On the query complexity of easy to certify total functions

Artem Kaznatcheev

April 19, 2011

Consider a non-constant total function $f : \{0, 1\} \to \{0, 1\}$. Let b be the output that corresponds to the part of the function that is harder to certify. In other words, we will call the bigger certificate $C(f) = C_b(f) = u$ and the smaller $C_{\bar{b}}(f) = v$. Thus, we have that $u \geq v \geq 1$ (the last inequality follows from the fact that f is non-constant). Now consider an input x such that $f(x) = b$ and $C(f) = C_x(f)$ and let S be a minimal certificate of size $|S| = u$. Define S^x as the set of all strings x' such that x' and x agree on all bits in S. More formally:

$$S^x = \{x' \mid \forall i \in S \; x'_i = x_i\} \tag{1}$$

Since S is a certificate, we know that $f(S^x) = b$, where we overloaded notation in the obvious way to serve as shorthand for $\forall x' \in S^x \; f(x') = b$. Further, since f is total, we know that $|S^x| = 2^{n-u}$.

Let $x(i)$ be x with the i-th bit flipped. Consider an arbitrary $i \in S$. If for all $x' \in S^{x(i)}$ we have $f(x) = b$ then i is non-necessary for S to be a certificate, and we can remove it, contradicting the fact that we picked a minimal certificate. Thus:

$$\forall i \in S, \; \exists y \in S^{x(i)} \text{ s.t. } f(y) = \bar{b}. \tag{2}$$

Let $Y_i = S^{x(i)} \cap f^{-1}(\bar{b})$, we just showed that for every $i \in S$, this set is non-empty.

Over all the $y \in Y_i$ consider the one with the smallest minimal certificate. In other words, for every Y_i pick a y such that for all $y' \in Y_i$ $C_y(f) \leq C_{y'}$. From the definition of certificate complexity, we thus know that $C_y(f) \leq C_{\bar{b}}(f) = v$. Let S_y be a minimal certificate for y.

Imagine that $S \cap S_y = \emptyset$ then there exists a $z \in S^x \cup S^y_y$. However, such a z is paradoxical since it is b-certified by S and $\bar{b}$-certified by S_y. Thus, $|S \cap S_y| \geq 1$, in fact, they must overlap on a bit on which x and y differ. In other words, we must have $i \in S_y$.

Now, consider the set $(S \cup S_y)^y$. We will show that this is a subset of Y_i. Since any $y' \in (S \cup S_y)^y$ agrees with y on S_y, we have a $\bar{b}$-certificate for y'. In other words, $f((S \cup S_y)^y) = \bar{b}$. Further, since $\forall j \in S \; y_j = x(i)_j$, we have that $(S \cup S_y)^y) \subseteq S^{x(i)}$. Putting the two together, we prove the claim $(S \cup S_y)^y \subseteq Y_i$.

Now we can do a simple calculation to lower bound the size of Y_i:

$$|Y_i| \geq |(S \cup S_y)^y| = 2^{n-|S \cup S_y|} \geq \frac{2^{n-u}}{2^{v-1}} \tag{3}$$

Further, notice that for each $y \in Y_i$ there exists an $x' \in S^x$ such that $y = x'(i)$ (i.e. they differ only on the i-th bit). Consider a bipartite graph with the left partition being S^x and the right partition being the union of the Y_i. Add an edge between $x'' \in S^x$ and $y'' \in \sum_{i \in S} Y_i$ if x'' and y'' differ by one bit. We already observed that for each y'' there is an edge to S^x, thus the total number of edges to S^x is greater than:

$$C_b(f) 2^{n - C_b(f) - C_{\bar{b}}(f) + 1} \tag{4}$$

From this, we can conclude that the average degree of a vertex is greater than $\frac{2C_b(f)}{2^{C_{\bar{b}}(f)}}$.

In particular there is some vertex x^* such that the size of its neighbourhood (which is equal to its degree) $|N(x^*)| \geq \frac{2C_b(f)}{2^{C_{\bar{b}}(f)}}$. Further for each $y'' \in N(x^*)$ we have $f(x^*) \neq f(y'')$ and each y'' differs from x^* by exactly one bit. In other words, we have shown that the sensitivity $s(f) \geq s_{x^*}(f) \geq \frac{2C_b(f)}{2^{C_{\bar{b}}(f)}}$. Consider the other bits of the certificate for x^* not all of them are used as flips to make some $y'' \in N(x^*)$. Some subset of these unused bits (plus potentially some bits outside S, but we haven't used any of those yet) must form another sensitivity block. Thus, we have:

$$bs(f) \geq \frac{2C_b(f)}{2^{C_{\bar{b}}(f)}} + 1 \tag{5}$$

Using either Ambainis' method or the polynomial method, it is not hard to show that $Q_2(f) = \Omega(\sqrt{bs(f)})$, thus:

$$Q_2(f) = \Omega(\sqrt{\frac{C_b(f)}{2^{C_{\bar{b}}(f)}}}) \tag{6}$$

For constant $C_{\bar{b}}$ it gives us what we desire: $D(f) = O(Q^2(f))$ for total functions f with one of its certificates of constant size.