NOTE ON CHEBYSHEV POLYNOMIALS

In this note we show that Chebyshev polynomials are completely bounded in the sense of [ABP19]. As an immediate corollary, using the characterization of quantum query algorithms from [ABP19] and a well-known result of Nisan and Szegedy [NS94], we recover the quantum algorithm for the OR_n function restricted to strings of Hamming weight at most 1, as implied by Grover.

For each $k \in \mathbb{N} \cup \{0\}$ the Chebyshev polynomial $T_k \in \mathbb{R}[x]$ is the degree-k polynomial defined recursively by

$$\begin{aligned} T_0(x) &= 1 \\ T_1(x) &= x \\ T_{k+1}(x) &= 2xT_k(x) - T_{k-1}(x). \end{aligned}$$

Define the n-variate polynomials $p_k \in \mathbb{R}[x_1, \dots, x_n]$ by

$$p_k(x_1, \dots, x_n) = T_k\Big(\frac{x_1 + \dots + x_n}{n}\Big). \tag{1}$$

1. Main lemma

Lemma 1.1. *For each $k \geq 2$ there exists a k-linear form F_k on $\mathbb{R}^n$ such that $\|F_k\|_{\mathrm{cb}} \leq 1$ and $F_k(x, \dots, x) = p_k(x)$ for each $x \in \{-1, 1\}^n$.*

Proof: Define the bilinear form F_2 on $\mathbb{R}^n$ and linear forms $f_1^1, \dots, f_1^n$ on $\mathbb{R}^n$ by

$$F_2(x, y) = \mathbb{E}_{i \in [n]}\Big[x_i\Big(\underbrace{2\mathbb{E}_{j \in [n]}[y_j] - y_i}_{f_1^i(y)}\Big)\Big], \tag{2}$$

where the expectations are over uniformly random indices in $[n]$. For $k \geq 2$, recursively define the $(k+1)$-linear form F_{k+1} and k-linear forms $f_k^1, \dots, f_k^n$ by

$$F_{k+1}(x, y, \mathbf{z}) = \mathbb{E}_{i \in [n]}\Big[x_i\Big(\underbrace{2F_k(y, \mathbf{z}) - y_i f_{k-1}^i(\mathbf{z})}_{f_k^i(y, \mathbf{z})}\Big)\Big], \tag{3}$$

for $x, y \in \mathbb{R}^n$ and $\mathbf{z} \in (\mathbb{R}^n)^{k-2}$.

We first show by induction on k that $F_k(x,\dots,x) = p_k(x)$ for every $x \in \{-1,1\}^n$. Since $x_i^2 = 1$ for $x_i \in \{-1,1\}$, it is easy to see from (2) that

$$F_2(x,x) = 2\big(\mathbb{E}_{i\in[n]}[x_i]\big)p_1(x) - 1 = p_2(x).$$

Let $k \geq 2$ and assume that the claim holds for k. Below, the number of repetitions of x in a sequence $(x,\dots,x)$ will vary but be clear from the context. Again using that $x_i^2 = 1$, it follows from (3) that

$$F_{k+1}(x,\dots,x) = 2\mathbb{E}_{i\in[n]}[x_i]F_k(x,\dots,x) - \mathbb{E}_{i\in[n]}\big[f^i_{k-1}(x,\dots,x)\big].$$

By the induction hypothesis, that $F_k(x,\dots,x) = p_k(x)$, we find that

$$\begin{aligned}
\mathbb{E}_{i\in[n]}\big[f^i_{k-1}(x,\dots,x)\big] &= \mathbb{E}_{i\in[n]}\Big[2F_{k-1}(x,\dots,x) - x_i f^i_{k-2}(x,\dots,x)\Big]\\
&= 2p_{k-1}(x) - \mathbb{E}_{i\in[n]}\big[x_i f^i_{k-2}(x,\dots,x)\big]\\
&= 2p_{k-1}(x) - F_{k-1}(x,\dots,x)\\
&= 2p_{k-1}(x) - p_{k-1}(x) = p_{k-1}(x).
\end{aligned}$$

Hence,

$$F_{k+1}(x,\dots,x) = 2\mathbb{E}_{i\in[n]}[x_i]p_k(x) - p_{k-1}(x) = p_{k+1}(x),$$

which proves the claim.

Next we show that $\|F_k\|_{\mathrm{cb}} \leq 1$. To this end, we first show that for every $k,d \in \mathbb{N}$, vector $v \in \mathbb{C}^d$ and collection of contractions $\mathbf{X} = ((X_i^1)_{i=1}^n,\dots,(X_i^k)_{i=1}^n)$ in $\mathbb{C}^{d\times d}$, we have

$$\mathbb{E}_{i\in[n]}\big[\|(f^i_k)_d(\mathbf{X})v\|_2^2\big] \leq \|v\|_2^2, \tag{4}$$

where $(f^i_k)_d$ is the "lifted" version of the k-linear form f^i_k as in (3).

We again induct on k. For $k=1$, the expectation (4) reduces to

$$\mathbb{E}_{i\in[n]}\big\|(2\mathbb{E}_{j\in[n]}[X_j] - X_i)v\big\|_2^2. \tag{5}$$

The above square norm equals

$$4\mathbb{E}_{j,k\in[n]}\langle X_j v, X_k v\rangle - 2\mathbb{E}_{j\in[n]}\big[\langle X_j v, X_i v\rangle\big] - 2\mathbb{E}_{k\in[n]}\big[\langle X_i v, X_k v\rangle\big] + \|X_i v\|_2^2. \tag{6}$$

The expectation over i in (5) thus causes the first three terms in (6) to cancel. The result follows since each X_i is a contraction.

