Variables Separated Equations and Finite Simple Groups

Mike Fried, UC Irvine, Talk at Idaho S. U. 10/02/08

[UMSt] www.math.uci.edu/~mfried/paplist-cov/UMStory.html.

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

Two problems from the 60s (Davenport's and Shinzel's) solved by the *monodromy method*. I explain that and the associated *Genus 0 Problem*. Another genus 0 problem, related to John Thompson, connects the Monster simple group to genus 0 modular curves. Both influenced by the same conference – Santa Cruz (proceedings in 1980).

§I. Abel and Dihedral functions

To integrate $\cos(\theta)^n$, 1st year calc. uses the nth *Chebychev* polynomial (with $T_n(\cos(\theta)) = \cos(n\theta)$): $T_n : \mathbb{P}^1_w = \mathbb{C}_w \cup \{\infty\} \to \mathbb{P}^1_z = \mathbb{C}_z \cup \{\infty\}$.

It is *branched* over $\{z_1, z_2, z_3\} = \{-1, +1, \infty\}$.

The trick : Find $T_n^*(w) = 2T_n(w/2)$ so $T_n^*(x+1/x) = x^n+1/x^n$ inductively, using degrees. Then substitute $x \mapsto e^{2\pi i\theta}$.

§I.A. The dihedral group with observations

T_n (n odd) is a *dihedral* function:

with a *b(ranch)c(ycle)d(escription)*:

$$\begin{aligned}\sigma_1 &= (2\,n)(3\,n{-}1)\cdots(\tfrac{n+1}{2}\,\tfrac{n+3}{2})\\ \sigma_2 &= (1\,n)(2\,n{-}1)\cdots(\tfrac{n-1}{2}\,\tfrac{n+3}{2})\\ \sigma_\infty &= (n\,n{-}1\cdots 1)\end{aligned}$$

- (generation) $\langle\sigma_1,\sigma_2\rangle = D_n = \{\left(\begin{smallmatrix}\pm 1 & b\\ 0 & 1\end{smallmatrix}\right)\}_{b\in\mathbb{Z}/n}$, order $2n$ dihedral group; C_2, involution conj. class $\Leftrightarrow -1$ in (1,1) position).
- (conjugacy classes) σ_i, $i=1,2$, are in C_2, σ_∞ is an n-cycle ($\frac{n-1}{2}$ conjugacy classes of these).
- (product-one) $\sigma_1\sigma_2\sigma_\infty = 1$.

Two dihedral function questions

- Q_1: From whence the $(\sigma_1, \sigma_2, \sigma_\infty)$?
  Answer: Use App. A: With $r = 3$. Always get an n-cycle at ∞ for polynomial f with $\deg(f) = n$.

- Q_2: If another function $f : \mathbb{P}^1_w \longrightarrow \mathbb{P}^1_z$ with similar bcd, how related to T_n?
  Answer: $\exists$ Möbius transforms. $\alpha_1, \alpha_2 \in \mathrm{PGL}_2(\mathbb{C})$ with $f = \alpha_2 \circ T_n \circ \alpha_1^{-1}(w)$: $f \sim^{\text{Möbius}} T_n$.

  Historical generalization: Abel used more general dihedral Möbius classes.

§I.B. $r = 4$ (not 3) branch dihedral functions

Denote *distinct* elements of $(\mathbb{P}^1_z)^4$ by U^4. S_4 (symmetries on $\{1, 2, 3, 4\}$) permutes coordinates of U^4.

Instead of $(\sigma_1, \sigma_2, \sigma_\infty)$ take $\sim^{\text{Möbius}}$ classes of functions with bcds among 4-tuples, $\mathrm{Ni}(D_n, \mathbf{C}_{2^4})$ (Nielsen classes), in $\mathbf{C}_{2^4}$ with generation and product-one —branched over any

$\boldsymbol{z} = \{z_1, \ldots, z_4\} \in U^4/S_4 \stackrel{\text{def}}{=} U_4 \stackrel{\text{def}}{=} U_{4,z}$.

One element of $\mathrm{Ni}(D_n, \mathbf{C}_{2^4})$: $(\sigma_1, \sigma_1^{-1}, \sigma_2, \sigma_2^{-1})$. Here's another: $(\sigma_1, \sigma_1^{-1}\sigma_2\sigma_1, \sigma_1^{-1}, \sigma_2^{-1})$.

