SCIENCE CHINA
Information Sciences

• HIGHLIGHT •

March 2018, Vol. 61 038102:1–038102:3
doi: 10.1007/s11432-017-9096-0

Several classes of negabent functions over finite fields

Gaofei WU[1], Nian LI[2,3], Yuqing ZHANG[1,4*] & Xuefeng LIU[1]

[1]*State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an* 710071*, China;*
[2]*Faculty of Mathematics and Statistics, Hubei Key Laboratory of Applied Mathematics, Hubei University, Wuhan* 430062*, China;*
[3]*Department of Informatics, University of Bergen, Bergen* N-5020*, Norway;*
[4]*National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences, Beijing* 100043*, China*

Received 22 January 2017/Accepted 19 April 2017/Published online 25 August 2017

Citation Wu G F, Li N, Zhang Y Q, et al. Several classes of negabent functions over finite fields. Sci China Inf Sci, 2018, 61(3): 038102, doi: 10.1007/s11432-017-9096-0

A Boolean function is called bent [1] if and only if it has a flat spectrum with respect to the Walsh-Hadamard transform. Bent functions have attracted a lot of attention due to their applications in coding theory and cryptography.

A Boolean function is called a negabent [2] function if it has flat spectrum with respect to the nega-Hadamard, $N^{\otimes n}$, transform, where $N = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & \sqrt{-1} \\ 1 & -\sqrt{-1} \end{smallmatrix}\right)$, and $\otimes$ is the tensor product. Bent-negabent functions are Boolean functions that are both bent and negabent.

Bent-negabent functions have been extensively studied recently. Parker and Pott [3] gave an important connection between bent and negabent functions, and showed that if n is even, then one can obtain negabent functions from any bent ones. By using this connection, Stănică et al. [4] gave a class of n-variable bent-negabent functions with algebraic degree $\frac{n}{4}+1$. Su et al. [5] considered the nega-Hadamard spectra of negabent functions, and constructed a class of bent-negabent functions with optimal algebraic degree by using complete permutation polynomials. Recently, Zhang et al. [6] constructed the first class of bent-negabent functions which are not in the completed Maiorana-McFarland class. On the other hand, it is also important to construct negabent functions over finite fields. Sarkar [7] considered negabent functions over finite fields, and characterized all the quadratic negabent monomials over finite fields. Recently, Zhou et al. [8] gave a class of cubic monomial negabent functions and a class of cubic negabent polynomials over finite fields.

In this article, by using some permutation trinomials over $\mathbb{F}_{2^n}$, we present some classes of negabent functions of the form $\mathrm{Tr}_1^n(\lambda x^{2^m+1}) + \mathrm{Tr}_1^n(ux)\mathrm{Tr}_1^n(vx)$, where $0 < m < n$. Then we show that the condition for the cubic monomials given by Zhou et al. [8] to be negabent is also necessary. Finally, we present a conjecture on negabent monomials whose exponents are of Niho type.

A Boolean function $f(x)$ is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. The Walsh-Hadamard transform of a function $f(x)$ at $a \in \mathbb{F}_2^n$ is defined by $W_f(a) = \sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+a\cdot x}$, where $a\cdot x$ is the standard inner product. If for any $a \in \mathbb{F}_2^n$, $|W_f(a)| = 2^{\frac{n}{2}}$, then $f(x)$ is called a bent function. It is known that an n-variable Boolean function $f(x)$ is bent if and only if $f(x)+f(x+a)$ is balanced for all nonzero $a \in \mathbb{F}_2^n$. The nega-Hadamard transform of $f(x)$ at $a \in \mathbb{F}_2^n$ is defined by $N_f(a) = N^{\otimes n}(-1)^{f(x)} = \sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+a\cdot x}\sqrt{-1}^{wt(x)}$, where $wt(x)$ is the

* Corresponding author (email: zhangyq@ucas.ac.cn)
The authors declare that they have no conflict of interest.

weight of the vector $x = (x_0, x_1, \ldots, x_{n-1})$, i.e., $wt(x) = \#\{i \mid x_i = 1, i \in \mathbb{Z}_n\}$. A function $f(x)$ is called a negabent function if $|N_f(a)| = 2^{\frac{n}{2}}$ for all $a \in \mathbb{F}_2^n$. Similarly, a function $f(x)$ is negabent if and only if $f(x) + f(x+a) + a \cdot x$ is balanced for all nonzero $a \in \mathbb{F}_2^n$.

