6.842 Randomness and Computation May 8, 2022

Homework 5 Problem 4

Yuchong Pan, Guanghao Ye

(a) *Proof.* Let $X = (X_1, \ldots, X_n) \in \{\pm 1\}^n$ be an (ε, k)-wise independent random vector for some $\varepsilon \in (0, 1)$ and $k \in [n]$. Let $S \subset [n]$ be such that $0 < |S| \le k$. By straightforward calculations (see, e.g., the proof of Problem 1 part (a) in Homework 2), for all $\ell \in [n]$,

$$\mathop{\mathbb{P}}_{(W_1,\ldots,W_\ell)\sim\mathsf{Unif}\{\pm 1\}^\ell}\left[\prod_{i=1}^{\ell} W_\ell = 1\right] = \frac{1}{2}.$$

Since X is (ε, k)-wise independent and since $0 < |S| \le k$,

$$\left|\mathop{\mathbb{P}}_{X}\left[\prod_{i\in S} X_i = 1\right] - \frac{1}{2}\right| = \left|\mathop{\mathbb{P}}_{X}\left[\prod_{i\in S} X_i = 1\right] - \mathop{\mathbb{P}}_{(W_1,\ldots,W_\ell)\sim\mathsf{Unif}\{\pm 1\}^\ell}\left[\prod_{i=1}^{\ell} W_\ell = 1\right]\right| \le \varepsilon.$$

WLOG, assume that

$$\mathop{\mathbb{P}}_{X}\left[\prod_{i\in S} X_i = 1\right] = \frac{1+\varepsilon_0}{2},$$

for some $\varepsilon_0 \in [0, 2\varepsilon]$ (the case $\mathbb{P}_X[\prod_{i\in S} X_i = 1] = (1-\varepsilon_0)/2$ for some $\varepsilon_0 \in [0, 2\varepsilon]$ is symmetric). Let $\lambda = 1/(1+\varepsilon_0) \in (0, 1]$. Let $Y = (Y_1, \ldots, Y_n) \in \{\pm 1\}^n$ be a random vector defined as follows:

(i) With probability λ, let $Y = X$.
(ii) With probability $1 - \lambda$, let Y be uniform over

$$\mathcal{W} := \left\{(x_1, \ldots, x_n) \in \{\pm 1\}^n : \prod_{i\in S} x_i = -1\right\}. \tag{1}$$

Then

$$\mathop{\mathbb{P}}_{Y}\left[\prod_{i\in S} Y_i = 1\right] = \lambda \mathop{\mathbb{P}}_{X}\left[\prod_{i\in S} X_i = 1\right] + (1-\lambda)\cdot 0 = \frac{1}{1+\varepsilon_0}\cdot\frac{1+\varepsilon_0}{2} = \frac{1}{2}.$$

For all $\mathcal{T} \subset \{\pm 1\}^n$,

$$\begin{aligned}
\mathop{\mathbb{P}}_{X}[X \in \mathcal{T}] - \mathop{\mathbb{P}}_{Y}[Y \in \mathcal{T}] &= \mathop{\mathbb{P}}_{X}[X \in \mathcal{T}] - \left(\lambda \mathop{\mathbb{P}}_{X}[X \in \mathcal{T}] + (1-\lambda) \mathop{\mathbb{P}}_{W\sim\mathsf{Unif}\,\mathcal{W}}[W \in \mathcal{T}]\right) \\
&= (1-\lambda)\left(\mathop{\mathbb{P}}_{X}[X \in \mathcal{T}] - \mathop{\mathbb{P}}_{W\sim\mathsf{Unif}\,\mathcal{W}}[W \in \mathcal{T}]\right) \\
&\le (1-\lambda)(1-0) = 1 - \frac{1}{1+\varepsilon_0} = \frac{\varepsilon_0}{1+\varepsilon_0} \\
&\le \varepsilon_0 \le 2\varepsilon.
\end{aligned}$$

Therefore,

$$\Delta(X, Y) = \max_{\mathcal{T}\subset\{\pm 1\}^n}\left(\mathop{\mathbb{P}}_{X}[X \in \mathcal{T}] - \mathop{\mathbb{P}}_{Y}[Y \in \mathcal{T}]\right) \le 2\varepsilon.$$

This completes the proof. ◻

(b) *Proof.* Let $X \in \{\pm 1\}^n$ be an (ε, k)-wise independent random vector for some $\varepsilon \in (0,1)$ and $k \in [n]$. We give a procedure in Algorithm 1 to obtain a k-wise independent random vector $Z \in \{\pm 1\}^n$ such that $\Delta(X, Z) \leq 2\varepsilon n^k$, where line 3 uses part (a). We denote by subscript $i \in [n]$ the i^{th} coordinate of a vector.

