ریاضی و جامعه
شاپا (چاپی): ۲۳۴۵-۶۴۹۳، شاپا(الکترونیکی): ۲۳۴۵-۶۵۰۷
جلد ۶، شماره ۲ (۱۴۰۰)، صص. ۸۷-۱۰۲

http://math-sci.ui.ac.ir
http://www.ui.ac.ir

آشنایی با وزن‌های همینگ تعمیم یافته

فرزانه فرهنگ بافتانی

چکیده. فرض کنیم C یک کد روی میدان متناهی باشد در این صورت $r-$ امین وزن همینگ تعمیم یافته آن را به‌صورت مینیمم اندازه محمل (ساپورت)های زیر کدهای r بعدی آن تعریف کرده و با نماد $d_r(C)$ نمایش می‌دهند. وزن‌های همینگ تعمیم یافته به خاطر کاربردهایی که در علوم مختلف از جمله رمزنگاری، مهندسی الکترونیک ، کامپیوتر و مخابرات دارند، از اهمیت ویژه‌ای برخوردارند. در این مقاله سعی شده است به تفصیل به بررسی این مفهوم مهم نظریه کدگذاری پرداخته شود و بخشی از کاربردهای آن نیز بررسی شده است.

۱. مقدمه

وزن‌های همینگ تعمیم یافته نخستین بار در سال ۱۹۹۱ توسط ویکتور وِی در مقاله معروفش تحت عنوان وزن‌های همینگ تعمیم یافته برای کدهای خطی معرفی شدند [۹]. در مقاله حاضر با استفاده از مقاله اشاره شده و مقالات بعد از آن، به محاسبه وزن‌های همینگ تعمیم یافته برای کدهای باینری [۹] و غیر باینری [۲] و [۳] می‌پردازیم. وزن‌های همینگ تعمیم‌یافته برای کدهایی مانند کد همینگ، دوگان کد همینگ، کد همینگ توسعه یافته، گُلِی و کد رید– مولر ارایه خواهد شد. با توجه به این که نتایج مهمی درباره وزن‌های همینگ تعمیم یافته به‌دست آمده است، نتایجی چون قضایای «یکنوایی»، «کران سینگلتون تعمیم یافته» و «دوآلیتی» از جمله نتایجی هستند که به بررسی آن‌ها خواهیم پرداخت. قضیه یکنوایی حاکی از آن است که وزن‌های همینگ تعمیم یافته یک کد، تشکیل یک دنباله اکیداً صعودی می‌دهند. کران سینگلتون تعمیم یافته، کرانی بالا برای وزن‌های همینگ تعمیم یافته است که این کران در صورت تساوی به خاصیت $r-MDS$ بودن تعبیر می‌شود. بررسی وزن‌های همینگ تعمیم یافته برای کدهای $r-MDS$ نتایج جالب و مهمی را به دنبال دارد. در این مقاله، وزن‌های همینگ تعمیم یافته برای کدهای غیر خطی نیز ارایه شده و قضایای مشابه حالت خطی بودن، آورده شده است. برای مطالعه بیشتر منبع [۱] را ببینید.

۲. تعاریف و مفاهیم مقدماتی

در این بخش، تعاریف و مفاهیم مورد نیاز برای فهم موضوع بررسی این مقاله را بیان می‌کنیم. برای مطالعه بیشتر منبع [۷] را ببینید.

عبارات و کلمات کلیدی: وزن همینگ، وزن همینگ تعمیم یافته، کد همینگ، دوگان کد، کدهای خطی، کدهای غیر خطی.
دبیرتخصصی رابط: علیرضا عبدالهی
نوع مقاله: ترویجی
تاریخ دریافت: ۱۴۰۰/۷/۱۵ تاریخ پذیرش: ۱۴۰۰/۱۱/۲۴

http://dx.doi.org/10.22108/MSCI.2022.130902.1473

تعریف ۱.۲. مجموعه q عضوی A را به‌عنوان الفبای کدی [۱] در نظر بگیرید. اعضای این مجموعه را نمادهای کد می‌نامند.

(الف) یک کلمه [۲] q آرایه به‌طول n روی A عبارت است از دنباله $x = x_1x_2\cdots x_n$ که در آن $x_i \in A$ برای هر i. برای راحتی در بعضی موارد x را به‌صورت $x = (x_1, x_2, \dots, x_n)$ نیز نمایش می‌دهند.

(ب) یک کد بلوکی [۳] q آرایه به‌طول n روی A عبارت است از مجموعه ای مانند C متشکل از کلمات q آرایه با طول مساوی n.

(ج) هر عضو از مجموعه C را یک کد کلمه [۴] در این مجموعه می‌نامیم.

(د) تعداد کد کلمات C را که با نماد $|C|$ نمایش داده می‌شود، اندازه C می‌نامیم.

(ه) نرخ اطلاعات کد [۵] C به‌طول n را به‌صورت $(\log_q^{|C|})/n$ تعریف می‌کنیم.

(و) یک کد به‌طول n و اندازه M را یک $(n, M)-$ کد می‌نامیم.

تعریف ۲.۲. فرض کنیم X و Y کلماتی به‌طول n روی مجموعه الفبایی A باشند. فاصله همینگ از X به Y که با نماد $d(X, Y)$ نمایش داده می‌شود، به‌صورت تعداد جایگاه‌هایی که X و Y در آن متفاوت هستند، تعریف می‌شود. اگر $X = x_1x_2\cdots x_n$ و $Y = y_1y_2\cdots y_n$ باشد آنگاه

$$d(X, Y) = d(x_1, y_1) + d(x_2, y_2) + +d(x_n, y_n),$$

که در آن x_i و y_i به‌عنوان کلماتی به‌طول یک در نظر گرفته می‌شود و

$$d(x_i, y_i) = \begin{cases} 1 & x_i \neq y_i, \\ 0 & x_i = y_i. \end{cases}$$

مثال ۳.۲. با فرض $C = \{001, 110, 101\}$ و با در نظر گرفتن

$$x = 001, y = 110, z = 101$$

داریم

$$d(x, y) = 3, d(x, z) = 1, d(y, z) = 2.$$

تعریف ۴.۲. فرض کنیم C یک کد با حداقل دو کد کلمه باشد، (مینیمم) فاصله C را با نماد $d(C)$ یا به‌اختصار d نمایش داده و به‌صورت زیر تعریف می‌کنیم

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

تعریف ۵.۲. یک کد به طول n و اندازه M و فاصله d را با نماد (n, M, d) نمایش می دهند.

