Mathematical and Computational Applications

MDPI

Article

The Average Hull Dimension of Negacyclic Codes over Finite Fields

Somphong Jitman [1] and Ekkasit Sangwisut [2,*]

[1] Department of Mathematics, Faculty of Science, Silpakorn University, Nakhon Pathom 73000, Thailand; sjitman@gmail.com

[2] Department of Mathematics and Statistics, Faculty of Science, Thaksin University, Phattalung 93110, Thailand

* Correspondence: ekkasit.sangwisut@gmail.com

Received: 6 August 2018; Accepted: 17 August 2018; Published: 20 August 2018

Abstract: Hulls of linear codes have been extensively studied due to their wide applications and links with the efficiency of some algorithms in coding theory. In this paper, the average dimension of the Euclidean hull of negacyclic codes of length n over finite fields $\mathbb{F}_q$, denoted by $E(n,-1,q)$, has been investigated. The formula for $E(n,-1,q)$ has been determined. Some upper and lower bounds of $E(n,-1,q)$ have been given as well. Asymptotically, it has been shown that either $E(n,-1,q)$ is zero or it grows the same rate as n.

Keywords: average hull dimension; negacyclic codes; hulls; self-reciprocal polynomials

MSC: 94B15, 94B05.

1. Introduction

In practice, communication systems are not 100% reliable due to noise or other forms of interference. Coding theory is a branch of Engineering Mathematics that has been introduced and applied to solve this problem since the 1960s. Codes have later been extensively studied and linked with other problems and applications.

In 1990, the (Euclidean) hull of a linear code has been introduced to classify finite projective planes in [1]. It is defined to be the intersection of a linear code and its Euclidean dual. Hulls of linear codes have various applications and play an important role in the efficiency determination of some algorithms in coding theory such as computing permutation equivalence of two linear codes and finding the automorphism group of linear codes (see, for example, [2–6]). Precisely, the efficiency of these computations is limited by the hull size of codes. In [7], the hulls of linear codes have been applied in constructing good entanglement-assisted quantum error correcting codes.

Properties of hulls of codes have been extensively studied. The average dimensions of the Euclidean hull of linear codes and of cyclic codes were given in [8,9], respectively. The dimensions of the hulls of cyclic codes and negacyclic codes were determined in [10]. Later, the complete study of the average dimension of the Hermitian hull of cyclic and constacyclic codes was given in [11,12]. It is of natural interest to study the average dimension of the Euclidean hull of constacyclic codes. In [13], it has been shown that the Euclidean dual of λ-constacyclic code is again λ-constacyclic if and only if $\lambda = \pm 1$. Therefore, the average dimension of the Euclidean hull of negacyclic codes ($\lambda = -1$) is the only remaining case.

In this paper, we focus on the average dimension of the Euclidean hull of negacyclic codes of length n over finite fields $\mathbb{F}_q$ as well as its lower and upper bounds. The paper is organized as follows. Basic properties of codes and polynomials over finite fields are recalled in Section 2. In Section 3,

the expression for $E(n,-1,q)$, the formula for the average dimension of neagcyclic codes, is given together with some upper bounds. In Section 4, upper and lower bounds on $E(n,-1,q)$ are derived. The summary and remarks are given in Section 5.

2. Preliminaries

Let p be a prime and let q be a p-power. Denote by $\mathbb{F}_q$ the finite field of order q and characteristic p. For given positive integers $k \leq n$, a *linear code* of length n and dimension k over $\mathbb{F}_q$ is a k-dimensional subspace of the $\mathbb{F}_q$-vector space $\mathbb{F}_q^n$. The Euclidean dual of a linear code C is defined to be

$$C^{\perp} = \left\{ (u_0, u_1 \ldots, u_{n-1}) \in \mathbb{F}_q^n \ : \ \sum_{i=0}^{n-1} u_i c_i = 0 \ \text{ for all } \ (c_0, c_1 \ldots, c_{n-1}) \in C \right\}.$$

The Euclidean hull of a linear code C is defined to be

$$\mathrm{Hull}(C) = C \cap C^{\perp}.$$

A linear code of length n over $\mathbb{F}_q$ is said to be *negacyclic* if $(-c_{n-1}, c_0, \ldots, c_{n-2}) \in C$ for all $(c_0, c_1, \ldots, c_{n-1}) \in C$.

Let $\mathcal{C}(n,-1,q)$ denote the set of all neagcyclic codes of length n over $\mathbb{F}_q$. The *average dimension of the hull of negacyclic codes of length* n over $\mathbb{F}_q$ is defined to be

$$E(n,-1,q) := \sum_{C \in \mathcal{C}(n,-1,q)} \frac{\dim \mathrm{Hull}(C)}{|\mathcal{C}(n,-1,q)|}.$$

Every non-zero negacyclic code C of length n over $\mathbb{F}_q$ can be viewed as an ideal of the principal ideal ring $\mathbb{F}_q[x]/\langle x^n+1 \rangle$ generated by a monic divisor $g(x)$ of x^n+1 (see [10]). In this case, $g(x)$ is called the *generator polynomial* for C and $\dim C = n - \deg(g(x))$.

For a polynomial $f(x) = a_0 + a_1 x + \cdots + a_k x^k \in \mathbb{F}_q[x]$ of degree k and $a_0 \neq 0$, the reciprocal polynomial of $f(x)$ is defined to be $f^*(x) := f(0)^{-1} x^{\deg f(x)} f\left(\frac{1}{x}\right)$. It is not difficult to see that $(f^*)^*(x) = f(x)$. Then, we have two types of polynomials. A polynomial $f(x)$ is called *self-reciprocal* if $f(x) = f^*(x)$. Otherwise, $f(x)$ and $f^*(x)$ are called a *reciprocal polynomial pair*.

