ZAŠTITNO KODOVANJE

Uvod

U prethodnom predavanju analiziran je model prolaska informacija kroz kanal i definisana prenesena (međusobna) informacija kao razlika prvobitne neizvjesnosti (entropije) i preostale neizvjesnosti po prijemu simbola o tome koji je simbol emitovan. Ova neizvjesnost se pojavljuje u realnim kanalima zbog grešaka koje mogu da se dogode pri prenosu.

Osnovno je pitanje kolika se količina informacija može pouzdano prenositi kroz jedan kanal? Odmah se postavlja prirodno pitanje – Šta je to pouzdan prenos? Odgovor je sledeći: Pouzdan prenos je prenos uz kontrolisanu dopuštenu – vjerovatnoću greške. Red veličine dopuštene vjerovatnoće greške varira u zavisnosti od imformacija koje se prenose (od 10^{-2} – 10^{-3} u ekstremno teškim slučajevima do 10^{-6} – 10^{-8} u nekim specijalnim telekomunikacionim sistemima).

Vjerovatnoća greške

Neka je dat binarni kanal (BC) definisan sljedećom kanalnom matricom:

$$P_{BC} = \begin{bmatrix} 1-g_1 & g_1 \\ g_2 & 1-g_2 \end{bmatrix}$$

Srednja vjerovatnoća greške je:

$$Q_e = P(X_1)\cdot g_1 + P(X_2)\cdot g_2$$

U slučaju jednako vjerovatnih ulaza svodi se na:

$$Q_e = 0,5\cdot(g_1 + g_2)$$

Ako je binarni kanal simetričan (BSC) $g_1 = g_2$

$$Q_e = 0,5\cdot(g + g) = g$$

U opštem slučaju kada imamo prenos sa *r* simbola najveća moguća vjerovatnoća greške je:

$$Q_e = 1 - \frac{1}{r} \qquad \text{(vrijedi i za } r = s \text{ i za } r \neq s\text{)}$$

uz uslov da su svi ulazni simboli podjednako vjerovatni.

Zaštitno kodovanje ponavljanjem poruke

Repetitivni kod (kod za detekciju i korekciju greške)

Repetitivni kod je najjednostavniji način zaštitnog kodovanja koji se svodi na višestruko ponavljanje jedne poruke (simbola)

Neka je dat BSC kanal definisan kanalnom matricom:

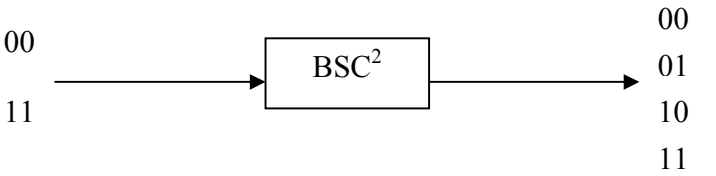
$$P_{BSC} = \begin{bmatrix} 1-g & g \\ g & 1-g \end{bmatrix}$$

i neka su ulazni simboli $\{X_1, X_2\} = \{0, 1\}$ jednako vjerovatni i neka je $g = 0{,}01 = 10^{-2}$ (vjerovatnoća greške pri prenosu).

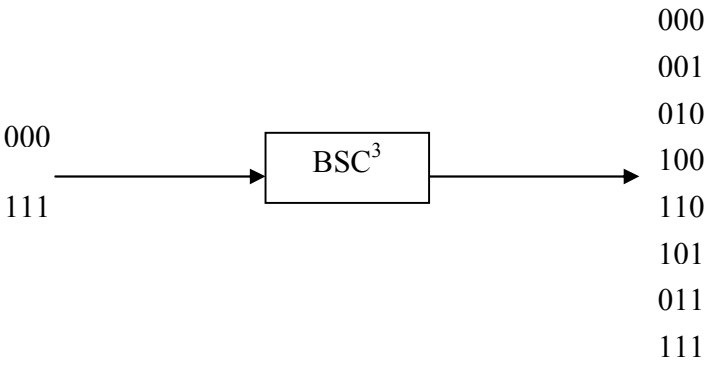
Na slici je prikazan ovaj kanal i liste simbola koji se pojavljuju na ulazu i izlazu:

U posmatranom slučaju vjerovatnoća greške je: $Q_e = g = 0{,}01 = 10^{-2}$ što je vrijednost koja je nekoliko puta veća od one koja se danas dozvoljava u sistemima za prenos podataka.

