Optimal bounds for sign-representing the intersection of two halfspaces by polynomials

Alexander A. Sherstov

The treshold degree of a function $f : \{0,1\}^n \to \{-1,1\}$ is the least degree of real polynomial p with $f(x) \equiv \mathrm{sgn} p(x)$, denoted $deg_{\pm}(f)$.

Theorem 1 (Main theorem) *For $n = 1, 2, 3, \ldots$, let $D(n)$ denote the maximum treshold degree of a function of the form $f(x) \wedge g(x)$, where $f, g : \{0,1\}^n \to \{-1,1\}$ are halfspaces. Then $D(n) = \Theta(n)$.*

We give a randomized algorithm which constructs two halfspaces on $\{0,1\}^n$ whose intersection has treshold degree $\Theta(n)$.

Tools

The binary entropy function $H(p) = -p \log p - (1-p)\log(1-p)$ ($H : [0,1] \to [0,1]$) is strictly increasing on $[0, 1/2]$. Fact:

$$\sum_{i=0}^{k} \binom{n}{i} \leq 2^{H(k/n)n}, \qquad k = 0, 1, 2, \ldots, \lfloor n/2 \rfloor.$$

Fourier transform.

- inner product: $\langle f, g \rangle = 2^{-n} \sum_{x \in \{0,1\}^n} f(x)g(x)$
- $\chi_S : \{0,1\}^n \to \{-1,1\}$: $\chi_S(x) = (-1)^{\sum_{i \in S} x_i}$ yields an orthonormal basis
- a unique representation: $f = \sum_{S \subseteq \{1,\ldots,n\}} \hat{f}(S)\chi_S$, where $\hat{f}(S) = \langle f, \chi_s \rangle$
- Parseval's identity: $\sum_{S \subseteq \{1,\ldots,n\}} \hat{f}(S)^2 = \langle f, f \rangle$

Analysis of random halfspaces

Lemma 2 *Let $f, g : \{0,1\}^n \to 0, 1$ be given functions. Fix an integer k with $0 \leq k \leq n/2$. For a set $S \subseteq \{1, \ldots, n\}$, define $F_S : \{0,1\}^n \to \{0,1\}$ by*

$$F_S(x) = f(x) \wedge \left(g(x) \oplus \bigoplus_{i \in S} x_i \right).$$

Fix a real $\zeta > 0$. Then with probability at least $1 - 2^{-n+H(k/n)n+2\zeta n}$ over a uniformly random choice of $S \in \mathcal{P}(\{1, 2, \ldots, n\})$, one has

$$\left| \hat{F}_S(T) - \frac{1}{2}\hat{f}(T) \right| \leq 2^{-\zeta n - 1}, \qquad |T| \leq k.$$

Lemma 3 *Fix an integer $k \geq 0$ and reals $\varepsilon, \zeta \in (0, 1/2)$. Choose sets $S_0, S_1, \ldots, S_k \in \mathcal{P}(\{1, 2, \ldots, n\})$ uniformly at random. Fix any integer s and define $f : \{0,1\}^n \to \{0,1\}$ by*

$$f(x) = 1 \Leftrightarrow \sum_{i=0}^{k} 2^i \sum_{j \in S_i} x_j \equiv s \pmod{2^{k+1}}.$$

Then with probability at least $1 - (k+1)2^{-n+H(\varepsilon)n+2\zeta n}$ over the choice of $S_0, S_1, \ldots, S_k$, one has

$$\left| \hat{f}(T) - \frac{\delta_{T,\emptyset}}{2^{k+1}} \right| \leq 2^{-\zeta n}, \qquad |T| \leq \varepsilon n.$$

