On the families of graphs with the fastest growth of girth and their usage in cryptography

Vasyl Ustimenko

Royal Holloway University of London
Institute of Telecommunication and Global Information Space, Kyiv, Ukraine
vasylustimenko@yahoo.pl
↪

Abstract. Symbolic computations with usage of algebraic graphs $A(n, F_q)$ and $A(n, F_q[x_1, x_2, \ldots, x_n])$ were used for the development of various cryptographic algorithms because the length of their minimal cycle (the girth) tends to infinity when n is growing. It was announced recently that for each commutative integrity ring the girth of $A(n, K)$ is $\geq 2n$. In this paper we present essentially shorter closed proof of this statement and evaluate the girth of some induced subgraphs of $A(n, K[x_1, x_2, \ldots, x_n])$.

Keywords: family of graphs of large girth, commutative integrity rings, symbolic computations, commutative ring of multivariate polynomials

Funding: This research is supported by British Academy Fellowship for Researchers at Risk 2022.

1 On lower bound for the girth of graphs $A(n, K)$ over integrity ring K

All graphs Γ in this paper are symmetric antireflexive binary relations on the set of their vertices V, i.e Γ is a subset of Cartesian product V with itself, such that $(x, y) \in \Gamma$ implies $(y, x) \in \Gamma$, for each $x \in V$ element (x, x) does not belong to Γ (see [1]). Missing definitions of Graph Theory such as path in the graph, cycle of length m, neighbour of the vertex, bipartite graph and etc. can be also found in [1].

Definition of commutative ring, integrity ring K and ring of multivariate polynomials $K[x_1, x_2, \ldots, x_n]$ reader can find in [2].

Let K be a commutative ring. We define $A(n, K)$ as a bipartite graph with the point set ${}^nP = K^n$ and line set ${}^nL = K^n$ (two copies of a Cartesian power of K are used). We will use brackets and parenthesis to distinguish tuples from ${}^nP$ and ${}^nL$. So $(p) = (p_1, p_2, \ldots, p_n) \in {}^nP$ and $[l] = [l_1, l_2, \ldots, l_n] \in {}^nL$. The incidence relation ${}^nI = A(n, K)$ (or the corresponding bipartite graph ${}^nI$) is given by condition p and l are incident if and only if the equations of the following kind hold:

$p_2 - l_2 = l_1 p_1$,
$p_3 - l_3 = p_1 l_2$,

p$_4 - l_4 = l_1 p_3$, (6)
$p_5 - l_5 = p_1 l_4$,
$\dots$,
$p_n - l_n = p_1 l_{n-1}$ for odd n and
$p_n - l_n = l_1 p_{n-1}$ for even n.

Graphs $A(m,K)$ were obtained in [3] as quotients of graphs $D(n,K)$). This incidence structure was defined in the following way.

Let K be an arbitrary commutative ring. We consider the totality P of points of kind

$x = (x) = (x_{1,0}, x_{1,1}, x_{1,2}, x_{2,2}, \dots, x_{i,i}, x_{i,i+1}, \dots)$ with coordinates from K
and the totality L of lines of kind
$y = [y] = [y_{0,1}, y_{1,1}, y_{1,2}, y_{2,2}, \dots, y_{i,i}, y_{i,i+1}, \dots]$.

We assume that tuples (x) and $[y]$ has finite support and a point (x) is incident with a line $[y]$, i. e. xIy or $(x)I[y]$, if the following conditions are satisfied:

$x_{i,i} - y_{i,i} = y_{i-1,i} x_{1,0}$,
$x_{i,i+1} - y_{i,i+1} = y_{0,1} x_{i,i}$, (8)
where $i = 1, 2, \dots$.

We denote the graph of this incidence structure as $A(K)$. We consider the set *Root* of indexes of points and lines of $A(K)$ as a subset of totality of all elements $(i+1, i+1)$, $(i, i+1)$, $(i+1, i)$, $i \geq 0$ of root system $\tilde{A}_1$ of affine type. We see that $Root = \{(1,0), (01), (11), (12), (22), (23), \dots\}$. So we introduce $R_{1,0} = Root - \{0,1\}$ and $R_{0,1} = Root - \{1,0\}$. It allows us to identify sets P and L with affine subspaces $\{f : R_{1,0} \to K\}$ and $\{f : R_{0,1} \to K\}$ of functions with finite supports.

