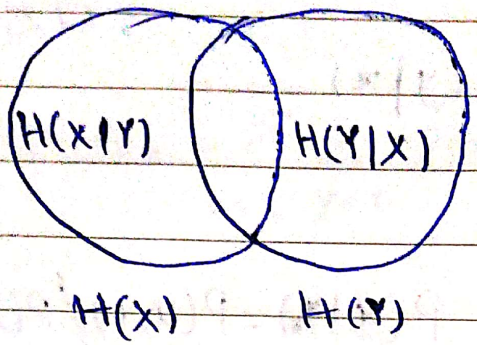
Date: ۱۴۰۰ / ۷ / ۲۷ یادداشت کلاسی Subject: امتین احسانی ۹۷۵۲۱۰۱۸

★ ویژگی‌های انتروپی شرطی



$$I(X;Y) = H(X) - H(X|Y)$$
$$I(X;Y) = H(Y) - H(Y|X)$$

$$\begin{cases} H(X,Y) = H(X) + H(Y|X) \\ \quad\quad\quad = H(Y) + H(X|Y) \end{cases}$$

مفهوم

↳ اگر Y را بدونی، چقدر دیگر از اطلاعات X باقی می‌ماند؟

★ شانون ← اصل کار ← مخابرات

↳ استفاده از تعاد ← ۱۹۴۹ ← امنیت

تحول یافت

↳ امنیت نوین

★

info. source (Sender) —info(x)→ Channel → receiver

به میزان $H(X)$ اطلاعات وارد کانال می‌شود ← $H(Y)$ به گیرنده می‌رسد

↳ به خاطر نویز کیسری

از اطلاعات ارسالی می‌رود

$$I(X;Y) = H(X) - H(X|Y)$$

↓ اطلاعات دریافت شده ← اطلاعات گم شده

↳ اطلاعات ارسال شده

اطلاعات مشترک که در مورد دریافت Y از X فراهم داشت ← اطلاعات مفید

Date: / / Subject:

$I(X;Y)$ → mutual info ★

$H(X|Y) = 0$

★ می خواهیم $I(X;Y)$ به سمت $H(X)$ میل کند

محاسبات ← اطلاعات گم نمی‌شود

key

plainText → encryption → ciphertext ★

متن اصلی ← با $H(X)$ وارد کانال می‌شود

ciphertext ← بازیابنده با $H(Y)$ می‌رسد

کلید ← مانند نویز مقداری از اطلاعات را می‌گیرد

اگر می‌خواهیم اطلاعات گم نشود ! ← تا با داشتن ciphertext

بتوانیم plain را

بدست آوریم

★ حوزه رمزنگاری ← دوست داریم $I(X;Y)$ صفر شود

↳ $H(X) = H(X|Y)$ ⟶

اگر Y را داشتیم ، X را نتوانیم پیدا کنیم

★ $H(X|Y,k)$ باید صفر باشد ← اگر Y و k را داشته باشیم

↳ صفر ← ابهام X