1 $Y \leftarrow X$
2 **foreach** $S \subset [n]$ *with* $0 < |S| \leq k$ **do**
3 construct a random vector $Y' \in \{\pm 1\}^n$ with $\mathbb{P}_{Y'}[\prod_{i \in S} Y'_i = 1] = 1/2$ and $\Delta(Y, Y') \leq 2\varepsilon$
4 $Y \leftarrow Y'$
5 $Z \leftarrow Y$
6 **return** Z

Algorithm 1: A procedure that, given an (ε, k)-wise independent random vector $X \in \{\pm 1\}^n$ where $\varepsilon \in (0,1)$ and $k \in [n]$, returns a k-wise independent random vector $Z \in \{\pm 1\}^n$ such that $\Delta(X, Z) \leq 2\varepsilon n^k$.

Note that $\Delta(Y, Y') \leq 2\varepsilon$ during each iteration. Let $(S_1, \ldots, S_\ell)$ be an enumeration of subsets $S \subset [n]$ with $0 < |S| \leq k$. By the triangle inequality,

$$\begin{aligned}
\Delta(X, Z) &\leq \Delta\left(X, S_1\right) + \sum_{i=2}^{\ell} \Delta\left(S_{i-1}, S_i\right) \\
&= 2\varepsilon |\{S \subset [n] : 0 < |S| \leq k\}| \\
&\leq 2\varepsilon \left| [n]^k \right| = 2\varepsilon n^k. \qquad (2)
\end{aligned}$$

Note that (2) follows from the fact that each k-tuple $(i_1, \ldots, i_k) \in [n]^k$ corresponds to a subset $S = \{i_1, \ldots, i_k\} \subset [n]$ with $0 < |S| \leq k$.

Now, we prove that Z is k-wise independent. Since $\mathbb{P}_{Y'}[\prod_{i \in S} Y'_i = 1] = 1/2$ in the iteration for each subset $S \subset [n]$ with $0 < |S| \leq k$, then it suffices to show that the iteration for a subset $S \subset [n]$ with $0 < |S| \leq k$ does not increase $|\mathbb{P}_{Y'}[\prod_{i \in T} Y'_i] - 1/2|$ for all $T \subset [n]$ with $0 < |T| \leq k$ and $S \neq T$. To see this, we first note that

$$\mathop{\mathbb{P}}_{W \sim \mathsf{Unif}\, \mathcal{W}}\left[\sum_{i \in T} W_i = 1\right] = \frac{1}{2},$$

where $\mathcal{W}$ is defined as in (1), by straightforward calculations (see, e.g., the proof of Problem 1 part (a) in Homework 2). Then

$$\begin{aligned}
\left| \mathop{\mathbb{P}}_{Y'}\left[\prod_{i \in T} Y'_i = 1\right] - \frac{1}{2} \right| &= \left| \left(\lambda \mathop{\mathbb{P}}_{Y}\left[\prod_{i \in T} Y_i = 1\right] + (1 - \lambda) \cdot \frac{1}{2} \right) - \frac{1}{2} \right| \\
&= \left| \lambda \left(\mathop{\mathbb{P}}_{Y}\left[\prod_{i \in T} Y_i = 1\right] - \frac{1}{2} \right) \right| = \lambda \left| \mathop{\mathbb{P}}_{Y}\left[\prod_{i \in T} Y_i = 1\right] - \frac{1}{2} \right|.
\end{aligned}$$

Since $\lambda \in (0,1]$, then this shows that the iteration for a subset $S \subset [n]$ with $0 < |S| \leq k$ does not increase $|\mathbb{P}_{Y'}[\prod_{i \in T} Y'_i] - 1/2|$ for all $T \subset [n]$ with $0 < |T| \leq k$ and $S \neq T$. Hence, at the end of the procedure, $\mathbb{P}_Z[\prod_{i \in S} Z_i] = 1/2$ for all $S \subset [n]$ with $0 < |S| \leq k$. This shows that Z is k-wise independent, completing the proof. $\square$