Let $k \geq 1$ and assume the claim for k. Let $X = (X_i^1)_{i=1}^n$ and let $\mathbf{Y} = ((X_i^2)_{i=1}^n,\dots,(X_i^k)_{i=1}^n)$. By definition of f^i_{k+1}, we then have that

$$(f^i_{k+1})_d(X,\mathbf{Y}) = 2(F_{k+1})_d(X,\mathbf{Y}) - X_i^1(f^i_k)_d(\mathbf{Y}).$$

Define $A = (F_{k+1})_d(X, \mathbf{Y})$ and $B_i = X_i^1(f_k^i)_d(\mathbf{Y})$, so that the above equals $2A - B_i$. Observe that by definition of F_{k+1}, we have

$$\mathbb{E}_{i\in[n]}[B_i] = (F_{k+1})_d(Y, \mathbf{X}) = A.$$

Hence,

$$\begin{aligned}
\mathbb{E}_{i\in[n]}\left[\left\|(f_k^i)_d(\mathbf{X})v\right\|_2^2\right] &= \mathbb{E}_{i\in[n]}\left[\|(2A - B_i)v\|_2^2\right] \\
&= \mathbb{E}_{i\in[n]}\left[4\|Av\|_2^2 - 2\langle Av, B_iv\rangle - 2\langle B_iv, Av\rangle + \|B_iv\|_2^2\right] \\
&= \mathbb{E}_{i\in[n]}\left[\|B_iv\|_2^2\right] \\
&= \mathbb{E}_{i\in[n]}\left[\|X_i(f_k^i)_d(\mathbf{Y})v\|_2^2\right] \\
&\leq \mathbb{E}_{i\in[n]}\left[\|(f_k^i)_d(\mathbf{Y})v\|_2^2\right] \\
&\leq \|v\|_2^2,
\end{aligned}$$

where the first inequality follows from the fact that X_i is a contraction and and the second inequality follows by the induction hypothesis. This proves (4).

Let $\mathbf{X}, X, \mathbf{Y}$ and v be as above. Then, by Jensen's inequality and (4),

$$\begin{aligned}
\|(F_k)_d(X, \mathbf{Y})v\|_2 &= \left\|\mathbb{E}_{i\in[n]}\left[X_i(f_{k-1}^i)_d(\mathbf{Y})\right]v\right\|_2 \\
&\leq \mathbb{E}_{i\in[n]}\left\|(f_{k-1}^i)_d(\mathbf{Y})v\right\|_2 \\
&\leq \left(\mathbb{E}_{i\in[n]}\left\|(f_{k-1}^i)_d(\mathbf{Y})v\right\|_2^2\right)^{1/2} \\
&\leq \|v\|_2
\end{aligned}$$

showing that $\|F_k\|_{\mathrm{cb}} \leq 1$. □

2. Obtaining Grover's algorithm.

Notation. For $i \in [n]$, let $e_i \in \{-1, 1\}^n$ be the vector with -1 on the ith position and 1s otherwise. Let OR_n be an n-bit function defined as: $\mathrm{OR}_n(x) = 1$ if and only if $x = 1^n$. Let $|x| = \sum_i x_i$.

Nisan and Szegedy [NS94] showed that the Chebyshev polynomials can be used to find low-degree polynomials that approximate OR_n. A slight modification of their argument allows us to recover a the existence of a $O(\sqrt{n})$-quantum query algorithm for OR_n restricted to strings of Hamming weight at most 1, as implied by Grover.

Lemma 2.1. *Let $D = \{e_i\}_{i\in[n]} \cup \{1^n\}$ and let $\mathrm{OR}_n : D \to \{-1, 1\}$. There exists a $O(\sqrt{n})$-query quantum algorithm that, on input x, outputs a sign with expected value $\mathrm{OR}(x)$, with error at most $1/4$.*

Proof: Let $d = 2\pi/5 \cdot \sqrt{n}$. Here, we show that

$$\left|T_d\Big(\frac{|x|}{n}\Big) - \mathrm{OR}(x)\right| \leq 1/4 \quad \text{for all } x \in D. \tag{7}$$

To see this, first observe that for $x = 1^n$, we have $T_d(|x|/n) = 1$ and $\mathrm{OR}_n(1^n) = 1$, so Eq. (7) is satisfied. Let $x = e_i$ for some $i \in [n]$. By the definition of Chebyshev polynomials, we have

$$T_d\Big(\frac{|x|}{n}\Big) = T_d\Big(1 - \frac{2}{n}\Big) = \cos\left(d \arccos\left(1 - \frac{2}{n}\right)\right).$$

By the Taylor series expansion of $\arccos(1-z)$ (around the point $z = 0$), we have $\arccos(1 - z) \geq \sqrt{2z}$. This implies that $d \arccos(1 - 2/n) \geq 2\pi/5 \cdot \sqrt{n} \cdot \sqrt{4/n} = 4\pi/5$. Using the monotonicity and negativity of $\cos(\phi)$ for $\phi \in (\pi/2, \pi)$, we have

$$T_d\Big(\frac{|x|}{n}\Big) = \cos\left(d \arccos\left(1 - \frac{2}{n}\right)\right) \leq \cos(4\pi/5) \leq -\frac{3}{4}.$$

In particular, for such xs the value of $\mathrm{OR}_n(x) = -1$, so Eq. (7) is satisfied.

The proof of the lemma follows from Eq. (1) and Lemma 1.1. □

References

[ABP19] Srinivasan Arunachalam, Jop Briët, and Carlos Palazuelos. Quantum query algorithms are completely bounded forms. *SIAM J. Comput*, 48(3):903–925, 2019. Preliminary version in ITCS'18.

[NS94] N. Nisan and M. Szegedy. On the degree of Boolean functions as real polynomials. *Computational Complexity*, 4(4):301–313, 1994. Earlier version in STOC'92.