به نام خدا

در جلسه گذشته بحث دیکدینگ کدهای بلوکی خطی را مطرح کردیم و یک روش دیکدینگ براساس سندرم معرفی کردیم. در ادامه می‌خواهیم روش دیگری برای دیکدینگ کدهای بلوکی خطی معرفی کنیم.

دیکدینگ براساس آرایه استاندارد Standard Array

همان طور که قبلاً هم اشاره شد، پایه براساس بیشتر روشهای دیکدینگ بر این است که براساس معیارهایی مانند بیشترین شباهت یا بیشترین احتمال پسین یا کمترین فاصله یا کمترین احتمال خطا، فضای برداری را به نواحی D_1، D_2، ... تقسیم بندی کنند. هر کدام از این ناحیه‌ها، متناظر با ناحیه دیکدینگ یکی از کلمات کد

$\underline{v}_1, \underline{v}_2, \ldots$ است. به این ترتیب با دریافت بردار $\underline{r}$

اگر بردار $\underline{r}$ در ناحیه‌ی دیکدینگ D_i (که متناظر با کلمه کد $\underline{v}_i$ است)

قرار بگیرد، دیکدر $\underline{v}_i$ را به عنوان کلمه کد ارسالی، بازیابی می‌کند.

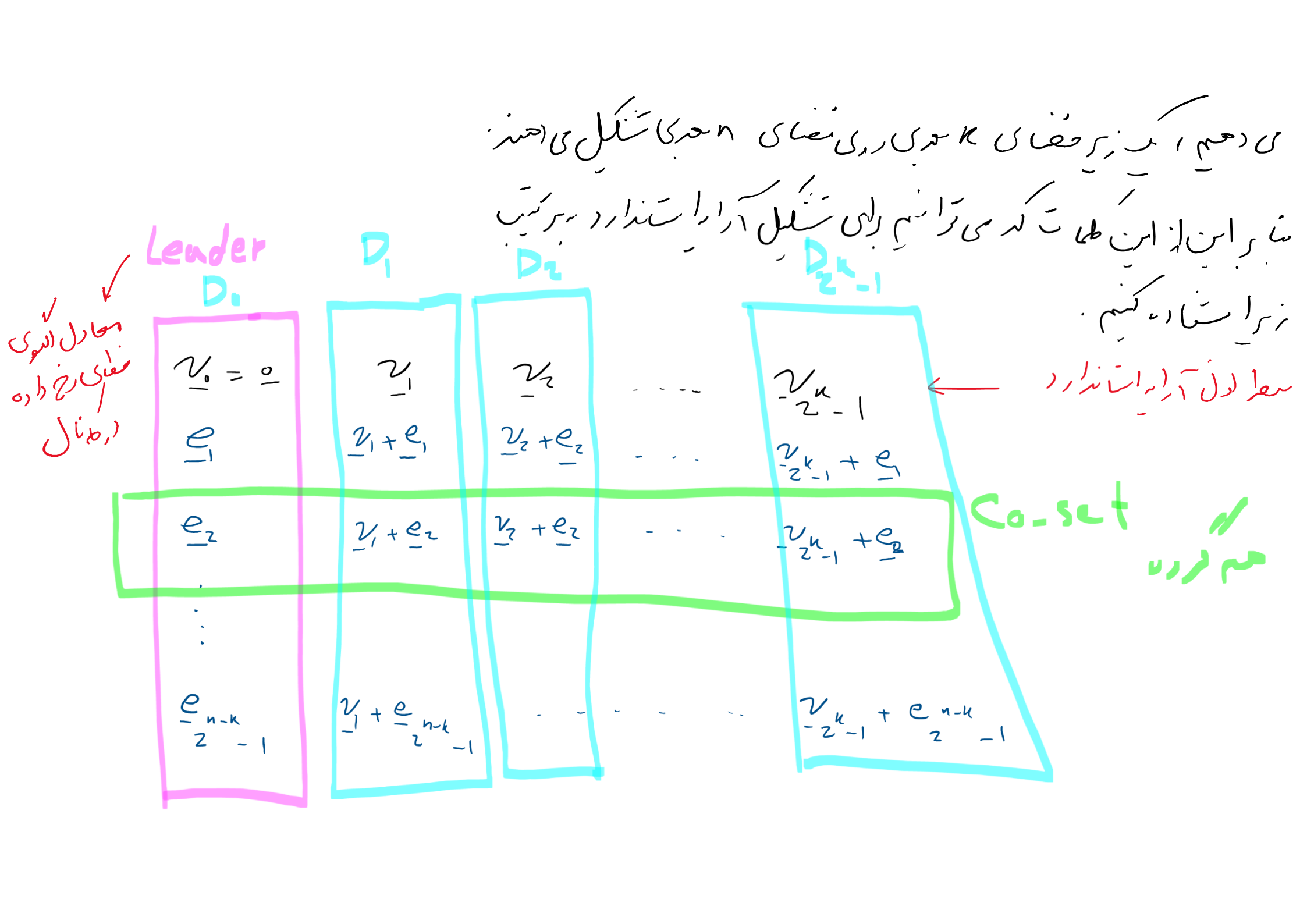
یکی از روشهایی که در جبر خطی برای ناحیه‌بندی فضای برداری به نواحی غیرهمپوشان (یعنی بدون عضو مشترک)

