# 3 Approximation by Linear Relations

In this section we approach hidden linearity of a Boolean map by looking for linear combinations of the output bits that linearly depend on a linear combination of the input bits, at least for some arguments.

## 3.1 Transformation of indicator functions

**Definition 1** For $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ the function $\vartheta_f : \mathbb{F}_2^n \times \mathbb{F}_2^q \longrightarrow \mathbb{R}$,

$$\vartheta_f(x, y) := \begin{cases} 1, & \text{if } y = f(x), \\ 0 & \text{else,} \end{cases}$$

is called the **indicator function** of $f$.

Let's calculate the Walsh transform of an indicator function; we'll encounter the set

$$L_f(u, v) := \{x \in \mathbb{F}_2^n \mid u \cdot x = v \cdot f(x)\},$$

where the function $v \cdot f$ coincides with the linear form corresponding to $u$. The bigger $L_f(u, v)$, the closer is the linear approximation of $f$ by $(u, v)$.

$$\begin{aligned} \hat{\vartheta}_f(u, v) &= \sum_{x \in \mathbb{F}_2^n} \sum_{y \in \mathbb{F}_2^q} \vartheta_f(x, y)(-1)^{u \cdot x + v \cdot y} \\ &= \sum_{x \in \mathbb{F}_2^n} (-1)^{u \cdot x + v \cdot f(x)} \\ &= \#L_f(u, v) - (2^n - \#L_f(u, v)). \end{aligned}$$

We have shown:

**Proposition 1** *For a Boolean map $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ the Walsh transform of the indicator function is $\hat{\vartheta}_f : \mathbb{F}_2^n \times \mathbb{F}_2^q \longrightarrow \mathbb{R}$,*

$$\hat{\vartheta}_f(u, v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{u \cdot x + v \cdot f(x)} = 2 \cdot \#L_f(u, v) - 2^n.$$

*In particular $-2^n \leq \hat{\vartheta}_f \leq 2^n$, and all the values of $\hat{\vartheta}_f$ are even.*

The derivation of this proposition gives as an intermediate result:

**Corollary 1** *Let $\beta : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$ the linear form corresponding to $v$. Then*

$$\hat{\vartheta}_f(u, v) = \hat{\chi}_{\beta \circ f}(u).$$

**Definition 2** For a Boolean map $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ the transformed function $\hat{\vartheta}_f : \mathbb{F}_2^n \times \mathbb{F}_2^q \longrightarrow \mathbb{R}$ of the indicator function $\vartheta_f$ is called the **(Walsh) spectrum** of $f$.

Imagine the spectrum $\hat{\vartheta}_f$ of $f$ as a $2^n \times 2^q$ matrix, whose rows are indexed by $u \in \mathbb{F}_2^n$ and whose columns are indexed by $v \in \mathbb{F}_2^q$, in the canonical order. By corollary 1 the columns are just the spectra of the Boolean functions $\beta \circ f$ for all the linear forms $\beta \in \mathcal{L}_q$.

**Corollary 2 (Column sums of the spectrum)** *Let $v \in \mathbb{F}_2^q$. Then*

$$\begin{aligned} \sum_{u \in \mathbb{F}_2^n} \hat{\vartheta}_f(u, v) &= \begin{cases} 2^n, & \text{if } v \cdot f(0) = 0, \\ -2^n & \text{else,} \end{cases} \\ \sum_{u \in \mathbb{F}_2^n} \hat{\vartheta}_f(u, v)^2 &= 2^{2n}. \end{aligned}$$

*Proof.* This follows from corollary 2 of the inversion formula in 2.2 and from corollary 1 together with Parseval's equation (proposition 4 in 2.3). $\diamond$

By proposition 5 in 2.4 we furthermore conclude:

$$\max |\hat{\vartheta}_f(\bullet, v)| = \max |\hat{\chi}_{\beta \circ f}| \geq 2^{n/2} \qquad \text{for each vector } v \in \mathbb{F}_2^q,$$

where equality holds, if and only if $\beta \circ f$ is bent. Hence:

**Corollary 3** *Let $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ be a Boolean map. Then*

$$\max_{\mathbb{F}_2^n \times (\mathbb{F}_2^q - \{0\})} |\hat{\vartheta}_f| \geq 2^{n/2}.$$

*Equality holds, if and only if $\beta \circ f$ is bent for each linear form $\beta : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$, $\beta \neq 0$.*

**Definition 3** (Nyberg, Eurocrypt 91) A Boolean map $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ is called **bent**, if for every linear form $\beta : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$, $\beta \neq 0$, the function $\beta \circ f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ is bent.

