دانشگاه صنعتی خواجه نصیرالدین طوسی

بسم الله الرحمن الرحیم

مقدمه‌ای بر تئوری کدگذاری

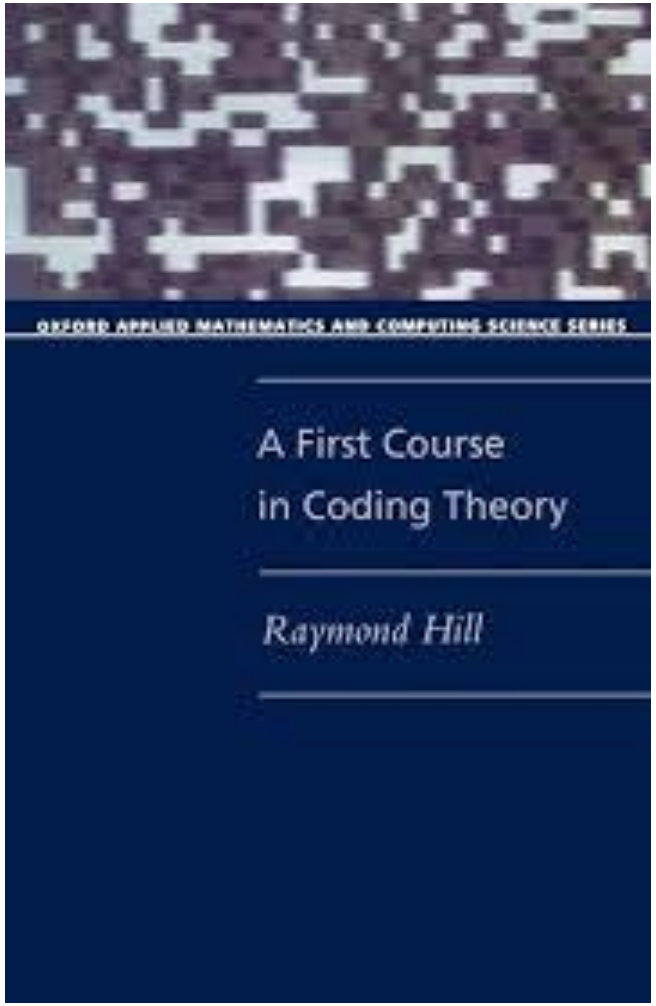
سیده سعیده قاضی

مهر ۱۴۰۴

دانشگاه صنعتی خواجه نصیرالدین طوسی

ارزشیابی درس

- میان‌ترم ۴ نمره
- پروژه (سمینار) ۶ نمره
- پایان‌ترم ۱۰ نمره



ghazi.saeedeh@gmail.com

تاریخ امتحان میان‌ترم
۱۴۰۴/۰۹/۰۸

دانشگاه صنعتی خواجه نصیرالدین طوسی

فصل اول: مقدمه‌ای بر کدهای تصحیح و خطا

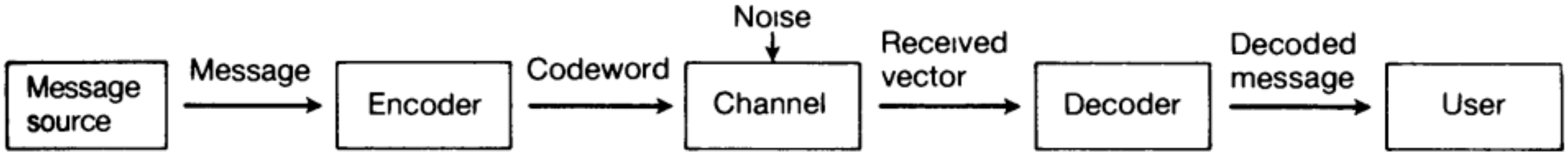
تصحیح خطاهای به وجود آمده ناشی از کانال ارتباطی نویزی

