Subject : Date فصل ۶

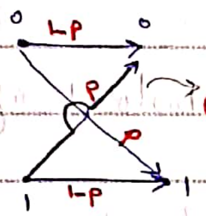
نظریه کدگذاری

در این فصل می خواهیم نظریه کدگذاری و کدگشایی را در سطح مقدماتی مطالعه و بررسی کنیم در جستجوی اطلاعاتی هستیم که انتقال این اطلاعات با مدلسازی در دودویی با رشته هایی از ۰ و ۱ نشان داده می شود.

در مخابرات دیجیتالی وقتی که اطلاعات در قالب رشته هایی از ۰ و ۱ ها منتقل می شود ممکن است مشکلات و مسائلی پیش بیاید. یعنی وقتی که نماد معینی مخابره می شود بر اثر نویزها و خطاهای مخابراتی نماد متفاوتی دریافت شود و باعث اتخاذ تصمیم غلط توسط دریافت کننده اطلاعات بشود.

در این فصل می خواهیم فنونی را بسازیم که بتواند مشکلات مخابره را آشکارسازی کند و در تصحیح غلط ها کمک کند. البته فقط می توان شانس مخابره صحیح را بهبود بخشیم.

مدلی که در این درس ارائه می شود مطابق شکل زیر است که از کانال دودویی متقارن استفاده می کند. که خط افقی به معنی صحیح مخابره است و خط مورب به معنی مخابره غلط است.



صفت دودویی به این دلیل به کار می رود که از ۰ و ۱ تشکیل شده است. یعنی همه درایه ها اعضای Z_2 هستند.

MICRO

Subject

Date

هر بیت با یکی از بیت های ۰ یا ۱ نشان داده می شود.

وقتی که فرستنده بیت ۰ یا ۱ را می فرستد به خاطر نویزها گیرنده اطلاعات دریافت صحیح را نداشته باشد.

فرستنده بهر بیتی که به غلط مخابره می شود احتمال ثابتی را نسبت می دهد. بنابراین اگر این احتمال مثلا p (که p کمتر از $\frac{1}{2}$ است) ثابت برای هر بیت ۰ و ۱ که به غلط مخابره می شوند نسبت داده شود این کانال را متقارن می نامند.

بنابراین کانال مخابراتی کانال متقارن دودویی است.

مثال: رشته C = 10110 ، C یک کلمه دودویی است که از Z_2^5 می آید.

$Z_2^5 = Z_2 \times Z_2 \times Z_2 \times Z_2 \times Z_2 \rightarrow C = (1,0,1,1,0)$

فرض کنیم هر یک از بیت های C از کانال متقارن دودویی ارسال می شود.

اگر p = 0.05 (یعنی مخابره غلط 0.05 باشد) در اینصورت احتمال ارسال کلمه C بدون خطا $= (1-0.05)^5 = 0.77$ (طبق قانون ضرب در صفر ترکیبات).

در سراسر بحث نظریه کدگذاری در این درس فرض می کنیم مخابره هیچ یک از بیت ها به هیچ وجه به مخابره بیت های قبل بستگی ندارد. بنابراین احتمال رخ دادن همه این پیشامدها مستقل از همدیگر هستند و برابر است با حاصلضرب احتمال های تک تک آنها.

MICRO

Subject :　　　　Date ....

مثال: احتمال اینکه دریافت شده کلمه $c = 10110$ با خطا کلمه به صورت $r = 00110$ باشد

چقدر است؟ چون فقط کلمه اول به اشتباه دریافت شده است پس فقط یک خطا داریم. 0.05 درصد

$0.05 \times (1 - 0.05)^4 = 0.041$

حال اگر بخواهد با خطا کلمه $t = 10000$ باشد. (غلط ... درست درست درست ... دومی)

$\underbrace{(1 - 0.05)^3}_{\text{۳ تا درست}} \times \underbrace{(0.05)^2}_{\text{۲ تا غلط}}$ ($1 - 0.05 = 0.95$)

خطا همواره به صورت $e_1 = 10000$ است. $e_1 + r = c$

و $e_2 = 00110$ که $e_2 + t = c$ می‌شود.

مقدار خطا نیز میتوان به صورت دودویی بیان شود.

گاهی مخابره کننده برای احتمال بسیار پایین خطا ها را نادیده می‌گیرد و می‌گوید این خطا هرگز رخ نمی‌دهد.

مثال: $c = 10110$ می‌فرستید و دریافت شده $r = 00100$

$(0.05)^2 \times (0.95)^3 = 0.002$

در این مثال خطای چندگانه شانس زیادی برای رخ دادن ندارند.

(چون مقدار 0.002 خیلی پایین است)

مثال: احتمال اینکه در مخابره $c = 10110$ دو خطا رخ دهد چقدر است؟

$\binom{5}{2} \times (0.05)^2 \times (0.95)^3 = 0.021$

چون ترکیب $\binom{5}{2}$ را نخوانده‌ایم

MICRO

Subject

Date / /

* احتمال اینکه حداکثر دو خطا رخ بدهد چقدر است؟

$$\binom{5}{0} \times (0.95)^5 + \binom{5}{1} \times (0.05)^1 \times (0.95)^4 + \binom{5}{2} (0.05)^2 (0.95)^3$$

قضیه ۱. فرض کنید c یک رشته n تایی از ۰ و ۱ باشد ($c \in Z_2^n$).

