نشریه علمی "پدافند الکترونیکی و سایبری"
سال هفتم، شماره ۲، تابستان ۱۳۹۸، ص ۱۲-۱

قاب‌های متناهی به‌عنوان کد: چند مشخصه‌سازی برای کدهای تصحیح‌کننده خطا و سه الگوریتم برای رفع خطا در انتقال اطلاعات

حسین جوانشیری[۱]، سعید علیخانی[۲*]، حمید مظاهری[۳]
۱- دانشیار، ۲- استاد، ۳- دانشیار، دانشکده علوم ریاضی دانشگاه یزد
(دریافت: ۹۶/۱۲/۱۹، پذیرش: ۹۷/۰۳/۰۶)

چکیده

کدهای خطی در نظریه کدگذاری، به ماتریس‌هایی که سطرهای آن‌ها تشکیل پایه برای یک فضای با بعد متناهی می‌دهد، متکی است. در این مقاله، پس از بیان مقدمات لازم برای قاب‌ها، به‌عنوان یک جایگزین انعطاف‌پذیر پایه‌ها، ابتدا ایده استفاده از قاب‌های متناهی در کدکردن اطلاعات را مطرح و سپس قاب‌هایی را معرفی خواهیم نمود که کدهای خطی معرفی‌شده توسط آن‌ها از توان بالایی در کشف و تصحیح خطاهای به‌وجودآمده در فرآیند انتقال اطلاعات برخوردار باشد. روش‌هایی برای ساخت مثال‌های جدیدی از چنین قاب‌هایی با استفاده از انواع شناخته‌شده آن‌ها مطرح شده و به‌طور ویژه نشان می‌دهیم خانواده‌های معرفی‌شده در برخی مقالات را می‌توان بسیار گسترده درنظر گرفت. در نهایت، ایده کدکردن اطلاعات را طوری اصلاح می‌نماییم که راه برای استفاده از دوگان‌های تقریبی و تعمیم‌یافته برای بازسازی اطلاعات دریافتی هموار شود. همچنین، چند الگوریتم برای بازسازی دقیق اطلاعات مخدوش‌شده دریافتی نیز ارایه شده است.

کلید واژه‌ها: GPS، قاب، عملگر، ماتریس، دوگان تقریبی، دوگان تعمیم‌یافته، کدگذاری، کدگشایی

۱- مقدمه

نظریه اطلاعات و کدگذاری دانش انتقال دقیق و اقتصادی داده‌ها از مکانی به مکان دیگر است. به‌عنوان نمونه، می‌توان به مکالمات تلفنی و ارسال تصویر از دیگر سیارات به زمین توسط ایستگاه‌های فضایی و نگهداری داده‌ها روی CD اشاره نمود. یک کد خطی به طول n روی میدان متناهی q عضوی از F_q، زیر فضایی از فضای برداری $F_q{}^n$ است. بنابراین، می‌توان از پایه‌های این فضا برای بیان عناصر فضا استفاده کرد. این پایه غالبا به‌صورت یک ماتریس بیان می‌شود که آن را ماتریس مولد کد می‌نامند و ماتریسی است که سطرهای آن پایه برای کد می‌باشند. با توجه به این‌که در حالت بعد متناهی بین عملگرها و ماتریس‌ها یک تناظر یک‌به‌یک وجود دارد، می‌توان گفت که هر ماتریس $k \times n$ای که سطرهای آن تشکیل پایه برای یک فضای برداری با بعد متناهی می‌دهد، ماتریس مولد یک کد خطی است. از این‌رو، در نظریه کدهای خطی، تمام چیزی که نیاز است عبارت است از عملگرهای خطی یا همان ماتریس‌های یک‌به‌یک که نقش کدگذاری را برعهده دارند و معکوس چپ آنها که نقش کدگشایی را بازی می‌کنند [۱-۴].

در سال‌های اخیر، قاب‌ها در فضاهای هیلبرت به‌دلیل برخورداری از خاصیت افزونگی نسبت به پایه‌ها، به‌عنوان یک جایگزین مناسب برای آن‌ها فراگیر شده‌اند. یادآوری می‌کنیم که مجموعه $F = \{f_1, \dots, f_n\}$ برای فضای هیلبرت H با بعد $k \le n$ یک قاب است، هرگاه آن را تولید کند [۵-۷]؛ به این معنی که برای هر $f \in H$ اعداد $c_1, \dots, c_n$ موجود باشند، به‌طوری‌که $f = \sum_{i=1}^{n} c_i f_i$؛ توجه کنید که برخلاف پایه‌ها، در تساوی اخیر یکتایی اعداد $c_1, \dots, c_n$ دارای اهمیت نیست. این ویژگی معادل این است که ثابت‌های مثبت A, B موجود باشند، به‌طوری‌که برای هر f در H داشته باشیم:

$$A\|f\|^2 \le \sum_{i=1}^{n} |\langle f, f_i\rangle|^2 \le B\|f\|^2.$$

اعداد A,B را کران‌های قاب می‌نامیم. به هر قاب F برای H، سه عملگر وابسته می‌شود که در نظریه قاب‌ها بسیار حائز اهمیت می‌باشد، برای معرفی آنها ابتدا اجازه دهید تذکر دهیم که در ادامه این متن F^n برای نمایش فضای n-بعدی اعداد حقیقی و یا مختلط به‌کار می‌رود.

۱. عملگر خطی $V_F: H \to F^n$ را برای هر $f \in H$ به‌صورت زیر تعریف می‌کنیم و آن را عملگر تجزیه قاب F می‌نامیم:

$$V_F(f) = (\langle f, f_1\rangle, \dots, \langle f, f_n\rangle).$$

* رایانامه نویسنده مسئول: alikhani@yazd.ac.ir

۲. عملگر خطی $V_F^*: F^n \to H$، الحاق عملگر V_F، برای هر بردار $(c_1, \dots, c_n)$ متعلق به F^n به‌صورت زیر قابل محاسبه و معرفی است و آن را عملگر ترکیب و یا عملگر بازسازی قاب F می‌نامیم.

$$V_F^*((c_1, \dots, c_n)) = \sum_{i=1}^{n} c_i f_i.$$

۳. عملگر قاب وابسته به قاب F، برای هر $f \in H$ به‌صورت زیر تعریف می‌شود:

$$S_F(f) = V_F^* V_F(f) = \sum_{i=1}^{n} \langle f, f_i \rangle f_i.$$

از [۷] یادآوری می‌کنیم که برای قاب F، عملگر V_F یک‌به‌یک، V_F^* پوشا و عملگر قاب آن، S_F، یک عملگر خودالحاق، مثبت و معکوس‌پذیر است. همچنین برای هر f در H نامساوی $\sum_{i=1}^{n} |\langle f, f_i \rangle|^2 \le B \|f\|^2$ برقرار است اگر و تنها اگر $\|V_F^*\| \le \sqrt{B}$ باشد. به‌ویژه، معکوس‌پذیر بودن عملگر S_F این امکان را فراهم می‌کند که هر f در H را به‌کمک فرمول بازسازی زیر نمایش دهیم:

$$f = \sum_{i=1}^{n} \langle f, S_F^{-1} f_i \rangle f_i = \sum_{i=1}^{n} \langle f, f_i \rangle S_F^{-1} f_i. \quad (۱)$$

اگر قرار دهیم $S_F^{-1}F = \{S_F^{-1} f_1, \dots, S_F^{-1} f_n\}$، آن‌گاه مجموعه $S_F^{-1}F$ یک قاب با کران‌های $\frac{1}{A}$ و $\frac{1}{B}$ برای H است که آن را دوگان کانونیک قاب F می‌نامند. تساوی (۱) برحسب عملگرها به‌صورت

$$V_{S_F^{-1}F}^* V_F = Id_H = V_F^* V_{S_F^{-1}F}$$

قابل بیان است؛ که در آن و در ادامه Id_H معرف عملگر همانی روی H است. در حالت کلی، اگر $G = \{g_1, g_2, \cdots, g_n\}$ یک قاب برای H باشد که تساوی $V_G^* V_F = Id_H = V_F^* V_G$ را برقرار کند، آنگاه قاب‌های F و G را دوگان یکدیگر گوییم. تعمیم‌هایی از رابطه دوگانی، به‌گونه‌ای که در ادامه به آن‌ها اشاره خواهیم نمود، در نظریه قاب‌ها مطرح است. قاب‌های F و G را دوگان تقریبی [۸] یکدیگر گوییم هرگاه

$$\|Id_H - V_F^* V_G\| < 1؛$$

آنها را دوگان تعمیم‌یافته [۸-۹] گوییم، هرگاه عملگر $V_F^* V_G$ معکوس‌پذیر باشد.

