Perfect edge state transfer on cubelike graphs

Xiwang Cao

Received: 23 March 2020 / Accepted: 13 August 2021 / Published online: 1 September 2021
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2021

Abstract
Perfect (quantum) state transfer has been proved to be an effective model for quantum information processing. In this paper, we give a characterization of cubelike graphs having perfect edge state transfer (PEST, in short). By using a lifting technique, we show that every bent function, and some semi-bent functions as well, can produce some graphs having PEST. Some concrete constructions of such graphs are provided. Notably, using our method, one can obtain some classes of infinite graphs possessing PEST.

Keywords Perfect (quantum) state transfer · Perfect edge state transfer · Eigenvalues of a graph · Bent function

Mathematics Subject Classification 05C25 · 81P45 · 81Q35

1 Introduction
A Random walk, an alternative name of a Markov chain, on graphs has been proved to be a fundamental tool with broad applications in various fields of mathematics and computer science. In the algorithmic context, random walks provide a general paradigm for sampling and exploring an exponentially large set of combinatorial structures (such as matchings in a graph), by using a sequence of simple, local transitions [2]. Quantum walks, the quantum mechanical counterpart of classical random walks, is an advanced tool for building quantum algorithms that has been recently shown to constitute a universal model of quantum computation. As a crucial part of quantum information processing and computation, quantum algorithm is the research field of
both mathematicians and engineers for the past few decades. Quantum walks on finite
graphs provide useful simple models for quantum transport phenomena, and have been
applied to spin chains for communication links in quantum computing.

We shall begin by formally describing a random walk on a graph: let $\Gamma = (V, E)$
be a graph with point set $V$ and edge set $E$. A random walk, starting from a vertex
$u_0 \in V$, if at $t$-th step we are at a node $u_t$, we move to a neighbor of $u_t$ with probability
given by probability distribution $P$. It is common practice to make the $uv$-entry of $P$ to
be $1/d(u_t)$, where $d(u_t)$ is the degree of vertex $u_t$. If $\Gamma$ is connected and non-bipartite,
then the distribution of the random walk, $D_t = P^t D_0$ converges to a stationary
distribution $\rho$ which is independent of the initial distribution $D_0$. For a $d$-regular
graph $\Gamma$, i.e., if all nodes have the same degree, the limiting probability distribution is
uniform over the nodes of the graph. There are many definitions which capture the rate
of the convergence to the limiting distribution. Some important parameters, such as
the mixing time, filling time, dispersion time, are imported to describe the properties
of a discrete random walk [2]. Examples of discrete random walks on graphs are a
classical random walk on a circle or on a 3-dimensional mesh [22,29].

There are two kinds of quantum walks on graphs. The first one, called discrete
quantum walks, consists of two quantum mechanical systems, named a walker and
a coin, as well as an evolution operator which is applied to both systems only in
discrete time steps. The mathematical structure of this model is evolution via unitary
operator, i.e., $|\psi\rangle_t = U^{t_2-t_1} |\psi\rangle_{t_1}$, where $U$ is the corresponding unitary operator. The
second one, named continuous quantum walks, consists of a walker and an evolution
(Hamiltonian) operator of the system that can be applied with no timing restrictions
at all, i.e., the walker walks any time. The mathematical structure of this model is
evolution via the Schrödinger equation. In this paper, we focus on the continuous
quantum walks. It has been shown that a continuous random walk on a graph is
determined by a sequence of matrices of the form $M(t)$, indexed by the vertices of $\Gamma$
and parameterized by a real positive time $t$. The $(u, v)$-entry of $M(t)$ represents the
probability of starting at vertex $u$ and reaching vertex $v$ at time $t$. Define a continuous
random walk on $\Gamma$ by setting

$$M(t) = \exp(i t (D - A)),$$

where $D$ is a diagonal matrix. Then each column of $M(t)$ corresponds to a probability
density of a walk whose initial state is the vertex indexing the column. For more
properties of quantum walks, we refer the reader to [29].

Upon certain choices of a time-independent Hamiltonian, the quantum system
defined in certain graphs will evolve $\exp(-i t A)$, where $A$ is the adjacency matrix
of the corresponding graph $\Gamma$. We name the matrix $\exp(-i t A)$ as the transfer matrix
of the graph $\Gamma$, which is defined by the following $n \times n$ matrix:

$$H(t) = H_{\Gamma}(t) = \exp(-i t A) = \sum_{s=0}^{+\infty} \frac{(-i t A)^s}{s!} = (H_{g,h}(t))_{g,h \in V}, \quad t \in \mathbb{R}, \quad (1)$$

\[ Springer \]
where \( n = |V| \) is the number of vertices in \( \Gamma \). In such a scenario, the dynamics of the quantum states in each vertex resembles in some aspects the dynamics of a random walk [18]. If \( |\psi(t)\rangle \) is a time-dependent amplitude vector on the vertices of the graph \( \Gamma \), then the evolution of the quantum walk is given by

\[
|\psi(t)\rangle = \exp(-itA)|\psi(0)\rangle.
\]

where \( |\psi(0)\rangle \) is the initial amplitude vector which is usually taken as \( e_a \), the standard vector associated with \( a \), for some node \( a \). The amplitude of the quantum walk on vertex \( b \) at time \( t \) is given by \( \psi_b(t) = \langle e_a | \psi(t) \rangle \), while the probability of vertex \( b \) at time \( t \) is

\[
p_b(t) = |\langle e_b' | \psi(t) \rangle|^2 = |e_b' \exp(-itA)e_a|^2.
\]

Since \( H(t) \) is a unitary matrix, we have

\[
0 \leq p_b(t) \leq 1 \text{ and } \sum_{b \in V} p(t) = 1.
\]

\( \Gamma \) is said to admit a **perfect state transfer** (PST, in short) from the node \( a \) to a node \( b \) at time \( t \) if

\[
|e_b' \exp(-itA)e_a| = 1.
\] (2)

Following this approach, Childs et al. [9] found a graph in which the continuous-time quantum walk spreads exponentially faster than any classical algorithm for a certain black-box problem. Childs also showed that the continuous-time quantum walk model is a universal computational model [10].

In the year 1998, Fahri and Gutmann [18] defined an analogue continuous quantum walk by using the operator \( H(t) \) defined in (1). (Note that \( H(t) \) is a unitary matrix for every \( t \), thus one defines a continuous quantum walk.) Suppose that the initial state of a walk is given by a density matrix \( \rho \) as physicists usually do. Then the state \( \rho(t) \) at time \( t \) is given by

\[
\rho(t) = H(t)\rho H(-t).
\]

We call a density matrix \( \rho \) a **pure state** if \( \text{rank}(\rho) = 1 \). We use \( e_a \) to denote the standard basis vector in \( \mathbb{C}^n \) indexed by the vertex \( a \). Then

\[
\rho_a = e_a e_a^t
\]

is the pure state associated to the vertex \( a \).

Physicists are interested in the question whether there exists a time \( t \) such that for two distinct vertices \( a \) and \( b \), it happens that

\[
\rho_a(t) = \gamma \rho_b,
\] (3)
where $\gamma$ is a unit-norm complex number. When the above phenomenon occurs, we say that there is perfect state transfer from $a$ to $b$ at the time $t$ in the graph. Note that it is easy to verify that (3) if and only if

$$|e_b^tH(t)e_a| = 1. \quad (4)$$

Thus, (2) and (3) are identical.

The phenomenon of perfect state transfer in quantum communication networks was originally introduced by Bose in [7]. This work motivated much research interest and many wonderful applications of related works have been found in quantum information processing and cryptography (see [1–4,6,13–15,19–21,27,30] and the references therein.) In his three papers [19–21], C. Godsil surveyed the art of PST and provided the close relationship between this topic and other researching fields such as algebraic combinatorics, coding theory etc. Bašić [5] and Cheung [12] presented a criterion on circulant graphs (the underlying group is cyclic) and cubelike graphs (the underlying group is $\mathbb{Z}_2^m$) having PST. Remarkably, Coutinho et al. [16] showed that one can decide whether a graph admits PST in polynomial time with respect to the size of the graph. In a previous paper [28], we present a characterization on connected simple abelian Cayley graph $\Gamma = \text{Cay}(G, S)$ having PST, we give a unified interpretation of many previously known results.

However, even though there are a lot of results on PST in literature, it is still quite rare in quantum walks. People are always interested in pursuing more graphs having PST.

Recently, the concept of perfect edge state transfer was introduced in [8]. Instead of representing quantum state by density matrices associated with vertices, Chen and Godsil [8] suggested to use the edges of a graph to index the density matrices. Let’s recall the main idea of [8] as follows.

For a given graph $\Gamma$ with $n$ vertices, let $A$ be the adjacency matrix of $\Gamma$. Let $\Delta$ be the degree matrix of $\Gamma$. The Laplacian matrix of $\Gamma$ is $L = \Delta - A$. If $L$ is the Hamiltonian associated to the quantum walk on $\Gamma$, the transition matrix is

$$U(t) = \exp(\imath tL).$$

See [8] for details. Chen et al. [8] use

$$|\psi_{(a,b)}(0)\rangle = \frac{1}{\sqrt{2}}(e_a - e_b)$$

to represent a quantum edge state. If $|\psi(t)\rangle$ is a time-dependent amplitude vector on the edges of the graph $\Gamma$, then the evolution of the quantum walk is given by

$$|\psi(t)\rangle = U(t)|\psi_{(a,b)}(0)\rangle.$$

The amplitude of the quantum walk on edge $(c, d)$ at time $t$ is given by

$$\psi_{(c,d)}(t) = |\frac{1}{\sqrt{2}}(e_c - e_d)'|\psi(t)\rangle| = \frac{1}{2}(e_c - e_d)'U(t)(e_a - e_b). \quad (5)$$
Denote
\[ p_{(c,d)}(t) := |\langle \sqrt{\frac{1}{2}}(e_c - e_d)^T \mid \psi_{(c,d)}(t) \rangle|^2, \quad \text{and} \]
\[ M_{a,b}(t) := \sum_{(c,d) \in E} \left| \frac{1}{2}(e_c - e_d)^T U(t)(e_a - e_b) \right|^2. \]

Then we say that the "probability" of edge \((c, d)\) at time \(t\) is
\[ \rho_{(c,d)}(t) = \left| \frac{1}{2}(e_c - e_d)^T U(t)(e_a - e_b) \right|^2 / M_{a,b}(t). \]

It is easy to see that
\[ 0 \leq p_{(c,d)}(t) \leq 1. \]

Unlike in the case of node-version state transfer, we don’t have \(M_{a,b}(t) = 1\) in general for the case of edge-version state transfer\(^1\).