In 2008, Sarkar [7] gave the following definition of negabent functions over finite fields.

Theorem 1 ([7])**.** Let $f(x)$ be a Boolean function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. Then $f(x)$ is negabent if and only if $\sum_{x\in\mathbb{F}_{2^n}}(-1)^{f(x)+f(x+a)+\mathrm{Tr}_1^n(ax)} = 0$ for all nonzero a in $\mathbb{F}_{2^n}$.

Let $a, b \in \mathbb{F}_{2^n}$, the Kloosterman sum over $\mathbb{F}_{2^n}$ is defined by $K_n(a,b) = \sum_{x\in\mathbb{F}_{2^n}^*}(-1)^{\mathrm{Tr}_1^n(ax+bx^{-1})}$.

Lemma 1 ([9, Theorem 5.45])**.** If $a, b \in \mathbb{F}_{2^n}$ are not both zero, then the Kloosterman sum satisfies $|K_n(a,b)| \leqslant 2\sqrt{2^n}$.

By Lemma 1, we have the following lemma.

Lemma 2. Let k be a positive integer and $q = 2^k$. For any $b \in \mathbb{F}_q^*$ and $c \in \mathbb{F}_q^*$, define $A = \#\{x \in \mathbb{F}_q^* \,|\, \mathrm{Tr}_1^k(bx) = 0, \mathrm{Tr}_1^k(cx^{-1}) = 1\}$. Then $A > 0$ if $k > 2$.

A polynomial $f \in \mathbb{F}_q[x]$ is called a permutation polynomial if the associated polynomial mapping $f : c \mapsto f(c)$ from $\mathbb{F}_q$ to itself is a permutation of $\mathbb{F}_q$ [9].

Lemma 3 ([9, p.118])**.** Let q be a prime power and $f(x) = \sum_{i=0}^{m-1} a_i x^{q^i} \in \mathbb{F}_q[x]$. Then $f(x)$ is a permutation polynomial over $\mathbb{F}_{q^m}$ if and only if $\gcd(\sum_{i=0}^{m-1} a_i x^i, x^m - 1) = 1$. Moreover, if $g(x)$ is the compositional inverse of $f(x)$, i.e., $f(g(x)) \equiv x \mod (x^{q^m} - x)$, then $g(x)$ is a q-polynomial over $\mathbb{F}_q$.

The following two lemmas can be proved by using Lemma 3.

Lemma 4. Let k be a positive integer and $f(x) = x + x^{2^k} + x^{2^{2k}}$, then $f(x)$ is a permutation polynomial over $\mathbb{F}_{2^n}$ if and only if $\gcd(n, 3k) = \gcd(n, k)$. Further, let $g(x)$ be the compositional inverse of $f(x)$. Then $g(x)$ is a 2-polynomial over $\mathbb{F}_2$ and $\mathrm{Tr}_1^n(g(x)) = \mathrm{Tr}_1^n(x)$.

Lemma 5. Let $n = rk$ and $f(x) = \lambda x + x^{2^k} + \lambda x^{2^{2k}}$, where r, k are positive integers and $\lambda \in \mathbb{F}_{2^k}^*$. Then $f(x)$ is a permutation polynomial over $\mathbb{F}_{2^n}$ if and only if $\gcd(\lambda + x + \lambda x^2, x^r - 1) = 1$. Further, let $g(x)$ be the compositional inverse of $f(x)$. Then $g(x)$ is a 2^k-polynomial over $\mathbb{F}_{2^k}$ and $\mathrm{Tr}_1^n(g(x)) = \mathrm{Tr}_1^n(x)$.

Some classes of negabent functions. In the following, by using some permutation polynomials over $\mathbb{F}_{2^n}$, we present several classes of negabent functions of the form $\mathrm{Tr}_1^n(\lambda x^{2^k+1}) + \mathrm{Tr}_1^n(ux)\mathrm{Tr}_1^n(vx)$ over $\mathbb{F}_{2^n}$, where $2 \leqslant k \leqslant n-1$, $\lambda \in \mathbb{F}_{2^n}$, and $(u,v) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^*$.

