Discrete Applied Mathematics 214 (2016) 116–125

Contents lists available at ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam

Existentially closed graphs via permutation polynomials over finite fields

Nguyen Minh Hai [a], Tran Dang Phuc [a], Le Anh Vinh [b,*]

[a] *Faculty of Mathematics, Mechanics and Informatics, Hanoi University of Science, Vietnam National University, Hanoi, Viet Nam*

[b] *University of Education, Vietnam National University, Hanoi, Viet Nam*

ARTICLE INFO

Article history:
Received 28 November 2014
Received in revised form 17 June 2015
Accepted 18 May 2016
Available online 25 July 2016

Keywords:
Existentially closed graphs
Permutation polynomial
Distance graphs

ABSTRACT

For a positive integer n, a graph is *n-existentially closed* or n-e.c. if we can extend all n-subsets of vertices in all possible ways. It is known that almost all finite graphs are n-e.c. Despite this result, until recently, only few explicit examples of n-e.c. graphs are known for $n > 2$. In this paper, we construct explicitly a 4-e.c. graph via a linear map over finite fields. We also study the colored version of existentially closed graphs and construct explicitly many $(3, t)$-e.c. graphs via permutation polynomials and multiplicative groups over finite fields.

1. Introduction

For a positive integer n, a graph is *n-existentially closed* or n-e.c. if we can extend all n-subsets of vertices in all possible ways. Precisely, for every pair of subsets A, B of vertex set V of the graph such that $A \cap B = \emptyset$ and $|A| + |B| = n$, there is a vertex z not in $A \cup B$ that joined to each vertex of A and no vertex of B. From the results of Erdős and Rényi [4], almost all finite graphs are n-e.c. Despite this result, until recently, only few explicit examples of n-e.c. graphs are known for $n > 2$. See [2] for a comprehensive survey on the constructions of n-e.c. graphs.

In [13], the third listed author studied a multicolor version of this adjacency property. Let n, t be positive integers. A t-edge-colored graph G is (n, t)-e.c. or (n, t)-existentially closed if for any t disjoint sets of vertices $A_1, \dots, A_t$ with $|A_1| + \cdots + |A_t| = n$, there is a vertex x not in $A_1 \cup \cdots \cup A_t$ such that all edges from this vertex to the set A_i are colored by the ith color. Since the complement of a graph can be viewed as a color class, the usual definition of n-e.c. graphs is the special case of $t = 2$.

For a positive integer N, the probability space $G_t(N, \frac{1}{t})$ consists of all t-colorings of the complete graph of order N such that each edge is colored independently by any color with the probability $\frac{1}{t}$. The third listed author showed [13, Theorem 1.1] that almost all graphs in $G_t(N, \frac{1}{t})$ have the property (n, t)-e.c. as $N \to \infty$. The proof of this theorem is similar to the proof that almost all finite graphs have n-e.c. property (see, for example, [4]). Although this result implies that there are many (n, t)-e.c. graphs, it is nontrivial to construct such graphs. The third listed author [13, theorem 1.2] constructed explicitly many graphs satisfying this condition. Let q be an odd prime power and $\mathbb{F}_q$ be the finite field with q elements. Let q be a prime power such that $t|(q-1)$ and ν be a generator of the multiplicative group of the field $\mathbb{F}_q$. We identify the color set with the set $\{0, \dots, t-1\}$. The graph $P_{q,t}$ is a graph with vertex set $\mathbb{F}_q$, the edge between two distinct vertices being colored by the ith color if their sum is of the form ν^j where $j \equiv i \bmod t$. One can show that $P_{q,t}$ is an (n, t)-e.c. graph when

* Corresponding author.
E-mail addresses: nguyenminhhai06@gmail.com (N.M. Hai), trandangphuc234@gmail.com (T.D. Phuc), vinhla@vnu.edu.vn (L.A. Vinh).

http://dx.doi.org/10.1016/j.dam.2016.05.017
0166-218X/

q is large enough. More precise, if q is a prime power such that

$$q > 3^{(t-1)n} q^{1/2} + n2^{(t-1)n}, \quad (1.1)$$

then $P_{q,t}$ has the (n, t)-e.c. property. (Note that, from the probabilistic argument, the upper bound for the smallest order of an (n, t)-e.c. is better than the bound in (1.1). The probabilistic bound, however, is not explicit.)

Note that the main motivation of that work is to construct new classes of n-e.c. graphs. From any (n, t)-e.c. graph, we can obtain an n-e.c. graph by dividing the color set into two sets. For a positive integer N and $0 < \rho < 1$, the probability space $G(N, \rho)$ consists of graphs with vertex set of size N so that two distinct vertices are joined independently with probability ρ. It is known that almost all graphs in $G(N, \rho)$ have the n-e.c. graphs. The above construction supports this statement by constructing explicitly n-e.c. graphs with edge density p for any $0 < \rho < 1$.

