5 Characterization of Bent Maps

In these section we summarize the properties of bent functions and maps proven in the former sections.

Theorem 1 *For a Boolean function $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ the following statements are equivalent:*

(i) *f is bent, i. e., $\hat{\chi}_f^2 = 2^n$ constant.*

(ii) *f is perfectly nonlinear, i. e., the difference function $\Delta_u f$ is balanced for all $u \in \mathbb{F}_2^n - \{0\}$.*

(iii) *The linear potential of f has the (smallest possible) value $\Lambda_f = 2^{-n}$.*

(iv) *The nonlinearity of f has the (largest possible) value $\sigma_f = 2^{n-1} - 2^{\frac{n}{2}-1}$.*

(v) *The differential potential of f has the (smallest possible) value $\Omega_f = \frac{1}{2}$.*

(vi) *The linearity distance of f has the (largest possible) value $\rho_f = 2^{n-2}$.*

Corollary 1 *If f is bent, then:*

(i) *n is even.*

(ii) *f doesn't have any linear structures $\neq 0$.*

(iii) *f has exactly $2^{n-1} \pm 2^{\frac{n}{2}-1}$ zeroes and is not balanced.*

(iv) *f fulfils the strict avalanche criterion.*

Theorem 2 *For a Boolean map $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ the following statements are equivalent:*

(i) *f is bent, i. e., for all linear forms $\beta \neq 0$ on $\mathbb{F}_2^q$ the function $\beta \circ f$ is bent.*

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

(iii) *$\hat{\vartheta}_f^2$ is constant $= 2^n$ on $\mathbb{F}_2^n \times (\mathbb{F}_2^q - \{0\})$.*

(iv) *The linear potential of f has the (smallest possible) value $\Lambda_f = 2^{-n}$.*

(v) *The nonlinearity of f has the (largest possible) value $\sigma_f = 2^{n-1} - 2^{\frac{n}{2}-1}$.*

(vi) *f is perfectly nonlinear, i. e., the differential potential has the (smallest possible) value $\Omega_f = 2^{-q}$.*

(vii) *The differential profile δ_f is constant $= 2^{-q}$ on $(\mathbb{F}_2^n - \{0\}) \times \mathbb{F}_2^q$.*

Corollary 2 *If f is bent, then:*

(i) *n is even.*

(ii) *f doesn't have any linear structures $\neq 0$.*

(iii) *f is not balanced.*

(iv) *Each coordinate function of f fulfils the strict avalanche criterion.*

[Extension of (i) without proof: ... *and* $n \geq 2q$; see the note in section 3.1.]

Corollary 3 *A balanced map $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ is not bent, in particular its differential potential $\Omega_f > 2^{-q}$, and its linear potential $\Lambda_f > 2^{-n}$.*