Šenonova teorema o kodovanju bez prisustva šuma

Milan M.Milosavljević

Teorema o kodovanju bez šuma

- Koristeći dosadašnje rezultate, u stanju smo da odredimo fundamentalnu donju granicu očekivane vrednosti prefiksnih kodova datog informacionog izvora.

TEOREMA 2.4 *Šenonova teorema kodovanja Deo I*

Za bilo koji diskretni izvor informacija bez memorije čija je entropija H(U), očekivana dužina D-arnog prefiksnog koda E[L] tog izvora, zadovoljava

$$E\left[L\right] \geq \frac{H(U)}{\log D},$$

Teorema o kodovanju bez šuma

Control Question 32

Consider some information source U, the symbols of which are $u_1 = 1$, $u_2 = 2$, $u_3 = 3$, and $u_4 = 4$, with the following probability distribution:

u_i	1	2	3	4
$P(U = u_i)$	0.5	0.25	0.125	0.125

Consider then the following encoding of it (where z_i is the codeword for u_i):

z_1	z_2	z_3	z_4
0	10	110	111

1. What is the expected code length?
2. Is the code considered an efficient code, i.e. optimal from the expected code length point of view?

Teorema o kodovanju bez šuma

- Teorema 2.4 daje jednu donju granicu za očekivanu dužinu koda datog izvora informacija. Kakva je ta granica? Da li ima i drugih granica (npr 1)?
- Jasno je da ovaj rezultat postaje visokovrednovan samo ako pokažemo da je ta granica najbolja moguća donja granica.
- Da bi smo ovo pokazali, potrebno je konstruisati konkretan kod čija se očekivana dužina kodnih reči proizvoljno tačno približava ovoj granici.

Šenon – Fanoov prefiksni kod

- Prvo ćemo konstruisati efikasan prefiksni kod, koji iako nije optimalan u opštem slučaju se dovoljno dobro približava donjoj granici očekivane vrednosti kodnih reči.
- Ideja se svodi na izbor d užine l_i kodne reči u_i tako da važi

$$l_i = \left\lceil -\frac{\log p_i}{\log D} \right\rceil ,$$

- gde $\lceil x \rceil$ označava celobrojnu vrednost takvu da je

$$x \leq \lceil x \rceil \leq x + 1.$$

Ovakav kod se naziva Šenon-Fanoov kod, budući da ga je Šenon implicitno dao u svom radu iz 1948 godine, a Fano ga je eksplicitno konstruisao.

Šenon – Fanoov prefiksni kod

- Da li ovakav kod uvek postoji?
- Odgovor je afirmativan na osnovu Kraftove nejednakosti. Zaista po definiciji operacije ⌈ ⌉ je

$$l_i \geq -\frac{\log p_i}{\log D},$$

- pa je

$$\sum_i D^{-l_i} \leq \sum_i D^{\frac{\log p_i}{\log D}} = \sum_i D^{\log_D p_i} = \sum_i p_i = 1.$$

- Sada ćemo istražiti koliko je ovaj kod dobar u odnosu na očekivanu dužinu koda. Po definiciji važi

$$l_i < -\frac{\log p_i}{\log D} + 1.$$

Šenon – Fanoov prefiksni kod

- Ako obe strane pomnožimo sa p_i i sumiramo po i, dobijamo

$$\sum_i p_i \, l_i < \frac{-\sum_i p_i \log p_i}{\log D} + \sum_i p_i,$$

$$E[L] < \frac{H(U)}{\log D} + 1.$$

- Vidimo da je očekivana vrednost kodnih reči Šenon-Fanoov koda udaljena najviše jedan simbol od donje granice date Teoremom 2.4. To znači da je ovaj kod prilično dobar i da što je entropija izvora veća on je sve bolji. Medjutim za male entropije izvora moguće je pronaći znatno bolji kod.

Šenon – Fanoov prefiksni kod

TEOREMA 2.5 *Šenonova teorema kodovanja, Deo II*

Za bilo koji diskretni izvor informacija bez memorije, čija je entropija H(U), postoji barem jedan D-arni prefiks kod čija je očekivana dužina kodnih reči E[L] data sa

$$E[L] < \frac{H(U)}{\log D} + 1.$$

Šenon – Fanoov prefiksni kod

Primer 2.15

Razmotrimo binarni (D=2) Šenon-Fanoov kod za izvor U sa četiri simbola čije su verovatnoće p1=0.4, p2=0.3, p3=0.2 i p4=0.1.

