CS 153 Current topics in theoretical computer science **Spring 2012**

Solution Set 2

Out: May 29

Please do not consult these solutions if you have not yet turned in the problem set!

1. Consider a 0/1 matrix $n \times n$ matrix M with entries $M_{i,j}$. The function $g(M)$ defined by

$$g(M) = \prod_{i,j,i',j' : i=i' \text{ or } j=j'} (1 - M_{i,j} M_{i',j'})$$

is 0 if there is any row or column of M with more than a single 1 in it, and 1 otherwise. The function $h(M)$ defined by

$$h(M) = \prod_i \left(1 - \prod_j (1 - M_{i,j})\right)$$

is 0 if there is a row of all 0's, and 1 otherwise. Together, $g(M)h(M) = 1$ iff M is a permutation matrix.

Now, let $M^k[i,j]$ denote the (i,j) entry in the k-th power, M^k. Note that $M^k[i,j]$ is a polynomial of degree k in the entries $M_{i,j}$, which can be computed by an arithmetic circuit of polynomial size. A permutation matrix M represents an n-cycle iff $M^k[1,1] = 0$ for $k = 1, 2, \ldots, n-1$. Using this, we see that

$$f(M,X) = g(M)h(M) \prod_{k=1}^{n-1} (1 - M^k[1,1]) \prod_{i,j} M_{i,j} X_{i,j}$$

is equivalent to $\prod_i X_{i,\sigma(i)}$ when M represents the n-cycle permutation σ, and 0 otherwise. Thus

$$\sum_{M \in \{0,1\}^{n\times n}} f(M,X) = \textsc{hc}_n(X)$$

which places $\textsc{hc}$ in VNP.

2. Recall that a $M_k(f)$ is a lower bound on the noncommutative formula complexity of a polynomial f of degree n, where $M_k[i,j]$ for $i \in [n]^k$ and $j \in [n]^{n-k}$ is the coefficient on the monomial $X_{i_1} X_{i_2} \ldots X_{i_k} X_{j_1} X_{j_2} \ldots X_{j_{n-k}}$ in f.

Now consider $M_k(\textsc{perm}_\textsc{n})$, and recall that $\textsc{perm}_\textsc{n}$ has variables $X_{a,b}$ for $a, b \in [n]$. All rows indexed by k-tuples $(a_1, b_1), \ldots (a_k, b_k)$ in which $(a_1, \ldots, a_k) \neq (1, 2, \ldots k)$ or $(b_1, \ldots, b_k)$ has repeated entries are zero (since $X_{a_1,b_1}, \ldots, X_{a_k,b_k}$ is not a prefix of any monomial occurring in $\textsc{perm}_\textsc{n}$). Similarly, columns indexed by $n-k$-tuples $(a_1, b_1), \ldots (a_{n-k}, b_{n-k})$ in which $(a_1, \ldots, a_{n-k}) \neq (k+1, \ldots, n)$ or $(b_1, \ldots, b_{n-k})$ has repeated entries are zero (since $X_{a_1,b_1}, \ldots, X_{a_{n-k},b_{n-k}}$ is not a suffix of any monomial occurring in $\textsc{perm}_\textsc{n}$). Thus the non-zero rows correspond to k-subsets of $[n]$ and the non-zero columns correspond to $(n-k)$-subsets of $[n]$; the corresponding entry of M_k is 1 iff the row-subset and column-subset are disjoint. Thus M_k contains the I_ℓ for $\ell = \binom{n}{k}$ as a submatrix, and so its rank is at least $\binom{n}{k}$.

For DET_n, the same argument shows that the non-zero rows of $M_k(\text{DET}_\text{N})$ correspond to k-subsets of $[n]$ and the non-zero columns correspond to $(n-k)$-subsets of $[n]$; the corresponding entry of M_k is ± 1 iff the row-subset and column-subset are disjoint, and so the rank is again at least $\binom{n}{k}$.

3. (a) As in class, a monotone circuit for a degree n homogeneous polynomial f of size s implies that f can be written as

$$f = \sum_{i=1}^{s} g_i h_i$$

where $n/3 \leq \deg(g_i) \leq 2n/3$ and $\deg(h_i) = n - \deg(g_i)$, and g_i and h_i have all non-negative coefficients.

Let $f_n(X)$ be the perfect matching polynomial for graph G_n, and consider a particular $g_i h_i$. Let S be the vertices incident to edges mentioned in g_i and T be the vertices incident to edges mentioned in h_i. Each monomial in g_i must be a perfect matching on S and each monomial in h_i must be a perfect matching on T, and S, T must partition the vertices of G_n; otherwise a monomial appear in $g_i h_i$ that is not a perfect matching of G_n.

By the degree constraints on g_i, h_i we have that $|S|, |T|$ satisfy the conditions of the first lemma, which we will apply with t a large constant (say, 100), to obtain a set E' of well-separated edges crossing the S, T cut.

For each edge $e \in E'$, select a G_{22} subgraph that has the "distinguished vertex v" (from the second lemma) as an endpoint of e. By the well-separated-ness of E', these subgraphs are all vertex-disjoint.

Now, every perfect matching M of the whole graph G_n can be decomposed uniquely into (i) a matching M' in G_n with no edges contained in any of the G_{22} subgraphs (but possibly including edges that touch the outer face of a G_{22} subgraph), and (ii) for each G_{22} subgraph, a perfect matching on the graph that remains after deleting the already-covered vertices on the outer face.

For each such matching M', we have by the second lemma, that the ratio of total perfect matchings within a G_{22} subgraph to perfect matchings within a G_{22} subgraph that *exclude* the $e \in E'$ (that was used to select it) – of which there must be at least one since monomials of $g_i h_i$ are perfect matchings of G_n that exclude E' – is $c > 1$. Thus the ratio of total perfect matchings that extend M' to those that occur in $g_i h_i$ (and therefore exclude E') is $c^{|E'|} \geq c^{\epsilon n} = \exp(n)$.

We conclude that a given $g_i h_i$ term contains monomials corresponding to only an exponentially small fraction of all perfect matchings, and thus s must be exponential in n, as desired.

(b) We prove that every $(+, -, \times)$ circuit of size s can be converted to one using only a single negation, of size $O(s)$. We then apply the fact that f_n is in VP.

The proof is by induction on the size of the circuit. If the original circuit is a single constant c or a variable X_i, then we replace it with $c - 0$ if c is positive or $0 - c$ if c is non-positive, or $X_i - 0$ in the case of a variable.

Then, for a general circuit, if the top gate is computing $f = g + h$, then we have by induction monotone circuits computing g', g'', h', h'' such that $g = g' - g''$ and $h = h' - h''$. We then can write $f = f' - f''$ with $f' = g' + h'$ and $f'' = g'' + h''$.

Similarly, if the top gate is computing $f = g \times h$, then we have by induction monotone circuits computing g', g'', h', h'' such that $g = g' - g''$ and $h = h' - h''$ and we then can write $f = f' - f''$ with $f' = g'h' + g''h''$ and $f'' = g''h' + h''g'$.

Finally, if the top gate is computing $f = g - h$, then we have by induction monotone circuits computing g', g'', h', h'' such that $g = g' - g''$ and $h = h' - h''$ and we then can write $f = f' - f''$ with $f' = g'' + h''$ and $f'' = g' + h'$.