1 Introduction

Standard Definitions. We identify the *long code* of $x \in \{0,1\}^s$ by $\mathsf{LC}(x) = \{f(x) \mid f : \{0,1\}^s \to \{0,1\}\}$. Informally, we evaluate x on every Boolean function on s bits. Notice that every Boolean function on s bits may be represented by its truth table. In other words, by specifying its evaluation on all the 2^s inputs. Alternatively, any string of length 2^s may be interpreted as a Boolean function on s bits. We denote 2^s by n. Since, there are 2^n Boolean functions on s bits, $\mathsf{LC}(\mathbf{x})$ is a string on length 2^n. We use the letters a, b to denote Boolean functions. It is easy to check that given a table f, $f \equiv \mathsf{LC}(\mathbf{x} : \{0,1\}^{2^s} \to \{0,1\})$, $f(a) + f(b) = f(a+b)$, for every $a, b \in \{0,1\}^{2^s}$.

For $\alpha \subset [n]$, define

$$\chi_\alpha : \{0,1\}^n \to \{0,1\}, \chi_\alpha(a) \triangleq \prod_{i\in\alpha} -1^{a(i)}$$

It is easy to check that the characters $\{\chi_\alpha\}_{\alpha\subseteq[n]}$ form an orthonormal basis for the space of functions $\{f : \{0,1\}^n \to \mathbb{R}\}$, where inner product is defined by $\langle f, g\rangle = \mathbb{E}_a[f(a)g(a)] = 2^{-n}\sum_a f(a)g(a)$. It follows that any function $f : \{0,1\}^n \to \{0,1\}$ can be written as $f = \sum_\alpha \hat{f}_\alpha \cdot \chi_\alpha$, where $\hat{f}_\alpha = \langle f, \chi_\alpha\rangle$. We start by recalling a few important properties of the characters of the space of Boolean functions.

Proposition 1.1. *For every character χ_α and any two vectors x, y, $\chi_\alpha(x \cdot y) = \chi_\alpha(x) \cdot \chi_\alpha(y)$.*

Proposition 1.2 (Orthonormality)**.** *For $k > 1$ and vector x, the following holds.*

$$\exists\ i, j \ \in\ [k] :\ \alpha_i \neq \alpha_j \Leftrightarrow \mathbb{E}_x\Big[\chi_{\alpha_1}(x) \cdot \chi_{\alpha_2}(x) \ldots \chi_{\alpha_k}(x)\Big] = 0$$

Proposition 1.3. *For every character χ_α, vector x and an integer y such that y mod $2 = 0$,*

$$\mathbb{E}_x\big[\left(\chi_\alpha\left(x\right)\right)^y\big] = 1$$

The Long Code Test. Let $f : \{0,1\}^n \to \{0,1\}$. We intend to test if $f : \{0,1\}^n \to \{0,1\}$ is in fact the legal encoding of a value $w \in [s]$. In other words, if $f(a) = a(w)$ for all $a \in [2^n]$.

Fix a parameter $\rho \in [0,1]$. The test picks two uniformly random vectors $a, b \in \{0,1\}^n$ and then $x \in \{0,1\}^n$ according to the following distribution: for every coordinate $i \in [n]$, with probability $1-\rho$ we choose $x_i = 0$ and $x_i = 1$ otherwise. It is useful to imagine x as a noise vector. The test accepts iff $f(a) + f(b) + f(a+b+x) = 0$. The test accepts iff $x_w = 0$, which happens with probability $1-\rho$. It follows from the construction that the test accepts any valid long code encoding with probability $1-\rho$. We now state a certain converse of that, which was established by Håstad's lemma [Hås01].

