Tatra Mt. Math. Publ. **33** (2006), 123–135

TATRA MOUNTAINS
Mathematical Publications

CLASSIFICATION OF BOOLEAN FUNCTIONS WITH RESPECT TO LINEAR EQUIVALENCE

Marcin Serwecinski

ABSTRACT. S-boxes are usually the only source of nonlinearity of block ciphers. So it is obvious that they should have good cryptographic properties. The linear and affine nonequivalence of the S-box coordinate functions is one of them.

In this paper we consider linear equivalence of Boolean functions. It could be described as group $\mathrm{GL}(n,2)$ action on the set of Boolean functions. We show how to derive the number of $\mathrm{GL}(n,2)$-orbits in the set of all Boolean functions and some of its proper subsets.

1. The cycle index of $\mathrm{GL}(n,2)$

This section contains basic definitions and facts about the cycle index. We especially investigate the cycle index of the general linear group $\mathrm{GL}(n,2)$ acting on the vector space $\mathbb{F}_2^n$.

We know that any permutation of a nonempty set X can be uniquely represented as a composition of disjoint cycles. Let j_k be the number of cycles of length k in this representation. Then the sequence $(j_1,\dots,j_{|X|})$ assigned to the permutation π is called a *cycle type of the permutation* π.

Let us consider an action of the group G on the nonempty set X. Action of the element $g\in G$ on the $x\in X$ will be denoted gx. Let $g\in G$. It is easy to see that the function $\varphi(g)$ defined as follows:

$$\varphi(g)(x)=gx\,,\qquad \text{for } x\in X\,,$$

is a permutation of the elements of the set X. The cycle index of the permutation $\varphi(g)$ will be denoted $\big(j_1(g),\dots,j_{|X|}(g)\big)$.

The cycle index of the group G acting on the set X is the polynomial $Z(G,X)\in\mathbb{Q}[x_1,\dots,x_{|X|}]$ defined by the formula

$$Z(G,X)\big(x_1,\dots,x_{|X|}\big)=\frac{1}{|G|}\sum_{g\in G}\prod_{i=1}^{|X|}x_i^{j_i(g)}\,.$$

2000 Mathematics Subject Classification: 05A15, 94A60.
Keywords: Boolean functions, cycle index, linear equivalence.

Observe that if $g_1, g_2 \in G$ are conjugate (i.e., there is $h \in G$ such that $g_2 = hg_1h^{-1}$), then permutations $\varphi(g_1)$ and $\varphi(g_2)$ have the same cycle type. Hence, the cycle index can be written in a more convenient way

$$\frac{1}{|G|}\sum_{C\in\mathcal{C}}|C|\prod_{i=1}^{|X|}x_i^{j_i(g_C)},$$

where $\mathcal{C}$ is the set of all conjugacy classes and g_C is a representative of the class $C \in \mathcal{C}$.

So, if we want to compute the cycle index $Z\big(\mathrm{GL}(n,2),\mathbb{F}_2^n\big)$, we have to determine the size of each conjugacy class and then find the cycle type of the permutation generated by a representative of each class. In the next part of this section we briefly show how the theory of rational canonical form can be applied to do this task. For more details on this topic we refer to [4], [5]. At the beginning let us introduce the following useful notation.

By the symbol $\mathrm{Aut}(\mathbb{F}_2^n)$ we denote the group of automorphisms of the vector space $\mathbb{F}_2^n$.

Let $\tau \in \mathrm{Aut}(\mathbb{F}_2^n)$ and let U be a subspace of $\mathbb{F}_2^n$. We say that the subspace $U < \mathbb{F}_2^n$ is *τ-invariant* if $\tau(U) \subset U$. Further let d be the dimension of the τ-invariant subspace U. We say that the subspace U is *τ-cyclic* if there exists a vector $v \in U$ such that the set $\{v, \tau(v),\ \tau^2(v),\ \ldots,\ \tau^{d-1}(v)\}$ forms a basis of the subspace U.

A nontrivial polynomial $\phi(x) = a_0 \oplus \sum_{i=1}^{n} a_i x^i \in \mathbb{F}_2[x]$ is called *an annihilating polynomial of automorphism τ* if and only if

$$\phi(\tau) := a_0 \cdot \mathrm{id}_{\mathbb{F}_2^n} \oplus \sum_{i=1}^{n} a_i \cdot \tau^i = \Theta,$$

where τ^i denotes the ith iteration of the automorphism τ.

Such polynomial of minimal degree is called a *minimal polynomial of the automorphism τ*.