مثال: ارسال دنباله‌ای از ۰ و ۱ ها از طریق یک کانال نویزی

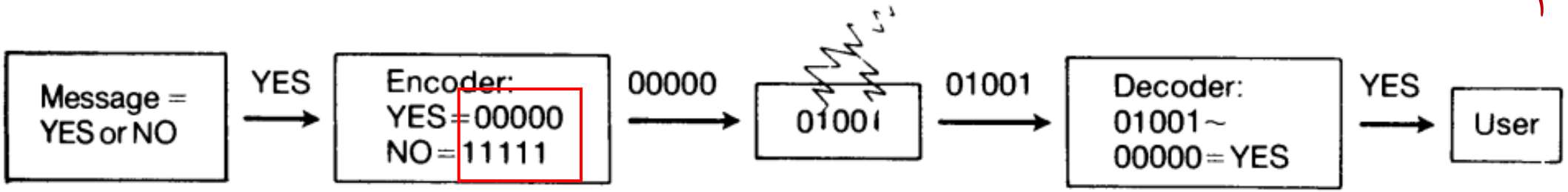
متفاوت بودن اطلاعات دریافت با ارسال شده

کد کردن اطلاعات با اضافه کردن داده (اضافه کردن مقدار خاص اضافی) به پیام
در صورتی که خطا رخ داده باشد، بتوانیم پیام اصلی را بدست آوریم

دانشگاه صنعتی خواجه نصیرالدین طوسی



مثال ۱



کدکلمه

در این مثال دو خطا رخ داده است

کد گشا بردار دریافت شده ۰۱۰۰۱ را به **نزدیک ترین کد کلمه** یعنی ۰۰۰۰۰ کدگشایی کرده است.

کد q-تایی مجموعه‌ای از دنباله‌ها است که هر علامت آن از مجموعه F_q انتخاب می‌شود. (شامل q عنصر متفاوت) الفبا

هر عنصر این مجموعه یک بردار یا کلمه نامیده می‌شود.

$$F_q = \{\lambda_1, \lambda_2, \ldots, \lambda_q\}$$

فاصله همینگ

فاصله همینگ برای دو رشته با طول مساوی، برابر تعداد مکان‌هایی است که سمبل‌های متناظر متفاوت هستند. به عبارت دیگر، کمترین تعداد جایگزینی هایی است که یک رشته به یک رشته دیگر تغییرپیدا کند، یا تعداد خطاهایی که یک رشته به رشته دیگر تبدیل گردد.

فاصله همینگ بین ۱۰۱۱۱۰۱ و ۱۰۰۱۰۰۱ برابر است با ۲
(چون فقط در دو موقعیت دوم و پنجم متفاوت‌اند)

دانشگاه صنعتی خواجه نصیرالدین طوسی

The Hamming distance is a legitimate distance function, or metric, since it satisfies the three conditions:

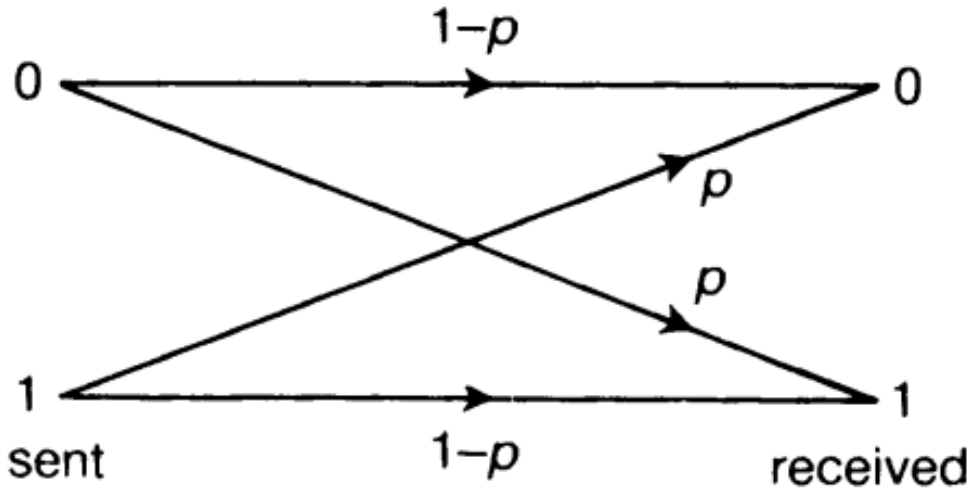
(i) $d(\mathbf{x}, \mathbf{y}) = 0$ if and only if $\mathbf{x} = \mathbf{y}$.
(ii) $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$ for all $\mathbf{x}, \mathbf{y} \in (F_q)^n$.
(iii) $d(\mathbf{x}, \mathbf{y}) \leqslant d(\mathbf{x}, \mathbf{z}) + d(\mathbf{z}, \mathbf{y})$ for all $\mathbf{x}, \mathbf{y}, \mathbf{z} \in (F_q)^n$.