**Remarks**

1. Because $L_f(0, 0) = \mathbb{F}_2^n$ we have $\hat{\vartheta}_f(0, 0) = 2^n$. Therefore every $f$ attains the upper bound in proposition 1; only some $f$ attain the lower bound.

2. If $u \neq 0$, we have

$$\hat{\vartheta}_f(u, 0) = \sum_{x \in \mathbb{F}_2^n} (-1)^{u \cdot x} = 0.$$

Therefore the first column of the spectrum, "column 0", is $(2^n, 0, \ldots, 0)^t$.

3. By the corollaries of proposition 1 a Boolean map is bent, if and only if
$$\hat{\vartheta}_f(u,v) = \pm 2^{n/2} \qquad \text{for all } u \in \mathbb{F}_2^n, v \in \mathbb{F}_2^q - \{0\},$$
i. e., if the spectrum (outside of column 0) takes the values $\pm 2^{n/2}$ only.

4. If a bent map $\mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ exists, $n$ is even by corollary 1 of proposition 5 in section 2.4.

**Exercise 1** Let $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$ be bijective. Show that the spectrum $\hat{\vartheta}_{f^{-1}}$ is given by the transposed matrix of $\hat{\vartheta}_f$.

**Exercise 2** Compare the spectrum in the case $q = 1$ with the spectrum of a Boolean function in the sense of section 2.

**Note** Nyberg, EUROCRYPT 91, has shown: A bent map $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ exists, if and only if $n$ even and $\geq 2q$. The proof is slightly outside this tutorial. (It's contained in the German version.)

Let $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ be affine, $f(x) = Ax + b$ where $A \in M_{n,q}(\mathbb{F}_2)$ and $b \in \mathbb{F}_2^q$. Then

$$L_f(u,v) = \{x \in \mathbb{F}_2^n | u^t x = v^t Ax + v^t b\} = \{x \in \mathbb{F}_2^n | (u^t - v^t A)x = v^t b\}.$$

This is the kernel of the linear form $u^t - v^t A$, if $v^t b = 0$. It is a parallel hyperplane, if $v^t b = 1$. We distinguish the cases

$$\#L_f(u,v) = \begin{cases} 2^n, & \text{if } v^t A = u^t \text{ and } v^t b = 0, \\ 0, & \text{if } v^t A = u^t \text{ and } v^t b = 1, \\ 2^{n-1}, & \text{if } v^t A \neq u^t. \end{cases}$$

Hence

$$\hat{\vartheta}_f(u,v) = 2 \cdot \#L_f(u,v) - 2^n = \begin{cases} 2^n, & \text{if } v^t A = u^t \text{ and } v^t b = 0, \\ -2^n, & \text{if } v^t A = u^t \text{ and } v^t b = 1, \\ 0, & \text{if } v^t A \neq u^t. \end{cases}$$

Therefore the spectrum contains exactly one entry $\pm 2^n$ in each column (i. e. for constant $v$), and only zeroes else.

If vice versa the spectrum of $f$ looks like this, then $\beta \circ f$ is affine for all linear forms $\beta\colon \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$, hence $f$ is affine. We have shown:

**Proposition 2** *The map $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ is affine, if and only if each column of the spectrum $\hat{\vartheta}_f$ of $f$ has exactly one entry $\neq 0$.*

**Exercise 3** Calculate the spectrum of the "half adder" $f : \mathbb{F}_2^2 \longrightarrow \mathbb{F}_2^2$, given by the component ANFs $f_1 = T_1T_2$ and $f_2 = T_1 + T_2$. Do the same for the "full adder" $f : \mathbb{F}_2^3 \longrightarrow \mathbb{F}_2^2$, given by the component ANFs $f_1 = T_1T_2 + T_1T_3 + T_2T_3$ and $f_2 = T_1 + T_2 + T_3$.

