ISSN 0861-7899

Философски алтернативи
Philosophical alternatives

6/2005
ГОДИНА XIV
VOL. XIV

СПИСАНИЕ НА ИНСТИТУТА
ЗА ФИЛОСОФСКИ ИЗСЛЕДВАНИЯ
ПРИ БАН

СЪДЪРЖАНИЕ

ФИЛОСОФСТВАНЕТО – РЕТРОСПЕКТИВНА САМОРЕФЛЕКСИЯ

СЪБИТИЯ, ФОРУМИ, КНИГИ

CONTENTS

RELIGION, MAN, TIME

LOGIC AND CULTURE

PHILOSOPHY OF SOCIETY

PHILOSOPHY OF SCIENCE AND OF KNOWLEDGE

MYTH AND LOGOS IN THE PHILOSOPHICAL TRADITION

PHILOSOPHIZING — A RETROSPECTIVE SELF-REFLECTION

EVENTS, FORUMS, BOOKS

ВАСИЛ ПЕНЧЕВ

КВАНТОВИЯТ КОМПЮТЪР: КВАНТОВИТЕ ОРДИНАЛИ И ТИПОВЕТЕ АЛГОРИТМИЧНА НЕРАЗРЕШИМОСТ[1]

Abstract

It is supposed a definition of quantum computer as a countable set of Turing machines on the ground of: quantum parallelism, reversibility, entanglement. Q—bit is the set of all the i^{-th} binary location cells transforming in parallel by unitary matrices. Church thesis is given in the quantum computer form. It is introduced notion of non—finite (but not infinite) potency.

„Изследванията за точковите множества ... аз от самото начало предприех не само заради спекулативния интерес, но едновременно и имайки предвид приложенията, които очаквах в *математическата физика* и в други науки.“[2]

Георг Кантор

Предмет на настоящото разглеждане е дали квантовият компютър, който по подобие на машината на Тюринг не представлява реална машина, а математически модел, нарушава тезиса на Чърч, че всяка ефективно изчислима функция е общо или частично рекурсивна (респ. че е машина на Тюринг). Идеята за квантов компютър, основаващ се също така и на състоянията на сдвояване [entanglement] с неадитивна ентропия, макар и примамлива с оглед съществено и принципно ускоряване посредством специални квантови алгоритми в сравнение с алгоритми, еквивалентни на машина Тюринг, за философите е интересна преди всичко поради връзката ѝ с подходите за обосноваване на математиката (интуиционизъм, формализъм), с теорията на множествата и проблема за актуалната и потенциална безкрайност, както и с континуум-хипотезата и нейните аналози и обобщения. Самото предположение, че може би съществуват алгоритми, които са разрешими на квантов компютър, но не са разрешими върху машина на Тюринг, е философски интересна (срв. с: Карлсон, 1999, с. 219).

Квантовият компютър, наред с *квантовата комуникация* и *квантовата криптография*, е подобласт на дисциплината *квантова информация*:

1. ПОСТАНОВКА НА ПРОБЛЕМА ОТ ГЛЕДНА ТОЧКА НА ИНТУИЦИОНИЗМА

Подложена на критика, в интуиционизма се отстранява актуалната, т.е. завършена безкрайност, която е в основата на Канторовата теория на множествата. Вместо нея се предполага безкрайността в качеството на процес, т. нар.

[1] Доклад, изнесен пред секция „Логика“ на 19 и 26 май 2004 г.
[2] Кантор, 1985, с. 167. На това място у Кантор ми обърна внимание Р. Люцканов.

потенциална безкрайност. Идеята в настоящата работа е да се разглеждат едновременно потенциална и актуална безкрайност, като потенциалната безкрайност се разположи между крайността и актуалната безкрайност[3]. Потенциалната безкрайност може да се въведе „актуално“ и с помощта на нестандартния анализ[4]. Като синоним на „потенциално безкрайното“ ще се използва терминът „некрайно“, за разлика от термина „безкрайно“, който е запазен за актуално безкрайното.

За да въведе своето разбиране за потенциална безкрайност, Брауер използва понятията „поток“ (вж. Клини, Весли, 1978, с. 65, 67) вместо множество, „последователност на избора“ (пак там, с. 66) (или „свободно възникваща последователност“), „закон на избора“ и „закон на съпоставянето“ (пак там). „Множеството или потокът интуиционистки не се мисли като „съвкупността“ от своите елементи даже в случай, когато всички (разрешени) последователности от избори се завършват, и по такъв начин елементите сами по себе си се явяват интуиционистки завършени обекти. Да се постъпи така би значело да се въведе завършена (актуална) безкрайност“ (Клини, Весли, 1978, с. 66). „Обектите, съпоставяни на изборите, могат да бъдат естествени числа, интервали с рационални краища и произволни обекти; доколкото за дадения поток тези обекти трябва да се избират от зададено изброимо множество, могат да се приемат от абстрактна гледна за естествени числа“ (Клини, Весли, 1978, с. 67).