Let C be a negacyclic code of length n over $\mathbb{F}_q$ with the generator polynomial $g(x)$ and let $h(x) = \frac{x^n+1}{g(x)}$. Then, $h^*(x)$ is a monic divisor of x^n+1 and it is the generator polynomial of $C^{\perp}$ by Lemma 2.1 of [13]. Therefore, $\mathrm{Hull}(C)$ is generated by the polynomial $\mathrm{lcm}(g(x), h^*(x))$ (see Theorem 1 of [10]).

Recall that the characteristic of $\mathbb{F}_q$ is p. Then, a positive integer n can be written in the form of $n = \overline{n} p^{\nu}$, where $p \nmid \overline{n}$ and $\nu \geq 0$. Using arguments similar to those in Section 4 of [10], up to permutation, there exist nonnegative integers $\mathtt{s}$ and $\mathtt{t}$ such that

$$x^n + 1 = \left(x^{\overline{n}} + 1\right)^{p^{\nu}} = \prod_{i=1}^{\mathtt{s}} g_i(x)^{p^{\nu}} \prod_{j=1}^{\mathtt{t}} f_j(x)^{p^{\nu}} f_j^*(x)^{p^{\nu}}, \tag{1}$$

where $f_j(x)$ and $f_j^*(x)$ are a reciprocal polynomial pair and $g_i(x)$ is a monic irreducible self-reciprocal polynomial for all $1 \leq i \leq \mathtt{s}$ and $1 \leq j \leq \mathtt{t}$.

For a given negacyclic code C of length n over $\mathbb{F}_q$, based on the factorization in (1), the generator polynomial of C can be viewed of the form

$$g(x) = \prod_{i=1}^{\mathtt{s}} g_i(x)^{u_i} \prod_{j=1}^{\mathtt{t}} f_j(x)^{z_j} \left(f_j^*(x)\right)^{w_j},$$

where $0 \leq u_i, z_j, w_j \leq p^\nu$. It follows that the generator polynomial of $C^\perp$ is

$$h^*(x) = \prod_{i=1}^{\mathtt{s}} g_i(x)^{p^\nu - u_i} \prod_{j=1}^{\mathtt{t}} f_j(x)^{p^\nu - w_j} \left(f_j^*(x)\right)^{p^\nu - z_j},$$

and hence the generator polynomial of Hull(C) is

$$\operatorname{lcm}(g(x), h^*(x)) = \prod_{i=1}^{\mathtt{s}} g_i(x)^{\max\{u_i,\, p^\nu - u_i\}} \prod_{j=1}^{\mathtt{t}} f_j(x)^{\max\{z_j,\, p^\nu - w_j\}} \left(f_j^*(x)\right)^{\max\{w_j,\, p^\nu - z_j\}}. \tag{2}$$

Since 1 and -1 are identical when the characteristic of $\mathbb{F}_q$ is even, in the rest of this paper, we assume that the characteristic p of $\mathbb{F}_q$ is odd.

3. The Average Dimension $E(n, -1, q)$

In this section, we focus on an explicit expression for the formula of the average dimension of the Euclidean hull of negacyclic codes of length n over $\mathbb{F}_q$. Employing techniques similar to those for the cyclic case in [9], slightly different results for the negacyclic case can be deduced.

Assume that $x^{\overline{n}} + 1$ has the factorization in the form of Equation (1) and let $B_{\overline{n},-1,q} = \sum_{i=1}^{\mathtt{s}} \deg g_i(x)$. The expectation $E(\,\cdot\,)$ in Lemma 1 can be obtained using arguments similar to those in the proof of Proposition 22 of [9] .

Lemma 1. *Let p be an odd prime and let ν be a nonnegative integer. Let $0 \leq u, z, w \leq p^\nu$. Then, the following statements hold:*

1. $E(\max\{u, p^\nu - u\}) = \frac{3p^\nu + 1}{4}$.
2. $E(\max\{z, p^\nu - w\}) = \frac{p^\nu(4p^\nu + 5)}{6(p^\nu + 1)}$.

The average dimension of the Euclidean hull of neagcyclic codes of length n over $\mathbb{F}_q$ can be determined as follows.

Theorem 1. *Let $\mathbb{F}_q$ be a finite field of order q and odd characteristic p and let n be a positive integer such that $n = \overline{n}p^\nu$, $p \nmid \overline{n}$ and $\nu \geq 0$. Then, the average dimension of the Euclidean hull of negacyclic codes of length n over $\mathbb{F}_q$ is*

$$E(n, -1, q) = n\left(\frac{2p^\nu + 1}{6(p^\nu + 1)}\right) - B_{\overline{n},-1,q}\left(\frac{p^{2\nu} + 2p^\nu + 3}{12(p^\nu + 1)}\right). \tag{3}$$

Proof. By Lemma 1, Equation (2), and arguments similar to those in the proof of Theorem 3.2 of [11], it can be deduced that

$$\begin{aligned} E(n, -1, q) &= n\left(\frac{1}{3} - \frac{1}{6(p^\nu + 1)}\right) - B_{\overline{n},-1,q}\left(\frac{p^\nu + 1}{12} + \frac{2}{12(p^\nu + 1)}\right) \\ &= n\left(\frac{2p^\nu + 1}{6(p^\nu + 1)}\right) - B_{\overline{n},-1,q}\left(\frac{p^{2\nu} + 2p^\nu + 3}{12(p^\nu + 1)}\right). \end{aligned}$$

This completes the proof. □

The next corollary is a direct consequence of Theorem 1.

