KERDOCK-LIKE BENT FUNCTIONS
Jacques Wolfmann

To cite this version:
Jacques Wolfmann. KERDOCK-LIKE BENT FUNCTIONS. 2016. hal-01284625

HAL Id: hal-01284625
https://univ-tln.hal.science/hal-01284625
Preprint submitted on 7 Mar 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
KERDOCK-LIKE BENT FUNCTIONS

J.WOLFMANN

Abstract. We introduce bent functions similar to bent functions whose binary representative vectors are members of the famous Kerdock code.

1. Introduction

1.1. Elementary definitions.
$\mathbb{F}_2$ is the finite field of order 2.
A $m$-boolean function is a map from $\mathbb{F}_2^m$ into $\mathbb{F}_2$.
Weight: $w(F) = \sharp \{ v \in \mathbb{F}_2^m \mid F(v) = 1 \}$.
Derivative: $e \in \mathbb{F}_2^m : (D_e F)(X) = F(X) + F(X + e)$.
Fourier coefficients:
$\hat{F}(v) = \sum_{X \in \mathbb{F}_2^m} (-1)^{F(X) + <v,X>}$ where $<,>$ inner product of $\mathbb{F}_2^m$.
The set $\{ \hat{F}(v) \mid v \in \mathbb{F}_2^m \}$ is independent of the choice of $<,>$.
Definitions:
$F$ is bent if: $\forall v \in \mathbb{F}_2^m : \hat{F}(v)$ is in $\{-2^{m/2}, 2^{m/2}\}$.
Exist only when $m$ is even.
$F$ is near-bent if: $\forall v \in \mathbb{F}_2^m : \hat{F}(v)$ is in $\{-2^{(m+1)/2}, 0, 2^{(m+1)/2}\}$.
Exist only when $m$ is odd.

Bent functions were introduced by Rothaus in [6]. They are interesting for Coding Theory, Cryptology and Sequences and were the topic of a lot of works. See for instance [2], [5] Chap. 14, [7], [1].

For further use we need the following Proposition.

Proposition 1. The distribution of the Fourier coefficients of a $(2t - 1)$-near bent function $f$ is:
\[
\hat{f}(v) = \begin{cases} 
2^t & \text{number of } v: 2^{2t-3} + (-1)^{f(0)}2^{t-2} \\
0 & \text{number of } v: 2^{2t-2} \\
-2^t & \text{number of } v: 2^{2t-3} - (-1)^{f(0)}2^{t-2}.
\end{cases}
\]

Proof. See Proposition 4 in [1]).

1.2. Special representations of boolean functions.
1) Using finite fields:
$\mathbb{F}_2^m$ identified with the field $\mathbb{F}_{2^m}$.

Key words and phrases. Bent Functions, Kerdock.
In this case the inner product $<,>$ of $\mathbb{F}_{2^m}$ is defined by:

$$<a, x> = \text{tr}(ax)$$

where $\text{tr}$ is the trace of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$.

2) Representative vector (truth table)

Indexing $\mathbb{F}_{2^m}$ with any order $e_0, e_1, \ldots, e_{2^m-1}$ the representative vector of a $m$-boolean function $F$ is the binary vector $(F(e_i))_{i=0}^{2^m-1}$.

This vector depends on the choice of the order of $\mathbb{F}_{2^m}$.

3) A two-variable representation.

This is the representation chosen by Kerdock to introduce his famous code.

We identify $\mathbb{F}_{2^2t}$ with the product:

$$\mathbb{F}_{2^2t} = \{X = (u, \nu) \mid u \in \mathbb{F}_{2^{2t-1}}, \nu \in \mathbb{F}_2\}.$$ 

If $F$ is a $(2^t)$-boolean function then define two $(2^{t-1})$-boolean functions $f_0, f_1$, such that $f_0(u) = F(u, 0)$ and $f_1(u) = F(u, 1)$.

The two-variable representation (TVR) of $F$ is defined by the 2-variable polynomial:

$$\phi_F(x, y) = (y + 1)f_0(x) + yf_1(x)$$

This is a representation of $F$ in the following sense. Since:

$$\phi_F(u, 0) = f_0(u) = F(u, 0), \phi_F(u, 1) = f_1(u) = F(u, 1).$$

then if $X = (u, \nu)$, with $u = 0$ or $u = 1$: $F(X) = \phi_F(u, \nu)$.