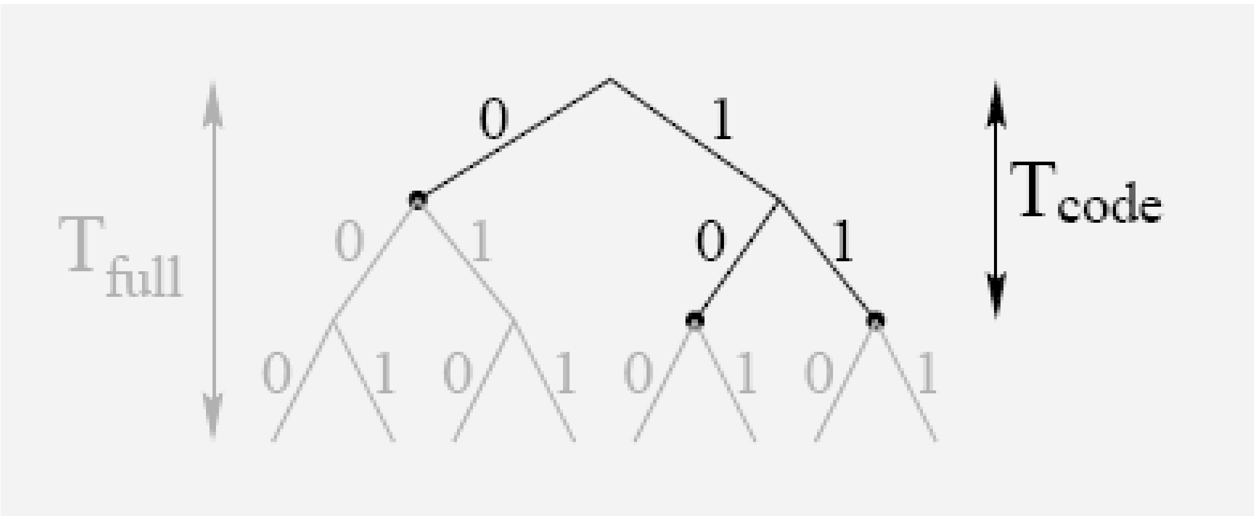
Kodne reči su date dužinama

$$l_1 = -\lceil \log_2 0.4 \rceil = 2, \qquad l_2 = -\lceil \log_2 0.3 \rceil = 2,$$
$$l_3 = -\lceil \log_2 0.2 \rceil = 3, \text{ and} \qquad l_4 = -\lceil \log_2 0.1 \rceil = 4.$$

Kod konstruišemo na osnovu postupka datog u dokazu Kraftove nejednakosti.

Kako se konstruiše kodno stablo (T_{code})

- Neka su zadate dužine kodnih reči $l_1, l_2, \ldots, l_N$
$$L = \max_i l_i + 1$$
- Konstruisati potpuno kodno stablo dubine L (T_{full})
- Za čvorove koje proglasimo kodnim rečima izvršiti potkresivanje odgovarajućeg podstabla ispod tog čvora



Kako se konstruiše kodno stablo (T_{code})

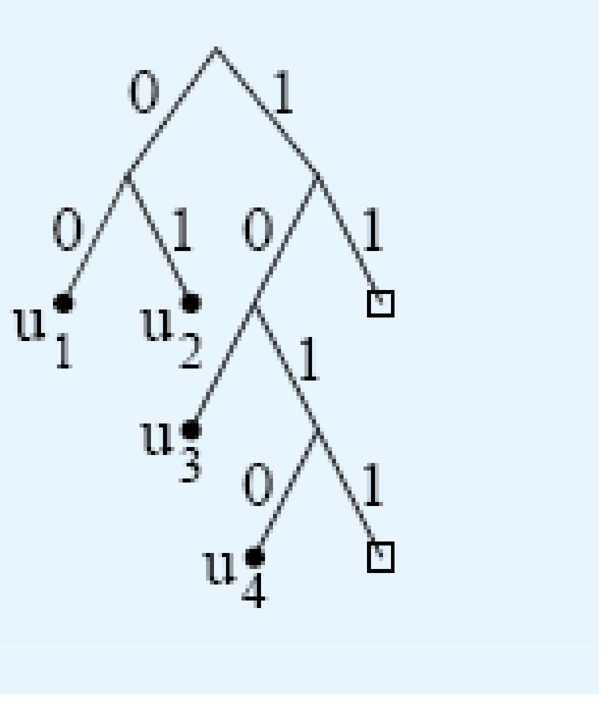
1. Startovati sa jednim čvorom (koren)
2. Za svako k iz [0,L]