مطرح شد، روش آرایه استاندارد است. غیرهمپوشان بودن نواحی دیکدینگ، تضمین می‌کند که هیچ ابهامی

در دیکدینگ وجود نداشته باشد.

در ادامه می‌خواهیم از ساختار آرایه استاندارد برای ناحیه‌بندی فضای برداری و انجام عملیات دیکدینگ استفاده کنیم.

می‌دانیم که کلمات کد یک کد بلوکی خطی $C(n,k)$ که آنها را با $\underline{v}_0 = \underline{0}$ ، $\underline{v}_1$ ، $\underline{v}_2$ ، ... ، $\underline{v}_{2^k-1}$ نمایش



می‌دهیم، یک زیرفضای k بعدی روی فضای n بعدی تشکیل می‌دهند.

بنابراین از این کلمات کد می‌توانیم برای تشکیل آرایه استاندارد به ترتیب زیر استفاده کنیم.

معادل الگوی خطای رخ داده در کانال

Leader D_0	D_1	D_2		D_{2^k-1}
$\underline{v}_0 = \underline{0}$	$\underline{v}_1$	$\underline{v}_2$	$\cdots$	$\underline{v}_{2^k-1}$
$\underline{e}_1$	$\underline{v}_1 + \underline{e}_1$	$\underline{v}_2 + \underline{e}_2$	$\cdots$	$\underline{v}_{2^k-1} + \underline{e}_1$
$\underline{e}_2$	$\underline{v}_1 + \underline{e}_2$	$\underline{v}_2 + \underline{e}_2$	$\cdots$	$\underline{v}_{2^k-1} + \underline{e}_2$
$\vdots$				
$\underline{e}_{2^{n-k}-1}$	$\underline{v}_1 + \underline{e}_{2^{n-k}-1}$	$\cdots$	$\cdots$	$\underline{v}_{2^k-1} + e_{2^{n-k}-1}$

سطر اول آرایه استاندارد

Co-set

هم گروه

می‌دانیم که تمامی اعضای فضای برداری n بعدی، یک بار و فقط یک بار در آرایه استاندارد ظاهر می‌شوند. بنابراین می‌توانیم ستون مربوط به v_i را به صورت ناحیه دیکدینگ v_i در نظر بگیریم و آن را با D_i نمایش دهیم. بنابراین در نهایت $D_0, D_1, \dots, D_{2^k-1}$ ناحیه دیکدینگ متناظر با کلمات کد $v_0, v_1, \dots, v_{2^k-1}$ خواهیم داشت.

