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

Solution Set 2

Out: May 31

1. We first show, in general, that if $X, Y, Z \subseteq G$ satisfy the triple product property with $|X| = |Y| = |Z| = n$, then there is a multiplicative matching in G of cardinality at least cn^2, for an absolute constant $c > 0$. We use the fact that the tensor $\langle n, n, n \rangle$ has a diagonal of cardinality $m = cn^2$. This means that there are sets $S, T, U \subseteq [n]^2$, each of cardinality m, for which the subset $D \subseteq ([n]^2)^3$ given by

$$D = (S \times T \times U) \cap \{((i,j),(j,k),(k,i)) : i,j,k \in [n]\}$$

has the property that each of three canonical projections is injective.

Identify $[n]$ with each of X, Y, Z, and define the following functions from $[n]^2$ to G:

$$\begin{aligned} a(x,y) &= xy^{-1} \\ b(y,z) &= yz^{-1} \\ c(z,x) &= zx^{-1} \end{aligned}$$

Our multiplicative matching will be given by the set of triples:

$$\{(a(x,y), b(y,z), c(z,x)) : ((x,y),(y,z),(z,x)) \in D\}.$$

Notice that for any such triple we have $a(x,y)b(y,z)c(z,x) = 1$. Suppose we have three triples, not all equal:

$$(a(x,y), b(y,z), c(z,x)), \quad (a(x',y'), b(y',z'), c(z',x')), \quad (a(x'',y''), b(y'',z''), c(z'',x'')).$$

Notice that

$$((x,y),(y,z),(z,x)) \in (S \times T \times U)$$

(since $a(x,y) = xy^{-1}$ determines (x,y), $b(y,z) = yz^{-1}$ determines (y,z), and $c(z,x) = zx^{-1}$ determines (z,x), by the TPP) and

$$((x',y'),(y',z'),(z',x')) \in (S \times T \times U)$$

and

$$((x'',y''),(y'',z''),(z'',x'')) \in (S \times T \times U),$$

for the same reasons. Now, suppose for the purpose of contradiction that

$$a(x,y)b(y',z')c(z'',x'') = 1.$$

Then by the Triple Product Property, it must be that $y = y'$, $z' = z''$, and $x'' = x$, and so $((x, y), (y', z'), (z'', x''))$ is in the support of $\langle n, n, n \rangle$. But as we have argued,

$$((x, y), (y', z'), (z'', x'')) \in (S \times T \times U),$$

and thus this triple is included in our multiplicative matching, and so not all three projections can be injective, a contradiction.

Now, we must prove that in the triangle TPP construction in $G = S_N$ (for $N = n(n+1)/2$), then size of each of the subgroups X, Y, Z is at least $|G|/e^{\Omega(N)}$. Then plugging in to the previous argument gives the desired multiplicative matching.

Note that $|X| = |Y| = |Z| = n!(n-1)!(n-2)! \cdots 2!1!$.

Using the fact that $2^n > \binom{n}{i} = n!/((n-i)!i!)$, we see that

$$|X|^2 \geq (n+1)!^n / 2^{n(n+1)} \geq (n/(2e))^{n(n+1)},$$

where the last inequality used Stirling's approximation which implies that $n! \geq (n/e)^n$.

On the other hand we have

$$|G| = N! \leq \text{poly}(n) \cdot (n(n+1)/2)/e)^{n(n+1)/2} \leq \text{poly}(n) \cdot e^{O(N)} \cdot n^{n(n+1)},$$

and combining with the above lower bound on $|X|$, we obtain the desired result.

2. (a) Set f to be the function which is 1 on $0 \in F_p^n$, and 0 on the rest of the domain; i.e.,

$$f(X_1, X_2, \ldots, X_n) = \alpha \cdot \prod_{i=1}^{n} \prod_{a \in F_p, a \neq 0} (X_i - a),$$

where $\alpha = 1/\prod_{a \in F_p, a \neq 0}(-a)^n$ is a normalizing scalar. Clearly this f has degree $(p-1)n$, and M_f is a permutation matrix, which has full rank.

(b) Notice that $f(i+j)$ is a polynomial on $2n$ variables, with total degree d. Let S be the set of monomials in i of total degree at most $d/2$. Then because each monomial of total degree d must have i-degree at most $d/2$ OR j-degree at most $d/2$, we can write

$$f(i+j) = \sum_{M \in S} M(i) Q_M(j) + \sum_{M \in S} M(j) Q'_M(i),$$

where the Q_M and Q'_M are polynomials. But this is a rank $2|S|$ decomposition of M_f, and the claim follows from the observation that $|S| = \binom{d/2+n}{n}$.