فاصله همینگ همواره مناسب ترین نیست

$(F_{10})^3 \quad d(428, 438) = d(428, 468)$

کانال متقارن q-تایی

احتمال خطای کانال p می باشد.



فرض کنیم کانال ارتباطی یک کانال متقارن دودویی باشد، اگر یک کدکلمه به طول n از طریق این کانال منتقل شود، احتمال اینکه هیچ خطایی رخ ندهد برابر است با:

$$(1-p)^n$$

دانشگاه صنعتی خواجه نصیرالدین طوسی

احتمال بروز خطا در یک محل مشخص:

$$p(1-p)^{n-1}$$

احتمال بروز خطا در i محل مشخص:

$$p^{i}(1-p)^{n-i}$$

Example 1.8 Consider the binary repetition code of length 3

$$C = \begin{cases} 000 \\ 111 \end{cases}.$$

Suppose the codeword 000 is transmitted. Then the received vectors which will be decoded as 000 are 000, 100, 010 and 001. Thus the probability that the received vector is decoded as the transmitted codeword 000 is

$$(1-p)^3 + 3p(1-p)^2 = (1-p)^2(1+2p).$$

دانشگاه صنعتی خواجه نصیرالدین طوسی

An important parameter of a code C, giving a measure of how good it is at error-correcting, is the *minimum distance*, denoted $d(C)$, which is defined to be the smallest of the distances between distinct codewords. That is,

$$d(C) = \min \{d(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}\}.$$

For example, it is easily checked that for the codes of Example 1.5, $d(C_1) = 1$, $d(C_2) = 2$ and $d(C_3) = 3$.

Theorem 1.9 (i) A code C can detect up to s errors in any codeword if $d(C) \geqslant s + 1$.

(ii) A code C can correct up to t errors in any codeword if $d(C) \geqslant 2t + 1$.

دانشگاه صنعتی خواجه نصیرالدین طوسی

فرض کنید کد تکرار باینری با طول ۵ برای یک کانال متقارن باینری که احتمال خطای سمبل آن p است، به کار گرفته می‌شود. نشان دهید که احتمال خطای کلمه برای این کد برابر است با:

$$10p^3 - 15p^4 + 6p^5$$

یک کد خوب (n,M,d) باید طول n کوچکی داشته باشد (برای انتقال سریع پیام‌ها)، مقدار M بزرگی داشته باشد (تا بتوان طیف گسترده‌ای از پیام‌ها را منتقل کرد) و فاصله d بزرگی داشته باشد (تا بتوان خطاهای زیادی را تصحیح کرد). این اهداف با یکدیگر در تضاد هستند و موضوعی که معمولاً به آن «مسئله اصلی نظریه کدگذاری» گفته می‌شود، این است که یکی از پارامترهای n,M,d را با داشتن مقادیر دو پارامتر دیگر بهینه کنیم.

یک کد(n,M,d) یعنی:

- طول کلمه‌های کد = n
- تعداد کلمه‌های کد = M
- حداقل فاصله بین کلمات کد = d
- اگر بگوییم q-ary یعنی کلمات از حروف یک الفبای q-تایی ساخته شدن (مثلاً باینری یعنی $q=2$)

حالا $A_q(n,d)$ یک تابع/نماد هست که می‌گوید:

بیشترین تعداد کلمه (یعنی بزرگترین M) که می‌تواند برای یک کد با طولn، حداقل فاصله d و الفبای q-تایی وجود داشته باشد.