**Exercise 4** How does the spectrum of a Boolean map from $\mathbb{F}_2^n$ to $\mathbb{F}_2^q$ behave under affine transformations of its domain and range?

## 3.2 Balanced maps and the preimage counter

From the last section we know the first column of the spectrum. Now let's look at the first row. We'll meet the **preimage counter**

$$\nu_f(y) := \#f^{-1}(y) = \#\{x \in \mathbb{F}_2^n \mid f(x) = y\} = \sum_{x \in \mathbb{F}_2^n} \vartheta_f(x, y),$$

We have

$$\begin{aligned}
\hat{\vartheta}_f(0, v) &= \sum_{x \in \mathbb{F}_2^n} \sum_{y \in \mathbb{F}_2^q} \vartheta_f(x, y)(-1)^{v \cdot y} \\
&= \sum_{y \in \mathbb{F}_2^q} \nu_f(y)(-1)^{v \cdot y} \\
&= \hat{\nu}_f(v).
\end{aligned}$$

Summing up we get

$$\sum_{v \in \mathbb{F}_2^q} \hat{\vartheta}_f(0, v) = \sum_{v \in \mathbb{F}_2^q} \hat{\nu}_f(v) = 2^q \cdot \nu_f(0)$$

by 2.2. Note that $\nu_f(0)$ is the number of zeroes of $f$. We have shown:

**Lemma 1** *Let $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ be a Boolean map. Then*

$$\begin{aligned}
\hat{\vartheta}_f(0, v) &= \hat{\nu}_f(v), \\
\sum_{v \in \mathbb{F}_2^q - \{0\}} \hat{\vartheta}_f(0, v) &= 2^q \cdot \nu_f(0) - 2^n.
\end{aligned}$$

**Exercise 1** Let $V(f) = \{x \in \mathbb{F}_2^n \mid f(x) = 0\}$ be the zero set of $f$. Show that

$$\sum_{v \in \mathbb{F}_2^q} \hat{\vartheta}_f(u, v) = 2^q \cdot \sum_{x \in V(f)} (-1)^{u \cdot x}$$

for each $u \in \mathbb{F}_2^n$. (Row sums of the spectrum.)

For cryptology one of the most important properties of Boolean functions is balancedness (that however has nothing to do with nonlinearity). Unbalanced maps give a nonuniform distribution of their output and facilitate statistical attacks.

**Definition 4** A map $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ is called **balanced**, if all its fibers $f^{-1}(y)$ for $y \in \mathbb{F}_2^q$ have the same size.

**Remarks**

1. $f$ is balanced, if and only if the preimage counter $\nu_f$ is constant.
2. If $f$ is balanced, then $f$ is surjective, in particular $n \geq q$, and the constant value of the preimage counter is $\nu_f = 2^{n-q}$; if $n = q$, then exactly the bijective maps are balanced.
3. By remark 3 in section 2.1 and remark 2 above, $f$ is balanced, if and only if $\hat{\nu}_f(0) = 2^n$ and $\hat{\nu}_f(v) = 0$ for $v \neq 0$. By lemma 1 this happens, if and only if
$$\hat{\vartheta}_f(0, v) = \begin{cases} 2^n & \text{for } v = 0, \\ 0 & \text{else.} \end{cases}$$
In this way the balancedness is tied to the first row ("row 0") of the spectrum.
4. A Boolean *function* $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ is balanced, if it takes the values 0 und 1 each exactly $2^{n-1}$ times; in other words, if its truth table contains exactly $2^{n-1}$ zeroes, or if $d(f, 0) = 2^{n-1}$. Corollary 2 in section 2.1, applied to the linear form 0, yields that $f$ is balanced, if and only if $\hat{\chi}_f(0) = 0$.
5. Because the total number of all preimages is $2^n$, we have
$$\sum_{y \in \mathbb{F}_2^q} \nu_f(y) = 2^n.$$

**Exercise 2** Show that an affine map $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ is balanced, if and only if it is surjective.

