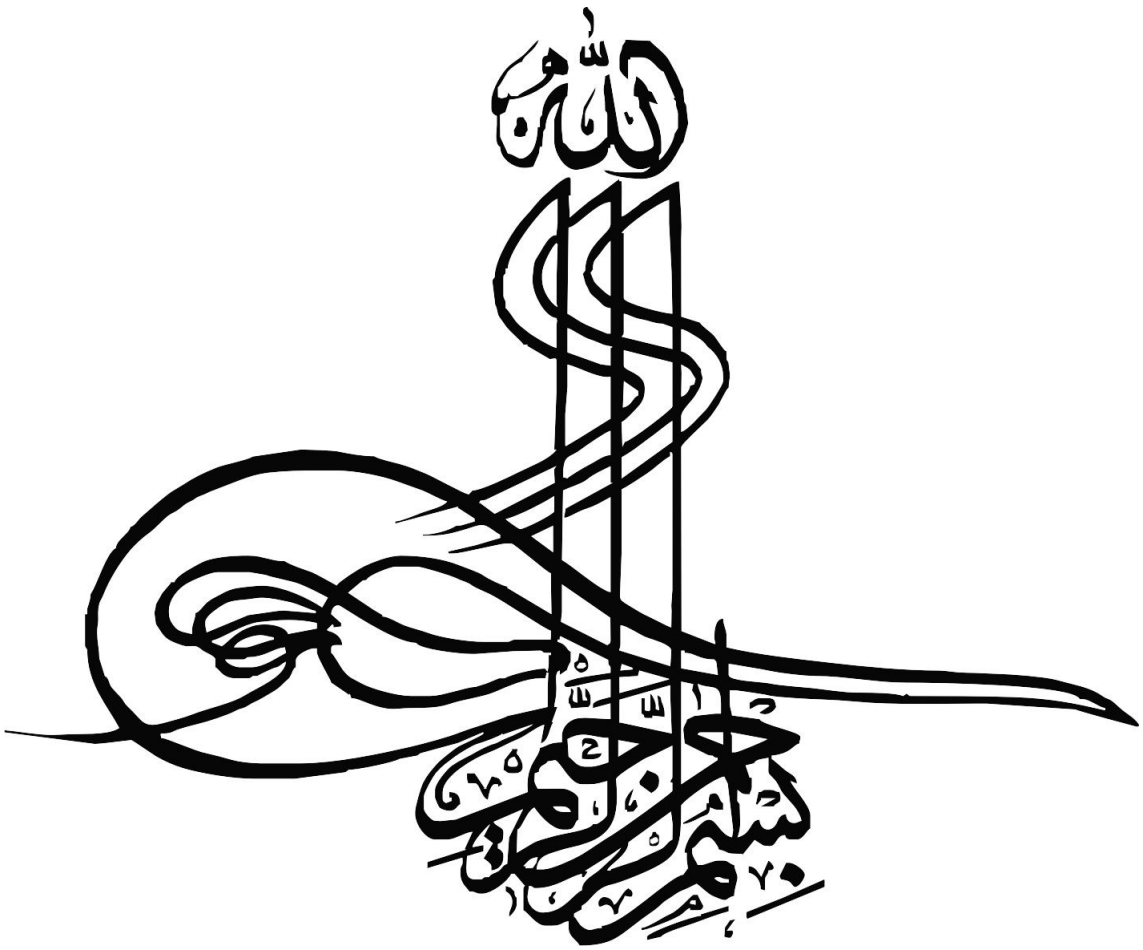
بسم الله الرحمن الرحيم

باسمه تعالی

مدیریت تحصیلات تکمیلی

تعهدنامه اصالت اثر

اینجانب **صغری محمدی** متعهد می‌شوم که مطالب مندرج در این پایان نامه/ رساله حاصل کار پژوهشی اینجانب است و دستاوردهای پژوهشی دیگران که در این پژوهش از آن‌ها استفاده شده است، مطابق مقررات ارجاع و در فهرست منابع و مآخذ ذکر گردیده است. این پایان نامه/ رساله قبلا برای احراز هیچ مدرک هم‌سطح یا بالاتر ارائه نشده است. در صورت اثبات تخلف (در هر زمان) مدرک تحصیلی صادر شده توسط دانشگاه از اعتبار ساقط خواهد شد.

