6.4. Discrepancy Lower Bound

6.4.a. The Discrepancy of GIP

In this subsection we prove a lower bound for GIP by using the discrepancy method. Specifically, we show that $Disc_{\text{unif}}(GIP^n_k) \leq e^{\exp(-n/4^4)}$.

We first introduce a slightly modified notation to facilitate easier algebraic handling. Define a function $f$ as follows: $f(x_1, \ldots, x_k) = 1$ if $GIP_n^k(x_1, \ldots, x_k) = 0$ and $-1$ if $GIP_n^k(x_1, \ldots, x_k) = 1$. In this case, instead of working directly with the discrepancy we will use:

$$\Delta_k(n) = \max_{\phi_1 \ldots, \phi_k} \left| E_{x_1, x_2, \ldots, x_k} f(x_1, \ldots, x_k) \cdot \phi_1(x_1, \ldots, x_k) \cdots \phi_k(x_1, \ldots, x_k) \right|,$$

where the maximum is taken over all functions $\phi : \{0, 1\}^k \to \{0, 1\}$ such that $\phi_i$ does not depend on $x_i$, and the expectation is over all $2^k$ possible choices of $x_1, \ldots, x_k$.

First, it should be clear that $Disc_{\text{unif}}(GIP_n^k) = \Delta_k(n)$. This is because the product $\phi_1(x_1, \ldots, x_k) \cdots \phi_k(x_1, \ldots, x_k)$ gives 1 on a collection of points that forms a cylinder intersection, and, conversely, any cylinder intersection can be written as such a product. In addition, because we changed to the $[-1, 1]$ notation, the expectation plays the same role as the difference in probabilities previously did.

We define constants $\beta_i$ recursively: $\beta_0 = 0$, and $\beta_i = \sqrt{\frac{1 + \beta_{i-1}}{2}}$. It follows by induction that $\beta_i \leq 1 - 4i^{-k} < e^{-i^{-k}}$. We will prove the following upper bound on $\Delta_k(n)$.

**Lemma 6.17:** $\Delta_k(n) \leq (\beta_i)^n$, for all $k \geq 1$, $n \geq 0$.

**Proof:** Observe that $\Delta_1(n) = 0$, because in this case $\phi_i$ must be constant and $E_{x_1} f(x_1) = 0$ (in the case that $n = 0$, we get $\Delta_1(0) = 1$. To overcome this, we define $\phi_0 = 1$ for this proof). We proceed by induction on $k$. Let $k \geq 2$, and fix $\phi_1, \ldots, \phi_k$ that achieve the value of $\Delta_k(n)$. Because $\phi_i$ does not depend on $x_i$, and is bounded in absolute value by 1,

$$\Delta_k(n) \leq E_{x_1, x_2, \ldots, x_k} \left[ |E_{x_1, x_2, \ldots, x_k} f(x_1, \ldots, x_k) \cdot \phi_1(x_1, \ldots, x_k) \cdots \phi_k(x_1, \ldots, x_k) | \right].$$

In order to estimate the right-hand side, we will use a special case of the Cauchy–Schwarz inequality stating that for any random variable $z$: $(E|z|^2)^{1/2} \leq E|z|$. Thus our estimate is:

$$\Delta_k(n) \leq \left( E_{x_1, x_2, \ldots, x_k} \left[ |E_{x_1, x_2, \ldots, x_k} f(x_1, \ldots, x_k) \cdot \phi_1(x_1, \ldots, x_k) \cdots \phi_k(x_1, \ldots, x_k) | \right] \right)^{1/2} = \left( E_{x_1, x_2, \ldots, x_k} \left[ f(x_1, \ldots, x_k, u) \cdot f(x_1, \ldots, x_k, v) \right] \right)^{1/2} \cdot \left( \phi_1^u \cdot \phi_1^v \cdots \phi_k^u \cdot \phi_k^v \right)^{1/2},$$

where $\phi_i^u$ stands for $\phi_i(x_1, \ldots, x_{k-1}, u)$, and $\phi_i^v$ for $\phi_i(x_1, \ldots, x_{k-1}, v)$.

