
بسم الله الرحمن الرحيم

دانشگاه زنجان

دانشکده علوم- گروه ریاضی

پایان نامه کارشناسی ارشد

عنوان :

کدهای خودد و آل اکسترمال

دانشجو:

مریم ناصری

استاد راهنما:

دکتر مژگان امامی

شهریور ۱۳۹۰

تقدیم به:

پدر و مادرم

و

بهترین همراه زندگیم که همیشه در کنارش خواهم ماند.

تشکر و قدردانی

سپاس بی کران، پروردگار یکتا را که، هستی‌مان بخشید و به همنشینی رهروان علم و دانش مفتخرمان نمود و خوشه چینی از علم و معرفت را روزی‌مان ساخت.

از پدر فداکار و مادر مهربانم که همواره حامی من بوده اند سپاسگزارم و دستان‌شان را می بوسم.

از استاد گرامیم خانم دکتر امامی به خاطر تلاش های بی وقفه‌شان در طول این یک سال کمال تشکر را دارم.

در پایان، از سه برادرم که همیشه و در همه حال پشتیبانم بوده اند تشکر و برایشان آرزوی خوشبختی می نمایم.

همچنین برای دو برادر زاده‌ام میلاد و محیا آرزوی سلامتی و موفقیت را از خداوند منان خواهانم.

کدهای خوددوآل اکسترمال

چکیده

در این رساله، سعی می‌کنیم توزیع وزنی کدهای خوددوآل به طول $n \leq ۷۲$ را که بیشترین مینیمم فاصله‌ی ممکن d را دارند، مشخص کنیم و هم‌چنین تمام کدهای خوددوآل دوتایی اکسترمال تا طول ۷۲ و کدهای خوددوآل سه‌تایی اکسترمال تا طول ۶۰ را دسته‌بندی می‌کنیم. هر چند وجود بعضی از کدهای خوددوآل اکسترمال هنوز نامعلوم است.

فرم چندجمله‌ای وزن‌شمار کدهای خوددوآل، روی $GF(۲)$ و $GF(۳)$ را شرح داده یک فرم واضح برای این توزیع وزنی که مینیمم فاصله‌ی بین کلمات کدی تا حد ممکن بزرگ باشد را ارائه می‌دهیم. نتیجه می‌شود که برای کدهای خوددوآل به طول n روی $GF(۲)$ که تمام وزن‌هایش مضرب ۴ است، $d \leq ۴[n/۲۴] + ۴$ و برای کدهای خوددوآل روی $GF(۳)$، $d \leq ۳[n/۱۲] + ۳$ برقرار می‌باشد.

هدف نهایی در این رساله، ساخت بعضی از کدهای خوددوآل اکسترمال جدید و ارائه روش‌های کلی برای تولید این کدها بر اساس چندجمله‌ای وزن‌شمار آن‌ها می‌باشد. هم‌چنین کدهای خوددوآل دوتایی اکسترمال را که چندجمله‌ای وزن‌شمار مشخصی داشتند اما وجود خود کد معلوم نبود را نیز با استفاده از ماتریس‌هایی که معرفی می‌کنیم می‌سازیم. علاوه بر آن یک روش ساخت برای کدهای خوددوآل سه‌تایی نیز معرفی می‌کنیم، با استفاده از این روش یک سری کدهای خوددوآل سه‌تایی از ماتریس‌های وزنی به دست می‌آید.