Theorem 2. Let $n = 2k$, $\lambda \in \mathbb{F}_{2^k}$ and $(u,v) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^*$. Then $f(x) = \mathrm{Tr}_1^k(\lambda x^{2^k+1}) + \mathrm{Tr}_1^n(ux)\mathrm{Tr}_1^n(vx)$ is negabent on $\mathbb{F}_{2^n}$ if and only if one of the following conditions is satisfied:

(1) $\lambda \neq 1$, $(\mathrm{Tr}_1^n(\frac{u}{1+\lambda}), \mathrm{Tr}_1^n(\frac{(\lambda u^{2^k}+u)v}{1+\lambda^2}), \mathrm{Tr}_1^n(\frac{v}{1+\lambda})) \in \{(0,0,0),(0,0,1),(1,0,0),(1,1,1)\}$;

(2) $\lambda = 1$, $k = 2$, $u, v, u+v \notin \mathbb{F}_{2^k}$;

(3) $\lambda = 1, k = 1$, $u \neq v$.

Corollary 1. Let $f(x)$ with $u \neq v$ be given as in Theorem 2 and $\mathbb{N}_\lambda$ denote the number of ordered pairs (u,v) such that $f(x)$ is negabent. Then $\mathbb{N}_\lambda = (2^{n-1}-2)(2^n-1)$ for any fixed $\lambda \neq 1$ and $\mathbb{N}_1 = 6, 96$ for $k = 1, 2$ respectively.

Let $n = 2k$, $\lambda \in \mathbb{F}_{2^k}^*$ and $(u,v) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^*$. In [10], Mesnager showed that the function $f(x) = \mathrm{Tr}_1^k(\lambda x^{2^k+1}) + \mathrm{Tr}_1^n(ux)\mathrm{Tr}_1^n(vx)$ is bent if and only if $\mathrm{Tr}_1^n(\lambda^{-1}u^{2^k}v) = 0$.

Together with Theorem 2, we have the following corollary.

Corollary 2. Let $n = 2k$, $\lambda \in \mathbb{F}_{2^k}^*$ and $(u,v) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^*$. Then $f(x) = \mathrm{Tr}_1^k(\lambda x^{2^k+1}) + \mathrm{Tr}_1^n(ux)\mathrm{Tr}_1^n(vx)$ is bent-negabent on $\mathbb{F}_{2^n}$ if and only if one of the following conditions are satisfied:

(1) $\lambda \neq 1$, $(\mathrm{Tr}_1^n(\frac{u}{1+\lambda}), \mathrm{Tr}_1^n(\frac{(\lambda u^{2^k}+u)v}{1+\lambda^2}), \mathrm{Tr}_1^n(\lambda^{-1}u^{2^k}v)) = (0,0,0)$ or $(\mathrm{Tr}_1^n(\frac{u}{1+\lambda}), \mathrm{Tr}_1^n(\frac{(\lambda u^{2^k}+u+1+\lambda)v}{1+\lambda^2}), \mathrm{Tr}_1^n(\lambda^{-1}u^{2^k}v)) = (1,0,0)$;

(2) $\lambda = 1$, $k = 2$, $u, v, u+v \notin \mathbb{F}_{2^k}$ and $\mathrm{Tr}_1^n(u^{2^k}v) = 0$.

As a special case of Theorem 2, if $\lambda = 0$, then it gives the necessary and sufficient conditions for $\mathrm{Tr}_1^n(ux)\mathrm{Tr}_1^n(vx)$ to be negabent on $\mathbb{F}_{2^n}$ for even n. The following theorem shows the negabent property of $\mathrm{Tr}_1^n(ux)\mathrm{Tr}_1^n(vx)$ for both even and odd n.

Theorem 3. Let $f(x) = \mathrm{Tr}_1^n(ux)\mathrm{Tr}_1^n(vx)$, where $(u,v) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^*$. Then $f(x)$ is negabent on $\mathbb{F}_{2^n}$ if and only if one of the following conditions are satisfied:

(1) $\mathrm{Tr}_1^n(u) = 0$ and $\mathrm{Tr}_1^n(uv) = 0$;

(2) $\mathrm{Tr}_1^n(u) = 1$ and $\mathrm{Tr}_1^n((u+1)v) = 0$.

