

ساخت ماتریس‌های نمونه‌برداری یقینی بر اساس توابع هش

محمد مهدی محدث^۱، دانشجو، محمدحسین کهای^۲، دانشیار

۱- دانشکده مهندسی برق - دانشگاه علم و صنعت ایران - تهران - ایران - mohamadmm1368@gmail.com

۲- دانشکده مهندسی برق - دانشگاه علم و صنعت ایران - تهران - ایران - kahaei@iust.ac.ir

چکیده: ماتریس‌های نمونه‌برداری نقش اساسی در حسگری فشرده دارند. این ماتریس‌ها به صورت تصادفی و یقینی قابل ساخت هستند. ماتریس‌های یقینی به علت اینکه حافظه کمتری برای ذخیره‌سازی نیاز دارند مورد توجه زیادی قرار گرفته‌اند. در این مقاله دسته‌ای از ماتریس‌های حسگری یقینی، با استفاده از توابع هش ساخته می‌شوند. برای این منظور ابتدا یک ماتریس کد اولیه ساخته می‌شود، سپس با استفاده از ماتریس توابع هش، یک ماتریس جدید ساخته می‌شود. در نهایت با یک‌سازی تمامی درایه‌های این ماتریس، ماتریس نمونه‌برداری ساخته می‌شود. این دسته از ماتریس‌ها دارای ابعاد $p^2 \times p^3$ و ضریب هم‌دوسی $1/p$ هستند. نتایج شبیه‌سازی نشان می‌دهند که به ازای مقادیر کم p بازسازی سیگنال اصلی به ازای نمونه‌برداری توسط این دسته از ماتریس‌ها عملکرد بهتری نسبت به ماتریس‌های یقینی تولیدشده توسط کدهای BCH دارد.

واژه‌های کلیدی: تابع هش، ماتریس کد، ضریب هم‌دوسی، RIP.

Low coherence deterministic matrices construction using Hash functions

M. M. Mohades¹, Student, M. H. Kahaei², Associate professor

1- School of Electrical Engineering, IUST, Tehran, Iran, mohamad.mohaddes@gmail.com

2- School of Electrical Engineering, IUST, Tehran, Iran, kahaei@iust.ac.ir

Abstract: Deterministic measurement matrices have a crucial character in compressive sensing (CS) applications. These matrices can be generated randomly and deterministically. Due to less memory needed for storage, deterministic matrices have been taken into consideration vastly rather than random ones. In this paper, by use of Hash functions (HF), a group of new measurement matrices has been presented. For this purpose, first, a primary matrix of code is generated then by use of Hash matrices a new matrix is produced. Finally by normalizing the new matrix elements, measurement matrix will be generated. Through this construction, a group of measurement matrices with size of $p^2 \times p^3$ and coherence coefficient equal to $1/p$, where p is a prime integer, will be obtained. Simulation results illustrate that for low values of p , proposed matrices slightly outweigh BCH sampling matrices.

Keywords: Hash function, coherence coefficient, matrix of code, restricted isometry property (RIP).

تاریخ ارسال مقاله: ۹۴/۱۰/۱۴

تاریخ اصلاح مقاله: ۹۵/۲/۴

تاریخ پذیرش مقاله: ۹۵/۲/۱۳

نام نویسنده مسئول: محمدحسین کهای

نشانی نویسنده مسئول: تهران، خیابان نارمک، دانشگاه علم و صنعت، دانشکده برق.

۱- مقدمه

حسگری فشرده روشی شناخته شده به منظور نمونه‌برداری از سیگنال‌های تنک است. سیگنال s تنک^۱، سیگنالی است با طول n که حداکثر s ورودی غیرصفر داشته باشد. در این روش، ترکیب خطی از نمونه‌های سیگنال به عنوان بردار اندازه‌گیری^۲ ذخیره می‌شوند. به عبارتی $y_{m \times 1} = A_{m \times n} x_{n \times 1}$ است که در آن y بردار اندازه‌گیری، x سیگنال s تنک و $A_{m \times n}$ ماتریس نمونه‌برداری است که $m \ll n$ است. در حالت $m < n$ ، مسئله $y_{m \times 1} = A_{m \times n} x_{n \times 1}$ زمانی که y معلوم و x مجهول است و باید بازسازی شود، بی‌شمار جواب دارد و به منظور به دست آوردن جواب اصلی باید مسئله زیر حل شود [۱]:

$$\arg \min_x \|x_{n \times 1}\|_{l_0} \quad \text{s.t.} \quad y_{m \times 1} = A_{m \times n} x_{n \times 1} \quad (1)$$

که در آن $\|\cdot\|_{l_0}$ نشان دهنده نرم صفر یک بردار است.

از آنجایی که مسئله نرم صفر یک مسئله غیرمحدب و مشتق‌ناپذیر است، یک مسئله NPC^۳ است و به منظور حل آن باید جستجوی کامل انجام شود، که این موضوع به ازای ابعاد بزرگ سیگنال غیرممکن است [۲]. بنابراین این مسئله را با یک مسئله نرم ۱ تقریب می‌زنند و مسئله به صورت زیر بیان می‌شود [۳، ۴]:

$$\arg \min_x \|x_{n \times 1}\|_{l_1} \quad \text{s.t.} \quad y_{m \times 1} = A_{m \times n} x_{n \times 1} \quad (2)$$

کندس و تائو [۵] یک شرط کافی برای قابلیت بازسازی سیگنال نمونه‌برداری شده توسط ماتریس نمونه‌برداری مطرح کردند که این شرط RIP^۴ نام دارد. یک ماتریس نمونه‌برداری در شرط RIP از درجه s صدق می‌کند اگر δ_s با شرط $0 \leq \delta_s \leq 1$ وجود داشته باشد که به ازای هر سیگنال s تنک، ماتریس نمونه‌برداری در رابطه زیر صدق کند:

$$\forall x \in R^n \quad 1 - \delta_s \leq \frac{\|\Phi x\|_2^2}{\|x\|_2^2} \leq 1 + \delta_s \quad (3)$$

که δ_s ثابت RIC^۵ نام دارد. اگر ماتریس نمونه‌برداری در شرط RIP صدق کند امکان بازسازی یکنای سیگنال توسط کمینه‌سازی L_1 وجود دارد. دو دسته کلی از ماتریس‌های نمونه‌برداری، ماتریس‌های تصادفی^۶ و یقینی^۷ هستند. نشان داده شده که اگر درایه‌های ماتریس نمونه‌برداری $A_{m \times n}$ دارای توزیع یکسان باشند و همچنین $s \leq C m / \log(n/s)$ (C) ثابت، n, m ابعاد ماتریس و s درجه تنکی باشد، با احتمال زیاد شرط RIP از درجه s را ا قناع می‌کند [۶]. در ماتریس‌های یقینی شرط RIP با استفاده از ضریب همدوسی ماتریس بررسی می‌شود.

ضریب همدوسی ماتریس یقینی Φ با ستون‌های $\phi_1, \phi_2, \dots, \phi_n$ به صورت زیر تعریف می‌شود:

$$\mu(\Phi) = \max_{i \neq j} \frac{|\langle \phi_i, \phi_j \rangle|}{\|\phi_i\|_2 \cdot \|\phi_j\|_2} \quad 1 \leq i, j \leq n \quad (4)$$

قضیه ۱. ماتریس یقینی دلخواه $A_{m \times n}$ با همدوسی μ شرط RIP از درجه s را ا قناع می‌کند که $s < \frac{1}{\mu} + 1$ و $\delta_s < \mu(s-1)$ است [۷].

قضیه زیر که به کران ولش^۸ مشهور است، حداقل ضریب همدوسی یک ماتریس یقینی را تعیین می‌کند [۸].

