14. Short codes and sum of squares II.

Lecturer: Massimo Lauria

Disclaimer: this lecture note has neither been reviewed by the main lecturer, nor peer-review by any other student. It is released as it is for the convenience of the students.

`http://www.csc.kth.se/~lauria/sos14/`

This lecture continue on the topic of short codes and SOS. Two examples are discussed. The first is the example of Hypercube, and the second is the Reed-Muller codes. The lecture is also based on the same paper[1] from Leture 13.

[1] Boaz Barak, Parikshit Gopalan, Johan Håstad, Raghu Meka, Prasad Raghavendra, and David Steurer. Making the long code shorter. In *Proceedings of the 53rd Annual Symposium on Foundations of Computer Science (FOCS '12)*, pages 370–379, 2012

Example on Hypercube

We want to look at a graph which is a small set expander and that has many eigenvalues that are $\geq 1 - \varepsilon$. Consider a graph G with $V = \{0,1\}^R$ and connect vertices $\{x, y\}$ if $d(x, y) = \varepsilon n$. For a Cayley graph: $V = \{0,1\}^R$, such that there is an edge between x and $x + t$ if $t \in \mathcal{T} \subseteq \mathbb{F}_2^R$. It is always true that the eigenvalues

$$\lambda_\alpha = \mathop{\mathbb{E}}_{t \in \mathcal{T}}[\chi_\alpha(t)],$$

where $\chi_\alpha(t)$ are the corresponding characters. So, for G where the number of vertices is 2^n, we have

$$\lambda_\alpha = (1 - 2\varepsilon)^{|\alpha|}.$$

This is a large number if $|\alpha|$ is small, and in particular when $|\alpha| = 1$. We want to check how many eigenvalues $\geq 1 - \varepsilon$. We need

$$(1 - 2\delta)^{|\alpha|} \geq 1 - \varepsilon,$$

which is true if $|\alpha| \cdot 2\delta \leq \varepsilon$, which implies that for all $|\alpha| \leq \frac{\varepsilon}{2\delta}$, the eigenvalues$\lambda_\alpha$ will be large. We note that if we have smaller δ, we get larger number of large eigenvalues.

Is the hypercube a small set expander? We shall look at the bilinear form

$$\langle \mathbb{1}_S, G\mathbb{1}_S \rangle$$

from the last lecture, which we want to bound. The Fourier expansion of $\mathbb{1}_S$ is given by

$$\mathbb{1}_S(x) = \sum_\alpha \hat{\mathbb{1}}_\alpha \chi_\alpha(x)$$

We can split this sum according to the size of eigenvalues so that

$$\mathbb{1}_S = f^{small} + f^{large}$$

in which the f^{small} corresponds to the large eigenvalues, $k \leq |\alpha|$, and the f^{large} corresponds to the small eigenvalues, $k > |\alpha|$. Noting that

$$G\mathbb{1}_S(x) = \sum_\alpha \lambda_\alpha \hat{\mathbb{1}}_\alpha \chi_\alpha(x)$$

we can have the following bound

$$\langle \mathbb{1}_S, Gf^{large} \rangle \leq (1-2\delta)^k \mu(S)$$

To have a similar bound on the smaller part, we need to look at hypercontractivity. Consider $\|f\|_p = \mathbb{E}[|f|^p]^{\frac{1}{p}}$ as a function of p^2, where $1 \leq p \leq \infty$. One observation, by jensen's inequality, is that the p-norm is an increasing function of p. Moreover if f is of degree k, then all p-norms are within $c_{k,p}$ constant of each other.