Corollary 1. *Assume the notations as in Theorem 1. Then, the following statements hold:*

1. $E(n, -1, q) < \frac{n}{3}$.
2. $E(\overline{n}, -1, q) = \frac{\overline{n} - B_{\overline{n},-1,q}}{4}$.
3. $E(\overline{n}, -1, q) < \frac{\overline{n}}{4}$.

4. Properties of $B_{\overline{n},-1,q}$ and Bounds on $E(n,-1,q)$

In this section, some number theoretical tools are constructed and applied to study properties of $B_{\overline{n},-1,q}$. As a consequence, lower and upper bounds for $E(n,-1,q)$ can be derived using $B_{\overline{n},-1,q}$.

For an odd prime power q, let $N_q := \{\ell \geq 1 \,:\, \ell \text{ divides } q^i + 1\}$. For coprime positive integers i and j, denote by $\mathrm{ord}_j(i)$ the multiplicative order of i modulo j. An element in N_q has the following properties.

Lemma 2. *Let q be an odd prime power. If $\ell \in N_q$ and $\ell > 2$, then $\mathrm{ord}_\ell(q)$ is even.*

Proof. Since $\ell \in N_q$, there exists the smallest positive integer k such that $\ell | (q^k + 1)$. It follows that $\ell | (q^{2k} - 1)$. Then, $\mathrm{ord}_\ell(q) | 2k$. Since $\mathrm{ord}_\ell(q) \nmid k$, $\mathrm{ord}_\ell(q)$ is even. □

Next, we introduce a partition for the set N_q. For each integer $\alpha \geq 0$, let

$$P_{q,\alpha} := \{\ell \in N_q \,:\, 2^\alpha || \,\mathrm{ord}_\ell(q)\},$$

where $2^\alpha || k$ is used if α is the integer such that $2^\alpha | k$ and $2^{\alpha+1} \nmid k$. Then, we have $N_q = P_{q,0} \cup P_{q,1} \cup P_{q,2} \cdots$.

Theorem 2 (Theorem 4 of [9])**.** *Let q be an odd prime power and let ℓ be a positive integer. Then, the following statements hold:*

1. *Let ℓ be an odd integer. If $\ell > 1$ is such that $\ell = \prod_{i=1}^{k} p_i^{e_i}$ the prime factorization of ℓ. Then, $\ell \in N_q$ if and only if there exists $\alpha > 0$ such that $p_i \in P_{q,\alpha}$ for all i. In this case, we have $\ell \in P_{q,\alpha}$.*
2. *Let $\beta \geq 1$ be an integer. Then $2^\beta \in N_q$ if and only if 2^β divides $q+1$. Moreover, if $2^\beta \in N_q$, $\beta \geq 2$, then $2^\beta \in P_{q,1}$.*
3. *Let q and ℓ be odd. Then, $2\ell \in N_q$ if and only if $\ell \in N_q$. In this case, ℓ and 2ℓ belong to the same set $P_{q,\alpha}$.*
4. *Let $\ell = 2^\beta \overline{\ell}$ where $\overline{\ell}$ is odd and $\beta \geq 2$. Then, $\ell \in N_q$ if and only if $2^\beta \in N_q$ and $\overline{\ell} \in P_{q,1}$. In this case, we have $\ell \in P_{q,1}$.*

The characterization of elements in $P_{q,\alpha}$ are given in the following corollary.

Corollary 2. *Let $\gamma \geq 1$ be an integer such that $2^\gamma | (q+1)$. Let ℓ be a positive integer relatively prime to q and let $2^\beta || \ell$. Then, the following statements hold:*

1. *$P_{q,0} = \{1, 2\}$.*
2. *$\ell \in P_{q,1}$ if and only if either ℓ has an odd prime divisor, each odd prime divisor of ℓ belongs to $P_{q,1}$ and $0 \leq \beta \leq \gamma$, or $\ell = 2^\beta$ and $2 \leq \beta \leq \gamma$.*
3. *Let $\alpha \geq 2$. Then, $\ell \in P_{q,\alpha}$ if and only if ℓ has an odd prime divisor, each odd prime divisor of ℓ belongs to $P_{q,\alpha}$ and $0 \leq \beta \leq 1$.*

Lemma 3. *Let $\alpha \geq 1$ an integer and let ℓ be a positive integer. If $\ell \in P_{q,\alpha}$, then $\ell \geq 2^\alpha + 1$.*

Proof. By Corollary 2, we have $\ell \geq 3$. Since $\ell \in P_{q,\alpha}$, it follows that $2^\alpha || \,\mathrm{ord}_\ell(q)$. By Little Fermat's Theorem, we have $\mathrm{ord}_\ell(q) | \phi(\ell)$. Then, $2^\alpha | \phi(\ell)$. Hence, $2^\alpha \leq \phi(\ell) \leq \ell - 1$. □

Let $\Omega := \{j \in \mathbb{N} \,:\, j | 2\overline{n} \text{ and } 2 \nmid \overline{n}\}$. Next, we give the expression of $B_{\overline{n},-1,q}$.

Lemma 4. *Assume that $x^{\overline{n}} + 1$ is factorized as in Equation (1). Then,*

$$B_{\overline{n},-1,q} = \sum_{j \in \Omega \cap N_q} \phi(j),$$

where ϕ is the Euler's totient function.

