# An argument for Hamiltonicity

Vadym Fedyukovych

August 23, 2008

**Abstract**

A constant-round interactive argument is introduced to show existence of a Hamiltonian cycle in a directed graph. Graph is represented with a characteristic polynomial, top coefficient of a verification polynomial is tested to fit the cycle, soundness follows from Schwartz-Zippel lemma.

## 1 Introduction

A protocol to show existence of a Hamiltonian cycle in a graph was introduced by Blum [Blu86, CF01]. Protocol uses binary challenges, and need to be repeated to achieve soundness. Protocols with 'large' challenges achieve low soundness error without repeating; example is Schnorr protocol with challenges chosen from a finite field.

We explore options resulting from algebraic structure of responses of a variant of Schnorr protocol. A protocol for Hamiltonian cycle is given in this report. Protocol is an argument on assumption of hardness of discrete logarithm problem. Protocol has a simulator algorithm, and is honest verifier perfect zero knowledge.

## 2 Preliminaries

**Definition 1** (Graph characteristic polynomial)**.** Let $\Gamma$ be a labelled directed graph defined with a set of edges $\mathbb{E}(\Gamma)$ and a set of vertices $\mathbb{V}(\Gamma)$. Non-zero labels $w_v \in \mathbb{F}_q, v \in \mathbb{V}(\Gamma)$ and flags $u_e \in \{0,1\}, e \in \mathbb{E}(\Gamma)$ are assigned to nodes and vertices. Consider a mapping to a ring of polynomials over finite field:

$$\Gamma \to f(x,y;\Gamma) = \prod_{\vec{e}_{HT} \in \mathbb{E}(\Gamma)} (1 + xw_H + yw_T) \tag{1}$$

We say $f(x,y;\Gamma)$ is a *graph characteristic polynomial*.

This definition appeared with a protocol for graph isomorphism. A similar characteristic polynomial was introduced with a protocol for vertex colorability. A related definition of set characteristic function appeared with set reconciliation [MTZ01].

**Definition 2.** *Hamiltonian cycle* is an alternating sequence $v_0, e_1, v_2, e_2 \dots v_p$ of vertices and edges of a graph $\Gamma$, $|\mathbb{V}(\Gamma)| = p$ such that all edges are different, $v_p = v_1$, and $v_i \neq v_j$ for all other pairs $(i, j)$. We denote set of edges that form the cycle with $\mathbb{H}(\Gamma)$.

**Lemma 1** (Schwartz-Zippel [Sch80], a case of a univariate polynomial)**.** *Probability to choose a root of a nonzero polynomial $f(z)$ of degree at most $d$ by sampling $z$ at random from a domain of cardinality $D$ is at most $\frac{d}{D}$.*

# 3 Protocol

Consider a graph with a prime number of vertices: $|\mathbb{V}(\Gamma)| = p$. Let $\mathbb{F}_q$ be a field with a prime number of elements such that $p|q-1$. It follows a cyclic subgroup of order $p$ exists in a multiplicative group of residue classes $Z_q^*$. Let $a^p = 1 \pmod q$, $a \neq 1$.

To recognise a cycle, we assign labels to vertices such that $w_j = a^j$, $j = 0 \dots p$, with index $j$ incrementing along the sequence. We also assign flags to edges such that $u_e = 1$ for $e \in \mathbb{H}(\Gamma)$, and $u_e = 0$ for all other edges that are not part of the cycle.

Consider a polynomial $f_w(x, y, z) \in \mathbb{F}_q[X, Y, Z]$ for some $\{\alpha_v\}$, $\alpha_v \in \mathbb{F}_q$, $v \in \mathbb{V}(\Gamma)$:

$$f_w(x, y, z) = \prod_{\vec{e}_{HT} \in \mathbb{E}(\Gamma)} (z + (x(zw_H + \alpha_H) + y(zw_T + \alpha_T)))$$

Top coefficient of $f_w(x, y, z)$ is graph characteristic polynomial:

$$f_w(x, y, z) = \sum_{k=0}^{n} f_k(x, y) z^k, \qquad n = |\mathbb{E}(\Gamma)|, \qquad f_n(x, y) = f(x, y; \Gamma)$$