اکنون در مرحله‌ای هستیم که می‌توانیم به معرفی نحوه کدکردن اطلاعات به کمک قاب‌های متناهی بپردازیم. برای این منظور، فرض کنید مجموعه $F = \{f_1, f_2, \cdots, f_n\}$ یک قاب برای H همراه با عملگر تجزیه V_F است. یکی از ایده‌هایی که برای استفاده از قاب‌های متناهی در نظریه کدگذاری مطرح می‌باشد، به این صورت است که برای کدکردن اطلاعات یا سیگنال f، که به‌طور طبیعی متعلق به یک فضای با بعد متناهی H است، بردار

$$V_F f = (\langle f, f_1 \rangle, \dots, \langle f, f_n \rangle)^T$$

را به‌عنوان نسخه کدشده f در نظر می‌گیرند. سپس بردار $V_F f$ از فرستنده (الف) به دریافت‌کننده (ب) ارسال و درنهایت توسط عملگر بازسازی قاب F، که در این متن با نماد V_F^* نشان داده می‌شود کدگشایی می‌گردد؛ برای اطلاعات بیشتر مراجع [۶،۲ و ۱۳-۱۰] را به‌عنوان نمونه ملاحظه کنید. به‌طور دقیق‌تر، در مقایسه با کدهای خطی کلاسیک که به کمک پایه‌ها معرفی می‌شوند، ماتریس‌هایی که سطرهای آن تشکیل یک قاب می‌دهند را به‌عنوان ماتریس مولد کدهای خطی در نظر می‌گیرند. اما، از آنجا که کانال‌های ارتباطی همواره درگیر نویز یا امواج می‌باشند، فرآیند ارسال همواره بدون خطا نیست. به‌طور دقیق‌تر، احتمال دارد گیرنده به‌واسطه نویز بردار $(\langle f, f_1 \rangle + \varepsilon_1, \dots, \langle f, f_n \rangle + \varepsilon_n)$ را به‌عنوان ضرایب قاب اطلاعات کدشده f دریافت کند. از این‌رو، دریافت‌کننده، سیگنال دریافت‌شده را به‌صورت زیر بازسازی خواهد نمود:

$$\sum_{i=1}^{n} (\langle f, f_i \rangle + \varepsilon_i) S^{-1} f_i = \sum_{i=1}^{n} \langle f, f_i \rangle S^{-1} f_i + S^{-1} \left(\sum_{i=1}^{n} \varepsilon_i f_i \right)$$
$$= f + S^{-1} V^*(\varepsilon_1, \dots, \varepsilon_n).$$

بنابراین، اگر سیگنال بازسازی‌شده را با $\tilde{f}$ نشان دهیم، آن‌گاه:

$$\tilde{f} - f = S^{-1} V^*(\varepsilon_1, \dots, \varepsilon_n)^T.$$

به‌عنوان نمونه، ممکن است بردار $(\varepsilon_1, \dots, \varepsilon_n)$ به‌گونه‌ای به بردار $V_F f$ در فرآیند ارسال اضافه شود که برخی از مولفه‌های بردار $V_F f$ را ازدست بدهیم یا به اصطلاح مخدوش شوند؛ و یا ترتیب اولیه عناصر بردار $V_F f$ را دچار تغییر آرایش کند. بنابراین، هرگز نمی‌توان اطمینان صددرصد داشت که کلیه بیت‌های اطلاعات به‌شکل کاملا صحیح منتقل شود. ازاین‌رو، ابزارها، روش‌ها و الگوریتم‌های کدکردن اطلاعات باید به‌گونه‌ای برنامه‌ریزی شوند که توان بازسازی اطلاعات دریافتی ناقص را داشته باشند. در الگوریتم‌های کدگذاری اطلاعات به کمک قاب‌های متناهی، تمرکز در انتخاب قاب مناسب برای تولید کدهای خطی می‌باشد. برخی قاب‌های مناسب برای تولید کدهای خطی در مقاله [۱۰] معرفی شده‌اند. درحقیقت، مولفان در مرجع [۱۰]، ضمن معرفی قاب‌های m-مازاد یکنواخت، تقریباً خودشناس و تقریباً توانمند نسبت به مخدوش‌شدگی، نشان دادند که کدهای خطی معرفی‌شده توسط این قاب‌ها در بازسازی اطلاعات دریافتی ناقص بسیار کارساز هستند. اما، چالشی که موجود است، ساختن مثال و نمونه‌هایی از این نوع قاب‌ها، به‌ویژه در ابعاد بالا می‌باشد. در مقالات [۱۱ و ۱۴]، با استفاده از ویژگی‌های اعداد اول و البته محاسباتی بسیار پیچیده، مولفان توانسته‌اند مثال‌هایی از این نوع

قاب‌ها برای فضای n-بعدی اعداد حقیقی، R^n، معرفی کنند. تا آنجا که ما موضوع را می‌شناسیم، نمونه‌های واقعی دیگری از این نوع قاب‌ها تاکنون مطرح و معرفی نشده است. سوالاتی که به‌طور طبیعی به ذهن می‌رسد اینها هستند که: آیا می‌توان مثال‌های واقعی این نوع قاب‌ها را گسترده‌تر نمود؟ اگر تغییرات اندکی در عناصر یک قاب‌های m-مازاد یکنواخت، تقریباً خودشناس و یا تقریباً توانمند نسبت به مخدوش‌شدگی ایجاد شود، آیا قاب خاصیتش را ازدست خواهد داد؟ تا چه میزان تغییرات خواص این قاب‌ها پایدار هستند؟ دیگر این‌که، آیا ساختن این قاب‌ها تنها محدود به استفاده از اعداد اول است؟

بخشی از مقاله حاضر به پاسخ دادن سوالات فوق اختصاص دارد. به‌طور دقیق‌تر، مقاله حاضر از دو بخش تشکیل شده است. در بخش اول قاب‌های مناسب برای ساختن کدهای خطی با توان بالا در تصحیح خطا را یادآوری می‌کنیم. سپس، نشان می‌دهیم این خانواده از قاب‌ها تحت انواع خاصی از آشوب پایدار بوده و از این‌رو، اگر G، یک مجموعه از عناصر H باشد که در یک همسایگی مناسب از یک قاب m-مازاد یکنواخت، تقریباً خودشناس و یا تقریباً توانمند نسبت به مخدوش‌شدگی انتخاب شده است، آنگاه G یک مثال جدید از قابی با همان نوع خواهد بود. در بخش دوم، یک ایده جدید برای کدکردن اطلاعات به کمک قاب‌های متناهی مطرح می‌کنیم که این ایده راه برای کدگشایی و بازسازی اطلاعات ارسالی با استفاده از روابط دوگانی تقریبی [۸] و تعمیم‌یافته [۹-۸] هموار می‌کند. سپس، به معرفی چند الگوریتم برای تصحیح خطای اطلاعات کدشده دریافتی خواهیم پرداخت.

۲- تعاریف و چند مشخصه‌سازی برای قاب‌های مفید در کدگذاری

در سراسر این مقاله H یک فضای هیلبرت با بعد متناهی از بعد k و n یک عدد طبیعی بزرگتر یا مساوی آن است. نماد F برای نمایش قاب $\{f_1, f_2, \cdots, f_n\}$ برای H به‌کار می‌رود. همچنین، $Q: H \to H$ یک عملگر معکوس‌پذیر است و نمادهای $N(T)$ و $T(H)$ را، به‌ترتیب، برای نمایش فضای پوچ و فضای برد عملگر T به کار خواهیم برد.

اولین رده از قاب‌های مفید در نظریه کدگذاری، قاب‌هایی هستند که برای بازسازی ضرایب قاب مخدوش‌شده درحالتی‌که مکان مخدوش‌شدن (از دست دادن) آن‌ها در بردار $(\langle f, f_1\rangle, \dots, \langle f, f_n\rangle)^T$ برای ما مشخص باشد، بسیار مفید است. قبل از یادآوری تعریف آن‌ها از مقاله [۱۰]، ابتدا اجازه دهید یادآوری کنیم که قاب F برای H یک قاب دقیق است، هرگاه حذف هر کدام از عناصر آن باعث شود که مجموعه باقیمانده برای H یک قاب نباشد؛ به‌عبارت دیگر قاب F دقیق است هرگاه حذف هریک از عناصر آن فضای H را تولید نکند.

تعریف ۲-۱. قاب F برای H را m-مازاد یکنواخت گوییم هرگاه حذف هر m عنصر دلخواه از آن یک قاب دقیق برای H معرفی کند.

