On regular forests given in terms of algebraic geometry, new families of expanding graphs with large girth and new multivariate cryptographical algorithms

Urszula Romańczuk, Vasyl Ustymenko
Maria Curie-Skodowska University in Lublin (Poland)

urszula_romanczuk@yahoo.pl, vasyl@hektor.umcs.lublin.pl

EXTENDED ABSTRACT

We are going to observe interpretations of q-regular forest (q-regular simple graph without cycles) in terms of algebraic geometry over finite field $\mathbb{F}_q$. More precisely we are interested in sequences of q-regular algebraic graphs Γ_i, defined by nonlinear equations, such that their projective limit T is well defined and does not contain cycles. So, the girth of Γ_i is growing with the growth of parameter i. We assume additionally that Γ_i, $i \to \infty$ is a family of expanders. So the upper limit of second largest eigenvalues of Γ_i is bounded away from q.

The talk is dedicated to new applications of such simple graphs of increasing girth with good expansion properties to the and designing of cryptographical algorithms (stream ciphers, key exchange protocols, public key algorithms digital signatures,constructions of hash functions). We speak about the usage of classical explicit constructions (see [6] and further references) as well as applications of the new families of graphs.

Recall that the girth is the length of minimal cycle in the simple graph. Studies of maximal size $ex(C_3, C_4, \ldots, C_{2m}, v)$ of the simple graph on v vertices without cycles of length $3, 4, \ldots, 2m$, i.e. graphs of girth $> 2m$, form an important direction of Extremal Graph Theory. As it follows from famous Even Circuit Theorem by P. Erdős' we have inequality

$$ex(C_3, C_4, \ldots, C_{2m}, v) \leq cv^{1+1/m},$$

where c is a certain constant. The bound is known to be sharp only for $m = 2, 3, 5$. The first general lower bounds of kind

$$ex(v, C_3, C_4, \ldots C_n) = \Omega(v^{1+c/n}),$$

where c is some constant $< 1/2$ were obtained in the 50th by Erdős' via studies of *families of graphs of large girth*, i.e. infinite families of simple regular graphs Γ_i of degree k_i and order v_i such that

$$g(\Gamma_i) \geq c\log_{k_i} v_i,$$

where c is the independent of i constant. Erdős' proved the existence of such a family with arbitrary large but bounded degree $k_i = k$ with $c = 1/4$ by his famous probabilistic method.

Just two explicit families of regular simple graphs of large girth with unbounded girth and arbitrarily large k are known: the family $X(p, q)$ of Cayley graphs for $PSL_2(p)$, where p and q are primes, had been defined by G. Margulis [5] and investigated by A. Lubotzky, Sarnak [2] and Phillips, and the family of algebraic graphs $CD(n, q)$ [3]. The best known lower bound for $d \neq 2, 3, 5$ had been deduced from the existence of mentioned above families of graphs

$$ex(v, C_3, C_4, \ldots, C_{2d}) \geq c(v^{1+2/(3d-3+e)})$$

where $e = 0$ if d is odd, and $e = 1$ if d is even.

By the theorem of Alon and Boppana, large enough members of an infinite family of q-regular graphs satisfy the inequality $\lambda \geq 2\sqrt{q-1} - o(1)$, where λ is the second largest eigenvalue in absolute value. Ramanujan graphs are q-regular graphs for which the inequality $\lambda \leq 2\sqrt{q-1}$

holds. We say that regular graphs of bounded degree q form a family of Ramanujan graphs if the second lagest eigenvalue of each graph is bounded from above by $2\sqrt{q-1}$

It is clear that a family of Ramanujan graphs of bounded degree q has the best possible spectral gap $q-\lambda$. We say, that family of q-regular graphs Γ_i is a family of *almost Ramanujan graphs* if its second largest eigenvalues are bounded above by $2\sqrt{q}$.

The mentioned above family $X(p,q)$ is a family of Ramanujan graphs. That is why we refer to them as Cayley - Ramanujan graphs. The family $CD(n,q)$ is a family of almost Ramanujan graphs. It is known that if $q \geq 5$ these graphs are not Ramanujan despite the projective limit $CD(q)$ of $CD(n,q)$ is a q-regular tree. The reason is that the eigenspace of $CD(q)$ is not a Hilbert space (topology is p-adic).