دانشگاه صنعتی خواجه نصیرالدین طوسی

فرض کنید $q=2$ (یعنی کد باینری باشد، $n=3$، و $d=2$.
سؤال: بیشترین تعداد کلمه کد (M) که می‌توانیم داشته باشیم چند است؟

یکی از جواب‌ها می‌تواند باشد: $\{000, 111\} \rightarrow$ اینجا $M = 2$.
نمی‌توانیم M را بزرگ‌تر کنیم بدون اینکه شرط $d=2$ بشکند.
پس در این حالت:

$$A_2(3, 2) = 2$$

Theorem 2.1 (i) $A_q(n, 1) = q^n$. (ii) $A_q(n, n) = q$.

هم ارزی کدها

دانشگاه صنعتی خواجه نصیرالدین طوسی

دو کد q-تایی را **معادل** می‌نامیم اگر یکی را بتوان با ترکیبی از عملیات زیر از دیگری به‌دست آورد:

(A) جابه‌جایی مکان‌های کد (یعنی تغییر ترتیب جایگاه‌های یک کلمه کد).
(B)جابه‌جایی نمادهایی که در یک مکان ثابت ظاهر می‌شوند (یعنی بازبرچسب‌گذاری حروف در یک ستون مشخص).

اگر کد را به صورت یک ماتریس $M \times n$ نمایش دهیم که هر سطر آن یک کلمه کد است:
عمل نوع A جابه‌جایی ستون‌ها (یعنی عوض کردن ترتیب جایگاه‌ها).
عمل نوع B تغییر نام سمبل‌های یک ستون (مثلاً در یک ستون، همه صفرها را ۱ کنیم و همه ۱ها را صفر کنیم).

واضح است که فاصله‌های بین کلمات کد با این نوع عملیات (جابه‌جایی ستون‌ها یا جابه‌جایی نمادها در یک ستون) تغییر نمی‌کنند.

بنابراین کدهای معادل، **پارامترهای یکسانی** (n,M,d) خواهند داشت و همان تعداد خطا را می‌توانند تصحیح کنند.
در واقع، اگر فرض کنیم کانال **متقارن** q**-تایی** باشد، عملکرد کدهای معادل از نظر **احتمال تصحیح خطا** کاملاً یکسان خواهد بود.

دانشگاه صنعتی خواجه نصیرالدین طوسی

$$C_3 = \begin{cases} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1. \end{cases} \quad \overset{?}{\longleftrightarrow} \quad C = \begin{cases} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{cases}$$

$$\begin{pmatrix} 0 & 1 \\ \downarrow & \downarrow \\ 1 & 0 \end{pmatrix}$$

جایگشت را روی نمادهای موجود در موقعیت سوم C اعمال کنید و سپس موقعیت‌های ۲ و ۴ را با هم جابجا کنید.

دانشگاه صنعتی خواجه نصیرالدین طوسی

$$C = \begin{cases} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{cases} \overset{?}{\Longleftrightarrow} \begin{cases} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 2 & 2 & 2 \end{cases}.$$

Lemma 2.3 Any q-ary (n, M, d)-code over an alphabet $\{0, 1, \ldots, q-1\}$ is equivalent to an (n, M, d)-code which contains the all-zero vector $\mathbf{0} = 0\,0 \cdots 0$.

این لم میگوید: با اعمال عملیات **معادل بودن** (یعنی جابه‌جا کردن ستون‌ها یا تغییر برچسب نمادها در هر ستون) همیشه می‌توانیم آن کد رو به شکلی بازنویسی کنیم که بردار همه صفرها هم جزو کد باشد.

مثال: فرض کنید کد زیر را داریم (روی الفبای باینری، $q = 2$):

$$C = \{111, 010\}$$

بردار 000 داخل کد نیست.

یکی از کلمات کد را (مثلاً اولین کلمه) به بردار صفر تبدیل کنیم.

کد جدید برابر است با:

$$C' = \{101, 000\}$$

حالا بردار همه صفرها 000 داخل کد هست.
طول کد، تعداد کلمات و حداقل فاصله تغییری نکرد.