Jedan od načina da se ona **smanji** je da se svaki informacioni simbol ponovi više puta. Na primjer, da se simbol **0** šalje kao kodna riječ **00**, a simbol **1** kao kodna riječ **11**. Međutim, zbog mogućih grešaka na izlazu kanala mogu se pojaviti i **01** ili **10**. Novonastala situacija se sada može predstaviti slikom:



ili



Na prijemu se može primjeniti više pravila odlučivanja. Jedan način odlučivanja je da kada stigne kodna riječ **00** smatra se da je ulazna poruka **0** i analogno za kodnu riječ **11**. Međutim, kada su izlazne kombinacije **01** ili **10** smatra se da je došlo do pojave (jedonstruke) greške pri prenosu. U tom slučaju bi se moglo, ako postoji kanal povratne veze, zatražiti ponavljanje poruke, dok se u slučaju da nema ovakvog kanala poruka može obilježiti kao netačna (ekvivalentno kanalu sa brisanjem).

Greška se neće otkriti samo u slučaju da su se u toku prenosa jedne kodne riječi dogodile dvije greške – oba bita su progrešna. Na taj način se vjerovatnoća da greška neće biti otkrivena (detektovana) smanjuje i iznosi:

$$Q_e = g^2 = 10^{-4}$$

Cijena koja se plaća za smanjenje vjerovatnoće greške je smanjenje brzine prenosa (protoka informacija), jer se sada za prenos količine informacije od 1 Šenona koriste ne jedan nego dva bita ili više.

Ovo, sa svoje strane, može da utiče na potreban propusni opseg. Da bi se ovo kvantitativno opisalo pogodno je uvesti jednu veličinu - **Kodni količnik (odnos)(Code Rate)**:

$$R = \frac{\log M}{n} \left[\frac{Sh}{b} \right]$$

gdje je M – broj različitih jednako vjerovatnih poruka (simbola) koje je potrebno prenijeti kroz kanal.

Ako je $M = 2^k$ tada je:

$$R = \frac{k}{n} \quad (0 \le R \le 1)$$

k – broj informacionih bita u kodnoj riječi.
n – dužina kodne riječi

U prethodno analiziranom slučaju kodni količnik (a i brzima prenosa) se smanjuje za pola, tj. potrebno je dva bita u kanalu po svakom Šenonu informacija.

U slučaju ako se **0** koduje sa **000** i **1** sa **111**, uzme se isti princip odlučivanja (detekcije) greške tada se kombinacije **000** dekoduju kao **0**, odnosno **111** kao **1**, a u svim ostalim slučajevima smatra se da su se pojavile greške. Vjerovatnoća neotkrivene greške po poruci biće $Q_e = g^3 = 10^{-6}$, ali će se kodni količnik smanjiti na trećinu svoje prvobitne vrijednosti. Ovakvim pravilom odlučivanja biće otkrivene sve jednostruke i dvostruke greške koje su se dogodie pri prenosu kodne riječi.

Međutim, može se uzeti i drugačije pravilo odlučivanja. Pored kodne riječi **000** postoji mogućnost da se prime i kombinacije koje sadrže po jednu jedinicu i dvije nule (**001**, **010**, **100**). Pošto je vjerovatnoća greške po bitu 0,01 to je daleko veća vjerovatnoća da su ove kombinacije potekle od kodne riječi **000** nego od kodne riječi **111**. Dakle, kada se prime

kombinacije sa manjim brojem jedinica može se smatrati da je emitovana kodna riječ **000** (poruka **0**), a kada se prime kombinacije sa većim brojem jedinica, odlučuje se da je emitovana kodna riječ **111** (poruka **1**).