Notation: $F = [f_0, f_1]$  

Let $\alpha$ be a primitive root of $\mathbb{F}_{2^t-1}$. As order of $\mathbb{F}_{2^t}$ we choose:

$$\mathbb{F}_{2^t} : (0, 0), (\alpha^0, 0) \ldots (\alpha^i, 0) \ldots (\alpha^{n/2-2}, 0) \mid (0, 1), (\alpha^0, 1) \ldots (\alpha^i, 1) \ldots (\alpha^{n/2-2}, 1)$$

The representative vector of $F = [f_0, f_1]$ is:

$$(f_0(0) \ldots f_0(\alpha^i) \ldots f_0(\alpha^{n/2-2}) \ldots f_1(0) \ldots f_1(\alpha^i) \ldots f_1(\alpha^{n/2-2}))$$

1.3. From Near-bent to Bent.

We now characterize the $f_0, f_1$ when $F = [f_0, f_1]$ is bent.

**Proposition 2. (well known)**

A $(2^t)$-boolean function $F = [f_0, f_1]$ is a bent if and only if:

(a) $f_0$ and $f_1$ are near-bent.

(b) $\forall u \in \mathbb{F}_{2^{2t-1}} \mid \hat{f}_0(u) \mid + \mid \hat{f}_1(u) \mid = 2^t$

**Proof.** A proof is given in [9],Proposition 14.

Remark: (b) means that one of $|\hat{f}_0(a)|$ and $|\hat{f}_1(a)|$ is equal to $2^t$ and the other one is equal to 0.
1.4. The Kerdock code.

Notation:
\[ Q(x) = \sum_{j=1}^{t-1} \text{tr}(x^{2^j+1}) \]

If \( e \in \mathbb{F}_{2^m} \): \( t_e(x) = \text{tr}(ex) \), \( Q_e(x) = Q(ex) \).

**Definition 3.**
The Kerdock code of length \( 2^{2t} \) is the set of the representative vectors of the \( 2^t \)-boolean functions
\[ F = [Q_u, Q_u + t_u] + \text{affine-linear form} \]
with \( u \in \mathbb{F}_{2^{2t-1}} \).

Example: The representative vector of \( F = [Q_u, Q_u + t_u] \) is:
\[ m = (f_0(0) \ldots f_0(\alpha^i) \ldots f_0(\alpha^{n/2-2}) \ f_1(0) \ldots f_1(\alpha^i) \ldots f_1(\alpha^{n/2-2})) \]
with \( f_0(x) = Q_u(x) \) and \( f_1(x) = (Q_u + t_u)(x) \).

**Theorem 4. (Kerdock)**
With the above notations:
If \( u \neq 0 \) then:
\[ F = [Q_u, Q_u + t_u] + \text{affine-linear form} \text{ is a Bent Function.} \]


**Remark:**
From the elementary properties of bent functions, \( F = [Q_u, Q_u + t_u] + \text{affine-linear form} \) is bent if and only if \( [Q_u, Q_u + t_u] \) is bent. Hence we restrict our research to \( [Q_u, Q_u + t_u] \).

**Definition:** For the sequel of the paper \( [Q_u, Q_u+t_u] \) is called a Kerdock bent function.

The Kerdock code \( K_{2t} \) is a binary non-linear code with several interesting properties. For instance:
1) \( [Q_u, Q_u + t_u] \) is a bent functions
2) \( [Q_u, Q_u + t_u] + [Q_v, Q_v + t_v] \) is a bent function.

**A problem:**
The question of this paper is to replace \( t_u \) in \( [Q_u, Q_u + t_u] \) by another \( 2t-1 \)-boolean function, for example \( t_r \), to get another bent function.

1.5. Main tools.

**Definition 5.**
If \( f \) is a \((2t-1)-\text{near-bent function}\) then \( \text{I}_f \) is the indicator of the set \( \{ x \in \mathbb{F}_{2^{2t-1}} \mid \hat{f}(x) = 0 \} \) where \( \hat{f} \) is the Fourier transform of \( f \).
(In other words, \( \text{I}_f(x) = 1 \) if and only if \( \hat{f}(x) = 0 \).)

