Assignment 8

Karan Sikka
ksikka@andrew.cmu.edu
E
April 6, 2012

Rehashing Old Problems (Frodo's Problem)

Thanks for the hint. We used the result from 0b of assignment 4. We restate it here:
$S_k(n)$ is a polynomial in n of degree at most $k+1$.

$S_k(n)$ is defined as:

$$S_k(n) = 1^k + 2^k + 3^k ... + n^k = \sum_{i=1}^{n} i^k$$

To make this proof easier, we start the sum at 0 instead of 1. Note that it is still the same.

We will let $k = 4$ because the result is $S_4(n) = \sum_{i=0}^{n} i^4$.

By the first sentence in this proof, we can say that $S_4(n)$ is a polynomial of degree at most 5. Mathematically, $S_4(n)$ is equal to:

$$\sum_{i=0}^{n} i^4 = an^5 + bn^4 + cn^3 + dn^2 + en + f$$

for some $a, b, c, d, e, f \in \mathbb{R}$. We can deduce the values for $< a, b, c, d, e, f >$ and that will be the answer to the question.

We know f must be 0, because when we evaluate $S_4(0)$, we get

$$0 = 0^5 a + 0^4 b + 0^3 c + 0^2 d + 0e + f = f$$

We can further reduce the form for the polynomical $S_4(n)$

$$\sum_{i=0}^{n} i^4 = an^5 + bn^4 + cn^3 + dn^2 + en$$

for some $a, b, c, d, e \in \mathbb{R}$.

Let us say

$$P(n) = an^5 + bn^4 + cn^3 + dn^2 + en$$

Then

$$P(n-1) = a(n-1)^5 + b(n-1)^4 + c(n-1)^3 + d(n-1)^2 + e(n-1)$$

We take their difference and see that

$$\sum_{i=0}^{n} i^4 - \sum_{i=0}^{n-1} i^4 = n^4$$

Then we substitute for their expanded forms

$$n^4 = an^5 + bn^4 + cn^3 + dn^2 + en - (a(n-1)^5 + b(n-1)^4 + c(n-1)^3 + d(n-1)^2 + e(n-1))$$

By simple yet tedious algebra, we get

$$n^4 = (5a)n^4 + (4b - 10a)n^3 + (3c - 6b + 10a)n^2 + (2d - 3c + 4b - 5a)n + (e - d + c - b + a)$$

And then we add some $0n^k$ terms to make a relationship clear between the LHS and the RHS:
$n^4 + 0n^3 + 0n^2 + 0n + 0 =$
$(5a)n^4 + (4b - 10a)n^3 + (3c - 6b + 10a)n^2 + (2d - 3c + 4b - 5a)n + (e - d + c - b + a)$
From this, we get the following system of eqns

$$\begin{aligned} 5a &= 1 \\ 4b - 10a &= 0 \\ 3c - 6b + 10a &= 0 \\ 2d - 3c + 4b - 5a &= 0 \\ e - d + c - b + a &= 0 \end{aligned}$$

We solved this system using gaussian elination, and we checked that the following answers do indeed satisfy this system.

$$a = \frac{1}{5}, \quad b = \frac{1}{2}, \quad c = \frac{1}{3}, \quad d = 0, \quad e = \frac{-1}{30}$$

$$\sum_{i=0}^{n} i^4 = \frac{n^5}{5} + \frac{n^4}{2} + \frac{n^3}{3} - \frac{n}{30}$$

Transitivity of Sadness (Tim's Problem)

Let $y \in \mathbb{F}^n$ such that $y \in C$ so $Hy = 0$. We will examine the constraints on y. Start by noticing that y has the following structure:

$$y = \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = \left[\begin{array}{c} y_1 \\ \vdots \\ y_r \\ \hline y_{r+1} \\ \vdots \\ y_n \end{array}\right]$$

Now we start from a true statement and deduce a few things:

$$
\begin{aligned}
& Hy = [I|A]y = 0 \\
\implies \quad & [I|A] \left[\begin{array}{c} y_1 \\ \vdots \\ y_r \\ \hline y_{r+1} \\ \vdots \\ y_n \end{array}\right] = 0 \\
\implies \quad & I \begin{bmatrix} y_1 \\ \vdots \\ y_r \end{bmatrix} + A \begin{bmatrix} y_{r+1} \\ \vdots \\ y_n \end{bmatrix} = 0 \qquad \text{(by multiplication, and I is } r \times r\text{)} \\
\implies \quad & I \begin{bmatrix} y_1 \\ \vdots \\ y_r \end{bmatrix} = -A \begin{bmatrix} y_{r+1} \\ \vdots \\ y_n \end{bmatrix} \qquad \text{(by subtraction)}
\end{aligned}
$$