گام آغازین ما برای ارائه نتایج این بخش، لم زیر است که با انجام محاسبات نه‌چندان سختی قابل مشاهده است و از این‌رو، ما از ارائه اثبات آن صرف‌نظر می‌کنیم.

لم ۲-۲. قاب F، m-مازاد یکنواخت (به‌ترتیب، دقیق) است اگر و تنها اگر مجموعه $QF := \{Qf_1, \dots, Qf_n\}$ یک قاب m-مازاد یکنواخت (به‌ترتیب، دقیق) باشد.

اکنون فرض کنید F یک قاب m-مازاد یکنواخت است، آن‌گاه طبق تعریف مجموعه $F_{i_1,\dots,i_{n-m}} = \{f_{i_1}, \dots, f_{i_{n-m}}\}$، که حاصل از حذف m عنصر مجموعه F است، یک قاب است. بنابراین، عملگر قاب آن به‌صورت زیر قابل معرفی است

$$S_{i_1,\dots,i_{n-m}} f = \sum_{j=1}^{n-m} \langle f, f_{i_j}\rangle f_{i_j}.$$

قابل توجه است که، $S_{i_1,\dots,i_{n-m}}$ یک عملگر خودالحاق، مثبت و معکوس‌پذیر است. همچنین برای خواننده علاقه‌مند بسیار سخت نخواهد بود که بررسی کند این عملگر در نامساوی $S_{i_1,\dots,i_{n-m}} \le S_F$ صادق است. بنابراین، قضیه ۵-۲-۲ از مرجع [۱۵] نتیجه می‌دهد که

$$\|S_{i_1,\dots,i_{n-m}}\| \le \|S_F\| \text{و} \|S_F^{-1}\| \le \|S_{i_1,\dots,i_{n-m}}^{-1}\|.$$

به کمک لم ۲-۲، نمادگذاری و مشاهدات اخیر، می‌توانیم قضیه زیر را فرمول‌بندی و اثبات کنیم که در آن به بررسی پایداری قاب‌های m-مازاد یکنواخت تحت یک آشوب خاص پرداخته‌ایم. ازاین‌رو، اگر مجموعه G در یک همسایگی مناسب از یک قاب m-مازاد یکنواخت شناخته‌شده انتخاب شود، آنگاه با مثال جدیدی از این نوع قاب‌ها مواجه خواهیم شد.

قضیه ۲-۳. فرض کنید F یک قاب m-مازاد یکنواخت با کران‌های A و B برای H است. اگر $G = \{g_1, \dots, g_n\}$ یک زیرمجموعه از بردارهای H باشد که

$$\mu_F := \sum_{i=1}^{n} \|f_i - g_i\| \|S_F^{-1}(f_i)\| < 1$$

و علاوه بر این، برای هر انتخـاب $1 \le i_1 < \cdots < i_{n-m} \le n$ از اعداد طبیعی

$$\mu_{i_1,\dots,i_{n-m}} := \sum_{j=1}^{n-m} \left\| f_{i_j} - g_{i_j} \right\| \left\| S^{-1}_{i_1,\dots,i_{n-m}}(f_{i_j}) \right\| < 1.$$

آن‌گاه G یک قاب m-مازاد یکنواخت برای H است.

برهان. ابتدا نشان می‌دهیم که G یک قاب برای H است. برای این منظور، فرض کنید $Q_F: H \to H$ نگاشتی با ضابطه زیر است:

$$Q_F(f) = \sum_{i=1}^{n} \langle f, S_F^{-1}(f_i)\rangle\, g_i (f \in H).$$

مشاهده می‌شود که:

$$\begin{aligned} \|f - Q_F(f)\| &= \left\| \sum_{i=1}^{n} \langle f, S_F^{-1}(f_i)\rangle (f_i - g_i) \right\| \\ &\le \sum_{i=1}^{n} \|f_i - g_i\| \|S_F^{-1}(f_i)\| \|f\| \\ &\le \mu_F \|f\|. \end{aligned}$$

ازاین‌رو، Q_F عملگری معکوس‌پذیر است که $\|Q_F^{-1}\| \le \frac{1}{1-\mu_F}$. لذا برای هر f متعلق به H داریم:

$$\begin{aligned} \|f\|^2 = \langle f, f\rangle &= \langle \sum_{i=1}^{n} \langle Q_F^{-1}(f), S_F^{-1}(f_i)\rangle g_i\, , f\rangle \\ &\le \left(\sum_{i=1}^{n} |\langle Q_F^{-1}(f), S_F^{-1}(f_i)\rangle|^2 \right)^{\frac{1}{2}} \left(\sum_{i=1}^{n} |\langle f, g_i\rangle|^2 \right)^{\frac{1}{2}} \\ &\le \frac{1}{\sqrt{A}} \|Q_F^{-1}(f)\| \left(\sum_{i=1}^{n} |\langle f, g_i\rangle|^2 \right)^{\frac{1}{2}} \\ &\le \frac{1}{\sqrt{A}} \times \frac{1}{1-\mu_F} \|f\| \left(\sum_{i=1}^{n} |\langle f, g_i\rangle|^2 \right)^{\frac{1}{2}}. \end{aligned}$$

این نتیجه می‌دهد که:

$$(1-\mu_F)^2 A \, \|f\| \le \sum_{i=1}^{n} |\langle f, g_i\rangle|^2.$$

از طرفی به سادگی دیده می‌شود که شرط کران بالای قاب نیز برای مجموعه G برقرار است. اکنون برای اثبات m-مازاد یکنواخت بودن قاب G فرض کنید $G_{i_1,\dots,i_{n-m}} = \{g_{i_1}, \dots, g_{i_{n-m}}\}$ یک زیر مجموعه $n-m$ عضوی از G است. واضح است که بدون از دست دادن هیچ کلیتی می‌توان فرض نمود که $1 \le i_1 < \cdots < i_{n-m} \le n$. با استفاده از شرط $\mu_{i_1,\dots,i_{n-m}} < 1$ و مشابه فوق، می‌توان مشاهده نمود که نگاشت $Q_{i_1,\dots,i_{n-m}}: H \to H$ با ضابطه

$$Q_{i_1,\dots,i_{n-m}}(f) = \sum_{j=1}^{n-m} \langle f, S^{-1}_{i_1,\dots,i_{n-m}}(f_{i_j})\rangle\, g_{i_j}$$

معکوس‌پذیر و $G_{i_1,\dots,i_{n-m}}$ یک قاب برای H است. اکنون، گزاره ۸-۴-۵ مرجع [۷] و دقیق بودن قاب $F_{i_1,\dots,i_{n-m}}$ نتیجه می‌دهد که:

$$Q_{i_1,\dots,i_{n-m}}\left(f_{i_j}\right) = g_{i_j} (j = 1, \dots, n-m).$$

درنهایت، این تساوی و لم ۲-۱ اثبات قضیه را کامل می‌کند.

برای معرفی دومین رده از قاب‌های مفید در کدگذاری، نیازمند معرفی برخی مقدمات هستیم. برای این منظور، فرض کنید F یک قاب m-مازاد یکنواخت برای H است. ازاین‌رو،طبق تعریف زیرمجموعه $F_{m,\dots,n} := \{f_{m+1}, f_{m+2}, \cdots, f_n\}$ از F یک قاب دقیق برای H است. لذا، با استفاده از دقیق بودن قاب $F_{m,\dots,n}$، می‌توان اسکالرهای منحصربه‌فرد $\{a_{i,m+1}, a_{i,m+2}, \cdots, a_{i,n}\}$ را طوری انتخاب نمود که:

$$f_i = \sum_{j=m+1}^{n} -\overline{a_{i,j}} f_j \qquad i = 1,2, \cdots, m,$$

که در آن، $\overline{a_{i,j}}$ به مزدوج عدد مختلط $a_{i,j}$ اشاره دارد. بنابراین، اگر $(\langle f, f_1\rangle, \dots, \langle f, f_n\rangle)$ برداری دلخواه در $V_F(H)$ باشد، آن‌گاه برای هر عدد طبیعی $1 \le i \le m$ داریم:

$$\langle f, f_i\rangle + \sum_{j=m+1}^{n} a_{i,j} \langle f, f_j\rangle = 0.$$

حال، اگر ماتریس $m \times n$، $M_{F;m+1,\dots,n}$ را به‌صورت زیر تعریف شود،

$$M_{F;m+1,\dots,n} = \begin{pmatrix} 1 & \cdots & 0 & a_{1,m+1} & \cdots & a_{1,n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 1 & a_{m,m+1} & \cdots & a_{n,n} \end{pmatrix},$$