Consider another polynomial $f_u(x, y, z) \in \mathbb{F}_q[X, Y, Z]$ for some $\beta_e \in \mathbb{F}_q$,

$$f_u(x, y, z) = \prod_{\vec{e}_{HT} \in \mathbb{E}(\Gamma)} (z + (zu_e + \beta_e)(xw_H + yw_T))$$

Top coefficient of $f_u(x, y, z)$ is characteristic polynomial of the cycle in the graph:

$$f_u(x, y, z) = \sum_{i=0}^{n} f_i(x, y) z^i, \quad f_n(x, y) = f(x, y; \mathbb{H}(\Gamma))$$

Let $\{\Theta_v\}$, $\{\Phi_e\}$ be responses of Okamoto protocol [Oka92] for commitments to labels and flags:

$$\Theta_v = sw_v + \alpha_v$$
$$\Phi_e = tu_e + \beta_e$$

Consider a *verification polynomial*:

$$F(x, y, s, t) = \prod_{\vec{e}_{HT} \in \mathbb{E}(\Gamma)} (ts + \Phi_e(x\Theta_H + y\Theta_T)) \tag{2}$$

Anyone can produce an estimate of $F(x, y, s, t)$ using Verifier' challenges and Prover' responses. Verifier tests that top coefficient of $F(x, y, s, t)$ is

$$C_a(x, y) = \prod_{j=0}^{p-1} (1 + xa^j + ya^{j+1}) \tag{3}$$

Common input is graph $\Gamma$, group $\mathbb{G}$, and group members $g, h$. Auxiliary input of Prover is a sequence of graph vertices that is a cycle. Protocol is shown of Figure 1.

**Lemma 2** (Recognising Hamiltonicity). *A Hamiltonian cycle exists in a graph $\Gamma, |\mathbb{V}(\Gamma)| = p$ for some prime $p, p|q-1$ if, and only if labels $w_v, v \in \Gamma$ can be assigned with $\{a^j\}$ for some $a \in Z_q^*$, $a^p = 1$, $a \neq 1$ such that*

$$\exists(\Gamma' \subset \Gamma): \quad f(x, y; \Gamma') \equiv \prod_{j=0}^{p-1} (1 + xa^j + ya^{j+1}) \tag{4}$$

*Proof.* It is clear that labels $w_v = a^j$ can be assigned to vertices along the sequence indexed with $j$ for any given $a$ such that characteristic polynomial of the cycle will be of the form (4), in case a cycle exists. We show that any subgraph with characteristic polynomial (4) is a Hamiltonian cycle.

We observe that characteristic polynomial is a product of $p$ linear polynomials that are relatively prime to one another. It follows there are exactly $p$ edges in such a graph, such that each edge connects a vertex labelled with $a^j$ and a vertex labelled with $a^{p+1}$. It follows that vertices and edges form a sequence.

We also observe there are exactly $p$ different values of the form $a^j$, $j = 0 \dots p-1$, such that the sequence never crosses itself.

From $a^p = a^0$ it follows that the last vertex in the sequence is the same as the first one, such that sequence is a cycle. □

It is clear honest Verifier always accepts for an honest Prover such that completeness holds for the protocol shown on Figure 1.

**Lemma 3** (Soundness). *Probability for an honest Verifier to accept for any Prover and any graph $\Gamma$ without Hamiltonian cycle running protocol shown on Figure 1 is at most $\frac{4|\mathbb{E}(\Gamma)|+2|\mathbb{V}(\Gamma)|}{q}$ over random choices of Verifier.*

*Proof.* We show that Prover responses are estimates of polynomials that are linear in challenge, flags used are chosen from $\{0, 1\}$ with probability at least $1 - \frac{2}{q}$, and that $f_a(x, y) \not\equiv 0$ for

$$f_a(x, y) = C_a(x, y) - f(x, y; \Gamma')$$

with probability at most $\frac{2n+2p}{q}$.

