

域GF(2)上行列式 $|B_n|$ 的次数

麦结华

(广西大学数学系)

摘 要

本文引进了 D 子集的概念, 并运用它求出了域 $GF(2)$ 上的行列式 $|B_n|$ 的次数与 n 的函数关系。

The Degree of Determinant $|B_n|$ over the Field $GF(2)$

Mai Jie-hua

(Guangxi University)

Abstract

In this paper the concept of D -subsets is introduced and used to find the relationship between the degree of determinant $|B_n|$ and n over the field $GF(2)$.

引 言

在 1973 年的一次国际性数学会议上, J. Pelikán 提出猜测: 同余式组

$$\sum_{i=1}^{n-k} a_i a_{i+k} \equiv 1 \pmod{2}, (k=0, 1, \dots, n-1)$$

当 $n \geq 5$ 时无整数解。屠规彰否定了这个猜测, 指出当 $n=12$ 时, 该同余式组有解:

$$\begin{cases} a_1 = a_2 = a_6 = a_7 = a_8 = a_{10} = a_{12} = 1 \\ a_3 = a_4 = a_5 = a_9 = a_{11} = 0 \end{cases}$$

此外,屠规彰还给出了该同余式组有解的充要条件^[2]。

上述的同余式组等价于域 $GF(2)$ 上的非线性方程组

$$\begin{pmatrix} a_1 & 0 & 0 & \cdots & 0 \\ a_2 & a_1 & 0 & \cdots & 0 \\ a_3 & a_2 & a_1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_n & a_{n-1} & a_{n-2} & \cdots & a_1 \end{pmatrix} \begin{pmatrix} a_n \\ a_{n-1} \\ a_{n-2} \\ \vdots \\ a_1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} \quad (1)$$

在探讨方程组(1)有解的充要条件的过程中,屠规彰得到了形如 $|B_n|$ 的行列式,其中

$$B_n = \begin{pmatrix} b_1 & 1 & 0 & \cdots & 0 \\ b_2 & b_1 & 1 & \cdots & 0 \\ b_3 & b_2 & b_1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b_n & b_{n-1} & b_{n-2} & \cdots & b_1 \end{pmatrix} \quad (2)$$

为由 $GF(2)$ 上的变元 $b_1, b_2, \dots, b_n$ 及0, 1组成的矩阵。

如果我们仅仅考虑行列式 $|B_n|$,易知 $|B_n|$ 的展开式中含有一项 b_1^n ,但因每个 b_i 都是 $GF(2)$ 的数,故有 $b_i^k = b_i (k \geq 1)$ 。所以,当 $n > 1$ 时, $|B_n|$ 的各项仅是 $b_{i_1}, b_{i_2}, \dots, b_{i_l}$ 的乘积, $i_1 < i_2 < \dots < i_l$,我们称为项 $b_{i_1} b_{i_2} \cdots b_{i_l}$ 的次数。为此,屠规彰提出:行列式 $|B_n|$ 的次数与 n 有何函数关系。

本文考察了 $|B_n|$ 的结构,找出了计算 $|B_n|$ 的较为简单的公式,并且发现了 $|B_n|$ 的次数与 n 的函数关系。

§1. D 子集

设 $X_n = \{(r, s) : r=1, 2, \dots, n; s=1, 2, \dots, n\}$ 是直角坐标平面上 n^2 个整数点的集合,则任何一个 $n \times n$ 矩阵都可以看作是一个从 X_n 到某一个域上的映射。

对于 $1, 2, \dots, n$ 的任一种排列 $r_1, r_2, \dots, r_n$,我们称点集 $\{(1, r_1)(2, r_2) \cdots (n, r_n)\}$ 为 X_n 的一 D 个子集。对于任一矩阵 $C = (c_{ij})_{n \times n}$ 及 X_n 上的任一 D 子集 S ,让我们作与 C 和 S 有关的矩阵 $C(S) = (a_{ij})_{n \times n}$ 如下:

$$a_{ij} = \begin{cases} c_{ij} & , \quad \text{若 } (i, j) \in S; \\ 0 & , \quad \text{若 } (i, j) \in X_n - S. \end{cases}$$