صغری محمدی

امضا

تهران- لویزان- کد پستی ۱۶۷۸۸- صندوق پستی ۱۶۳- ۱۶۷۸۵- تلفن ۹- ۲۲۹۷۰۰۶۰ (داخلی ۲۳۷۴)- نمابر ۲۲۹۷۰۰۱۱- پست الکترونیکی: **sru@sru.ac.ir**

دانشکده علوم پایه

کدهای ضد جعل W–امن

نگارش

صغری محمدی

استاد راهنما : دکتر حمیدرضا میمنی

استاد مشاور : دکتر علی زعیم‌باشی

پایان‌نامه برای دریافت درجه کارشناسی ارشد

در رشته ریاضی محض

مهر ۱۳۹۱

بسمه تعالی

شماره: ۱۰۴۹۲/۱۴
تاریخ: ۹۱/۱۱/۲۹
پیوست: ----------

دانشگاه تربیت دبیر شهید رجایی

صورتجلسهٔ دفاع پایان‌نامه تحصیلی دوره کارشناسی ارشد

با تأییدات خداوند متعال و با استعانت از حضرت ولی عصر (عج) جلسه دفاع از پایان‌نامه کارشناسی‌ارشد خانم صغری محمدی رشتهٔ ریاضی‌محض تحت عنوان گدهای ضد جعل W – امن،که در تاریخ: ۹۱/۷/۹ با حضور هیأت محترم داوران در دانشگاه تربیت دبیر شهید رجائی برگزار گردید و نتیجه به شرح زیر می باشد.

☐ قبول (بادرجه ..بسیار خوب.. امتیاز ..۱۸/۴..) ☐ دفاع مجدد ☐مردود

۱ ـعالی (۲۰ – ۱۹)

۲ ـ بسیار خوب (۱۸/۹۹ – ۱۸)

۳ ـ خوب (۱۷/۹۹ – ۱۶)

۴ ـ قابل قبول (۱۵/۹۹ – ۱۴)

۵- غیرقابل قبول (کمتر از ۱۴)

اعضاء	نام و نام خانوادگی	مرتبه علمی	امضاء
استاد راهنما	دکتر حمیدرضا میمنی	استاد	
استاد مشاور	دکتر علی زعیم باشی	استادیار	
استاد داور داخلی	دکتر مجتبی قربانی	استادیار	
استاد داور خارجی	دکتر حسین حاجی‌ابوالحسن	استاد	
نماینده تحصیلات تکمیلی	دکتر فرزانه نوروزی‌لرکی	استادیار	

دکتر ایوب اسماعیل پور
رئیس دانشکده علوم پایه

تهران، لویزان، کد پستی:۱۵۸۱۱-۱۶۷۸۸
صندوق پستی: ۱۶۳-۱۶۷۸۵
تلفن: ۹-۲۲۹۷۰۰۶۰ فکس: ۲۲۹۷۰۰۳۳
Email:sru@sru.ac.ir
www.srttu.edu

ما دیده به راه قدمت دوخته‌ایم در قلب حزین مهر تو اندوخته‌ایم

تقدیم به

دوای درد دلهای بی‌تاب و چشم های عاشق و منتظر "مهدی فاطمه «عج»"

تقدیم و تشکر

درود و سپاس فراوان خدای را که بر این بنده خود منت نهاد و توفیقی عنایت فرمودند که در سایه ولایت مولایمان حضرت صاحب‌الزمان و نایب برحقش آیت الله العظمی، امام خامنه‌ای و به برکت خون شهیدانمان، توانستم مرحله دیگری از تحصیلاتم را با موفقیت به پایان برسانم.

