دانشگاه جامع امام حسین(ع)
دانشکده و پژوهشکده فنی و مهندسی

مجله علمی- پژوهشی «علوم و فناوری‌های پدافند غیرعامل»
سال اول، شماره ۲، زمستان ۱۳۸۹: ص ۳۱-۲۵

Available online:
www.adst.ir

خواص جبری جمع مدولی به پیمانه 2^t با r عملوند

مهدی علائیان*[۱]، علیرضا رحیمی‌پور[۲]، سیدمجتبی دهنوی[۳]

۱- دانشیار، ۲- کارشناس ارشد، دانشگاه علم و صنعت ایران، دانشکده ریاضی

E-mail: alaeiyan@iust.ac.ir

(دریافت: ۸۸/۱۰/۰۷ ، پذیرش: ۸۹/۰۶/۰۷)

چکیده

یکی از پرکاربردترین عملگرها در رمزنگاری متقارن، جمع مدولی به پیمانه 2^t است. بنابراین بررسی خواص این عملگر نقش مهمی در طراحی و تحلیل رمزهای متقارن دارد. خواص جبری این عملگر در با دو عملوند مورد مطالعه قرار گرفته است. ما در این مقاله به‌منظور رسیدن به نتایج بهتر و بیشتر در این زمینه، برخی از خواص جبری را برای عملوندهایی با $r \geq 2$ تعمیم داده‌ایم. به‌عبارت دقیق‌تر درجه جبری مؤلفه‌ای توابع بولی از جمع مدولی را به‌عنوان یک تابع بولی برداری در نظر گرفته‌ایم و تعداد عبارت‌ها و متغیرها در این توابع بولی را تعیین نموده و پس از تجزیه و تحلیل نظری در حالت‌های خاص، یک الگوریتم کارا برای یافتن درجه مؤلفه‌ای توابع بولی در حالت کلی پیشنهاد کرده‌ایم. با استفاده از این الگوریتم، درجه جبری مؤلفه‌ای توابع بولی برای جمع مدولی به پیمانه 2^{32}، با سه تا هشت عملوند قابل محاسبه است.

کلیدواژه‌ها: جمع مدولی به پیمانه 2^t؛ تابع بولی؛ شکل نرمال جبری؛ درجه جبری

Algebrical Properties of Modular Addition Modulo 2^t with r Operant

M. Alaeiyan[1*], A. R. Rahimpour[2], S. M. Dehnavi[3]
Department of Mathematic, Iran University of Science and Technology
Email: alaeiyan@iust.ac.ir

Abstract

Modular addition modulo 2^t is one of the most applicable operators in symmetric cryptography. Therefore, investigating the properties of this operator has a significant role in design and analysis of symmetric ciphers. Algebraic properties of this operator have been studied for two operands in [1]. In this contribution, to obtain more accurate results in this area, we generalize some of the algebraic properties of this operator for $r \geq 2$ operands. More precisely, we consider the algebraic degree of the component Boolean functions of modular addition as a vectorial Boolean function and determine the number of terms and variables in these Boolean functions. After some theoretical analysis in special cases, we propose an efficient algorithm for finding the degree of these Boolean functions general case. Using this algorithm, the algebraic degree of the component Boolean functions for modular addition modulo 2^{32}, with three up to eight operands is calculated.

Keywords: Modular Addition Modulo 2^t; Boolean Functions

۱. مقدمه

جمع مدولی به پیمانه 2^t یکی از کاربردی‌ترین عملگرها در رمز نگاری متقارن است. در اینجا t یک عدد صحیح مثبت است که معمولاً برابر ۸، ۱۶، ۳۲ و یا ۶۴ است. برای مثال، جمع مدولی در [۲] و [۱۱] برای رمزهای جریانی، و جمع مدولی در [۳]، [۹]، [۱۰] و [۱۲] برای رمزهای قطعه‌ای استفاده شده است. در [۱] خواص جبری عملگرها برای دو عملوند مورد مطالعه قرارگرفته و ANF مؤلفه توابع بولی تعیین شده است. برای اطلاعات بیشتر به [۴]، [۵]، [۶]، [۷] و [۸] مراجعه شود. توجه شود که جمع‌آوری ANF از توابع بولی در [۱] برای حالت‌های کلی با $r \geq 2$ عملوند، کاری دشوار است اما برای کاربردهای بسیاری در طراحی و تحلیل رمزهای متقارن، شناختن درجه جبری توابع مؤلفه‌ای و تعداد عبارت‌ها و متغیرها در توابع مؤلفه‌ای بسیار مهم و مفید می‌باشد. در بخش ۲ تعاریف و قضایای مقدماتی را مطرح می‌کنیم؛ در بخش ۳ در مورد قضیه اصلی یافتن درجه جبری مؤلفه توابع بولی در حالت‌های خاص بحث خواهیم کرد و در بخش ۴، الگوریتم را ارائه می‌نماییم. در ضمن، طرح برهان قضیه‌هایی که در آنها ارجاع به مراجع داده نشده است، کار نویسندگان می‌باشد که جزء نوآوری‌های مقاله محسوب می‌گردد.

