Today:
- Polynomials
- Coding Theory
- Connections with complexity

12/9/05

1

Remember alg deciding EQ_{ROBP}

$\langle B_1 \rangle \longrightarrow q_1(x_1, \cdots x_n) \longrightarrow q_1(a_1, a_2 \cdots a_n) \pmod f$

$\langle B_2 \rangle \longrightarrow q_2(x_1 \cdots x_n) \longrightarrow q_2(a_1, a_2 \cdots a_n) \pmod f$ $\quad$ f is prime

choose a_i's randomly from $\{0, \cdots, f-1\}$

<u>Polynomials</u> Example: How many real roots?

$x^3 - 2x^2 - x + 2$

$(x-1)(x^2 - x - 2)$

Same reasoning works for polynomials mod f, for f prime

<u>Lemma (10.14)</u> The equation $c_d x^d + c_{d-1} x^{d-1} + \cdots c_1 x + c_0 \equiv 0 \pmod f$, f is prime, $a_d, \cdots a_0 \in \mathbb{Z}$, has at most d solutions (unless $c_d = c_{d-1} = \cdots = c_0 = 0$)

<u>Proof</u> Induction:
- If $d = 0$ obvious
- Assume true for $d-1$. If poly has a root w, factor out $(x-w)$. Remaining poly has degree $d-1$ and hence at most $d-1$ roots. Total of $\leq d$ roots

---

Note: it is <u>essential</u> that f is prime ($x^2 \equiv 0 \bmod 16$ has roots $x=0, x=4$, $x=8, x=12$)

Polynomials mod f factor uniquely if f prime

<u>Corollary 1</u> If $p \neq 0$ is a degree d polynomial, $\Pr_{a \in \{0, \cdots f-1\}}[p(a) \equiv 0] \leq d/f$

<u>Corollary 2</u> If $p \neq q$ are two degree at most d polynomials, $\Pr_a[p(a) \equiv q(a)] \leq d/f$

Lemma (10.15) (Schwartz-Zippel) If $p \neq 0$ is a polynomial on m vars, (eg $x_1^2x_2 + x_1x_3$) each with max degree d, then $\Pr_{a_1, a_2 \cdots a_m}[p(a_1, a_2, \cdots, a_m) = 0] \leq md/f$

Proof Induction on m

- When $m=1$, done by lemma 10.14
- Assume true for $m-1$. Write p as $p_0 + x_1 p_1 + x_1^2 p_2 + \cdots x_1^d p_d$ where $p_0, p_1 \cdots p_d$ are polynomials on $x_2, x_3, \cdots x_m$

If $p(a_1, a_2 \cdots a_m) = 0$, then either

i) Each p_i evaluates to 0 on $a_2, \cdots a_m$, or

ii) a_1 is a root of the single variable poly $c_0 + c_1x_1 + c_2x_1^2 + \cdots c_d x_1^d$ obtained by setting $c_i = p_i(a_2, \cdots a_m)$

Probability that (i) occurs $\leq$ Prob$[p_0(a_2 \cdots a_m) = 0] \leq \frac{(m-1)d}{f}$ by inductive hypothesis

Probability that (ii) occurs $\leq d/f$ by lemma 10.14

Total prob that (i) or (ii) occur $\leq \frac{(m-1)d}{f} + \frac{d}{f} = \frac{md}{f}$

Coding Theory

Example: Repetition Code

Messages		Codewords
131	$\xrightarrow{\text{Encode}}$	111 333 111
231	$\longrightarrow$	222 333 111

Code "corrects" 1 error

Code "detects" 2 errors

3 or more errors are bad since that can change one codeword into another

Reed-Solomon Code

Messages $\qquad\qquad$ codewords

$131 \xrightarrow{\text{Encode}} p(0)\,p(1)\,p(2)\cdots p(6)$

$p(x) = x^2+3x+1 \pmod 7$

231

$q(x) = 2x^2+3x+1 \pmod 7 \mapsto q(0)\,q(1)\cdots q(6)$

Note that if messages are different, $p \neq q$, so by lemma 10.14 corollary the codewords agree on at most 2 places, So they disagree on 5 places!

Thus code "detects" 4 errors

code "corrects" 2 errors