Problem Set 5 Solutions

Problem 5.1 (Euclidean division algorithm).

(a) For the set $\mathbb{F}[x]$ of polynomials over any field $\mathbb{F}$, show that the distributive law holds: $(f_1(x) + f_2(x))h(x) = f_1(x)h(x) + f_2(x)h(x)$.

Using the associative and commutative laws and the rules of polynomial arithmetic, we have

$$(f_1(x) + f_2(x))\, h(x) = \left(\sum_i (f_{1i} + f_{2i})x^i\right)\left(\sum_j h_j x^j\right) = \sum_i \sum_j (f_{1i} + f_{2i})h_j x^{i+j}$$

and

$$f_1(x)h(x) + f_2(x)h(x) = \sum_i \sum_j (f_{1i}h_j + f_{2i}h_j)x^{i+j}.$$

Finally, $(f_{1i} + f_{2i})h_j = f_{1i}h_j + f_{2i}h_j$ by the distributive law over $\mathbb{F}$.

(b) Use the distributive law to show that for any given $f(x)$ and $g(x)$ in $\mathbb{F}[x]$, there is a unique $q(x)$ and $r(x)$ with $\deg r(x) < \deg g(x)$ such that $f(x) = q(x)g(x) + r(x)$.

Suppose that $f(x)$ can be written in two ways:

$$f(x) = q(x)g(x) + r(x) = q'(x)g(x) + r'(x)$$

where $\deg r(x) < \deg g(x)$ and $\deg r'(x) < \deg g(x)$. Using the distributive law, we have

$$(q(x) - q'(x))g(x) + (r(x) - r'(x)) = 0. \tag{1}$$

If $q(x) = q'(x)$, then $(q(x) - q'(x))g(x) = 0$, so (1) implies $r(x) = r'(x)$. If $q(x) \neq q'(x)$, then $(q(x) - q'(x))g(x) \neq 0$ and has degree $\geq \deg g(x)$, whereas $r(x) - r'(x)$ has degree $< \deg g(x)$, so (1) cannot hold. Thus the quotient $q(x)$ and remainder $r(x)$ are unique.

Problem 5.2 (unique factorization of the integers).

Following the proof of Theorem 7.7, prove unique factorization for the integers $\mathbb{Z}$.

We follow the statement and proof of Theorem 7.7, replacing statements about polynomials by corresponding statements about integers:

Theorem 7.0 (Unique factorization of integers) *Every positive integer $n \in \mathbb{Z}$ with magnitude $|n| \geq 2$ may be written in the form*

$$n = \prod_{i=1}^{k} p_i,$$

where each $p_i, 1 \leq i \leq k$, is a prime integer. This factorization is unique, up to the order of the factors.

Proof. If n is a prime, then $n = n$ is the desired unique factorization. If n is not a prime, then n can be factored into the product ab of two nontrivial factors each less than n, which in turn can be factored, and so forth. Since magnitudes decrease with each factorization, this process can only terminate in a prime factorization.

Now we need to prove uniqueness. Thus assume hypothetically that the theorem is false and let n be the smallest integer that has more than one such factorization,

$$n = a_1 \cdots a_k = b_1 \cdots b_j; \qquad j, k \geq 1, \tag{2}$$

where $a_1, \ldots, a_k$ and $b_1, \ldots, b_j$ are prime integers. We will show that this implies an integer n' smaller than n with non-unique factorization, and this contradiction will prove the theorem. Now a_1 cannot appear on the right side of (2), else it could be factored out for an immediate contradiction. Similarly, b_1 cannot appear on the left. Without loss of generality, assume $b_1 \leq a_1$. By the Euclidean division algorithm, $a_1 = qb_1 + r$. Since a_1 is prime, $r \neq 0$ and $0 < r < b_1 \leq a_1$. Now r has a prime factorization $r = r_1 \cdots r_n$, where b_1 is not a divisor of any of the r_i, since it has greater magnitude. Substituting into (2), we have

$$(qb_1 + r_1 \cdots r_n)a_2 \cdots a_k = b_1 \cdots b_j,$$

or, defining $n' = r_1 \cdots r_n a_2 \cdots a_k$ and rearranging terms,

$$n' = r_1 \cdots r_n a_2 \cdots a_k = b_1 \left(b_2 \cdots b_j - q a_2 \cdots a_k\right).$$

Now n' is positive, because it is a product of positive integers; it is less than n, since $r < a_1$; and it has two different factorizations, with b_1 a factor in one but not a divisor of any of the factors in the other; contradiction. □

Problem 5.3 (finding irreducible polynomials).