قضیه ۲. حداقل ضریب همدوسی ماتریس یقینی $A_{m \times n}$ برابر است با $\mu_{\min}$ که از رابطه زیر به دست می‌آید (با شرط $m \leq n$):

$$\mu_{\min} = \sqrt{\frac{n-m}{m(n-1)}} \quad (5)$$

در حالتی که $m \ll n$ باشد، رابطه بالا به صورت زیر ساده می‌شود:

$$\lim_{\frac{n}{m} \rightarrow \infty} \mu_{\min} = \frac{1}{\sqrt{m}} \quad (6)$$

با استفاده از رابطه ۶ و قضیه ۱ می‌توان دید که در یک ماتریس یقینی $m = O(s^2)$ است که m از درجه s^2 است. درحالی که در یک ماتریس تصادفی $m \geq O\left(s \log\left(\frac{n}{s}\right)\right)$ است [۹]. بنابراین به ازای RIP با درجه یکسان، ممکن است ماتریس نمونه‌برداری یقینی به تعداد سطرهاى بیش‌تری نسبت به ماتریس تصادفی برای یک نمونه‌برداری قابل بازسازی نیاز داشته باشد. با این وجود به منظور ذخیره کردن ماتریس یقینی حافظه کم‌تری نسبت به ماتریس‌های تصادفی مورد نیاز است. زیرا که برای ذخیره کردن ماتریس تصادفی باید تمامی درایه‌های آن را ذخیره کرد، حال آنکه یک ماتریس یقینی با توابع معلومی ساخته می‌شود و بنابراین نیازی به ذخیره تمامی المان‌های آن نیست. علاوه بر این پیاده‌سازی ماتریس‌های یقینی نسبت به ماتریس‌های تصادفی ساده‌تر است. بنابراین ساخت ماتریس‌های یقینی مورد توجه زیادی قرار گرفته است.

در طی چند سال اخیر ماتریس‌های نمونه‌برداری یقینی مختلفی ارائه شدند که ساختار بیش‌تر آن‌ها بر اساس میدان‌های متناهی است. در [۱۰] DeVore با استفاده از چندجمله‌ای‌های روی میدان متناهی $\mathbb{F}_p$ ماتریس‌های دودویی با ابعاد $p^2 \times p^{r+1}$ و ضریب همدوسی r/p تولید کرده است که RIP با درجه $s < p/r + 1$ را ارضا می‌کند. در [۱۱]، نویسندگان با الهام از روش DeVore و با استفاده از کدهای هندسه جبری ماتریس‌های باینری تولید کرده‌اند و به ازای دو خم معروف بیضوی و هرمیتین ضریب همدوسی ماتریس‌های متناظر را به دست آورده‌اند.

در [۱۲]، کدهای BCH با فاصله همینگ زیاد به منظور تولید ماتریس‌های یقینی دوقطبی با ابعاد $2^{O(2^{\frac{p-1}{2}})} \times (2^l - 1)$ و ضریب همدوسی $\mu \leq (2^{l-1} - 1)/(2^l - 1)$ استفاده شده‌اند. این دسته از ماتریس‌ها شرط RIP از درجه $s \leq 2^l + 1$ را ارضا می‌کنند. در [۱۳]، با استفاده از کدهای BCH p -تایی، ساختار ماتریس‌های [۱۲] تعمیم یافته‌اند و نشان داده شده است که با افزایش p ضریب همدوسی ماتریس به کران ولش نزدیک می‌شود.

از طرفی دیگر ماتریس‌های نمونه‌برداری یقینی وجود دارند که شرط RIP را ارضا نمی‌کنند اما در حسگری فشرده کاربرد دارند. در ماتریس‌های نمونه‌برداری مبتنی بر ضریب همدوسی همواره $m \geq O(s^2)$ است اما در [۱۴] با استفاده از ماتریس مجاورت گراف‌های Extractor ماتریس‌های نمونه‌برداری یقینی ساخته شده‌اند که $m \geq O(s)$ است و قابلیت بازسازی سیگنال s تنک وجود دارد. این ماتریس زمانی کارایی

علامت $\oplus$ به معنای جمع المان به المان است و جمع در میدان $\mathbb{F}_p$ انجام می‌شود.

دلیل استفاده از توابع هش و اصول جایگذاری ستونی به‌منظور تولید ماتریس حسگری در ادامه آمده است.

طبق قضیه قبل با استفاده از ماتریس‌های کدی که فاصله همینگ بالایی دارند و دارای کد تمام ۱ هستند می‌توان ماتریس‌های حسگری با ضریب همدوسی پایین طراحی کرد. ماتریس‌های الگوی هش را می‌توان از روی ماتریس‌های کد تولید کرد. حال اگر یک ماتریس کد اولیه با فاصله همینگ بالا در یک ماتریس الگوی هش جایگذاری ستونی شود، ماتریسی به دست می‌آید که می‌تواند فاصله همینگ زیادی داشته باشد. بنابراین در این مقاله از ماتریس‌های هش در طراحی ماتریس‌های حسگری یقینی استفاده می‌شود.

۱-۱-۲ - مراحل ساخت ماتریس کد با فاصله همینگ بالا و شامل کد تمام ۱ با استفاده از توابع هش

مراحل ۱ تا ۸ نحوه ساخت ماتریس را نشان می‌دهند، این مراحل با استفاده از یک مثال روی میدان متناهی $\mathbb{F}_4$ که در آن $p = 2$ است، پی‌گیری می‌شوند:

۱- بردارهای $\mathbf{u}_1$ و $\mathbf{u}_2$ و ماتریس مولد کد $\mathbf{G}$ را به‌صورت زیر در نظر بگیرید:

$$\mathbf{u}_1 = (1 \ 1 \ \dots \ 1)^T, \mathbf{u}_2 = (0 \ 1 \ \dots \ p-1)^T$$

$$\mathbf{G} = \begin{pmatrix} \mathbf{u}_1^T \\ \mathbf{u}_2^T \end{pmatrix} = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 0 & 1 & \dots & p-1 \end{pmatrix} \quad (8)$$

$\mathbf{u}_2$ شامل تمامی المان‌های میدان متناهی $\mathbb{F}_2$ است.

مثال:

$$\mathbf{G} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad (9)$$

۲- المان‌های میدان $\mathbb{F}_{p^2}$ را به‌صورت زیر در نظر بگیرید که α ریشه اولیه میدان است:

$$\mathbb{F}_{p^2} = \{0, \dots, i\alpha + j, \dots, (p-1)\alpha + p-1\} \quad (10)$$

که در رابطه بالا $i, j \in \mathbb{F}_p$ هستند.

مثال بر روی میدان $\mathbb{F}_4$

$$\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\} \quad (11)$$

۳- ماتریس کدی که توسط ماتریس مولد $\mathbf{G}$ روی میدان $\mathbb{F}_p$ تولید می‌شود را به‌عنوان ماتریس اولیه $\mathbf{A}$ در نظر بگیرید. ستون‌های این ماتریس به شکل زیر خواهند بود:

$$i\mathbf{u}_1 + j\mathbf{u}_2 \quad \text{for } i, j \in \mathbb{F}_p \quad (12)$$

ماتریس $\mathbf{A}$ دارای p سطر و p^2 ستون خواهد بود. هر ستون از ماتریس $\mathbf{A}$ معادله‌ای به فرم $i\mathbf{u}_1 + j\mathbf{u}_2$ دارد و به خاطر فرمی که بردارهای $\mathbf{u}_1$ و $\mathbf{u}_2$ دارند مانند یک چندجمله‌ای درجه یک است. پس هر دو ستونی که از ماتریس $\mathbf{A}$ در نظر گرفته شوند حداکثر در یک نقطه با هم مشترک هستند. بنابراین ماتریس کد موجود دارای

مناسب دارد که نمونه‌های سیگنال بدون نویز باشند. در [۱۵] نویسنده با استفاده از کدهای Reed-Muller ماتریس‌های دوقطبی با ابعاد $2^{l+1} \times 2^{l+1}$ تولید کرده است. با وجود اینکه کران پایین برای درجه RIP این دسته از ماتریس‌ها به اثبات نرسیده است اما نتایج شبیه‌سازی نشان‌دهنده عملکرد مناسب این ماتریس‌ها است. علاوه‌براین ماتریس‌های نمونه‌برداری یقینی ارائه شده‌اند که شرایط NSP^۱ را اقلان کرده و در حسگری فشرده کاربرد دارند. شرط NSP یک شرط ضعیف‌تر نسبت به شرط RIP است که اگر سیگنال تنک، نویزی باشد دیگر کاربرد ندارد. ازجمله این ماتریس‌ها ماتریسی است که با به‌کارگیری توابع هش در [۱۶] ارائه شده است.

