CS 70 Spring 2017 — Discrete Mathematics and Probability Theory — Rao — **DIS 4b**

1 Polynomial Short

(a) What is the minimum number of points necessary to uniquely determine a degree d polynomial?

(b) Let p be a degree 6 polynomial and q be a degree 4 polynomial. What is the maximum possible degree of $p+q$? What is the minimum possible degree? What about $p \cdot q$?

Solution:

(a) $d+1$.

(b) The degree of $p+q$ is 6.

The degree of $p \cdot q$ is 10.

2 Roots

Let's make sure you're comfortable with roots of polynomials in the familiar real numbers $\mathbb{R}$. Recall that a polynomial of degree d has at most d roots. In this problem, assume we are working with polynomials over $\mathbb{R}$.

(a) Suppose $p(x)$ and $q(x)$ are two different nonzero polynomials with degrees d_1 and d_2 respectively. What can you say about the number of solutions of $p(x) = q(x)$? How about $p(x) \cdot q(x) = 0$?

(b) Consider the degree 2 polynomial $f(x) = x^2 + ax + b$. Show that, if f has exactly one root, then $a^2 = 4b$.

(c) What is the *minimum* number of real roots that a nonzero polynomial of degree d can have? How does the answer depend on d?

Solution:

(a) A solution of $p(x) = q(x)$ is a root of the polynomial $p(x) - q(x)$, which has degree at most $\max(d_1, d_2)$. Therefore, the number of solutions is also at most $\max(d_1, d_2)$.

A solution of $p(x) \cdot q(x) = 0$ is a root of the polynomial $p(x) \cdot q(x)$, which has degree $d_1 + d_2$. Therefore, the number of solutions is at most $d_1 + d_2$.

(b) If there is a root c, then the polynomial is divisible by $x-c$. Therefore it can be written as $f(x) = (x-c)g(x)$. But $g(x)$ is a degree one polynomial and by looking at coefficients it is obvious that its leading coefficient is 1. Therefore $g(x) = x-d$ for some d. But then d is also a root, which means that $d = c$. So $f(x) = (x-c)^2$ which means that $a = -2c$ and $b = c^2$, so $a^2 = 4b$.

(c) If d is even, the polynomial can have 0 roots (e.g., consider $x^d + 1$, which is always positive for all $x \in \mathbb{R}$). If d is odd, the polynomial must have at least 1 root (a polynomial of odd degree takes on arbitrarily large positive and negative values, and thus must pass through 0 inbetween them at least once).

3 Roots: The Next Generations

Now go back and do it all over in modular arithmetic...

Which of the facts from above stay true when $\mathbb{R}$ is replaced by GF(p) [i.e., integer arithmetic modulo the prime p]? Which change, and how? Which statements won't even make sense anymore?

Solution:

(a) The upper bounds on the number of roots still hold.

(b) This continues to hold in any field.

(c) Even degree polynomials can still have 0 roots, for example $x^2 + 1 \pmod 3$ (or similar FLT-inspired forms). However, we lose the guarantee that every odd degree polynomial must have a root (though we are still assured of this at degree 1). For example, $x^3 + x + 1 \pmod 5$ has no roots.

4 How Many Polynomials?

Let $P(x)$ be a polynomial of degree 2 over GF(5). As we saw in lecture, we need $d+1$ distinct points to determine a unique d-degree polynomial.

(a) Assume that we know $P(0) = 1$, and $P(1) = 2$. Now we consider $P(2)$. How many values can $P(2)$ have? How many distinct polynomials are there?

(b) Now assume that we only know $P(0) = 1$. We consider $P(1)$, and $P(2)$. How many different $(P(1), P(2))$ pairs are there? How many different polynomials are there?

(c) How many different polynomials of degree d over $GF(p)$ are there if we only know k values, where $k \leq d$?

Solution:

(a) 5 polynomials, each for different values of $P(2)$.

(b) Now there are 5^2 different polynomials.

(c) p^{d+1-k} different polynomials. For $k = d+1$, there should only be 1 polynomial.

