ON ELKIES’ METHOD FOR BOUNDING THE TRANSITIVITY DEGREE OF GALOIS GROUPS

DOMINIK BARTH AND ANDREAS WENZ

Abstract. In 2013 Elkies described a method for bounding the transitivity degree of Galois groups. Our goal is to give additional applications of this technique, in particular verifying that the Galois group of the degree 276 polynomial over a degree 12 number field computed by Monien is isomorphic to the sporadic Conway group $\text{Co}_3$.

1. Preliminaries

For a fixed number field $K$ let $p$ and $q$ be coprime polynomials in $K[X]$. Our goal is to find the arithmetic Galois group of the degree $n$ polynomial $p(X) - tq(X) \in K(t)[X]$, that is

$$A := \text{Gal}(p(X) - tq(X) \mid K(t)).$$

Let $N$ be the splitting field of $p(X) - tq(X)$ over $K(t)$ and $L := \bar{K} \cap N$ be the algebraic closure of $K$ in $N$. Then, the geometric Galois group of $p(X) - tq(X)$ is given by $G := \text{Gal}(p(X) - tq(X) \mid L(t))$. It is well known that $G$ is normal in $A$.

In order to study $A$ and $G$, we will reduce the above polynomials modulo a suitable prime: The ring of integers of $K$ will be denoted by $\mathcal{O}_K$. For a fixed prime ideal $p$ in $\mathcal{O}_K$ we write $p^\alpha$ and $q^\alpha$ for the reduction of $p$ and $q$ modulo $p$. Accordingly, the arithmetic and geometric Galois group of the reduced polynomial are defined in the same way:

$$A_p := \text{Gal}(p^\alpha(X) - tq^\alpha(X) \mid (\mathcal{O}_K/p)(t))$$

and

$$G_p := \text{Gal}(p^\alpha(X) - tq^\alpha(X) \mid L_p(t))$$

where $L_p := \bar{\mathcal{O}_K/p} \cap N_p$ with $N_p$ being the splitting field of $p^\alpha(X) - tq^\alpha(X)$. Again, $G_p$ is normal in $A_p$.

2. A method by Elkies

The following technique described by Elkies (see [3]) bounds the transitivity degree of $G_p$:

Assume, $G_p$ is $k$-transitive and $A_p = G_p$. Let $C_0$ and $C_1$ be the projective $t$- and $x$-lines over the finite field $\mathbb{F}_\lambda \cong \mathcal{O}_K/p$. By introducing the relation $p^\alpha(x) - tq^\alpha(x) = 0$ we obtain a cover $C_1/C_0$ ramified over exactly $m$ points with ramification structure $(s_1, \ldots, s_m) \in (S_n)^m$. Its Galois closure will be denoted by $\tilde{C}$.

Let $(G_p)_k$ be the stabilizer of a $k$-element set in $G_p$ and $C_k := \tilde{C}/(G_p)_k$. The corresponding cover $C_k/C_0$ is of degree $\binom{n}{k}$ with ramification structure $(\sigma_1, \ldots, \sigma_m)$ induced by the natural action of $(s_1, \ldots, s_m)$ on $k$-element subsets. As $G_p$ acts faithfully on $n$ elements, it can be shown easily that the action on $k$-element subsets is also faithful if $k \not\in \{0, n\}$. In particular $\text{ord}(\sigma_i) = \text{ord}(s_i)$ for $i = 1, \ldots, m$. Further note that $C_k$ is an irreducible curve with full
constant field $\mathbb{F}_\lambda$ (due to $A_\pi = G_\pi$). Therefore, the number of $\mathbb{F}_\lambda$-rational points on $C_k$ has to satisfy the Hasse-Weil bound $|\#C_k(\mathbb{F}_\lambda) - (\lambda + 1)| \leq 2g(C_k)\sqrt{\lambda}$, in particular

$$ (1) \quad \#C_k(\mathbb{F}_\lambda) \leq \lambda + 1 + 2g(C_k)\sqrt{\lambda}. $$

Here, $g(C_k)$ denotes the genus of $C_k$. In order to check if $C_k$ is indeed compatible with the above bound, we need to determine $\#C_k(\mathbb{F}_\lambda)$ and $g(C_k)$.

We will use the following notation: For a permutation $s \in S_n$ let $\pi_k(s)$ be the number of invariant $k$-element subsets of $s$.

**Counting $\mathbb{F}_\lambda$-rational points on $C_k$.** With finitely many exceptions the $\mathbb{F}_\lambda$-rational points on $C_k$ correspond to a degree $k$ factor of a $\mathbb{F}_\lambda$-specialization of $p_\lambda(X) - tq_\lambda(X)$ over $\mathbb{F}_\lambda(t)$.