For any positive integers n and t, let $f(n, t)$ be the order of the smallest (n, t)-e.c. graph. It follows from (1.1) that

$$f(n, t) \leq 9^{(t-1)n} + n2^{(t-1)n}.$$

In particular, if $n = 3$ then $f(3, t) = O(9^{3t})$, which is of exponential order. We recall that the expressions $A \ll B$ and $A = O(B)$ are each equivalent to the statement that $|A| \leq cB$ for some constant $c > 0$. In [15], the second listed author gave new explicit constructions of $(3, t)$-graphs of polynomial order. Let p be a prime such that $t|(p-1)$, $\mathbb{F}_p$ be the finite field of p elements, and ν be a generator of the multiplicative group of the field. We identify the color set with the set $\{0, \ldots, t-1\}$. For any $d \geq 2$, the graph $Q_{p^d,t}$ is the complete graph with the vertex set $\mathbb{F}_p^d$, the edge between two distinct vertices $\boldsymbol{x}, \boldsymbol{y}$ being colored by the ith color if their distance

$$\|\boldsymbol{x} - \boldsymbol{y}\| = (x_1 - y_1)^2 + \cdots + (x_d - y_d)^2$$

is of the form ν^j where $j \equiv i \bmod t$. The third listed author [15, Theorem 1.1] showed that $Q_{p^d,t}$ is an $(3, t)$-e.c. graph when $p \geq t^6$ and $d \geq 5$. As an immediate corollary, $f(3, t) = O(t^{30})$, which is of polynomial order.

1.1. Permutation polynomials

The main purpose of this paper is to give other explicit constructions of $(3, t)$-graphs via permutation polynomials with two advantages over previous known results. First, we can relax the condition $t|(p-1)$. Second, we can construct explicitly $(3, t)$-e.c. graphs with arbitrarily color density. Let p be a prime and $\mathbb{F}_p$ be the finite field of p elements. Suppose that $f(x)$ is a polynomial over $\mathbb{F}_p$ of degree smaller than p. A basic question in the theory of finite fields is to estimate the size V_f of the value set $\{f(a) \mid a \in \mathbb{F}_q\}$. Because a polynomial $f(x)$ cannot assume a given value of more than $\deg(f)$ times over a field, one has the trivial bound

$$\left\lfloor \frac{p-1}{\deg(f)} \right\rfloor + 1 \leq V_f \leq p. \quad (1.2)$$

If the lower bound in (1.2) is attained, then $f(x)$ is called a minimal value set polynomial. The classification of minimal value set polynomials is the subject of several papers; see [3,5,6,10]. The results in these papers assume that p is large compared to the degree of $f(x)$.

If the upper bound in (1.2) is attained, then $f(x)$ is called a permutation polynomial. The classification of permutation polynomials has received considerable attention. See the book of Lidl and Niederreiter [9] and the survey article by Mullen [11]. We identify $\mathbb{F}_p$ with the set $\{0, 1, \ldots, p-1\}$. Let $\mathcal{A} = A_1 \cup \cdots \cup A_t$ be a partition of $\mathbb{F}_p$ such that each A_i is a block of consecutive numbers in $\mathbb{F}_p$, that is for any $1 \leq i \leq t$, there exist t_i, s_i such that $A_i = \{t_i + 1, \ldots, t_i + s_i\}$. Let $f \in \mathbb{F}_p[x]$ be a permutation polynomial of degree at least 2. We also need to assume that p is large compared to the degree of $f(x)$. For any $1 \leq i \leq t$, set $V_i = \{f(a) : a \in A_i\}$. For any $d \geq 2$, the graph $G_{f,\mathcal{A}}^d$ is the complete graph with the vertex set $\mathbb{F}_p^d$; the edge between two distinct vertices $\boldsymbol{x}, \boldsymbol{y}$ being colored by the ith color if their distance $\|\boldsymbol{x} - \boldsymbol{y}\| \in V_i$. We claim that $G_{f,\mathcal{A}}^d$ is an $(3, t)$-e.c. graph when $d \geq 5$ and $|A_i| \gg \deg(f) p^{5/6} \log p$ for all $1 \leq i \leq t$.

Theorem 1.1. *Let f be a nonlinear permutation polynomial over $\mathbb{F}_p$ and let $\mathcal{A} = A_1 \cup \cdots \cup A_t$ be a partition of $\mathbb{F}_p$ such that each A_i is a block of consecutive numbers of cardinality $|A_i| \gg \deg(f) p^{5/6} \log p$. For any $d \geq 5$, the graph $G_{f,\mathcal{A}}^d$ has $(3, t)$-e.c. property.*

Note that these graphs are just Cayley graphs of $\mathbb{F}_p^d$. To construct non-Cayley $(3, t)$-e.c. graphs, we need to adjust the definition of $G_{f,\mathcal{A}}^d$ slightly using the following notion of mixed distance between two points $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_p^d$:

$$\|\boldsymbol{x} - \boldsymbol{y}\|_m = 2x_1y_1 + (x_2 - y_2)^2 + \cdots + (x_d - y_d)^2.$$

Theorem 1.2. *Let f be a nonlinear permutation polynomial over $\mathbb{F}_p$ and let $\mathcal{A} = A_1 \cup \cdots \cup A_t$ be a partition of $\mathbb{F}_p$ such that each A_i is a block of consecutive numbers of cardinality $|A_i| \gg \deg(f) p^{5/6} \log p$. For any $d \geq 6$, the graph $H_{f,\mathcal{A}}^d$ is the complete graph with the vertex set $\mathbb{F}_p^d$; the edge between two distinct vertices $\boldsymbol{x}, \boldsymbol{y}$ being colored by the ith color if their mixed distance*

$$\|\boldsymbol{x} - \boldsymbol{y}\|_m \in \{f(a) : a \in A_i\}.$$

Then $H_{f,\mathcal{A}}^d$ is a non-Cayley $(3, t)$-e.c. graphs.

The proof of Theorem 1.2 is exactly the same as the proof of Theorem 1.1 and is left to the interested reader.