Consider a Prover capable of producing responses $\Theta'$, $\Omega'$ to a challenge $s$ such that

$$g^{\Theta'} h^{\Omega'} W^{-s} = R, \qquad \Theta' \neq \Theta, \quad \Omega' \neq \Omega$$

for

$$\Theta = sw + \alpha, \qquad \Omega = sr + \gamma$$
$$W = g^w h^r, \qquad R = g^\alpha h^\gamma$$

and for some $w, r, \alpha, \gamma \in \mathbb{F}_q$. It follows such a Prover is also capable of taking a logarithm using his responses as follows:

$$\log_h(g) = -\frac{\Omega' - \Omega}{\Theta' - \Theta}$$

We consider it infeasible for a polynomial Prover to produce valid responses $\Theta, \Omega$ other than estimates of polynomials that are linear both in challenge of Verifier and in value committed.

Consider a Prover capable of producing responses $\Phi, \Delta$ to a challenge $t$ such that

$$g^{-\Phi(\Phi - t)} h^{-\Delta} N^t E = 1$$

for

$$\Phi = tu + \beta$$
$$\Delta = t\delta + \pi$$
$$N = g^\tau h^\chi, \quad E = g^\rho h^\lambda$$

for some $u \notin \{0, 1\}$ and for some $\delta, \beta, \pi, \tau, \rho, \chi, \lambda \in \mathbb{F}_q$. It follows $f_t(z) \not\equiv 0$ for any $\beta, \tau, \rho$:

$$f_t(z) = -(zu + \beta)(z(u-1) + \beta) + \tau z + \rho$$

From Schwartz-Zippel lemma it follows there is at most $\frac{2}{q}$ probability to choose a root of $f_t(z)$ at random: $f_t(t) = 0$. It also follows that such a Prover is capable of taking a logarithm in case $f_t(t) \neq 0$ using his responses as follows:

$$\log_h(g) = \frac{\Delta - \chi t - \lambda}{f_t(t)}$$

We consider it infeasible for a polynomial Prover to produce valid responses $\Phi, \Delta$ such that $f_t(t) \neq 0$. It follows there is at most $\frac{2}{q}$ probability for an honest Verifier to accept at (14) for any Prover and for any flag $u \notin \{0, 1\}$ over random choices of challenge $t$.

Consider a Prover capable of producing responses $\{\Phi_e\}, \{\Theta_v\}, \Psi$ to challenges $x_c, y_c, s, t$ such that

$$g^{-F} h^{-\Psi} \left( \prod_{k=0}^{n-1} (M_k)^{s^k} \right)^{t^n} \prod_{i=0}^{n-1} (D_i)^{t^i} = 1$$

for

$$F = \prod_{\vec{e}_{HT} \in \mathbb{E}(\Gamma)} (ts + \Phi_e(x_c\Theta_H + y_c\Theta_T)) - t^n s^n \prod_{j=0}^{p-1} (1 + x_c a^j + y_c a^{j+1})$$

$$\Phi_e = tu_e + \beta_e$$

$$\Theta_v = sw_v + \alpha_v$$

and for some $\Psi$. From Lemma 2 it follows $f_a(x, y) \not\equiv 0$ for any subgraph of $\Gamma$. From Schwartz-Zippel lemma it follows there is at most $\frac{2p}{q}$ probability to choose a root of $f_a(x, y)$ at random: $f_a(x_c, y_c) = 0$. In case $f_a(x_c, y_c) \neq 0$ it follows $f_s(z) \not\equiv 0$ for any $\{s_k\}$:

$$f_s(z) = f_a(x_c, y_c)s^n + \sum_{k=0}^{n-1} s^k m_k$$

From Schwartz-Zippel lemma it follows there is at most $\frac{n}{q}$ probability to choose a root of $f_s(z)$ at random: $f_s(s) = 0$. In case $f_s(s) \neq 0$ it follows $f_{st}(z) \not\equiv 0$ for any $\{d_i\}$:

$$f_{st}(z) = f_s(s)z^n + \sum_{i=0}^{n-1} z^i d_i$$

From Schwartz-Zippel lemma it follows there is at most $\frac{n}{q}$ probability to choose a root of $f_{st}(z)$ at random: $f_{st}(t) = 0$. It follows that such a Prover is capable of taking a logarithm in case $f_{st}(t) \neq 0$ using his responses as follows:

$$\log_h(g) = (f_{st}(t))^{-1}(\Psi - t^n \sum_{k=0}^{n-1} s^k \eta_k - \sum_{i=0}^{n-1} t^i \mu_i)$$

We consider it infeasible for a polynomial Prover to produce valid responses $\{\Phi_e\}, \{\Theta_v\}, \Psi$ such that $f_{st}(t) \neq 0$. It follows there is at most $\frac{2n+2p}{q}$ probability for an honest Verifier to accept at (15) for any Prover and for any graph without Hamiltonian cycle over random choices of challenges $x_c, y_c, s, t$.

