1 Block Sensitivity

Block sensitivity is a lower bound on all query complexity measures (?)

Definition 1 (Block sensitivity)**.** *For an input $x \in \{0,1\}^N$ and a subset of variables $S \subseteq \{1, 2, \ldots, N\}$, $x^{(S)}$ is the input obtained from x by changing all $x_i, i \in S$ to opposite values. The block sensitivity $bs(f)$ is the maximum k for which there is an input $x \in \{0,1\}^N$ and pairwise disjoint subsets $S_1, \ldots, S_k \subseteq \{1, \ldots, N\}$ with $f(x) \neq f(x^{(S_i)})$ for all $1 \leq i \leq k$*

What does this mean in the context of error-correcting codes? We want to know the block sensitivity of f, our decoding algorithm. For linear decoding, we have $f : \{0,1\}^n \to \{0,1\}^k$ where the messages are of length k and the codewords have $n - k$ check bits.

Theorem 1. *For linear codes $\mathscr{C} = [n, k]$ with minimum distance d, the nearest neighbor decoding function $f : \{0,1\}^n \to \{0,1\}^k$ has a block sensitivity*

$$bs(f) \leq \frac{n}{\lfloor \frac{1}{2}(d-1) \rfloor + 1}$$

Proof. Our linear code has minimum distance d. By (theorem 2 in MacWilliams and Sloane), the code can correct $\lfloor \frac{1}{2}(d-1) \rfloor$ errors. Thus, $f(x) = f(x^{(S)})$ where $|S| \leq \lfloor \frac{1}{2}(d-1) \rfloor$. Correct decoding is not guaranteed when $|S| > \lfloor \frac{1}{2}(d-1) \rfloor$. There are at most $n/(\lfloor \frac{1}{2}(d-1) \rfloor + 1)$ pairwise disjoint sets of size $\lfloor \frac{1}{2}(d-1) \rfloor + 1$ in $\{1, \ldots, n\}$, which could all potentially lead to decoding errors. Thus,

$$bs(f) \leq \frac{n}{\lfloor \frac{1}{2}(d-1) \rfloor + 1}.$$

□

2 Certificate Complexity

For an input $x \in \{0,1\}^N$, a certificate is a set $S \subseteq \{1, \ldots, N\}$ with the property that the variables $x_i, i \in S$ determine the value of $f(x)$.

Definition 2 (Certificate complexity)**.** *$S \subseteq \{1, \ldots, N\}$ is a certificate on an input x if, for any $y \in \{0,1\}^N$ such that $x_i = y_i, i \in S$, we have $f(x) = f(y)$. $C_x(f)$ is the minimum size $|S|$ of a certificate S on input x. The certificate complexity $C(f)$ is the maximum of $C_x(f)$ over all $x \in \{0,1\}$.*

Theorem 2. *For a linear code $\mathscr{C} = [n, k]$ with distance d, the nearest neighbor decoding function f has certificate complexity $C(f) = n - d + 1$.*

Proof. Nearest neighbor decoding relies on the minimum distance d between any two codewords. Our code $\mathscr{C}$ has minimum distance d; thus, there exist received codewords x and y with distance $2 \cdot \lfloor \frac{1}{2}(d-1) \rfloor = d - 1$ apart (centered around a codeword u) in which $f(x) = u = f(y)$.

Then, the minimum certificate that can exist between x and y is a set S of size $n - (d - 1) = n - d + 1$. Since d is the minimum distance for $\mathscr{C}$, we can bound the minimum certificate size for any received codeword r , $C_r(f) \leq n - d + 1$. Thus, the maximum certificate size $C_x(f)$ for all $x \in \{0, 1\}^n$, i.e. the total certificate complexity of $\mathscr{C}$ is $n - d + 1$.

$\square$