EXPOSITIONES
MATHEMATICAE

Expo. Math 16 (1998), 263-270

Mathematical Note

Probabilistic Galois Theory of Reciprocal Polynomials

S. Davis[1], W. Duke[2], X. Sun[3]

1.Probabilistic Galois theory

What is the most likely Galois group of a randomly chosen monic integral polynomial of fixed degree n? Under appropriate assumptions the answer is: the full symmetric group S_n. This satisfying result was found by van der Waerden in 1936.

Instead of fixing a polynomial and studying its properties individually, probabilistic Galois theory studies a set of polynomials and the likely properties of a randomly chosen individual. One natural choice for the set is all monic integral polynomials $f(x) = x^n + a_1x^{n-1} + ... + a_n$ with

$$H(f) = \max(|a_1|, ...|a_n|) \leq N.$$

This set contains $(2N + 1)^n$ polynomials if N is an integer. Let us recall that the Galois group of f is defined to be the Galois group of its splitting field, that it acts as a permutation group on the roots of f and hence may be considered as a subgroup of S_n. This action is transitive exactly when the polynomial is irreducible over the rationals.

Probabilistic Galois theory begins by trying to count the number $R_n(N)$ of reducible polynomials in our set. Let's suppose that $n > 2$, for the case $n = 2$ is a little different and easily handled. Van der Waerden [W1] gave the upper bound

[1] Research supported by a National Physical Science Consortium Fellowship, by Rutgers University and by stipend support from the National Security Agency
[2] Research supported in part by NSF Grant DMS-9500797
[3] Research supported by Rutgers University and The Institute of Applied Mathematics, Academia Sinica, Beijing.

0723-0869/98/030263-08$3.10

$$R_n(N) \ll N^{n-1}. \tag{1}$$

Here we are using the handy notation $\ll$ to shorten the equivalent formulation: $R_n(N) \le CN^{n-1}$ for some positive constant C (the *implied constant*) depending only on n. Thus, since the total number of polynomials in our set is about $(2N)^n$, the probability that a randomly chosen polynomial is reducible is $\ll N^{-1}$, which tends to 0 as N tends to infinity. The reader is encouraged to observe that the upper bound for $R_n(N)$ is *sharp* in the sense that no exponent smaller than $n-1$ is valid. Actually, in 1963 Chela [Che] found the asymptotic formula

$$R_n(N) \sim c_n N^{n-1}$$

for a certain positive constant c_n.

We are now in a position to reconsider our opening question. Let us denote by $E_n(N)$ the number of polynomials in our set with Galois group a proper subgroup of S_n. In the classical terminology, we are counting the polynomials "with affect." Since S_n acts transitively on the roots it is clear that $R_n(N) \le E_n(N)$. In fact, van der Waerden suggested that the bound (1) should also hold for $E_n(N)$. Although he was not able to show this, he did give a sufficiently good estimate to conclude that S_n is the dominant Galois group, i.e. the probability that the Galois group is all of S_n tends to 1 as $N \to \infty$. The actual bound for $E_n(N)$ was improved by Knobloch [Kno] in 1956 and then a big advance in the subject was made by Gallagher [Gal] in 1973 when he applied a powerful tool from analytic number theory, the large sieve, to this problem. Gallagher obtained the bound

$$E_n(N) \ll N^{n-1/2} \log N,$$

giving a significant step toward the expected bound N^{n-1}. Later Lefton [Lef], using a different method, improved this when $n = 3$ to $N^{2+\epsilon}$ for any $\epsilon > 0$ thus getting essentially the best possible result for cubic polynomials.

Acknowledgment: We thank R. Bumby for helpful comments on an earlier version of this paper.

2. Reciprocal polynomials

Our principal objective in this paper is to illustrate some of the techniques used in probabilistic Galois theory and at the same time make a contribution to the subject by considering a natural variation of our opening problem. We impose invariance properties on the polynomials by considering the simplest such property, namely that the polynomial f be reciprocal: $f(x) = x^n f(1/x)$. This means that the coefficients of f are palindromic, that is $a_n = 1, a_{n-1} = a_1, \ldots$. The roots of such polynomials occur in reciprocal pairs. Also, a simple computation shows that $f(x) = x^m g(x + \frac{1}{x})$ for some polynomial g of degree m. We shall assume that $n = 2m$ is even since every odd degree reciprocal polynomial has -1 as a root.