برای مخابره c از یک کانال دودویی متقارن استفاده می‌کنیم که احتمال مخابره غلط هر نماد p است در این صورت: الف) احتمال دریافت $r = c + e$ که در آن e همان

$c - e$ چون در Z_2، 1 و -1 برابر با است بنابراین هیچ تاثیری ندارد.

الگوی خطا نمای خاصی است که متشکل از k تا ۱ و $n-k$ تا ۰ است.

k تا خطا ... $n-k$ تا درست.

$e = c + r$ برابر است با $p^k \cdot (1-p)^{n-k}$

ب) احتمال وقوع k خطا در مخابره برابر است با $\binom{n}{k} p^k \times (1-p)^{n-k}$

اثبات الف) وقتی که ۰ در الگوی خطای نمای e با هر نماد متناظر آن در c جمع شود تغییر در نماد

ایجاد نمی‌شود. ولی اگر ۱ نمادی در e باشد با نماد متناظر آن در c جمع شود، نماد را به ۱ و

نماد ۱ را به صفر تبدیل می‌کند. بنابراین دقیقاً k تا نماد خطا و $n-k$ نماد بدون خطا مخابره

می‌شود. بنابراین احتمال دریافت $r = c + e$ برابر است با $p^k \cdot (1-p)^{n-k}$

اثبات ب) چون k خطا داریم و این k خطا می‌توانند در هر k مکان رخ بدهند لذا احتمال

OMICRO

Subject :

Date

دریافت c با k خطا طبق قانون ضرب در حالت ترکیبات برابر است با $\binom{n}{k} \times p^k (1-p)^{n-k}$

تعریف: یک کانال متقارن دودویی را خوب فرض می‌کنیم هرگاه $p < 10^{-5}$

ولی همواره فرض می‌کنیم که p از $\frac{1}{2}$ کوچکتر باشد. ($p < \frac{1}{2}$)

برای بهتر برون دقت مخابره از طریق کانال متقارن دودویی انواعی از طرح‌های کدگذاری را بیان

به کار برد که در آنها تمادهای اضافی وارد می‌شوند.

فرض کنیم $n, m \in Z^+$ (n, m دو عدد صحیح مثبت) و $n > m$ باشد. w را یک زیرمجموعه

غیرتهی از Z_2^m (یعنی یک مجموعه غیرتهی از رشته‌های m تایی دودویی) بگیرید.

و فرض می‌کنیم w در واقع پیام مخابره شده باشد.

به هر $w \in W$، $n-m$ نماد اضافی را از راه‌های خاص اضافه می‌کنیم تا واژه کد c

ساخته شود که $c \in Z_2^n$. این فرآیند از $w \in W$ به $c \in Z_2^n$ را فرآیند کدگذاری می‌نامند

که می‌تواند به صورت یک تابع مانند $E : W \longrightarrow Z_2^n$ باشد.

$E(w) = C$

فرض کنیم $C = \{ c \in Z_2^n \text{ s.t. } E(w) = C \mid \exists w \in W, E(w) = C \}$ این یک تابع ۱-۱ است. زیرا $w_1 \neq w_2$ باشد

آنگاه طی عملیات $c_1 \neq c_2$ می‌شود زیرا $E(w_1) \neq E(w_2)$ است.

MICRO

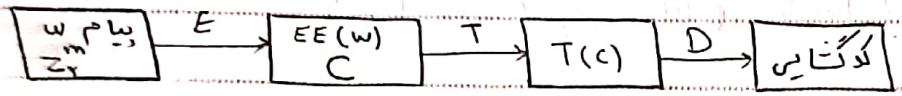
Subject

Date

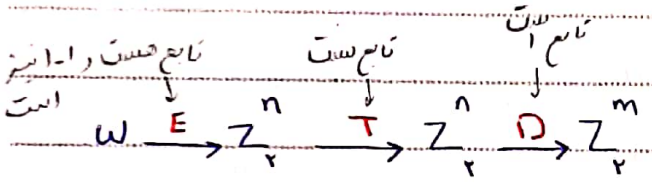
E از w به C یک تابع 1-1 و پوشا است.

حال فرض کنیم C پس از مخابره به صورت $T(C)$ دریافت شود. $T(C) \in Z_2^n$

اینجا $T(C)$ لزوماً تابع نیست چون ممکن است $T(C)$ در زمان مقاومت مخابره C متفاوت باشد.



$$D \circ Z_2^n \to Z_2^m \quad *$$



$$w \to C \to T(C) \to w'$$

انتظار این است که w همان w باشد. یعنی $\underbrace{D \circ T \circ E}_{\text{همانی}}(w) \stackrel{?}{=} w$

که این یک انتظار بالایی است. علاوه بر این لازم است که شیب $\frac{m}{n}$ خیلی نزدیک به 1 باشد چون هر چقدر به 1 نزدیکتر باشد هم پیدا کردن اشکالات راحت‌تر و هم تصحیح آن اشکالات به صورت $\frac{m}{n}$ نرخ کدگذاری، توابع E و D را نیز به ترتیب تابع کدگذاری و کدگشایی می‌نامند.

به کدهای ساخته شده به صورت (n, m) را یک کد بلوکی می‌نامند.

مثال: کد بلوکی $(m+1, m)$ را بسازید که $m \geq 8$

یعنی واژه‌ها از Z_2^8 می‌آیند و میروند به Z_2^9 آنگاه به شکل $T(C)$ در می‌آیند

Subject : Date

وقتی D لستایش پیدا می کند به صورت w درمی آید.