Lemma 1.4 (Corollary 22.25 in [AB09])**.** *For every $\delta, \epsilon > 0$, if f passes the long code test with probability with $1/2 + \delta$, then for $k = \frac{1}{2\rho}\log\frac{1}{\epsilon}$, there exists α with $|\alpha| \leq k$ such that $\hat{f}_\alpha \geq 2\delta - \epsilon$.*

Say f is a purported long code table given to the verifier. We denote by T_{r} (the long code) test performed by the verifier on randomness r. The verifier accepts iff T_{r} evaluates to 0. We are interested in analyzing the soundness of a variant of $T_{\mathsf{r}_1} \cdot T_{\mathsf{r}_2}$, for $\mathsf{r}_1, \mathsf{r}_2$ drawn from the uniform distribution. Our new verifier chooses a, b, c, d uniformly at random from $\{0,1\}^n$ and x, y are noise vectors. The new test may be expressed as the following.

$$\big[f(a) + f(b) + f(a+b+x)\big] \cdot \big[f(c) + f(d) + f(c+d+y)\big] = 0$$

$$\begin{aligned}\Leftrightarrow & f(a)\cdot f(c)+f(a)\cdot f(d)+f(a)\cdot f(c+d+y)+\\ & \qquad f(b)\cdot f(c)+f(b)\cdot f(d)+f(b)\cdot f(c+d+y)\\ & \qquad\qquad f(a+b+x)\cdot f(c)+f(a+b+x)\cdot f(d)+f(a+b+x)\cdot f(c+d+y)=0\\ \Leftrightarrow & f(a\cdot c)+f(a\cdot d)+f(a\cdot (c+d+y))+\\ & \qquad f(b\cdot c)+f(b\cdot d)+f(b\cdot (c+d+y))\\ & \qquad\qquad f((a+b+x)\cdot c)+f((a+b+x)\cdot d)+f((a+b+x)\cdot (c+d+y))=0\end{aligned}$$

We transform $\{0,1\}$ to $\{\pm 1\}$ via the mapping $b \to (-1)^b$. This also maps the usual XOR operation on $GF(2)$ to a product operation and the multiplication operation to a new operation $\otimes$. We now recall a few basic properties of the operation $\otimes$.

Proposition 1.5 ($\otimes$ distributes over the product)**.** *For every m, n, k,*

$$m \otimes (n \cdot k) = (m \otimes n) \cdot (m \otimes k)$$

Now, the "new" test may be written as the following.

$$\begin{aligned}& f(a\otimes c)\cdot f(a\otimes d)\cdot f(a\otimes (c\cdot d\cdot y))\cdot f(b\otimes c)\cdot f(b\otimes d)\cdot f(b\otimes (c\cdot d\cdot y))\cdot\\ & \qquad f((a\cdot b\cdot x)\otimes c)\cdot f((a\cdot b\cdot x)\otimes d)\cdot f((a\cdot b\cdot x)\otimes (c\cdot d\cdot y))=1\end{aligned}$$

We would now analyze the soundness of the test discussed in the prequel. Say, the verifier accepts the test by probability $1/2+\delta$, for some $\delta > 0$. Since the product terms like $a \otimes c$ and others may not be uniformly distributed, we use a standard trick of replacing $f(a\cdot c)$ by $f(e\cdot a \oplus c)\cdot f(e)$, where e is chosen uniformly at random from $\{0,1\}^n$.

$$2\cdot\delta = \mathbb{E}\Big[f((a\otimes c)\cdot e)\cdot f(e)\cdot f((a\otimes d)\cdot e)\cdot f(e)\ldots\ldots f\left(((a\cdot b\cdot x)\otimes (c\cdot d\cdot y)\cdot e\right)\cdot f(e)\Big]$$

