QUANTUM RANDOM WALK APPLICATIONS

H. Tonchev

Institute for Nuclear Research and Nuclear Energy, BAS

Institute of Solid State Physics, BAS

22.12.2022 г.

QUANTUM RANDOM WALKS

Quantum analogue of random walk

Quantum random walk is a quantum analogue of classical random walk. There is a particle that makes a walk on the graph as in the classical case. However, in contrast with classical walk, the state of quantum walk can be a superposition of states. During the quantum walk interferences occur due to exitance of different ways to reach particular position. It can be constructive that increase probability to be at this particular position and destructive that decreases this probability.

After measurement, the position of quantum walker collapses and it can be found at only one position. If during each step of the quantum walk measurement occurs quantum walk collapses to classical.

DISCRETE TIME QUANTUM RANDOM WALK

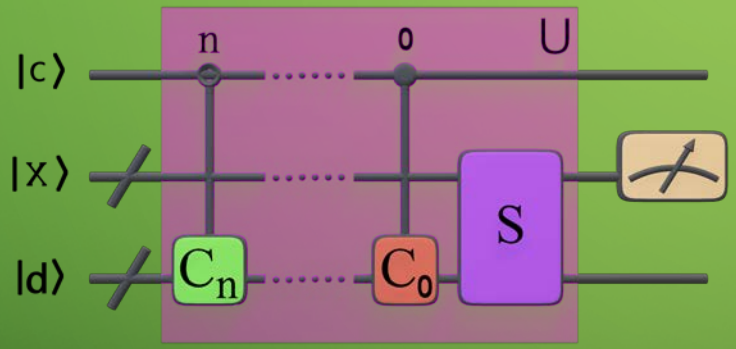
Irregular Graph

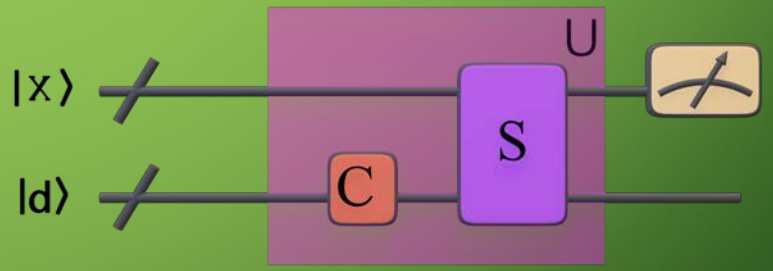
c – control register

x – node register

d – edge register

Regular Graph





In case of regular graph the whole register of the system is:

$$|\psi\rangle = |x\rangle \otimes |d\rangle = |x, d\rangle$$

where x is the state of the node register and d state of the register of the edges (coin register)

Quantum random walk step is achieved by making quantum random walk iteration. To make w steps means to apply w times DTQRW iteration on initial register.

$$U|\psi_0\rangle = |\psi_1\rangle$$

$$|\psi_0\rangle \xrightarrow{U} |\psi_1\rangle \xrightarrow{U} |\psi_2\rangle \xrightarrow{U} \dots \xrightarrow{U} |\psi_W\rangle$$

Quantum walk iteration (U) consists of the following steps:

- Coin operator (C) is applied on coin state
- Shift operator (S) is applied after the coin.

Depending on the coin register state, Shift operator moves walker to the next position in the node register.

$$U = S.\mathfrak{C}$$

Coin Operator

Coin operator C is applied on coin space at each step:

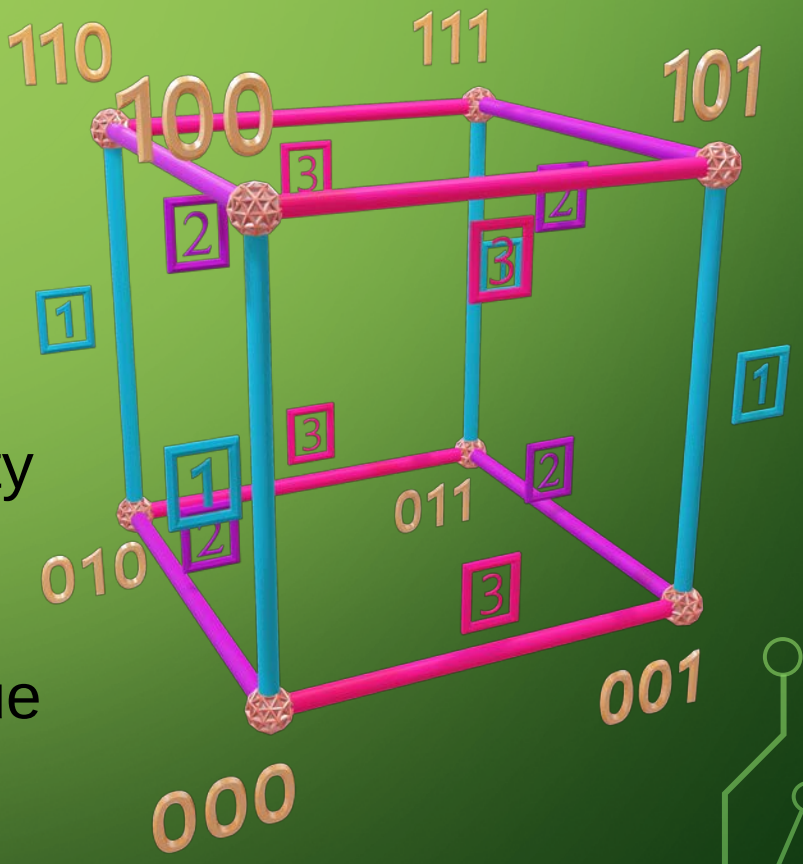
$$\mathfrak{C} = I \otimes C$$

At this step node register remains unchanged. Coin operator changes the state of the coin register (determines the graph's edges). This state defines the probability to go from the current node to each of the nodes connected by an edge. Coin register can be in superposition of states, because it is a quantum state.

During the evolution the coin space can go to different superposition of states.

Coin representation is complex unitary matrix, with dimension equal to the number of edges. Shift operator changes the walker position on the graph depending on the state of the coin.

$$C = \begin{pmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,m} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m,1} & c_{m,2} & \cdots & c_{m,m} \end{pmatrix}$$



At this figure the probability a walker to go trough edges with the same color corresponds to the same value of the edge register

Shift Operator

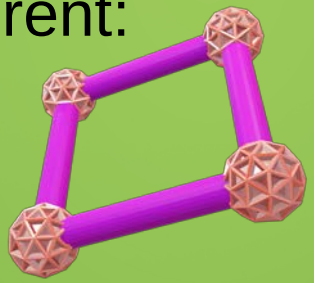
Shift operator is applied at each iteration.

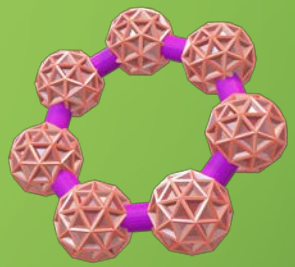
$$S = \sum_{\mathrm{d}=0}^{d_{max}-1} \sum_{\mathrm{x}=x_{min}}^{x_{max}} |x \oplus e_d, d\rangle\langle \mathrm{x}, \mathrm{d}|$$

where d_{max} is the coin register dimension, interval $\{x_{min}, x_{max}\}$ consists of all possible states of node register and e_d corresponds to the edge vector d that connects one state of node register to another state.

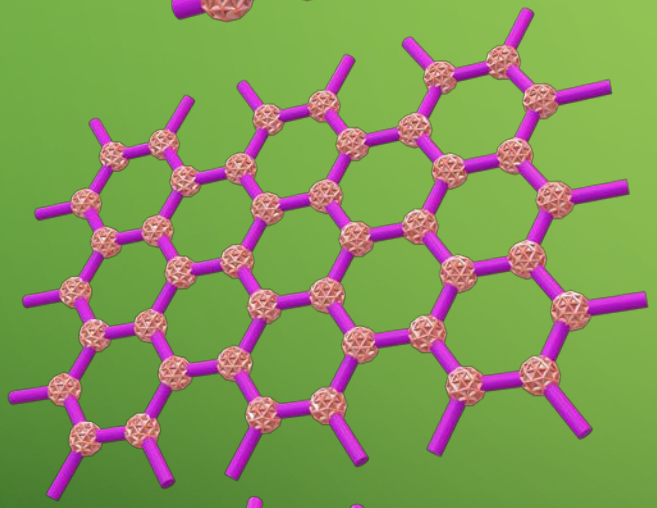
In this way, depending on the coin register state, Shift operator moves walker by changing the state of node register to the next position or superposition of positions.

