A spectral characterisation of $t$-designs

Cunsheng Ding

Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China

Abstract

There are two standard approaches to the construction of $t$-designs. The first one is based on permutation group actions on certain base blocks. The second one is based on coding theory. These approaches are not effective as no infinite family of $t$-designs with $t \geq 5$ is constructed with them. The objective of this paper is to give a spectral characterisation of all $t$-designs by introducing a characteristic Boolean function of a $t$-design. We will determine the spectra of the characteristic function of $(n - 2)/2\cdot(n,n/2,1)$ Steiner systems and prove properties of such designs.

Keywords: Boolean function, Steiner system, $t$-design, Walsh transform.

2000 MSC: 05B05, 51E10, 94B15

1. Introduction

Let $\mathcal{P}$ be a set of $n \geq 1$ elements, and let $\mathcal{B}$ be a set of $k$-subsets of $\mathcal{P}$, where $k$ is a positive integer with $1 \leq k \leq n$. Let $t$ be a positive integer with $t \leq k$. The pair $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ is called a $t$-(n,k,λ) design, or simply $t$-design, if every $t$-subset of $\mathcal{P}$ is contained in exactly $\lambda$ elements of $\mathcal{B}$. The elements of $\mathcal{P}$ are called points, and those of $\mathcal{B}$ are referred to as blocks. We usually use $b$ to denote the number of blocks in $\mathcal{B}$. A $t$-design is called simple if $\mathcal{B}$ does not contain repeated blocks. In this paper, we consider only simple $t$-designs. A $t$-design is called symmetric if $n = b$. It is clear that $t$-designs with $k = t$ or $k = n$ always exist. Such $t$-designs are trivial. In this paper, we consider only $t$-designs with $n > k > t$. A $t$-(n,k,λ) design is referred to as a Steiner system if $t \geq 2$ and $\lambda = 1$, and is denoted by $S(t,k,n)$.

The existence and constructions of $t$-designs have been a fascinating topic of research for hundreds of years [2, 3, 6, 7, 9, 11, 12]. One fundamental construction is the group action approach [3, Chapter III], which employs transitive or homogeneous permutation groups. The fatal limitation of this approach lies in the fact that highly transitive or homogeneous permutation groups do not exist [3, Chapter V]. Another fundamental construction is based on error-correcting codes [2, 11, 12]. This approach makes use of the automorphism group of the code or the Assmus-Mattson Theorem, and has also limitations. By now no infinite family of 4-designs is directly constructed from codes. While there are many constructions of $t$-designs with flexible parameters in the literature and important progresses on the existence of $t$-designs have been made [8, 10, 14, 15, 16], the author is not aware of any nontrivial characterisation of $t$-(n,k,λ) designs. The main objective of this paper is to present a spectral characterisation of $t$-(n,k,λ) designs. This is done by studying the characteristic Boolean function of a $t$-(n,k,λ) design. As
an application of this characterisation, we will determine the spectra of the characteristic function of \((n - 2)/2\cdot\langle n, n/2, 1 \rangle\) Steiner systems, and prove properties of such designs.

2. Krawtchouk polynomials and their properties

In this section, we introduce Krawtchouk polynomials and summarize their properties, which will be needed in subsequent sections. A proof of these results could be found in [3, Ch. 5, Sections 2 and 7].

Let \(n\) be a positive integer, and let \(x\) be a variable taking nonnegative values. The Krawtchouk polynomial is defined by

\[
P_k(x) = \sum_{j=0}^{k} (-1)^j \binom{x}{j} \binom{n-x}{k-j}
\]

where \(0 \leq k \leq n\). It is easily seen that

\[
(1+z)^{n-x}(1-z)^x = \sum_{k=0}^{n} P_k(x)z^k.
\]

The following alternative expressions will be useful later.

**Theorem 1.** Let symbols and notations be the same as before.
- \(P_k(x) = \sum_{j=0}^{k} (-2)^j \binom{x}{j} \binom{n-x}{k-j}\).
- \(P_k(x) = \sum_{j=0}^{k} (-1)^j 2^{k-j} \binom{n-x+j}{j} \binom{n-x}{k-j}\).

The orthogonality of Krawtchouk polynomials is documented below.

**Theorem 2.** For nonnegative integers \(r\) and \(s\),

\[
\sum_{i=0}^{n} \binom{n}{i} P_r(i)P_s(i) = 2^n \binom{n}{r} \delta_{r,s},
\]

where \(\delta_{r,s} = 1\) if \(r = s\) and \(\delta_{r,s} = 0\) if \(r \neq s\).

**Theorem 3.** For nonnegative integers \(r\) and \(s\),

\[
\binom{n}{i} P_r(i) = \binom{n}{s} P_s(s).
\]

**Theorem 4.** For nonnegative integers \(r\) and \(s\),

\[
\sum_{i=0}^{n} P_r(i)P_s(i) = 2^n \delta_{r,s}.
\]

**Theorem 5.** Let \(u \in GF(2)^n\) with Hamming weight \(\text{wt}(u) = i\). Then

\[
\sum_{\text{wt}(v) = k} (-1)^{u \cdot v} = P_k(i).
\]
The next theorem documents further basic properties of the Krawtchouk polynomials.

**Theorem 6.** Let symbols and notation be as before.
- \( \sum_{k=0}^{n} \binom{n-k}{j} P_k(x) = 2^j \binom{n-x}{j} \).
- \( P_k(i) = (-1)^i P_{n-k}(i), 0 \leq i \leq n. \)
- \( P_n(k) = (-1)^k. \)
- \( P_k(1) = \binom{n-2k}{n}. \)
- \( P_k(0) = \binom{n}{k}. \)

**Theorem 7.** Let symbols and notation be as before. We have
\[ P_k(x) = (-1)^k P_k(n-x). \]

**Proof.** By definition,
\[ P_k(n-x) = \sum_{j=0}^{k} (-1)^j \binom{n-x}{j} \binom{x}{k-j}. \]
Substituting \( k-j \) with \( i \), we get
\[ P_k(n-x) = \sum_{i=0}^{k} (-1)^{k-i} \binom{n-x}{i} \binom{x}{k-i} = (-1)^k P_k(x). \]

\[ \square \]

### 3. Basics of \( t \)-designs

In this paper, we will consider \( t \)-designs with the point set \( \mathcal{P} = \{1, 2, \cdots, n\} \), where \( n \) is a positive integer. For simplicity, we use \([i..j]\) to denote the set \( \{i, i+1, \cdots, j\} \) for any two positive integers \( i \) and \( j \) with \( i \leq j \). For an integer \( i \) with \( 0 \leq i \leq n \), denote by \( \binom{\mathcal{P}}{i} \) the set of all \( i \)-subsets of \( \mathcal{P} \).

We will need the following lemmas later [3, p. 15].

**Lemma 8.** Let \( \mathcal{D} \) be a \( t \)-(\( n,k,\lambda_0 \)) design. Let \( s \) be an integer with \( 1 \leq s \leq t \leq k \). Then \( \mathcal{D} \) is also an \( s \)-(\( n,k,\lambda_s \)) design, where
\[ \lambda_s = \lambda \frac{\binom{n-s}{l-s}}{\binom{k-s}{l-s}}. \]

In addition,
\[ b := \lambda_0 = \lambda \frac{\binom{n}{l}}{\binom{k}{l}} \]
is the number of blocks in the design \( \mathcal{D} \).
Let \( \mathcal{D} = (\mathcal{P}, \mathcal{B}) \) be a \( t-(n,k,\lambda) \) design. Define \( \overline{\mathcal{D}} = \{ \binom{\mathcal{P}}{k} \setminus B : B \in \mathcal{B} \} \), and let \( \overline{\mathcal{D}} = (\mathcal{P}, \overline{\mathcal{B}}) \).