که بخش اول آن ماتریس همانی $m \times m$ است، آن‌گاه برای هر بردار $c = (c_1, c_2, \cdots, c_n)$ در $V_F(H)$ خواهیم داشت:

$$M_{F;m+1,\dots,n} c^T = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \qquad (۲)$$

برعکس فرض کنید c برداری در F^n است که در تساوی (۲) صادق است. چون $F_{m,\dots,n}$ یک قاب دقیق است، آن‌گاه پوشایی عملگر V_F، تضمین می‌کند که عنصر f متعلق به H موجود است، به‌طوری‌که:

$$\langle f, f_j\rangle = c_j \qquad j = m+1, \cdots, n.$$

در اینجا لازم به یادآوری است که قاب‌های دقیقا در یک فضای هیلبرت، دقیقا قاب‌های هم‌ارز پایه‌های ریس هستند. بنابراین، خواهیم داشت:

$$\langle f, f_j\rangle = \sum_{j=1}^{n} -a_{i,j}c_j = c_i \qquad i = 1,2,\cdots,m.$$

لذا، $c \in V_F(H)$. این مشاهدات در حقیقت اثباتی برای گزاره زیر است:

گزاره ۲-۴: فرض کنیم F یک قاب m-مازاد یکنواخت برای H و Q یک ماتریس معکوس‌پذیر است. آنگاه برای هر انتخاب $1 \le i_1 < \cdots < i_{n-m} \le n$ از اعداد طبیعی ماتریس $M_{F;i_1,\ldots,i_{n-m}}$، که بخشی از ستون‌های آن ماتریس همانی $m \times m$ است، وجود دارد به‌طوری‌که:

$$V_{Q^*F}(H) = V_F Q(H) = V_F(H) = N(M_{F;i_1,\ldots,i_{n-m}})$$

در این رابطه، Q^*F قاب m-مازاد یکنواخت $Q^*F := \{Q^*f_1, Q^*f_2, \cdots, Q^*f_n\}$ است.

دومین رده از قاب‌های مفید در نظریه کدگذاری قاب‌هایی است که برای شناسایی ترتیب اصلی عناصر بردار $V_F(f)$، درصورتی‌که دریافت‌کننده یک تغییر آرایش‌یافته از آن را دریافت کند، بسیار کارساز هستند.

تعریف ۲-۵. فرض کنید F یک قاب m-مازاد یکنواخت برای H و M یک ماتریس است که به ازای آن $V_F(H) = N(M)$. دراین‌صورت، قاب F را تقریباً خودشناس گوییم، هرگاه برای هر ماتریس $\widetilde{M}$ که حاصل از یک تجدید آرایش از ستون‌های ماتریس M است، داشته باشیم:

$$rank(M) < rank\binom{M}{\widetilde{M}}.$$

گزاره بعدی که به‌سادگی از گزاره ۲-۴ و تعریف ۲-۵ نتیجه می‌شود، برای اثبات قضیه ۲-۷ زیر مورد استفاده قرار خواهد گرفت.

گزاره ۲-۶. فرض کنید F یک قاب برای H و Q یک عملگر معکوس‌پذیر است. دراین‌صورت، F یک قاب m-مازاد یکنواخت و تقریباً خودشناس است اگر و تنها اگر مجموعه $QF := \{Qf_1, \ldots, Qf_n\}$ یک قاب m-مازاد یکنواخت و تقریباً خودشناس باشد.

قضیه ۲-۷. فرض کنید F یک قاب m-مازاد یکنواخت و تقریباً خودشناس با کران‌های A و B برای H است. همچنین فرض کنید $G = \{g_1, \ldots, g_n\}$ یک زیرمجموعه از بردارهای H است که

$$\mu_F := \sum_{i=1}^{n} \|f_i - g_i\| \|S_F^{-1}(f_i)\| < 1$$

و علاوه بر این، برای هر انتخاب $1 \le i_1 < \cdots < i_{n-m} \le n$ از اعداد طبیعی

$$\mu_{i_1,\ldots,i_{n-m}} := \sum_{j=1}^{n-m} \left\|f_{i_j} - g_{i_j}\right\| \left\|S^{-1}_{i_1,\ldots,i_{n-m}}(f_{i_j})\right\| < 1.$$

آنگاه G نیز یک قاب m-مازاد یکنواخت و تقریباً خودشناس برای H است.

برهان. ابتدا توجه داریم که قضیه ۲-۳ نتیجه می‌دهد که G یک قاب m-مازاد یکنواخت برای H است. اکنون برای اثبات تقریباً خودشناس بودن آن، مشابه روند اثبات قضیه ۲-۳، می‌توان مشاهده نمود که نگاشت $Q_{m+1,\ldots,n}: H \to H$ با ضابطه:

$$Q_{m+1,\ldots,n}(f) = \sum_{i=m+1}^{n} \langle f, S^{-1}_{m+1,\ldots,n}(f_i)\rangle g_i$$

معکوس‌پذیر و برای هر $i = m+1, \ldots, n$ داریم:

$$Q_{m+1,\ldots,n}(f_i) = g_i.$$

بنابراین، اگر $\{a_{i,m+1}, a_{i,m+2}, \cdots, a_{i,n}\}$ مجموعه‌ای از اسکالرهای منحصربه‌فردی باشند که تساوی زیر به ازای آنها برقرار است

$$f_i = \sum_{j=m+1}^{n} -\overline{a_{i,j}} f_j \qquad i = 1,2,\cdots,m,$$

آنگاه معکوس‌پذیربودن ماتریس $Q_{m+1,\ldots,n}$ نتیجه می‌دهد که مجموعه $\{a_{i,m+1}, a_{i,m+2}, \cdots, a_{i,n}\}$، اسکالرهای منحصربه‌فردی هستند که تساوی زیر را نیز برقرار می‌کنند

$$g_i = \sum_{j=m+1}^{n} -\overline{a_{i,j}} g_j \qquad i = 1,2,\cdots,m.$$

ازاین‌رو، $M_{F;m+1,\ldots,n} = M_{G;m+1,\ldots,n}$. بنابراین، خودشناس بودن قاب F خودشناس بودن G را نتیجه می‌دهد.

در ادامه می‌خواهیم، سومین رده از قاب‌های مناسب برای ساختن کدهای خطی تصحیح‌کننده خطا را معرفی کنیم. برای این منظور، فرض کنید که F یک قاب m-مازاد یکنواخت برای H و l یک عدد طبیعی کمتر اکید از m است. برای هر انتخاب $1 \le i_1 < \cdots < i_{n-l} \le n$ از اعداد طبیعی و هر $f \in H$ تعریف می‌کنیم:

$$V_{F;i_1,\ldots,i_{n-l}} f := (\langle f, f_1\rangle, \ldots, \langle f, f_{n-l}\rangle).$$

از آنجا که مجموعه $\{f_1, \ldots, f_{n-l}\}$ یک قاب برای H است، به‌سادگی قابل مشاهده است که نگاشت $V_{F;i_1,\ldots,i_{n-l}}$، یک عملگر خوش‌تعریف و یک‌به‌یک است. از طرفی m-مازاد یکنواخت قاب F به‌همراه $l < m$، نتیجه می‌دهد که مجموعه

$$F_{i_{m-l+1},\ldots,i_{n-l}} = \{f_{i_{m-l+1}}, \ldots, f_{i_{n-l}}\}$$

یک قاب دقیق است. ازاین‌رو، برای هر $1 \le p \le m-l$، ضرایب اسکالر منحصربه‌فرد $a_{p,j}$ چنان پیدا می‌شود که:

$$f_{i_p}=\sum_{j=m-l+1}^{n-l}-\overline{a_{p,j}}f_{i_j}.$$

بنابراین، اگر $M_{F;i_1,\dots,i_{n-l}}$ ماتریسی $(m-l)\times(n-l)$ باشد که به‌صورت زیر معرفی می‌شود:

$$M_{F;i_1,\dots,i_{n-l}}=\begin{pmatrix}1 & \cdots & 0 & a_{1,m-l+1} & \cdots & a_{1,n-l}\\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots\\ 0 & \cdots & 1 & a_{m-l,m-l+1} & \cdots & a_{m-l,n-l}\end{pmatrix}$$

که بخش اول آن ماتریس همانی $(m-l)\times(m-l)$ است، آن‌گاه، مشابه گزاره ۲-۴ می‌توان گفت که:

$$V_{Q^*F;i_1,\dots,i_{n-l}}(H)=V_{F;i_1,\dots,i_{n-l}}Q(H)=V_{F;i_1,\dots,i_{n-l}}(H)\\ =N(M_{F;i_1,\dots,i_{n-l}}).$$