На привичния за нас Канторов език същността на интуиционистката идея е да се представи потенциалната безкрайност като отношение на изброими множества: това в числителя, определяно чрез „закона за избора“, а това в знаменателя — чрез „закона за съпоставянето“. Действително изброимото множество е равномощно на всяко свое безкрайно подмножество. Ако се построи множество, което да е изоморфно на тяхното отношение, а Брауеровата „последователност от избори“ дава възможност именно за такова построяване, то мощността на така построеното множество е „некрайна“. При това изглежда, че ще съществуват изброимо много некрайни мощности. Може да се направи аналогия с границата на отношението на две числови редици, всяка от които клони към безкрайност, но границата на отношението може да е произволно крайно и поради това във всеки случай различно число. Например да разгледаме като „съпоставяно множество“ (т.е. онова, което се дефинира чрез „закона за съпоставяне“) множеството от всички естествени числа (което множество в качеството на поток Брауер нарича универсален поток), а като „избрано множество“ (т.е. онова, което се дефинира чрез „закона за избора“) — множе-

[3] Така както според Канторовата теория съществуват най-разнообразни мощности на множествата от актуалната безкрайност, в т. III. ще се предположат разнообразни некрайни мощности. Както ще се обсъди в т. VII., изглежда, може да се постави въпросът за съответствието между степените на Тюрингова неразрешимост (образуват множество с изброима мощност) и некрайните множества с последователно намаляваща мощност. Тогава въпросът за не-Тюринговите неразрешимости ще може да се свърже с т. нар. принцип на конструктивния подбор, или принципа на Марков. В настоящия контекст той може да се постави така: между крайните и некрайните множества няма друг тип множества; още една формулировка: некрайните множества от ред (вж. т. III.) с мощност, равна или по-голяма от изброима, са крайни.

[4] Нестандартните елементи на модела могат да се разглеждат и като „идеални“, „инфинитезимални“ безкрайно малки и безкрайно големи числа. Точките на неотделимите множества, които се разглеждат по-нататък, биха били свързани с разглеждането на нестандартните безкрайно-близки точки.

ството от кратните на някое естествено число *n*. Можем да приемем, че мощността на некрайното множество е безкрайност от тип (-*n*) и некрайните множества ще бъдат изброимо много (или пък при интуиционисткия подход — „некрайно много“). Следователно потенциалната безкрайност може да се мисли като вероятността чрез изброимо много избори (дефинирани от „закона за избора“) да се изберат всички елементи от някое изброимо множество (дефинирани чрез „закона за съпоставянето“).

Трябва да се прави разлика между крайно и конструктивно (респ. интуитивно валидно построение) построение, както и между конструктивно построение и актуална безкрайност, а на свой ред конструктивните построения биват крайни и некрайни. Една идея в настоящата работа е, че некрайните построения и респ. некрайните множества могат да се представят като сдвоени крайно множество N и изброимо безкрайно множество A, при което това крайно множество N съответства еднозначно на изброимо безкрайното множество на избора при една последователност на избора, а множеството A — на изброимо безкрайното съпоставяно множество. Крайното множество N ще съответства на степента на неразрешимост върху машина на Тюринг на некрайното построение. Не е изключено квантовият компютър да може да изпълнява алгоритми, неразрешими върху машина на Тюринг, като уточняването на това твърдение се намира в гл. 7.

Може да се предположи, че при некрайните множества ще съществува приблизителен аналог на теоремата на Гьодел за непълнотата (Коэн, 1969, с. 68, 71, 78), а именно, че могат конструктивно да се построят некрайни множества, които не се определят еднозначно от избраното и съпоставяното множество, т.е. не могат да се представят като сдвояване на крайно и безкрайно множество.

2. ПОСТАНОВКА НА ПРОБЛЕМА ОТ ГЛЕДНА ТОЧКА НА ТЕОРИЯТА НА МНОЖЕСТВАТА

Няколко основни твърдения:

1. Съществува поне едно не-крайно кардинално число *z*, такова че: 2^z=a, т.е. множеството от подмножествата на множеството с некрайно кардинално число *z* е с мощността *a* на изброимо множество.

2. n<z<a, или мощността на всяко крайно множество *n* е по-малка от мощността на некрайното множество *z*, а последната на свой ред е по-малка от мощността на изброимото множество *a*.

3. z=алеф(-1), т.е. некрайното множество е равномощно на множеството от ординали, строго по-малки от ординала на изброимото множество.

4. Съществува безкраен намаляващ ред от некрайни (с изключение на първото, което е на изброимото множество) кардинални числа:

алеф(0), алеф(-1), алеф(-2), алеф(-3), алеф(-4), ... алеф(-i),... ... .

или

a, z, z-1, z-2, z-3, ... z-i+1, ...,

при което

2^{z-i}=z-i+1.

5. Този ред, т.е. редът от некрайни кардинални числа, който ще означавам с z_i, съвпада[5] с реда на кардиналните числа от множествата на всички ординални числа на n-сводимите по Тюринг алгоритми, или с изброима степен на неразрешимост (т.е. със съответно множество, съдържащо разрешимото като истинско подмножество). Последният ред е нарастващ:

алеф(n), алеф(n)+1, алеф(n)+2, алеф(n)+3, ..., алеф(n)+j, ...

При това алеф(n) означава кардиналното число на множеството от всички крайни ординали и съответният ординал (по теоремата за добрата наредба на всяко множество, следваща от аксиомата за избора) на 1-сводимия по Тюринг неразрешим алгоритъм; алеф(n)+1 означава кардиналното число на множеството от ординали, по-малки или равни на ординала на 1-сводимия по Тюринг неразрешим алгоритъм, или на втория неразрешим алгоритъм. Първият неразрешим алгоритъм има ординално число с 1 по-голямо (т.е. с единица отдясно) от всеки разрешим алгоритъм; вторият има ординално число с 1 по-голямо (пак с единица отдясно) от първия неразрешим алгоритъм и т.н. Обичайният метод за построяването на неразрешими алгоритми е диагоналният (Роджерс, 1972, с. 27; Мартин-Леф, 1975, 29—30), възхождащ към Канторовото доказателство за съществуване на неизброими множества.

Твърдението 5. може да се запише така:

За всяко i съществува j и обратно, за всяко j съществува i, такова, че: алеф(-i) = алеф(n)+j.