**Lemma 9.** Let \( \mathcal{D} = (\mathcal{P}, \mathcal{B}) \) be a \( t-(n,k,\lambda) \) design. Then \( \overline{\mathcal{D}} = (\mathcal{P}, \overline{\mathcal{B}}) \) is an \( s-(n,n-k,\overline{\lambda}_s) \) design for all \( 1 \leq s \leq t \), where

\[
\overline{\lambda}_s = \sum_{i=0}^{s} (-1)^i \binom{s}{i} \lambda_i.
\]  

(7)

In particular,

\[
\overline{\lambda}_t := \frac{\lambda^{(n-k)}_t}{t}.
\]

The design \( \overline{\mathcal{D}} \) is called the complement design of \( \mathcal{D} \). We will employ the two foregoing lemmas later.

Let \( \mathcal{D} = (\mathcal{P}, \mathcal{B}) \) be a \( t-(n,k,\lambda) \) design. Let \( i \) and \( j \) be two nonnegative integers, and let \( X = \{ p_1, p_2, \ldots, p_{i+j} \} \) be a set of distinct points. Denote by \( \lambda_{(i,j)} \) the number of blocks \( B_t \) of \( \mathcal{D} \) such that

\[
B_t \cap \{ p_1, p_2, \ldots, p_{i+j} \} = Y := \{ p_1, p_2, \ldots, p_i \}.
\]

These numbers \( \lambda_{(i,j)} \) are called block intersection numbers.

A proof of the following theorem can be found in [3, p. 101].

**Theorem 10.** Let \( \mathcal{D} = (\mathcal{P}, \mathcal{B}) \) be a \( t-(n,k,\lambda) \) design. Let \( i \) and \( j \) be nonnegative integers. Then the number \( \lambda_{(i,j)} \) depends only on \( i \) and \( j \), but not the points in \( X \) and \( Y \) if \( i+j \leq t \) or \( \lambda = 1 \) and \( X \) is contained in some block of \( \mathcal{D} \).

We first have the following result.

**Lemma 11.** Let \( \mathcal{D} = (\mathcal{P}, \mathcal{B}) \) be a \( t-(n,k,\lambda) \) design. Let \( i \) and \( j \) be nonnegative integers. If \( 0 \leq i + j \leq t \), then

\[
\lambda_{(i,j)} = \frac{\lambda^{(n-i-j)}_{(k-i)}}{(k-i)}.
\]

The following facts about these \( \lambda_{(i,j)} \) are well known:

- \( \lambda_{(i,0)} = \lambda_i \) for \( 0 \leq i \leq t \).
- \( \lambda_{(0,j)} = \lambda_j \) for \( 0 \leq i \leq t \).
- \( \lambda_{(i,j)} = \lambda_{(i,j-1)} + \lambda_{(i+1,j)} \) for \( i + j \leq t \), which is called the triangular formula.

Consider now a \( t-(n,t+1,1) \) design \( \mathcal{D} \). Let \( X \) be any block of \( \mathcal{D} \) and let \( Y \) be an \( i \)-subset of \( X \). Denote by \( \lambda_{(i,t+1-j)}(X,Y) \) the number of blocks \( B_j \) in \( \mathcal{B} \) such that \( B_j \cap X = Y \),

where \( X \) is a block in \( \mathcal{B} \) and \( Y \) is \( i \)-subset of \( X \). By Theorem 11, these numbers \( \lambda_{(i,t+1-j)}(X,Y) \) depend only on \( i \) and \( t \). Hence, the triangle formula above still holds for \( 0 \leq i + j \leq t + 1 \) [2, p. 9].

We have then the following theorem.
Theorem 12. Let $\mathbb{D}$ be a $t$-$(n,t+1,1)$ design $\mathbb{D}$. Let $X$ be any block of $\mathbb{D}$ and let $Y$ be a $j$-subset of $X$. Then

$$\hat{\lambda}_{(t-(j-1),j)}(X,Y) = (-1)^{j-1} \sum_{\ell=0}^{j-1} (-1)^{j} \binom{n-1}{\ell+1} + (-1)^j$$

for $1 \leq j \leq t+1$.

Proof. With the triangular formula, we have

$$\hat{\lambda}_{(t-(j-1),j)}(X,Y) = (-1)^j \hat{\lambda}_{(t+1,0)}(X,\emptyset) + \sum_{\ell=0}^{j-1} (-1)^{j} \hat{\lambda}_{(t-(j-1)+\ell,j-1-\ell)}$$

for $1 \leq j \leq t+1$. By definition, $\hat{\lambda}_{(t+1,0)}(X,\emptyset) = 1$. The desired conclusion then follows from Lemma 11.

4. A spectral characterization of $t$-designs

A Boolean function with $n$ variables is a function $f(x_1,x_2,\ldots,x_n)$ from $\text{GF}(2)^n$ to $\{0,1\}$, which is viewed as a subset of the set of real numbers. In other words, Boolean functions in this paper are special real-valued functions unless otherwise stated. Let $x = (x_1,x_2,\ldots,x_n)$. The first kind of Walsh transform $\hat{f}$ of $f$ is defined by

$$\hat{f}(w) = \sum_{x \in \text{GF}(2)^n} f(x)(-1)^{w \cdot x},$$

where $w = (w_1,w_2,\ldots,w_n) \in \text{GF}(2)^n$, $w \cdot x = \sum_{i=1}^{n} w_i x_i$ is the standard inner product in the vector space $\text{GF}(2)^n$. The multiset $\{\hat{f}(w) : w \in \text{GF}(2)^n\}$ is called the spectra of $f(x)$. It is easily verified that the inverse transform is given by

$$f(x) = \frac{1}{2^n} \sum_{w \in \text{GF}(2)^n} \hat{f}(w)(-1)^{w \cdot x}.$$  

The support $\text{Supp}(f)$ of $f$ is defined by

$$\text{Supp}(f) = \{ u \in \text{GF}(2)^n : f(u) = 1 \} \subseteq \text{GF}(2)^n.$$ 

The mapping $f \mapsto \text{Supp}(f)$ is a one-to-one correspondence from the set of all Boolean functions with $n$ variables to the power set of $\text{GF}(2)^n$. The weight $\omega(f)$ of $f$ is defined to be the cardinality of $\text{Supp}(f)$.

The support of a vector $b = (b_1,b_2,\ldots,b_n) \in \text{GF}(2)^n$ is defined by

$$\text{Supp}(b) = \{ 1 \leq i \leq n : b_i = 1 \} \subseteq [1..n],$$

where $[i..j]$ denotes the set $\{i,i+1,\ldots,j\}$ for two nonnegative integers $i$ and $j$ with $i \leq j$. It is obvious that the mapping

$$\varphi : b \mapsto \text{Supp}(b)$$

is a one-to-one correspondence from $\text{GF}(2)^n$ to $2^{[1..n]}$, which denotes the power set of $[1..n]$. 

5
Let \( \mathcal{P} = [1..n] \) be a set of \( n \geq 1 \) elements, and let \( \mathcal{B} = \{ B_i : 1 \leq i \leq b \} \) be a set of \( k \)-subsets of \( \mathcal{P} \), where \( k \) is a positive integer with \( 1 \leq k \leq n \), and \( b \) is a positive integer. The pair \( \mathcal{D} = (\mathcal{P}, \mathcal{B}) \) is called an incidence structure. The characteristic function of the incidence structure \( \mathcal{D} \), denoted by \( f_\mathcal{D}(x) \), is the Boolean function of \( n \) variables with support
\[
\{ \varphi^{-1}(B_i) : 1 \leq i \leq b \}.
\] (12)

We are now ready to present a spectral characterization of \( t \)-designs.

