SCIENCE CHINA
Information Sciences

• **Supplementary File** •

Two classes of rotation symmetric semi-bent functions

Qinglan ZHAO[1,2] & Dong ZHENG[2*]

[1]*School of Information Security Engineering, Shanghai Jiaotong University, Shanghai* 200240*, China;*
[2]*NELWS Laboratory, Xi'an University of Post and Telecommunications, Xi'an* 710121*, China*

Appendix A Proof of Theorem 1

Lemma 1 ([1]). Let f be a $2m$-variable Boolean function which can be expressed in the form : $f(x,y)=\pi(x)\cdot y\oplus h(x)$, where $x,y\in\mathbb{F}_2^m$, π is a mapping on $\mathbb{F}_2^m$ and h is an m-variable Boolean function. We have

1. If π is a 2-to-1 mapping, then f is a semi-bent function.
2. For $w\in\mathbb{F}_2^m$, if the set $S_w=\{x\in\mathbb{F}_2^m \mid \pi(x)=w\}$ is either empty or an s-dimensional affine subspace of $\mathbb{F}_2^m$, then f is a semi-bent function if and only if one of the following two conditions holds: (a) $s=1$; (b) $s=2$ and the restriction of h to S_w, viewed as a 2-variable function, has algebraic degree 2.

Lemma 2 (Theorem 1 in [2, p. 190]). Let $\mathscr{L}$ be a cyclic code of length n in $\mathbb{F}_2[x]/(x^n-1)$. Then
(1) There is a unique monic polynomial $g(x)$ of minimal degree in $\mathscr{L}$. $g(x)$ is a generator polynomial of $\mathscr{L}$.
(2) $g(x)$ is a factor of x^n-1.
(3) The dimension of $\mathscr{L}$ is $n-s$, $s=deg(g)$.
(4)If $g(x)=g_0+g_1x+\ldots+g_sx^s$, then $\mathscr{L}$ is generated by the rows of the generator matrix

$$G=\begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_s & & 0\\ & g_0 & g_1 & \cdots & g_{s-1} & g_s & \\ & & & \cdots & \cdots & & \\ 0 & & g_0 & \cdots & \cdots & & g_s \end{bmatrix}$$

Let $W=\{x\in\mathbb{F}_2^{2m} \mid x_{m+i}=0,\ 0\leqslant i\leqslant m-1\}$ and $V=\{x\in\mathbb{F}_2^{2m} \mid x_i\oplus x_{m+i}=0,\ 0\leqslant i\leqslant m-1\}$. Since W and V are two supplementary m-dimensional vector subspaces of $\mathbb{F}_2^{2m}$, the direct sum of W and V is $2m$-dimensional vector subspace. Hence, for any vector $x\in\mathbb{F}_2^{2m}$, x can be uniquely expressed by $x=a\oplus y$ with $a=(x_0\oplus x_m, x_1\oplus x_{m+1},\ldots,x_{m-1}\oplus x_{2m-1},0,0\ldots,0)\in W$ and $y=(x_m,x_{m+1},\ldots,x_{2m-1},x_m,x_{m+1},\ldots,x_{2m-1})\in V$. This substitution will be used in the proofs of our main theorems.

The proof of Theorem 1: Replacing x by $a\oplus y$ where $a\in W$ and $y\in V$, we have

$$\begin{aligned}
\bigoplus_{k=0}^{n-1}\rho_n^k(x_0x_{t_0}) &= \bigoplus_{k=0}^{n-1}\rho_n^k\big[(a_0\oplus y_0)(a_{t_0}\oplus y_{t_0})\big]\\
&= \bigoplus_{k=0}^{n-1}\rho_n^k(a_0a_{t_0})\oplus\bigoplus_{k=0}^{n-1}\rho_n^k(a_0y_{t_0})\oplus\bigoplus_{k=0}^{n-1}\rho_n^k(a_{t_0}y_0)\oplus\bigoplus_{k=0}^{n-1}\rho_n^k(y_0y_{t_0})\\
&= \Big[\bigoplus_{k=0}^{m-t_0-1}\rho_n^k(a_0a_{t_0})\oplus\bigoplus_{k=m-t_0}^{m-1}\rho_n^k(a_0a_{t_0})\oplus\bigoplus_{k=m}^{2m-1}\rho_n^k(a_0a_{t_0})\Big]\\
&\quad\oplus\Big[\bigoplus_{k=0}^{m-1}\rho_n^k(a_0y_{t_0})\oplus\bigoplus_{k=m}^{2m-1}\rho_n^k(a_0y_{t_0})\Big]\\
&\quad\oplus\Big[\bigoplus_{k=0}^{m-t_0-1}\rho_n^k(a_{t_0}y_0)\oplus\bigoplus_{k=m-t_0}^{2m-t_0-1}\rho_n^k(a_{t_0}y_0)\oplus\bigoplus_{k=2m-t_0}^{2m-1}\rho_n^k(a_{t_0}y_0)\Big]
\end{aligned}$$