   A) Pripisati kodnu reč čvoru tekuće dubine k, tako je $l_i = k$

   B) Razviti sve preostale čvorove tekuće dubine k, generišući za svaki D naslednika (dece)

Šenon – Fanoov prefiksni kod

Nastavak Primera 2.15



Na osnovu Leme o dužini puta, imamo

$$E[L] = 1 + 0.7 + 0.3 + 0.3 + 0.1 = 2.4,$$

Šenon – Fanoov prefiksni kod

Nastavak Primera 2.15

Direktan račun daje

$$H(U) = 0.4 \log 0.4 + 0.3 \log 0.3 + 0.2 \log 0.2 + 0.1 \log 0.1 \simeq 1.8 \text{ bit}.$$

Vidimo da je zadovoljena nejednakost

$$E[L] < \frac{H(U)}{\log D} + 1.$$

Odnosno 2.4 < 1.8+1=2.8.

Medjutim vidi se da ovaj kod nije optimalan. Kada bi smo upotrebili 4 kodne reči dužine 2, imali bi smo kraću očekivanu dužinu koda E[L]=2.

Šenon – Fanoov prefiksni kod

Control Question 33

Consider a source U, the entropy of which is 2.15 bit. For the following values (2.75, 2.05, 3.25, 2.15), do you think a binary binary prefix-free codes of U with such a expected code length could exist? Do you think a better code, i.e. another binary prefix-free codes of U with a shorter expected code length, can exist? (yes, no, or maybe)

expected code length	could exist?	does a better code exist?		
		no	maybe	yes, for sure
2.75				
2.05				
3.25				
2.15				

Hafmanov kod

- Hafmanov algoritam kodovanja izvora informacija bez memorije, pomoću D-arnog prefiksnog koda, daje optimalan kod minimalne moguće očekivane vrednosti kodnih reči.
- Neka izvor U ima n simbola $u_1,u_2,...,u_n$, sa odgovarajućim verovatnoćama $p_1,p_2,....,p_n$.

HAFMANOV KOD

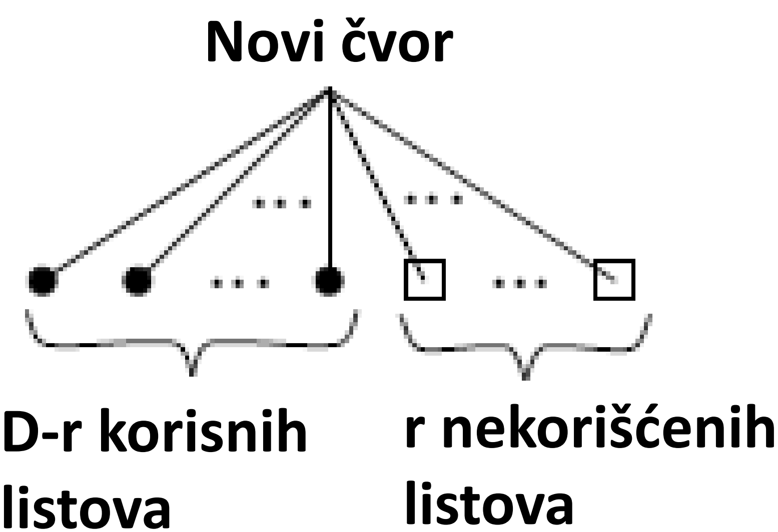
1. Startujemo sa svih n čvorova, koji će na kraju kodovanja biti listovi.

