Föreläsning 3

MA1508

Varians

Vi antog förra gången att vi hade en följd $X_1, X_2, \ldots$ av oberoende stokastiska variabler med samma fördelning. Vi kallade variansen av dem för w. (Så vi kunde tänka oss att det är resultaten från att upprepa samma slumpmässiga försök många gånger.)

Vi defininerade

$$\hat{X}_n = \frac{1}{n}\sum_{i=1}^{n} X_i.$$

Detta är en stokastisk variabel som motsvarar medelvärdet av de första n försöken. Låt oss räkna ut variansen av den. Genom att använda de räknelagar vi har nämnt så får vi att

$$\mathrm{Var}(\hat{X}_n) = \mathrm{Var}\left(\frac{1}{n}\sum_{i=1}^{n} X_i\right) = \frac{1}{n^2}\,\mathrm{Var}\left(\sum_{i=1}^{n} X_i\right) = \frac{1}{n^2}\sum_{i=1}^{n}\mathrm{Var}(X_i) =$$

$$= \frac{1}{n^2}\sum_{i=1}^{n} w = \frac{1}{n^2}\cdot nw = \frac{w}{n}.$$

Att variansen avtar med ökande n är nästan ett fullständigt bevis av Stora talens lag.

Låt mig visa lite bilder som illustrerar hur sannolikhetsfördelningen av ett tärningskast ser ut, och sannolikhetsfördelningen för genomsnittet av 16 tärningskast. (Se Canvassidan för bilderna.)

Bilderna illustrerar att sannolikhetsfördelningen inte bara koncentreras kring medelvärdet för stora n, det illustrerar också Centrala Gränsvärdessatsen som säger att fördelningen kommer bli allt mer lik den så kallade normalfördelningen (också kallad Gaussfördelningen).

Normalfördelningen har ni sett på gymnasiet. Den dyker upp i många sammanhang, t ex spridningen av resultaten på högskoleprovet och aktiekursers förändringar. I kommunikationssammanhang antar man ofta att bruset som stör signalen man skickar är normalfördelat.

Binära, oktala och hexadecimala talsystemet

Låt oss repetera något annat. I kommunikationssammanhang jobbar man oftast med binär data, dvs data (och meddelanden osv) som kodats bara med 1:or och 0:or. Vi minns att varje heltal lika gärna kan representeras i det binära talsystemet. Om vi vill att en binär sträng ska tolkas som ett heltal kan vi skriver en nedsänkt 2:a efter den.

Exempel 1.

$$11011_2 = 16 + 8 + 2 + 1 = 27.$$

△

Att skriva stora tal binärt tar väldigt mycket plats. Som alternativ används därför också det oktala talsystemet och det hexadecimala talsystemet.

För att översätta från binära talsystemet till det oktala tittar vi på 3 siffror i taget och skriver dem som ett tal i $\{0, 1, \ldots, 7\}$.

Exempel 2. Om vi ska skriva 11011_2 oktalt kan vi skriva om som 011011_2 så att antalet siffror är delbart med 3. Vi får 2 grupper med 3 siffror och eftersom $011_2 = 3$ så blir

$$11011_2 = 33_8.$$

△

Om vi vill skriva ännu mer kompakt kan vi använda hexadecimala talsystemet (bas 16). Då grupperar vi de binära siffror i grupper om 4 och översätter till ett tal mellan 0 och 15. Fast talen $10, 11$,osv skrivs A, B, C, D, E, F.

Mod 2

Vi kommer också vilja räkna på ett annat sätt med våra binära strängar. Ni minns förhoppningsvis modulo räkningar från diskret matematik. Räknar vi modulo 2 så är $0 + 0 = 0$, $0 + 1 = 1$, $1 + 0 = 1$ och $1 + 1 = 0$. Det finns också multiplikation modulo 2 där $0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0$ och $1 \cdot 1$.

Notera att additionen fungerar precis som den operationen som kallas XOR inom logiken och teorin för digitala kretsar. Operationen med multiplikation är precis som AND.