اگر بردار دریافتی r در ناحیه‌ی D_i قرار بگیرد، دیکدر کلمه کد v_i را به عنوان کلمه کد ارسالی بازیابی می‌کند. با توجه به اینکه بردارهایی که در ناحیه D_i قرار می‌گیرند، باید بیشترین شباهت را به کلمه کد v_i داشته باشند، leader ها $(e_1, e_2, \dots, e_{2^{n-k}-1})$ به گونه‌ای که انتخاب می‌شوند که کمترین وزن همینگ را داشته باشند. به عبارت دیگر برای

انتخاب leader ها از وزن همینگ 1 شروع می‌کنیم و تمام بردارهای
به طول n با وزن همینگ 1 را که در سطرهای متناظر ظاهر شده‌اند
به عنوان انتخاب leader می‌کنیم. با همین ترتیب جلو می‌رویم تا آرایه
استاندارد کامل شود. می‌دانیم که هر عضو فضای برداری یک بار و فقط یک بار در این آرایه ظاهر
می‌شود. به این ترتیب روند رمزگذاری به این صورت است که با دریافت بردار r، در آرایه استاندارد
جستجو می‌کنیم و مکان r را در آرایه پیدا می‌کنیم. فرض کنیم بردار r در سطر iام و ستون jام
از آرایه استاندارد قرار دارد. در این صورت الگوی خطای رخ داده در کانال e_j است و کلمه کد ارسالی
c_j بوده است.

در شکل آرایه‌ای ندارد، با توجه به اینکه می‌دانیم قابلیت تصحیح خطای

که بلوکی حداقل دارد $t = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor$ است، می‌توانیم نتیجه

بگیریم که تمامی الگوهای خطای با وزن کمتر یا مساوی t به عنوان leader

انتخاب می‌شوند (در ادامه به صورت یک قضیه اثبات می‌کنیم) نکات مربوط به این موضوع را با یک مثال

بررسی می‌کنیم و سپس به بیان قضیه خواهیم پرداخت.

مثال - $C(5,2)$ مثال قبل با

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

آرایه استاندارد را برای دیکدینگ این کد تشکیل دهید.

$\underline{u}$	$\underline{v}$	
0 0	0 0 0 0 0	$\rightarrow \underline{v}_0$
0 1	0 1 1 0 1	$\rightarrow \underline{v}_1$
1 0	1 0 1 1 1	$\rightarrow \underline{v}_2$
1 1	1 1 0 1 0	$\rightarrow \underline{v}_3$

$d_{min} = 3$

$t = 1$

$n = 5, \quad k = 2$ ، تعداد پیام $= 2^k = 4$

تعداد کلمات کد $=$

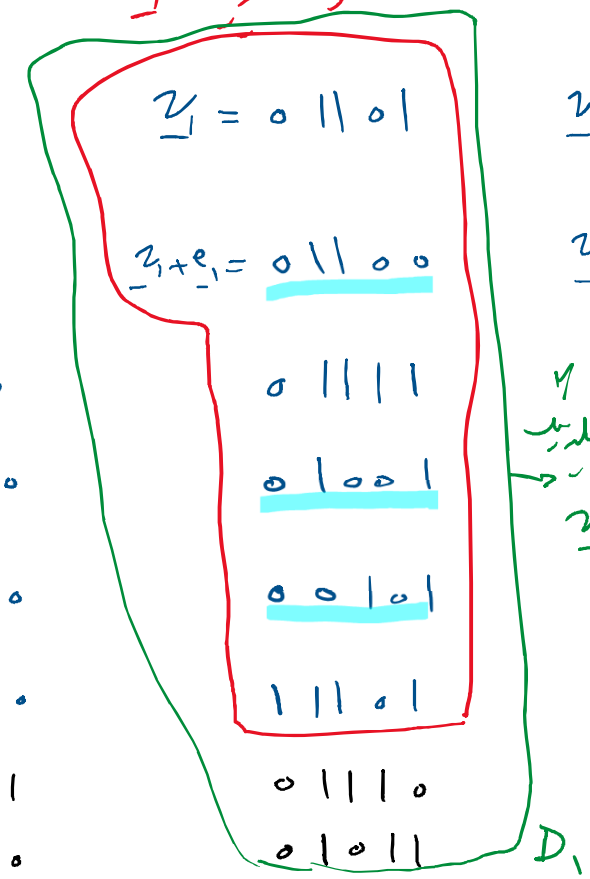
تعداد اعضای فضای n بعدی $= 2^n = 2^5 = 32$

تعداد سطر آرایه $= 2^{n-k} = 2^3 = 8$

incomplet decoding
Bounded Distance

اگر دیکدر را براساس این قسمت از آرایه پیاده کنیم، دیکدر غیرکامل داریم که failure دارد