Let k be a positive integer. Each sequence $\lambda = (\lambda_1, \ldots, \lambda_k) \in \mathbb{N}_0^k$ such that

$$k = \sum_{i=1}^{k} i\lambda_i$$

is called a cycle type of k.

Suppose that $q(x) = a_0 + a_1x + \cdots + a_{d-1}x^{d-1}$ is a polynomial with coefficient in $\mathbb{F}_2$. By *companion matrix of the polynomial q* we mean the matrix $C(q)$

defined in the following way

$$C(q) = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & a_0 \\ 1 & 0 & \cdots & 0 & 0 & a_1 \\ 0 & 1 & \cdots & 0 & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & a_{d-2} \\ 0 & 0 & \cdots & 0 & 1 & a_{d-1} \end{pmatrix}.$$

Let further $k \in \mathbb{N}$. *Hypercompanion matrix* of the polynomial q^k is the matrix $H(q^k)$ defined as follows

$$H(q^k) = \left.\begin{pmatrix} C(q) & 0 & 0 & \cdots & 0 & 0 \\ E_{1,d} & C(q) & 0 & \cdots & 0 & 0 \\ 0 & E_{1,d} & C(q) & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & & 0 & \cdots & C(q) & 0 \\ 0 & & 0 & \cdots & E_{1,d} & C(q) \end{pmatrix}\right\} \quad k \text{ times},$$

where $E_{1,d} = [e_{i,j}] \in M_{d\times d}(\mathbb{F}_2)$ is given by

$$e_{i,j} = \begin{cases} 1, & (i,j) = (1,d), \\ 0, & \text{otherwise}. \end{cases}$$

Let $\tau \in \mathrm{Aut}(\mathbb{F}_2^n)$ and $q = q_1^{k_1} \dots q_s^{k_s}$ be a minimal polynomial of τ such that the polynomial q_i is irreducible for $i = 1 \dots s$. From the theory of rational canonical form (see [1]) we know that vector space $\mathbb{F}_2^n$ can be represented as a direct sum of s τ-invariant subspaces U_i such that $q_i^{k_i}$ is a minimal polynomial of $\tau|_{U_i}$. On the other hand, each of these τ-invariant subspaces U_i is a direct sum of a few τ-cyclic subspaces $W_{i,j}$. The theorems presented bellow show how this decomposition can affect the matrix of the automorphism τ.

Theorem 1. *Let $q \in \mathbb{F}_2[x]$ be an irreducible polynomial of degree d and let $\tau \in \mathrm{Aut}(\mathbb{F}_2^{kd})$. If q^k is a minimal polynomial of τ, then there exist a basis and a cycle type $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_k)$ of k, such that the matrix of the automorphism τ has a block diagonal form*

$$D(q,\lambda) = \mathrm{diag}\big(\underbrace{C(q), \dots C(q)}_{\lambda_1}, \underbrace{H(q^2), \dots, H(q^2)}_{\lambda_2}, \dots, \underbrace{H(q^k), \dots, H(q^k)}_{\lambda_k}\big).$$

Using this theorem we finally get the following representation

THEOREM 2. *Let $q = q_1^{k_1} q_2^{k_2} \dots q_s^{k_s}$ be a minimal polynomial of $\tau \in \mathrm{Aut}(\mathbb{F}_2^n)$, such that polynomials q_i are distinct and irreducible. Then there exist a basis of $\mathbb{F}_2^n$ and sequences $\lambda^{(1)} = \big(\lambda_1^{(1)}, \dots, \lambda_{d_1}^{(1)}\big)$, ..., $\lambda^{(s)} = \big(\lambda_1^{(s)}, \dots, \lambda_{d_s}^{(s)}\big)$ such that the matrix of the automorphism τ has the form*

$$\mathrm{diag}\big(D(q_1, \lambda^{(1)}), D(q_2, \lambda^{(2)}), \dots, D(q_s, \lambda^{(s)})\big)\,,$$

where $\lambda^{(i)}$ is the cycle type of k_i, for $i = 1, \dots, s$.

We know that the matrices of the automorphism represented in different bases are conjugate. Thus each conjugacy class can be represented by a block diagonal matrix as in Theorem 2. Consequently, each conjugacy class of $\mathrm{GL}(n,2)$ can be uniquely represented by certain decomposition of the minimal polynomial of its representative. Next theorem shows how to determine the size of each conjugacy class.