تعریف ۲-۸. فرض کنید که F یک قاب m-مازاد یکنواخت برای H و l یک عدد طبیعی کمتر اکید از m است. قاب F را نسبت به l-مخدوش‌شدگی تقریباً توانمند گوییم، هرگاه برای هر دو انتخاب دلخواه

$$1\le i_1<\cdots<i_{n-l}\le n \quad \text{و} \quad 1\le i'_1<\cdots<i'_{n-l}\le n$$

با شرط $(i_1,\dots,i_{n-l})\neq(i'_1,\dots,i'_{n-l})$ داشته باشیم:

$$V_{F;i_1,\dots,i_{n-l}}(H)\neq V_{F;i'_1,\dots,i'_{n-l}}(H).$$

خواننده علاقه‌مند به‌سادگی می‌تواند گزاره‌ای با این حکم که قاب m-مازاد یکنواخت F نسبت به l-مخدوش‌شدگی تقریباً توانمند است اگر و تنها اگر به‌ازای عملگر معکوس‌پذیر Q مجموعه $\{Qf_1,\dots,Qf_n\}$ یک قاب m-مازاد یکنواخت باشد که نسبت به l-مخدوش‌شدگی تقریباً توانمند است، اثبات کند. اما، تمایل داریم، برای فراهم کردن روشی برای ساخت مثال‌های جدید از قاب‌های توانمند نسبت به مخدوش‌شدگی شناخته شده، پایداری این نوع از قاب‌ها را تحت آشوب بررسی کنیم. قضیه زیر به بررسی پایداری این نوع از قاب‌ها، تحت آشوب، پرداخته است؛ که به‌جهت شباهت روند اثبات آن با قضیه ۲-۷ و مختصرگویی از اثبات آن صرف‌نظر می‌کنیم.

قضیه ۲-۹. فرض کنید F یک قاب m-مازاد یکنواخت با کران‌های A و B برای H است که به‌ازای یک عدد طبیعی l کمتر اکید از m، نسبت به l-مخدوش‌شدگی تقریباً توانمند می‌باشد. همچنین فرض کنید $G=\{g_1,\dots,g_n\}$ یک زیرمجموعه از بردارهای H است که:

$$\mu_F:=\sum_{i=1}^{n}\|f_i-g_i\|\|S_F^{-1}(f_i)\|<1$$

و علاوه‌بر این، برای هر انتخاب $1\le i_1<\cdots<i_{n-m}\le n$ از اعداد طبیعی

$$\mu_{i_1,\dots,i_{n-m}}:=\sum_{j=1}^{n-m}\|f_{i_j}-g_{i_j}\|\left\|S^{-1}_{i_1,\dots,i_{n-m}}(f_{i_j})\right\|<1.$$

آن‌گاه G نیز یک قاب m-مازاد یکنواخت برای H است که نسبت به l-مخدوش‌شدگی تقریباً توانمند می‌باشد.

این بخش را با ارائه قضیه زیر و یک مثال که نتیجه‌ای مستقیم از آن است به پایان می‌رسانیم. قابل توجه است که این قضیه نیز پایداری قاب‌ها m-مازاد یکنواخت، تقریباً خودشناس و تقریباً توانمند نسبت مخدوش‌شدگی، نسبت به‌نوعی دیگر از آشوب را مورد بررسی قرار می‌دهد. به‌کمک این قضیه و قضیه ۳-۱ از مرجع [۱۴] مشاهده می‌شود که اگر $r_1,\dots,r_n$ اعداد حقیقی باشند که در یک همسایگی مناسب از اعداد اول متمایز $p_1,\dots,p_n$ انتخاب شوند، آنگاه مثال‌های جدیدی از قاب‌های تقریباً خودشناس و تقریباً توانمند نسبت مخدوش‌شدگی برای R^n قابل احتصال است.

قضیه ۲-۱۰. فرض کنید F یک قاب برای H با کران‌های A و B است. اگر برای مجموعه $G=\{g_1,g_2,\cdots,g_n\}$ اعداد $\alpha,\beta\in(0,1)$ موجود باشند به‌طوری‌که برای هر بردار $(c_1,c_2,\dots,c_n)^T\in F^n$ داشته باشیم:

$$\left\|\sum_{i=1}^{n}c_i(f_i-g_i)\right\|\le\alpha\left\|\sum_{i=1}^{n}c_if_i\right\|+\beta\left\|\sum_{i=1}^{n}c_ig_i\right\| \qquad (۳)$$

آنگاه G یک قاب با کران‌های $A\left(\frac{1-\alpha}{1+\beta}\right)^2$ و $B\left(\frac{1+\alpha}{1-\beta}\right)^2$ است. همچنین، احکام زیر برقرار است.

۱. اگر F، یک قاب m-مازاد یکنواخت باشد، آن‌گاه G نیز m-مازاد یکنواخت است.

۲. اگر F، یک قاب تقریباً خودشناس باشد، آن‌گاه G نیز تقریباً خودشناس است.

۳. اگر F، یک قاب تقریباً توانمند نسبت به l-مخدوش‌شدگی باشد، آن‌گاه G نیز تقریباً توانمند نسبت به l-مخدوش‌شدگی است.

برهان. ابتدا توجه داریم که، بنا بر آنچه در مقدمه بیان شد، $\|V_F^*\|\le\sqrt{B}$ و به‌ویژه نامساوی (۳) نتیجه می‌دهد که برای هر بردار $(c_1,c_2,\dots,c_n)\in F^n$ داریم:

$$\left\|\sum_{i=1}^{n}c_ig_i\right\|\le\frac{1+\alpha}{1-\beta}\left\|\sum_{i=1}^{n}c_if_i\right\|\\ \le\frac{1+\alpha}{1-\beta}\|V_F^*\|\left(\sum_{i=1}^{n}c_i^2\right)^{\frac{1}{2}}.$$

از این‌رو، اگر $U: F^n \to H$ را با ضابطه

$$U((c_1, c_2, \dots, c_n)) = \sum_{i=1}^{n} c_i g_i$$

درنظر بگیریم، آن‌گاه $\|U\| \leq \frac{1+\alpha}{1-\beta}\sqrt{\mathrm{B}}$ است. بنابراین، عملگر U خوش‌تعریف، کراندار و در حقیقت $U = V_G^*$. این مشاهدات نتیجه می‌دهد که برای هر $f \in H$ نامساوی زیر برقرار است:

$$\sum_{i=1}^{n} |\langle f, g_i\rangle|^2 \leq \left(\frac{1+\alpha}{1-\beta}\right)^2 B\|f\|^2.$$

به‌طور مشابه، می‌توان نشان داد که:

$$A\left(\frac{1-\alpha}{1+\beta}\right)^2 \|f\|^2 \leq \sum_{i=1}^{n} |\langle f, g_i\rangle|^2 (f \in H).$$

لذا G یک قاب برای H است. علاوه‌بر این، استفاده مجدد از نامساوی (۳) نشان می‌دهد که برای هر بردار $(c_1, c_2, \dots, c_n)$ در F^n داریم:

$$\begin{aligned}\|V_F^*((c_1, \dots, c_n)^T) - V_G^*((c_1, \dots, c_n)^T)\| \\ \leq \alpha\|V_F^*((c_1, \dots, c_n)^T)\| \\ + \beta\|V_G^*((c_1, \dots, c_n)^T)\|.\end{aligned}$$

اکنون واضح است که عضویت اعداد α و β در بازه $(0,1)$ نتیجه می‌دهد که $N(V_F^*) = N(V_G^*)$. این تساوی و نتیجه ۴،۵ از مرجع [۶] بیانگر این است که عملگر معکوس‌پذیر T موجود است به‌طوری‌که برای هر $i = 1, \dots, n$ تساوی $g_i = T(f_i)$ برقرار است. بنابراین، احکام ۱، ۲ و ۳ نتیجه‌ای مستقیم از نتایج ارائه‌شده در فوق است.

قضیه اخیر و قضیه ۱-۳ مرجع [۱۴] مثال زیر را برای ما به ارمغان می‌آورد.

مثال ۲-۱۱. فرض کنید n و k دو عدد طبیعی هستند که $n - 2 \geq k \geq 2$ و همچنین فرض کنید $p_1, \dots, p_n$ و $q_1, \dots, q_n$ دو انتخاب از اعداد اول متمایز هستند. برای هر $i = 1, \dots, n$ تعریف کنید:

$$f_i = (1, \sqrt{p_i}, \dots, (\sqrt{p_i})^{k-1})^T$$

و

$$g_i = (1, \sqrt{q_i}, \dots, (\sqrt{q_i})^{k-1})^T.$$

۱. اگر $Q: R^k \to R^k$ یک عملگر معکوس‌پذیر باشد، آنگاه، مجموعه $\{Q^*f_1, \dots, Q^*f_n\}$ یک قاب برای R^k است که هم تقریباً خودشناس و هم تقریباً توانمند نسبت به $(n-k-1)$-مخدوش‌شدگی می‌باشد.