Theorem 4 (Key property of random halfspaces) *Fix an integer $k \geq 0$ and reals $\varepsilon, \zeta \in (0, 1/2)$. Choose integers $w_1, w_2, \ldots, w_n$ uniformly at random from $\{0, 1, \ldots, 2^{k+1} - 1\}$. For $s \in \mathbb{Z}$, define $f_s : \{0,1\}^n \to \{0,1\}$ by*

$$f_s(x) = 1 \Leftrightarrow \sum_{i=0}^{n} w_i x_i \equiv s \pmod{2^{k+1}}.$$

Then with probability at least $1 - (k+1)2^{-n+H(\varepsilon)n+2\zeta n+k+1}$ over the choice of $w_1, w_2, \ldots, w_n$, one has

$$\left| \hat{f}_s(T) - \frac{\delta_{T,\emptyset}}{2^{k+1}} \right| \leq 2^{-\zeta n}, \qquad |T| \leq \varepsilon n, \qquad s \in \mathbb{Z}.$$

Zeroing out correlations by a change of distribution

$f, g : X \to (R)$, X finite, then $\langle f, g \rangle = \frac{1}{|X|} \sum_{x \in X} f(x) g(x)$.

Theorem 5 *Let $f, \chi_1, \ldots, \chi_k : X \to \{-1, +1\}$ be given functions on a finite set X. Suppose that*

$$\sum_{i=1}^{k} |\langle f, \chi_i \rangle| < \frac{1}{2},$$

$$\sum_{j=1, j \neq i}^{k} |\langle \chi_i, \chi_j \rangle| \leq \frac{1}{2}, \qquad i = 1, 2, \ldots, k.$$

Then there exists a probability distribution μ on X such that

$$\mathbb{E}_\mu[f(x)\chi_i(x)] = 0, \qquad i = 1, 2, \ldots, k.$$

Theorem 6 *Let $\alpha > 0$ be a sufficiently small absolute constant. Choose integers $w_1, w_2, \ldots, w_n$ uniformly at random from $\{0, 1, \ldots, 2^{\lfloor \alpha n \rfloor + 1} - 1\}$. For $s \in \mathbb{Z}$, define*

$$X_s = \left\{ x \in \{0,1\}^n : \sum_{i=1}^{n} w_i x_i \equiv s \pmod{2^{\lfloor \alpha n \rfloor} + 1} \right\}.$$

Then with probability at least $1 - e^{-n/3}$ over the choice of $w_1, w_2, \ldots, w_n$, there is a distribution μ_s on X_s (for each s) such that

$$\mathbb{E}_{\mu_s}[p(x)] = \mathbb{E}_{\mu_t}[p(x)]$$

for any $s, t \in \mathbb{Z}$ and any polynomial p of degree at most $\lfloor \alpha n \rfloor$.

Reduction to a univariate problem

Another tools: rational aproximation.

- $\deg p(x)/q(x) := \max\{\deg(p), \deg(q)\}$, where p, q are polynomials on $\mathbb{R}^n$
- $f : X \to \{-1, +1\}$, where $X \subseteq \mathbb{R}^n$. For $d \geq 0$ define

$$R(f, d) = \inf_{p,q} \sup_{x \in X} \left| f(x) - \frac{p(x)}{q(x)} \right|,$$

  where the infimum is over all polynomials p, q of degree up to d such that $q|_X \not\equiv 0$.
- $R^+(f, d) = \inf_{p,q} \sup_{x \in X} \left| f(x) - \frac{p(x)}{q(x)} \right|$ where q is positive on X
- $R^+(f, 2d) \leq R(f, d) \leq R^+(f, d)$
- $S \subseteq \mathbb{R}$: $R^+(S, d) = \inf_{p,q} \sup_{x \in S} \left| \mathrm{sgn} x - \frac{p(x)}{q(x)} \right|$

Theorem 7 (Sherstov) *Let n, d be positive integers, $R = R^+(\{\pm 1, \pm 2, \ldots, \pm n\}, d)$. For $1 \leq d \leq \log n$,*

$$\exp\left\{ -\Theta\left(\frac{1}{n^{1/(2d)}} \right) \right\} \leq R < \exp\left\{ -\frac{1}{n^{1/d}} \right\}.$$

For $\log n < d < n$,

$$R = \exp\left\{ -\Theta\left(\frac{1}{\log(2n/d)} \right) \right\}.$$

For $d \geq n$, $\quad R = 0$.

