Записки научных
семинаров ПОМИ
Том 373, 2009 г.

R. T. Faizullin

FUNCTIONAL APPROACH FOR HAMILTONIAN CIRCUIT AND GRAPH ISOMORPHISM PROBLEMS

Abstract. The aim of this work is to establish relation between well-known basic problems of cryptanalysis as Hamiltonian Circuit and graph isomorphism problems and global optimization problem for classes of functionals constructed as sums of low dimensional polynomials.

The aim of this work is to establish relation between well-known basic problems of cryptanalysis [1, 2] as Hamiltonian Circuit and Subgraph Isomorphism problems and global optimization problem for classes of functionals constructed as sums of low dimensional polynomials. Let's consider for arbitrary graph the well-known Hamiltonian Circuit problem (to find a circle way vertex by vertex where vertices are not equal). We can numerate the graph vertices via numbers r_j where $r_1 = 3$ and $r_{j+1} = 2r_j + s_j$. We have the sum: $R = \sum\limits_{j=1}^{n} r_j$ from which we can recognize r_i without order. Let's take Υ_i as a set of contacted vertices with vertex i where i is one of the numbers r_j.

Then we can write:

Theorem 0.1. *If there are s Hamiltonian circuits with path numbers $t_1^r, .., t_n^r, 1 \le r \le s$ then for every $m \ge 2$ from natural numbers global minimum which equal to zero of every functionals:*

$$\begin{aligned} S_m(x_1, ., x_n) = &\sum_{v=1}^{n} \prod_{j=1}^{n} \prod_{l,p \in \Upsilon_{i,\, i=r_v}} ((i + l + p - x_{j-1} - x_j - x_{j+1})^2 \\ &+ (mi + l + p - x_{j-1} - mx_j - x_{j+1})^2 + \Theta \\ D_m(x_1, ., x_n) = &\sum_{v=1}^{n} \prod_{j=1}^{n} \prod_{l,p \in \Upsilon_{i,\, i=r_v}} ((i/lp - x_j/x_{j-1}x_{j+1})^2 \\ &+ (i^2/lp - x_j^2/x_{j+1}x_{j-1})^2) + \Theta \end{aligned}$$

Key words and phrases. Hamiltonian circuit, graph isomorphism, optimiztion problem, polynomial functional.

where

$$\Theta = (R - \sum_{w+1}^{n} x_w)^2$$

give us natural numbers $x_1 = t_1^r, .., x_n = t_n^r$ *for one of the* r.

Let's consider $D_m(x_1, .., x_n) = 0$ where every part of the sum is equal to zero or in other words for every unique number i/lp there exist equal value $x_j/x_{j-1}x_{j+1}$. Hence, we can write $\alpha x_j/\beta x_{j-1}\gamma x_{j+1} = i/lp$. Then $\alpha = \beta\gamma$ but if we consider $(i/lp - x_j/x_{j-1}x_{j+1})^2$ and $(i^2/lp - x_j^2/x_{j+1}x_{j-1})^2)$ we can write $\alpha = 1$ and $x_j = i$ so every part of the sum which equals to zero is related to only one number j. Also, number of the same parts is equal to n. We can write $lp = x_{j-1}x_{j+1}$ and factors of product are natural numbers related to other clauses, then $x_{j-1} = l$ and $x_{j+1} = p$.

We can say x_{j-1}, x_j, x_{j+1} are vertices l, i, p are part of Hamiltonian Circuit. If it's not right then there are three other natural numbers $x_{j_1-1}, x_{j_1}, x_{j_1+1}$ which mark other part of the circle $x_1, x_2, .., x_n$. Then x_{j_1} is equal to i but x_{j_1-1} is not equal to l. Hence there are not enough numbers of the 'thirds' for every i.

For S the proof is the same, so the sums are similar for products of D.

How can we solve the problem numerically? We can consider stationary point conditions:

$$\frac{\partial S}{\partial x_j} = 0 \; j = 1, ..n$$

as the system of nonlinear equations where unknowns are x_j. It's more effective approach than $\nabla D = 0$ solving.

$$\Pi_{i1jlp} = (\prod_{j=1}^{n} \prod_{l,p \in \Upsilon_{i,i=r_v}} ((i + l + p - x_{j-1} - x_j - x_{j+1})^2$$
$$+ (mi + l + p - x_{j-1} - mx_j - x_{j+1})^2)/((i + l + p - x_j - x_{j+1} - x_{j+2})$$

or

$$\Pi_{i1jlp} = \Pi_i/(((i + l + p - x_j - x_{j+1} - x_{j+2})^2 +$$
$$((i + l + p - x_j - mx_{j+1} - x_{j+2})^2)$$

and

$$\begin{aligned}
\Pi_{i2jlp} &= \Pi_i/(((i+l+p-x_j-x_{j+1}-x_{j+2})^2 \\
&\quad +((mi+l+p-x_j-mx_{j+1}-x_{j+2})^2) \\
\Pi_{i3jlp} &= \Pi_i/(((i+l+p-x_{j-}-x_j-x_{j+1})^2 \\
&\quad +((mi+l+p-x_{j-}-mx_j-x_{j+1})^2) \\
\Pi_{i4jlp} &= \Pi_i/(((i+l+p-x_{j-}-x_j-x_{j+1})^2 \\
&\quad +((mi+l+p-x_{j-}-mx_j-x_{j+1})^2)
\end{aligned}$$