Now observe that for every particular choice of $u$ and $v$, we can express the product $f(x_1, \ldots, x_{k-1}, u) f(x_1, \ldots, x_{k-1}, v)$ in terms of the function $f$ on $k - 1$ strings of possibly shorter length. Inspection reveals that the value of $f(x_1, \ldots, x_{k-1}, u) f(x_1, \ldots, x_{k-1}, v)$ is simply $f(z_1, \ldots, z_{k-1})$, where $z_i$ is the restriction of $x_i$ to the coordinates $j$ such that $u_j \neq v_j$ (here is where the particular properties of $f$ are used). We will now view each $x_i$ as composed of two parts: $z_i$ and $y_i$, where $z_i$ is the part of $x_i$ where $u_j \neq v_j$, $y_i$ the part of $x_i$ where $u_j = v_j$ (this is done separately for every $u, v$).
MULTIPLAYER COMMUNICATION COMPLEXITY

For every particular choice of $u, v$ and consequently $y_1, \ldots, y_{k-1}$, we define functions of the "$z$-parts":

\[ s^{u,v,y_1,\ldots,y_{k-1}}(z_1, \ldots, z_{k-1}) = \phi_t(x_1, \ldots, x_{k-1}, u) \cdot \phi_t(x_1, \ldots, x_{k-1}, v), \]

where the $x_i$s are obtained by the concatenation of the corresponding $y_i$ and $z_i$. We can now rewrite the previous estimate as

\[ \Delta_t(n) \leq \left( E_{x_1,\ldots,x_{k-1}}[S^{u,v,y_1,\ldots,y_{k-1}}] \right)^{1/2}, \]

where $S^{u,v,y_1,\ldots,y_{k-1}}$ is defined as

\[ E_{z_1,\ldots,z_{k-1}}[f(z_1, \ldots, z_{k-1}) \cdot s^{u,v,y_1,\ldots,y_{k-1}}(z_1, \ldots, z_{k-1}) \cdot \ldots \cdot s^{u,v,y_1,\ldots,y_{k-1}}(z_1, \ldots, z_{k-1})]. \]

Now $S^{u,v,y_1,\ldots,y_{k-1}}$ can be estimated via the induction hypothesis, because $f$ and the $\xi_i$s are all functions of $k-1$ strings. Moreover, note that $s^{u,v,y_1,\ldots,y_{k-1}}$ does not depend on $z_i$. Thus the previous estimate of $\Delta_t(n)$ is bounded by

\[ \Delta_t(n) \leq \left( E_{x_1,\ldots,x_{k-1}}[\Delta_{k-1}(m_{u,v})] \right)^{1/2} \leq \left( E_{x_1,\ldots,x_{k-1}}[\beta_{k-1}] \right)^{1/2}, \]

where $m_{u,v}$ is the length of the strings $z_j$, which is equal to the number of locations $j$ such that $u_j \neq v_j$.

Because $u$ and $v$ are distributed uniformly in $\{0, 1\}^n$, $m_{u,v}$ is distributed according to the binomial distribution. For any constant $m$, the probability that $m_{u,v} = m$ is exactly $\binom{n}{m} 2^{-n}$. Thus the previous estimate gives:

\[ \Delta_t(n) \leq \left[ \sum_{m=0}^{n} \frac{n}{m} \right]^{1/2} 2^{-n} \beta_{k-1} = 2^{-n} (1 + \beta_{k-1})^{1/2} = \beta_k, \]

which completes the proof of the lemma.

To conclude, this shows that $\text{Disc}^\text{uniform}(GIP^k) \leq 1/e^{3^{-n}}$, which implies that the deterministic (and even randomized) communication complexity of $GIP^k$ is $\Omega(n/4^k)$. In fact, by Exercise 6.15, we also get a bound for $D^\text{uniform}_{1/2-\epsilon}(f)$ and $R_{1/2-\epsilon}(f)$ of $\Omega(\log \epsilon + n/4^k)$.

6.5. Simultaneous Protocols

The protocols presented in Examples 6.3 and 6.4 are of a very restricted form: the communication sent by each party does not depend at all on the previous communication sent by other parties. We can imagine all parties speaking "simultaneously" and each writing, on a common blackboard, a function of the $k-1$ parts of the input it can see. After all parties have spoken, the answer should be determined by what is written on the blackboard. We call such protocols simultaneous.

Definition 6.18: The simultaneous communication complexity of $f$, $D^\text{sim}(f)$, is the cost of the best simultaneous protocol that computes $f$. 