U posmatranim slučaju nema potrebe za ponavljanjem, već se greške ispravljaju na prijemu. Greška **neće biti detektovana** i ispravljena ukoliko se pri prenosu dogodi da sva tri bita budu pogrešna ili da budu pogrešna bilo koja dva bita od tri, pa je **vjerovatnoća neotkrivene greške**:

$$Q_e = \binom{3}{0} g^3 + \binom{3}{1} g^2 (1-g)$$

$$\binom{n}{k} = \frac{n(n-1)...(n-k+1)}{k!} = \frac{n!}{k!(n-k)!}$$

Ovakvim pravilom odlučivanja ispravljaju se **samo jednostruke greške**.

Primjer:

Neka se poruka **0** koduje sa 5 bita ($n = 5$, $k = 1$)

Poruka	Kodna riječ
0	00000
1	11111

Na prijemu postoje $2^n = 32$ moguće kombinacije. Ako se usvoji pravilo odlučivanja da se smatra da nije bilo grešaka pri prenosu kada stigne kombinacija bita **00000** (odnosno **11111**), a da se sve ostale kombinacije smatraju greškom, tada će vjerovatnoća neotkrivene greške biti $Q_e = g^5 = 10^{-10}$ i tom prilikom otkriće se sve jednostruke, dvostruke, trostruke i četvorostruke greške.

S druge strane, ako se sve kombinacije sa 3, 4 i 5 nula pripišu kodnoj riječi **00000** (i analogno se uradi sa kombinacijama koje imaju više jedinica) otkriće se i ispravljati sve jednostruke i dvostruke greške, ali će vjerovatnoća neotkrivene greške biti:

$$Q_e = \binom{5}{0} g^5 + \binom{5}{1} g^4 (1-g) + \binom{5}{2} g^3 (1-g)^2$$

Sada je kodni količnik $R = \frac{1}{5}$

Na osnovu prethodno rečenog možemo zaključiti da povećanje broja ponovljenih bita smanjuje vjerovatnoću greške i zavisno od pravila odlučivanja omogućava detekciju i korekciju grešaka, ali uz veliku cijenu jer se kodni količnik (a samim tim i brzina prenosa) drastično smanjio.

Prirodno je postaviti pitanje da li postoji neki drugi način da se izvrši zaštitno kodovanje i smanji vjerovatnoća greške, a da se pri tome ne smanji mnogo kodni količnik.

Odgovor daje II Šenonova teorema.

II Šenonova teorema

Neka je dat BC kanal sa vjerovatnoćom greške p_g čija je maksimalna prenešena informacija $I_{\max} = 1 - H(g) = C$, tada se za dovoljno veliko n može od 2^n raspoloživih sekvenci u kanalu izabrati kod sa M kodnih riječi (M – podjednako vjerovatne poruke) tako da vjerovatnoća greške pri prenosu bude proizvoljno mala.

$$\text{ili } R \le C \text{ na } n \text{ (veliko) } Q_e \to 0$$

Broj mogućih različitih kodova je: $\begin{pmatrix} 2^n \\ 2^k \end{pmatrix}$

Blok kodovi

Druga Šenonova teorema je pokazala da postoje dobri zaštitni kodovi, ali je ostavila otvoren problem kako ih treba naći, osim smjernice da kodne riječi treba da budu što duže.

Osnovni model pri zaštitnom kodovanju je takav da se smatra da na ulaz u koder dolaze statistički nezavisni, podjednako vjerovatni biti. Ukoliko bi se ovi biti prenosili takvi kakvi se pojavljuju na ulazu u koder ne bi bilo moguće nikakvo otkrivanje (detektovanje) grešaka. Da bi se greške nastale pri prenosu otkrile i ispravile mora se u prenošene poruke unijeti izvjesna redudansa. Ova redudansa se može unijeti na različite načine, pa se kodovi mogu upravo i podijeliti prema načinu njenog unošenja. Elementarna podjela je na **blok kodove** i **konvolucione kodove**.

