بسم الله الرحمن الرحيم

دانشگاه زنجان

دانشکده علوم

گروه ریاضی

سیستم‌های تفاضلی مجموعه‌ها

پایان‌نامهٔ کارشناسی ارشد

سعید زراعتی شمس‌آبادی

استاد راهنما: دکتر مژگان امامی

۱۳۸۷

دانشگاه زنجان

شماره: ۲۳۶۰۳۴/دع

تاریخ: ۸۷/۱۱/۲۷

صورتجلسه دفاع از پایان نامه کارشناسی ارشد

با تأییدات خداوند متعال و با استعانت از حضرت ولی‌عصر (عج) جلسه دفاع از پایان‌نامه کارشناسی‌ارشد

آقای **سعید زراعتی شمس‌آبادی** رشته **ریاضی** گرایش **کاربردی**

تحت عنوان : **سیستم‌های تفاضلی مجموعه‌ها**

در تاریخ ۸۷/۱۱/۲۷ با حضور هیأت محترم داوران در دانشگاه زنجان برگزارگردید و نظر هیأت داوران بشرح زیر می‌باشد:

قبول(با درجه :......عالی......... امتیاز: ....۱۹/۰۰.........) دفاع مجدد ☐ مردود ☐

۱- عالی(۲۰-۱۸)

۲- بسیارخوب(۱۷/۹۹- ۱۶)

۳- خوب(۱۵/۹۹- ۱۴)

۴- قابل قبول(۱۳/۹۹- ۱۲)

عضو هیأت داوران	نام و نام خانوادگی	رتبه علمی	امضاء
۱- استاد راهنما	دکتر مژگان امامی	استادیار	
۲- استاد ممتحن خارج ازدانشگاه	دکتر منوچهر ذاکر	دانشیار	
۳- استاد ممتحن داخل دانشگاه	دکتر سیدمحسن نجفیان	استادیار	
۴- نماینده تحصیلات تکمیلی	دکتر ابراهیم احمدی	استادیار	

دانشگاه زنجان
دکتر نعمت‌ا... ارشدی
مدیر تحصیلات تکمیلی دانشگاه

دکتر محمدعلی اسمخانی
معاون آموزشی و تحصیلات تکمیلی
دانشکده علوم
۸۷/۱۲/۳

تقدیم به پدر عزیزم

پدری که برای من مادر هم بوده است، پدری که تمام جوانی‌اش را صرف من کرده است. پدری که شب‌ها تا صبح بالای سر من بیدار بوده است، پدری که همیشه مرا در آغوش گرم خود خوابانیده است. پدری که هیچ وقت مرا تنها نگذاشته و نخواهد گذاشت. پدری که چون شمع آب شد تا دنیا برای من روشن شود.

پدر عزیزم؛ هیچ وقت نمی‌توانم همه‌ی خوبی‌هایت را ببینم چه برسد به این که بازگو کنم.

پدر عزیزتر از جانم، همیشه محبت‌هایت جلوی چشمانم است.

همیشه در قلب منی

دوستت دارم

سعید تو

قدردانی و تشکر

در ابتدا، خداوند مهربان را شکر می‌گویم که در تنهاترین لحظات زندگی‌ام مرا تنها نگذاشته و هیچ گاه مرا به حال خودم وانمی‌گذارد.

از استاد راهنمایم، خانم دکتر مژگان امامی، کمال تشکر و قدردانی را دارم که در همه‌ی زمینه‌ها همکاری لازم را مبذول داشته‌اند و همیشه با صبر و حوصله مرا یاری نموده‌اند. لازم به‌ذکر است که ایشان در انتخاب موضوع پایان‌نامه، تصویب آن، جمع آوری منابع و مقالات، ویرایش پایان‌نامه و به‌خصوص در حل مسائل و مشکلات آن، بیش از انتظار، مرا یاری کرده‌اند. برای ایشان موفقیت و سربلندی در همه‌ی عرصه‌های زندگی‌شان را از درگاه ایزد منان خواستارم.

از دکتر خسروشاهی کمال نیز متشکرم؛ ایشان با معرفی من به پروفسور تانچف [1]، راهی برای دستیابی به مقالات باز کردند.

از پروفسور تانچف ، استاد دانشگاه MTU[2]، سپاسگزارم، ایشان با در اختیار قرار دادن برخی از مقالاتشان، مرا در فهم هر چه بهتر موضوع یاری نمودند.