Proof. By Equation (1), we have

$$x^{\overline{n}}+1=\prod_{i=1}^{\mathtt{s}}g_i(x)\prod_{j=1}^{\mathtt{t}}f_j(x)f_j^*(x).$$

From Equation (29) of [10], $x^{\overline{n}}+1$ can be factored as

$$x^{\overline{n}}+1=\prod_{j\in\Omega\cap N_q}\prod_{i=1}^{\gamma(j)}g_{ij}(x)\prod_{j\in\Omega\setminus N_q}\prod_{i=1}^{\beta(j)}f_{ij}(x)f_{ij}^*(x),$$

where $\gamma(j)=\frac{\phi(j)}{\mathrm{ord}_j(q)}$, $\beta(j)=\frac{\phi(j)}{2\,\mathrm{ord}_j(q)}$, $f_{ij}(x)$ and $f_{ij}^*(x)$ are a monic irreducible-reciprocal polynomial pair of degree $\mathrm{ord}_j(q)$, and $g_{ij}(x)$ is a monic irreducible self-reciprocal polynomial of degree $\mathrm{ord}_j(q)$.

Altogether, it can be concluded that

$$\prod_{i=1}^{\mathtt{s}}g_i(x)=\prod_{j\in\Omega\cap N_q}\prod_{i=1}^{\gamma(j)}g_{ij}(x).$$

Hence,

$$B_{\overline{n},-1,q}=\sum_{i=1}^{\mathtt{s}}\deg(g_i(x))=\sum_{j\in\Omega\cap N_q}\gamma(j)\deg(g_{ij}(x))=\sum_{j\in\Omega\cap N_q}\frac{\phi(j)}{\mathrm{ord}_j(q)}\cdot\mathrm{ord}_j(q)=\sum_{j\in\Omega\cap N_q}\phi(j)$$

as desired. □

Remark 1. *From Lemma 4, we have the following facts. The set $\Omega\cap N_q$ can be empty. For convenience, the empty summation will be regarded as 0. In this case, $B_{\overline{n},-1,q}=\sum_{j\in\Omega\cap N_q}\phi(j)=\sum_{j\in\emptyset}\phi(j)=0$. For example, $B_{4,-1,3}=0$ since $\Omega\cap N_3=\emptyset$.*

The expression of the set Ω can be simplified using the definition of $\overline{n}$ as follows.

Lemma 5. *Write $\overline{n}=2^\beta n'$, where n' is an odd integer and β is a non-negative integer. Then, $\Omega=\{2^{\beta+1}k:k\in\mathbb{N}$ and $k|n'\}$.*

Proof. Let $\overline{n}=2^\beta n'$. Then, we have $\Omega=\{j\in\mathbb{N}:j|2\overline{n}$ and $2\nmid\overline{n}\}=\{j\in\mathbb{N}:j|2^{\beta+1}n'$ and $j\nmid 2^\beta n'\}$. Hence, $2^{\beta+1}|j$ for all $j\in\Omega$, which implies $\Omega=\{2^{\beta+1}k:k\in\mathbb{N}$ and $k|n'\}$. □

The following result is a consequence of Lemma 5 and Theorem 2.

Proposition 1. *Let $\gamma\geq 1$ be the integer such that $2^\gamma||(q+1)$. Then, the following statements hold:*

1. *$\Omega\cap N_q=\emptyset$ if and only if $\beta+1>\gamma$.*
2. *$\Omega\cap N_q=\Omega$ if and only if $\beta+1\leq\gamma$ and $2\overline{n}\in N_q$.*
3. *$\emptyset\subsetneq\Omega\cap N_q\subsetneq\Omega$ if and only if $\beta+1\leq\gamma$ and $2\overline{n}\notin N_q$.*

Proof. To prove (i), assume that $\beta+1\leq\gamma$. Then, by Theorem 2, it can be concluded that $2^{\beta+1}\in N_q$. Hence, $\Omega\cap N_q\neq\emptyset$.

Conversely, assume that $\beta+1>\gamma\geq 1$. Then, $\beta+1\geq 2$. Let $j\in\Omega$. By Lemma 5, $j=2^{\beta+1}k$ for some $k|n'$. Therefore, $j\notin N_q$ by Theorem 2, which implies $\Omega\cap N_q=\emptyset$.

To prove (ii), assume that $\Omega\cap N_q=\Omega$. Then, $\Omega\subseteq N_q$. Since $2\overline{n}\in\Omega$, we have $2\overline{n}\in N_q$. Hence, $2^{\beta+1}n'=2\overline{n}\in N_q$ which implies $\beta+1\leq\gamma$ by Theorem 2.

Conversely, assume that $\beta+1\leq\gamma$ and $2\overline{n}\in N_q$. Let $j\in\Omega$. Then, $j|2\overline{n}$. Since $2\overline{n}\in N_q$, $j\in N_q$, $\Omega\subseteq N_q$.

Statement (iii) follows immediately from (i) and (ii). □

By Proposition 1, we have the following corollary.

Corollary 3. *Let $\gamma \geq 1$ be the integer such that $2^\gamma || (q+1)$. Then, the following statements hold:*

1. $B_{\overline{n},-1,q} = 0$ *if and only if* $\beta + 1 > \gamma$.
2. $B_{\overline{n},-1,q} = \overline{n}$ *if and only if* $\beta + 1 \leq \gamma$ *and* $2\overline{n} \in N_q$.
3. $0 < B_{\overline{n},-1,q} < \overline{n}$ *if and only if* $\beta + 1 \leq \gamma$ *and* $2\overline{n} \notin N_q$.

