2018

A complete characterization of plateaued Boolean functions in terms of their Cayley graphs

Riera, Constanza; Solé, Patrick; Stnic, Pantelimon

A complete characterization of plateaued Boolean functions in terms of their Cayley graphs

Constanza Riera[1], Patrick Solé, Pantelimon Stănică[2]

[1]Department of Computing, Mathematics, and Physics,
Western Norway University of Applied Sciences
5020 Bergen, Norway; csr@hvl.no
[2] CNRS/LAGA, University of Paris 8, 2 rue de la Liberté,
93 526 Saint-Denis, France; patrick.sole@telecom-paristech.fr
[3] Department of Applied Mathematics, Naval Postgraduate School,
Monterey, CA 93943, USA; pstanica@nps.edu

Abstract

In this paper we find a complete characterization of plateaued Boolean functions in terms of the associated Cayley graphs. Precisely, we show that a Boolean function f is s-plateaued (of weight $= 2^{(n+s-2)/2}$) if and only if the associated Cayley graph is a complete bipartite graph between the support of f and its complement (hence the graph is strongly regular of parameters $e = 0, d = 2^{(n+s-2)/2}$). Moreover, a Boolean function f is s-plateaued (of weight $\neq 2^{(n+s-2)/2}$) if and only if the associated Cayley graph is 3-walk-regular (and also ℓ-walk-regular, for all odd $\ell \geq 3$) with some explicitly given parameters.

Keywords: Plateaued Boolean functions, Cayley graphs, strongly regular, walk regular.

1 Introduction

Boolean functions are very important objects in cryptography, coding theory, and communications, and have connections with many areas of discrete mathematics [4, 5]. In particular bent functions, which offer optimal resistance to linear cryptanalysis, when used in symmetric cryptosystems, have been extensively studied [13, 15]. They were shown in [1, 2] to be connected to strongly regular graphs. This connection occurs through the Cayley graph with generator set the support of the Boolean function (denoted by Ω_f below). Namely, having two nonzero components in the Walsh-Hadamard spectrum translates at the Cayley graph level as having three eigenvalues. This link is often referred to as the *Bernasconi-Codenotti correspondence*.

In this paper, we extend this connection by relating semibent and, in general, plateaued functions with a special class of walk-regular graphs. Plateaued Boolean functions are characterized as having three values in their Walsh-Hadamard spectrum [12].

Their corresponding Cayley graphs belong to a special class of regular graphs with either three or four eigenvalues in their spectrum. The three eigenvalue case is dealt with by the strong regularity and the four eigenvalues case corresponds to the strongly t-walk-regular graphs introduced by Fiol and Garriga [9]. The special case of four eigenvalues of these graphs was studied in particular in [8].

The material is organized as follows. The next section compiles the necessary notions and definitions on Boolean functions and graph spectra. Section 3 derives the main characterization result of the paper.

2 Preliminaries

2.1 Boolean functions

Let $\mathbb{F}_2$ be the finite field with two elements and $\mathbb{Z}$ be the ring of integers. For any $n \in \mathbb{Z}^+$, the set of positive integers, let $[n] = \{1, \ldots, n\}$. The Cartesian product of n copies of $\mathbb{F}_2$ is $\mathbb{F}_2^n = \{\mathbf{x} = (x_1, \ldots, x_n) : x_i \in \mathbb{F}_2, i \in [n]\}$ which is an n-dimensional vector space over $\mathbb{F}_2$, which we will denote by $\mathbb{V}_n$. We will denote by $\oplus$, respectively, $+$, the operations on $\mathbb{F}_2^n$, respectively, $\mathbb{Z}$. For any $n \in \mathbb{Z}^+$, a function $F : \mathbb{V}_n \to \mathbb{F}_2$ is said to be a *Boolean function* in n variables. The set of all Boolean functions will be denoted by $\mathcal{B}_n$. A Boolean function can be regarded as a multivariate polynomial over $\mathbb{F}_2$, called the *algebraic normal form* (ANF)

$$f(x_1, \ldots, x_n) = a_0 \oplus \sum_{1 \le i \le n} a_i x_i \oplus \sum_{1 \le i < j \le n} a_{ij} x_i x_j \oplus \cdots \oplus a_{12\ldots n} x_1 x_2 \ldots x_n,$$

where the coefficients $a_0, a_{ij}, \ldots, a_{12\ldots n} \in \mathbb{F}_2$. The maximum number of variables in a monomial is called the (*algebraic*) *degree*.