Remark 1. Theorem 3 shows that $\mathrm{Tr}_1^n(x)\mathrm{Tr}_1^n(vx)$ is negabent for any nonzero $v \in \mathbb{F}_{2^n}$ when n is odd and $u = 1$, which was given in Theorem 8 in [8]. Note that the negabent property is not preserved by linear transform, i.e., $f(x)$ is negabent on $\mathbb{F}_{2^n}$ does not imply that $f(ax)$ is negabent on $\mathbb{F}_{2^n}$ for all $a \in \mathbb{F}_{2^n}^*$. Thus, Theorem 3 is not covered by Theorem 8 in [8].

Theorem 4. Let n be an even integer and k be a positive integer such that $\gcd(n, 3k) = \gcd(n, k)$.

Then $f(x) = \mathrm{Tr}_1^n(x^{2^k+1}) + \mathrm{Tr}_1^n(x)\mathrm{Tr}_1^n(vx)$ is negabent on $\mathbb{F}_{2^n}$ if $\mathrm{Tr}_1^n(v) = 0$.

Theorem 5. Let r and k be two integers such that rk is even. Let $n = rk$, $\lambda \in \mathbb{F}_{2^k}^*$ and $\gcd(\lambda + x + \lambda x^2, x^r - 1) = 1$. Then $f(x) = \mathrm{Tr}_1^n(\lambda x^{2^k+1}) + \mathrm{Tr}_1^n(x)\mathrm{Tr}_1^n(vx)$ is negabent on $\mathbb{F}_{2^n}$ if $\mathrm{Tr}_1^n(v) = 0$.

Remark 2. Notice that if one takes $n = rk$ in Theorem 4 then Theorem 4 is a special case of Theorem 5 due to the fact that $\gcd(1+x+x^2, x^r-1) = 1$ if and only if $\gcd(rk, 3k) = \gcd(rk, k)$. For the values of n, k with $\gcd(n, k) \neq k$, the results in Theorem 4 are not covered by Theorem 5.

By Theorem 5 we can obtain the following results if we take $r = 3, 4, 5$ respectively.

Corollary 3. Let k be an even integer and $n = 3k$. Let $\lambda \in \mathbb{F}_{2^k} \setminus \{0, 1\}$. Then $f(x) = \mathrm{Tr}_1^n(\lambda x^{2^k+1}) + \mathrm{Tr}_1^n(x)\mathrm{Tr}_1^n(vx)$ is negabent on $\mathbb{F}_{2^n}$ if $\mathrm{Tr}_1^n(v) = 0$.

Corollary 4. Let $n = 4k$ and $\lambda \in \mathbb{F}_{2^k}^*$. Then $f(x) = \mathrm{Tr}_1^n(\lambda x^{2^k+1}) + \mathrm{Tr}_1^n(x)\mathrm{Tr}_1^n(vx)$ is negabent on $\mathbb{F}_{2^n}$ if $\mathrm{Tr}_1^n(v) = 0$.

Corollary 5. Let k be an even integer and $n = 5k$. Let $\lambda \in \mathbb{F}_{2^k} \setminus \{0, \omega, \omega^2\}$, where ω is a primitive element of $\mathbb{F}_{2^2}$. Then $f(x) = \mathrm{Tr}_1^n(\lambda x^{2^k+1}) + \mathrm{Tr}_1^n(x)\mathrm{Tr}_1^n(vx)$ is negabent on $\mathbb{F}_{2^n}$ if $\mathrm{Tr}_1^n(v) = 0$.

On a class of cubic negabent functions. In [8], Zhou and Qu showed that $\mathrm{Tr}_1^{2k}(\lambda x^d)$ is negabent on $\mathbb{F}_{2^{2k}}$ if $\lambda \in \mathbb{F}_2$, where $d = 2^k + 3$ and $k \geqslant 3$ is odd. In fact, by using Lemma 2, we can prove that $\lambda \in \mathbb{F}_2$ is also necessary for $\mathrm{Tr}_1^{2k}(\lambda x^d)$ to be negabent.