با یاد خانواده عزیزم مخصوصاً پدر و مادر گرامی‌ام و همچنین پدر و مادر همسرم که شوق پیمودن این راه را در من زنده کردند و همواره مشوق من بوده و در همه حال مایه دلگرمی‌ام در طول تحصیلاتم بودند.

از همه افرادی که در دوران تحصیلم به هر نحوی در رسیدن من تا به این پایه نقش داشته‌اند، مخصوصاً خانم آسیه رفیعی‌پور و خانم پریسا فیروزی تشکر و قدردانی می‌کنم.

از زحمات بی‌وقفه و مستمر جناب آقای دکتر حمیدرضا میمنی که راهنمایی این پایان‌نامه را به عهده داشتند و همواره با رهنمودهای خود مرا در انجام این تحقیق یاری نمودند، صمیمانه تشکر و قدردانی می‌کنم. همچنین از زحمات و راهنمایی‌های جناب آقای دکتر علی زعیم‌باشی کمال تشکر را دارم.

از همسر خود که در زمان تحصیل با از خودگذشتگی، زمینه مطالعه و تحقیق را برایم فراهم نمودند کمال تشکر و قدردانی را به عمل می‌آورم. همچنین از فرزندانم که یار و یاور من در تعالی مراحل زندگی و نیز انجام این تحقیق بودند، تشکر می‌کنم و شکیبایی آنان را می‌ستایم.

مابدان مقصد عالی توانیم رسید هم مگر پیش نهد لطف شما گامی چند

صغریٰ محمدی

مهر ۱۳۹۱

چکیده

کدهای ضدجعل امن برای محافظت در مقابل توزیع غیر مجاز اسناد دیجیتالی استفاده می‌شود. این کدها در اسناد جاسازی می‌شوند، تا کپی‌های مختلف، شناسایی شوند. یک گروه از تبانی‌کننده‌ها با در اختیار داشتن کپی‌هایی با کدکلمه‌های مختلف، ممکن است قادر باشند کالاهایی با کلمه جعلی تولید کنند که قادر به ردیابی نباشند. در این پایان‌نامه کدهای c-امن با ε خطا را بررسی می‌کنیم که اجازه می‌دهد یکی از c-تبانی‌کننده‌ها را با احتمال خطای ε ردیابی کند. این کدها را با استفاده از یک کد داخلی و یک ساختار خارجی می‌سازیم. خصوصیات مهم کد داخلی که به کار می‌بریم این است که هرگز کاربر بی‌گناه، متهم نمی‌شود و کد داخلی مذکور برای هر تعداد از کدکلمه‌ها، قابل ساختن است. همچنین نشان خواهیم داد که برای ساختار خارجی می‌توان از یک کد ردیابی یا خانواده‌ای از توابع چکیده‌ساز استفاده کرد.

واژگان کلیدی: کدهای ضدجعل، کدهای امن، کدهای ضدجعل امن و کدهای ردیابی

فهرست مطالب

فهرست علائم و اختصارات

بیشترین فاصله کدی ..... $d_{\max}$

خانواده چکیده‌ساز ..... HF

خانواده چکیده‌ساز تام ..... PHF

خانواده چکیده‌ساز جداکننده ..... SHF

خانواده آزاد از فشردگی ..... SFF

سیستم جداکننده ..... SS

فاصله کدی کد C ..... $d(C)$

کد تصحیح‌کننده خطا ..... ECC

کد ردیابی ..... TA

کد ضد جعل ..... FPC

کد ضد جعل امن ..... SFPC

کمترین فاصله دو کد کلمه در کد C ..... $d_{\min}$

مجموعه جایگاه‌های غیر قابل کشف کد C ..... $U(C)$

مجموعه جایگاه‌های قابل کشف کد C ..... $D(C)$

مجموعه ممکن کد C ..... $F(C)$

مجموعه نسل کد C ..... $\mathrm{Desc}(C)$

ماتریس ویژه ..... SM

وزن همینگ C ..... $W(C)$

فصل ۱

تعاریف و قضایای مقدماتی

مقدمه

در این فصل به طور خلاصه تعاریف و قضایایی را که در فصل‌های بعدی مورد استفاده قرار می‌گیرد، بیان می‌کنیم. مطالب این فصل بر اساس مراجع [۱، ۲، ۳، ۴، ۵، ۶، ۷] می‌باشد.