Theorem 8 (Sherstov) *Let $f : X \to \{-1, +1\}$ and $g : Y \to \{-1, +1\}$ be given functions, where $X, Y \subseteq \mathbb{R}^n$ are arbitrary finite sets. Assume that f and g are not identically false. Let $d = \deg_\pm(f \wedge g)$. Then*

$$R^+(f, 4d) + R^+(g, 2d) < 1.$$

Proposition 9 *Let $n_1, \ldots, n_k$ be positive integers, $|x| := x_1 + x_2 + \ldots + x_n$. Consider a function $F : \{0,1\}^{n_1} \times \ldots \times \{0,1\}^{n_k} \to \{-1, +1\}$ such that $F(x_1, \ldots, x_k) \equiv f(|x_1|, \ldots, |x_k|)$ for some $f : \{0, 1, \ldots, n_1\} \times \ldots \times \{0, 1, \ldots, n_k\} \to \{-1, +1\}$. Then for all d, $R^+(F, d) = R^+(f, d)$.*

Theorem 10 (Reduction to a univariate problem) *Put $k = \lfloor \alpha n \rfloor$, where $\alpha > 0$ is the absolute constant from Theorem 6. Choose $w_1, w_2, \ldots, w_n \in \{0, 1, \ldots, 2^{\lfloor \alpha n \rfloor + 1} - 1\}$ uniformly at random. Define $f : \{0,1\}^n \times \{0, 1, 2, \ldots, n\} \to \{-1, +1\}$ by*

$$f(x, t) = sgn\left(\frac{1}{2} + \sum_{i=1}^{n} w_i x_i - 2^{k+1} t \right).$$

Then with probability at least $1 - e^{-n/3}$ over the choice of $w_1, w_2, \ldots, w_n$, one has

$$R^+(f, d) \geq R^+(\{\pm 1, \pm 2, \ldots, \pm 2^k\}, d), \qquad d = 0, 1, \ldots, k.$$

Theorem 11 *Put $k = \lfloor \alpha n \rfloor$, where $\alpha > 0$ is the absolute constant from Theorem 6. Choose $w_1, w_2, \ldots, w_n$ uniformly at random from $\{0, 1, \ldots, 2^{\lfloor \alpha n \rfloor + 1} - 1\}$. Define $f : \{0,1\}^{2n} \to \{-1, +1\}$ by*

$$f(x) = sgn\left(\frac{1}{2} + \sum_{i=1}^{n} w_i x_i - 2^{k+1} \sum_{i=n+1}^{2n} x_i\right).$$

Then with probability at least $1 - e^{-n/3}$ over the choice of $w_1, w_2, \ldots, w_n$, one has

$$R^+(f, d) \geq R^+(\{\pm 1, \pm 2, \ldots, \pm 2^k\}, d), \qquad d = 0, 1, \ldots, k.$$

Now it is easy to prove the main result.

Theorem 12 (Main result) *Fix sufficiently small absolute constants $\alpha > 0$ and $\beta = \beta(\alpha) > 0$. Choose integers $w_1, w_2, \ldots, w_n \in \{0, 1, \ldots, 2^{\lfloor \alpha n \rfloor + 1} - 1\}$ uniformly at random. Then with probability at least $1 - e^{-n/3}$, the function $f : \{0,1\}^{2n} \to \{-1, +1\}$ given by*

$$f(x) = sgn\left(\frac{1}{2} + \sum_{i=1}^{n} w_i x_i - 2^{\lfloor \alpha n \rfloor + 1} \sum_{i=n+1}^{2n} x_i\right)$$

obeys $\deg_{\pm}(f \wedge f) \geq \lfloor \beta n \rfloor$.