We find that the Galois group of a reciprocal polynomial is usually as large as possible. This group is isomorphic to the group of all signed permutations on $m = n/2$ objects. We realize it as a subgroup $\mathcal{G}$ of S_{2m} by taking for the m objects the reciprocal root pairs and interpreting a change of sign as an interchange of the roots of a given pair. The group $\mathcal{G}$ has order $2^m m!$ and is isomorphic to a semidirect product of $(Z/2Z)^m$ with S_m. It is clear that the Galois group of a reciprocal polynomial is a subgroup of $\mathcal{G}$ since the Galois group must send a pair of reciprocal roots to another such pair.

Let $\mathcal{E}_m(N)$ be the number of reciprocal polynomials f of degree $2m$ with $H(f) \le N$ and with Galois group a proper subgroup of $\mathcal{G}$. The following result is proved in section 4.

Theorem 1. *We have that*

$$\mathcal{E}_m(N) \ll N^{m-1/2} \log N$$

with the implied constant depending only on m.

Since the total number of reciprocal polynomials we are considering is about $(2N)^m$ we see that this result implies that the Galois group of a random reciprocal polynomial is likely to be $\mathcal{G}$.

To prove this we use a development of the ideas of van der Waerden and Gallagher together with some new combinatorial arguments. The main idea is to detect reciprocal polynomials whose Galois groups are proper subgroups of $\mathcal{G}$ by showing that certain cycle types must be missed by the groups and hence, using a fundamental fact from Galois theory, the polynomials must not factor modulo primes in the corresponding ways. Then the large sieve

inequality limits the number of reciprocal polynomials which do not have these corresponding splitting types. This is done by treating the polynomials as integer vectors whose reductions modulo primes may be sieved.

It appears likely that more general results can be proved for other classes of invariant polynomials.

3. Cycles and splitting types

In this section we give some needed information on the structure of $\mathcal{G}$ and on the factorization of a reciprocal polynomial modulo a prime.

Let N_ℓ be the number of ℓ-cycles in $\mathcal{G}$.

Lemma 1. *For $\ell \geq 2$ we have $N_\ell = 0$ unless $\ell = 2k$, in which case*

$$N_{2k} = 2^{k-1}\binom{m}{k}(k-1)!.$$

Proof. That $N_\ell = 0$ for odd $\ell > 1$ and $N_2 = m$ follow since $\mathcal{G}$ is pair preserving. We claim that every $2k$-cycle can be uniquely expressed as a product of an odd number of those 2-cycles in $\mathcal{G}$ which move only those roots permuted by the $2k$-cycle and a k-cycle of (ordered) pairs of reciprocal roots. We count the number of k-cycles of pairs by noting that there are $\binom{m}{k}$ ways to pick k pairs in the representation and $(k-1)!$ ways they can be ordered. There are exactly 2^{k-1} choices of combinations of 2-cycles. The product of these gives Lemma 1.

The claim is shown by combining the following two facts. The number of 2-cycles in the decomposition is odd since any product of a 2-cycle and a k-cycle of pairs is a $2k$-cycle. For example,

$$(i,-i)(1,...,k)(-1,...,-k) = (1,...,i,-(i+1),...,-k,-1,...,-i,i+1,...k)$$

The uniqueness of the decomposition is based on the fact that $\mathcal{G}$ is a semidirect product of two subgroups.

□

We next show that a proper subgroup of $\mathcal{G}$ must miss some cycles.

Lemma 2. *If a subgroup H of $\mathcal{G}$ contains 2-cycles, 4-cycles,$(2m-2)$-cycles and $2m$-cycles then $H = \mathcal{G}$.*

Proof. Since H contains a 2-cycle and a $2m$-cycle, by conjugation it contains all the 2-cycles. It is enough to show that H contains all 2-cycles of pairs. Since all 2-cycles are present in H, the decomposition in the proof of Lemma 1 implies that H contains a 2-cycle of pairs, α, an $(m-1)$-cycle of pairs, β and an m-cycle of pairs, γ. Without loss of generality, we let

$$\alpha = (i,j)(-i,-j), \qquad \gamma = (1,2,...,m)(-1,-2,...,-m)$$

where $i < j$. Let the pair represented by 1 and -1 be the fixed pair of β. By conjugation of α by the $i-1$ power of γ we obtain a 2-cycle of pairs, α', that acts on the fixed pair of β: $\alpha' = \gamma^{i-1}\alpha\gamma^{1-i} = (1, j-i+1)(-1,-(j-i+1))$. Then, by conjugation of α' by powers of β we obtain those 2-cycles of pairs which transpose this fixed pair with any other pair.