* Corresponding author (email: zhengdong_xupt@sina.com)

$$\begin{aligned}&\oplus 2\bigoplus_{k=0}^{m-1}\rho_m^k(y_0y_{t_0})\\ =&\bigoplus_{k=0}^{m-t_0-1}\rho_m^k(a_0a_{t_0})\oplus\bigoplus_{k=0}^{m-1}\rho_m^k(a_0y_{t_0})\oplus\bigoplus_{k=0}^{m-1}\rho_m^k(a_{t_0}y_0)\\ =&\bigoplus_{k=0}^{m-t_0-1}\rho_m^k(a_0a_{t_0})\oplus\bigoplus_{k=0}^{m-1}\rho_m^k\big[(a_{m-t_0}\oplus a_{t_0})y_0\big].\end{aligned}\tag{A1}$$

Consequently,

$$\begin{aligned}f_1(x)=&f_1(a\oplus y)\\ =&g_1(a_0\oplus y_0\oplus a_m\oplus y_m,\ldots,a_{m-1}\oplus y_{m-1}\oplus a_{2m-1}\oplus y_{2m-1})\oplus\bigoplus_{k=0}^{n-1}\rho_n^k\big[(a_0\oplus y_0)(a_{t_0}\oplus y_{t_0})\big]\\ =&g_1(a_0,\ldots,a_{m-1})\oplus\bigoplus_{k=0}^{m-t_0-1}\rho_m^k(a_0a_{t_0})\oplus\bigoplus_{k=0}^{m-1}\rho_m^k\big[(a_{m-t_0}\oplus a_{t_0})y_0\big]\\ =&\pi(a)\cdot y\oplus h_1(a),\end{aligned}$$

where

$$\pi(a)=(a_{m-t_0}\oplus a_{t_0},a_{m-t_0+1}\oplus a_{t_0+1},\ldots,a_{m-t_0-1}\oplus a_{t_0-1})$$

and

$$h_1(a)\ =\ g_1(a_0,\ldots,a_{m-1})\oplus\bigoplus_{k=0}^{m-t_0-1}\rho_m^k(a_0a_{t_0}).\tag{A2}$$

Next we need only consider the case $1\leqslant t_0\leqslant q$ since it is similar to the case $q+1\leqslant t_0\leqslant 2q$. Let s=gcd$(2t_0,m)$. According to Lemma 2, π is a 2^s-to-1 mapping since $\gcd(x^{m-t_0}\oplus x^{t_0},x^m\oplus 1)=x^s\oplus 1$. Since m is odd, we have that $s\neq 2$. Hence, by Lemma 1, $f_1(x)$ is a semi-bent function if and only if $gcd(2t_0,m)=1$.

Appendix B Proof of Theorem 2

In order to investigate the degree of the constrcted $2m$-variable RotS semi-bent functions for even m, we first give the following lemma.

Lemma 3. Let $m\geqslant 4$ be even, and $n=2m$. Let $g(x)$ be an m-variable quadratic RotS Boolean function with the form

$$g(x)=\bigoplus_{t=1}^{\frac{m}{2}-1}c_t\big[\bigoplus_{k=0}^{m-1}\rho_m^k(x_0x_t)\big]\oplus c_{\frac{m}{2}}\bigoplus_{k=0}^{\frac{m}{2}-1}\rho_m^k(x_0x_{\frac{m}{2}}),\tag{B1}$$

where $c_{\frac{m}{2}},c_t\in\mathbb{F}_2$. Then $\widehat{g}(x)$ can be expressed as the following form

$$\widehat{g}(x)=\bigoplus_{t=1}^{m-1}c_t\big[\bigoplus_{k=0}^{n-1}\rho_n^k(x_0x_t)\big],\tag{B2}$$

where $c_t=c_{m-t}$.