Expanding properties of $X(p,q)$ and $D(n,q)$ and the and high girth property of both families can be used for the construction of fast stream ciphers with good mixing properties[8]. Notice that both properties had been use for construction of good class of LDPC error correcting codes which is an important pratical tool of security for satellite communications. The usage of $CD(n,q)$ as Tanner graphs producing LDPC codes lead to better properties of corresponding codes in the comparison with the use of Cayley - Ramanujan graphs (see [4]).

Both families $X(p,q)$ and $CD(n,q)$ are consist of edge transitive graphs, their expansion properties and property to be graphs of large girth hold also for random graphs, which have no automorphisms at all. To make better deterministic approximation of random graph we can look at regular expanding graphs of increasing girth without edge transitive automorphism group (see [7]).

THEOREM *For each prime power $q, q \geq 3$ there exist a family of q-regular bipartite almost Ramanujan graphs of large girth without edge transitive automorphism group.*

The proof of the theorem is based on new explicit construction of the families satisfying condition of formulated above theorem. The new cryptographical algorithms based on walks of new graphs and their analogs defined over arithmetical rings will be presented at the conference.

The important direction of Multivariate Cryptography is a search for a families of invertible polynomial maps f_n of $\mathbb{F}_q^n$ with the degree bounded degree (usually degrees are 2 or 3), such that the growth of degree f_n^{-1} with the growth of n is supported by mathematical statement (see [1] an further references). Absence of mathematical theory here motivates alternative research on cryptographical applications of computable multivariate functions f_n with the degree cn, $c > 0$ for f_n and its inverse.

We present pseudocubical cryptosystem from this class, such that the list of cubical public rules are given in terms of standard variables $x_1, x_2, \ldots, x_n$ corresponding to characters from the plainspace and extra characters $y_1, y_2, \ldots, y_t$, where $t = f(n)$ is a certain linear function from n. The list of rules is of kind

$$x_i \to g_i(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_t), \quad i = 1, 2, \ldots, n,$$

where f_i are cubical expressions and recursive "compression rules":

$$\begin{aligned}
&y_1 \to h_1(x_1, x_2, \ldots, x_n,),\\
&y_2 \to h_2(x_1, x_2, \ldots, x_n, y_1,),\\
&y_3 \to h_3(x_1, x_2, \ldots, x_n, y_1, y_2),\\
&\qquad \ldots\\
&y_t \to h_t(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_{t-1}).
\end{aligned}$$

The resulting encryption map has degree cn, $c \geq 1/4$. So the algorithm is resistant against plain linearisation attacks. We can prove that the order of the map is growing to infinity with the growth of parameter n.

Traditionally one subset of vertices of a bipartite graphs is denoted by $V_1 = P$ and called a set of points and another one $V_2 = L$ is called a set of lines. Let K be a commutative ring, P and L be two copies of Cartesian power K^n, where $n \geq 2$ is an integer. Brackets and parenthesis will allow the reader to distinguish points and lines. In this note we assume that if z $\in K^n$, then (z) $\in P$ and [z] $\in L$.

Let us introduce an infinite bipartite graph $D(K)$ defined on sets of points of kind

$$(\mathrm{x}) = (x_1, x_2, x_3, x_3', \ldots, x_n, x_n', \ldots)$$

and lines of kind

$$[y] = [y_1, y_2, y_3, y'_3, \dots, y_n, y'_n, \dots]$$

via incidence relation $I : (x)I[y]$ if and only if the following relations hold

$$\begin{aligned} x_2 - y_2 &= y_1 x_1, \\ x_3 - y_3 &= x_1 y_2, \\ x_4 - y_4 &= y_1 x_3, \\ x_5 - y_5 &= x_1 y_4, \\ &\dots \end{aligned}$$

together with equalities

$$\begin{aligned} x'_3 - y'_3 &= y_1 x_2, \\ x'_4 - y'_4 &= x_1 y'_3, \\ x'_5 - y'_5 &= y_1 x'_4, \\ &\dots . \end{aligned}$$

If n is odd then $x_n - y_n = x_1 y_{n-1}$ and $x'_n - y'_n = y_1 x'_{n-1}$. If n is even then $x_n - y_n = y_1 x_{n-1}$ and $x'_n - y'_n = x_1 y'_{n-1}$.