For a Boolean function $f \in \mathcal{B}_n$, we define its sign function $\hat{f}$ by $\hat{f}(\mathbf{x}) = (-1)^{f(\mathbf{x})}$. For $\mathbf{u} = (u_1, \ldots, u_n)$, $\mathbf{x} = (x_1, \ldots, x_n)$, we let $\mathbf{u} \cdot \mathbf{x} = \sum_{i=1}^n u_i x_i$ be the regular scalar (inner) product on $\mathbb{V}_n$. For a binary string $\mathbf{s}$, we let $\bar{\mathbf{s}}$ denote the binary complement of $\mathbf{s}$. The (Hamming) *weight* of a binary string $\mathbf{s}$, denoted by $wt(\mathbf{s})$, is the number of nonzero bits in $\mathbf{s}$.

We order $\mathbb{F}_2^n$ lexicographically, and denote $\mathbf{v}_0 = (0, \ldots, 0, 0)$, $\mathbf{v}_1 = (0, \ldots, 0, 1)$, $\mathbf{v}_{2^n-1} = (1, \ldots, 1, 1)$. The *truth table* of a Boolean function $f \in \mathcal{B}_n$ is the binary string of length 2^n, $[f(\mathbf{v}_0), f(\mathbf{v}_1), \ldots, f(\mathbf{v}_{2^n-1})]$ (we will often omit the commas). The (Hamming) *weight* of a function f is the cardinality of the support $\Omega_f = \{\mathbf{x} : f(\mathbf{x}) = 1\}$, that is, is the weight of its truth table. We define the *Fourier transform* of f by

$$\mathcal{W}_f(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{V}_n} f(\mathbf{x}) (-1)^{\mathbf{u} \cdot \mathbf{x}},$$

and the *Walsh-Hadamard transform* of f by

$$\mathcal{W}_{\hat{f}}(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x})} (-1)^{\mathbf{u} \cdot \mathbf{x}}.$$

A function f for which $|\mathcal{W}_{\hat{f}}(\mathbf{u})| = 2^{n/2}$ for all $\mathbf{u} \in \mathbb{V}_n$ is called a *bent* function [14]. Further recall that $f \in \mathcal{B}_n$ is called *plateaued* if $|\mathcal{W}_{\hat{f}}(\mathbf{u})| \in \{0, 2^{(n+s)/2}\}$ for all $\mathbf{u} \in \mathbb{V}_n$ for a fixed integer s depending on f (we also call f then *s-plateaued*). If $s = 1$ (n must then be odd), or $s = 2$ (n must then be even), we call f *semibent*. For more on Boolean functions (bent, semibent, plateaued, etc.), the reader can consult [3, 4, 5, 13] and the references therein.

2.2 A short primer on strong regularity and walk regularity

A graph is *regular of degree* r (or r-regular) if every vertex has degree r, where the degree of a vertex is defined as the number of edges incident to it. We say that an r-regular graph G is a *strongly regular graph* (srg) with parameters (v, r, e, d) if there exist nonnegative integers e, d such that for all vertices $\mathbf{u}, \mathbf{v}$ the number of vertices adjacent to both $\mathbf{u}, \mathbf{v}$ is e, (resp. d), if $\mathbf{u}, \mathbf{v}$ are adjacent, (resp. nonadjacent). See [6] for further properties of these graphs.