دانشگاه صنعتی خواجه نصیرالدین طوسی

Taking F_2 to be the set $\{0, 1\}$, we define two operations on $(F_2)^n$. Let $\mathbf{x} = x_1x_2 \cdots x_n$ and $\mathbf{y} = y_1y_2 \cdots y_n$ be two vectors in $(F_2)^n$. Then the *sum* $\mathbf{x} + \mathbf{y}$ is the vector in $(F_2)^n$ defined by

$$\mathbf{x} + \mathbf{y} = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n),$$

while the *intersection* $\mathbf{x} \cap \mathbf{y}$ is the vector in $(F_2)^n$ defined by

$$\mathbf{x} \cap \mathbf{y} = (x_1y_1, x_2y_2, \ldots, x_ny_n).$$

The terms $x_i + y_i$ and x_iy_i are calculated modulo 2 (without carrying); that is, according to the addition and multiplication tables

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

دانشگاه صنعتی خواجه نصیرالدین طوسی

$$11100 + 00111 = 11011$$

$$11100 \cap 00111 = 00100.$$

The *weight* of a vector $\mathbf{x}$ in $(F_2)^n$, denoted $w(\mathbf{x})$, is defined to be the number of 1s appearing in $\mathbf{x}$.

Lemma 2.5 If $\mathbf{x}$ and $\mathbf{y} \in (F_2)^n$, then $d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} + \mathbf{y})$.

Proof The sum $\mathbf{x} + \mathbf{y}$ has a 1 where $\mathbf{x}$ and $\mathbf{y}$ differ and a 0 where $\mathbf{x}$ and $\mathbf{y}$ agree.

دانشگاه صنعتی خواجه نصیرالدین طوسی

Lemma 2.6 If $\mathbf{x}$ and $\mathbf{y} \in (F_2)^n$, then

$$d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x}) + w(\mathbf{y}) - 2w(\mathbf{x} \cap \mathbf{y}).$$

Proof $d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} + \mathbf{y}) =$ (number of 1s in $\mathbf{x}$) + (number of 1s in $\mathbf{y}$) $- 2$(number of positions where both $\mathbf{x}$ and $\mathbf{y}$ have a 1) $= w(\mathbf{x}) + w(\mathbf{y}) - 2w(\mathbf{x} \cap \mathbf{y})$.

دانشگاه صنعتی خواجه نصیرالدین طوسی

Theorem 2.7 Suppose d is odd. Then a binary (n, M, d)-code exists if and only if a binary $(n+1, M, d+1)$-code exists.

فرض کنید d فرد باشد.
در این صورت یک کد باینری $(n، M، d)$وجود دارد اگر و تنها اگر یک کد باینری$(n+1، M، d+1)$وجود داشته باشد.

چرا شرط "فرد بودن d" مهمه؟

چون وقتی یک بیت اضافی به همه کلمات اضافه می‌کنیم (مثلاً همه‌جا یک «بیت توازن» که مجموع بیت‌ها را زوج/فرد کند)، فاصله همینگ بین هر جفت کلمه دقیقاً یک واحد تغییر می‌کند.

- اگر dفرد باشد → تبدیل میشود به $d+1$(که زوج هست).
- اگر dزوج باشد، این ترفند جواب نمی‌دهد.

دانشگاه صنعتی خواجه نصیرالدین طوسی

Corollary 2.8 If d is odd, then $A_2(n+1, d+1) = A_2(n, d)$.
Equivalently, if d is even, then $A_2(n, d) = A_2(n-1, d-1)$.

این قضیه نشان می‌دهد که بین کدهایی که طولشان یک بیت بیشتر است و حداقل فاصله‌شان یک واحد بزرگ‌تر است، یک هم‌ارزی وجود دارد.

وقتی d فرد است:

اگر یک کد با طول n و فاصله d بسازیم، می‌توانیم آن را به کدی با طول $n+1$ و فاصله $d+1$ گسترش بدهیم، بدون اینکه تعداد کلمات تغییر کند.

وقتی d زوج است:

برای پیدا کردن $A(n, d)$، کافی است مقدار $A(n, -1d-1)$ را نگاه کنیم. یعنی اضافه کردن یک بیت به همه کلمات (و تنظیم درست آن) فاصله را یکی زیاد می‌کند و طول را یکی افزایش می‌دهد.

دانشگاه صنعتی خواجه نصیرالدین طوسی

Binomial coefficients

If n and m are integers with $0 \leqslant m \leqslant n$, then the *binomial coefficient* $\binom{n}{m}$, pronounced 'n choose m', is defined by

$$\binom{n}{m} = \frac{n!}{m!\,(n-m)!},$$

where $m! = m(m-1)\cdots 3.2.1$ for $m > 0$
and $\quad 0! = 1$.