در این مقاله با استفاده از توابع هش و اصول جایگذاری ستونی، ماتریس‌های حسگری یقینی با ابعاد $p^2 \times p^3$ و ضریب همدوسی $1/p$ ارائه شده است. با توجه به کران ولش این دسته از ماتریس‌ها به‌طور مجانبی بهینه هستند.

ادامه مقاله به این صورت سازمان‌دهی شده است: در بخش ۲ ماتریس نمونه‌برداری طراحی می‌شود و ضریب همدوسی آن محاسبه می‌شود. در بخش ۳ نتایج شبیه‌سازی ارائه می‌شود. نتیجه‌گیری در بخش ۴ آمده است.

۲- ارائه ماتریس‌های حسگری یقینی با ضریب همدوسی کم

در زیربخش ۱-۲ روش ساخت ماتریس حسگری یقینی بر اساس توابع هش توضیح داده می‌شود و در زیر بخش ۲-۲ ضریب همدوسی ماتریس حسگری محاسبه می‌شود.

۱-۲ - روش ساخت ماتریس‌های حسگری یقینی بر اساس توابع هش طبق قضیه زیر می‌توان از ماتریس‌های کد با فاصله همینگ زیاد، ماتریس‌های حسگری فشرده با همدوسی کم تولید نمود. که بعد از بیان این قضیه، در بخش‌های بعد نحوه تولید ماتریس‌های این مقاله ارائه می‌شود.

قضیه ۳ [۱۳]. فرض کنید $C[N; n, p, d_{\min}]$ یک کد خطی p سمبلی بر روی میدان $\mathbb{F}_p$ با حداقل فاصله $d_{\min}$ باشد، به‌طوری‌که بردار تمام یک متعلق به فضای کد باشد. فرض کنید $\tilde{\mathbf{A}}_{N \times p^{l-1}}$ ماتریس حاصل از کنار هم گذاشتن بردارهای کد به‌صورت ستونی باشد به‌نحوی که از هر مجموعه به شکل $\{\mathbf{a}, \mathbf{a} \oplus \mathbf{1}_{N \times 1}, \dots, \mathbf{a} \oplus (\mathbf{p}-1)_{N \times 1}\}$ دقیقاً یکی انتخاب شده باشد. اکنون اگر ماتریس $\mathbf{A}_{N \times p^{l-1}}$ از به توان رساندن و سپس یک‌ه کردن ماتریس $\tilde{\mathbf{A}}$ به‌صورت زیر ساخته شود:

$$\tilde{\mathbf{A}} = [\tilde{a}_{\alpha\beta}]_{\alpha, \beta} \Rightarrow \mathbf{A} = \frac{1}{\sqrt{N}} \left[e^{j \frac{2\pi}{p} \tilde{a}_{\alpha\beta}} \right]_{\alpha, \beta} \quad (17)$$

آنگاه ضریب همدوسی ماتریس $\mathbf{A}$ حداکثر برابر با $(p(p-1)N - p^2 d_{\min}) / 2N$ خواهد بود.

$$\mathbf{B}(\mathbf{P}) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \end{pmatrix} \quad (18)$$

همان‌طور که واضح است به ازای المان‌های ماتریس $\mathbf{P}$ ستون معادل از ماتریس $\mathbf{A}$ انتخاب و جایگذاری شده است.

۷- ماتریس نمونه‌برداری را به شکل زیر تولید کنید:

توجه شود که ماتریس $\mathbf{B}(\mathbf{P})$ همانند مثال قبل بر روی میدان

$\mathbb{F}_p$ قرار دارد.

$$\mathbf{B}(\mathbf{P}') = [b_{rs}]_{r,s} \Rightarrow \mathbf{S} = \frac{1}{\sqrt{p^2}} \left[e^{j \frac{2\pi}{p} b_{rs}} \right]_{r,s} \quad (19)$$

که $1/\sqrt{p^2}$ ضریب یک‌سازی است و $\mathbf{B}(\mathbf{P}')$ از روی ماتریس $\mathbf{B}(\mathbf{P})$ با حذف کد تمام ۱ و تمامی ترکیبات خطی آن به دست می‌آید نحوه ساخت ماتریس $\mathbf{B}(\mathbf{P}')$ در بخش ۲-۳-۳ توضیح داده می‌شود.

به‌طورمثال $\mathbf{B}(\mathbf{P}')$ به‌صورت زیر خواهد شد:

$$\mathbf{B}(\mathbf{P}') = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \quad (20)$$

$$\mathbf{S} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 \end{pmatrix} \quad (21)$$

۸- در بخش ۲-۲ اثبات می‌شود که ضریب همدوسی این ماتریس برابر با $1/p$ است.

به‌طورمثال بدیهی است که همدوسی ماتریس رابطه (۲۱) برابر با $0/5$ است.

۲-۱-۲- بررسی ماتریس $\mathbf{B}(\mathbf{P})$ برای داشتن شرایط قضیه ۳

در این قسمت باید ابتدا اثبات کرد که ماتریس $\mathbf{B}(\mathbf{P})$ یک ماتریس کد و شامل کد تمام ۱ است. همچنین باید نشان داد که فاصله همینگ این ماتریس بزرگ است. به‌منظور اثبات این که ماتریس $\mathbf{B}(\mathbf{P})$ یک ماتریس کد است باید نشان داد که مجموع هر دو کلمه از ماتریس $\mathbf{B}(\mathbf{P})$ یا به عبارتی مجموع هر دو ستون از این ماتریس، روی میدان $\mathbb{F}_p$ یک کلمه کد است که در ماتریس $\mathbf{B}(\mathbf{P})$ وجود دارد.

۲-۱-۳- اثبات ماتریس کد بودن $\mathbf{B}(\mathbf{P})$

دو ستون دلخواه p و p' از ماتریس $\mathbf{P}$ را به شکل زیر در نظر بگیرید (خواننده می‌تواند روابط زیر را با توجه به مثال‌هایی که در بخش ۲-۱-۲ در ارتباط با نحوه ساخت ماتریس روی میدان متناهی $\mathbb{F}_4$ آورده شده است پی‌گیری نماید):

فاصله همینگ برابر با $p-1$ است.

مثال به ازای $p=2$

$$\mathbf{A} = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \quad (13)$$

۴- ماتریس کدی را که توسط ماتریس مولد $\mathbf{G}$ روی میدان $\mathbb{F}_{p^2}$ تولید می‌شود را به‌عنوان ماتریس الگوی هش $\mathbf{P}$ در نظر بگیرید. ماتریس الگوی هش ماتریسی است که در ادامه از آن به‌منظور جایگذاری ستونی و تولید ماتریس کد دلخواه استفاده می‌شود. این موضوع در ادامه بررسی می‌شود. آیین ستون این ماتریس به شکل زیر خواهند بود:

$$\psi_i = a u_1 + b u_2 \quad (14)$$

در رابطه بالا $a, b \in \mathbb{F}_{p^2}$ هستند. ماتریس Ψ دارای p سطر و p^2 ستون است. فاصله همینگ این ماتریس کد هم برابر با $p-1$ است.

مثال به ازای میدان $\mathbb{F}_4$ ماتریس Ψ به‌صورت زیر خواهد بود:

$$\Psi = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 1 & \alpha & \alpha+1 \\ 0 & 1 & 0 & 1 & \alpha & \alpha+1 & 0 & 1 \\ \alpha & \alpha+1 & \alpha & \alpha+1 & 0 & \alpha & \alpha+1 & 1 \\ \alpha & \alpha+1 & \alpha+1 & \alpha & \alpha+1 & 1 & 0 & \alpha \end{pmatrix} \quad (15)$$

۵- یک تناظر یک‌به‌یک بین المان‌های میدان $\mathbb{F}_{p^2}$ و بردارهای با فرم $i u_1 + j u_2$ را در نظر بگیرید. به عبارتی:

$$\phi: i\alpha + j \rightarrow i u_1 + j u_2 \quad (16)$$

که $i, j \in \mathbb{F}_p$ هستند و ϕ یک تناظر بین المان‌های ماتریس $\mathbf{P}$ و ستون‌های ماتریس $\mathbf{A}$ ایجاد می‌کند که در جایگذاری ستونی مورد استفاده قرار می‌گیرد.