For each positive integer $k \geq 2$, we obtain an incidence structure (P_k, L_k, I_k) as follows. Firstly, P_k and L_k are obtained from P and L, respectively, by simply projecting each vector onto its k initial coordinates. The incidence I_k is then defined by imposing the first $k-1$ incidence relations and ignoring all the other ones. The incidence graph corresponding to the structure (P_k, L_k, I_k) is denoted by $A_k(K)$. The comparison of equations of $A_k(K)$ and $A(k,K)$ allows to justify the isomorphism of these graphs. It is convenient for us to identify graphs $A(k,K)$ with graphs $A_k(K)$ and write indexes of coordinates of points and lines as elements from *Root*.

The procedure to delete last coordinates of points and lines of graph $A(n,K)$ defines the homomorphism ${}^n\Delta$ of $A(n,K)$ onto $A(n-1,K)$, $n > 2$. The family of these homomorphisms defines natural projective limit of $A(n,K)$ which coincides with $A(K)$. We introduce the colour function ρ on vertexes of graph $A(K)$ or $A(n,K)$ as x_{10} for the point $(x_{10}, x_{11}, x_{12}, \dots)$ and y_{01} for the line $[y_{01}, y_{11}, x_{12}, \dots]$. We refer to $\rho(v)$ for the vertex v as *colour* of vertex v.

As it follows directly from definitions for each vertex v and each colour $a \in K$ there is exactly one neighbour of v with the colour v. We refer to this fact as linguistic property of graphs $A(n,K)$ and $A(K)$. In fact such property were used for the definition of the class of linguistic graphs (see [3] and further references).

Let us consider a special automorphisms of graphs $A(K)$ and $A(n,K)$ defined over arbitrary commutative ring K. We take the list L of coordinates of the point of incidence structure $A(K)$ consisting of (10), (11), (12), (22), ..., (ii), $(i,i+1)$, ... Let $<$ stands for the natural order on L presented in the written above sequence. Assume that ${}^nL$ stands for the first n elements of L. For each element α from L we introduce automorphism $T_{\alpha,t}$, $t \in K$ moving point $(p) = (p_{1,0}, p_{1,1}, p_{1,2}, \dots)$ to $({}^1p) = ({}^1p_{1,0}, {}^1p_{1,1}, {}^1p_{1,2}, \dots)$ and line $[l_{0,1}, l_{1,1}, l_{1,2}, \dots]$ to the line $[{}^1l_{0,1}, {}^1l_{1,1}, {}^1l_{1,2}, \dots]$ accordingly to the following rules.

(1) If $\alpha = (k,k)$, $k > 0$ then $T_{\alpha,t}((p))$ has coordinates ${}^1p_{1,0} = p_{10}$, ${}^1p_{1,1} = p_{1,1}$, ..., ${}^1p_{k-1,k} = p_{k-1,k}$, ${}^1p_\alpha = p_\alpha + t$, ${}^1p_{i-1,i} = p_{i-1,i} - p_{i-k-1,i-k)t}$, ${}^1p_{ii} = p_{ii} - p_{i-k,i-k}t$ for each i, $i > k$ and $T_{\alpha,t}([l])$ has coordinates ${}^1l_{01} = l_{01}$, ${}^l_{11} = l_{11}$, ..., ${}^1l_{i-1,i} = l_{i-1,i}$, ${}^1l_\alpha = l_\alpha + t$, ${}^1l_{i-1,i} = l_{i-1,i} - l_{i-k-1,i-k}t$, ${}^1l_{ii} = l_{ii} - l_{i-k,i-k}t$, ... for each i, $i > k$.

(2) In the case of $\alpha = (i,i+1)$, $i \geq 1$ transformation $T_{\alpha,t}$ changes coordinate $p_{i,i+1}$ of (p) for $p_{i,i+1} + t$ and does not change its other coordinates, $T_{\alpha,t}([l])$ coincides with $[l]$.

(3) In the case of $\alpha = (1,0)$ transformation $T_{\alpha,t}$ changes the first coordinate $p_{1,0}$ of point for $p_{1,0} + t$ and does not change its other coordinates, the tuple $T_{\alpha,t}([l])$ has coordinates l_{01}, $l_{11} - l_{0,1}t$, ..., l_{i-1i}, $l_{i,i} - l_{i-1,i}t$, $i > 1$.

PROPOSITION 1.1.

(1) *Transformations $T_{\alpha,t}$ are automorphism of the graph $A(K)$.*

(2) *They generate group $H(K)$ which preserves partition sets of $A(K)$ and acts as point transitive transformation group.*

Proof. Direct check justifies that written above transformations preserves the incidence relation between points and lines. Let p $= (p_{1,0}, p_{11}, p_{12}, \dots)$ be an arbitrary point. Then consecutive application of transformations $T_{\alpha,t(\alpha)}$, $\alpha \in L$ accordingly to defined above order $<$ with appropriate ring elements $t(\alpha)$ allows us to move the point p to $(0,0,\dots)$. Thus the action of the group is transitive on P.

