A new class of monomial bent functions

Anne Canteaut*, Pascale Charpin* and Gohar M. Kyureghyan†
*INRIA projet CODES, B.P. 105, 78153 Le Chesnay Cedex, France
{Anne.Canteaut, Pascale.Charpin}@inria.fr
†Department of Mathematics, Otto-von-Guericke University of Magdeburg,
Universitätplatz 2, 39106 Magdeburg, Germany
Gohar.Kyureghyan@Mathematik.Uni-Magdeburg.DE

***Abstract*— We study the Boolean functions on $\mathbf{F}_{2^n}$, $n = 6r$, of the form $x \mapsto Tr(\lambda x^d)$ with $d = 2^{2r} + 2^r + 1$. Our main result is the characterization of those λ for which they are bent.**

I. Introduction

A number of recent papers are devoted to the characterization of new classes of bent functions. The main purpose could be to determine such functions which do not belong to the main known classes, for instance, in order to exhibit non-normal bent functions [3] or to construct bent functions by concatenating quadratic functions [4]. Another purpose consists in finding new expressions of bent functions. It is essentially the expressions by means of trace-functions which are considered in [7], [8], [9]. More generally, considering any polynomial $P(x)$ in $\mathbf{F}_{2^n}[x]$, it can be viewed as function with n inputs and n outputs. The properties of P are then studied by means of their 2^n component functions, the Boolean functions $x \mapsto Tr(\lambda P(x))$ where Tr is the trace function from $\mathbf{F}_{2^n}$ to $\mathbf{F}_2$. Determining the weights of these functions is of great interest in coding theory and cryptography (see [1], [7] and [5], for instance).

Our paper has to be replaced in this context. The general purpose is to study the so-called *monomial* functions, that is the functions $x \mapsto Tr(\lambda x^d)$ on $\mathbf{F}_{2^n}$, notably to determine for which λ they are bent. Here $n = 6r$, for some integer $r > 1$, and we study, for $\lambda \in \mathbf{F}_{2^n}^*$, the functions :

$$f_\lambda(x) = Tr(\lambda x^d),\ d = 2^{2r} + 2^r + 1. \quad (1)$$

We first prove that the weight of f_λ takes only three values when λ runs through $\mathbf{F}_{2^n}^*$, one of them corresponding to the bent case. We later describe the set of those λ such that f_λ is bent and we prove that these functions are Maiorana and McFarland bent functions. Moreover, we prove that a part of them form a subspace of dimension $2r$ of bent functions of degree 3. We also give the spectra of the derivatives of the functions f_λ.

This paper is an extended abstract. Some proofs are omitted. The proofs which are given are generally sketches of proofs.

II. Preliminaries

In the whole paper, α is a primitive root of $\mathbf{F}_{2^n}$. The linear Boolean functions on $\mathbf{F}_{2^n}$ are the functions

$$\varphi_a \ :\ x \mapsto Tr(ax),\ a \in \mathbf{F}_{2^n}^*,$$

We use notation Tr for the trace function on $\mathbf{F}_{2^n}$. But, for any k dividing n and $n = uk$, we denote as follows the trace function from $\mathbf{F}_{2^n}$ to $\mathbf{F}_{2^k}$:

$$T_k^n(\beta) = \beta + \beta^{2^k} + \ldots + \beta^{2^{k(u-1)}}.$$

For any Boolean function f on $\mathbf{F}_{2^n}$, we denote by $\mathcal{F}(f)$ the following value related to the Walsh transform of f:

$$\mathcal{F}(f) = \sum_{x \in \mathbf{F}_{2^n}} (-1)^{f(x)} = 2^n - 2wt(f)\ , \quad (2)$$

where $wt(f)$ is the Hamming weight of f, i.e., the number of $x \in \mathbf{F}_{2^n}$ such that $f(x) = 1$. The function f is said to be *balanced* if and only if $\mathcal{F}(f) = 0$ or, equivalently, $wt(f) = 2^{n-1}$. The *Walsh spectrum* of f is the multiset

$$\{\mathcal{F}(f + \varphi_a), a \in \mathbf{F}_{2^n}\}\ .$$

For even n, a function is *bent* if and only if its Walsh spectrum contains the values $\{\pm 2^{n/2}\}$ only.