Kod blok kodova posmatra se prenos podataka (bita ili simbola) u blokovima. Prema tome, zadatak blok kodera je da prihvati izvjestan broj (k) statistički nezavisnih i podjednako vjerovatnih bita i da ih predstavi odgovarajućom kodnom riječi od n bita. Blok se označava sa (n, k) dok se $R = \frac{k}{n}$ naziva kodni količnik.

a) Kodovi sa jednostavnim provjerama na parnost

Kodovi ovog tipa su vjerovatno najstariji primjenjeni zaštitni kodovi. Kod njih se jednostavno na k informacionih bita dodaje jedan i samo jedan kontrolni bit ($n = k + 1$) **provjere na parnost** tako da ukupan broj jedinica u kodnoj riječi bude paran. Samim tim u dekoderu se može otkriti **neparan broj grešaka** nastalih pri prenosu kodne riječi.

Kodni količnik je $R = \frac{n-1}{n} \quad n = k + 1$

Ovakav kod služi za detekciju greške!

Kao koder (i kao dekoder) može se koristiti elementarno digitalno kolo sa dva stanja koje broji jedinice u kodnoj riječi – na predaji broji jedinice u informacionim simbolima i po potrebi dodaje jedinicu (ili nulu) na kraju kodne riječi, a na prijemu samo broji jedinice u prispjeloj sekvenci bita.

Vjerovatnoća pojave k grešaka u nekoj poruci sa n bita jednaka je:

$$\binom{n}{k} g^k (1-g)^{n-k}$$

Ovaj kod ne može detektovati paran broj grešaka nastalih pri prenosu.

Vjerovatnoća pojave parnog broja grešaka je:

$$\sum_{m=1}^{n/2} \binom{n}{2m} g^{2m} (1-g)^{n-2m}$$

Primjer:

Neka imamo 7 bita korisne informacije, a osmi bit je za detekciju greške:

$$0 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1 \quad 0 \quad \boxed{1} \qquad k = 7 \quad n = 8$$

Kodni količnik je $R = \dfrac{\log 2^7}{8} = \dfrac{7}{8}$

Ukupan broj poruka je $M = 2^k = 2^7$

Kada će se ovdje dogoditi greške koje nijesmo u stanju da detektujemo?

Ako se dogode dvije greške (par)

$$\begin{array}{cccccccc} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{array} \longrightarrow \text{dvije greške – ista vrijednost kontrolnog bita}$$

Vjerovatnoća pojave dvije greške je:

$$\sum_{m=1}^{4} \binom{8}{2m} g^{2m} (1-g)^{8-2m} = \binom{8}{2} g^2 (1-g)^6 + \binom{8}{4} g^4 (1-g)^4 + \binom{8}{6} g^6 (1-g)^2 + \binom{8}{8} g^8$$

b) Pravougaoni kod *(kod za detekciju i korekciju greške)*

Informacioni biti se ne moraju posmatrati "jednodimenzionalno", oni se mogu složiti i "dvodimenzionalno" u okviru matrice i tada se može izvršiti dodavanje provjera na parnost i po vrstama i po kolonama, prema sledećoj šemi:

$$\left|\begin{array}{ccc|c} i_{11} & . & i_{1k_2} & c \\ . & & . & . \\ i_{k_1 1} & . & i_{k_1 k_2} & . \\ \hline c & . & . & c \end{array}\right|$$

Ako se u jednom bloku posmatra $k_1 \cdot k_2$ informacionih bita, kodna riječ će sadržati ukupno $n = (k_1 + 1)(k_2 + 1)$ bita od kojih će $k_1 + k_2 + 1$ biti kontrolni biti.