* اگر دیکدر را براساس آرایه‌ی کامل شده پیاده‌سازی کنیم، دیکدر کامل خواهیم داشت و failure نداریم. Complete decoding



کره دیکدینگ $\underline{v}_1$

$\underline{v}_0 = \underline{0}$	$\underline{v}_1 = 01101$	$\underline{v}_2 = 10111$	$\underline{v}_3 = 11010$
$\underline{e}_1 = 00001$	$\underline{v}_1+\underline{e}_1 = 01100$	$\underline{v}_2+\underline{e}_1 = 10110$	$\underline{v}_3+\underline{e}_1 = 11011$
$\underline{e}_2 = 00010$	01111	10101	11000
$\underline{e}_3 = 00100$	01001	10011	11110
$\underline{e}_4 = 01000$	00101	11111	10010
$\underline{e}_5 = 10000$	11101	00111	01010
$\underline{e}_6 = 00011$	01110	10100	11001
$\underline{e}_7 = 00110$	01011	10001	11100

D_1

ناحیه دیکدینگ $\underline{v}_1$

آرایه استاندارد با الگوهای خطای با وزن 1 کامل نشده است.

آرایه استاندارد با دو الگوی خطای به وزن 2 کامل شده است.

* بردار دریافتی $\underline{r} = (1,1,1,1,1)$ را ریکد کنید.

در آرایه استاندارد جستجو می‌کنیم، $\underline{r}$ در ناحیه دیکدینگ $\underline{v}_2$ قرار گرفته است. بنابراین کلمه کد ارسالی $\underline{v}_2 = 10111$ بوده است. همچنین می‌بینیم که $\underline{r}$ در سطر هم‌گروه $\underline{e}_4$ قرار گرفته است. بنابراین الگوی خطای رخ داده در کانال $\underline{e}_4 = 01000$ بوده است و

$$\hat{\underline{v}} = \underline{r} + \underline{e}_4 = \underline{v}_2$$

* کد کامل، کدی است که آرایه استاندارد آن با انتخاب تمامی الگوهای خطا با وزن کمتر یا مساوی t، کامل می‌شود یا به عبارت دیگر برای آن داریم،

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{t} = 2^{n-k}$$

یعنی کران بسته بندی کروی در تساوی برقرار باشد.

قضیه: برای یک کد بلوکی خطی $C(n,k)$ با فاصله همینگ حداقل d_{min}، تمامی الگوهای خطا به طول n با وزن همینگ کمتر یا مساوی t $\left(t = \left[\frac{d_{min}-1}{2}\right]\right)$ می‌توانند به عنوان leader در آرایه استاندارد انتخاب شوند. پس از انتخاب این الگوهای خطا، از بین الگوهای خطا با وزن $t+1$، دست‌کم یک الگوی خطا وجود دارد که نمی‌تواند به عنوان leader انتخاب شود.

اثبات: برای اثبات قسمت اول قضیه، دو بردار $\underline{x}$ و $\underline{y}$ با وزن همینگ کمتر یا مساوی t را در نظر می‌گیریم و نشان می‌دهیم که $\underline{x}$ و $\underline{y}$ نمی‌توانند هم گروه باشند. به عبارت دیگر اگر یکی از این دو بردار به عنوان leader انتخاب شود، دومی در سطرهای قبلی ظاهر نمی‌شود و می‌تواند به عنوان leader انتخاب شود.

می‌دانیم که $w(\underline{x}) \leq t$,

$w(\underline{y}) \leq t$

$\Longrightarrow \quad w(\underline{x}+\underline{y}) \leq w(\underline{x}) + w(\underline{y}) \leq 2t < d_{min}$

$t = \left[\frac{d_{min}-1}{2} \right]$

می‌خواهیم نشان دهیم که $\underline{x}$ و $\underline{y}$ نمی‌توانند هم‌گروه باشند. برای اثبات از برهان خلف کمک می‌گیریم.