□

We also need to count the number of reciprocal polynomials which have certain factorization types modulo a prime p. Say a polynomial has *splitting type ℓ for p* if its factorization into irreducibles (mod p) consists of distinct factors which are all linear except for one factor of degree ℓ. Let $\omega_\ell(p)$ be the number of degree $2m$ reciprocal polynomials with coefficients defined (mod p) which have splitting type ℓ for p. The following lemma indicates a close relation exists between $\omega_\ell(p)$ and the number of corresponding cycles of $\mathcal{G}$. To prove the lemma, we will use the decomposition $f(x) = x^m g(x+\frac{1}{x})$ and the classical formula of Dedekind [Ded] (see also [LN]) for the number of all degree m irreducible polynomials (mod p) :

$$m^{-1}\sum_{d|m}\mu(d)p^{m/d}, \tag{2}$$

where μ is the Möbius function.

Lemma 3. *For $\ell \geq 2$ we have $\omega_\ell(p) = 0$ unless $\ell = 2k$ in which case*

$$\omega_{2k}(p) - \frac{N_{2k}}{|\mathcal{G}|}p^m \ll p^{m-1}.$$

Proof. First observe that a unique irreducible factor of degree $\ell > 1$ must be reciprocal. It follows that $\omega_\ell(p) = 0$ for odd $\ell > 1$ since an irreducible reciprocal polynomial must have even degree.

Let $f(x) = x^m g(x+\frac{1}{x})$. Note that for f to be irreducible g must be irreducible. This allows us to compute $\omega_{2m}(p)$, the number of irreducible

reciprocal polynomials, by counting the number of irreducible g and excluding those for which f is reducible. If g is irreducible then f cannot have a proper reciprocal factor. It follows that if g is irreducible yet f is reducible then

$$f(x) \equiv x^m h(x) h(1/x)$$

where h is irreducible and non-reciprocal of degree m. The number of such f is by (2) a polynomial in p with leading term $p^m/2m$ since when counting the polynomials $h(x)$, the reciprocal polynomials of degree m contribute at most $p^{m/2}$ when m is even, none otherwise. By (2) we conclude

$$\omega_{2m}(p) - \frac{p^m}{2m} \ll p^{m-1}. \tag{3}$$

To count $\omega_{2k}(p)$ generally we simply apply (3) with $m = k$ and count the remaining $2m - 2k$ linear factors, which occur in pairs. This leads to

$$\omega_{2k}(p) - \frac{p^{m-k}}{2^{m-k}(m-k)!} \frac{p^k}{2k} \ll p^{m-1}.$$

so the proof is finished by Lemma 1 and the formula $|\mathcal{G}| = 2^m m!$.

□

One may consider other cycle and splitting types, not just those special ones considered here which are sufficient for our purposes. In fact, Gallagher used a result similar to Lemma 3 for all cycle types of S_n.

4. Sieving polynomials by splitting type

The main tool used in the proof of Theorem 1 is a multidimensional form of the large sieve inequality that allows one to estimate the number of integral polynomials whose reductions modulo primes are not evenly distributed over all residue classes. Let $\pi(x)$ be the number of primes $p \le x$ and $\pi_{f,\ell}(x)$ be the number of primes $p \le x$ such that f has splitting type ℓ for p. Below we will prove, using the large sieve, that $\pi_{f,\ell}(x)$ does not differ much from $(N_\ell/|\mathcal{G}|)\pi(x)$ for most f. Precisely, we have

Lemma 4. *For each ℓ we have*

$$\sum_{H(f) \le N} (\pi_{f,\ell}(x) - (N_\ell/|\mathcal{G}|)\pi(x))^2 \ll N^m \pi(x)$$

where the sum is over reciprocal polynomials f, provided $N \ge x^2$.

