A GENERALIZED CLASS OF POLYNOMIALS THAT ARE HARD TO FACTOR

ERICH KALTOFEN
(UNIVERSITY OF DELAWARE)
DAVID R. MUSSER
(GE RESEARCH SCHENECTADY)
B. DAVID SAUNDERS
(RESSELAER POLYTECH.)

PROBLEM: HOW FAST CAN INTEGER POLYNOMIALS BE FACTORED ?

SUBPROBLEM: HOW FAST DOES THE BERLEKAMP-HENSEL ALGORITHM RUN IN ITS WORST CASE ?

ANSWER TO SUBPROBLEM:

$$\text{norm}(a_0 + a_1 x + \ldots + a_n x^n) \equiv |a_0| + |a_1| + \ldots + |a_n|$$

$$\text{size}(f) \equiv \deg(f) * \log(\text{norm}(f))$$

THE FOLLOWING DOMINANCE RELATION HOLDS FOR THE WORST TIME COMPL. OF THE BERLEKAMP-HENSEL ALGORITHM:

$$2^{\frac{\text{size}(f)}{\log\log(\text{size}(f))}} \prec T_{\text{worst}}(f)$$

FACTOR:

$\delta \equiv \deg f$, $\nu \equiv \log \text{norm } f$

$$5x^{11}+10x^9-10x^8+10x^7-20x^6+10x^5-20x^4+5x^3-20x^2+10$$

CONTENT — $\delta \cdot \nu^2$

CONTENT = 5

PP = $x^{11}+2x^9-2x^8+2x^7-4x^6+2x^5-4x^4+x^3-4x^2-2$

SQUARE FREE — $\delta^4 \cdot \nu^2$

$(x^2+1)^2$

$(x^7-2x^4+x^3-2)$

DISTINCT DEGREE — $\delta^3 \cdot \nu$

PROVES x^2+1 IRREDUCIBLE

$(x^3+5)(x^4+1)$ MOD 7

"deg 3" "deg 2"

BERLE-KAMP — $\delta^3 \cdot \nu$

$x^4+1 \equiv (x^2+3x+1)(x^2+4x+1)$ MOD 7

COEFF. BOUND — $\delta \cdot \nu$

768

HENSEL — $\delta^3 \cdot \nu$

$(x^3+5) \cdot (x^2+3x+1) \cdot (x^2+4x+1)$ MOD 7

$(x^3+47) \cdot (x^2+10x+1) \cdot$ ——— MOD 49

$(x^3+2399) \cdot (x^2+2166x+1) \cdot (x^2+235x+1)$ MOD 2401

COMBI-NATIONS — $2^\delta \cdot \delta\nu^2$

$(x^3-2) \cdot (x^4+1)$

$$5\,(x^2+1)^2\,(x^3-2)\,(x^4+1)$$

NOTATION:

$$\prod_{0 \le i_j < r} \left(x - \zeta_r^{i_1} \sqrt[r]{2} - \zeta_r^{i_2} \sqrt[r]{3} - \dots \zeta_r^{i_n} \sqrt[r]{p_n}\right) \quad \zeta_r = e^{\frac{2\pi i}{r}}$$

$$\equiv f_{r;\,2,3,\dots,p_n}(x)$$

$$\Psi_{G(n)}(x) \qquad G(n) = 3 \cdot 5 \cdot \dots \cdot p_n$$

$$\equiv f^{*}_{G(n);\,\phi}(x)$$

$$\prod_{\substack{2 \le i_0 < r \\ (i_0, r) = 1}} \prod_{0 \le i_j < r} \left(x - \zeta_r^{i_0} - \zeta_r^{i_1} \sqrt[r]{2} - \dots - \zeta_r^{i_n} \sqrt[r]{p_n}\right)$$

$$\equiv f^{*}_{r;\,2,3,\dots,p_n}(x)$$

DEFINITION: $\lambda(r)$

$s^{\lambda(r)} \equiv 1 \pmod{r}$ FOR $(s, r) = 1$

AND $\lambda(r)$ IS MINIMAL WITH THIS PROPERTY.