۲. اگر $Q_1, Q_2: R^k \to R^k$ دو عملگر معکوس‌پذیر باشند، آن‌گاه برای هر $\alpha, \beta \in (0,1)$ مجموعه

$$\{\alpha Q_1^* f_1 + \beta Q_2^* g_1, \dots, \alpha Q_1^* f_n + \beta Q_2^* g_n\}$$

یک قاب برای R^k است که هم تقریباً خودشناس و هم تقریباً توانمند نسبت به $(n-k-1)$-مخدوش‌شدگی می‌باشد.

۳- نحوه کدکردن اطلاعات و چند الگوریتم تصحیح خطا

برای انتقال سیگنال f متعلق به فضای H از انتقال‌دهنده (الف) به دریافت‌کننده (ب) به این ترتیب عمل می‌کنیم که ابتدا عملگر معکوس‌پذیر Q را برای رمزگذاری اطلاعات بر سیگنال f اثر می‌دهیم، سپس از (الف) ضرایب $(\langle Qf, f_1\rangle, \langle Qf, f_2\rangle, \cdots, \langle Qf, f_n\rangle)^T$ را انتقال دهیم. دریافت‌کننده در صورت دریافت صحیح بردار ذکرشده، به کمک فرمول زیر می‌تواند سیگنال f را بازسازی کند.

$$f = \sum_{i=1}^{n} \langle Qf, f_i\rangle Q^{-1}S^{-1}f_i.$$

این نحوه کدکردن اطلاعات، از چندین جهت دارای مزیت است. اولین مزیت آن، این است که قبل از ارسال اطلاعات، ابتدا آن را توسط نگاشت Q رمزگذاری می‌کنیم و از این رو فرآیند ارسال یک طرح ترکیبی کدگذاری و رمزگذاری است. همان‌طور که می‌دانیم، تامین امنیت داده‌ها یک مساله چالش برانگیز است. همچنین، داشتن توان بالا در تصحیح خطای اطلاعات دریافتی ناقص و یا به حداقل رساندن خطاهای فرآیند ارسال، باعث بالا بردن امنیت اطلاعات نمی‌شود. به‌عبارت دیگر، هر استراق سمع‌کننده‌ای به‌راحتی می‌تواند حضور اطلاعات کدشده را تشخیص دهد و اطلاعات را شناسایی کند. به‌عنوان مثال، در انتقال تصویر و یا هر حوزه‌ی مرتبط با پردازش تصویر، قبل از فرآیند انتقال و کدکردن تصویر، یکی از روش‌های آشوب مانند نگاشت آرنولد و یا نگاشتی که در الگوریتم نهان‌نگاری مورد استفاده قرار می‌گیرد [۴ و ۱۳]، را روی بلوک‌های تصویر اعمال می‌کنیم. این کار موجب مقاوم‌تر شدن و امن‌شدن انتقال تصویر می‌گردد. شایان ذکر است که، تبدیل آرنولد یکی از روش‌های نگاشت آشوبی دوبعدی برای تصاویر دیجیتالی است. تبدیل آرنولد تصویری با اندازه N×N به‌صورت زیر است:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

که در آن، $x, y \in \{0,1, \dots, \mathrm{N}-1\}$ می‌باشند. هر پیکسل (x, y) در تصویر به پیکسل (x', y') توسط معادله فوق تبدیل می‌گردد و هنگامی که همه پیکسل‌های تصویر تبدیل شدند، تصویر آشوب‌شده به‌دست می‌آید. تبدیل آرنولد یک فرآیند تناوبی

است، از این‌رو، مختصات موقعیت اصلی (x,y) پس از t تکرار برمی‌گردد. فاکتور t تناوب تبدیل نامیده می‌شود. این تبدیل به‌علت افزایش تعداد کلیدهای امنیتی، امنیت بیشتری را فراهم می‌کند. بنابراین، در انتقال تصویر برای افزایش امنیت و بهبود مقاومت ارسال، نگاشت آرنولد و یا نگاشت استفاده‌شده در یکی از روش‌های نهان‌نگاری تصویر، روی تصویر اعمال می‌شود. به‌کمک استفاده از این نگاشت در انتقال تصویر، اطلاعات می‌تواند بر روی کانال‌های ارتباطی فرستاده شود بدون اینکه هیچ‌گونه اطلاعاتی برای گیرنده غیرمجاز فاش شود. در ادامه شکل (۱) را مشاهده می‌کنیم که با استفاده از نگاشت آرنولد و تناوب ۵ تبدیل شده است و سپس با اعمال دوباره این الگوریتم به شکل اولیه بازگردانده شده است.

شکل (۱): تصویر اصلی و تصویر تبدیل شده توسط نگاشت آرنولد با تناوب ۵

دومین مزیتی که این روش کدکردن اطلاعات به‌همراه دارد. هموار کردن راه برای استفاده از روابط دوگانی تقریبی [۸] و تعمیم‌یافته [۹-۸] است.

اما همانطور که در بخش اول اشاره کردیم، ارسال اطلاعات کدشده به‌علت دریافت امواج به‌دور از خطا نیست. از این‌رو، این بخش را به ارائه الگوریتم‌هایی برای تصحیح خطاهای رخ داده احتمالی در فرآیند ارسال اطلاعات کدشده به کمک قاب‌های متناهی اختصاص داده‌ایم. برای رسیدن به این هدف، بخش را به سه زیربخش، که هر بخش به یکی از محتمل‌ترین خطای احتمالی در فرآیند ارسال اختصاص دارد، تقسیم نموده‌ایم. در هر زیر بخش ضمن معرفی نحوه‌ی رخ دادن خطا، به قابی که برای مقابله با این خطا در فرآیند کدکردن اطلاعات مفید است نیز اشاره خواهیم کرد.

۳-۱- الگوریتم بازسازی ضرایب قاب مخدوش‌شده با مکان مشخص

این الگوریتم، حالتی را مورد توجه دارد که در بردار ضرایب قاب اطلاعات کدگذاری‌شده f، تعداد l عنصر در مکان‌های مشخص را از دست داده باشیم و یا به اصطلاح مخدوش شده باشند. برای بازسازی اطلاعات انتقال‌یافته از کانال‌های ارتباطی که چنین خطایی در آن‌ها احتمال وقوع دارد، استفاده از قاب‌های m-مازاد یکنواخت با شرط $m \geq l$ مفید است.

الگوریتم ۳-۱-۱- فرض کنیم F یک قاب m-مازاد یکنواخت و Q یک ماتریس معکوس‌پذیر است. همچنین فرض کنید $c = (\langle Qf, f_1\rangle, \dots, \langle Qf, f_n\rangle)$ بردار ضرایب قاب اطلاعات کدگذاری‌شده f باشد. برای هر $1 \leq i \leq n$ قرار می‌دهیم:
$c_i = \langle Qf, f_i\rangle$.

اگر $l \leq m$ و $j_1, \dots, j_l$ مکان‌های مشخصی باشند که مقادیر $c_{j_1}, \cdots, c_{j_l}$ دریافت نشده است، آنگاه این ضرایب از حل دستگاه معادله خطی زیر قابل احتصال است:

$$M(c_1, c_2, \cdots, c_n)^T = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}_{m\times 1},$$

که در آن، M ماتریسی است که توسط گزاره ۲-۴ و توضیحات قبل از آن با انتخاب اعداد $1 \leq j_1 < \cdots < j_{n-l} \leq n$، با این شرط که هیچ‌کدام از آن‌ها با اعداد $j_1, \dots, j_l$ برابر نباشند، معرفی می‌شود.

