Difficulty of Factoring Polynomials and Finding Roots

Russell Miller,

Queens College &

Graduate Center – CUNY

September 12, 2008

CUNY Logic Workshop

Root Set and Splitting Set

Defn.: The *splitting set* of a computable field F is

$S_F = \{p(X) \in F[X] : \exists q_0, q_1 \in F[X](q_0 \cdot q_1 = p)\}$.

The *root set* of F is

$$R_F = \{p(X) \in F[X] : \exists a \in F(p(a) = 0)\}.$$

F has a *splitting algorithm* if S_F is computable, and a *root algorithm* if R_F is computable.

Bigger questions: find the irreducible factors of $p(X)$, and find all its roots in F.

Fact: $R_F \leq_T S_F$ for every computable field F.

Rabin's Theorem

Defn.: A homomorphism $g : F \to E$ of computable fields is a *Rabin embedding* if g is computable and E is algebraically closed and algebraic over the image $g(F)$.

Intuition: E is an effective algebraic closure of F.

Rabin's Theorem:
1. Every computable field F is the domain of some Rabin embedding g into some E.
2. F has a splitting algorithm iff that Rabin embedding has image $g(F)$ computable within E.

Relativizing Rabin

Corollary: For a computable F, the following are Turing-equivalent:

- the image $g(F)$ within E, for any Rabin embedding $g : F \to E$;
- the splitting set S_F;
- the root set R_F;
- the *root function* for F, which tells how many roots each $p(X) \in F[X]$ has in F.

Other Reduction Procedures

Defn.: A is *m-reducible to* B, $A \leq_m B$, if there exists a total computable function h such that

$$x \in A \iff h(x) \in B.$$

A is 1-*reducible to* B, $A \leq_1 B$, if this h may be taken to be 1-to-1.

Jump Theorem: $A \leq_T B$ iff $A' \leq_1 B'$.

m-reducibility is strictly stronger than Turing reducibility – so how do R_F and S_F compare under $\leq_m$?

Positive Result

Thm.: For any computable field F with a computable transcendence basis, $S_F \leq_1 R_F$. In particular, this holds for any algebraic field F.

Problem: Given a polynomial $p(X) \in F[X]$, compute another polynomial $q(X) \in F[X]$ such that

$$p(X) \text{ splits } \iff q(X) \text{ has a root.}$$

$\boxed{S_F \leq_m R_F}$

Let P be the c.e. subfield of F generated by its transcendence basis (so F is algebraic over P). Let F_s be the subfield $P[0, \ldots, s-1]$. Kronecker showed that every such F_s has a splitting algorithm.

Procedure: For a given $p(X)$, find an s with $p \in F_s[X]$. Check first whether p splits there. If so, pick its $q(X)$ to be a linear polynomial. If not, find the splitting field K_s of $p(X)$ over F_s, and the roots $r_1, \ldots, r_d$ of $p(X)$ in K_s.

Theorems about Fields

Prop.: For $F_s \subseteq L \subseteq K_s$, $p(X)$ splits in $L[X]$ iff there exists $\emptyset \subsetneq I \subsetneq \{r_1, \ldots, r_d\}$ such that L contains all elementary symmetric polynomials in I.

Theorem of the Primitive Element: Every finite algebraic field extension is generated by a single element.

And we can effectively find a primitive generator x_I for each intermediate field L_I generated by the elementary symmetric polynomials in I. Let $q(X)$ be the product of the minimal polynomials $q_I(X) \in F_s[X]$ of each x_I.

$\boxed{\textbf{This works!}}$

$\Rightarrow$: If $p(X)$ splits in $F[X]$, then F contains some L_I. But then $x_I \in F$, and $q_I(x_I) = 0$.

$\Leftarrow$: If $q(X)$ has a root $x \in F$, then some $q_I(x) = 0$, so x is F_s-conjugate to some x_I. Then some $\sigma \in \mathrm{Gal}(K_s/F_s)$ maps x_I to x. But σ permutes the set $\{r_1, \ldots, r_d\}$, so x generates the subfield containing all elementary symmetric polynomials in $\sigma(I)$. Then F contains this subfield, so $p(X)$ splits in $F[X]$.

Reverse Reduction

Thm.: There exists an algebraic computable field F such that $R_F \not\leq_m S_F$.

Strategy to show that a single φ_e is not an m-reduction from R_F to S_F: name a witness polynomial $q_e(X) = X^5 - X - 1$, say, whose Galois group over $\mathbb{Q}$ is S_5, and start with $F_0 = \mathbb{Q}$. If $\varphi_e(q_e)\downarrow$ to some polynomial $p_e(X) \in F_0[X]$, then either keep $F = F_0$ (if p_e is reducible there), or add a root of q_e to F_0 (if $\deg(p_e) < 2$), or ...

Defeating one φ_e

Let L be the splitting field of $p_e(X)$ over F_0, containing all roots $x_1, \ldots, x_n$ of p_e. If $F_0[x_1]$ contains no r_i, then let $F = F_0[x_1]$. Else say (WLOG) $r_1 = h(x_1)$ for some $h(X) \in F_0[X]$. Then each $h(x_j) \in \{r_1, \ldots, r_d\}$, and each r_i is $h(x_j)$ for some j. Let F be the fixed field of G_{12}:

$$\{\sigma \in \mathrm{Gal}(L/F_0) : \{\sigma(r_1), \sigma(r_2)\} = \{r_1, r_2\}\}.$$

Then each $\sigma \in G_{12}$ fixes $I = \{x_j : h(x_j) \in \{r_1, r_2\}\ \}$ setwise. So F contains all polynomials symmetric in I, and $p_e(X)$ splits in F.

But there is a $\tau \in G_{12}$ which fixes no r_i. So $q_e(X)$ has no root in F.

Defeating all φ_e

Use distinct witness polynomials $q_e(X)$ against each φ_e.

Problem: We have to wait to see whether $\varphi_e(q_e)$ ever converges. While we wait, we must keep all roots of q_e out of F.

Solution: An injury-priority argument. When $\varphi_e(q_e)\downarrow$, our procedure may injure any strategy for defeating φ_i $(i > e)$, but must not do anything to upset our procedure against any φ_j $(j < e)$.

Lemma (Keating): We may choose q_e with degree prime to all $\deg(q_j)$ $(j < e)$, and with symmetric Galois group over F_s.

So adding roots of q_e to F will not adjoin any roots of any q_j $(j < e)$.

Avoiding Injury

Problem: We choose $q_e(X)$, and then φ_e chooses $p_e(X)$. So we can control the r_i, but not the x_j. Putting an x_j into F to defeat one φ_e may ruin our strategy against another $\varphi_{e'}$.
Solution: If $F_s[r_1]$ contains no symmetric subfield $L_I \subset L$, then adjoin r_1 to F. If some L_I satisfies $L_I \subsetneq F_s[r_1]$, adjoin L_I to F.
Lemma: Otherwise, at least one subgroup G_{12}, G_{13}, or G_{23} contains some symmetric subfield L_I. Extend F to be the fixed field of that subgroup.