On the affine classification of cubic bent functions

Sergey Agievich

National Research Center for Applied Problems of Mathematics and Informatics

Belarusian State University

Fr. Skorina av. 4, 220050 Minsk, Belarus

agievich@bsu.by

Abstract

We consider cubic boolean bent functions, each cubic monomial of which contains the same variable. We investigate canonical forms of these functions under affine transformations of variables. In particular, we refine the affine classification of cubic bent functions of 8 variables.

1 Preliminaries

Let V_n be an n-dimensional vector space over the field $\mathbb{F}_2$, and $\mathcal{F}_n$ be the set of all boolean functions $V_n \to \mathbb{F}_2$. We identify a function $f \in \mathcal{F}_n$ of $\mathbf{x} = (x_1, \ldots, x_n)$ with its algebraic normal form, that is, a polynomial of the ring $\mathbb{F}_2[x_1, \ldots, x_n]$ reduced modulo the ideal $(x_1^2 - x_1, \ldots, x_n^2 - x_n)$. Denote by $\deg f$ the degree of such polynomial.

The Walsh–Hadamard transform associates with $f \in \mathcal{F}_n$ the function

$$\hat{f}(\mathbf{u}) = \sum_{\mathbf{x} \in V_n} \chi(f(\mathbf{x}) + \mathbf{x} \cdot \mathbf{u}), \quad \mathbf{u} \in V_n,$$

where $\chi(a) = (-1)^a$ is the additive character of $\mathbb{F}_2$ and $\mathbf{x} \cdot \mathbf{u}$ is the dot product of two vectors. Denote by $\hat{\mathcal{F}}_n$ the image of $\mathcal{F}_n$ under the mapping $f \mapsto \hat{f}$.

Let $\mathcal{B}_n$ be the set of all boolean *bent functions* of n variables: $f \in \mathcal{B}_n$ if $|\hat{f}(\mathbf{u})| = 2^{n/2}$ for all $\mathbf{u} \in V_n$. Bent functions were introduced by Rothaus in 1976 [7], and since then have been widely studied. It is clear that $\mathcal{B}_n \neq \varnothing$ only for even n. Therefore, when we write $\mathcal{B}_n$, we mean that n is even.

Let $\mathbf{AGL}_n$ be the general affine group of transformations of V_n. An element $\sigma \in \mathbf{AGL}_n$ acts as follows: $\sigma(\mathbf{x}) = \mathbf{x}A + \mathbf{b}$, where A is an invertible $n \times n$ matrix over $\mathbb{F}_2$, $\mathbf{b} \in V_n$. Extend the action of $\mathbf{AGL}_n$ on $\mathcal{F}_n$ in a natural way:

$$\sigma(f)(\mathbf{x}) = f(\mathbf{x}A + \mathbf{b}),$$

and call two functions *affine equivalent* if one can be obtained from the other by a transformation $\sigma \in \mathbf{AGL}_n$ and addition of an affine function l ($\deg l \leq 1$).

It is known that affine equivalent functions are both bent or both not bent. In this connection it would be interesting to find the number and representatives of affine equivalence classes of $\mathcal{B}_n$.

By Dickson's theorem (see, for example, [6]), any quadratic function $f(x_1, \dots, x_n)$ is affine equivalent to the function

$$x_1x_2 + \ldots + x_{2m-1}x_{2m}. \tag{1}$$

The number $2m$ here is determined uniquely and called the rank of f ($\operatorname{rank} f$). It is known that f is bent iff $\operatorname{rank} f = n$ and, consequently, every quadratic bent function of n variables is affine equivalent to the function (1) with $m = n/2$.

Unfortunately, obtaining similar classification even for cubic bent functions is a more complex problem. Today, such classification is completed only for $n = 6$: any cubic bent function of 6 variables is affine equivalent to one of the three functions given by Rothaus in [7].

Hou in [5] has considered cubic bent functions of 8 variables. Using the classification of cubic forms (see [2, 4]), Hou stated that any such function $f(\mathbf{x})$, $\mathbf{x} \in V_8$, is affine equivalent to one of the following:

$$\begin{aligned}
f_1(\mathbf{x}) &= x_1x_2x_3 + q_1(\mathbf{x}),\\
f_2(\mathbf{x}) &= x_1x_2x_3 + x_2x_4x_5 + q_2(\mathbf{x}),\\
f_3(\mathbf{x}) &= x_1x_2x_7 + x_3x_4x_7 + x_5x_6x_7 + q_3(\mathbf{x}),\\
f_4(\mathbf{x}) &= x_1x_2x_3 + x_2x_4x_5 + x_3x_4x_6 + q_4(\mathbf{x}),\\
f_5(\mathbf{x}) &= x_1x_2x_3 + x_2x_4x_5 + x_3x_4x_6 + x_1x_4x_7 + q_5(\mathbf{x}),
\end{aligned}$$

where $\deg q_i = 2$. Thus, to complete the classification, it remains to refine the functions q_i. Hou refined q_1, further we will refine q_2 and q_3.