۲. تعاریف و قضایای مقدماتی

فرض کنیم Z_2 حلقه اعداد صحیح به پیمانه‌های ۲ باشد. حاصل ضرب مستقیم t نسخه از Z_2 را می‌توان به‌عنوان یک فضای برداری در نظر گرفت که بردارها به‌صورت $\bar{x}$ نشان داده می‌شوند. با استفاده از تعریف Z_2^t و Z_{2^t}، واضح است که Z_{2^t} حلقه اعداد صحیح به پیمانه 2^t است.

$$\varphi : Z_2^t \to Z_{2^t}$$

$$\bar{x} = (x_t, ..., x_1) \mapsto x = \sum_{i=1}^{t} x_i \, 2^{i-1}$$

یک رابطه ترتیبی جزئی $\leq$ روی Z_2^t به‌صورت زیر تعریف می‌شود:

$$\bar{x} \leq \bar{a} \Leftrightarrow \forall i, \quad x_i \leq a_i, \qquad 1 \leq i \leq t$$

که در نماد بالا اگر $\bar{x} = (x_t, ..., x_1)$ و $\bar{u} = (u_t, ..., u_1)$ آنگاه $\bar{x}^u$ به‌صورت زیر تعریف می‌شود:

$$\bar{x}^u = x_1^{u_1} ... x_t^{u_t}$$

هر تابع $f : Z_2^t \to Z_2$ یک تابع بولی نامیده می‌شود. فرض می‌کنیم f یک تابع بولی باشد، در این صورت f را می‌توان توسط ANF خودش به‌صورت زیر نشان داد:

$$f(\bar{x}) = \bigoplus_{u \in Z_{2^t}} h_u \bar{x}^u; \quad h_u \in Z_2 \qquad (1)$$

که در اینجا ضرایب توسط $h_u = h(\bar{u}) = \bigoplus_{\bar{x} \leq \bar{u}} f(\bar{x})$ تعیین می‌شوند. برای اطلاعات بیشتر در این زمینه به [۱]، [۴]، [۶] و [۱۲] مراجعه شود.

درجه جبری یک تابع بولی عبارت است از تعداد متغیرها در طولانی‌ترین عبارت ANF خودش، یا متناظراً بزرگ‌ترین وزن همینگ از $\bar{u}$ها، برای هر $h_u \neq 0$.

هر تابع $f : Z_2^t \to Z_2^m$ یک *تابع بولی برداری* نامیده می‌شود. به‌وضوح $f = (f_1, f_2, ..., f_m)$ که هر f_i، $1 \leq i \leq t$ تابعی بولی $f_i : Z_2^t \to Z_2$ است، یک تابع بولی برداری می‌باشد.

ثابت شده است که جمع مدولی را می‌توان به فرم بولی و به شکل زیر نشان داد:

فرض کنیم که $\bar{x} = (x_t, ..., x_1)$ و $\bar{y} = (y_t, ..., y_1)$ و $r = x + y$ به پیمانه 2^t. اگر $\bar{r} = (r_t, ..., r_1)$ آنگاه داریم:

$$\begin{aligned} r_1 &= x_1 \oplus y_1 \oplus c_1, & c_1 &= 0 \\ r_i &= x_i \oplus y_i \oplus c_i, & c_i &= x_{i-1} y_{i-1} \oplus x_{i-1} c_{i-1} \oplus y_{i-1} c_{i-1} \qquad i \geq 1. \end{aligned} \qquad (2)$$

برای اطلاعات بیشتر در این زمینه به [۵]، [۷]، [۸] و [۱۱] مراجعه شود.

قضیه ۲-۱:

فرض کنید که ANF یک تابع بولی

$$f : Z_2^t \to Z_2$$
$$\bar{x} \to f(\bar{x})$$

برابر $\bar{x}^u$ باشد که $u \in Z_{2^t}$. آنگاه ANF تابع $f(\bar{x}+\bar{y})$ به شکل:

$$f(\bar{x}+\bar{y}) = \bigoplus_{c=0}^{u} \bar{x}^{(u-c)}\bar{y}^{c} \qquad (۳)$$

است که تفاضل در Z انجام شده است.
اثبات: به [۱] مراجعه شود.