A graph is said to have **perfect edge state transfer** (PEST, in short) from an edge \((a, b)\) to edge \((c, d)\) if
\[ \left| \frac{1}{2}(e_a - e_b)^T U(t)(e_c - e_d) \right| = 1. \]

Obviously, if \(\Gamma\) is a \(k\)-regular graph, then
\[ U(t) = \exp(it(\Delta - A)) = \exp(it(kI - A)) = \exp(itk)H(-t). \]

Thus, for a given regular graph \(\Gamma\), it has PEST from an edge \((a, b)\) to edge \((c, d)\) if and only if there exists a complex scalar \(\gamma\) with \(|\gamma| = 1\) satisfying
\[ H(t)(e_a - e_b) = \gamma(e_c - e_d). \]

One can also use edge state to represent a quantum state by density matrices. A density matrix is a semidefinite matrix of trace 1. A density matrix \(D\) represents a pure state if \(\text{rank}(D) = 1\). If \(e_a\) denotes the standard basis vector in \(\mathbb{C}^n\) indexed by the vertex \(a\) in graph \(\Gamma\), then
\[ D_{(a,b)} = \frac{1}{2}(e_a - e_b)(e_a - e_b)^T \]

is a pure state associated with the edge \((a, b)\) in \(\Gamma\), which is called the density matrix of edge \((a, b)\).

\(^1\) The author would like to express his grateful thankfulness to one of the reviewers for pointing out some possible defaults in the definition of edge-version state transfer.
Given a density matrix $D_{(a,b)}$ as the initial state of a continuous quantum walk, then the state that $D_{(a,b)}(t)$ is transferred to at time $t$ is given by

$$D_{(a,b)}(t) = U(t)D_{(a,b)}U(-t),$$

where $U(t) = \exp(itL)$ is the usual transition matrix associated with $\Gamma$ whose Laplacian matrix is $L$. Given two edges $(a, b)$ and $(c, d)$, we say that there is perfect state transfer between the edges $(a, b)$ and $(c, d)$ if there is a time $t$ such that

$$D_{(c,d)} = U(t)D_{(a,b)}(t)U(-t).$$

Particularly, if $\Gamma$ is a regular graph, then by (11), we have for any two density matrices $P$ and $Q$,

$$Q = U(t)PU(-t) \iff Q = H(t)PH(-t).$$

One can verify the equivalence of Eqs. (10), (12) and (15).

By the very definition, we have the following comparison of PST and PEST:

| PST | PEST |
|-----|------|
| Initial state | $Q_a = e_a e_a^t$ | $D_{(a,b)} = \frac{1}{2}(e_a - e_b)(e_a - e_b)^t$ |
| State at time $t$ | $Q_a(t) = H(t)Q_a H(-t)$ | $D_{(a,b)}(t) = U(t)D_{(a,b)}U(-t)$ |
| Constrains | $Q_a(t) = \gamma Q_b$ | $D_{(a,b)}(t) = \gamma D_{(c,d)}$ |

Therefore, the model of perfect edge state transfer is established parallely as that of perfect vertex state transfer. Note again that, in the following context, as in [8], we investigate graphs admitting PEST just by inspecting the validity of (10). In other words, we say mathematically that a graph has PEST between the two edges $(a, b)$ and $(c, d)$ if and only if the number $p_{c,d}(t)$ defined in (6) achieves its upper bound 1 at some time $t$.

Edge state transfer shares a lot of properties with vertex state transfer and has potential applications in quantum information computation [8]. Moreover, Chen and Godsil [8] showed that, on a fixed number of vertices, there are more graphs with perfect edge state transfer than graphs with perfect vertex state transfer. There is a huge advantage of Laplacian edge state transfer and this is also why Laplacian edge state transfer is more interesting.

Chen and Godsil [8] provided a sufficient and necessary condition under which a graph has PEST. As applications of this characterization, Chen and Godsil proved the following results:

- the path $P_n$ has PEST if and only if $n = 3, 4$;
- the cycle $C_n$ has PEST if and only $n = 4$;
- if two graphs have PEST at the same time $t$, then so does their Cartesian product;
– if a graph has PEST, then its complement also has PEST;
– if a graph \( \Gamma \) has PEST, then the join of graphs \( \Gamma \boxplus \Delta \) also has PEST for some graphs \( \Delta \).

In a recent paper [23], we proved that if a graph has PST, then it also has PEST. For more applications and backgrounds of PEST, we refer the reader to [8] and the reference therein.

However, up to date, there is no general characterization on which graphs have PEST. Even though there are some necessary and sufficient conditions for a graph to have PEST in [8, Lemma 2.4, Theorem 3.9] (see also Lemma 2 in this paper), these conditions are not easy to be verified. Thus, a basic question for us is how to find simple and easily verified characterizations on graphs that have PEST. Especially for some particular graphs such as circulant graphs, cubelike graphs, Hamming graphs, etc. Moreover, more concrete constructions of graphs having PEST are always desirable.

The main purpose of this paper is to present an explicit and easy to be verified condition for a cubelike graph to have PEST. See Lemma 1 and Theorem 1. By taking a trace-orthogonal basis of \( \mathbb{F}_{2^m} \) (the finite field of size \( 2^m \)) over \( \mathbb{F}_2 \), one can check the above-mentioned conditions just by evaluating the inner product of some vectors, including the calculating of the eigenvalues of the related graphs. Thus, Theorem 1 is a simplification of [8, Lemma 2.4, Theorem 3.9]. Moreover, by utilizing a so-called lift technique, we construct some families of infinite cubelike graphs admitting PEST by employing (semi-)bent functions. The main idea of the technique is as follows: Since for a Cayley graph \( \text{Cay}(G, S) \), its eigenvalues are exactly the Walsh–Hadamard transformation of the characteristic function of the connection set \( S \). In order to find graphs whose eigenvalues satisfy the condition of Theorem 1, we embed a vector space into a larger vector space. Then we can suitably separate the eigenvalues by some planes. Moreover, in \( \mathbb{F}_{2^m} \), every subset is one-to-one corresponding to a Boolean function, namely, the characteristic function. As a result, the eigenvalues of the graphs are represented by the Fourier spectra of the Boolean functions. By importing some specific Boolean functions, we can control the eigenvalues of graphs. Following this approach, we show that every bent function, and some semi-bent functions as well, can lead to a cubelike graph having PEST. See Theorem 3 and Theorem 4. Some concrete constructions are provided in Sect. 6.

The paper is organized as follows: In Sect. 2, we introduce some preliminaries which are needed in our discussion. In Sect. 3, we give a simple characterization of cubelike graphs having PEST. In Sect. 4, we give a lower bound for the time at which a cubelike graph has PEST. We establish some links between (semi)Bent functions and cubelike graphs having PEST in Sect. 5. We provide some concrete constructions of cubelike graphs having PEST in Sect. 6. Finally, in Sect. 7, we make some concluding remarks. Some open questions are proposed for further study.

## 2 Preliminaries

In this section, we give some notation and definitions which are needed in our discussion.
Firstly, throughout this paper, we use $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ to stand for the set of non-negative integers, the integers ring, rational numbers field, real numbers field and complex numbers field, respectively.

### 2.1 Character group of an abelian group

Let $G$ be a finite abelian group. It is well-known that $G$ can be decomposed as a direct product of cyclic groups:

$$G = \mathbb{Z}_{n_1} \otimes \cdots \otimes \mathbb{Z}_{n_r} \quad (n_s \geq 2),$$

where $\mathbb{Z}_m = (\mathbb{Z}/m\mathbb{Z}, +)$ is a cyclic group of order $m$.

For every $x = (x_1, \cdots, x_r) \in G$, $(x_s \in \mathbb{Z}_{n_s})$, the mapping

$$\chi_x : G \to \mathbb{C}, \quad \chi_x(g) = \prod_{s=1}^{r} \omega_{n_s}^{x_s g_s} \quad (\text{for } g = (g_1, \cdots, g_r) \in G)$$

is a character of $G$, where $\omega_{n_s} = \exp(2\pi i / n_s)$ is a primitive $n_s$-th root of unity in $\mathbb{C}$.

For $x, y \in G$, we define $\chi_x \chi_y : G \to \mathbb{C}$ by

$$\forall g \in G, (\chi_x \chi_y)(g) = \chi_x(g) \chi_y(g).$$

Then it can be shown that $\hat{G} = \{\chi_x | x \in G\}$ form a group which we call it the dual group or the character group of $G$. Moreover, the mapping $G \to \hat{G}$, $x \mapsto \chi_x$ is an isomorphism of groups. Furthermore, it is easy to see that

$$\chi_x(g) = \chi_g(x) \text{ for all } x, g \in G.$$

### 2.2 Trace-orthogonal basis

Let $\mathbb{F}$ be a field, $V_1, V_2$ be linear spaces over $\mathbb{F}$. A bilinear form over $\mathbb{F}$ is a two-variable function $B(x, y)$ on $V_1 \times V_2$ satisfying:

1. $B(ax + by, z) = aB(x, z) + bB(y, z)$, $\forall x, y \in V_1, z \in V_2, a, b \in \mathbb{F}$;
2. $B(x, ay + bz) = aB(x, z) + bB(y, z)$, $\forall x \in V_1, y, z \in V_2, a, b \in \mathbb{F}$.

