Some Thoughts and Solutions

吴章昊

516030910593

目录

Solutions & Thoughts

Matrix multiplication test

Problem

For matrix $A, B, C \in \mathbb{F}_2^{n\times n}$, in order to verify the equation $AB = C$, we use the method below:

1. Randomly pick several vectors $r_i \in \mathbb{F}_2^n$
2. Test whether $A(Br_i) = Cr_i$
3. If $\exists i, s.t. A(Br_i) \neq Cr_i$, then $AB \neq C$. If, otherwise, what is the probability for error assertion, $P(error)$?

Thoughts

This problem is highly related to how A, B and C are generated, i.e. the probability for AB=C. Without loss of generality, we assume that $P(AB = C)/P(AB \neq C) = t > 0$

Firstly, we calculate $P(ABr = Cr|AB \neq C)$.

As $AB \neq C,\ AB - C \neq 0,\ ABr = Cr \Rightarrow r \in ker(AB - C)$.

Because $|ker(AB-C)| = n-k$, where k is the rank of $AB-C$, $k \geq 1$,

$$\begin{aligned} P(ABr = Cr|AB \neq C) &= P(r \in ker(AB - C)|AB \neq C) \\ &= \frac{|ker(AB - C)|}{|\mathbb{F}_2^n|} \\ &= \frac{2^{n-k}}{2^n} \\ &= 2^{-k} \leq \frac{1}{2} \end{aligned}$$

Therefore, $P(\cap_{i=1}^n ABr_i = Cr_i|AB \neq C) = \prod_{i=1}^n P(ABr = Cr|AB \neq C) \leq \frac{1}{2^n}$

According to Bayes' Theorem, let event $E = \cap_{i=1}^{n} ABr_i = Cr_i$

$$\begin{aligned} P(error) &= P(AB \neq C|E) \\ &= \frac{P(E|AB \neq C)P(AB \neq C)}{P(E|AB \neq C)P(AB \neq C) + P(E|AB = C)P(AB = C)} \\ &= \frac{P(E|AB \neq C)}{P(E|AB \neq C) + P(AB = C)/P(AB \neq C)} \\ &= \frac{1}{1 + \frac{t}{P(E|AB \neq C)}} \leq \frac{1}{1 + t2^n} \end{aligned}$$

In my opinion, the error bound is related to the tendency of the verification program. If AB is likely to be equal to C, the error bound($\sim O(\frac{1}{2^n})$) would decrease rapidly, as the number of test cases increases. However, if the AB is much likely to be not equal to C, the error boud might decrease much slower, and the program might be much less efficient.

P53T30 Hunter with his dogs

Problem

A hunter has two hunting dogs. One day, on the trail of some animal,the hunter comes to a place where the road diverges into two paths. He knows that each dog, independently of the other, will choose the correct path with probability p. The hunter decides to let each dog choose a path, and if they agree, take that one, and if they disagree, to randomly pick a path. Is his strategy better than just letting one of the two dogs decide on a path?

Solution

Let the two hunting dogs be d1 and d2, event A = {d1 choose the correct path}, event B = {d2 choose the correct path}, event C = {The hunter choose the same path}.

As A and B are independent, $P(A \cap B) = P(A)P(B)$. Also, $P(A \cap B^c) = P(A)P(B^c)$, $P(A^c \cap B) = P(A^c)P(B)$, $P(A^c \cap B^c) = P(A^c)P(B^c)$

The situation can be divided into 4 parts:

1. The two dogs choose the same correct path.

$$P(C|A \cap B) = 1,\ P(A \cap B) = p^2$$

2. d1 choose the correct path but d2 does not.

$$P(C|A \cap B^c) = 1/2,\ P(A \cap B^c) = p(1-p)$$

3. d2 choose the correct path but d1 does not.

$$P(C|A^c \cap B) = 1/2,\ P(A^c \cap B) = p(1-p)$$

4. The two dogs both choose the wrong path.

$$P(C|A^c \cap B^c) = 0,\ P(A^c \cap B) = (1-p)(1-p)$$

Therefore, $P(C) = P(C|A \cap B)P(A \cap B) + P(C|A \cap B^c)P(A \cap B^c) + P(C|A^c \cap B)P(A^c \cap B) + P(C|A^c \cap B^c)P(A^c \cap B^c) = p$. This strategy is the same as just letting one of the two dogs decide on a path.