THEOREM 1:

$f_{r;p_1,\ldots,p_n}(x)$ AND $f^*_{r;p_1,\ldots,p_n}(x) \in \mathbb{Z}[x]$

AND

a) $f_{r;p_1,\ldots,p_n}(x)$ IS IRREDUCIBLE AND FOR $r \geq 3$ $f^*_{r;p_1,\ldots,p_n}(x)$ HAS IRRED. FACTORS OF DEGREE AT LEAST $2r^n$.

b) IF $r = 2, 4, 6$ OR ODD THEN $f^*_{r;p_1,\ldots,p_n}(x)$ IS COMPLETELY IRREDUCIBLE.

THEOREM 2:

FOR ANY PRIME q:

a) $f_{r;p_1,\ldots,p_n}(x) \pmod q$ AND $f^*_{r;p_1,\ldots,p_n}(x) \pmod q$ FACTOR INTO IRREDUCIBLE POLYNOMIALS OF DEGREE AT MOST $r\lambda(r)$.

SPECIAL CASE: r PRIME AT MOST r.

b) $\psi_r(x) \pmod q$ FACTORS INTO POLYNOMIALS OF DEGREE AT MOST r.

E.G.:

1. $\sigma(\rho)=\rho$, $\sigma(\sqrt[3]{2})=\sqrt[3]{2}$, $\sigma(\sqrt[3]{3})=\rho\sqrt[3]{3}$.

$\pi_\sigma=(\alpha_1\ \alpha_2\ \alpha_3)(\alpha_4\ \alpha_5\ \alpha_6)(\alpha_7\ \alpha_8\ \alpha_9)$

2. $\tau(\rho)=\rho^2$, $\tau(\sqrt[3]{2})=\rho\sqrt[3]{2}$, $\tau(\sqrt[3]{3})=\rho^2\sqrt[3]{3}$.

$\pi_\tau=(\alpha_1\ \alpha_6)(\alpha_2\ \alpha_5)(\alpha_3\ \alpha_4)(\alpha_7\ \alpha_9)(\alpha_8)$

ALL PERMUTATIONS OF THE GALOIS GROUP OF $f_{3;2,3}(x)$ HAVE CYCLES OF LENGTHS AT MOST 3.

PROOF:

a) $\sigma(\rho)=\rho$ AND $\sigma(\sqrt[3]{p})=\rho^i\sqrt[3]{p}$:

$\sigma\sigma(\sqrt[3]{p})=\rho^i\rho^i\sqrt[3]{p}$, $\sigma\sigma\sigma(\sqrt[3]{p})=\rho^{3i}\sqrt[3]{p}=\sqrt[3]{p}$

b) $\sigma(\rho)=\rho^2$ AND $\sigma(\sqrt[3]{p})=\rho^i\sqrt[3]{p}$:

$\sigma\sigma(\rho)=\rho^4=\rho$

$\sigma\sigma(\sqrt[3]{p})=\rho^{2i}\rho^i\sqrt[3]{p}=\sqrt[3]{p}$

THE SPLITTING FIELD OF A POLYNOMIAL $a_0 \bmod p + a_1 \bmod p\, x + \ldots + a_n \bmod p\, x^n$ IS A FINITE ("GALOIS") FIELD IF p IS PRIME.

E.G.: $x^4 + 2x^3 + x^2 + 5$

ROOTS ARE $3+3i,\ 3-3i,\ 3+i,\ 3-i$

OF $\mathbb{Z}_7[i] = GF(7^2)$

THE GALOIS GROUP OF $GF(p^n)$ IS ISOMORPHIC TO $(\mathbb{Z}_n, +)$.

THEREFORE THE ABOVE POLYNOMIAL MUST HAVE QUADRATIC AND LINEAR FACTORS ONLY. $[(x^2+x+4)(x^2+x+3)]$

LEMMA: LET $\bar{f} \in \mathbb{Z}_p[x]$, p PRIME. $\bar{f}$ DOES NOT CONTAIN AN IRREDUCIBLE FACTOR OF DEGREE HIGHER THAN THE LONGEST CYCLE IN ITS GALOIS GROUP.

