Bryan Arnold

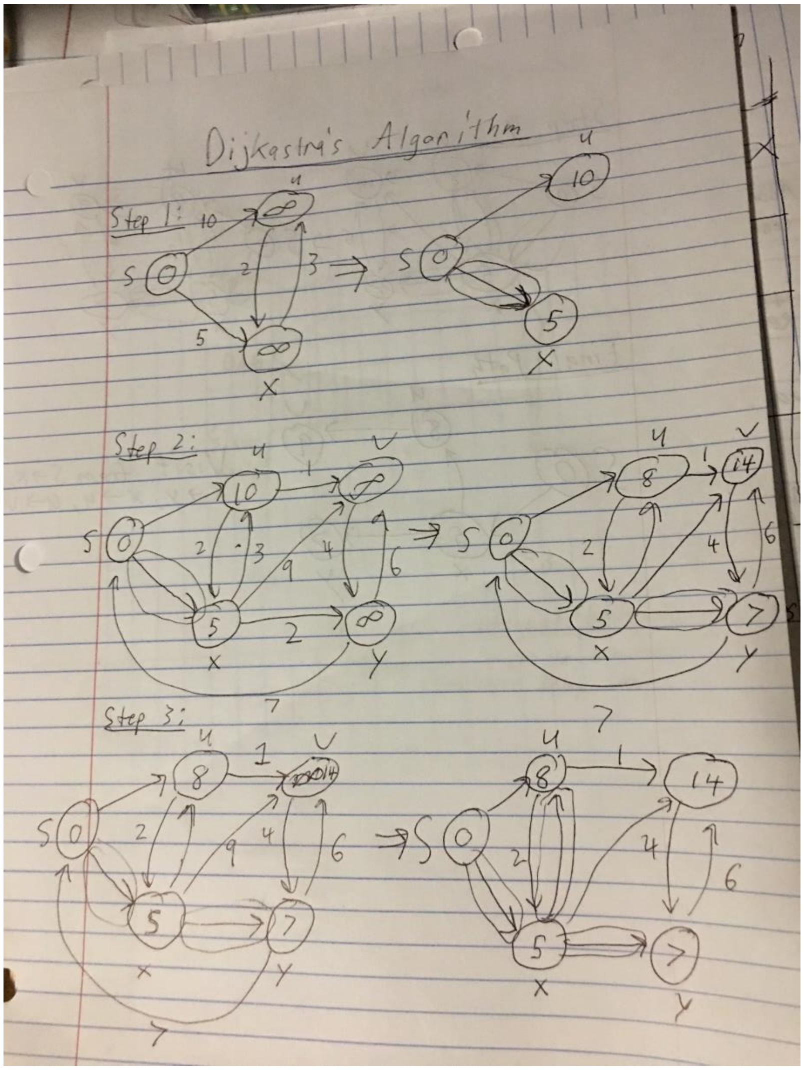
CSE 3500

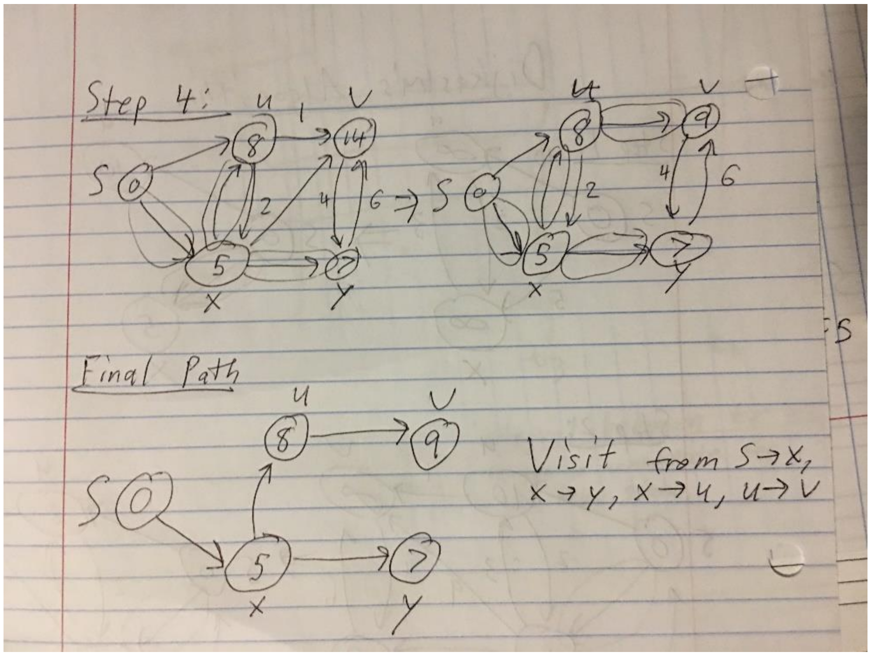
4/19/17

Homework 9

1 The shortest path algorithms

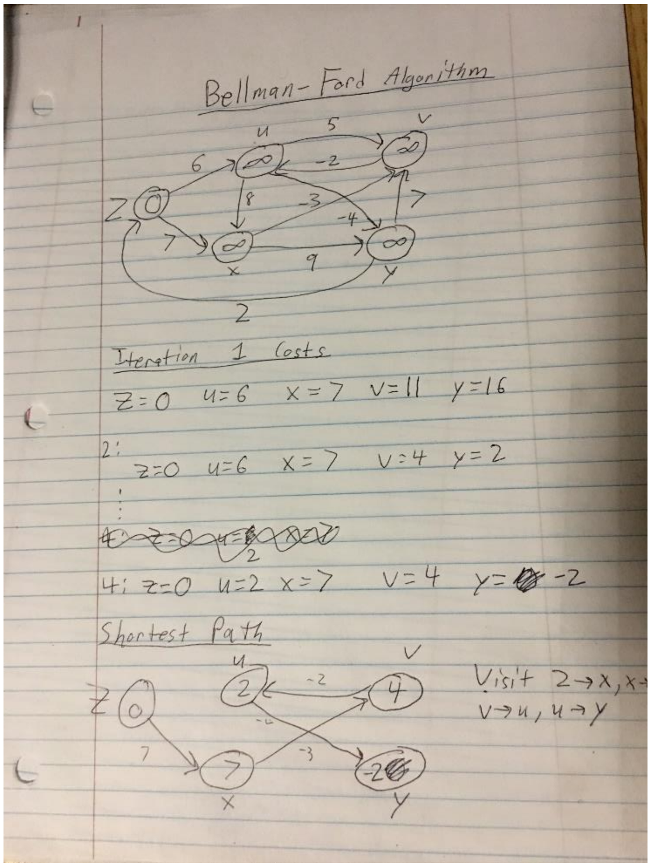
a) The path that is selected in each step of the algorithm for this graph is circled, and the weights given the current node being visited become the weights of the node (will change later to correct weight to node). The final path is shown in the second picture.





Visit from S→x,
x→y, x→u, u→v

b) There are four total iterators of the algorithm for this graph. Showing each step would be rather tedious, so I showed the total weights to certain nodes at some iterations, all the way to the final path.



Iteration 1 Costs

z=0 u=6 x=7 v=11 y=16

2:
z=0 u=6 x=7 v=4 y=2

⋮

~~4: z=0 u= x=7~~ 2

4: z=0 u=2 x=7 v=4 y= -2

Visit z→x, x→
v→u, u→y

2 The shortest path problem

As stated in the question, we are given a directed weighted graph G = (V, E). The edges that leave the source vertex can have negative weights, and all other edge weights are nonnegative, making sure there are no negative-weight cycles. According to the last statement, we just must prove that for some vertex where the vertex v does not equal the source vertex, and they are connected by some negative weight edge e, the shortest path between the two must cover the negative weight edge e.

Let us assume we have a graph with vertices s, v1, and v2. Now, let us connect s to v1 by edge e1, and connect s to v2 by edge e2. V1 an v2 are also connected by some path p. Assume that the edges e1 and e2, since they are coming from the source, that they are negative weight edges. Next, assume that the shortest path from s to v1 is s -> e2 -> v2 -> p -> v1. This means that e2 + p < e1 according to the supposition statement in the question. Now, a negative cycle can be shown by e1 + e2 + p < 2e1 < 0. This creates a contradiction that the negative weight edge e. This means that the statement to be proven earlier is true by contradiction, making it so the Dijkstra's algorithm is correct.