Proof. According to $(B1)$, we have

$$\begin{aligned}\widehat{g}(x)=&g(x_0\oplus x_m,\ldots,x_{m-1}\oplus x_{2m-1})\\ =&\bigoplus_{t=1}^{\frac{m}{2}-1}c_t\big\{\bigoplus_{k=0}^{m-1}\rho_n^k\big[(x_0+x_m)(x_t+x_{t+m})\big]\big\}\oplus c_{\frac{m}{2}}\bigoplus_{k=0}^{\frac{m}{2}-1}\rho_n^k\big[(x_0+x_m)(x_{\frac{m}{2}}+x_{\frac{m}{2}+m})\big]\\ =&\bigoplus_{t=1}^{\frac{m}{2}-1}\big[c_t\bigoplus_{k=0}^{n-1}\rho_n^k(x_0x_{m-t}\oplus x_0x_t)\big]\oplus c_{\frac{m}{2}}\bigoplus_{k=0}^{n-1}\rho_n^k(x_0x_{\frac{m}{2}})\\ =&\bigoplus_{\substack{t=1,\\ t\neq\frac{m}{2}}}^{m-1}\big[c_t\bigoplus_{k=0}^{n-1}\rho_n^k(x_0x_t)\big]\oplus c_{\frac{m}{2}}\bigoplus_{k=0}^{n-1}\rho_n^k(x_0x_{\frac{m}{2}})\\ =&\bigoplus_{t=1}^{m-1}c_t[\bigoplus_{k=0}^{n-1}\rho_n^k(x_0x_t)],\end{aligned}$$

where $c_t=c_{m-t}$.

The proof of Theorem 2: By replacing x by $a\oplus y$ where $a\in W$ and $y\in V$, we have the following equation.

$$f_2(x)=f_2(a\oplus y)$$

$$=g_2(a_0,\ldots,a_{m-1})\oplus\bigoplus_{t=1}^{m-1}\{c_t\bigoplus_{k=0}^{n-1}\rho_n^k[(a_0\oplus y_0)(a_t\oplus y_t)]\}\oplus\bigoplus_{k=0}^{n-1}\rho_n^k(a_0\oplus y_0)(a_{t_0}\oplus y_{t_0}). \tag{B3}$$

Note that $c_t=c_{m-t}$, for $0<t<m$. Then we have

$$\begin{aligned}
&\bigoplus_{t=1}^{m-1}\{c_t\bigoplus_{k=0}^{n-1}\rho_n^k[(a_0\oplus y_0)(a_t\oplus y_t)]\}\\
&=\bigoplus_{t=1}^{\frac{m}{2}-1}c_t\big[\bigoplus_{k=0}^{n-1}\rho_n^k(a_0\oplus y_0)(a_t\oplus y_t)\oplus\bigoplus_{k=0}^{n-1}\rho_n^k(a_0\oplus y_0)(a_{m-t}\oplus y_{m-t})\big]\oplus c_{\frac{m}{2}}\bigoplus_{k=0}^{n-1}\rho_n^k(a_0\oplus y_0)(a_{\frac{m}{2}}\oplus y_{\frac{m}{2}})\\
&\text{(by Equation(A1) with } t_0 \text{ replaced by } t\ )\\
&=\bigoplus_{t=1}^{\frac{m}{2}-1}c_t\{\bigoplus_{k=0}^{m-t-1}\rho_m^k(a_0a_t)\oplus\bigoplus_{k=0}^{m-1}\rho_m^k[(a_{m-t}\oplus a_t)y_0]\oplus\bigoplus_{k=0}^{m-(m-t)-1}\rho_m^k(a_0a_{m-t})\oplus\bigoplus_{k=0}^{m-1}\rho_m^k[(a_t\oplus a_{m-t})y_0]\}\\
&\oplus c_{\frac{m}{2}}\bigoplus_{k=0}^{\frac{m}{2}-1}\rho_m^k(a_0a_{\frac{m}{2}})\\
&=\bigoplus_{t=1}^{\frac{m}{2}-1}c_t\big[\bigoplus_{k=0}^{m-t-1}\rho_m^k(a_0a_t)\oplus\bigoplus_{k=0}^{t-1}\rho_m^k(a_0a_{m-t})\big]\oplus c_{\frac{m}{2}}\bigoplus_{k=0}^{\frac{m}{2}-1}\rho_m^k(a_0a_{\frac{m}{2}})\\
&=\bigoplus_{t=1}^{\frac{m}{2}-1}c_t\bigoplus_{k=0}^{m-1}\rho_m^k(a_0a_t)\oplus c_{\frac{m}{2}}\bigoplus_{k=0}^{\frac{m}{2}-1}\rho_m^k(a_0a_{\frac{m}{2}}).
\end{aligned}\tag{B4}$$