از آقای دکتر اسمخانی تشکر می‌کنم؛ ایشان در حل برخی از مسائل جبری این پایان نامه مرا یاری کردند.

از جناب آقای جواد ابراهیمی، دانشجوی دکتری دانشگاه SFU [3]، کمال تشکر و قدردانی را دارم. ایشان نه تنها به من، بلکه به کلیه‌ی دانشجویان ایرانی در دستیابی به مقالاتی که در ایران در دسترس نیست، یاری می‌رسانند که کار ایشان قابل ستایش و تحسین است.

از آقای دیوید کلارک [4]، دانشجوی دکتری دانشگاه MTU، نیز ممنونم؛ ایشان مرا در دستیابی به یکی از مقالاتی که تا آن موقع به چاپ نرسیده بود یاری رساندند.

تشکر ویژه‌ای از خانم نعمتی دارم که مرا در نگارش پایان‌نامه در محیط‌های فارسی‌تک و Powerpoint بی‌نهایت یاری رساندند و هم‌چنین در ویرایش و تصحیح مطالب از لحاظ نگارشی بیش از اندازه با من همکاری داشتند.

در این جا، جا دارد از دوست عزیز و شفیقم، آقای مصطفی قادریان بسیار تشکر کنم ؛ ایشان همیشه با همراهی و همدلی‌هایشان مرا تشویق به ادامه‌ی کارهای پژوهشی نموده‌اند.

---

[1] V.Tonchev

[2] Michigan Technological University

[3] Siman Fraser University

[4] David Clark

از همسر عزیزم که مراتشویق به ادامه‌ی تحصیل کرده و می‌کند کمال تشکر و قدردانی را دارم و هم‌چنین از صبر و بردباری ایشان در زمان تحصیلم، بی‌نهایت سپاس‌گزارم.

در نهایت باز هم از پدرم تشکر می‌کنم که هر چقدر هم تشکر بکنم کم است.

سعیدزراعتی

بهمن ۱۳۸۷

چکیده

سیستم‌های تفاضلی مجموعه‌ها (DSS) ساختارهای ترکیبیاتی هستند که در ارتباط با انطباق کدی به وجود آمده‌اند. در این رساله ابتدا برای هر عدد اول n به طوری که $n \equiv ۳ \pmod{۴}$، یک روش برای ساختن DSS ها از افراز مجموعه‌های تفاضلی دوری معرفی می‌شود؛ سپس برای اعداد اول n به طوری که $n \equiv ۱ \pmod{۴}$، به ساختاری مشابه آن‌را گسترش می‌دهیم که این ساختار از افراز گردایه اعداد مربعی بهره می‌جوید. در انتها یک الگوریتم برای یافتن DSS های بهینه معرفی می‌شود.

فهرست مندرجات

مقدمه ۱

۱ مفاهیم و تعاریف اولیه ۳

۲ سیستم‌های تفاضلی مجموعه‌ها و کدهای همگام با آن‌ها ۶

۱.۲ سیستم تفاضلی مجموعه‌ها (DSS) و شاخص کاما-آزاد ۶

۲.۲ کاربرد $\rho(C)$ و $d(C)$ و بهترین حالت این دو نسبت به یکدیگر ۹

۳.۲ کدهای همگام با DSS ها ۱۰

۴.۲ DSS های بهینه ۱۳

۳ DSS های به‌دست آمده از افراز مجموعه‌های تفاضلی ۱۵

۱.۳ تبدیل‌پذیری هر مجموعه تفاضلی به DSS ۱۵

۲.۳ به‌دست آوردن DSS های کامل منظم برای $n = mq + ۱$ های اول ۱۸

۳.۳ به‌دست آوردن DSS های کامل منظم از افراز گردآیه عناصر مربعی غیرصفر برای n های اولی که $n \equiv ۳ \pmod{۴}$ ۲۰