易知,当 D 子集 $S = \{(1, r_1), \dots, (n, r_n)\}$ 时,行列式

$$|C(S)| = (-1)^{T(S)} \prod_{i=1}^n C_i r_i$$

其中 $T(S)$ 是从 $1, 2, \dots, n$ 到 $r_1, r_2, \dots, r_n$ 的置换的逆序数。显然

$$|C| = \sum_{S \text{ 是 } X_n \text{ 的 } D \text{ 子集}} |C(S)| \quad (3)$$

(3)式表明, $|C(S)|$ 实际上是 $|C|$ 的展开式中的一项。据此, 我们称矩阵 $C(S)$ 为矩阵 C 的一项。如果 $|C(S)| \neq 0$, 则称 $C(S)$ 为 C 的非零项。

对任何两个 D 子集 $S = \{(1, r_1), \dots, (i, r_i)\} \subset X_i$ 及 $S' = \{(1, r'_1), \dots, (j, r'_j)\} \subset X_j$, 规定它们的连接和为

$$S \oplus S' = \{(1, r_1), \dots, (i, r_i), (i+1, i+r'_1), \dots, (i+j, i+r'_j)\}$$

显然, $S \oplus S'$ 是 X_{i+j} 中的 D 子集。 D 子集之间的连接和运算满足结合律, 但一般来说不满足交换律。

下面我们记 $S_1 = \{(1, 1)\} \subset X_1$,

$$S_i = \{(1, 2), (2, 3), \dots, (i-1, i), (i, 1)\} \subset X_i, i \geq 2$$

称 S_i 为 i 阶的一类 D 子集, ($i \geq 1$)。如果

$S = S_{i_1} \oplus S_{i_2} \oplus \dots \oplus S_{i_k}, k \geq 1, i_j \geq 1$, 则称 S 是一个 k 段的二类 D 子集。我们有

引理1. 设 S 是 X_n 的 D 子集, 则 $B_n(S)$ 是 (2) 式所示矩阵 B_n 的非零项的充要条件是 S 是 X_n 的二类 D 子集。

证明: 如果 S 是 X_n 的二类 D 子集, 由定义知

$$S = S_{i_1} \oplus S_{i_2} \oplus \dots \oplus S_{i_k} \oplus = \{(1, 2), (2, 3), \dots, (i_1, 1), \dots, (i_1+1, i_1+2),$$

$$(i_1+i_2, i_1+1), \dots, \left(\sum_{j=1}^{k-1} i_j+1, \sum_{j=1}^{k-1} i_j+2\right), \dots, \left(\sum_{j=1}^k i_j, \sum_{j=1}^{k-1} i_j+1\right)\},$$

由 (2) 式可知

$$\begin{aligned} |B_n(S)| &= (-1)^{T(S)} \prod_{i=1}^n b_{i, r_i} = (-1)^{T(S)} (1^{i_1-1} \cdot b_{i_1}) (1^{i_2-1} \cdot b_{i_2}) \dots (1^{i_k-1} \cdot b_{i_k}) \\ &= (-1)^{T(S)} b_{i_1} b_{i_2} \dots b_{i_k} \neq 0 \end{aligned}$$

即 $B_n(S)$ 是 B_n 的非零项。

反之, 若 $B_n(S)$ 是 B_n 的非零项, 即是

$$|B_n(S)| = (-1)^{T(S)} \prod_{i=1}^n b_{i, r_i} \neq 0, \text{ 也就是每一个 } b_{i, r_i} \neq 0.$$