6. Въвеждаме ново кардинално число p_1, чийто смисъл е избор на един елемент сред изброимо множество, съдържащо избрания елемент. То може да се дефинира строго като отношение на кардиналното число подмножествата на някое изброимо множество, съдържащи точно един елемент, към кардиналното число на изброимото множество на естествените числа. Това символично можем да запишем така: $p_1=a_{\{1\}}/a$. Интуитивният смисъл на кардиналното число p_1 е на вероятност: на вероятността да бъдат изброени всички елементи на изброимо множество, след като се осъществят изброимо много избори на един елемент.

7. Аналогично образуваме нарастващ ред $p_j=a_{\{j\}}/a$:

$p_1, p_2, p_3, p_4, \dots p_j, \dots$

8. p_j=алеф(n)+j

Фактически до съществуването на некрайни кардинали и ординали се достига и в обичайно излаганата теория на множествата с т. нар. парадокс на Сколем. Относно този парадокс Пол Коен пише: „Този парадокс, състоящ се в това, че изброим модел може да съдържа неизброимо множество, се разяснява със забележката, че твърдението за неизброимостта на някакво множество означава само несъществуване на взаимно еднозначно изображение на това

[5] Твърдението за това съвпадение е изводимо въз основа на аксиомата на избора и следователно е в пряка връзка с хипотезата за континуума. Изглежда, че аксиомата за избора следва от континуум-хипотезата само при неявното допускане за отделимост на елементите на множеството (вж. по-подробно в края на настоящата глава и глава IV). При „неотделими множества“, каквито са некрайните, е допустимо аксиомата за избора да бъде съвместима с отрицанието на континуум-хипотезата и оттук също така с неадитивността на ентропията на дизюнктните подмножества на едно множество, тъй като, грубо казано, не е съвсем ясно, без уточнения, какво означава да се избере елемент от „неотделимо множество“ (той може да е неотделим от други елементи и неговият избор „повлича“ и другите елементи, от които е в някакъв смисъл неотделим). Неадитивна (Цалисова) ентропия се въвежда напр. в (Рудой, 2003, 22—28).

множество върху множеството на всички цели числа. Неизброимото множество в M съдържа в действителност само изброимо количество елементи от M, но в M не съществува никакво взаимно еднозначно изображение на това множество върху множеството на всички цели числа“ (Коэн, 1969, с. 39). Нещата идват по местата си, ако кажем, че изброим модел може да съдържа некрайно множество.

Парадоксът на Сколем произтича от теоремата на Льовенхайм—Сколем (напр. Коэн, 1969, с. 37), „доказателството на която почти съвпада с доказателството на теоремата за пълнотата“ (Коэн, 1969, с. 37, 29; Успенский, 1982, с. 52, 53). „Много интересна черта на теоремата за пълнотата е информацията за мощността на онези модели, съществуването на които тя твърди. От нея произтича например, че както и да формализираме теорията на множествата с всички нейни изводи, отнасящи се до съществуването на множества с голяма мощност, предлаганото от нас множество от аксиоми ще има изброим модел“ (Коэн, 1969, с. 35). И оттук по теоремата на Льовенхайм—Сколем (т. нар. парадокс на Сколем) ще следва наличието на некрайно подмножество на този модел, който ще има поне един праобраз в съвкупността от аксиоми на теорията на множествата.

Във философски контекст може да се каже, че тъй като съществуването на некрайни множества следва от теоремата за пълнотата, то логическата завършеност поражда некрайни множества. Самата теорема за непълнотата може да се разглежда като построяване чрез диагоналния метод (оригиналното доказателство на Гьодел) или чрез рекурсивни функции (доказателството ѝ от Коен) на некрайно множество.

Едно друго следствие от теоремата на Гьодел за пълнотата гласи: „Ако S допуска безкраен модел или даже произволно големи крайни модели, то S допуска модел с произволно големи мощности“ (Коэн, 1969, с. 34). Тогава от наличието на некрайни модели следва наличието на модели с произволно големи мощности. От това и от горните два абзаца следват съвместимостта и изводимостта на некрайните множества от теорията на множествата.

Същевременно: „Това следствие показва, че никаква система от аксиоми не може да има единствен (с точност до изоморфизъм) модел, с изключение на случаите, когато този единствен модел е краен. Оттук се вижда, че обичайните математически системи, например на естествените числа или на реалните числа, притежаващи, както е прието да се смята, само един модел, не могат да бъдат описани от *никаква* формална система аксиоми. Както вече се спомена, при разглеждането на класическите аксиоми за тези системи се разкрива, че не образуват формална система в нашия смисъл, понеже те говорят неформално за множество“ (Коэн, 1969, с. 35). Въвеждането на некрайните множества в известен смисъл уточнява (но не изчерпателно, т.е. не формализира) понятието за множество например като изискване за отделимост на елементите на едно множество: всеки елемент на едно множество може да бъде разглеждан независимо от всеки друг и замяната на един елемент на едно множество не води до изменение на нито един друг елемент на същото множество. В неформалното говорене за множество в рамките на досегашната теория на множествата фигурира неявно горното твърдение. Но то не е формулирано като аксиома (срв. с: Медведев, 1982, с. 30). Ето защо в нейните рамки може да се изведе коректно теоремата за непълнотата. В действителност обаче разглеждането на некрайни множества влече след себе си отхвърляне неявното твърдение за отделимост на елементите на едно множество. В същата редица на отхвърляне на твърдението за отделимост на елементите е и отхвърлянето на тезиса на Чърч и понятието за квантов алгоритъм, основаващ се на състоянията на сдвояване и неадитивна ентропия[6]. Понятието за отделимост се въвежда в топологията в качеството на специална аксиома, която се предлага в различни по сила формулировки. Трябва да се постави въпросът, дали не следва да бъде преместена и съответно преформулирана тази аксиома от топологията в теорията на множествата и в метаматическите построения. Такъв подход по същество следва Успенски, който разглежда понятието за отделимост и неотделимост във връзка с рекурсивните и изчислими функции (Успенский, 1960, с. 281 и 277—293) и във връзка с теоремата на Гьодел за непълнота (Успенский, 1982, 43—48) и посочва две интересни теореми: „(Теорема за неотделимостта.) *Съществуват две непресичащи се рекурсивно-изчислими множества, неотделими посредством общорекурсивни множества*" (Успенский, 1960, с. 283). „Ако множеството от доказуемите и опровержими в дадена дедуктика съждения са неотделими, то тази дедуктика е непопълнима" (Успенский, 1982, с. 47; вж. и с. 45).