We consider transformations ${}^nT_{\alpha,t}$, $\alpha \in {}^nL$ which correspond to natural action of $T_{\alpha,t}$ on the vertices of graph $A(n,K)$. Similarly to previous statement we justify the following statement.

PROPOSITION 1. 2.

(1) *The transformation ${}^nT^{\alpha,t}$ are automorphism of the graph $A(n,K)$.*

(2) *They generate group ${}^nH(K)$ which preserves partition sets of $A(n,K)$ and acts as point transitive transformation group.*

LEMMA 1.1.

As we mentioned above graph $A(n,K)$ satisfies to linguistic property. Thus the path (0), v_1, v_2, ..., v_{n-1} in the graph $A(n,K)$ are determined by colours z_i of elements v_i, $i = 1,2,\dots,n-1$.

LEMMA 1. 2 (two numbers lemma).

Let $v_0, v_1, v_2, \dots, v_{n-1}$ be the path of $A(n,K)$ starting in zero point $v_0 = (0,0,\dots,0)$ given by the tuple of colours z_1, z_2, ..., z_{n-1}. Then last two coordinates of v_{n-1} are $z_1z_2(z_1 - z_3)(z_2 - z_4)\dots(z_{n-3} - z_{n-1})$ and $zn - 1z_1z_2(z_1 -$

$z_3)(z_2-z_4)\dots(z_{n-3}-z_{n-1})$. The last two coordinates of v_1, v_2, $\dots$, v_{n-3} equal to 0.

The proof of this statement can be obtained via straight usage of mathematical induction. This statement was used in [3] for the prove of the fact that girth $D(n,K)$ is at least $n+5$ in the case of integrity ring K.

COROLLARY 1. 1.

Let v_0, v_1, v_2, $\dots$, v_{n-1} be the path in the graph $A(n-1,K)$ with $v_0=(0,0,\dots,0)$ and $\rho(v_i)=z_i$. Then the last coordinate of the destination point v_{n-1} is $z_1z_2(z_1-z_3)(z_2-z_4)\dots(z_{n-3}-z_{n-1})$. The last coordinate of v_{n-2} is zero.

Noteworthy that for the path as above the conditions $z_i-z_{i+2}\neq 0$ and $z_2\neq 0$ hold.

COROLLARY 1.2.

Assume that conditions of previous statement hold, z_1 is not a zero and K is an integrity ring. Then the last coordinate of the tuple v_{n-1} is not a zero but the last coordinate of v_{n-3} is zero.

As we mentioned above the procedure to cut the last coordinate of each vertex of graph $A(n,K)$ defines colour preserving homomorphism ${}^n\Delta$ from the graph $A(n,K)$ to $A(n-1,K)$. So if graph $A(n-1,K)$ has no cycles of length s then graph $A(n,k)$ does not have C_{2s} as well.

THEOREM 1.1 [4].

Let K be an integrity ring. Then the girth of graph $A(n,K)$ is at least $2n$.

Proof. As it follows from the definitions of graphs $A(2,K)$ and $A(3,K)$ they are isomorphic to well investigated graphs $D(2,K)$ and $D(3,K)$ (see [11]). Thus their girth are ≥ 6 and ≥ 8 respectively. It means that graphs $A(n,K)$, $n\geq 4$ do not contain cycles C_4 and C_6. So the girth of $A(4,K)$ is at least 8. Let us consider graph $A(5,K)$ and assume that it has cycle C of length 8. Let (p) be some point from this cycle. We can apply automorphism τ from ${}^5H$ which moves point (p) to point $(0,0,0,0,0)$. Thus $\tau(C)$ is formed by two paths of kind (0), $[v_1]$, (v_2), $[v_3]$, (v_4), $[v_5]$ of colours z_1, z_2, z_3, z_4, z_5 and (0), $[u_1]$, (u_2), $[u_3]$ of colours y_1, y_2, z_5 such that $[u_3]=[v_5]$. Noteworthy that $y_1\neq z_1$. Without loss of generality we can assume that $z_1\neq 0$. Then according to Corollary 1.2 the last coordinate of $[v_5]$ is different from zero but the last coordinate of $[u_3]$ equals 0. Thus we get a contradiction. So the graph $A(5,K)$ has no cycles C_4, C_6 and C_8. It means that its girth is ≥ 10 and graphs $A(n,K)$, $n\geq 5$ has no cycles C_4, C_6, C_8.