由 (2) 可知

$$b_{i, r_i} = \begin{cases} b_i - r_i + 1, & \text{当 } r_i \leq i; \\ 1, & \text{当 } r_i = i+1; \\ 0, & \text{当 } r_i > i+1. \end{cases}$$

故知每个 $S = \{(i, i+1)\} \cup \{(j, r_j) | r_j \leq j\}$ 。下面对 n 采用归纳法。当 $n=2$ 时, $B_n(S) = \{(1, 1), (2, 2)\} \cup \{(1, 2), (2, 1)\}$, $S' = S_1 \oplus S_1$ 和 $S'' = S_2$ 都是 X_2 的二类 D 子集。

假设 $n-1$ 时, 结论成立。当 n 时, 对一个 S , $|B_n(S)| = (-1)^{T(S)} \prod_{i=1}^n b_{i, r_i}$,

如果 $b_n, r_n = b_n, n = b_1$ 时, 则

$|B_n(S)| = (-1)^{T(S)} \left(\prod_{i=1}^n b_i, r_i \right) b_{n,n}$, 其中 $\prod_{i=1}^{n-1} b_i, r_i \neq 0$, 存在 $n-1$ 级矩阵 B_{n-1} ,

使 $|B_{n-1}(S')| = (-1)^{T(S')} \prod_{i=1}^{n-1} b_i, r_i$. 由归纳假设知 $S' = S_{i_1} \oplus S_{i_2} \oplus \cdots \oplus S_{i_k}$, 所以

$S = S_{i_1} \oplus S_{i_2} \oplus \cdots \oplus S_{i_k} \oplus S_{i_{k+1}}$, 其中 $i_{k+1} = 1$. 如果 $b_n, r_n \neq 0, r_n < n, b_n, r_n = b_{n-r_n+1}$,

于是由(2)知, $|B_n(S)| = (-1)^{T(S)} \prod_{i=1}^n b_i, r_i = (-1)^{T(S)} \left(\prod_{i=1}^{r_n-1} b_i, r_i \right) \cdot$

$\cdot \left(\prod_{i=r_n}^n b_i, r_i \right) = (-1)^{T(S)} \left(\prod_{i=1}^{r_n-1} b_i, r_i \right) \left(\prod_{i=r_n}^{n-1} b_i, i+1 \right) b_{n, r_n} = (-1)^{T(S)} \cdot$

$\cdot \left(\prod_{i=1}^{r_n-1} b_i, r_i \right) \left(\prod_{i=1}^{n-r_n+1} b_i \right)$.

其中 $\prod_{i=1}^{r_n-1} b_i, r_i \neq 0$, 存在 r_n-1 级矩阵 B_{r_n-1} , 使 $|B_{r_n-1}(S')| = (-1)^{T(S')}$

$\prod_{i=1}^{r_n-1} b_i, r_i$. 由归纳假设知 $S = S_{i_1} \oplus S_{i_2} \oplus \cdots \oplus S_{i_k}$, 所以 $S = S_{i_1} \oplus S_{i_2} \oplus \cdots \oplus S_{i_k} \oplus$