THEOREM 3. (Kung [4]) Let $q \in \mathbb{F}_2[x]$ be an irreducible polynomial of degree d, and $\lambda = (\lambda_1, \dots, \lambda_k)$ be a cycle type of k. Then the size of the centralizer of $D(q, \lambda)$ in $\mathrm{GL}(n,2)$ is equal to

$$b(d, \lambda) := \prod_{i=1}^{k} \prod_{j=1}^{\lambda_i} \big(2^{d\mu_i} - 2^{d(\mu_i - j)}\big)\,,$$

where

$$\mu_i := \sum_{j=1}^{i} j\lambda_j + \sum_{j=i+1}^{k} i\lambda_j\,.$$

COROLLARY 1. *Let $q = q_1^{k_1} q_2^{k_2} \dots q_s^{k_s}$ be a minimal polynomial of $\tau \in \mathrm{Aut}(\mathbb{F}_2^n)$, where q_i are distinct and irreducible polynomials of degree d_i. Let further $\lambda^{(i)}$ be a cycle type of k_i for all $i = 1, \dots, s$. Then the size of conjugacy class of the matrix*

$$\mathrm{diag}\big(D(q_1, \lambda^{(1)}), D(q_2, \lambda^{(2)}), \dots, D(q_s, \lambda^{(s)})\big)$$

is equal to

$$\frac{|\mathrm{GL}(n,2)|}{\prod_{i=1}^{s} b(d_i, \lambda_i)}\,.$$

Next theorem shows how to determine the cycle index of the product of two groups from cycle indices of these groups. Let us consider finite sets $R \subset \mathbb{N}^n$, $S \subset \mathbb{N}^m$ and polynomials f, g with coefficient over $\mathbb{Q}$ defined as follows:

$$f(x_1, \dots, x_n) = \sum_{\vec{r} \in R} a_{\vec{r}} \prod_{i=1}^{n} x_i^{\vec{r}_i}\,,$$

$$g(x_1, \dots, x_m) = \sum_{\vec{s} \in S} b_{\vec{s}} \prod_{l=1}^{m} x_l^{\vec{s}_l}\,.$$

Then *the cross product of polynomials* f *and* g is the polynomial $f \times g \in \mathbb{Q}[x_1, \dots, x_{n \cdot m}]$ defined in the following way:

$$(f \times g)(x_1, \dots, x_{n \cdot m}) := \sum_{\vec{r} \in R} \sum_{\vec{s} \in S} a_{\vec{r}} b_{\vec{s}} \prod_{i=1}^{n} \prod_{l=1}^{m} x_i^{\vec{r_i}} \times x_l^{\vec{s_l}},$$

where

$$x_a^c \times x_b^d := x_{\mathrm{lcm}(a,b)}^{c \cdot d \cdot \gcd(a,b)}.$$

Theorem 4. *Let the group* G *act on the set* X*, and let the group* H *act on the set* Y*. Then the cycle index of the action defined as follows:*

$$(G \times H) \times (X \times Y) \ni \big((g,h),(x,y)\big) \longmapsto (gx, hy) \in X \times Y$$

is

$$Z(G \times H, X \times Y) = Z(G, H) \times Z(H, Y).$$

Using those notations we are finally able to describe $Z\big(\mathrm{GL}(n,2), \mathbb{F}_2^n\big)$ in a form proposed by Fripertinger in [5]. Let us consider a sequence $(q_1, \dots, q_{l_n})$ containing all irreducible polynomials over $\mathbb{F}_2$ of degree less or equal to n, different from the polynomial $f(x) = x$. Further let d_i be the degree of ith polynomial in the sequence, and let l_n be the length of the sequence.

Theorem 5. (See [3], [5].) *The cycle index* $Z\big(\mathrm{GL}(n,2), \mathbb{F}_2^n\big)$ *can be computed as*

$$\frac{1}{\big|\mathrm{GL}(n,2)\big|} \sum_{(k_1,\dots,k_{l_n})} \sum_{(\lambda^{(1)},\dots,\lambda^{(l_n)})} \frac{\big|\mathrm{GL}(n,2)\big|}{\prod\limits_{i=1}^{l_n} b\big(q_i, \lambda^{(i)}\big)} \times_{i=1}^{l_n} \times_{j=1}^{k_i} x_1 \prod_{k=1}^{j} \big(x_{e_{i,k}}^{a_{i,k}}\big)^{\times \lambda_j^{(i)}},$$

where

$$e_{i,k} = \min\{e \in \mathbb{N}\colon\ q_i^k \mid x^e - 1\}$$
$$a_{i,k} = \frac{2^{k d_i} - 2^{(k-1) d_i}}{e_{i,k}}.$$

The first sum is running over all $(k_1, \dots, k_{l_n}) \in \mathbb{N}_0^{l_n}$ *such that*

$$\sum_{i=1}^{l_n} d_i \cdot k_i = n.$$

The second sum is running over all $(\lambda^{(1)}, \dots, \lambda^{(l_n)})$ *such that* $\lambda^{(i)}$ *is a cycle type of* k_i *for all* $i = 1, \dots, l_n$.