$$\begin{aligned}
\Pi_{i5jlp} &= \Pi_i/(((i+l+p-x_j-x_{j-1}-x_{j-2})^2 \\
&\quad +((i+l+p-x_j-mx_{j-1}-x_{j-2})^2) \\
\Pi_{i6jlp} &= \Pi_i/(((i+l+p-x_j-x_{j-1}-x_{j-2})^2 \\
&\quad +((mi+l+p-x_j-mx_{j-1}-x_{j-2})^2) \\
\frac{\partial S}{\partial x_j} &= \sum_{i\in I}\sum_{l,p\in\Upsilon_{i,i=r_v}} (\Pi_{i1jlp}(i+l+p-x_j-x_{j+1}-x_{j+2}) \\
&\quad +\Pi_{i2jlp}(mi+l+p-x_j-mx_{j+1}-xj+2) \\
&\quad +\Pi_{i3jlp}(i+l+p-x_{j-1}-x_j-x_{j+1}) \\
&\quad +\Pi_{i4jlp}(mi+l+p-mx_{j-1}-m^2x_j-mx_{j+1})+\dots)
\end{aligned}$$

It's seems easy for exact solution: every Π_{ikjlp} is equal to 0. But we can see for large m where $m \gg n$, and for $|\Pi_{ikjlp}| \geq \varepsilon$ every other stationary points lies near 0.

Then the solution, related to global minima lies in kernel of first derivative of Φ and convergence of Newton like methods is very bad. We can solve system of equations $\Phi(\overline{x}) = 0$ with help of some kind of low relaxation methods for values of vertices $n \leq 15$.

Our problem is NP-complete and problem of global extremum NP-complete too. But if we find exact local minimum which equals to ε, we can test the problem for some m and it could give us a part of the answer for $co-NP$ problem – Hamiltonian Graph. Computational experiments give us usual values of local minimums near 10^6 for theta-graphs and near 10^{-20} for Hamiltonian Graphs.

On the other hand we can write:

Theorem 0.2. *If for given graph and for point* $x_1, .., x_n$ $|S_m(x_1, .., x_n)| \leq (m-1)^2$ *then there is at least one Hamiltonian circuit.*

If $|S_m| \leq \varepsilon$ then for every part of the sum we can write $|\Pi_i| \leq \varepsilon$ and there is at least one factor where

$$\begin{aligned}&(((i + l + p - x_{j-1} - x_j - x_{j+1})^2 \\ &+ ((mi + l + p - x_{j-1} - mx_j - x_{j+1})^2) \leq \varepsilon\end{aligned}$$

Then we can write

$$((i + l + p - x_{j-1} - x_j - x_{j+1})^2 \leq \varepsilon_1$$

$$((mi + l + p - x_{j-1} - mx_j - x_{j+1})^2 \leq \varepsilon_2$$

$$|i + l + p - x_{j-1} - x_j - x_{j+1}| \leq \sqrt{\varepsilon_1}$$

and

$$|(m-1)i - (m-1)x_j \pm \sqrt{\varepsilon_1}| \leq \sqrt{\varepsilon_2}$$

or

$$|(m-1)i - (m-1)x_j| \leq \sqrt{\varepsilon_2} + \sqrt{\varepsilon_1}$$

We can say when $\varepsilon \leq (m-1)^2$ x_j lies 'near' i.

Let x_{j-1} and x_{j+1} lie near $\overline{l}, \overline{p}$.

Then $\overline{l} = l, \overline{p} = p$. Otherwise the factor would be greater then ε. The proof is over.

Let us consider prime numbers r_i. Then we can write.

Theorem 0.3. *Let us consider two graphs* G_1 *and* G_2. *Numbers of the vertices* G_1 *are* r_i. *Numbers of the vertices of* G_2 *are natural numbers* $j = 1, 2, , ..n$ *and for every* j *related unknown weight is equal to* x_j.

If there exists a vector $x_1, .., x_n$ *where* $I_m(x_1, .., x_n) = 0$ *and function with* $m \geq 2$

$$\begin{aligned}I_m(x_1, .., x_n) = \sum_{v=1}^{n} \prod_{j=1}^{n} ((i / \prod_{p \in \Upsilon_{i, i=r_v}} p - x_j / \prod_{s \in \Upsilon_j} x_s)^2 \\ + (i^m / \prod_{p \in \Upsilon_{i, i=r_v}} p - x_j^m / \prod_{s \in \Upsilon_j} x_s)^2)\end{aligned}$$

then graphs G_k are isomorphic and isomorphism can be described as ϕ : $i \to j$, where $i = x_j$.

Modified form of I_m is:

$$SubI_m(x_1,.,x_n) = \sum_{w=1,i=r_w}^{n} \prod_{j=1}^{n} \prod_{|\Omega_i|=\left|\Upsilon_{x_j}\right|} ((i/\prod_{l_z\in\Omega_i} l_z - x_j/\prod_{x_v\in\Upsilon_{x_j}} x_v)^2 + (i^m/\prod_{l_z\in\Omega_i} l_z - x_j^m/\prod_{x_v\in\Upsilon_{x_j}} x_v)^2$$
$$\Omega_i \subseteq \Upsilon_i$$

can give us a functional associated with SUBGRAPH ISOMORPHISM PROBLEM with the same result. Proof is the same as for theorem 1.

References

1. M. Blum, *How to prove a Theorem So No One Else Can Claim It.* Proceedings of the International Congress of Mathematicians, Berkeley, CA, 1986, pp. 1444–1451.
2. O. Coldreich, *Proof that yield nothing but their validity or all languages in NP have zero-knowledge proof systems.* — J. ACM. **38** No. 3 (1991), 691–729.

Omsk State Technical University,
Russia

E-mail: r.t.faizullin@mail.ru

Поступило 21 сентября 2009 г.