۴ DSS ها و باقیمانده‌های مربعی ۲۴

۱.۴ مجموعه تفاضلی نسبی ۲۴

۲.۴ یک DSS منظم با پارامترهای (n, m, q, ρ)، وقتی $n = ۲mq + ۱$ ۲۶

۳.۴ بررسی حالات $m = ۲, ۳, ۴, ۵, ٦$ ۳۰

۵ یک الگوریتم برای یافتن DSS های بهینه ۴۵

۱.۵ تعاریف و لم‌های لازم برای الگوریتم ۴۵

۲.۵ به‌دست آوردن q ـ افراز ۴۷

۳.۵ روندی برای یافتن DSSها ۴۸

پیوست ۱ . . . . ۵۲

پیوست ۲ . . . . ٦۱

منابع ۹٦

واژه‌نامه‌ی فارسی به انگلیسی ۹۷

واژه‌نامه انگلیسی به فارسی ۹۸

مقدمه

با معرفی کدها بحث انتقال آن‌ها از طریق یک کانال مطرح شد، برای این منظور از روش‌های مختلفی استفاده می‌شد که یکی از این راه‌ها، پشت سر هم قرار دادن کلمه‌ها به طول n، به‌صورت یک دنباله‌ی متناهی از اعداد یا حروف است.

در طول مسیر کانال ممکن است عواملی که ما آن‌ها را خطا می‌نامیم روی دنباله اثر کرده و یک سری از جمله‌های این دنباله‌ها را تغییر دهد؛ از طرف دیگر ممکن است در حین عمل ارسال و دریافت، چند جمله‌ی اول یا آخر دنباله گم شود (فرض بر این است در طی عمل انتقال، جمله‌های دنباله می‌توانند دچار خطا شده و تغییر کنند، ولی هیچ جمله‌ای گم نمی‌شود).

در این‌جا اولین مشکلی که با آن روبرو هستیم این است که در دنباله‌ی دریافتی کدام n درآیه‌ی متوالی یک کلمه‌ی کدی می‌باشد؛ پس برای هر کد نیاز به تعریف مشخصه‌ای بود که بیانگر قدرت تشخیص خود کلمه‌ها از اتصالشان بود؛ این کار اولین بار به‌طور رسمی‌توسط گُلُمْب [۱]، گُرْدُن [۲] و وِلْچ [۳] در سال ۱۹۵۸ انجام شد که آن را شاخص کاما-آزاد یک کد نامیدند [۵].

حال در کدهای q تایی با طول و شاخص کاما-آزاد مشخص، چیزی که اهمیت می‌یابد این است که کدام کد دارای تعداد کلمه‌ها کدی بیشتری است؛ پس با پارامترهای داده شده کدی که دارای بیشترین تعداد کلمه بوده، بهینه است.

لونشتین [۴] در سال ۱۹۷۱ به فکر به‌دست آوردن کدهایی افتاد که شاخص کاما-آزاد آن از مقدار مشخصی کمتر نباشد؛ بدین منظور نوعی طرح ترکیبیاتی به نام سیستم تفاضلی مجموعه‌ها (DSS) با پارامترهای $(n, \tau_0, \tau_1, \ldots, \tau_{n-1}, \rho)$ را معرفی کرد، سپس از روی این DSS، یک کد غیرخطی با حداقل شاخص کاما-آزاد ρ به‌دست آورد [۶]، به‌علاوه نشان داد که برای DSS های با n، ρ و q یکسان، بعد کد به‌دست آمده حداکثر $n - \sqrt{\frac{q\rho(n-1)}{q-1}}$ می‌باشد.

---

۱ S.W.Golomb

۲ B.Gordon

۳ L.R.Welch

۴ V.I. Levenshtein

پس از معرفی DSSها توسط لونشتین، این موضوع چند دهه به فراموشی سپرده شد تا این‌که تانچف [1] به فکر روشی برای ساختن DSSها افتاد؛ سرانجام او در سال ۲۰۰۳ موفق به ساختن DSSها برای n های اولی که $n \equiv ۳(mod ۴)$ از افراز مجموعه‌های دوری شد و از افراز گردآیه اعداد مربعی که یک $(n, \frac{n-۱}{۲}, \frac{n-۳}{۴})$ مجموعه‌ی دوری بود DSS منظم کامل به‌دست آورد [۱۱].

سپس در سال ۲۰۰۸ موته [2] و دیگران برای n های اولی که $n \equiv ۱ \pmod{۴}$، موفق به ساخت DSS ها از افراز گردآیه اعداد مربعی شدند [۹].

سرانجام در سال ۲۰۰۷ تانچف با کمک دیگران الگوریتمی برای یافتن DSSهایی ارائه کرد که کدهای به‌دست آمده از روی این DSSها دارای بیشترین بعد ممکن باشند [۱۲].