برای بیان درستی عملکرد این الگوریتم از لحاظ ریاضی، به جهت ارجاع بهتر و توضیح مناسب، بدون از دست دادن هیچ کلیتی فرض می‌کنیم که $j_1 = 1$، $j_2 = 2$، .... و $j_l = l$. بنابراین، از ضرایب قاب اطلاعات کدشده مقادیر $c_n, \dots, c_{l+1}$ برای ما مشخص است و مقادیر مجهول $c_l, \dots, c_1$ را رتیب با $x_l, \dots, x_1$ نمایش می‌دهیم؛ به‌عبارت دیگر ما به‌جای بردار $(c_1, c_2, \cdots, c_n)$ بردار $\tilde{c} = (x_1, x_2, \cdots, x_l, c_{l+1}, \dots, c_n)$ را دریافت کرده‌ایم. چون بردار $\tilde{c}$، بردار ضرایب قاب اطلاعات کدشده f است، باید در دستگاه خطی:

$$M_{F;m+1,\dots,n}\tilde{c}^T = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \qquad (۴)$$

صادق باشد. بنابراین، اگر ماتریس $M_{F;m+1,\dots,n}$ را به دو زیر ماتریس M_1 و M_2 که به ترتیب شامل l ستون اول و مابقی

ستون‌های آن هستند تقسیم کنیم، آن‌گاه تساوی (۴) به‌صورت زیر تبدیل خواهد شد:

$$M_1\begin{pmatrix}x_1\\ \vdots\\ x_l\end{pmatrix}+M_2\begin{pmatrix}c_{l+1}\\ \vdots\\ c_n\end{pmatrix}=\begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix}_{m\times 1}.$$

این نتیجه می‌دهد که:

$$\begin{pmatrix}x_1\\ \vdots\\ x_l\end{pmatrix}=-M_2\begin{pmatrix}c_{l+1}\\ \vdots\\ c_n\end{pmatrix}.$$

لذا، مقادیر مجهول $x_1,\dots,x_l$ از تساوی اخیر قابل محاسبه است.

۳-۲- الگوریتم بازسازی ضرایب قاب مخدوش‌شده با مکان نامشخص و ترتیب درست

حالت دیگری که می‌تواند در فرآیند بازسازی اطلاعات کدشده اخلال ایجاد کند، این است که در بردار ضرایب قاب اطلاعات کدگذاری‌شده f، تعداد l عنصر در مکان‌های نامشخص را از دست داده باشیم و یا به‌اصطلاح مخدوش شده باشند. به‌طور دقیق‌تر، فرض کنید که از بردار $c=(c_1,\dots,c_n)$ به‌عنوان ضرایب قاب اطلاعات کدشده اطلاعات f، فقط زیر بردار $\hat{c}=(c_{i_1},\dots,c_{i_{n-l}})$ از آن در دسترس ما است؛ یعنی، اگر $(\langle Qf,f_1\rangle,\dots,\langle Qf,f_n\rangle)$ دریافت مقادیری باشند که از بردار $c_{i_1},\dots,c_{i_{n-l}}$ دریافت شده‌اند، آن‌گاه:

۱. ترتیب اندیس‌های به‌صورت $i_1<\cdots<i_{n-l}$ است.

۲. اطلاعی در مورد مقدار دقیق اندیس‌های $i_1,\dots,i_{n-l}$ در دسترس نیست.

سوالی که به‌طور طبیعی به ذهن می‌رسد این است که آیا می‌توان مابقی ضرایب قاب و در نتیجه اطلاعات کدشده را از این اطلاعات ناقص دریافت‌شده بازسازی نمود. الگوریتم زیر به بازسازی ضرایب مخدوش‌شده در صورت رخ دادن چنین حالتی می‌پردازد. همان‌طور که خواهیم دید، یک کد خطی معرفی‌شده توسط قاب‌ها زمانی توان مقابله با رخ دادن چنین خطایی در یک کانال ارتباطی را دارد که سطرهای ماتریس مولد آن یک قاب m-مازاد یکنواخت وتقریباً توانمند نسبت به l-مخدوش‌شدگی به‌ازای یک l کمتر اکید از m باشد.

الگوریتم ۳-۲-۱- فرض کنیم F یک قاب m-مازاد یکنواخت است که به‌ازای یک l کمتر اکید از m نسبت به l-مخدوش‌شدگی تقریباً توانمند می‌باشد. همچنین فرض کنید که از بردار ضرایب قاب اطلاعات کدشده $fc=(\langle Qf,f_1\rangle,\dots,\langle Qf,f_n\rangle)$، که در آن Q یک ماتریس معکوس‌پذیر است، دریافت‌کننده، تنها زیربردار $x=(x_1,\dots,x_{n-l})$ را دریافت نموده است؛ به‌عبارت دیگر تنها $(n-l)$-مولفه از بردار c در دسترس ما قرار دارد و همچنین برای ما مشخص نیست که مثلا x_l چندمین مولفه از بردار c است ولی می‌دانیم که ترتیب چینش مولفه‌های بردار x همان ترتیب اصلی آنها در بردار ضرایب قاب است. با توجه به الگوریتم ۳-۱-۱، برای بازسازی ضرایب قاب مخدوش‌شده، کافیست مشخص کنیم که برای هر $1\le p\le n-l$، اسکالر x_l متناظر کدام مولفه از بردار c می‌باشد. برای این منظور مراحل زیر را پیگیری می‌کنیم:

۱. برای هر انتخاب $(n-l)$-تایی از اعداد طبیعی $1\le i_1<\cdots<i_{n-l}\le n$ ماتریس $M_{F,i_1,\dots,i_{n-l}}$ را براساس توضیحات قبل از تعریف ۲-۸ محاسبه می‌کنیم.

۲. اعداد $i_1^o,\dots,i_{n-l}^o$ را به‌عنوان انتخابی از اعداد طبیعی مرحله ۱ در نظر می‌گیریم که تابع $\|M_{F,i_1,\dots,i_{n-l}}x\|$ در آن مقدار مینیمم خود را اخذ می‌کند، به‌عبارت دیگر قرار می‌دهیم:

$$(i_1^o,\dots,i_{n-l}^o)=\arg\min\{\|M_{F,i_1,\dots,i_{n-l}}x\|,\ 1\le i_1<\cdots<i_{n-l}\le n\}.$$

۳. قرار می‌دهیم $c=(c_1,\dots,c_n)$، که در آن، برای هر $p=1,\dots,n-l$ داریم $c_{i_p^o}=x_p$. به‌عبارت دیگر x_p نشان‌دهنده مولفه i_p^oام بردار ضرایب قاب است. بدین ترتیب مکان ضرایب مخدوش‌شده برای ما مشخص می‌شود.

۴. اکنون که مکان ضرایب در دسترس و مخدوش‌شده برای ما مشخص شده است، مشابه الگوریتم ۳-۱-۱ با حل یک دستگاه خطی، ضرایب قاب مخدوش‌شده و در نتیجه اطلاعات کدشده قابل بازسازی است.

برای بیان صحت عملکرد این الگوریتم از لحاظ ریاضی، با توجه به توضیحات ذکرشده در الگوریتم ۳-۱-۱، فقط کافی است علت درستی عملکرد مراحل ۱ تا ۳ الگوریتم حاضر، که به تعیین مکان اتفاق افتادن مخدوش‌شدگی در بردار c اختصاص دارد، را توضیح دهیم. برای این منظور، ابتدا توجه داریم که برای اعداد طبیعی

$$1\le i_1<\cdots<i_{n-l}\le n \quad \text{و} \quad 1\le i_1'<\cdots<i_{n-l}'\le n$$

توانمند بودن قاب F نسبت به l-مخدوش‌شدگی نتیجه می‌دهد که بردار $V_{F,i_1,\dots,i_{n-l}}f$ متعلق به $N(M_{H,i_1',\dots,i_{n-l}'})$ است اگر و تنها اگر تساوی زیر برقرار باشد:

$$(i_1,\dots,i_{n-l})=(i_1',\dots,i_{n-l}').$$

از طرفی، چون $x=(x_1,\dots,x_{n-l})$ یک زیر بردار از بردار c است، پس اعداد طبیعی $1\le i_1<\cdots<i_{n-l}\le n$ موجودند

به‌طوری که:

$$x \in V_{H,i_1,\dots,i_{n-l}}(H) = N\left(M_{H,i_1,\dots,i_{n-l}}\right).$$

از این‌رو، برای تعیین مقدار اعداد طبیعی $i_{n-l},\dots,i_1$ کافی است بررسی کنیم که برای چه انتخابی از اعداد طبیعی $1 \le i_1 < \cdots < i_{n-l} \le n$ تساوی زیر برقرار است.

$$M_{F,i_1,\dots,i_{n-l}}x = \begin{pmatrix}0\\ \vdots \\ 0\end{pmatrix}.$$

به‌عبارت دیگر، کافی است بردار $(i_1^o,\dots,i_{n-l}^o)^T$ را به‌عنوان انتخابی از اعداد طبیعی مرحله ۱ در نظر بگیریم که تابع $\left\|M_{F,i_1,\dots,i_{n-l}}x\right\|$ در آن مقدار کمینه خود را که در حقیقت صفر است را اخذ می‌کند.