قضیه ۲-۲:
فرض کنید که $\bar{y}_1, \bar{y}_2, ...\bar{y}_r \in Z_2^t$ و f تابعی ذکر شده در قضیه ۲-۱ باشد. در این صورت AFN تابع $f(\bar{y}_1+\bar{y}_2+...\bar{y}_r)$ به‌صورت زیر است:

$$f(\bar{y}_1+\bar{y}_2+...+\bar{y}_r) = \bigoplus_{\substack{k_1,k_2...k_r\geq 0 \\ k_1+...k_r=u}} \bar{y}_1^{k_1}...\bar{y}_r^{k_r} \qquad (۴)$$

اثبات: از قضیه ۲-۱، $(r-1)$-بار استفاده می‌کنیم. قرار می‌دهیم $\bar{x}_1 \equiv \bar{y}_2+...+\bar{y}_r$ و از قضیه ۲-۱ استفاده می‌کنیم:

$$f(\bar{y}_1+\bar{y}_2+...\bar{y}_r) = f(\bar{y}_1+\bar{x}_1) = \bigoplus_{c_1=0}^{u} \bar{y}_1^{u-c_1}\bar{x}_1^{c_1}, \qquad (۵)$$

طبق فرمول $\bar{x}_1$ داریم:

$$\bar{x}_1^{c_1} = (\bar{y}_2+...+\bar{y}_r)^{c_1}; \qquad (۶)$$

و این معادل است با یک تابع f_1 با ANF، $\bar{x}^{c_1}$. حال قرار می‌دهیم: $\bar{x}_2 \equiv \bar{y}_3+...+\bar{y}_r$ و دوباره قضیه ۲-۱ را به‌کار می‌بریم.

$$\bar{x}^{c_1} = f_1(\bar{x}_1) = f(\bar{y}_2+\bar{x}_2) = \bigoplus_{c_2=0}^{c_1} \bar{y}_2^{(c_1-c_2)}\bar{x}_2^{c_2} \qquad (۷)$$

با جایگذاری رابطه (۷) در (۵) داریم:

$$f(\bar{y}_1+\bar{y}_2+...\bar{y}_r) = \bigoplus_{c_1=0}^{u} \bar{y}_1^{(u-c_1)}\bar{x}_1^{c_1} = \bigoplus_{c_1=0}^{u} \bar{y}_1^{(u-c_1)}\left(\bigoplus_{c_2=0}^{c_1} \bar{y}_2^{(c_1-c_2)}\bar{x}_2^{c_2}\right) \qquad (۸)$$

با ادامه فرایند بالا و به‌کارگیری مکرر قضیه ۲-۱ داریم:

$$f(\bar{y}_1+\bar{y}_2+...\bar{y}_r) = \bigoplus_{c_1=0}^{u} \bar{y}^{(u-c_1)}\left(\bigoplus_{c_2=0}^{c_1} \bar{y}_2^{(c_1-c_2)}\left(\bigoplus_{c_3=0}^{c_2} \bar{y}_3^{(c_2-c_3)}\left(...\left(\bigoplus_{c_r-1}^{c_r-2} \bar{y}_{r-1}^{(c_{r-2}-c_{r-1})}\bar{y}_r^{c_{r-1}}\right)\right)\right)\right). \qquad (۹)$$

رابطه (۹) با تغییر متغیرها، رابطه (۴) را نتیجه می‌دهد.
با در نظر گرفتن قضیه ۲-۲ درجه جبری مؤلفه‌های توابع بولی از جمع مدولی به پیمانه 2^t به صورت زیر تعیین می‌شود:
برای $u = 2^0, 2^1, ...2^{t-1}$ و $f(x) = \bar{x}^u$ ، با در نظر گرفتن رابطه (۴) و این واقعیت که تمام عبارت‌های سمت راست این رابطه متفاوتند، می‌توانیم درجات جبری مؤلفه توابع فوق‌الذکر را به‌دست آوریم. بنابراین اگر ما $\max \sum_{i=1}^{r} wt(k_i)$ را در تمام مجموعه‌های به شکل $\{k_1, k_2, ..., k_r\}$ بیابیم می‌توانیم درجه جبری مؤلفه‌ای این توابع بولی را به‌دست آوریم.

۳. قضیه اصلی

فرض کنیم که n، u و t سه عدد صحیح نامنفی باشند، معادله زیر را در نظر می‌گیریم:

$$X_1 + X_2 + ... + X_{2^n} = 2^u \qquad (۱۰)$$

که در آن X_i ها ($1 \leq i \leq 2^u$) اعدادی در Z_{2^t} هستند و $0 \leq u \leq t$. همان‌طور که می‌دانیم این معادله دارای $\binom{2^u+2^n-1}{2^u}$ جواب صحیح نامنفی است که برابر تعداد عبارت‌های در ANF، u-امین مؤلفه تابع است که $0 \leq u \leq t$. بنابراین، واقعیت زیر را داریم؛

واقعیت ۳-۱:
تعداد عبارت‌های در ANF از u-امین مؤلفه تابع جمع مدولی به پیمانه 2^t با $r = 2^n$ عملوند برابر است با $\binom{2^u+r-1}{2^u}$، همچنین بررسی اینکه تعداد متغیرها در ANF، u-امین مؤلفه تابع برابر است با $r(u+1)$، به‌راحتی صورت می‌گیرد. بنابراین داریم؛

واقعیت ۳-۲:
تعداد متغیرها در ANF، u-امین مؤلفه تابع، $0 \leq u \leq t$ از جمع مدولی به پیمانه 2^t با $r = 2^n$ عملوند برابر است با $r(u+1)$.

