Assignment 2: CS 201 (Fall 2018)

I pledge on my honor that I have not given or received any unauthorized assistance.

Name: Nalli Bhavita Roll No.: 170409

1. (5) Let $G = (V, E)$ be an undirected graph with m edges. We pick a subset S of V at random by choosing a vertex with probability 1/2. What is the expected number of edges between S and $V - S$? Hint: Linearity of expectation.
Solution:
Let us define a random variable X equal to number of edges between S and V-S
Now to find expected number of edges between S and $V - S$ we will use linearity of expectation as X (binomial random variable) can be written as the sum of independent bernoulli variables
X = X1 + X2 + X3 Xi
thus E(X) = E(X1) + E(X2) + E(X3) + ... + E(Xi)
Xi = 1 if there exists an edge between S and V-S and P(Xi) = p i.e the probability that Xi occurs
p = 1/2 as for every edge E(u,v) there are two cases, first is u vertex belongs to S , v vertex belongs to V-S and viceversa and probability that a vertex is choosen from either of one set is 1/2 thus
p= 1/2*1/2 + 1/2*1/2 = 1/2
Xi = 0 otherwise
Thus E(Xi) = 1/2*1 + 0*1/2 = 1/2
thus E(X) = $\sum_{k=1}^{m} 1/2$ where k = an edge between S and V-S , thus following linearity of expectation
= m/2

□

2. (2+3) Prove the following.
   - Let P be an alternating path for a matching M. Consider P as a set of edges. Show that $M' = (M \setminus P) \cup (P \setminus M)$ is a matching such that $|M'| \geq |M|$.
   - Let M be an $n \times n$ matrix with entries 0 and 1. You are given that every row and every column has exactly k ones. Show that it is possible to find n ones in the matrix such that no two of them are in the same row or same column.

Solution:
Q.2 a
As P is an alternating path i.e it consists of alternate matched edges(of M)and unmatched edges(of M') thus it has two possibilities either it contains one more edge in M' than in M or one more edge in M than in M'.But if there is one more edge in M than in M' we will get an alternating path over M' which is not possible as it is given that P is an alternating path for a matching M thus it contains one more edge in M' than in M which shows $\mid M' \mid = \mid M \mid +1$ and thus proves $\mid M' \mid >= \mid M \mid$
Now we need to prove that M' is a matching. Suppose it is not a matching. Then M' must contain two edges say, E and E' which are incident to the same vertex, say V . These two edges cannot belong to M \ P , since M is a matching and therefore does not contain two edges incident to the same node. Since P is an alternating path, E and E' cannot belong to P \ M. Hence, the only possibility that remains is E ∈ M \P and E' ∈ P \ M. Since V is incident to E ∈ $M\setminus$ P and not part of M because E' ∉ M and path P is an alternating path, V must be incident to an edge E" on P which is also in the matching: E" ∈ $P \cap M$. Hence, in M, V is incident to $E \in M$ and E" ∈ M, which is in contradiction with M being a matching. Thus our assumption is wrong and M' is also a matching
Q.2 (b)
M is a n x n matrix with entries 0 and 1 given that every row and every column has exactly k ones.
Let us define two sets X,Y. Now take a subset S of X, define N(S) to be the set in Y adjacent to S.
If $\mid N(S) \mid >= \mid S \mid$ called as Halls condition is satified for all subsets S of X, then there is a complete

matching in $G = (X \bigcup Y, E)$
So here taking X to be a row or coloumn and Y to be cells containing entries 1 .If Hall's condition is satisfied for all subsets S of X then we can show that it is possible to find n ones in the matrix such that no two of them are in the same row or same column.
$N(S) := \{v \in Y : \exists u \in S : (u, v) \in E\}$. where E is the relation between cells containing 1 to each row or coloumn and as there are k elements in each row or coloumn containing one thus $| N(S) |$=k where $| S |$=1 for a particular row or coloumn thus Hall's condition is satisfied thus there is a complete matching over X i.e each coloumn and each row is matched with one cell containing 1 and it is possible to find n ones in the matrix such that no two of them are in the same row or same column.

□

3. (5) Give pseudocode for an efficient (polynomial in $\log n$) algorithm to calculate $a^b \mod n$ for some natural numbers a, b, n.
Solution:
Q.3 In this below code we will use the formula
(a*b) mod n =((a mod n)(b mod n) mod n)
Pseudo code-:

```
main()
{
Input the values of a,b,n
int ans ;
ans = call a function say func to find a^b mod n value and pass a,b,n as parameters
print the ans
}

func( with a,b,n as parameters)
{
int result = 1 ; // Initialize result
if(a is more than or equal to n )
{
a = a mod n ;
}
while (b > 0)
{
// If b is odd, multiply a with result
if (b mod 2 not equal to 0)
result = (result*a) mod n;
b=b/2;
a = (a*a) mod n;
}
return result;
}
```

As we can see the function iterates for $log(b)$ times thus time complexity is O(log b).

□

4. (5) Define $\phi(m)$ to be the number of natural numbers less than m and coprime to m (their GCD with m is 1). Let n be an odd number, show that $\phi(n) = \phi(2n)$.
Solution:
$\Phi(m)$ is defined to be the number of natural numbers less than m and coprime to m (i.e their GCD with m is 1).
Let us take $\Phi(n)$= k where n is an odd number thus ,now inorder to find $\Phi(2 * n)$ we will two cases-:

note: n being an odd number , it has only odd primes in its prime factorization

Case-I Numbers from [1,n]
All the numbers which are coprime to n are also coprime to 2*n except for all those numbers which are even (and have only those prime factors which are not in n (let x represent those numbers)).Thus number of coprimes in this range are k-x.

Case-II Numbers from [n+1,2*n]
We will try to create a bijective mapping from set of numbers [1,n] to set of numbers [n+1,2*n]
f(y) = y+n where y = all those numbers which are even and have only those prime factors which are not in n
and we can see that these are only coprime, to 2*n in this range as y have no common prime factors with n and n is coprime with 2 thus y+n is coprime to 2*n

So, number of coprimes = (k-x) + x = k
Hence we have proved that $\Phi(n) = \Phi(2 * n)$

$\square$