واژه‌های کلیدی : کد خوددوآل - شادُو کد- کد اکسترمال- چندجمله‌ای وزن‌شمار

فهرست مطالب

مقدمه

در اواسط جنگ جهانی دوم، چند ریاضیدان بزرگ و در راس آن‌ها کلودشانون [۱] بررسی جامعی را درباره‌ی اصول ارتباطات شروع کردند. حاصل این بررسی در سال ۱۹۴۸ طی مقاله‌ای با عنوان نظریه‌ی ریاضی ارتباطات [۴۷] منتشر شد و انقلابی را در علم ارتباطات و کدگذاری پدید آورد، به طوری‌که از آن زمان تا به حال علم ارتباطات بر مبنای نظریات شانون پیشرفت‌های عظیمی کرده است. از نیمه‌ی دوم قرن بیستم، مطالعه‌ی ریاضی در دو حیطه‌ی مهم و گسترده‌ی نظریه‌ی ارتباطات و نظریه‌ی کدگذاری آغاز شد. نظریه‌ی ارتباطات، اساسا مدل ریاضی انتقال اطلاعات و کران‌های دست یافتنی در این تبادل را بررسی می‌کند و بیشتر بر احتمالات متکی است در صورتی که نظریه‌ی کدگذاری، با استفاده از ابزارهای جبری و هم‌چنین ریاضیات ترکیبی در صدد ایجاد ساختارهایی است که این کران‌ها را محقق و ممکن سازد.

شانون که در آزمایشگاه‌های شرکت تلفن بِل[۲] کار می‌کرد، در مقاله‌ی خود نشان داد ساختارهایی وجود دارند که با استفاده از آن‌ها می‌توان خطای ناشی از حضور اختلال در تبادل اطلاعات را به دلخواه کاست، اما اثبات وی تنها جنبه‌ی وجودی داشت و به این پرسش که چنین ساختارهایی چگونه باید ساخته شوند پاسخی نمی‌داد. دو سال بعد همینگ[۳] که او نیز همکار شانون در بِل بود و در مورد روش‌های ذخیره‌ی اطلاعات تحقیق می‌کرد در مقاله‌ی [۲۵]، نخستین بار زیر ساختارهای ترکیبیاتی را معرفی کرد که امروزه با نام نظریه‌ی کدگذاری یا نظریه‌ی کدهای تصحیح کننده‌ی خطا بررسی می‌شود. همینگ متوجه شد که برای حل مسئله، به دنباله‌هایی نیاز هست که به اندازه‌ی کافی با یکدیگر تفاوت داشته باشند و مفهوم فاصله را تعریف کرد که با نام خود او معروف است.

مبحث اصلی نظریه‌ی کدگذاری، مطالعه‌ی روش‌هایی برای انتقال اطلاعات به صورت دقیق و کارآمد از محلی به محل دیگر است. در این رساله از بین مباحث نظریه‌ی کدگذاری به بررسی کدهای

[۱] C. E. Shannon
[۲] Bell
[۳] Hamming

خاصی می‌پردازیم که به کدهای خوددوآل معروفند.

کدهای خوددوآل به دلایل زیر جزء کدهای جالب می‌باشند

۱. این کدها شامل بهترین کدهای تصحیح کننده‌ی خطا می‌باشند.

۲. کدهای خوددوآل ارتباط قوی با ترکیبیات، نظریه‌ی گروه‌ها و شبکه‌ها دارند و کاربرد این کدها در انتقال اطلاعات، شمارش و نظریه‌ی طرح‌ها می‌باشد.

کدهای خوددوآل به دلیل وسعت مطالب و روش‌های ساخت متعددی که دارند، از طریق ماتریس‌های وزنی، ماتریس‌های آدامار و طرح‌ها... ساخته می‌شوند که به عنوان موضوع این رساله مورد بررسی قرار می‌گیرند.