We will use the following observation: each cubic monomial of f_2 contains the variable x_2 and each cubic monomial of f_3 contains x_7. In accordance with this observation, consider cubic bent functions of the form

$$f(u, v, \mathbf{x}) = ua(v, \mathbf{x}) + b(u, v, \mathbf{x}), \quad \mathbf{x} \in V_n, \quad \deg a = 2, \quad \deg b \leq 2. \tag{2}$$

Let us examine the properties of such functions.

2 Results

Before proceeding, recall the notion of bent rectangles from [1]. Let $f \in \mathcal{F}_n$ and m, k be positive integers such that $n = m + k$. Define the function

$$\overset{\square}{f}(\mathbf{u},\mathbf{v}) = \sum_{\mathbf{y}\in V_k} \chi(f(\mathbf{u},\mathbf{y}) + \mathbf{v}\cdot\mathbf{y}), \quad \mathbf{u}\in V_m, \quad \mathbf{v}\in V_k,$$

and call it the *rectangle* of f. Denote by $\overset{\square}{\mathcal{F}}_{m,k}$ the set of all such rectangles.

For a fixed $\mathbf{u}$ call the mapping $\mathbf{v} \mapsto \overset{\square}{f}(\mathbf{u},\mathbf{v})$ a *column* of $\overset{\square}{f}$. Analogously, for a fixed $\mathbf{v}$ call the mapping $\mathbf{u} \mapsto \overset{\square}{f}(\mathbf{u},\mathbf{v})$ a *row* of $\overset{\square}{f}$. By definition, each row of $\overset{\square}{f}$ is an element of $\hat{\mathcal{F}}_k$. If furthermore each column of $\overset{\square}{f}$ multiplied by $2^{(m-k)/2}$ is an element of $\hat{\mathcal{F}}_m$, then the rectangle $\overset{\square}{f}$ is called *bent*.

In [1] we pointed out the following correspondence between bent functions and bent rectangles.

Proposition 1. *A function $f \in \mathcal{F}_{m+k}$ is bent if and only if a rectangle $\overset{\square}{f} \in \overset{\square}{\mathcal{F}}_{m,k}$ is bent.*

Using 2-row bent rectangles $\overset{\square}{f} \in \overset{\square}{\mathcal{F}}_{1,n+1}$, we can proof the following result.

Proposition 2. *A cubic bent function of the form* (2) *is affine equivalent to the function*

$$u(h(\mathbf{x}) + v) + g(\mathbf{x}), \tag{3}$$

where $h(\mathbf{x}) = x_1x_2 + \ldots + x_{2m-1}x_{2m}$ and g is a quadratic bent function such that $g + h$ is also bent.

Let $\mathrm{Stab}_{\mathbf{AGL}_n}(h)$ be the stabilizer of h in $\mathbf{AGL}_n$, that is, the set of all $\sigma \in \mathbf{AGL}_n$ such that $\sigma(h) = h$. To refine (3), we have the following possibilities:

(a) apply to g transformations of $\mathrm{Stab}_{\mathbf{AGL}_n}(h)$,

(b) add h to g by replacing u with $u + 1$.

Proceed with the transformations (a). We need to know the canonical form to which we can reduce a quadratic bent function $g(\mathbf{x})$ by elements of $\mathrm{Stab}_{\mathbf{AGL}_n}(x_1x_2 + \ldots + x_{2m-1}x_{2m})$. Let us state a result in this direction. It will be convenient to rename variables and talk about a classification of quadratic bent functions $g(\mathbf{x},\mathbf{y},\mathbf{z})$, $\mathbf{x},\mathbf{y} \in V_m$, $\mathbf{z} \in V_{2k}$, under the action of $\mathrm{Stab}_{\mathbf{AGL}_{2(m+k)}}(\mathbf{x}\cdot\mathbf{y})$.

Before stating the result, define for $r = 1, 2, \ldots$ the function

$$\rho(\mathbf{x},\mathbf{y},z_1,z_2) = y_1z_1 + x_1y_2 + x_2y_3 + \ldots + x_{r-1}y_r + x_rz_2, \quad \mathbf{x},\mathbf{y} \in V_r,$$

and call it the *chain* of rank $2r+2$. For $r=0$ and "empty" vectors $\mathbf{x},\mathbf{y}$ call $\rho(\mathbf{x},\mathbf{y},z_1,z_2)=z_1z_2$ the chain of rank 2. Denote by

$$C(\alpha_1,\alpha_2,\ldots,\alpha_r)=\begin{pmatrix}0&0&\ldots&0&\alpha_1\\1&0&\ldots&0&\alpha_2\\0&1&\ldots&0&\alpha_3\\ \ldots&\ldots&\ldots&\ldots&\ldots\\0&0&\ldots&1&\alpha_r\end{pmatrix}$$

the companion matrix of the polynomial $p(\lambda)=\alpha_1+\alpha_2\lambda+\ldots+\alpha_r\lambda^{r-1}+\lambda^r$. The characteristic polynomial of $C=C(\alpha_1,\ldots,\alpha_r)$ equals $p(\lambda)$ and C is invertible iff $\alpha_1\neq 0$.