3. ДИАГОНАЛНИЯТ МЕТОД, АКСИОМАТА ЗА ИЗБОРА И КОНТИНУУМ-ХИПОТЕЗАТА

Диагоналният метод възхожда още към древността, към приписваното на Питагор и неговата школа откритие за несъизмеримостта на диагонала на квадрата към неговите страни (напр. Славков, 1971, 166—167; Славков, 1976, 49—52). Впоследствие е употребен от Кантор за доказателството на неизброимостта на ирационалните числа (напр. Курош, 1956, 357—358). Оригиналното доказателство на Гьодел на първата теорема за непълнотата използва метода на аритметизация и след това почти буквално повтаря диагоналното доказателство на Кантор (срв. с: Kleene, 1952, 6—8).

„Сега накратко ще набележим първоначалното доказателство на първата теорема за непълнотата. Това доказателство фактически е по-кратко [от приведеното от Пол Коен] и макар по същество да използва същите доводи, то не използва понятието за рекурсивна функция. Диагоналният аргумент се използва непосредствено към съжденията от Z_1. Преди всичко да номерираме по някакъв естествен начин всички формули с една свободна променлива $A_n(x)$. Нека $B(n)$ бъде съждение за това, че $A_n(n)$ не е доказуемо. Тогава $B(n)$ трябва да съвпада с $A_{n0}(n)$ за някое естествено число n_0, което може да се изчисли в явен вид. Сега съждението $B(n_0)$ интуитивно твърди, че самото то не е доказуемо. Поточно, ако $B(n_0)$ е доказуемо, то то е истинно, а затова $An_0(n_0)$ не е доказуемо. Но $A_{n0}(n_0)$ съвпада с $B(n_0)$, така че $B(n_0)$ не е доказуемо — противоречие. Ако не-$B(n_0)$ е доказуемо, то $B(n_0)$ е невярно и следователно $A_{n0}(n_0)$ съвпада с $B(n_0)$ е доказуемо — отново противоречие. И така, нито $B(n_0)$, нито не-$B(n_0)$ не е доказуемо" (Коэн, 1969, с. 72).

Ще използвам диагоналния аргумент в „обратна форма", за да въведа некрайни мощности. Нека е дадена съвкупност от z редици, всяка от които се състои от z едноцифрени числа. По диагоналния метод съставям число x, чието добавяне към съвкупността от z редици е превръща в изброима. Тъй като то е съставено по диагоналния метод, z трябва да бъде мощност, строго по-малка

[6] Принципът за отделимост на елементите на едно множество може да се формулира и като принцип за адитивността на ентропията на дизюнктните подмножества на едно множество.

от изброимата ***a***. Но z не може да бъде и крайна, защото тогава ***x*** щеше да съдържа краен брой цифри, следователно n<z<a. Очевидно, за да се състави числото x, се използва аксиомата за избора, а именно, че от всяка от z-те на брой редици може да се вземе точно един от z-те елемента. Фактически аксиомата за избора се използва и в това, че се предполага (по теоремата на Цермело), че множеството от всички изброими множества може да се нареди добре, така че макар *z* да не е изброима мощност, то z+1, където добавено число е съставено по диагоналния метод, вече е изброима и следователно се явява най-малката изброима мощност, или респ. мощността на най-малкото изброимо множество в добре нареденото множество от всички изброими множества. Приведеното разсъждение показва изключително тясната връзка между аксиомата за избора и диагоналния метод. Напълно аналогично в Канторовото доказателство за неизброимостта на континуума се предполага, че множеството от всички неизброими множества може да се нареди добре, след като посредством диагоналния метод можем да добавим още едно множество към множеството от всички изброими множества.

Аксиомата за избора вече неявно беше използвана в твъдение 5 от глава III, тъй като множеството от некрайни числа z, z—1, z—2, ... е подобно на множеството на отрицателните цели числа. „Множеството от всички отрицателни цели числа ..., -(n+1), -n, ..., -3, -2, -1 и всяко подобно на него множество се нарича множество от порядков тип w*. В множеството има последен елемент -1, но очевидно няма първи елемент; ето защо това множество, бидейки наредено, не е добре наредено и порядковият тип w* не е порядково число. *Нещо повече, налице е твърде простата, но въпреки това важна теорема: За това едно наредено множество да не е добре наредено, необходимо и достатъчно е в него да съществува подмножество от типа w**" (Александров, 1977, 62—63). За да съвпадне с множеството от некрайните числа с редицата на степените на неразрешимите по Тюринг алгоритми (което е добре наредено), трябва да се използва теоремата на Цермело, така че и множеството от некрайните числа да е добре наредено. Теоремата на Цермело гласи: „всяко множество може да бъде добре наредено" (Александров, 1977, с. 82) и при нейното доказателство се използва аксиомата за избора (напр.: Александров, 1977, с. 74; Медведев, 1982, с. 26).