We consider a Prover passing verification equations such that $f_t(t) = 0$ for any edge due to unlucky choice of challenge $t$, or $f_{st}(t) = 0$ (due to choice of challenges $x_c, y_c, s, t$) to win the game. This probability estimate is sufficient for our purposes; a better estimate may be developed by considering options and strategies available to Prover.

We conclude there is at most $\frac{2p}{q}$ probability for such a Verifier to accept while choosing $(x_c, y_c)$, $\frac{n}{q}$ while choosing $s$, and $\frac{2}{q}n + \frac{n}{q}$ while choosing $t$, unless Prover is capable of taking logarithms in the group used. This probability is exponentially small in group order bitsize. □

**Lemma 4** (Of knowledge). *Protocol shown on Figure 1 has an extractor algorithm, and is of knowledge.*

Extractor is based on rewinding procedure: make Prover respond to two different challenges without choosing another set of initial random coins. All labels and flags are produced with an algorithm developed for Schnorr protocol [Sch89].

**Lemma 5** (Zero knowledge). *Protocol shown on Figure 1 has a simulator algorithm, and is honest verifier zero knowledge.*

Simulator algorithm is shown on Figure 2. Probability distribution for group elements $\{R_v\}$, $\{Q_e\}$, $\{E_e\}$, $D_0$ is flat due to $\{\Omega_v\}$, $\{\Delta_e\}$, $\{\Lambda_e\}$, $\Psi$ chosen independently with flat distribution.

# 4 Discussion

Algebraic properties of responses were shown to be useful for constructing protocols with low soundness error. Protocol introduced can be extended to exact travelling salesman problem [Luc94, Luc95].

# References


[Blu86] Manuel Blum. How to prove a theorem so no one else can claim it. In *International Congress of Mathematicians*, pages 444–451, 1986.

[CF01] Ran Canetti and Marc Fischlin. Universally composable commitments. In *CRYPTO*, pages 19–40, 2001.

[Luc94] Stefan Lucks. How to exploit the intractability of exact tsp for cryptography. In *FSE*, pages 298–304, 1994.

[Luc95] Stefan Lucks. How traveling salespersons prove their identity. In *IMA Conf.*, pages 142–149, 1995.

[MTZ01] Y. Minsky, A. Trachtenberg, and R. Zippel. Set reconciliation with nearly optimal communication complexity. In *International Symposium on Information Theory*, page 232, 2001. `http://citeseer.ist.psu.edu/minsky00set.html`.

[Oka92] Tatsuaki Okamoto. Provably secure and practical identification schemes and corresponding signature schemes. In *CRYPTO*, pages 31–53, 1992.

[Sch80] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27(4):701–717, 1980.

[Sch89] Claus-Peter Schnorr. Efficient identification and signatures for smart cards. In *CRYPTO*, pages 239–252, 1989.

1. Prover chooses $\{r_v\}$, $\{\delta_e\}$, $\{\alpha_v\}$, $\{\beta_e\}$, $\{\gamma_v\}$, $\{\pi_e\}$, produces and sends $\{W_v\}$, $\{U_e\}$, $\{R_v\}$, $\{Q_e\}$:

$$W_v = g^{w_v} h^{r_v} \qquad U_e = g^{u_e} h^{\delta_e} \qquad R_v = g^{\alpha_v} h^{\gamma_v} \qquad Q_e = g^{\beta_e} h^{\pi_e} \tag{5}$$