**Theorem 13.** Let \( \mathcal{D} = (\mathcal{P}, \mathcal{B}) \) be an incidence structure, where the point set \( \mathcal{P} = [1..n] \), the block set \( \mathcal{B} = \{ B_1, B_2, \ldots, B_b \} \), the block size \( |B_i| \) is \( k \), and \( k \) and \( b \) are positive integers. Then \( \mathcal{D} \) is a \( t \)-(\( n,k,\lambda \)) design if and only if for each integer \( h \) with \( 0 \leq h \leq t \),
\[
\hat{f}_\mathcal{D}(w) = \frac{\lambda \sum_{i=0}^{h} (-1)^i \binom{h}{i} \binom{n-h}{k-i}}{\binom{n}{k}} = \frac{\lambda P_{\lambda}^{(h)}(h)}{\binom{n}{k}}
\] (13)
for all \( w \in \text{GF}(2)^n \) with \( \varpi(w) = h \).

**Proof.** We first prove the necessity of the conditions in (13). Assume that \( \mathcal{D} \) is a \( t \)-(\( n,k,\lambda \)) design. Let \( w \) be a vector in \( \text{GF}(2)^n \) with \( \varpi(w) = h \), where \( 0 \leq h \leq t \). The inner product \( w \cdot \varphi^{-1}(B_i) \) is given by
\[
w \cdot \varphi^{-1}(B_i) = |\text{Suppt}(w) \cap B_i| \mod 2.
\]
Note that \( |\text{Suppt}(w) \cap B_i| \) takes on only values in the following set
\[
\{0, h, h-1, \ldots, 1, 0\}.
\]

It then follows from Lemma 11 that
\[
|\{1 \leq j \leq b : |\text{Suppt}(w) \cap B_j| = i\}| = \binom{h}{i} \lambda \text{Suppt}(w, i) = \frac{\lambda \binom{h}{i} \binom{n-h}{k-i}}{\binom{n}{k}},
\]
where \( 0 \leq i \leq h \). Note that \( h \leq t \leq k \). By convention, \( \binom{h}{i} = 0 \) if \( i > h \). We now deduce that
\[
\hat{f}_\mathcal{D}(w) = \sum_{i=0}^{h} (-1)^i |\{1 \leq j \leq b : |\text{Suppt}(w) \cap B_j| = i\}|
\]
\[
= \lambda \sum_{i=0}^{h} (-1)^i \binom{h}{i} \binom{n-h}{k-i}
\]
\[
= \lambda \sum_{i=0}^{k} (-1)^i \binom{h}{i} \binom{n-h}{k-i}
\]
\[
= \lambda P_{\lambda}^{(h)}(h)
\]
\[
\frac{\binom{n}{k}}{\binom{n}{k}}.
\]
This proves the necessity of the conditions in (13).

We now prove the sufficiency of the conditions in (13) by induction. We first prove that \( \mathcal{D} \) is a \( 1-(n,k,\lambda_1) \) design. For each \( w \) in \( \text{GF}(2)^n \) with weight 1, the conditions in (13) in the case \( h = 1 \) say that
\[
\hat{f}_\mathcal{D}(w) = \lambda P_{\lambda}(1)
\]
}\( \binom{n}{k} \).
The first alternative expression of the Krawtchouk polynomial given in Theorem 1 yields

\[ P_k(1) = \binom{n}{k} - 2 \binom{n-1}{k-1}. \]

We have then

\[ \hat{f}_D(w) = \lambda_0 \frac{\binom{n}{k} - 2 \binom{n-1}{k-1}}{\binom{n-t}{k-t}}. \]  \hspace{1cm} (14)

By the definition of binomial coefficients,

\[ \binom{n}{k} \binom{k}{t} = \frac{n!}{k!(n-k)!} \frac{k!}{t!(k-t)!} = \frac{n!}{t!(n-t)!(k-t)!} = \binom{n}{t} \binom{n-t}{k-t}. \]

Consequently,

\[ \frac{\binom{n}{k}}{\binom{n-t}{k-t}} = \binom{n}{t} \binom{n-t}{k-t}. \]  \hspace{1cm} (15)

Similarly, one can prove that

\[ \frac{\binom{n-1}{k-1}}{\binom{n-t-1}{k-t-1}} = \binom{n-1}{t} \binom{n-t-1}{k-t-1}. \]  \hspace{1cm} (16)

Plugging (15) and (16) into (14), we obtain

\[ \hat{f}_D(w) = \lambda_0 - 2\lambda_1 = b - 2\lambda_1. \]

Suppose that Suppt(w) = \{i\}, where 1 ≤ i ≤ n. Assume that i is incident with u blocks in \( B \). It then follows from the definition of \( \hat{f}_D(w) \) that

\[ \hat{f}_D(w) = b - 2u. \]

Consequently, \( u = \lambda_1 \), which is independent of i. By definition, \( D \) is a 1-(n, k, \lambda_1) design.

Suppose now that \( D \) is an s-(n, k, \lambda_s) design for all s with 1 ≤ s ≤ h - 1 and h ≤ t. We now prove that it is also an h-(n, k, \lambda_h) design. Let w be a vector in GF(2)^n with Hamming weight h. By induction hypothesis and Lemma 11 we have

\[ |\{1 \leq j \leq b : \text{Suppt}(w) \cap B_i = i\}| = \binom{h}{i} \lambda_{(i,h-i)} \]
for all \( i \) with \( 1 \leq i \leq h - 1 \). As a result, we obtain

\[
\hat{f}_D(w) = \sum_{i=1}^{b} (-1)^{\phi^{-1}(B_i) \cdot w}
\]

\[
= \sum_{i=0}^{h} (-1)^i \sum_{j=0}^{b-1} (-1)^j \left\{ 1 \leq j \leq b : |\text{Suppt}(w) \cap B_i| = i \right\}
\]

\[
= \sum_{i=0}^{\frac{b-1}{2}} (-1)^i \sum_{j=0}^{\frac{b-1}{2}} (-1)^j \left\{ 1 \leq j \leq b : |\text{Suppt}(w) \cap B_i| = i \right\}
\]

\[
= \sum_{i=0}^{\frac{b-1}{2}} (-1)^i \left[ \left( \frac{h}{i} \right) \lambda_i \right]
\]

\[
\sum_{i=0}^{\frac{b-1}{2}} (-1)^i \left[ \left( \frac{h}{i} \right) \lambda_i \right] + \sum_{i=0}^{\frac{b-1}{2}} (-1)^i \left( \frac{h}{i} \right) \lambda_i.
\]

It then follows from (13) that

\[
\left| \left\{ 1 \leq j \leq b : |\text{Suppt}(w) \cap B_i| = h \right\} \right| = \frac{\lambda_{(\frac{k-b}{k})}}{\binom{n-h}{k}} = \frac{\lambda_{(\frac{k-b}{k})}}{\binom{n-h}{k}} = \lambda_b,
\]

which depends only on \( h \). By assumption, \( \text{Suppt}(w) = h \). This means that \( \text{Suppt}(w) \) is contained in exactly \( \lambda_b \) blocks in \( B \). The proof is then completed.

\[\square\]

**Example 1** (Fano plane in finite geometry). Let \( \mathcal{P} = \{1, 2, 3, 4, 5, 6, 7\} \) and

\[
\mathcal{B} = \{\{1, 2, 3\}, \{1, 4, 5\}, \{1, 6, 7\}, \{2, 4, 7\}, \{2, 5, 6\}, \{3, 4, 6\}, \{3, 5, 7\}\}.
\]

Then \( \mathbb{D} = (\mathcal{P}, \mathcal{B}) \) is a 2-(7,3,1) design, i.e., Steiner triple system \( S(2,3,7) \).