The p-norm of the indicator function over S is given by

$$\|\mathbb{1}_S\|_p = \mathbb{E}[\mathbb{1}_S^p]^{\frac{1}{p}} = \mathbb{E}[\mathbb{1}_S]^{\frac{1}{p}}$$

and since $\mathbb{E}[\mathbb{1}_S] = \mu(S)$,

$$\|\mathbb{1}_S\|_p = \mu(S)^{\frac{1}{p}}.$$

Therefore, if the set size $\mu(S)$ is small, the p-norm $\|\mathbb{1}_S\|_p$ grows significantly with p. In particular we have

$$\|f\|_4^4 \leq q^k \|f\|_2^4.$$

Now using Hölder inequality, we can have a bound on the bilinear form applied to the smaller part

$$\langle \mathbb{1}_S, Gf^{small} \rangle \leq \|Gf^{small}\|_4 \; \|\mathbb{1}_S\|_{\frac{4}{3}}.$$

since f has low degree, and 2-norm, 4-norm are about the same. Because $\|Gf^{small}\|_4 \leq 2^k \|Gf^{small}\|_2$, we see that

$$\langle \mathbb{1}_S, Gf^{small} \rangle \leq 2^k \mu(S)^{1/4} \mu(S).$$

Using the two bounds that we found, we can bound $\langle \mathbb{1}_S, G\mathbb{1}_S \rangle$. First, we can pick $k = -log(\frac{\varepsilon}{2})/2\delta$ so that $\langle \mathbb{1}_S, Gf^{small} \rangle \leq \frac{\varepsilon}{2}\mu(S)$. Then, having $\mu(S) \leq (2k)^4 (\frac{\varepsilon}{2})^4$, means that we have also that $\langle \mathbb{1}_S, Gf^{large} \rangle \leq \frac{\varepsilon}{2}\mu(S)$. Therefore we have,

$$\langle \mathbb{1}_S, G\mathbb{1}_s \rangle \leq \varepsilon \mu(S).$$

Reed-Muller Codes

Now we turn our attention to Reed-Muller codes constructions. Consider the space P_d^n of multivariate polynomials with n variables and of degree d. Then we construct the code on all evaluations of points in that space $(p(x))_{x \in \{0,1\}^n}$ such that $deg(p) \leq d$. Let $R = 2^n$, and consider $V = P_d^n$. There will be an edge between a given point p and $p + \Pi_{i=1}^d L_i(x)$, where L_i is an affine function defined as

$$L_i(x) = a_0^i + \sum_{j=1}^n a_j^i x_j.$$

We note here that for any p with degree $d \neq 0$, we have $|\{x | p(x) \neq 0\}| \geq 2^n / 2^d$. This can be shown using induction and noting that $x_i \in 0, 1$.

The dual space of Reed-Muller codes is all functions $Q(x)$ such that $\forall p \in P_d^n$ it hold that $\sum_{x \in \{0,1\}^n} p(x)Q(x)$ is even. It is a known fact that this is exactly $P^n_{n-(d+1)}$. A useful observation to see this is to note that $\sum_x p(x)$ is odd if and only if p is of degree n of $\mathbb{F}_2$.

We proceed similarly as the hypercube example. The characters are now the same as before, however the points in our space now are multivariate polynomials on the hypercube. So we define

$$\chi_\alpha(p) = (-1)^{\sum_x \alpha(x)p(x)}.$$

It then holds that $\chi_\alpha \equiv \chi'_\alpha$ if $\alpha = \alpha' + Q$ for all $Q \in P^n_{n-(d+1)}$.

The argument for this case follows exactly the same lines as that in the first section. Consider a set $S \subset P^d_n$, and define the indicator function of the set on the space $\mathbb{1}_s : P^d_n \to \{0, 1\}$. As in the first section we split the Fourier expansion of the indicator function into two parts

$$\mathbb{1}_S = f^{small} + f^{large}.$$

the eigenvalues here are

$$\lambda_\alpha = \mathop{\mathbb{E}}_{\Pi_i L_i}[\chi_\alpha(\Pi^r_{i=1} L_i)],$$

where we choose here the smallest representative for χ_α. For example, let the size of α, that is the number of points for which $\alpha = 1$, be 1 and call that point x_0, then

$$\lambda_\alpha = \mathbb{E}[(-1)^{\Pi^d_{i=1} L_i(x_0)}] = 1 - 2^{-(d-1)}$$

This will give us large eigenvalues.

References

[BGH+12] Boaz Barak, Parikshit Gopalan, Johan Håstad, Raghu Meka, Prasad Raghavendra, and David Steurer. Making the long code shorter. In *Proceedings of the 53rd Annual Symposium on Foundations of Computer Science (FOCS '12)*, pages 370–379, 2012.