Noisy Gossiping

Li Yunpeng[1] [2]

November 20, 2002

[1]Graduate Student in Department of Computer Science Hong Kong University of Science and Technology
[2]Email:fatpeng@cs.ust.hk

Abstract

This manuscript is my personal summary and reading digest based on Andrew Yao's seminar on November 14, 2002. There are only two publications about this problem. Andy also proposed a PhD topics about Lower Bound in Noisy Gossiping problem in Nov 7. I wish I could find something interested.

Part I

Finding Parity [1]

Chapter 1

Preliminaries

1.1 Problem Description

Consider a broadcast network of $N+1$ nodes in which each binary digit transmitted by each node is received by each other node via a binary symmetric channel of crossover probability $\epsilon < 1/2$. The errors on these channels are independent over transmitters, receivers, and time. Each node has a binary state, and the problem under consideration is for one special node, called the receiver, to determine the parity of the set of node states. in particular, we want to minimize the number of binary digits that must be sent by each node to enable the receiver to determine parity within some allowable error probability P^*. We assume that whatever algorithm is used for transmitting the required information, all nodes know the algorithm and there is no contention between transmissions; thus each binary digit transmitted is received and identified by all other nodes, subject to the noise introduced by the binary symmetric channels.

The above problem was first formulated by El Gamal. We also can change the problem a little: receiver need to find the state of each other node. Note that the conventional coding theory of information theory cannot be used here because each node has only one bit of information to communicate. This situation of communicating a limited amount of information is common in network protocols and more generally in the control of distributed systems. It seems that when one node transmits a single binary message, the other N nodes could make a good decision because there are N samples of it with independent noise. However, they cannot verified their value at all for there are noise when they exchange the received messages.

1.2 A "Trivial" Solution

The straightforward approach to this problem is for each node to broadcast its own state j times for some integer j. Define X be the random variable that in the j times the error happens X times. The receiver will make an error in decoding a given node's state with a probability ϵ_j is:$Pr[X > \frac{j}{2}]$. Because each broadcast is independent and the crossover probability $\epsilon < 1/2$,by the Chernoff Bound.

$$\begin{aligned} Pr[X \geq \frac{j}{2}] &= \sum_{i=j/2}^{j} \binom{j}{i} \epsilon^i (1-\epsilon)^{j-i} \\ &\leq (4\epsilon(1-\epsilon))^{j/2} \end{aligned}$$

So ϵ_j is closely upper bounded by

$$\epsilon_j \leq \alpha^{-j}, \ \ \alpha = [4\epsilon(1-\epsilon)]^{-1/2} \tag{1.1}$$

Chapter 2

A *loglogn* Approach

2.1 Some Probability Theory

At first, let's focus on some observation about k independent events.

Definition 1 (z-transform) *Suppose there are k independent Bernoulli trials, $X_1, X_2, \cdots, X_k$ and $p_i = Pr[X_i = 1]$ for all $i = 1 \cdots k$. The z-transform is defined as*

$$f(z) = \prod_{i=1}^{k} [(1 - p_i) + p_i \cdot z]$$

Theorem 2.1.1 *Given a z-transform of k independent Bernoulli trials,$f(z)$. If we toss the k trials simultaneously, the coefficient of z^i is the probability of i events happened.*

Corollary 1 *If there are k independent Bernoulli trials $X_1, X_2, \cdots, X_k$, the probability of odd number of trials happen,i.e.$|\{X_i | X_i = 1,\ i = 1 \cdots k\ \}| =$ odd is $[f(1) + f(-1)]/2$*

Chapter 3

Some Ideas

Part II

Noisy Radio Networks[2]

Bibliography

[1] R.G.Gallager, *Finding Parity in a Simple Broadcast Network*, IEEE Transactions on Information Theory, Vol.34(1998), pp176-180

[2] Kushilevitz,E..Mansour,Y, *Computation in Noisy Radio Networks*, ACM-SIAM SODA,1998,pp 236-243

Appendix A

Probability Preliminaries

A.1 The Markov and Chebyshev Inequalities

Let X be a discrete random variable and $f(x)$ be any real-valued function. Then the expectation of $f(x)$ is given by

$$E[f(x)] = \sum_x f(x)Pr[X = x]$$

Theorem A.1.1 (Markov inequality) *Let Y be a random variable assuming only non-negative values. Then for all $t \in \Re^+$*

$$Pr[Y \geq t] \leq \frac{E[Y]}{t}$$

Equivalently

$$Pr[Y \geq kE[Y]] \leq \frac{1}{k}$$

Proof

Define a function by $f(y) = 1 \ \ if \ y \geq t$ and 0 otherwise. Then $Pr[y \geq t] = E(f(y)]$. Since $f(y) \leq \frac{y}{t}$ for all y

$$E[f(y)] \leq E[\frac{y}{t}] = \frac{E[y]}{t}$$

Q.E.D.