For a Boolean function f on $\mathbb{V}_n$, we define the *Cayley graph* of f to be the graph $G_f = (\mathbb{V}_n, E_f)$ whose vertex set is $\mathbb{V}_n$, and whose set of edges is defined by

$$E_f = \{(\mathbf{w}, \mathbf{u}) \in \mathbb{V}_n \times \mathbb{V}_n \,:\, f(\mathbf{w} \oplus \mathbf{u}) = 1\}.$$

The adjacency matrix A_f is the matrix whose entries are $A_{i,j} = f(\mathbf{i} \oplus \mathbf{j})$ (where $\mathbf{i}$ is the binary representation as an n-bit vector of the index i). It is simple to prove that A_f has the dyadic property: $A_{i,j} = A_{i+2^{k-1},j+2^{k-1}}$. One can derive from its definition that G_f is a *regular graph of degree* $wt(f) = |\Omega_f|$ (see [6, Chapter 3] for further definitions and properties of these graphs).

Given a graph f and its adjacency matrix A, the *spectrum* $Spec(G_f)$ is the set of eigenvalues of A (called also the eigenvalues of G_f). We assume throughout that G_f is connected (in fact, one can show that all connected components of G_f are isomorphic) [1, 6].

It is known (see [6, pp. 194–195]) that a connected r-regular graph is strongly regular if and only if it has exactly three distinct eigenvalues $\lambda_0 = r, \lambda_1, \lambda_2$ (so $e = r + \lambda_1\lambda_2 + \lambda_1 + \lambda_2$, $d = r + \lambda_1\lambda_2$). Bent functions exactly correspond to those strongly regular graphs with $e = d$ (Bernasconi-Codenotti corespondence).

The following result is known [6, Th. 3.32, p. 103] (the second part follows from a counting argument and is also well known).

Proposition 1. *If A is the adjacency matrix of a strongly r-regular graph of parameters e, d and $|V| = v$, then*

$$A^2 = (e - d)A + (r - d)I + dJ,$$

where J is the all 1 matrix. Further, $r(r - e - 1) = d(v - r - 1)$.

The distance in the graph $\Gamma = (V, E)$ between two vertices $x, y \in V$, denoted by $d(x, y)$, is given by the length of the shortest path between x and y. The diameter of a graph is $D = \max_{x,y \in V} d(x, y)$. A connected graph is called *distance-regular* of

parameters (c_i, a_i, b_i) (called intersection numbers), if, for all $0 \leq i \leq D$, and for all vertices x, y with $d(x, y) = i$, among the neighbors of y, there are c_i that are at distance $i-1$ from x, a_i at distance i, and b_i at distance $i+1$ (thus Γ is regular of degree $r = b_0$).

Fiol and Garriga [9] introduced t-walk-regular graphs as a generalization of both distance-regular and walk-regular graphs. We call a graph $\Gamma = (V, E)$ a *t-walk-regular* (assuming Γ has its diameter at least t) if the number of walks of every given length ℓ between two vertices $x, y \in V$ depends only on the distance between x, y, provided it is $\leq t$. In [8], van Dam and Omidi generalized this concept and called Γ a *strongly ℓ-walk-regular* with parameters $(\sigma_\ell, \mu_\ell, \nu_\ell)$ if there are $\sigma_\ell, \mu_\ell, \nu_\ell$ walks of length ℓ between every two adjacent, every two non-adjacent, and every two identical vertices, respectively. Certainly, every strongly regular graph of parameters (v, r, e, d) is a strongly 2-walk-regular graph with parameters (e, d, r).

Similarly to Proposition 1, the adjacency matrix A of a strongly ℓ-walk-regular graph will satisfy the following property.

Proposition 2 ([8])**.** *Let $\ell > 1$, and A be the adjacency matrix of a graph Γ. Then Γ is a strongly ℓ-walk-regular with parameters $(\sigma_\ell, \mu_\ell, \nu_\ell)$ if and only if*

$$A^\ell + (\mu_\ell - \sigma_\ell)A + (\mu_\ell - \nu_\ell)I = \mu_\ell J.$$

3 Plateaued Boolean functions

In general, the spectrum of the Cayley graph of an s-plateaued Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ will be 4-valued, and therefore the graph will not be strongly regular (see [5, Theorem 9.7]). This can be easily deduced from the fact that, if the Walsh-Hadamard transform of a Boolean function takes values in $\{0, \pm k\}$ (for s-plateaued functions, $k = 2^{(n+s)/2}$), then the Fourier transform of f takes values in $\{wt(f), 0, \pm\frac{k}{2}\}$ (recall that the Fourier transform of f gives the graph spectrum of the corresponding Cayley graph), as the following argument shows.