Lemma. *Any quadratic bent function $g(\mathbf{x},\mathbf{y},\mathbf{z})$, $\mathbf{x},\mathbf{y}\in V_m$, $\mathbf{z}\in V_{2k}$, by a transformation of* $\mathrm{Stab}_{\mathbf{AGL}_{2(m+k)}}(\mathbf{x}\cdot\mathbf{y})$ *and addition of an affine function can be reduced to the form*

$$\sum_{i=1}^{k}\rho_i(\mathbf{x}_i,\mathbf{y}_i,z_{2i-1},z_{2i})+\mathbf{y}_{k+1}Q\mathbf{x}_{k+1}^{\mathrm{T}},$$

where

(i) $\mathbf{x}_i,\mathbf{y}_i\in V_{m_i}$, $i=1,\ldots,k+1$, *such that* $(\mathbf{x}_1,\ldots,\mathbf{x}_{k+1})=\mathbf{x}$ *and* $(\mathbf{y}_1,\ldots,\mathbf{y}_{k+1})=\mathbf{y}$*;*

(ii) ρ_i *is the chain of rank* $2m_i+2$, $i=1,\ldots,k$*;*

(iii) Q *is the uniquely determined square matrix of order* m_{k+1}, *"empty" for* $m_{k+1}=0$ *and having the form*

$$Q=\mathrm{diag}(C_1,\ldots,C_d)$$

for $m_{k+1}>0$. *In the last case C_i are invertible companion matrices with characteristic polynomials $p_i(\lambda)$ such that $p_1(\lambda)\mid p_2(\lambda)$, $p_2(\lambda)\mid p_3(\lambda),\ldots,$ $p_{d-1}(\lambda)\mid p_d(\lambda)$.*

Interesting in view of Proposition 2 quadratic bent functions $g(\mathbf{x},\mathbf{y},\mathbf{z})$ have the additional property: $g(\mathbf{x},\mathbf{y},\mathbf{z})+\mathbf{x}\cdot\mathbf{y}$ is also bent. This property imposes the following restriction on Q: the addition of 1 to its diagonal elements keeps the matrix invertible. Hence, if $C_i=C_i(\alpha_1,\ldots,\alpha_r)$ is a diagonal companion matrix of Q, then $r\geq 2$ and $\alpha_2+\ldots+\alpha_r=1$.

Example. Let $m+k=3$. Under the stated restrictions on the diagonal matrices of Q, the function $g(\mathbf{x},\mathbf{y},\mathbf{z})$ by a transformation of $\mathbf{AGL}_6(\mathbf{x}\cdot\mathbf{y})$ and addition of an affine function can be reduced to one of the following forms:

$m=1$	$m=2$	$m=3$
$y_1z_1+x_1z_2+z_3z_4$	$y_1z_1+x_1y_2+x_2z_2$	$x_1y_2+x_2y_3+x_3(y_1+y_2)$
	$x_1y_2+x_2(y_1+y_2)+z_1z_2$	$x_1y_2+x_2y_3+x_3(y_1+y_3)$

Concentrate on the case $m = 3$, $k = 0$. We have two canonical functions $\mathbf{y}Q\mathbf{x}^{\mathrm{T}}$ and $\mathbf{y}\tilde{Q}\mathbf{x}^{\mathrm{T}}$, where

$$Q = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad \tilde{Q} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

Let I_r be the identity $r \times r$ matrix. The characteristic polynomial of $Q + I_3$ coincides with the characteristic polynomial of $\tilde{Q}$ and we can choose an invertible matrix S such that

$$S^{-1}(\tilde{Q} + I_3)S = Q.$$

It means that by adding the function $\mathbf{x} \cdot \mathbf{y}$ to $\mathbf{y}\tilde{Q}\mathbf{x}^{\mathrm{T}}$ and then applying the transformation $(\mathbf{x}, \mathbf{y}) \mapsto (\mathbf{x}S^{\mathrm{T}}, \mathbf{y}S^{-1})$ of $\mathrm{Stab}_{\mathbf{AGL_6}}(\mathbf{x} \cdot \mathbf{y})$, we get the function $\mathbf{y}Q\mathbf{x}^{\mathrm{T}}$.

Using the example above, we immediately obtain the following result that actually contains refinements of the functions f_1, f_2, f_3 from the previous section.

Proposition 3. *Let $f(u, v, x_1, \ldots, x_6)$ be a cubic bent function of the form* (2)*. Then f is affine equivalent to one of the following functions:*

$$\begin{aligned}
&u(x_1x_2 + v) + x_1x_3 + x_2x_4 + x_5x_6, \\
&u(x_1x_2 + x_3x_4 + v) + x_1x_4 + x_2x_5 + x_3x_6, \\
&u(x_1x_2 + x_3x_4 + v) + x_1x_4 + x_3(x_2 + x_4) + x_5x_6, \\
&u(x_1x_2 + x_3x_4 + x_5x_6 + v) + x_1x_4 + x_3x_6 + x_5(x_2 + x_4).
\end{aligned}$$

Now, to complete the affine classification of $\mathcal{B}_8$, it remains to refine quadratic parts of the functions f_4 and f_5. Note that every cubic monomial of these functions contains at least one of the variables x_1, x_4 (or, for example, x_2, x_4) and it is promising to use 4-row bent rectangles for the classification.

