The uniform marginals lemma in [GPW17]

Xinyu Wu*

September 27, 2018

Abstract

We present an alternative proof of the uniform marginals lemma in [GPW17], using some facts about the level-k Fourier weights of Boolean functions.

1 Uniform marginals lemma

First, we change notation to use $\{-1,1\}$ instead of $\{0,1\}$ in the index gadget g. Recall that n is the number of gadgets, and m is the number of inputs of each gadget. Section 4 of [GPW17] reduces the uniform marginals lemma to proving the following. We can take "ρ-structured" to mean that the first k coordinates are free, while the next $n-k$ coordinates are fixed. We also only need to use the assumptions of "ρ-structured" instead of "ρ-essentially-structured" in this proof.

Lemma 1 ([GPW17, Lemma 8, restated]). *View $\boldsymbol{X}$ as a probability distribution on $[m]^k$ and $\boldsymbol{Y}$ as a probability distribution on $(\{-1,1\}^m)^k$, satisfying that for every $I \subseteq [k]$,*

(i) $\boldsymbol{D}_\infty(\boldsymbol{X}_I) \leq 0.1|I|\log m$

(ii) $\boldsymbol{D}_\infty(\boldsymbol{Y}_I) \leq n^3$

where $\boldsymbol{X}_I$ denotes projection onto the coordinates in I.

Then, for any $z \in \{-1,1\}^k$, $G(\boldsymbol{X},\boldsymbol{Y})$ is $1/n^3$-pointwise-close to the uniform distribution.

The proof makes use of the following lemma.

Lemma 2 ([GPW17, Lemma 9]). *If a random variable $\boldsymbol{z}$ over $\{-1,1\}^k$ satisfies*

$$\left|\mathbf{E}\left[\prod_{i\in I} \boldsymbol{z}_i\right]\right| \leq 2^{5|I|\log n} \tag{1}$$

for every $I \subseteq [k]$, then $\boldsymbol{z}$ is $1/n^3$-pointwise-close to uniform.

*Computer Science Department, Carnegie Mellon University. xinyuw1@andrew.cmu.edu

For simplicity, we will show that the conditions to use Lemma 2 are satisfied for $I = [k]$; restricting to any I works since the hypothesis on $\boldsymbol{X}$ and $\boldsymbol{Y}$ work for any I.

Next, we make some definitions and observations. Let $\varphi_Y : (\{-1,1\}^m)^k \to [0,1]$ be the probability density function on $\boldsymbol{Y}$, defined by

$$\varphi_Y(y) = |\boldsymbol{Y}| \cdot \mathbf{Pr}[\boldsymbol{Y} = y].$$

where $|\boldsymbol{Y}|$ denotes the size of the domain of $\boldsymbol{Y}$. Such a density function has the property that $\mathbf{E}[\varphi_Y] = 1$.

We write φ_Y in the Fourier basis as

$$\varphi_Y(y) = \sum_{S \subseteq (\{\pm 1\}^m)^k} \widehat{\varphi_Y}(S)\chi_S(y)$$

where $\chi_S(y) := \prod_{i \in S} y_i$ is the parity function. We also have the formula for the Fourier coefficients

$$\widehat{\varphi_Y}(S) = \mathop{\mathbf{E}}_{y \text{ unif.}}[\varphi_Y(y)\chi_S(y)].$$

If we have $S \in [m]^k$, we can interpret S as an index into the km bits of y, and define $\widehat{\varphi_Y}(S)$ accordingly.

Also define $\|\varphi_Y\|_\infty = \max_y \varphi_Y(y)$ and notice that

$$\log\|\varphi_Y\|_\infty = \log \max_y \varphi_Y(y) = \log \max_y |\boldsymbol{Y}| \, \mathbf{Pr}[\boldsymbol{Y} = y] = \log |\boldsymbol{Y}| - \boldsymbol{H}_\infty(\boldsymbol{Y}) = \boldsymbol{D}_\infty(\boldsymbol{Y}).$$

We use the notation $\boldsymbol{Y}^{(i)}$ for the i^{th} block of m bits, and $\boldsymbol{Y}^{(i)}_{\boldsymbol{X}_i}$ as indexing into the block. Inequality (1) then becomes

$$\left| \mathbf{E}\left[\prod_{i=1}^k \boldsymbol{Y}^{(i)}_{\boldsymbol{X}_i} \right] \right| \leq 2^{-5k \log n}, \tag{2}$$

Fix $S \in [m]^k$. We then have

$$\left| \mathop{\mathbf{E}}_{Y \sim \varphi_Y}\left[\prod_{i=1}^k Y^{(i)}_{S_i} \right] \right| = \left| \mathop{\mathbf{E}}_{y \text{ unif.}}\left[\varphi_Y(y) \prod_{i=1}^k y^{(i)}_{S_i} \right] \right| = |\widehat{\varphi_Y}(S)|.$$

Next, from assumption (i) on $\boldsymbol{X}$, we have

$$\max_x \log \mathbf{Pr}[\boldsymbol{X} = x] \leq 0.1k \log m - \log |X| = -0.9k \log m.$$