Некрайни мощности могат да се въведат и като се използва аксиомата за избора, и без да се използва аксиомата за избора. Аксиомата за избора е тясно свързана с континуум-хипотезата, като и двете са изводими от аксиомата за конструктивността на Гьодел. От друга страна, неотделимите множества нарушават[7] хипотезата за континуума и следователно не изпълняват аксиомата за конструктивността на Гьодел. Тоест неотделимите множества (и в т. ч. някои некрайни множества) са неконструктивни множества (в смисъла на Гьодел).

Хипотезата на Суслин може до известна степен да онагледи с експлицитен пример първата теорема на Гьодел за непълнотата.Наличието на неотделими множества противоречи както на аксиомата за конструктивността, тъй като неотделимите множества са неконструктивни, така и на хипотезата на Суслин, защо няма причина на действителната права да няма неотделими множества, въпреки че аксиомата за конструктивността и хипотезата на

[7] Действително неотделимото множество S може да се дефинира като такова, при което мощността на множеството M от неговите подмножествата не е 2^S, при което могат да се различават същински неотделими множества с подадитивност на ентропията на елементите, за които $cardM<2^S$, и свръхотделими множества с наддитивност на ентропията, за които $cardM>2^S$.

Суслин си противоречат помежду си. От друга страна, наличието на неотделими множества, изглежда, е съвместимо както с обобщената континуум-хипотезата (в т. ч. аксиомата за избора), така и с тяхното отрицание. Вероятно е предположението, че от наличието на неотделими множества следва хипотезата за измеримия кардинал (която на свой ред се изключва от аксиомата за конструктивността). Чрез подходящо обобщение на понятие за мяра (комплексна мяра, операторна мяра), тя може да се въведе за неотделимите и неизмеримите множества, при което не само всяка функция, но и всяко бинарно отношение е интегрируемо върху такава обобщена мяра.

4. ОРДИНАЛ И КАРДИНАЛ НА ФИЗИЧЕСКАТА ВЕЛИЧИНА В КВАНТОВАТА МЕХАНИКА

В класическата физика измерената величина се представя с някое рационално число. На такава основа можем да приемем, че ординалът и съответно кардиналът на „наблюдаемата" (в смисъла на *измерената* величина) в класическата физика е краен, ***n***. В квантовата механика на физическата величина в крайна сметка също се съпоставя някое рационално число f_{cp}, но то се получава като закръглена до рационална реална стойност на функционал, съпоставящ две вълнови функции (напр.: Ландау, Лишфиц, 1974, с. 19; Петров, Петров, 1989, с. 16) — Ψ и FΨ, където F е линеен ермитов оператор (Ландау, Лишфиц, 1974, с. 24; Петров, Петров, 1989, с. 11) в хилбертово пространство от комплексни функции. Според тълкуванието на Макс Борн (напр. Петров, Петров, 1989, 134—139; вж. и: Стефанов, 1999, 63—64; Feynman, 1982, p. 485) което е широко разпространено и към което се придържам в настоящето изложение, $|\Psi|^2$ има смисъл на вероятност. В съответствие с твърдения 6, 7 и 8 в глава III на $|\Psi|^2$ и $|F\Psi|^2$ ще съпоставя две некрайни мощности p_i и p_j, така че за крайния ординал или кардинал на измерената величина n_{fcp} да е в сила $n_{fcp}=|i - j|$.

Това разглеждане позволява да се определят некрайните мощности и като търсения от Айнщайн „елемент на реалността" в квантовата механика, но той не би отговарял на изискванията (Эйнштейн, 1966, с. 605, 608; вж. и: Adami, Cerf, 1999, p. 258, 257) (които впрочем са заимствани от модела на класическата физика): 1) на всяка физическа величина съответствува не един, а два „елемента от реалността"; 2) тези „елементи от реалността" са некрайни и в този смисъл са нелокални и неопределени.

Може да се покаже, че на всяка Ψ функция се съпоставя точно едно неотделимо множество от определен (най-прост) тип. На трансформацията Ψ в $|\Psi|^2$ съответства преобразуване на неотделимото множество в отделимо. Това навежда на мисълта, че некрайните множества с кардинали, определени по начин както в глава III, могат да се превърнат в конструктивни, ако се приеме „принципът на конструктивния подбор" („принципът на Марков"). Този подход е формулиран и като твърдения 5 и 8 в глава 3. С обсъждането на некрайните множества като конструктивни веднага се оказват валидни аксиомата за избора и обобщената континуум-хипотеза. Неотделимите множества в собствен смисъл (на които се съпоставя Y функция) притежават мощност по-голяма или равна на измеримия кардинал и дори само поради това не могат да бъдат разглеждани като конструктивни.

5. КВАНТОВИЯТ КОМПЮТЪР

Квантовият компютър[8] — както и машината на Тюринг[9] — е математически модел на изчислителен процес. Ако моделът на квантовия компютър се основава на някакво обобщение на машината на Тюринг, можем да говорим за квантова машина на Тюринг[10]. Принципните отлики на квантовата от класичес-

---

[8] Различен е подходът за определяне на „квантов компютър" по следния начин: „Квантовите компютри са физически устройства, изпълняващи логически операции над квантови състояния посредством унитарни преобразования, без да нарушават квантовите суперпозиции в процеса на изчисление. Много схематично работата на квантовия компютър може да се представи като последователност от три операции: 1) запис (подготовка) на началното състояние; 2) изчисление (унитарни преобразования на началните състояния); 3) извод на резултата (измерване, проекция на крайното състояние)" (Килин, 1999, 517—518).