3 Proofs

Proof of Proposition 1

Let $f \in \mathcal{B}_n$. Define the function $g \in \mathcal{F}_n$ by the rule

$$\chi(g(\mathbf{v}, \mathbf{u})) = 2^{-n/2} \hat{f}(\mathbf{u}, \mathbf{v}), \quad \mathbf{u} \in V_k, \quad \mathbf{v} \in V_m,$$

and determine the corresponding rectangle $\overset{\square}{g} \in \overset{\square}{\mathcal{F}}_{k,m}$:

$$\begin{aligned}\overset{\square}{g}(\mathbf{v},\mathbf{u}) &= 2^{-n/2} \sum_{\mathbf{x}\in V_m} \hat{f}(\mathbf{x},\mathbf{v})\chi(\mathbf{u}\cdot\mathbf{x}) \\ &= 2^{-n/2} \sum_{\mathbf{x}\in V_m} \sum_{\mathbf{w}\in V_m} \sum_{\mathbf{y}\in V_k} \chi(f(\mathbf{w},\mathbf{y}) + \mathbf{x}\cdot\mathbf{w} + \mathbf{v}\cdot\mathbf{y} + \mathbf{u}\cdot\mathbf{x}) \\ &= 2^{-n/2} \sum_{\mathbf{y}\in V_k} \sum_{\mathbf{w}\in V_m} \chi(f(\mathbf{w},\mathbf{y}) + \mathbf{v}\cdot\mathbf{y}) \sum_{\mathbf{x}\in V_m} \chi((\mathbf{w}+\mathbf{u})\cdot\mathbf{x}).\end{aligned}$$

Since for $\mathbf{a} \in V_m$,

$$\sum_{\mathbf{x}\in V_m} \chi(\mathbf{a}\cdot\mathbf{x}) = \begin{cases} 2^m, & \mathbf{a} = \mathbf{0}, \\ 0 & \text{otherwise}, \end{cases}$$

we have

$$\overset{\square}{g}(\mathbf{v},\mathbf{u}) = 2^{m-n/2} \sum_{\mathbf{y}\in V_k} \chi(f(\mathbf{u},\mathbf{y}) + \mathbf{v}\cdot\mathbf{y}) = 2^{(m-k)/2}\, \overset{\square}{f}(\mathbf{u},\mathbf{v}).$$

Therefore, each column of $\overset{\square}{f}$ multiplied by $2^{(m-k)/2}$ is an element of $\overset{\wedge}{\mathcal{F}}_m$ and $\overset{\square}{f}$ is bent.

Conversely, if $\overset{\square}{f}$ is bent then $\overset{\square}{g}(\mathbf{v},\mathbf{u}) = 2^{(m-k)/2}\, \overset{\square}{f}(\mathbf{u},\mathbf{v})$ is well defined rectangle that corresponds to the function $g(\mathbf{v},\mathbf{u})$, $\chi(g(\mathbf{v},\mathbf{u})) = 2^{-n/2}\, \hat{f}(\mathbf{u},\mathbf{v})$. Hence $|\hat{f}(\mathbf{u},\mathbf{v})| = 2^{n/2}$ for all $\mathbf{u}$, $\mathbf{v}$ and f is bent.

Proof of Proposition 2

Let $f(u,v,\mathbf{x})$ have the form (2). Construct the rectangle $\overset{\square}{f} \in \overset{\square}{\mathcal{F}}_{1,n+1}$. The rows of $\overset{\square}{f}$ are results of applying the Walsh-Hadamard transform to the functions

$$f_1(v,\mathbf{x}) = b(0,v,\mathbf{x}), \quad f_2(v,\mathbf{x}) = a(v,\mathbf{x}) + b(1,v,\mathbf{x}).$$

The functions f_i are quadratic and Dickson's theorem yields

1) $|\hat{f}_i(\mathbf{w})| \in \{0, 2^{n+1-\operatorname{rank} f_i/2}\}$, $\mathbf{w} \in V_{n+1}$;

2) the supports $E_i \subset V_{n+1}$ of $\hat{f}_i$ are flats of dimensions $\operatorname{rank} f_i$.

Examining the restrictions on columns of $\overset{\square}{f}$, we conclude that $\overset{\square}{f}$ is bent iff $\dim E_{1,2} = n$ and $E_1 \cap E_2 = \varnothing$.

Using an affine transformation of $(v,\mathbf{x})$, we can make

$$E_1 = \{(0,\mathbf{x})\colon \mathbf{x} \in V_n\}, \quad E_2 = \{(1,\mathbf{x})\colon \mathbf{x} \in V_n\}.$$

It means that f is affine equivalent to the function

$$u(g_1(\mathbf{x}) + g_2(\mathbf{x}) + v) + g_1(\mathbf{x}), \quad g_i \in \mathcal{B}_n, \quad \deg g_i = 2.$$

Let $\operatorname{rank}(g_1+g_2)=2m$. Using an affine transformation of $\mathbf{x}$, we can convert $g_1(\mathbf{x})+g_2(\mathbf{x})$ to the form $h(\mathbf{x})+l(\mathbf{x})$, where $h(\mathbf{x})=x_1x_2+\ldots+x_{2m-1}x_{2m}$ and l is an affine function. Now replacing now v with $v+l$, we obtain the function

$$u(h(\mathbf{x})+v)+g(\mathbf{x}), \quad g, g+h \in \mathcal{B}_n, \quad \deg g = 2,$$

that is affine equivalent to f.