مثال ۶.۲. با فرض $C = \{001, 110, 101\}$ و با در نظر گرفتن

$$x = 001, y = 110, z = 101$$

داریم

$$d(x, y) = 3, d(x, z) = 1, d(y, z) = 2$$

در نتیجه $d = 1$. توجه کنید که C یک $(3, 3, 1)$ کد خواهد بود.

[1] code alphabet [2] word [3] block code [4] codeword [5] information rate

http://dx.doi.org/10.22108/MSCI.2022.130902.1473

۳. کدهای خطی

منظور از F_q در سراسر این مقاله، میدان متناهی از مرتبه q است.

تعریف ۱.۳. یک کد خطی مانند C به‌طول n روی F_q عبارت است از هر زیر فضای دلخواه از F_q^n.

مثال ۲.۳. کدهای زیر کدهای خطی هستند:

(الف) $C = \{(a, a, \dots, a) : a \in F_q\}$. این کد، کد تکرار نامیده می‌شود.

(ب) $C = \{۰۰۰, ۰۰۱, ۱۰۰, ۱۰۱\}, (q = ۲)$

(پ) $C = \{۰۰۰۰, ۰۰۱۱, ۰۲۰۲, ۰۲۱۰, ۰۱۱۲, ۰۰۲۲, ۰۱۰۱, ۰۲۲۱, ۰۱۲۰\}, (q = ۳)$.

تعریف ۳.۳. فرض کنیم S زیرمجموعه‌ای ناتهی از F_q^n باشد. $S^\perp$ را به‌صورت زیر تعریف می‌کنیم

$$S^\perp = \{v \in F_q^n : v.s = ۰, \forall s \in S\}$$

که در آن «.» ضرب نقطه‌ای است.

تعریف ۴.۳. فرض کنیم C کد خطی در F_q^n باشد.

(الف) $C^\perp$ را کد دوگان C می‌نامیم.

(ب) بعد کد خطی C را همان بعد C به‌عنوان فضای برداری روی F_q تعریف می‌کنیم و با نماد $dim(C)$ نمایش می‌دهیم.

قضیه ۵.۳. *فرض کنیم C کد خطی به‌طول n روی F_q باشد. در این صورت*

(الف) *$|C| = q^{dimC}$ به‌عبارت دیگر $dimC = \log_q |C|$.*

(ب) *$C^\perp$ کد خطی است و $dimC + dimC^\perp = n$.*

(ج) $(C^\perp)^\perp = C$.

مثال ۶.۳. با فرض $C = \{۰۰۰۰, ۱۰۱۰, ۰۱۰۱, ۱۱۱۱\}$ داریم

$$dim(C) = log_۲|C| = ۲.$$

و همچنین $C^\perp = \{۰۰۰۰, ۱۰۱۰, ۰۱۰۱, ۱۱۱۱\}$. در نتیجه $dim(C^\perp) = ۲$. توجه کنید که این مثال در قضیه قبلی صدق می‌کند.

تبصره ۷.۳. کد خطی C به‌طول n و با بعد k روی F_q را غالباً یک $[n, k]-$ کد q آرایه و در صورتی‌که q طبق متن معلوم باشد یک $[n, k]-$ کد می‌نامیم. در این‌صورت C یک $(n, q^k)-$ کد خطی نیز هست. اگر فاصله d برای C مشخص باشد در این‌صورت آن را $[n, k, d]-$ کد خطی می‌نامیم.

۴. وزن همینگ[6]

تعریف ۱.۴. فرض کنیم x یک کلمه در F_q^n باشد. وزن (همینگ) x را با نماد $wt(x)$ نمایش داده و آن را به‌صورت تعداد درایه‌های ناصفر در x تعریف می‌کنیم یعنی $wt(x) = d(x, ۰)$، که در آن ۰ کلمه صفر است.

[6] hamming weight

http://dx.doi.org/10.22108/MSCI.2022.130902.1473

تبصره ۲.۴. برای هر x در F_q وزن همینگ به‌صورت زیر تعریف می‌شود:

$$wt(x) = d(x, ۰) = \begin{cases} ۱ & x \neq ۰ \\ ۰ & x = ۰ \end{cases}.$$

تعریف ۳.۴. فرض کنیم C یک کد (نه لزوماً خطی) باشد. مینیمم وزن (همینگ) برای C که با نماد $wt(C)$ نمایش داده می‌شود عبارت است از کوچکترین وزن کد کلمات ناصفر در C. به‌عبارت دیگر

$$wt(C) = min\{wt(x); x \neq ۰, x \in C\}$$

قضیه ۴.۴. *فرض کنیم C یک کد خطی روی F_q باشد. در این‌صورت* $d(C) = wt(C)$.

مثال ۵.۴. کد خطی $C = \{۰۰۰۰, ۰۱۰۰, ۰۰۰۱, ۰۱۰۱\}$ را در نظر بگیرید. با احتساب تعداد جایگاه‌های غیرصفر هر کلمه داریم:

$$wt(۰۱۰۰) = ۱, wt(۰۰۰۱) = ۱, wt(۰۱۰۱) = ۲$$

لذا خواهیم داشت

$$d(C) = min\{۱, ۱, ۲\} = ۱.$$

تبصره ۶.۴. با توجه به قضیه فوق، در کدهای خطی می‌توان به‌جای محاسبه فاصله کد کلمات از یکدیگر در کد C، $wt(x)$ها را محاسبه کرده و مینیمم آنها همان مینیمم وزن همینگ کد C خواهد بود و این یکی از مزایای کد خطی است. از دیگر مزایای کد خطی می‌توان به وجود پایه در این کدها اشاره کرد زیرا کدهای خطی، فضای برداری هستند و در نتیجه دارای پایه هستند. اگر اعضای پایه کد خطی را در یک ماتریس قرار دهیم، آن ماتریس، ماتریس مولد کد مذکور نامیده می‌شود. در ادامه، تعاریف مرتبط با پایه کدهای خطی را شرح خواهیم داد.

تعریف ۷.۴. ماتریس مولد [۷] برای یک کد خطی مانند C عبارت است از ماتریسی مانند G که سطرهای آن تشکیل یک پایه برای C می‌دهند.

تعریف ۸.۴. ماتریس کنترل زوجیت [۸] برای کد خطی C عبارت است از ماتریسی مانند H که H ماتریس مولد $C^{\perp}$ است.