A. The Maiorana and McFarland bent functions

The Maiorana and McFarland class of bent functions was introduced in [10] and extensively studied by Dillon [6]. It is usually called the *class* $\mathcal{M}$ of bent functions. By the next lemma, we give the expression of functions of $\mathcal{M}$ that we will use later.

Lemma 1: Let $n = 2t$ and $V = \mathbf{F}_{2^t}$. Let us denote by W a subspace of representatives of the cosets of V, that is $\mathbf{F}_{2^n} = \cup_{a \in W}(a + V)$. Define the functions

$$f \ :\ (x, a) \in V \times W \quad \mapsto \quad T_1^t\left(x\pi(a) + h(a)\right)$$

where π is a bijection from W to V and h is any function from W to V. Then f is a bent function which belongs to the class $\mathcal{M}$.

Remark 1: The previous lemma can be generalized by taking a *shift* of $\mathbf{F}_{2^t}$ instead of $\mathbf{F}_{2^t}$, *i.e.*, $V = \{0\} \cup \gamma\mathbf{F}_{2^t}^*$, $\gamma \notin \mathbf{F}_{2^t}^*$. In other terms, the *shifts* of the function f (of Lemma 1), the functions $y \mapsto f(\gamma y)$, are also in $\mathcal{M}$.

B. Definition of the class f_λ

From now on, we consider Boolean functions on $\mathbf{F}_{2^n}$ with $n = 6r$, $r > 1$. Note that,

$$2^n - 1 = (2^{3r} - 1)(2^{3r} + 1) = d(2^{2r} - 1)(2^{2r} - 2^r + 1).$$

Consider f_{α^i}, defined by (1), for $0 \le i \le d-1$. For any ℓ, $0 \le \ell \le (n/d)-1$, the function f_λ with $\lambda = \alpha^i \alpha^{\ell d}$ is a shift of f_{α^i}. Thus f_λ has the same Walsh spectrum as f_{α^i}. Let us define the set of *shifts* of α^i (modulo d) :

$$sh(i) = \{ \ \alpha^{i+\ell d} \mid 0 \le \ell \le (n/d)-1 \ \}.$$

The next lemma is obvious.

Lemma 2: For any i, $0 \le i \le d-1$, $sh(i) \cap \mathbf{F}_{2^{3r}}$ is not empty. Consequently, the subset of $\mathbf{F}_{2^{3r}}$

$$\{ \ \alpha^{j(2^{3r}+1)} \mid 0 \le j \le d-1 \ \}$$

is a set of representatives of the $sh(i)$.

According to the previous lemma, to study the spectra of all the functions f_λ, defined by (1), it is sufficient to study the functions

$$f_\lambda(x) = Tr(\lambda x^d), \ \begin{cases} d = 2^{2r}+2^r+1, \\ \lambda = \alpha^{j(2^{3r}+1)}, \\ 0 \le j \le d-1. \end{cases} \tag{3}$$

III. On the spectrum of the f_λ

In this section f_λ is defined by (3). We denote by β a primitive root of $\mathbf{F}_{2^{3r}}$ and let $\mathcal{G} = \langle \gamma \rangle$ be the subgroup of $\mathbf{F}_{2^n}$ of order $2^{3r}+1$. Since $gcd(2^{3r}+1, 2^{3r}-1) = 1$ then any nonzero $x \in \mathbf{F}_{2^n}$ can be written as follows:

$$x = yz \ , \quad y \in \mathbf{F}^*_{2^{3r}} \ \text{ and } \ z \in \mathcal{G}. \tag{4}$$

A. The weight of f_λ

Recall that $wt(f_\lambda)$ is the weight of f_λ. We are going to show that there are three possibilities only for $wt(f_\lambda)$ (Theorem 1).

Proposition 1: Let us define

$$L_\lambda = \{ \ z \in \mathcal{G} \mid T_r^{6r}(\lambda z^d) \ne 0 \ \}.$$

Then the weight of f_λ is $wt(f_\lambda) = d \ 2^{r-1} \# L_\lambda$.

