AM 106: Applied Algebra **Prof. Salil Vadhan**

Problem Set 9

Assigned: Fri. Nov. 30, 2018 Due: Mon. Dec. 10, 2018 (11:59pm sharp)

- You must submit your problem sets electronically on the course Canvas site. If you use LaTeX, please submit both the source (`.tex`) and the compiled file (`.pdf`). Name your files `PS9-yourlastname`.
- For SAGE problems, also submit a pdf version of your SAGE notebook.
- Aim for clarity and conciseness in your solutions, emphasizing the main ideas over low-level details.

Problem 1. (Computations in $F[x]$, 8pts) Factor the polynomial $x^5 + 2x^3 + x^2 + x \in \mathbb{Z}_3[x]$ into irreducible factors.

Problem 2. (Bivariate polynomials, 20pts) Let R be a commutative ring with unity. The ring $R[x, y]$ of bivariate polynomials over R consists of all expressions of the form $p(x, y) = \sum_{i,j\geq 0} a_{i,j}x^i y^j$, where $a_{i,j} \in R$, only finitely many of the $a_{i,j}$ are nonzero, and addition and multiplication are defined as usual (with $x^i y^j \cdot x^k y^\ell = x^{i+k}y^{j+\ell}$). The *degree* of such a polynomial p is the maximum of $i + j$ over all nonzero coefficients $a_{i,j}$.

1. Find an ideal in $\mathbb{Q}[x, y]$ that is not principal. (This is in contrast to the univariate polynomial ring $\mathbb{Q}[x]$, which is a principal ideal domain.)
2. Exhibit a nonzero bivariate polynomial $p(x, y) \in \mathbb{Z}[x, y]$ that has infinitely many zeroes. (This is in contrast to univariate polynomials $p(x) \in \mathbb{Z}[x]$, which can have only finitely many zeroes.)
3. Despite the above, it can be shown that a low-degree polynomial cannot have too many roots in any finite "cube". Specifically, show that if R is an integral domain, $S \subseteq R$ is finite, and $p(x, y) \in R[x, y]$ is a nonzero polynomial of degree d, then the fraction of points $(\alpha, \beta) \in S \times S$ on which $p(\alpha, \beta) = 0$ is at most $d/|S|$. (Hint: group terms as $p(x, y) = \sum_{j=0}^{k} p_j(x)y^j$, and classify the roots according to whether or not $p_k(\alpha) = 0$.)

   By a similar argument and induction, the same can be shown for polynomial $p(x_1, \ldots, x_t)$ in any number of variables. This turns out to be very useful in algorithm design — it allows us to efficiently test whether a low-degree multivariate polynomial is zero by evaluating it on random points from S^t.
4. Let $R = \mathbb{F}$ be a finite field of size q, and consider the "bivariate Reed–Muller" code with alphabet $\mathbb{F}$ and blocklength $n = q^2$ where the codewords are bivariate polynomials of degree at most d over $\mathbb{F}$. That is, the messages $m \in \mathbb{F}^k$ are interpreted as giving the $k = (d+2)(d+1)/2$ coefficients of a bivariate polynomial $p_m \in \mathbb{F}[x, y]$ of degree at most d, yielding a codeword $(p_m(\gamma_1), \ldots, p_m(\gamma_n))$ where $\gamma_1, \ldots, \gamma_n$ are an enumeration of the elements of $\mathbb{F}^2$. Use Part 3 to show that this code has minimum distance at least $n \cdot (1 - d/q)$.

Problem 3. (Density of Irreducible Polynomials, 12pts) In this problem, you will prove a polynomial analogue of the celebrated "Prime Number Theorem," which states that the fraction of numbers between 1 and N that are prime is approximately $1/\ln N$ as $N \to \infty$. While the proof of the Prime Number Theorem for integers is very sophisticated (using complex analysis!), you have learned enough in AM106 to prove an analogous statement for polynomials over a finite field.

Let $F = \mathbb{F}_q$, and $E = \mathbb{F}_{q^n}$ for some prime power q. You may assume that E contains F as a subfield; we've seen this when q is prime (every field of characteristic p contains $\mathbb{Z}_p = \mathbb{F}_p$ as a subfield) but it is also true for prime powers q that $\mathbb{F}_{q^n}$ contains $\mathbb{F}_q$ as a subfield.

1. Show that every element $a \in E$ is the zero of a nonzero polynomial in $F[x]$ of degree at most n. (Hint: view $1, a, a^2, a^3, \ldots$ as elements of the vector space E over the field F.)

2. Deduce that every element $a \in E$ is the zero of a *monic, irreducible* polynomial in $F[x]$ of degree at most n.

3. Use Part 2 to prove that the number of monic irreducible polynomials in $F[x]$ of degree at most n is at least q^n/n, and that the fraction of monic polynomials of degree at most n that are irreducible is at least $(1 - 1/q)/n$.

Consequently, irreducible polynomials are not too rare and we can find irreducible polynomials in time poly(n) by randomly choosing polynomials of degree at most n and testing them for irreducibility by using an efficient algorithm for polynomial factorization.

Problem 4. (Decoding Reed–Solomon Codes, 20pts) After the website Magic Seaweed discovered their surfing spot and started providing daily forecasts for it, Alice, Bob, and Eve gave up on keeping the spot secret and resigned themselves to a crowded lineup. This made it no longer necessary for them to encrypt their surfing plans. However, due increasing amounts of sea salt crusted on their cellphones, their communications started to become error-prone, forcing them to utilize error-correcting codes. Specifically, they use a q-ary Reed–Solomon code for $q = 128$ (so that alphabet symbols can be conveniently interpreted as ASCII characters) with message length $k = 32$ and blocklength $n = 128$. In SAGE, we have provided you with the received word after a codeword sent by Alice was corrupted in approximately 30% of its positions. Use the decoding algorithm for Reed–Solomon codes to find Alice's original message as an ASCII string. As usual, see the PS9 tips in `http://seas.harvard.edu/~salil/am106/fall18/SAGE.html` for more instructions.