$$\begin{aligned}2\cdot\delta = \mathbb{E}_{a,b,c,d,e,x,y}\Bigg[& \left(\sum_{\alpha_1}\hat{f}_{\alpha_1}\chi_{\alpha_1}((a\otimes c)\cdot e)\right)\cdot\left(\sum_{\alpha_2}\hat{f}_{\alpha_2}\chi_{\alpha_2}(e)\right)\cdot\left(\sum_{\alpha_3}\hat{f}_{\alpha_3}\chi_{\alpha_3}((a\otimes d)\cdot e)\right)\ldots\\ & \ldots\left(\sum_{\alpha_{17}}\hat{f}_{\alpha_{17}}\chi_{\alpha_{17}}((a\cdot b\cdot x)\otimes (c\cdot d\cdot y)\cdot e)\right)\cdot\left(\sum_{\alpha_{18}}\hat{f}_{\alpha_{18}}\chi_{\alpha_{18}}(e)\right)\Bigg]\end{aligned}$$

$$\begin{aligned}2\cdot\delta = \mathbb{E}_{a,b,c,d,e,x,y}\Bigg[& \sum_{\alpha_1,\alpha_2,\ldots\alpha_{18}}\hat{f}_{\alpha_1}\hat{f}_{\alpha_2}\ldots\hat{f}_{\alpha_{18}}\ \chi_{\alpha_1}((a\otimes c)\cdot e))\cdot\chi_{\alpha_2}(e)\cdot\chi_{\alpha_3}((a\otimes d)\cdot e))\ldots\\ & \ldots\chi_{\alpha_{17}}((a\cdot b\cdot x)\otimes (c\cdot d\cdot y)\cdot e)\cdot\chi_{\alpha_{18}}(e)\Bigg]\end{aligned}$$

By linearity of expectation, the above expression may be written as follows.

$$\begin{aligned}2\cdot\delta = \sum_{\alpha_1,\alpha_2\ldots\alpha_{18}}\hat{f}_{\alpha_1}\hat{f}_{\alpha_2}\ldots\hat{f}_{\alpha_{18}}\quad \mathbb{E}_{a,b,c,d,e,x,y}\Bigg[& \chi_{\alpha_1}((a\otimes c)\cdot e))\cdot\chi_{\alpha_2}(e)\cdot\chi_{\alpha_3}((a\otimes d)\cdot e))\ldots\\ & \ldots\chi_{\alpha_{17}}((a\cdot b\cdot x)\otimes (c\cdot d\cdot y)\cdot e)\cdot\chi_{\alpha_{18}}(e)\Bigg]\end{aligned}$$

We apply Proposition 1.1 to simplify the above expression to the following.

$$2 \cdot \delta = \sum_{\alpha_1,\alpha_2 \dots \alpha_{18}} \hat{f}_{\alpha_1} \hat{f}_{\alpha_2} \dots \hat{f}_{\alpha_{18}} \quad \mathbb{E}_{a,b,c,d,e,x,y} \Bigg[\chi_{\alpha_1}(a \otimes c) \cdot \chi_{\alpha_1}(e) \cdot \chi_{\alpha_2}(e) \cdot \chi_{\alpha_3}(a \otimes d) \cdot \chi_{\alpha_3}(e) \dots$$
$$\dots \chi_{\alpha_{17}}((a \cdot b \cdot x) \otimes (c \cdot d \cdot y)) \cdot \chi_{\alpha_{17}}(e) \cdot \chi_{\alpha_{18}}(e) \Bigg]$$

Since e is mutually independent from a, b, c, d, x, y, we have

$$2 \cdot \delta = \sum_{\alpha_1,\alpha_2 \dots \alpha_{18}} \hat{f}_{\alpha_1} \hat{f}_{\alpha_2} \dots \hat{f}_{\alpha_{18}} \quad \mathbb{E}_{a,b,c,d,x,y} \Bigg[\chi_{\alpha_1}(a \otimes c) \cdot \chi_{\alpha_3}(a \otimes d) \dots \chi_{\alpha_{17}}((a \cdot b \cdot x) \otimes (c \cdot d \cdot y)) \Bigg] \cdot$$
$$\mathbb{E}_e \Bigg[\chi_{\alpha_1}(e) \cdot \chi_{\alpha_2}(e) \cdot \chi_{\alpha_3}(e) \dots \chi_{\alpha_{18}}(e) \Bigg]$$