Proof: Using (4), we express $wt(f_\lambda)$ as an integer sum on the pairs (y,z). We get

$$\begin{aligned} wt(f_\lambda) &= \sum_{x \in \mathbf{F}_{2^n}} Tr(\lambda x^d) = \sum_{z, \ y} Tr(\lambda (zy)^d) \\ &= \sum_{z \in \mathcal{G}} \sum_{y \in \mathbf{F}_{2^{3r}}} T_1^r \left(y^d T_r^{6r}(\lambda z^d) \right) \\ &= \sum_{z \in \mathcal{G}} d \sum_{\rho \in \mathbf{F}_{2^r}} T_1^r \left(\rho T_r^{6r}(\lambda z^d) \right) \\ &= \# L_\lambda \times d \times 2^{r-1}, \end{aligned}$$

∎

We denote by $\overline{L_\lambda}$ the set $\mathcal{G} \setminus L_\lambda$:

$$\overline{L_\lambda} = \{ \ z \in \mathcal{G} \mid T_r^{6r}(\lambda z^d) = 0 \ \}.$$

Lemma 3: Set, for any $\lambda \in \mathbf{F}_{2^{3r}}$,

$$N_\lambda = \{ \ y \in \mathbf{F}^*_{2^{3r}} \mid T_r^{3r}(\lambda y) = 0 \ \text{ and } \ T_1^{3r}(\frac{1}{y}) = 1 \ \}.$$

Then $\# \overline{L_\lambda} = 2 \times \# N_\lambda + 1$.

Theorem 1: The functions f_λ (and λ itself) are defined by (3). Let us denote by G_d the subgroup of order d of $\mathbf{F}^*_{2^{3r}}$. Consider the solutions $v \in G_d$ of the equation:

$$v^2 \ + \ v \ \frac{T_r^{3r}(\lambda)}{\lambda^{2^r}} \ + \ \frac{1}{\lambda^{2^r-1}} = 0. \tag{5}$$

Then $\mathcal{F}(f_\lambda) = 2^n - 2^r d \ \# L_\lambda$ with :

(a) Equation (5) has only one solution in G_d if and only if $T_r^{3r}(\lambda) = 0$; in this case $\# L_\lambda = 2^{2r}(2^r-1)$.

(b) If Equation (5) has no solution in G_d then $\# L_\lambda = 2^r(2^{2r} - 2^r - 1)$.

(c) Otherwise, Equation (5) has two solutions in G_d and $\# L_\lambda = 2^r(2^{2r} - 2^r + 1)$.

Consequently, we obtain:

case	$\mathcal{F}(f_\lambda)$
(a)	2^{3r}
(b)	$2^{4r} + 2^{3r+1} + 2^{2r}$
(c)	$-(2^{4r} + 2^{2r})$

Proof: According to Lemma 3, we are going to compute $\# N_\lambda$. Since $2^{3r}-1 = (2^r-1)d$ we can express any $y \in \mathbf{F}^*_{2^{3r}}$ as follows:

$$y = u\beta^i, \ u = \beta^{kd}, \ 0 \le k \le 2^r-2 \ \text{ and } \ 0 \le i \le d-1.$$

Thus

$$\# N_\lambda = \#\{ \ y \in \beta^i \mathbf{F}^*_{2^r} \mid T_r^{3r}(\lambda \beta^i) = 0 \ \text{ and } \ T_1^{3r}(\frac{1}{y}) = 1 \ \}.$$

Set $I = \{ \ i \mid T_r^{3r}(\lambda \beta^i) = 0 \}$. So $\# I = 2^r + 1$, because the polynomial $x + x^{2^r} + x^{2^{2r}}$ has 2^{2r} roots in $\mathbf{F}_{2^{3r}}$ and $y \in x\mathbf{F}^*_{2^r}$ is such a root as soon as x is a root too. Hence

$$\begin{aligned} \# N_\lambda &= \sum_{i \in I} \#\{ \ y \in \beta^i \mathbf{F}^*_{2^r} \mid T_1^r(\frac{1}{u} T_r^{3r}(\beta^{-i})) = 1 \ \} \\ &= 2^{r-1}(2^r + 1 - \#\{ \ i \in I \mid T_r^{3r}(\beta^{-i}) = 0 \}). \end{aligned} \tag{6}$$