V. Tonchev[1]

Y. Mutoh[2]

فصل ۱

مفاهیم و تعاریف اولیه

در این فصل کلیه‌ی تعاریف و قضایای مقدماتی مورد استفاده در فصول بعدی ارائه شده است. قابل ذکر است که کلیه‌ی مطالب این فصل از منابع [۱۰،۸،۷،۴،۳،۲،۱] برگرفته شده است.

به مجموعه‌ای که می‌تواند عضو تکراری داشته باشد مجموعه چندگانه می‌گوییم. اگر n و q دو عدد طبیعی باشند آنگاه F_q و F_q^n را به‌صورت زیر تعریف می‌کنیم:

$$F_q = \{0, 1, \dots, q-1\},$$

$$F_q^n = \{(a_1, \dots, a_n) \mid a_i \in F_q \,,\, 1 \leq i \leq n\}.$$

فرض کنیم G یک گروه باشد؛ اگر یک عنصر $\alpha \in G$ وجود داشته باشد به‌طوری که $G = \{\alpha^m | m \in Z\}$، آنگاه G را یک گروه دوری (تولید شده توسط α) می‌نامیم؛ در این حالت α را مولد G گوییم و می‌نویسیم $G = < \alpha >$.

اگر F میدانی متناهی باشد آنگاه $F \setminus \{0\}$ گروهی دوری است و آن‌را با F^* نشان می‌دهیم؛ حال اگر α مولد گروه دوری F^* باشد آنگاه α را عنصر اولیه و α^{2i} ها را عناصر مربعی میدان F می‌نامیم و گردآیه‌ی عناصر مربعی را با Q نشان می‌دهیم.

به ازای هر عدد اول p و هر عدد صحیح مثبت n، با تقریب یک یکریختی، یک و فقط یک میدان با p^n عنصر وجود دارد. بنابراین اگر q یک توان اول باشد، F_q یک میدان متناهی از مرتبه q است که هر میدان متناهی از مرتبه q با آن

یکریخت است؛ در این حالت برای $0 < i \leq q-1$، i را می‌توان، i امین توان یک عنصر اولیه F_q در نظر گرفت.

W زیرفضایی خطی از فضای خطی V روی میدان F است هرگاه:

$$W \subseteq V, \quad \forall \alpha, \beta \in F, \forall w_1, w_2 \in W;\ \alpha w_1 + \beta w_2 \in W.$$

یک کد q تایی به طول n، یک زیرمجموعه از F_q^n است ؛ هم‌چنین یک کد خطی q تایی به طول n، یک زیرفضای خطی از F_q^n است. فاصله همینگ بین دو بردار $y = y_1 \dots y_n \in F_q^n$ و $x = x_1 \dots x_n$ را با $d(x, y)$ نشان می‌دهیم و عبارت است از تعداد مکان‌هایی در هر دو بردار که دارای مؤلفه یکسان نیستند یا به‌طور معادل:

$$d(x, y) = |\{i | x_i \neq y_i\}|.$$

فرض کنید C یک کد روی میدان F_q باشد؛ مینیمم فاصله‌ی کلمه‌ها کد C را با $d(C)$ نشان می‌دهیم و آن‌را به‌صورت زیر تعریف می‌کنیم:

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

بنابراین هر کلمه‌ی کدی که حداکثر $[\frac{d(c)-1}{2}]$ خطا دارد را می‌توانیم تصحیح کنیم؛ در حالتی که C یک کد خطی روی میدان F_q باشد؛ برای هر بردار $a \in F_q^n$، مجموعه $a + C$ را یک هم رده از کد C گوییم و آن‌را به‌صورت زیر تعریف می‌کنیم:

$$a + C = \{a + x | x \in C\}.$$

فرض کنید $x = x_1 x_2 \dots x_n$؛ i امین شیفت به چپ x عبارت است از $x_{i+1} \dots x_n x_1 x_2 \dots x_i$. به روش مشابه شیفت به راست x تعریف می‌شود.

یک PBD [1] یا یک طرح زوجی متعادل (v, K, λ)، عبارت است از گردآیه‌ای از زیرمجموعه‌های یک مجموعه‌ی v عضوی مثل D، که به هر مجموعه‌ی آن یک بلوک گفته می‌شود، به شرط آن که سایز هر بلوک کوچکتر از v و در K قرار داشته باشد و هر دو عضو D دقیقاً در λ بلوک وجود داشته باشند.

[1] Pairwise balanced design

فرض کنید G یک گروه و $H \leq G$؛ اگر $a \in G$ آنگاه $aH = \{ah \,|\, h \in H\}$ را یک هم‌مجموعه چپ و $Ha = \{ha \,|\, h \in H\}$ را یک هم‌مجموعه راست H در G می‌نامیم.