۱.۱ کد

تعریف ۱.۱.۱. فرض کنید $A = \{a_1, a_2, \ldots, a_q\}$ یک مجموعه از اندازه q باشد که به آن الفبای کدی می‌گویند و عناصر آن را نمادهای کدی می‌نامند.

الف- یک کلمه q-آرایه به طول n روی A، دنباله $w = w_1 w_2 \ldots w_n$ است که برای هر $1 \leq i \leq n$، $w_i \in A$ است. در واقع w یک دنباله n تایی $(w_1 w_2 \ldots w_n)$ است.

ب- یک کد بلوکی (کد) q-آرایه به طول n روی A، یک مجموعه ناتهی C از کلمه‌های q-آرایه به طول n است.

$$\varnothing \neq C \subseteq A^n = \underbrace{A \times A \times \ldots \times A}_{n \text{ بار}}$$

ج- به اعضای کد C، کدکلمه می‌گویند.

د- تعداد کدکلمه‌ها در C را با $|C|$ نمایش داده و آن را اندازه C می‌نامند.

ه- یک کد به طول n و اندازه M را یک (n, M)-کد می‌نامند.

و- یک (n, M)-کد q-آرایه را می‌توان به صورت ماتریس $M \times n$، با q نماد، نمایش داد به گونه‌ای که هر سطر ماتریس متناظر یک کدکلمه باشد.

تذکر ۲.۱.۱. توجه کنید که هر کدکلمه، یک کلمه محسوب می‌شود ولی عکس آن لزوماً برقرار نیست.

تذکر ۳.۱.۱. گاهی اوقات، کدکلمه را یک کلمه ثبت‌شده و کلمه را کلمه ثبت‌نشده نیز می‌گویند. همچنین در کاربرد کدها، هر عضو A^n را کاربر، اعضای $C \subseteq A^n$ را کاربر ثبت‌شده و اعضای $A^n \setminus C$ را کاربر ثبت‌نشده می‌نامند.

تعریف ۴.۱.۱. یک کد روی الفبای کدی $F_2 = \{0, 1\}$، یک کد دودویی نامیده می‌شود.

تعریف ۵.۱.۱. برای دو حرف از حروف الفبای $A = \{a_1, \ldots, a_q\}$ فاصله همینگ به صورت زیر تعریف می‌شود:

$$d(a_i, a_j) = \begin{cases} 1 & \text{اگر } i \neq j \\ 0 & \text{اگر } i = j \end{cases}$$

و از آنجا فاصله دو کلمه $X = x_1 x_2 \ldots x_n$ و $Y = y_1 y_2 \ldots y_n$ به صورت زیر بیان می‌شود:

$$d(X, Y) = \sum_{i=1}^{n} d(x_i, y_i) = |\{i \mid x_i \neq y_i\}|$$

به وضوح

$$۱) \quad d(X,Y) \geq ۰$$

$$۲) \quad d(X,Y) = ۰ \Leftrightarrow X = Y$$

$$۳) \quad d(X,Y) = d(Y,X)$$

$$۴) \quad d(X,Y) \leq d(X,Z) + d(Z,Y)$$

پس d تعریف شده در بالا یک متر و فضای حاصل، فضای متریک است.

تعریف ۶.۱.۱. فرض کنید C یک (n,M)-کد q-آرایه باشد. فاصله (فاصله کدی) C به صورت کوچکترین فاصله همینگ بین کدکلمه‌ها تعریف می‌شود. به عبارت دیگر:

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

تذکر ۷.۱.۱. در برخی موارد، تعریف بالا را به عنوان $d_{\min}$ بیان کرده و $d_{\max}$ را به صورت زیر تعریف می‌کنند:

$$d_{\max} = \max\{d(X,Y) : X,Y \in C, X \neq Y\}$$

تعریف ۸.۱.۱. یک کد به طول n، اندازه M و فاصله d را با (n,M,d)-کد نمایش داده و اعداد n، M و d را پارامترهای کد می‌نامیم.