Proof. By Proposition 1, $\beta + 1 > \gamma$ if and only if $\Omega \cap N_q = \emptyset$. Equivalently,

$$B_{\overline{n},-1,q} = \sum_{j \in \Omega \cap N_q} \phi(j) = \sum_{j \in \emptyset} \phi(j) = 0.$$

This proves (i).

By Proposition 1, $\beta + 1 \leq \gamma$ and $2\overline{n} \in N_q$ if and only if $\Omega \cap N_q = \Omega$. Equivalently,

$$B_{\overline{n},-1,q} = \sum_{j \in \Omega \cap N_q} \phi(j) = \sum_{j \in \Omega} \phi(j) = \sum_{k | n'} \phi(2^{\beta+1}k) = 2^\beta \sum_{k | n'} \phi(k) = 2^\beta n' = \overline{n}.$$

Statement (iii) can be deduced directly from (i) and (ii). □

Corollary 4. *Assume the notations as above. Then, the following statements hold:*

1. $E(n,-1,q) = n\left(\frac{1}{3} - \frac{1}{6(p^\nu+1)}\right)$ *if and only if* $\beta + 1 > \gamma$.
2. *If* $\beta + 1 > \gamma$, *then* $\frac{n}{4} \leq E(n,-1,q) < \frac{n}{3}$.

Proof. The first statement can be deduced directly from Theorem 1 and Corollary 3. The second statement follows from Corollary 1 and the fact that $\frac{1}{6(p^\nu+1)}$ reaches its maximum value $\frac{1}{12}$ when $\nu = 0$. □

Next, we focus on the case where $\beta + 1 \leq \gamma$. Let ℓ be a positive integer relatively prime to q. Let $\ell = 2^\beta p_1^{e_1} \dots p_k^{e_k}$ be the prime factorization of ℓ, where $\beta \geq 0$, $k \geq 0$, $p_1, p_2, \dots, p_k$ are distinct odd primes, and $e_i \geq 1$ for all $i = 1, 2, \dots, k$. Partition the index set $\{1, \dots, k\}$ into $K', K_1, K_2, \dots$ as follows:

1. $i \in K'$ if $p_i \notin P_{q,\alpha}$ for all $\alpha \geq 1$,
2. $i \in K_\alpha$ if $p_i \in P_{q,\alpha}$.

Let $d' = \prod_{i \in K'} p_i^{e_i}$ and $d_\alpha = \prod_{i \in K_\alpha} p_i^{e_i}$ for all $1 \leq \alpha \leq k$. For convenience, the empty product will be referred to as 1. Therefore, we have $\ell = 2^\beta d' d_1 d_2 \dots$ which is called the N_q-factorization of ℓ, where $d_i = 1$ for all but finitely many integers i. By Theorem 2, we have $d_\alpha \in P_{q,\alpha}$. The characterization of $\ell \notin N_q$ is given in the following lemma.

Lemma 6 (Lemma 9 of [9])**.** *Let $\gamma \geq 1$ be the integer such that $2^\gamma || (q+1)$. Let $\ell \geq 2$ be such that $\gcd(\ell, q) = 1$ and let $\ell = 2^\beta d' d_1 d_2 \dots$ be the N_q-factorization of ℓ. If $\ell \notin N_q$, then at least one of the following conditions is valid:*

1. $\beta > \gamma$.
2. $d' > 1$.
3. $\beta \geq 2$ *and* $d_\alpha > 1$ *for an integer* $\alpha \geq 2$.
4. $d_{\alpha_1} > 1$ *and* $d_{\alpha_2} > 1$ *for two distinct* $\alpha_1 \geq 1$ *and* $\alpha_2 \geq 1$.

The following proposition provides a simplified expression of $B_{\overline{n},-1,q}$.

Proposition 2. *Let $\overline{n} = 2^\beta d' d_1 d_2 \ldots$ be an N_q-factorization of $\overline{n} = 2^\beta n'$. If $\beta + 1 \leq \gamma$ and $2\overline{n} \notin N_q$, then*

$$B_{\overline{n},-1,q} = \begin{cases} d_1 + \sum_{\alpha \geq 2}(d_\alpha - 1), & \text{if } \beta = 0, \\ 2^\beta d_1, & \text{if } \beta \neq 0. \end{cases}$$

Proof. We distinguish the proof into two cases where $\beta = 0$ and $\beta \neq 0$.

Case 1 $\beta = 0$. We have $\overline{n} = d' d_1 d_2 \ldots = n'$. By Lemma 5 and Theorem 2, we have

$$\begin{aligned} B_{\overline{n},-1,q} &= \sum_{j \in \Omega \cap N_q} \phi(j) = \sum_{k | \overline{n},\ 2k \in N_q} \phi(2k) = \phi(2) + \sum_{\alpha \geq 1} \sum_{k | d_\alpha,\ k \neq 1} \phi(2k) \\ &= 1 + \sum_{\alpha \geq 1} \sum_{k | d_\alpha,\ k \neq 1} \phi(k) = 1 + \sum_{\alpha \geq 1} (d_\alpha - 1) = d_1 + \sum_{\alpha \geq 2} (d_\alpha - 1). \end{aligned}$$

Case 2 $\beta \neq 0$. We have $\beta + 1 \geq 2$ and $\overline{n} = 2^\beta d' d_1 d_2 \ldots = 2^\beta n'$. By Corollary 2, we have $2^{\beta+1} k \in N_q$. Since $k | n'$ if and only if $k | d_1$, it follows that

$$B_{\overline{n},-1,q} = \sum_{j \in \Omega \cap N_q} \phi(j) = \sum_{k | n',\ 2^{\beta+1} k \in N_q} \phi(2^{\beta+1} k) = \sum_{k | d_1} \phi(2^{\beta+1} k) = 2^\beta \sum_{k | d_1} \phi(k) = 2^\beta d_1.$$

The results follow.