Let $V_1 = V_2 = \mathbb{F}_{2^m}$ which is viewed as a linear space over $\mathbb{F}_2$. Then it is easily seen that for $x, y \in \mathbb{F}_{2^m}$, $B(x, y) := \text{Tr}(xy)$ defines a bilinear form on $\mathbb{F}_{2^m}$, where $\text{Tr}(\cdot)$ is the trace operator. A trace-orthogonal basis for $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$ is a basis $\{\alpha_1, \cdots, \alpha_m\}$ satisfying:

$$\text{Tr}(\alpha_i \alpha_j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

It is known that for every finite field of even characteristic, there always exists a trace-orthogonal basis, see [25]. Let $x, y \in \mathbb{F}_{2^m}$ and suppose that $x = \sum_{i=1}^{m} x_i \alpha_i$, $y = \sum_{i=1}^{m} y_i \alpha_i$.
\[ y = \sum_{i=1}^{m} y_i \alpha_i, \quad x_i, y_i \in \mathbb{F}_2, \quad i = 1, \cdots, m. \] Then

\[ \text{Tr}(xy) = \sum_{i,j} x_i y_j \text{Tr}(\alpha_i \alpha_j) = \sum_{i=1}^{m} x_i y_i. \] \hspace{1cm} (17)

### 3 A characterization of cubelike graphs having PEST

Let \( G \) be an abelian group with order \( n \). Let \( S \) be a subset of \( G \) with \( |S| = s \geq 1 \), \( 0 \notin S = -S := \{ -z : z \in S \} \) and \( G = \langle S \rangle \). Suppose that \( \Gamma = \text{Cay}(G, S) \) is the Cayley graph with the connection set \( S \). Take a matrix \( P = \frac{1}{\sqrt{n}} (\chi_g(h))_{g,h \in G} \) and projection \( E_x = p_x p^*_x \), where \( p_x \) is the \( x \)-th column of \( P \). Then the adjacency matrix \( A \) of \( \Gamma \) has the following spectral decomposition:

\[ A = \sum_{g \in G} \lambda_g E_g, \] \hspace{1cm} (18)

where

\[ E_x = p_x p^*_x = \frac{1}{n} (\chi_x(g-h))_{g,h \in G}, \] \hspace{1cm} (19)

and

\[ \lambda_g = \sum_{s \in S} \chi_g(s), \quad g \in G. \] \hspace{1cm} (20)

Meanwhile, the transfer matrix \( H(t) \) has the following decomposition:

\[ H(t) = \sum_{g \in G} \exp(i \lambda_g t) E_g. \] \hspace{1cm} (21)

Thus, we have, for every pair \( u, v \in G \),

\[ H(t)_{u,v} = \sum_{g \in G} \exp(i \lambda_g t) (E_g)_{u,v} = \frac{1}{n} \sum_{g \in G} \exp(i \lambda_g t) \chi_g(u - v). \] \hspace{1cm} (22)

Therefore,

\[ \frac{1}{2} (e_c - e_d)^t H(t) (e_a - e_b) \]

\[ = \frac{1}{2} \left( H(t)_{c,a} - H(t)_{c,b} - H(t)_{d,a} + H(t)_{d,b} \right) \]

\[ = \frac{1}{2n} \sum_{x \in G} \exp(i \lambda_x) \left( \chi_x(c - a) - \chi_x(c - b) - \chi_x(d - a) + \chi_x(d - b) \right) \]
\[
\sum_{x \in G} \exp(i t \lambda_x) \chi_x(c) - \chi_x(d) \frac{\chi_x(a) - \chi_x(b)}{2} = 2 \sum_{x \in G} \exp(i t \lambda_x) \chi_x(c - a) \frac{1 - \chi_x(d - c) 1 - \chi_x(b - a)}{2}.
\]

(23)

In the sequel, we always assume that \((a, b), (c, d)\) are edges of the concerned graph. To avoid the trivial case, we assume that \(b \neq c, a \neq d\).

Below, we let \(G = (\mathbb{F}_q, +)\) be the additive group of the finite field \(\mathbb{F}_q\). The character group of \(G\) is

\[\hat{G} = \left( \mathbb{F}_q, + \right) = \{ \chi_z : z \in \mathbb{F}_q \},\]

where for \(g, z \in \mathbb{F}_q\), \(\chi_z(g) = (-1)^{\text{Tr}(zg)}\), and \(\text{Tr} : \mathbb{F}_q \rightarrow \mathbb{F}_2\) is the trace operator. It is easy to see that \(G \simeq \mathbb{F}_2^m\) which is an \(m\)-dimensional linear space over \(\mathbb{F}_2\). If we view \(\mathbb{F}_2^m\) as the additive group of the finite field \(\mathbb{F}_q\) with \(q = 2^m\), then

\[\hat{G} = \mathbb{F}_2^m = \{ \chi_z : z \in \mathbb{F}_2^m \},\]

where for \(g = (g_1, \cdots, g_m), z = (z_1, \cdots, z_m) \in \mathbb{F}_2^m\),

\[\chi_z(g) = (-1)^{z \cdot g}, \quad z \cdot g = \sum_{j=1}^m z_j g_j \in \mathbb{F}_2.\]

The above two representations of additive characters of \(\mathbb{F}_2^m\) can be unified by taking a trace-orthogonal basis over \(\mathbb{F}_2^m / \mathbb{F}_2\) (see (17)).

In the finite field \(\mathbb{F}_2^m\), it is known that the number of \(x \in \mathbb{F}_2^m\) such that \(\chi_x(\theta) = 1\) is \(2^{m-1}\), where \(\theta \neq 0\) is any nonzero element in \(\mathbb{F}_q\). Thus, the number of nonzero terms in the RHS of (23) is upper bounded by \(2^{m-1} = n/2\). Write

\[
|\alpha| = (\alpha(x))_{x \in G}, \quad \text{where} \quad \alpha(x) = \exp(i t \lambda_x) \chi_x(c - a) \frac{1 - \chi_x(d - c) 1 - \chi_x(b - a)}{2}.
\]

\(\alpha\) is an \(n\)-dimensional vector with at most \(n/2\) nonzero coordinates, and the absolute value of each nonzero coordinate is \(\leq 1\). Therefore, we deduce that

\[
\left| \frac{1}{2}(e_c - e_d)^t H(t)(e_a - e_b) \right|^2 = 1
\]

if and only if

\[
|\langle \alpha | \beta \rangle| = \frac{n}{2},
\]

(25)

\(\square\) Springer
where $\beta$ is obtained by replacing the nonzero entry of $\alpha$ with 1, see (23). Thanks to the Cauchy–Schwarz inequality, we have

$$\frac{n}{2} = |\langle \alpha | \beta \rangle| \leq \|\alpha\| \cdot \|\beta\| \leq \sqrt{n/2} \sqrt{n/2} = \frac{n}{2}.$$  

(25) implies that all the nonzero coordinates of $\alpha$ should be equal, and the number of nonzero terms should be $n/2$. Thus, we have $a + b = c + d$ and, for every $x \notin \ker(\text{Tr}((b + a)X))$, we have $1 - \chi_x(d - c) - \chi_x(b - a) = 1$. Therefore, for every $x \notin \ker(\text{Tr}((b + a)X))$, one should have that $\exp(it\lambda_x)\chi_x(c + a)$ is a constant. As a consequence, (24) holds true if and only if the following conditions hold:

1. $d + c = b + a$;
2. for all $x \notin \ker(\text{Tr}((b + a)X))$, $\exp(it\lambda_x)\chi_x(c + a)$ is a constant.

Take an element $x_0 \in \mathbb{F}_{2^n}$ satisfying $\text{Tr}((b + a)x_0) = 1$ and $\text{Tr}((c + a)x_0) = 0$. Then (2) is equivalent to $\exp(it\lambda_{x_0} - \lambda_x)) = \chi_x(c + a)$ for all $x \in \mathbb{F}_{2^n}$ satisfying $\text{Tr}((b + a)x) = 1$.

Thus, we have the following preliminary result:

**Lemma 1** Let $\Gamma = \text{Cay}(\mathbb{F}_{2^n}, S)$ be a cubelike graph over $\mathbb{F}_{2^n}$ with $|S| = s$. For $a, b, c, d \in \mathbb{F}_{2^n}$, $\Gamma$ has PEST between $(a, b)$ and $(c, d)$ if and only if

1. $a + b + c + d = 0$;
2. Let $x_0 \in \mathbb{F}_{2^n}$ such that $\text{Tr}((b + a)x_0) = 1$, $\text{Tr}((c + a)x_0) = 0$. Then $\exp(it\lambda_{x_0} - \lambda_x)) = \chi_x(c + a)$ for all $x \in \mathbb{F}_{2^n}$ satisfying $\text{Tr}((b + a)x) = 1$.

Consequently, we have

**Corollary 1** Let $\Gamma = \text{Cay}(\mathbb{F}_{2^n}, S)$ be a cubelike graph over $\mathbb{F}_{2^n}$ with $|S| = s$. For $a, b, c, d, \alpha \in \mathbb{F}_{2^n}$, $\Gamma$ has PEST between $(a, b)$ and $(c, d)$ if and only if $\Gamma$ has PEST between $(a + \alpha, b + \alpha)$ and $(c + \alpha, d + \alpha)$.

**Remark 1** By Corollary 1, whether a cubelike graph has PEST or not is independent on the initial edge state.

Define two subsets in $\mathbb{F}_{2^n}$ by

$$\Omega_+ = \{x \in \mathbb{F}_{2^n} : \text{Tr}((c + a)x) = 0, \text{Tr}((b + a)x) = 1\},$$

$$\Omega_- = \{x \in \mathbb{F}_{2^n} : \text{Tr}((c + a)x) = 1, \text{Tr}((b + a)x) = 1\}. \quad (26)$$

It is easily seen that

$$\Omega_+ \cap \Omega_- = \emptyset, \quad \Omega_+ \cup \Omega_- = \{x \in \mathbb{F}_{2^n} : \text{Tr}((b + a)x) = 1\}.$$

If we take a trace-orthogonal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, then (26) has the following form:

$$\Omega_+ = \{x = (x_1 \cdots x_m) \in \mathbb{F}_{2^n}^m : (c + a) \cdot x = 0, (b + a) \cdot x = 1\},$$

$$\Omega_- = \{x = (x_1 \cdots x_m) \in \mathbb{F}_{2^n}^m : (c + a) \cdot x = 1, (b + a) \cdot x = 1\}. \quad (27)$$
where the “·” is the standard inner product of two vectors, and \( a, b, c, d \) are the vectors corresponding to \( a, b, c, d \), respectively. Thus, in the very beginning, we can use the inner product to define the characters of \( F_2^m \) instead of using the trace mapping. This will make things easier for us. Only in the case of the isomorphism \( F_2^m \cong F_2^m \) as linear spaces over \( F_2 \) is concerned, we need to use the trace-orthogonal basis.

Recall that the 2-adic exponential valuation of rational numbers which is a mapping defined by

\[
v_2 : \mathbb{Q} \rightarrow \mathbb{Z} \cup \{\infty\}, v_2(0) = \infty, v_2\left(2^{\ell} \frac{a}{b}\right) = \ell, \text{ where } a, b, \ell \in \mathbb{Z} \text{ and } 2 \nmid ab.
\]

We assume that \( \infty + \infty = \infty + \ell = \infty \text{ and } \infty > \ell \text{ for any } \ell \in \mathbb{Z} \). Then \( v_2 \) has the following properties. For \( \beta, \beta' \in \mathbb{Q} \),

(P1) \( v_2(\beta\beta') = v_2(\beta) + v_2(\beta') \);
(P2) \( v_2(\beta + \beta') \geq \min\{v_2(\beta), v_2(\beta')\} \) and the equality holds if \( v_2(\beta) \neq v_2(\beta') \).