Kodni količnik je sada $R = \dfrac{k_1 \cdot k_2}{(k_1 + 1)(k_2 + 1)}$ i njegova najveća vrijednost se dobija kada je:

$k_1 = k_2 = k$, tada je: $n = (k + 1)^2$ i iznosi $R = \dfrac{k^2}{(k+1)^2}$, a broj kontrolnih bita je $2k + 1$

Primjer:

$(n, k) = (9, 4)$

i_1	i_2	c_1
i_3	i_4	c_2
c_3	c_4	c_5

$k = 4$ broj informacionih bita
$n = 9$ dužina kodne riječi u bitima
$n - k = 5$ broj kontrolnih bita (koliko je njih toliko je kontrola na parnost)

i – informacioni biti
c – kontrolni biti

$$\left.\begin{array}{l} i_1 \oplus i_2 \oplus c_1 = 0 \\ i_3 \oplus i_4 \oplus c_2 = 0 \\ i_1 \oplus i_3 \oplus c_3 = 0 \\ i_2 \oplus i_4 \oplus c_4 = 0 \end{array}\right\} \text{ 0 u slučaju na nema greške}$$

c_5 provjerava čitavu matricu:

$$i_1 \oplus i_2 \oplus i_3 \oplus i_4 \oplus c_1 \oplus c_2 \oplus c_3 \oplus c_4 \oplus c_5 = 0$$

Što se tiče sposobnosti koda za detektovanje i ispravljanje grešaka imamao sledeće zaključke: Ukoliko se dogodila samo jedna greška na bloku informacionih bita, tada će odgovarajuće provjere po vrsti i koloni, u čijem je presjeku pogrešan bit, ukazati tačno na njegovu poziciju, tj. takva se greška može ispraviti.

c) Tougaoni kod

Primjer:

(15, 10)
$n = 15$ dužina kodne riječi
$k = 10$ broj informacionih bita
$n - k = 5$ kontrolnih bita

i_1	i_2	i_3	i_4	c_1
i_5	i_6	i_7	c_2	
i_8	i_9	c_3		
i_{10}	c_4			
c_5				

c_1 kontroliše $i_1,\ i_2,\ i_3,\ i_4$
c_2 kontroliše $i_5,\ i_6,\ i_7,\ i_4$
c_3 kontroliše $i_8,\ i_9,\ i_3,\ i_7$
c_4 kontroliše $i_{10},\ i_2,\ i_6,\ i_9$
c_5 kontroliše $i_1,\ i_5,\ i_8,\ i_{10}$

Glavni nedostatak ovih blok kodova je što se mora sačekati na prijemu da stigne cio "višedimenzionalni" blok, pa se tek može krenuti sa provjerama.

Hemingov kod

Hemingov kod (7, 4) je prikazan još 1948g. u Šenonovom pionirskom radu. U tom radu se opisuje ne samo pomenuti kod, već čitava klasa kodova ovog tipa i uvodi niz pojmova koji se i danas koriste (Hemingovo rastojanje, ekvivalentnost kodova, sistematski kodovi).

Heming je prikazao familiju kodova za otkrivanje (detekciju) i ispravljanje (korekciju) jedne greške kod kojih **sindrom**, dobijen kao rezultat provjera na parnost izvršenih na prijemu, u binarnoj notaciji pokazuje poziciju pogrešnog bita, ako je došlo do **jedne greške**.

U medicini sindrom predstavlja skup simptoma karakterističnih za neko oboljenje, dok je ovdje to rezultat provjera na parnost izvršenih na prijemu koje pokazuju da li je došlo do jedne greške i gdje je greška.

Heming najprije određuje broj različitih vrijednosti sindroma i zaključuje da broj provjera $(n - k)$ treba da zadovoljava nejednakost:

$$2^{n-k} \geq n + 1$$

jer postoji n pozicija u kodnoj riječi gdje bi se mogla desiti greška, kao i slučaj kada do greške nije došlo.

Kontrolni biti mogli bi se na predaji dodati iza informacionih, na kraju kodne riječi. Pošto je Heming pošao od ideje da binarno pročitana vrijednost sindroma treba da pokazuje

poziciju pogrešnog bita, kontrolni biti se ne stavljaju na poslednje mjesto, već na mjesta prema sledećem rasporedu:

c_1 - prvi kontrolni bit treba postaviti na poziciju koja je definisana sa $2^0 = 1$

c_2 - drugi kontrolni bit treba postaviti na poziciju $2^1 = 2$

c_3 - treći kontrolni bit treba postaviti na poziciju $2^2 = 4$, itd.