P53T31 Communication through a noisy channel

Problem

A binary (0 or 1) symbol transmitted through a noisy communication channel is received incorrectly with probability ϵ_0 and ϵ_1, respectively (see Fig 1). Errors in different symbol transmissions are independent.

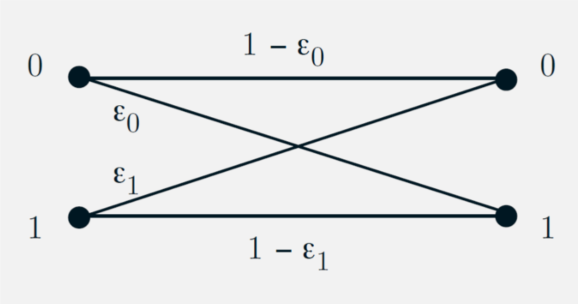

图 1: Error probabilities in a binary communication channel

(a) Suppose that the channel source transmits a 0 with probability p and transmits a 1 with probability 1−p. What is the probability that a randomly chosen symbol is received correctly?

(b) Suppose that the string of symbols 1011 is transmitted. What is the probability that all the symbols in the string are received correctly?

(c) In an effort to improve reliability, each symbol is transmitted three times and the received symbol is decoded by majority rule. In other words, a 0 (or 1) is transmitted as 000 (or 111, respectively), and it is decoded at the receiver as a 0 (or 1) if and only if the received three-symbol string contains at least two 0s (or 1s, respectively). What is the probability that a transmitted 0 is correctly decoded?

(d) For what values of ϵ_0 is there an improvement in the probability of correct decoding of a 0 when the scheme part (c) is used?

(e) Suppose that the channel source transmits a 0 with probability p and transmits a 1 with probability 1 − p, and that the scheme of part (c) is used. What is the probability that a 0 was transmitted given that the received string is 101?

Solution

Let events $T_s = \{\text{string s is transmitted}\}$, $R_s = \{\text{string s is received}\}$, $C = \{\text{The symbol is received correctly}\}$

(a) The probability $P(C)$ that a randomly chosen symbol is received correctly:

$$\begin{aligned} P(C) &= P(C|T_0)P(T_0) + P(C|T_1)P(T_1) \\ &= (1-\epsilon_0)p + (1-\epsilon_1)(1-p) \\ &= 1-\epsilon_1 + (\epsilon_1 - \epsilon_0)p \end{aligned}$$

(b) As the correctness is independent with each other, the probability is: $(1-\epsilon_1)^3(1-\epsilon_0)$

(c) The symbols received should be among $S = \{000, 001, 010, 100\}$, the probability $P(S) = (1-\epsilon_0)^3 + \binom{3}{1}(1-\epsilon_0)^2\epsilon_0 = (1-\epsilon_0)^2(1+2\epsilon_0)$

(d) The probability is improved when:

$$(1-\epsilon_0)^2(1+2\epsilon_0) > 1-\epsilon_0 \Leftrightarrow 0 < \epsilon_0 < 1/2$$

(e) $P(R_{101}|T_0) = \epsilon_0^2(1-\epsilon_0)$, $P(T_0) = p$, $P(R_{101}|T_1) = \epsilon_1(1-\epsilon_1)^2$, $P(T_1) = 1-p$. According to the Bayes Theorem, the probability would be:

$$\begin{aligned} P(T_0|R_{101}) &= \frac{P(R_{101}|T_0)P(T_0)}{P(R_{101}|T_1)P(T_1) + P(R_{101}|T_0)P(T_0)} \\ &= \frac{\epsilon_0^2(1-\epsilon_0)p}{\epsilon_1(1-\epsilon_1)^2(1-p) + \epsilon_0^2(1-\epsilon_0)p} \end{aligned}$$