برای مثال ستون‌های ماتریس $\mathbf{A}$ به‌صورت زیر با مثال رابطه (۱۵) در تناظر خواهد بود:

$$\mathbf{A} = \begin{pmatrix} 0\alpha+0=0 & 0\alpha+1=1 & 1\alpha+0=\alpha & 1\alpha+1=\alpha+1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \quad (17)$$

جایگذاری ستونی دو ماتریس به‌صورت زیر تعریف می‌شود:

تعریف. ماتریس اولیه $\mathbf{A} \in \mathbb{R}^{r \times m}$ با $\mathbf{A}=(a_{ij})$ و همچنین ماتریس الگو $\mathbf{A}'$ را $\mathbf{P}=(p_{ij})$ با فرم $\mathbf{P} \in \{1, \dots, m\}^N \times n$ ستونی ماتریس $\mathbf{A}$ در ماتریس $\mathbf{P}$ ماتریس $\mathbf{B}(\mathbf{P})=(b_{ij}) \in \mathbb{R}^{N \times n}$ است به‌گونه‌ای که $b_{(\beta-1)r+s,\gamma} = a_{s,p_{\beta\gamma}}$ است به ازای $1 \leq \gamma \leq n$ ، $1 \leq \beta \leq N$ و $1 \leq s \leq r$.

۶- ماتریس $\mathbf{B}(\mathbf{P})$ که حاصل جایگذاری ستونی ماتریس $\mathbf{A}$ در ماتریس $\mathbf{P}$ طبق تناظر ϕ است را در نظر بگیرید.

در ادامه اثبات می‌شود که ماتریس $\mathbf{B}(\mathbf{P})$ یک ماتریس کد خطی است که شامل کد تمام ۱ است و همچنین با محاسبه فاصله همینگ آن نشان داده می‌شود که در شرایط قضیه ۳ صدق می‌کند.

به‌طورمثال ماتریس $\mathbf{B}(\mathbf{P})$ معادل با روابط ۱۵ و ۱۷ به شکل زیر خواهد بود؛ به ازای $p=2$:

در این حالت طبق جایگذاری ستونی، ستون‌های متفاوتی از ماتریس **A** روبروی هم قرار می‌گیرند که فاصله همینگ آن‌ها برابر است با $p-1$ ، بنابراین در نهایت حداقل فاصله بین دو ستون از ماتریس **B(P)** برابر با $p^2 - p$ خواهد بود.

(۲) دو کلمه‌کد از ماتریس **P** در $p-1$ المان با هم متفاوت باشند. طبیعتاً این دو کلمه‌کد در یک المان با هم مشترک هستند.

در این حالت طبق جایگذاری ستونی، به جای $p-1$ المان از این دو کلمه‌کد، ستون‌های متفاوتی از ماتریس **A** که فاصله همینگ آن‌ها برابر با $p-1$ است روبروی هم قرار می‌گیرند و فقط در المان مشترک این دو کلمه‌کد، یک ستون از ماتریس **A** قرار می‌گیرد. بنابراین در نهایت حداقل فاصله بین دو ستون ماتریس **B(P)** برابر خواهد بود با $p^2 - (p-1) - p = (p-1)^2$.

پس فاصله همینگ ماتریس **B(P)** برابر است با $(p-1)^2$ ؛ که به‌طور جدی و با افزایش مقدار p ، فاصله همینگ به سمت طول کد، $n = p^2$ میل می‌کند. بنابراین ماتریس کد **B(P)** تمامی شرایط قضیه ۳ را دارد و می‌توان از این قضیه به‌منظور تولید ماتریس حسگری استفاده کرد.

۲-۳-۱- نحوه ساخت ماتریس‌های **B(P')**

در قضیه ۳ بیان شد که از هر مجموعه به شکل $\{a, a \oplus \mathbf{1}_{N \times 1}, \dots, a \oplus (p-1) \cdot \mathbf{1}_{N \times 1}\}$ فقط یکی انتخاب شود. برای این منظور می‌توان کد تمام یک را از ماتریس کد حذف کرد که با حذف کد تمام یک، تمامی ترکیب‌های خطی آن هم حذف خواهد شد. همان‌طور که بیان شد ستون $\alpha \mathbf{u}_1$ از ماتریس الگوی هش متناظر با کد تمام یک از ماتریس **B(P)** است، بنابراین به‌منظور حذف کد تمام یک از ماتریس **B(P)**، کافی است ستون $\alpha \mathbf{u}_1$ از ماتریس الگوی هش حذف شود. طبیعی است که با حذف ستون $\alpha \mathbf{u}_1$ باید تمامی ستون‌هایی که در ماتریس کد توسط این ستون تولید می‌شده‌اند هم حذف شوند تا خاصیت خطی بودن کد باقی بماند. بنابراین ستون‌های ماتریس الگوی هش جدید که با **P'** نمایش داده می‌شود به‌صورت زیر خواهد بود:

$$a\mathbf{u}_1 + b\mathbf{u}_2 \quad \text{for } a \in \mathbb{F}_p, b \in \mathbb{F}_p \quad (29)$$

به‌عبارت دیگر طبق رابطه بالا به‌منظور حذف ستون $\alpha \mathbf{u}_1$ کافی است که ضریب a فقط متعلق به $\mathbb{F}_p$ باشد زیرا که ضریب α متعلق به میدان بالاتر یعنی میدان $\mathbb{F}_{p^2}$ است.

- ماتریس **B(P')** حاصل جایگذاری ستونی ماتریس **A** طبق

ماتریس الگوی **P'** است.

- اینکه $a \in \mathbb{F}_p$ است تضمین می‌کند در ماتریس **B(P')** کد

تمام یک وجود ندارد.

- حال می‌توان ماتریس حسگری **S** را بر اساس **B(P')** مطابق

قضیه ۳ به‌دست آورد.

۲-۲- محاسبه ضریب همدوسی ماتریس حسگری **S**

همدوسی ماتریس **S** با ستون‌های $s_1, s_2, \dots, s_n$ برابر است با:

$$\begin{cases} \mathbf{p} = a\mathbf{u}_1 + b\mathbf{u}_2 \\ a = a_1\alpha + a_2, b = b_1\alpha + b_2 \\ \mathbf{p}' = a'\mathbf{u}_1 + b'\mathbf{u}_2 \\ a' = a_1'\alpha + a_2', b' = b_1'\alpha + b_2' \end{cases} \quad (22)$$

که در روابط بالا $a, b, a', b' \in \mathbb{F}_{p^2}$ و $a_1, a_2, b_1, b_2, a_1', a_2', b_1', b_2' \in \mathbb{F}_p$ هستند.

المان‌های دو ستون **p** و **p'** به‌صورت زیر قابل بیان هستند:

$$\mathbf{p} = (p_\gamma)_{p \times 1}, \mathbf{p}' = (p'_\gamma)_{p \times 1} \quad (23)$$

که به ازای $\gamma \in \mathbf{u}_2$ روابط (۲۳) و (۲۴) به‌صورت زیر برقرارند:

$$\begin{cases} p_\gamma = c_{1\gamma}\alpha + c_{2\gamma} \\ p'_\gamma = c'_{1\gamma}\alpha + c'_{2\gamma} \end{cases} \quad (24)$$

$$\begin{cases} c_{1\gamma} = a_1 + b_1\gamma, c_{2\gamma} = a_2 + b_2\gamma \\ c'_{1\gamma} = a'_1 + b'_1\gamma, c'_{2\gamma} = a'_2 + b'_2\gamma \end{cases} \quad (25)$$

طبق نگاشت φ که در بالا بیان شد، ستون‌های **b** و **b'** از ماتریس **B(P)**، بر اساس ستون‌های **p** و **p'** از ماتریس الگوی هش و با قرار دادن ستون متناظر از ماتریس **A** به دست می‌آیند. حال باید دید که آیا مجموع دو ستون دلخواه **b** و **b'**، برابر با ستون دیگری از **B(P)** خواهد شد یا خیر.