Assume that graph $A(6,K)$ has a cycle C of length 10. Without loss of generality we can assume that C contains zero point and formed by two paths of kind (0), $[v_1]$, (v_2), $[v_3]$, (v_4), $[v_5]$, (v_6) of colours z_i, $i=1,2,\dots,6$ with $z_1\neq 0$ and (0), $[u_1]$, (u_2), $[u_3]$, (u_4) of colours y_1, y_2, y_3, z_6 such that $[u_4]=[v_6]$. According to the Corollary 1.2 last coordinate of v_6 is not zero but last coordinate of u_4 is 0. So we get a contradiction. Thus girth of $A(n,K)$, $n\geq 6$ is ≥ 12. Continuation of this process for $n=7,8,\dots$ justifies the statement.

The fact that the girth of homogeneous algebraic graphs $A(n, K)$, $K \neq F_2$ defined over the field K is bounded by $2n+2$ is proven in [4]. So we justify the following statement.

PROPOSITION 1.1.

Let K be a field with more than 2 elements. Then the girth of graph $A(n.K)$ is $2n$ or $2n+2$.

2 Cryptographically significant corollaries

Let K be commutative integrity ring containing at least two elements. We consider nonempty subsets R and S of $K[x_1, x_2, \ldots, x_n]$ for $n \geq 1$. Let ${}^{R,S}A(n, K[x_1, x_2, \ldots, x_n]$ be the induced subgraph of $A(n, K)$ of all points and lines with colours from R and S respectively. According to famous result by D. Hilbert $K[x_1, x_2, \ldots, x_n]$ is also an integrity ring. So the girth of infinite graph A(n, K[$\mathrm{x}_1, x_2, \ldots, x_n$]) is $\geq 2n$ and the following statement holds.

PROPOSITION 2.1.

The girth of graph ${}^{R,S}A(n, K[x_1, x_2, \ldots, x_n])$ is at least $2n$.

COROLLARY 2.1.

Let K be a field $\neq F_2$ and subsets R and S contain the field of constants K then the girth of graph $\Gamma = {}^{R,S}A(n, K[x_1, x_2, \ldots, x_n])$ is $2n$ or $2n+2$.

This statement follows from the fact that Γ contains induced subgraph $A(n, K)$ which contains the cycle of length $2n$ or $2n+2$. Similarly we get the following statement.

COROLLARY 2.2.

Let K be a field of odd characteric p and subsets R and S contain prime field F_p then the girth of graph $\Gamma =^{R,S} A(n, K[x_1, x_2, \ldots, x_n])$ is $2n$ or $2n+2$.

These results about the girth of induced subgraphs can be used for further investigation of properties of cryptographic systems based on symbolic computations with usage of graphs $A(n, F_q[x_1, x_2, \ldots, x_n])$ such as [5, [6], [7], see also 4 and [8] and further references.

1. A. Brower, A. Cohen, A. Nuemaier, *Distance regular graphs*, Springer, Berlin,1989.
2. B. L, Van Der Waerden, *Algebra*, Vol 1, Springer V, 2011, 265 pp.
3. V. Ustimenko , *Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography*, Journal of Mathematical Sciences.- Springer. v.140. No.3. 2007. P. 412-434.
4. V. Ustimenko, *New results on algebraic graphs of large girth and their impact on Extremal Graph Theory and Algebraic Cryptography*, IACR e-print archive, 2022/1489.
5. V. Ustimenko, M. Klisowski, *On Noncommutative Cryptography with cubical multivariate maps of predictable density*, In Intelligent Computing, Proceedings of the 2019 Computing Conference, Volume 2, Part of Advances in Intelligent Systems and Computing, AISC, volume 99, pp, 654-674.
6. V. Ustimenko, M. Klisowski, *On $D(n;q)$ -quotients of large girth and hidden homomorphism based cryptographic protocols*, Communication Papers of the 17th Conference on Computer Science and Intelligence Systems, M. Ganzha, L. Maciaszek, M. Paprzycki, D. lzak (eds). ACSIS, Vol. 32, pages 199206 (2022).

7. V. Ustimenko, T.Chojecki, *On Multivariate Maps of High Degree for the Post Quantum Protection of Virtual Organizations (short paper)*, CEUR Workshop, Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2022), 156-161.
8. V. Ustimenko, *On Extremal Algebraic Graphs and Multivariate Cryptosystems*, IACR e-print archive, 2022/1537.