Before proving Lemma 4, we show that it implies Theorem 1. By [W2, sec.61] we know that if f has splitting type ℓ for some prime p then the Galois group of f, as a permutation group on the roots of f, contains an ℓ-cycle. Thus by Lemma 2, each polynomial with Galois group a proper subgroup of $\mathcal{G}$ will have $\pi_{f,\ell}(x) = 0$ for some $\ell \in \{2, 4, 2m-2, 2m\}$. ¿From Lemma 4 with $x = \sqrt{N}$ we conclude that

$$\mathcal{E}_m(N) \ll N^m/\pi(\sqrt{N}) \ll N^{m-1/2} \log N$$

after applying the prime number theorem, and this is Theorem 1.

Lemma 4 is a particular application of the large sieve. To describe this, for each prime p, let $\Omega(p)$ be a subset of $Z^m/(pZ)^m$. For each vector $a \in Z^m$, let $P(a, x)$ be the number of primes $p \le x$ for which $a \pmod p$ is in $\Omega(p)$ and set

$$P(x) = \sum_{p \le x} |\Omega(p)| p^{-m}.$$

The following result, which is Lemma A in [Gal], shows that most integer vectors are evenly distributed in different residue classes modulo primes.

Lemma 5. *For $N \ge x^2$,*

$$\sum_{|a| \le N} (P(a, x) - P(x))^2 \ll N^m P(x)$$

where the implied constant depends only on m and $|a| = max(|a_1|, ..., |a_m|)$.

To apply this to Lemma 4, identify a with the coefficients $(a_1, \ldots, a_m)$ of f so $H(f) = |a|$ and $f \pmod p$ corresponds to $a \pmod p$. Let $\Omega(p)$ be the set of f having splitting type ℓ for p so $|\Omega(p)| = \omega_\ell(p)$ and $P(a, x) = \pi_{f,\ell}(x)$ By Lemma 3 we have

$$P(x) - (N_\ell/|\mathcal{G}|)\pi(x) \ll \sum_{p \le x} p^{-1} \ll \log(\log x).$$

Finally, Lemma 4 follows from Lemma 5 by a straightforward application of Cauchy's inequality.

We remark that Gallagher stated a result similar to Lemma 4 for all of the splitting types of S_n. Thus in concluding his theorem for $E_n(N)$, he summed over all splitting types where as we only used the four particular types in Lemma 2. Gallagher's ideas may be extended as we did for reciprocal polynomials to determine dominant Galois groups for other polynomial sets.

References

[Car] L. Carlitz, Some theorems on irreducible reciprocal polynomials over a finite field, J. Reine und Angew. Math. 227 (1967) 212–220.

[Che] R. Chela, Reducible polynomials, J. London Math Soc., 38 (1963), 183–188.

[Ded] R. Dedekind, Abriss einer Theorie der höhern Congruenzen in Bezug auf einen reelen primzahl Modulus, J. Fur Reine und Angew. Math. 54 (1857) 1–26.

[Gal] P.X. Gallagher. "The large sieve and probabilistic Galois theory." Collection: Analytic number theory (Proc. Symmp. Pure Math. Vol. XXIV St. Louis Univ., St. Louis, Mo., 1972) pp. 91-101. Copyright: Amer. Math. Soc. Providence, R.I.

[Kno] H.-W.Knobloch, Die Seltenheit der reduziblen Polynome, Jber. Deutsch. Math. Verein. 59 (1956), Abt 1, 12–19.

[Lef] P. Lefton, On the Galois groups of cubics and trinomials, Acta Arith. 35 (1979), 239–246.

[LN] R. Lidl and H. Niederreiter, Introduction to finite fields and their applications. Revision of the 1986 first edition. Cambridge University Press, Cambridge, 1994. xii+416 pp.

[W1] B. L. van der Waerden. Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt, Monatsh. Math., 43 (1936) 133–147.

[W2] B. L. van der Waerden. Moderne Algebra. Vol. 1. Springer, Berlin, 1935; English transl., Ungar, New York, 1949, MR 10, 587.

Received: 20.8.97

Department of Mathematics-Hill Center
Rutgers, The State University of New Jersey
110 Frelinghuysen RD
USA-Piscataway, NJ 08854-8019