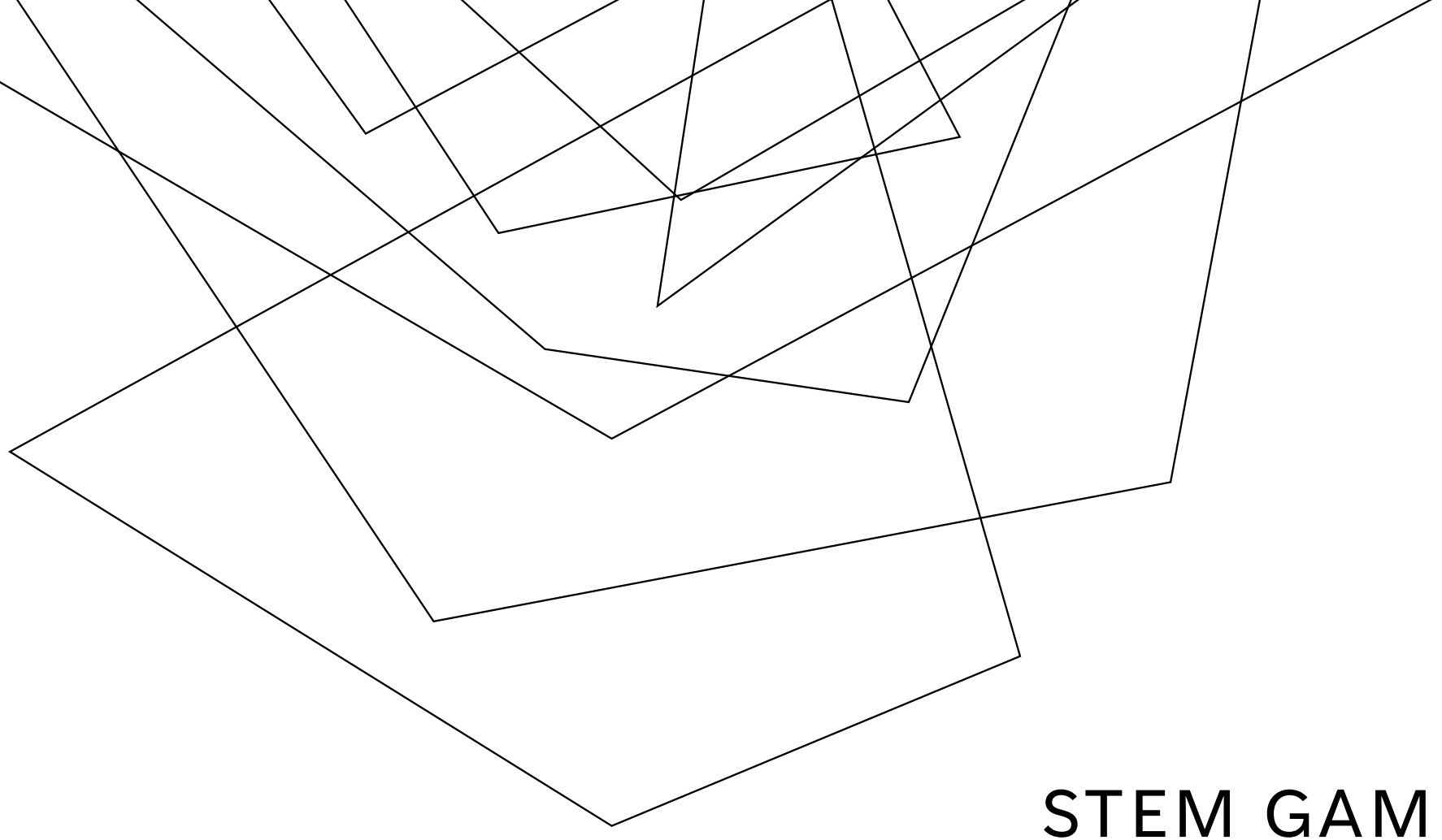
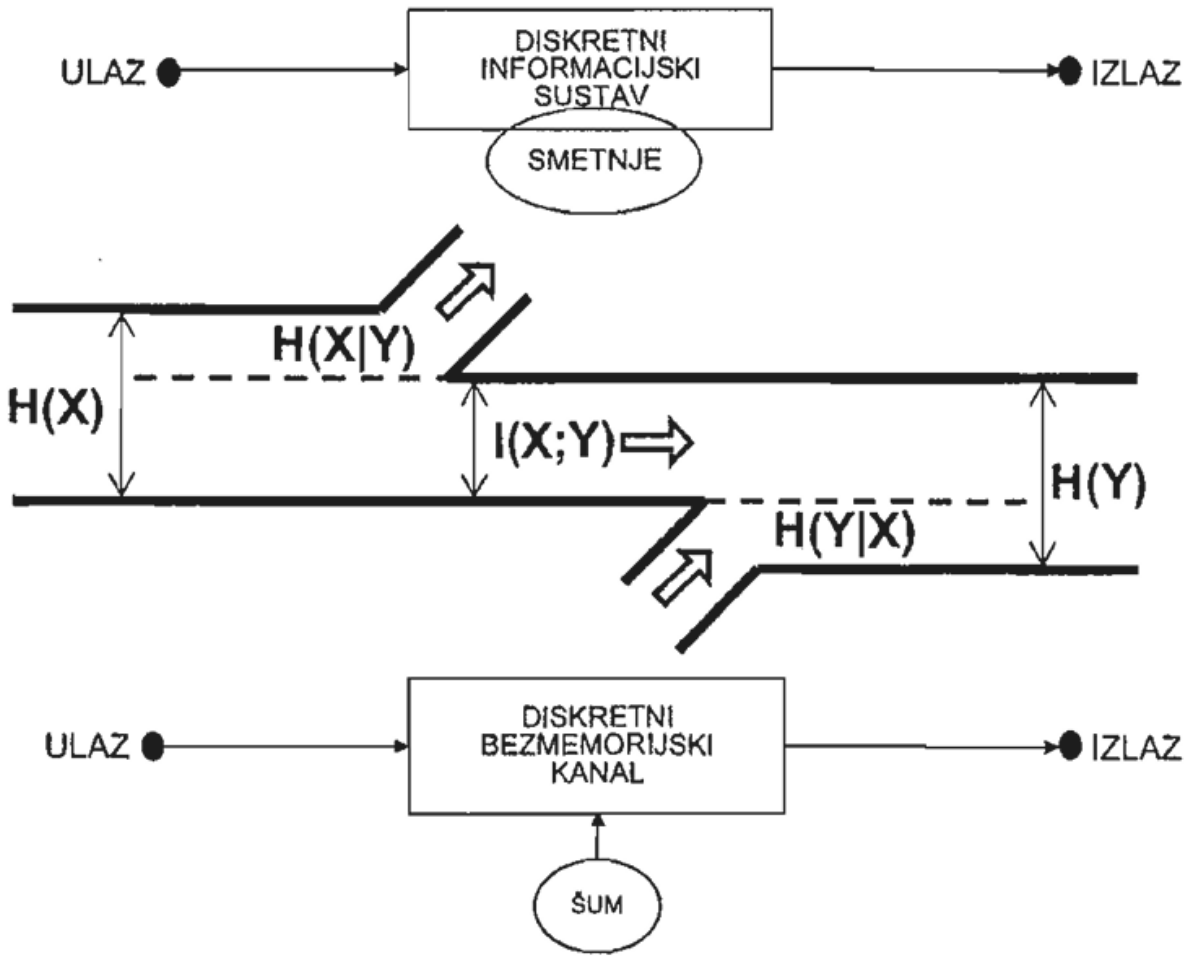