The characteristic function \( f_\mathbb{D} \) of \( \mathbb{D} \) is given by

\[
x_1x_2x_3x_4x_5x_6x_7 + x_1x_2x_3x_4 + x_1x_2x_3x_5 + x_1x_2x_3x_6 + x_1x_2x_3x_7 + x_1x_2x_4x_5 + x_1x_2x_4x_6 + x_1x_2x_4x_7 + x_1x_2x_5x_6 + x_1x_2x_5x_7 + x_1x_2x_6x_7 + x_1x_3x_4x_5 + x_1x_3x_4x_6 + x_1x_3x_4x_7 + x_1x_3x_5x_6 + x_1x_3x_5x_7 + x_1x_3x_6x_7 + x_1x_4x_5x_6 + x_1x_4x_5x_7 + x_1x_4x_6x_7 + x_2x_3x_4x_5 + x_2x_3x_4x_6 + x_2x_3x_4x_7 + x_2x_3x_5x_6 + x_2x_3x_5x_7 + x_2x_3x_6x_7 + x_2x_4x_5x_6 + x_2x_4x_5x_7 + x_2x_4x_6x_7 + x_3x_4x_5x_6 + x_3x_4x_5x_7 + x_3x_4x_6x_7 + x_3x_5x_6x_7 + x_4x_5x_6x_7,
\]

where the additions and multiplications are over \( GF(2) \).

**Example 2.** Let \( \mathcal{P} = [1..12] \), and let \( \mathbb{D} = (\mathcal{P}, \mathcal{B}) \) be the Steiner system \( S(5,6,12) \). Then the characteristic function of \( D \) is given by

\[
f_\mathbb{D}(x) = \sum_{(i_1,i_2,i_3,i_4,i_5,i_6) \in \mathcal{B}} x_{i_1}x_{i_2}x_{i_3}x_{i_4}x_{i_5}x_{i_6} + \sum_{(i_1,i_2,i_3,i_4,i_5,i_6,\pi) \in \binom{\mathcal{P}}{6}} x_{i_1}x_{i_2}x_{i_3}x_{i_4}x_{i_5}x_{i_6}x_{\pi},
\]

\[8\]
where \( \binom{n}{7} \) denotes the set of all 7-subsets of \([1..12]\). Hence, the algebraic form of \( f_2(x) \) has 924 terms, but looks interesting in the sense that it is compact and simple.

5. The algebraic normal form of the characteristic function \( f_D \) of \( t \)-designs \( \mathbb{D} \)

In the previous section, we view Boolean functions as real-valued functions taking on only the two integer 0 and 1. Any Boolean function of \( n \) variables can also be viewed as a function from \( \text{GF}(2)^n \) to \( \text{GF}(2) \).

Let \( f(x) \) be a Boolean function from \( \text{GF}(2)^n \) to \( \text{GF}(2) \). Suppose that the support of \( f \) is \( \{v_1, \ldots, v_b\} \), where \( b \) is a positive integer. Let \( v_i = (v_{i,1}, v_{i,2}, \ldots, v_{i,n}) \in \text{GF}(2)^n \) for each \( i \), and let \( \bar{v}_{i,j} = v_{i,j} + 1 \in \text{GF}(2) \) for all \( i \) and \( j \). Let \( B(d,n) \) denote the set of all \( d \)-subsets of \([1..n]\).

By definition,

\[
f(x) = \sum_{i=1}^{b} (x_1 + \bar{v}_{i,1})(x_2 + \bar{v}_{i,2}) \cdots (x_n + \bar{v}_{i,n})
\]

where all the additions and multiplications are over \( \text{GF}(2) \), and an empty product is defined to be 1 by convention. The expression in (17) is called the algebraic normal form of \( f \). The expression \( \prod_{i=1}^{d} x_{ij} \) is called a term of degree \( d \) in the algebraic normal form, which appears in the form if and only if its coefficient is 1.

We will need the following lemma when we study the algebraic normal forms of the characteristic function \( f_D \) of \( t \)-designs \( \mathbb{D} \) later [3, p. 15].

**Lemma 14.** Suppose that \((\mathcal{P}, \mathcal{B})\) is a \( t \)-\( (n,k,\lambda) \) design. Suppose that \( Y \subseteq \mathcal{P} \), where \( |Y| = s \leq t \). Then there are exactly \( \lambda_s \) blocks in \( \mathcal{B} \) that contain all the points in \( Y \), where the \( \lambda_s \) is defined in [5].

**Theorem 15.** Let \( \mathbb{D} = ([1..n], \mathcal{B}) \) be a \( t \)-\( (n,k,\lambda) \) design, where \( n \geq k \geq t \geq 1 \), and let \( f_D \) be the characteristic function of \( \mathbb{D} \). Then we have the following regarding the algebraic normal form of \( f_D \):

- All terms of degree no more than \( k - 1 \) vanish.
- A term \( x_{i_1} x_{i_2} \cdots x_{i_k} \) appears if and only if \( \{i_1, i_2, \cdots, i_k\} \) is a block in \( \mathcal{B} \), where \( \{i_1, i_2, \cdots, i_k\} \) is a \( k \)-subset of \([1..n]\). Hence, there are exactly \( b \) terms of degree \( k \) in the algebraic normal form.
- For each \( h \) with \( 1 \leq h \leq t \), either all terms of degree \( n - h \) appear or none of them appears, depending on the parity of \( b - \sum_{i=1}^{d} \binom{h}{i} \lambda_i \).
- The term \( x_{i_1} x_{i_2} \cdots x_n \) of degree \( n \) appears if and only if \( b \) is odd.

**Proof.** Let \( \mathbb{D} = ([1..n], \mathcal{B}) \), where \( \mathcal{B} = \{B_1, B_2, \cdots, B_b\} \). Let

\[
\varphi^{-1}(B_i) = (b_{i,1}, b_{i,2}, \cdots, b_{i,n}) \in \text{GF}(2)^n
\]

for \( 1 \leq i \leq b \). Let \( \bar{b}_{i,j} = b_{i,j} + 1 \) for all \( i \) and \( j \). Denote by \( B_{(d,n)} \) the set of all \( d \)-subsets of \([1..n]\).
It follows from (17) that

\[
f_D(x) = \sum_{i=1}^{n} \prod_{j=1}^{b} \bar{b}_{i,j} + \prod_{i=1}^{n} x_i \\
+ \sum_{d=1}^{n-1} \sum_{\{i_1, \ldots, i_d\} \in B(d, n)} \left( \sum_{i=1}^{b} \frac{1}{\prod_{j=1}^{n} b_{i,j}} \right) \prod_{j=1}^{d} x_j. \tag{18}
\]

Since \(k \geq 1\), for each fixed \(i\) one of \(\bar{b}_{i,j}\) must be zero. Consequently, the constant term

\[
\sum_{i=1}^{b} \prod_{j=1}^{n} \bar{b}_{i,j} = 0.
\]

Note that the coefficient of the term \(\prod_{j=1}^{b} x_j\) is

\[
\sum_{i=1}^{b} \prod_{j \in [1..n] \setminus \{i_1, \ldots, i_d\}} \bar{b}_{i,j}. \tag{19}
\]

Consider now the case that \(1 \leq d \leq k - 1\). In this case, \(n - d > n - k\). It then follows that

\[
\prod_{j \in [1..n] \setminus \{i_1, \ldots, i_d\}} \bar{b}_{i,j} = 0
\]

for each \(i\) with \(1 \leq i \leq b\). We then deduce that the sum in (19) is zero. This completes the proof of the conclusion in the first part.