The two Theorems below are the main tools of the present work.
Theorem 6. (McGuire and Leander)  
Let \( f \) be a \((2t - 1)\)-near-bent function and let \( v \) be in \( \mathbb{F}_{2^{2t-1}} \).  
\( D_v(\hat{f}) = 1 \) if and only if \([f, f + t_v] \) is a bent-function.  

Proof. See [4], Theorem 3. \( \square \)

Theorem 7. (W)  
Let \( f \) be a \((2t - 1)\)-near-bent function.  
Let \( \omega \) be in \( \mathbb{F}_{2^{2t-1}} \) and let \( \epsilon \) be in \( \mathbb{F}_2 \).  
If \( D_\omega f = \epsilon \) then \( \hat{f}(x) = 0 \) if and only if \( t_\omega(x) = 1 + \epsilon \).

Remark: According to the definition of \( \hat{f} \) this lemma means that if \( D_\omega f = \epsilon \) then \( \hat{f}(x) = 0 \) if and only if \( t_\omega(x) = 1 + \epsilon \).

Proof. \( \hat{f}(u) = \sum_{x \in \mathbb{F}_{2^{2t-1}}} (-1)^{f(x) + \text{tr}(ux)} = 2^{2t-1} - 2w(f + \text{tr}(ux)) \).  
\( \hat{f}(u) = 0 \) if and only if \( w(f + t_u) = 2^{2t-2} \).

\( D_\omega f = \epsilon \) means that \( f(x + \omega) = f(x) + \epsilon \).  
The transform \( \tau : x \rightarrow x + \omega \) is a permutation of \( \mathbb{F}_{2^{2t-1}} \) and then preserves the weight of every \((2t - 1)\)-Boolean function. Thus:

\[
\sharp\{x \mid f(x) + \text{tr}(ux) = 1\} = \sharp\{x \mid f(x + \omega) + \text{tr}(u(x + \omega)) = 1\}.
\]

\((E)\) \(\sharp\{x \mid f(x) + \text{tr}(ux) = 1\} = \sharp\{x \mid f(x) + \epsilon + \text{tr}(ux) + \text{tr}(u\omega) = 1\} \).

Now assume \( \text{tr}(u\omega) + \epsilon = 1 \). The right hand member of \((E)\) is:

\[
\sharp\{x \mid f(x) + \text{tr}(ux) = 0\} = 2^{2t-1} - \sharp\{x \mid f(x) + \text{tr}(ux) = 1\}.
\]

Hence \((E)\) becomes:

\[
\sharp\{x \mid f(x) + \text{tr}(ux) = 1\} = 2^{2t-1} - \sharp\{x \mid f(x) + \text{tr}(ux) = 1\}.
\]

In other words \( w(f + t_u) = 2^{2t-1} - w(f + t_u) \) and thus:

Conclusion:  
If \( \text{tr}(u\omega) + \epsilon = 1 \) then \( w(f + t_u) = 2^{2t-2} \) which is equivalent to \( \hat{f}(u) = 0 \).  
For every \( \epsilon \) the number of \( u \) such that \( \text{tr}(u\omega) + \epsilon = 1 \) is \( 2^{2t-2} \). This is also the number of \( u \) such that \( \hat{f}(u) = 0 \) (see Proposition 1). Then, immediately: \( \hat{f}(u) = 0 \) if and only if \( \text{tr}(u\omega) + \epsilon = 1 \).

This means \( \hat{f} = t_\omega + \epsilon \). \( \square \)

2. RESULTS

The goal is to find all the \( r \) such that \([Q_u, Q_u + t_v] \) is bent or such that \([Q_u + Q_v, Q_u + Q_v + t_v] \) is bent.  
Strategy:

For \( f = Q_u \) or \( f = Q_u + Q_v \), in order to apply Theorem 5(McGuire and Leander) we have to find \( \hat{f} \) and \( D_v(\hat{f}) \).
2.1. The case. \([Q_u, Q_u + t_r].\)

**Theorem 8.**

If \(f = Q_u\) then \(\hat{I}_f = \epsilon + t_{u-1}\) with \(\epsilon \in \mathbb{F}_2\).