LEMMA: LET f BE A MONIC SEPARABLE POLYNOMIAL IN $\mathbb{Z}[x]$ AND LET $\bar{f} \in \mathbb{Z}_p[x]$ BE ITS NATURAL PROJECTION MODULO A PRIME NUMBER p. IF $\bar{f}$ IS SEPARABLE (OVER $\mathbb{Z}_p$) THE GALOIS GROUP OF $\bar{f}$ OVER $\mathbb{Z}_p$ IS A SUBGROUP (AS A PERMUTATION GROUP ON THE SUITABLY ARRANGED ROOTS) OF THE GALOIS GROUP OF f OVER $\mathbb{Q}$.

LEMMA: LET r BE AN INTEGER ≥ 2, ζ_r BE A PRIMITIVE r-th ROOT OF UNITY, AND LET $p_1, \ldots, p_n$ BE DISTINCT POSITIVE PRIMES:

a) $[\mathbb{Q}(\sqrt[r]{p_1}, \ldots, \sqrt[r]{p_n}) : \mathbb{Q}] = r^n$.

b) IF $r \geq 3$ THEN $2r^n \leq [\mathbb{Q}(\zeta_r, \sqrt[r]{p_1}, \ldots, \sqrt[r]{p_n}) : \mathbb{Q}] \leq \varphi(r)\, r^n$.

c) IF r IS ODD OR 2, 4, OR 6 THEN $[\mathbb{Q}(\zeta_r, \sqrt[r]{p_1}, \ldots, \sqrt[r]{p_n}) : \mathbb{Q}] = \varphi(r)\, r^n$.

LEMMA: ASSUMPTIONS AS ABOVE.

$$\sqrt[r]{p_n} \notin \mathbb{Q}(\zeta_r, \sqrt[r]{p_1}, \ldots, \sqrt[r]{p_{n-1}}).$$

PROOF THAT $f_{3,2,3}(x)$ IS IRREDUCIBLE:

SINCE $[\mathbb{Q}(\sqrt[3]{2},\sqrt[3]{3}):\mathbb{Q}]=9$ IT IS SUFFICIENT TO SHOW THAT $\mathbb{Q}(\sqrt[3]{2},\sqrt[3]{3})=\mathbb{Q}(\sqrt[3]{2}+\sqrt[3]{3})$.

WE SHOW THAT $\sqrt[3]{3} \in \mathbb{Q}(\sqrt[3]{2}+\sqrt[3]{3})$

CONSIDER $x^3-3=0$

$(\sqrt[3]{2}+\sqrt[3]{3}-x)^3-2=0$

BOTH POLYNOMIALS VANISH AT $\sqrt[3]{3}$

BUT HAVE NO OTHER ROOT IN COMMON

(OTHERWISE $\sqrt[3]{2}+\sqrt[3]{3}-\rho^i\sqrt[3]{3}=\rho^j\sqrt[3]{2}$, $i=1,2$.

HENCE $\sqrt[3]{3}=(\rho^j\sqrt[3]{2}-\sqrt[3]{2})/(1-\rho^i) \in \mathbb{Q}(\rho,\sqrt[3]{2})$)

THEREFORE THE EUKLIDEAN ALGORITHM IN $\mathbb{Q}(\sqrt[3]{2}+\sqrt[3]{3})[x]$ PRODUCES $x-\sqrt[3]{3}$ WHOSE COEFFICIENTS ARE IN $\mathbb{Q}(\sqrt[3]{2}+\sqrt[3]{3})$.

CONJECTURE:

IF THE GALOIS GROUP OF f CONTAINS A PERMUTATION WHOSE CYCLE LENGTHS REPRESENT "SUFFICIENTLY FAITHFULLY" THE DEGREE VECTOR OF THE FACTORS OF f THEN

$$t(f) \prec p(\text{size}(f))$$

WHERE p IS A FIXED POLYNOMIAL.

E.G.:

$f = f_1 \cdots f_k$, $\deg(f_i) = n_i$

$$(1, \ldots, n_1)(n_1+1, \ldots, n_1+n_2) \cdots (n_1+\ldots+n_{k-1}+1, \ldots, n_1+\ldots+n_k)$$

(n_1, n_2, n_k under the respective cycles)

IS AN ELEMENT OF G_f.