$w \longrightarrow C$

$w = w_1 w_2 \cdots w_8$

$C = w_1 w_2 \cdots w_8 (w_1 + w_2 + \cdots + w_8)$

$w_9 = w_1 + w_2 + w_3 + \cdots + w_8$

این جمع در Z_2 است

$I(C) =$ ۹ بیتی است

$D(I(C)) =$ ۸ بیتی

اگر تعداد ۱ های w فرد باشد آنگاه در c یک ۱ بیشتر از w خواهیم داشت.

$E(11001110) = 110011101 = C$

$E(11000000) = 110000000$

در این حالت میتوان خطاهای متعدد در مخابره پیام پیدا کنیم.

اگر احتمال خطاهای هر بیت p باشد احتمال حداکثر یک خطا برابر است با

$(1-p)^9 + \binom{9}{1}(1-p)^8 \cdot p$

خطا نداریم — ۱ خطا داریم

در این حالت تصحیح یک خطا مشکل است.

اگر $p = 0.001$ احتمال حداکثر یک خطا برابر است با: 0.999964

اگر خطای در این مثال آشکار سازیم و بتوانیم نهادی به فرستنده ارسال کنیم تا مخابره واژه c را

تکرار کند و آن قدر این ارسال مکرر را ادامه دهیم واژه های دریافتی حاوی تعداد زوجی ۱ باشند

©MICRO

Subject Date

در اینصورت احتمال اینکه پیام به طور صحیح دریافت شود برابر است ۰/۹۹۹۹۶۴

اگر تعداد زوجی خطا در هر بایت پیام رخ دهد، در این صورت T(c) به عنوان یک کد واژه صحیح

پذیرفته خواهد شد. و ۸ مولفه اول T(c) به عنوان واژه w پذیرفته می شود.

اگر پیام ۱۱۰۱۰۱۱۰ از طریق کانال (۸ و ۱+۸) مخابره کنیم احتمال مخابره صحیح با $p=0.1$

عبارت است از $(0.999)^8 = 0.992028$. اما به کد بلوکی زوجیت می توان احتمال دریافت

پیام صحیح به ۰/۹۹۹۹۶۴ افزایش داد.

در کانال متقارن معمولی نرخ کدگذاری ۱ است. اما در کانال زوجیت بلوکی (۸ و ۱+۸) برابر

است با $\frac{8}{9}$.

اگر بجای یک واژه ۸ بیتی، ۲۰ واژه ۸ بیتی بفرستیم، در حالت معمولی احتمال مخابره صحیح است

$(0.999)^{160} = 0.852076$

اما اگر به صورت بلوکی (۸ و ۱+۸) بفرستیم، آنگاه ۲۰ واژه ۹ بیتی میفرستیم با $p=0.001$ چون

هر واژه ۹ بیتی به طور صحیح با احتمال ۰/۹۹۹۹۶۴ فرستاده می شود. در مجموع احتمال $(0.999964)^{20}$

فرستاده شدن صحیح ۲۰ واژه از طریق کانال زوجیت است که برابر است با ۰/۹۹۲۸۰

MICRO

صفحه

Subject : .... Date ....

مثال ۱: $(n=3m, m)$ که $c \in Z_2^{3m}$ و $w \in Z_2^{m}$. (چگونگی ساختن کد از Z_2^{m} به Z_2^{3m})

براساس کد تکرار سه گانی $(3m, m)$ این واژه را می سازیم

$w = w_1 w_2 \dots w_m$

$c = w_1 \dots w_m, w_1 \dots w_m, w_1 \dots w_m$

$c \longrightarrow T(c) \in Z_2^{3m}$

$D(T(c)) \longrightarrow Z_2^{m}$

ضابطه D را به صورت زیر تعریف می کنیم:

حرف

$1 \;,\; m+1 \;,\; 2m+1$

$2 \;,\; m+2 \;,\; 2m+2$

$3 \;,\; m+3 \;,\; 2m+3$

$\vdots \qquad \vdots \qquad \vdots$

$m \;,\; m+m=2m \;,\; 2m+m=3m$

در هر یک از این سه تایی ها اگر اکثریت با ۱ بود در $D(T(c))$ به جای i ام ۱ می گذاریم

اگر اکثریت با صفر بود در $D(T(c))$ به جای i ام صفر می گذاریم

به عنوان مثال در همین مثال اگر $m=8$ و $n=3\times 8=24$ داریم:

$w = 11011001$

$c = 11011001, 11011001, 11011001$

$T(c) = 10110011, 11010101, 10011011$

(اولی هر ۳ با هم و بعد دومی هر ۳ با هم و بعد به همین ترتیب)

$D(T(c)) = 10010011$

Subject	Date

در این کدبندی (m و km) k همواره خواسته زمانی که بخواهید کدگشایی را از طریق اکثریت بیت باز کنید.

براساس مثال بالا بین خطا داریم که خطا در جای دوم، پنجم و هفتم پیش آمده است. اگر خطا از دو

یا بیشتر از دو باشد به طوری که خطای دوم، هشت یا شانزده خانه بعد از خطای اول باشد رخ ندهد.