اکنون $\sum X_i$ را به $\overline{X}_i$ ها یعنی بردارهایی در $Z_۲^t$ تبدیل می‌کنیم. با در نظر گرفتن قضیه ۲-۲ و رابطه (۴) جواب‌هایی با مجموع وزن همینگ ماکزیمم را جستجو می‌کنیم که آن را جواب‌های بهینه می‌نامیم.

بنابراین نتیجه اصلی مقاله را به‌صورت زیر داریم؛

قضیه ۳-۳:

با نمادهای ذکر شده بالا برای $n < u$، مجموع وزن همینگ از جواب‌های بهینه عبارت است از:

$$\sum_{i=۱}^{۲^n} wt(X_i) = ۲^n(u-n) + ۲^{۲n-u} \qquad n \geq u-n, \qquad (۱۱)$$

$$\sum_{i=۱}^{۲^n} wt(X_i) = (۲^n - ۱)(u-n) + n + ۱ \qquad n < u-n \qquad (۱۲)$$

و اگر $n \geq u$، آنگاه مجموع وزن همینگ ماکزیمم برابر ۲^n است.

اثبات: دو حالت در نظر می‌گیریم؛

حالت اول:

اگر $n \geq u$ دو رسته را در نظر می‌گیریم.

رسته I، متناظر است با حالتی که $n \geq u-n$ و رسته II، متناظر است با حالتی که $n < u-n$. ابتدا جوابی را برای هر رسته می‌یابیم و سپس ثابت می‌کنیم که این جواب‌ها، جواب‌های بهینه هستند.

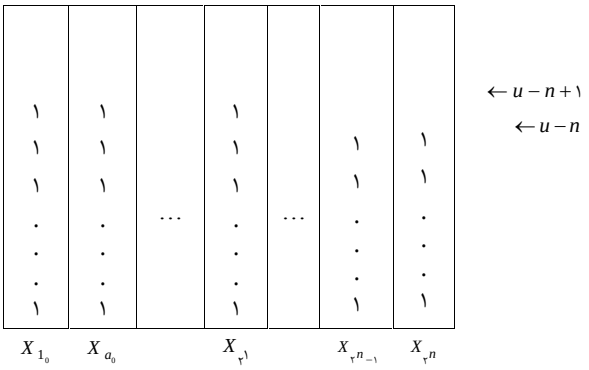
رسته I:

$$\begin{aligned} &X_۱ = \ldots = X_{۲^j} = ۳^{u-n+۱} - ۱ \qquad u = ۲n - j, \\ &X_۱ = \ldots = X_{۲^{j'}} = ۳^{u-n+۱} - ۱ \qquad ۰ \leq j \leq n-۱ \end{aligned} \qquad (۱۳)$$

رسته II:

$$\begin{aligned} &X_۱ = ۲^{u-n+۱} \\ &X_۲ = \ldots = X_{۲^n-۱} = ۲^{u-n} - ۱ \\ &X_{۲^n} = ۲^n - ۱ \end{aligned} \qquad (۱۴)$$

مجموع وزن همینگ از این جواب‌ها در روابط (۱۱) و (۱۲) هستند و به‌وضوح این جواب‌ها در معادله‌های (۱۰) صدق می‌کنند. جدول A در شکل (۱) را در نظر می‌گیریم؛ برای هر جواب این جدول ۲^n ستون دارد. ستون‌های جدول A با نمایش X_i ها در $Z_۲^t$ متناظرند. هر ستون از پائین به بالا براساس مشخصه‌های ۱ تا t مرتب شده است.



شکل ۱. جدول A

عناصر این جدول را با $A(i,j)$ نشان می‌دهیم که در آن $۱ \leq i \leq t$ و $۱ \leq j \leq ۲^n$. $A(*,j)$ و $A(i,*)$ به‌ترتیب بیانگر ستون j–ام و سطر i–ام جدول A هستند و نماد $one(A)$ را برای عدد یک '۱' جدول A به‌کار می‌بریم.

اگر $A(i,j) = '1'$ آنگاه $A(i,j)$ را $۲^{i-۱}$ و در غیر این‌صورت آن را صفر در نظر می‌گیریم و $sum(A)$ را حاصل جمع تمام درایه‌های جدول A تعریف می‌کنیم. حال دو رسته مذکور را در نظر می‌گیریم.