Now set $w = \beta^i$. We have to solve

$$T_r^{3r}(\lambda w) = 0 \ \text{ and } \ T_r^{3r}(w^{-1}) = 0.$$

which we transform into

$$w^{2^{r+1}-2} + w^{2^r-1} \frac{\delta}{\lambda^{2^r}} + \frac{1}{\lambda^{2^r-1}} = 0,$$

where $\delta = T_r^{3r}(\lambda)$. Setting $v = w^{2^r-1}$, we get (5). This is an equation of degree 2 which has 0, 1 or 2 solutions in $\mathbf{F}^*_{2^{3r}}$. If it has 2 solutions, v_1 and v_2, then $v_1 \in G_d$ implies $v_2 \in G_d$ since $v_1 v_2 = 1/\lambda^{2^r-1}$. So (5) has one and only one solution in G_d if and only if $\delta = 0$. Using (6) we get $\# N_\lambda = 2^{r-1}2^r$ and further $\# L_\lambda$ completing the proof of the case **(a)**. In the same way, we compute $\# L_\lambda$ for the cases **(b)** and **(c)**. ∎

B. Another expression of f_λ

Set $V = \mathbf{F}_{2^{3r}}$ and let W be a subspace of $\mathbf{F}_{2^n}$ which is a set of representatives of the cosets of V, that is

$$\mathbf{F}_{2^n} = \bigcup_{a \in W} (a + V).$$

Thus, for any $x \in \mathbf{F}_{2^n}$ there is a unique pair $(y,a) \in V \times W$ such that $x = y + a$. Then, we define

$$f_\lambda(y,a) = f_\lambda(y+a) = Tr\left(\lambda(y+a)^d\right). \qquad (7)$$

Theorem 2: Recall that $\delta = T_r^{3r}(\lambda)$. Define the function π from W to V:

$$\pi(a) = \lambda^{2^{2r}}(a + a^{2^{3r}})^{2^{2r}+2^r} + \delta\ T_{3r}^{6r}(a^{2^{2r}+2^r}) \qquad (8)$$

Then, for any $(y,a) \in V \times W$:

$$\begin{aligned} f_\lambda(y,a) \quad &= \quad T_1^{3r}\Big(y^{2^r+1}\delta(a+a^{2^{3r}})^{2^{2r}} + y\pi(a) \\ &\qquad + \lambda(a^d + a^{2^{3r}d})\Big). \end{aligned} \qquad (9)$$

Proof: We compute $f_\lambda(y,a)$, which is defined by (7) :

$$\begin{aligned} &f_\lambda(y,a) \ = \ Tr(\lambda(y+a)^d) = \\ &Tr(\lambda y^d) \ + \ Tr\left(\lambda(a^{2^{2r}}y^{2^r+1} + a^{2^r}y^{2^{2r}+1} + ay^{2^r(2^r+1)})\right) \\ &+ \ Tr\left(\lambda(y^{2^{2r}}a^{2^r+1} + y^{2^r}a^{2^{2r}+1} + ya^{2^r(2^r+1)} + a^d)\right) \\ &= \ A + B + C, \end{aligned}$$

First $A = Tr(\lambda y^d) = 0$ since λ and y are in $\mathbf{F}_{2^{3r}}$. Now, using trace properties, we have

$$\begin{aligned} B \quad &= \quad Tr\left(y^{2^r+1}(\lambda a^{2^{2r}} + \lambda^{2^r}a^{2^{2r}} + \lambda^{2^{2r}}a^{2^{2r}})\right) \\ &= \quad Tr\left(y^{2^r+1}a^{2^{2r}}(\lambda + \lambda^{2^r} + \lambda^{2^{2r}})\right) \\ &= \quad T_1^{3r}\left(y^{2^r+1}\delta\ (a+a^{2^{3r}})^{2^{2r}}\right). \end{aligned}$$

Finally the part which is affine relatively to y is:

$$\begin{aligned} C \quad &= \quad Tr\Big(y(\lambda a^{2^r(2^r+1)} + \lambda^{2^r}a^{2^r(2^r+1)} \\ &+ \quad \lambda^{2^{2r}}a^{2^{2r}(2^{2r}+1)}) + \lambda a^d\Big) \\ &= \quad T_1^{3r}(y\ \pi(a) + \lambda\ T_{3r}^{6r}(a^d)). \end{aligned}$$