به عبارت دیگر اگر هر یک از بیت های پیام اصلی دو بار یا بیشتر مجاوره غلط نشود می توان خطاها

را بیوا کرد. احتمال کدگشایی صحیح برای هر بیت برابر است با $p = 0.001$

$$(0.999)^3 + \binom{3}{1}(0.999)^2(0.001) = 0.999997$$

بنابراین دریافت و کدگشایی صحیح یک پیام ۸ بیتی به طریق بالا برابر است با

$$(0.999997)^8 = 0.999976$$

تمرینات کد بخش اول ۱۶_۴ ص ۱۰۱۷ (سری تمرینات ۴_۱)

حل تمرینات ۴_۱۶ ص ۱۰۱۷

۱. $C \subseteq Z_2^7$، c واژه کد، e خطاها، r واژه دریافتی: موارد خواسته شده را بدست آورید.

الف) $c = 1010110$ $\quad e = c + r = 0010101$

$r = 1011111$

$e = 0010101$

ب) $c = 1010110$ $\quad r = 1111011$

$e = 0101101$

MICRO

Subject :   Date ....

۲- $p = 0.05$ ، اگر $C = 011011101$ مخابره می‌شود

الف) احتمال اینکه واژه دریافتی $r = 011111101$ چقدر است: چون فقط یک خطا در چهارمین بیت داریم و مشخص است خطا کجا بوده بنابراین ترکیب $\binom{9}{1}$ نیست و فقط داریم:

$$(1-0.05)^8 \times (0.05)^1$$

ب) احتمال رخ دادن یک خطای منفرد چقدر است؟ $\binom{9}{1}(1-0.05)^8 \times (0.05)^1$

" " " دو خطا چقدر است؟

$$\binom{9}{2}(1-0.05)^7 \times (0.05)^2$$

ج) احتمال اینکه سه خطا رخ دهد که هیچ دوتای آن ها متوالی نباشند؟

هفتم پنجم اول — ششم چهارم اول — پنجم سوم اول

هشتم پنجم اول — هفتم چهارم اول — ششم سوم اول

نهم پنجم اول — هشتم چهارم اول — هفتم سوم اول

نهم چهارم اول — هشتم سوم اول

نهم سوم اول

نهم هفتم اول — هشتم ششم اول

نهم ششم اول

هشتم ششم دوم — هفتم پنجم دوم — ششم چهارم دوم

نهم " دوم — هشتم " " — هفتم " "

نهم " " — هشتم " "

نهم " "

MICRO

نهم هفتم دوم

Subject   Date

هشتم ششم سوم   هفتم پنجم سوم
نهم // سوم   هشتم // //
                    نهم // //

نهم هفتم سوم

نهم هفتم پنجم نهم هفتم ...   هشتم ششم چهارم
                    نهم // //
هفتم درست ۶   پنجم ۳۵   چهارم
احتمال خطا ۳

$\frac{3}{4} \times (1-0/5)^{6} \times (0/5)^{3}$

۲. $(9,3)$ ، $E: Z_2^3 \longrightarrow Z_2^9$ ، $D: Z_2^9 \longrightarrow Z_2^3$ کدگشایی

الف) واژه‌های دریافتی را کدگشایی کنید.

$C_1 = 111\,101\,100$

بیشترین تا ۳ نقطه خطا (در نظر می‌گیریم)

$w_1 = 101\,((2t-1)m, m)$ $k, m+k, 2m+k, \ldots, (2t+k)$

ب) سه واژه دریافتی ۳ که $D(r) = 000$ $m = 3$

011   100   000
111   000   000
000   111   000
000   000   111
000   000   000

پ) به ازای هر w تعداد $|D^{-1}(w)|$ را پیدا کنید
یعنی (چه تعداد واژه دریافتی ۳ داریم که $D(r) = w$)

$w = w_1 w_2 w_3$ $w_1 w_1 w_1$
$w_1 \bar{w}_1 w_1$ ($w_1 = 0 \longrightarrow \bar{w}_1 = 1$ و برعکس)
$\bar{w}_1 w_1 w_1$
$w_1 w_1 \bar{w}_1$

ص ۱۲

۵ خطا ۴ و ۴ انتظار، ۲ تصحیح | ۲ خطا ۲ و ۲ انتظار بدون تصحیح | ۳ خطا ۲ و ۲ انتظار، ۱ تصحیح

Subject: | Date

$4 \times 4 \times 4 = 64$ بنابراین خطاست $|\bar{D}(w)| = 64$

حالت برای w_1 — حالت برای w_2 — حالت برای w_3

۴- تابع کدگذاری $(5m, m)$ ، $E : Z_2^m \to Z_2^{5m}$ ، $E(w) = wwwww$

کدگشایی D بر قاعده اکثریت عمل می‌کند. با فرض اینکه $p = 0/05$

احتمال کدگشایی صحیح و مخابره نماد صفر؟

$0 = 00 \ldots 0$ (m بار)

$(1 - 0/05)^m + (1 - 0/05)^{m-1} \times (0/05)^1 + (1 - 0/05)^{m-2} \cdot (0/05)^2$

ب) سؤال الف ۲ اشکال دارد.