**Exercise 3** Let $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ be any Boolean function, and $\breve{f} : \mathbb{F}_2^{n+1} \longrightarrow \mathbb{F}_2$ defined by $\breve{f}(x_0, x_1, \ldots x_n) = x_0 + f(x_1, \ldots x_n)$. Show that $\breve{f}$ is balanced.

**Proposition 3** (Seberry/Zhang/Zheng, Eurocrypt 94) *A Boolean map $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ is balanced, if and only if for each linear form $\beta : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$, $\beta \neq 0$, the linear form $\beta \circ f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ is balanced.*

*Proof.* If $f$ is balanced, then obviously each component function $f_1, \ldots f_q : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ is balanced. An arbitrary linear form $\beta \neq 0$ can be transformed to the first coordinate function by a linear automorphism of $\mathbb{F}_2^q$; therefore $\beta \circ f$ is balanced too.

For the opposite direction we have to show, that the preimage counter is constant, $\nu_f = 2^{n-q}$. By corollary 1 in section 3.1 we have $\hat{\vartheta}_f(0,v) = \hat{\chi}_{v\cdot f}(0) = 0$ for every $v \in \mathbb{F}_2^q - \{0\}$. Moreover $\hat{\vartheta}_f(0,0) = 2^n$. Therefore the assertion follows from remark 3. $\diamond$

We also can express the balancedness by the convolution square of the preimage counter $\nu_f$:

**Proposition 4** *Let $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ be a Boolean map. Then the following statements are equivalent:*

(i) *$f$ is balanced.*

(ii) *$\nu_f * \nu_f = 2^{2n-q}$ constant.*

(iii) *$\nu_f * \nu_f(0) = 2^{2n-q}$.*

*Proof.* "(i) $\Longrightarrow$ (ii)" is almost trivial:

$$\nu_f * \nu_f(v) = \sum_{y\in\mathbb{F}_2^q} \nu_f(y)\nu_f(v+y) = 2^q \cdot 2^{n-q} \cdot 2^{n-q} = 2^{2n-q}.$$

"(ii) $\Longrightarrow$ (iii)" is the reduction to a special case.
"(iii) $\Longrightarrow$ (i)": We have

$$\begin{aligned} 2^{2n-q} = \nu_f * \nu_f(0) &= \sum_{y\in\mathbb{F}_2^q} \nu_f(y)^2, \\ 2^n &= \sum_{y\in\mathbb{F}_2^q} \nu_f(y). \end{aligned}$$

The Cauchy-Schwarz inequality yields

$$2^{2n} = \left[\sum_{y\in\mathbb{F}_2^q} 1 \cdot \nu_f(y)\right]^2 \le \sum_{y\in\mathbb{F}_2^q} 1^2 \cdot \sum_{y\in\mathbb{F}_2^q} \nu_f(y)^2 = 2^q \cdot 2^{2n-q}.$$

Since we have equality, $\nu_f(y)$ is a constant multiple of 1. $\diamond$

### 3.3 The linear profile

Let $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ be a Boolean map. In section 3.1 we introduced the sets $L_f(u,v)$ for $u \in \mathbb{F}_2^n$ and $v \in \mathbb{F}_2^q$. By proposition 1 we have

$$\#L_f(u,v) = 2^n - d(\alpha, \beta \circ f) = 2^{n-1} + \frac{1}{2}\,\hat{\vartheta}_f(u,v),$$

if $\alpha$ and $\beta$ are the linear forms corresponding to $u$ and $v$. We use the notation:

$$\begin{aligned} p_f(u,v) &:= \frac{\#L_f(u,v)}{2^n} = 1 - \frac{d(\alpha, \beta\circ f)}{2^n} = \frac{1}{2} + \frac{\hat{\vartheta}_f(u,v)}{2^{n+1}}, \\ \lambda_f(u,v) &:= (2p_f(u,v)-1)^2 = \frac{1}{2^{2n}} \cdot \hat{\vartheta}_f(u,v)^2. \end{aligned}$$

**Definition 5** The function

$$\lambda_f : \mathbb{F}_2^n \times \mathbb{F}_2^q \longrightarrow \mathbb{R}$$

is called the **linear profile** of $f$. The quantities $p_f(u,v)$ and $\lambda_f(u,v)$ are called the **probability** and the **potential** of the linear relation $(u,v) \in \mathbb{F}_2^n \times \mathbb{F}_2^q$ for $f$.