I) $n \geq u-n$: فرض کنیم که $i = 2n-j$، $0 \leq j \leq n$ (جدول A را ملاحظه کنید). چون برای هر سطر $۱ \leq i \leq u-n+۱$ تمام درایه‌های '۱' در جدول A حداقل مقدار ممکن را دارند بنابراین جواب ارائه شده بهینه است.

II) $n < u-n$: در این حالت جدول A به صورت شکل (۲) در می‌آید. فرض کنیم جدول A متناظر با جواب دیگری باشد که

$$\{Y_۱, Y_۲, \ldots Y_{۲^{n-۱}}, Y_{۲^n}\} \qquad (۱۵)$$

جواب این جدول ۲^n ستون دارد. ستون‌های جدول A با نمایش X_i ها در $Z_۲^t$ متناظرند. هر ستون از پائین به بالا براساس مشخصه‌های ۱ تا t مرتب شده است.

مجموع وزن همینگ از این جواب‌ها در روابط (۱۱) و (۱۲) هستند و به‌وضوح این جواب‌ها در معادله‌های (۱۰) صدق می‌کنند. جدول A در شکل (۱) را در نظر می‌گیریم؛ برای هر جواب این جدول ۲^n ستون دارد. ستون‌های جدول A با نمایش X_i ها در $Z_۲^t$ متناظرند. هر ستون از پائین به بالا براساس مشخصه‌های ۱ تا t مرتب شده است.

عناصر این جدول را با $A(i,j)$ نشان می‌دهیم که در آن $۱ \leq i \leq t$ و $۱ \leq j \leq ۲^n$. $A(*,j)$ و $A(i,*)$ به‌ترتیب بیانگر ستون j–ام و سطر i–ام جدول A هستند و نماد $one(A)$ را برای عدد یک '۱' جدول A به‌کار می‌بریم.

اگر $A(i,j) = '1'$ آنگاه $A(i,j)$ را $۲^{i-۱}$ و در غیر این‌صورت آن را صفر در نظر می‌گیریم و $sum(A)$ را حاصل جمع تمام درایه‌های جدول A تعریف می‌کنیم. حال دو رسته مذکور را در نظر می‌گیریم.

I) $n \geq u-n$: فرض کنیم که $i = 2n-j$، $0 \leq j \leq n$ (جدول A را ملاحظه کنید). چون برای هر سطر $۱ \leq i \leq u-n+۱$ تمام درایه‌های '۱' در جدول A حداقل مقدار ممکن را دارند بنابراین جواب ارائه شده بهینه است.

II) $n < u-n$: در این حالت جدول A به صورت شکل (۲) در می‌آید. فرض کنیم جدول A متناظر با جواب دیگری باشد که

$$\{Y_۱, Y_۲, \ldots Y_{۲^{n-۱}}, Y_{۲^n}\} \qquad (۱۵)$$

و $one(B) > one(A)$. جدول B_A^* را به‌صورت زیر تعریف می‌کنیم.

$$B_A^*(i,j) = \begin{cases} 0 & B(i,j) = A(i,j) = '1' \\ B(i,j) & o.w \end{cases}$$

جدول A_B^*، به همان صورت تعریف می‌کنیم. به جدول‌های A_B^* و B_A^* مراجعه کنید (شکل (۳)).

فرض کنیم که k- تا '۱' در $A_B^*(s_i+۱,t_i)$ که $۱ \le i \le k$ و m- تا '۱' در $B_B^*(l_i+۲,۲^n)$ برای $۱ \le j \le m$, $n < l_i \le u-n$. داریم:

$$sum(A_B^*) = ۲^{s_۱} + ۲^{s_۲} + \ldots + ۲^{s_k} = ۲^{l_۱} + ۲^{l_۲} + \ldots ۲^{l_m} = sum(B_A^*) \quad (۱۶)$$

چون تمام '۱' ها در B_A^* ارزش متفاوت دارند توجه شود که '۱'ها در $B_A^*(i,۲^n)$ ، $(n < i \le u-n)$ هستند پس از ساده‌سازی سمت چپ معادله (۱۶) و حذف عبارت‌های مساوی از دو طرف معادله، هیچ‌یک از ۲^{s_i} ها و ۲^{l_i} ها با هم مساوی نیستند و بنابراین دو طرف معادله (۱۶) عبارت‌های متمایز دارند. بدون از دست دادن کلیت، فرض کنیم که s_l کمترین توان است. داریم:

$$1 + 2^{s_۲ - s_۱} + \ldots + 2^{s_k - s_۱} = 2^{l_۱ - s_۱} + 2^{l_۲ - s_۱} + \ldots + 2^{l_m - s_۱},$$

که یک تناقض است. بنابراین جواب (۱۴) بهینه است.