اگر G یک گروه جمعی باشد هم‌مجموعه‌ی چپ و راست به‌ترتیب عبارت‌اند از:

$$H + a = \{h + a \,|\, h \in H\}\ ,\ a + H = \{a + h \,|\, h \in H\}\,.$$

اگر G یک گروه آبلی باشد هم‌مجموعه‌های چپ و راست عضو دلخواه $a \in G$ با هم برابرند و به آن هم‌مجموعه گوییم؛ حال مدار H تحت G عبارت است از تمام هم‌مجموعه‌های چپ H در G.

قضیه ۱.۰.۱ (نامساوی چبیشف): فرض کنید q یک عدد صحیح مثبت باشد و برای $\circ \leq i \leq q - ۱$، a_i ها و b_i ها اعدادی صحیح باشند، آنگاه داریم:

$$(\sum_{i=\circ}^{q-۱} a_i)(\sum_{i=\circ}^{q-۱} b_i) \leq q\,(\sum_{i=\circ}^{q-۱} a_i b_i)\,.$$

در زیر به معرفی قضیه‌ای می‌پردازیم که به‌نام محک اویلر معروف است.

قضیه ۲.۰.۱ فرض کنید n یک عدد اول فرد و a یک عدد صحیح باشد به‌طوری که n و a نسبت به هم اول باشند؛

a در GF(n) یک عدد مربعی است اگر و تنها اگر $a^{\frac{n-۱}{۲}} \equiv ۱ \pmod{n}$ و

a در GF(n) یک عدد غیر مربعی است اگر و تنها اگر $a^{\frac{n-۱}{۲}} \equiv -۱ \pmod{n}$.

از محک اویلر نتیجه می‌شود که:

۲ در GF(n) یک عدد مربعی است اگر و تنها اگر $n \equiv \pm ۱ \pmod{۸}$ و

۲ در GF(n) یک عدد غیر مربعی است اگر و تنها اگر $n \equiv \pm ۳ \pmod{۸}$.

فصل ۲

سیستم‌های تفاضلی مجموعه‌ها و کدهای همگام با آن‌ها

در این فصل، ابتدا سیستم تفاضلی مجموعه‌ها و شاخص کاما-آزاد را تعریف کرده، سپس شاخص کاما-آزاد و مینیمم فاصله‌ی کلمه‌ها یک کد را با هم مقایسه می‌کنیم؛ در بخش سوم نشان می‌دهیم که چگونه از روی یک DSS [1] می‌توان یک کد با شاخص کاما-آزاد حداقل ρ به‌دست آورد و در انتها، کرانی برای DSSهای بهینه به‌دست می‌آوریم.

۱.۲ سیستم تفاضلی مجموعه‌ها (DSS) و شاخص کاما-آزاد

در این بخش پس از معرفی سیستم تفاضلی مجموعه‌ها و شاخص کاما-آزاد، نشان می‌دهیم شاخص کاما-آزاد کدهای خطی صفر است؛ سپس در گزاره‌ای نشان می‌دهیم شاخص کاما-آزاد یک کد چگونه می‌تواند ما را در تشخیص یک کلمه‌ی کدی از اتصال دو کلمه‌ی کدی یاری کند.

تعریف ۱.۱.۲ یک سیستم تفاضلی مجموعه‌ها (DSS) با پارامترهای $(n, \tau_۰, \tau_۱, \ldots, \tau_{q-۱}, \rho)$ عبارت است از، گردآیه‌ای شامل q زیرمجموعه مجزای $\{۱, ۲, \ldots, n\} \supseteq Q_i$، $|Q_i| = \tau_i$ و $۰ \le i \le q - ۱$، به‌طوری که هر عدد i،

[1] Difference System of Sets

$1 \leq i \leq n-1$، حداقل ρ بار در مجموعه چندگانه زیر موجود باشد:

$$\{a-b \pmod n) |\, a \in Q_i \,, b \in Q_j \,, 0 \leq i,j \leq q-1, i \neq j\}. \qquad (1)$$

یک DSS کامل است اگر هر عدد i، $1 \leq i \leq n-1$، دقیقاً ρ بار در مجموعه چندگانه (۱) موجود باشد.