تبصره ۹.۴. اگر C یک $[n, k]-$ کد خطی باشد در این‌صورت ماتریس مولد C یک ماتریس $k \times n$ است و ماتریس کنترل زوجیت C یک ماتریس $(n-k) \times n$ است.

با توجه به اینکه با استفاده از اعمال سطری مقدماتی می‌توان یک ماتریس را به‌صورت پلکانی در آورد، لذا تعاریف زیر را داریم:

تعریف ۱۰.۴. (الف) ماتریس مولد به فرم $(I_k|X)$ را فرم استاندارد می‌نامیم.
(ب) ماتریس کنترل زوجیت به فرم $(Y|I_{n-k})$ را فرم استاندارد می‌نامیم.

قضیه زیر به ما کمک می‌کند تا در حالتی که ماتریس کنترل زوجیت یک کد خطی را داریم، بتوانیم اعضای کد و همچنین ماتریس مولد آن را تعیین کنیم.

[7] Generator Matrix [8] parity check matrix

قضیه ۱۱.۴. *فرض کنیم C یک $[n,k]-$ کد خطی روی F_q باشد و H ماتریس کنترل زوجیت آن باشد. در این‌صورت با فرض $v \in F_q^n$ داریم*

$$v \in C \Longleftrightarrow vH^T = 0.$$

به‌ویژه اگر G یک ماتریس $k \times n$ باشد در این‌صورت G ماتریس مولد برای C است اگر و فقط اگر سطرهای G مستقل خطی باشند و $GH^T = 0$.

قضیه ۱۲.۴. *فرض کنیم C یک کد خطی و H ماتریس کنترل زوجیت آن باشد. در این صورت گزاره‌های زیر معادلند:*

(الف) $d(C) = d$

(ب) هر $d-1$ ستون H مستقل خطی هستند و H یک d ستون وابسته خطی دارد.

۵. معرفی چند کد اساسی

۱.۵. کد همینگ باینری.

تعریف ۱.۵. فرض کنید $r \geq 2$. کد خطی دو دویی به طول $n = 2^r - 1$ با ماتریس کنترل زوجیت H که ستون‌های آن شامل بردارهای ناصفر F_2^r هستند، کد همینگ باینری به طول $2^r - 1$ نامیده می‌شود و با نماد $Ham(r,2)$ نمایش داده می‌شود.

قضیه ۲.۵. *کد همینگ $Ham(r,2)$ یک $[2^r-1, 2^r-1-r, 3]-$ کد است.*

مثال ۳.۵. با توجه به تعریف فوق مثال زیر را داریم:

$$Ham(3,2) = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

۲.۵. کد همینگ غیر باینری.

تعریف ۴.۵. فرض کنید $r \geq 2$. کد خطی $q-$ آرایه که ماتریس کنترل زوجیت آن H، از دقیقا یک بردار ناصفر از هر زیر فضای برداری با بعد یک از F_q^r ساخته می‌شود را کد همینگ $q-$ آرایه می‌نامند و با نماد $Ham(r,q)$ نمایش می‌دهند.

برای نوشتن ماتریس کنترل زوجیت کد همینگ کافی است به تذکر زیر توجه کنیم.

تبصره ۵.۵. یک روش ساده برای نوشتن ماتریس کنترل زوجیت $Ham(r,q)$، لیست کردن ستون های $r-$تایی ناصفر در F_q^r است که درایه ناصفر اولشان یک است.

قضیه ۶.۵. *کد همینگ $Ham(r,q)$ یک $[\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1} - r, 3]-$ کد است.*

مثال ۷.۵.

$$Ham(3,4) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 2 & 2 & 2 & 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 1 \end{bmatrix}$$

http://dx.doi.org/10.22108/MSCI.2022.130902.1473

[خواننده احتمالا متوجه این نکته شده است که در ستون‌هایی که با عدد یک شروع شده‌اند، در سطر سوم آنها اعضای میدان $F_۳$ مرتباً جاگذاری شده است و در سطر دوم، ابتدا یک‌ها و سپس صفرها و دوها جاگذاری شده است. در ستون‌هایی که با صفر شروع شده‌اند، در سطر دوم آنها یک و در سطر آخرشان باز اعضای $F_۳$ قرار دارند در ستون آخر ماتریس هم $(۱, ۰, ۰)$ جاگذاری شده است. خواننده به سادگی می‌تواند فرمول کلی ماتریس کنترل زوجیت برای $Ham(۳, q)$ را به‌دست آورد. (مطلب نویسنده)]

۳.۵. همینگ توسعه یافته.

تعریف ۸.۵. برای هر کد مانند C روی F_q ، کد توسعه یافته‌ی C که با نماد $\bar{C}$ نمایش داده می‌شود به‌صورت زیر تعریف می‌شود

$$\bar{C} = \{(c_۱, c_۲, \dots, -\sum_{i=۱}^{n} c_i) : (c_۱, \dots, c_n) \in C\}.$$

در حالتی‌که $q = ۲$ ، درایه $\sum_{i=۱}^{n} c_i = -\sum_{i=۱}^{n} c_i$ که به کد کلمه $(c_۱, \dots, c_n)$ اضافه می‌شود، درایه کنترل زوجیت نامیده می‌شود.

قضیه ۹.۵. *اگر C یک $(n, M, d)-$ کد روی F_q باشد، آنگاه $\bar{C}$ یک $(n+۱, M, d')-$ کد روی F_q است که در آن $d \le d' \le d+۱$. اگر C خطی باشد آنگاه $\bar{C}$ نیز خطی است. به‌علاوه در حالتی‌که C خطی است*

$$\bar{H} = \left[\begin{array}{ccccc|c} & & H & & & ۰ \\ \hline ۱ & ۱ & ۱ & \cdots & & ۱ \end{array}\right]$$

ماتریس کنترل زوجیت $\bar{C}$ است اگر H ماتریس کنترل زوجیت C باشد.

۴.۵. کد رید– مولر.