We now prove the conclusion of the second part. Consider any \(k\)-subset \(\{i_1, i_2, \ldots, i_b\}\) of \([1..n]\) and the corresponding product \(x_{i_1}x_{i_2}\ldots x_{i_b}\) whose coefficient is

\[
\sum_{i=1}^{b} b_{i,j_1} b_{i,j_2} \cdots b_{i,j_{n-k}}, \tag{20}
\]

where \(\{j_1, j_2, \ldots, j_{n-k}\} = [1..n] \setminus \{i_1, i_2, \ldots, i_b\}\). Since \(D\) is simple, the summation in (20) is 1 if and only if for exactly one \(i\) with \(1 \leq i \leq b\) the vector \((b_{i,j_1}, b_{i,j_2}, \ldots, b_{i,j_{n-k}})\) is the all-zero vector, which is the same as that the vector \((b_{i_1, j_1}, b_{i_2, j_2}, \ldots, b_{i_b, j_{n-k}})\) is the all-one vector. The desired conclusion in the second part then follows.

We then prove the conclusion in the third part. Let \(1 \leq h \leq t\). The coefficient of the term \(x_{i_1}x_{i_2}\ldots x_{i_{n-h}}\) is

\[
\sum_{i=1}^{b} \prod_{j=1}^{h} b_{i,j},
\]

where \(\{j_1, j_2, \ldots, j_h\} = [1..n] \setminus \{i_1, i_2, \ldots, i_{n-h}\}\). By Lemma [14] the total number of \(\varphi^{-1}(B_i)\) such that \(\prod_{j=1}^{h} b_{i,j} = 1\) is equal to

\[
b - \sum_{i=1}^{b} \binom{h}{i} \lambda_i,
\]

which depends on \(h\) and is independent of the specific elements in \(\{j_1, j_2, \ldots, j_h\}\). Hence, the conclusion of the third part follows. The last conclusion is obvious. \[\square\]
Note that Theorem 15 does not give information on terms of degree between $k + 1$ and $n - t - 1$ in the algebraic normal form of $f_\mathcal{D}(x)$ of a $t$-design $\mathcal{D}$. In Example 1 Theorem 15 gives information on all terms of degree in $\{0, 1, 2, 3, 5, 6, 7\}$, but not terms of degree 4. In fact, in the algebraic normal form in Example 1 only 28 out of 35 terms of degree 4 appear.

6. Properties of the spectra of the characteristic function $f_\mathcal{D}$ of $t$-designs

Our task in this section is to provide further information on the spectra of the characteristic function $f_\mathcal{D}$ of $t$-designs, in addition to the information given in Theorem 15. Such information may be useful in settling the existence of certain $t$-designs.

The following lemma will be employed later in this paper, and can be proved easily.

**Lemma 16.** Let $f(x)$ be a Boolean function with $n$ variables. Then

1. $\sum_{w \in \text{GF}(2)^n} \hat{f}(w) = 2^n f(0)$; and
2. $\sum_{w \in \text{GF}(2)^n} \hat{f}(w)^2 = 2^n \sum_{z \in \text{GF}(2)^n} f(z) = 2^n \mu(w)$.

**Lemma 17.** Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be an incidence structure, where the point set $\mathcal{P} = [1..n]$, the block set $\mathcal{B} = \{B_1, B_2, \ldots, B_b\}$, the block size $|B_i|$ is $k$, and $k$ and $b$ are positive integers. Let $f_\mathcal{D}$ be the characteristic function of $\mathcal{D}$. Then

$$\hat{f}_\mathcal{D}(\bar{w}) = (-1)^k \hat{f}_\mathcal{D}(w),$$

where $w \in \text{GF}(2)^n$ and $\bar{w} = 1 + w$ which is the complement of $w$.

**Proof.** Note that $|B_i| = k$ for each $i$ with $1 \leq i \leq b$. By definition, we have

$$\hat{f}_\mathcal{D}(\bar{w}) = \sum_{i=1}^{b} (-1)^{(1+w)\phi^{-1}(B_i)} = (-1)^k \sum_{i=1}^{b} (-1)^w \phi^{-1}(B_i) = (-1)^k \hat{f}_\mathcal{D}(w).$$

The following result demonstrates a relationship on the spectra of the characteristic function $f_\mathcal{D}$ of an incidence structure.

**Theorem 18.** Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be an incidence structure, where the point set $\mathcal{P} = [1..n]$, the block set $\mathcal{B} = \{B_1, B_2, \ldots, B_b\}$, the block size $|B_i|$ is $k$, and $k$ and $b$ are positive integers. Let $f_\mathcal{D}$ be the characteristic function of $\mathcal{D}$. Then

$$\sum_{w \in \text{GF}(2)^n} (\hat{f}_\mathcal{D}(w))^3 = 0.$$

**Proof.** Note that $|B_i| = |B_j| = |B_\ell| = k \geq 1$. If $\phi^{-1}(B_i) + \phi^{-1}(B_j) + \phi^{-1}(B_\ell) = 0$, then $i, j, \ell$ must be pairwise distinct, and

$$(B_i \cup B_j) \setminus (B_i \cap B_j) = B_\ell.$$  

It then follows that

$$|B_i \cap B_j| = k.$$  

Note that $|B_i| = |B_j| = k$. We deduce that $B_i = B_j$. This leads to a contradiction. Consequently,

$$\{ (i, j, \ell) \in \{1, 2, \ldots, b\}^3 : \phi^{-1}(B_i) + \phi^{-1}(B_j) + \phi^{-1}(B_\ell) = 0 \} = \emptyset.$$
By definition, 

\[ \hat{f}_D(w) = \sum_{i=1}^{b} (-1)^{w \cdot \phi^{-1}(B_i)}. \]

It then follows that

\[ \sum_{w \in \text{GF}(2)^n} (\hat{f}_D(w))^3 = \sum_{w \in \text{GF}(2)^n} \sum_{j=1}^{b} \sum_{\ell=1}^{b} \left( \sum_{i=1}^{b} (-1)^{w \cdot (\phi^{-1}(B_i) + \phi^{-1}(B_j) + \phi^{-1}(B_\ell))} \right) \]

\[ = \sum_{i=1}^{b} \sum_{j=1}^{b} \sum_{\ell=1}^{b} \left( \sum_{w \in \text{GF}(2)^n} (-1)^{w \cdot (\phi^{-1}(B_i) + \phi^{-1}(B_j) + \phi^{-1}(B_\ell))} \right) \]

\[ = 2^n \left| \{ (i, j, \ell) \in \{1, 2, \ldots, b \}^3 : \phi^{-1}(B_i) + \phi^{-1}(B_j) + \phi^{-1}(B_\ell) = 0 \} \right| \]

\[ = 0. \]

**Theorem 19.** Let \( \mathbb{D} = (P, B) \) be a \( t-(n, n/2, \lambda) \) design, where \( n \) is even. Then \( \hat{f}_D(w) = 0 \) for all \( w \in \text{GF}(2)^n \) with \( wt(w) \) being odd and \( 1 \leq wt(w) \leq t \).