Based on the previous preparations, we present our main result as follows.

**Theorem 1** Let \( \Gamma = \text{Cay}(\mathbb{F}_2^m; S) \) be a Cayley graph over \( \mathbb{F}_2^m \) with \( |S| = s \). For \( a, b, c, d \in \mathbb{F}_2^m \), \( \Gamma \) admits PEST between \( (a, b) \) and \( (c, d) \) if and only if the following two conditions hold:

1. \( a + b + c + d = 0 \);
2. Let \( x_0 \in \Omega_+ \). Then for all \( x \in \Omega_- \), \( v_2(\lambda_{x_0} - \lambda_x) \) are the same number, say \( \rho \). Moreover, for every \( y \in \Omega_+ \), we have \( v_2(\lambda_{x_0} - \lambda_y) \geq \rho + 1 \), where \( \Omega_+, \Omega_- \) are defined by (26).

Furthermore, if the conditions (1), (2) are satisfied, then the time \( t \) at which the graph has PEST is \( t = \frac{(2u+1)\pi}{M} \) for any integer \( u \), where \( M = \gcd(\lambda_{x_0} - \lambda_x : x_0 \neq x \in \mathbb{F}_2^m, \text{Tr}((a + b)x)) = 1 \).

**Proof** The main idea of the proof is an analogue of [28, Theorem 2.4]. If \( \Gamma \) has PEST at time \( t \), then for \( x, x' \in \Omega_- \), we have

\[
\exp(it(\lambda_{x_0} - \lambda_x)) = \chi_x(c + a), \quad \exp(it(\lambda_{x_0} - \lambda_{x'})) = \chi_{x'}(c + a).
\]  

(28)

Write \( t = 2\pi T \). Then (28) becomes

\[
T(\lambda_{x_0} - \lambda_x) - \frac{1}{2} \in \mathbb{Z}, \quad T(\lambda_{x_0} - \lambda_{x'}) - \frac{1}{2} \in \mathbb{Z}.
\]

(29)

Thus, \( T \in \mathbb{Q} \) and \( T \neq 0 \). Therefore, \( v_2(T(\lambda_{x_0} - \lambda_x)) = v_2(T(\lambda_{x_0} - \lambda_{x'})) = -1 \) and then \( v_2(\lambda_{x_0} - \lambda_x) = v_2(\lambda_{x_0} - \lambda_{x'}) = -1 - v_2(T) \). That is, for all \( x \in \Omega_- \), \( v_2(\lambda_{x_0} - \lambda_x) \) is a constant, say, \( \rho \).

For every \( y \in \Omega_+ \), condition (2) of Lemma 1 means that

\[
\exp(it(2\pi T(\lambda_{x_0} - \lambda_y)) = \chi_y(c + a) = (-1)^{\text{Tr}((c+a)y)} = 1.
\]
Thus, $T(\lambda_{x_0} - \lambda_y) \in \mathbb{Z}$. Then $v_2(T(\lambda_{x_0} - \lambda_y)) \geq 0$, i.e., $v_2(\lambda_{x_0} - \lambda_y) \geq -v_2(T) = \rho + 1$.

Conversely, if for all $x \in \Omega_-$, $v_2(\lambda_{x_0} - \lambda_x) = \rho$ and for every $y \in \Omega_+$, $v_2(\lambda_{x_0} - \lambda_y) \geq \rho + 1$, then

$$\exp(iT(\lambda_{x_0} - \lambda_x)) = \chi_x(c + a) \iff T(\lambda_{x_0} - \lambda_x) - \frac{1}{2} \in \mathbb{Z},$$

and

$$\exp(iT(\lambda_{x_0} - \lambda_y)) = \chi_y(c + a) \iff T(\lambda_{x_0} - \lambda_y) \in \mathbb{Z}.$$ 

Using the same argument as [28, Theorem 2.4], we get the desired result. $\square$

For any two states $e_a - e_b$ and $e_c - e_d$, they are termed strongly cospectral in $\Gamma$ if and only if $E_x(e_a - e_b) = \pm E_x(e_c - e_d)$ holds for all $x \in \mathbb{F}_{2^m}$.

Now we let $\bigwedge_{ab,cd}^+$ denote the set of eigenvalues such that

$$E_x(e_a - e_b) = E_x(e_c - e_d)$$

and let $\bigwedge_{ab,cd}^-$ denote the set of eigenvalues such that

$$E_x(e_a - e_b) = -E_x(e_c - e_d).$$

It is easy to see that $\bigwedge_{a,b} = \bigwedge_{c,d} = \bigwedge_{ab,cd}^+ \cup \bigwedge_{ab,cd}^-$, $\bigwedge_{ab,cd}^+ \cap \bigwedge_{ab,cd}^- = \emptyset$, where $\bigwedge_{a,b}$ (resp. $\bigwedge_{c,d}$) is the set of eigenvalues $\lambda_x$ such that $E_x(e_a - e_b) \neq 0$ (resp. $E_x(e_c - e_d) \neq 0$).

Using strongly cospectrality, Chen and Godsil [8] derived a characterization of perfect edge state transfer as follows.

**Lemma 2** [8, Lemma 2.4] Let $\Gamma = (V, E)$ be a graph and $(a, b), (c, d) \in E$. Perfect edge state transfer between $(a, b)$ and $(c, d)$ occurs at time $t$ if and only if all of the following conditions hold.

(a) Edge states $e_a - e_b$ and $e_c - e_d$ are strongly cospectral. Let $\lambda_0 \in \bigwedge_{ab,cd}^+.$

(b) For all $\lambda_x \in \bigwedge_{ab,cd}^+$, there is an integer $k$ such that $t(\lambda_0 - \lambda_x) = 2k\pi$.

(c) For all $\lambda_x \in \bigwedge_{ab,cd}^-$, there is an integer $k$ such that $t(\lambda_0 - \lambda_x) = (2k + 1)\pi$.

One can use Lemma 2 to give an alternative proof of Theorem 1. Indeed, for the cubelike graph, we have $E_x(e_a - e_b) = \pm E_x(e_c - e_d)$ if and only if $\text{Tr} \left((b + a)x\right) = \text{Tr} \left((c + d)x\right)$ for all $x \in \mathbb{F}_{2^m}$. Therefore, $e_a - e_b$ and $e_c - e_d$ are strongly cospectral in $\Gamma$ if and only if $a + b + c + d = 0$. Moreover, let $t = 2\pi T$. Then condition (b) in Lemma 2 is equivalent to $T(\lambda_{x_0} - \lambda_x) \in \mathbb{Z}$ for $x \in \Omega_+$. Meanwhile, the condition (c) is equivalent to $T(\lambda_{x_0} - \lambda_x) \in \frac{1}{2} + \mathbb{Z}$ for $x \in \Omega_-$. Where $\Omega_+, \Omega_-$ are defined in (26).
4 A lower bound for the time at which a cubelike graph has PEST

In view of Corollary 1, we can assume that the initial state edge is \((0, b)\), where \(b \neq 0\). Moreover, we have the following result.

**Lemma 3** Let \(\Gamma = \text{Cay}(\mathbb{F}_{2^m}; S)\) be a cubelike graph over \(\mathbb{F}_{2^m}\) with \(|S| = s\). Let \(b, c, d \in \mathbb{F}_{2^m}\) and \(b \neq 0\). Denote a set \(S' = b^{-1}S = \{b^{-1}z : z \in S\}\). Then \(\Gamma = \text{Cay}(\mathbb{F}_{2^m}; S)\) has PEST at time \(t\) between \((0, b)\) and \((c, d)\) if and only if \(\Gamma' = \text{Cay}(\mathbb{F}_{2^m}, S')\) has PEST between \((0, 1)\) and \((b^{-1}c, b^{-1}d)\) at time \(t\).

**Proof** Firstly, it is obvious that \(b + c + d = 0 \iff 1 + b^{-1}c + b^{-1}d = 0\).

For condition (2). The eigenvalues of \(\Gamma'\) are

\[
\lambda'_x = \sum_{z \in S'} \chi_x(z) = \sum_{z \in S} \chi_x(b^{-1}z) = \sum_{z \in S} \chi_{b^{-1}x}(z) = \lambda_{b^{-1}x}.
\]

Suppose that \(\Gamma\) has PEST between \((0, b)\) and \((c, d)\). Then by substituting \(x\) by \(b^{-1}x\) in the condition (2), we have whenever \(b^{-1}x \in \ker(\text{Tr}(bX))\), i.e., \(x \in \ker(\text{Tr}(X))\),

\[
\exp(it(\lambda_{x_0} - \lambda'_x)) = \exp(it(\lambda_{x_0} - \lambda_{b^{-1}x})) = \chi_{b^{-1}x}(c) = \chi_x(b^{-1}c).
\]

Thus, by Lemma 1, \(\Gamma'\) has PEST between \((0, 1)\) and \((b^{-1}c, b^{-1}d)\).

The converse direction can be proved similarly. \(\square\)

In the following, we consider the minimum time \(t\) at which a cubelike graph has PEST. We will provide a lower bound on the time \(t\). As we will see that in Sect. 6, the lower bound is almost tight in some cases.

By Lemmas 1 and 3, in the next context, without loss of generality, we only consider whether \(\Gamma\) has PEST between \((0, 1)\) and \((c, d)\).

Define two subset of \(\mathbb{F}_{2^m}\) by setting \(T_i = \{x \in \mathbb{F}_{2^m}, \text{Tr}(x) = i\}, i = 0, 1\). In the following context, we fix \(x_0\) as an element in \(\Omega_+\).

Firstly, we have the following result.

**Theorem 2** Let \(S\) be a subset of \(\mathbb{F}_{2^m}\) with \(0 \notin S\) and \(\langle S \rangle = \mathbb{F}_{2^m}\). Suppose that \(\Gamma = \text{Cay}(\mathbb{F}_{2^m}, S)\) has PEST between two edges \((0, 1)\) and \((c, d)\) at time \(t\). Then \(t\) is of the form \(\frac{(2a+1)\pi}{M}\), \(a \in \mathbb{Z}\), where \(M = \gcd(\lambda_{x_0} - \lambda_x : x \in T_1)\), \(s = |S|\), and \(x_0\) is a prescribed element in \(\Omega_+ = \{x \in \mathbb{F}_{2^m} : \text{Tr}((c + a)x) = 0, \text{Tr}((b + a)x) = 1\}\). Consequently, the minimum time \(t\) is \(\frac{\pi}{M}\). Moreover, if there is an element \(z_0(\neq 1)\) in \(S\) such that \(1 + z_0 \notin S\), then \(M\) is a power of 2, say, \(M = 2^\ell\), and \(\ell \leq \left\lfloor \frac{\log_2(2^{(s+3)})}{2} \right\rfloor\).