Fix $t_0 \in \mathbb{F}_1^1(\mathbb{F}_\lambda)$ not contained in the ramification locus $S$ of $p_\lambda(X) - tq_\lambda(X)$. The Frobenius permutation on the $n$ roots of the specialization $p_\lambda(X) - t_0q_\lambda(X)$ will be denoted by $\text{Frob}(t_0)$. Then, the number of $\mathbb{F}_\lambda$-rational points on $C_k$ lying over $t_0$ is given by $\pi_k(\text{Frob}(t_0))$, therefore

$$ (2) \quad \#C_k(\mathbb{F}_\lambda) \geq \sum_{t_0 \in \mathbb{F}_1^1(\mathbb{F}_\lambda) \backslash S} \pi_k(\text{Frob}(t_0)). $$

**Computing the genus of $C_k$.** Since the cover $C_k/\mathbb{C}_0$ has ramification structure $(\sigma_1, \ldots, \sigma_m)$ the Riemann-Hurwitz formula yields

$$ (3) \quad g(C_k) = 1 - \binom{n}{k} + \frac{1}{2} \sum_{i=1}^{m} \text{ind}(\sigma_i) $$

where $\text{ind}(\sigma_i) := \binom{i}{k} - \text{number of cycles of } \sigma_i$. One can easily deduce

$$ (4) \quad \text{ind}(\sigma_i) \leq \left( \binom{n}{k} - \pi_k(s_i) \right) \left( 1 - \frac{1}{\text{ord}(s_i)} \right). $$

Note that equality holds if the order of $s_i$ is prime.

**Picking a sufficiently large prime.** Contrary to the previous sections we now assume that $G_\pi$ is not $k$-transitive. Let $d$ be the number of orbits of $G_\pi$ acting on $k$-element subsets. We expect $\sum_{t_0 \in \mathbb{F}_1^1(\mathbb{F}_\lambda) \backslash S} \pi_k(\text{Frob}(t_0)) \approx d\lambda$ for large $\lambda$ due to the orbit-counting theorem in combination with Chebotarev’s density theorem.

By comparing the latter heuristics with the Hasse-Weil bound (1) we get the approximate estimate $d\lambda \leq \lambda + 2g(C_k)\sqrt{\lambda}$, which leads to $\lambda \leq \frac{4g(C_k)^2}{(d-1)^2}$ in the case $d > 1$. If we choose $\lambda$ to be sufficiently greater than $\frac{4g(C_k)^2}{(d-1)^2}$, we are able to distinguish whether $G_\pi$ is $k$-transitive.

3. Applications

3.1. The sporadic group $\text{Co}_3$. In this section we will refer to the polynomials $p(X) := -k_3\tilde{p}_3(X)$ and $q(X) := k_2\tilde{p}_2(X)$ presented in [5] Proposition 1] of degree 276. They are contained in $K[X]$ with $K := \mathbb{Q}(\alpha)$ where

$$ \alpha^{12} - 2\alpha^{11} + 9\alpha^{10} - 20\alpha^9 + 38\alpha^8 - 73\alpha^7 + 101\alpha^6 - 86\alpha^5 + 55\alpha^4 - 46\alpha^3 + 42\alpha^2 - 24\alpha + 6 = 0. $$
An easy computation shows that \( p(X) - tq(X) \in K(t)[X] \) is ramified over 0, 1 and \( \infty \) with ramification structure \((3^{92}, 7^{39}, 1^3, 2^{132}, 1^{12})\).

**Theorem.** The polynomial \( p(X) - tq(X) \in K(t)[X] \) defines a regular Galois extension over \( K(t) \) with Galois group isomorphic to the sporadic Conway group \( Co_3 \).

**Proof.** Pick the prime ideal \( \mathfrak{p} := (7 \cdot 10^9 + 1, \alpha + 2738443742) \) in \( \mathcal{O}_K \) of norm \( \lambda := 7 \cdot 10^9 + 1 \). Note that \( \mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_\lambda \). Because

\[
p_p(X) = \frac{p(X) - tq(X)}{X - a} \in \mathbb{F}_\lambda[t][X]
\]

is irreducible, \( A_p \) must be 2-transitive. Additionally, the discriminant of \( p_p(X) = -q_p(X) \in \mathbb{F}_\lambda[t][X] \) is a square. Combining both results, we find \( A_p \in \{Co_3, A_{276}\} \) by the classification of finite 2-transitive groups. In both cases we have \( G_p = A_p \) because \( G_p \) is normal in \( A_p \).

