A Proof for the Birch Swinnerton-Dyer Conjecture

Brian Haney¹

Original Paper July 12, 2020

Revised Draft March 11, 2021

Final Draft March 11, 2023

¹ Thank you to Mom, Brad, Broderick, Sam, Jagah, Pelumi, Zirimway, and Xi for always believing in me.

Table of Contents

Dedication	3
Abstract	
Introduction	
I. Birch and Swinnerton-Dyer Conjecture	
II. Proof	<u>9</u>
Conclusion	12
References	13
Appendix I. Objections and Responses	14

Dedication

All else being peripheral, this work is dedicated to the late and the great, Hal Finney. On March 19, 2013, Hal Finney created a topic in the Bitcoin Forum, Bitcoin and me (Hal Finney). A visionary for freedom and privacy, Finney will always be a keystone to Bitcoin's success. No matter the circumstances, Finney saw the good in life, he wrote:

"Today, I am essentially paralyzed. I am fed through a tube, and my breathing is assisted through another tube. I operate the computer using a commercial eyetracker system. It also has a speech synthesizer, so this is my voice now. I spend all day in my power wheelchair. I worked up an interface using an arduino so that I can adjust my wheelchair's position using my eyes.

It has been an adjustment, but my life is not too bad. I can still read, listen to music, and watch TV and movies. I recently discovered that I can even write code. It's very slow, probably 50 times slower than I was before. But I still love programming and it gives me goals."²

Finney's words reflect his pain and suffering after being terminally diagnosed with amyotrophic lateral sclerosis, which is commonly known as Lou Gehrig's disease. Still his strength was signified by his expressions of gratitude for the things he loved in life, including programming and the pursuit of noble goals. Proving BSD is to me a noble goal because it stands for the principle that impossible is nothing and that mathematics matters.

3

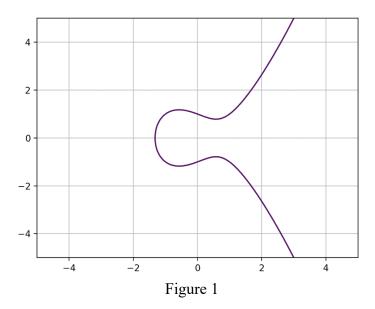
² Hal Finney, Bitcoin and me (Hal Finney) (March 19, 2013), https://bitcointalk.org/index.php?topic=155054.0.

Abstract

The Birch Swinnerton-Dyer Conjecture states that the number of rational points on an elliptic curve are infinite. This paper develops the logical formalism for a reinforcement learning system embedded with a quantum search algorithm. The formalism proves the rational points on high dimensional elliptical curves are infinite.

Introduction

The Birch Swinnerton-Dyer (BSD) Conjecture is a millennium prize problem, for which the Clay Mathematics Institute is offering a prize. The BSD problem relates to the nature of elliptic curves. In short, there does not exist a method of finding all points on elliptic curves. Elliptic curves are two-dimensional objects – essentially lop-sided oval shapes. Further, the BSD deals with the division of the finite and infinite of points on an elliptic curve.



Generally, elliptic curves contain rational numbers. Interestingly, a majority of scholarship surrounding the BSD deals with abelian groups. Abelian groups are numeric groups whose elements can be re-ordered, but still yield the same product. Elliptic curves are defined as a group over a finite field. With a suitable change of variables, every elliptic curve with real coefficients can be put in the standard form:

$$y^2 = x^3 + Ax + B$$

For some constants A and B. An elliptic curve is a smooth projective curve of genus 1 with a distinguished point.

Specifically, an elliptic curve is a projective curve of genus 1 with a distinguished point. The projective plane is set to $\mathbb{P}^2(k)$ for all nonzero triples (x, y, z) in k^3 modulo the equivalence relation $(x, y, z) \sim (x, x, x, y, x, z)$. The projective point (x : y : z) is the equivalence class for (x, y, z). Points of the form (x : y : 1) are called affine points. They form an affine plane $\mathbb{A}^2(k)$ embedded $\mathbb{P}^2(k)$. Points of the form (x : y : 0) are called points at infinity. These consist of the points (x : 1 : 0) and the point (1 : 0 : 0), which form the line at infinity: this is a copy of $\mathbb{P}^1(k)$ embedded in $\mathbb{P}^2(k)$.

