Functional Approach for Hamiltonian Circuit and Graph Isomorphism Problems

R. T. Faizullin, Omsk State Technical University, r.t.faizullin@mail.ru

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 well-known Hamiltonian Circuit problem (way via circle vortex by vortex where vortexes is not equal). We can numerate the graph vortexes via prime numbers r_j where $r_1 = 3$ and $r_{j+1} = 2r_j + s_j$. We have the sum: $R = \sum_{j=1}^{n} r_j$ from which we can recognize r_i without order. Let's Υ_i is a set of contacted vortexes with vortex i where i is one of the numbers r_j .

Then we have next result:

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

$$S_m(x_1, ., x_n) = \sum_{v=1}^{n} \prod_{j=1}^{n} \prod_{l,p \in \Upsilon_{i,i=r_v}} ((i + l + p$$

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

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

$$+(i^2/lp - x_j^2/x_{j+1}x_{j-1})^2) + \Theta$$

where

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

give to us natural numbers $x_1 = t_1^r, .., x_n = t_n^r$ for one of the r. Moreover, if there exist constant $\varepsilon \simeq 1$ and there value of S_m or D_m equal to ε there are at list one Hamiltonian circuit.

Let's consider $D_m(x_1, .., x_n) = 0$ where every part of sum is equal to zero or on the other words for every unique number i/lp 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 sum which equal to zero related with only one number j. Also, number of same parts is equal to n. We can write $lp = x_{j-1}x_{j+1}$ and factors of product are natural numbers related with other clauses then $x_{j-1} = l$ and $x_{j+1} = p$.

We can say x_{j-1}, x_j, x_{j+1} are vortexes l, i, p part of Hamiltonian Circuit. If it's not then there are three other natural numbers $x_{j_1-1}, x_{j_1}, x_{j_1+1}$ marked 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 proof is same so sums are similar for products of D.

How we can solve 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 then consideration of ∇D. We can solve it with help of some kinds of well known low relaxation methods.

Note, our problem is NP-complete and problem of global extremum NP-complete too. But if we find exact global minimum which equal to ε we can tested problem for some large m and it can give to as part of the answer for $co-NP$ problem - Hamiltonian Graph.

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

Theorem 0.2 *Let us consider two graphs G_1 G_2. Numbers of the vertexes G_1 are r_i. Numbers of the vertexes of G_2 are natural numbers $j = 1, 2, ..n$ and for every j related unknown weight x_j.*

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

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

$$+(i^m/\prod_{p\in\Upsilon_{i,i=r_v}} p - x_j^m/\prod_{s\in\Upsilon_j} x_s)^2)$$

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

Modified form of I_m:

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

$$-x_j/\prod_{x_v\in\Upsilon_{x_j}} x_v)^2 + (i^m/\prod_{l_z\in\Omega_i} l_z - x_j^m/\prod_{x_v\in\Upsilon_{x_j}} x_v)^2$$

$$\Omega_i \subseteq \Upsilon_i$$

can give to us functional associated with SUBGRAPH ISOMORPHISM PROBLEM with same result.

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. V.38, No 3, 1991. P. 691-729.