2. The number of equivalence classes of $\mathfrak{B}_n$, $\mathfrak{B}_n^k$, $\mathfrak{B}_n^{\deg(n)}$, $R(m,n)$, $R(r,n)/R(m,n)$

In this section $Z\big(\mathrm{GL}(n,2)\big)$ denotes the cycle index of the group $\mathrm{GL}(n,2)$ acting on the set $\mathbb{F}_2^n$.

Let $\mathfrak{B}_n$ denote the set of all Boolean functions over $\mathbb{F}_2^n$. We can consider the group $\mathrm{GL}(n,2)$ action on the set $\mathfrak{B}_n$ defined as follows:

$$A \cdot f = f(A^{-1}x), \qquad \text{for all } x \in \mathbb{F}_2^n,$$

where $f \in \mathfrak{B}_n$ and $A \in \mathrm{GL}(n,2)$.

We say that Boolean functions f and g are linearly equivalent if and only if they belong to the same orbit of the action of $\mathrm{GL}(n,2)$ on the set $\mathfrak{B}_n$.

Theorem 6. (See [3].) *The number of equivalence classes in $\mathfrak{B}_n$ equals*

$$Z\big(\mathrm{GL}(n,2)\big)(2,\dots,2).$$

It is easy to see that some properties of Boolean functions, like Hamming weight, algebraic degree and nonlinearity, are invariant under the action of the group $\mathrm{GL}(n,2)$. So, it seems to be sensible to consider action of the group $\mathrm{GL}(n,2)$ on a family of Boolean functions with the given property.

Let $\mathrm{hwt}(f)$ denote the Hamming weight of the function $f \in \mathfrak{B}_n$, and let $\deg(f)$ denote the degree of a function $f \in \mathfrak{B}_n$ represented as a polynomial in the algebraic normal form. Then we define

$$\mathfrak{B}_n^k := \big\{f \in \mathfrak{B}_n : \mathrm{hwt}(f) = k\big\},$$
$$\mathfrak{B}_n^{\deg(k)} := \big\{f \in \mathfrak{B}_n : \deg(f) = k\big\},$$
$$R(k,n) := \big\{f \in \mathfrak{B}_n : \deg(f) \leqslant k\big\}.$$

In the next theorems we show how one can use the cycle index $Z\big(\mathrm{GL}(n,2)\big)$ to compute the number of equivalence classes in the set $\mathfrak{B}_n^k$. At the beginning let us introduce a few useful notations.

- Let t_k be the number of equivalence classes in $\mathfrak{B}_n^k$. By $T(x) = \sum\limits_{i=1}^{\infty} t_k x^k$ we mean the generating function of the sequence $(t_k\colon k = 1, 2\dots)$.
- Let $f \in \mathbb{F}_2[x_1,\dots,x_n]$. By $\mathrm{Coef}_{(\alpha_1,\dots,\alpha_n)}(f)$ we denote the coefficient of the monomial $x_1^{\alpha_1}\dots x_n^{\alpha_n}$ taken from the polynomial f.
- Let $f \in \mathbb{F}_2[x_1,\dots,x_n]$ be a polynomial of the form

  $$f(x_1,\dots,x_n) := \sum_{(k_1,\dots,k_n)\in\mathbb{N}_0^n} a_{(k_1,\dots,k_n)} x_1^{k_1}\dots x_n^{k_n}.$$

  We denote by $f[x+1]$ the polynomial defined as follows:

  $$f[x+1](x) := \sum_{(k_1,\dots,k_n)\in\mathbb{N}_0^n} a_{(k_1,\dots,k_n)}(1+x)^{k_1}(1+x^2)^{k_2}\dots(1+x^n)^{k_n}.$$

THEOREM 7. *The number of equivalence classes in* $\mathfrak{B}_n^k$ *is equal to*

$$\mathrm{Coef}_{(k)}\big(Z\big(\mathrm{GL}(n,2)\big)[x+1]\big)\,.$$

P r o o f . Using Polya's theorem (see [KLIN]) we get immediately that

$$T(x) = Z\big(\mathrm{GL}(n,2)\big)[x+1](x)\,.$$

Hence $t_k = \mathrm{Coef}_{(k)}\big(Z\big(\mathrm{GL}(n,2)\big)[x+1]\big)$. □

This number can be computed more directly in the following way:

THEOREM 8. *The number of equivalence classes in* $\mathfrak{B}_n^k$ *is equal to*

$$\frac{1}{\big|\mathrm{GL}(n,2)\big|} \sum_{(\alpha_1,\dots,\alpha_{2^n})\in\mathbb{N}_0^n} \mathrm{Coef}_{(\alpha_1,\dots,\alpha_{2^n})}\big(Z\big(\mathrm{GL}(n,2)\big)\big) \sum_{(\beta_1,\dots,\beta_{2^n})} \binom{\alpha_1}{\beta_1}\cdots\binom{\alpha_{2^n}}{\beta_{2^n}}\,,$$

where the second sum is running over all 2^n*-tuples* $(\beta_!,\dots,\beta_{2^n})$ *such that*

$$\sum_{i=1}^{2^n} i\beta_i = k \quad \text{and} \quad 0 \leqslant \beta_1 \leqslant \alpha_1\,,\dots,\, 0 \leqslant \beta_{2^n} \leqslant \alpha_{2^n}\,.$$

P r o o f . Let $A \in \mathrm{GL}(n,2)$ and let $(\alpha_1,\dots,\alpha_{2^n})$ be a cycle type of the permutation $\varphi(A)$. Note that $f \in \mathrm{Fix}_{\mathfrak{B}_n^k}(A)$ if and only if f is constant on each cycle of the permutation $\varphi(A)$ and $\mathrm{hwt}(f) = k$. So it is easy to see that for each sequence $(\beta_1,\dots,\beta_{2^n})$ such that

$$\sum_{i=1}^{2^n} i\beta_i = k\,, \qquad \text{where } 0 \leqslant \beta_1 \leqslant \alpha_1\,,\dots,\, 0 \leqslant \beta_{2^n} \leqslant \alpha_{2^n}\,,$$

there exist exactly

$$\binom{\alpha_1}{\beta_1}\cdots\binom{\alpha_{2^n}}{\beta_{2^n}}$$

Boolean functions, which take one on β_1 cycles of length 1, β_2 cycles of length $2,\dots,$ β_{2^n} cycles of length 2^n. It is obvious that the Hamming weight of functions constructed in that way is equal to k. Hence

$$\big|\mathrm{Fix}_{\mathfrak{B}_n^k}(A)\big| = \sum_{\substack{(\beta_1,\dots,\beta_{2^n})\\ 0\leqslant\beta_1\leqslant\alpha_1,\dots,\,0\leqslant\beta_{2^n}\leqslant\alpha_{2^n}\\ \sum_i i\beta_i = k}} \binom{\alpha_1}{\beta_1}\cdots\binom{\alpha_{2^n}}{\beta_{2^n}}\,.$$

To finish the proof note that there exist exactly $\mathrm{Coef}_{(\alpha_1,\dots,\alpha_{2^n})}\big(Z\big(\mathrm{GL}(n,2)\big)\big)$ matrices $A \in \mathrm{GL}(n,2)$ such that $(\alpha_1,\dots,\alpha_{2^n})$ is a cycle type of the permutation $\varphi(A)$. □

In a similar way we get the following theorem

Theorem 9. *The number of equivalence classes in* $\mathfrak{B}_n^{\deg(n)}$ *is equal to*

$$\frac{1}{\left|\mathrm{GL}(n,2)\right|} \sum_{(\alpha_1,\ldots,\alpha_{2^n})\in\mathbb{N}_0^n} \mathrm{Coef}_{(\alpha_1,\ldots,\alpha_{2^n})}\big(Z\big(\mathrm{GL}(n,2)\big)\big)\cdot 2^{\alpha_E} \sum_{i=1,3,\ldots,2^n-1} \binom{\alpha_O}{i},$$

where $\alpha_O = \alpha_1+\alpha_3+\cdots+\alpha_{2^n-1}$ *and* $\alpha_E = \alpha_2+\alpha_4+\cdots+\alpha_{2^n}$.

Proof. At the beginning note the following simple facts:

- If the Hamming weight of $f, g \in \mathfrak{B}_n$ is even, then the Hamming weight of $f\oplus g$ is even too.
- Let $\{k_1,\ldots,k_s\} \subsetneq \{1,\ldots,n\}$. The Hamming weight of a Boolean function $f(x_1,\ldots,x_n) = x_{k_1}\cdot\ldots\cdot x_{k_s}$ is even.
- Let $f(x_1,\ldots,x_n) = x_1\cdot\ldots\cdot x_n$ be a Boolean function. Then $f(x) = 0$ if and only if $x = (1,1,\ldots,1)$.