Vi kan också räkna modulärt med strängar. T ex kan vi vilja räkna

$$01100 + 11110 = 10010.$$

Det kommer antingen framgå av sammanhanget eller så får jag säga det om vi menar modulär addition eller något annat (t ex vanlig addition av tal som råkar vara skrivna på binär form.) Man hade kunnat tänka sig att definiera en särskild additionssysmbol som stod för modulär addition, men det är ofta smidigt att hålla sig till den vanliga symbolen.

Man kan också räkna modulo andra tal än 2. T ex när man räknar modulo 3 så kan vi hålla oss till talen 0, 1 och 2. Det gäller då t ex att $1 + 1 = 2$ och $1 + 2 = 0$.

Logaritm bas 2

Låt oss passa på att repetera något annat som vi kommer behöva ibland. Minns ni begreppet *logaritm*? Mer specifikt kommer vi vara intresserade av logaritmer i bas 2.

Det gäller t ex att $\log_2(8) = 3$. Det beror på att $2^3 = 8$. Eftersom $2^5 = 32$ så blir $\log_2(32) = 5$.

Man vad blir $\log_2(9)$? Finns det ett tal, a, med egenskapen att $2^a = 9$? Ja, det finns det, men det är inte ett heltal. Vi med hjälp av miniräknare eller dator kan vi räkna ut att $\log_2(9) \approx 3.1699$.

Om vi definierar en funktion $f(x) = \log_2(x)$ så kommer den vara definierad för alla positiva x. Den blir växande (strängt växande säger vi matematiker) så att en ökning i x alltid leder till en ökning i $f(x)$. Vi kan göra $f(x)$ hur stort som helst genom att välja x tillräckligt stort, men ökningstakten är inte snabb för stora x. Den växer mycket långsammare än t ex kvadratrotsfunktionen.

Vi kommer ofta vara intresserade av logaritmen av tal mellan 0 och 1. $\log_2(0)$ är odefinierat eftersom 2^a aldrig kan bli 0. Men $\log_2(1) = 0$.

Andra exempel:$\log_2(1/2) = -1$, eftersom $2^{-1} = \frac{1}{2}$. Och $\log_2(1/32) = -5$. Det verkar som att när x är väldigt nära 0, men lite större än 0, så kommer $\log_2(x)$ vara ett ett stort negativt tal. Det stämmer, och när x närmar sig 0 så kommer $\log_2(x)$ blir hur negativt som helst.

Men den stickar inte iväg med $-\infty$ särskilt snabbt. Om vi t ex räknar $\frac{1}{32} \cdot \log_2(1/32)$ så får vi $\frac{-5}{32}$. Plottar man grafen av $x \cdot \log_2(x)$ så ser man att det verkar som att $x \cdot \log_2(x)$ går mot 0 när x går mot 0, vilket man också kan bevisa.

Just den kombinationen, $g(x) = -x \cdot \log_2(x)$, där man multiplicerar x med logaritmen av x, dyker upp i termodynamiken. Där kallas den entropin och är något sorts mått på oordningen. (Fråga mig inte om detaljer för de kan jag inte.) Mer intressant för oss är att den också kommer spela en väldigt stor roll i vår kurs, och kallas entropin även där.

Introduktion till felrättande koder

Låt oss nu komma in på ett av kursens huvudämnen, teorin för felrättande koder. Vi antar att Alice och Bob kommunicerar över en kanal som låter Alice skicka ettor eller nollor.

Tyvärr finns det en sannolikhet p för att kanalen förvandlar en etta till en nolla, eller tvärtom. Vi antar sannolikheten att en etta blir en nolla är samma som sannolikheten att en nolla blir en etta.

Vi antar också att sannolikheten att det blir fel i en bit är oberoende av vad som händer med de andra bitarna i meddelandet.

Om Alice skickar ett meddelande av längd n så är sannolikheten $(1-p)^n$ att inga bitfel inträffar vid överföringen.

Exempel 3. Om Alice skickar meddelandet 01 och $p = 0.1$ så är sannolikheten $0.9^2 = 0.81$ att meddelandet kommer fram oförändrat. Sannolikheten är $0.9 \cdot$

$0.1 = 0.09$ att Bob tar emot 11 och det är samma sannolikhet att han tar emot 00. Sannolikheten att han tar emot 10 är $0.1^2 = 0.01$. Så sannolikheten för ett fel är 18% och sannolikheten för två fel är 1%. △