**Proof** The minimum time \(t\) such that \(\Gamma\) has PEST is \(\frac{\pi}{M}\) by Theorem 1. We proceed to prove that if there is an element \(z_0(\neq 1)\) in \(S\) such that \(1 + z_0 \notin S\), then \(M = 2^\ell\) is a power of 2. Furthermore, if \(\Gamma\) has PEST, then \(\ell \leq \left\lfloor \frac{\log_2(2^{(s+3)})}{2} \right\rfloor\).

For any cubelike graph \(\text{Cay}(\mathbb{F}_{2^m}, S)\), we claim that \(M = \gcd(\lambda_{x_0} - \lambda_x : x \in T_1)\) is a divisor of \(2^m\) if there is an element \(z_0(\neq 1)\) in \(S\) such that \(1 + z_0 \notin S\). Before going
to prove the claim, we first prove the following:

$$\sum_{x \in T_1} \chi_x(z) = \begin{cases} 2^{m-1}, & \text{if } z = 0, \\ -2^{m-1}, & \text{if } z = 1, \\ 0, & \text{if } z \neq 0, 1. \end{cases}$$ \hspace{1cm} (30)$$

$$\sum_{x \in T_0} \chi_x(z) = \begin{cases} 2^{m-1}, & \text{if } z \in \mathbb{F}_2, \\ 0, & \text{otherwise}. \end{cases}$$ \hspace{1cm} (31)

Note that the map $L : \mathbb{F}_{2^m} \to T_0; x \mapsto x^2 + x$ is two-to-one and $\text{Tr}(x) = \text{Tr}(x^2)$ for all $x \in \mathbb{F}_{2^m}$. Thus,

$$\sum_{x \in T_1} \chi_x(z) = \frac{1}{2} \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{Tr}(x^2+x+\delta)z} = \begin{cases} 2^{m-1} \chi_z(\delta), & \text{if } z \in \mathbb{F}_2, \\ 0, & \text{otherwise}. \end{cases}$$

where $\delta \in \mathbb{F}_{2^m}$ with $\text{Tr}(\delta) = 1$. This completes the proof of (30). (31) can be proved similarly.

Now, we prove the claim.

Suppose that on the contrary, there is an odd prime $p$ which is divisor of $M$. Let $\lambda_{x_0} - \lambda_x = Mt_x$ for all $x \in T_1$, where $t_x \in \mathbb{Z}$. Then we compute

$$M \sum_{x \in T_1} t_x = \sum_{x \in T_1} (\lambda_{x_0} - \lambda_x) = \lambda_{x_0} 2^{m-1} - \sum_{z \in S} \sum_{x \in T_1} \chi_x(z) = (\lambda_{x_0} + 1_S(1)) 2^{m-1},$$

where $1_S$ is the characteristic function of $S$, i.e., $1_S(x) = 1$ if $x \in S$ and 0 otherwise. We note that the last equality is based on (30) and the fact that $0 \not\in S$. Thus, $\lambda_{x_0} \equiv -1_S(1) \pmod{p}$, and then $\lambda_x \equiv -1_S(1) \pmod{p}$ for all $x \in T_1$. Now, for the element $z_0$ in $S$, $1 + z_0 \not\in S$, we have, on the one hand,

$$\sum_{x \in T_1} \lambda_x \chi_x(z_0) = \sum_{y \in S} \sum_{x \in T_1} \chi_x(y + z_0) = 2^{m-1}(\text{by (30)}).$$

On the other hand,

$$\sum_{x \in T_1} \lambda_x \chi_x(z_0) \equiv \sum_{x \in T_1} (-1_S(1)) \chi_x(z_0) \equiv (-1_S(1)) \sum_{x \in T_1} \chi_x(z_0) \equiv 0 \pmod{p}.$$

Consequently, we have $p | 2^{m-1}$ which is a contradiction. This proves the claim. That is, $M$ is a power of 2, say, $M = 2^\ell$.

Now, assume that $\Gamma$ has PEST. Then for every $x \in \Omega_-$, we have $v_2(\lambda_{x_0} - \lambda_x) = \rho$. Moreover, for $y \in \Omega_+$, $v_2(\lambda_{x_0} - \lambda_y) \geq \rho + 1$. Where $\Omega_+$ and $\Omega_-$ is defined by (26), or (27). Thus, $M = \gcd(\lambda_{x_0} - \lambda_x : x \in T_1) = 2^\rho$. So that we have $\rho = \ell$. 

Springer
For \( x \in \Omega_-, \) write \( \lambda_{x_0} - \lambda_x = 2^\rho \zeta(x), \) where \( \zeta(x) \in \mathbb{Z} \) and \( 2 \nmid \zeta(x). \) Then
\[
\sum_{x \in T_1} \lambda_x^2 = \sum_{y, z \in S} \sum_{x \in T_1} \chi_x(y + z) = 2^{m-1} (s - |\{z : z \in S, 1 + z \in S\}) , \tag{32}
\]
Moreover,
\[
\sum_{x \in T_1} (\lambda_{x_0} - \lambda_x)^2 = 2^{m-1} (\lambda_{x_0}^2 + 2\lambda_{x_0} \cdot 1_S(1) + s - |\{z : z \in S, 1 + z \in S\}) .
\]
As a consequence, we have
\[
\sum_{x \in \Omega_-} (\lambda_{x_0} - \lambda_x)^2 \leq \sum_{x \in T_1} (\lambda_{x_0} - \lambda_x)^2 \leq 2^{m-1} (s^2 + 3s) . \tag{33}
\]
Meanwhile,
\[
\sum_{x \in \Omega_-} (\lambda_{x_0} - \lambda_x)^2 = \sum_{x \in \Omega_-} 2^{2\rho} \zeta(x)^2 \geq 2^{2\rho} 2^{m-2} \quad \text{(by } 2 \nmid \zeta(x)). \tag{34}
\]
Combining (33) and (34) together, we get
\[
2^{2\rho} \leq 2s(s + 3) .
\]
That is
\[
\ell = \rho \leq \left\lfloor \frac{\log_2(2s(s + 3))}{2} \right\rfloor .
\]
This completes the proof. \( \Box \)

5 Bent functions and PEST

Let \( f : \mathbb{F}_{2^m}^m \to \mathbb{F}_2 \) be a Boolean function. If we endow the vector space \( \mathbb{F}_{2^m}^m \) with the structure of the finite field \( \mathbb{F}_{2^m} \), thanks to the choice of a basis of \( \mathbb{F}_{2^m} \) over \( \mathbb{F}_2 \), then every non-zero Boolean function \( f \) defined on \( \mathbb{F}_{2^m} \) has a (unique) trace expansion of the form:
\[
f(x) = \sum_{j \in \Gamma_m} \text{Tr}_1^{o(j)}(a_jx^j) + \epsilon(1 + x^{2^m-1}), \forall x \in \mathbb{F}_{2^m},
\]
where \( \Gamma_m \) is the set of integers obtained by choosing one element in each cyclotomic coset of 2 modulo \( 2^m - 1 \), \( o(j) \) is the size of the cyclotomic coset of 2 modulo \( 2^m - 1 \) containing \( j \), \( a_j \in \mathbb{F}_{2^{o(j)}} \) and \( \epsilon = \text{wt}(f) \) modulo 2 where \( \text{wt}(f) \) is the Hamming weight of the image vector of \( f \), that is, the number of \( x \) such that \( f(x) = 1 \). Denote...
Table 1 Walsh spectrum of semi-bent functions $f$ with $f(0) = 0$

| Value of $\hat{f}(x)$, $x \in \mathbb{F}_{2^m}$ | Frequency |
|------------------------------------------------|-----------|
| 0                                              | $2^{m-1} + 2^{m-2}$ |
| $2^{k+1}$                                      | $2^{m-3} + 2^{k-2}$ |
| $-2^{k+1}$                                     | $2^{m-3} - 2^{k-2}$ |

$supp(f) = \{x \in \mathbb{F}_{2^m} : f(x) = 1\}$. It is obvious that the map $f \mapsto supp(f)$ gives a one-to-one mapping from the set of Boolean functions to the power set of $\mathbb{F}_{2^m}$.

The Walsh–Hadamard transform of $f$ is defined by

$$\hat{f}(a) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{f(x) + \text{Tr}(ax)}, \forall a \in \mathbb{F}_{2^m}.$$ 

**Definition 1** Let $m = 2k$ be a positive even integer. A Boolean function $f$ is called bent if $\hat{f}(a) \in \{ \pm 2^k \}$ for all $a \in \mathbb{F}_{2^m}$.

**Definition 2** Let $m$ be a positive integer. A Boolean function $f$ from $\mathbb{F}_{2^m} \rightarrow \mathbb{F}_2$ is said to be semi-bent if $\hat{f}(a) \in \{ 0, \pm 2^{\lfloor m/2 \rfloor} \}$.

It is well-known that bent function exists on $\mathbb{F}_{2^{2k}}$ for every $k$. Moreover, for every positive integer $k$, there are many family of such functions. Semi-bent functions also exist in $\mathbb{F}_{2^m}$ for all integer $m \geq 1$. See for example, [24].

Let $f : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_2$ be a Boolean function. $S = supp(f) \subseteq \mathbb{F}_{2^m}$. For the cubelike graph $\Gamma = \text{Cay}(\mathbb{F}_{2^m}, S)$, its eigenvalues are

$$\lambda_x = \sum_{z \in S} \chi_x(z) = \sum_{y \in \mathbb{F}_{2^m}} \frac{1 - (-1)^{f(y)}}{2} \chi_x(y) = -\frac{1}{2} \hat{f}(x), 0 \neq x \in \mathbb{F}_{2^m}. \quad (35)$$

For bent and semi-bent functions, the following results are known. See for example [24], page 72 and page 422.