Indeed, we have $C = Tr(yD + \lambda a^d)$ where

$$\begin{aligned} T_{3r}^{6r}(D) \quad &= \quad (\lambda^{2^{2r}} + \delta)T_{3r}^{6r}(a^{2^{2r}+2^r}) + \lambda^{2^{2r}}T_{3r}^{6r}(a^{2^{4r}+2^{2r}}) \\ &= \quad \lambda^{2^{2r}}T_{3r}^{6r}\left(a^{2^{2r}}(a+a^{2^{3r}})^{2^r}\right) + \delta T_{3r}^{6r}(a^{2^{2r}+2^r}) \\ &= \quad \lambda^{2^{2r}}(a+a^{2^{3r}})^{2^{2r}+2^r} + \delta\ T_{3r}^{6r}(a^{2^{2r}+2^r}) \end{aligned}$$

which is exactly $\pi(a)$, completing the proof of (9). ■

C. The bent functions f_λ

Theorem 3: The function f_λ, defined by (3), is bent if and only if $\lambda + \lambda^{2^r} + \lambda^{2^{2r}} = 0$.

There are $2^r + 1$ such bent functions and, at all

$$(2^{2r} - 1)(2^{3r} + 1)$$

bent functions defined by (1). All these bent functions belong to the class $\mathcal{M}$. Moreover, let us define

$$\mathcal{B} = \{\ f_\lambda \mid \lambda \in \mathbf{F}_{2^{3r}},\ T_r^{3r}(\lambda) = 0\ \},$$

where f_0 is the null function. Then $\mathcal{B}$ is a subspace of the space of Boolean functions on $\mathbf{F}_{2^n}$. Its dimension is $2r$ and any function $f_\lambda \in \mathcal{B}^*$ is a cubic bent function.

Proof: First, if $\delta \neq 0$ then f_λ cannot be bent. This was proved by Theorem 1. Consider f_λ expressed by (9) with $\delta = 0$. Notation is as in Theorem 2. Then we get:

$$f_\lambda(y,a) = T_1^{3r}\left(y\pi(a) + \lambda(a^d + a^{2^{3r}d})\right) \qquad (10)$$

with $\pi(a) = \lambda^{2^{2r}}(a + a^{2^{3r}})^{2^{2r}+2^r}$. Clearly the function $a \mapsto a + a^{2^{3r}}$ is a bijection from W to V. Since 2^r+1 and $2^{3r}-1$ are coprime, we can conclude that π is a bijection from W to V. According to Lemma 1, the functions expressed by (10) are bent functions belonging to the class $\mathcal{M}$.

It is not difficult to prove that the cardinality of

$$\{\ \lambda = \alpha^{\ell(2^{3r}+1)} \mid 0 \leq \ell \leq d-1,\ T_r^{3r}(\lambda) = 0\ \}$$

is equal to $2^r + 1$. Then we get $2^r + 1$ bent functions defined by (3), each of them having $(2^n - 1)/d$ shifts. Moreover, as it was explained in Remark 1 these shifts are also elements of $\mathcal{M}$. The proof is completed by using the linearity of the trace function and by computing the cardinality of $\mathcal{B}$. ■

Concerning the spectra of the non bent functions f_λ, our numerical results suggest several conjecture. Notably, we conjecture that *there are three spectra only, corresponding to the three possible weights of f_λ.*

IV. Other properties

In this section, we give, without proofs, some other results on the properties of the functions f_λ. First the divisibility of the Walsh spectrum can be deduced from Theorems 1 and 2.

Corollary 1: Assume that λ is such that f_λ is not bent. Set $k = 2r$. Then for all $b \in \mathbf{F}_{2^n}$

$$\mathcal{F}(f_\lambda + \varphi_b) \equiv 0 \pmod{2^k}.$$

Moreover, this does not hold for $k > 2r$.

Let us define the derivative of f_λ with respect to $a \in \mathbf{F}_{2^n}^*$:

$$D_a f_\lambda(x) = Tr(\lambda x^d) + Tr(\lambda(x+a)^d).$$

These functions are quadratic and have the following form:

$$D_a f_\lambda(x) = Tr(\mu x^{2^{2r}+1} + Ax^{2^r+1} + Bx + \mu)$$

with

$$\mu = \lambda a^d,\ A = \mu + \mu^{2^{5r}},\ B = \mu + \mu^{2^{4r}} + \mu^{2^{5r}}.$$

The spectra of these functions are completely known as soon as the dimension of the *kernel of their symplectic forms* is known.