تعریف ۱۰.۵. کد رید– مولر (مرتبه اول) $R(۱, m)$ ، کدهایی باینری‌اند که برای هر عدد صحیح مانند $m \ge ۱$ ، به‌صورت بازگشتی به شکل زیر تعریف می‌شوند

(الف) $R(۱, ۱) = F_۲^۲ = \{۰۰, ۰۱, ۱۰, ۱۱\}$

(ب) برای هر $m \ge ۱$ داریم

$$R(۱, m+۱) = \{(\mathbf{u}, \mathbf{u}) : \mathbf{u} \in R(۱, m)\} \cup \{(\mathbf{u}, \mathbf{u}+۱) : \mathbf{u} \in R(۱, m)\}$$

قضیه ۱۱.۵. *برای $m \ge ۱$، کد رید– مولر $R(۱, m)$ یک $[۲^m, m+۱, ۲^{m-۱}]-$ کد خطی است به‌طوری‌که هر کد کلمه به‌جز ۰ و ۱ دارای وزن $۲^{m-۱}$ است.*

۶. محمل یک کد

تعریف محمل [9] [۹]، [۱]. فرض کنیم C یک $[n, k]-$ کد خطی و D یک زیر کد باشد. محمل D را با نماد $supp(D)$ نمایش داده می‌شود و به‌صورت مجموعه جایگاههای نه همگی صفر از D تعریف می‌کنیم. به‌عبارت دیگر

$$supp(D) = \{i | \exists (x_۱, x_۲, \dots, x_n) \in D; x_i \neq ۰\}$$

[9] support

http://dx.doi.org/10.22108/MSCI.2022.130902.1473

با این تعریف واضح است که یک $[n,k]-$ کد، یک کد خطی با رتبه k و اندازه محمل کمتر یا مساوی n است زیرا در هر کلمه به طول n حداکثر n جایگاه مخالف صفر ممکن است وجود داشته باشد. لازم به ذکر است که زیرکد یک کد خطی، عبارت است از کد خطی که در آن کد واقع می‌شود.

۷. وزن همینگ تعمیم یافته [10]

تعریف ۱.۷. فرض کنیم C یک $[n,k]-$ کد خطی باشد. $r-$ امین وزن همینگ C که با نماد $d_r(C)$ نمایش می‌دهیم را کوچکترین اندازه محمل زیر کد $r-$ بعدی از C تعریف می‌کنیم. به‌عبارت دیگر

$$d_r(C) = min\left\{|supp(D)| : D \subseteq C, dim(D) = r\right\}.$$

توجه کنید که $d_۱(C)$ همان وزن همینگ قدیمی C است. یعنی $d_۱(C) = d(C)$. زیرا فرض کنیم

$$d_۱(C) = a, d(C) = b.$$

داریم

$$d_۱(C) = a \Rightarrow \exists D \subseteq C; dim(D) = ۱, |supp(D)| = a \Rightarrow D =< x >,$$

توجه کنید که هر عضو D مضربی از x یا صفر است. اگر جایگاهی در x مخالف صفر باشد آنگاه مضرب غیر صفر آن جایگاه نیز مخالف صفر خواهد بود و در نتیجه داریم $|supp(D)| = wtx = a$. از طرفی $d(C)$ مینیمم وزن هست لذا داریم $d(C) \leq$ $wtx = a$ پس $b \leq a$. حال با توجه به اینکه $d(C) = b$ داریم

$$\exists x(\neq ۰) \in C; wtx = b$$

قرار می‌دهیم $D' =< x >$. در نتیجه خواهیم داشت

$$|supp(D')| = wtx = b, dim(D') = ۱ \Rightarrow d_۱(C) \leq |supp(D')| \Rightarrow a \leq b$$

در نتیجه خواهیم داشت $a = b$ (اثبات نویسنده).

برای کد خطی C مفهوم سلسله وزن [11] را با نماد WH نمایش داده و به‌صورت مجموعه اعداد صحیح زیر تعریف می‌کنیم:

$$WH = \{d_r(C) : ۱ \leq r \leq k\}.$$

در حالتی‌که C غیر خطی باشد، تعریف می‌کنیم

$$d_r(C) = min\left\{|supp(D)| : D \subseteq C, q^{r-۱} <| D |\leqslant q^r\right\}.$$

توجه کنید که تعریف فوق را می‌توان به‌صورت زیر هم نوشت

$$d_r(C) = min\left\{|supp(D)| : D \subseteq C, | D |= q^{r-۱} + ۱\right\}.$$

زیرا فرض کنیم D عضوی از مجموعه سمت راست رابطه بالا باشد. در این‌صورت اندازه آن به‌صورت یکی از موارد زیر خواهد بود

$$q^{r-۱} + ۱, q^{r-۱} + ۲, \ldots, q^r$$

[10] generalized hamming weight [11] weight hierarchy

http://dx.doi.org/10.22108/MSCI.2022.130902.1473

فرض کنیم $|D| = q^{r-1} + i$ لذا خواهیم داشت

$$\exists D' \subset C; |D'| = q^{r-1} + 1, D' \subset D$$

پس

$$|supp(D'| \leq |supp(D)|.$$

در نتیجه می‌توان نوشت

$$d_r(C) = min\left\{|supp(D)| : D \subseteq C, |\ D\ | = q^{r-1} + 1\right\}$$

(اثبات نویسنده).

مثال ۲.۷. فرض کنیم

$$C = \{0000, 0001, 1110, 1111\},$$

با در نظر گرفتن

$$D_1 = \{0000, 0001\}, D_2 = \{0000, 1110\}, D_3 = \{0000, 1111\}$$

داریم

$$supp(D_1) = \{4\}, supp(D_2) = \{1, 2, 3\}, supp(D_3) = \{1, 2, 3, 4\}.$$

حال طبق تعریف ارایه شده خواهیم داشت

$$d_1(C) = min\{|supp(D_1)|, |supp(D_2)|, |supp(D_3)|\} = min\{1, 3, 4\} = 1.$$

قضیه زیر رابطه بین وزن‌های همینگ تعمیم یافته یک کد را نشان می‌دهد. توجه کنید که این مقادیر یک زنجیر اکیداً صعودی تشکیل می‌دهند و از طول کد هم بیشتر نیستند.