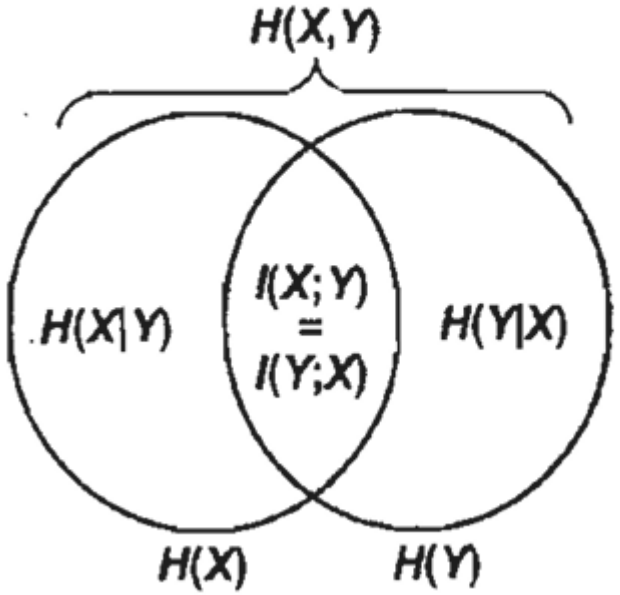
STEM GAMES – M ARENA

Roko Čubrić, Borna Gojšić, David Janjić, Roko Karničić,

Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva

Odnosi informacijskih mjera – pregledni prikaz





Igor S. Pandžić et al. (2009.), *Uvod u teoriju informacije i kodiranje*, Element