Observe that each Boolean function of degree less than n can be represented as a sum of its monomial. We can infer from this that the Hamming weight of such a function is even.

On the other hand, if we add to a Boolean function a monomial $x_1\ldots x_n$, we change this function only on one argument. Thus

$$\deg(f) = n \iff \mathrm{hwt}(f) \text{ is odd}, \qquad \text{for } f\in\mathfrak{B}_n.$$

Using this we get the Boolean function $f\in \mathrm{Fix}_{\mathfrak{B}_n^{\deg(n)}}(A)$ if and only if f is constant on each cycle of the permutation $\varphi(A)$, and takes one on the odd number of the odd-length cycles. So, if the cycle type of the permutation $\varphi(A)$ is $(\alpha_1,\ldots,\alpha_{2^n})$, then

$$\left|\mathrm{Fix}_{\mathfrak{B}_n^{\deg(n)}}(A)\right| = 2^{\alpha_2+\alpha_4+\cdots+\alpha_{2^n}} \sum_{i=1,3,\ldots,2^n-1} \binom{\alpha_1+\alpha_3+\cdots+\alpha_{2^n-1}}{i}.$$

□

Let $\mathcal{P}_k(n)$ be a family of all at most k-element subsets of $\{1,\ldots,n\}$. It is obvious that $R(k,n)$ can be seen as a vector space over $\mathbb{F}_2$. The basis of $R(k,n)$ is

$$\mathfrak{R} = \left\{\prod_{i\in S} x_i \colon S\in\mathcal{P}_k(n)\right\}.$$

We assume that $\prod_{i\in\emptyset} x_i = 1$.

Observe that $\dim\big(R(k,n)\big)$ equals $W = \binom{n}{k}+\binom{n}{k-1}+\cdots+\binom{n}{1}+1$. Note that the action of $A\in\mathrm{GL}(n,2)$ on $R(k,n)$ is really a linear isomorphism of the vector space $R(k,n)$. Let $C^r(A)$ be a matrix of this isomorphism with respect to the basis $\mathfrak{R}$.

The observation above, under the notation from Theorem 5, leads us to the following formula

Theorem 10. *Let $1 \leqslant k \leqslant n$. The number of equivalence classes in $R(k,n)$ is equal to*

$$\frac{1}{\left|\mathrm{GL}(n,2)\right|} \sum_{(k_1,\dots,k_{l_n})} \sum_{(\lambda^{(1)},\dots,\lambda^{(l_n)})} \frac{\left|\mathrm{GL}(n,2)\right|}{\prod_{i=1}^{l_n} b(q_i,\lambda^{(i)})} 2^{W-\mathrm{rank}(C^r(A)-I_W)},$$

where $W = \binom{n}{k}+\binom{n}{k-1}+\dots+\binom{n}{1}+1$ and $A = \mathrm{diag}\big(D(q_1,\lambda^{(1)}),\dots,D(q_{l_n},\lambda^{(l_n)})\big)$. The first sum is running over all $(k_1,\dots,k_{l_n}) \in \mathbb{N}_0^{l_n}$ such that

$$\sum_{i=1}^{l_n} d_i \cdot k_i = n\,.$$

The second sum is running over all $(\lambda^{(1)},\dots,\lambda^{(l_n)})$ such that $\lambda^{(i)}$ is a cycle type of k_i for all $i=1,\dots,l_n$.

Proof. It is easy to see that for any $A \in \mathrm{GL}(n,2)$

$$\begin{aligned}\left|\mathrm{Fix}_{R(k,n)}(A)\right| &= \left|\left\{f \in R(k,n)\colon A\cdot f = f\right\}\right| \\ &= \left|\ker\big(C_W(A)-I_W\big)\right| = 2^{W-\mathrm{rank}(C_W(A)-I_W)}\,.\end{aligned}$$

So, using Burnside's lemma, Theorem 3 and notations from Theorem 5 we easily get the formula from the thesis. □

Let $n(B)$ denote the number of equivalence classes in the set B with respect to linear equivalence. At the beginning of this section we observe, that the action of the matrix $A \in \mathrm{GL}(n,2)$ on the Boolean function $f \in \mathfrak{B}_n$ doesn't change the degree of the function f. So, it is easy to see the following