قضیه ۳.۷. [۲] قضیه یکنوایی [12] *فرض کنیم C یک کد خطی به‌طول n با $k > 0$ باشد. داریم*

$$1 \leq d_1(C) < d_2(C) < \cdots < d_k(C) \leqslant n.$$

تبصره ۴.۷. می دانیم که ماتریس مولد کد $C = [n, k]$ را می‌توان به‌صورت $G = (I_k|A)$ نوشت که در آن I_k یک ماتریس همانی از مرتبه k و A یک ماتریس $(n-k) \times k$ است. برای محاسبه‌ی d_r ما نیازمند زیرفضاهای r بعدی کد هستیم. اگر زیرفضای تولید شده توسط r سطر اول ماتریس فوق را که یک زیر فضای r بعدی است در نظر بگیریم، واضح است که تعداد جایگاه‌های غیرصفر واقع در r سطر اول ماتریس همانی واقع در ماتریس مولد فوق برابر r است و در بین جایگاه‌های کناری این سطرها در ماتریس A حداکثر $n-k$ جایگاه ناصفر می‌توانند وجود داشته باشد زیرا سطرها بردارهایی به‌طول n هستند و لذا خواهیم داشت $d_r(C) \leqslant r + n - k$. (اثبات نویسنده). در نتیجه قضیه زیر را داریم:

قضیه ۵.۷. *(کران سینگلتون تعمیم یافته). [۱] فرض کنیم C یک $[n, k]-$ کد خطی باشد. آنگاه داریم*

$$d_r(C) \leqslant n - k + r.$$

(وقتی $r = 1$ این همان کران سینگلتون است.) توجه کنید که اثبات ارائه شده در تبصره بالا به مراتب کوتاهتر و ساده‌تر از اثبات ارائه شده در منبع [۱] است.

[12] monotonicity

http://dx.doi.org/10.22108/MSCI.2022.130902.1473

تعریف ۶.۷. [۱] کد خطی $[n,k,d]$ روی F_q را MDS [13] گوییم هرگاه داشته باشیم

$$d = n - k + ۱.$$

تعریف ۷.۷. [۱] کد خطی C با پارامترهای $[n,k,d]$ را r- MDS گوییم هرگاه داشته باشیم

$$d_r(C) = n - k + r.$$

با این تعریف واضح است که یک MDS کد، یک ۱-MDS کد است (کافی است قرار دهید $r = ۱$).

اگر $C = [n,k]$ یک MDS کد روی F_q باشد در این‌صورت $d_۱ = n - k + ۱$ و همچنین با این فرض (فرض استقرا) که $d_r = n - k + r$ با استفاده از قضایای «کران سینگلتون تعمیم یافته» و «یکنوایی»، خواهیم داشت

$$n - k + r = d_r < d_{r+۱} \leq n - k + r + ۱ \Rightarrow$$

$$n - k + r < d_{r+۱} \leq n - k + r + ۱ \Rightarrow d_{r+۱} = n - k + r + ۱$$

در نتیجه کد C یک $r - MDS$ کد خواهد بود (اثبات نویسنده). به‌عبارت بهتر نتیجه زیر را خواهیم داشت:

نتیجه ۸.۷. [۱] *اگر C یک MDS کد روی F_q باشد، آنگاه C یک $r - MDS$ نیز می‌باشد که در آن $۱ \leq r \leq k$.*

مشابه آنچه که در بالا توضیح داده شد، می‌توان با اثبات مشابه نتیجه گرفت که

نتیجه ۹.۷. [۱] *اگر C یک $r - MDS$ کد روی F_q باشد، آنگاه C یک $r_۱ - MDS$ کد نیز هست که در آن $r \leq r_۱ \leq k$.*

تعریف ۱۰.۷. [۱] اگر C یک کد روی F_q باشد که $(r-۱)MDS$ نیست ولی روی F_q یک $r - MDS$ کد است، آنگاه C را یک $p_r - MDS$ کد می‌نامیم.

استیون دوگرتی در مقاله [۱] نشان داده است که ارتباطی بین فاصله همینگ $C^{\perp}$ و MDS بودن کد C وجود دارد به این‌صورت که

قضیه ۱۱.۷. [۱] *فرض کنیم C یک $[n,k,d]$ کد و $C^{\perp}$ یک $[n, n-k, d^{\perp}]$ کد باشد. داریم*

(الف) *اگر $d^{\perp} = ۱$ آنگاه C برای هر $۱ \leq r \leq k$ ، $p_r - MDS$ کد نیست.*

(ب) *اگر $d^{\perp} > ۱$ آنگاه C یک $p_{k-d^{\perp}+۲} - MDS$ کد است.*

قضیه زیر یکی از کاربردی‌ترین قضایایی است که در اثبات قضایای ما در مقاله [۳] نقش چشمگیری داشته است.

قضیه ۱۲.۷. [۹] *فرض کنیم C کد خطی و H ماتریس کنترل زوجیت و همچنین $H_i(۱ \leqslant i \leqslant n)$ بردارهای ستونی آن باشد. فرض کنیم $< H_i : i \in I >$ نمایشگر فضای تولید شده توسط این بردارها باشد. در این‌صورت داریم*

$$d_r(C) = min\{|X| : |X| - rank(< H_i : i \in X >) \geq r\}.$$

[13] maximum distance seperable

http://dx.doi.org/10.22108/MSCI.2022.130902.1473

قضیه فوق حاکی است که برای محاسبه‌ی $d_r(C)$ می‌توان به این شکل عمل کرد که در بین ستون‌های ماتریس کنترل زوجیت، ستون‌هایی را انتخاب می‌کنیم که اگر رتبه فضای پیموده شده توسط آن ستون‌ها را از تعداد آن ستون‌ها کم کنیم حاصل برابر r شود. سپس مینیمم اندازه‌های این ستون‌ها را به‌دست می‌آوریم. مینیمم به‌دست آمده همان $d_r(C)$ خواهد بود یعنی بزرگتر مساوی را می‌توان با تساوی جابه‌جا کرد. به‌عبارت دیگر

$$d_r(C) = min\{|X| : |X| - rank(< H_i : i \in X >) = r\}.$$

(مطلب نویسنده).