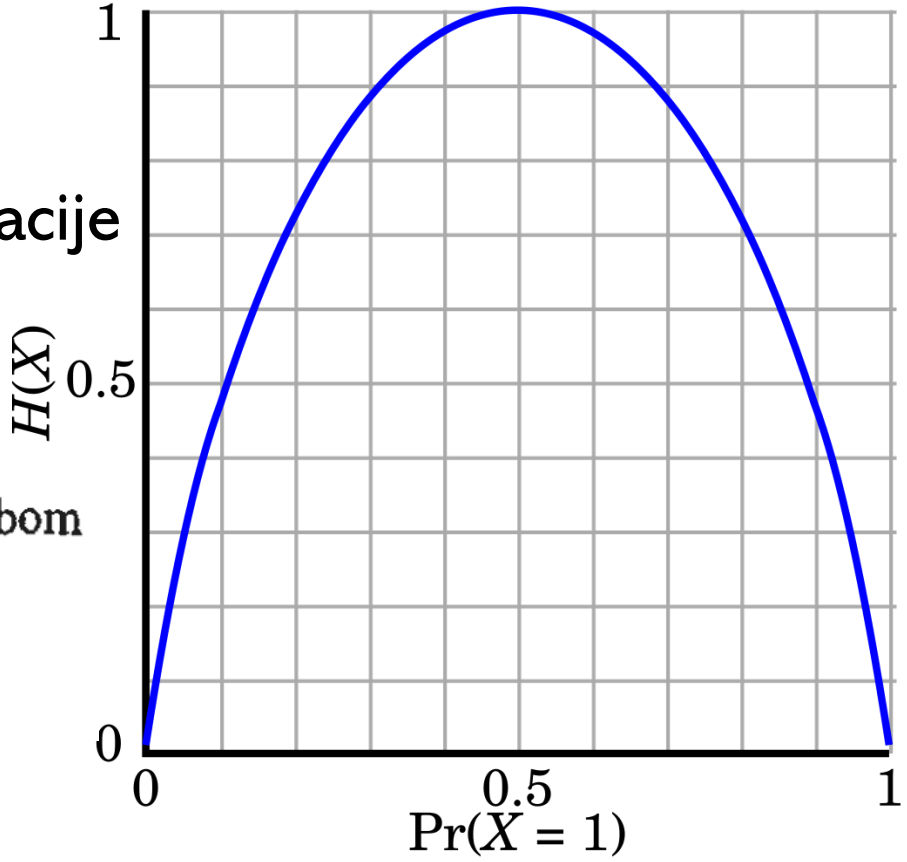
ENTROPIJA KAO MJERA

$I(E) = -\log_b(p(E))$ - Količina informacije

$H(X) = -\sum_x p(x)\log_b(p(x))$ - Prosječna količina informacije

Entropiju jednodimenzionalne slučajne varijable X s kontinuiranom razdiobom definiramo izrazom

$$H(X)=E\left[-\log f_X(X)\right]=-\int_{-\infty}^{\infty} f_X(x)\log f_X(x)dx,$$