در فصل یک تعاریف و قضایای مقدماتی لازم را می‌آوریم. در فصل دو، شادُو کدهای دوتایی بررسی می‌شود که در به دست آوردن چندجمله‌ای وزن‌شمار کدهای دوتایی فوق به کار می‌رود. در فصل سه، کران مربوط به این کدها و فرم کلی چندجمله‌ای‌های وزن‌شمار کدهای خوددوآل دوتایی در حالت‌های زوجی منفرد و زوجی مضاعف و هم‌چنین برای کدهای خوددوآل سه‌تایی محاسبه می‌شود که این چندجمله‌ای‌ها برای کدهای خوددوآل اکسترمال به طول‌های $n \leq ۷۲$ در پیوست الف آورده می‌شود. در فصل چهار با ارائه روش‌های ساخت برای کدهای خوددوآل دوتایی، کدهایی را که چندجمله‌ای وزن‌شمار آن‌ها معلوم اما وجود خود کد نامعلوم است، برای طول‌های $n = ۳۴, ۳۸, ۴۰, ۴۲$ بررسی می‌کنیم و نحوه‌ی ساخت کدهای خوددوآل اکسترمال با طول‌های $n = ۴۴, ۵۴, ۵۸$ را به صورت جدول در پیوست پ می‌آوریم. در فصل پنج روش ساخت کدهای خوددوآل سه‌تایی به صورت قضایایی ارائه می‌شود، سپس به ساخت این کدها با استفاده از ماتریس‌های وزنی بر طبق قضایای معرفی شده می‌پردازیم. در پیوست ب، یک جدول از کدهای خوددوآل دوتایی اکسترمال را که تاکنون برای طول‌های $n \leq ۷۲$ بر طبق آخرین اطلاعات پیدا شده است ارائه می‌دهیم. در پیوست‌های ت، ج و چ ماتریس‌هایی را که برای ساخت کدهای خوددوآل دوتایی در فصل چهار به کار می‌رود ارائه می‌کنیم.

مریم ناصری

شهریور ۹۰

فصل ۱

تعاریف و قضایای مقدماتی

در این فصل ابتدا یک تعریف کلی از کد ارائه کرده و سپس به تعریف کد خطی و قضایای مربوط به آن، طرح‌های بلوکی و ماتریس‌های خاص موردنیاز فصول آتی برای ساخت کدها اشاره می‌کنیم. با ذکر این نکته که تمام کدها در این رساله کد خطی می‌باشند.

۱.۱ کدهای خطی

تعریف ۱.۱. کد C، مجموعه‌ی دنباله‌ای از نمادهای به طول n است که هر نماد از میدان $GF(q) = \{۰, ۱, ۲, \cdots, q-۱\}$ که q توانی از یک عدد اول است انتخاب می‌شود. به عبارت دیگر کد، تعدادی بردار از فضای برداری $V(n,q) = \{x_۱x_۲\cdots x_n \mid x_i \in GF(q)\}$ به طول n می‌باشد که مولفه‌های این بردارها از $GF(q)$ انتخاب می‌شوند.

- هریک از بردارهای یک کد را کلمه‌ی کدی می‌نامند.

تعریف ۲.۱. فاصله‌ی همینگ[۱] بین دو بردار $X = x_۱x_۲\cdots x_n$ و $Y = y_۱y_۲\cdots y_n$ تعداد مکان‌هایی است که با هم اختلاف دارند و به صورت زیر نمایش داده می‌شود

$$d(X,Y) = |\{i \mid x_i \neq y_i \, , \, ۱ \leq i \leq n\}| \, .$$

یکی از پارامترهای مهم کد C مینیمم فاصله‌ی d می‌باشد که به عنوان کوچکترین فاصله بین

[۱] Hamming distance

کلمات کدی مجزا تعریف می‌شود

$$d(C) = min\{d(X,Y) \mid X,Y \in C\ ,\ X \neq Y\}\ .$$

با توجه به توضیحات قبل کد C با پارامترهای n, M, d را به صورت $[n, M, d]$ -کد نشان می‌دهند که n طول کلمات کدی، M تعداد کل کلمات کدی و d مینیمم فاصله کد می‌باشد.

تعریف ۳.۱. یک زیرفضای k بعدی از فضای برداری $V(n,q)$ کد خطی نامیده شده و با $[n,k]_q$ نشان داده می‌شود. به طور معادل، زیرمجموعه‌ی C از $V(n,q)$ یک کدخطی است اگرو تنها اگر

۱. $\forall\, U, V \in C \Rightarrow U + V \in C$ ،

۲. $\forall\, U \in C, \lambda \in GF(q) \Rightarrow \lambda.U \in C$.