Ovi kontrolni biti vrše provjere na parnost informacionih bita. Tako da c_1 vrši provjeru parnosti onih informacionih bita čije pozicije kada se podijele sa 2 imaju ostatak 1. To će biti sve neparne pozicije (3, 5, 7, ...).

Drugi kontrolni bit c_2 vrši provjere na parnost onih informacionih bita koji se nalaze na pozicijama koje pri dijeljenju sa $2^2 = 4$ imaju ostatak 2 i 3. Te pozicije su (3, 6, 7, 10, 11, 14, 15...).

Treći kontrolni bit c_3 vrši provjeru na parnost onih informacionih bita koji se nalaze na pozicijama koje pri dijeljenju sa $2^3 = 8$ imaju ostatak 4, 5, 6, 7. Te pozicije su (5, 6, 7, 12, 13, 14, 15...).

Primjer:

Hemingovim kodom (7, 4) kodovati sekvencu **1101**.

Pošto je $n = 7$, $k = 4$, $(n - k) = 3$ imamo tri kontrolna bita i broj potrebnih provjera na parnost mora zadovoljiti nejednakost:

$$2^{n-k} \geq n+1 \qquad 2^3 \geq 7+1 \quad \text{(tačno)}$$

Na osnovu prethodnog izlaganja najprije se određuju pozicije informacionih i kontrolnih bita.

pozicija	1	2	3	4	5	6	7
	c_1	c_2	i_1	c_3	i_2	i_3	i_4

tj.

pozicija	1	2	3	4	5	6	7
	c_1	c_2	1	c_3	1	0	1

Vrijednosti kontrolnih bita su:

$c_1 = i_1 \oplus i_2 \oplus i_4 = 1 \oplus 1 \oplus 1 = 1$ (ovaj bit provjerava parnost informacionih bita sa 3, 5, 7 pozicije)

$c_2 = i_1 \oplus i_3 \oplus i_4 = 1 \oplus 0 \oplus 1 = 0$ (ovaj bit provjerava parnost informacionih bita sa 3, 6, 7 pozicije)

$c_3 = i_2 \oplus i_3 \oplus i_4 = 1 \oplus 0 \oplus 1 = 0$ (ovaj bit provjerava parnost informacionih bita sa 5, 6, 7 pozicije)

Kodirana riječ je sada:

pozicija	1	2	3	4	5	6	7
	1	0	1	0	1	0	1
	X_1	X_2	X_3	X_4	X_5	X_6	X_7

Neka se pri prenosu dogodila greška na šestoj poziciji, tj. neka je vektor greške:

$$e = [0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0]_{1\times 7(1\times n)}$$

Tj. ako se desi pri prenosu jedna greška, vektor greške, dimenzija $1\times n$, na svim pozicijama ima **0** sem na poziciji na kojoj se dogodila greška.

Sekvenca na prijemu će biti:

$$Y_i = X_i \oplus e_i \text{ tj.}$$

$$Y = [1 \quad 0 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1] + [0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0]$$

$$Y = [1 \quad 0 \quad 1 \quad 0 \quad 1 \quad 1 \quad 1]_{1\times 7}$$

$y_1 \quad y_2 \quad y_3 \quad y_4 \quad y_5 \quad y_6 \quad y_7$

Na prijemu se sada formiraju elementi sindroma (ima ih $n - k$, u ovom slučaju 3)

$$S_1 = Y_1 \oplus Y_3 \oplus Y_5 \oplus Y_7 = 1 \oplus 1 \oplus 1 \oplus 1 = 0$$

$$S_2 = Y_2 \oplus Y_3 \oplus Y_6 \oplus Y_7 = 0 \oplus 1 \oplus 1 \oplus 1 = 1$$

$$S_3 = Y_4 \oplus Y_5 \oplus Y_6 \oplus Y_7 = 0 \oplus 1 \oplus 1 \oplus 1 = 1$$

Sindrom je sada $S = \{S_3, S_2, S_1\}$ = **110** što u binarnoj notaciji predstavlja broj 6, zaključuje se da se greška dogodila na šestoj poziciji i ispravlja se.