فرض کنید ستون‌های **b** و **b'** طبق نگاشت φ به شکل زیر هستند:

$$\mathbf{b} = (b_\gamma)_{p^2 \times 1}, \mathbf{b}' = (b'_\gamma)_{p^2 \times 1} \quad (26)$$

که به ازای $\gamma \in \mathbf{u}_2$:

$$b_\gamma = c_{1\gamma}\mathbf{u}_1 + c_{2\gamma}\mathbf{u}_2, b'_\gamma = c'_{1\gamma}\mathbf{u}_1 + c'_{2\gamma}\mathbf{u}_2 \quad (27)$$

بنابراین به ازای $\gamma \in \mathbf{u}_2$ رابطه زیر برقرار خواهد بود:

$$\begin{aligned} \mathbf{b}'' &= \mathbf{b} + \mathbf{b}' = c_{1\gamma}\mathbf{u}_1 + c_{2\gamma}\mathbf{u}_2 + c'_{1\gamma}\mathbf{u}_1 + c'_{2\gamma}\mathbf{u}_2 \\ &= (c_{1\gamma} + c'_{1\gamma})\mathbf{u}_1 + (c_{2\gamma} + c'_{2\gamma})\mathbf{u}_2 \\ &= (a_1 + b_1\gamma + a'_1 + b'_1\gamma)\mathbf{u}_1 \\ &\quad + (a_2 + b_2\gamma + a'_2 + b'_2\gamma)\mathbf{u}_2 \\ &= ((a_1 + a'_1) + (b_1 + b'_1)\gamma)\mathbf{u}_1 \\ &\quad + ((a_2 + a'_2) + (b_2 + b'_2)\gamma)\mathbf{u}_2 \end{aligned} \quad (28)$$

بدیهی است که ستون **b''** معادل آن است که ابتدا ستون‌های **p** و **p'** را در ماتریس الگوی هش با همدیگر جمع کرده و سپس ماتریس متناظر آن را طبق نگاشت φ به دست آورد. بنابراین می‌توان نتیجه گرفت که **b''** هم یک ستون از ماتریس **B(P)** است. بنابراین یک ماتریس کد خطی است.

از طرفی باید توجه کرد که طبق نگاشت φ المان α متناظر با بردار $\mathbf{u}_1$ است و لذا ستون $\alpha \mathbf{u}_1$ از ماتریس الگوی هش متناظر با کد تمام یک از ماتریس **B(P)** خواهد بود. بنابراین ماتریس **B(P)** یک ماتریس کد خطی است که بردار کد تمام ۱ هم متعلق به آن است.

اکنون به‌منظور استفاده از قضیه ۳ باید فاصله همینگ این ماتریس کد را به دست آورد. فاصله همینگ این ماتریس کد با توجه به تحلیل زیر قابل محاسبه است.

۲-۳-۱-۲- فاصله همینگ ماتریس کد **B(P)**

همان‌طور که بیان شد ماتریس **A** یک ماتریس کد با فاصله همینگ $p-1$ است. همچنین ماتریس **P**، یک ماتریس کد با فاصله همینگ $p-1$ است. بنابراین دو حالت پیش می‌آید:

(۱) دو کلمه‌کد از ماتریس **P** در هر p المان با هم متفاوت باشند.

شده است. در نتیجه برای $\gamma \in \mathbf{u}_2$ ، $c_{1\gamma}'' = a_1'' + b_1''\gamma$ است و بنابراین $b_{1\gamma}'' = a_1'' + b_1''\gamma$ خواهد بود، در این حالت مقدار a_1'' تأثیری ندارد. در این حالت رابطه زیر برقرار است:

$$\frac{1}{p^2} \left| \sum_{\gamma \in \mathbf{u}_2} \sum_{\lambda \in \mathbf{u}_2} e^{j \frac{2\pi}{p} (b_{1\gamma}'')} \right| = \frac{1}{p^2} \left| \sum_{\gamma \in \mathbf{u}_2} \sum_{\lambda \in \mathbf{u}_2} e^{j \frac{2\pi}{p} (a_1'' + b_1''\gamma)} \right| = 0 \quad (41)$$

در این حالت فرض کنید $b_2'' \neq 0$ و a_2'' هر مقدار دلخواهی باشد. پس $c_{2\gamma}'' = a_2'' + b_2''\gamma$ و $b_{2\gamma}'' = c_{2\gamma}'' + c_{2\gamma_1}''\lambda$ خواهند بود که در این حالت مقدار $c_{2\gamma_1}''$ مهم نیست. همچنین فرض کنید $c_{2\gamma_1}'' = 0$ که طبیعتاً به ازای $\gamma \neq \gamma_1$ مقدار $c_{2\gamma}'' = 0$ است. بنابراین:

$$\begin{aligned} \frac{1}{p^2} \left| \sum_{\gamma \in \mathbf{u}_2} \sum_{\lambda \in \mathbf{u}_2} e^{j \frac{2\pi}{p} (b_{2\gamma}'')} \right| &= \frac{1}{p^2} \left| \sum_{\gamma \in \mathbf{u}_2} \sum_{\lambda \in \mathbf{u}_2} e^{j \frac{2\pi}{p} (c_{2\gamma}'' + c_{2\gamma_1}''\lambda)} \right| \\ &= \frac{1}{p^2} \left| \sum_{\lambda \in \mathbf{u}_2} \sum_{\gamma \in \mathbf{u}_2 - \{\gamma_1\}} e^{j \frac{2\pi}{p} (c_{2\gamma}'' + c_{2\gamma_1}''\lambda)} + \sum_{\gamma \in \mathbf{u}_2 - \{\gamma_1\}} \sum_{\lambda \in \mathbf{u}_2} e^{j \frac{2\pi}{p} (c_{2\gamma}'' + c_{2\gamma_1}''\lambda)} \right| \\ &= \frac{1}{p^2} \left| \sum_{\lambda \in \mathbf{u}_2} \sum_{\gamma \in \mathbf{u}_2 - \{\gamma_1\}} e^{j \frac{2\pi}{p} (c_{2\gamma}'' + 0\lambda)} + \sum_{\gamma \in \mathbf{u}_2 - \{\gamma_1\}} \sum_{\lambda \in \mathbf{u}_2} e^{j \frac{2\pi}{p} (c_{2\gamma}'' + c_{2\gamma_1}''\lambda)} \right| = \frac{1}{p} \end{aligned} \quad (42)$$

فرض کنید که $b_2'' = 0$ و $a_2'' \neq 0$ باشد، در این حالت هم مقدار $c_{1\gamma_1}''$ مهم نخواهد بود. بنابراین $c_{2\gamma}'' = a_2''$ و رابطه زیر برقرار است:

$$\begin{aligned} \frac{1}{p^2} \left| \sum_{\gamma \in \mathbf{u}_2} \sum_{\lambda \in \mathbf{u}_2} e^{j \frac{2\pi}{p} (b_{2\gamma}'')} \right| &= \frac{1}{p^2} \left| \sum_{\gamma \in \mathbf{u}_2} \sum_{\lambda \in \mathbf{u}_2} e^{j \frac{2\pi}{p} (c_{2\gamma}'' + c_{2\gamma_1}''\lambda)} \right| \\ &= \frac{1}{p^2} \left| \sum_{\gamma \in \mathbf{u}_2} \sum_{\lambda \in \mathbf{u}_2} e^{j \frac{2\pi}{p} (c_{2\gamma}'' + a_2''\lambda)} \right| = 0 \end{aligned} \quad (43)$$

بنابراین با توجه به این چند حالت می‌توان نتیجه گرفت که ضریب همدوسی ماتریس $\mathbf{S}$ برابر است با $1/p$. به عبارتی:

$$\mu(\mathbf{S}) = \max_{\mathbf{b}' \in \mathbf{B}(\mathbf{P}')} \frac{1}{p^2} \left| \sum_{\gamma \in \mathbf{u}_2} \sum_{\lambda=1}^p e^{j \frac{2\pi}{p} (b_{1\gamma}'')} \right| = \frac{1}{p} \quad (44)$$

واضح است که این ماتریس طبق کران ولش به‌طور مجانبی بهینه است.