A plane projective curve C_f / k is a homogenous polynomial f(x, y, z) with coefficients in k^1 . The degree of C_f is the degree of f(x, y, z). For any field K containing k, the $K-rational\ points$ of C_f form the set:

$$C_f(K) = \{(x : y : z) \in \mathbb{P}^2(k) \mid f(x, y, z) = 0\}$$

A point $P \in C_f(K)$ is singular if $\frac{\partial f}{\partial x}$, $\frac{\partial f}{\partial y}$, $\frac{\partial f}{\partial z}$ all vanish at P. C_f is nonsingular if there are no singular points $C_f(\bar{k})$.

Over \mathbb{C} , an irreducible projective curve is a connected compact manifold. The genus can be defined algebraically over any field. The Newton polytope of a polynomial $f(x,y) = \sum a_{ij}x^iy^j$ is the convex hull of the set $\{(i,j): a_{ij} \neq 0\}$ in \mathbb{R}^2 . One way to compute the genus for an irreducible curve defined by an affine equation f(x,y) = 0 is to count the integer lattice points in the interior for its Newton polytope:

$$y^2 = x^3 + Ax + B$$

The Narrow Weierstrass equation $y^2 = x^3 + Ax + B$ defines a projective genus 1 curve over k with the rational point (0:1:0). The General Weierstrass equation:

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

works over any field.

Zero is the point at infinity. Three points on a line sum to zero. P + Q + R = 0. The set E(k) is an abelian group. The point (0:1:0) at infinity is the identity element 0. The inverse of P = (x:y:z) is the point at -P = (x:-y:z). Commutativity is: P + Q = Q + P. Associativity is: P + (Q + R) = (P + Q) + R.

Computing P + Q = R is algebraic. The coordinates for R are rational functions for the coordinates of P and Q. By adding a point to itself iteratively, compute 2P = P + P, 3P = P + P + P, and in general, $nP = P + \cdots + P$ for any positive n. Further, define 0P = P and (-n)P = -nP. Thus, scalar multiplication by any integer n is computable.

When $k = \mathbb{C}$ the group operation of $E(\mathbb{C}) \simeq \mathbb{C} / L$ is complex number addition, modulo the lattice L. The group $E(\mathbb{Q})$ may be finite or infinite, but in every case, it is finitely generated.

The group $E(\mathbb{Q})$ is a finitely generated abelian group. Thus:

$$E(\mathbb{Q}) \simeq \mathbb{T} \oplus \mathbb{Z}^r$$

Where the torsion subgroup T is a finite abelian group corresponding to the elements of $E(\mathbb{Q})$ with finite order, and r is the rank of $E(\mathbb{Q})$. The torsion subgroup T of $E(\mathbb{Q})$ is well understood. The torsion subgroup of $E(\mathbb{Q})$ is isomorphic to one of the following:

$$\mathbb{Z} / n\mathbb{Z}$$
 or $\mathbb{Z} / 2\mathbb{Z} \oplus \mathbb{Z} / 2m\mathbb{Z}$,

Where $n \in \{1,2,3,4,5,6,7,8,9,10,12\}$ and $m \in \{1,2,3,4\}$.

If $C(\mathbb{Q})$ is non-empty, then C is parametrized by rational functions and there are infinitely many rational points. If a non-singular projective model C has a rational point, then $C(\mathbb{Q})$ has a natural structure as an abelian group with this point as the identity element, C and elliptic curve over \mathbb{Q} . This group is finitely generated. If C an elliptic curve over \mathbb{Q} , then

$$C(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus C(\mathbb{Q})^{tors}$$

For some integer $r \ge 0$, where $C(\mathbb{Q})^{tors}$ is a finite abelian group. The integer r is called an algebraic rank of C. It is zero only if $C(\mathbb{Q})$ is finite.

I. Birch and Swinnerton-Dyer Conjecture

The case of cubic equations in two-variable is the first case where, there is no known method to find all the rational solutions – thus BSD. If the Birch and Swinnerton-Dyer Conjecture was true, then there would be a method to find all rational solutions to a cubic equation in two variables, and, to determine whether it has infinitely many rational solutions.

