplying by γ_q on $\mathbb{F}_{q^{v+1}} = F_q^{v+1}$ induces an *n*-cycle in $\mathrm{PGL}_{v+1}(\mathbb{F}_q)$.

Why projective Linear Groups arise

1. $\mathrm{PGL}_{v+1}(\mathbb{F}_q)$ has two (inequivalent) doubly transitive *permutation* representations: On points and on hyperplanes.
2. An incidence matrix conjugates between them: They are equivalent as group representations.
3. Euler's Thm. gives a cyclic generator, γ_q, of $\mathbb{F}^*_{q^{v+1}}$. Multiplying by γ_q on $\mathbb{F}_{q^{v+1}} = F_q^{v+1}$ induces an *n*-cycle in $\mathrm{PGL}_{v+1}(\mathbb{F}_q)$.
4. Conjecture [Fr73]: Two equivalent doubly transitive reps. and *n*-cycle: Except for one of deg 11, all are *nearly* PGL_{v+1} s. Proof (from classification) [Fr99, §9], based on [CKS76].

III.B: Punchlines on Davenport (f indecomposable)

1. Davenport's Question: $\exists$ DPs over $\mathbb{Q}$? *Multiplier Theorem* $\implies g$ is complex conjugate to f. No DPs over $\mathbb{Q}$.
   Equivalent to σ_∞ not conjugate to σ_∞^{-1}.
   No use of classification; first use of *Branch Cycle Argument*.

III.B: Punchlines on Davenport (f indecomposable)

1. Davenport's Question: $\exists$ DPs over $\mathbb{Q}$? *Multiplier Theorem* $\implies$ g is complex conjugate to f. No DPs over $\mathbb{Q}$. Equivalent to σ_∞ not conjugate to σ_∞^{-1}. No use of classification; first use of *Branch Cycle Argument*.
2. Answer to Schinzel's Problem: If $f(x) - h(y)$ factors (over $\mathbb{C}$), then $h = g(h_2(y))$ with (f, g) a DP over some field.

III.B: Punchlines on Davenport (f indecomposable)

1. Davenport's Question: $\exists$ DPs over $\mathbb{Q}$? *Multiplier Theorem* $\Longrightarrow$ g is complex conjugate to f. No DPs over $\mathbb{Q}$.
   Equivalent to σ_∞ not conjugate to σ_∞^{-1}.
   No use of classification; first use of *Branch Cycle Argument*.
2. Answer to Schinzel's Problem: If $f(x) - h(y)$ factors (over $\mathbb{C}$), then $h = g(h_2(y))$ with (f, g) a DP over some field.
3. Degrees of DPs over some number field K:

$$n = 7, 11, 13, 15, 21, 31.$$

   For each n, we know exactly what K s carry DPs.

III.C: From III.B, Hints at the *Genus 0* Problem

1. For $n = 7, 13, 15$ (resp. described in [Fr80, §B], [CoCa99], [Fr99,§8]) there are non-trivial Möbius equivalence families of Davenport pairs. For $n = 7 = 1 + 2 + 2^2$, $G_f = \mathrm{PGL}_3(\mathbb{Z}/2)$.

III.C: From III.B, Hints at the *Genus 0* Problem

1. For $n = 7, 13, 15$ (resp. described in [Fr80, §B], [CoCa99], [Fr99,§8]) there are non-trivial Möbius equivalence families of Davenport pairs. For $n = 7 = 1 + 2 + 2^2$, $G_f = \mathrm{PGL}_3(\mathbb{Z}/2)$.
2. $n = 7$ branch cycles: $(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$; $\sigma_1, \sigma_2, \sigma_3$ involutions, each fixing the 3 points, on some hyperplane; σ_4 a 7-cycle.

1. For $n = 7, 13, 15$ (resp. described in [Fr80, §B], [CoCa99], [Fr99,§8]) there are non-trivial Möbius equivalence families of Davenport pairs. For $n = 7 = 1 + 2 + 2^2$, $G_f = \mathrm{PGL}_3(\mathbb{Z}/2)$.
2. $n = 7$ branch cycles: $(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$; $\sigma_1, \sigma_2, \sigma_3$ involutions, each fixing the 3 points, on some hyperplane; σ_4 a 7-cycle.
    - *Riemann-Hurwitz*: Cover with these branch cycles has genus $\mathbf{g}_7 = 0$: $2(7+\mathbf{g}_7\text{-}1) = \sum_{i=1}^{4} \mathrm{ind}(\sigma_i) = 3 \cdot 2 + 6 \implies \mathbf{g}_7 = 0$.

1. For $n = 7, 13, 15$ (resp. described in [Fr80, §B], [CoCa99], [Fr99,§8]) there are non-trivial Möbius equivalence families of Davenport pairs. For $n = 7 = 1 + 2 + 2^2$, $G_f = \mathrm{PGL}_3(\mathbb{Z}/2)$.
2. $n = 7$ branch cycles: $(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$; $\sigma_1, \sigma_2, \sigma_3$ involutions, each fixing the 3 points, on some hyperplane; σ_4 a 7-cycle.
   - *Riemann-Hurwitz*: Cover with these branch cycles has genus $\mathbf{g}_7 = 0$: $2(7+\mathbf{g}_7\text{-}1)=\sum_{i=1}^{4} \mathrm{ind}(\sigma_i) = 3 \cdot 2 + 6 \implies \mathbf{g}_7=0$.
3. Two genus 0 j-line covers parametrize the (f, g) pairs – two reduced Hurwitz spaces – conjugate over $\mathbb{Q}(\sqrt{-7})$.