حالت دوم:

اگر $n \ge u$ آنگاه دو جواب زیر را ارائه می‌کنیم:

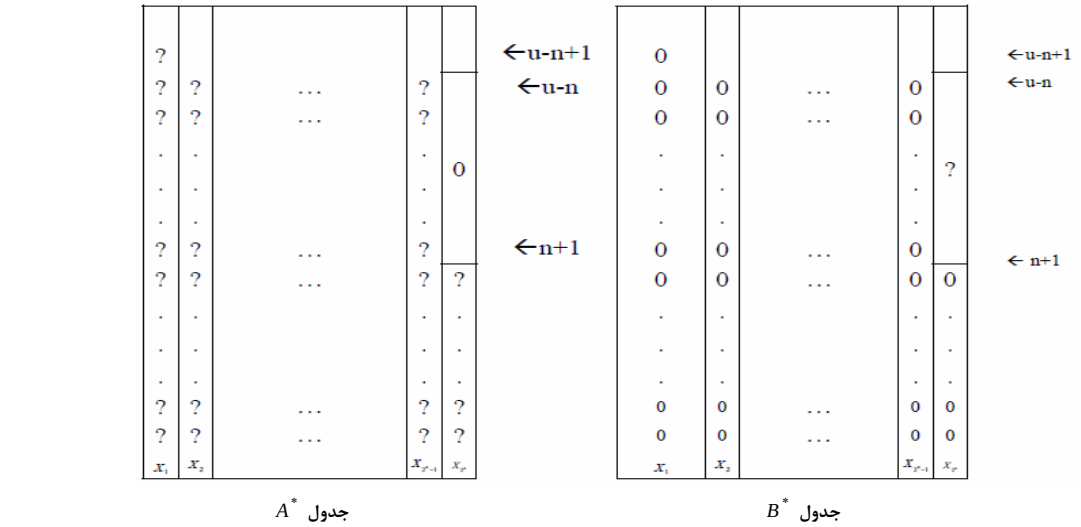
$$X_۱ = X_۲ = \ldots = X_{۲^n} = ۱$$

برای $n = u$، و برای $n > u$:

$$X_۱ = X_۲ = \ldots = X_{۲^u} = ۱ , \quad X_{۲^u+۱} = \cdots = X_{۲^n} = ۰$$

۱					
۱	۱	…	۱	۰	← $u-n+1$
۱	۱	…	۱		← $u-n$
.	.		.		
.	.		.		۰
.	.		.		
.	.		.		
۱	۱	…	۱	۱	← n
۱	۱	…	۱	۱	
.	.		.	.	
.	.		.	.	
.	.		.	.	
۱	۱	…	۱	۱	
X_1	X_2		X_{2^n-1}	X_{2^n}	

شکل ۲. جدول **A**



شکل ۳. جدول‌های A^* و B^*

چون تمام'۱' ها در جدول A در شکل (۴) حداقل مقدار ممکن را در هر حالت دارند بنابراین جواب‌های نشان داده شده بهینه هستند.

۴. الگوریتم برای یافتن جواب‌های بهینه

در این بخش، روشی برای یافتن حل کارآمد مسئله در یافتن درجه جبری مؤلفه توابع بولی در حالت کلی ارائه می‌کنیم که در ضمیمه می‌توان درجه جبری مؤلفه توابع بولی را برای جمع مدولی به پیمانه $۲^{۳۲}$ با دو تا هشت عملوند مشاهده کرد.

با در نظر گرفتن نمادها و فرض‌های بخش ۳ از $A(۱,۱)$ شروع می‌کنیم و عناصر '۱' را در جدول A در مکان‌های $A(۱,۱)$ و $A(۲,۱)$ ... $A(۱,۲)$ و $A(۲,۲)$ و... قرار می‌دهیم و این فرایند را تا وارد شدن یک '۱' اضافی در جدول A ادامه می‌دهیم که $sum(A \geq ۲^u)$ حاصل گردد. سایر عناصر را '۰' قرار می‌دهیم. اکنون از این سطر حذف می‌کنیم تا $sum(A) = ۲^u$، در غیر این صورت عناصر'۱' را از ردیف‌های پایین‌تر حذف می‌کنیم و این فرایند را به‌طور مشابه ادامه می‌دهیم.