Why such $f : \mathbb{P}^1_w \longrightarrow \mathbb{P}^1_z$ exists

- App. A gives compact surface cover $f : X \longrightarrow \mathbb{P}^1_z$.
- R(iemann)-H(urwitz) (App. B) $\Longrightarrow X$ has genus 0.
- R(iemann)-R(och) $\Longrightarrow$ X analytically $\mathbb{P}^1_w$.
- Each z_i has a unique unramified $w_i \mapsto z_i$
  (w_i corresponds to length 1 disjoint cycle in σ_i):

$$f \leftrightarrow (\boldsymbol{w}, \boldsymbol{z}) \in U_{4,w} \times U_{4,z} \quad \mapsto [\sim^{\text{Möbius}}]$$
$$\mathrm{PGL}_2(\mathbb{C}) \backslash U_{4,w} \times U_{4,z} / \mathrm{PGL}_2(\mathbb{C}) \quad = (\mathbb{P}^1_{jw} \setminus \infty) \times (\mathbb{P}^1_{jz} \setminus \infty).$$

  Image is the modular curve called $X_0(n)$.

§II. Davenport and Schinzel Problems
Separated Variables Equations

Consider polynomial pairs (f, g): degrees m and n (> 0). Unless said, exclude $g(x) = f(ax + b)$.
Separated Variables Equation: (*) $f(x) - g(y) = 0$.

Davenport's Problem: For what (f, g) over $\mathbb{Q}$ are ranges on $\mathbb{Z}/p$ (p a prime) equal for almost all p.
For K a number field, there is an the analog.

Schinzel's Problem: When is (*) *reducible*?

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

§II.A. Splitting variables

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

(*2) $f : \mathbb{P}^1_x \to \mathbb{P}^1_z$ and $g : \mathbb{P}^1_y \to \mathbb{P}^1_z$ (we added ∞).

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.

The fiber product $\mathbb{P}^1_x \times_{\mathbb{P}^1_z} \mathbb{P}^1_y$ consists of the $\{(x', y') \mid f(x') = g(y')\}$, but we want the non-singular model (*normalization*) of this.

§II.B. Introducing Galois groups

f has a Galois closure cover $\hat{f} : \hat{X}_f \to \mathbb{P}^1_z$ (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*.

Symmetric group S_m permutes the coordinates:
Galois group G_f, subgroup of S_m fixing $\hat{X}_f$;
Denote the permutation representation by T_f.

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. Gives

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

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

§II.C. Translating Davenport to Group Theory

This starts the *monodromy method*. As expected, particular problems require an expert to *translate*: Use Chebotarev Density Theorem.

Equivalent to (f, g) a Davenport pair: $\forall\ \sigma \in G_{f,g}$, $(*^3)$ $T_f(\sigma)$ fixes an integer $\Leftrightarrow$ $T_g(\sigma)$ fixes an integer.

Two serious general problems:

Group Problem P_1: What groups, and permutation pairs, give such a $G_{f,g}$; what has this to do with the classification of simple groups?

Converse Problem P_2: Even answering P_1, from whence polynomials (f, g) satisfying Davenport?

§III. Primitivity, cycles and the Classification

- Primitive $\Leftrightarrow$ no group properly between G_f and $G_f(1) = \{g \in G_f \mid T_f(g)(1) = 1\}$.
- Doubly Transitive $\Leftrightarrow$ $G_f(1)$ transitive on $\{2, \ldots, m\}$.

[A-O-S85]: Primitive group template of 5 patterns: 4 from (*almost*) simple groups; rest from *affine groups*.

Classifying Doubly transitive groups is easier. Also, if you can't assume a group is primitive, even the classification has yet to be helpful.

III.A. Translating Primitivity for $f : X \to \mathbb{P}^1_z$

- 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).

For f a rational function:

- Primitive $\Leftrightarrow$ can't decompose f as $f_1 \circ f_2$ with both $\deg(f_i)$s exceeding 1.
- DoublyTransitive $\Leftrightarrow (f(x)-f(y)/(x-y)$ *irreducible*.

III.B. Further Group translation of Davenport

Key Observations:

1. Polynomial (of degree m) *branch cycles* (p. 4) include an n-cycle σ_∞ at ∞.
2. If T_f *primitive*, then T_f *doubly transitive* unless f is (Möbius equivalent to) Chebychev (p. 2) or cyclic ($x \mapsto x^n$) [Fr70].