[9] „Да разгледаме крайно механично устройство, което е свързано с хартиена лента, безкрайна в двете посоки. Лентата е разделена по цялата дължина на клетки с равен размер. ... Устройството е такова, че лентата може да се движи през него, при това точно една клетка се намира вътре. За клетката, намираща се вътре в устройството, ще говорим като за клетка, *разглеждана* от устройството. Посоките по лентата ще наречем съответно *дясна* и *лява*. Устройството е в състояние да осъществява една от четирите основни операции: (1) може да запише „1" в разглежданата клетка, ако там вече не е записана „1"; може да изтрие написаното в четената клетка и по такъв начин да я направи празна, ако тя вече не е била празна; (3) може да премести своето внимание една клетка вдясно (да придвижи лентата една клетка вляво); (4) може да премести своето внимание една клетка вляво (да премести лентата с една клетка вдясно). Устройството в активно състояние осъществява основните операции със скорост една операция за единица време. Понякога в случая, когато устройството е извършило една операция, ще казваме, че е направена *стъпка* в работата на устройството. При завършване на всяка стъпка устройството само по себе си (като нещо, различно от лентата) притежава една от фиксирано крайно множество възможни (механически) структури. Такива структури ще наричаме *вътрешни състояния*. За означаване на различните вътрешни състояния ще използваме символите q_i, i=0,1,2, ... Накрая, устройството е конструрирано така, че неговото поведение се описва с краен списък от детерминирани правила. Тези правила определят по текущото вътрешно състояние и запис в четената клетка, каква операция трябва да се осъществи следваща и какво трябва да бъде следващото вътрешно състояние (в края на тази следваща операция). Нека 1 и B означават възможните записи във всяка клетка (B съответствува на *празната* клетка). Нека 1, B, R и L означават основните операции (1), (2), (3) и (4) съответно. (Операция (1) не осъществява изменение на лентата, ако в разглежданата клетка вече има „1", а операция B не осъществява изменение на лентата, ако разглежданата клетка е празна.) Така наборът от правила, определящи поведението на устройството, може да се запише като набор от *четворки*. Всяка четворка се състои от символи (поред) за (i) вътрешно състояние, (ii) възможен запис в клетката, (iii) операция, (iv) вътрешно състояние. Четворката (i, ii, iii, iv) изразява такова правило: при наличие на (i) и (ii) устройството осъществява (iii) и преминава в (iv). Ще предполагаме, че всеки набор от такива четворки е набор от правила за някое устройство, въвеждайки само единственото ограничение, че всеки две различни четворки трябва да се различавт в (i) или в (ii). Ще наричаме това ограничение *условие за съвместимост*; при това условие наборът от правила не може да изисква две или повече различни действия в едно и също време. Обаче не предполагаме, че в набора от правила се предвижда всяка комбинация (i) и (ii); по такъв начин допускаме, че при някакви обстоятелства устройството не може да извърши никаква операция. В такива случаи ще казваме, че устройството е спряло" (Роджерс, 1972, 30—31). Вж. също така: (Kleene, 1952, 356—362).

[10] „Квантовите машини на Тюринг (QTM) е най-добре да се мислят като квантовомеханични обобщения на вероятностните Тюрингови машини (PTM). В PTM, ако инициализирате лентата в някоя първоначална конфигурация и стартирате машината, без да наблюдавате машината известно време t, то състоянието се описва от вероятностно разпределение между всички възможни състояния, достижими от първоначалното състояние за време t. Аналогично, в една QTM, ако стартирате машината в някоя първоначална конфигурация, и ѝ позволявате да се развива за време t, тогава нейното състояние след време t се описва като суперпозиция от всички състояния, достижими за време t. Ключовата разлика е, че в класическата PTM се следва само една отделна изчислителна траектория, докато в QTM се следват всички изчислителни траектории и получената суперпозиция е резултат от сумирането на всички възможни траектории, достижими за

ката машина на Тюринг по мое мнение са три: квантовият паралелизъм, обратимостта и квантовото сдвояване. *Принципът на квантовия паралелизъм* означава, че квантовата машина на Тюринг може да се представи като изброимо много машини на Тюринг, работещи паралелно, но с един единствен общ изход. *Обратимостта* означава, че последователността от стъпки на всяка машина на Тюринг е обратима, т.е. изчислението на всяка своя стъпка може да се върне произволен брой стъпки назад, вкл. до своето начало, и отново да почне да се осъществява: ако класическата машина на Тюринг се движи „напред", то квантовата допуска произволни движения „напред — назад". *Квантовото сдвояване* означава, че произволни две (а следователно произволно крайно или изброимо количество) клетки от една от изброимото множество класически машини на Тюринг, представящи квантовата, се променят синхронно, при промяна точно в една от тях.

Строгото математическо определение на класическата машина на Тюринг е: „Нека T={0, 1} и S={0, 1, 2, 3}. Тогава машината на Тюринг може да се определи като изображение на крайно подмножество от множеството N X T в S X N [с X е означено декартово произведение]. Тук T представлява записите в клетката, S — операциите, които следва да се осъществяват, а N дава възможните номера на вътрешните състояния" (Роджерс, 1972, 31—32).

За да се изпълни изискването за квантов паралелизъм, трябва да се разгледа изброимо множество от такива изображения, заради обратимостта всяко изображение трябва да е биективно и поради това могат да се разглеждат направо четворките, които са елементи на декартовото произведение N X T X S X N. Сдвояването обаче налага да се разглеждат изображения между тези четворки, т.е. изображение на N X T X S X N в себе си.