پ) به ازای $m = 2$ واژه دریافتی ۱۰۰۱۰۱۰۰۱۱۱۰ = ۳ را کدگشایی کنید $m = 2$

یعنی یکبار به ۱ ، ۳ ، ۵ ، ۷ ، ۹ نگاه می‌کنیم و اکثریت ۰ یا ۱ را می‌گذاریم و بار دیگر به ۲ ، ۴ ، ۶ ، ۸ ، ۱۰ نگاه می‌کنیم و اکثریت را قرار می‌دهیم

$w = 01$

ت) $m = 2$ ، همه واژه دریافتی ۲ را چنان بیابید که $D(r) = 00$

00 00 00 0 0 0 0

11 0 0 0 0 0 0 0 0

00 11 00 0 0 0 0

ث) $|\bar{D}^1(w)|$ پیدا کنید $m = 2$ ، $w = w_1 w_2$

$w_1 w_1$

$w_1 w_1$

$w_1 w_1$

$\to 3 \times 3 = 9$

Subject Date

تمرینات کتاب ۵-۱۶ و ۶-۱۶

۱. کلیه واژه‌های دریافتی که با این $S = (101010,1)$ فاصله ۱ دارند را بنویسید

$S(101010,1) = \{111010, 001010, 100010, 101110, 101000, 101011\}$

۲. هر یک از واژه‌های دریافتی را کدگشایی کنید. $E: Z_2^2 \to Z_2^6$

- هر واژه r که در $S(000000,1)$ قرار گرفت: $D(r)=00$
- هر واژه r که در $S(101010,1)$ قرار گرفت: $D(r)=01$

$r = 110101$

چون فاصله‌اش باید با ۲ کلمه باشد با کلمه‌ی ... به $S(010101,1)$ می‌رسیم

یعنی ۷ $\{$ 00 10 01 11

000000

101010

010101

111111

ب) 110000 چون 110000 در هیچ کره‌ای که مرکز آن چهار واژه و به شعاع ۱ وجود ندارد.

$D(110000) = 00$ یا 11 یا 10 یا 01

۳. الف) اگر $x \in Z_2^{10}$ آنگاه اندازه‌ی $|S(x,1)| = ?$

$|S(x,1)| = 11$

$\binom{10}{0} + \binom{10}{1} = 10+1 = 11$

$|S(x,2)| = \binom{10}{2} + \binom{10}{1} + \binom{10}{0}$

$S(x,k) = \binom{10}{k} + \binom{10}{k-1} + \dots + \binom{10}{0}$

صفحه ۱۴

Scanned by CamScanner

Subject : Date

۴: $E: Z_2^5 \to Z_2^{25}$ ، فاصله min = ۹ و بیشترین مقدار k را چنان بیابید که بتوان تا خطای حداکثر k را آشکار کرد؟

min فاصله ۹ است پس میتوان طبق قضیه تا ۸=۱-۹ خطا را آشکار کرد

و تا $4 = \frac{9-1}{2}$ خطا را میتوان تصحیح کرد

۵- فاصله min را بین واژه‌های کد زیر پیدا کنید. $E: Z_2^2 \to Z_2^5$

الف)

$00 \to 00001 = c_1$ $d(c_1, c_2)$ $d(c_2, c_3)$

$01 \to 01010 = c_2$ $d(c_1, c_3)$ $d(c_2, c_4)$

$10 \to 10100 = c_3$ $d(c_1, c_4)$ $d(c_3, c_4)$

$11 \to 111111 = c_4$

اگر فاصله min زوج باشد (۲k) بنابراین ۲k-۱ را آشکار و $\frac{2k-1}{2}$ را تصحیح می‌کنیم (ادامه دارد)

۶. به کمک ماتریس زوجیت H واژه‌های دریافتی زیر را کدگشایی کنید

الف) ۱۱۱۱۰۱

$$H = \begin{bmatrix} 10 & 11 & 00 \\ 11 & 00 & 10 \\ 01 & 10 & 01 \end{bmatrix} \quad H \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \to w = (11011)$$

۷. تابع کدگذاری $E: Z_2^2 \to Z_2^5$ با ماتریس مولد $G = \begin{bmatrix} 10 & 11 & 0 \\ 01 & 01 & 1 \end{bmatrix}$ تعریف می‌شود

(*) دقت جبری ندارد باید همه حالت های ممکن را بنویسیم

MICRO®

صفحه ۱۵

Subject Date

همه‌ی واژه‌های کد را تعیین کنید.

00 → $C_1 = G(00) = 00000$

10 → $C_2 = G(10) = 10110$

01 → $C_3 = G(01) = 01011$

11 → $C_4 = G(11) = 11101$

* درباره‌ی تصحیح خطاهای کد چه می‌توان گفت؟

چون d_{min} فاصله بین واژه‌های دریافتی ۳ است می‌توان یک خطا را تصحیح و دو خطا را آشکار کرد.

* ماتریس زوجیت H را پیدا کنید.

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}_{2\times 5}$$ (I | A)

$$G = (I_2 \mid A)$$

$$H = (B \mid I_3)$$

$$E(w) = (w_1, w_2)\, G = (w_1, w_2, w_3, w_1+w_2, w_2)$$

w_3 w_4 w_5

$$w_3 + w_2 = 0$$
$$w_4 + w_1 + w_2 = 0$$
$$w_5 + w_2 = 0$$

$$\begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}_{3\times 5} \begin{pmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \\ w_5 \end{pmatrix}_{(5\times 1)} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}_{3\times 1}$$

H ماتریس زوجیت است.