یک DSS منظم است اگر همه زیرمجموعه‌های Q_i از یک اندازه یکسان $\tau_0 = \tau_1 = \ldots = \tau_{q-1} = m$ باشند؛ برای یک DSS منظم روی n نقطه و q زیرمجموعه به اندازه m، از نماد (n, m, q, ρ) استفاده می‌شود.

مثال ۱.۱.۲ فرض کنید $n = 9$، $Q_0 = \{1, 2\}$ و $Q_1 = \{3, 5\}$ باشند. تفاضل‌های بین دو مجموعه به‌پیمانه ۹ عبارت است از:

$$\begin{aligned} 3-1 &\equiv 2 \pmod 9, & 1-3 &\equiv 7 \pmod 9,\\ 5-1 &\equiv 4 \pmod 9, & 1-5 &\equiv 5 \pmod 9,\\ 3-2 &\equiv 1 \pmod 9, & 2-3 &\equiv 8 \pmod 9,\\ 5-2 &\equiv 3 \pmod 9; & 2-5 &\equiv 6 \pmod 9, \end{aligned}$$

بنابراین مجموعه (۱) به‌فرم زیر درمی آید:

$$\{1, 2, 3, 4, 5, 6, 7, 8\};$$

حال با توجه به این‌که هر عدد i، $1 \leq i \leq 8 = 9-1$، حداقل یک بار در مجموعه بالا قرار دارد، پس Q_0 و Q_1 تشکیل یک DSS با پارامترهای $(9, 2, 2, 1)$ می‌دهند؛ از یک طرف چون هر عدد i، $1 \leq i \leq 8$ دقیقاً یک بار در مجموعه بالا قرار دارد، DSS فوق کامل است و از طرف دیگر چون اندازه Q_0 و Q_1 با هم یکسان است، DSS فوق منظم نیز هست آن‌را با نماد $(9, 2, 2, 1)$ نشان می‌دهیم.

تعریف ۲.۱.۲ اگر $y = y_1 \ldots y_n \in F_q^n$ و $x = x_1 x_2 \ldots x_n$ و $0 \leq i \leq n-1$، آنگاه i امین اتصال x و y به‌صورت زیر تعریف می‌شود:

$$T_i(x, y) = x_{i+1} \ldots x_n y_1 \ldots y_i;$$

به‌ویژه $T_i(x,x)$، یک جایگشت دوری از x یا i امین شیفت به چپ از x است.

تعریف ۳.۱.۲ شاخص کاملاً‌آزاد از یک کد $C \subseteq F_q^n$ را با $\rho = \rho(C)$ نشان می‌دهند و عبارت است از:

$$\rho = \min\{\, d(z, T_i(x,y)) \,|\, x, y, z \in C,\ i = 1, \ldots, n-1\},$$

که d فاصله همینگ بین بردارها در F_q^n است.

گزاره ۱.۱.۲ شاخص کاملاً‌آزاد کدهای خطی صفر است.

اثبات. بردار صفر متعلق به همه کدهای خطی است، بنابراین برای هر کد خطی C داریم:

$$0 \leq \rho(C) = \min\{d(x, T_i(y,z)) \,|x, y, z \in C\ ,\ 1 \leq i \leq n-1\} \leq d(0, T_i(0,0)) = d(0,0) = 0,$$

در نتیجه $\rho(C) = 0$ است. □

قرارداد ۱.۱.۲ از این به بعد هرجا کلمه شاخص را به‌کار بردیم منظورمان شاخص کاملاً‌آزاد است و هر جا از متن برداشت شود که بحث راجع به یک کد، مثل کد C، است به جای $\rho(C)$ از ρ استفاده می‌کنیم.

گزاره ۲.۱.۲ اگر شاخص یک کد $C \subseteq F_q^n$ ، برابر $\rho(C)$ باشد آنگاه یک کلمه کدی یا یک اتصال از کلمه‌ها کدی که حداکثر $[\frac{\rho(C)-1}{2}]$ خطا دارد را می‌توانیم تشخیص بدهیم.