$S_{i_{k+1}}$, 其中 $i_{k+1} = r_n$, 从而结论对 n 时成立。

§ 2. 行列式 $|B_n|$ 的计算

我们以 R 表示 X_n 的所有二类 D 子集的集合, 据(3)式及引理1可知

$$|B_n| = \sum_{S \in R} |B_n(S)| \quad (4)$$

我们称直角坐标平面上连结点 $(n, 1)$ 与点 $(1, n)$ 的直线段为 X_n 的次对角线, 若 X_n 的一个 D 子集是对称图形并以 X 的次对角线为对称轴, 就称该 D 子集是**对称的**. X_n 的次对角线的中点是 $\left(\frac{n+1}{2}, \frac{n+1}{2}\right)$. 因为 X_n 的任一个二类 D 子集与连 $(n, 1)$ 至 $\left(\frac{n+1}{2}, \frac{n+1}{2}\right)$ 的线段至多有一个公共点, 故若以 Q 表示 X_n 的所有的对称二类 D 子集的集合, 则我们可以把 Q 分拆为互不相交集 $Q_0, Q_1, \dots, Q\left[\frac{n+1}{2}\right]$ 的和集. 其中, Q_0 表示 Q 中所有与连 $(n, 1)$ 至 $\left(\frac{n+1}{2}, \frac{n+1}{2}\right)$ 的线段无公共点的 D 子集的集合, Q_i 表示 Q 中所有包含点 $(n+1-i, i)$ 的 D 子集的集合 $(i=1, 2, \dots, \left[\frac{n+1}{2}\right])$. 记号 $[x]$ 表示数 x 的整数部分)。

引理2. 设 Q 表示 X_n 的所有对称 D 二类子集的集合, 则有

(i) 若 n 为奇数, 则 $Q_0 = \phi$; 若 n 为偶数, 则 $Q_0 = \{S \oplus S'; S \text{ 为 } X_{\frac{n}{2}} \text{ 的二类 } D \text{ 子集},$

S' 为 S 关于次对角线的对称象;

(ii) $Q_1 = \{S_n\}$;

(iii) 对于 $i=2, \dots, \left[\frac{n+1}{2}\right]$, $Q_i = \{S \oplus S_{n+2-i} \oplus S' : S \text{ 为 } X_{i-1} \text{ 的二类 } D \text{ 子集,}$

S' 为 S 关于次对角线的对称象 $\}$ 。

这只要由 Q_i 的定义便可立即得出。我们还易得出下面定理。

定理1. 设矩阵 B_n 如(2)式所示, 令 $|B_0| = b_0 = 1$, 则

$$|B_n| = \sum_{i=0}^{\left[\frac{n}{2}\right]} b_{n-2i} |B_i|, \quad (n=1, 2, \dots). \quad (5)$$

证明: 因为 X_n 的不对称的 D 子集成对出现 (每一个不对称的 D 子集与它关于 X_n 的次对角对称象总能配成一对), 又因为 $GF(2)$ 上任何相同的代数式之和为零, 故知

$$\sum_{S \in R-Q} |B_n(S)| = 0. \text{ 于是, 从(4)式立刻得到}$$

$$|B_n| = \sum_{S \in Q} |B_n(S)| = \sum_{i=0}^{\left[\frac{n}{2}\right]} \sum_{S \in Q_i} |B_n(S)|$$

注意到在 $GF(2)$ 上 $(b_{j_1} b_{j_2} \cdots b_{j_k})^2 = b_{j_1} b_{j_2} \cdots b_{j_k}$, 由引理即可推出

$$\sum_{S \in Q_0} |B_n(S)| = \begin{cases} 0, & \text{若 } n \text{ 为奇数;} \\ |B_{\frac{n}{2}}|, & \text{若 } n \text{ 为偶数。} \end{cases}$$

$$\sum_{S \in Q_1} |B_n(S)| = b_n;$$

$$\sum_{S \in Q_i} |B_n(S)| = b_{n+2-2i} |B_{i-1}|, \quad \left(i=2, \dots, \left[\frac{n+1}{2}\right]\right).$$

总之就是

$$|B_n| = \sum_{i=0}^{\left[\frac{n}{2}\right]} b_{n-2i} |B_i|, \quad (n=1, 2, \dots)$$

运用定理1, 我们可以简化 $|B_n|$ 的计算。[注1]例如, 我们很容易算出

$$|B_1| = b_1; \quad |B_2| = b_1 + b_2; \quad |B_3| = b_3 + b_1;$$

$$|B_4| = b_4 + b_2 b_3 + (b_2 + b_1); \quad |B_5| = b_5 + b_3 b_1 + (b_1 b_2 + b_1);$$