Let E be an elliptic curve, let r be its rank, and let N_p denote the number of points E(mod p). Then

$$\prod_{p \le X} \frac{N_p}{p} \sim c \cdot (\log X)^r$$

Birch and Swinnerton-Dyer also provided an explicit expression for c in terms of E; this is called the strong form of the conjecture. Let E be an elliptic curve, let r be its rank, and let N_p denote the number of points $E \pmod{p}$. Set, $a_p = p + 1 - N_p$, and define the incomplete L-function of E by:

$$L(E,s) = \prod_{p \nmid 2\Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

Conjecture (Birch and Swinnerton-Dyer) The Taylor Expansion of $L^*(C, s)$ at s = 1 has the form

$$L(C,s) = c(s-1)^r + higher order terms$$

With

$$c \neq 0$$
 and $r = rank(C(\mathbb{Q}))$.

In particular, this conjecture asserts that

$$L(C,1)=0 \Leftrightarrow C(\mathbb{Q})$$

is infinite. [16]

II. Proof

A proof is an inferential argument for a mathematical statement, showing that the stated assumptions logically guarantee the conclusion. The model for proving the BSD is conceptually straightforward. A deep reinforcement learning agent [14] uses a quantum search algorithm [13] to identify all point on the elliptic curve over the field \mathbb{Q} . All classical fields $C(\mathbb{Q})$ are fields of limited dimensionality, reduced from a quantum field $Q(\mathbb{Q})$. [17, 22]

The offered proof proves the number of rational points on a finite elliptic curve is infinite. In other words, the L-function's order is equivalent to the rank $C(\mathbb{Q})$. The proof is described as a series of three transformations.

First, if a non-singular projective model C has a rational point, then $C(\mathbb{Q})$ has a natural structure as an abelian group with this point as the identity element.

$$Q \in \mathbb{Q}$$

The Quantum Ising Model is a method for statistical mechanics, where variables are binary and the relationship between variables is represented by couplings. [19] The Ising Model uses a Quantum Energy Measurement (QEM) function is to describe the total amount of energy in a quantum system.

$$Q_s(s) = -\frac{1}{2} \sum_i \Delta(s) \sigma_i^x + \varepsilon(s) \Big(-\sum_i h_i \sigma_i^z + \sum_{i < j} J_{ij} \sigma_i^z \sigma_j^z \Big).$$

The input for the QEM function is the state of the system. In other words, the QEM returns the energy measurement for any particular state.

$$-\frac{1}{2}\sum_{i}\Delta(s)\sigma_{i}^{x}$$
,

And, the output is the energy measurement of the system.

$$\varepsilon(s) \Big(- \sum_i h_i \sigma_i^z + \sum_{i < j} J_{ij} \sigma_i^z \sigma_j^z \Big),$$

Then,

$$L(C,1) = 0 \Leftrightarrow C(\mathbb{O})$$

$$C(\mathbb{Q}) \to \mathbb{Z}^r \oplus C(\mathbb{Q})^{tors}$$

$$L(C,1)=0 \Leftrightarrow \mathbb{Z}^r \oplus C(\mathbb{Q})^{tors}$$

Where,

$$L(C,1) = 0 \Leftrightarrow \mathbb{Z}^r \oplus \mathcal{C}(\mathbb{Q})^{tors} \to L(C,1) = 0 \Leftrightarrow \mathcal{C}(\mathbb{Q})$$

The energy description Q is given to transform the state space for field $C(\mathbb{Q})$.

$$Q = \sum_{i=1}^{N} [\varepsilon_i \sigma_i^Z + \Delta_i \sigma_i^X] + \sum_{i=1}^{N} \sum_{j>i}^{N} J_{ij} \sigma_i^Z \sigma_j^Z.$$

Where $C(\mathbb{Q}) \to Q(\mathbb{Q})$.

The quantum field $Q(\mathbb{Q})$ is a quantum subfield for classical fields.

$$Q(\mathbb{Q}) \to \mathcal{C}(\mathbb{Q}) \to \mathbb{Z}^r \oplus \mathcal{C}(\mathbb{Q})^{tors}$$

Second, deep reinforcement learning is a new type of machine learning resulting from the technical convergence of two more mature machine learning methods, deep learning and reinforcement learning. Deep Q-Networks (DQNs) are deep neural networks embedded in the reinforcement learning architecture, representing these two systems' convergence. The DQN algorithm combines Q-learning with a neural network to maximize an agent's reward.