**Lemma 4** Let $m = 2k$ be a positive even integer. Let $f$ be a Boolean function on $\mathbb{F}_{2^m}$, $S = supp(f)$.

1. If $f$ be a bent function, then $|S| = 2^m \pm 2^{k-1}$. Moreover, define a function $\tilde{f}$, called the dual of $f$, by

$$\tilde{f}(x) = 2^k (-1)^{\hat{f}(x)}.$$ 

Then $\tilde{f}$ is also a bent function. As a consequence, the numbers of occurrences of $\hat{f}(x)$ taking the values $\pm 2^k$ are $2^m \pm 2^{k-1}$ or $2^m \mp 2^{k-1}$.

2. If $f$ is a semi-bent function, then $|S| \in \{ 2^{m-1}, 2^{m-1} \pm 2^{k-1} \}$. Moreover, we have the following table.
It is known also that if $f$ is a bent function, then so is its complementary function, i.e.,

$$g = 1 + f.$$  

Obviously, if $|\text{supp}(f)| = 2^{m-1}+2^{k-1}$, then $|\text{supp}(1 + f)| = 2^{m-1} - 2^{k-1}$.

If $m = 2k + 1$ is an odd number, then we have the following concrete constructions of cubelike graphs having PEST. In these constructions, we use a so-called lifting technique. Precisely, we first take a bent function or semi-bent function $f$ on $\mathbb{F}_2^{2k}$, then find its support $S$. We construct a subset in $\mathbb{F}_2^{2k+1}$ by

$$S' = \{(0, z) : z \in \text{supp}(f)\} \cup \{(1, z) : z \in \text{supp}(f)\}. \tag{36}$$

We then show that one can find a flat to separate the plane $T_1$ into $\Omega_+$ and $\Omega_-$. The main idea of the "lifting technique" is to divide the eigenvalues of the graphs into two parts, such that in one part of $T_1$, the corresponding eigenvalues are all zero. Then hopefully, we can get some desired graphs having PEST. The following two results, namely, Theorems 3 and 4, are obtained following this approach.

**Theorem 3** Let $m = 2k + 1$, $k \geq 2$. Let $f$ be a bent function on $\mathbb{F}_2^{2k}$ satisfying $f(1, 1, \ldots, 1) = 1$. Let $S = \text{supp}(f) \subseteq \mathbb{F}_2^{2k}$ and let $S'$ be defined in (36). Take

$$a = (00^{(2k)}), b = (11^{(2k)}), c = (10^{(2k)}), d = (01^{(2k)}) \in \mathbb{F}_2^m.$$

Let $\Gamma = \text{Cay}(\mathbb{F}_2^m, S')$ be the cubelike graph associated with the connection set $S'$. Then $\Gamma$ has PEST between $(a, b)$ and $(c, d)$ at time $\frac{\pi}{2^k}$.

**Proof** By (27) and the choice of $a, b, c, d$, it is obvious that

$$\Omega_+ = \{(x_1, \ldots, x_m) \in \mathbb{F}_2^m : x_1 + \cdots + x_m = 1, x_1 = 0\},$$

$$\Omega_- = \{(x_1, \ldots, x_m) \in \mathbb{F}_2^m : x_1 + \cdots + x_m = 1, x_1 = 1\}.$$

The eigenvalues of $\Gamma$ are determined by the following:

For every $x \in \mathbb{F}_2^{2k}$,

$$\lambda_{\{0x\}} = \sum_{z \in S} (-1)^{0-z \cdot x} + \sum_{z \in S} (-1)^{1-z \cdot x} = 2\chi_x(S).$$

where \(\chi_x(S) = \sum_{z \in S} (-1)^{z \cdot x} = -2^{k-1}(-1)^{f(x)} = \pm 2^{k-1}\) by (35). Moreover,

$$\lambda_{\{1x\}} = \sum_{z \in S} (-1)^{0-z \cdot x} + \sum_{z \in S} (-1)^{1-z \cdot x} = 0.$$

Therefore, for every $x = (x_1 \cdots x_m) \in \Omega_+$, $v_2(\lambda_{x_0} - \lambda_x) = v_2(\pm 2^k \pm 2^k) \geq k + 1$. Meanwhile, for every $y = (y_1 \cdots y_m) \in \Omega_-$, $v_2(\lambda_{y_0} - \lambda_y) = v_2(\pm 2^k) = k$. The desired result follows with Theorem 1.\hfill \Box

We can also use some semi-bent functions to get cubelike graphs which have PEST. Before going to present our result, we need a lemma first.
Lemma 5 [17] Let $m = 2k + 1$ be an odd integer, $k \geq 2$. Let $f(x) = \text{Tr}(x^{2^e+1})$, where $e$ is a positive integer satisfying $\gcd(e, m) = 1$. Then

$$\hat{f}(a) = \begin{cases} 
0, & \text{if } \text{Tr}(a) = 0, \\
\pm 2^k, & \text{if } \text{Tr}(a) = 1.
\end{cases} \tag{37}$$

Now, we give our construction of cubelike graphs having PEST based on semi-bent functions.

**Theorem 4** Let $m = 2k + 1$, $k \geq 1$ be a positive integer. Let $f(x) = \text{Tr}(x^{2^e+1})$ which is a semi-bent function on $\mathbb{F}_{2^{2k+1}}$. Let $S = \text{supp}(f)$. Then $|S| = 2^{2k}$. Define a subset of $\mathbb{F}_2 \times \mathbb{F}_2^m$ by (36). Put

$$a = (00^{(m)}) , \quad b = (11^{(m)}) , \quad c = (01^{(m)}) , \quad d = (10^{(m)}) \in \mathbb{F}_2^m .$$

Let $\Gamma = \text{Cay}(\mathbb{F}_2^{m+1}, S')$ be the cubelike graph associated with the connection set $S'$. Then $\Gamma$ has PEST between $(a, b)$ and $(c, d)$ at time $\frac{\pi}{2^k+1}$.

**Proof** The proof of this result is similar to that of Theorem 3. We embed $\mathbb{F}_2 \times \mathbb{F}_2^m$ into $\mathbb{F}_2^{m+1}$ as a vector space. Recall that the dual group of $\mathbb{F}_2 \times \mathbb{F}_2^m$ is $\hat{\mathbb{F}}_2 \times \hat{\mathbb{F}}_2^m$, i.e.,

$$\{ \chi_{(u,x)} = \chi_u \chi_x : \chi_u \in \hat{\mathbb{F}}_2, \chi_x \in \hat{\mathbb{F}}_2^m \} .$$

For every $(v, y) \in \mathbb{F}_2 \times \mathbb{F}_2^m$, $\chi_{(u,x)}(v, y) = \chi_u(v) \chi_x(y) = (-1)^{u+v+\text{Tr}(xy)}$. If we fixed a trace-orthogonal basis of $\mathbb{F}_2^m$ over $\mathbb{F}_2$, then $\text{Tr}(xy) = x \cdot y$, where $x$ (resp. $y$) is the vector corresponding to $x$ (resp. $y$). Since $b - a = (11 \cdots 1) = d - c$, we have

$$\chi_{(u,x)}(b - a) = \chi_{(u,x)}(d - c) = (-1)^{u+x-(1-1)} = (-1)^{u+\text{Tr}(x)} .$$

We note that under a trace-orthogonal basis $\{ \alpha_1, \cdots, \alpha_m \}$ of $\mathbb{F}_2^m$ over $\mathbb{F}_2$, the vector $1 \cdots 1$ corresponds to 1 in $\mathbb{F}_2^m$, i.e., $\sum_{i=1}^m \alpha_i = 1$. This fact can be proved as the following:

Since for every fixed $i$, $\text{Tr}(\alpha_i \sum_{j=1}^m \alpha_j) = \sum_{j=1}^m \text{Tr}(\alpha_i \alpha_j) = 1$, for every $x = \sum_{j=1}^m x_j \alpha_j \in \mathbb{F}_2^m$, we have

$$\text{Tr}(x (\sum_{i=1}^m \alpha_i - 1)) = \sum_{j=1}^m x_j (\sum_{i=1}^m \text{Tr}(\alpha_j \alpha_i) - 1) = 0 .$$

Thus, $\sum_{j=1}^m \alpha_j = 1$.

Therefore, in this case, we have

$$T_1 = \{(u, x) \in \mathbb{F}_2 \times \mathbb{F}_2^m : u + \text{Tr}(x) = 1\}, \quad \text{and},$$

$$\Omega_- = \{(0, x) \in \mathbb{F}_2 \times \mathbb{F}_2^m : \text{Tr}(x) = 1\} \subseteq T_1 ,$$

$$\Omega_+ = \{(1, x) \in \mathbb{F}_2 \times \mathbb{F}_2^m : \text{Tr}(x) = 0\} \subseteq T_1 .$$

(See (23) also for the idea of how to chose $a, b, c, d$).
Since \( \hat{f}(0) = 0 \), \( |S| = 2^{m-1} \). By Lemma 5 and (35), the eigenvalues of \( \Gamma \) are

\[
\lambda_{(00)} = |S'| = 2|S| = 2^m, \quad \lambda_{(1x)} = 0, \quad \forall x, \quad \lambda_{(0x)} = \pm 2^{k+1}, \quad \forall (0, x) \in \Omega_-
\]

Thus, for every \( y \in \Omega_- \), \( v_2(\lambda_{x_0} - \lambda_y) = v_2(0 \pm 2^{k+1}) = k + 1 \), and for \( x \in \Omega_+ \), \( v_2(\lambda_{x_0} - \lambda_x) = v_2(0 - 0) = \infty > k + 1 \). Thus, we get the desired result by Theorem 1.

\[\square\]

**Remark 1** In Theorem 4, we just use a special semi-bent function to construct some cubelike graphs having PEST. Using the same idea, one can obtain many such graphs by taking some other semi-bent functions.

### 6 Some concrete constructions

In this section, we present some examples to illustrate our results. Note that all the results in this section are verified by using Magma.

**Example 1** Let \( m = 3 \) and \( S = \{(001), (110), (010), (101)\} \in \mathbb{F}_2^3 \). Let \( \Gamma = \text{Cay}(\mathbb{F}_2^3, S) \) be the cubelike graph associated with the connection set \( S \). Then \( \Gamma \) doesn’t have PEST between \((000, 001)\) and \((c, c + (001))\) for every \( c \in \mathbb{F}_2^3 \).

