Comments on the Inclusion-Exclusion Principle
(related to the top paragraph on the second page of Assignment 2)
by Hao Xia[1]
October 14, 2006

Inclusion-exclusion principle

For any finite set of events $\{E_1, E_2, \ldots, E_n\}$, we have

$$\begin{aligned}
\Pr\left[\bigcup_{i=1}^{n} E_i\right] &= \sum_{i=1}^{n} \Pr[E_i] + \sum_{k=2}^{n} (-1)^{k+1} \sum_{i_1 < \ldots < i_k} \Pr\left[\bigcap_{j=1}^{k} E_{i_j}\right] \\
&= \sum_{i=1}^{n} \Pr[E_i] - \sum_{i,j:i<j} \Pr[E_i \cap E_j] + \sum_{i,j,k:i<j<k} \Pr[E_i \cap E_j \cap E_k] - \\
&\quad - \ldots + (-1)^{n+1} \Pr[E_1 \cap E_2 \cap \ldots \cap E_n]
\end{aligned}$$

Here is a sketch of the proof. To show that the LHS equals the RHS, we show that the RHS counts each element of $\bigcup A_i$ exactly once. Suppose an element a is in k many A_i's. This means, that the first term of the RHS counts it k many times. Write this as $\binom{k}{1}$. The second term counts it $\binom{k}{2}$ many times. The third, $\binom{k}{3}$, etc., and the k-th term counts it $\binom{k}{k}$ many times. Put it all together, the LHS equals

$$\sum_{i=1}^{k} (-1)^{i+1} \binom{k}{i} = (1 + (-1))^k + 1 = 1.$$

Further, note that in the I-E principle, if we take the first k many terms, where k is odd, we get an upper bounds, and if k is even, we get a lower bound. In particular, this observation gives us the so called **Boole's Inequality**: $|\bigcup A_i| \leq \sum |A_i|$.

Upper bound for Pr[circuit is wrong]

For a circuit of size s, use E_i, $i = 1, 2, \ldots, s$, to denote the event that gate i is wrong, with probability $\Pr[E_i] \leq \frac{\epsilon}{s}$ for some constant $\epsilon \in (0, 1)$. We know that if the whole circuit is going wrong, there must be some gate being wrong, but we can not make the same claim in the opposite direction. Thus we know

$$\Pr[\text{circuit is wrong}] \leq \Pr\left[\bigcup_{i=1}^{s} E_i\right]$$

[1] With a proof of the I-E Principle and related comments by M. Soltys

Elegant way

By directly applying Boole's inequality, we have

$$\begin{aligned}\Pr[\text{circuit is wrong}] &\leq \Pr\left[\bigcup_{i=1}^{s} E_i\right] \\ &\leq s \cdot \max_i\{\Pr[E_i]\} \\ &\leq s \cdot \frac{\epsilon}{s} = \epsilon\end{aligned}$$

□

Brute force way when E_is are independent

The independence of each E_i gives us the ability to write the probability of all gates working properly as a product of individual probability. Thus we have

$$\begin{aligned}\Pr\left[\bigcup_{i=1}^{s} E_i\right] &= 1 - \prod_{i=1}^{s}(1 - \Pr[E_i]) \\ &\leq 1 - \left(1 - \frac{\epsilon}{s}\right)^s\end{aligned}$$

Now we focus on $(1 - \frac{\epsilon}{s})^s$. Consider its Taylor expansion about $\epsilon = 0$, we have

$$\left(1 - \frac{\epsilon}{s}\right)^s = 1 - \epsilon + R_2$$

where R_2 is the remainder. By using the Lagrange remainder for R_2, we know that

$$\begin{aligned}\exists \xi \in (0, \epsilon) \qquad R_2 &= \frac{\epsilon^2}{2} \cdot f^{(2)}(\xi) \\ &= \frac{\epsilon^2}{2} \cdot \frac{s-1}{s}\left(1 - \frac{\xi}{s}\right)^{s-2} \geq 0\end{aligned}$$

Hence we get

$$\left(1 - \frac{\epsilon}{s}\right)^s \geq 1 - \epsilon$$

Use the above inequality for our bound for $\Pr[\bigcup_{i=1}^{s} E_i]$, and we finally have

$$\begin{aligned}\Pr[\text{circuit is wrong}] &\leq \Pr\left[\bigcup_{i=1}^{s} E_i\right] \\ &\leq 1 - (1 - \epsilon) = \epsilon\end{aligned}$$

□