The reward acts as a feedback mechanism, allowing the agent to learn independent of human training. The rewards are used to update the agent's knowledge over time, so it learns to take actions returning the highest rewards. [7, 9] For each time step, the reward is a number,

$$R_t \in \mathbb{R}$$
,

which is associated with a corresponding action.

$$a^* = arg \max_{a} ER(s|a).$$

The value function is used to compute the value of a given state according to a defined policy. The value function V^{π} is equal to the expected sum of the discounted rewards for executing policy π . [23]

$$V^{\pi}(s) = \mathbb{E}[R(s_0) + R(s_1) + \cdots | s_0 = s, \pi(s)].$$

The DQN algorithm's Bellman Equation is defined. [15]

$$Q^*(s,a) = E_{s'\sim\varepsilon} \left[r + \max_{a'} Q^*(s',a') | s, a \right].$$

Thus, a neural network is a state-action value function, allowing for more efficient programming and model development. [10]

$$Q(s, a; \emptyset) \rightarrow (s, a).$$

For each state in the agent's environment, the field $Q(\mathbb{Q})$, the agent applies the Quantum Search Algorithm, to search the field for all points. The Quantum Search Algorithm (QSA) searches the

quantum field $Q(\mathbb{Q})$ by algorithmic method. The algorithm begins where all rational points (\mathbb{Q}) are in search space with an equal superposition $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x} |x\rangle$. Where O_p is a quantum oracle, apply O_p to $|\psi\rangle$.

$$O_p: |Q, a\rangle \to |Q, P(Q) \oplus a\rangle,$$

$$for all Q \in \mathbb{Q}$$

Flip the sign of all basis vectors that represent a solution.

$$\begin{split} O|\psi\rangle &\to Q \oplus -Q \\ O: Q_{i}|\psi_{O}\rangle - Q_{i}|\psi_{O}\rangle &\to Q_{i+1}|\psi_{O}\rangle - Q_{i+1}|\psi_{O}\rangle \end{split}$$

Perform an inversion about the average, a transformation that maps every amplitude $A - \delta$ to $A + \delta$, where A is the average of the amplitudes. [18]

$$\sum_{i=0}^{N-1} (a_i) |\psi\rangle \to \sum_{i=0}^{N-1} (2A - a_i) |\psi\rangle$$

Where,

$$N = \infty$$

The agent is rewarded for each point it finds, taking action associated with the collection of rational points in the quantum state space modeling the classical elliptic curve $C(\mathbb{Q})$ in high dimensionality.

Third, the L-Function is a method on the complex plane. Where, the complex plane is a quantum field, which underlies a classical field.

$$L(Q,1) = 0 \Leftrightarrow Q(\mathbb{Q})$$
$$Q(\mathbb{Q}) = 0 \Leftrightarrow Q(\mathbb{Q})$$
$$Q(\mathbb{Q}) = C(\mathbb{Q})|\psi\rangle$$

Thus,

$$L(Q,1) = 0 \Leftrightarrow Q(\mathbb{Q}) = \infty$$
 and
$$L(C,1) = 0 \Leftrightarrow C(\mathbb{Q}) = \infty$$

Conclusion

In sum, this paper proves the Birch Swinnerton-Dyer Conjecture. The proof provides a logical support that the rational points on high dimensional elliptical curves are infinite.