Substituting (A1) and (B4) into (B3), we obtain

$$\begin{aligned}
f_2(x)&=g_2(a_0,\ldots,a_{m-1})\oplus\bigoplus_{t=1}^{\frac{m}{2}-1}\{c_t\bigoplus_{k=0}^{m-1}\rho_m^k(a_0a_t)\}\oplus c_{\frac{m}{2}}\bigoplus_{k=0}^{\frac{m}{2}-1}\rho_m^k(a_0a_{\frac{m}{2}})\\
&\quad\oplus\bigoplus_{k=0}^{m-t_0-1}\rho_m^k(a_0a_{t_0})\oplus\bigoplus_{k=0}^{m-1}\rho_m^k[(a_{m-t_0}\oplus a_{t_0})y_0]\\
&=\pi(a)\cdot y\oplus h_2(a),
\end{aligned}$$

where

$$\pi(a)=(a_{m-t_0}\oplus a_{t_0},a_{m-t_0+1}\oplus a_{t_0+1},\ldots,a_{m-t_0-1}\oplus a_{t_0-1})$$

and

$$h_2(a)=g_2(a_0,\ldots,a_{m-1})\oplus\bigoplus_{t=1}^{\frac{m}{2}-1}\big[c_t\bigoplus_{k=0}^{m-1}\rho_m^k(a_0a_t)\big]\oplus c_{\frac{m}{2}}\bigoplus_{k=0}^{\frac{m}{2}-1}\rho_m^k(a_0a_{\frac{m}{2}})\oplus\bigoplus_{k=0}^{m-t_0-1}\rho_m^k(a_0a_{t_0}).$$

Note that f_2 is not semi-bent when $t_0=\frac{m}{2}$ (which implies $\pi=0$). Without loss of generality, we suppose that $0<t_0<\frac{m}{2}$. Similarly to the discussion of Theorem 1, we deduce that f_2 can be semi-bent only if $s=2$ since m is even, where $s=gcd(2t_0,m)$.

When $s=2$, let G be the kernel of π. Then

$$G=\{x\mid\pi(x)=\mathbf{0},x\in\mathbb{F}_2^m\}=\{\mathbf{0},\mathbf{1},(0,1,0,1,\ldots,0,1),(1,0,1,0,\ldots,1,0)\}$$

where $\mathbf{0}$ is the all zero vector and $\mathbf{1}$ is the all one vector. For any $w\in\mathbb{F}_2^m$, let $S_w=\{x\in\mathbb{F}_2^m\mid\pi(x)=w\}$. There must exist some $b\in\mathbb{F}_n^m$ such that, for any $a\in S_\omega$, there exists a unique $e\in G$ such that $a=b\oplus e$. We represent the restriction of $h_2(a)$ to S_w as

$$h_2'=A\oplus B\oplus C$$

with

$$\begin{aligned}
A&=\bigoplus_{a_0a_{i_1r}\ldots a_{i_lr}\in\Gamma'(m)}v_{a_0a_{i_1r}\ldots a_{i_lr}}\bigoplus_{k=0}^{|O_m(a_0a_{i_1r}\ldots a_{i_lr})|-1}\rho_m^k\big[(b_0\oplus e_0)\ldots(b_{i_lr}\oplus e_{i_lr})\big],\\
B&=\bigoplus_{t=1}^{\frac{m}{2}-1}\{c_t\bigoplus_{k=0}^{m-1}\rho_m^k\big[(b_0\oplus e_0)(b_t\oplus e_t)\big]\},\\
C&=c_{\frac{m}{2}}\bigoplus_{k=0}^{\frac{m}{2}-1}\rho_m^k\big[(b_0\oplus e_0)(b_{\frac{m}{2}}\oplus e_{\frac{m}{2}})\big]\oplus\bigoplus_{k=0}^{m-t_0-1}\rho_m^k\big[(b_0\oplus e_0)(b_{t_0}\oplus e_{t_0})\big].
\end{aligned}$$