**Proof.**

\[Q_u(x) = \sum_{j=1}^{t-1} \text{tr}((ux)^{2^j+1}).\]

If \(f_j(x) = (ux)^{2^j+1}\) then \(D_{u-1}f_j(x) = (ux)^{2^j+1} + [u(x + u^{-1})]^{2^j+1}\)

\[= ux + u^{2^j}x^{2^j+1}.\]

\[\text{tr}(f_j(x)) = \text{tr}(x) + \text{tr}(u^{2^j}x^{2^j}) + \text{tr}(1) = \text{tr}(1) = 1\]

\[D_{u-1}Q_u(x) = \sum_{j=1}^{t-1} D_{u-1}f_j(x) = \sum_{j=1}^{t-1} 1 = t - 1 = \epsilon \in \mathbb{F}_2.\]

According to the previous theorem: \(\hat{I}_{Q_u} = t_{u-1} + \epsilon.\)

2.2. The case. \([Q_u + Q_v, Q_u + Q_v + t_r]\)

Under the assumption on \(u\) and \(v\) then \([Q_u + Q_v, Q_u + Q_v + t_u + t_v]\) is a bent function. (See Theorem 4, 5)

Hence \(f(x) = Q_u + Q_v\) is near-bent (proposition 3).

Now we search \(\omega \in F_{2^{2r-1}}\) such that \(D_\omega f = \epsilon\) with \(\epsilon \in \mathbb{F}_2\).

\[D_\omega f = D_\omega Q_u + D_\omega Q_v.\]

\[Q_u(x) = \sum_{j=1}^{t-1} \text{tr}[f_{u,j}(x)]\] with \(f_{u,j}(x) = (ux)^{2^j+1}.\)

Since \(D_\omega, \sum, \text{tr}\) are additive functions then:

\[D_\omega Q_u = \sum_{j=1}^{t-1} \text{tr}[D_\omega f_{u,j}].\]

\[D_\omega f_{u,j}(x) = u^{2^j+1}x^{2^j+1} + u^{2^j+1}(x + \omega)^{2^j+1}.\]

\[(x + \omega)^{2^j+1} = (x + \omega)^{2^j}(x + \omega) = (x^{2^j} + \omega^{2^j})(x + \omega)\]

\[= x^{2^j+1} + \omega^{2^j}x + \omega x^{2^j} + \omega^{2^j+1}.\]

\[D_\omega Q_u(x) = \sum_{j=1}^{t-1} \text{tr}[u^{2^j+1}(\omega^{2^j}x + \omega x^{2^j} + \omega^{2^j+1})].\]

With \(m = 2t - 1\) and since \(x^m = x\) and \(u^m = u:\)

\[\hat{f}(u) = \sum_{x \in \mathbb{F}_{2^{2r-1}}(-1)f(x)\text{tr}(ux)} = 2^{2t-1} - 2w(f + \text{tr}(ux)). \sum_{j=1}^{t-1} \text{tr}[u^{2^j+1}\omega x^{2^j}]] = \sum_{j=1}^{t-1} \text{tr}[(u^{2^j+1}\omega x^{2^j})^{2m-1}] = \sum_{j=1}^{t-1} \text{tr}[u\omega^{2m-j}].\]
and thus:
\[ D_\omega Q_u(x) = \sum_{j=1}^{t-1} \text{tr}[u(\omega^j)^2 x] + \sum_{j=1}^{t-1} \text{tr}[u(\omega^{2^m-j}) x] + \sum_{j=1}^{t-1} \text{tr}[(u^{2^j+1})\omega^{2^j+1}] \]

When \( j \) runs from 1 to \( t-1 \) then \( m-j \) runs from 2\( t-2 \) to \( t \).
Hence: \( D_\omega Q_u = \sum_{j=1}^{t-1} \text{tr}[D_\omega f_{u,j}] \).
\[ D_\omega Q_u(x) = \text{tr}[u \sum_{j=1}^{2t-2} (u \omega^{2^j}) x] + \sum_{j=1}^{t-1} \text{tr}[(u^{2^j+1})\omega^{2^j+1}] \].