فرض می‌کنیم که $\underline{x}$ ، $\underline{y}$ هم‌گروه باشند. در این صورت می‌توان نوشت:

$$\left.\begin{aligned} \underline{x} &= \underline{v}_i + \underline{e}_\ell \\ \underline{y} &= \underline{v}_j + \underline{e}_\ell \end{aligned}\right\} \leftarrow \quad \exists\, \underline{v}_i, \underline{v}_j, \underline{e}_\ell$$

$$\Rightarrow \quad \underline{x} + \underline{y} = \underline{v}_i + \underline{v}_j$$

از طرفی دیگر می‌دانیم که حاصل جمع هر دو کلمه کد، یک کلمه کد از $C(n,k)$ است. بنابراین می‌توان نوشت

$$\exists\, \underline{v}_m \in C(n,k)$$

$$\Rightarrow \quad \underline{x} + \underline{y} = \underline{v}_m$$

می‌دانیم که کمترین وزن همینگ کلمات کد برابر d_{min} است بنابراین

$$\Rightarrow \quad w(\underline{x} + \underline{y}) = w(\underline{v}_m) \geq d_{min}$$

با توجه به اینکه $d_{min} > w(\underline{x}+\underline{y})$ برقرار است،

اینکه $\underline{x}+\underline{y} = \underline{v}_m$ نمی‌تواند برقرار باشد.

بنابراین $\underline{x}$ و $\underline{y}$ نمی‌توانند هم‌گروه باشند. اگر $\underline{x}$

به عنوان leader انتخاب شود، $\underline{y}$ در مرحله‌های قبلی ظاهر نمی‌شود و می‌تواند به عنوان leader

انتخاب شود.

* برای اثبات قسمت دوم، باید نشان دهیم که دست‌کم یکی از گره‌های همسایه‌ی بازنی $t+1$ وجود دارد که نمی‌تواند به عنوان leader انتخاب شود. (توجه داشته باشید که تمام گره‌های همسایه‌ی بازنی کمترین وزن t به عنوان leader انتخاب شده‌اند.)

برای این منظور، دو بردار n تایی $\underline{x}$ و $\underline{y}$ با شرایط زیر را در نظر می‌گیریم.

1- دو بردار $\underline{x}$ و $\underline{y}$ هیچ‌کدام در هیچ صفر مشترکی نداشته باشند

2- جمع $\underline{x}$ و $\underline{y}$ یک کلمه کد از $C(n,k)$ با وزن d_{min} باشد.

با توجه به خطی بودن کد می‌توان نوشت،

$$w(\underline{x}+\underline{y}) = w(\underline{x}) + w(\underline{y})$$

با توجه به خاصیت دوم می‌توان نوشت،

$$w(\underbrace{\underline{x}+\underline{y}}_{\underline{v}}) = d_{min} = w(\underline{v})$$

$$2t+1 \leq d_{min} \leq 2t+2$$

$$t = \left[\frac{d_{min}-1}{2}\right] \xrightarrow{d \in \mathbb{N}} t \leq \frac{d_{min}-1}{2} < t+\frac{1}{2}$$

$$\Rightarrow \quad 2t+1 \leq w(\underline{x}) + w(\underline{y}) \leq 2t+2$$

اگر $w(\underline{x}) = t+1$ برقرار باشد آنگاه:

$w(\underline{y})$ یا برابر t است یا برابر $t+1$

اگر $\underline{y}$ به عنوان leader انتخاب شده باشد، $\underline{x}$ نمی‌تواند به عنوان leader انتخاب شود

اصرن با $\underline{y}$ هم کرده است و در سطرهای قبلی ظاهر شده است!

$\underline{x} + \underline{y} = \underline{z}$

$\Rightarrow \quad \underline{x} = \underline{z} + \underline{y}$ ← اگر $\underline{y}$ به عنوان leader انتخاب شده باشد، $\underline{x}$ در آن سطر (هنگام کردن) ظاهر شده است و نمی‌تواند leader باشد.

استفاده از سندروم در دیکدینگ براساس آرایه استاندارد

همان طور که در روند دیکدینگ براساس آرایه استاندارد، دیدیم.
در روند دیکدینگ، باید یافتن بردار e جستجو در آرایه را هم به
بردار کلمه کد ارسالی x به دست بیاوریم و هم به الگوی خطای
رخ داده در کانال e پی می‌بریم. در صورتی که داشتن یکی از این اطلاعات برای انجام عملیات دیکدینگ
کافی است. از طرف دیگر ذخیره آرایه استاندارد به خصوص زمانی که ابعاد کد بزرگ باشند، حافظه
زیادی از سیستم اشغال می‌کند. بنابراین می‌توانیم آرایه استاندارد به فرم خلاصه‌تری در بیاوریم و
ذخیره‌سازی کنیم. برای این منظور از سندروم کمک می‌گیریم.