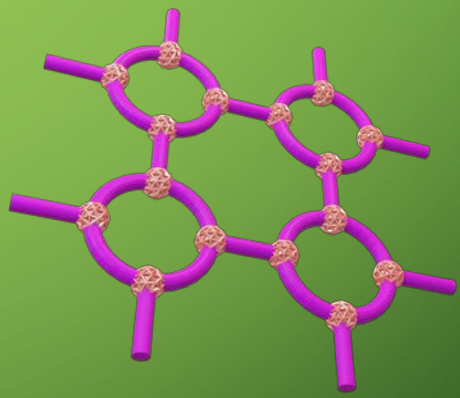
Shift operator S defines the topology of the walked object. In the next examples coin operators can be the same but shift operator is different:



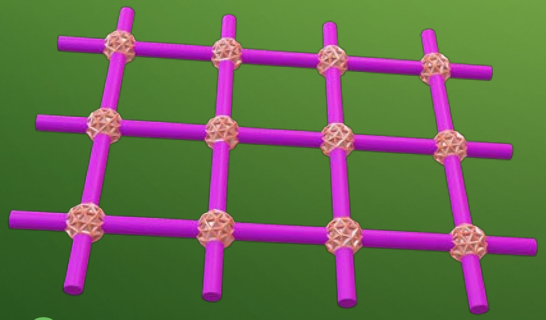


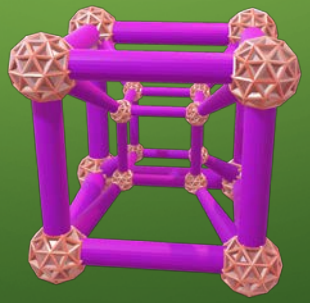
Coin Register Size is 2

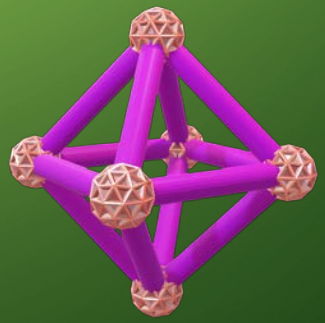




Coin Register Size is 3







Coin Register Size is 4

After the required number of steps is made node register is measured. During the measurement quantum superposition collapses to classical state.

If measurement is made at each walk iteration step, quantum walk collapses to classical.

Last time the following examples of DTQRW on different structures was shown: Line, Circle, Segment, Square grid and Hypercube.

DISCRETE TIME QRW MODIFICATIONS

Types of discrete time QRW

Different modifications of quantum random walk were constructed in order to use QRW to tackle a different problems. Examples for some modifications are:

Directed QRW – It is analogous to classical random walk on directed graph. Nodes are connected by the one directional edges, and cant be traversed in opposite direction. Self-loops are also allowed. This modification is used for 2-sat satisfiability problems.

Lazy (or Lackadaisical) QRW – By analogy to classical lazy walk, it allows walker to not only move in direction but also stay in place. It can be used to make quantum random walk search in simplex with success probability equal to 1.

Alternate quantum walk – Uses more than one shift operator to traverse a higher dimensional grid by QW on lines. Each line has different direction. This modification is used in quantum cryptography.

Multi-walker QRW – Uses more than one walker that traverse the graph. Such walker can also be entangled. By properly choosing the entanglement a bosonic (bosonic random walk) or fermionic (fermionic random walk) statistics can be obtained. This modification is also used in studying graph isomorphism problem.

Multi-coin QRW – At each step it uses the same shift operator but different coin. This walk is used to generate different probability amplitude distributions and phase distributions. This makes this modification ideal for initializing the initial state of quantum computer or as random number generator with desired distribution.