تعریف ۹.۱.۱. فرض کنید A یک میدان باشد اگر کد C یک زیرفضای برداری A^n باشد، آن‌گاه کد C، یک کد خطی نامیده می‌شود.

تذکر ۱۰.۱.۱. اگر کد C یک کد خطی باشد، آن‌گاه می‌توانیم بعد آن را به عنوان بعد یک فضای برداری روی میدان A، محاسبه کنیم. دقت کنید که اگر A یک میدان متناهی با q عنصر باشد، آن‌گاه برای یک کد خطی C با پارامترهای (n,M,d) خواهیم داشت $k = Log_q M$ که در آن k، بعد کد خطی C است.

برای یک کد خطی با پارامترهای (n, M, d) و با بعد k ما نماد $[n, k, d]$ را به کار می‌بریم.

مثال ۱.۱.۱۱. فرض کنید $C = \{۰۰۰۰, ۱۰۱۰, ۰۱۰۱, ۱۱۱\}$ در این صورت، $C \subseteq \{۰, ۱\}^۴$ و $|C| = ۴$ و نیز، $k = Log_۲۴ = ۲$ و همچنین فاصله کدی برابر $d = ۲$ می‌باشد. بنابراین C یک کد با پارامترهای $[۴, ۲, ۲]$ است.

$$\begin{pmatrix} ۰ & ۰ & ۰ & ۰ \\ ۱ & ۰ & ۱ & ۰ \\ ۰ & ۱ & ۰ & ۱ \\ ۱ & ۱ & ۱ & ۱ \end{pmatrix}$$

ماتریسی است که متناظر با کد C است.

تعریف ۱.۱.۱۲. یک مجموعه C از N کلمه به طول L روی الفبایی از q حرف، را که فاصله همینگ هر جفت از کلمه‌های آن، حداقل D باشد یک $(L, N, D)_q$-کد تصحیح‌کننده خطا می‌گویند، این کد را به اختصار با $(L, N, D)_q - ECC$ نشان می‌دهند.

تعریف ۱.۱.۱۳. زیرمجموعه $S \subseteq F_q^n$ را دوری گوییم اگر $(a_۱, a_۲, \ldots, a_n) \in S$، آن‌گاه $(a_n, a_۱, \ldots, a_{n-۱}) \in S$.

تذکر ۱.۱.۱۴. کدخطی C را دوری گوییم هرگاه یک مجموعه دوری باشد.

تعریف ۱.۱.۱۵. یک خانواده از کدهای دوری به نام رید-سالامون وجود دارد که دارای پارامترهای زیر است:

$[q + ۱, \lambda + ۱, d]$ که $\lambda \geq ۱$ و q توانی از عدد اول که $q \geq \lambda$، این کد q-آرایه از اندازه $q^{\lambda+۱}$ و طول $q + ۱$ است.

تعریف ۱.۱.۱۶. فرض کنید $\Gamma = \{w^{(1)}, w^{(2)}, \ldots, w^{(p)}\}$ یک (ℓ, p)-کد و $\mathcal{C}$ یک (L, N)-کد p-آرایه باشد. ترکیب Γ و $\mathcal{C}$ را با Γ' نشان داده و آن را به صورت زیر تعریف می‌کنیم:

برای هر کدکلمه $v = v_1 v_2 \ldots v_L \in \mathcal{C}$، قرار دهید:

$$W_v = w^{(v_1)} || w^{(v_2)} || \ldots || w^{(v_L)}$$

که $||$ به معنی الحاق رشته‌هاست. که Γ' مجموعه همه کلمه‌های W_v است که یک $(\ell L, N)$-کد می‌باشد. کد Γ' را کد الحاقی Γ و $\mathcal{C}$ می‌نامند. معمولاً کد $\mathcal{C}$ را کد خارجی و کد Γ را کد داخلی می‌نامند.