References

- [1] P.L. Chebyshev, Démonstration élémentaire d'une proposition Générale de la théorie des probabilities, 33 J. Reine Angew. Math. 259 (1846).
- [2] Oliver Wendell Holmes, Jr., The Path of the Law, 10 HARV. L. REV. 457 (1897).
- [3] Константин Эдуардович Цколковский, Исследование Мировых пространств реактивными приборами (1903).
- [4] Albert Einstein, Über die von der molekularkinetischen Theorie der Wärme geforderte Bewegung von in ruhenden Flüssigkeiten suspendierten Teilchen, 322 Annalen der Physik 549 (1905).
- [5] Otto Jespersen, Language: Its Nature, Development, and Origin (1922).
- [6] M. Fré chet, Mé thode des fonctions arbitraires. Thé orie des événements en châine dans le cas d'un nombre fini d'e tats possibles. Paris, Gauthier-Villars (1938).
- [6i] Richard P. Feynman, The Principle of Least Action in Quantum Mechanics (May 1942) (Ph.D. dissertation, Princeton University).
- [6f] R.P. Feynman, Space-Time Approach to Non-Relativistic Quantum Mechanics, 20, REVS. MOD. PHYS. 367, 367 (1948).
- [7] C.E. Shannon, A Mathematical Theory of Communication, Bell Systems Technical Journal (1948).
- [8] J. Coates, A. Wiles, On the Conjecture of Birch and Swinnerton-Dyer (1977).
- [9] Leslie Pack Kaelbling, Learning in Embedded Systems (1990).
- [10] PAUL JOHN WERBOS, THE ROOTS OF BACKPROPAGATION FROM ORDERED DERIVATIVES TO NEURAL NETWORKS AND POLITICAL FORECASTING (1994).
- [11] Andrew John Wiles, Modular elliptic curves and Fermat's Last Theorem (1995).
- [12] Peter W. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer 20 (1995).
- [13] Lov K. Grover, Quantum Computers can Search Arbitrarily Large Databases by a Single Query, Vol. 79 Physical Review Letters No. 23, 4709 (1997).
- [14] Leslie Pack Kaelbling, et al., Reinforcement Learning: A Survey, J. of Artificial Intelligence Research (1996).
- [15] Jeanne C. Fromer, Learning Optimal Discourse Strategies in a Spoken Dialogue System, MIT (1998).
- [16] Andrew Wiles, The Birch and Swinnerton-Dyer Conjecture (2006).
- [17] Margaret Cuonzo, Paradox, MIT Press (2014).
- [18] ELEANOR RIEFFEL, WOLFGANG POLAK, QUANTUM COMPUTING (2014).
- [19] Maria Schuld, et al., An introduction to quantum machine learning (2014).
- [20] MYKEL J. KOCHENDERFER, DECISION MAKING UNDER UNCERTAINTY (2015).
- [21] Brent Johnson, An Introduction to the Birch and Swinnerton-Dyer Conjecture, Rose-Hulman Undergraduate Mathematics Journal (2015).
- [22] R. SHANKAR, QUANTUM FIELD THEORY AND CONDENSED MATTER (2017).
- [23] Serena Yeung, et al., Learning to Learn from Noisy Web Videos (2017).

Appendix I. Objections and Responses

Author's Note

Over the years, I have solicited objections and critique to the proof originally proposed in July of the year 2020. I amended the paper based on certain objections in the year 2021. Over time, it became more and more difficult to find constructive criticism, so I distilled the best objections to three main arguments, developed them, and authored appropriate responses.

Objection 1

The proof is merely a combination of concepts. The proof is a combination of various mathematical ideas and theories, including quantum mechanics, deep reinforcement learning, and dynamic programming, but it does not seem to have a direct connection to the Birch and Swinnerton-Dyer Conjecture. The quantum search algorithm and agent are unclear and ambiguous. Specifically, there is no express expression for convergence to an unbounded number of points. Particularly this mathematics is unclear:

$$L(Q,1) = 0 \Leftrightarrow Q(\mathbb{Q})$$

$$Q(\mathbb{Q}) = 0 \Leftrightarrow Q(\mathbb{Q})$$

$$Q(\mathbb{Q}) = C(\mathbb{Q})|\psi\rangle$$

Perhaps, an AI wrote the paper with a bunch of related number theory papers as the input.

Response 1

The proof is not merely a combination of concepts. The proof relies on three essential concepts to mathematically prove the Birch Swinnerton-Dyer Conjecture. While these three concepts are not typically foundational in mainstream cryptography, it is for that very reason that they enable break through crypto mechanics for fostering applied innovations and mathematical theories.

Concept 1. The non-singular projective model C has a rational point, then $C(\mathbb{Q})$ has a natural structure as an abelian group, which projects on the quantum plane: $Q \in \mathbb{Q}$.

Concept 2. Second, deep reinforcement learning is a new type of machine learning resulting from the technical convergence of two more mature machine learning methods, deep learning, and reinforcement learning.

Concept 3. Third, the L-Function is a method on the complex plane. Where, the complex plane is a quantum field, which underlies a classical field.