اثبات. فرض کنید کلمه v را به ما داده‌اند. ابتدا ρ_1 و ρ_2 را به‌صورت زیر محاسبه می‌کنیم:

$$\rho_1 = min\, d(v,z)\ ; z \in C,$$

$$\rho_2 = min\, d(v, T_i(x,y));\ x, y \in C,\ i = 1, \ldots, n-1,$$

حال به بررسی چهار حالت زیر می‌پردازیم:

حالت اول: اگر $\rho_1,\rho_2 \leq [\frac{\rho(C)-1}{2}]$، آنگاه وجود دارند $x,y,z \in C$ و $1 \leq i \leq n-1$، به‌طوری که $d(v,z)=\rho_1$ و $d(v,T_i(x,y))=\rho_2$؛ پس با استفاده از نامساوی مثلث داریم:

$$\rho(C) \leq d(z,T_i(x,y)) \leq d(z,v)+d(v,T_i(x,y)) = \rho_1+\rho_2 \leq 2[\frac{\rho(C)-1}{2}] < \rho(C)\,,$$

و این تناقض است، در نتیجه این حالت هیچ موقع اتفاق نمی‌افتد.

حالت دوم: اگر $\rho_1 \leq [\frac{\rho(C)-1}{2}]$ و $\rho_2 > [\frac{\rho(C)-1}{2}]$، آنگاه با توجه به این‌که از یک طرف فاصله کلمه v از کلمه‌ها کدی کوچکتر از $\frac{\rho(C)}{2}$ و از اتصال کلمه‌ها کدی بزرگتر از $\frac{\rho(C)}{2}$ است و از طرف دیگر کمتر از $\frac{\rho(C)}{2}$ خطا دارد پس حتماً یک کلمه کدی است.

حالت سوم: اگر $\rho_1 > [\frac{\rho(C)-1}{2}]$ و $\rho_2 \leq [\frac{\rho(C)-1}{2}]$، آنگاه با توجه به این‌که از یک طرف فاصله کلمه v از اتصال کلمه‌ها کدی کوچکتر از $\frac{\rho(C)}{2}$ و از کلمه‌ها کدی بزرگتر از $\frac{\rho(C)}{2}$ است و از طرف دیگر کمتر از $\frac{\rho(C)}{2}$ خطا دارد پس حتماً یک اتصال از کلمه‌ها کدی است.

حالت چهارم: اگر $\rho_1,\rho_2 > [\frac{\rho(C)-1}{2}]$، آنگاه با توجه به این‌که از یک طرف فاصله کلمه v از کلمه‌ها کدی و اتصالات کلمه‌ها کدی بیشتر از $[\frac{\rho(C)-1}{2}]$ است ولی از طرف دیگر باید کمتر از $[\frac{\rho(C)-1}{2}]$ خطا داشته باشد پس نمی‌تواند کلمه‌ی کدی یا اتصالی از کلمه‌ها کدی باشد، که این حالت نیز هیچ موقع اتفاق نمی‌افتد.

□

۲.۲ کاربرد $\rho(C)$ و $d(C)$ و بهترین حالت این دو نسبت به یکدیگر

برای ارسال کلمه‌ها کدی از طریق یک کانال، آنها را به‌صورت یک دنباله پشت سرهم قرار می‌دهیم و درآیه به درآیه ارسال می‌کنیم؛ مثلاً فرض کنید k کلمه $x_i = x_{i1}x_{i2}\ldots x_{in} \in C$، $1 \leq i \leq k$، را بخواهیم ارسال کنیم دنباله ارسالی عبارت است از:

$$x_{11}\cdots x_{1n}x_{21}\cdots x_{2n}\cdots x_{k1}\cdots x_{kn}.$$

در طی عمل ارسال، ممکن است یک سری خطا روی دنباله ایجاد شود و تعدادی از درآیه‌ها را تغییر دهد، از طرف دیگر در طی عمل دریافت، ممکن است چند درآیه اول یا آخر گم شود (فرض بر این است که درآیه‌های دریافتی متوالی هستند و در بین آنها چیزی گم نشده است)؛ حال اگر دنباله دریافتی عبارت باشد از:

$$d_1 d_2 \cdots d_m$$

که $n \leq m \leq kn$ است باید از روی دنباله دریافتی کلمه‌ها کدی را تشخیص دهیم و سپس آن‌ها را تصحیح کنیم. بدین منظور در گام اول با فرض این‌که در هر n مؤلفه متوالی از دنباله دریافتی، حداکثر $[\frac{\rho(C)-1}{2}]$ خطا رخ داده باشد، می‌توانیم کلمه‌ها کدی را که حداکثر این مقدار خطا دارند تشخیص بدهیم و در گام بعدی این کلمه‌ها کدی را در صورتی که حداکثر $[\frac{d(C)-1}{2}]$ خطا داشته باشند، تصحیح کنیم.