تعریف ۱.۱.۱۷. فرض کنید x کلمه‌ای در F_q^n است. وزن همینگ x را به صورت زیر تعریف می‌کنیم که تعداد جایگاه‌های غیر صفر در x است.

$$W(x) = d(x, 0) = \min |\{i \mid x_i \neq 0\}|$$

تعریف ۱.۱.۱۸. فرض کنید C یک کد خطی روی F_q باشد، وزن همینگ C را به صورت زیر تعریف می‌کنیم:

$$W(C) = \min\{W(x) \mid x \in C, x \neq 0\}$$

۲.۱ توابع چکیده‌ساز

در این بخش، مفاهیم خانواده چکیده‌ساز را بیان می‌کنیم. این خانواده از توابع نقش اساسی را در ساخت کدهای ضدجعل امن بازی می‌کنند که در ادامه به آن اشاره شده است.

تعریف ۱.۲.۱. فرض کنید $n \geq m$ باشد. یک (n, m)-تابع چکیده‌ساز، یک تابع $h : A \to B$ است که $|A| = n$ و $|B| = m$. یک (n, m)-خانواده چکیده‌ساز، یک مجموعه متناهی H از (n, m)-توابع

چکیده‌ساز می‌باشد به‌طوری‌که برای هر $h \in H$، h تابعی از مجموعه n عضوی A به مجموعه m عضوی B است. یک (n,m)-خانواده چکیده‌ساز با $|H| = N$ را با $HF(N;n,m)$ نشان می‌دهند.

تذکر ۲.۲.۱. می‌توان یک $HF(N;n,m)$، را با یک ماتریس $N \times n$ با m نماد نمایش داد به‌گونه‌ای که هر سطر ماتریس، متناظر یک تابع در H باشد.

اکنون متناظر با کد C یک خانواده چکیده‌ساز که با $H(C)$ نمایش داده می‌شود به صورت زیر می‌سازیم:

فرض کنید C یک (N,n)-کد q-آرایه باشد. ماتریس نمایش آن را با M نمایش دهید، که ماتریسی $n \times N$ با q نماد می‌باشد. $H(C)$ را یک $HF(N;n,m)$ تعریف کنید، به‌گونه‌ای که ماتریس نمایش آن M^T باشد. بنابراین اگر $C = \{x^1, x^2, \ldots, x^n\}$ باشد و $1 \le j \le N$، آن‌گاه تابع $h_j \in H(C)$ به صورت زیر تعریف می‌شود:

$$h_j(i) = x_j^i \quad 1 \le i \le n$$

فرم کلی ماتریس معرفی شده در بالا به صورت زیر می‌باشد:

$$M = \begin{array}{c} \\ x^1 \\ \vdots \\ x^i \\ \vdots \\ x^n \end{array} \begin{array}{c} \begin{array}{ccccc} h_1 & \ldots & h_j & \ldots & h_N \end{array} \\ \begin{bmatrix} x_1^1 & \ldots & x_j^1 & \ldots & x_N^1 \\ \vdots & & & & \vdots \\ x_1^i & \ldots & x_j^i & \ldots & x_N^i \\ \vdots & & & & \vdots \\ x_1^n & \ldots & x_j^n & \ldots & x_N^n \end{bmatrix} \end{array}$$

و ماتریس نمایش $H(C)$ برابر با M^T است.

تعریف ۳.۲.۱. فرض کنید n و m و w اعداد صحیحی باشند که $n \geq m \geq w \geq ۲$. یک (n,m,w)-خانواده چکیده‌ساز تام، یک (n,m)-خانواده چکیده‌ساز H است به‌طوری‌که برای هر $X \subseteq A$ با $|X| = w$، حداقل یک تابع $h \in H$ وجود داشته باشد که $h|_X$ یک‌به‌یک باشد. یک (n,m,w)-خانواده چکیده‌ساز تام با $|H| = N$ را با $\mathrm{PHF}(N;n,m,w)$ نشان می دهیم.

خانواده چکیده‌ساز تام ابتدا توسط مهلهورن[۱] در [۵] معرفی شد و از مدت‌ها پیش موضوع تحقیقات گسترده‌ای قرار گرفتند.