Corollary 2. *The number of equivalence classes in $\mathfrak{B}_n^{\deg(k)}$ is equal to*

$$n\big(R(k,n)\big) - n\big(R(k-1,n)\big)\,.$$

Let $r \leqslant m \leqslant n$ be positive integers. A linear equivalence of the Boolean functions can be extended in the natural way on the set $R(m,n)/R(k,n)$. Indeed, we would say that $f \in R(m,n)$ and $g \in R(m,n)$ are linearly equivalent with respect to $R(m,n)/R(r,n)$ if there exists a matrix $A \in \mathrm{GL}(n,2)$ such that

$$(A\cdot f) \oplus g \in R(r,n)\,.$$

Let $\mathcal{P}_{(r,m)}(n)$ be the set of all at last $r+1$ and at most m-element subsets of $\{1,\dots,n\}$. Similarly like above, an action of $A \in \mathrm{GL}(n,2)$ on $R(m,n)/R(r,n)$ is in fact a linear isomorphism of $R(m,n)/R(r,n)$ treated as a vector space with the base

$$\mathfrak{R} = \left\{\prod_{i\in C} X_i + R(r,n)\colon C \in \mathcal{P}_{(r,m)}(n)\right\}.$$

Let $C^{(r,m)}$ be a matrix of this isomorphism with respect to the base $\mathfrak{R}$.

Using the same notations and arguments as in Theorem 10 we can prove the following

Theorem 11. *The number of equivalence classes in $R(m,n)/R(r,n)$ is equal to*

$$\frac{1}{\bigl|\mathrm{GL}(n,2)\bigr|}\sum_{(k_1,\dots,k_{l_n})}\sum_{(\lambda^{(1)},\dots,\lambda^{(l_n)})}\frac{\bigl|\mathrm{GL}(n,2)\bigr|}{\prod_{i=1}^{l_n} b\bigl(q_i,\lambda^{(i)}\bigr)}\cdot 2^{W-\mathrm{rank}(C^{(r,m)}(A)-I_W)},$$

where $W=\binom{n}{m}+\binom{n}{m-1}+\dots+\binom{n}{k+1}$ *and* $A=\mathrm{diag}\bigl(D\bigl(q_1,\lambda^{(1)}\bigr),\dots,D\bigl(q_{l_n},\lambda^{(l_n)}\bigr)\bigr)$. *The first sum is running over all* $(k_1,\dots,k_{l_n})\in\mathbb{N}_0^{l_n}$ *such that*

$$\sum_{i=1}^{l_n} d_i\cdot k_i = n\,.$$

The second sum is running over all $(\lambda^{(1)},\dots,\lambda^{(l_n)})$ *such that* $\lambda^{(i)}$ *is a cycle type of* k_i *for all* $i=1,\dots,l_n$.

Appendix

Using formulas presented above we determine the number of equivalence classes in sets $\mathfrak{B}_n$, $\mathfrak{B}_n^k$, $\mathfrak{B}_n^{\deg(k)}$ and $R(r,n)/R(m,n)$ for $n \leqslant 9$. The results are gathered in tables presented bellow.

It is worth to note at this moment, that due to Xiang-Dong Hou [6]

$$n\big(R(r,m)/R(r-1,m)\big) = n\big(R(m-r,m)/R(m-r-1,m)\big)\,.$$

This observation reduces the number of cases which need to be computed.

Table 1. The number of equivalence classes in $\mathfrak{B}_n$.

n	$n(\mathfrak{B}_n)$
1	4
2	8
3	20
4	92
5	2 744
6	950 998 216
7	2 076 795 963 681 989 019 155 896
8	21 651 217 007 530 946 175 606 768 762 255 421 159 692 845
	640 522 169 779 616
9	19 164 625 518 533 795 827 661 741 108 695 400 180 191 405
	615 589 638 483 112 955 504 956 683 835 092 273 159 898 364
	755 826 684 230 506 355 795 035 616 608 356 302 228 832

Table 2. The number of equivalence classes in $\mathfrak{B}_n^k$.

n/k	1	2	3	4	5	6	7	8	9	10	11	12
1	2											
2	2	2	2	1								
3	2	2	3	4	3	2	2	1				
4	2	2	3	5	7	9	11	12	11	9	7	5
5	2	2	3	5	8	14	23	35	55	84	117	158
6	2	2	3	5	8	15	29	54	107	227	495	1 131
7	2	2	3	5	8	15	30	61	135	329	887	2 728
8	2	2	3	5	8	15	30	62	143	368	1 070	3 700
9	2	2	3	5	8	15	30	62	144	377	1 122	4 010