注1 根据行列式的一般理论, 我们本来可以直接导出 $|B_n| = \sum_{i=1}^n b_i |B_{n-i}|$ 但是利用(5)式比它来得简便

多了。

$$|B_{11}| = b_{11} + b_6 b_1 + b_7 |B_2| + b_5 |B_3| + b_3 |B_4| + b_1 |B_5| \\ = b_{11} + b_6 b_1 + b_7 b_2 + b_7 b_1 + b_5 b_3 + b_5 b_4 + b_3 b_2 b_1 + b_3 b_2 + b_2 b_1 + b_1.$$

今考虑任一非负整数序列 $L = (i_0, i_1, \dots, i_k), (k \geq 0)$ 。

规定 L 的权为

$$w(L) = w(i_0, i_1, \dots, i_k) = \sum_{j=0}^k 2^j i_j \quad (6)$$

若 $w(L) = n$, 且最后 $i_k > 0$, 则称 L 为一个 W_n 序列, 我们把所有的 W_n 序列的集合记为 W_n , 又规定非负整数 i 与序列 $L = (i_0, i_1, \dots, i_k)$ 的连结和为

$$i * L = (i, i_0, \dots, i_k). \text{ 今记 } W_0 = \phi, i * W_0 = \{i\}, \text{ 以及} \\ i * W_n = \{i * L : L \in W_n\}, (n \geq 1).$$

$$\text{引理3. } W_n = \bigcup_{i=0}^{\left[\frac{n}{2}\right]} (n-2i) * W_i, (n=1, 2, \dots).$$

证明: 显然 $(n-2i) + 2i = (n-2i) + 2w(L), w(L) = i$, 由定义知

$$W_n = \bigcup_{i=0}^{\left[\frac{n}{2}\right]} (n-2i) * W_i.$$

仍设 $b_0 = 1$, 对任一 W_n 序列 $L = (i_0, i_1, \dots, i_k)$, 令

$$b(L) = b_{i_0} b_{i_1} \dots b_{i_k} \quad (7)$$

显然有 $b_i b(L) = b(i * L)$. 由定理1和引理3, 不难用归纳法证明

$$\text{定理2. } |B_n| = \sum_{L \in W_n} b(L), (n=1, 2, \dots). \quad (8)$$

定理2给出了直接计算行列式 $|B_n|$ 的途径. 特别是, 当我们只需知道 $|B_n|$ 中某些项时, 运用(8)式更为方便。

§ 3. $|B_n|$ 的次数

对于 $r=1, 2, \dots$, 记 $m_r = w(r, r-1, \dots, 2, 1)$.

由(6)式可知

$$m_r = r + 2(r-1) + 2^2(r-2) + \dots + 2^{r-2} \cdot 2 + 2^{r-1} = 2^{r+1} - r - 2 \quad (9)$$

引理4. 设 W_n 序列 $L(i_0, i_1, \dots, i_k)$ 含有 λ 个彼此不等的正整数, 如果 $n < m_r$, 则 $\lambda < r$.

证明: 让我们从 L 中选出一个子序列 $L' = (j_1, \dots, j_\lambda)$, 使得 $j_1, \dots, j_\lambda$ 是互不相等的正整数. 易见 $w(L') \leq w(L)$. 逐次调动序列 L' 中相邻的两个数的位置, 最后必能得到 $j_1, \dots, j_\lambda$ 的诸数的由大到小的排列 $L'' = (j_{a_1}, \dots, j_{a_\lambda})$. 易知 $w(L'') \leq w(L')$. 因为

$j_{a_1} \geq \lambda, j_{a_2} \geq \lambda - 1, \dots, j_{a_\lambda} \leq 1$, 故 $m_\lambda = w(\lambda, \lambda - 1, \dots, 1) \leq w(L'')$ 。综上所述, 得知 $m_\lambda \leq w(L) = n < m_r$, 从而推出 $\lambda < r$ 。