Lemma 4: Let us denote by $K(a,\lambda)$ the kernel of the symplectic form of $D_a f_\lambda$. Set $\mu = \lambda a^d$ and $A = \mu + \mu^{2^{5r}}$ and define the polynomial of $\mathbf{F}_{2^n}^*[x]$:

$$P(x) = \mu x^{2^{2r}} + Ax^{2^r} + (\mu x)^{2^{4r}} + (Ax)^{2^{5r}}.$$

Then $K(a,\lambda)$ is the subspace of the roots of P in $\mathbf{F}_{2^n}$.

It is easy to check that $\mathbf{F}_{2^r}$ is included in $K(a,\lambda)$ for any a and for any λ. But, we can prove that there is always a root of P which is not in $\mathbf{F}_{2^r}$. Further, we obtain the following result.

Theorem 4: Let $a, \lambda \in \mathbf{F}_{2^n}^*$. Set $\mu = \lambda a^d$ and

$$\sigma = \mu^{2^r+2^{4r}} + \mu^{2^r+2^{3r}} + \mu^{2^{2r}+2^{4r}}.$$

Then

$$\dim K(a, \lambda) = \begin{cases} 2r & \text{if } \sigma \neq 0 \\ 4r & \text{if } \sigma = 0. \end{cases}$$

Consequently, the Walsh transform of $D_a f_\lambda$ takes the values $\{0, \pm 2^{5r}\}$ if $\sigma = 0$ and $\{0, \pm 2^{4r}\}$ otherwise.

We can also give the form of some kernels $K(a, \lambda)$. In particular, the biggest dimension $4r$ appears for the λ corresponding to bent functions; moreover, in this case, the kernel contains the subfield $\mathbf{F}_{2^{3r}}$.

V. Conclusion

The complete classification of monomial bent functions is not achieved. Actually, little is known about this corpus, as recalled in [9]. They do not all lie in the known classes, especially in class $\mathcal{M}$. For instance, some bent functions characterized in [7], namely with *Kasami exponents*, are not normal [3], implying that they do not belong to any previously known class. On the other hand, the most recent result on monomial bent functions is due to Leander [9] who proved that the functions $g_\lambda : x \mapsto Tr(\lambda x^d)$ on $\mathbf{F}_{2^{4r}}$, $d = (2^r + 1)^2$, belong to $\mathcal{M}$ for a specific value of λ. Using our method (Theorem 2), we show that all functions g_λ, for $\lambda \in \mathbf{F}_{2^{2r}}$, can be viewed as a concatenation of affine functions.

References

[1] T. Berger, A. Canteaut, P. Charpin and Y. Laigle-Chapuy, "On Almost Perfect Nonlinear functions," *IEEE Trans. Inform. Theory*, to appear.

[2] A. Canteaut and P. Charpin, "Decomposing bent functions," *IEEE Trans. Inform. Theory*, 49(8), pp. 2004-19, August 2003.

[3] A. Canteaut, M. Daum, G. Leander and H. Dobbertin, "Normal and non normal bent functions," *Discrete Applied Mathematics*, Vol. 154, Issue 2, pp. 202-18, February 2006.

[4] P. Charpin, C. Tavernier and E. Pasalic, "On bent and semi-bent quadratic Boolean functions," *IEEE Trans. Inform. Theory*, 51(12), pp. 4287-98, December 2005.

[5] C. Carlet and P. Gaborit, "Hyper-bent functions and cyclic codes," *Jour. Comb. Theory*, Series A, to appear.

[6] J. Dillon, "Elementary Hadamard Difference sets," Ph.D. dissertation, University of Maryland, 1974.

[7] J. Dillon and H. Dobbertin, "New cyclic difference sets with Singer parameters," *Finitie Fields and Their Applications*, 10(2004) 342-389.

[8] N.G. Leander, "Bent functions with 2^r Niho exponents," In *Proceedings of of the 2005 International Workshop on Coding and Cryptography* (WCC 2005), Bergen (Norway), pp. 454-61, March 2005.

[9] N.G. Leander, "Monomial bent functions," In *Proceedings of of the 2005 International Workshop on Coding and Cryptography* (WCC 2005), Bergen (Norway), pp. 461-70, March 2005.

[10] R. L. McFarland, "A family of noncyclic difference sets," *J. Combin. Theory Ser. A*, vol. 15, pp. 1–10, 1973. vol. 20, 1983.