Computing Galois groups II

David P. Roberts
University of Minnesota, Morris

1. Frobenius computations:
Example with $G = S_{15875}$

2. Three-point covers and specialization:
Malle's M_{22} cover

3. Coarse vs. fine comparison:
Bosman's $PGL_2(\mathbb{F}_q)$ polynomials

1. Frobenius Computations: Example with $G = S_{15875}$. A criterion of Jordan says that if a Frobenius partition $\lambda_p \vdash n$ contains a prime $j \in (n/2, n-3]$ then a transitive G is all of A_n or S_n. If the Galois group is really S_n then a given λ_p has a Jordan prime j with probability

$$\sum_{j \in (n/2, n-3]} \frac{1}{j} \approx \frac{\log 2}{\log n} \quad (\approx 7\% \text{ for } n = 15875).$$

Other more complicated criteria have weaker hypotheses and give the same conclusion.

Example: Several years ago we found a polynomial with degree $n = 15875$ and discriminant $D = -2^{130729}5^{63437}$. To prove that its Galois group is all of S_{15875} we used a criterion of Manning and four Frobenius partitions:

p	$\lambda_p \vdash 15875$										
3	10194	3365	2123	155	20	10	5	3			
7	7332	2492	1642	1388	1077	1011	818	72	24	10	9
11	9784	3238	1272	648	480	143	139	133	17	12	9
13	6808	4493	3803	626	74	39	13	8	6	3	2

2. Three-point covers and specialization: Malle's M_{22} cover. The theory of three-point covers proves the existence of one-parameter families of number fields with quite varied generic Galois group (e.g. the monster sporadic group M with $|M| \approx 8 \cdot 10^{53}$). The place $v = \infty$ plays a central role in this theory.

As an example, the polynomial

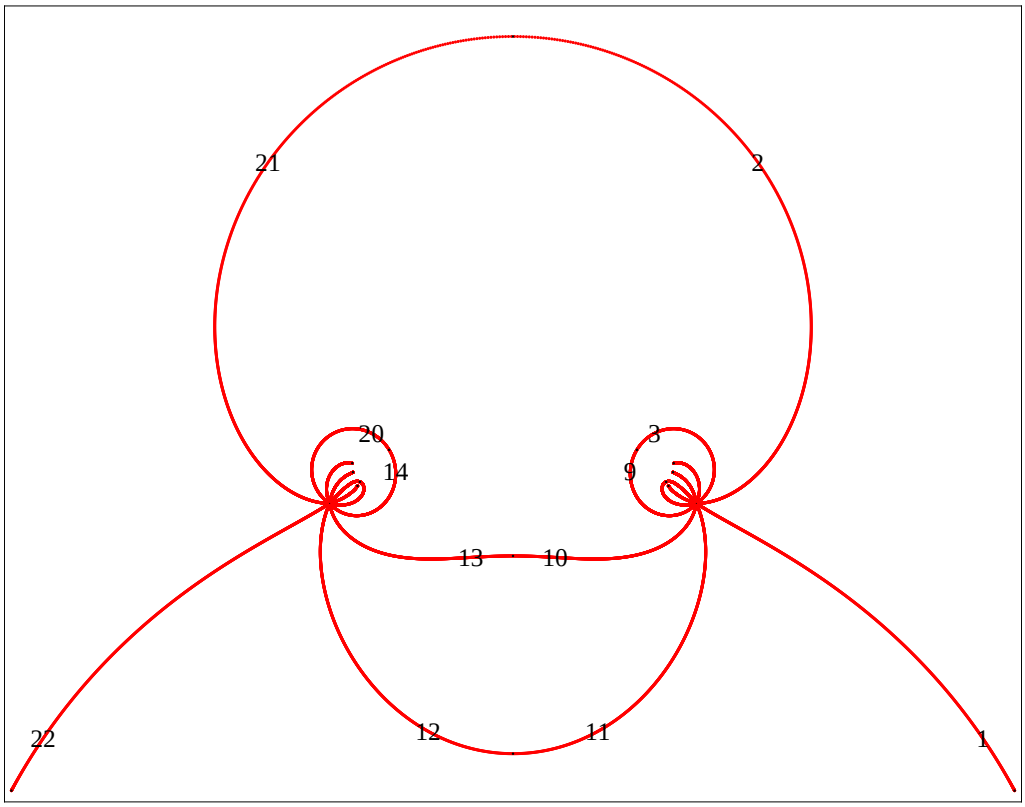
$$f(t,x) = \left(19x^3 - 12x^2 + 28x + 32\right)^2 \cdot \left(5x^4 + 34x^3 - 119x^2 + 212x - 164\right)^4 - 2^{22}t\left(x^2 - x + 3\right)^{11}$$