Proof of Lemma

We will use notations that can be easily understood by the following example: the transformation that replaces x_1 with x_1+x_2, y_2 with y_2+y_1 and does not change all other variables is denoted by $\{x_1 \curvearrowright x_1+x_2, y_2 \curvearrowright y_2+y_1\}$.

Start the proof with two auxiliary results.

Sublemma 1. *Any quadratic bent function $g(\mathbf{x},\mathbf{y})$, $\mathbf{x},\mathbf{y}\in V_m$, by a transformation of* $\mathrm{Stab}_{\mathbf{AGL}_{2m}}(\mathbf{x}\cdot\mathbf{y})$ *and addition of an affine function can be reduced to the form*

$$\mathbf{y}Q\mathbf{x}^{\mathrm{T}}, \quad Q=\operatorname{diag}(C_1,\ldots,C_d),$$

where C_i are invertible companion matrices with characteristic polynomials $p_i(\lambda)$ such that $p_1(\lambda)\mid p_2(\lambda)$, $p_2(\lambda)\mid p_3(\lambda),\ldots,$ $p_{d-1}(\lambda)\mid p_d(\lambda)$. The matrix Q is determined uniquely.

Proof. During the proof we will consecutively eliminate monomials x_ix_j and y_iy_j in g, then bring g to the form $\mathbf{y}Q\mathbf{x}^{\mathrm{T}}$ and prove the uniqueness of Q.

1. Write

$$g(\mathbf{x},\mathbf{y}) = x_1(a_2x_2+\ldots+a_mx_m+b_1y_1+b_2y_2+\ldots+b_my_m+c)+g_1(x_2,\ldots,x_m,\mathbf{y}).$$

If some of the coefficients a_i, b_i, $i=2,\ldots,m$, are nonzero, then by renumbering the variables x_i, y_i and interchanging x_2 and y_2 if necessary, we can make $b_2=1$.

Now by the transformations

(a) $\{x_1 \curvearrowright x_1+b_1x_2, y_2 \curvearrowright y_2+b_1y_1\}$,

(b) $\{y_2 \curvearrowright y_2+a_2x_2+a_2\}$,

(c) $\{y_2 \curvearrowright y_2+a_ix_i+b_iy_i+a_ib_i, x_i \curvearrowright x_i+b_ix_2, y_i \curvearrowright y_i+a_ix_2\}$, $i=3,\ldots,m$,

and addition of x_1 if necessary, we bring g to the form

$$x_1y_2+g_2(x_2,\ldots,x_m,\mathbf{y}).$$

Applying similar transformations to

$$g_2(x_2,\ldots,x_m,\mathbf{y}) = x_2(a_3'x_3+\ldots+a_m'x_m+b_1'y_1+\ldots+b_m'y_m+c')+g_3(x_3,\ldots,x_m,\mathbf{y})$$

and further, at some stage we get the function

$$x_1y_2 + x_2y_3 + \ldots + x_{r-1}y_r + x_r(\alpha_1y_1 + \ldots + \alpha_ry_r) + g_4(x_{r+1}, \ldots, x_m, \mathbf{y}).$$

2. Denote $\mathbf{x}_1 = (x_1, \ldots, x_r)$, $\mathbf{y}_1 = (y_1, \ldots, y_r)$ and rewrite this function as

$$\mathbf{y}_1C\mathbf{x}_1^{\mathrm{T}} + g_4(x_{r+1}, \ldots, x_m, \mathbf{y}),$$

where $C = C(\alpha_1, \ldots, \alpha_r)$ is a companion matrix.

The matrices C and C^{T} are similar, that is, there exists an invertible matrix S such that $S^{-1}CS = C^{\mathrm{T}}$. Using the transformation $\{\mathbf{x}_1 \curvearrowright \mathbf{y}_1S^{\mathrm{T}}, \mathbf{y}_1 \curvearrowright \mathbf{x}_1S^{-1}\}$, we bring g to the form

$$x_1y_2 + x_2y_3 + \ldots + x_{r-1}y_r + x_r(\alpha_1y_1 + \ldots + \alpha_ry_r) + g_5(\mathbf{x}, y_{r+1}, \ldots, y_m).$$

3. If g_5 contains the monomial x_1x_2, eliminate it by replacing y_2 with $y_2 + x_2 + 1$. Next eliminate the monomials x_1x_j, $3 \le j \le m$, by the transformations $\{y_2 \curvearrowright y_2+x_j, y_j \curvearrowright y_j+x_2\}$ and the monomials x_1y_j, $r+1 \le j \le m$, by the transformations $\{y_2 \curvearrowright y_2+y_j, x_j \curvearrowright x_j+x_2\}$.