By [5, Eq. (2.15)],

$$\mathcal{W}_f(\mathbf{w}) = 2^{n-1}\delta(\mathbf{w}) - \frac{1}{2}\mathcal{W}_{\hat{f}}(\mathbf{w}).$$

Note that, for $\mathbf{w} = \mathbf{0}, \mathcal{W}_f(\mathbf{0}) = wt(f)$. By Parseval's identity (see [5]), $2^{2n} = \sum_{\mathbf{w}\in\mathbb{F}_2^n} |\mathcal{W}_f(\mathbf{w})|^2$, the multiplicity of $\pm k$ is $\frac{2^{2n}}{k^2}$. Hence, the multiplicity of these eigenvalues will be (assuming $wt(f) \neq \frac{k}{2}$; the other case follows easily):

(*i*) If f is balanced, then $\mathcal{W}_{\hat{f}}(\mathbf{0}) = 0$, while $\mathcal{W}_f(\mathbf{0}) = wt(f)$. Then, the multiplicity of $\lambda_1 = wt(f)$ is 1, the multiplicity of $\lambda_3 = 0$ is $2^n - \frac{2^{2n}}{k^2} - 1$, while the multiplicities of $\lambda_2, \lambda_4 = \pm\frac{k}{2}$ will sum to $\frac{2^{2n}}{k^2}$.

(*ii*) If f is not balanced, then $\mathcal{W}_{\hat{f}}(\mathbf{0}) = \pm k$, while $\mathcal{W}_f(\mathbf{0}) = wt(f)$. Then, the multiplicity of $\lambda_1 = wt(f)$ is 1, the multiplicity of 0 is $2^n - \frac{2^{2n}}{k^2}$, while the multiplicities of $\pm\frac{k}{2}$ will sum to $\frac{2^{2n}}{k^2} - 1$.

Example: $n = 3$, $f = x_1x_2 \oplus x_1x_3 \oplus x_2x_3$, which is semibent, since $\mathcal{W}_{\hat{f}}(\mathbf{w}) = (0\ 4\ 4\ 0\ 4\ 0\ 0\ -4))^T$. We compute that $\mathcal{W}_f(\mathbf{w}) = (4\ -2\ -2\ 0\ -2\ 0\ 0\ 2)^T$, which is 4-valued.

Certainly, if f is semibent, the multiplicities are more precisely known (see [12], for example). For instance, if n is odd (without loss of generality, we assume that $f(\mathbf{0}) = 0$), the multiplicities of the spectra coefficients of $\hat{f}$ are

value	multiplicity
0	2^{n-1}
$2^{(n+1)/2}$	$2^{n-3} + 2^{(n-3)/2}$
$-2^{(n+1)/2}$	$2^{n-3} - 2^{(n-3)/2}$.

We show in Figure 1 the Cayley graph of a semibent function.