□

Theorem 3. *Let q be an odd prime power and $2^\gamma || (q+1)$. Let $n = \overline{n} p^\nu$, where $p \nmid \overline{n}$ and $\nu \geq 0$. Let $\overline{n} = 2^\beta n'$, where $2 \nmid n'$. Then, the following statements hold:*

1. *$E(n,-1,q) = 0$ if and only if $\beta + 1 \leq \gamma$, $\nu = 0$, and $2\overline{n} \in N_q$.*
2. *If $\beta + 1 \leq \gamma$, $\nu > 0$, and $2\overline{n} \in N_q$, then $\frac{n}{6} \leq E(n,-1,q) < \frac{n}{4}$.*
3. *If $\beta + 1 \leq \gamma$ and $2\overline{n} \notin N_q$, then $\frac{n}{12} \leq E(n,-1,q) < \frac{n}{3}$.*

Proof. By Equation (3), $E(n,-1,q) = 0$ if and only if

$$\frac{B_{\overline{n},-1,q}}{\overline{n}} = \frac{4p^{2\nu} + 2p^\nu}{p^{2\nu} + 2p^\nu + 3}.$$

By Corollary 3, it is not difficult to see that $\frac{B_{\overline{n},-1,q}}{\overline{n}} \leq 1$ and $\frac{B_{\overline{n},-1,q}}{\overline{n}} = 1$ if and only if $\beta + 1 \leq \gamma$ and $2\overline{n} \in N_q$. On the other hand, we have $\frac{4p^{2\nu}+2p^\nu}{p^{2\nu}+2p^\nu+3} \geq 1$ and $\frac{4p^{2\nu}+2p^\nu}{p^{2\nu}+2p^\nu+3} = 1$ if and only if $p^\nu = 1$. Therefore, $\frac{B_{\overline{n},-1,q}}{\overline{n}} = \frac{4p^{2\nu}+2p^\nu}{p^{2\nu}+2p^\nu+3}$ if and only if $\beta + 1 \leq \gamma$, $2\overline{n} \in N_q$ and $p^\nu = 1$. This proves (i).

To prove (ii), assume that $\beta + 1 \leq \gamma$, $\nu > 0$, and $2\overline{n} \in N_q$. By Corollary 3, we have $B_{\overline{n},-1,q} = \overline{n}$. By Equation (3), it follows that

$$E(n,-1,q) = n\left(\frac{2p^\nu + 1}{6(p^\nu + 1)}\right) - \overline{n}\left(\frac{p^{2\nu} + 2p^\nu + 3}{12(p^\nu + 1)}\right) = \frac{\overline{n}}{12(p^\nu + 1)}\left(3p^{2\nu} - 3\right) = \frac{n}{4}\left(1 - \frac{1}{p^\nu}\right).$$

It is not difficult to see that $E(n,-1,q) < \frac{n}{4}$. Since $\nu > 0$, it follows that $p^\nu \geq 3$. Hence, the minimum value of $1 - \frac{1}{p^\nu}$ is $\frac{2}{3}$. Therefore, we have $\frac{n}{6} \leq E(n,-1,q) < \frac{n}{4}$.

To prove (iii), assume that $\beta + 1 \leq \gamma$ and $2\overline{n} \notin N_q$.

Case 1 $\gcd(n,q) \neq 1$. By Corollary 1, we have $E(n,-1,q) = \frac{\overline{n} - B_{\overline{n},-1,q}}{4}$. Then, by Equation (3), $E(n,-1,q)$ can be expressed as

$$\frac{E(n,-1,q)}{n} = \frac{1}{4} - \frac{1}{4p^\nu} + \frac{E(\bar{n},-1,q)}{n}\left(\frac{p^{2\nu} + 2p^\nu + 3}{3(p^\nu + 1)}\right) \geq \frac{1}{4} - \frac{1}{4p^\nu}. \tag{4}$$

It is not difficult to see that $\frac{E(n,-1,q)}{n} \geq \frac{1}{6}$ for all $p^\nu \geq 3$. Hence, $E(n,-1,q) \geq \frac{n}{6}$.

Case 2 $\gcd(n,q) = 1$. Let $\overline{n} = 2^\beta d' d_1 d_2 \dots$ be an N_q-factorization of $\overline{n}$ and

$$\overline{n} = 2^\beta d' d_1 d_2 \dots = 2^\beta d' d_{\alpha_1} d_{\alpha_2} \dots d_{\alpha_j},$$

where $d_{\alpha_i} > 1$ for all $1 \leq i \leq j$ and $\alpha_1 < \alpha_2 < \cdots < \alpha_j$. Note that if d_{α_i} and d' are greater than 1, then they are greater than or equal to 3.

Case 2.1 $\beta = 0$. We have $\overline{n} = d' d_{\alpha_1} d_{\alpha_2} \dots d_{\alpha_j}$. It is easy to verify that

$$\frac{B_{\overline{n},-1,q}}{n} = \frac{d_1 + \sum_{\alpha \geq 2}(d_\alpha - 1)}{d' d_1 d_2 \dots} = \frac{1 - j + \sum_{i=1}^{j} d_{\alpha_j}}{d' d_{\alpha_1} d_{\alpha_2} \dots d_{\alpha_j}}.$$

By Lemma 6, we have the following six subcases:

Case 2.1.1 $d' = 1$ and $j = 0$. Then, $\overline{n} = 1$ and $2\overline{n} = 2 \in N_q$, a contradiction.