**Proof.** By the second part of Theorem 6, \( P_{n/2}(i) = 0 \) for all odd \( i \) with \( 0 \leq i \leq n \). The desired conclusion then follows from Theorem 13. \( \square \)

### 7. The spectra of the characteristic function \( f_D(x) \) of \( \frac{n-2}{2} \) designs

In this section, we determine the spectra of the characteristic function \( f_D \) of \( \frac{n-2}{2} \) designs.

#### 7.1. Necessary conditions for the existence of a \( t-(n, k, \lambda) \) design

As a corollary of Lemma 8, we have the following.

**Corollary 20.** If a \( t-(n, k, \lambda) \) design exists, then

\[ \binom{k - i}{t - i} \text{ divides } \lambda \binom{n - i}{t - i} \]  \quad (22)

for all integer \( i \) with \( 0 \leq i \leq t \).

As a corollary of Theorem 13, we have also the following.

**Corollary 21.** If a \( t-(n, k, \lambda) \) design exists, then

\[ \binom{n - t}{k - t} \text{ divides } \lambda P_k(h) \]  \quad (23)

for all integer \( h \) with \( 0 \leq h \leq t \).

Note that the divisibility conditions in (22) should be equivalent to those in (23) if a \( t-(n, k, \lambda) \) design exists. It is open if they are equivalent.

The next result is a special case of Corollary 20 [6, p. 102], and is equivalent to the conditions in Corollary 20.
Corollary 22. If a $t-(n, t+1, 1)$ design exists, then

$$\gcd(n-t, \text{lcm}(1, 2, \cdots, t+1)) = 1.$$  \hspace{1cm} (24)

The following follows from Corollary 22.

Theorem 23. If an $(n-2)/2-(n,n/2,1)$ design exists for even $n \geq 4$, then $n \equiv 0 \pmod{4}$.

Later in this paper we will make use of the fact that $n \equiv 0 \pmod{4}$ from time to time.

The next two theorems are from [6, p. 102], and document some necessary conditions of the existence of Steiner systems. These bounds are derived from the Johnson bounds for constant weight codes.

Theorem 24. If a $t-(n, k, 1)$ design exits, then

$$\left( \begin{array}{c} k \\ t-1 \end{array} \right) \frac{k-t}{n-k-1} \leq \left[ \frac{k}{t-1} \left[ \frac{k-1}{t-2} \left[ \cdots \left[ \frac{k-t+3}{2} \right] \cdots \right] \right] \right].$$  \hspace{1cm} (25)

and

$$\left( \begin{array}{c} k \\ k-t+1 \end{array} \right) \frac{k-t}{n-k-1} \leq \left[ \frac{k}{k-t+1} \left[ \frac{k-1}{k-t} \left[ \cdots \left[ \frac{t+1}{2} \right] \cdots \right] \right] \right].$$  \hspace{1cm} (26)

Theorem 25. Let $t = 2h + \delta$ with $\delta \in \{0, 1\}$. If a $t-(n,k,1)$ design exists, then

$$\left( \begin{array}{c} n \\ t \end{array} \right) \geq \left( \begin{array}{c} n \delta \\ k \end{array} \right) \left( \begin{array}{c} n-\delta \\ h \end{array} \right) \left( \begin{array}{c} k \\ t \end{array} \right).$$  \hspace{1cm} (27)

The following result is a fundamental result whose proof can be found in [3, p. 103].

Theorem 26. Every $t-(n,k,\lambda)$ design with $n \leq k+t$ is trivial in the sense that all $k$-subsets occur as blocks.

Theorem 27. The only $t-(n,k,\lambda)$ design with $t \geq n/2$ is the trivial $t-(n,n,1)$ design $(\mathcal{P}, \mathcal{B})$ with $\mathcal{P} = [1..n]$ and $\mathcal{B} = \{[1..n]\}$.

Proof. Suppose $D = (\mathcal{P}, \mathcal{B})$ is a $t-(n,k,\lambda)$ design with $t \geq \lfloor n/2 \rfloor$. Then by Theorem [13] and Lemma [17] the Walsh spectra of $f_D$ is uniquely determined. Hence, the Boolean function $f_D$ is uniquely determined. This means that it must be the trivial $t-(n,n,1)$ design $(\mathcal{P}, \mathcal{B})$ with $\mathcal{P} = [1..n]$ and $\mathcal{B} = \{[1..n]\}$. \hspace{1cm} \Box

We remark that the conclusion of Theorem 27 is stronger than that of Theorem 26 in this special case.

Note that for $t-(n,k,\lambda)$ designs, we have $1 \leq t \leq k \leq n$. In view of Theorems 26 and 27 the most interesting designs are $(n-2)/2-(n,n/2,\lambda)$ designs for even $n$ and $(n-3)/2-(n,k,\lambda)$ designs for odd $n$ and $k \in \{(n-1)/2, (n+1)/2\}$.
7.2. The spectra of the characteristic function $f_D(x)$ of $(n-2)/2\cdot(n,n/2,1)$ Steiner systems

Theorem 13 and Lemma 17 show that $\hat{f}_D(w)$ is known for all $w \in \text{GF}(2)^n$ except those with $\text{wt}(w) = n/2$ when $D$ is an $(n-2)/2\cdot(n,n/2,1)$ Steiner system. In this section, we determine $\hat{f}_D(w)$ for all $w \in \text{GF}(2)^n$ with $\text{wt}(w) = n/2$.

**Theorem 28.** Let $D = (\mathcal{P}, \mathcal{B})$ be an incidence structure, where the point set $\mathcal{P} = [1..n]$, the block set $\mathcal{B} = \{B_1, B_2, \cdots, B_b\}$, the block size $|B_i|$ is $k$, and $k$ and $b$ are positive integers. If $D$ is an $(n-2)/2\cdot(n,n/2,1)$ design, where $n$ is even, then

$$
\sum_{w \in \text{GF}(2)^n, \text{wt}(w) = n/2} \hat{f}_D(w) = -\frac{4}{n+2} \sum_{h=0}^{(n-2)/2} \binom{n}{h} P_{n/2}(h), \tag{28}
$$

and

$$
\sum_{w \in \text{GF}(2)^n, \text{wt}(w) = n/2} (\hat{f}_D(w))^2 = 2^{2n} b - \frac{8}{(n+2)^2} \sum_{h=0}^{(n-2)/2} \binom{n}{h} (P_{n/2}(h))^2, \tag{29}
$$

$$
\sum_{w \in \text{GF}(2)^n, \text{wt}(w) = n/2} (\hat{f}_D(w))^3 = -\frac{16}{(n+2)^3} \sum_{h=0}^{(n-2)/2} \binom{n}{h} (P_{n/2}(h))^3. \tag{30}
$$

**Proof.** By Theorem 28, the block size $k = n/2$, which is even. We first prove (28). Note that $\hat{f}_D(0) = 0$, as $k = n/2 \geq 2$. It follows from Lemmas 16, 17 and Theorem 13 that

$$
\sum_{w \in \text{GF}(2)^n, \text{wt}(w) = n/2} \hat{f}_D(w) = 2^n f(0) - (-1)^k + 1 \sum_{w \in \text{GF}(2)^n, \text{wt}(w) = n/2} \hat{f}_D(w)
$$

$$
= -2 \left( \sum_{w \in \text{GF}(2)^n, \text{wt}(w) = n/2} \hat{f}_D(w) \right)
$$

$$
= -\frac{4}{n+2} \sum_{h=0}^{(n-2)/2} \binom{n}{h} P_{n/2}(h).
$$

We now prove (29). It follows from Lemmas 16, 17 and Theorem 13 that

$$
\sum_{w \in \text{GF}(2)^n, \text{wt}(w) = n/2} (\hat{f}_D(w))^2 = 2^{2n} b - 2 \sum_{w \in \text{GF}(2)^n, \text{wt}(w) = n/2} (\hat{f}_D(w))^2
$$

$$
= 2^{2n} b - \frac{8}{(n+2)^2} \sum_{h=0}^{(n-2)/2} \binom{n}{h} (P_{n/2}(h))^2.
$$

The proof of (30) is similar and omitted. \qed

**Theorem 29.** Let $D = (\mathcal{P}, \mathcal{B})$ be an $(n-2)/2\cdot(n,n/2,1)$ design, where $n \equiv 0 \pmod{4}$. If $w \in \text{GF}(2)^n$ has odd weight $h$ with $1 \leq h \leq t$, then $\hat{f}_D(w) = 0$. 