در حالت خاص، یک کد دوتایی خطی است اگروتنها اگر حاصل جمع هر دو کلمه‌ی کدی نیز یک کلمه‌ی کدی باشد.

اگر در کدخطی C مینیمم فاصله d معلوم باشد، کد خطی C را به صورت $[n,k,d]_q$ نمایش می‌دهیم. در یک کد خطی تعداد کل کلمات برابر $M = q^k$ می‌باشد.

مثال. کدهای زیر خطی می‌باشند

۱. $C = \{(\lambda, \cdots, \lambda) : \lambda \in GF(q)\}$ این کد را کد تکرار می‌نامند.

۲. $C = \{۰۰۰, ۰۰۱, ۰۱۰, ۰۱۱\}$ با $q = ۲$.

۳. $C = \{۰۰۰۰, ۱۱۰۰, ۲۲۰۰, ۰۰۰۱, ۰۰۰۲, ۱۱۰۱, ۱۱۰۲, ۲۰۰۱, ۲۲۰۲\}$ با $q = ۳$.

لم ۱.۱.۱. [۴۳] *فاصله همینگ یک تابع فاصله یا متریک است و در سه شرط زیر صدق می‌کند*

۱. $d(X,Y) = ۰ \iff X = Y$.

۲. $\forall\, X, Y \in GF(q)^n : d(X,Y) = d(Y,X)$.

۳. $\forall\, X, Y, Z \in GF(q)^n : d(X,Z) \leq d(X,Y) + d(Y,Z)$.

برهان. بررسی شرایط (۱) و (۲) آسان است. برای بررسی شرط (۳)، $d(X,Z)$ معادل با کمترین تعداد تغییراتی است که باید در X ایجاد کرد تا به Z تبدیل شود. اما برای تبدیل X به Z ابتدا X را به Y و سپس Y را به Z تبدیل می‌کنیم. □

تعریف ۴.۱. ماتریس $G_{k\times n}$ را که سطرهای آن تشکیل یک پایه برای $[n,k,d]$-کد خطی می‌دهد، ماتریس مولد [۲]کد خطی می‌نامند.

بقیه‌ی کلمات کدی از ترکیب خطی سطرهای ماتریس مولد به دست می‌آید.

- اگر ماتریس مولد کد خطی به صورت $G=[I,A]$ باشد که I ماتریس همانی $k\times k$ و A یک ماتریس $k\times(n-k)$ است، G را فرم استاندارد ماتریس مولد می‌نامند.
- اگر $X = x_1\cdots x_n$ یک کلمه‌ی کدی از کد خطی C باشد آنگاه وزن بردار X تعداد درایه‌های غیر صفر X می‌باشد

$$w(X)=|\{i \mid x_i\neq 0\}| .$$

تعریف ۵.۱. $W(C)$ را مینیمم وزن کد خطی C یا مینیمم وزن کلمات کدی غیر صفر می‌نامند هرگاه داشته باشیم

$$W(C)=min_{X\in C}w(X) .$$

لم ۲.۱.۱. [۴۳] *اگر X، Y دو بردار متعلق به $V(n,q)$ باشد، آنگاه $d(X,Y)=w(X-Y)$.*

برهان. بردار $X-Y$ در مکان‌هایی درایه‌های غیرصفر دارد که هر دو بردار X و Y در آن درایه با هم اختلاف داشته باشند. از آن‌جا که $w(X-Y)$ تعداد درایه‌های غیرصفر بردار $X-Y$ است، لذا این تعداد برابر با تعداد مکان‌هایی است که X و Y باهم اختلاف دارند. پس داریم

$$d(X,Y)=w(X-Y) .$$ □

- اگر $q=2$ باشد، آنگاه $d(X,Y)=w(X-Y)=w(X+Y)$.