MICRO

۱۶

Subject :

Date

ب) با استفاده زوجیت H واژه‌های دریافتی زیر را کدگشایی کنید.

$$H\begin{pmatrix}1\\1\\1\\0\\1\end{pmatrix}=\begin{pmatrix}0\\0\\0\end{pmatrix}$$

واژه پنج : 11101

MICRO

Subject : Date

بخش سوم: کدهمینگ (کدهمینگ)

اصول کلی توانایی طرح‌های کدگذاری در آشکارسازی و تصحیح خطاها را در این بخش مطالعه و بررسی می‌کنیم کار را با مثال آغاز می‌کنیم.

مثال: $C \in Z_2^4$ و مجموعه کدها از Z_2^4 بیابید.

فرض کنیم $c_1 = 0111$ ، $c_2 = 1111$ دو عضو در مجموعه کدهای C در Z_2^4 باشند

در اینجا هم فرستنده و هم گیرنده عناصر C را می‌شناسند بنابراین اگر فرستنده c_1 را ارسال کند

گیرنده واژه $c_2 = 1111 = T(c_1)$ را دریافت کند.

ممکن است به خطا بگوید این درست است و تصمیم می‌گیرد c_2 را قبول کند و این باعث

خطا می‌شود. اگرچه یک بیت اختلاف خبر است اما ممکن است در بعضی c_1 و c_2 اختلاف

خاصی داشته باشند.

حال سؤال است که چه بکنیم که این ناخوشایندی خبر نشود و خطا کمتر شود و تصحیح صورت گیرد

یا حداقل اشکال را متوجه بشویم.

تعریف: اگر $x = x_1 x_2 x_3 \dots x_n \in Z_2^n$ که x یک عدد صحیح مثبت است. وزن x با $W_t(x)$

نشان داده می‌شود عبارت است از تعداد 1 های در دنباله x.

MICRO

Subject Date

تعریف: اگر x و y دو عضو در Z_2^n باشند $d(x,y)$ که فاصله بین x و y نامیده می‌شود عبارتست از تعداد مؤلفه‌های x_i و y_i که $x_i \neq y_i$ ، $1 \leq i \leq n$

$$d(x,y) = \sum_{i=1}^{n} d(x_i,y_i)$$

به عنوان مثال: در Z_2^5 :

$$x = 11001 \quad , \quad y = 01110$$

$w_t(x)$ ← تعداد ۱های موجود در x است

$w_t(y)$ ← تعداد ۱های موجود در y است

$$w_t(x) = 3$$
$$w_t(y) = 3$$

$d(x,y)$ جاهایی که x و y با هم اختلاف دارند یعنی اولی در یکی ۱ و در دیگری ۰ است این همان اختلاف است

$$d(x,y) = 4$$

$$x+y = 10111 \Rightarrow w_t(x+y) = 4$$
$$w_t(x,y) = d(x,y)$$

لم: به ازای هر x و y در Z_2^n :

$$w_t(x+y) \leq w_t(x) + w_t(y)$$

اثبات: اگر مؤلفه i ام $x+y$ یعنی x_i+y_i ۱ باشد آنگاه دو حالت وجود دارد:

(۱) $x_i = 1$ و $y_i = 0$ یا (۲) $x_i = 0$ و $y_i = 1$

بنابراین به ازای هر مؤلفه ۱ در سمت چپ در $x+y$ حداقل یک ۱ یا دو ۱ در سمت راست داریم.

اگر مؤلفه i ام $x+y$ یعنی x_i+y_i برابر ۰ باشد دو حالت وجود دارد $x_i = 0$ و $y_i = 0$ یا $x_i = y_i = 1$ در این حالت نیز در سمت راست ۰ یا دو تا ۱ داریم.

پس در هر دو حالت تعداد ۱های سمت راست بزرگتر مساوی تعداد ۱های سمت چپ است.

این حکم را ثابت می‌کند.

Subject : Date

□ حال می خواهیم نشان بدهیم که فاصله d در Z_2^n یک متریک است. این قضیه زیر را داریم:

قضیه: تابع فاصله d روی $Z_2^n \times Z_2^n$ که به صورت زیر تعریف می شود

$d(x,y) = \sum_{i=1}^{n} (x_i + y_i)$ برای هر سه عضو دلخواه x, y, z در Z_2^n.

الف) $d(x,y) \geq 0$

ب) $d(x,y) = 0 \iff x = y$ ب) $d(x,y) = d(y,x)$

ت) $d(x,z) \leq d(x,y) + d(y,z)$

اثبات:

الف) طبق تعریف واضح است

ب) اگر $x = y$ واضح است هر دو مؤلفه x_i و y_i برابر هستند پس $x_i + y_i = 0$

و لذا $d(x,y) = \sum_{i=1}^{n} x_i + y_i = 0$.

برعکس نیز واضح است اگر $\sum (x_i + y_i) = 0$ باشد پس تا $x_i + y_i = 0$ هستند بنابراین

این یعنی هر مؤلفه y_i و x_i یا 1 هستند یا 0 که $y_i = x_i$ و $x = y$ است.

پ) اثبات واضح است.

Subject Date

ت: می‌دانیم $w_t(x+y) = d(y,y) = 0$

$$d(x,z) = w_t(x+z) = w_t(\overbrace{x+y}^{x} + \overbrace{y+z}^{y}) \leq w_t(x+y) + w_t(y+z)$$

طبق نامساوی مثلث

نکته: هرگاه سؤال بود که متریک همینگ را تعریف کنید باید قضیه فوق با ۴ شرط را تعریف کنیم.
(هم صورت قضیه و هم ۴ شرط)

در هر فضای متریک می‌توان گوی به مرکز x و به شعاع r را تعریف کرد.