14
Proof. The desired conclusion follows from Theorem 19.

**Theorem 30.** Let \( w \in \text{GF}(2)^n \) with \( \text{Suppt}(w) = B_i \) being a block of an \((n - 2)/2\cdot(n,n/2,1)\) design \( D = (\mathcal{P}, \mathcal{B}) \). Then

\[
\hat{f}_D(w) = \sum_{h=0}^{n/2} \left( \frac{n/2}{h} \right) - \frac{2 \sum_{h=0}^{n/2} \left( \frac{n/2}{h} \right) \sum_{\ell=0}^{h-1} (-1)^\ell \left( \frac{(n+2)/2}{\ell+1} \right)}{n+2}.
\]

Proof. Note that \( n \equiv 0 \pmod{4} \). It follows from Lemma 11 and Theorem 12 that

\[
\lambda_{(\frac{n}{2} - j,j)} = (-1)^j + \frac{2(-1)^{j-1} \sum_{\ell=0}^{j-1} (-1)^\ell \left( \frac{(n+2)/2}{\ell+1} \right)}{n+2}
\]

for \( 1 \leq j \leq n/2 \). We have then

\[
\begin{align*}
\hat{f}_D(w) &= \sum_{j=0}^{b} (-1)^{|B_j|} = 1 + \sum_{h=0}^{(n-2)/2} (-1)^h \left( \frac{n/2}{h} \right) \lambda_{(\frac{n}{2} - h,h)} \\\noalign{\vspace{1em}}
&= 1 + \sum_{h=1}^{n/2} (-1)^h \left( \frac{n/2}{h} \right) \lambda_{(\frac{n}{2} - h,h)} \\
&= 1 + \sum_{h=1}^{n/2} (-1)^h \left( \frac{n/2}{h} \right) \left[ (-1)^h + \frac{2(-1)^{h-1} \sum_{\ell=0}^{h-1} (-1)^\ell \left( \frac{(n+2)/2}{\ell+1} \right)}{n+2} \right] \\
&= \sum_{h=0}^{n/2} \left( \frac{n/2}{h} \right) - \frac{2 \sum_{h=0}^{n/2} \left( \frac{n/2}{h} \right) \sum_{\ell=0}^{h-1} (-1)^\ell \left( \frac{(n+2)/2}{\ell+1} \right)}{n+2}.
\end{align*}
\]

The proof is then completed.

The following theorem will complete the task of determining the spectra of the characteristic function \( f_D \) for \((n - 2)/2\cdot(n,n/2,1)\) Steiner systems.

**Theorem 31.** Let \( D = ([1,n], \mathcal{B}) \) be an \((n - 2)/2\cdot(n,n/2,1)\) Steiner system. Let \( w \in \text{GF}(2)^n \) with \( \text{wt}(w) = n/2 \). Let \( B = \text{Suppt}(w) \). Then

\[
\hat{f}_D(w) = \sum_{i=0}^{n/2} (-1)^i y_i,
\]

where \( y_0,y_1,\ldots,y_{n/2} \) are uniquely determined by the following system of equations:

\[
\left\{ \begin{array}{l}
\sum_{r=0}^{n/2} {\binom{i}{r}} y_i = \left( \frac{n/2}{r} \right) \lambda_r, \quad 0 \leq r \leq \frac{n-2}{2}, \\
y_0 = y_{\frac{n}{2}} = 1 \quad \text{if } B \in \mathcal{B}, \\
y_0 = y_{\frac{n}{2}} = 0 \quad \text{if } B \not\in \mathcal{B}.
\end{array} \right.
\]

(32)
Proof. Define
\[ y_i = |\{1 \leq j \leq b : |B \cap B_j| = i}\} | \]
for \(0 \leq i \leq n/2\). It then follows from [1, p. 179] that
\[ \sum_{i=0}^{n/2} \binom{i}{r} y_i = \binom{n/2}{r} \lambda_r, \quad 0 \leq r \leq \frac{n}{2} \]
and
\[ y_0 - y_{n/2} = \sum_{r=0}^{n/2} (-1)^r \binom{n/2}{r} \lambda_r. \]

One can prove that
\[ \sum_{r=0}^{n/2} (-1)^r \binom{n/2}{r} \lambda_r = 0. \]
The desired conclusion then follows from
\[ \hat{f}_D(w) = \sum_{j=1}^{b} (-1)^{|\text{Supp}(w) - B_j|} = \sum_{i=0}^{n/2} (-1)^i y_i. \]

We remark that the values \(y_0, y_1, \ldots, y_{n/2}\) in Theorem [31] can be derived easily from [31], though their expressions may look a little complex. As a consequence of Theorem [31] we have the following,

Corollary 32. Every \((n-2)/2-(n,n/2,1)\) design \(D\) is self-complementary, i.e., the complement of a block is also a block of the design, i.e., \(D = \overline{D}\).

Proof. The desired conclusion follows from the fact that \(y_0 = y_{n/2}\) in the proof of Theorem [31].

Theorem [31] and Corollary [32] tell us that \(\hat{f}_D(w)\) takes on two different values depending on whether \(\text{Supp}(w) \in B\) or \(\text{Supp}(w) \in \left(\binom{1, n}{n/2}\right) \setminus B\) for all \(w \in GF(2)^n\) with \(\text{wt}(w) = n/2\).

Table 1: Spectra of \(f_D\)

| Weight of \(w\) | Multiset \(\{\hat{f}_D(w)\}\) |
|----------------|--------------------------|
| 0, 12          | \{132\}                  |
| 1, 11          | \{0^{12}\}               |
| 2, 10          | \{-1^{26}\}              |
| 3, 9           | \{0^{20}\}               |
| 4, 8           | \{4^{195}\}              |
| 5, 7           | \{0^{792}\}              |
| 6              | \{-1^{792}, 52^{132}\}   |

Example 3. Consider the 5-(12, 6, 1) Steiner system from the extended ternary Golay code of length 12. The spectra \(\hat{f}_D(w)\) is given in Table [31].
7.3. The existence of Steiner systems \((n - 2)/2-(n, n/2, 1)\)

We are concerned with the existence of \((n - 2)/2-(n, n/2, 1)\) designs for even \(n\). The integers \(n\) in the range \(8 \leq n \leq 150\) that satisfies the conditions in (22) (23) are given in the set
\[
\{8, 12, 20, 24, 32, 36, 44, 56, 60, 72, 80, 84, 92, 104, 116, 120, 132, 140, 144\}. \tag{33}
\]
The parameters \((n - 2)/2-(n, n/2, 1)\) for all the \(n\) in the set above also satisfy Conditions (24), (26), and (27). So, they are admissible parameters of \((n - 2)/2-(n, n/2, 1)\) designs according to these known necessary conditions.