Обобщавайки, *квантовата машина на Тюринг е изброимо множество изображения на N X T X S X N в себе си*. При това определение не е отчетен начинът на редукция на множеството изображения до едно единствено изображение — изходът на квантовата машина на Тюринг.

Естествено е да се наложи изискването card N = const за всички класически машини на Тюринг, образуващи квантовата. Тогава множеството $\{i \text{ X } T \text{ X } S \text{ X } к\}_j$, j = 1, 2, 3,..., където j е поредният номер на класическата машина на Тюринг от множеството, образуващи квантовата, ще представлява *квантовата операция*, извършвана върху един *квантов бит,* кубит, q-bit. Един *квантов бит* може да се дефинира[11] като подмножество на множеството c_1I0)+c_2I1),

време t. ... ...QTM има потенциала за кодиране на много входове на задачата едновременно на една и съща лента, и да осъществява изчисление върху всички входове за времето, което би отнело да се извърши само едно от изчисленията класически. Този метод носи названието „квантов паралелизъм" (Williams, Clearwater, 1999, p. 25). Несъвпадаща с излаганата реализация на квантова машина на Тюринг се описва в: (Mahler, Kim, 1999, 93—101). Файнман показва, че класически компютър не може да симулира квантова система в реално време и още през 1981 г. предлага „квантовите компютри" като „универсални квантови симулатори" (Feynman, 1982, p. 474). В доклад, изнесен през 1984 г., показва, че квантовият компютър, определен като квантовомеханичен симулатор, може да симулира действието на класически компютър (Фейнман, 1986). Тези работи на Файнман ознаменуват възникването на идеята за квантов компютър.

[11] Кубитът може да се разглежда и като *единица за квантова суперпозиция*."*... суперпозицията, която се среща в квантовата механика, съществено се отличава от суперпозицията във всяка класическа теория*" (Дирак, 1979, 26—27). „*... на всяко състояние на динамичната система в определен момент от времето съответствува кет-вектор* [векторът на състоянието на системата], *при което това съответствие е такова, че ако състоянието е образувано в резултат на суперпозиция от някои други състояния, то кет-векторът на това състояние се изразява линейно чрез съответните кет-вектори на другите състояния и обратно*" (Дирак, 1979, с. 29).

където с I0), I1) са означени две ортогонални състояния в хилбертовото пространство, а c_1 и c_2 са две комплексни числа, такива че: $|c_1|^2+|c_2|^2=1$. С други думи, квантовият бит е изоморфен на подмножество на единичната сфера в евклидовото пространство. Квантовата операция е биективно изображение на един квантов бит в друг, т.е. на едно подмножество на единичната сфера в друго и следователно унитарна трансформация[12]. При това положение квантовият компютър (пренебрегвайки засега квантовото сдвояване) може да се представи като лента с клетки и устройство, при което лентата преминава, досущ като класическа машина на Тюринг[13]. Отликите са две: във всяка клетка е записан не бит, а кубит; освен командите „вляво!" и „вдясно!" квантовият компютър извършва произволна унитарна трасформация, всяка от които може да се представи като изброима съвкупност от елементарните операции „запиши 1!" и „запиши 0!". В крайна сметка при измерването на изхода обаче съвкупността от кубитове се редуцира до последователност от нули и единици[14].

Описанието на сдвояването в скицирания модел е следното. Определени подмножества (при максимална степен на сдвояване цялата единична сфера) в кубитовете в две различни клетки са идентични и съответно операцията върху единия веднага променя другия.

Квантовият компютър, разгледан като черна кутия, преобразува една крайна последователност от нули и единици в друга такава. При това обаче входната е някакъв краен ординал, докато изходната е отношение между два субтрансфинитни (некрайни) ординала. Очевидно е, че квантовата машина на Тюринг не е класическа и следователно не е частично или общорекурсивна функция. Тезисът на Чърч обаче все пак остава открит въпрос във видоизменена форма: дали на квантовата машина на Тюринг (макар и с експоненциално забавяне в общия случай) не съответства винаги някоя общо или частично рекурсивна функция, която да е в състояние да приведе всеки вход на QTM във всеки съответен на този вход изход?

6. КВАНТОВИТЕ ОРДИНАЛИ И ТИПОВЕТЕ АЛГОРИТМИЧНА НЕРАЗРЕШИМОСТ

Квантовите ординали вече бяха въведени в глава 2. и в твърдение 5. от същата глава беше постулирано съвпадението им с типовете алгоритмична несводимост по Тюринг. Принципът за конструктивния подбор (принципът на Марков) се интерпретира от теоретико-множествена гледна точка като отсъствие на нов тип ординали, по-големи от крайните, но по-малки от некрайните. При това положение най-малката степен[15] на алгоритмична несводимост по

---

[12] Срв. с бел. 7.

[13] От това също е очевидно, че квантова машина на Тюринг може да симулира класическа, например полагайки произволен кубит за 1, а липсата на кубит за празна клетка.

[14] Лентата от кубитове с извършвани върху тях унитарни операции общо може да се представи като биективно изображение на две подмножества (две бинарни отношения) на декартовото произведение от хилбертовото пространство със себе си. Една у-функция е вектор в хилбертовото пространство (при някакъв пълен ортоготален базис ψ_i, един кубит q в нея представлява компонент-променлива, в този вектор: $\psi=(c_1, c_2, c_3, ..., q, ..., c_i, ...)$. $c_1, c_2, c_3, ..., c_i...$ — комплексни константи.