Case 2.1.2 $d' = 1$ and $j = 1$. Thus, $\overline{n} = d_{\alpha_1}, 2\overline{n} = 2d_{\alpha_1} \in N_q$, a contradiction.

Case 2.1.3 $d' > 1$ and $j = 0$. We have $\overline{n} = d'$. Thus, $\frac{B_{\overline{n},-1,q}}{n} = \frac{1}{d'} \leq \frac{1}{3}$.

Case 2.1.4 $d' > 1$ and $j = 1$. Thus, $\overline{n} = d' d_{\alpha_1}$. Therefore, $\frac{B_{\overline{n},-1,q}}{n} = \frac{d_{\alpha_1}}{d' d_{\alpha_1}} = \frac{1}{d'} \leq \frac{1}{3}$.

Case 2.1.5 $j = 2$. Hence, $\overline{n} = d' d_{\alpha_1} d_{\alpha_2}$. Without loss of generality, we may assume that $d_{\alpha_2} \leq d_{\alpha_1}$. We have

$$\frac{B_{\overline{n},-1,q}}{n} = \frac{-1 + d_{\alpha_1} + d_{\alpha_2}}{d' d_{\alpha_1} d_{\alpha_2}} \leq \frac{2d_{\alpha_1}}{d' d_{\alpha_1} d_{\alpha_2}} \leq \frac{2}{d' d_{\alpha_2}} \leq \frac{2}{d_{\alpha_2}} \leq \frac{2}{3}.$$

Case 2.1.6 $j \geq 3$. Then, $\overline{n} = d' d_{\alpha_1} d_{\alpha_2} \dots d_{\alpha_j}$. Let $d_{\alpha_r} = \max_{1 \leq i \leq j} d_{\alpha_i}$.

$$\frac{B_{\overline{n},-1,q}}{n} = \frac{1 - j + \sum_{i=1}^{j} d_{\alpha_i}}{d' d_{\alpha_1} \dots d_{\alpha_j}} \leq \frac{\sum_{i=1}^{j} d_{\alpha_i}}{d' d_{\alpha_1} \dots d_{\alpha_j}} \leq \frac{j d_{\alpha_r}}{d' d_{\alpha_1} \dots d_{\alpha_j}} = \frac{j}{d' \prod_{1 \leq i \leq j,\, i \neq r} d_{\alpha_i}} \leq \frac{j}{\prod_{1 \leq i \leq j,\, i \neq r} d_{\alpha_i}}.$$

Let s be an index such that $j - 1 \leq s \leq j$ and $s \neq r$. Then, $j < 2^{j-1} \leq 2^s \leq 2^{\alpha_s}$. Since $d_{\alpha_s} \in P_{q,\alpha_s}$, we have $d_{\alpha_s} \geq 2^{\alpha_s} + 1$ by Lemma 3. Hence, $j < 2^{\alpha_s} < d_{\alpha_s}$. Therefore,

$$\frac{B_{\overline{n},-1,q}}{n} \leq \frac{j}{\prod_{1 \leq i \leq j,\, i \neq r} d_{\alpha_i}} \leq \frac{d_{\alpha_s}}{\prod_{1 \leq i \leq j,\, i \neq r} d_{\alpha_i}} = \frac{1}{\prod_{1 \leq i \leq j,\, i \neq r, i \neq s} d_{\alpha_i}} \leq \frac{1}{3}.$$

Case 2.2 $\beta \neq 0$. Then, $\overline{n} = 2^\beta d' d_1 d_2 \dots = 2^\beta d' d_{\alpha_1} d_{\alpha_2} \dots d_{\alpha_j}$. It follows that

$$\frac{B_{\overline{n},-1,q}}{n} = \frac{2^\beta d_1}{2^\beta d' d_1 d_2 \dots} = \frac{1}{d' d_2 d_3 \dots}.$$

By Lemma 6, we have the following six subcases.

Case 2.2.1 $d' = 1$ and $j = 0$. Then, $\overline{n} = 2^\beta$ and $2\overline{n} = 2^{\beta+1} \in N_q$, a contradiction.

Case 2.2.2 $d' = 1$ and $j = 1$. Note that $\beta + 1 \geq 2$. If $\alpha_1 = 1$, then $\overline{n} = 2^\beta d_1$ and $2\overline{n} = 2^{\beta+1} d_1 \in N_q$, a contradiction. Otherwise, $\alpha_1 \neq 1$. Then, $\overline{n} = 2^\beta d_{\alpha_1}$ and $2\overline{n} = 2^{\beta+1} d_{\alpha_1} \notin N_q$. Hence,

$$\frac{B_{\overline{n},-1,q}}{n} = \frac{1}{d_{\alpha_1}} \leq \frac{1}{3}.$$

Case 2.2.3 $d' > 1$ and $j = 0$. Then, $\overline{n} = 2^\beta d'$ and $2\overline{n} = 2^{\beta+1} d'$. Hence,

$$\frac{B_{\overline{n},-1,q}}{n} = \frac{1}{d'} \leq \frac{1}{3}.$$

Case 2.2.4 $d' > 1$ and $j = 1$. Then, $\overline{n} = d'd_{\alpha_1}$. It follows that

$$\frac{B_{\overline{n},-1,q}}{n} \leq \frac{1}{d'} \leq \frac{1}{3}.$$

Case 2.2.5 $j = 2$. Then, $\overline{n} = d'd_{\alpha_1}d_{\alpha_2}$. We have

$$\frac{B_{\overline{n},-1,q}}{n} \leq \frac{1}{d'd_{\alpha_2}} \leq \frac{1}{d_{\alpha_2}} \leq \frac{1}{3}.$$

