풀이

STEP III 1995, 문제 13

확률과 통계 • 잡음이 있는 이진 통신로

STEP III 1995, 13번 문제

더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:

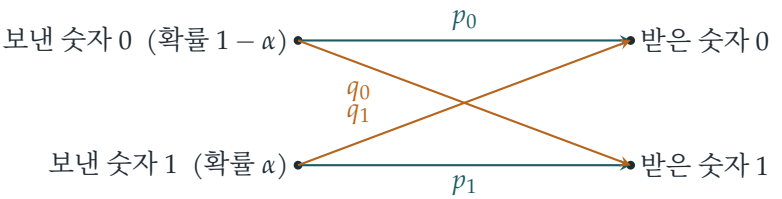
step.maths.org/questions/95-s3-q13

핵심 아이디어

모든 것은 숫자를 한 번에 하나씩 살펴보는 데서 나온다. 각 숫자는 "이진 채널(binary channel)"을 지나간다. 즉 0 또는 1로 보내진 뒤, 그대로 남거나 뒤집힌다. 숫자 하나에 무슨 일이 일어나는지 알고 나면, 메시지 전체는 그것의 서로 독립(independent)인 복사본 여러 개일 뿐이므로 확률을 곱하면 된다. 중계기(booster)에 대해서는, 숫자가 두 구간을 지난 뒤 정확히 도착하려면 **짝수** 번 뒤집히면 된다는 점을 알아차리는 것이 요령이다.

풀이

이 풀이 전체에서 메시지의 길이를 $N = 10^k$로 쓴다. 문제의 의도대로, 원래 메시지의 숫자들은 서로 독립이고(각 숫자는 확률 α로 1이다), 케이블은 각 숫자를 다른 모든 숫자와 독립적으로 처리한다고 가정한다. 숫자 하나에 대한 그림은 아래와 같다.



메시지 전체를 정확히 받을 확률

특정한 숫자 하나를 정확히 받는 사건을 C라 하자. 그 숫자는 그대로 남은 0이거나 그대로 남은 1이므로

$$\mathrm{P}(C) = (1-\alpha)p_0 + \alpha p_1.$$

N개의 숫자가 서로 독립이므로

$$\mathrm{P}(\text{메시지 전체가 정확함}) = [(1-\alpha)p_0 + \alpha p_1]^{10^k}.$$

확률 β

숫자를 1로 받는 경우는 그 숫자가 1이었고 그대로 남은 경우이거나, 0이었는데 뒤집힌 경우이다.

$$\beta = \alpha p_1 + (1-\alpha)q_0.$$

이제

$$\begin{aligned}\beta = \alpha &\iff \alpha p_1 + (1-\alpha)q_0 = \alpha \iff (1-\alpha)q_0 = \alpha(1-p_1) = \alpha q_1 \\ &\iff q_0 = \alpha(q_0+q_1) \iff \alpha = \frac{q_0}{q_0+q_1},\end{aligned}$$

이다. 마지막 단계에서는 q_0+q_1로 나누었는데, 이 값은 케이블이 완벽한 경우($q_0 = q_1 = 0$이며, 이때는 자명하게 $\beta = \alpha$이다)가 아니면 양수이다. 모든 단계는 거꾸로도 성립하므로, 이것이 요구된 "필요충분조건"이다. 말로 하면, 케이블을 지나도 1의 비율이 변하지 않을 필요충분조건은 $0 \to 1$ 흐름(즉 $(1-\alpha)q_0$)과 $1 \to 0$ 흐름(즉 αq_1)이 균형을 이루는 것이다.

모두 0인 메시지

조건이 성립하고 받은 숫자가 모두 0이라고 하자. (보낸 숫자, 받은 숫자) 쌍들은 자리마다 서로 독립이므로, 메시지 전체가 정확할 조건부 확률(conditional probability)은 숫자 하나에 대한 확률 P(보낸 숫자0 | 받은 숫자0)들의 곱이다.

> ? **생각해 보기** "0을 받았다"는 사실을 무엇을 보냈는지에 대한 명제로 어떻게 바꿀까?

베이즈 정리(Bayes' theorem)를 쓴다. 숫자를 0으로 받을 확률은 $1-\beta$이고, 조건에 따라 $\beta = \alpha$이므로 $1-\beta = 1-\alpha$이다. 따라서

$$\mathrm{P}(\text{보낸 숫자0} \mid \text{받은 숫자0}) = \frac{(1-\alpha)p_0}{1-\beta} = \frac{(1-\alpha)p_0}{1-\alpha} = p_0,$$

이고, 그러므로

$$\mathrm{P}(\text{메시지가 정확함} \mid \text{모두 0을 받음}) = p_0^{10^k}.$$

반반의 확률

$q_0 = q_1 = q$이고 $\alpha = \frac{1}{2}$이면, 각 숫자가 정확할 확률은 $\frac{1}{2}(1-q) + \frac{1}{2}(1-q) = 1-q$이다. 숫자 10^6개로 된 메시지에 대해서는

$$(1-q)^{10^6} = \tfrac{1}{2} \quad \Longrightarrow \quad 10^6 \ln(1-q) = -\ln 2.$$

이어야 한다. q가 매우 작으므로 $\ln(1-q) \approx -q$이고, 따라서

$$q \approx \frac{\ln 2}{10^6} \approx 6.93 \times 10^{-7}.$$

중계기 추가하기

q는 길이의 제곱에 비례하므로, 길이를 절반으로 줄이면 q는 $2^2 = 4$로 나누어진다. 따라서 케이블의 각 절반은 확률 $q/4$로 숫자를 뒤집으며, 이는 다른 절반과 독립이다(중계기는 받은 것을 그대로 다시 보낼 뿐이다).