引理5. 若 $L = (j_1, j_2, \dots, j_\lambda)$ 是个 W_n 序列, 且 $j_1 > j_2 > \dots > j_\lambda > 0$, 则在 W_n 中就不会有别的序列能同时包含 $j_1, \dots, j_\lambda$ 这 λ 个正整数。

证明: 设 $L = (j_1, j_2, \dots, j_\lambda)$ 是一个 W_n 序列, 若有另一个 W_n 序列 L' 亦同时包含有 $j_1, \dots, j_\lambda$, 且 $L' \neq L$, 则仿照引理4的证明可推出 $n' = w(L') > w(L) = n$, 因而 $L' \notin W_n$ 。

现在, 我们考虑行列式 $|B_n|$ 的次数, $|B_n|$ 的次数就是把它展开并简化后保存下来的各项的最高次数。由定理2知 $|B_n|$ 的次数不超过各个 $b(L) (L \in W_n)$ 的次数的最大值。但对任 $L = (i_0, \dots, i_k) \in W_n$, $b(L) = b_{i_0} b_{i_1} \dots b_{i_k}$, 由于 $GF(2)$ 上的变元 b_i 的2次方仍然等于 b_i 以及 $b_0 = 1$, 故知 $b(L)$ 的次数应该等于 $\{i_0, \dots, i_k\}$ 中彼此不等的正整数的个数。因此, 据引理4立得

引理6. 如果 $n < m_r$, 则 $|B_n|$ 的次数小于 r 。

引理7. 如果 $L = \{j_1, \dots, j_\lambda\}$ 是个 W_n 序列, 且 $j_1 > j_2 > \dots > j_\lambda$, 则 $|B_n|$ 的展开式在化至最简之后仍然包含有 $b_{j_1} b_{j_2} \dots b_{j_\lambda}$ 这一项。

证明: 因为 $L \in W_n$, 故(8)式右边包含有 $b_{j_1} b_{j_2} \dots b_{j_\lambda}$ 这一项又据引理5知该项在(8)式右边只出现一次, 它不会在(8)式右边的求和过程中, 因与同类项合并后而消失。因此, 由定理2知 $|B_n|$ 的展开式在化至最简之后, 仍然包含有 $b_{j_1} b_{j_2} \dots b_{j_\lambda}$ 这一项。

运用引理7, 我们不须进行复杂的计算就可以判定 $|B_n|$ 的展开式(在化简之后)是否包含哪些项。例如, 若以记号 $b_{i_1} b_{i_2} \dots b_{i_k} \in |B_n|$ 表示 $b_{i_1} b_{i_2} \dots b_{i_k}$ 是 $|B_n|$ 的展开式中的一项, 则有 $b_3 b_2 b_1 \in |B_{11}|$, $b_{17} b_2 b_1 \in |B_{25}|$, $b_4 b_3 b_2 b_1 \in |B_{26}|$, 等等。

定理3. 设行列式 $|B_n|$ 的次数为 d_n , 则对于 $r = 1, 2, \dots$, 当 $2^{r+1} - r - 2 < n < 2^{r+2} - r - 3$ 时, $d_n = r$ 。

证明: 因为 $u < 2^{r+2} - r - 3 = m_{r+1}$, 由引理6知 $d_n \geq r$ 。另一方面, 令 $k = n - 2m_{r-1}$, (若 $r = 1$, 则令 $k = n$), 由 $n \geq m_r$ 可得 $k \geq m_r - 2m_{r-1} = r$ 。于是, 由引理7知 $|B_n|$ 的展开式在化至最简之后仍然包含有 $b_r b_{r-1} b_{r-2} \dots b_2 b_1$ 这一项。因此, 我们最后有 $d_n = r$ 。

参 考 文 献

[1] Hajnal et al ed., Infinite and finite sets, (1975).

[2] 屠规彰, 关于组合数论的一个猜测, 自然杂志, 1卷5期(1978), 274页。