با توجه به ساختار آرایه استاندارد، می‌بینیم که سندرم تمام اعضای یک هم‌گروه با هم برابر هستند. بنابراین به جای ذخیره کل آرایه استاندارد، می‌توانیم سندرم مربوط به هم‌گروه‌ها را ذخیره و نگه داری کنیم.

قضیه: تمای 2^k عضو یک هم‌گروه، سندرم یکسان دارند و سندرم هم‌گروه‌های مختلف متمایز است.

اثبات قسمت اول: فرض کنیم x و y دو بردار به طول n هم‌گروه باشند. در این صورت برای

$$\exists\, \underline{v}_i, \underline{v}_j, \underline{e}_l \; ; \begin{cases} \underline{x} = \underline{v}_i + \underline{e}_l \\ \Longrightarrow \\ \underline{y} = \underline{v}_j + \underline{e}_l \end{cases}$$

$$\Longrightarrow \begin{cases} \underline{S}_x = \underline{x}\, H^T = (\underline{v}_i + \underline{e}_l)\, H^T = \underline{0} + \underline{e}_l H^T = \underline{e}_l H^T \\ \underline{S}_y = \underline{y}\, H^T = (\underline{v}_j + \underline{e}_l)\, H^T = \underline{0} + \underline{e}_l H^T = \underline{e}_l H^T \end{cases}$$

$$\Longrightarrow \quad \underline{S}_x = \underline{S}_y$$

اثبات قسمت دوم: باید نشان دهیم که هم گروه های مختلف (سطرهای مختلف آرایه استاندارد) سندرم های متفاوت دارند.

دو هم گروه مختلف با leader های $\underline{e}_l$ و $\underline{e}_m$ را در نظر می گیریم و نشان می دهیم که اعضای این دو هم گروه سندرم های متفاوتی دارند. برای این منظور از برهان خلف کمک می گیریم. فرض می کنیم که اعضای این دو هم گروه، سندرم یکسان داشته باشند یعنی

$$\underbrace{\underline{e}_m H^T}_{\text{سندرم همگروه } m \text{ ام}} = \underbrace{\underline{e}_l H^T}_{\text{سندرم همگروه } l \text{ ام}} \Longrightarrow (\underline{e}_m + \underline{e}_l) H^T = \underline{0}$$

یعنی $\underline{e}_m + \underline{e}_l$ یک کلمه کد $\underline{v}$ از $C(n,k)$ است.

$$\Rightarrow \underline{e}_m + \underline{e}_f = \underline{v}$$

$$\Rightarrow \underline{e}_m = \underline{v} + \underline{e}_f$$

یعنی $\underline{e}_m$ و $\underline{e}_f$ در یک هم‌گردی هستند که خلاف عرض است. بنابراین هم‌گردهای متفاوت، سندرم‌های متفاوت دارند.

⇐ یک رابطه یک به یک بین سندرم‌ها و هم‌گردها برقرار است.

⇐ به جای ذخیره‌سازی یک هم‌گردی، می‌توانیم سندرم مربوط به آن هم‌گردی را ذخیره‌سازی کنیم

به جای ذخیره‌سازی 2^k حالت مختلف، فقط اطلاعات 2^{n-k} هم‌گردی (سطرهای آرایه استاندارد) را

ذخیره سازی می کنیم. به این ترتیب روند دیکدینگ به صورت زیر خواهد بود.

* با دریافت بردار $\underline{r}$ ، ابتدا سندرم بردار $\underline{r}$ را تشکیل می دهیم.

$$\underline{s} = \underline{r} H^T$$

* سپس در جدول خلاصه شده، آرایه استاندارد، الگوی خطای مربوط به سندرم $\underline{s}$ را مشخص می کنیم ($\underline{e}$)

* کلمه کد ارسالی برابر خواهد بود

$$\hat{\underline{v}} = \underline{r} + \underline{e}$$