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

Solution Set 1

Out: May 8

1. The tensor in question is described by this trilinear form:

$$\begin{aligned} &a_{1,1}b_{1,1}c_{1,1} + a_{1,2}b_{2,1}c_{1,1} \quad + \\ &a_{2,1}b_{1,1}c_{1,2} + a_{2,2}b_{2,1}c_{1,2} \quad + \\ &a_{1,1}b_{1,2}c_{2,1} + a_{1,2}b_{2,2}c_{2,1} \quad + \\ &a_{2,1}b_{1,2}c_{2,2} + a_{2,2}b_{2,2}c_{2,2} \end{aligned}$$

We use the substitution method. Clearly the above trilinear form depends on $a_{1,1}$; thus in any rank decomposition there must be a product $\alpha(\vec{a})\beta(\vec{b})\gamma(\vec{c})$ with the coeffcient of $a_{1,1}$ in α not equal to zero. Set $a_{1,1}$ to a linear form in the a's that makes α (and this entire product) zero. Then by setting $b_{1,1} = 0$ and $b_{1,2} = 0$, we see that the trilinear form still depends on $a_{1,2}$, and therefore there must be another product in the rank decomposition $\alpha'(\vec{a})\beta'(\vec{b})\gamma'(\vec{c})$ with the coeffcient of $a_{1,2}$ in α' not equal to zero. Set $a_{1,2}$ to a linear form in the a's that makes α' (and this entire product) zero. Now set $c_{1,1} = c_{2,1} = 0$. What remains is the trilinear form of 1×2 by 2×2 matrix multiplication, unaffected by the substitutions so far. Since $\langle 1, 2, 2\rangle$ has 4 linearly independent slices, there must be at least 4 remaining terms in the rank decomposition, for a total of at least 6, as desired.

2. We use the fact that $a_{i,j}b_{j,k}c_{k,i} = 1$ for all $i \in [n], j \in [m], k \in [p]$, repeatedly. For any group element t, we can replace $b_{j,k}$ with $b_{j,k}t$ and $c_{k,i}$ with $t^{-1}c_{k,i}$ without changing the defining property of the a's, b's, and c's. We will do this for $t = c_{1,1}$. This lets us assume without loss of generality that $c_{1,1} = 1$.

   We would like to write $\{a_{i,j} | i \in [n]\}$ as a right-translation of a set X by something that depends only on j. We notice that $a_{i,j} = (b_{j,k}c_{k,i})^{-1} = c_{k,i}^{-1}b_{j,k}^{-1}$ and this holds for all k, so it holds in particular for $k = 1$. Thus we have:

$$a_{i,j} = c_{1,i}^{-1}b_{j,1}^{-1}.$$

   We would like to write $\{b_{j,k} | k \in [p]\}$ as a left-translation of a set Z by something that depends only on j. We have that $b_{j,k} = a_{i,j}^{-1}c_{k,i}^{-1}$ for all i, so in particular (with $i = 1$) we have:

$$b_{j,k} = a_{1,j}^{-1}b_{k,1}^{-1}.$$

   We will choose our $x_i = c_{1,i}^{-1}$ and our $z_k = b_{k,1}$. We will be done if we can select the y_j so that

$$y_j^{-1}y_{j'} = b_{j,1}^{-1}a_{1,j'}^{-1} \quad \Leftrightarrow \quad j = j',$$

and indeed, since $a_{1,j}b_{j_1} = c_{1,1} = 1$ we get that $b_{j,1} = a_{1,j}^{-1}$ and so $y_j = a_{1,j}^{-1}$ meets this requirement. In summary we have

$$X = \left\{c_{1,i}^{-1} : i \in [n]\right\} \;\; Y = \left\{a_{1,j}^{-1} : j \in [m]\right\} \;\; Z = \{b_{k,1} : k \in [p]\}\,.$$

Then $x_i^{-1}x_{i'}y_j^{-1}y_{j'}z_k^{-1}z_{k'} = 1$ is equivalent to the statement:

$$c_{1,i}c_{1,i'}^{-1}\left(b_{j,1}^{-1}a_{1,j'}^{-1}\right)b_{k,1}^{-1}b_{k',1} = 1$$

which is equivalent to:

$$\left(c_{1,i'}^{-1}b_{j,1}^{-1}\right)\left(a_{1,j'}^{-1}b_{k,1}^{-1}\right) = c_{1,i}^{-1}b_{k',1}^{-1} = c_{1,i}^{-1}c_{1,1}b_{k',1}^{-1} = \left(c_{1,i}^{-1}b_{1,1}^{-1}\right)\left(a_{1,1}^{-1}b_{k',1}^{-1}\right)$$

The left-hand-side is just $a_{i',j}b_{j',k}$ and the right-hand-side is $a_{i,1}b_{1,k'} = c_{i,k'}$, so we get $i = i', j = j', k = k'$ as required.

3. Pick uniformly random elements $s, t, u \in G$. The expected size of $|Xs \cap A|$ is $|X|$ times $|A|/|G|$ by linearity of expectation, and similarly the expected size of $|Yt \cap A|$ is $|Y|$ times $|A|/|G|$ and the expected size of $|Zu \cap A|$ is $|Z|$ times $|A|/|G|$. Fixe s, t, u that realize at least these expectations.

   Note that for any particular s, t, u, the sets Xs, Yt, Zu satisfy the triple product property if X, Y, Z do. So the sets $X' = (Xs \cap A), Y' = (Yt \cap A)$ and $Z'(Zu \cap A)$ do as well. Since A is abelian:

$$|X'||Y'||Z'| \leq |A|,$$

   and we have just argued that

$$|X||Y||Z|(|A|/|G|)^3 \leq |X'||Y'||Z'|;$$

   putting these together completes the proof.