Representation Thm: For (f, g) a Davenport pair:

1. $\deg(f) = \deg(g)$, $\hat{X}_f = \hat{X}_g$, so $G_f = G_g$; and
2. $T_f = T_g$ as group representations, but not as permutation representations.

Equal degree argument

Get branch cycle σ_∞ in $G_{f,g}$ (p. 4) 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, while $T_g(\sigma')$ moves each integer. This contradicts (*^{3}) on p. 10. A fancier version of this gives $\hat{X}_f = \hat{X}_g$ and $G_f = G_g$.

(*^{4}) Another Version: Zeros $\{x_i\}_{i=1}^n$ of $f(x) - z$ 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.

III.C. Double Transitivity and Difference sets

Since T_f is doubly transitive, representation theory gives this much stronger conclusion:

$(*^5)$ $x_1 = y_1 + y_{\alpha_2} + \cdots + y_{\alpha_k}$, $2 \le k \le (n-1)/2$:

The representation space is the same for xs and ys.

Multiplier Thm: Write $R_1 = \{1, \alpha_2, \ldots, \alpha_k\} \mod n$

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

Argument for # 1

Acting by σ_∞ – translating subscripts – gives collections R_i, $i = 1, \ldots, n$. The # 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. That is, normalize its appearance as a difference with 1st integer is a "1."

Double transitivity of T_f is equivalent to $G_f(1)$ transitive on $\{2, \ldots, n\}$: no dependence on u on the appearances of $\{1, u+1\}$ in all the R_is.

§IV. What groups give Davenport pairs and how? How this pointed to all Genus 0 Monodromy

This is the start of the Brumer-McLaughlin-Misera-Feit-Thompson-Guralnick-Saxl-Müller interactions told in [UMSt]. Story to show how to use the power of group theory, vs how to study groups. I answer these points from p. 10:

- P_1: What groups could possibly arise as G_f with (f, g) a D(avenport)P(air).
- P_2: From those, how to produce all Davenport pairs.
- Genus 0 Problem: What are the monodromy groups of rational functions?

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

$\mathrm{PGL}_{v+1}(\mathbb{F}_q)$ has two (inequivalent) doubly transitive permutation representations: On points and on hyperplanes. An incidence matrix conjugates between them: Equiv. reps.

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 $\mathrm{PGL}_{v+1}(\mathbb{F}_q)$.

§IV.B. Punchlines on Davenport (f indecomposable)

1. Davenport's Original Question: $\exists$ DPs over $\mathbb{Q}$? From Mult. Thm #2 (p. 15) $\Longrightarrow$ g is complex conjugate to f. So, the answer is "No!"
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 Davenport pair over some field.
3. Degrees of DPs: $n = 7, 11, 13, 15, 21, 31$. For each n, we know exactly what fields carry DPs.
4. Two equivalent doubly transitive reps. and n-cycle: Except for one of deg 11, all are PGL_{v+1}s (from classification).

§IV.C. From #3, Hints at the *Genus 0 Problem*

For the cases $n = 7, 13, 15$ there are non-trivial Möbius equivalence (p. 4) families of Davenport pairs. For $n = 7 = 1 + 2 + 2^2$, $G_f = \mathrm{PGL}_3(\mathbb{Z}/2)$.