3 A problem related to number theory

i) First, it is known that p and q are both arbitrarily chosen prime numbers such that n = pq. This means that 1 < p < q in the set of natural numbers, and p and q are distinct prime numbers.

Since relative primality has to do to with the greatest common denominator, it is known as well that gcd(e, (p – 1)(q – 1)) = 1.

Now, we can begin to break down the problem using Fermat's little theorem. First, as gcd(e, (p – 1)(q – 1)) = gcd(e, ϕ(n)), we know that there must exist some a and b in the set of all positive integers. This makes it so that e * a + b * ϕ(n) = 1.

Deriving this further by utilizing mod, we get that the modulo of ϕ(n) = (p – 1)(q – 1) turns the previous equation with a and b into e * a = 1 (mod ϕ(n)).

Now, e * a can be replaced with d, satisfying the requirement of d ≡ a (mod ϕ(n) thus satisfying e * d ≡ 1 (mod ϕ(n)). Since, e is some number greater than or equal to 1 as well as d according to this statement, it can be said that 1 ≤ d ≤ (p – 1)(q – 1).

ii) Using the findings from the previous problem, let us look at $x^{ed}\ (mod\ n)$.

As e * d ≡ (mod ϕ(n)) we can have it so that e * d = 1 + k * ϕ(n) for some integer k.

Now, plug into the original equation at the start of this problem:

$$x^{ed} = x^{1+k*\phi(n)}$$

Simplify down to $x^{ed} = x * x^{k*\phi(n)}$

Now consider the following from the initial equation: $x^{\phi(n)}\ (mod\ n)$

Looking at Fermat's theorem, you can have it so that $x^{\Phi(n)} \equiv 1 \text{ (mod n)}$

Now, all we do is simplify down from previously stated parts of this question until we reach an answer:

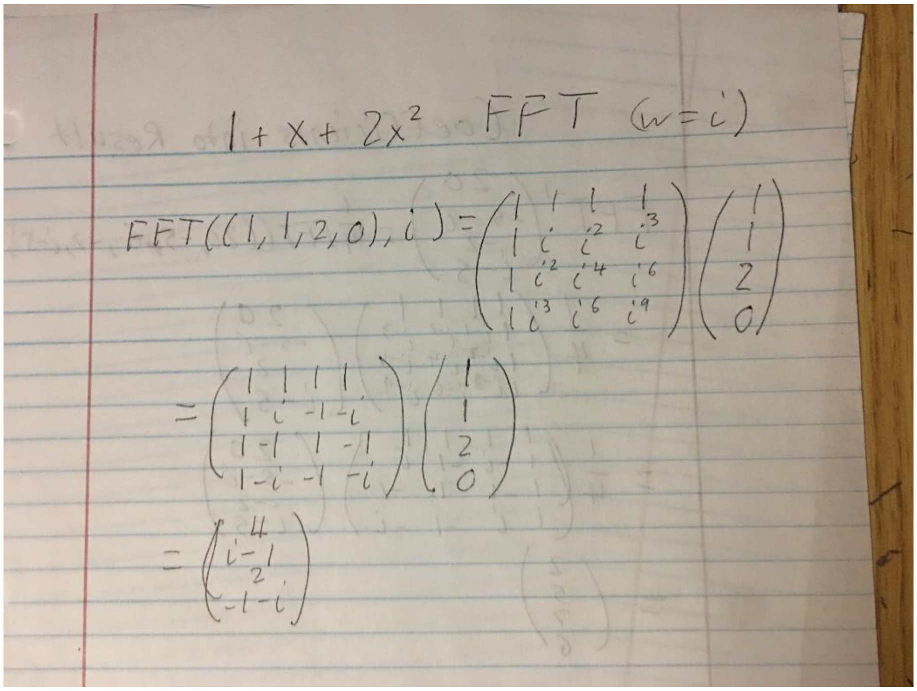
$$x^{k*\Phi(n)} \equiv 1^k \equiv 1 \text{ (mod n)}$$
$$x^{ed} \equiv x * 1 \text{ (mod n)}$$

Thus it can be seen that $x^{ed} \equiv x \text{ (mod n)}$.