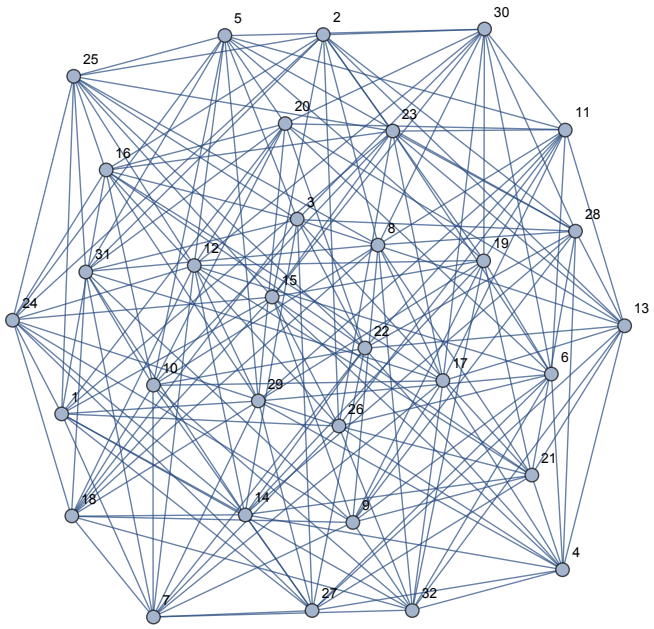

Figure 1: Cayley graph associated to the semibent $f(\mathbf{x}) = x_1x_2 \oplus x_3x_4 \oplus x_1x_4x_5 \oplus x_2x_3x_5 \oplus x_3x_4x_5$

3.1 s-Plateaued Boolean functions f with $wt(f) = 2^{(n+s-2)/2}$

Theorem 3. *If $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is s-plateaued and $wt(f) = 2^{(n+s-2)/2}$, then G_f (if connected) is the complete bipartite graph between the vectors in Ω_f and vectors in $\mathbb{F}_2^n \setminus \Omega_f$ (if disconnected, it is a union of complete bipartite graphs). Moreover, G_f is a strongly regular graph with $(e, d) = \left(0, 2^{(n+s-2)/2}\right)$.*

Proof. We know that the Walsh-Hadamard spectra of $\hat{f}$ in this case is $\{0, \pm 2^{(n+s)/2}\}$ and therefore, the spectra of f is also 3-valued, that is, $\{wt(f), 0, \pm 2^{(n+s-2)/2}\} = \{0, \pm 2^{(n+s-2)/2}\}$, and thus, the Cayley graph of f in this case is strongly regular. Now,

from [6], we know that if G_f has three distinct eigenvalues $\lambda_0 = wt(f) > \lambda_1 = 0 > \lambda_2 = -\lambda_0$, then G_f is the complete bipartite graph between the nodes in Ω_f and nodes in $\mathbb{F}_2^n \setminus \Omega_f$.

Since the eigenvalues of the strongly regular graph G_f of f can be expressed in terms of the parameters e, d, namely

$$\lambda_0 = wt(f),\ \lambda_{1,2} = \frac{1}{2}\left(e - d \pm \sqrt{(e-d)^2 - 4(d - wt(f))}\right),$$

or equivalently, $e = r + \lambda_1\lambda_2 + \lambda_1 + \lambda_2, d = r + \lambda_1\lambda_2$, and using our knowledge of the Walsh-Hadamard spectra of f, renders the last claim. □

3.2 General s-plateaued Boolean functions

We now assume that f is s-plateaued and $wt(f) \neq 2^{(n+s-2)/2}$, and, therefore, the spectrum of G_f is 4-valued. It is known (see [11]) that if G is connected and regular with four distinct eigenvalues, then G is walk-regular. In fact, in our case a result much stronger is true (see our theorem below). We will need the following two propositions (we slightly change notations, to be consistent).

Proposition 4 (van Dam and Omidi [8, Proposition 4.1])**.** *Let Γ be a connected regular graph with four distinct eigenvalues $r > \lambda_2 > \lambda_3 > \lambda_4$. Then Γ is strongly 3-walk-regular if and only if $\lambda_2 + \lambda_3 + \lambda_4 = 0$.*

Proposition 5 (van Dam and Omidi [8, Proposition 3.1])**.** *A connected r-regular graph Γ on v vertices is strongly ℓ-walk-regular with parameters $(\sigma_\ell, \mu_\ell, \nu_\ell)$ if and only if all eigenvalues except r are roots of the equation*

$$x^\ell + (\mu_\ell - \sigma_\ell)x + \mu_\ell - \nu_\ell = 0,$$

and r satisfies

$$r^\ell + (\mu_\ell - \sigma_\ell)r + \mu_\ell - \nu_\ell = \mu_\ell v.$$

In our main theorem of this section we show the counterpart for the Bernasconi-Codenotti equivalence in the case of plateaued functions.