۳- نتایج شبیه‌سازی

در این بخش با استفاده از الگوریتم بازسازی OMP^{11} که یک تکنیک بازسازی مبتنی بر همدوسی است، عملکرد ماتریس‌های پیشنهادی، با ماتریس‌های حسگری یقینی بر اساس کد BCH [۱۳] و ماتریس‌های تصادفی مقایسه می‌شوند.

مقایسه این دسته از ماتریس‌ها در حالت‌های زیر صورت می‌پذیرد:

- ۱- در حالت اول با افزایش درجه تنکی سیگنال، درصد بازسازی سیگنال، شبیه‌سازی می‌شود. افزایش درجه تنکی سیگنال تا جایی ادامه می‌یابد که درصد بازسازی سیگنال صفر شود. در این حالت فرض می‌شود که بردار اندازه‌گیری $\mathbf{y}_{m \times 1}$ بدون نویز باشد. به ازای هر درجه تنکی s ، ۱۰۰۰ سیگنال با درجه تنکی s به‌طور تصادفی تولید می‌شود و درصد بازسازی به ازای این تعداد سیگنال محاسبه می‌شود. برای مثال اگر به ازای درجه تنکی s ، الگوریتم

$$\mu(\mathbf{S}) = \max_{\mathbf{s}' \neq \mathbf{s}} \frac{|\langle \mathbf{s}', \mathbf{s} \rangle|}{\|\mathbf{s}'\|_2 \cdot \|\mathbf{s}\|_2} \quad (30)$$

به علت یک بودن ستون‌های ماتریس $\mathbf{S}$ ، رابطه بالا به‌صورت زیر بیان می‌شود:

$$\mu(\mathbf{S}) = \max_{\mathbf{s}' \neq \mathbf{s}} |\langle \mathbf{s}', \mathbf{s} \rangle| \quad (31)$$

فرض کنید ستون‌های متمایز $\mathbf{b}$ و $\mathbf{b}'$ از ماتریس $\mathbf{B}(\mathbf{P}')$ به ازای $\gamma \in \mathbf{u}_2$ و $\lambda = 1, \dots, p$ طبق نگاشت ϕ به شکل زیر هستند:

$$\begin{aligned} \mathbf{b} &= (\mathbf{b}_{\gamma})_{p \times 1}, \quad \mathbf{b}_{\gamma} = (b_{\lambda\gamma})_{p \times 1} = c_{1\gamma} \mathbf{u}_1 + c_{2\gamma} \mathbf{u}_2 \\ \mathbf{b}' &= (\mathbf{b}'_{\gamma})_{p \times 1}, \quad \mathbf{b}'_{\gamma} = (b'_{\lambda\gamma})_{p \times 1} = c'_{1\gamma} \mathbf{u}_1 + c'_{2\gamma} \mathbf{u}_2 \end{aligned} \quad (32)$$

بنابراین المان‌های دو ستون دلخواه و متمایز $\mathbf{s}'$ ، $\mathbf{s}$ به ازای $\gamma \in \mathbf{u}_2$ به‌صورت زیر هستند:

$$\mathbf{s} = \frac{1}{\sqrt{p^2}} \left(e^{j \frac{2\pi}{p} b_{1\gamma}} \dots e^{j \frac{2\pi}{p} b_{1p}} \dots e^{j \frac{2\pi}{p} b_{p\gamma}} \dots e^{j \frac{2\pi}{p} b_{pp}} \right)^T \quad (33)$$

و

$$\mathbf{s}' = \frac{1}{\sqrt{p^2}} \left(e^{j \frac{2\pi}{p} b'_{1\gamma}} \dots e^{j \frac{2\pi}{p} b'_{1p}} \dots e^{j \frac{2\pi}{p} b'_{p\gamma}} \dots e^{j \frac{2\pi}{p} b'_{pp}} \right)^T \quad (34)$$

پس همدوسی این دو ستون به‌صورت زیر قابل نگارش است:

$$|\langle \mathbf{s}', \mathbf{s} \rangle| = \frac{1}{p^2} \left| \sum_{\gamma \in \mathbf{u}_2} \sum_{\lambda=1}^p e^{j \frac{2\pi}{p} (b_{\lambda\gamma} - b'_{\lambda\gamma})} \right| \quad (35)$$

همان‌طور که گفته شد ماتریس $\mathbf{B}(\mathbf{P}')$ یک ماتریس کد است بنابراین:

$$\mathbf{b}, \mathbf{b}' \in \mathbf{B}(\mathbf{P}') \Rightarrow \mathbf{b}'' = \mathbf{b} - \mathbf{b}' \in \mathbf{B}(\mathbf{P}') \quad (36)$$

پس رابطه همدوسی به شکل زیر قابل بیان خواهد بود:

$$|\langle \mathbf{s}', \mathbf{s} \rangle| = \frac{1}{p^2} \left| \sum_{\gamma \in \mathbf{u}_2} \sum_{\lambda=1}^p e^{j \frac{2\pi}{p} (b_{\lambda\gamma})} \right| \quad (37)$$

ضریب همدوسی برابر خواهد بود با:

$$\mu(\mathbf{S}) = \max_{\mathbf{b}'' \in \mathbf{B}(\mathbf{P}')} \frac{1}{p^2} \left| \sum_{\gamma \in \mathbf{u}_2} \sum_{\lambda=1}^p e^{j \frac{2\pi}{p} (b_{\lambda\gamma})} \right| \quad (38)$$

البته باید توجه کرد که $\mathbf{b}'' \neq 0$ است و به‌صورت زیر بیان می‌شود:

$$\begin{aligned} \mathbf{b}'' &= (\mathbf{b}''_{\gamma})_{p \times 1}, \\ \mathbf{b}''_{\gamma} &= (b''_{\lambda\gamma})_{p \times 1} = c_{1\gamma}'' \mathbf{u}_1 + c_{2\gamma}'' \mathbf{u}_2 \end{aligned} \quad (39)$$

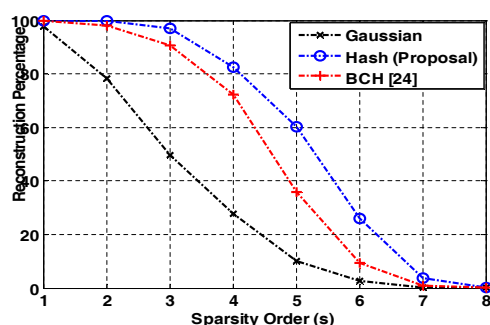
که در رابطه بالا $\lambda, \gamma \in \mathbf{u}_2$ و $c_{1\gamma}'' = a_1'' + b_1''\gamma$ ، $c_{2\gamma}'' = a_2'' + b_2''\gamma$ هستند. همچنین $a_1'', a_2'', b_1'', b_2'' \in \mathbb{F}_p$ است و بنابراین $c_{1\gamma}''$ و $c_{2\gamma}''$ به ازای تمامی $\gamma \in \mathbf{u}_2$ نمی‌توانند صفر باشند. معادلات موجود در رابطه (۳۹) که در ادامه می‌آید را در نظر بگیرید. این دو معادله در قسمت بعد به‌منظور تکمیل اثبات مورد استفاده قرار می‌گیرند.

$$\left| \sum_{c \in \mathbf{u}_2} e^{j \frac{2\pi}{p} (a+bc)} \right| = 0, \quad \left| \sum_{c \in \mathbf{u}_2} e^{j \frac{2\pi}{p} (d)} \right| = p \quad (40)$$