By replacing \( u \) by \( v \) we find a similar result and finally:
\[ D_\omega f(x) = \text{tr}\left( u \sum_{j=1}^{2t-2} (u \omega^{2^j}) x + v \sum_{j=1}^{2t-2} (v \omega^{2^j}) x \right) + \epsilon \text{ with } \epsilon \in \mathbb{F}_2. \]
\[ \hat{f}(u) = \sum_{x \in \mathbb{F}_{2^{2t-1}}} (-1)^{f(x)+\text{tr}(ux)} = 2^{2t-1} - 2w(f+\text{tr}(ux)). \]
It follows that \( D_\omega f \) is a constant function if and only if
\[ (*) \quad u \sum_{j=1}^{2t-2} (u \omega^{2^j}) + v \sum_{j=1}^{2t-2} (v \omega^{2^j}) = 0. \]

Remark that \( \sum_{j=1}^{2t-2} (u \omega^{2^j}) = u \omega + \text{tr}(u \omega) \) and
\[ \sum_{j=1}^{2t-2} (v \omega^{2^j}) = v \omega + \text{tr}(v \omega). \]
Then \( (*) \) becomes:
\[ (*) \quad (u^2 + v^2)\omega + utr(u \omega) + vtr(v \omega) = 0. \]

Case 1: \( \text{tr}(u \omega) = \text{tr}(v \omega) = 0 \).
we find the trivial solution \( \omega = 0 \).

Case 2: \( \text{tr}(u \omega) = \text{tr}(v \omega) = 1 \).
\[ \omega = (u+v)^{-1} \text{ and } \text{tr}(u \omega) = \text{tr}(u(u+v)^{-1}), \quad \text{tr}(v \omega) = \text{tr}(v(u+v)^{-1}). \]
This leads to \( \text{tr}(\omega u) + \text{tr}(\omega v) = \text{tr}[(u+v)(u+v)^{-1}] = \text{tr}(1) = 1 \) if \( \text{tr}(u^{-1}r) = 1 \).
which is impossible because \( \text{tr}(u \omega) = \text{tr}(v \omega) \).

Case 3: \( \text{tr}(u \omega) = 1, \text{tr}(v \omega) = 0 \).
\[ D_\omega Q_u = \sum_{j=1}^{t-1} \text{tr}[D_\omega f_{u,j}], \quad \omega = u(u^2 + v^2)^{-1} \]
Case 4: \( \text{tr}(u \omega) = 0, \text{tr}(v \omega) = 1 \).
\[ \omega = v(u^2 + v^2)^{-1}. \]

In case 3, \( \text{tr}(u \omega) = \text{tr}(u(u^2 + v^2)^{-1}) = \text{tr}[(u(u+v)^{-1})^2]. \]
\[ = \text{tr}(u(u+v)^{-1}). \]
Similarly in case 4:
\[ \text{tr}(v \omega) = \text{tr}(v(u+v)^{-1}). \]
Then \( \text{tr}(u(u+v)^{-1}) = \text{tr}(v(u+v)^{-1}) \) is impossible since
\[ \text{tr}(u^{-1}r) = 1. \]
\[ \text{tr}(u(u+v)^{-1}) + \text{tr}(v(u+v)^{-1}) = \text{tr}((u+v)(u+v)^{-1}) = \text{tr}(1) = 1. \]
Conclusion:

**Proposition 10.** \( f = Q_u + Q_v \).
If \( \omega \) is a non-zero element such that \( D_\omega f = \epsilon \) with \( \epsilon \in \mathbb{F}_2 \) then:
\[ \omega = u(u^2 + v^2)^{-1} \text{ if } \text{tr}(u(u+v)^{-1}) = 1. \]
\[ \omega = v(u^2 + v^2)^{-1} \text{ if } \text{tr}(v(u+v)^{-1}) = 1. \]