Theorem 6. Let $n = 2k$, $q = 2^k$ and $d = q + 3$, where $k \geqslant 3$ is odd. Then $\mathrm{Tr}_1^n(\lambda x^d)$ is negabent on $\mathbb{F}_{2^n}$ if and only if $\lambda \in \mathbb{F}_2$.

At the end of this article, we present a conjecture on negabent monomials whose exponents are of Niho type, namely the exponents of the form $d = r(2^m - 1) + 1$, where $m = n/2$ and $1 \leqslant r \leqslant 2^m$. Notice that $d_1 = r_1(2^m - 1) + 1$ and $d_2 = r_2(2^m - 1) + 1$ lie in the same cyclotomic coset modulo $2^n - 1$ if and only if $r_1 \equiv r_2 \pmod{2^m + 1}$ or $r_1 + r_2 \equiv 1 \pmod{2^m + 1}$.

Conjecture 1. Let $n = 2m$ and $d = r(2^m - 1) + 1$, where $2 \leqslant r \leqslant 2^{m-1} + 1$. Then $\mathrm{Tr}_1^n(\alpha x^d)$ is a negabent function if and only if one of the following two conditions holds:

(1) (Cubic functions, Theorem 6) m is odd, $r = 2^{m-2} + 1 \equiv \frac{3}{4} \pmod{2^m + 1}$ and $\alpha \in \mathbb{F}_2$.

(2) (Quadratic functions, [7]) $r = 2^{m-1} + 1 \equiv \frac{1}{2} \pmod{2^m + 1}$ and $\alpha + \alpha^{2^m} \neq 1$.

This conjecture has been verified by Magma for $n \leqslant 14$. We encourage the reader to prove the conjecture or show that there exist more negabent monomials whose exponents are of Niho type.

Acknowledgements This work was supported by Fundamental Research Funds for the Central Universities (Grant No. JB161504), China Postdoctoral Science Foundation (Grant No. 2016M602776), National Natural Science Foundation of China (Grant Nos. 61671013, 61602361, 61572460, 61402352), National Key R&D Program of China (Grant No. 2016YFB0800703), Open Project Program of the State Key Laboratory of Information Security (Grant No. 2017-ZD-01), National Development and Reform Commission (Grant No. (2012)1424), China 111 Project (Grant No. B16037), and Norwegian Research Council.

Supporting information Appendixes A–C. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Rothaus O S. On 'bent' functions. J Combin Theory A, 1976, 20: 300–305
2 Parker M G. The constabent properties of Golay-Davis-Jedwab sequences. In: Proceedings of IEEE International Symposium on Information Theory, Sorrento, 2000. 302
3 Parker M G, Pott A. On boolean functions which are bent and negabent. In: Proceedings of International Workshop on Sequences, Subsequences, and Consequences, Los Angeles, 2007. 9–23
4 Stănică P, Gangopadhyay S, Chaturvedi A, et al. Investigations on bent and negabent functions via the nega-Hadamard transform. IEEE Trans Inf Theory, 2012, 58: 4064–4072
5 Su W, Pott A, Tang X. Characterization of negabent functions and construction of bent-negabent functions with maximum algebraic degree. IEEE Trans Inf Theory, 2013, 59: 3387–3395
6 Zhang F, Wei Y, Pasalic E. Constructions of bent-negabent functions and their relation to the completed Maiorana-McFarland class. IEEE Trans Inf Theory, 2015, 61: 1496–1506
7 Sarkar S. Characterizing negabent boolean functions over finite fields. In: Proceedings of the 7th International Conference on Sequences and Their Applications, Waterloo, 2012. 77–88
8 Zhou Y, Qu L. Constructions of negabent functions over finite fields. Cryptogr Commun, 2017, 9: 165–180
9 Lidl R, Niederreiter H. Finite fields. In: Encyclopedia of Mathematics and Its Applications. 2nd ed. Cambridge: Cambridge University Press, 1997
10 Mesnager S. Several new infinite families of bent functions and their duals. IEEE Trans Inf Theory, 2014, 60: 4397–4407