**Note** The use of the square in the definition of the linear profile follows a proposal of MATSUI 1999. Unusual, but, as we shall see, useful too, is the normalization by the coefficient $\frac{1}{2^{2n}}$.

**Remarks**

1. We have

$$0 \leq \lambda_f(u,v) \leq 1,$$

$$p_f(u,v) = \frac{1 \pm \sqrt{\lambda_f(u,v)}}{2},$$

and by proposition 1 in 3.1 all values of $\lambda_f$ are integer multiples of $\frac{1}{2^{2n-2}}$.

2. Several properties of the linear profile immediately follow from the corresponding statements for the spectrum. The column 0 of the linear profile is

$$\lambda_f(u,0) = \begin{cases} 1, & \text{if } u = 0, \\ 0 & \text{else.} \end{cases}$$

All column sums of the linear profile are 1:

$$\sum_{u\in\mathbb{F}_2^n} \lambda_f(u,v) = 1.$$

In particular for each $v \in \mathbb{F}_2^q$ there is a $u \in \mathbb{F}_2^n$ such that $\lambda_f(u,v) \geq \frac{1}{2^n}$. Furthermore $f$ is balanced, if and only if row 0 of the linear profile is $10\ldots0$, and $f$ is bent, if and only if all columns except column 0 are constant $= \frac{1}{2^n}$.

**Exercise 1** Write down the linear profile for all the maps where you formerly determined the spectrum.

The quantity

$$\Lambda_f := \max\{\lambda_f(u,v) \mid u \in \mathbb{F}_2^n, v \in \mathbb{F}_2^q, (u,v) \neq 0\}$$

denotes the maximal potential of a non trivial linear relation. The bigger $\Lambda_f$, the "closer" to linearity is $f$. Linear cryptanalysis uses $\Lambda_f$ as its measure of linearity.

**Definition 6** For a Boolean map $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ the quantity $\Lambda_f$ is called the **linear potential** of $f$.

**Remarks**

1. Always $0 \leq \Lambda_f \leq 1$. If $f$ is affine, then $\Lambda_f = 1$.
2. We have
$$\Lambda_f = \frac{1}{2^{2n}} \cdot \max_{(\mathbb{F}_2^n \times \mathbb{F}_2^q) - \{(0,0)\}} \hat{\vartheta}_f^2.$$
3. In the case $q = 1$ we have
$$\Lambda_f = \frac{1}{2^{2n}} \cdot \max \hat{\chi}_f^2.$$
4. More generally for $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$
$$\Lambda_f = \frac{1}{2^{2n}} \cdot \max_{\beta \in \mathcal{L}_q - \{0\}} \hat{\chi}_{\beta \circ f}^2 = \max_{\beta \in \mathcal{L}_q - \{0\}} \Lambda_{\beta \circ f}.$$

**Exercise 2** Show that $\Lambda_f$ is invariant under affine transformations of the range and domain of $f$.

**Exercise 3** Show that $\Lambda_f = \Lambda_{f^{-1}}$ if $f$ is bijective.

From corollary 2 of proposition 1 we have:

**Proposition 5** (Chabaud/Vaudenay, Eurocrypt 94) *Let $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ be a Boolean map. Then*
$$\Lambda_f \geq \frac{1}{2^n};$$
*equality holds, if and only if $f$ is bent.*

### 3.4 The nonlinearity of Boolean maps

**Definition 7** (i) (Pieprzyk/Finkelstein 1988) The **nonlinearity** of a Boolean function $f \in \mathcal{F}_n$ is the Hamming distance

$$\sigma_f := d(f, \mathcal{A}_n)$$

between $f$ and the subspace of affine functions.

