# Information complexity of AND

Yuval Filmus

June 27, 2017

Let $\pi$ be a protocol for the AND function which is correct with probability at least $1-\epsilon$ on each input. The goal of this section is to lower bound the information complexity of $\pi$ with respect to the distribution $\mu$ given by $\mu(0,0) = \mu(0,1) = \mu(1,0) = 1/3$.

For a transcript $t$, let $p(t|xy)$ be the probability that the transcript of $\pi$ is $t$ if the inputs are $x, y$. We will also use the similar notations $p(t|X = x)$ and $p(t|Y = y)$.

Our starting point is an application of Pinsker's lemma, which states that $D(Q\|R) \geq \frac{1}{2}\|Q - R\|^2$, where $\|Q - R\|$ denotes total variation distance.

**Lemma 1.** *Suppose that*

$$\sum_t |p(t|00) - p(t|01)| + |p(t|00) - p(t|10)| \geq \delta.$$

*Then* $\mathsf{IC}_\mu(\pi) = \Omega(\delta^2)$.

*Proof.* Suppose without loss of generality that $\sum_t |p(t|00) - p(t|01)| \geq \delta/2$. Expressing $I(Y; \Pi|X)$ using Kullback–Leibler divergence, we get

$$I(Y; \Pi|X) \geq \frac{2}{3} I(Y; \Pi|X = 0) = \frac{2}{3} D(Q\|R),$$

where $Q, R$ are distributions on pairs $(y, t)$ given by

$$Q(y,t) = \Pr[Y = y, \Pi = t|X = 0] = \Pr[Y = y|X = 0]p(t|0y) = \frac{p(t|0y)}{2},$$
$$R(y,t) = \Pr[Y = y|X = 0]p(t|X = 0) = \frac{p(t|00) + p(t|01)}{4}.$$

Pinsker's inequality implies that

$$I(Y; \Pi|X) \geq \frac{1}{3}\|Q - R\|^2 \geq \frac{1}{3}\left(\sum_t |Q(0,t) - R(0,t)|\right)^2 =$$
$$\frac{1}{48}\left(\sum_t |p(t|00) - p(t|01)|\right)^2 \geq \frac{\delta^2}{192}. \quad \square$$

We can lower-bound the quantity in Lemma 1 using the cut-and-paste property $p(t|00)p(t|11) = p(t|01)p(t|10)$, which follows from the rectangular property of protocols.

**Lemma 2.** *It holds that*

$$\sum_t |p(t|00) - p(t|01)| + |p(t|00) - p(t|10)| = \Omega((1/2 - \epsilon)^2).$$

*Proof.* Denote by $T_0$ the set of transcripts that cause $\pi$ to output 0. Since $\pi$ is correct with probability at least $1 - \epsilon$ on input $(0, 0)$, we have

$$\sum_{t \in T_0} p(t|00) \geq 1 - \epsilon. \tag{1}$$

Let $\delta$ be a constant to be determined. Let $B$ denote the set of transcripts in $T_0$ which satisfy

$$|p(t|00) - p(t|01)| + |p(t|00) - p(t|10)| \leq \delta p(t|00).$$

If $t \in B$ then

$$p(t|00)p(t|11) = p(t|01)p(t|10) \geq (1 - \delta)^2 p(t|00)^2,$$

and so $p(t|11) \geq (1 - 2\delta)p(t|00)$. Since $t \in T_0$ and $\pi$ is correct with probability at least $1 - \epsilon$ on input $(1, 1)$, we must have

$$\epsilon \geq \sum_{t \in T_0} p(t|11) \geq (1 - 2\delta) \sum_{t \in B} p(t|00) \geq \sum_{t \in B} p(t|00) - 2\delta. \tag{2}$$

Equations (1) and (2) together imply that

$$\sum_{t \in T_0 \setminus B} p(t|00) \geq 1 - 2\epsilon - 2\delta,$$

and so

$$\sum_{t \in T_0 \setminus B} |p(t|00) - p(t|01)| + |p(t|00) - p(t|10)| \geq (1 - 2\epsilon - 2\delta)\delta.$$

Choosing $\delta = (1/2 - \epsilon)/2$ completes the proof (with a hidden constant of 1/2). □

Combining both parts, we get the desired lower bound.

**Theorem 1.** *Let $\pi$ be a randomized communication protocol for AND, which is correct with probability at least $1 - \epsilon$ on every input. Let $\mu$ be the inputs distribution $\mu(0, 0) = \mu(0, 1) = \mu(1, 0) = 1/3$. Then*

$$\mathsf{IC}_\mu(\pi) = \Omega((1/2 - \epsilon)^4).$$