Using this equality, we can make a substitution in the top part of y. The steps are shown as follows:

$$
\begin{aligned}
\begin{bmatrix} y/_1 \\ \vdots \\ y_n \end{bmatrix} &= \left[\begin{array}{c} y_1 \\ \vdots \\ y_r \\ \hline y_{r+1} \\ \vdots \\ y_n \end{array}\right] \\
&= \left[\begin{array}{c} I \begin{bmatrix} y_1 \\ \vdots \\ y_r \end{bmatrix} \\ \hline I \begin{bmatrix} y_{r+1} \\ \vdots \\ y_n \end{bmatrix} \end{array}\right] \qquad \text{(by def of identity)} \\
&= \left[\begin{array}{c} -A \begin{bmatrix} y_{r+1} \\ \vdots \\ y_n \end{bmatrix} \\ \hline I \begin{bmatrix} y_{r+1} \\ \vdots \\ y_n \end{bmatrix} \end{array}\right] \qquad \text{(substitute using previous result)}
\end{aligned}
$$

$$= \left[\frac{-A}{I}\right] \begin{bmatrix} y_{r+1} \\ \vdots \\ y_n \end{bmatrix} \qquad \text{(by rules of multiplication)}$$

$$= G \begin{bmatrix} y_{r+1} \\ \vdots \\ y_n \end{bmatrix}$$

This result shows that the vector y is a linear combination of the columns of G. Therefore C, the set of all y such that $Hy = 0$, is span of the columns of G, by the definition of span.

Proof that the columns of G are linearly independent:
If G has 1 column, then it's linearly independent.

If it has more, then pick one of the column vectors in G. The bottom r elements in G consist of r-1 zeros and 1 one, because it was constructed from the Identity matrix. Say the 1 is in row m. All other elements in row m are zero because they were formed by the identity matrix. Therefore, you cannot obtain that 1 from a linear combination of the other columns. Therefore the columns of G are linearly independent.

Aren't Games Fun? (JD's Problem)

Each 3×2 board can be represented as a matrix

$$\begin{bmatrix} a & b \\ c & d \\ e & f \end{bmatrix}$$

Where a, b, c, d, e, f are the integers $\mod 2$. Hence they can only be 1 or 0, and $1 + 1 \equiv 0$).

A solvable board is one which is able to reach this state

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$$

after adding linear combinations of the following matrices, each one of which represents a move on the board:

$$A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 0 \end{bmatrix}, B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}, C = \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 1 & 1 \end{bmatrix}, D = \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix}, E = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 0 \end{bmatrix}, F = \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 0 & 1 \end{bmatrix}$$

Claim:
All solvable boards have the following property:

$$a + e \equiv b + f \equiv c + d$$

The proof is on induction on the number of moves until reaching the terminal solved board shown above.

Base Case:
When there are 0 moves required to reach the solved board, the board must be the solved board. Since each element is 0, the claim obviously holds because $0 \equiv 0 \equiv 0$

Inductive Hypothesis:
Assume that for all boards which are k moves away from the solved board for $k < n$ for some $n \in \mathbb{N}$, the claim holds.

Inductive Step:
Consider a board which is k moves away from the solved board for $k < n$ for some $n \in \mathbb{N}$. By the IH, the claim holds. We will show that by applying any of the 6 possible moves $(A...F)$, the claim will still hold.

In the move A, $a + e \equiv b + f \equiv c + d \equiv 1$. If you add A to a board in which the IH is satisfied, then the IH will still be satisfied since

$$(a + e)_{IH} \equiv (b + f)_{IH} \equiv (c + d)_{IH}$$

then adding board A to the IH board gives,

$$(a + e)_{IH} + (a + e)_A \equiv (b + f)_{IH} + (b + f)_A \equiv (c + d)_{IH} + (c + d)_A$$

and by substitution,

$$(a + e)_{IH} + 1 \equiv (b + f)_{IH} + 1 \equiv (c + d)_{IH} + 1$$

Similar logic applies for B, C, D because of symmetry.

In the move E, $a + e \equiv b + f \equiv c + d \equiv 0$. Then the same pattern of logic used for A can be applied for E, and by symmetry, for F.

Therefore, we have proved that if a board is solvable, $a + e \equiv b + f \equiv c + d$.

The number of solvable boards is upper bounded by the number of boards which satisfy the property above.

Counting the number of boards with the property: Consider the pairs of entries in the board $(a, e), (b, f), (c, d)$. If we make a square white, we'll say it's 1, if we make a square black, we'll say it's 0. Then in order for the property to hold, each one of the above pairs must be the same color or different colors.

If each square in the pair is the same color as the other element in the pair, then there are 8 possible boards like this, because there are 2 colors for each of the 3 pairs, and $2^3 = 8$ different colorings.

If each square in the pair is a different color from the other element in the pair, then there are 8 possible boards like this, because there are 2 possible colorings for each of the 3 pairs, and $2^3 = 8$ different colorings.