[15] Такава съществува според теоремата на Цермело и респ. приемането на аксиомата за избора и в крайна сметка, на континуум-хипотезата. По-нататък ще се развие възгледът, споменат в бел. 9, че аксиомата за избора може да бъде валидна (при известно осмисляне и обобщение за

Тюринг се отъждествява с квантовия ординал, а квантовите ординали се оказват еквивалентни на множества конструктивни по Гьодел. В заключение бих искал да изкажа следната хипотеза: квантова машина на Тюринг, представима като един кубит, е еквивалентна на най-малката степен на алгоритмична неразрешимост по Тюринг, а отношението на еквивалентност на сводимост по Тюринг в тази степен на неразрешимост е изоморфно на унитарна трансформация върху кубита; квантова машина на Тюринг, представима като два кубита, е еквивалентна на следващата степен и така нататък. Различни сдвоявания между два съседни кубита ще съответстват на *нецели* некрайни ординали и кардинали. Някои (или може би дори всички) неотделими множества се представят като наредено множество от кубитове и сдвоявания между тях.

В заключение може да се каже, че тезисът на Чърч, подобно на всеки философски въпрос, с нови отрития не се решава, а се видоизменя.

ЛИТЕРАТУРА

А л е к с а н д р о в, П. (1977). Введение в теорию множеств и общую топологию. М., Наука.

Д и р а к, П. (1979). Принципы квантовой механики. М., Наука.

К л и н и, С., Р. В е с л и. (1978). Основания интуиционитской математики. М., Наука.

К а н т о р, Г. (1985). О различных теоремах из теории точечных множеств в n-кратно протяженном непрерывно пространстве Gn. Сообщение второе. — В: Труды по теории множеств. М., Наука, 154—169.

К а р л с о н, А. (1999). Квантови компютри. — Светът на физиката, 3.

К и л и н, С. (1999). Квантовая информация. — Успехи физических наук, т. 169, № 5.

К о э н, П. (1969). Теория множеств и континуум-гипотеза. М., Наука.

К у р о ш, А. (1956). Курс высшей алгебры. Москва.

М а р т и н-Л е ф, П. (1975). Очерки по конструктивной математике. М., Мир.

М е д в е д е в. (1982). Ранная история аксиомы выбора. М., Наука.

Л а н д а у, Л., Е. Л и ф ш и ц. (1974). Квантовая механика. Нерелятивисткая теория. (Теоретическая физика. Т. III.) М., Наука.

П е т р о в, А. и С. П е т р о в. (1989). Квантова механика. Интерпретации и алтернативи. 1927—1987. С., Наука и изкуство.

Р о д ж е р с, Х. (1972). Теория рекурсивных функций и эфективная вычислимость. М., Мир.

С л а в к о в, С. (1971). Аспекти на математическото познание (философски анализ). С., Наука и изкуство.

С л а в к о в, С. (1976). Философия, математика, действителност. С., Издателство на БАН.

С т е ф а н о в, А. (1999). Що е физическа реалност? Габрово, Alma mater international.

Р у д о й, Ю. (2003). Обобщенная информационная энтропия и неканоническое распредление в равновесной статистической механике. — Теоретическая и математическая физика. Т. 135, № 1.

У с п е н с к и й, В. (1960). Лекции о вычислимых функциях. М., ГИФМЛ.

У с п е н с к и й, В. (1982). Теорема Геделя о неполноте. М., Наука.

У с п е н с к и й, В. (1988). Машина Поста. М., Наука.

Ф е й н м а н, Р. (1986). Квантовомеханические ЭВМ. — Успехи физических наук, т. 149, № 4.

неотделими множества) заедно с отрицанието на континуум-хипотезата. За целта едновременно трябва да се допусне *неизпълнението* на условията ***(1)*** и ***(2)***: (Хипотезата за континуума е хипотеза на Г. Кантор, състояща се в това, че всяко безкрайно подмножество на континуума R е равномощно или на множеството на естествените числа, или на R. Еквивалентна формулировка (при наличието на аксиомата за избора) е: $2^{\text{алеф}(0)}$=алеф(1). Обобщението на това равенство за произволни кардинални числа се нарича обобщена континуум-хипотеза: за всяко ординално число $2^{\text{алеф}(\alpha)}$=алеф(α+1). ***(1)***. При отсъствието на аксиомата за избора обобщената континуум-хипотеза се формулира във вида: за всяко ***к*** не съществува такова ***m***, че $k<m<2^k$ ***(2)***, където ***k***, ***m*** са променливи за безкрайни кардинални числа. От ***(2)*** произтича аксиомата за избора и ***(1)***, а от ***(1)*** и аксиомата за избора произтича ***(2)***). При това междинните степени и на некрайните мощности от тип „не-алеф“ и от тип „алеф“. При това положение е за предпочитане формулировката на аксиомата за избора във формата: „Всяка мощност е алеф.“

Эйнштейн, А. (1966). Можно ли считать квантовомеханическое описание физической реальности полным? — В: Собрание научных трудов. Т. 3. М., Наука.
Adami, C., N. Cerf. (1999). What Informatiom Theory Can Tell Us About Quantum Reality. —In: Quamtum computing and quantim communications. New York, Springer.
Feynman, R. (1982). Simulating Physics with Computers. — International Journal of Theoretical Physics, Vol. 21, N 6—7.
Kleene, S. (1952). Introduction to metamathematics. Amsterdam, North-holland publishing.
Mahler, G., I. Kim. (1999). Correlation between correlations: Process and Time in Quantum Networks. — In: Quamtum computing and quantim communications. New York, Springer.
Williams, C., S. Springer. (1999). Explorations in quantum computing. New York, Springer.