(a) Find all prime polynomials in $\mathbb{F}_2[x]$ of degrees 4 and 5. [Hint: There are three prime polynomials in $\mathbb{F}_2[x]$ of degree 4 and six of degree 5.]

We can immediately eliminate all polynomials which have the degree-1 factor x (*i.e.,* whose constant term is 0) or the degree-1 factor $x + 1$ (*i.e.,* which have an even number of nonzero coefficients). This eliminates $\frac{3}{4}$ of the candidate polynomials. We then need to sieve out only multiples of the degree-2 prime polynomial $x^2 + x + 1$ and the two degree-3 prime polynomials, $x^3 + x + 1$ and its reverse, $x^3 + x^2 + 1$.

This leaves four degree-4 polynomials. One of these is $(x^2 + x + 1)^2 = x^4 + x^2 + 1$. The remaining three are prime:

$$x^4 + x + 1, x^4 + x^3 + 1, x^4 + x^3 + x^2 + x + 1.$$

Similarly, this leaves eight degree-5 polynomials. Two of these are multiples of the degree-2 prime polynomial with one of the two degree-3 prime polynomials, namely $(x^2 + x + 1)$ $(x^3 + x + 1) = x^5 + x^4 + 1$ and its reverse, $x^5 + x + 1$. The remaining six are prime:

$$x^5 + x^2 + 1, x^5 + x^3 + x^2 + x + 1, x^5 + x^4 + x^2 + x + 1,$$

and their reverses $x^5 + x^3 + 1, x^5 + x^4 + x^3 + x^2 + 1, x^5 + x^4 + x^3 + x + 1$.

(b) Show that $x^{16} + x$ factors into the product of the prime polynomials whose degrees divide 4, and $x^{32} + x$ factors into the product of the prime polynomials whose degrees divide 5.

The prime polynomials whose degrees divide 4 are $x, x+1, x^2+x+1$ and the three degree-4 prime polynomials above. Straightforward polynomial multiplication shows that

$$x(x+1)(x^2+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)(x^4+x+1) = x^{16}+x.$$

(Note that $(x^2+x+1)(x^4+x^3+1)(x^4+x+1) = x^{10}+x^5+1$ and $(x+1)(x^4+x^3+x^2+x+1) = x^5+1$.)

Similarly, the prime polynomials whose degrees divide 5 are $x, x+1$ and the six degree-5 prime polynomials above. Again, straightforward polynomial multiplication shows that their product is $x^{32}+x$.

Problem 5.4 (The nonzero elements of $\mathbb{F}_{g(x)}$ form an abelian group under multiplication).

Let $g(x)$ be a prime polynomial of degree m, and $r(x), s(x), t(x)$ polynomials in $\mathbb{F}_{g(x)}$.

(a) Prove the distributive law, i.e., $(r(x) + s(x)) * t(x) = r(x) * t(x) + s(x) * t(x)$. [Hint: Express each product as a remainder using the Euclidean division algorithm.]

By the distributive law for ordinary polynomials, we have

$$(r(x)+s(x))t(x) = r(x)t(x) + s(x)t(x).$$

Following the hint, write $r(x)t(x) = q_1(x)g(x) + r_1(x)$, $s(x)t(x) = q_2(x)g(x) + r_2(x)$, and $(r(x)+s(x))t(x) = q_3(x)g(x) + r_3(x)$, where $\deg r_i(x) < \deg g(x)$ for $i = 1, 2, 3$. Then $r(x) * t(x) = r_1(x)$, $s(x) * t(x) = r_2(x)$, and $(r(x) + s(x)) * t(x) = r_3(x)$. Now from the equation above,

$$q_3(x)g(x) + r_3(x) = q_1(x)g(x) + r_1(x) + q_2(x)g(x) + r_2(x).$$

which implies

$$0 = (q_3(x) - q_1(x) - q_2(x))g(x) + (r_3(x) - r_1(x) - r_2(x))$$

Since $0 = 0q(x) + 0$ and such a decomposition is unique, we have $r_3(x) = r_1(x) + r_2(x)$.

(b) For $r(x) \neq 0$, show that $r(x) * s(x) \neq r(x) * t(x)$ if $s(x) \neq t(x)$.