In similar way we can eliminate the monomials x_2x_3, $\ldots$, x_2x_m, x_2y_{r+1}, $\ldots$, x_2y_m, x_3x_4, $\ldots$, $x_{r-1}x_r$, $x_{r-1}y_{r+1}$, $\ldots$, $x_{r-1}y_m$ and hence obtain the function

$$\begin{aligned} &x_1y_2 + x_2y_3 + \ldots + x_{r-1}y_r + x_r(\alpha_1y_1 + \ldots + \alpha_my_m + \beta_{r+1}x_{r+1} + \ldots + \beta_mx_m) \\ &\quad + g_6(x_{r+1}, \ldots, x_m, y_{r+1}, \ldots, y_m). \end{aligned}$$

If $\alpha_{r+1} = \ldots = \alpha_m = \beta_{r+1} = \ldots = \beta_m = 0$, we continue to eliminate monomials x_ix_j, y_iy_j in the function g_6 of a lesser number of variables. Otherwise, if some of the coefficients $\alpha_{r+1}, \ldots, \alpha_m$, $\beta_{r+1}, \ldots, \beta_m$ are nonzero, then return to step 1, bring g to the form

$$x_1y_2 + x_2y_3 + \ldots + x_{r'-1}y_{r'} + x_{r'}(\alpha_1'y_1 + \ldots + \alpha_{r'}'y_{r'}) + g_4'(x_{r'+1}, \ldots, x_m, \mathbf{y}), \quad r' > r,$$

and repeat steps 2, 3.

4. Using the manipulations above, we can eliminate all monomials x_ix_j, y_iy_j and bring g to the form $\mathbf{y}Q\mathbf{x}^{\mathrm{T}}$, where Q is an $m \times m$ matrix. Given an invertible matrix S of order m, we can replace $(\mathbf{x}, \mathbf{y})$ with $(\mathbf{x}S^{\mathrm{T}}, \mathbf{y}S^{-1})$ and thus pass from Q to the similar matrix $\tilde{Q} = S^{-1}QS$. Under an appropriate choice of S, we can bring Q to the Frobenius canonical form given in the statement.

On the other hand, if g is equivalent to $\mathbf{y}\tilde{Q}\mathbf{x}^{\mathrm{T}}$ under the action of $\mathrm{Stab}_{\mathbf{AGL}_{2m}}(\mathbf{x} \cdot \mathbf{y})$, then the matrices Q and $\tilde{Q}$ are similar. Indeed, the equivalence of $\mathbf{y}Q\mathbf{x}^{\mathrm{T}}$ and $\mathbf{y}\tilde{Q}\mathbf{x}^{\mathrm{T}}$ means that there exists an invertible matrix A of order $2m$ such that

$$A\begin{pmatrix} 0 & I_m \\ I_m & 0 \end{pmatrix}A^{\mathrm{T}} = \begin{pmatrix} 0 & I_m \\ I_m & 0 \end{pmatrix}, \quad A\begin{pmatrix} 0 & Q \\ Q^{\mathrm{T}} & 0 \end{pmatrix}A^{\mathrm{T}} = \begin{pmatrix} 0 & \tilde{Q} \\ \tilde{Q}^{\mathrm{T}} & 0 \end{pmatrix}.$$

Hence invariant polynomials of the λ-matrices

$$\begin{pmatrix} 0 & \lambda I_m + Q \\ \lambda I_m + Q^{\mathrm{T}} & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & \lambda I_m + \tilde{Q} \\ \lambda I_m + \tilde{Q}^{\mathrm{T}} & 0 \end{pmatrix}$$

are equal (see, for example, [3, ch. 6]). Consequently, invariant polynomials of the λ-matrices $\lambda I_m + Q$ and $\lambda I_m + \tilde{Q}$ are equal too, matrices Q, $\tilde{Q}$ are similar and have the same Frobenius canonical form. $\square$

Sublemma 2. *Any quadratic bent function $g(\mathbf{x}, \mathbf{y}, \mathbf{z})$, $\mathbf{x}, \mathbf{y} \in V_m$, $\mathbf{z} \in V_{2k}$, $k > 0$, that does not contain the monomials $z_i z_j$, $1 \le i < j \le 2k$, by a transformation of $\mathrm{Stab}_{\mathbf{AGL}_{2(m+k)}}(\mathbf{x} \cdot \mathbf{y})$ and addition of an affine function can be reduced to the form*

$$y_1 z_1 + x_1 y_2 + \ldots + x_{r-1} y_r + x_r z_2 + g'(x_{r+1}, \ldots, x_m, y_{r+1}, \ldots, y_m, z_3, \ldots, z_{2k}).$$

Proof. We divide the proof into four steps.