We now invoke Proposition 1.2 to conclude that the expectation is 0 unless $\alpha_1 = \alpha_2 \dots = \alpha_{18}$. Therefore,

$$2 \cdot \delta = \sum_{\alpha} \hat{f}_{\alpha}^{18} \; \mathbb{E}_{a,b,c,d,x,y} \Bigg[\chi_{\alpha}(a \otimes c) \cdot \chi_{\alpha}(a \otimes d) \dots \chi_{\alpha}((a \cdot b \cdot x) \otimes (c \cdot d \cdot y)) \Bigg] \cdot \mathbb{E}_e \Bigg[\big(\chi_{\alpha}(e)\big)^{18} \Bigg]$$

By Proposition 1.3, $\mathbb{E}_e \Bigg[\big(\chi_{\alpha}(e)\big)^{18} \Bigg] = 1$. Hence,

$$\begin{aligned} 2 \cdot \delta &= \sum_{\alpha} \hat{f}_{\alpha}^{18} \quad \mathbb{E}_{a,b,c,d,x,y} \Bigg[\chi_{\alpha}\left((a \otimes c) \cdot \chi_{\alpha}(a \otimes d) \dots \chi_{\alpha}((a \cdot b \cdot x) \otimes (c \cdot d \cdot y)\right) \Bigg] \\ &= \sum_{\alpha} \hat{f}_{\alpha}^{18} \quad \mathbb{E}_{a,b,c,d,x,y} \Bigg[\chi_{\alpha}\Big((a \otimes c) \cdot (a \otimes d) \cdot (a \otimes (c \cdot d \cdot y)) \cdot \\ &\qquad (b \otimes c) \cdot (b \otimes d) \cdot b \otimes (c \cdot d \cdot y) \cdot \\ &\qquad ((a \cdot b \cdot x) \otimes c) \cdot ((a \cdot b \cdot x) \otimes d) \cdot \big((a \cdot b \cdot x) \otimes (c \cdot d \cdot y)\big) \Big) \Bigg] \end{aligned}$$

Invoking Proposition 1.5, we rewrite the above as.

$$\begin{aligned} 2 \cdot \delta &= \sum_{\alpha} \hat{f}_{\alpha}^{18} \quad \mathbb{E}_{a,b,c,d,x,y} \Bigg[\chi_{\alpha}\Big((a \otimes y) \cdot \\ &\qquad (b \otimes y) \cdot \\ &\qquad (a \cdot b \cdot x) \otimes y \Big) \Bigg] \\ &= \sum_{\alpha} \hat{f}_{\alpha}^{18} \; \mathbb{E}_{x,y} \Big[\chi_{\alpha}(x \otimes y) \Big] \end{aligned}$$

Denote $x \otimes y$ by z. Notice that each coordinate of z in the above equation is drawn is chosen independently from the product distribution of $x \otimes y$. Since, each coordinate of x, y is independently set to 1 with probability $1-\rho$ and -1 otherwise, $\mathbb{E}\left[z_w\right] = \mathbb{E}\left[x_w \otimes y_w\right] = 1 \cdot ((1-\rho)^2 + \rho^2) - 1 \cdot 2 \cdot (1-\rho) \cdot \rho = 1 - 4\rho + 4\rho^2$. Now, since each coordinate is chosen independently, $\mathbb{E}_z\left[\chi_\alpha(z)\right] = \mathbb{E}_z\left[\prod_{w \in \alpha} z_w\right]$. Hence,

$$2\delta = \sum_\alpha \hat{f}_\alpha^{18} \left(1 - 4 \cdot \rho \cdot (1-\rho)\right)^{|\alpha|}$$

References

[AB09] S. Arora and B. Barak. *Computational Complexity - A Modern Approach*. Cambridge University Press, 2009. 1

[Hås01] J. Håstad. Some optimal inapproximability results. *Journal of the ACM*, 48(4):798–859, 2001. 1