   Izračunajmo ostatak r pri delenju 1-n sa D-1. (Primetimo da za n parno, r će uvek biti nula)

   Učinimo svih n čvorova "aktivnim".

Hafmanov kod

2. Formirajmo novi čvor, čija su deca-čvorovi D-r najmanje verovatnih aktivnih čvorova i r neiskorišćenih čvorova (listova)



Označiti D-r aktivnih čvorova kao “ne aktivne”

Novo kreirani čvor označiti kao “aktivan”

Hafmanov kod

Dodeliti novokreiranom čvoru verovatnoću jednaku sumi upravo deaktiviranih D-r čvorova.

3. Ako postoji samo jedan aktivan čvor tada se procedura okončava. Taj čvor je ujedno i koren konačnog kodnog stabla. U suprotnom, postaviti r=0 i ići na korak 2.

- Prefiksni kod koji rezultuje u opisanoj proceduri se naziva Hafmanov kod, budući da je upravo opisani algoritam prvi dao Hafman 50-tih goduna XX veka.

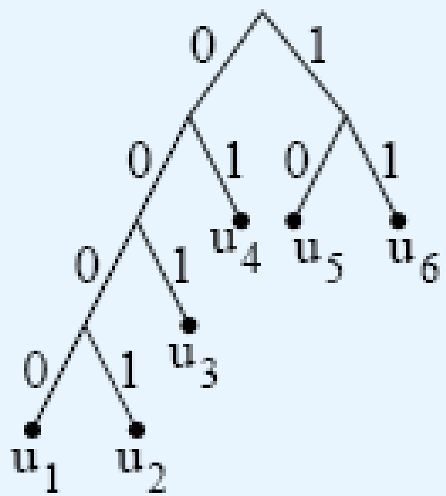
Hafmanov kod

Primer 2.16 *Binarni Hafmanov kod*

Neka je dat izvor U

U	u_1	u_2	u_3	u_4	u_5	u_6
p_i	0.05	0.1	0.15	0.27	0.20	0.23

Jedan Hafmanov kod za izvor U je dat sa



z_1	z_2	z_3	z_4	z_5	z_6
0000	0001	001	01	10	11

Hafmanov kod

Nastavak Primera 2.16

Verovatnoće unutrašnjih čvorova su date u tabeli

$v_1 = u_1 \oplus u_2$	$v_2 = v_1 \oplus u_3$	$v_3 = u_5 \oplus u_6$	$v_4 = v_2 \oplus u_4$	$v_5 = v_4 \oplus v_3$
0.15	0.30	0.43	0.57	1

Primetimo da je

$$E[L] = 2\ (0.2 + 0.23 + 0.27) + 3\ (0.15) + 4\ (0.1 + 0.05)\ = 2.45$$

Ili pomoću Leme dužine puta

$$E[L] = 1 + 0.57 + 0.43 + 0.30 + 0.15 = 2.45$$

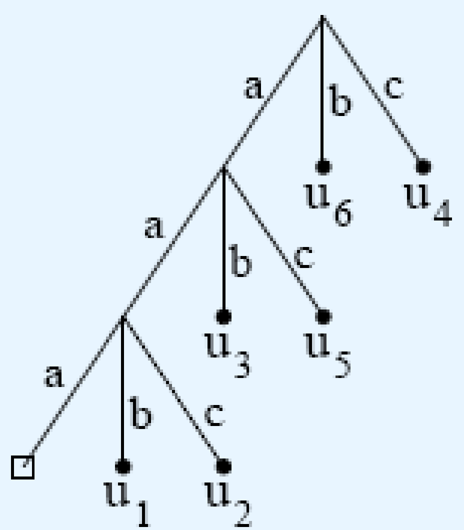
Dok je entropija izvora U

$$H(U) = -\sum_{i=1}^{6} p_i \log p_i = 2.42 \text{ bit.}$$

Hafmanov kod

Primer 2.17 *Ternarni Hafmanov kod*

Neka je izvor informacija U, kao u prethodnom primeru 2.16. Ako upotrebimo ternarni kod D=3, ostatak od 1-n=1-6=-5 pri deljenju sa D-1=3-1=2 iznosi r=1. (Provera -5=-3·2+1). Stoga treba uvesti jedan neiskorišćeni list. Hafmanov kod u ovom slučaju je dat sa