4 FFT

The multiplication of 1 + x + 2x^2 and 2 + 3x is the multiplication of two polynomials. The first polynomial has a degree of 2, and the second has a degree of 1. 3 < 4, and 4 is a power of two, so use 2 as the appropriate power of 2. W = i. So, the following are the FFTs for the polynomials:

First polynomial FFT:



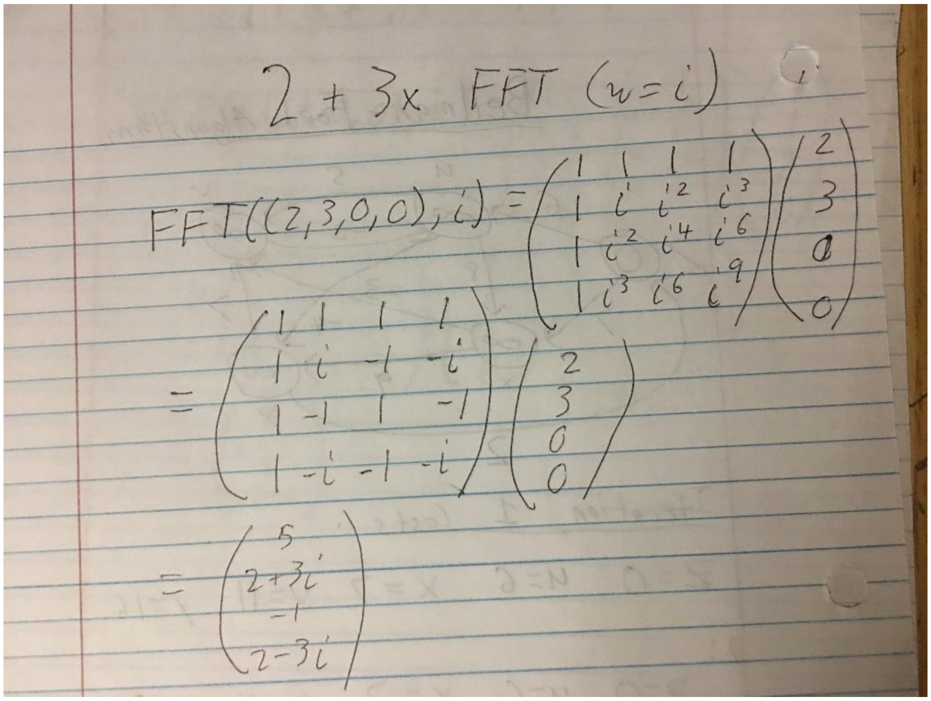
$1 + x + 2x^2$ FFT $(w = i)$

$$FFT((1,1,2,0), i) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & i^2 & i^3 \\ 1 & i^2 & i^4 & i^6 \\ 1 & i^3 & i^6 & i^9 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 2 \\ 0 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & -i \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 2 \\ 0 \end{pmatrix}$$

$$= \begin{pmatrix} 4 \\ i-1 \\ 2 \\ -1-i \end{pmatrix}$$

Second polynomial FFT:



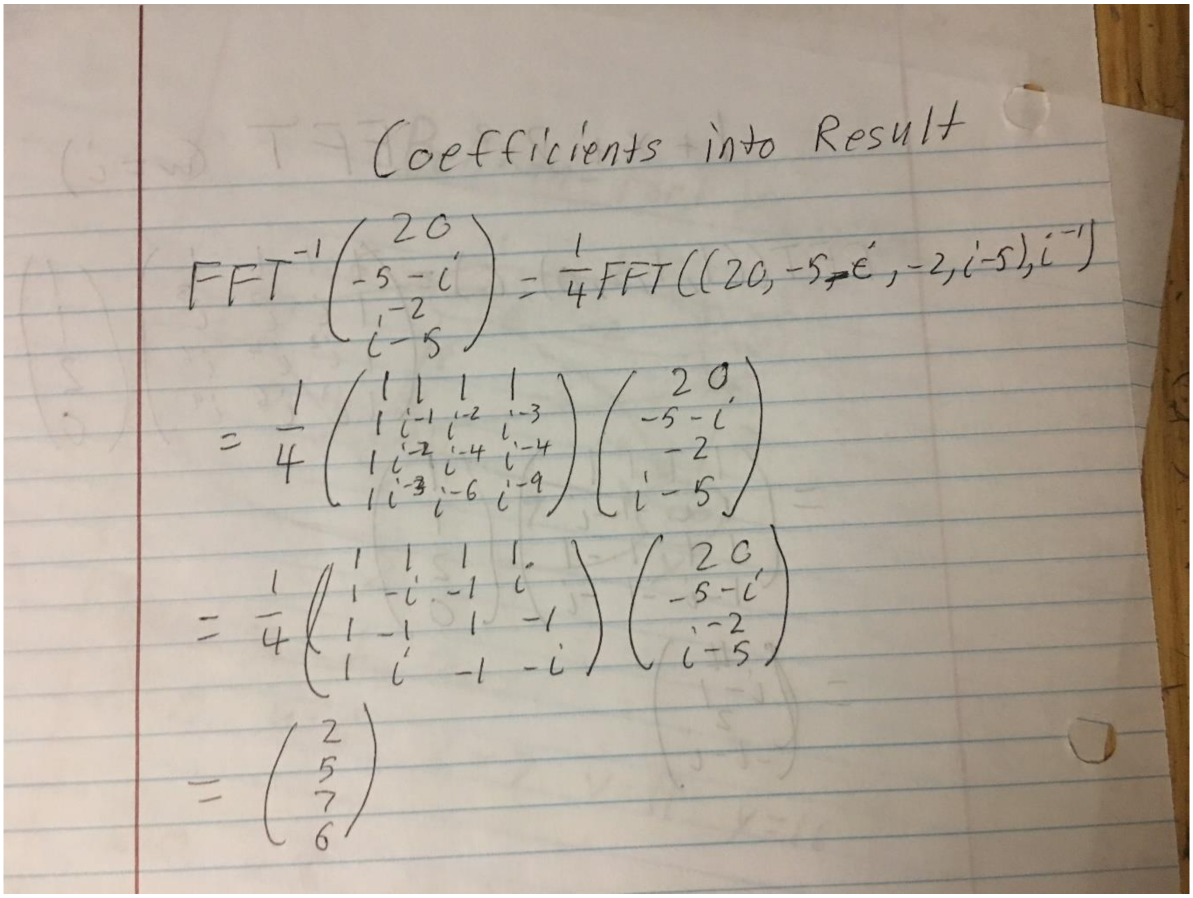
2 + 3x FFT (w = i)

$$FFT((2,3,0,0), i) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & i^2 & i^3 \\ 1 & i^2 & i^4 & i^6 \\ 1 & i^3 & i^6 & i^9 \end{pmatrix} \begin{pmatrix} 2 \\ 3 \\ 0 \\ 0 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & -i \end{pmatrix} \begin{pmatrix} 2 \\ 3 \\ 0 \\ 0 \end{pmatrix}$$

$$= \begin{pmatrix} 5 \\ 2+3i \\ -1 \\ 2-3i \end{pmatrix}$$

I know it said this part did not have to be done, but I did it anyway for fun/practice. The coefficients:



Coefficients into Result

$$FFT^{-1}\begin{pmatrix} 20 \\ -5-i \\ -2 \\ i-5 \end{pmatrix} = \frac{1}{4} FFT((20, -5-i, -2, i-5), i^{-1})$$

$$= \frac{1}{4} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i^{-1} & i^{-2} & i^{-3} \\ 1 & i^{-2} & i^{-4} & i^{-4} \\ 1 & i^{-3} & i^{-6} & i^{-9} \end{pmatrix} \begin{pmatrix} 20 \\ -5-i \\ -2 \\ i-5 \end{pmatrix}$$

$$= \frac{1}{4} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{pmatrix} \begin{pmatrix} 20 \\ -5-i \\ -2 \\ i-5 \end{pmatrix}$$

$$= \begin{pmatrix} 2 \\ 5 \\ 7 \\ 6 \end{pmatrix}$$

Based off the final resulting matrix, the polynomial multiplication result would be:

$$2 + 5x + 7x^2 + 6x^3$$