Under the assumption that \( G_p \) is 3-transitive we study the curve \( C_3 \). Combining (1) and (3) yields \( g(C_3) = 40782 \). Now, (2) gives us \#\( C_3(\mathbb{F}_\lambda) \geq 13999925705 \) whereas \#\( C_3(\mathbb{F}_\lambda) \leq 13824133843 \) by the Hasse-Weil bound (1). This is a contradiction, thus \( G_p \) cannot be 3-transitive. We remain with \( G_p = Co_3 \).

Since \( p \) is a prime of good reduction for \( p(X) - tq(X) \in K(t)[X] \), a theorem of Beckmann, see [4, Proposition 10.9], implies \( G = G_p = Co_3 \). Since \( G \) is normal in \( A \) and \( N_{S_{276}}(Co_3) = Co_3 \) we end up with \( A = G = Co_3 \). \( \square \)

The most delicate part in the previous proof is the computation of the right hand side of (2). In the following we explain in greater detail this time consuming task (implementation in PARI/GP [6] with a total computing time of about 8 days using 550 threads simultaneously at the High Performance Computing Cluster at the University of Würzburg).

For the sake of simplicity we write \( f(X) := p_p(X) - t_0q_p(X) \) for some \( t_0 \not\in S \). In the case \( k = 3 \) the following holds: If \( f(X) \in \mathbb{F}_\lambda[X] \) has exactly \( d_i \) irreducible factors of degree \( i \) for \( i \in \{1, 2, 3\} \) then \( \pi_3(\text{Frob}(t_0)) = (d_3) + d_1d_2 + d_3 \). Note that if a specialization reduces the degree, we have to add 1 to \( d_1 \).

In order to find \( d_1 \) we compute \( p_1(X) := \gcd(X^{\lambda} - X, f(X)) \). Clearly, \( d_1 = \deg(p_1) \). Since \( \lambda \) is too large for an efficient computation, we replace \( X^{\lambda} - X \) with its reduction modulo \( f(X) \), which can be determined by the exponentiation by squaring-method. In the same fashion we find \( d_2 \) and \( d_3 \): For \( p_2(X) := \gcd(X^{\lambda} - X, \frac{f(X)}{p_1(X)}) \) and \( p_3(X) := \gcd(X^{\lambda} - X, \frac{f(X)}{p_1(X)p_2(X)}) \) we have \( d_2 = \frac{1}{2} \deg(p_2) \) and \( d_3 = \frac{1}{3} \deg(p_3) \).

Partial results for the computation of the right hand side of (2) can be found in the ancillary Magma-readable file.

### 3.2. The symplectic group \( \text{PSp}_6(2) \)

In [1] both authors and Joachim König computed four-branch-point covers with Galois group \( G \) isomorphic to the 2-transitive symplectic group \( \text{PSp}_6(2) \). In order to verify \( G = \text{PSp}_6(2) \), standard techniques yield that \( G \) is either \( \text{PSp}_6(2) \) or an alternating group. In contrast to the arguments given in [1] to rule out the last case we now apply Elkies’ method to give an alternative proof for \( G = \text{PSp}_6(2) \). Assume, \( G \) is 3-transitive, then for both covers appearing in [1], see Theorem 4.2 and Theorem 5.2, we get a contradiction by computing \#\( C_3(\mathbb{F}_\lambda) \):
In the accompanying file we provide a program written in Magma [2] to illustrate the computation of \( \#C_3(\mathbb{F}_\lambda) \) for both PSp\(_6(2)\)-covers.

**Acknowledgments**

We would like to thank Stephan Elsenhans and Peter Müller for some helpful discussions.

**References**

[1] Dominik Barth, Joachim König, and Andreas Wenz. An approach for computing families of multi-branch-point covers and applications for symplectic Galois groups, 2018, arXiv:1803.08778.

[2] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. J. Symbolic Comput., 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[3] Noam D. Elkies. The complex polynomials \( P(x) \) with \( \text{Gal}(P(x) - t) \cong M_{23} \). In ANTS X. Proceedings of the tenth algorithmic number theory symposium, San Diego, CA, USA, July 9–13, 2012, pages 359–367. Berkeley, CA: Mathematical Sciences Publishers (MSP), 2013.

[4] Gunter Malle and Bernd Heinrich Matzat. Inverse Galois theory. 2nd edition. Berlin: Springer, 2nd edition edition, 2018.

[5] Hartmut Monien. The sporadic group Co3, Hauptmodul and Belyi map, 2018, arXiv:1802.06923.

[6] The PARI Group. PARI/GP version 2.11.1, Univ. Bordeaux, 2018, http://pari.math.u-bordeaux.fr/