z_1	z_2	z_3	z_4	z_5	z_6
aab	aac	ab	c	ac	b

$v_1 = u_1 \oplus u_2$	$v_2 = v_1 \oplus u_3 \oplus u_5$	$v_3 = v_2 \oplus u_6 \oplus u_4$
0.15	0.50	1

$$E\,[L] = 1 + 0.5 + 0.15 = 1.65$$

$$\frac{H(U)}{\log 3} = \frac{2.42}{1.59} = 1.52.$$

Control Question 34

Consider the unfair dice with the following probability distribution:

1	2	3	4	5	6
0.17	0.12	0.10	0.27	0.18	0.16

The purpose of this question is to build one binary Huffman code for this dice. For this code, we will use the convention to always give the label `0` to the least probable branch and the label `1` to the most probable branch. Furthermore, new nodes introduced will be named 7, 8, etc..., in that order.

1. What are the first two nodes to be regrouped? What is the corresponding probability?
2. What are then the next two nodes that are regrouped? What is the corresponding probability?
3. Keep on giving the names of the two nodes to be regrouped and the corresponding probability.
4. Give the Huffman code found for this source:

$u_i =$	1	2	3	4	5	6
$z_i =$						

Optimalnost Hafmanovog koda

- Sada nam je cilj da pokažemo da je Hafmanov kod optimalan, a to znači da ne postoji neki drugi prefiksni kod čija je očekivana dužina kodnih reči manja od očekivane dužine kodnih reči Hafmanovog koda.
- Važno je uočiti da postoji jako puno optimalnih kodova. Svaka permutacija kodnih simbola jednog optimalnog koda, takodje daje optimalni kod. Svaka zamena kodnih reči koje odgovaraju jednakoverovatnim simbolima datog izvora, takodje je optimalan kod. Hafmanov algoritam konstruiše samo jedan od njih.
- Prvo ćemo navesti svojstva optimalnih kodova.

Optimalnost Hafmanovog koda

Za jedan kod ćemo reći da je optimalan ukoliko je $\sum_{i=1}^{n} p_i l_i$ minimalna moguća na skupu svih prefiksnih kodova datog izvora informacija, gde je sa l_i označena dužina kodne reči simbola u_i koji se emituje sa verovatnoćom p_i.

Lema 2.2

Za svaki optimalni kod izvora sa n mogućih simbola, važi

$$p_i > p_j \Longrightarrow l_i \leq l_j, \qquad \mathrm{i, j} = 1,2, \dots \mathrm{n}.$$

Lema 2.3

Broj listova u D-arnom stablu je 1+k (D-1), gde je k broj unutrašnjih čvorova, uključujući koren.

Optimalnost Hafmanovog koda

Lema 2.4

Za dati izvor informacija U, u kodnom stablu koje odgovara optimalnom D-arnom prefiksnom kodu za U, postoji najviše D-2 neiskorišćenih listova i svi se oni nalaze na maksimalnoj dubini kodnog stabla.

Šta više, postoji optimalni D-arni kod za U, u kome su svi neiskorišćeni listovi, deca jednog istog roditeljskog čvora.

Lema 2.5

Broj neiskorišćenih listova u kodnom stablu koje odgovara optimalnom D-arnom prefiksnom kodu izvora U sa n simbola je jednak pozitivnom ostatku deljenja n-1 sa D-1.

Optimalnost Hafmanovog koda

Lema 2.6

Postoji optimalni D-arni prefiksni kod izvora U sa n simbola ($n \geq 2$) takav da se D-r najmanje verovatnih kodnih reči razlikuje samo po poslednjem simbolu, gde je r ostatak delenja 1-n sa D-1 (stoga je D-r≥ 2).

Teorema 2.6

Hafmanovo kodovanje je optimalno, što znači da ako je Z jedan Hafmanov kod informacionog izvora U, a X drugi jednoznačni kod istog izvora, tada je $E[L_X] \geq E[L_Z]$.