We also consider the family of graphs $B(m, n, K)$ for case $m \leq n$, whose vertices are points of kind

$$(x) = (x_1, x_2, x_3, x'_3, \dots, x_{m+2}, x'_{m+2}, x'_{m+3}, x'_{m+4}, \dots, x'_{n+2})$$

from set $P_{m,n} = K^{m+n+2}$ and lines of kind

$$[y] = [y_1, y_2, y_3, y'_3, \dots, y_{m+2}, y'_{m+2}, y'_{m+3}, y'_{m+4}, \dots, y'_{n+2}]$$

from $L_{m,n} = K^{m+n+2}$ such that (x) and [x] are incident if and only if relations from the written above list holds for variables
$\{x_1, x_2, x_3, x'_3, \dots, x_{n+2}, x'_{n+2}, x'_{n+3}, \dots, x'_{m+2}\} \cup \{y_1, y_2, y_3, y'_3, \dots, y_{m+2}, y'_{m+2}, y'_{m+3}, \dots, y'_{n+2}\}$. We refer to written above list as list of variables of graph $B(m, n, K)$.

There is a natural homomorphism $\phi_{m,n}$ from $D(K)$ onto $B(m, n, K)$ defined via procedure of deleting coordinates of infinite points (x) and lines [y] which do not belong to written above finite list.

If $K = \mathbb{F}_q$ be the finite fields of q elements then $B(m, n, K) = B(m, n, q)$. We have the following results:

PROPOSITION *The projective limit of $B(m, n, K) = B(m, n, q)$ if $n \to \infty$ is an forest consisting of $t = [m/2]$ infinite q-regular trees.*

THEOREM *If $m = cn + d$, $c > 0$ then family of algebraic graphs $B(m, n, q)$ is a q-regular bipartite almost Ramanujan graphs of large girth without edge transitive automorphism group.*

We define the colour $\rho(v)$ of vertex v (point or line) from $B(m, n, K)$ as first coordinate of corresponding tuple. For each vertex v of the graph $B(m, n, K)$ there is exactly one neighbour $N_\alpha(v)$ of colour $\rho(v) + \alpha$ for chosen $\alpha \in K$. The map $v \to N(v)$ is a bijection.

We can prove that all connected components of graphs $B(m, n, K)$ are isomorphic. Let us denote by $CB(m, n, K)$ the graph isomorphic to connected component of $B(m, n, K)$. Let N'_α be the restriction of the operator N_α onto the set of vertices of chosen connected component $CB(m, n, K)$. If charK $\neq 2$ then connected component of the graph is the solution variety for the system of equations

$$\begin{aligned} a_1(v) &= b_1, \\ a_2(v) &= b_2, \\ &\dots \\ a_t(v) &= b_t. \end{aligned}$$

One can eliminate $t = [m/2]$ variables in operator N_α using the above system of equations and this way determine the operator N'_α. In our cryptographic algorithms we using this operators to increase the security.

Keywords
multivariate cryptography, family of graphs of large girth, expanding graphs, Ramanujan graphs, regular trees via algebraic equations

Bibliography

[1] Ding J., Gower J. E., Schmidt D. S., *Multivariate Public Key Cryptosystems*, Springer, Advances in Information Security, 25 (XVIII) (2006): 260.

[2] A. Lubotsky, R. Philips, P. Sarnak, *Ramanujan graphs*, J. Comb. Theory., 115, N 2., (1989), 62-89.

[3] F. Lazebnik, V. A. Ustimenko and A. J. Woldar, *A New Series of Dense Graphs of High Girth*, Bull (New Series) of AMS, v.32, N1, (1995), 73-79.

[4] D. MacKay and M. Postol, *Weakness of Margulis and Ramanujan - Margulis Low Dencity Parity Check Codes*, Electronic Notes in Theoretical Computer Science, 74 (2003), 8pp.

[5] G. Margulis, *Explicit group-theoretical constructions of combinatorial schemes and their application to desighn of expanders and concentrators*, Probl. Peredachi Informatsii., 24, N1, 51-60. English translation publ. Journal of Problems of Information transmission (1988), 39-46.

[6] V. Ustimenko, *On the extremal graph theory for directed graphs and its cryptographical applications* In: T. Shaska, W.C. Huffman, D. Joener and V. Ustimenko, Advances in Coding Theory and Cryptography, Series on Coding and Cryptology, vol. 3, 181-200 (2007).

[7] V. A. Ustimenko, U. Romańczuk, *On Extremal Graph Theory, Explicit Algebraic Constructions of Extremal Graphs and Corresponding Turing Encryption Machines*, in "Artificial Intelligence, Evolutionary Computing and Metaheuristics ", In the footsteps of Alan Turing Series: Studies in Computational Intelligence, Vol. 427, Springer, January, 2013, 257-285.