Since these are disjoint outcomes, there are $8 + 8 = 16$ boards which satisfy the property. Upon checking by hand, we see that all 16 of these boards are indeed solvable. Therefore there are 16 solvable boards, and they are the ones which satisfy the claim in the induction proof.

Learn to be Cool (Mark's Problem)

(a) Let us define $P(x)$ as an irreducible polynomial and $R(x)$ as a polynomial such that $deg(R) < deg(P)$. We must show that there exists a polynomial $S(x)$ such that $R(x)S(x) \mod P(x) \equiv 1$.

Using Euclid's extended algorithm, we can say that there exists an equation of the form:

$$A(x)P(x) + B(x)R(x) = gcd(R(x), P(x))$$

where A and B are polynomials in the field.

We know that $gcd(R(x), P(x))|P(x)$. Thus, since P(x) is irreducible, $gcd(R(x), P(x)) = c$ where c is a constant. Then it follows,

$$A(x)P(x) + B(x)R(x) = c$$

$B(x)R(x) \equiv c \mod P(x)$, by taking the equation above mod P(x).

We know that c has a multiplicative inverse in $\mathbb{F}_p$ because p is prime and every element less than p is relatively prime with p except 1. As an edge case, if c is 1, then it's inverse is 1 because 1 is its own inverse.

Then we multiply both sides by c^{-1} to obtain

$$c^{-1}B(x)R(x) \equiv 1 \mod P(x)$$

.

Let $S(x) = c^{-1}B(x)$, and we have shown that there exists a polynomial S(x) such that $S(x)R(x) \equiv 1 \mod P(x)$.

(b) For this proof, a_i and b_i are coefficients. Let $P(x)$ be a polynomial of degree k. Then P(x) can be represented as

$$P(x) = a_k x^k + a_{k-1}x^{k-1}...a_1 k + a_0$$

Since any remainder of polynomial division has a degree smaller than its divisor, the maximum degree a polynomial mod P(x) can have is $k - 1$ (a result proved in lecture). So let Q(x) be a polynomial and $Q(x) \mod P(x) = b_{k-1}x^{k-1}...b_1 k + b_0$

We know that there are p residue classes in $\mathbb{F}_p$: $\{0, 1, 2...p-1\}$. Thus each of the coefficients in the polynomial $Q(x) \mod P(x)$ has p different values. There are k coefficients $b_{k-1}, b_{k-2}...b_1, b_0$ and each of these coefficients can be p potential values by the same logic above. Therefore Q(k) could be one of p^k distinct polynomials.

(c) Closure of E under addition and multiplication
For all a, b in E, both $a + b$ and ab are in E.

Associativity of addition and multiplication
For all a, b, and c in E,
$a + (b + c) \equiv (a + b) + c$
$a(bc) = (ab)c$

Commutativity of addition and multiplication
For all a and b in E,
$a + b = b + a$
$ab = ba$

Existence of additive and multiplicative identity elements
0 is the additive identity and 1 is the multiplicative identity

Existence of additive inverses and multiplicative inverses
For every a in E, there exists an element $-a$ in E, such that $a + -a = 0$. Mult. inverse is trickier.

Distributivity of multiplication over addition
For all a, b and c in E, $a(b + c) = (ab) + (ac)$

These follow naturally from the fact that the coefficients of the elements in E are the integers mod p, which we know is a field.

Ditzy Dancing (Jasmine's Problem)

For this problem, we will call the number of steps that Jasmine dances for, n. We are going to examine the situation where Jasmine is back at 0 after n steps. In order to be at 0, Jasmine must have moved right as often as she moved left. If she moved right k steps, she must have moved left k steps, and she must have stayed still for s steps where

$$\text{Steps left + steps right + steps standing still = total steps}$$

$$\implies k + k + s = n$$

$$\implies 2k + s = n$$

$$\implies s = n - 2k$$

Note that since $2k$ is even, s is even when n is even and s is odd when n is odd.

Meh (Sang's Problem)

(a) Forwards implication
WTS if S is linearly independent, then $\sum_{i=1}^{k} a_i v_i = 0 \implies a_i = 0$.

AFSOC that some $a_i \neq 0$. Without loss of generality, let $i = 1$. Then,

$$a_1 v_1 + a_2 v_2 + \cdots + a_k v_k = 0$$

Then by subtraction

$$a_1 v_1 = -a_2 v_2 - \cdots - a_k v_k$$

Then divide by a_1 ($a_1 \neq 0$)

$$v_1 = \Big(-\frac{a_2}{a_1}\Big) v_2 + \cdots + \Big(-\frac{a_k}{a_1}\Big) v_k$$

Now we see that a vector is a linear combination of the other vectors in the set. Hence, S cannot be linearly independent. Contradiction.

Thus, we can conclude that if S is linearly independent, all $a_i = 0$.