توجه کنید که این جواب در هر سطری است به غیر از سطر آخر، حداکثر یکی از عناصر '۰' است؛ چون در غیر این صورت این دو عنصر می‌توانند با یک '۱' از سطر بالا جایگزین شوند. اکنون ادعا می‌کنیم که این جواب، جمع وزنی همینگ ماکزیمم دارد و بنابراین بهینه است. فرض کنیم جواب دیگری با جمع وزنی همینگ بزرگ‌تری موجود باشد مجدداً یک جدول B به این جواب نسبت می‌دهیم و مانند قبل جدول A_B^* و B_A^* را می‌سازیم. فرض کنیم که $m-$عنصر '۱' در $۱ \leq i \leq m$ $A_B^*(k_i+۱, s_i)$ و $n-$ عنصر '۱' در $B_A^*(l_j+۱, t_j)$ $۱ \leq j \leq n$, $n > m$ وجود داشته باشند از معادله (۱۰) داریم:

$$۲^{l_۱} + ۲^{l_۲} + ... + ۲^{l_n} = ۲^{k_۱} + ۲^{k_۲} + ... ۲^{k_m}. \quad (۱۹)$$

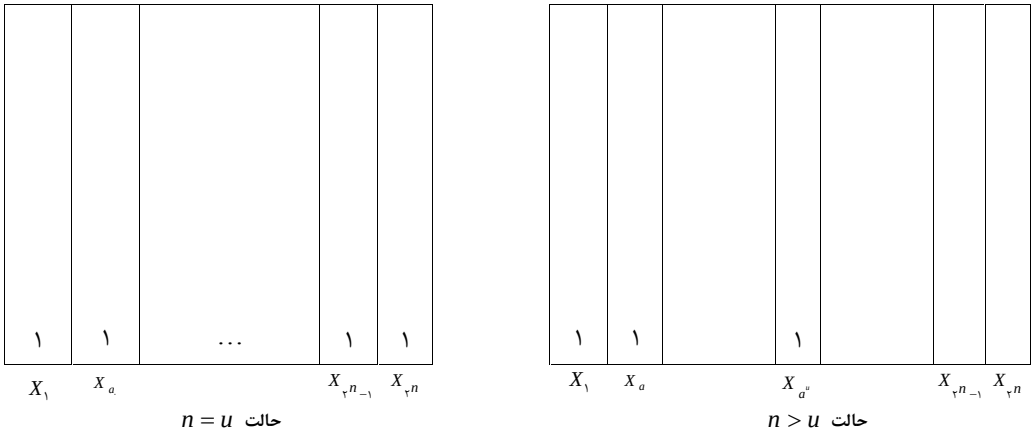
مانند رسته II از حالت (۱) در قضیه ۳-۳ و بدون از دست دادن کلیت فرض کنیم که $l_۱$ دارای کمترین توان است بنابراین:

$$۱ + ۲^{l_۲ - l_۱} + ... + ۲^{l_n - l_۱} = ۲^{k_۱ - l_۱} + ... ۲^{k_m - l_۱} \quad (۲۰)$$

که یک تناقض است.

۵. نتیجه‌گیری

ما پس از بررسی خواص جبری جمع مدولی با $r \geq ۲$ عملوند و با در نظر گرفتن درجه جبری مؤلفه‌ای توابع بولی از جمع مدولی به‌عنوان یک تابع بولی برداری، تعداد عبارت‌ها و متغیرها در این توابع بولی را تعیین کردیم و پس از محاسبه و بررسی در حالت‌های خاص، یک الگوریتم مناسب برای یافتن درجه مؤلفه‌ای توابع بولی در حالت کلی پیشنهاد کردیم. با استفاده از این الگوریتم، درجه جبری مؤلفه‌ای توابع بولی برای جمع مدولی به پیمانه $۲^{۳۲}$، با سه تا هشت عملوند به‌راحتی قابل محاسبه است. از طرفی چون شناختن درجه جبری توابع مؤلفه‌ای و تعداد عبارت‌ها و متغیرها در توابع مؤلفه‌ای برای کاربردهایی در طراحی و تحلیل رمزهای متقارن بسیار مهم و مفید می‌باشد، لذا یافته‌های این مقاله در نوع خود حائز اهمیت است.



شکل ۴. جدول A

۶. ضمیمه: درجه جبری مولفه توابع بولی برای جمع مدولی به پیمانه 2^{32} با دو تا هشت عملوند

	۰	۱	۲	۳	۴	۵	۶	۷	۸	۹	۰۱	۱۱	۱۲	۱۳	۱۴	۱۵
۲	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱۴	۱۵	۱۶
۳	۱	۲	۳	۵	۷	۹	۱۱	۱۳	۱۵	۱۷	۱۹	۲۱	۲۳	۲۵	۲۷	۲۹
۴	۱	۲	۴	۶	۹	۱۲	۱۵	۱۸	۲۱	۲۴	۲۷	۳۰	۳۳	۳۶	۳۹	۴۲
۵	۱	۲	۴	۶	۹	۱۳	۱۷	۲۱	۲۵	۲۹	۳۳	۳۷	۴۱	۴۵	۴۹	۵۳
۶	۱	۲	۴	۷	۱۱	۱۵	۲۰	۲۵	۳۰	۳۵	۴۰	۴۵	۵۰	۵۵	۶۰	۶۵
۷	۱	۲	۴	۷	۱۱	۱۶	۲۲	۲۸	۳۴	۴۰	۴۶	۵۲	۵۸	۶۴	۷۰	۷۶
۸	۱	۲	۴	۸	۱۲	۱۸	۲۵	۳۲	۳۹	۶۴	۵۳	۶۰	۶۷	۷۴	۸۱	۸۸