The equation $r(x) * s(x) = r(x) * t(x)$ implies $r(x) * (s(x) - t(x)) = 0$; but since $g(x)$ is irreducible, this implies either $r(x) = 0$ or $s(x) = t(x)$.

(c) For $r(x) \neq 0$, show that as $s(x)$ runs through all nonzero polynomials in $\mathbb{F}_{g(x)}$, the product $r(x) * s(x)$ also runs through all nonzero polynomials in $\mathbb{F}_{g(x)}$.

By part (b), the products $r(x) * s(x)$ are all nonzero and are all distinct as as $s(x)$ runs through the $|\mathbb{F}|^m - 1$ nonzero polynomials in $\mathbb{F}_{g(x)}$, so they must be all of the $|\mathbb{F}|^m - 1$ nonzero polynomials in $\mathbb{F}_{g(x)}$.

(d) Show from this that $r(x) \neq 0$ has a mod-$g(x)$ multiplicative inverse in $\mathbb{F}_{g(x)}$; i.e., that $r(x) * s(x) = 1$ for some $s(x) \in \mathbb{F}_{g(x)}$.

By part (c), the products $r(x) * s(x)$ include every nonzero polynomial in $\mathbb{F}_{g(x)}$, including 1. Therefore, given $r(x) \neq 0 \in \mathbb{F}_{g(x)}$, there exists a unique $s(x) \neq 0 \in \mathbb{F}_{g(x)}$ such that $r(x) * s(x) = 1$; *i.e.,* such that $s(x)$ is the multiplicative inverse of $r(x)$ in $\mathbb{F}_{g(x)}$.

Since the multiplication operation $*$ is associative and commutative and has identity 1, it follows that the nonzero elements of $\mathbb{F}_{g(x)}$ form an abelian group under multiplication.

Problem 5.5 (Construction of $\mathbb{F}_{32}$)

(a) Using an irreducible polynomial of degree 5 (see Problem 5.3), construct a finite field $\mathbb{F}_{32}$ with 32 elements.

We can construct $\mathbb{F}_{32}$ using any of the 6 irreducible polynomials of degree 5 found in Problem 5.3. Using $g(x) = x^5 + x^2 + 1$, the field $\mathbb{F}_{32}$ is defined as the set of all 32 binary polynomials of degree 4 or less under polynomial arithmetic modulo $g(x)$.

(b) Show that addition in $\mathbb{F}_{32}$ can be performed by vector addition of 5-tuples over $\mathbb{F}_2$.

The sum of two polynomials of degree 4 or less is obtained by a componentwise sum of their coefficients, whether modulo $g(x)$ or not.

(c) Find a primitive element $\alpha \in \mathbb{F}_{32}$. Express every nonzero element of $\mathbb{F}_{32}$ as a distinct power of α. Show how to perform multiplication and division of nonzero elements in $\mathbb{F}_{32}$ using this "log table."

The set $\mathbb{F}_{32}^*$ of nonzero elements of $\mathbb{F}_{32}$ is the set of roots of the equation $x^{31} = 1$ in $\mathbb{F}_{32}$; *i.e.,* every $\beta \in \mathbb{F}_{32}^*$ satisfies $\beta^{31} = 1$, so the multiplicative order of every element must divide 31, which is prime. There is one element of multiplicative order 1, namely 1. The remaining 30 elements must therefore have multiplicative order 31; *i.e.,* there are 30 primitive elements in $\mathbb{F}_{32}^*$. Therefore $\alpha = x$ must be primitive. We compute its powers, reducing x^5 to $x^2 + 1$ as necessary:

$$
\begin{aligned}
\alpha &= x, \\
\alpha^2 &= x^2, \\
\alpha^3 &= x^3, \\
\alpha^4 &= x^4, \\
\alpha^5 &= x^2 + 1, \\
\alpha^6 &= x^3 + x, \\
\alpha^7 &= x^4 + x^2, \\
\alpha^8 &= x^3 + x^2 + 1, \\
\alpha^9 &= x^4 + x^3 + x, \\
\alpha^{10} &= x^4 + 1, \\
\alpha^{11} &= x^2 + x + 1, \\
\alpha^{12} &= x^3 + x^2 + x, \\
\alpha^{13} &= x^4 + x^3 + x^2,
\end{aligned}
$$