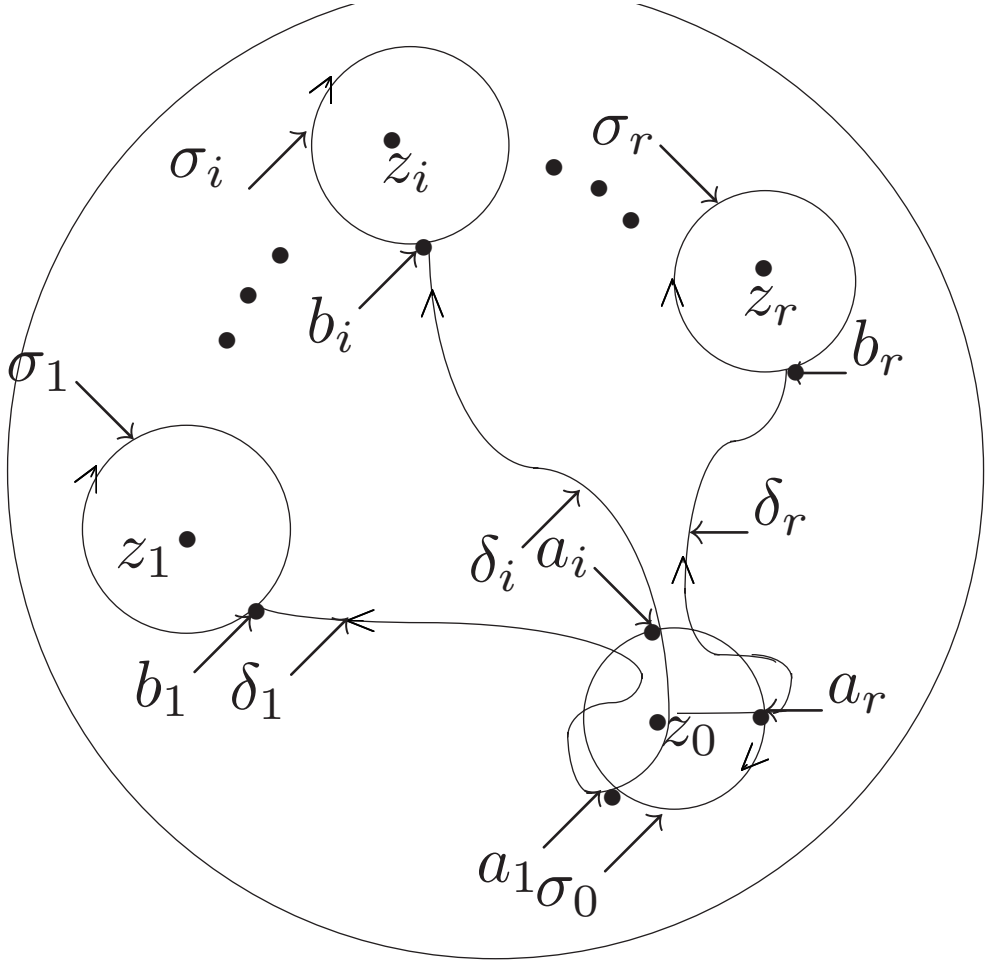
Example branch cycles: $(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ with $\sigma_1, \sigma_2, \sigma_3$ involutions, each fixing the 3 points, on some hyperplane, and σ_4 is a 7-cycle. R(iemann)-H(urwitz) (App. B) says any cover with these branch cycles has genus $\mathbf{g}_7 = 0$:

(*^{5}) $2(7+\mathbf{g}_7\text{-}1) = \sum_{i=1}^{4} \mathrm{ind}(\sigma_i) = 3 \cdot 2 + 6 \implies \mathbf{g}_7 = 0$.

Comments on the three families $n = 7, 13, 15$

- Their Möbius equivalence classes form a genus 0 j-line cover. Each has definition field $\mathbb{Q}$, but is not a modular curve.
- These form approximately half of the genus 0 families of polynomials whose monodromy groups aren't close to dihedral or Alternating groups as determined by Müller [Mü].
- Data from other problems [Fr80] also gave something akin to the result here: Only polynomials of finitely many degrees have (close to) projective linear groups as monodromy group.

Genus 0: Excluding groups related to A_n, S_n, D_n and $\mathbb{Z}/n$s, rational functions have only finitely other possible monodromy groups.



App. A: Punctured Sphere Classical Generators: Explanation next 2 pages

Pieces in the figure

Ordered closed paths $\delta_i\sigma_i\delta_i^{-1} = \bar{\sigma}_i,\ i = 1, \ldots, r,$ are *classical generators* of $\pi_1(U_{\boldsymbol{z}}, z_0)$.

Discs, $i = 1, \ldots, r$: D_i with center z_i; all disjoint, each excludes z_0; b_i be on the boundary of D_i.

Clockwise orientation: Boundary of D_i is a path σ_i with initial and end point b_i; δ_i a simple *simplicial* path: initial point z_0 and end point b_i. Assume δ_i meets none of $\sigma_1, \ldots, \sigma_{i-1}, \sigma_{i+1}, \ldots, \sigma_r$, and it meets σ_i only at its endpoint.