کره‌ای

تعریف: برازای هر $n,k \in Z^+$ و $x \in Z_2^n$ کره‌ای به مرکز x و به شعاع k را به صورت زیر تعریف می‌شود.

$$S(x,k) = \{ y \in Z_2^n \mid d(x,y) \leq k \}$$

مرکز، شعاع

به عنوان مثال: فرض کنید $n=3$ باشد. $k=2$ و $x=110 \in Z_2^3$

مانند می‌توند برجایی که (ها) هم (متفاوت) دارند.

$$S(x,y) = \{ y \in Z_2^3 \mid d(x,y) \leq 2 \}$$

$$= \{ 101, 111, 000, 011, 100, 010, 110 \}$$

$\binom{3}{2}=3$ $\binom{3}{1}=3$ $\binom{3}{0}=1$

مثال: $x \in Z_2^4$, $x=1111$, $k=2$ (وقتی شعاع ۲ باید اضافه‌ها را بنویسیم کما میا یا ۲ است.

$$S(x,2) = \{ 1111, 0111, 1011, 1101, 1110, 0011, 0101, 0110, 1001, 1010, 1100 \}$$

$\binom{4}{0}=1$ $\binom{4}{1}=4$ $\binom{4}{2}=6$

MICRO

صد ۲۱

Subject : Date

قضیه: فرض کنیم $E: w \to c$ تابع کدگذاری باشد که در آن $w \subseteq Z_2^m$ مجموعه همه پیام‌هاست و $E(w) = C \subseteq Z_2^n$ مجموعه واژه‌های کد $m < n$.

برای $k \in Z^+$ می‌توان خطاهای مخابره دارای وزن حداکثر k را آشکارسازی کرد اگر و تنها اگر min فاصله بین واژه‌های کد حداقل $k+1$ باشد.

اثبات: مجموعه‌ی واژه‌های کد (C) هم برای فرستنده و هم برای گیرنده معلوم است بنابراین اگر $w \in W$ یک پیام (برای ارسال) و $c = E(w)$ پیام مخابره شده باشد. فرض کنیم $c + T(c) = r$. با توجه به فرض $d(c_i, c_j) \geq k+1$ آنگاه مخابره c می‌تواند به k خطا $c_i \in C$ منجر شود که در این حالت r در C نخواهد بود پس همه خطاها مثل e که $w_H(e) \leq k$ را می‌توان آشکارسازی کرد.

برعکس: اگر بتوان تا k خطا را آشکارسازی کرد. فرض کنیم c_1, c_2 دو واژه کد باشند و فرض خلف کنیم که $d(c_1, c_2) < k+1$ به عبارت دیگر $d(c_1, c_2) \leq k$. که در اینصورت $c_2 = c_1 + e$ که $w_H(e) \leq k$. در این حالت اگر c_1 را ارسال کنیم و c_2 را دریافت کنیم چون اختلاف k است آنگاه احساس می‌کنیم که c_2 همان c_1 است و این آشکارسازی خطا تا حداکثر k را از بین می‌برد پس تناقض داریم.

MICRO

Subject

کی شرط لازم و کافی برای اینکه بتوانیم k خطا را اشکار کنیم؟

حضیه: فرض کنیم E و C و w همان داده‌های حضیه‌ی باشند $k \in Z^+$ ، $E : w \to C$

می‌توان کدگشایی $D : Z_2^n \to w$ چنان بسازیم که همه خطا مجموعه با وزن حداکثر k را تصحیح کند اگر و تنها اگر min فاصله بین دو واژه کد (اعضای C) حداقل $2k+1$ باشد

اگر لغت حین خطا را می‌توانیم آشکار کنیم باید min فاصله بین دو واژه کد $k+1$ باشد
اگر لغت حین خطا را می‌توانیم تصحیح کنیم باید min فاصله بین دو واژه کد $2k+1$ باشد

□ چند نکته در رابطه با اثبات حضیه فوق:

- اگر $c \in C$ یک کد واژه باشد کره‌ای به مرکز c و به شعاع k $S(c,k)=k$

تابع $D : Z_2^n \to w$ به صورت زیر تعریف کنید:

اگر $r \in Z_2^n$ و اگر به ازای یک کد واژه c ، $r \in S(c,k)$ در اینصورت می‌توان گفت که $D(r)=w$ (حداقل فاصله بین هر دو واژه در C ، $(2k+1)$ است. که در آن

$$E(w)=c \quad , \quad T(c)=r \quad , \quad D(r)=D(T(E(w)))=w$$

یعنی r واژه‌ای است که خیلی نزدیک به c است.

اما در این حالت اگر به ازای هر r در C ، $r \notin S(c,k)$ در این حالت $D(r)=w$ که w به محض انتخاب شدن ثابت نگه داشته می‌شود. تنها مسئله‌ای که در این نکته

Subject :

Date

ممکن است پیش بیاید اینکه D تابع نباشد و این وقتی ممکن است اتفاق بیافتد که

$r \in S(c_1, k)$ ، $r \in S(c_2, k)$

مثال: $w = Z_2^2$ ، $E : w \to Z_2^6$ ، $E(00) = 000000 \to c_1$

$E(10) = 101010 \to c_2$

$E(01) = 010101 \to c_3$

$E(11) = 111111 \to c_4$

$C = \{000000, 101010, 010101, 111111\}$

$d(c_i, c_j) \geq 3$ ، $2k+1 = 2 \cdot 1 + 1 = 3$

۲ - ۱ = ۱ خطا را تشخیص میدهد

۱ خطا را تصحیح کند.