لم ۳.۱.۱. [۴۳] *اگر X و Y بردارهایی در $GF(2)^n$ باشند آنگاه*

$$w(X+Y)=w(X)+w(Y)-2w(X\cap Y)$$

[۲] Generator matrix

که $X \cap Y = (x_1y_1, \cdots, x_ny_n)$ *می‌باشد.*

برهان.

$$\begin{aligned} d(X,Y) &= w(X+Y) \\ &= (\text{تعداد یک‌های X}) + (\text{تعداد یک‌های Y}) - ۲(\text{تعداد یک‌های مشترک X،Y}) \\ &= w(X) + w(Y) - ۲w(X \cap Y) . \end{aligned}$$

□

قضیه ۴.۱.۱. [۳۰] *مینیمم فاصله‌ی کد خطی C، مینیمم وزن هرکلمه‌ی کدی غیر صفر است*

$$W(C) = d(C) .$$

برهان. دو کلمه‌ی کدی X و Y از کد خطی C وجود دارند که مینیمم فاصله را تولید می‌کنند. بنابراین داریم

$$d(X,Y) = d(C) .$$

طبق لم، $d(X,Y) = w(X-Y)$. بنابراین خواهیم داشت

$$d(C) = d(X,Y) = w(X-Y) .$$

چون C یک کد خطی است پس $X-Y$ نیز یک کلمه‌ی کدی از کد خطی C می‌باشد، طبق تعریف مینیمم وزن داریم

$$d(C) = w(X-Y) \geq W(C) \Rightarrow d(C) \geq W(C) . \qquad (۱)$$

هم‌چنین کلمه‌ی کدی چون X وجود دارد که مینیمم وزن را تولید می‌کند، در نتیجه

$$W(C) = w(X) .$$

از طرفی چون C یک کد خطی و شامل کلمه‌ی کدی صفر نیز می‌باشد پس می‌توان نوشت

$$w(X) = w(X - \mathbf{0}) .$$

بنابراین داریم

$$W(C) = w(X) = w(X - \mathbf{0}) = d(X, \mathbf{0}) .$$

بنا به تعریف مینیمم فاصله

$$d(X, \mathbf{0}) \geq d(C) .$$

پس می‌توان نتیجه گرفت

$$W(C) = d(X, \mathbf{0}) \geq d(C). \qquad (۲)$$

لذا حکم از (۱) و (۲) حاصل می‌شود. □

تذکر ۱.۱. مینیمم فاصله و مینیمم وزن یک کد را در حالت خلاصه با d و W نشان می‌دهیم.

تعریف ۶.۱. اگر C یک کد خطی روی میدان متناهی $GF(q)$ باشد، کد دوآل C مجموعه‌ی بردارهایی از $V(n,q)$ می‌باشد که بر هر کلمه‌ی کدی C عمود است

$$C^{\perp} = \{v \in V(n,q) \mid u.v = ۰, \forall\, u \in C\} .$$

تعریف ۷.۱. ماتریس زوج‌آزمایی [۳] کد خطی C، ماتریسی است مانند H که ماتریس مولد کد خطی $C^{\perp}$ می‌باشد. ماتریس H یک ماتریس $(n-k) \times n$ می‌باشد که در شرط $GH^T = \mathbf{0}$ که H^T ترانهاده‌ی H و $\mathbf{0}$ ماتریس تماما صفراست، صدق می‌کند.

قضیه ۵.۱.۱. [۳۰] *فرض کنید C یک $[n,k]$- کد خطی با ماتریس مولد G باشد، آنگاه $v \in V(n,q)$ عضوی از $C^{\perp}$ است اگروتنها اگر v بر هر سطر G عمود باشد*

$$v \in C^{\perp} \iff v.G^T = \mathbf{0} .$$

برهان. فرض می‌کنیم $v \in C^{\perp}$ نشان می‌دهیم $v.G^T = \mathbf{0}$.