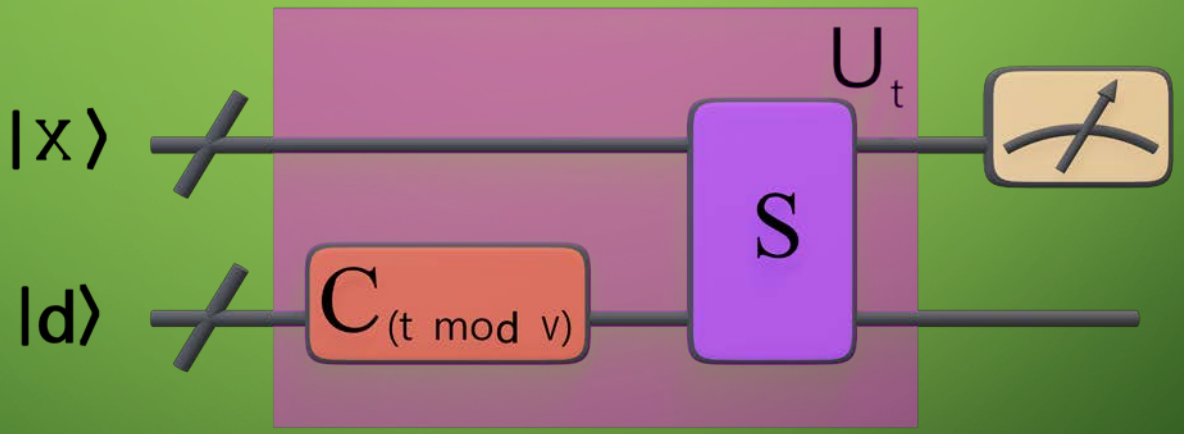
Multi-coin Quantum Random Walk

This modification of QRW have use standard shift operator for this topology. However at each step a different coin is used. If there are “v” coins at step t, the coin is:

$$C_t = C_{t \bmod v}$$

$$U_t = S.(I \otimes C_t)$$

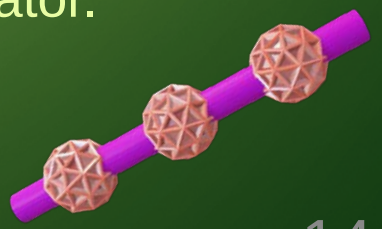
$$|\psi_0\rangle \xrightarrow{U_1} |\psi_1\rangle \xrightarrow{U_2} |\psi_2\rangle \xrightarrow{U_3} \dots \xrightarrow{U_n} |\psi_n\rangle$$



In case of line for coins can be used any 2D operator.

$$C_{2k+1} = C_1$$

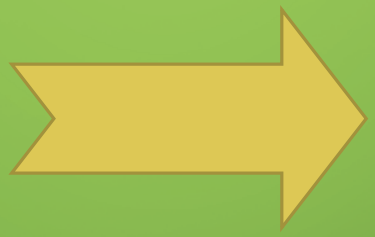
$$C_{2k} = C_0$$



Example for two coined walk on line with two coins is shown bellow. Coin register is in state $(|0\rangle + |1\rangle)/\sqrt{2}$ and both coins are Hadamard and Balanced:

$C=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$

$C=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & i\\ i & 1\end{bmatrix}$



Important case is when coin is of the following type:

$$C_t=\frac{1}{\sqrt{2}}\begin{bmatrix}cos(f_1(t)) & e^{If_2(t)}sin(f_1(t))\\ e^{-If_2(t)}sin(f_1(t)) & -cos(f_1(t))\end{bmatrix}$$

Examples when a one coin is used, and it dependent of the iteration is shown below. Initial state of coin register is $(|0\rangle + |1\rangle)/\sqrt{2}$

$$C_t = \frac{1}{\sqrt{2}} \begin{bmatrix} cos(2\pi \frac{t}{36}) & sin(2\pi \frac{t}{36}) \\ sin(2\pi \frac{t}{36}) & cos(2\pi \frac{t}{36}) \end{bmatrix}$$

$$C_t = \frac{1}{\sqrt{2}} \begin{bmatrix} cos(2\pi \frac{t}{36}) & e^{2\pi i \frac{t}{22}} sin(2\pi \frac{t}{36}) \\ e^{-2\pi i \frac{t}{22}} sin(2\pi \frac{t}{36}) & cos(2\pi \frac{t}{36}) \end{bmatrix}$$

When on odd position is used the one coin and on even the other:

There is also modifications where coin depends also of the position:

$$C_{t,n} = \frac{1}{\sqrt{2}} \begin{bmatrix} cos(f(t,n)) & e^{If_2(t)} sin(f(t,n))) \\ e^{-If_2(t)} sin(f(t))) & -cos(f(t,n))) \end{bmatrix}$$

APPLICATIONS OF QUANTUM WALKS

Programable quantum computer

Quantum walks on line can be used to obtain an arbitrary superposition of states in the quantum register by performing a quantum walk with coins with appropriate parameters. This framework can also be used to make arbitrary qudit state.

