CS 153 **Current topics in theoretical computer science**	**Spring 2022**

Problem Set 2

Out: May 12 — *Due:* **May 27**

Reminder: you are encouraged to work in small groups; however you must turn in your own write-up and note with whom you worked. You may consult any materials related to this course. The full honor code guidelines and collaboration policy can be found in the course syllabus.

Please attempt all problems. **Please turn in a hard copy or email me your solutions.**

1. Given a group G, a multiplicative matching of cardinality m in G is given by three sequences of group elements $a_1, a_2, \ldots, a_m$, $b_1, b_2, \ldots, b_m$ and $c_1, c_2, \ldots, c_m$, with the property that

$$a_i b_j c_k = 1 \quad \Leftrightarrow \quad i = j = k.$$

   Give a multiplicative matching in S_n of cardinality at $n!/\exp(n)$. Hint: find a way to use the triangle TPP construction; use Stirling's approximation to help calculate the cardinality. You may take as given that the tensor $\langle n, n, n \rangle$ contains a diagonal of cardinality cn^2 for an absolute constant $c > 0$.

2. Let $f : F_p^n \to F_p$ be a polynomial of total degree d. Set $N = p^n$ and define the matrix M_f to be the $N \times N$ matrix with $M[i,j] = f(i+j)$ (where $i, j \in F_p^n$).

   (a) Give an example of a function f for which the matrix f for which M_f has full rank. Hint: your f will have total degree $(p-1)n$.

   (b) Prove that in general, the rank of M_f is at most $2\binom{d/2+n}{n}$.

3. Recall that a two-families construction in an abelian group H consists of two families of subsets $A_1, \ldots, A_n$ and $B_1, \ldots, B_n$ with these properties:

   - for all i, $|A_i B_i| = |A_i||B_i|$, and
   - for all i, and all $j \neq k$, $(A_i + B_i) \cap (A_j + B_k) = \emptyset$.

   The "two-families" conjecture is that there is a sequence of groups H containing two-families constructions, for which $|A_i| = |B_i| \geq |H|^{1/2-o(1)}$ and $n \geq |H|^{1/2-o(1)}$. As we proved in class, this would imply $\omega = 2$.

   (a) Let H be an abelian group and recall that H is isomorphic to $\prod_i Z_{q_i}^{k_i}$, where the q_i are distinct prime powers. Given a two-families construction $A_1, \ldots, A_n$, $B_1, \ldots, B_n$ in H, give a two-families construction $A'_1, \ldots, A'_n$, $B'_1, \ldots, B'_n$ in the H', the cyclic group of order $N = |H| \prod_i 2^{k_i}$, with matching sizes: i.e., $|A'_i| = |A_i|$ and $|B'_i| = |B_i|$.

   (b) Show that that if $N = |H| \prod_i 2^{k_i}$ is greater than $|H|^{1+\delta}$ (for a constant $\delta > 0$), then T_H (the tensor of H-multiplication) has slice-rank at most $|H|^{1-r(\delta)}$, where r is an increasing function of δ (i.e., as δ approaches zero, so does $r(\delta)$). You will want to use this theorem from class:

Theorem 2.1 *If an abelian group H has a subgroup isomorphic to Z_p^k then T_H has slice-rank at most $|H|/c^k$ for an absolute constant $c > 1$.*

(c) You may recall from class that we showed that a two-families construction in H implies a STPP construction in H^3, and an STPP construction in H^3 implies a multiplicative matching in H^3. Tracing through these constructions, we find that a two-families construction yielding the bound $\omega \leq 2 + \delta$ implies a multiplicative matching in H^3 of size at least $(|H|^3)^{1-c\delta}$, for an absolute constant $c > 0$.

Prove that if the two-families conjecture is true for any sequence of abelian groups H, then the two-families conjecture is true for the sequence of groups $H = \mathrm{Cyc}_N$.