Meeting Boundary of D_0

D_0 intersections: D_0 with center z_0; disjoint from each $D_1, \ldots, D_r$. Consider a_i, first intersection of δ_i and boundary σ_0 of D_0.

Crucial ordering: Conditions on $\delta_1, \ldots, \delta_r$:

- pairwise nonintersecting, except at z_0; and
- $a_1, \ldots, a_r$ are in order clockwise around σ_0.

Since paths are simplicial, last condition is independent of D_0, for D_0 sufficiently small.

App. B: R(iemann)-H(urwitz)

R-H: Computes the genus g_X of a degree n cover $\varphi : X \longrightarrow \mathbb{P}^1_z$ from these ingredients.

- $\boldsymbol{z}_\varphi$ are the branch points, and $(\bar{\sigma}_1, \ldots, \bar{\sigma}_r)$ are classical generators (App.A$_1$) of $\pi_1(U_{\boldsymbol{z}_\varphi})$.
- $X^0 = \varphi^{-1}(U_{\boldsymbol{z}_\varphi})$. So, $\varphi^0 : X^0 \longrightarrow U_{\boldsymbol{z}}$ is unramified, giving $\varphi_* : \pi_1(U_{\boldsymbol{z}_\varphi}) \longrightarrow S_n$.
- $\varphi_*(\bar{\sigma}_1, \ldots, \bar{\sigma}_r) = (\sigma_1, \ldots, \sigma_r)$.

Branch cycles and the genus

With $\mathrm{ind}(\sigma_i) = n - |\sigma_i \text{ orbits}|$,

$$2(n+g_X-1)=\sum_{i=1}^{r}\mathrm{ind}(\sigma_i).$$

Then, $(g_1,\dots,g_r)$ are *branch cycles* of φ.

Exercise:Compute genus of a cover with branch cycles $\boldsymbol{g} \in \mathrm{Ni}(D_{p^k+1}, \mathbf{C}_{2^4})^{\mathrm{abs}}$ in §I.B (p. 5). Same for $\boldsymbol{g} \in \mathrm{Ni}(D_{p^k+1}, \mathbf{C}_{2^4})^{\mathrm{in}}$.

App.C. Dragging a function by its branch points

Continuity on the space of such f s: You can drag the classical generators on $U_{\boldsymbol{z}^0} = \mathbb{P}^1_z \setminus \boldsymbol{z}^0$ along any path $P(t), t \in [0,1]$ based at $\boldsymbol{z}^0 \in U_r$ to classical generators on $U_{P(t)}$.

Upshot: You can drag f_0 to f_t *by its branch points*. If P is closed, representing $[P] \in \pi_1(U_r, \boldsymbol{z}^0)$, then f_1 (usually) has a different bcd, denoted $(\boldsymbol{g})q_{[P]}$, (relative to the original classical generators).

Bibliography

[A-O-S] 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, The 2-transitive permutation representations 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, The field of definition of function fields and a problem in the reducibility of polynomials in two variables, Ill. J. Math. 17 (1973), 128-146.

[Fr87] M. Fried, Irreducibility results for separated variables equations, J. Pure and Appl. Alg. 48 (1987), 9-22.

[Fr99] M. Fried, Variables Separated Polynomials and Moduli Spaces, No. Th. in Prog., eds. K. Gyory, H. Iwaniec, J. Urbanowicz, Schinzel Festschrift, Sum. 1997, Walter de Gruyter, Berlin-NY (Feb. 1999), 169-228.

[Fr05] M. Fried, Relating two genus 0 problems of John Thompson, Volume for John Thompsons 70th birthday, in Progress in Galois Theory, H. Voelklein and T. Shaska editors 2005 Springer Science, 51-85.

[GLS] D. Gorenstein, R. Lyons, R. Solomon, The Classification of Finite Simple Groups, Number 3, Mathematical Surveys and Monographs, 40 ISBN:0821803913.

[LPS] M. Liebeck, C. Praeger, J. Saxl, The maximal factorizations of the finite simple groups and their automorphism groups, Mem. AMS 86 #432 (1990).

[Mü95] P. Mller, Primitive monodromy groups of polynomials, Proceedings of the Recent developments in the Inverse Galois Problem conference, vol. 186, 1995, AMS Cont. Math series, pp. 385401.

[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.