Any single and multiqubit operation applied on quantum register can be simulated by discrete time quantum walk. At the beginning of the walk the state is the same as the one on which qubit operation should be applied. Walk changes this state to an one which would result if the corresponding single or multiqubit operator is applied. This model can be used as alternative of circuit model, and also for building quantum processor based on quantum walk. In this way, both quantum circuit and DTQRW models are computationally equivalent to quantum Turing Machine.

Quantum walk can be implemented efficiently in various quantum systems like ion trap, quantum dots array, superconducting circuit and nitrogen-vacancy centers in diamond. This property makes the quantum walk very perspective method for making universal quantum computer.

Algorithms

Discrete time Quantum random walk search (DTQRWS) – Quantum algorithm designed to search in unordered data base structured as graph (graph can be arbitrary connected). It uses oracle and two coins. First coin for the walk, and second one to mark the solutions. The algorithm is probabilistic and quadratically faster ($O(\sqrt{N})$ oracle queries) than its classical counterpart ($O(N)$). The original algorithm has probability to find solution ½, however for given topologies some modifications exists where probability to find solution can be increased. For example, after modifications for hypercube probability reaches approximately $1 - O(1/n)$.

Evaluating Boolean Formula algorithm – uses combination of quantum phase estimation and QRWS algorithms to a weighted tree. Algorithm is probabilistic with probability to find solution approximately 75% and requires $O(\sqrt{N})$ oracle queries.

Element Distinctness algorithm – If there is a list of elements written as binary numbers, this probabilistic quantum algorithm (approximately $1 - O(N^{1/(k+1)})$ checks if all elements are different, or there are repetitive elements. In the expression N is the number of elements and k of them have repetition. This task is solved by transforming the list into a graph, and DTQRWS is used. Element Distinctness solves this task for $\sim O(N^{3/4})$ oracle queries and its classical counterpart for $\sim O(N)$.

There are many other quantum algorithms based on quantum walks, examples of such algorithms are:

- Quantum algorithms for finding subgraphs in graph. Examples are quantum algorithms for finding a triangle and star subgraphs in graph
- Quantum algorithm for graph isomorphism (check if two graphs are isomorphic)
- Quantum Simulated Annealing (it solves combinatorial problems)

Quantum simulations in Physics

Fermionic and bosonic quantum field theories can be derived by using quantum random walk and quantum cellular automata.

Bose-Einstein model of dark matter with three particle repulsive interaction. According to this model few-particle correlations imply a first-order phase transition. This will lead to dark matter with properties of ideal gas with temperature determined by the quantum fluctuations. Oscillations between bound and unbound states of three particles are studied by classical and quantum walks.

QW is used to simulate Lattice Boltzmann methods model in computational fluid dynamics.

Design of new lasers and materials in condensed matter physics by Floquet Engineering with quantum walks.

QW can be used to entangle particles (like photons).

Also, continuous walks are used for finding the ground state of spin glasses.

QS in Mathematics

Quantum walks are used for simulations of Non-Commutative Geometry.

There is quantum Heuristic algorithm checking if the value satisfies k-sat equation. It is based on continuous time quantum walk on Hypercube. An additional potential barrier is added in the graph that increases tunneling and scattering trough the cube. Algorithm uses not only operator based quantum computations but also uses multiple measurements during the implementation of the algorithm. Probability to success is 2/3 and number of iterations is equal to the number of the Boolean variables.

2-sat satisfiability problems can also be checked with directional quantum random walks.

Optimization problems can be solved efficiently by using quantum walk. Example for such problems are:

Traveling Salesman – to visit all points of graph just once with minimal possible total path.

Vehicle routing problem (generalized case of Traveling salesman) – Finds optimal set of routes for M vehicles to traverse in order to deliver to L customers.