Experimental data indicates that there are infinitely many admissible parameters \((n - 2)/2-(n, n/2, 1)\) Steiner systems with parameters \(3-(8, 4, 1)\) and \(5-(12, 6, 1)\) exist. But the existence of Steiner systems with such parameters is open in general. It would be possible to show the nonexistence of an \((n - 2)/2-(n, n/2, 1)\) Steiner system \(D\) with the spectra of its characteristic function \(f_D(x)\) developed in Section 7.

7.4. The construction of Steiner systems \((n - 2)/2-(n, n/2, 1)\)

The correspondence from a Boolean function \(f(x)\) to its spectra is not one-to-one. For the characteristic function \(f_D(x)\) of an \((n - 2)/2-(n, n/2, 1)\) Steiner system, \(f_D(w)\) is a constant for all \(w \in GF(2)^n\) with fixed weight \(h\) except \(h = n/2\). Since \(f_D(w)\) takes on two distinct values for all \(w \in GF(2)^n\) with \(wz(w) = n/2\), the spectra of an \((n - 2)/2-(n, n/2, 1)\) Steiner system does not give enough information for constructing the characteristic function of such Steiner system with the inverse Walsh transform approach.

8. Binary linear codes from the characteristic functions of \(t\)-designs

The incidence matrix of a \(t-(n, k, \lambda)\) design \(D\) can be viewed as a matrix over any field \(GF(q)\) and its rows span a linear code of length \(n\) over \(GF(q)\). This is the classical construction of linear codes from \(t\)-designs and has been intensively studied [2].

Any \(t-(n, k, \lambda)\) design \(D\) can also be employed to construct a binary linear code of length \(2^n - 1\) and dimension \(n + 1\). This is done via the characteristic Boolean function of the design. It is likely that the weight distribution of the code could be determined. Below we demonstrate this approach with \((n - 2)/2-(n, n/2, 1)\) Steiner systems.

Let \(f(x)\) be a Boolean function with \(n\) variables such that \(f(0) = 0\) but \(f(x) = 1\) for at least one \(x \in GF(2)^n\). We now define a linear code by
\[
C_f = \{(uf(x) + v \cdot x)| u \in GF(2), v \in GF(2)^n\} \tag{34}
\]
This construction goes back to [4, 13]. It is clear that the weight distribution of the code \(C_f\) is determined by the Walsh spectra of \(f(x)\).

For any \((n - 2)/2-(n, n/2, 1)\) design \(D\), the spectra of the characteristic function \(f_D\) were completely determined in Section 7. Hence, one can write out the weight distribution of the binary linear code \(C_{f_D}\).

**Example 4.** Let \(f_D\) be the characteristic function of the Steiner system \(S(5, 6, 12)\) in Example 3. Then the binary code \(C_{f_D}\) has parameters \([2^{12} - 1, 13, 132]\) and the weight distribution distribution in Table 8.

Another construction of binary linear codes with Boolean functions was treated in [5]. The characteristic function \(f_D\) of any \(t-(n, k, \lambda)\) design could be plugged in and obtain a binary linear code of length \(\lambda(\binom{t}{k})/\binom{t}{1}\) and dimension \(n\) with at most \(n + 1\) weights.
Table 2: Weight distribution

| Weight $w$ | No. of codewords $A_w$ |
|------------|------------------------|
| 0          | 1                      |
| 132        | 1                      |
| $2^{11} - 12$ | 924                 |
| $2^{11}$   | 6143                   |
| $2^{11} + 4$ | 990                  |
| $2^{11} + 52$ | 132               |
| $2^{11} + 132$ | 1                   |

9. Conclusions and remarks

The main contribution of this paper is the spectral characterisation of $t$-designs documented in Theorem 13. It is open how to use this characterisation to construct or show the existence of $t$-designs with certain parameters. The second contribution is the new necessary condition for the existence of $t$-$(n, k, \lambda)$ designs given in Corollary 21. The third contribution is the results of the algebraic normal form of the characteristic function $f_D(x)$ of $t$-designs summarised in Theorem 15. Another contribution is the self-complementary property of $(n-2)/2$-$(n, n/2, 1)$ Steiner systems introduced in Corollary 32. The last contribution is the properties of the spectra $\hat{f}_D(w)$ for Steiner systems with parameters $(n-2)/2$-$(n, n/2, 1)$, which was described in Section 7.2. In addition, we demonstrated two constructions of linear codes from $t$-designs.

It was conjectured that the divisibility conditions in (22) are also efficient for the existence of $t$-$(n, k, \lambda)$ Steiner systems except a finite number of exceptional $n$ given fixed $t$, $k$ and $\lambda$. Earlier progresses on this conjecture were made in [14, 15, 16], and recent advances were made in [8]. It is open if the characterisation in Theorem 13 could be employed to attack this conjecture in a different way.

Acknowledgements

The author thanks Dr. Shuxing Li for reading the first version of this paper and giving helpful comments. The author’s research was supported by the Hong Kong Research Grants Council, under Project No. 16300415.

References

[1] W. O. Alltop, Extending $t$-designs, J. Comb. Theory A 18 (1975) 177–186.
[2] E. F. Assmus Jr., J. D. Key, Designs and Their Codes, Cambridge University Press, Cambridge, 1992.
[3] T. Beth, D. Jungnickel, H. Lenz, Design Theory, Cambridge University Press, Cambridge, 1999.
[4] C. Carlet and C. Ding, Nonlinearities of S-boxes, Finite Fields and Their Applications 13 (2007) 121–135.
[5] C. Ding, A construction of binary linear codes from Boolean functions, Discrete Mathematics 339 (2016) 2288–2303.
[6] C. J. Colbourn, J. H. Dinitz, Handbook of Combinatorial Designs, 2nd Edition, CRC Press, New York, 2007.
[7] W. C. Huffman, V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge, 2003.
[8] P. Keevash, The existence of designs, [arXiv:1401.3665]
[9] F. J. MacWilliams, N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.
[10] L. Teirlinck, Nontrivial $t$-designs without repeated blocks exist for all $t$, Discrete Math. 65(3) (1987) 301–311.
[11] V. D. Tonchev, Codes and designs, in: V. S. Pless, W. C. Huffman, (Eds.), Handbook of Coding Theory, Vol. II, Elsevier, Amsterdam, 1998, pp. 1229–1268.
[12] V. D. Tonchev, Codes, in: C. J. Colbourn, J. H. Dinitz, (Eds.), Handbook of Combinatorial Designs, 2nd Edition, CRC Press, New York, 2007, pp. 677–701.
[13] T. Wadayama, T. Hada, K. Wakasugi, M. Kasahara, Upper and lower bounds on maximum nonlinearity of n-input m-output Boolean function, Designs, Codes Cryptography 23 (2001) 23–33.
[14] R. M. Wilson, An existence theory for pairwise balanced designs I. Composition theorems and morphisms, J. Combinatorial Theory Ser. A 13 (1972) 220–245.
[15] R. M. Wilson, An existence theory for pairwise balanced designs II. The structure of PBD-closed sets and the existence conjectures, J. Combinatorial Theory Ser. A 13 (1972) 246–273.
[16] R. M. Wilson, An existence theory for pairwise balanced designs III. Proof of the existence conjectures, J. Combinatorial Theory Ser. A 18 (1975) 71–79.