> ? **생각해 보기** 숫자가 정확히 도착하는 경우는 "두 절반이 모두 정확히 전송하는" 경우뿐일까?

아니다. 두 절반에서 모두 뒤집힌 숫자는 원래대로 돌아온다. 따라서

$$\mathrm{P}(\text{숫자가 정확함}) = \left(1-\frac{q}{4}\right)^2 + \left(\frac{q}{4}\right)^2 = 1 - \frac{q}{2} + \frac{q^2}{8} \approx 1 - \frac{q}{2},$$

이며, 여기서 q^2 차수의 항은 무시하였다. (두 번 뒤집히는 경우가 바로 그런 항 가운데 하나이므로 답에는 영향을 주지 않지만, 그 이유를 짚어 볼 가치가 있다.) 이제 메시지 전체가 정확할 확률은

$$\left(1-\frac{q}{2}\right)^{10^6}.$$

이다. 같은 차수까지 $(1-\frac{q}{2})^2 \approx 1-q$이므로

$$\left(1-\frac{q}{2}\right)^{10^6} \approx (1-q)^{10^6/2} = \left[(1-q)^{10^6}\right]^{1/2} = \left(\tfrac{1}{2}\right)^{1/2} = \frac{1}{\sqrt{2}} \approx 0.707.$$

따라서 중계기는 완벽한 메시지를 받을 확률을 $\frac{1}{2}$에서 약 0.71로 높인다. 여기서 q의 수치는 전혀 필요하지 않았다는 점에 주목하자. 원래 조건 $(1-q)^{10^6} = \frac{1}{2}$이 모든 일을 해 주었다. $e^{-10^6 q} = \frac{1}{2}$에 같은 생각을 적용하면 $e^{-10^6 q/2} = 1/\sqrt{2}$를 얻는다.

검산

- 길이 4인 모든 보낸 메시지와 받은 메시지를 정확히 열거하면($p_0 = 0.9$, $p_1 = 0.8$일 때) $[(1-\alpha)p_0 + \alpha p_1]^4$도, α에 대한 조건 아래에서의 조건부 확률 $p_0^4 = 0.6561$도 그대로 재현된다.
- $(1-q)^{10^6} = \frac{1}{2}$을 정확히 풀면 $q = 6.9315 \times 10^{-7}$이며, 이는 유효숫자 다섯 자리까지 $\ln 2/10^6$과 일치한다.
- 이 q로 중계기가 있을 때의 정확한 확률 $\left[(1-\frac{q}{4})^2 + (\frac{q}{4})^2\right]^{10^6}$을 계산하면 0.707107이며, $1/\sqrt{2}$와 일치한다.

- 타당성 점검: $q_0 = q_1$이면 조건으로부터 $\alpha = \frac{1}{2}$을 얻는데, 이는 대칭성이 요구하는 바와 같다.

흔한 실수

- 각 절반의 오류 확률을 $q/2$로 잡는 것. 오류는 길이의 **제곱**에 비례하므로 $q/4$이다.
- "모두 0" 부분의 답을 $(1-\alpha)^N$이나 p_0만으로 쓰는 것. 각 숫자에 대한 조건부 확률을 구해 10^k제곱해야 한다.

STEP 너머

이것은 정보 이론(information theory)의 **이진 채널**이다. $q_0 = q_1$이면 이진 대칭 채널(binary symmetric channel)이 되는데, 이는 잡음이 있는 채널이 얼마나 많은 정보를 전달할 수 있는지에 대한 섀넌(Shannon)의 이론과, 오류 정정 부호(error-correcting codes)의 출발점이다. 오류 정정 부호는 중복을 덧붙여서, 가끔 일어나는 뒤집힘을 단지 드물게 만드는 데 그치지 않고 찾아내어 바로잡을 수 있게 한다. 중계기를 이용한 계산은 두 단계 마르코프 연쇄(Markov chain)이기도 하다. 뒤집힘 확률들은 전이 행렬(transition matrix)을 곱하는 방식으로 합성된다. Grimmett와 Welsh의 *Probability: An Introduction*(확률론 입문)은 조건부 확률과 마르코프 연쇄를 알맞은 수준에서 다룬다.

Beyond STEP 풀이: https://beyondstep.keithmcnulty.org/ko/. 풀이 글은 CC0 1.0이다. 문제 자체의 저작권은 © Cambridge University Press & Assessment에 있으며 여기에 싣지 않는다. 영어 원문을 기계 번역하였으며 아직 검토되지 않았다.