QS in Biology and Molecular Biology

A taxon is group of one or more populations of organisms that a grouped based on shared characteristic. Taxons have taxonomy rank – lower rank taxa are ordered into higher order one. Example of such taxa are class, order, family, genus, and species. A probability tensor that give which multi-taxa can evolve from one taxon are made by using multi-walker quantum walk with entangled coins applied on tree graphs. Interferences between walkers during the walk gives the probability a such multi-taxon to exist.

Proteins binds to a specific targets (a given sequence of DNA nucleotides). A quantum walks with coin position entanglement is used for simulation of the electron in pi orbital. A binding process that forms can form a pi-pi connection (the two orbitals overlaps side by side by valence bound theory) with a dimer in the sequence. Such model gives better results than diffusion models that have a errors in order of magnitude.

Simulation of other systems exists, including protein folding and photosynthesis.

Machine Learning

The unsupervised machine learning task of node clustering can be made more efficiently by QRW.

Training classical Neural Network – Quantum walks can be used for faster determination of node weights of classical NN. Quantum walks also can speedup backtracking in ML algorithm.

Quantum graph neural network – a quantum analogue of classical graph neural network. Machine learning is based on learning the parameters of the coins used during the walk. Different variants of such NN were studied, including:

- Convolutional graph neural network
- Recurrent graph Neural Network

Recently, quantum walks are studied for application in language processing.

Cryptography

The Public Key Cryptographic Protocol for key distribution QKD uses quantum random walk on circle for encryption.

Alice chose one pure state in computational basis. Next she uses this state as initial state of node register for quantum walk on circle with chosen by her coin initial state. Walk coin is rotation matrix with phase multipliers in the front of each matrix element. She uses as secret key the following parameters: initial state of the node register, number of iteration steps and angle that is used to determine rotation and phases in coin matrix elements. Quantum walk mixes states on the circle, and resulted wave function is send to Bob. States are uniformly mixed.

Bob encodes message by making translation on the circle and sends back resulted wavefunction to Alice. Quantum walk on circle commutates with the translation.

If Eve intercepts the message she can’t implement the walk, without knowing the key. When Alice receives the message by Bob, she can obtain it by just making a reverse quantum walk and subtract initial state of the node register.

QKD itself is used as fundament for other cryptographic protocols, like for example:

1) Quantum Secure Direct Communication (QSDC) – allows exchange of multiple messages
2) Controlled Quantum Dialogue – middlemen makes communication channel between communicating party without receiving any information of the messages
3) Quantum key distribution protocol – generates secure key for communication purpose known by both participants

Quantum Secure Direct Communication

QKD can be generalized for Quantum Secure Direct Communication (QSDC).

Alice generates n walk states by using the generated by her coin on randomly chosen of her state on walk and coin registers as before. She sends all of the states to Bob.

Half of them (n/2) chosen randomly of Bob will be measured. He sends to Alice coordinates of the measured circuit by classical channel. She sends the keys of those messages to Bob. Next Bob reverses quantum walk and measure the states. Alice sends the messages in those states and by the errors he can evaluate eavesdropping.

Bob uses half of the remaining walk states to encode message in the same way as in QKD, and the remaining (decoy) states leaves unchanged. He sends back to Alice all n/2 states.

After Alice receives the states, Bob sends her the coordinates of the decoy walks and Alice reverse the walk. She ureses decoys to check for eavesdropping by comparing them with the original message. If there is not eavesdropping, Alice decodes the n/4 walk states that contain the message.

More Topologies in QC

Circle is not the only topology used in quantum cryptography, examples of encryption based on other topologies are:

1) Quantum random walk on simplex is used for building a Hash function

2) Image encryption and steganography (hiding one image in to other) protocols are made with key created by alternate quantum walk on square grid and also by using quantum walk on torus.

Quantum signature schemes of different type are created by using quantum walk and quantum teleportation like:

1) Proxy (allows an original signer to delegate his signing right to another)

2) Blind (content of the message is disguised before signed)

3) Arbitrated (arbiter is needed to the use the scheme by signer).

THANK YOU FOR YOUR ATTENTION!

This work was supported by the Bulgarian Science Fund under contract KP-06-M48/2 /26.11.2020.

Participants: Hristo Tonchev and Petar Danev