Theorem 6. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function, and assume that G_f is connected, and that $r := wt(f) \neq 2^{(n+s-2)/2}$. Then, f is s-plateaued (with 4-valued spectra for f) if and only if G_f is strongly 3-walk-regular of parameters $(\sigma, \mu, \nu) = (2^{-n}r^3 + 2^{n+s-2} - 2^{s-2}r, 2^{-n}r^3 - 2^{s-2}r, 2^{-n}r^3 - 2^{s-2}r)$ (hence $\mu = \nu$).*

Proof. We first assume that f is s-plateaued and so, its spectra is $\{0, \pm 2^{(n+s)/2}\}$. Consequently, the spectra of G_f is 4-valued (since $r := wt(f) \neq 2^{(n+s-2)/2}$), namely $\{r = wt(f), \lambda_2 := 2^{(n+s-2)/2}, \lambda_3 := 0, \lambda_4 := -2^{(n+s-2)/2}\}$. The fact that G_f is strongly 3-walk-regular follows from Proposition 4, since $\lambda_2 + \lambda_3 + \lambda_4 = 0$, which certainly happens for our graphs. Moreover, the parameters (σ, μ, ν) (we removed, for convenience,

the subscripts $\ell = 3$) can be found using Proposition 5 as solutions to the diophantine system (recall that in our case $v = 2^n$ and $r = wt(f)$)

$$\begin{aligned} 0 &= 2^{3(n+s-2)/2} + (\mu - \sigma)2^{(n+s-2)/2} + \mu - \nu, \\ 0 &= -2^{3(n+s-2)/2} - (\mu - \sigma)2^{(n+s-2)/2} + \mu - \nu, \\ \mu\, 2^n &= r^3 + (\mu - \sigma)r + \mu - \nu, \end{aligned}$$

namely, $(\sigma, \mu, \nu) = (2^{-n}r^3 + 2^{n+s-2} - 2^{s-2}r, 2^{-n}r^3 - 2^{s-2}r, 2^{-n}r^3 - 2^{s-2}r)$.

Conversely, assuming G_f is a 3-walk-regular graph with the above parameters, then the eigenvalues $\lambda_2 > \lambda_3 > \lambda_4$ will satisfy the equation

$$x^3 + (\mu - \sigma)x + \mu - \nu = 0,$$

which will render the roots, $\lambda_2 = 2^{(n+s-2)/2}, \lambda_3 = 0, \lambda_4 = -2^{(n+s-2)/2}$. The claim is shown. □

Remark 7. *Using a result of Godsil* [10] *one can easily show (under mild conditions – thus removing strongly regular ones, for example) that the graphs corresponding to plateaued functions are not distance-regular.*

In fact, from [8] we know that the graph with four distinct eigenvalues is ℓ-walk-regular for any odd $\ell \geq 3$, but in our case we can show a lot more, by finding the involved parameters precisely.

Theorem 8. *If A is the adjacency matrix of the Cayley graph corresponding to an s-plateaued with 4-valued spectra (of f), then G_f is ℓ-walk-regular for any odd ℓ of parameters $(\sigma_\ell, \mu_\ell, \nu_\ell)$, where $\ell = 2t + 1$, $\sigma_\ell = \mu\frac{2^{(n+s-2)t} - r^{2t}}{2^{n+s-2} - r^2} + 2^{(n+s-2)t}$, $\mu_\ell = \nu_\ell = \mu\frac{2^{(n+s-2)t} - r^{2t}}{2^{n+s-2} - r^2}$. Further, the following identity holds, for all $t \geq 1$,*

$$A^{2t+1} = 2^{(n+s-2)t}A + \mu\frac{2^{(n+s-2)t} - r^{2t}}{2^{n+s-2} - r^2}\, J \ ,$$

where $(\sigma, \mu, \nu) = (2^{-n}r^3 + 2^{n+s-2} - 2^{s-2}r, 2^{-n}r^3 - 2^{s-2}r, 2^{-n}r^3 - 2^{s-2}r)$.