has discriminant $-2^{484}11^{253}(t-1)^7t^{15}$. For generic t it has Galois group the Mathieu group M_{22} of order

$$22 \cdot 21 \cdot 20 \cdot 48 = 443,520 = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11.$$

Note that $f(1,x)$ factors as $f_7(x)^2 f_8(x)$.

Solving for t gives $t = \phi(x)$. Thinking of the rational function ϕ geometrically as a map from P^1_x to P^1_t we can look at the preimage of $[1, \infty]$. This *dessin* has 22 edges:



Rotation operators about endpoints are
b=(2, 21)(3, 9)(6, 8)(10, 13)(11, 12)(14, 20)(15, 17)
(1)(4)(5)(7)(16)(18)(19)(22),
c=(1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11)(12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22).

They satisfy $\langle b, c \rangle = M_{22}$. The operator a defined by $abc = 1$ has cycle structure $4^4\,2^3$.

For all $t \in \mathbb{Q} - \{0, 1\}$ let $F(t)$ be the number field $\mathbb{Q}[x]/f(t, x)$. For $t \in (1, \infty)$, the set $X(t)_\infty$ is identified with the set of edges. One has $G(t)_\infty \subseteq M_{22}$ with equality generically.

For generic t, Frobenius elements suffice to prove $G_\infty(t) = M_{22}$.

If $p \notin \{2, 11\}$, ramification of $F(t)$ is tame, with τ_p being $[a^i]$, $[b^i]$, or $[c^i]$, according to whether t is p-adically i-close to 0, 1, or ∞. The general version of this statement lets one understand tame specialization of general three-point covers, even without an equation.

There are non-generic specialization points. For example $F(2401/192)$ has Galois group $PGL_2(\mathbb{F}_{11})$. It has the same splitting field as

$$x^{12} - 4x^{11} - 4x^{10} + 16x^9 + 24x^8 - 30x^7 - 78x^6 \\ -18x^5 + 72x^4 + 86x^3 + 52x^2 + 16x + 2.$$

The root discriminant of the splitting field is $2^{7/6}\, 3^{5/6}\, 11^{3/4} \approx 52.75$. This is the lowest known GRD of a $PGL_2(\mathbb{F}_{11})$ field.

3. Coarse vs. fine comparison: Bosman's $PGL_2(\ell^f)$ polynomials. In a series of papers, Bosman starts with classical modular forms and numerically computes associated degree $\ell^f + 1$ polynomials. For example, from the unique modular form $\sum a_k q^k \in \mathbb{Z}[[q]]$ of weight 22 and level 1, considered modulo $\ell = 23$, he gets

$$x^{24} - 11x^{23} + 46x^{22} - 1127x^{20} + 6555x^{19} - 7222x^{18}$$
$$-140737x^{17} + 1170700x^{16} - 2490371x^{15} - 16380692x^{14}$$
$$+99341324x^{13} + 109304533x^{12} - 2612466661x^{11}$$
$$+4265317961x^{10} + 48774919226x^9 - 244688866763x^8$$
$$-88695572727x^7 + 4199550444457x^6$$
$$-106063480531 44x^5 - 252034146530 24x^4$$
$$+1858433461820 48x^3 - 2288229551238 83x^2$$
$$-1021047515459130x + 278665520487 6088.$$

Assuming the numerical computation introduces no errors, the set of bad primes and the Galois group are known from the source, here $\{23\}$ and $PGL_2(23)$. Even Frobenius classes are almost completely known from the a_p.