Application to Birch Swinnerton-Dyer Conjecture.

$$L(Q,1) = 0 \Leftrightarrow Q(\mathbb{Q})$$

$$Q(\mathbb{Q}) = 0 \Leftrightarrow Q(\mathbb{Q})$$

$$Q(\mathbb{Q}) = C(\mathbb{Q})|\psi\rangle$$

Leads to

$$L(Q,1) = 0 \Leftrightarrow Q(\mathbb{Q}) = \infty$$

and

$$L(C,1) = 0 \Leftrightarrow C(\mathbb{Q}) = \infty$$

because quantum neural networks,

 $\begin{array}{cccc} x_i & \oplus & x_{i+1} \oplus x_l \\ x_j & \oplus & x_{j+1} \oplus x_m \\ x_k & \oplus & x_{k+1} \oplus \end{array} \quad x_n$

And

the dualling quantum neural networks for variables t_n and x_n – which may be associated to finite points on an elliptic curve. Then, the following equations consolidate the structure to three subquantum parts consisting of functions q, a, and b. [6i] [6f]

$$F[q(x,t),a(x,t),b(x,t)] = \iiint_{0}^{\infty} q(x,t),a(x,t),b(x,t)\Delta q \Delta a \Delta b$$

$$F[q(x,t),a(x,t),b(x,t)] = \iiint_{-\infty}^{0} q(x,t),a(x,t),b(x,t)\Delta q \Delta a \Delta b$$

The second equation is the transposed matrix for the first equation, which may be implemented as far as practical depending on the specific security structure. The next equation consolidates variables t_n and x_n according to three functional elements, α , β , and γ .

$$s^{\alpha} = \int x \rangle \langle t : s^{\beta} = \int x \rangle \langle t : s^{\gamma} = \int x \rangle \langle t$$

Finally, the math forms singularity.

$$s^* = \int i^3$$

Conclusion. Therefore, the proof combines three keystone concepts with specific application to the Birch Swinnerton-Dyer Conjecture for the purpose of proving the conjecture via the key principle, rational points on high dimensional elliptical curves are infinite.

Objection 2

The proof lacks clarity and rigor. The proof is not written in a clear and rigorous manner, and it is difficult to understand the steps and their relationship to the Birch and Swinnerton-Dyer Conjecture.

Response 2

The proof does not lack clarity nor rigor. The proof is broken into three essential claims, the three claims form the ultimate proof with mathematically meticulous detail.

Claim 1. The non-singular projective model C has a rational point, then $C(\mathbb{Q})$ has a natural structure as an abelian group, which projects on the quantum plane: $Q \in \mathbb{Q}$.

Claim 2. Second, deep reinforcement learning is a new type of machine learning resulting from the technical convergence of two more mature machine learning methods, deep learning, and reinforcement learning. The deep reinforcement learning algorithm is an agent for optimality and this applies to the quantum search problem.

Claim 3. Third, the L-Function is a method on the complex plane. Where, the complex plane is a quantum field, which underlies a classical field. In particular, the Birch and Swinnerton-Dyer conjecture asserts that:

$$L(C,1)=0 \Leftrightarrow C(\mathbb{Q})$$

is infinite.

Proving this in reliance on the parsimony principle demands the following logical conclusion.

$$L(C,1) = 0 \Leftrightarrow C(\mathbb{O}) = \infty$$

The clarity of the above short form is supported by the rigor of mathematics developed throughout this paper. Therefore, the proof is both clear and rigorous to someone of ordinary skill in the technical art.

Objection 3

The proof fails to validate the quantum field architecture derived from the classical system on which it departs the modern theories of cryptography. Moreover, the proof merely assumes the passivity of classical systems across the quantum plane via transformational math.

Response 3

The proof validates the quantum field architecture derived from the classical system via three singularizing transformations to prove the number of rational points on any given elliptical curve is infinite.

Transformation 1. The classical field $C(\mathbb{Q})$ projects on the quantum plane: $Q \in \mathbb{Q}$.

Transformation 2. The deep reinforcement learning algorithm optimizes the search function in both classical and quantum systems.

Transformation 3. Every classical field in a complex plane rest on a quantum field. This is a fundamental property of the physical universe, digital information included. Therefore, the proof validates the quantum field architecture derived from the classical system.