III.C: From III.B, Hints at the *Genus 0* Problem

1. For $n = 7, 13, 15$ (resp. described in [Fr80, §B], [CoCa99], [Fr99,§8]) there are non-trivial Möbius equivalence families of Davenport pairs. For $n = 7 = 1 + 2 + 2^2$, $G_f = \mathrm{PGL}_3(\mathbb{Z}/2)$.
2. $n = 7$ branch cycles: $(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$; $\sigma_1, \sigma_2, \sigma_3$ involutions, each fixing the 3 points, on some hyperplane; σ_4 a 7-cycle.
   - *Riemann-Hurwitz*: Cover with these branch cycles has genus $\mathbf{g}_7 = 0$: $2(7+\mathbf{g}_7\text{-}1)=\sum_{i=1}^4 \mathrm{ind}(\sigma_i) = 3 \cdot 2 + 6 \implies \mathbf{g}_7=0$.
3. Two genus 0 j-line covers parametrize the (f, g) pairs – two reduced Hurwitz spaces – conjugate over $\mathbb{Q}(\sqrt{-7})$.
4. A cover gives a bundle: Both families parametrize the same family of rank 7 bundles (over $\mathbb{Q}$). Similarly, for $n = 13$ and 15.

1. For $n = 7, 13, 15$ (resp. described in [Fr80, §B], [CoCa99], [Fr99,§8]) there are non-trivial Möbius equivalence families of Davenport pairs. For $n = 7 = 1 + 2 + 2^2$, $G_f = \mathrm{PGL}_3(\mathbb{Z}/2)$.
2. $n = 7$ branch cycles: $(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$; $\sigma_1, \sigma_2, \sigma_3$ involutions, each fixing the 3 points, on some hyperplane; σ_4 a 7-cycle.
   - *Riemann-Hurwitz*: Cover with these branch cycles has genus $\mathbf{g}_7 = 0$: $2(7+\mathbf{g}_7\text{-}1)=\sum_{i=1}^4 \mathrm{ind}(\sigma_i) = 3 \cdot 2 + 6 \implies \mathbf{g}_7=0$.
3. Two genus 0 j-line covers parametrize the (f, g) pairs – two reduced Hurwitz spaces – conjugate over $\mathbb{Q}(\sqrt{-7})$.
4. A cover gives a bundle: Both families parametrize the same family of rank 7 bundles (over $\mathbb{Q}$). Similarly, for $n = 13$ and 15.
5. Ron Solomon [So01] says things about "groups appearing in Nature:" Do *rational functions* appear in nature?

[A-O-S85] M. Aschbacher and L. Scott, Maximal subgroups of finite groups, J. Algebra 92 (1985), 44–80.
[CoCa99] J.-M. Couveignes and P. Cassou-Noguès, Factorisations explicites de g(y)-h(z), Acta Arith. 87 (1999), no. 4, 291–317.
[CKS76] C.W. Curtis, W.M. Kantor and G.M. Seitz, 2-transitive permutation reps. of the finite Chevalley groups, TAMS 218 (1976), 1–59.
[DL63] H. Davenport and D.J. Lewis, Notes on Congruences (I), Qt. J. Math. Oxford (2) 14 (1963), 51–60.
[Fr73] M. Fried, Field of definition of function fields and . . . reducibility of polynomials in two variables, Ill. J. Math. 17 (1973), 128–146.
[Fr80] M. Fried, Exposition on an Arithmetic-Group Theoretic Connection via Riemann's Existence Theorem, Santa Cruz Conf. on Finite Groups, A.M.S. Pub. 37 (1980), 571–601.
[Fr99] M. Fried, Variables Separated Polynomials and Moduli Spaces, No. Th. in Prog., Schinzel Festschrift, Sum. 1997, Walter de Gruyter, Berlin-NY (Feb. 1999), 169–228.
[Fr05a] M. Fried, Relating two genus 0 problems of John Thompson, Volume for John Thompson's 70th birthday, in Progress in Galois Theory, H. Voelklein and T. Shaska editors 2005 Springer Science, 51–85.

[Fr05b] M. Fried, The place of exceptional covers among all diophantine relations, J. Finite Fields **11** (2005) 367–433.
[FGS93] M. Fried, R. Guralnick and J. Saxl, Schur Covers and Carlitz's Conjecture, Israel J.; Thompson Volume 82 (1993), 157–225.
[GLS] D. Gorenstein, R. Lyons, R. Solomon, Classification of Finite Simple Groups, No. 3, Math. Surveys and Monographs, 40 ISBN:0821803913.
[LPS] M. Liebeck, C. Praeger, J. Saxl, Maximal factorizations of finite simple groups . . . , Mem. AMS 86 #432 (1990).
[Mc67] C. MacCluer, On a conjecture of Davenport and Lewis concerning exceptional poly- nomials, Acta. Arith. 12 (1967), 289–299.
[Mü95] 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, 385–401.
[Sc71] A. Schinzel, Reducibility of Polynomials, Int. Cong. Math. Nice 1970 (1971), Gauthier-Villars, 491–496.
[So01] R. Solomon, A Brief History of the Classification of Finite Simple Groups, BAMS 38 (3) (2001), 315–352.
[UMSt] http://www.math.uci.edu/˜mfried/paplist-cov/UMStory.html.