Kao što se kod razmatranog primjera može uočiti, ovaj kod može da ispravlja **jednostruke greške**.

Kodovi za detekciju i ispravljanje greške u matričnom obliku

Svaki vektor dužine n bita oblikovan kombinacijom od k linearno nezavisnih osnovnih vektora $g_1, g_2, ..., g_k$ je binarni (n, k) blok kod. U tom slučaju se kodna riječ C može naći na sljedeći način:

$$C = i \cdot G$$

gdje je i informacioni vektor od k informacionih bita $i = [i_i]_{1\times k}$, a G generišuća matrica dimenzija $k \times n$.

$$C_{1\times n} = i_{1\times k} \cdot G_{k\times n}$$

Ako se kontrolni biti (a njih ima (n - k)) stavljaju na poslednje mjesto generišuća matrica ima oblik:

$$G = \left[I_k \;\vdots\; P \right]_{k\times n}$$

gdje je I_k jedinična matrica dimenzije $k\times k$, a P je paritetna matrica dimenzija $k\times(n-k)$, čije kolone pokazuju pozicije gdje se uzimaju provjere na parnost.

Primjer:

Kod sa jedonstrukim paritetom (tj. gdje smo imali samo jedan kontrolni bit postavljen na kraju sekvence) $c_1 = i_1 \oplus i_2 \oplus ... \oplus i_k$

$$C = \left[i_1 \quad ... \quad i_k \right]_{1\times k} \qquad \left[\begin{array}{ccccc:c} 1 & 0 & 0 & ... & 0 & 1 \\ 0 & 1 & 0 & ... & 0 & 1 \\ . & & & & & . \\ . & & & & & . \\ . & & & & & . \\ 0 & 0 & 0 & ... & 1 & 1 \end{array}\right]_{k\times n}$$

Ovdje je paritetna matrica P dimenzije $k\times 1$

$$P = \begin{bmatrix} 1 \\ 1 \\ . \\ . \\ 1 \end{bmatrix}_{k\times 1}$$

Primjer:

Repetitivni kod sa ponavljanjem tri bita, $k = 1$, $n = 3$

$C = \left[i_1 \quad i_1 \quad i_1 \right]_{1\times 3} = i_1 \cdot G \Rightarrow G = \left[1 \quad 1 \quad 1 \right]_{1\times 3}$, a paritetna matrica $P = \left[1 \quad 1 \right]_{1\times 2}$

Primjer:

Pravougaoni kod (9, 4)

$n = 9$, $k = 4$, (n - k) = 5 – pet kontrolnih bita, pet provjera na parnost

$$C_{1\times 9} = i_{1\times 4} \cdot G_{4\times 9}$$

$$\left[i_1 \quad i_2 \quad i_3 \quad i_4 \quad c_1 \quad c_2 \quad c_3 \quad c_4 \quad c_5 \right] = \left[i_1 \quad i_2 \quad i_3 \quad i_4 \right] \cdot \left[I_{4\times 4} \;\vdots\; P_{4\times 5} \right]$$

i_1	i_2	c_1
i_3	i_4	c_2
c_3	c_4	c_5

c_1 - provjerava parnost i_1 i i_2
c_2 - provjerava parnost i_3 i i_4
c_3 - provjerava parnost i_1 i i_3
c_4 - provjerava parnost i_2 i i_4
c_5 - provjerava parnost i_1, i_2, i_3 i i_4

pa je paritetna matrica:

$$P = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}_{4\times 5}$$

a generišuća:

$$G = \left[\begin{array}{cccc:ccccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{array}\right]_{4\times 9}$$

Primjer:

Hemingov kod (7, 4)

$$C_{1\times 7} = i_{1\times 4} \cdot G_{4\times 7}$$

$$\begin{bmatrix} c_1 & c_2 & i_1 & c_3 & i_2 & i_3 & i_4 \end{bmatrix}_{1\times 7} = \begin{bmatrix} i_1 & i_2 & i_3 & i_4 \end{bmatrix}_{1\times 4} \cdot G_{4\times 7}$$

Ako kontrolne bite c_1, c_2, c_3 stavljamo na kraju onda se generišuća matrica konstruiše kao i u prethodnim slučajevima.