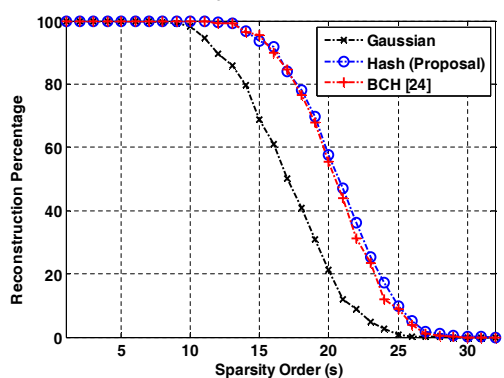
که در این رابطه $\mathbf{u}_2 = \{0, 1, \dots, p-1\}$ و $a, b, d \in \mathbf{u}_2$ مقادیر ثابتی هستند. بسته به مقادیر $c_{1\gamma}''$ و $c_{2\gamma}''$ عبارت داخلی رابطه (۳۷) چند حالت خواهد داشت:

$$c_{2\gamma}'' = 0 \quad \forall \gamma \in \mathbf{u}_2 \quad (1)$$

در این حالت باید $b_1'' \neq 0$ باشد زیرا کد تمام ۱ از ماتریس کد حذف



شکل ۱: درصد بازسازی سیگنال بر حسب درجه

تنکی در میدان $\mathbb{F}_3$ 

شکل ۲: درصد بازسازی سیگنال بر حسب درجه تنکی در میدان

متناهی $\mathbb{F}_7$

علاوه بر این شکل‌های ۱ و ۲ عملکرد بهتر ماتریس‌های یقینی طراحی شده در این مقاله نسبت به ماتریس‌های یقینی ارائه شده در [۱۳] را نشان می‌دهند. برای مثال در شکل ۱ در درجه تنکی ۵ بازسازی دقیق به ازای نمونه‌برداری با ماتریس یقینی ارائه شده در این مقاله حدود ۲۰٪ عملکرد بهتری نسبت به ماتریس یقینی بر اساس کدهای BCH [۱۳] دارد. دلیل عملکرد بهتر ماتریس‌های یقینی ارائه شده، ضریب همدوسی کمتر آن‌ها است. اما شکل ۲ نشان می‌دهد که با افزایش مقدار p ، عملکرد هر دو ماتریس یقینی به هم نزدیک می‌شود. زیرا با افزایش p ، همدوسی این دسته از ماتریس‌ها که به ترتیب عبارت‌اند از: $1/p$ و $1/(p-1)$ تقریباً به هم دیگر برابر می‌شوند.

۲-۳ - حالت دوم

در این حالت سیگنال‌های با درجه تنکی متفاوت با استفاده از ماتریس‌های حسگری نمونه‌برداری می‌شوند. سپس نویز گوسی سفید با بردار اندازه‌گیری به گونه‌ای جمع می‌شود که نسبت سیگنال به نویز ورودی برابر با ۱۵dB باشد. میزان توان سیگنال به توان نویز خروجی در شکل‌های ۳ و ۴ رسم شده‌اند. نتایج به دست آمده نشان می‌دهد که ماتریس‌های یقینی پیشنهادی در این مقاله به علت داشتن ضریب همدوسی کمتر عملکرد بهتری نسبت به دسته‌ای از ماتریس‌های یقینی ارائه شده در [۱۳] دارند. همچنین باید توجه کرد که با مقایسه شکل ۳ و ۴ می‌توان دید که با افزایش p ، عملکرد هر دو ماتریس یقینی به هم نزدیک می‌شود. شکل‌های ۳ و ۴ نشان می‌دهند که هرچه درجه تنکی سیگنال x کمتر باشد SNR خروجی بیش‌تر است. به طور مثال به ازای

بازسازی فقط بتواند ۹۰۰ سیگنال را به طور دقیق بازسازی کند، آنگاه درصد بازسازی برابر با ۹۰٪ خواهد بود.

۲- در حالت دوم بردار اندازه‌گیری سیگنال s تنک با نویز گوسی سفید جمع‌شونده آلوده می‌شود. SNR ورودی به ازای تمامی درجه‌های تنکی یکسان خواهد بود. در این حالت نسبت توان سیگنال به نویز در خروجی بر حسب افزایش درجه تنکی رسم می‌شود. در این حالت هم به ازای هر درجه تنکی ۱۰۰۰ سیگنال مختلف تولید شده و نتایج روی این تعداد سیگنال متوسط‌گیری می‌شوند.

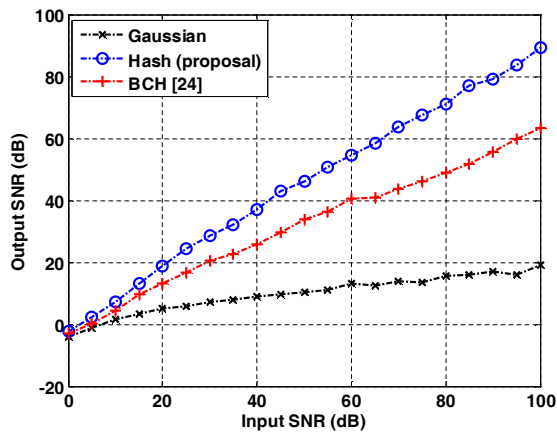
۳- در حالت سوم فرض می‌شود که درجه تنکی سیگنال ثابت است و بردار اندازه‌گیری با نویز گوسی سفید و جمع‌شونده آلوده می‌شود. در این حالت SNR در خروجی بر حسب SNR در ورودی ترسیم می‌شود. مشابه دو حالت قبل به ازای هر مقدار نسبت توان سیگنال به نویز در ورودی، میانگین‌گیری بر روی ۱۰۰۰ سیگنال مختلف انجام می‌شود.

در هر سه حالت ماتریس‌های حسگری یقینی بر روی میدان‌های متناهی $\mathbb{F}_3$ و $\mathbb{F}_7$ تولید شده‌اند. ماتریس‌های طراحی شده بر اساس توابع هش دارای ابعاد 9×27 و 49×343 و ضرایب همدوسی $1/3$ و $1/7$ هستند. همچنین ماتریس‌های یقینی بر اساس کد BCH دارای ابعاد 8×27 و 48×343 و ضرایب همدوسی $1/2$ و $1/6$ هستند. ماتریس‌های حسگری تصادفی هم دارای ابعاد مشابه با ماتریس‌های هش هستند و المان‌های آن‌ها دارای توزیع گوسی مستقل و یکسان هستند و ستون‌های آن یک‌سازی شده‌اند.

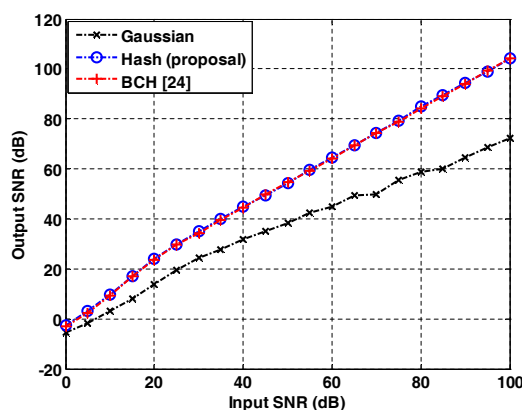
۳-۱ - حالت اول

شکل‌های ۱ و ۲ نشان‌دهنده درصد بازسازی سیگنال بر حسب درجه تنکی هستند. در این حالت فرض شده است که نویز وجود ندارد. زمانی که با استفاده از یک ماتریس حسگری یقینی نمونه‌برداری انجام شود، طبق شرط RIP بازسازی یکتای سیگنال تا درجه تنکی برابر با $1/\mu$ امکان‌پذیر است.

اما همان‌طور که در شکل ۲ مشاهده می‌شود به ازای نمونه‌برداری با ماتریس‌های یقینی، حتی به ازای درجه تنکی بیش‌تر از ۷ نیز سیگنال به طور دقیق بازسازی می‌شود. در توضیح این مسئله باید ابتدا به این موضوع اشاره کرد که ضریب همدوسی شرط RIP را به طور کامل نتیجه نمی‌دهد و ممکن است ماتریس، شرط RIP را از درجه بالاتری برقرار کند که از ضریب همدوسی نتیجه نشود. البته قابل ذکر است که حتی ممکن است ماتریسی شرط RIP را با درجه بالایی اقلان کند ولی باز هم سیگنال با درجه تنکی بالاتری را بتواند نمونه‌برداری کند که شرط RIP نتواند آن را نشان دهد.