3. (a) Assume that the distinct prime powers q_i are in increasing order; i.e., $q_1 < q_2 < q_3 < \ldots < q_t$. Set $r_i = 2q_i$. Define the map $f : \prod_i [r_i]^{k_i} \to \text{Cyc}_N$ by

$$\begin{aligned} f(a^{(1)}, a^{(2)}, \ldots a^{(t)}) &= \sum_{j=0}^{k_1-1} a_j^{(1)} r_1^j \\ &+ r_1^{k_1} \sum_{j=0}^{k_2-1} a_j^{(2)} r_2^j \end{aligned}$$

$$
\begin{aligned}
&+ \quad r_1^{k_1} r_2^{k_2} \sum_{j=0}^{k_3-1} a_j^{(3)} r_3^j \\
&+ \quad \cdots \\
&+ \quad r_1^{k_1} r_2^{k_2} \cdots r_{t-1}^{k_{t-1}} \sum_{j=0}^{k_t-1} a_j^{(t)} r_t^j,
\end{aligned}
$$

where $[n]$ denotes the integers $\{0, 1, 2, \ldots, n-1\}$.

It is clear then that $f(a^{(1)}, a^{(2)}, \ldots a^{(t)}) \bmod r_1^{k_1}$ is the integer whose base-r_1 digits are $a^{(1)}$. After subtracting this, and dividing by $r_1^{k_1}$, the remaining integer mod $r_2^{k_2}$ is the integer whose base-r_2 digits are $a^{(2)}$, and so on... Therefore the map is injective.

Moreover, if the entries in the vector $a^{(i)}$ are at most $(r_i - 1)/2$, and the entries in the vector $b^{(i)}$ are at most $(r_i - 1)/2$, it holds that

$$f(a^{(1)}, a^{(2)}, \ldots a^{(t)}) + f(b^{(1)}, b^{(2)}, \ldots b^{(t)}) = f(a^{(1)} + b^{(1)}, a^{(2)} + b^{(2)}, \ldots a^{(t)} + b^{(t)}),$$

since there are no "carries" in the addition in the integers.

We can apply the map f to H by identifying the elements of Z_{p_i} with the integers $\{0, 1, \ldots, p_i - 1\}$. Now if we apply map f to each of the elements of the A_i and B_i sets that make up the two-families construction, we obtain sets of the same cardinality (by injectivity), and by the aforementioned observation, we find that f is injective on $H + H$. This means that the defining axioms of the two-families construction hold for the A_i' and B_i' sets, as required (i.e. if some $f(a) + f(b) \in A_i' + B_i'$ was the same as some $f(c) + f(d) \in A_j' + B_k'$, then

$$f(a + b) = f(a) + f(b) = f(c) + f(d) = f(c + d)$$

which implies $a + b = c + d$ by injectivity but $a + b \in A_i + B_i$ and $c + d \in A_j + B_k$, etc...)

(b) Fix $\delta > 0$, set $k = \sum_i k_i$, and arrange the prime powers in increasing order (with repetitions) so that

$$H \cong Z_{p_1} \times Z_{p_2} \times Z_{p_3} \times \cdots \times Z_{p_k}$$

and $p_1 \leq p_2 \leq p_3 \leq \cdots \leq p_k$. We are going to break H into the part with prime powers less that $L = 2^{1/\delta}$ and the rest, denoted H_0 and H_1, so $H = H_0 \times H_1$. If $|H_0| = \prod_{i: p_i \leq L} p_i \leq |H|^\delta$, then we claim $N \leq |H|^{2\delta + (1+\delta)}$. This is because $2p_i \leq p_i^2$ for all i, and so we get that the size of H_0 at most squares, while the size of H_1 gets raised to at most $(1 + \delta)$ because $p_i > L$ implies $2p_i < p_i^{1+\delta}$. So, if $N > |H|^{1+3\delta}$, it must be that $|H_0| > |H|^\delta$.

But the prime powers appearing in H_0 are bounded by the constant L, and so one of them must appear at least $t = \log_L |H_0|/L$ times, and then by the Theorem, the slice rank of H is at most $|H|/c^t \leq |H|/|H_0|^{\log c/(L \log L)} = |H|^{1 - c'\delta^2/2^{1/\delta}}$, where $c' > 0$ is an absolute constant.

(c) Suppose we can prove $\omega \leq 2 + \delta$ for via and two-families construction in H. We are given that this implies a multiplicative matching in H^3 of cardinality at least $|H|^{3(1-c\delta)}$, which means that the slice rank of T_{H^3} is at least $|H|^{3(1-c\delta)}$ as well.

We claim that $N \leq |H|^{1+\delta'}$ (for δ' such that $r(\delta') > c\delta$). If not, then by the previous part, the slice rank of T_H is at most $|H|^{1-r(\delta')}$, which implies that the slice rank of T_{H^3} is at most $|H|^{3(1-r(\delta'))}$, a contradiction.

So by the first part, we have a two-families construction in Z_N with $N \leq |H|^{1+\delta'}$. If the two-families conjecture is true in a sequence of groups, then δ can be made arbitrarily small, and thus δ' can be made arbitrarily small. Thus we have a construction in cyclic groups where the size and number of the sets A_i, B_i remains the same, and the size of the containing group approaches $|H|$. If the first original construction proved the two-families conjecture, then this one does as well.