Case 2.2.6 $j \geq 3$. Then, $\overline{n} = d'd_{\alpha_1} \dots d_{\alpha_j}$. Hence,

$$\frac{B_{\overline{n},-1,q}}{n} \leq \frac{1}{d'd_{\alpha_2} \dots d_{\alpha_j}} \leq \frac{1}{d_{\alpha_j}} \leq \frac{1}{3}.$$

Altogether, we have $B_{\overline{n},-1,q} \leq \frac{2n}{3}$, and, hence,

$$E(n,-1,q) = \frac{\overline{n} - B_{\overline{n},-1,q}}{4} \geq \frac{n - \frac{2n}{3}}{4} = \frac{n}{12}.$$

□

From Theorem 3 and Corollary 4, we can conclude that the average dimension of the Hull of negacyclic codes of length $n = p^\nu \overline{n}$ over $\mathbb{F}_q$ is zero if and only if $\beta + 1 \leq \gamma$, $\nu = 0$, and $2\overline{n} \in N_q$. For the other cases, the average dimension of the Hull of negacyclic codes of length $n = p^\nu \overline{n}$ over $\mathbb{F}_q$ is bounded by $\frac{n}{12}$ and $\frac{n}{3}$. In these cases, $E(n,-1,q)$ grows at the same rate as the length n of the codes as n tends to ∞.

5. Conclusions

Due to their wide applications and links with the efficiency of some algorithms in coding theory, properties of hulls of cyclic codes and their generalization in terms of λ-constacyclic codes have been extensively studied. The average dimension of the Euclidean hull of cyclic codes has been studied in [9]. A complete study of the average dimension of the Hermitian hull of cyclic and constacyclic codes was given in [11,12]. Therefore, the remaining case is the Euclidean hull of negacyclic codes (see [13]). This paper provides a complete study for this problem. The detailed comparison for the results on the Euclidean case is given in Table 1 and the Hermitian case is given in [12].

Table 1. The lower and upper bounds for $E(n,1,q)$ and $E(n,-1,q)$.

λ	$n = p^\nu \overline{n}$	Lower Bounds	Upper Bounds	Remarks
1	$n \in N_q$	0	0	Theorem 25 of [9]
	$n \notin N_q$	$\frac{n}{12}$	$\frac{n}{3}$	
-1	$\beta + 1 > \gamma$	$\frac{n}{4}$	$\frac{n}{3}$	Corollary 4
	$\beta + 1 \leq \gamma$, $\nu = 0$, and $2\overline{n} \in N_q$	0	0	Theorem 3
	$\beta + 1 \leq \gamma$, $\nu > 0$, and $2\overline{n} \in N_q$	$\frac{n}{6}$	$\frac{n}{4}$	
	$\beta + 1 \leq \gamma$ and $2\overline{n} \notin N_q$	$\frac{n}{12}$	$\frac{n}{3}$	

Author Contributions: E.S. gave the initial concept and established the results in Section 4. S.J. stated and proved the results in Section 3. S.J. and E.S. wrote the paper.

Acknowledgments: This research was supported by the Thailand Research Fund and the Office of Higher Education Commission of Thailand under Research Grant MRG6080054.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Assmus, E.F.; Key, J.D. Affine and projective planes. *Discrete Math.* **1990**, *83*, 161–187. [CrossRef]
2. Leon, J. Computing automorphism groups of error-correcting codes. *IEEE Trans. Inf. Theory* **1982**, *3*, 496–511. [CrossRef]
3. Leon, J. Permutation group algorithms based on partition, I: theory and algorithms. *J. Symbolic Comput.* **1991**, *12*, 533–583. [CrossRef]
4. Sendrier, N. Finding the permutation between equivalent binary code. In Proceedings of the IEEE International Symposium on Information Theory, Ulm, Germany, 29 June–4 July 1997.
5. Sendrier, N. Finding the permutation between equivalent codes: The support splitting algorithm. *IEEE Trans. Inf. Theory* **2000**, *46*, 1193–1203. [CrossRef]
6. Sendrier, N.; Skersys, G. On the computation of the automorphism group of a linear code. In Proceedings of the 2001 IEEE International Symposium on Information Theory, Washington, DC, USA, 29 June 2001.
7. Guenda, K.; Jitman, S.; Gulliver, T.A. Constructions of good entanglement-assisted quantum error correcting codes. *Des. Codes Cryptogr.* **2018**, *86*, 121–136. [CrossRef]
8. Sendrier, N. On the dimension of the hull. *SIAM J. Appl. Math.* **1997**, *10*, 282–293. [CrossRef]
9. Skersys, G. The average dimension of the hull of cyclic codes. *Discrete Appl. Math.* **2003**, *128*, 275–292. [CrossRef]
10. Sangwisut, E.; Jitman, S.; Ling, S.; Udomkavanich, P. Hulls of cyclic and negacyclic codes over finite fields. *Finite Fields Appl.* **2015**, *33*, 232–257. [CrossRef]
11. Jitman, S.; Sangwisut, E. The average dimension of the Hermitian hull of cyclic codes over finite fields of square order. *AIP Conf. Proc.* **2016** *1775*, 030026.
12. Jitman, S.; Sangwisut, E. The average dimension of the Hermitian hull of constacyclic codes over finite fields. *arXiv* **2017**, arXiv:1702.00275.
13. Yang, Y.; Cai, W. On self-dual constacyclic codes over finite fields. *Des. Codes Cryptogr.* **2015**, *74*, 355–364. [CrossRef]

© 2018 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).