We are now in position to find all \( \epsilon \in \mathbb{F}_{2^{2t-1}} \) such that \([f, f + t \epsilon] \) is a bent function and consider the case \( \epsilon = r + s \)
Theorem 11.
Let $u \neq 0$, $tr(u^{-1}r) = 1$, $v \neq 0$, $tr(v^{-1}s) = 1$, $u \neq v$, $r \neq s$.
Define $\omega$ by:
\[
\omega = u(u^2 + v^2)^{-1} \text{ if } tr(u(u + v))^{-1} = 1.
\]
\[
\omega = v(u^2 + v^2)^{-1} \text{ if } tr(v(u + v))^{-1} = 1.
\]
If $tr(\omega(r + s)) = 1$ then:
\[
[Q_u, t_r] + [Q_v, t_s]
\]
is a bent function.

Proof.
Applying Theorem 7, since $D_\omega f = \epsilon$ then $I_\omega = t_\omega + \epsilon$. Now, if $e \in \mathbb{F}_{2t-1}$ then $D_e I_f(x) = I_f(x + e) = tr(\omega x + tr(\omega(x + e)) = tr(\omega x) + tr(\omega e) = tr(\omega e)$. Hence $D_e I_f(x) = 1$ if and only if $tr(\omega e) = 1$.

From Theorem 5, $[f, f + t_s]$ is a bent function if and only if $tr(\omega e) = 1$.
Now if $f = Q_u + Q_v$ then $[f, f + t_r + s] = [Q_u, Q_u + r] + [Q_v, Q_v + s]$ is a bent function if and only if $tr(\omega(r + s)) = 1$. \qed

3. Another construction.

Theorem 12.
Let $\gamma$ be in $\mathbb{F}_{2t-1}$, $tr(u^{-1}r) = 1$ then:
\[
[Q_u + t_1 t_\gamma, Q_u + t_r + t_1 t_\gamma]
\]
is a bent function.

Proof.
This is a special case of Theorem 20 of [10] with $f_0 = Q_u$ and $f_1 = Q_u + t_r$. \qed

Examples:
\[
[Q_u + t_1 t_\gamma, Q_u + t_r + t_1 t_\gamma] \text{ with } tr(u^{-1}r) = 1.
\]
\[
[Q_u + Q_v + t_1 t_\gamma, Q_u + Q_v + t_r + s + t_1 t_\gamma] \text{ with conditions of Theorem 11 on } u, v, r, s.
\]

4. Conclusions

By using a slight modification of Kerdock bent functions we have introduced new bent functions.

The number of new bent functions $[Q_u, Q_u + t_r]$ (Theorem 9) is greater than the number of Kerdock bent functions $[Q_u, Q_u + t_u]$.

The number of new bent functions $[Q_u + t_1 t_\gamma, Q_u + t_r + t_1 t_\gamma]$, $u \neq 0$, $tr(u^{-1}r) = 1$, $\gamma \neq 0$ (Theorem 12) is greater than the number of Kerdock bent functions $[Q_u, Q_u + t_r]$.

It is easy to check that:
Bent Functions

<table>
<thead>
<tr>
<th>Function</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>$[Q_u, Q_u + t_u], u \neq 0$</td>
<td>$(2^{2t-1} - 1)$</td>
</tr>
<tr>
<td>$[Q_u, Q_u + t_r]$ with $tr(u^{-1}r) = 1$</td>
<td>$2^{2t-2}(2^{2t-1} - 1)$</td>
</tr>
<tr>
<td>$[Q_u + t_1t_r, Q_u + t_r + t_1t_r]$</td>
<td>$2^{4t-3}(2^{2t-1} - 1)$</td>
</tr>
</tbody>
</table>

$[Q_u, Q_u + t_u] + [Q_v, Q_v + t_v]$          $(2^{2t-1} - 1)^2$
$[Q_u, Q_u + t_r] + [Q_v, Q_v + t_s]$         $A(2^{2t-1} - 1)^2$

with $A = \sharp\{(r, s) \mid tr(u^{-1}r) = 1, tr(u^{-1}s) = 1, tr(\omega(r + s) = 1)\}$.

(Notations of Theorem 11.)

5. References


IMATH(IAA), Université de Toulon, CS 60584, 83041 TOULON CEDEX9
\textit{E-mail address:} wolfmann@univ-tln.fr