$D : Z_2^6 \to w$

$S(c_1, 1), S(c_2, 1), S(c_3, 1), S(c_4, 1) \to Exv = 28$

تعداد بیت‌هایی که اختلاف دارند را بنویسیم

$S(c_1, 1) = \{c_1 و 100000, 010000, 001000, 000100, 000010, 000001\}$

هر یک از چهارگروه ۷ عضو دارند اگر دو بیتی از ۲۸ واژه کد در این چهارگروه باشد.

اگر $x \in (01, 10, 11)$ ، $x \in S(c_1, 1)$

$D(x) = 01$ ، $D(x) = 00$

اگر x غیر این ۲۸ واژه در Z_2^6 باشد یعنی آن ۳۶ واژه دیگر $D(x) = w_0$

MICRO

صد ۲۴

Subject Date

اما در مورد آشکارسازی خطا، اگر $c = 10101$ ، $T(c) = 11101 = 2$ ،

امتیاز این برنامه (8) است.

۲. دوازده کد C بیت.

اگر $T(c) = 111111$ در این حالت نمی‌توان خطا را پیدا کرد چون فقط می‌کنیم

$w = 11$ است.

بررسی زوجیت و ماتریس های مولد:

می خواهیم توابع کدگذاری و کدگشایی با ماتریس هایی که داده شده اند و درایه های آن در Z_2 است بررسی کنیم.

مثال: فرض $G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}_{3\times 6}$ درایه های این ماتریس در Z_2 هستند. سه ستون

اول ماتریس همانی است. اگر ماتریس 3×3 که از سه ستون آخر بدست می آید A بنامیم

و ماتریس 3×3 اول را همانی I بنامیم می توان $G = [I_3 | A]$ ماتریس مولد.

با استفاده از G تابع کدگذاری را به صورت زیر تعریف می کنیم:

$E : Z_2^3 \longrightarrow Z_2^6$

$E(w) = wG$

$E(110) = (110)\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} = (110101)$

$(1\times 3)(3\times 6) = 1\times 6$

A

Subject :   Date

$E(010) = (010011)$

$Z_2^3 = 2^3 = 8$ واژه کد دارد $= \{000, 001, 010, 100, 110, 101, 011, 111\}$ ($w_1, w_2, w_3, w_4, w_5, w_6, w_7, w_8$)

با ضرب هر یک از $w_1, w_2, \ldots, w_8$ در G، ۸ کد واژه در Z_2^6 که آن‌ها را در C قرار می‌دهیم.

$C = \{000000, 100110, 010011, \ldots, 111000\}$

اگر ماتریس اصلی G را بر ماتریس که ۳ سطر اول همان همانی است و سه سطر بعدی
را بنویسیم آن را با ضرب abc در ۱۱۱ بدست آوریم (به عنوان مثال)

$\underbrace{111}_{w} A = (abc) \Rightarrow 111G = (111abc)$

با توجه به ماتریس مولد G و $w = w_1 w_2 w_3$ ، $E(w) = (w_1 w_2 w_3 (w_1+w_3)(w_1+w_2)(w_2+w_3))$

$w_4 = w_1 + w_3 \overset{\text{چون}}{\Longrightarrow} w_1 + w_3 + w_4 = 0$

$w_5 = w_1 + w_2 \overset{\text{چون}}{\Longrightarrow} w_1 + w_2 + w_5 = 0$

$w_6 = w_2 + w_3 \overset{\text{چون}}{\Longrightarrow} w_2 + w_3 + w_6 = 0$

چون $w_i = -w_i$ ، $w_i + w_i = 0$

$w_1 + 0w_2 + w_3 + w_4 + 0w_5 + 0w_6 = 0$

$w_1 + w_2 + 0w_3 + 0w_4 + w_5 + 0w_6 = 0$

$0w_1 + w_2 + w_3 + 0w_4 + 0w_5 + w_6 = 0$

MICRO

$$H_{3\times6} \cdot \begin{pmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \\ w_5 \\ w_6 \end{pmatrix}_{6\times1} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}_{3\times1}$$

$$H = \begin{bmatrix} 1&0&1&1&0&0 \\ 1&1&0&0&1&0 \\ 0&1&1&0&0&1 \end{bmatrix} \begin{bmatrix} w_1 \\ \vdots \\ w_6 \end{bmatrix}$$

در H سه ستون آخر ماتریس همانی I_3 است سه ستون اول را B بنامید

بنابراین $H = [B | I_3]$ که $B = A^t$

در اینجا نیز مانند قبل خطاهای منفرد (تک خطا) را می‌توان تصحیح کرد. و خطاهای دوگانه را می‌توان تشخیص داد. (آشکار کرد)

اگر $T(C) = r$ ، $r^t = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$ و $H.r^t = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$ ، r واژه کد نیست.

پس می‌توان حداقل یک خطا را آشکار سازیم $d(101100, r) = 1$ به ازای هر یک از عناصر دیگر $c \in C$ ، $d(r,c) \geq 2$ اگر $r = c + e = 101101 = 101100 + 000001$ می‌توان تشخیص داد. خطای مخابره دارای وزن 1 در مؤلفه سوم رخ داده است. آیا این یک اتفاق است یا نه به مؤلفه‌های دیگر بستگی دارد؟