$$
\begin{aligned}
\alpha^{14} &= x^4 + x^3 + x^2 + 1, \\
\alpha^{15} &= x^4 + x^3 + x^2 + x + 1, \\
\alpha^{16} &= x^4 + x^3 + x + 1, \\
\alpha^{17} &= x^4 + x + 1, \\
\alpha^{18} &= x + 1, \\
\alpha^{19} &= x^2 + x, \\
\alpha^{20} &= x^3 + x^2, \\
\alpha^{21} &= x^4 + x^3, \\
\alpha^{22} &= x^4 + x^2 + 1, \\
\alpha^{23} &= x^3 + x^2 + x + 1, \\
\alpha^{24} &= x^4 + x^3 + x^2 + x, \\
\alpha^{25} &= x^4 + x^3 + 1, \\
\alpha^{26} &= x^4 + x^2 + x + 1, \\
\alpha^{27} &= x^3 + x + 1, \\
\alpha^{28} &= x^4 + x^2 + x, \\
\alpha^{29} &= x^3 + 1, \\
\alpha^{30} &= x^4 + x, \\
\alpha^{31} &= 1.
\end{aligned}
$$

The product of α^i and α^j is α^{i+j}. The quotient of α^i divided by α^j is α^{i-j}. In both cases the exponents are computed modulo 31, since $\alpha^{31} = 1$.

(d) Discuss the rules for multiplication and division in $\mathbb{F}_{32}$ when one of the field elements involved is the zero element, $0 \in \mathbb{F}_{32}$.

The product of 0 with any field element is 0. Division by 0 is not defined; *i.e.,* it is illegal (as with the real or complex field).

Problem 5.6 (Second nonzero weight of an MDS code)

Show that the number of codewords of weight $d+1$ in an (n, k, d) linear MDS code over $\mathbb{F}_q$ is

$$
N_{d+1} = \binom{n}{d+1} \left((q^2 - 1) - \binom{d+1}{d} (q - 1) \right),
$$

where the first term in parentheses represents the number of codewords with weight $\geq d$ in any subset of $d+1$ coordinates, and the second term represents the number of codewords with weight equal to d.

Consider any subset of $d + 1 = n - k + 2$ coordinates. Take two of these coordinates and combine them with the remaining $k - 2$ coordinates to form an information set. Fix the components in the $k - 2$ coordinates to zero, and let the remaining two coordinates run freely through $\mathbb{F}_q$. These q^2 information set combinations must correspond to q^2

codewords. (In fact, we may view this subset of codewords as a shortened $(d+1, 2, d)$ MDS code.)

One of these codewords must be the all-zero codeword, since the code is linear. The remaining $q^2 - 1$ codewords must have weight d or $d+1$. Since there are $q-1$ codewords of weight d with support in any subset of d coordinate positions, the number of codewords of weight d whose support is in any subset of $d+1$ coordinate positions is $\binom{d+1}{d}(q-1)$ (the number of codewords of weight d in a $(d+1, 2, d)$ MDS code). So the number of codewords of weight $d+1$ in any $d+1$ coordinate positions is

$$\left((q^2-1) - \binom{d+1}{d}(q-1)\right).$$

Since there are $\binom{n}{d+1}$ distinct subsets of $d+1$ coordinate positions, the given expression for N_{d+1} follows.

Note that

$$\left((q^2-1) - \binom{d+1}{d}(q-1)\right) = (q+1)(q-1) - (d+1)(q-1) = (q-d)(q-1).$$

This implies that if $n > d$, then $d \leq q$, since otherwise N_{d+1} would become negative. In other words, there exists no $(n, k, d = n-k+1)$ MDS code over $\mathbb{F}_q$ with $q < d < n$. For example, there exist no binary MDS codes other than the $(n, n, 1), (n, n-1, 2)$ and $(n, 1, n)$ codes (and $(n, 0, \infty)$, if you like). More generally, when $n \geq q+2$, there exist forbidden values of d, namely $q+1 \leq d \leq n-1$.

Similarly, by considering shortened codes of lengths $d+2, d+3, \ldots, n$, we can compute $N_{d+2}, N_{d+3}, \ldots, N_n$.

Problem 5.7 (N_d and N_{d+1} for certain MDS codes)

(a) Compute the number of codewords of weights 2 and 3 in an $(n, n-1, 2)$ SPC code over $\mathbb{F}_2$.