In order to discuss the non-linearized part of h_2', we begin from the first part A, which is the restriction of $g_2(a)$ to S_w. Note that $i_1,\ldots,i_l$ are even when r is odd, and $e_i=e_j$ when $i\equiv j \bmod 2$. We have $e_{i_jr}=e_0$, $1\leqslant j\leqslant l$ for both odd r and

even r. So there is no non-linearized part relative to e in part A. Next we discuss the second part B. For $1 \leqslant t \leqslant \frac{m}{2}-1$, we have

$$\bigoplus_{k=0}^{m-1} \rho_m^k\left[(b_0 \oplus e_0)(b_t \oplus e_t)\right] = \bigoplus_{k=0}^{m-1} \rho_m^k\left(b_0 b_t \oplus b_0 e_t \oplus b_t e_0 \oplus e_0 e_t\right).$$

If t is even, then

$$\bigoplus_{k=0}^{m-1} \rho_m^k(e_0 e_t) = \bigoplus_{k=0}^{m-1} \rho_m^k(e_0 e_0) = (\frac{m}{2} \bmod 2)(e_0 \oplus e_1).$$

If t is odd, then

$$\bigoplus_{k=0}^{m-1} \rho_m^k(e_0 e_t) = \bigoplus_{k=0}^{m-1} \rho_m^k(e_0 e_1) = (m \bmod 2)(e_0 e_1) = 0.$$

According to the above remark, we see that there is no non-linearized part in part B.

Therefore, the non-linearized part of h_2' is the non-linearized part NC in part C:

$$NC = c_{\frac{m}{2}} \bigoplus_{k=0}^{\frac{m}{2}-1} \rho_m^k(e_0 e_{\frac{m}{2}}) \oplus \bigoplus_{k=0}^{m-t_0-1} \rho_m^k(e_0 e_{t_0}).$$

We investigated it in two cases.

Case 1. When $c_{\frac{m}{2}} = 0$, we have $NC = \bigoplus_{k=0}^{m-t_0-1} \rho_m^k(e_0 e_{t_0})$. When $\gcd(t_0, m) = 2$, t_0 is even and $NC = (\frac{m-t_0}{2} \bmod 2)(e_0 \oplus e_1)$. By Case 2 of Lemma 1, f can not be semi-bent when $\gcd(t_0, m) = 2$. When $\gcd(t_0, m) = 1$, t_0 and $m - t_0$ are odd. We have $NC = ((m - t_0) \bmod 2)(e_0 e_1) = e_0 e_1$ which implies $deg(h_2') = 2$. So f is semi-bent if and only if $\gcd(2t_0, m) = 2$ and $\gcd(t_0, m) = 1$.

Case 2. When $c_{\frac{m}{2}} = 1$, we have $NC = \bigoplus_{k=0}^{\frac{m}{2}-1} \rho_m^k(e_0 e_{\frac{m}{2}}) \oplus \bigoplus_{k=0}^{m-t_0-1} \rho_m^k(e_0 e_{t_0})$. Furthermore, when $m \equiv 0 \pmod 4$, $\bigoplus_{k=0}^{\frac{m}{2}-1} \rho_m^k(e_0 e_{\frac{m}{2}}) = (\frac{m}{4} \bmod 2)(e_0 \oplus e_1)$. When $\gcd(t_0, m) = 2$, $NC = (\frac{m}{4} \bmod 2)(e_0 \oplus e_1) \oplus (\frac{m-t_0}{2} \bmod 2)(e_0 \oplus e_1)$, which which implies $deg(h_2') < 2$. When $\gcd(t_0, m) = 1$, $NC = (\frac{m}{4} \bmod 2)(e_0 \oplus e_1) \oplus e_0 e_1$, which implies $deg(h_2') = 2$. Therefore, when $c_{\frac{m}{2}} = 1$ and $m \equiv 0 \pmod 4$, f_2 is semi-bent if and only if $\gcd(2t_0, m) = 2$ and $\gcd(t_0, m) = 1$. When $m \equiv 2 \pmod 4$, $\bigoplus_{k=0}^{\frac{m}{2}-1} \rho_m^k(e_0 e_{\frac{m}{2}}) = e_0 e_1$, and in the same manner we conclude that f_2 is semi-bent if and only if $\gcd(2t_0, m) = 2$ and $\gcd(t_0, m) = 2$, which completes the proof of part(2) of Theorem 2.