Entropija Bernoullijeve slučajne variable u ovisnosti o p - Wiki

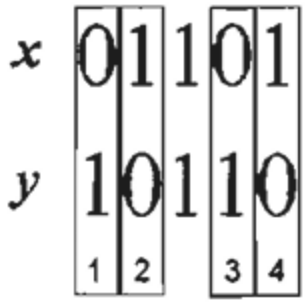
KODIRANJE I SAVRŠENI KODOVI

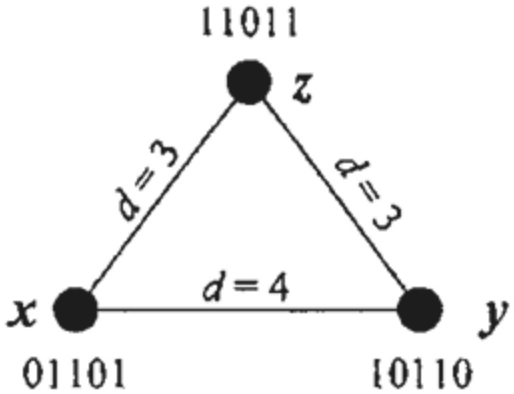
- Code[n,k(,d)]
- n = r + k
- Mogućnost detektiranja d-1 grešaka i ispravljanja (d-1)/2
- Paritetni bitovi

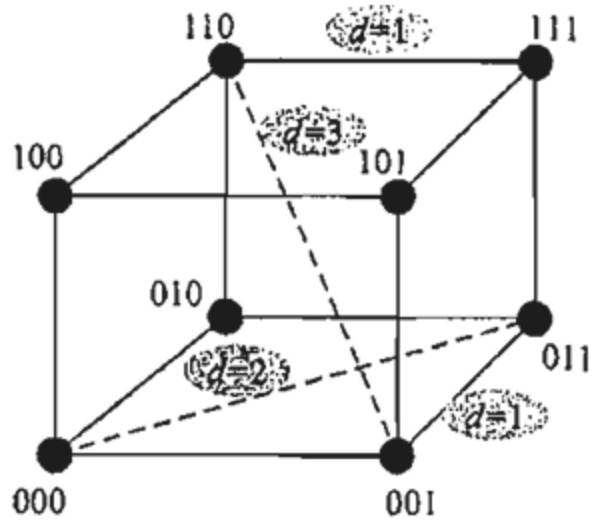
Bits	P_1	P_2	D_1	P_3	D_2	D_3	D_4	P_4	D_5	D_6	D_7	D_8	D_9	D_{10}	D_{11}
P_1	X		X		X		X		X		X		X		X
P_2		X	X			X	X			X	X			X	X
P_3				X	X	X	X					X	X	X	X
P_4								X	X	X	X	X	X	X	X

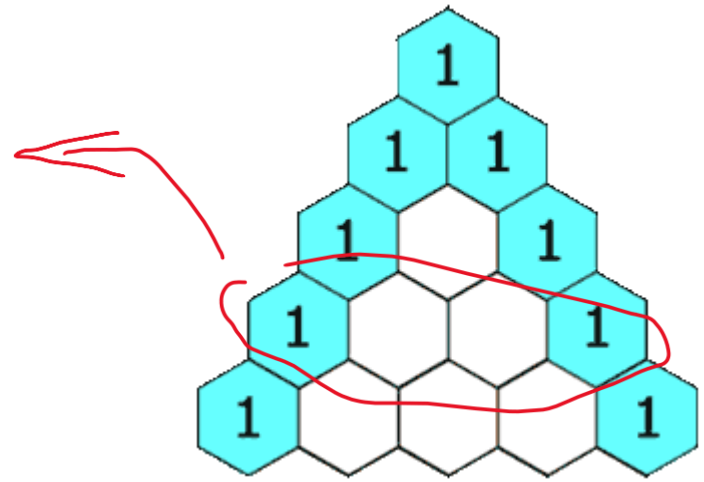
Hamming[15,11,3]