بین مجموعه وزن‌های همینگ تعمیم یافته کد C و وزن‌های همینگ تعمیم یافته دوگان آن یعنی $C^{\perp}$ رابطه‌ای به‌صورت زیر برقرار است:

قضیه ۱۳.۷. [۹] *قضیه دوآلیتی (دوگان)* [14] *فرض کنیم C یک $[n,k]-$ کد خطی باشد. در این‌صورت*

$$\{d_r(C)|1 \leq r \leq k\} = \{1, 2, ..., n\} \setminus \{n + 1 - d_r(C^{\perp}) : 1 \leq r \leq n - k\}.$$

قضیه ۱۴.۷. [۹] *(کران گریسمر Griesmer) . برای هر $[n,k]-$ کد داریم*

$$n \geq \sum_{i=0}^{k-1} \lceil d_1/2^i \rceil.$$

قضیه ۱۵.۷. [۹] *(وزن‌های تعمیم یافته برای برخی کدها)*

(الف) *فرض کنیم C کد رید- مولر مرتبه اول با اندازه محمل 2^m و بعد $m+1$ باشد. در این‌صورت*

$$d_r(C) = 2^{m-1} + 2^{m-2} + \cdots + 2^{m-r}, \forall 1 \leq r \leq m$$

و

$$d_{m+1}(C) = 2^m.$$

(ب) *کد دوگان همینگ: فرض کنیم C دوگان همینگ با اندازه محمل $2^m - 1$ و بعد m باشد. در این‌صورت*

$$d_r(C) = 2^{m-1} + 2^{m-2} + \cdots + 2^{m-r}, \forall 1 \leq r \leq m.$$

(ج) *کد همینگ: فرض کنیم C کد همینگ با اندازه محمل $n = 2^m - 1$ و دارای رتبه $k = 2^m - m - 1$ باشد. در این‌صورت داریم*

$$\{d_r(C) : 1 \leq r \leq k\} = \{1, 2, \ldots, n\} \setminus \{2^i : 0 \leq i < m\}.$$

(د) *کد همینگ توسعه یافته: فرض کنیم C کد همینگ توسعه یافته با اندازه محمل 2^m و بعد $2^m - m - 1$ باشد. در این‌صورت*

$$d_r(C) = 1 + d_r(C'), \forall 1 \leq r \leq m.$$

که در آن C' کد همینگ توسعه نیافته متناظر است.

[14] duality

http://dx.doi.org/10.22108/MSCI.2022.130902.1473

مثال ۱۶.۷. کد همینگ $C = Ham(۴,۲)$ را در نظر بگیرید. توجه کنید که $n = ۲^۴ - ۱ = ۱۵, k = ۲^۴ - ۴ - ۱ = ۱۱$. داریم

$$\{d_r(C); ۱ \leq r \leq ۱۱\} = \{۱,۲,\ldots,۱۵\} \backslash \{۲^i | ۰ \leq i \leq ۳\} =$$

$$\{۱,۲,\ldots,۱۵\} \backslash \{۱,۲,۴,۸\} = \{۳,۵,۶,۷,۹,۱۰,۱۱,۱۲,۱۳,۱۴,۱۴\}$$

در نتیجه با استفاده از قضیه یکنوایی خواهیم داشت

$$d_۱ = ۳, d_۲ = ۵, d_۳ = ۶, d_۴ = ۷, d_۵ = ۹, d_۶ = ۱۰, d_۷ = ۱۱, d_۸ = ۱۲, d_۹ = ۱۳, d_{۱۰} = ۱۴, d_{۱۱} = ۱۵$$

همچنین برای $C^{\perp}$ داریم

$$d_۱ = ۲^۳ = ۸, d_۲ = ۲^۳ + ۲^۲ = ۱۲, d_۳ = ۲^۳ + ۲^۲ + ۲^۱ = ۱۴, d_۴ = ۲^۳ + ۲^۲ + ۲^۱ + ۱ = ۱۵.$$

اثبات مطالبی را که در ادامه آورده شده است، می‌توانید در مقاله [۳] پیدا کنید. لازم به ذکر است که سلسله وزن کدهای همینگ در حالت باینری در مقاله [۹] به‌دست آمده است ولی ما در مقاله [۳]، در حالت کلی (غیر باینری هم) این سلسله وزن را به‌دست آورده‌ایم که در ادامه گفته می‌شود.

۸. سلسله وزن کدهای همینگ

قضیه ۱.۸. [۳] *برای* $Ham(r,q)$ *داریم*

$$d_l(C) = \begin{cases} l+۲ & ۱ \leq l \leq q-۱, \\ l+۳ & (T_۲ - ۱ =)q \leq l \leq q^۲ + q - ۲(= T_۳ - ۳), \\ l+۴ & (T_۳ - ۲ =)q^۲ + q - ۱ \leq l \leq q^۳ + q^۲ + q - ۳(= T_۴ - ۴), \\ \vdots & \\ l+r & T_{r-۱} - (r-۲) \leq l \leq T_r - r. \end{cases}$$

که در آن $T_i = \dfrac{q^i - ۱}{q - ۱}$.

مثال ۲.۸. با در نظر گرفتن کد $C = Ham(۳,۳)$ خواهیم داشت

$$d_l(C) = \begin{cases} l+۲ & ۱ \leq l \leq ۲, \\ l+۳ & ۳ \leq l \leq ۱۰, \end{cases}$$

در نتیجه سلسله وزن کد فوق به‌صورت زیر خواهد بود

$$WH = \{۳,۴,۶,۷,۸,۹,۱۰,۱۱,۱۲,۱۳\}.$$

http://dx.doi.org/10.22108/MSCI.2022.130902.1473

۹. سلسله وزن دوگان کدهای همینگ

قضیه ۱.۹. [۳] *فرض کنیم $S(r,q)$ بیانگر دوگان کد همینگ $Ham(r,q)$ باشد. سلسله وزن همینگ برای $S(r,q)$ به‌صورت زیر است*

$$\{q^{r-1}, q^{r-1}+q^{r-2}, q^{r-1}+q^{r-2}+q^{r-3}, \dots, q^{r-1}+q^{r-2}+q^{r-3}+\cdots+q+1\}.$$

مثال ۲.۹. با در نظر گرفتن کد همینگ $C = Ham(3,3)$ طبق قضیه فوق خواهیم داشت

$$d_l(C^{\perp}) = \{q^{r-1}, q^{r-1}+q^{r-2}, ..., q^{r-1}+q^{r-2}+\cdots+q+1\} = \{9, 12, 13\}.$$

۱۰. کدهای همینگ و MDS بودن

قضیه ۱.۱۰. [۱] *$Ham(r,q)$ یک $P_s - MDS$ کد است که در آن*

$$s \geq ((q^r-1)/q-1) - q^{r-1} - (r-2).$$

مثال ۲.۱۰. برای کد همینگ $Ham(3,3) = [13,10,3]$ داریم

$$s \geq \frac{3^3-1}{3-1} - 3^2 - 1 \Rightarrow s \geq 13-9-1 \Rightarrow s \geq 3$$

لذا کد $Ham(3,3)$ یک s-MDS کد است برای $s \geq 3$.