2. Verifier chooses and sends $(x_c, y_c)$
3. Prover chooses $\{\eta_k\}$, produces $\{m_k\}$ $\{M_k\}$, sends $\{M_k\}$:

$$\prod_{\vec{e}_{HT} \in \mathbb{E}(\Gamma)} (z + x_c(zw_H + \alpha_H) + y_c(zw_T + \alpha_T)) = \sum_{k=0}^{n} z^k m_k \quad M_k = g^{m_k} h^{\eta_k} \tag{6}$$

4. Verifier chooses and sends $s$
5. Prover chooses $\{\mu_i\}$, $\{\chi_e\}$, $\{\lambda_e\}$, produces $\{\Theta_v\}$, $\{\Omega_v\}$, $\{d_i\}$, $\{D_i\}$, $\{\tau_e\}$, $\{\rho_e\}$, $\{N_e\}$, $\{E_e\}$, sends $\{\Theta_v\}$, $\{\Omega_v\}$, $\{D_i\}$, $\{N_e\}$, $\{E_e\}$:

$$\Theta_v = sw_v + \alpha_v \qquad \Omega_v = sr_v + \gamma_v \tag{7}$$

$$\prod_{\vec{e}_{HT} \in \mathbb{E}(\Gamma)} (zs + (zu_e + \beta_e)(x_c\Theta_H + y_c\Theta_T)) = \sum_{i=0}^{n} z^i d_i \qquad D_i = g^{d_i} h^{\mu_i} \tag{8}$$

$$(zu_e + \beta_e)(z(u_e - 1) + \beta_e) = \tau_e z + \rho_e \qquad N_e = g^{\tau_e} h^{\chi_e} \qquad E_e = g^{\rho_e} h^{\lambda_e} \tag{9}$$

6. Verifier chooses and sends $t$
7. Prover produces and sends $\{\Phi_e\}$, $\{\Delta_e\}$, $\{\Lambda_e\}$, $\Psi$:

$$\Phi_e = tu_e + \beta_e \qquad \Delta_e = t\delta_e + \pi_e \tag{10}$$

$$\Lambda_e = t\chi_e + \lambda_e \qquad \Psi = t^n \sum_{k=0}^{n-1} \eta_k s^k + \sum_{i=0}^{n-1} \mu_i t^i \tag{11}$$

8. Verifier produces

$$F = \prod_{\vec{e}_{HT} \in \mathbb{E}(\Gamma)} (ts + \Phi_e(x_c\Theta_H + y_c\Theta_T)) - t^n s^n \prod_{j=0}^{p-1} (1 + x_c a^j + y_c a^{j+1}) \tag{12}$$

Verifier accepts if

$$g^{\Theta_v} h^{\Omega_v} W_v^{-s} = R_v \qquad g^{\Phi_e} h^{\Delta_e} U_e^{-t} = Q_e \tag{13}$$

$$g^{-\Phi_e(\Phi_e - t)} h^{-\Lambda_e} N_e^t E_e = 1 \tag{14}$$

$$g^{-F} h^{-\Psi} \left( \prod_{k=0}^{n-1} (M_k)^{s^k} \right)^{t^n} \prod_{i=0}^{n-1} (D_i)^{t^i} = 1 \tag{15}$$

Figure 1: An argument for Hamiltonicity

1. Verifier chooses at random from $\mathbb{F}_q$

$$\{\Theta_v\}, \{\Omega_v\}, \{\Phi_e\}, \{\Delta_e\}, \{\Lambda_e\}, \Psi$$

2. Verifier chooses random group elements

$$\{W_v\}, \{U_e\}, \{N_e\}, \{M_k\}_{k=0\ldots n}, \{D_i\}_{i=1\ldots n}$$

3. Verifier produces

$$R_v = g^{\Theta_v} h^{\Omega_v} W_v^{-s} \qquad Q_e = g^{\Phi_e} h^{\Delta_e} U_e^{-t} \tag{16}$$

$$E_e = g^{\Phi_e(\Phi_e - t)} h^{\Lambda_e} N_e^{-t} \tag{17}$$

$$D_0 = g^F h^\Psi \left( \prod_{k=0}^{n-1} (M_k)^{s^k} \right)^{-t^n} \prod_{i=1}^{n-1} (D_i)^{-t^i} \tag{18}$$

Figure 2: Simulator for argument for Hamiltonicity