Proof. From our Theorem 6, we know that

$$A^3 = (\sigma - \mu)A + \mu J,$$

since we know that $\mu = \nu$. We will show our result by induction, and so, for simplicity we label $x_1 := \sigma - \mu = 2^{n+s-2}, y_1 = \mu = 2^{-n}r^3 - 2^{s-2}r$. Assume now that

$$A^{2t+1} = x_t A + y_t J. \tag{1}$$

First, observe that, since our graph is regular of degree r, then $AJ = rJ$, and more general, $A^k J = r^k J$. Multiplying (1) by A^2, we get

$$\begin{aligned} A^{2t+3} &= x_t A^3 + y_t A^2 J \\ &= x_t(x_1 A + y_1 J) + y_t r^2 J \\ &= x_t x_1 A + (x_t y_1 + y_t r^2)J, \end{aligned}$$

and consequently, we get the recurrences

$$x_{t+1} = x_t x_1$$
$$y_{t+1} = x_t y_1 + y_t r^2.$$

Solving the system, we get $x_{t+1} = x_1^{t+1} = (\sigma - \mu)^{t+1} = 2^{(n+s-2)(t+1)}$ and $y_{t+1} = y_1 \frac{x_1^{t+1} - r^{2(t+1)}}{x_1 - r^2} = \mu \frac{2^{(n+s-2)(t+1)} - r^{2(t+1)}}{2^{n+s-2} - r^2}$ and our claim is shown. □

References

[1] A. Bernasconi, B. Codenotti, *Spectral Analysis of Boolean Functions as a Graph Eigenvalue Problem*, IEEE Trans. on Computers 48:3 (1999), 345–351.

[2] A. Bernasconi, B. Codenotti, J. M. VanderKam, *A Characterization of Bent Functions in terms of Strongly Regular Graphs*, IEEE Trans. on Computers 50:9 (2001), 984–985.

[3] L. Budaghyan, Construction and Analysis of Cryptographic Functions, Springer-Verlag, 2014.

[4] C. Carlet, *Boolean Functions for Cryptography and Error Correcting Codes*, Chapter of the volume "Boolean Models and Methods in Mathematics, Computer Science, and Engineering", Cambridge University Press (Eds. Y. Crama, P. Hammer) (2010), pp. 257–397.

[5] T. W. Cusick, P. Stănică, Cryptographic Boolean Functions and Applications, 2nd Ed. (Academic Press, San Diego, CA, 2017); 1st Ed., 2009.

[6] D. M. Cvetkovic, M. Doob, H. Sachs, Spectra of Graphs, Academic Press, 1979.

[7] E. R. van Dam, W. H. Haemers, *A characterization of distance-regular graphs with diameter three*, J. Algebraic Combin. 6 (1997), 299–303.

[8] E. R. van Dam, G. R. Omidi, *Strongly walk-regular graphs*, J. Combin. Theory Ser. A 120 (2013), 803–810.

[9] M. A. Fiol, E. Garriga, *Spectral and geometric properties of k-walk-regular graphs*, Electron. Notes Discrete Math. 29 (2007), 333–337.

[10] C. D. Godsil, *Bounding the diameter of distance-regular graphs*, Combinatorica 8:4 (1988), 333–343.

[11] X. Huang, Q. Huang, *On regular graphs with four distinct eigenvalues*, Linear Algebra and Its Applications 512 (2017), 219–233.

[12] S. Mesnager, *On semi-bent functions and related plateaued functions over the Galois field* $\mathbb{F}_{2^n}$, Proceedings "Open Problems in Mathematics and Computational Science", LNCS, Springer, pp. 243–273, 2014.

[13] S. Mesnager, Bent functions: fundamentals and results, Springer Verlag, 2016.

[14] O. S. Rothaus, *On Bent Functions*, J. Combinatorial Theory, Series A 20 (1976) 300–305.

[15] N. Tokareva, Bent Functions, Results and Applications to Cryptography, Academic Press, San Diego, CA, 2015.