The field discriminant of the computed polynomial is -23^{43}. Frobenius partitions λ_p agree with their a_p through very large p, and hence agree with $PGL_2(\mathbb{F}_{23})$-statistics.

$a_p^2/p \in \mathbb{F}_{23}$	ϵ	Type	λ_p	#	Freq
$5, 10, 17, 22$	$-$	I	24	2046	$4/24$
$7, 20$	$-$	I	8^3	1032	$2/24$
$9, 18$	$+$	I	12^2	1022	$2/24$
3	$+$	I	6^4	520	$1/24$
2	$+$	I	4^6	474	$1/24$
1	$+$	I	3^8	520	$1/24$
0	$+$	I	2^{12}	252	$1/48$
$11, 14, 15, 19, 21$	$-$	S	$22\,1^2$	2725	$5/22$
0	$-$	S	$2^{11}\,1^2$	277	$1/44$
$6, 8, 12, 13, 16$	$+$	S	$11^2\,1^2$	2783	$5/22$
4	$+$	U	$23\,1$	491	$1/23$
4	$+$	ISU	1^{24}	0	$1/\lvert G\rvert$

This absolutely enormous agreement does not by itself rigorously confirm that the computed polynomial is correct. One way to obtain rigorous confirmation is to verify that the Galois group is indeed $PGL_2(\mathbb{F}_{23})$. Then the Khare-Wintenberger Serre result can be applied.

In general, let F be a number field, v a place of $\mathbb{Q}$, and index roots in C_v so that $X_v = \{1, \ldots, n\}$. Suppose one highly suspects G_v is in a conjugacy class $\mathcal{G}$ of subgroups $G \subset S_n$, say self-normalizing. Then $|\mathcal{G}| = n!/|G|$. One wants to identify G_v among all its conjugates in $\mathcal{G}$.

Knowledge that G_v contains the Frobenius element $\sigma_v \in S_n$ cuts down the possibilities for G_v to a smaller set $\mathcal{G}(\sigma_v)$. Suppose that σ_v has cycle type λ_v. Let $|S_n[\lambda_v]|$ be the number of permutations of cycle type λ_v in S_n. Let $|\mathcal{G}[\lambda_v]|$ be the number of such permutations in any $G \in \mathcal{G}$. Then the savings is a factor of

$$\frac{|\mathcal{G}|}{|\mathcal{G}(\sigma_v)|} = \frac{|S_n[\lambda_v]|}{|\mathcal{G}[\lambda_v]|}.$$

For $\lambda_v = 1^n$, these ratios are one and in this case there is of course no savings.

In general, for $G = PGL_2(\ell) \subseteq S_{\ell+1}$ one has

$$|\mathcal{G}| \;=\; \frac{(\ell+1)!}{(\ell+1)\ell(\ell-1)} = (\ell-2)!$$

For e.g. c and σ of cycle types $2^{(\ell+1)/2}$ and $\ell+1$ respectively,

$$|\mathcal{G}(c)| \;=\; \frac{(\ell-2)!}{(\ell-2)!!} = 2^{(\ell+1)/2}(\frac{\ell+1}{2})!$$

$$|\mathcal{G}(\sigma)| \;=\; \frac{(\ell-2)!}{(\ell-2)!} = 1!$$

Time to compute G_p in our example:

p	λ_p	poss	Timing
2	$11^2\,1^2$	22	(poly bad)
3	$11^2\,1^2$	22	17.55 sec
5	24	1	3.96 sec
7	$22\,1^2$	2	5.22 sec
11	$22\,1^2$	2	5.24 sec
13	$11^2\,1^2$	22	18.47 sec
17	8^3	128	25.04 sec
19	$22\,1^2$	2	4.63 sec
29	–	–	(field bad)
29	4^6	122880	7757.54 sec
31	3^8	11022480	(error)
37	24	1	3.79 sec
43	$22\,1^2$	2	4.57 sec
47	$11^2\,1^2$	22	23.46 sec
53	$2^{11}\,1^2$	7431782400	(error)
59	6^4	1296	138.83 sec
61	24	1	3.93 sec

Using $C = \mathbb{Q}_{p^f}$ instead of $C = \mathbb{C}$ can be crucial!