اما باید به این نکته توجه داشت که کلمه‌ها کدی به‌دست آمده از گام اول، ممکن است حداکثر $[\frac{\rho(C)-1}{2}]$ خطا داشته باشند ولی ما در گام دوم تنها می‌توانیم کلمه‌ها کدی با حداکثر $[\frac{d(C)-1}{2}]$ خطا را تصحیح کنیم. پس برای این‌که حتماً یک روند صحیح طی شود، قدرت تصحیح کنندگی ما نباید کمتر از قدرت تشخیص ما باشد و این یعنی $[\frac{d(C)-1}{2}]$ نباید کوچکتر از $[\frac{\rho(C)-1}{2}]$ باشد.

ولی اگر $[\frac{d(C)-1}{2}]$ هم بزرگتر از $[\frac{\rho(C)-1}{2}]$ باشد با توجه به این‌که در گام اول نمی‌توانیم کلمه‌ای با $[\frac{d(C)-1}{2}]$ خطا را تشخیص دهیم سودی برای ما نخواهد داشت پس بهترین حالت این است که $[\frac{\rho(C)-1}{2}] = [\frac{d(C)-1}{2}]$.

۳.۲ کدهای همگام با DSS ها

لونشتین[1] در سال ۱۹۷۱ ساختاری را معرفی کرد که در طی انجام مراحل آن، از روی یک DSS یک کد خطی ساخته شده، سپس هم رده‌ای از آن به‌دست می‌آید که شاخص کاملاً‌ـآزاد آن حداقل ρ است [٦].

در زیر به معرفی این ساختار می‌پردازیم.

[1] V. I. Levenshtein

فرض کنید $\{Q_0, \ldots, Q_{q-1}\}$ یک DSS با پارامترهای $(n, \tau_0, \ldots, \tau_{q-1}, \rho)$ باشد؛ r را به صورت زیر محاسبه کنید:

$$r = \sum_{i=0}^{q-1} |Q_i| = |\bigcup_{i=0}^{q-1} Q_i| = \sum_{i=0}^{q-1} \tau_i \,,$$

اگر کد خطی C را به این صورت تعریف کنید که در جایگاه‌هایی که متعلق به هر کدام از Q_i ها هستند، مقدار صفر قرار بگیرد و در بقیهٔ جایگاه‌ها هر عضو دلخواه F_q قرار بگیرد یا به‌طور معادل:

$$C := \{(a_1, \ldots, a_n) \in F_q^n | j \in Q_i \to a_j = 0\},$$

آنگاه C یک کد خطی با بعد $n-r$ است (بردارهای پایه آن $n-r$ بردار e_j[۲] است که $j \notin \cup Q_i$).

سپس کد C' را به این صورت تعریف کنید که در هر بردار C، در جایگاه‌هایی که متعلق به هر کدام از Q_i ها هستند مقدار i جایگزین شود یا به‌طور معادل:

$$C' := \{(a_1, \ldots, a_n) \in F_q^n | j \in Q_i \to a_j = i\}.$$

حال اگر در بردار صفر، در جایگاه‌هایی که متعلق به هر کدام از Q_i ها هستند مقدار i را جایگزین کنید و بردار حاصل را x بنامید آنگاه:

$$C' = C + x,$$

پس C' هم رده‌ای از کد خطی C است؛ از آن‌جایی که $0 \notin C'$، کد C' غیرخطی است.

تعریف ۱.۳.۲ کد غیر خطی C' را که در روند بالا از یک DSS به‌دست آمد، کد همگام آن DSS می‌نامند.

با توجه به این‌که در DSS اولیه، هر عدد مخالف صفر حداقل ρ بار ظاهر می‌شود، آنگاه برای شاخص کاما-آزاد کد C'، که آن‌را با نماد $\rho(C')$ نشان می‌دهیم، خواهیم داشت:

گزاره ۱.۳.۲ $\rho(C') \geq \rho$.

اثبات. با توجه به ساختار کلمه‌ها کدی C'، هر دو کلمه کدی دلخواه، در مکان جایگاه‌هایی که متعلق به Q_j است، مقدار j را دارا می‌باشند؛ بنابراین وقتی i امین اتصال دو کلمه کدی را در نظر بگیریم مانند این است که مکان جایگاه‌هایی که

[۲] e_j یک بردار n تایی است که تنها مؤلفه j ام آن یک است و بقیه مؤلفه‌های آن صفر است.