[۳] Parity check matrix

چون $v \in C^{\perp}$ ، پس

$$\forall\, u \in C : u.v = ۰\,.$$

از طرفی u یک کلمه‌ی کدی از کد خطی C می‌باشد، پس u به عنوان سطری از ماتریس مولد G یا ترکیب خطی سطرهای ماتریس مولد G می‌باشد، پس v بر هر سطر ماتریس مولد G عمود است، بنابراین داریم

$$v.G^{T} = \mathbf{0}. \qquad (۱)$$

برعکس، فرض می‌کنیم $v.G^{T} = \mathbf{0}$. در این صورت اگر g_i ، $\forall\, i : \ ۱ \leq i \leq k$ سطرهای ماتریس G باشند، آنگاه می‌دانیم هر کلمه‌ی کدی چون u از کد C بایستی ترکیب خطی از سطرهای ماتریس مولد G باشد

$$\begin{aligned}\forall\, u \in C : u &= \alpha_{۱} g_{۱} + \alpha_{۲} g_{۲} + \cdots + \alpha_{k} g_{k} \\ u.v &= \alpha_{۱}(v.g_{۱}) + \alpha_{۲}(v.g_{۲}) + \cdots + \alpha_{k}(v.g_{k}) \\ &= ۰ + ۰ + \cdots + ۰ = ۰ \Rightarrow v \in C^{\perp}\,.\end{aligned}$$

□

قضیه ۶.۱.۱. [۳۰] *فرض کنید C یک $[n,k]$-کد خطی روی $GF(q)$ باشد، آنگاه کد $C^{\perp}$ یک $[n, n-k]$-کد خطی می‌باشد.*

برهان. ابتدا نشان می‌دهیم که کد $C^{\perp}$ یک کد خطی است. یعنی نشان می‌دهیم یک زیرفضا از $V(n,q)$ می‌باشد.
فرض می‌کنیم $v_{۱}, v_{۲} \in C^{\perp}$ و $\lambda, \mu \in GF(q)$ باشند، پس

$$\begin{aligned}\forall\, u \in C : (\lambda v_{۱} + \mu v_{۲}).u &= \lambda v_{۱} u + \mu v_{۲} u = \lambda ۰ + \mu ۰ = ۰ \\ &\Rightarrow \lambda v_{۱} + \mu v_{۲} \in C^{\perp}\,.\end{aligned}$$

بنابراین $C^{\perp}$ یک کد خطی می‌باشد.

اگر فرض کنیم

$$G = \begin{pmatrix} g_{11} & \cdots & g_{1n} \\ \vdots & \ddots & \vdots \\ g_{k1} & \cdots & g_{kn} \end{pmatrix}$$

ماتریس مولد کد C باشد، می‌دانیم هر بردار $v = v_1 v_2 \cdots v_n \in C^\perp$ بر سطرهای ماتریس G عمود است. یعنی داریم

$$\begin{aligned} v_1 g_{11} + v_2 g_{12} + \cdots + v_n g_{1n} &= 0 \\ v_1 g_{21} + v_2 g_{22} + \cdots + v_n g_{2n} &= 0 \\ &\vdots \\ v_1 g_{k1} + v_2 g_{k2} + \cdots + v_n g_{kn} &= 0 . \end{aligned}$$

دستگاه معادلات فوق از k معادله و n مجهول تشکیل شده است، چون تعداد معادلات از تعداد مجهولات کمتر است لذا دستگاه جواب غیربدیهی دارد. برای حل دستگاه از فرم استاندارد ماتریس مولد استفاده کرده و مجهولات را به دست می‌آوریم.

$$G = \begin{pmatrix} g_{11} & g_{12} \cdots & g_{1n} \\ g_{21} & g_{22} \cdots & g_{2n} \\ \vdots & \ddots & \vdots \\ g_{k1} & g_{k2} \cdots & g_{kn} \end{pmatrix} = \begin{pmatrix} 1 & 0 \ldots 0 & a_{11} & a_{12} \ldots a_{1(n-k)} \\ 0 & 1 \ldots 0 & a_{21} & a_{22} \ldots a_{2(n-k)} \\ \vdots & \ddots & \vdots & \ddots \\ 0 & 0 \ldots 1 & a_{k1} & a_{k2} \ldots a_{k(n-k)} \end{pmatrix}$$