http://datagenetics.com/blog/january42016/index.html









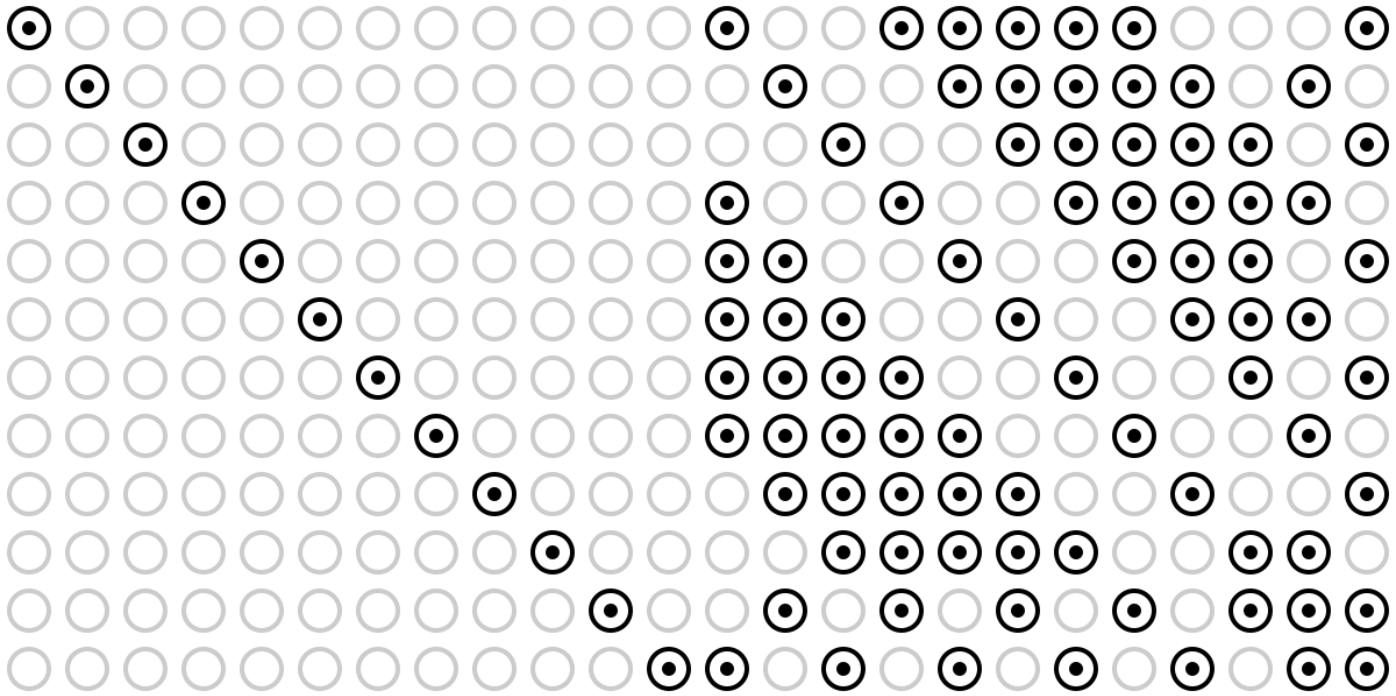
Slika 4.2: Grafičke interpretacije svojstava Hammingove udaljenosti

PERFEKTAN KÔD: Binarni $(n, M, 2t+1)$ kôd koji zadovoljava izraz:

$$M = \frac{2^n}{\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots \binom{n}{t}}$$

ZADATAK – DAN 3

- Osmisliti zaštitni kod u kanalu čiji šum može prouzročiti do 10 pogrešaka na 100 bitova



Golay[24,12,8]

Golay[23,12,7] je perfektan kod

Djeljenje 100 zaštitnih bitova u 8 grupa po 12

Hamming[7,4,3] za preostala 4 bita poruke

BOLJE RJEŠENJE – REED-SOLOMON KODOVI

- d = n-k+1

Primjena	RS parametri	Zašto?
CD/DVD (ECC)	RS(28, 24)	Ispravlja greške nastale ogrebotinama
QR kodovi	RS(26, 16)	Omogućuje čitanje oštećenih kodova
NASA Deep Space	RS(255, 223)	Otporan na šum u svemirskoj komunikaciji
SSD/HDD (NAND flash)	RS(128, 112)	Ispravlja višebitne greške u memoriji
DVB-S2 (satelitski TV)	RS(204, 188)	Zaštita od gubitaka u prijenosu

U BANKOVNIM TRANSAKCIJAMA

1. Inicijalizacija transakcije
2. Validacija i autorizacija
3. Procesiranje transakcije u bazi podataka
4. Potvrda i završetak transakcije

DJELOVI TRANSAKCIJE KOJI TREBAJU ZAŠTITU

- Potencijalne greške na fizičkom sloju:
  - Bit-flipovi (Single Event Upset - SEU) – Reed-Solomon, Golay,...
  - Kvarovi u mrežnoj infrastrukturi
  - Kvarovi u pohrani podataka (SSD/HDD) – Hammingovi kodovi
  - Problemi u HSM (Hardware Security Module)
- Danas u upotrebi:
  - Optika
  - Bakreni kabeli (Ethernet) i bežični prijenos se izbjegavaju zbog učestalosti grešaka
- Cilj – brzina i sigurnost = efikasnost