انگیزه نامگذاری چنین مجموعه‌هایی به عنوان خانواده چکیده‌ساز تام این است که ما یک خانواده از توابع چکیده‌ساز داریم با این ویژگی که اگر حداکثر w تا از عضوها در هم ریخته شوند، آن‌گاه حداقل یک تابعی در این خانواده یافت می‌شود که اگر روی w تا عضو در هم ریخته شده بکار بسته شود، هیچ تصادمی رخ نمی‌دهد.

یک (n,m,w)-خانواده چکیده‌ساز تام با $|H| = N$، در فرم ماتریسی، یک ماتریس $N \times n$ با درایه‌های ورودی $۱, ۲, \ldots, m$ است، با این خاصیت که در هر w ستون، حداقل یک سطر وجود دارد که w درایه مربوط به ستون‌های مذکور آن متفاوت هستند.

مثال ۴.۲.۱. در زیر یک $\mathrm{PHF}(۲;۵,۴,۳)$ آمده است.

$$\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۳ \\ ۱ & ۱ & ۲ & ۱ & ۳ \end{pmatrix}$$

[۱] Mehlhorn

اکنون اگر هر سه ستونی را انتخاب کنیم سطری وجود دارد به‌طوری‌که درایه‌های ستون‌های متناظر آن سطر، متمایز از هم‌اند. برای مثال اگر ستون‌های اول و سوّم و چهارم را در نظر بگیرید سطر اول وجود دارد که درایه‌های متناظر ستون‌های مربوطه، متمایز از هم‌اند.

قضیه ۵.۲.۱. [۴] و [۶]. برای هر عدد صحیح $k \geq ۰$ یک $\mathrm{PHF}(v^{k+۱}; v^{۲^k}, ۴, ۴)$ وجود دارد.

ساختار بازگشتی زیر در بدست آوردن ساختار صریح برای کلاس نامتناهی از خانواده چکیده‌ساز تام مفید است.

لم ۶.۲.۱. [۶]. فرض کنید یک $\mathrm{PHF}(N_۰; n_۰, m, w)$ وجود داشته باشد، به‌طوری‌که $\gcd(n_۰, \binom{w}{۲}!) = ۱$. در این صورت یک $\mathrm{PHF}\left(\left(\binom{w}{۲}+۱\right)^j N_۰; n_۰^{۲^j}, m, w\right)$ برای هر عدد صحیح $j \geq ۰$ وجود دارد.

تعریف ۷.۲.۱. فرض کنید n و m و $w_۱$ و $w_۲$ اعداد صحیح مثبتی باشند به‌طوری‌که $n \geq m$. یک $(n, m, \{w_۱, w_۲\})$-خانواده چکیده‌ساز جداکننده یک (n, m)-خانواده چکیده‌ساز H است به‌طوری‌که برای هر $X_۱, X_۲ \subseteq A$ با $|X_۱| = w_۱$ و $|X_۲| = w_۲$ و $X_۱ \cap X_۲ = \varnothing$، حداقل یک تابع $h \in H$ وجود داشته باشد به طوری که $\{h(x) : x \in X_۱\} \cap \{h(x) : x \in X_۲\} = \varnothing$. یک $(n, m, \{w_۱, w_۲\})$-خانواده چکیده‌ساز جداکننده با $|H| = N$ را با $\mathrm{SHF}(N; n, m, \{w_۱, w_۲\})$ نشان می‌دهیم.

یک $(n, m, \{w_۱, w_۲\})$-خانواده چکیده‌ساز جداکننده در فرم ماتریسی، یک ماتریس $N \times n$ با درایه‌های $۱, ۲, \ldots, m$ است، با این خاصیت که در هر انتخاب $w_۱$ و $w_۲$ ستون مجزا، حداقل یک سطر وجود داشته باشد به‌طوری‌که درایه‌های مربوط به $w_۱$ ستون آن سطر با درایه‌های مربوط به $w_۲$ ستون همان سطر، هیچ اشتراکی نداشته باشد.