برای فهم بهتر بخش کاربرد، مطالعه منابع [۶] و [۸] می‌تواند کمک شایانی بکند.

۱۱. کاربرد

فرض کنیم H یک ماتریس کنترل زوجیت $n \times k$ باشد که در آن k رتبه آن است. فرض کنید $1 \leq m \leq 2^k, \{A_m\}$ کد تعریف شده توسط H و همدسته‌های آن باشد. بنابراین $|A_m| = 2^{n-k}$ برای هر $1 \leq m \leq 2^k$ ،برای کد کردن پیام $s = (s_1, s_2, \dots, s_k)$ کدکننده، انتخابی تصادفی در بین 2^{n-k} عضو A_m که متناظر با s هستند، انجام می‌دهد. این کار معادل با این است که X^n یک انتخاب تصادفی از 2^{n-k} جواب $HX^t = s^t$ باشد که در آن t ترانهاده ماتریس است. کدکننده X^n را مشاهده می‌کند و HX^t را محاسبه می‌کند که همان جواب است. برای مطالعه بیشتر منبع [۸] را ببینید.

تعریف ۱.۱۱. [۸] فرض کنیم $C_1, C_2, \dots, C_n$ ستون‌های H باشند. فرض کنیم $\phi \subseteq \{1, 2, \dots, n\}$ و $D(\phi)$ بعد زیرفضای پیموده شده توسط $\{C_n\}_{n\in\phi}$ باشد. با در نظر گرفتن H به‌عنوان ماتریس کنترل زوجیت از مرتبه $n \times k$ ، برای $0 \leq \mu \leq n$ تعریف می‌کنیم

$$D^*(\mu) = min_{|\phi|=n-\mu} D(\phi)$$

قضیه ۲.۱۱. [۸] *فرض کنیم $D^*(\mu)$ متناظر با ماتریس کنترل زوجیت H با مرتبه $n \times k$ باشد. فرض کنیم w و w' به ترتیب وزن مینیمم کد و کد دوگان تعریف شده توسط H باشند. در این‌صورت داریم*

$$D^*(\mu) = \begin{cases} n-\mu & n-w+1 \leq \mu \leq n, \\ k & 0 \leq \mu \leq w'-1 \end{cases}$$

http://dx.doi.org/10.22108/MSCI.2022.130902.1473

قضیه ۳.۱۱. [۸] *برای کد کننده وکد گشاینده ساخته شده توسط ماتریس کنترل زوجیت H داریم*

$$\Delta = D^*(\mu).$$

توجه کنید که

$$\Delta_\mu = k - (\text{ابهام در } \mu)$$

همان ابهامی که دشمن در دریافت پیام کد شده با آن روبرو می‌شود.

فرستنده k بیت از اطلاعات را برای انتقال دادن به دریافت کننده، با استفاده از n کاربر در دست دارد. دشمن می‌تواند به هر s بیت از انتخابش گوش دهد. کانال انتقال را می‌توان بدون نویز فرض کرد. تمرکز بر روی این مساله است که دشمن از به‌دست آوردن اطلاعات زیاد، باز داشته شود. برای این کار می‌توان از کد خطی $[n, k]$ مانند C به‌روش زیر استفاده کرد:

- ۲^k همدسته [۱۵] وجود دارد.
- کدکننده یک همدسته را بر اساس k بیت از اطلاعات انتخاب می‌کند و یک بردار تصادفاً انتخاب شده را از آن همدسته انتقال می‌دهد.
- دشمن همه اطلاعات کد C را دارد اما دسترسی به فرایند تصادفی انتخاب یک بردار از همدسته را ندارد.

برای فهم بهتر مساله، مثالی ارایه می‌کنیم:

مثال ۴.۱۱. کد همینگ $C = [۱۵, ۱۱]$ را در نظر بگیرید. توجه کنید که $r = ۴, q = ۲$ بنا به آنچه در مثال ۱۶.۷ گذشت، داریم

$$WH(C) = \{۳, ۵, ۶, ۷, ۹, ۱۰, ۱۱, ۱۲, ۱۳, ۱۴, ۱۵\}.$$

توجه کنید که برای کد فوق داریم

$$d_۴ = ۷, d_۳ = ۶, d_۲ = ۵.$$

همچنین

$$WH(C^\perp) = \{۸, ۱۲, ۱۴, ۱۵\}.$$

از این کد می‌خواهیم برای انتقال $k = ۴$ بیت از اطلاعات استفاده کنیم. فرض کنیم s تعداد بیت‌هایی باشد که دشمن اجازه بهره برداری از آن را دارد. قرار می‌دهیم

$$\Delta_s = k - (\text{ابهام در } s)$$

از طرفی با توجه به تعریف ۱.۱۱ و قضیه ۳.۱۱ داریم

$$\Delta_s = min_{|I|=n-s} rank(< H_i : i \in I >)$$

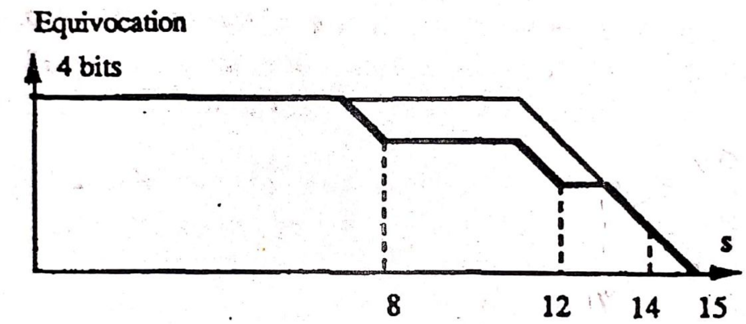
که H_i بردارهای ستونی ماتریس کنترل زوجیت C هستند و $< H_i : i \in I >$ زیرفضای تولید شده توسط بردارهای داخل براکت است.نمودار ضمیمه شده را که محور افقی آن s و محور عمودی آن Δ_s است را ببینید. با توجه به نمادگذاری‌های قضیه ۲.۱۱، اگر w و w' را به ترتیب وزن همینگ C و $C^\perp$ در نظر بگیریم، داریم

$k = ۴, w = ۳, w' = ۸$ لذا داریم

$$\Delta_s = \begin{cases} ۱۵ - s & ۱۳ \le s \le ۱۵, \\ ۴ & ۰ \le s \le ۷, \end{cases}$$