Table 3. The number of equivalence classes in $\mathfrak{B}_n^{\deg(k)}$.

n	k	$n\big(\mathfrak{B}_n^{\deg(k)}\big)$
3	2	3
3	3	5
4	2	5
4	3	16
4	4	23
5	2	6
5	3	80
5	4	598
5	5	686
6	2	8
6	3	757
6	4	3 939 543
6	5	233 809 244
6	6	237 749 554
7	2	9
7	3	80 815
7	4	1 934 414 690 956 432
7	5	4 056 247 857 394 100 638 856
7	6	515 142 741 128 688 463 112 860
7	7	519 198 990 920 497 254 788 974
8	2	11
8	3	937 791 544
8	4	1 093 107 121 512 362 512 031 910 472 063
8	5	78 766 668 621 158 799 536 752 313 300 299 154 591 345 413 964
8	6	21 143 766 530 150 308 123 368 588 373 980 747 176 141 860 582 839 263 092
8	7	5 391 660 485 273 819 567 157 164 801 560 015 107 934 407 882 923 509 504 228
8	8	5 412 804 251 882 736 543 901 692 190 563 855 289 923 211 410 130 542 444 904
9	2	12
9	3	973 026 584 921 804
9	4	82 754 468 136 661 651 120 435 283 949 988 112 136 021 307 592 798 166
9	5	7 039 971 572 706 602 949 455 989 138 811 171 881 353 315 052 127 268 322 165 692 962 971 764 363 400 891 572 275 686 892
9	6	136 172 854 457 568 318 961 063 909 838 382 488 184 202 549 582 743 203 174 673 459 962 519 002 932 977 476 295 802 119 457 566 273 228 112 409 280 081 804
9	7	9 357 727 303 835 407 139 517 891 206 769 115 535 728 761 108 966 217 577 031 288 299 251 402 179 008 252 972 056 815 209 934 681 645 153 230 334 333 001 333 404 762 520
9	8	4 781 798 652 329 477 376 921 459 817 648 119 865 595 244 288 727 552 597 702 168 855 597 933 711 252 661 448 479 337 466 297 154 445 615 056 399 675 805 152 439 937 306 008
9	9	4 791 156 379 633 448 956 915 435 277 173 850 045 047 851 403 897 409 620 778 238 876 239 170 958 773 068 289 974 591 188 956 671 057 626 588 948 758 904 152 089 075 557 208

TABLE 4. The number of equivalence classes in $R(r,n)/R(r-1,n)$.

n	r		n	r	
6	1	2	8	2	5
6	2	4	8	3	32
6	3	6	8	4	999
7	1	2	9	1	2
7	2	4	9	2	5
7	3	12	9	3	349
8	1	2	9	4	121 597 673 132 830

TABLE 5. The number of equivalence classes in $R(r,n)/R(r-2,n)$.

n	r		n	r	
6	6	4	8	6	3 796 971
6	5	10	8	5	15 906 817 974 000 898 238
6	4	85	9	9	4
7	7	4	9	8	14
7	6	11	9	7	1 901 080 489 588
7	5	1 596	9	6	2 352 023 447 452 061 418 406 916
7	4	7 384 214			942 567 657 188 954
8	8	4	9	5	10 344 308 517 082 634 461 072 433
8	7	13			388 471 967 127 642 980 660 605 202

REFERENCES

[1] LANG, S.: *Algebra*, Addison–Wesley Publishing Company, Inc., 1965.

[2] KLIN, M. CH.—PÖSCHEL, R.—ROSENBAUM, K.: *Angewandte Algebra für Mathematiker und Informatiker*, Deutcher Verlag der Wissenschaften, Berlin, 1988.

[3] HARRISON, M. A.: *On the classification of Boolean functions by the general linear and affine groups*, J. Soc. Appl. Ind. Math. **12** (1964), 285–299.

[4] KUNG, J. P. S.: *The cycle structure of a linear transformation over a finite field*, Linear Algebra Appl. **36** (1981), 141–155.

[5] FRIPERTINGER, H.: *Cycle indices of linear, affine and projective groups*, Linear Algebra Appl. **263** (1997), 133–156.

[6] XIANG-DONG HOU: $\mathrm{GL}(m,2)$ *acting on* $R(r,m)/R(r-1,m)$, Discrete Math. **149** (1996), 99–122.

Received November 15, 2004

Institute of Mathematics
University of Silesia
ul. Bankowa 14
PL–40-007 Katowice
POLAND
E-mail: ptasiek@ux2.math.us.edu.pl