We have $N_2 = (q-1)\binom{n}{2} = \binom{n}{2}$; *i.e.,* there is a weight-2 codeword for every coordinate pair. Then $N_3 = (q-d)(q-1)\binom{n}{3} = 0$. This is consistent with the definition of an SPC code as the set of all even-weight n-tuples.

(b) Compute the number of codewords of weights 2 and 3 in an $(n, n-1, 2)$ linear code over $\mathbb{F}_3$.

Here we have $N_2 = (q-1)\binom{n}{2} = 2\binom{n}{2}$; *i.e.,* there are two weight-2 codewords for every coordinate pair. Then $N_3 = (q-d)(q-1)\binom{n}{3} = 2\binom{n}{3}$.

For example, the $(3, 2, 2)$ RS code over $\mathbb{F}_3$ has generators $(111, 012)$ and codewords $\{000, 111, 222, 012, 120, 201, 021, 102, 210\}$, with $N_2 = 6$ and $N_3 = 2$. Thus in general a zero-sum code over a field larger than $\mathbb{F}_2$ has odd-weight codewords.

(c) Compute the number of codewords of weights 3 and 4 in a $(4, 2, 3)$ *linear code over* $\mathbb{F}_3$.

Here we have $N_3 = (q-1)\binom{4}{3} = 2(4) = 8$, so all non-zero codewords have weight 3. (Verification: $N_4 = 0$ because $q = d$.) The $(4, 2, 3)$ linear code over $\mathbb{F}_3$ given in the introduction of Chapter 8 (or in the next problem) is an example of such a code, called a "tetracode."

Problem 5.8 ("Doubly" extended RS codes)

(a) Consider the following mapping from $(\mathbb{F}_q)^k$ *to* $(\mathbb{F}_q)^{q+1}$. *Let* $(f_0, f_1, \ldots, f_{k-1})$ *be any* k*-tuple over* $\mathbb{F}_q$, *and define the polynomial* $f(z) = f_0 + f_1 z + \cdots + f_{k_1} z^{k-1}$ *of degree less than* k. *Map* $(f_0, f_1, \ldots, f_{k-1})$ *to the* $(q+1)$*-tuple* $(\{f(\beta_j), \beta_j \in \mathbb{F}_q\}, f_{k-1})$— *i.e., to the RS codeword corresponding to* $f(z)$, *plus an additional component equal to* f_{k-1}.

Show that the q^k $(q+1)$*-tuples generated by this mapping as the polynomial* $f(z)$ *ranges over all* q^k *polynomials over* $\mathbb{F}_q$ *of degree less than* k *form a linear* $(n = q+1, k, d = n-k+1)$ *MDS code over* $\mathbb{F}_q$. *[Hint:* $f(z)$ *has degree less than* $k-1$ *if and only if* $f_{k-1} = 0$.*]*

The code evidently has length $n = q + 1$. It is linear because the sum of codewords corresponding to $f(z)$ and $f'(z)$ is the codeword corresponding to $f(z) + f'(z)$, another polynomial of degree less than k. Its dimension is k because no polynomial other than the zero polynomial maps to the zero $(q+1)$-tuple.

To prove that the minimum weight of any nonzero codeword is $d = n - k + 1$, use the hint and consider the two possible cases for f_{k-1}:

- If $f_{k-1} \neq 0$, then $\deg f(z) = k - 1$. By the fundamental theorem of algebra, the RS codeword corresponding to $f(z)$ has at most $k-1$ zeroes. Moreover, the f_{k-1} component is nonzero. Thus the number of nonzero components in the code $(q+1)$-tuple is at least $q - (k-1) + 1 = n - k + 1$.
- If $f_{k-1} = 0$ and $f(z) \neq 0$, then $\deg f(x) \leq k - 2$. By the fundamental theorem of algebra, the RS codeword corresponding to $f(z)$ has at most $k-2$ zeroes, so the number of nonzero components in the code $(q+1)$-tuple is at least $q-(k-2) = n-k+1$.

(b) Construct a $(4, 2, 3)$ *linear code over* $\mathbb{F}_3$. *Verify that all nonzero words have weight 3.*

The generators of an extended RS $(4, 2, 3)$ "tetracode" over $\mathbb{F}_3$ are $(1110, 0121)$, and the code is $\{0000, 1110, 2220, 0121, 1201, 2011, 0212, 1022, 2102\}$, with $N_3 = 8$ and $N_4 = 0$ (as shown in Problem 5.7(c); compare the zero-sum $(3, 2, 2)$ code of Problem 5.7(b)).