By Lemma 3, for convenience, we suppose that there is no quadratic monomial in g_2. If $deg(g_2)$ is 0 or 1, then $deg(f_2) = 2$. If $deg(g_2) \geqslant 3$, then $deg(f_2) = deg(g_2)$.

Appendix C Construction of balanced RotS semi-bent functions

We only give a construction of balanced RotS semi-bent functions based on Theorem 1 as instance.

Corollary 1. With the same notations as in Theorem 2, we have

(1) For $g_1(\mathbf{0}) \oplus g_1(\mathbf{1}) = 0$, f_1 is a balanced RotS semi-bent function if and only if $gcd(2t_0, m) = 1$ and t_0 is even.

(2) For $g_1(\mathbf{0}) \oplus g_1(\mathbf{1}) = 1$, f_1 is a balanced RotS semi-bent function if and only if $gcd(2t_0, m) = 1$ and t_0 is odd.

Proof. From the proof of Theorem 1 , we conclude that $\pi(\mathbf{0}) = \pi(\mathbf{1}) = \mathbf{0}$ if $s = gcd(2t_0, m) = 1$. Then

$$\begin{aligned} W_{f_1}(\mathbf{0}) &= \sum_{a \in W, y \in V} (-1)^{\pi(a) \cdot y \oplus h_1(a)} \\ &= \sum_{a \in W} (-1)^{h_1(a)} \sum_{y \in V} (-1)^{\pi(a) \cdot y} \\ &= ((-1)^{h_1(\mathbf{0})} + (-1)^{h_1(\mathbf{1})}) 2^m . \end{aligned}$$

By Equation (A2), it is followed that f_1 is balanced if $g_1(\mathbf{0}) + g_1(\mathbf{1}) + m - t_0 = 1 \pmod 2$. Hence the conclusions hold.

Similarly, a balanced RotS semi-bent function can be constructed from Theorem 2 by restricting the value of $g_2(\mathbf{1})$, $g_2(\mathbf{0})$, $g_2(0, 1, 0, 1, \ldots, 0, 1)$, $g_2(1, 0, 1, 0, \ldots, 1, 0)$, and t_0.

Appendix D Examples

The following Example 1 and Example 2 belongs to the class of RotS semi-bent functions constructed by Theorem 1 and Theorem 2 respectively .

Example 1. Let $n = 10$, and $\widehat{g}(x)$ be a function with the form given by (4). Then

$$f_1(x) = \widehat{g}(x) \oplus \bigoplus_{k=0}^{9} \rho_{10}^k(x_0x_1)$$

is a RotS semi-bent function with degree 4.

Example 2. Let $n = 12$, $m = 6$, $p = 6$, $r = 1$ and $g_2(x) = \bigoplus_{k=0}^{5} \rho_6^k(x_0x_2x_4)$. By the Case 2 of Theorem 2,

$$\begin{aligned} f_2(x) &= g_2(x_0 \oplus x_6, \ldots, x_5 \oplus x_{11}) \oplus \bigoplus_{k=0}^{11} \rho_{12}^k(x_0x_3) \oplus \bigoplus_{k=0}^{11} \rho_{12}^k(x_0x_2) \\ &= \bigoplus_{k=0}^{11} \rho_{12}^k(x_0x_2x_4) \oplus \bigoplus_{k=0}^{3} \rho_{12}^k(x_0x_4x_8) \oplus \bigoplus_{k=0}^{11} \rho_{12}^k(x_0x_3) \oplus \bigoplus_{k=0}^{11} \rho_{12}^k(x_0x_2), \end{aligned}$$

is a RotS semi-bent function.

References

1 Carlet C, Gao G P, Liu W F. Results on constructions of rotation symmetric bent and semi-bent functions, in: Sequences and Their Applications-SETA 2014, Springer, 21-33.

2 MacWilliams F J , Sloane N J A. The theory of error correcting codes, Vol. 16, Elsevier, 1977.