(ii) (Nyberg 1992) For a Boolean map $f : \mathbb{F}_2^n \longrightarrow F_2^q$ the **nonlinearity** is

$$\sigma_f := \min\{\sigma_{\beta \circ f} \mid \beta : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2 \text{ affine, } \beta \neq 0\}.$$

**Lemma 2** *The nonlinearity of a Boolean function $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ is*

$$\sigma_f = 2^{n-1} - \frac{1}{2} \max |\hat{\chi}_f|.$$

*Proof.* Let $\alpha$ be the linear form, $\bar{\alpha}$ the nonlinear affine function corresponding to $u \in \mathbb{F}_2^n$. Then by corollary 2 in 2.1

$$\begin{aligned}
d(f, \alpha) &= 2^{n-1} - \frac{1}{2}\hat{\chi}_f(u), \\
d(f, \bar{\alpha}) &= 1 - d(f, \alpha) = 2^{n-1} + \frac{1}{2}\hat{\chi}_f(u), \\
d(f, \{\alpha, \bar{\alpha}\}) &= 2^{n-1} - \frac{1}{2}|\hat{\chi}_f(u)|.
\end{aligned}$$

The assertion follows. $\diamond$

**Proposition 6** *The nonlinearity of a Boolean map $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ is*

$$\sigma_f = 2^{n-1} - \frac{1}{2} \max |\hat{\vartheta}_f|,$$

*where the maximum is taken over $\mathbb{F}_2^n \times \mathbb{F}_2^q - \{(0,0)\}$.*

*Proof.* This follows from lemma 2 and the corollary 1 in 3.1. (The points $(u, 0)$ don't affect the maximum). $\diamond$

Since the linear profile is $\lambda_f = \frac{1}{2^{2n}}\hat{\vartheta}_f^2$, for the linear potential we conclude:

**Corollary 1** (i) $\sigma_f = 2^{n-1} \cdot (1 - \sqrt{\Lambda_f})$, $\quad \Lambda_f = \left(1 - \frac{1}{2^{n-1}}\sigma_f\right)^2$.

(ii) (Meier/Staffelbach, Eurocrypt 89, for $q = 1$)

$$\sigma_f \leq 2^{n-1} - 2^{\frac{n}{2}-1},$$

*where the equality holds, if and only if $f$ is bent.*

In particular the nonlinearity and the linear potential are equivalent measures.

Since $\sigma_f$ is integer valued, we get better bounds for small $n$:

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|
| $\sigma_f \leq$ | 0 | 1 | 2 | 6 | 13 | 28 | 58 | 120 | 244 |

For $n = 3$ this gives the improved lower bound $\Lambda_f \geq \frac{1}{4}$. For $n = 5, 7, \ldots$ the analogously improved bounds $\frac{9}{256}, \frac{9}{1024}, \ldots$ become more and more uninteresting.

Because $\chi_f(u) = \pm 2^{n/2}$ for a bent function, from corollary 2 in 2.1 follows:

**Corollary 2** *If $f$ is a bent function, and $\alpha$ affine, then*

$$d(f, \alpha) = 2^{n-1} \pm 2^{\frac{n}{2}-1}.$$

**Corollary 3** *If $f$ is a bent function, then $f$ has exactly $2^{n-1} \pm 2^{\frac{n}{2}-1}$ zeroes; in particular $f$ is not balanced.*

*Proof.* $d(f, 0) = 2^{n-1} \pm 2^{\frac{n}{2}-1} \neq 2^{n-1}$. $\diamond$

**Exercise 1** Assuming the existence of a bent function, show that if $n$ is even, then there exists a balanced function $f \in \mathcal{F}_n$ whose nonlinearity is $\sigma_f = 2^{n-1} - 2^{\frac{n}{2}}$, and whose linear potential is $\Lambda_f = \frac{1}{2^{n-2}}$.

**Exercise 2** Let $f \in \mathcal{F}_n$, and let $\breve{f}$ as in exercise 3 of section 3.2. Express the linear profile, the linear potential, and the nonlinearity of $\breve{f}$ in terms of the corresponding quantities of $f$. Assuming the existence of a bent function for even $n$, show that for odd $n$ there exists a balanced function $f$ with $\sigma_f = 2^{n-1} - 2^{\frac{n-1}{2}}$, $\Lambda_f = \frac{1}{2^{n-1}}$.