	۱۶	۱۷	۱۸	۱۹	۲۰	۲۱	۲۲	۲۳	۲۴	۲۵	۲۶	۲۷	۲۸	۲۹	۳۰	۳۱
۲	۱۷	۱۸	۱۹	۲۰	۲۱	۲۲	۲۳	۲۴	۲۵	۲۶	۲۷	۲۸	۲۹	۳۰	۳۱	۳۲
۳	۳۱	۳۳	۳۵	۳۷	۳۹	۴۱	۴۳	۴۵	۴۷	۴۹	۵۱	۵۳	۵۵	۵۷	۵۹	۶۱
۴	۴۵	۴۸	۵۱	۵۴	۵۷	۶۰	۶۳	۶۶	۶۹	۷۲	۷۵	۷۸	۸۱	۸۴	۸۷	۹۰
۵	۵۷	۶۱	۶۵	۶۹	۷۳	۷۷	۸۱	۸۵	۸۹	۹۳	۹۳	۱۰۱	۱۰۵	۱۰۹	۱۱۳	۱۱۷
۶	۷۰	۷۵	۸۰	۸۵	۹۰	۹۵	۱۰۰	۱۰۵	۱۱۰	۱۱۵	۱۲۰	۱۲۵	۱۳۰	۱۳۵	۱۴۰	۱۴۵
۷	۸۲	۸۸	۹۴	۱۰۰	۱۰۶	۱۱۲	۱۱۸	۱۲۴	۱۳۰	۱۳۶	۱۴۲	۱۴۸	۱۵۴	۱۶۰	۱۶۶	۱۷۲
۸	۹۵	۱۰۲	۱۰۹	۱۱۶	۱۲۳	۱۳۰	۱۳۷	۱۴۴	۱۵۱	۱۵۸	۱۶۵	۱۷۲	۱۷۹	۱۸۶	۱۹۳	۲۰۰

۷. مراجع

[1] Breaken, A.; Semaef, I. M. "The ANF of Composition of Addition and Multiplication Mod 2n with a Bloolean Function."; Fast Software Encryption, Lecture Notes in Computer Science 2005, 3557, 112-125.

[2] Bluetoth, SIG. "Spectification of Bluetooth System."; Verson 1.1, 1 Febrary 22, 2001, available at http://www.bluetooth.com.

[3] Schneier, B.; Kelsey, J.; Whiting, D.; Wagner, D.; Hall, C.; Ferguson, N. "Two Fish: A 128-Bit Block Cipher."; 1998, Available via http://www. Counterpance.com/twofish.html.

[4] Bracken, C.; Byrne, E.; Markin, N.; McGuire, G. "On the Walsh Spectrum of a New APN Function."; Lecture Notes in Computer Science 2007, 4887, 92-98.

[5] Bracken, C.; Byrne, E.; Markin, N.; McGuire, G. "Determining the Nonlinearity of a New Family of APN Functions."; Lecture Notes in Computer Science 2007, 4851, 72-79.

[6] Bracken, C.; Byrne, E.; Markin, N.; McGuire, G. "An Infinite Family Of Quadratic Quadrinominal APN Functions."; arXiv" :0707.1223v1, 2007. Available at http://arxiv.org/abs/0707.1223.

[7] Bracken, C.; Byrne, E.; Markin, N.; McGuire. G.; "A Few More Quadratic APN Functions, Cryptography and Communications."; Online FirstTM, 10 November 2010, arXiv:0804.4799v1 (Submited on 30 Apr 2008) . Available at http://arxiv.org/abs/0804.4799v1.

[8] Bracken, C.; Byrne, E.; McGuire, G.; Nebe, G. "Automorphisms of Some APN Functions and an Inequivalence Result."; Elsevier 2010, 26.

[9] Burwick, C.; Coppersmith, D.; Avignon, E. D.; Gennaro, R.; Halevi, S.; Jutla, C.; Matyas Jr., S. M.; OConnor, L.; Peyravian, M.; Safford, D.; Zunic, N. "MARS: a Candidate Cipher for AES."; 1 st AES Conferevce, CA, USA 1998.

[10] .Jonsson, J.; Kaliski, Jr. B. S. "The RC6 Block Cipher."; August 1998, 1.1, Available at www.rsa.com/rsalabs/aes/.

[11] Rivest, R. L. "The RC4 Encryption Algorihm."; RSA Data Security, Inc., 1992.

[12] Lai, X.; Massey, J. L. "A Proposal for a New Block Encryption Standard."; Advances in Cryptology, Eurocrypt 1990, Lecture Notes in Computer Science 1991, 473, 389-404.