1. Since g does not contain the monomials $z_1 z_j$ and has full rank, g must contain at least one monomial of the form $x_i z_1$ or $y_i z_1$, say $y_1 z_1$. Write

$$g(\mathbf{x}, \mathbf{y}, \mathbf{z}) = (y_1 + l_1)(z_1 + l_2) + g_1(\mathbf{x}, y_2, \ldots, y_m, z_2, \ldots, z_{2k}),$$

where $l_1 = l_1(\mathbf{x}, y_2, \ldots, y_m)$ and $l_2 = l_2(\mathbf{x}, y_2, \ldots, y_m, z_2, \ldots, z_{2k})$ are affine functions. Replacing z_1 with $z_1 + l_2$, then using some of the transformations

(a) $\{y_1 \curvearrowright y_1 + x_1 + 1\}$,

(b) $\{y_1 \curvearrowright y_1 + x_i, y_i \curvearrowright y_i + x_1\}$, $2 \le i \le m$,

(c) $\{y_1 \curvearrowright y_1 + y_i, x_i \curvearrowright x_i + x_1\}$, $2 \le i \le m$,

and adding z_1 if necessary, we obtain the function

$$y_1 z_1 + g_2(\mathbf{x}, y_2, \ldots, y_m, z_2, \ldots, z_{2k}).$$

2. If g_2 does not contain the monomials $x_1 z_j$, then we proceed as in step 1 of the previous proof and bring g to the form

$$y_1 z_1 + x_1 y_2 + g_3(x_2, \ldots, x_m, y_2, \ldots, y_m, z_2, \ldots, z_{2k}).$$

Continuing with the function g_3 and further, at some stage we obtain one of the following functions:

$$\begin{aligned} y_1 z_1 + x_1 y_2 + \ldots + x_{r-1} y_r + x_r(\alpha_2 y_2 + \ldots + \alpha_r y_r) \\ + g_4(x_{r+1}, \ldots, x_m, y_2, \ldots, y_m, z_2, \ldots, z_{2k}), \end{aligned} \tag{4}$$

or

$$y_1z_1 + x_1y_2 + \ldots + x_{r-1}y_r + g_5(x_r, \ldots, x_m, y_2, \ldots, y_m, z_2, \ldots, z_{2k}), \tag{5}$$

where g_5 contains a monomial of the form x_rz_j, say x_rz_2.

Consider the function (4). If we replace x_i with $x_i + \alpha_{i+1}x_r$, $i = 1, \ldots, r-1$, we eliminate all monomials that contain x_r. Therefore the function (4) is not bent and we reject it.

Rewrite (5) as

$$y_1z_1 + x_1y_2 + \ldots + x_{r-1}y_r + (x_r + l_1)(z_2 + l_2) + g_6(x_{r+1}, \ldots, x_m, y_2, \ldots, y_m, z_3, \ldots, z_{2k}),$$

where $l_1 = l_1(x_{r+1}, \ldots, x_m, y_2, \ldots, y_m)$ and $l_2 = l_2(x_{r+1}, \ldots, x_m, y_2, \ldots, y_m, z_3, \ldots, z_{2k})$ are affine functions.

Replacing z_2 with $z_2 + l_2$, then using some of the transformations

(a) $\{x_r \curvearrowright x_r + x_i, y_i \curvearrowright y_i + y_r\}$, $r + 1 \le i \le m$,

(b) $\{x_r \curvearrowright x_r + y_i, x_i \curvearrowright x_i + y_r\}$, $2 \le i \le m$, $i \ne r$,

(c) $\{x_r \curvearrowright x_r + y_r + 1\}$,

and adding z_2 if necessary, we bring (5) to the form

$$y_1z_1 + x_1y_2 + \ldots + x_{r-1}y_r + x_rz_2 + g_7(x_{r+1}, \ldots, x_m, y_2, \ldots, y_m, z_3, \ldots, z_{2k}). \tag{6}$$

3. By the transformations $\{x_{r-1} \curvearrowright x_{r-1}+x_i, y_i \curvearrowright y_i+y_{r-1}\}$ eliminate the monomials y_rx_i, $r + 1 \le i \le m$, in (6). Next by the transformations $\{x_{r-1} \curvearrowright x_{r-1} + y_j, x_j \curvearrowright x_j + y_{r-1}\}$ eliminate the monomials y_ry_j, $2 \le j \le m$, $j \ne r-1$. The monomial $y_{r-1}y_r$ can be eliminated by replacing x_{r-1} with $x_{r-1} + y_{r-1} + 1$. In similar way consecutively eliminate all other monomials $y_{r-1}x_i, y_{r-1}y_j$, $\ldots$, y_2x_i, y_2y_j. Then eliminate possibly appeared monomials y_1x_i, y_1y_j by replacing z_1 with $z_1 + x_i$ or $z_1 + y_i$.

Finally we obtain the function

$$\begin{aligned} &y_1z_1 + x_1y_2 + \ldots + x_{r-1}y_r + x_rz_2 \\ &\quad + \sum_{i=2}^{r}\sum_{j=3}^{2k} a_{ij}y_iz_j + g'(x_{r+1}, \ldots, x_m, y_{r+1}, \ldots, y_m, z_3, \ldots, z_{2k}). \end{aligned} \tag{7}$$

4. If some of the coefficients a_{ij} are nonzero, then we proceed as follows

(a) interchange x_i and y_{r+1-i}, $i = 1, \ldots, r$,

(b) interchange z_1 and z_2,

(c) repeat step 2 and obtain the function

$$y_1z_1 + x_1y_2 + \ldots + x_{r'-1}y_{r'} + x_{r'}z_2 + g_7'(x_{r'+1}, \ldots, x_m, y_2, \ldots, y_m, z_3, \ldots, z_{2k}), \quad r' < r,$$

instead of (6),

(d) repeat steps 3, 4.