و اگر $v \in C^\perp$ پس $v.G^T = \mathbf{0}$، آنگاه

$$\begin{aligned} v_1 + a_{11} v_{k+1} + a_{12} v_{k+2} + \cdots + a_{1(n-k)} v_n &= 0 \\ v_2 + a_{21} v_{k+1} + a_{22} v_{k+1} + \cdots + a_{2(n-k)} v_n &= 0 \\ &\vdots \\ v_k + a_{k1} v_{k+1} + a_{k2} v_{k+2} + \cdots + a_{k(n-k)} v_n &= 0 \end{aligned}$$

لذا خواهیم داشت

$$C^{\perp} = \{(v_۱, v_۲, \cdots, v_n) \,|v_i + \sum_{j=۱}^{n-k} a_{ij}.v_{k+j} = ۰ : i = ۱, ۲, \cdots, k\} .$$

برای حل دستگاه مقادیر $v_{k+۱}, \cdots, v_n$ را به دلخواه انتخاب می‌کنیم، سپس مقادیر $v_۱, \cdots, v_k$ به طور منحصر به فرد محاسبه می‌گردند. بنابراین $|C^{\perp}|$ برابر با تعداد حالت‌هایی است که می‌توان $v_{k+۱}, \cdots, v_n$ را انتخاب نمود. با توجه به این که v_i ، $\forall\ k+۱ \leq i \leq n$ از $GF(q)$ انتخاب می‌شوند پس برای هر یک q حالت وجود دارد، بنابراین

$$|C^{\perp}| = q^{n-k} \Rightarrow dim(C^{\perp}) = n-k . \qquad \square$$

تذکر ۲.۱. طبق قضایای قبل اگر H ماتریس زوج‌آزمایی کد خطی C باشد، آنگاه کد C به طور کامل توسط ماتریس H مشخص می‌شود

$$C = \{X \in V(n,q) \mid X.H^T = \mathbf{0}\} .$$

حال نحوه‌ی به دست آوردن ماتریس زوج‌آزمایی H را از روی ماتریس مولد G طبق قضیه‌ای بررسی می‌کنیم.

قضیه ۷.۱.۱. [۳۰] *اگر $G = [I_k, A]$ شکل استاندارد ماتریس مولد $[n,k]$ -کد خطی C باشد، آنگاه ماتریس زوج‌آزمایی کد C به صورت $H = [-A^T, I_{n-k}]$ می‌باشد.*

برهان. فرض کنید فرم استاندارد ماتریس مولد G به صورت زیر باشد

$$G = \begin{bmatrix} ۱ & ۰ \ldots ۰ & a_{۱۱} & a_{۱۲} \ldots a_{۱(n-k)} \\ ۰ & ۱ \ldots ۰ & a_{۲۱} & a_{۲۲} \ldots a_{۲(n-k)} \\ \vdots & \ddots & \vdots & \ddots \\ ۰ & ۰ \ldots ۱ & a_{k۱} & a_{k۲} \ldots a_{k(n-k)} \end{bmatrix} .$$

ماتریس H را به صورت زیر در نظر می‌گیریم

$$H = \begin{bmatrix} -a_{11} & -a_{21} & \cdots & -a_{k1} & 1 & 0\cdots 0 \\ -a_{12} & -a_{22} & \cdots & -a_{k2} & 0 & 1\cdots 0 \\ \vdots & \ddots & \vdots & \ddots & & \\ -a_{1(n-k)} & -a_{2(n-k)} & \cdots & -a_{k(n-k)} & 0 & 0\cdots 1 \end{bmatrix}.$$

تعداد سطرهای ماتریس H ، $n-k$ می‌باشد و طبق ساختاری که شکل استاندارد دارد سطرهایش مستقل خطی است و بدیهی است که هر سطر H بر هر سطر G عمود است. □

تعریف ۸.۱. کد خطی C یک کد خوددوآل است هرگاه $C = C^{\perp}$ و یک کد خود متعامد است هرگاه $C \subseteq C^{\perp}$.