۳-۳- الگوریتم بازسازی ضرایب قاب در صورت تغییر آرایش

حالت دیگری که می‌تواند در فرآیند بازسازی اطلاعات کدشده اخلال ایجاد کند، تغییر آرایش و یا به‌اصطلاح به‌هم‌ریختن ترتیب دریافت ضرایب قاب اطلاعات کدگذاری‌شده f می‌باشد. به‌طور دقیق‌تر، فرض کنید برای هر $i = 1,\dots.,n$ مقدار $c_i = \langle Qf, f_i\rangle$ ضرایب قاب اطلاعات کدگذاری‌شده f باشد. با توجه به اینکه در فرآیند بازسازی اطلاعات کدشده از فرمول زیر استفاده می‌کنیم:

$$f = \sum_{i=1}^{n} \langle Qf, f_i\rangle Q^{-1}S^{-1}f_i$$

دریافت ضرایب قاب اطلاعات کدشده با همان ترتیب اصلی بسیار حائز اهمیت است. بنابراین، هرگونه تغییر آرایش در مجموعه ضرایب دریافت‌شده باعث خواهد شد که فرآیند بازسازی به درستی انجام نپذیرد. در ادامه الگوریتمی را معرفی می‌کنیم که در شناسایی ترتیب اصلی ضرایب قاب اطلاعات کدشده به ما کمک خواهد کرد. همانطور که مشاهده خواهیم نمود، در این مرحله، قاب‌های تقریباً خودشناس بسیار کارساز خواهند بود.

الگوریتم ۳-۳-۱- فرض کنیم F، یک قاب m-مازاد یکنواخت و تقریباً خودشناس باشد. همچنین فرض کنید، به‌ازای عملگر معکوس‌پذیر Q، بردار:

$$c = (\langle Qf, f_1\rangle, \dots, \langle Qf, f_n\rangle)$$

ضرایب قاب اطلاعات کدگذاری‌شده f باشد. اگر دریافت‌کننده، بردار $\hat{c} = (c_1, c_2, \dots, c_n)$، که یک تغییر آرایش یافته از بردار c است را به‌عنوان بردار ضرایب قاب دریافت کند. آنگاه، برای مشخص کردن اینکه هرکدام از c_iها کدام مولفه از بردار c است، به‌ترتیب زیر عمل می‌کنیم:

۱. برای هر تغییر آرایش $i_n,\dots,i_1$ از مجموعه اعداد $\{1,\dots,n\}$ مقدار $M(c_{i_1},\dots,c_{i_n})^T$ را محاسبه می‌کنیم، که در آن M ماتریسی است که تساوی $V_F(H) = N(M)$ به‌ازای آن برقرار است.

۲. اعداد $i_1^o,\dots,i_n^o$ را به‌عنوان تجدید آرایشی از مجموعه اعداد $\{1,\dots,n\}$ انتخاب می‌کنیم که مقدار $\left\|M(c_{i_1},\dots,c_{i_n})^T\right\|$ در آن کمینه شود، به‌عبارت دیگر قرار می‌دهیم

$$(i_1^o,\dots,i_n^o) = \arg\min\{\left\|M(c_{i_1},\dots,c_{i_n})^T\right\|, (i_1,\dots,i_n)\ \}.$$

۳. برای هر $j = 1,\dots,n$ قرار می‌دهیم $c_j^o = c_{i_j^o}$.

آن‌گاه می‌توان گفت که تساوی $c_j^o = \langle Qf, f_j\rangle$ ترتیب اصلی مولفه‌های ضرایب قاب را مشخص می‌کند. لذا، به کمک فرمول زیر می‌توانیم اطلاعات کدشده را بازسازی کنیم:

$$f = \sum_{j=1}^{n} c_j^o Q^{-1}S^{-1}f_j.$$

۴- نتیجه‌گیری

در این مقاله، ابتدا ایده استفاده از قاب‌های متناهی در کدکردن اطلاعات را مطرح و سپس قاب‌هایی را معرفی کردیم که کدهای خطی معرفی‌شده توسط آن‌ها از توان بالایی در کشف و تصحیح خطاهای به‌وجودآمده در فرآیند انتقال اطلاعات برخوردار باشد. روش‌هایی برای ساخت مثال‌هایی از چنین قاب‌هایی با استفاده از انواع شناخته‌شده آن‌ها مطرح کردیم و به‌طور ویژه نشان دادیم خانواده‌های معرفی‌شده در برخی مقالات را می‌توان بسیار گسترده در نظر گرفت. در نهایت، چند الگوریتم برای بازسازی دقیق اطلاعات مخدوش‌شده دریافتی نیز ارایه شده است.

۵- منابع

[1] M. Hadi and M. R. Pakravan, "Sequential decoding algorithms of convolutional codes: Implementation, improvement and comparison," Journal of Electronical & Cyber Defence, vol. 3, no. 2, pp. 61-73, 2017. (in Persian)

[2] M. Kenerkouhi and H. Tavakoli, "A new method for combining the channel coding with polar coding-based encryption," Journal of Electronical & Cyber Defence, vol. 4, no. 1, pp. 1-8, 2016. (in Persian)

[3] R. Mceliece, "The theory of information and coding," Cambridge University Press, 2002.

[4] A. Nourazar, Z. Noroozi, and M. Mir, "An optimal method for images steganography based on linear codes features," Journal of Electronical & Cyber Defence, vol. 5, no. 4, pp. 43-53, 2017. (in Persian)

[5] B.G. Bodmann and V. I. Paulsen, "Frames, graphs and erasures," Linear Algebra Appl.vol404, pp. 118-146, 2005.

[6] P. G. Casazza, "The art of frames theory," Taiwanese J. Math., vol. 4, pp. 129-201, 2005.

[7] O. Christensen, "An Introduction to Frames and Riesz Bases," second edition, Brikhauser, Boston, 2016.

[8] H. Javanshiri, "Some properties of approximately dual frames," Results Math, vol. 70, pp. 475-485, 2016.

[9] M. A. Dehghan and M. A. H. Fard, "G-dual frames in Hilbert spaces," UPB Sci. Bull., Series A,vol. 75, no. 1, pp. 129-140, 2013.

[10] D. Hanand and W. Sun, "Reconstruction of signals from frame coefficients with erasures at unknown locations," IEEE Trans. Inf. Theory, vol. 60, pp. 4013-4025, 2014.

[11] D. Han, F. Lv, and W. Sun, "Recovery of signals from unordered partial frame coefficients," Appl. Comput. Harm. Anal., vol. 44, pp. 38-58, 2018.

[12] R. Holmes and V. I. Paulsen, "Optimal frames for erasures," Linear Algebra Appl., vol. 394, pp. 31-51, 2004.

[13] D. Kalra, "Complex equiangular cyclic frames and erasures," Linear Algebra Appl, vol. 419, pp. 373-399, 2006.

[14] F. Lv and W. Sun, "Construction of robust frames in erasure recovery," Linear Algebra Appl., vol. 479, pp. 155-170, 2015.

[15] G. J. Murphy, C*-algebra, and Operator Theory, Academic Press, London, 1990.

[16] M. Mardanpour, M. A. Zare Chahooki, and H. Javanshiri, "Comparative analysis of effectiveness of extended wavelet transforms on transparency and robustness of image watermarking based on matrix factorization," Machine Vision and Image Processing (MVIP), vol. 4, no. 1, pp. 71-87, 2017. (in Persian)

Journal of Electronical & Cyber Defence
Vol. 7, No. 2, 2019, Serial No. 26

Finite Frame as Code: Some Characterizations for Error Correction Codes and Three Algorithms for Troubleshooting in Data Transfer

H. Javanshiri, S. Alikhani*, H. Mazaheri

*Department of Mathematics, Yazd University, Yazd, Iran

(Received: 10/03/2018, Accepted: 27/05/2018)

ABSTRACT

Linear codes in coding theory need matrices whose rows form a basis for a finite dimensional space. In this paper, after introducing some preliminaries about frames, we state the idea of using finite frames instead of basis for encoding of information and then we introduce some frames which their related linear codes are useful in finding and correcting errors in data transfer. A number of methods for producing examples of such frames are presented using some well-known frame types and we show specifically that the families of frames which have been considered in some papers can be extended. Finally, we modify the idea of encoding to facilitate the use of approximate and generalized duals for decoding of received information. Also, some algorithms for decoding of frame coefficients with erasures are proposed.

Keywords: Frame, Operator, Matrix, Approximate Dual, Encoding, Decoding

*Corresponding Author Email: alikhani@yazd.ac.ir