Theory of Computation

Solutions to Homework 4

Problem 1. Let $a, b \in \mathbb{N}$ and p be a prime. Show that $(a+b)^p = a^p + b^p \mod p$.

Proof. By the binomial expansion,

$$(a+b)^p = \sum_{r=0}^{p} \binom{p}{r} a^r \, b^{p-r}. \tag{1}$$

As p is a prime, $r!(p-r)!$ is not a multiple of p for $0 < r < p$. But $\binom{p}{r} = p!/(r!(p-r)!)$ is an integer and $p \,|\, p!$. Hence $\binom{p}{r}$ is a multiple of p for $0 < r < p$. Therefore, Eq. (1) gives $(a+b)^p = a^p + b^p \mod p$. □

Problem 2. The **permanent** of an $n \times n$ integer matrix A is defined as

$$\text{perm}(A) = \sum_{\pi} \prod_{i=1}^{n} A_{i,\pi(i)}.$$

Above, π ranges over all permutations of n elements. (It is similar to determinant but without the sign.) Show that if A is the adjacency matrix (hence a 0/1 matrix) of a bipartite graph G, then perm(A) equals the number of perfect matchings of G.

Proof. Given a bipartite graph $G = (I, J, E)$ that satisfies
(1) $I \cap J = \{\}$.
(2) For all $(i,j) \in E$, $i \in I \wedge j \in J$.
(3) $|I| = |J| = n$ [1].
Its adjancecy matrix A can be constructed as follows:

- A row of A is indexed by a vertex of I.
- A column of A is indexed by a vertex of J.
- For $A_{ij} \in A$,

$$a_{ij} = \begin{cases} 0, & \text{iff } (i,j) \notin E, \\ 1, & \text{iff } (i,j) \in E. \end{cases}$$

If there exists K perfect matching in G, then there also exists K corresponding permutation[2] functions

$$\pi_1 : I \to J, \quad \pi_2 : I \to J, \quad \ldots, \quad \pi_K : I \to J$$

[1] If not, its adjancecy matrix won't be a square one.
[2] Bijective, i.e., "1-1 and onto."

such that $(i, \pi_k(i)) \in E$ for all $i \in I$ and $k \in K$. It also implies that

$$\prod_{i=1}^{n} A_{i,\pi(i)} = \begin{cases} 1, & \pi \in \{\pi_1, \pi_2, \cdots, \pi_K\} \Leftrightarrow A_{1,\pi(1)} = A_{2,\pi(2)} = \cdots = A_{n,\pi(n)} = 1; \\ 0, & \pi \notin \{\pi_1, \pi_2, \cdots, \pi_K\}. \end{cases}$$

Thus, we have $\sum_{\pi} \prod_{i=1}^{n} A_{i,\pi(i)} = K = \langle \#$ of perfect matchings in $G \rangle$. $\square$