**Proof** The eigenvalues of \( \Gamma \) are

\[
\lambda_{(000)} = 4, \quad \lambda_{(011)} = -4, \quad \lambda_{(001)} = \lambda_{(010)} = \lambda_{(100)} = \lambda_{(101)} = \lambda_{(110)} = \lambda_{(111)} = 0.
\]

Therefore,

\[
\lambda_{(000)} = 4, \lambda_{(011)} = -4, \lambda_{(001)} = \lambda_{(010)} = \lambda_{(100)} = \lambda_{(101)} = \lambda_{(110)} = \lambda_{(111)} = 0.
\]

Take \( a = (000), b = (001), c = (111), d = (110) \). Then by (27),

\[
\Omega_+ = \{(x_1 x_2 x_3) \in \mathbb{F}_2^3 : x_1 + x_2 + x_3 = 0, x_3 = 1\}
\]

\[
\Omega_- = \{(x_1 x_2 x_3) \in \mathbb{F}_2^3 : x_1 + x_2 + x_3 = 1, x_3 = 1\}
\]

Thus,

\[
\Omega_+ = \{(001), (111)\}, \quad \Omega_- = \{(101), (011)\}.
\]

It is easy to see that the condition (2) of Theorem 1 fails, and then \( \Gamma \) doesn’t have PEST between \((a, b)\) and \((c, d)\). In fact, using the same way, we can check that there is no element \( z \in \mathbb{F}_2^3 \) such that \( \Gamma \) has PEST between \((000, 001)\) and \((z, z + (001))\). \(\square\)

However, if we change the connection set \( S \) in Example 1, then we may get a cubelike graph which has PEST, as the following example shows.

\[\square\] Springer
**Example 2** Let $S = \{(001), (110), (010)\} \in \mathbb{F}_2^3$. Let $\Gamma = \text{Cay}(\mathbb{F}_2^3, S)$ be the corresponding cubelike graph. Take $a = (000), b = (001), c = (101), d = (100)$. Then $\Gamma$ has PEST between $(a, b)$ and $(c, d)$.

**Proof** In this case, the eigenvalues of $\Gamma$ are

$$
\lambda_{(000)} = 3, \quad \text{and} \quad \lambda_{(x_1 x_2 x_3)} = (-1)^{x_1 + x_2} + (-1)^{x_3}, \quad (x_1 x_2 x_3) \neq (000).
$$

Hence, $\lambda_{(000)} = 3$ and

$$
\lambda_{(011)} = -3, \quad \lambda_{(001)} = \lambda_{(110)} = \lambda_{(100)} = 1, \quad \lambda_{(010)} = \lambda_{(101)} = \lambda_{(111)} = -1.
$$

Take $a = (000), b = (001), c = (101), d = (100)$. Then by (27) again,

$$
\Omega_+ = \{(x_1 x_2 x_3) \in \mathbb{F}_2^3 : x_1 + x_3 = 0, x_3 = 1\}
$$

$$
\Omega_- = \{(x_1 x_2 x_3) \in \mathbb{F}_2^3 : x_1 + x_3 = 1, x_3 = 1\}.
$$

Thus,

$$
\Omega_+ = \{(101), (111)\}, \quad \Omega_- = \{(001), (011)\}.
$$

Therefore, we have $\nu_2(\lambda_{x_0} - \lambda_{x}) = 1$ for $x \in \Omega_-$, and $\nu_2(\lambda_{x_0} - \lambda_{x}) \geq 2$ for $x \in \Omega_+$. By Theorem 1, $\Gamma$ has PEST between $(a, b)$ and $(c, d)$ at time $t = \frac{\pi}{2}$. \qed

**Remark 2** Note that the characteristic function of the connection set in Example 2 is

$$
f(x_1 x_2 x_3) = x_1 x_2 x_3 + x_1 x_3 + x_2 + x_3
$$

which is neither a bent function nor a semi-bent function on $\mathbb{F}_2^3$. The Walsh–Hadamard spectra of it are $\{6^{(1)}, 2^{(4)}, -2^{(3)}\}$. Note also that in this example, we just use the inner product to define the characters of $\mathbb{F}_2^3$. We don’t use a trace-orthogonal basis, thus in this example, $1 = (001) \in S$. Therefore, $(0, 1)$ is an edge of $\Gamma$.

**Example 3** Let $m = 4$ and $f(x_1 x_2 x_3 x_4) = x_1 x_4 + x_2 x_3 + x_1$ be a Boolean function from $\mathbb{F}_2^4$ to $\mathbb{F}_2$. Take $S = \text{supp}(f)$. Then there is no PEST in $\Gamma$. Define $S' = \{(0, z) : z \in S\} \cup \{(1, z) : z \in S\} \subseteq \mathbb{F}_2^5$ and let $\Gamma' = \text{Cay}(\mathbb{F}_2^5, S')$. Then $\Gamma'$ has PEST between two edges.

**Proof** The Walsh–Hadamard transformation of $f$ is

$$
\hat{f}(y_1 y_2 y_3 y_4) = \sum_{x_1, x_2, x_3, x_4 \in \mathbb{F}_2} (-1)^{x_1 + x_2 x_3 + x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4}
$$

$$
= -\sum_{x_1, x_2, x_3} (-1)^{x_1 + x_2 x_3 + x_1 y_1 + x_2 y_2 + x_3 y_3} \sum_{x_4} (-1)^{x_4 (x_1 + y_4)}
$$

Springer
\begin{align*}
&= -2(-1)^{y_4 + y_1 y_4} \sum_{x_2} (-1)^{x_2 y_2} \sum_{x_3} (-1)^{x_3 (x_2 + y_3)} \\
&= 4(-1)^{y_4 + y_1 y_4 + y_2 y_3}.
\end{align*}

Thus, \( f \) is a bent function. It is obvious that
\[
S = \{(1000), (0111), (0110), (1010), (1100), (1111)\}.
\]

The eigenvalues of \( \Gamma \) are:
\[
\lambda_x = \sum_{z \in S} (-1)^{z \cdot x} = (-1)^{x_1} + (-1)^{x_2 + x_3 + x_4} + (-1)^{x_2 + x_3} + (-1)^{x_1 + x_3} \\
+ (-1)^{x_1 + x_2} + (-1)^{x_1 + x_2 + x_3 + x_4}.
\]

Thus, we get the following table:

| \( x \) | (0000) | (0001) | (0010) | (0011) | (0100) | (0101) | (0110) | (0111) |
|---|---|---|---|---|---|---|---|---|
| \( \lambda_x \) | 6 | 2 | -2 | 2 | -2 | 2 | 2 | -2 |

| \( x \) | (1000) | (1001) | (1010) | (1011) | (1100) | (1101) | (1110) | (1111) |
|---|---|---|---|---|---|---|---|---|
| \( \lambda_x \) | -2 | -2 | -2 | -2 | -2 | -2 | 2 | 2 |

Moreover, if \( a = (0000), b = (1111), c = (1000), d = (0111) \), then
\[
\Omega_+ = \{(x_1 x_2 x_3 x_4) : x_1 + x_2 + x_3 + x_4 = 1, x_1 = 0\}, \\
\Omega_- = \{(x_1 x_2 x_3 x_4) : x_1 + x_2 + x_3 + x_4 = 1, x_1 = 1\}.
\]

That is
\[
\Omega_+ = \{(0100), (0010), (0001), (0111)\}, \Omega_- = \{(0000), (1011), (1110), (1101)\}
\]

One can verify that the condition (2) of Theorem 1 fails in this case. Thus, there is no PEST between \((a, b)\) and \((c, d)\). Similarly, by a direct checking, we can find that there is no PEST occurring in \( \Gamma \) for different choices of \( a, b, c, d \).

Now, we consider the graph \( \Gamma' \). For every \( x \in \mathbb{F}_2^4 \), we have
\[
\lambda_{(0x)} = \sum_{(0,z) \in S'} (-1)^{z \cdot x} + \sum_{(1,z) \in S'} (-1)^{z \cdot x} = 2 \sum_{z \in S} (-1)^{z \cdot x} = 2 \lambda_x,
\]
and
\[
\lambda_{(1x)} = \sum_{(0,z) \in S'} (-1)^{z \cdot x} + \sum_{(1,z) \in S'} (-1)^{1+z \cdot x} = 0.
\]
If we take 
\[ a = (0000), \quad b = (1111), \quad c = (1000), \quad d = (0111), \]
then
\[ \Omega'_+ = \{(x_1, x_2, x_3, x_4, x_5) \in \mathbb{F}_2^5 : x_1 + x_2 + \cdots + x_5 = 1, x_1 = 0\}, \]
\[ \Omega'_- = \{(x_1, x_2, x_3, x_4, x_5) \in \mathbb{F}_2^5 : x_1 + x_2 + \cdots + x_5 = 1, x_1 = 1\}. \]

Therefore,
\[ \Omega'_+ = \{(0x) : x \in \Omega_+ \cup \Omega_-\}, \quad \Omega'_- = \{(1x) : x \in \Omega_+ \cup \Omega_-\}. \]

The desired result now follows from Theorem 1. \( \Box \)

The following example is actually based on Theorem 4.

**Example 4** Let the connection set \( S \) be defined as
\[ S = \{(0111), (0101), (0011), (0110), (1111), (1011), (1101), (1110)\} \subseteq \mathbb{F}_2^4. \]

Let \( \Gamma = \text{Cay}(\mathbb{F}_2^4, S) \) be the cubelike graph with connection set \( S \). Take
\[ a = (0000), \quad b = (1111), \quad c = (1000), \quad d = (0111). \]

Then \( \Gamma \) has PEST between \((a, b)\) and \((c, d)\).