It is clear that after some iteration by the schema above we obtain the function of the form (7), where all the coefficients $a_{ij} = 0$. □

Return to the proof of Lemma. If g contains a monomial of the form z_iz_j, say z_1z_2, then we can write

$$g(\mathbf{x}, \mathbf{y}, \mathbf{z}) = (z_1 + l_1)(z_2 + l_2) + g_1(\mathbf{x}, \mathbf{y}, z_3, \ldots, z_{2k}),$$

where $l_1 = l_1(\mathbf{x}, \mathbf{y}, z_3, \ldots, z_{2k})$ and $l_2 = l_2(\mathbf{x}, \mathbf{y}, z_3, \ldots, z_{2k})$ are affine functions. Applying the transformation $\{z_1 \curvearrowright z_1 + l_1, z_2 \curvearrowright z_2 + l_2\}$, we bring g to the form

$$z_1z_2 + g_2(\mathbf{x}, \mathbf{y}, z_3, \ldots, z_{2k}).$$

In similar way we can isolate all other monomials of the form z_iz_j, then using sublemmas extract chains $\rho_i(\mathbf{x}_i, \mathbf{y}_i, z_{2i-1}, z_{2i})$ of ranks $2m_i + 2 \geq 4$ and finally fix the term $\mathbf{y}_{k+1}Q\mathbf{x}_{k+1}^{\mathrm{T}}$.

It remains to proof the uniqueness of the matrix Q. Let E and R be the square matrices of order $2(m+k)$ such that

$$(\mathbf{x}, \mathbf{y}, \mathbf{z})R(\mathbf{x}, \mathbf{y}, \mathbf{z})^{\mathrm{T}} = \sum_{i=1}^{k} \rho_i(\mathbf{x}_i, \mathbf{y}_i, z_{2i-1}, z_{2i}) + \mathbf{x}_{k+1}Q\mathbf{y}_{k+1}^{\mathrm{T}},$$
$$(\mathbf{x}, \mathbf{y}, \mathbf{z})E(\mathbf{x}, \mathbf{y}, \mathbf{z})^{\mathrm{T}} = \mathbf{x} \cdot \mathbf{y}.$$

Suppose that g can be reduced to yet another function

$$\sum_{i=1}^{k} \tilde{\rho}_i(\tilde{\mathbf{x}}_i, \tilde{\mathbf{y}}_i, z_{2i-1}, z_{2i}) + \tilde{\mathbf{x}}_{k+1}\tilde{Q}\tilde{\mathbf{y}}_{k+1}^{\mathrm{T}}, \quad \tilde{\mathbf{x}}_i, \tilde{\mathbf{y}}_i \in V_{\tilde{m}_i},$$

that represented by a matrix $\tilde{R}$. Repeating the arguments of step 4 of the proof of Sublemma 1, we conclude that invariant polynomials of the λ-matrices

$$S = \begin{pmatrix} 0 & R + \lambda E \\ R^{\mathrm{T}} + \lambda E & 0 \end{pmatrix}, \quad \tilde{S} = \begin{pmatrix} 0 & \tilde{R} + \lambda E \\ \tilde{R}^{\mathrm{T}} + \lambda E & 0 \end{pmatrix}$$

are coincide. To the chains ρ_i, $\tilde{\rho}_i$ there correspond blocks of S, $\tilde{S}$ such that all their invariant polynomials are equal to 1. It yields that invariant polynomials of the λ-matrices $Q + \lambda I_{m_{k+1}}$, $\tilde{Q} + \lambda I_{\tilde{m}_{k+1}}$ are equal and, consequently, $m_{k+1} = \tilde{m}_{k+1}$ and $Q = \tilde{Q}$.

References

1. S. V. Agievich. On the representation of bent functions by bent rectangles. In: *Probabilistic Methods in Discrete Mathematics: Proceedings of the Fifth International Petrozavodsk Conference (Petrozavodsk, June 1–6, 2000)*. Utrecht, Boston: VSP, pp. 121–135, 2002. Available at `http://arxiv.org/abs/math.CO/0502087`.

2. A. V. Cheremushkin. Methods of the affine and linear classification of binary functions. In: *Proceedings on discrete mathematics*, vol. 4, Moscow: Fizmatlit, pp. 273–314, 2001 (In Russian).

3. F. R. Gantmacher. *The theory of matrices*. NY: Chelsea Publishing Co., 1960.

4. X. Hou. *$GL(m, 2)$ acting on $R(r, m)/R(r-1, m)$*. Discrete Math., vol. 149, pp. 99–122, 1996.

5. X. Hou. *Cubic bent functions*. Discrete Math., vol. 89, pp. 149–161, 1998.

6. F. J. MacWilliams, N. J. A. Sloane. *Theory of error correction codes*. Amsterdam: North-Holland, 1977.

7. O. S. Rothaus. *On "bent" functions*. J. Comb. Theory, Ser. A, vol. 20, pp. 300–305, 1979.