شکل ۵: SNR_{OUT} برحسب SNR_{IN} در $\mathbb{F}_3$ ، به ازای $s=4$



شکل ۶: SNR_{OUT} برحسب SNR_{IN} در $\mathbb{F}_7$ ، به ازای $s=13$

۴- نتیجه‌گیری

در این مقاله در ابتدا با استفاده از یک ماتریس کد اولیه با فاصله همینگ زیاد و با استفاده از ویژگی توابع هش و اصول جایگذاری ستونی یک ماتریس کد جدید با فاصله همینگ زیاد تولید شد. سپس با یک‌سازی ستون‌های ماتریس کد جدید و حذف برخی از ستون آن یک ماتریس حسگری تولید شد. همچنین در این مقاله نشان داده شد که ابعاد این دسته از ماتریس‌ها $p^2 \times p^3$ است و ضریب همدوسی آن‌ها برابر با $1/p$ است.

نتایج شبیه‌سازی نشان دادند که به ازای مقادیر کم p عملکرد ماتریس‌های پیشنهادی در این مقاله نسبت به ماتریس‌های BCH به مراتب بهتر است، اما با افزایش مقدار p عملکرد این دو دسته از ماتریس‌ها یکسان می‌شود. از طرفی با افزایش مقدار p ضریب همدوسی ماتریس‌های پیشنهادی در این مقاله به کران ولش می‌رسد، بنابراین این ماتریس‌ها به‌طور مجانبی بهینه هستند.

مراجع

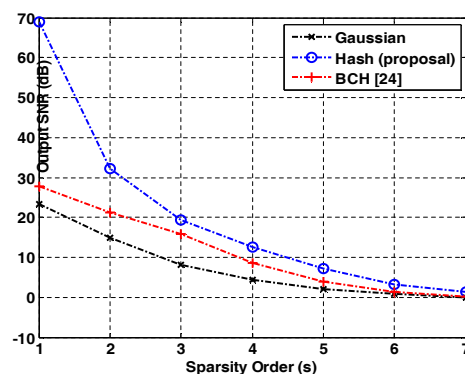
- [1] E. Candes, J. Romberg, and T. Tao, "Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 489-509, 2006.

درجه تنکی ۱، کافی است به هنگام بازسازی سیگنال اصلی، مؤلفه غالب تخمین زده شود و بنابراین بدیهی است که هرچه درجه تنکی کمتر باشد تخمین دقیق‌تری از سیگنال اصلی زده خواهد شد. البته باید متذکر شد که به ازای درجه تنکی ۱ این میزان درصد بازسازی غیرطبیعی است و احتمالاً به علت حضور داده‌های پرت این اتفاق می‌افتد و از آنجایی که نمودارهای به‌دست‌آمده به ازای درجه‌های تنکی بیشتر به هم نزدیک می‌شوند (همان‌گونه که توقع داشته‌ایم) روند شبیه‌سازی صحیح به‌نظر می‌رسد.

۳-۳- حالت سوم

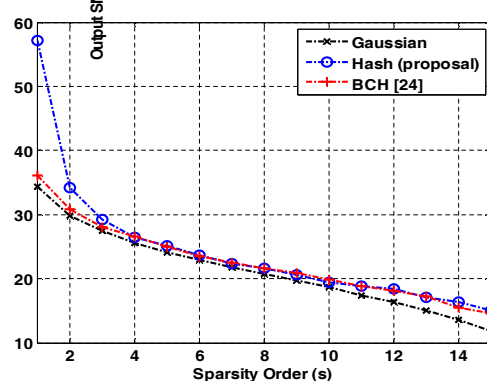
در این حالت درجه تنکی سیگنال ثابت می‌ماند و فقط به بردارهای اندازه‌گیری نویز اضافه می‌شود. شکل‌های ۵ و ۶ نشان‌دهنده میزان توان سیگنال به نویز در خروجی برحسب سطوح مختلف توان نویز در ورودی است. این دو شکل به ترتیب به ازای میدان‌های متناهی $\mathbb{F}_3$ و $\mathbb{F}_7$ بررسی شده‌اند. به‌منظور شبیه‌سازی این حالت، درجه تنکی سیگنال از درجه تنکی که شرط ضریب همدوسی تعیین می‌کند بیشتر در نظر گرفته می‌شود.

نمودارها نشان می‌دهند که به ازای نمونه‌برداری توسط هرکدام از ماتریس‌های یقینی یا تصادفی، توان سیگنال به نویز در خروجی تابعی از توان سیگنال به نویز در ورودی است. نتایج شبیه‌سازی در این حالت هم نتایج شبیه‌سازی در حالت‌های قبل را تأیید می‌کند.



شکل ۳: میزان SNR_{OUT} برحسب درجه تنکی سیگنال در $\mathbb{F}_3$

$SNR_{IN}=15\text{ dB}$



شکل ۴: میزان SNR_{OUT} برحسب درجه تنکی سیگنال در $\mathbb{F}_7$

$SNR_{IN}=15\text{ dB}$

- [10] R. De Vore, "Deterministic constructions of compressed sensing matrices," *J. Complexity*, vol. 23, no. 46, pp. 918-925, 2007.
- [11] S. Li, F. Gao, G. Ge, and S. Zhang, "Deterministic construction of compressed sensing matrices via algebraic curves," *IEEE Trans. Inf. Theory*, vol. 58, no. 8, pp. 5035-5041, 2012.
- [12] A. Amini, and F. Marvasti, "Deterministic construction of binary, bipolar and ternary compressed sensing matrices," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2360-2370, 2011.
- [13] A. Amini, V. Montazerhodjat, and F. Marvasti, "Matrices with small coherence using p-ary block codes," *IEEE Transaction on Signal Process.*, vol. 60, no. 1, pp. 172-181, 2012.
- [14] P. Indyk, "Explicit constructions for compressed sensing of sparse signals," *Proceedings of the 19th annual ACM-SIAM Symposium on Discrete Algorithms*, pp. 30-33, 2008.
- [15] S. D. Howard, A. R. Calderbank, and S. J. Searle, "A fast reconstruction algorithm for deterministic compressive sensing using second order Reed-Muller codes," *42nd Annual Conference on Information Sciences and Systems, CISS*, pp. 11-15, 2008.
- [16] C. J. Colbourn, D. Horsley, and C. McLean, "Compressive sensing matrices and hash families," *IEEE Transaction on Communications*, vol. 59, pp. 1840-1845, 2011.
- [2] B. K. Natarajan, "Sparse approximate solutions to linear systems," *SIAM Journal on Computing*, vol. 24, pp. 227-234, 1995.
- [3] S. S. Chen, D. L. Donoho, and M. A. Saunders, "Atomic decomposition by basis pursuit," *SIAM Journal on Scientific Computing*, vol. 20, pp. 33-61, 1998.
- [4] D. L. Donoho, and X. Huo, "Uncertainty principles and ideal atomic decomposition," *IEEE Trans. Inf. Theory*, vol. 47, pp. 2845-2862, 2001.
- [5] E. Candes, and T. Tao, "Decoding by linear programming," *IEEE Trans. Inf. Theory*, vol. 51, no. 12, pp. 4203-4215, 2005.
- [6] R. Baraniuk, M. Davenport, R. De Vore, and M. Wakin, "A simple proof of the restricted isometry property for random matrices," *Constructive Approximation*, vol. 28, pp. 253-263, 2008.
- [7] J. Bourgain, S. Dilworth, K. Ford, S. Konyagin, and D. Kutzarova, "Explicit constructions of RIP matrices and related problems," *Duke Mathematical Journal*, vol. 15, pp. 145-185, 2011.
- [8] L. Welch, "Lower bounds on the maximum cross correlation of signals," *IEEE Trans. Inf. Theory*, vol. 20, pp. 397-399, 1974.
- [9] E. J. Candes, and T. Tao, "Near-optimal signal recovery from random projections: Universal encoding strategies," *IEEE Trans. Inf. Theory*, vol. 52, pp. 5406-5425, 2006.

زیرنویس‌ها

-
- ¹ Sparse
 - ² Measurement vector
 - ³ Non polynomial complete
 - ⁴ Restricted isometry property
 - ⁵ Restricted isometry constant
 - ⁶ Random matrix
 - ⁷ Deterministic matrix
 - ⁸ Welch bound
 - ⁹ Null space property
 - ¹⁰ Pattern matrix
 - ¹¹ Orthogonal matching pursuit