Therefore, $\max_x \mathbf{Pr}[\boldsymbol{X} = x] \leq \frac{1}{m^{0.9k}}$, so

$$\mathop{\mathbf{E}}_{S \sim \boldsymbol{X}}[|\widehat{\varphi_Y}(S)|] \leq \frac{1}{m^{0.9k}} \sum_{S \in [m]^k} |\widehat{\varphi_Y}(S)|.$$

Then, we use Cauchy–Schwarz on the sum, and get

$$\frac{1}{m^{0.9k}} \sum_{S \in [m]^k} |\widehat{\varphi_Y}(S)| \le \frac{1}{m^{0.4k}} \left(\sum_{S \in [m]^k} \widehat{\varphi_Y}(S)^2 \right)^{1/2} \le \frac{1}{m^{0.4k}} \left(\sum_{\substack{S \subseteq [km] \\ |S| \le k}} \widehat{\varphi_Y}(S)^2 \right)^{1/2}. \tag{3}$$

In the last inequality, we switch to viewing $\boldsymbol{Y}$ as a distribution on $\{-1,1\}^{km}$. The valid Fourier coefficients in the original case are just those that have exactly one coordinate in each of the k blocks of m bits. So, we relax this by summing all Fourier coefficients of cardinality at most k.

Now, to analyze this quantity, we make the following definition.

Definition 1. The *Fourier weight up to degree k* of a function $f : \{-1,1\}^n \to [0,1]$ is

$$\mathbf{W}^{\le k}[f] = \sum_{\substack{S \subseteq [n] \\ |S| \le k}} \widehat{f}(S)^2.$$

We also require the following theorem from [O'D14, Chapter 9.5] [1].

Theorem 1 (Level-k inequality)**.** *Let $f : \{-1,1\}^n \to [0,1]$ have mean $\mathbf{E}[f] = \alpha$ and let $k \in \mathbb{N}^+$ be at most $2 \ln \frac{1}{\alpha}$. Then,*

$$\mathbf{W}^{\le k}[f] \le \left(\tfrac{2e}{k} \ln \tfrac{1}{\alpha}\right)^k \alpha^2.$$

Corollary 1. *Let φ be a density function, and let $k \in \mathbb{N}^+$ be at most $2 \ln \|\varphi\|_\infty$. Then,*

$$\mathbf{W}^{\le k}[\varphi] \le \left(\tfrac{2e}{k} \ln \|\varphi\|_\infty\right)^k.$$

Proof. Let $M := \|\varphi\|_\infty$. Apply the Level-k inequality to the function $f := \frac{\varphi}{M}$, which gives

$$\mathbf{W}^{\le k}[f] \le \left(\tfrac{2e}{k} \ln M\right)^k \tfrac{1}{M^2}.$$

But since $\widehat{f}(S) = \frac{1}{M}\widehat{\varphi}(S)$, we have $\mathbf{W}^{\le k}[f] = \frac{1}{M^2}\mathbf{W}^{\le k}[\varphi]$, so we conclude that

$$\mathbf{W}^{\le k}[\varphi] \le \left(\tfrac{2e}{k} \ln \|\varphi\|_\infty\right)^k.$$

□

From Equation (3), setting $C_k := \frac{2e}{k \log e}$, by the corollary and assumption (ii) we have

$$\frac{1}{m^{0.4k}} \left(\sum_{\substack{S \subseteq [km] \\ |S| \le k}} \widehat{\varphi_Y}(S)^2 \right)^{1/2} = \frac{1}{m^{0.4k}} (\mathbf{W}^{\le k}[\varphi_Y])^{1/2} \le \frac{1}{m^{0.4k}} (C_k D_\infty(\boldsymbol{Y}))^{1/2} \le \left(C_k \frac{n^3}{m^{0.8}} \right)^{k/2},$$

which is at most n^{-5k} when we set $m = n^{17}$, and this gives us the desired Inequality (2).

[1] The inequality there is stated for $f : \{-1,1\}^n \to \{0,1\}$, but it also applies to functions with range $[0,1]$. Following the proof in [O'D14], the fact that the range is $\{0,1\}$ is used in Corollary 9.8, to say that $\mathbf{E}[|\mathbb{1}_A(x)|^{4/3}|] = \mathbf{E}[\mathbb{1}_A(x)] = \alpha$. But if f is any function with range in $[0,1]$ such that $\mathbf{E}[f] = \alpha$, we have $\mathbf{E}[|f|^{4/3}] \le \mathbf{E}[f] = \alpha$, which is what we needed in the proof.

2 Acknowledgments

I would like to thank Ryan O'Donnell for suggesting this proof.

References

[GPW17] Mika Göös, Toniann Pitassi, and Thomas Watson. Query-to-communication lifting for BPP. In *Proceedings of the 58th Annual Symposium on Foundations of Computer Science*, 2017. (document), 1, 1, 2

[O'D14] Ryan O'Donnell. *Analysis of boolean functions*. Cambridge University Press, 2014. 1, 1