[15] coset

http://dx.doi.org/10.22108/MSCI.2022.130902.1473



حال برای رسم نمودار کافی است که مقدار Δ_s را در بازه $۸ \leq s \leq ۱۲$ تعیین کنیم. زیرا رابطه فوق برای بازه [۸, ۱۲] چیزی به‌دست نمی‌دهد. در حالتی‌که $s = ۸$ خواهیم داشت

$$\Delta_۸ = min(rankH_i : i \in I)_{|I|=۱۵-۸=۷}$$

می‌دانیم $d_۴ = ۷$ و از طرفی بنا به قضیه ۱۲.۷

$$min\{|X| : |X| - rank(< H_i : i \in X >) = ۴\} = d_۴$$

یعنی ۷ بردار وجود دارد که رتبه شان برابر ۳ است و این تعداد بردار، تعداد مینیمم است. در نتیجه $\Delta_۸ = ۳$. حال اگر $s = ۹$ باشد در این‌صورت $\Delta_۹ = min_{|I|=۶}(rankH_i : i \in I)$ چون $d_۳ = ۶$ و از طرفی بنا به قضیه ۱۲.۷

$$min\{|X| : |X| - rank(< H_i : i \in X >) = ۳\},$$

لذا ۶ بردار وجود دارد که رتبه شان ۳ است و این تعداد بردار، تعداد مینیمم است در نتیجه $\Delta_۹ = ۳$ به همین ترتیب با توجه به اینکه $\Delta_{۱۰} = min_{|I|=۵}(rankH_i : i \in I)$ و اینکه می‌توان ۵ بردار پیدا کرد که رتبه شان ۳ است، لذا خواهیم داشت $\Delta_{۱۰} = ۳$ و در نهایت خواهیم داشت $\Delta_{۱۱} = ۳$ اما در محاسبه $\Delta_{۱۲}$ با توجه به‌اینکه $\Delta_{۱۲} = min_{|I|=۳}(rankH_i : i \in I)$ و از طرفی $d_۱ = ۳$ و همچنین

$$min\{|X| : |X| - rank(< H_i : i \in X >) = ۱\} = d_۱,$$

در نتیجه ۳ بردار وجود دارد که رتبه شان ۲ است. در نتیجه خواهیم داشت $\Delta_{۱۲} = ۲$. چنانچه از نمودار بر می‌آید افت‌های منحنی در $\{۸, ۱۲, ۱۴, ۱۵\}$ رخ می‌دهد که این مجموعه همان سلسله وزن کد دوگان یعنی $C^\perp$ است.

نتیجه ۵.۱۱. *با در نظر گرفتن $\Delta_s = \Delta$ داریم*

$$d_{n-s-\Delta}(C^\perp) \leqslant n - s < d_{n-s-\Delta+۱}(C^\perp).$$

نتیجه فوق به این معنی است که افت‌های منحنی عدم قطعیت، دقیقاً در وزن‌های همینگ تعمیم یافته $C^\perp$ رخ می‌دهد. بنابراین سلسله وزن به‌طور کامل عملکرد یک کد خطی مانند C را روی کانال بهره‌برداری مخابراتی ۲ مشخص می‌کند.

مراجع

[1] S. T. Dougherty and S. Han, Higher Weights and Generalized MDS Codes, *Korean Math. Soc.*, no. 6 (2010) 1167–1182.

[2] F. Farhang Baftani and H. R. Maimani, The weight Hierarchy of Hadamard Codes, *Facta Univ. Ser. Math. Inform.*, **34** (2019) 797–803.

[3] F. Farhang Baftani and H. R. Maimani, The weight Hierarchy of Ham (r, q), *Italian Journal of Pure and applied Mathematics*, no 45, (2021).

[4] F. Farhang Baftani, The weight Hierarchy of $(u, u+v)$ Construction of Codes, *The* $51^s t$ *Annual Iranian Mathematics Conference*, Kashan, Iran, (2021) 15–20.

[5] F. Farhang Baftani, The weight Hierarchy of some BCH Codes, $11^t h$ *International Conference on Graph Theory and Algebraic Combinatorics*, Urmia University, Urmia, Iran, (2021).

[6] R. G. Gallager, *Information Theory and Reliable Communication*, Willey, New York, 1968.

[7] S. Ling and C. Xing, *Coding Theory A First Course*, Cambridge university press, 2004.

[8] L. H. Ozarow and A. D. Wyner, Wire- tap channel 2, *AT T Bell Labs Tech. J.*, **63** (1984) 2135-2157.

[9] V. K. Wei, Generalized Hamming Weights for linear codes, *IEEE Trans. Inform. Theory*, **37** (1991) 1412–1418.

فرزانه فرهنگ بافتانی

گروه ریاضی، واحد اردبیل، دانشگاه آزاد اسلامی، اردبیل، ایران.

far_farhang۲۰۰۷@yahoo.com

فرزانه فرهنگ بافتانی در شهر سراب از شهرهای استان آذربایجان شرقی متولد شده است. وی دوره کارشناسی خود، در رشته ریاضی را با کسب رتبه اول در دانشگاه محقق اردبیلی به پایان رساند و در دانشگاه تبریز دوره کارشناس ارشد خود را در گرایش جبر به پایان رساند. مقطع دکتری را در دانشگاه علوم و تحقیقات دانشگاه تهران در گرایش کدگذاری با راهنمایی جناب اقای دکتر حمیدرضا میمنی به پایان رسانید. علاقه وی در زمینه کاربرد مقالات ریاضی است.

http://dx.doi.org/10.22108/MSCI.2022.130902.1473

Introduction to Generalized Hamming Weight

Farzaneh Farhang Baftani

Abstract: Let C be a code over a finite field. The r-th Generalized Hamming weight(GHW), denoted by $d_r(C)$, is defined the minimum of support sizes of r- dimensional subcodes of C.GHW is important for its application in several fields such as Cryptography, Electronic Engineering, Computer and telecommunication Engineering. In this work, we will investigate this conception and its application.

Keywords: Hamming Weight, Generalized Hamming Weight, Hamming Code, Dual Code, Linear Codes, Non-linear Codes.

Farzaneh Farhang Baftani
Department of Mathematics, Ardabil Branch, Islamic Azad University, Ardabil, Iran.
Email: far_farhang2007@yahoo.com

Communicated by Alireza Abdollahi.
Article Type: Promotional.
Received: 07/10/2021, Accepted: 13/2/2022.

http://dx.doi.org/10.22108/MSCI.2022.130902.1473