Learning Parity

Zhiwei Zhang

February 1, 2019

1 Problem Brief

Given an unknown parity function

$$f : \{0, 1\}^n \to 0, 1,$$

we want to find a function g that behaves closely to f.

1.1 Application

Modeling for finding "revelant" subsets.

2 Information Theory Perspective

Given the input bitstring is "$x = x_1 x_2 \cdots x_n$", and the parity function is

$$f(x) = x_{i_1} + x_{i_2} + \cdots + x_{i_k} \pmod 2.$$

(Short notice that we actually substitute "k" for "n" in the original problem brief).

Let $B = \{x_{i_1}, x_{i_2}, \cdots, x_{i_k}\}$

Notation Definition . Here we specify a notiation:
For a input x of length n, we use

$$Parity(x(S)) = \sum_{i \in S} x_i \pmod 2.$$

Specifically, if $S = B$, then $Parity(x(S)) = Parity(x(B)) = f(x)$

We examine that for a random subset of bits T (the indices of the bits), where $|T| = |B| = k$, if we take s uniform random samples of inputs $x^{(1)}, x^{(2)}, \cdots, x^{(s)}$, what's the probability that it behaves exactly the same as the parity function.

We define event A_s for a given subset S as above: $\forall i \in \mathbb{Z} \cap [1, s]$, we have $Parity(x(S)) = f(x)$; and because of the property of binary addition, $P(A_s) = \frac{1}{2^s}$, where each input x has a probability of 1/2 of behaving the same as the parity function.

Since there are at most $\binom{n}{k}$ subsets $S! = B$, we have:

$$P(\cup_S A_S) \leq \binom{n}{k} \frac{1}{2^s}$$

If we want that probability to be less than 1/2, we will get $s > \log \binom{n}{k} \approxeq k \log n$.

Therefore we need $k \log n$ samples just to determine if the subset we try has decent probability of being the parity function. However, to determine which subset it is, we have to try $\binom{n}{k}$ times for all subsets.

Parity is especially hard to deal with, because everysubset has probability of $\frac{1}{2}$ behaving the same as the parity function on a given input since each bit can just simply flip and changes the parity from 0 to 1 or 1 to 0.

Information Theory solution is not efficient enough.

3 Gaussian Elimination

We can rewrite the parity function as $f(x) = \sum_i a_i x_i \pmod 2$ where $a_i = 1$ iff $i \in B$.

Immediately, we think of setting up equations and use Gaussian Elimination to solve!.

Indeed, it's convenient and important that $\boldsymbol{F_2}$ **is a field**, so we can find multiplicative inverses!

Therefore we just need n linearly independent samples and solve the problem using Gaussian Elimination.

This is polynomial time, much better than the Information Theory solution.