(iii) The number of different binary codes with $M = 5$ and $n = 5$ is $\binom{32}{5} = 201\,376$. Of course the number of inequivalent codes will be very much smaller than this.

دانشگاه صنعتی خواجه نصیرالدین طوسی

(iv) The number of binary vectors in $(F_2)^n$ of weight i is $\binom{n}{i}$, this being the number of ways of choosing i positions out of n to have 1s. For example, the vectors in $(F_2)^4$ of weight 2 are 1100, 1010, 1001, 0110, 0101, 0011. The one-to-one correspondence with the list of unordered selections in (i) above should be evident.

Definition. For any vector $\mathbf{u}$ in $(F_q)^n$ and any integer $r \geqslant 0$, the *sphere* of radius r and centre $\mathbf{u}$, denoted $S(\mathbf{u}, r)$, is the set $\{\mathbf{v} \in (F_q)^n \mid d(\mathbf{u}, \mathbf{v}) \leqslant r\}$.

فضای $(F_2)^n$ شامل همه بردارهای دودویی به طول n است.

$d(u,v)$ فاصله بین بردارهای u و v است.

کره $S(u, r)$ همه بردارهایی را شامل می‌شود که با u در حداکثر r بیت تفاوت دارند.

$d(C) \geq 2t + 1$

آنگاه کره‌های با شعاع t که مرکز آن‌ها روی کلمات کد C قرار دارد، **ناهمپوشان** هستند (یعنی هیچ اشتراکی با یکدیگر ندارند).

پس اگر t خطا یا کمتر در یک کلمه کد x رخ دهد، آنگاه بردار دریافتی y ممکن است با مرکز کره $S(x, t)$ متفاوت باشد، اما هرگز نمی‌تواند از آن کره خارج شود. بنابراین در فرایند رمزگشایی نزدیک‌ترین همسایه، y دوباره به x بازگردانده می‌شود.

دانشگاه صنعتی خواجه نصیرالدین طوسی

Lemma 2.15 A sphere of radius r in $(F_q)^n$ $(0 \leqslant r \leqslant n)$ contains exactly

$$\binom{n}{0} + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{r}(q-1)^r$$

vectors.

Theorem 2.16 (The *sphere-packing* or *Hamming bound*) A q-ary $(n, M, 2t+1)$-code satisfies

$$M\left\{\binom{n}{0} + \binom{n}{1}(q-1) + \cdots + \binom{n}{t}(q-1)^t\right\} \leqslant q^n. \qquad (2.17)$$

کران همینگ

در فضای n-بیتی، هر کدواژه مثل یک کره (Ball) از نقاط است که تا فاصله t از آن را شامل می‌شود (یعنی تمام کلمات که تا t خطا با آن فاصله دارند).

کران همینگ می‌گوید که این کره‌ها نباید هم‌پوشانی کنند. چون اگر دو تا از آن‌ها با هم هم‌پوشانی داشته باشند، در هنگام خطا نمی‌توانیم تشخیص دهیم که داده از کدام کدواژه آمده است.

اگر تساوی برقرار باشد به آن **کد کامل** می‌گویند.

$(F_2)^n$ یعنی تمام رشته های باینری به طول n

هر کدواژه یک نقطه در این فضاست.

$(F_2)^3$ مثلا اگر $n=3$ باشد آنگاه داریم:

$2^3 = 8$

000
001
010
011
100
101
110
111

اگر کدی بتواند تا t خطا را تصحیح کند، یعنی هر برداری که حداکثر t بیت اشتباه دارد، باید به طور یکتا به یکی از کدواژه‌ها نسبت داده شود.

کره با شعاع t یعنی مجموعه تمام رشته‌هایی که تا t خطا با آن کدواژه فاصله دارند (از نظر فاصله همینگ).

وقتی می‌گوییم این کره‌ها فضای دودویی را بدون هم‌پوشانی پر می‌کنند، یعنی هیچ نقطه‌ای از فضا بین دو کدواژه تقسیم نشده است. هر رشته دقیقاً به یکی از کدواژه‌ها نزدیک‌تر است این همان **کد کامل Perfect Code** است.