مثال. فرض کنید ماتریس مولد $[4, 2]_3$-کد خطی C به صورت زیر باشد

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 2 & 1 \end{bmatrix}.$$

آنگاه کلمات کدی و ماتریس مولد $[4, 2]_3$ -کد خطی $C^{\perp}$ به صورت زیر می‌باشد.

$$C = \{0000, 1011, 0121, 2022, 0212, 1102, 1220, 2110, 2201\}.$$

ماتریس مولد کد $C^{\perp}$ به صورت زیر می‌باشد

$$\mathbf{H} = \begin{bmatrix} 1 & 2 & 2 & 0 \\ 1 & 1 & 0 & 2 \end{bmatrix}.$$

از روی ماتریس مولد کد $C^{\perp}$ می‌توان کلمات کدی آن را به دست آورد

$$C^{\perp} = \{0000, 1220, 1102, 2110, 2201, 2022, 0121, 0212, 1011\}.$$

از آن‌جا که کلمات کدی C و $C^{\perp}$ عین هم می‌باشند و تعدادشان هم با هم برابر است پس کد C یک کد خوددوآل می‌باشد.

- اگر C یک $[n.k]$-کد خوددوآل باشد آنگاه تعداد کلمات کدهای C و $C^{\perp}$ باهم برابر است، یعنی داریم

$$q^k = q^{n-k} \Rightarrow k = n - k \Rightarrow k = \frac{n}{۲} .$$

بنابراین یک کد خوددوآل را به صورت $[n, \frac{n}{۲}]$ -کد نشان می‌دهیم.

تعریف ۹.۱. یک کد دوتایی زوج نامیده می‌شود اگر تمام کلمات کدی آن وزن زوج داشته باشد.

واضح است که کدهای خوددوآل دوتایی دارای وزن زوج می‌باشند. یعنی اگر C یک کد خوددوآل دوتایی باشد آنگاه معلوم است که

$$\forall\, X \in C : w(X) \equiv ۰ \pmod{۲} .$$

چون کد خوددوآل است پس هر دو سطر دلخواه و از جمله هر سطر بر خودش عمود است، بنابراین

$$X.X = x_۱x_۱ + \cdots + x_nx_n = \sum_{i=۰}^{n} x_i^۲ = \sum_{i=۰}^{n} x_i = ۰ \Rightarrow w(X) \equiv ۰ \pmod{۲} .$$

- بعضی از کدهای خوددوآل وجود دارند که وزن تمام کلمات آن مضرب ۴ می‌باشند به این‌گونه کدهای خوددوآل، کدهای خوددوآل زوجی مضاعف می‌نامند.

$$\forall\, X \in C : w(X) \equiv ۰ \pmod{۴} .$$

- کدهای خوددوآل زوجی مضاعف را کدهای نوع ۲[۴] نیز می‌نامند.
- اگر کد خوددوآل که زوجی مضاعف نباشد، آن را خوددوآل زوجی منفرد یا کد خوددوآل نوع ۱[۵] نامیده و هرگاه کد خوددوآل بیشترین مینیمم وزن ممکن برای آن طول را داشته باشد کد خوددوآل اکسترمال[۶] نامیده می‌شود.

تعریف ۱۰.۱. اگر یک سری از کلمات کدی کد C را انتخاب کنیم به طوری‌که این کلمات خود تشکیل یک کد بدهد، کد حاصل را یک زیرکد از کد C می‌نامند. این زیرکد می‌تواند خطی یا غیر خطی باشد.

[۴] Type II
[۵] Type I
[۶] Extremal