Theorem A.1.2 (Chebyshev's Inequality) *Let X be a random variable with expectation μ_x and standard deviation δ_x. Then for any $t \in \Re^+$*

$$Pr[|X - \mu_x \ \ \geq t \cdot \delta_x] \leq \frac{1}{t^2}$$

PROOF

Note that

$$Pr[|X - \mu_x| \geq t \cdot \delta_x] = Pr[|x - \mu_x|^2 \geq t^2 \cdot \delta_x^2$$

The random variable $Y = |X - \mu_x|^2$ has expectation ${\delta_x}^2$ and applying Markov's Inequality to Y bounds this probability from above by $1/t^2$.

A.2 Chernoff's Bound

For a random variable X, the quantity $E[e^{tX}]$ is called the *moment generating function* of X. This is because $E[e^{tX}]$ can be written as a power-series with terms of the form $t^k E[X^k]/k!$, and $E[X^k]$ is the kth *moment* of X for any positive integer k. The basic idea behind the Chernoff bound technique is to take the moment generating function of X and apply the Markov inequality to it. the sum of independent random variables appears in the exponent, and this turns into the product of random variables whose expectation we then bound.

Theorem A.2.1 (Chernoff's Bound) *Let $X_1, X_2, \cdots, X_n$ be independent Poisson trials such that, for $1 \leq i \leq n$ $Pr[X - i = 1] = p_i$ where $0 \leq p_i \leq 1$. Then for $X = \sum_{i=1}^m X_i$, $\mu = E[X] = \sum_{i=1}^n p_i$ and any $\delta > 0$*

$$Pr[X > (1+\delta) \cdot \mu] < \left[\frac{e^\delta}{(1+\delta)^{(1+\delta)}}\right]^\mu$$

PROOF

For any positive real t,

$$Pr[X > (1+\delta) \cdot \mu] = Pr[e^{tx} > e^{t(1+\delta)\mu}]$$

Applying the Markov's Inequality to the right hand side

$$Pr[X > (1+\delta) \cdot \mu] < \frac{E[e^{tx}]}{e^{t(1+\delta)\mu}}$$

Notice that the inequality is strict: this stems from our assumption that the p_i are not all identically 0 or 1, so that X assumes more than one value. We bound the right-hand side by observing that

$$E[e^{tx}] = E[exp(t \cdot \sum_{i=1}^n X_i)] = E[\prod_{i=1}^n exp(t \cdot X_i)]$$

Since X_i are independent, that random variables e^{tX_i} are also independent:

$$E[\prod_{i=1}^{n} exp(t \cdot X_i)] = \prod_{i=1}^{n} E[exp(t \cdot X_i)]$$

$$Pr[X > (1+\delta) \cdot \mu] < \frac{\prod_{i=1}^{n} E[exp(t \cdot X_i)]}{exp(t(1+\delta)\mu}$$

The random variable e^{tX_i} assumes the value e^t with probability p_i and the value 1 with $1 - p_i$. Computing $E[e^{tX_i}]$

$$\begin{aligned} Pr[X > (1+\delta) \cdot \mu] &< \frac{\prod_{i=1}^{n} [p_i \cdot e^t + 1 - p_i]}{exp(t(1+\delta)\mu)} \\ &= \frac{\prod_{i=1}^{n} [1 + p_i(e^t - 1)]}{exp(t(1+\delta)\mu)} \end{aligned}$$

Now we use the inequality $1 = x < e^x$ with $x = p_i(e^t - 1)$

$$\begin{aligned} Pr[X > (1+\delta) \cdot \mu] &< \frac{\prod_{i=1}^{n} exp(p_i(e^t - 1))}{exp(t(1+\delta)\mu)} \\ &= \frac{exp(\sum_{i=1}^{n} p_i(e^t - 1))}{exp(t(1+\delta)\mu)} \\ &= \frac{exp((e^t - 1) \cdot \mu)}{exp(t(1+\delta)\mu)} \end{aligned}$$

Observe that all of the above has been proved for any positive real t, we are now free to choose a particular value for t that yields the best possible bound. For this, we differentiate the last expression with respect to t and set to zero; solving for $t = ln(1+\delta)$. substituting this for t, obtain the Chernoff's Bound. *Q.E.D*

Corollary 2 *Let $0 < p < 1/2$, $q = 1 - p$ and k be an even integer. Then*

$$\sum_{i=k/2}^{k} \binom{k}{i} p^i q^{k-i} \leq (4pq)^{k/2}$$

Theorem A.2.2 *Let $X_1, X_2, \cdots, X_n$ be independent Poisson trials such that, for $1 \leq i \leq n$ $Pr[X - i = 1] = p_i$ where $0 \leq p_i \leq 1$. Then for $X = \sum_{i=1}^{m} X_i$, $\mu = E[X] = \sum_{i=1}^{n} p_i$ and any $0 < \delta < 1$*

$$Pr[X < (1-\delta) \cdot \mu] < exp(-\mu\delta^2/2)$$

If for all $i = 1, 2, \cdots, n$ $p_i = p$ we get

$$Pr[X < (p - \lambda)n] < e^{-2\lambda^2 n}$$

.