Međutim, ako kontrolne bite postavljamo prema binarnom rasporedu onda kolone paritetne matrice moramo postaviti na pozicije kontrolnih bita, tj:

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ c_1 & c_2 & i_1 & c_3 & i_2 & i_3 & i_4 \end{bmatrix}_{4\times 7}$$

$$c_1 = i_1 \oplus i_2 \oplus i_4$$
$$c_2 = i_1 \oplus i_3 \oplus i_4$$
$$c_3 = i_2 \oplus i_3 \oplus i_4$$

Na prijemu se provjera pariteta sprovodi na sljedeći način:

$$S = C \cdot H^T$$

gdje je H kontrolna matrica datog koda koja se dobija kao (u slučaju da su kontrolni biti postavljeni na posljednjem mjestu u kodnoj riječi):

$$H = \left[P^T \;\vdots\; I_m \right]_{(n-k)\times n}$$

gdje je P^T transponovana paritetna matrica, a I_m jedinična matrica dimenzija $(n-k)\times(n-k)$.

U slučaju da je $C \cdot H^T = 0$ kodna riječ je prenešena bez greške.

U slučaju greške je $S \neq 0$ i tada možemo pisati:

$$S = Y \cdot H^T = (X + e) \cdot H^T = \underbrace{X \cdot H^T}_{=0} + e \cdot H^T$$

$$S = e \cdot H^T$$

Slijedi da sindrom ne zavisi od predate kodne riječi već samo od greške.

Da bi se odredio vektor greške potrebno je riješiti ovu jednačinu. Ovo se rješava tako što se provjerava koji se bit promjenio.

Primjer:

Sekvencu **1101** kodovati Hemingovim kodom (7, 4) i provjeriti kodnu riječ na prijemu.

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}_{4\times 7} \qquad \begin{matrix} n = 7 \\ k = 4 \\ (n - k) = 3 \text{ kontrolna bita} \end{matrix}$$

$$\begin{matrix} c_1 & c_2 & i_1 & c_3 & i_2 & i_3 & i_4 \end{matrix}$$

$$P = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}_{4\times 3(tj.k\times(n-k))}$$

$$C = i \cdot G = \begin{bmatrix} 1 & 1 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}_{4\times 7} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}_{1\times 7}$$

Provjera na prijemu:

$$S = C \cdot H^T$$

Transponovana paritetna matrica je:

$$P^T = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}_{3\times 4}$$
$$i_1 \quad i_2 \quad i_3 \quad i_4$$

Pošto se kod Hemingovog koda kontrolni biti postavljaju prema binarnom rasporedu, kontrolna matrica je:

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}_{3\times 7((n-k)\times n)}$$
$$c_1 \quad c_2 \quad i_1 \quad c_3 \quad i_2 \quad i_3 \quad i_4$$

$$S = C \cdot H^T = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}_{1\times 7} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}_{7\times 3} = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix}_{1\times 3}$$

$S = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix}_{1\times 3}$ - nema greške pri prenosu.

U slučaju da je došlo do greške na 5. poziciji:

$$Y = C + e = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

imaćemo da je $Y \cdot H^T = S$.

$$\begin{bmatrix}1 & 0 & 1 & 0 & 0 & 0 & 1\end{bmatrix}_{1\times 7} \cdot \begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 1 & 1 & 0\\ 0 & 0 & 1\\ 1 & 0 & 1\\ 0 & 1 & 1\\ 1 & 1 & 1\end{bmatrix}_{7\times 3} = \begin{bmatrix}1 & 0 & 1\end{bmatrix}_{1\times 3}$$

$S = \begin{bmatrix}1 & 0 & 1\end{bmatrix}_{1\times 3}$ - vrijednost sindroma ukazuje da je do greške došlo na 5. poziciji (**101**$_2$ = **5**$_{10}$)