5 GCD of Polynomials

Let $A(x)$ and $B(x)$ be polynomials (with coefficients in $\mathbb{R}$). We say that $\gcd(A(x), B(x)) = D(x)$ if $D(x)$ divides $A(x)$ and $B(x)$, and if every polynomial $C(x)$ that divides both $A(x)$ and $B(x)$ also divides $D(x)$. For example, $\gcd((x-1)(x+1), (x-1)(x+2)) = x-1$. Notice this is the exact same as the normal definition of GCD, just extended to polynomials.

Incidentally, $\gcd(A(x), B(x))$ is the highest degree polynomial that divides both $A(x)$ and $B(x)$. In the subproblems below, you may assume you already have a subroutine `divide`$(P(x), S(x))$ for dividing two polynomials, which returns a tuple $(Q(x), R(x))$ of the quotient and the remainder, respectively, of dividing $P(x)$ by $S(x)$.

(a) Write a recursive program to compute `gcd`$(A(x), B(x))$.

(b) Write a recursive program to compute `extended-gcd`$(A(x), B(x))$.

Solution:

(a) Specifically, we wish to find a gcd of two polynomials $A(x)$ and $B(x)$, assuming that $\deg A(x) \geq \deg B(x) > 0$. Here, $\deg A(x)$ denotes the degree of $A(x)$.

We can find two polynomials $Q_0(x)$ and $R_0(x)$ by polynomial long division (see lecture note 7) which satisfy

$$A(x) = B(x)Q_0(x) + R_0(x), \qquad 0 \leq \deg R_0(x) < \deg B(x).$$

Notice that a polynomial $C(x)$ divides $A(x)$ and $B(x)$ if and only if it divides $B(x)$ and $R_0(x)$. [*Proof*: $C(x)$ divides $A(x)$ and $B(x)$, there exists $S(x)$ and $S'(x)$ s.t. $A(x) = C(x)S(x)$ and $B(x) = C(x)S'(x)$, so $R_0(x) = A(x) - B(x)Q_0(x) = C(x)(S(x) - S'(x)Q_0(x))$, therefore $C(x)$ divides $R_0(x)$ or $R_0(x) = 0$.]

We deduce that

$$\gcd(A(x), B(x)) = \gcd(B(x), R(x))$$

and set $A_1(x) = B_1(x), B_1(x) = R_0(x)$; we then repeat to get new polynomials $Q_1(x)$, $R_1(x)$, $A_2(x)$, $B_2(x)$, and so on. The degrees of the polynomials keep getting smaller and will eventually reach a point at which $B_N(x) = 0$; and we will have found our gcd:

$$\gcd(A(x), B(x)) = \gcd(A_1(x), B_1(x)) = \cdots = \gcd(A_N(x), 0) = A_N(x)$$

Here, we have the function that can perform the polynomial long division on $A(x)$ and $B(x)$ and return both the quotient $Q(x)$ and the remainder $R(x)$, i.e. $[Q(x), R(x)] = \mathrm{div}(A(x), B(x))$. The algorithm can be extended from the original integer-based GCD as follows:

```
function gcd(A(x), B(x)):
  if B(x) = 0:
    return A(x)
  else if deg A(x) < deg B(x):
    return gcd(B(x), A(x))
  else:
    (Q(x), R(x)) = div(A(x), B(x))
    return gcd(B(x), R(x))
```

(b) We will return a triple of polynomials $(d(x), g(x), h(x))$ such that $d(x) = \gcd(A(x), B(x))$ and $d(x) = g(x) \cdot A(x) + h(x) \cdot B(x)$.

```
function extended-gcd(A(x), B(x)):
  if B(x) = 0:
    return (A(x), 1, 0)
  else if deg A(x) < deg B(x):
    return extended-gcd(B(x), A(x))
  else:
    (Q(x), R(x)) = div(A(x), B(x))
    (d(x), g(x), h(x)) := extended-gcd(B(x), R(x))
    return (d(x), h(x), g(x) - Q(x) * h(x))
```