# On the construction of bent functions of $2k$ variables from a primitive polynomial of degree $k$

Joan-Josep Climent[1], Francisco J. García[2], Verónica Requena[1]

[1] *Departament d'Estadística i Investigació Operativa. Universitat d'Alacant*
*E-mails:* jcliment@ua.es, vrequena@ua.es
[2] *Departament de Mètodes Quantitatius i Teoria Econòmica. Universitat d'Alacant*
*E-mail:* francisco.garcia@ua.es

Consider the binary field $\mathbb{F}_2$ and let $n$ be a positive integer. A **Boolean function** of $n$ variables is a map $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$. We call the **support** of $f$ the set

$$\mathrm{Supp}\,(f) = \{\boldsymbol{a} \in \mathbb{F}_2^n \mid f(\boldsymbol{a}) = 1\}.$$

Boolean functions are widely used in different types of cryptographic applications such as block ciphers, stream ciphers and hash functions. The functions achieving the maximal possible nonlinearity possess the best resistance to the linear attack and they are called **bent** functions. Bent functions constitute a fascinating issue in cryptography, but unfortunately there is a mist hovering over their properties, their classification and their actual number.

From now on, we assume that $n = 2k$. Assume that $G_1, G_2, \ldots, G_t$ are linear subspaces of $\mathbb{F}_2^n$ of dimension $k$ such that $G_i \cap G_j = \{\mathbf{0}\}$ for $i, j = 1, 2, \ldots, t$ with $i \neq j$, and consider the set

$$B = \begin{cases} \bigcup_{i=1}^{t} G_i^*, & \text{if } \ t = 2^{k-1}, \\ \{\mathbf{0}\} \cup \bigcup_{i=1}^{t} G_i^*, & \text{if } \ t = 2^{k-1} + 1, \end{cases}$$

with $G_i^* = G_i \backslash \{\mathbf{0}\}$. Dillon [Elementary Hadamard Difference Sets, Ph.D. thesis, University of Maryland (1974)] proved that $B$ is the support of a bent function of $n$ variables.

Let $U$ and $V$ be $n \times k$ matrices such that $\begin{bmatrix} U & V \end{bmatrix}$ is invertible and assume that $C$ is the $k \times k$ companion matrix of a primitive polynomial of degree $k$ in $\mathbb{F}_2[\mathsf{X}]$. If $G_0 = \mathrm{Col}\,(V)$, $G_{2^k} = \mathrm{Col}\,(U)$ and

$$G_i = \mathrm{Col}\left(UC^{i-1} + V\right) \quad \text{for} \quad i = 1, 2, \ldots, 2^k - 1,$$

then we prove that $\dim G_i = k$, for $i = 0, 1, 2, \ldots, 2^k$, and $G_i \cap G_j = \{\mathbf{0}\}$ for $i \neq j$.

As a consequence, if $\mathcal{A} = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k, \boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k\}$ is a basis of $\mathbb{F}_2^n$ and consider the matrices

$$U = \begin{bmatrix} \boldsymbol{u}_1 & \boldsymbol{u}_2 & \cdots & \boldsymbol{u}_k \end{bmatrix} \qquad \text{and} \qquad V = \begin{bmatrix} \boldsymbol{v}_1 & \boldsymbol{v}_2 & \cdots & \boldsymbol{v}_k \end{bmatrix}$$

then

$$B = \bigcup_{i \in I} G_i^* \quad \text{and} \quad B = \{\mathbf{0}\} \cup \bigcup_{i \in J} G_j^*$$

are the supports of bent functions of $n$ variables where $I, J \subseteq \{0, 1, 2, \ldots, 2^k\}$ such that $\mathrm{Card}\,(I) = 2^{k-1}$ and $\mathrm{Card}\,(J) = 2^{k-1} + 1$.

**Agradecimientos:** This work was partially supported by Spanish grant MTM2011-24858 of the Ministerio de Economía y Competitividad.