**Proof** Under a trace-orthogonal basis of \( \mathbb{F}_2^4 \), we have
\[ T_1 = \{(x_1, x_2, x_3, x_4) \in \mathbb{F}_2^4 : x_1 + x_2 + x_3 + x_4 = 1\}, \]
\[ \Omega_+ = \{(x_1, x_2, x_3, x_4) \in \mathbb{F}_2^4 : x_1 + x_2 + x_3 + x_4 = 1, x_1 = 1\}, \]
\[ \Omega_- = \{(x_1, x_2, x_3, x_4) \in \mathbb{F}_2^4 : x_1 + x_2 + x_3 + x_4 = 1, x_1 = 0\}. \]

Thus,
\[ T_1 = \{(0000), (0100), (0010), (0001), (0111), (1011), (1101), (1110)\}, \]
\[ \Omega_+ = \{(1101), (1011), (1110), (1000)\}, \]
\[ \Omega_- = \{(0111), (0100), (0010), (0001)\}. \]

Moreover, for every \((x_1, x_2, x_3, x_4) \in \mathbb{F}_2^4\), the corresponding eigenvalue of \( \Gamma \) is
\[ \lambda_{(x_1, x_2, x_3, x_4)} \]
\[ = \sum_{s \in S} (-1)^{sx} \]
\[ = (-1)^{x_2 + x_3 + x_4} + (-1)^{x_2 + x_4} + (-1)^{x_3 + x_4} + (-1)^{x_2 + x_3}. \]
\[ +(-1)^{x_1+x_2+x_3} + (-1)^{x_1+x_2+x_4} + (-1)^{x_1+x_3+x_4} + (-1)^{x_1+x_2+x_3}. \]

So that we have
\[ \lambda_{(0111)} = 4, \lambda_{(0100)} = \lambda_{(0010)} = \lambda_{(0001)} = -4, \]
\[ \lambda_{(1101)} = \lambda_{(1011)} = \lambda_{(1110)} = \lambda_{(1000)} = 0. \]

Thus, for every \( x \in \Omega_- \), \( v_2(\lambda_{x_0} - \lambda_x) = v_2(\pm 4) = 2 \), and for every \( y \in \Omega_+ \), \( v_2(\lambda_{x_0} - \lambda_y) = \infty \). Hence, \( \Gamma \) has PEST between \((a, b)\) and \((c, d)\) at time \( \frac{\pi}{4} \).

Below, for the convenience of the reader, we would like to give an explanation on how we obtain the connection set \( S \). Firstly, we find a primitive polynomial of degree 3 over \( \mathbb{F}_2 \). Here we choose \( m(x) = x^3 + x^2 + 1 \). Suppose that \( m(\alpha) = 0 \). Then \( \mathbb{F}_8 = \mathbb{F}(\alpha) \). It can be verified that \( \{\alpha, \alpha^2, \alpha^4\} \) is a trace-orthogonal basis of \( \mathbb{F}_8 \) over \( \mathbb{F}_2 \). Take \( f(x) = \text{Tr}(x^3) \). Then by Lemma 5, \( f(x) \) is a semi-bent function. One can check that \( \text{supp}(f) = \{1, \alpha^3, \alpha^5, \alpha^6\} \). Secondly, we compute the coordinates of the elements in \( \text{supp}(f) \) under the trace-orthogonal basis.

\[
\begin{align*}
1 &= 1\alpha + 1\alpha^2 + 1\alpha^4, \\
\alpha^3 &= 1\alpha + 0\alpha^2 + 1\alpha^4, \\
\alpha^5 &= 0\alpha + 1\alpha^2 + 1\alpha^4, \\
\alpha^6 &= 1\alpha + 1\alpha^2 + 0\alpha^4.
\end{align*}
\]

Thus, we have \( \text{supp}(f) = \{(111), (101), (011), (110)\} \). Using the “lifting technique,” we get the connection set \( S \).

\[\square\]

7 Conclusion remarks

In this paper, we provide an explicit and tractable characterization on cubelike graphs having PEST (see Lemma 1 and Theorem 1). By importing a so-called lifting technique, we show that one can obtain cubelike graphs having PEST by using bent or semi-bent functions (see Theorems 3 and 4). In fact, we can also use some plateau functions to get graphs which have PEST, see Example 1. Characterizing such graphs is one of our further research topics.

As we mentioned in the introduction part of this paper, PEST is a newly proposed conception, many crucial questions about edge-based quantum walks haven’t been settled. In fact, instead of node-version continuous quantum walks, we just consider edge-version continuous quantum walks in this paper. Even though the edge-version continuous-type Markov chain is established by Chen and Godsil [8], there are still many questions waiting for answers. We list some of them as follows:

1. There are many kinds of node-version discrete random quantum walks on graphs, see for example [2,29]. However, there is no edge-version discrete random walks defined on graphs known in the literature so far, let alone the conceptions such as the transfer rate vs time etc.

For this question, we have the following possible approach to establishing a discrete random walk: For a given \( d \)-regular (directed) graph, firstly, for any node, we give
an ordering of the \(d\) edges associated with it. We start with an initial edge state \(D(a_0, b_0)\), if we are at an edge \((a_t, b_t)\) at the step \(t\), we then move to the next edge which is the \(r\)-th edge of the node \(b_t\) according to a probability distribution \(P\), where \(1 \leq r \leq d\). We think that this approach may produce a discrete random walk under some restraints on the graph and the probability distribution \(P\). Based on this, we can further investigate the deeper properties of the random walk. For example, we can study how to define the mixing time, filling time, the transfer rate vs time, etc. over an edge-version discrete quantum walk.

2. For the node-version quantum walks, it is not clear yet how to transform discrete quantum walks into continuous quantum walks and vice versa. This is an important issue for two reasons: (1) in the classical case, discrete and continuous random walks are connected via a limit process, and (2) it is not natural/elegant to have two different kinds of quantum diffusion, one of them with an extra particle (the quantum coin) with no clear connection between them. See [29] for details. For this question, we mention the following two papers for the interested readers.

(1) In [26], Strauch presents a connection between discrete and continuous quantum walks.
(2) In [11], Childs presents a framework for simulating a continuous quantum walk as a limit of discrete quantum walks.

Thus, the following question arises:
For edge-version quantum walks, is there any connection between discrete quantum walks and continuous quantum walks? Can we transform a continuous (edge-version) quantum walk into a discrete quantum walk?

3. In this paper, we just treat PEST on cubelike graphs, can we have some simplified characterizations on other graphs having PEST with respect to [8, Lemma 2.4, Theorem 3.9]? for example, Cayley graphs over abelian or nonabelian groups. Can we have some classifications on specific families of graphs having PEST?

Acknowledgements  The author would like to express his grateful thankfulness to the editor and the referee for their valuable comments and suggestions.

Funding  This work was supported by National Natural Science Foundation of China under the grant numbers: 11771007, 12171241.

References

1. Acevedo, O.L., Gobron, T.: Quantum walks on Cayley graphs. J. Phys. A Math. Gen. 39, 585–599 (2006)
2. Aharonov, D., Ambainis, A., Kempe, J., Vazirani, U.: Quantum Walks on Graphs, pp. 50–59. ACM Press, New York (2000)
3. Ahmadi, B., Haghighi, M.M.S., Mokhtar, A.: Perfect state transfer on the Johnson scheme. Arxiv arXiv:1710.09096v1 (2017)
4. Angeles-Canul, R.J., Norton, R., Opperman, M., Paribello, C., Russell, M., Tamon, C.: Perfect state transfer, integral circulants and join of graphs. Quantum Comput. Inf. 10, 325–342 (2010)
5. Bašić, M., Petković, M.D.: Some classes of integral circulant graphs either allowing or not allowing perfect state transfer. Appl. Math. Lett. 22, 1609–1615 (2009)
6. Bernasconi, A., Godsil, C., Severini, S.: Quantum networks on cubelike graphs. Phys. Rev. Lett. 91(20), 207901 (2003)
7. Bose, S.: Quantum communication through an unmodulated spin chain. Phys. Rev. Lett. 91(20), 207901 (2003)
8. Chen, Q., Godsil, C.: Edge state transfer. Arxiv arXiv:1906.01159v1 (2019)
9. Childs, A., Cleve, R., Deotto, E., Farhi, E., Gutmann, S., Spielman, D.: Exponential algorithmic speedup by a quantum walk. In: Proceedings of 35th ACM Symposium on Theory of Computing, pp. 59–68 (2003)
10. Childs, A.M.: Universal computation by quantum walk. Phys. Rev. Lett. 102(18), 180501 (2009)
11. Childs, A.: On the relationship between continuous and discrete time quantum walk. Commun. Math. Phys. 294(2), 581–603 (2010)
12. Cheung, W., Godsil, C.: Perfect state transfer in cubelike graphs. Linear Algebra Appl. 435(10), 2468–2474 (2011)
13. Christandl, M., Datta, N., Dorlas, T., Ekert, A., Kay, A., Landahl, A.J.: Perfect state transfer of arbitrary state in quantum spin networks. Phys. Rev. A 73(3), 032312 (2005)
14. Christandl, M., Datta, N., Ekert, A., Landahl, A.J.: Perfect state transfer in quantum spin networks. Phys. Rev. Lett. 92(18), 187902 (2004)
15. Coutinho, G.: Quantum State Transfer in Graphs. Ph.D. dissertation, University of Waterloo (2014)
16. Coutinho, G., Godsil, C.: Perfect state transfer is poly-time. Quantum Inf. Comput. 17(5 and 6), 495–602 (2017)
17. Dillon, J., Dobbertin, H.: New cyclic difference sets with Singer parameters. Finite Fields Appl. 10, 342–389 (2004)
18. Farhi, E., Gutmann, S.: Quantum computation and decision trees. Phys. Rev. A (3) 58(2), 915–928 (1998)
19. Godsil, C.: Periodic graphs. Electron. J. Combin. 18(1), #23 (2011)
20. Godsil, C.: State transfer on graphs. Discrete Math. 312(1), 129–147 (2012)
21. Godsil, C.: When can perfect state transfer occur? Electron. J. Linear Algebra 23, 877–890 (2012)
22. Lovasz, L., Winkler, P.: Mixing times. In: Aldous, D., Propp, J. (eds.) Microsurveys in Discrete Probability, Dimacs Series in Discrete Mathematics and Theoretical Computer Science, 41 (1998). https://doi.org/10.2307/2670027
23. Cao X., Feng, K.: Perfect state transfer on Cayley graphs over dihedral groups. Linear Multilinear Algebra. (2019). https://doi.org/10.1080/03081087.2019.1599805
24. Mesnager, S.: Bent Functions. Fundamentals and Results. Springer, Cham (2016)
25. Seroussi, G., Lempel, A.: Factorization of symmetric matrices and trace-orthogonal bases in finite fields. SIAM J. Comput. 9, 758–767 (1980)
26. Strauch, F.W.: Connecting the discrete and continuous-time quantum walks. Phys. Rev. A 74, 030301 (2006)
27. Štefaňák, M., Shoupý, S.: Perfect state transfer by means of discrete-time quantum walk on complete bipartite graphs. Quantum Inf. Process. 16(3), 72 (2017)
28. Tan, Y., Feng, K., Cao, X.: Perfect state transfer on abelian Cayley graphs. Linear Algebra Appl. 563, 331–352 (2019)
29. Venegas-Andraca, S.E.: Quantum walks: a comprehensive review. Quantum Inf. Process. 11, 1015–1106 (2012)
30. Zhan, H.: An infinite family of circulant graphs with perfect state transfer in discrete quantum walks. Quantum Inf. Process. 12 Art. 369 (2019)

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.