

Доклад по квантова информатика

Тема: Квантови компютърни науки

Мартин Попов, ФН: 82134

I. Квантова информатика

Квантовата информатика е наука, която е доста скоро формирана. Тя все още се развива и тепърва се уточняват нейните основи. Явява се по-скоро цел и демонстрация на квантовата статистика, която сама по себе си е завършена още средата на XX век.

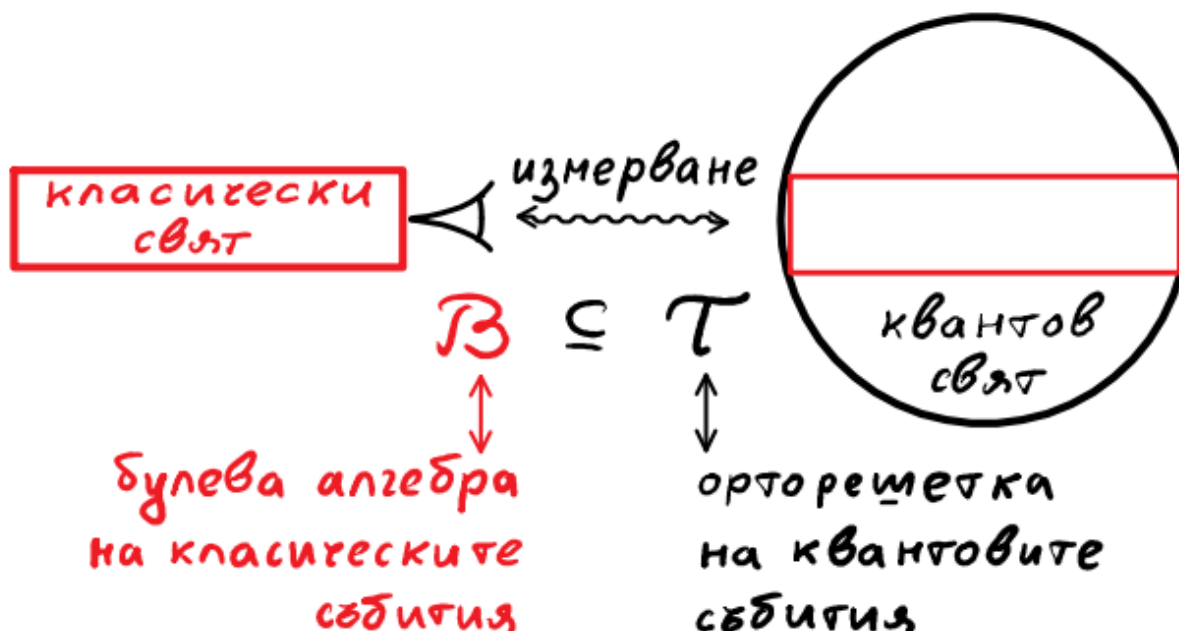
Квантовата информатика е област на изследване, която се занимава с прилагането на квантовата механика за обработка на информация. Съществуват два основни подхода към квантовата информатика: алгебричен подход и квантово-логически подход.

Алгебричният подход към квантовата информатика се основава на математическата рамка на алгебрата. При този подход квантовите състояния се представят чрез вектори в комплексно Хилбертово пространство, а квантовите операции се представят чрез линейни оператори. Алгебричният подход е подходящ за анализ на структурата на квантовите системи, както и за разработване на алгоритми за квантови изчисления.

Квантово-логическият подход, от друга страна, се основава на принципите на логиката. При този подход квантовите състояния се представят чрез логически съждения, а квантовите операции - чрез логически оператори. Квантово-логическият подход е подходящ за анализиране на семантиката на квантовите системи, както и за разработване на логически езици за изразяване и разсъждаване върху квантова информация.

Както алгебричният, така и квантово-логическият подход имат своите силни и слаби страни. Алгебричният подход е по-строг от математическа гледна точка, докато квантово-логическият подход е по-интуитивен и по-лесен за разбиране. В крайна сметка и двата подхода са необходими за пълното разбиране на квантовата информатика и изследователите в тази област използват и двата подхода, за да се справят с различните предизвикателства, които възникват при обработката на квантова информация.

Основната отличителна черта на квантовата теория е, че въвежда на аксиоматично ниво понятието за „наблюдател“, посредством понятието „наблюдаема“ и аксиомата за измерването на наблюдаеми (проекционния постулат).

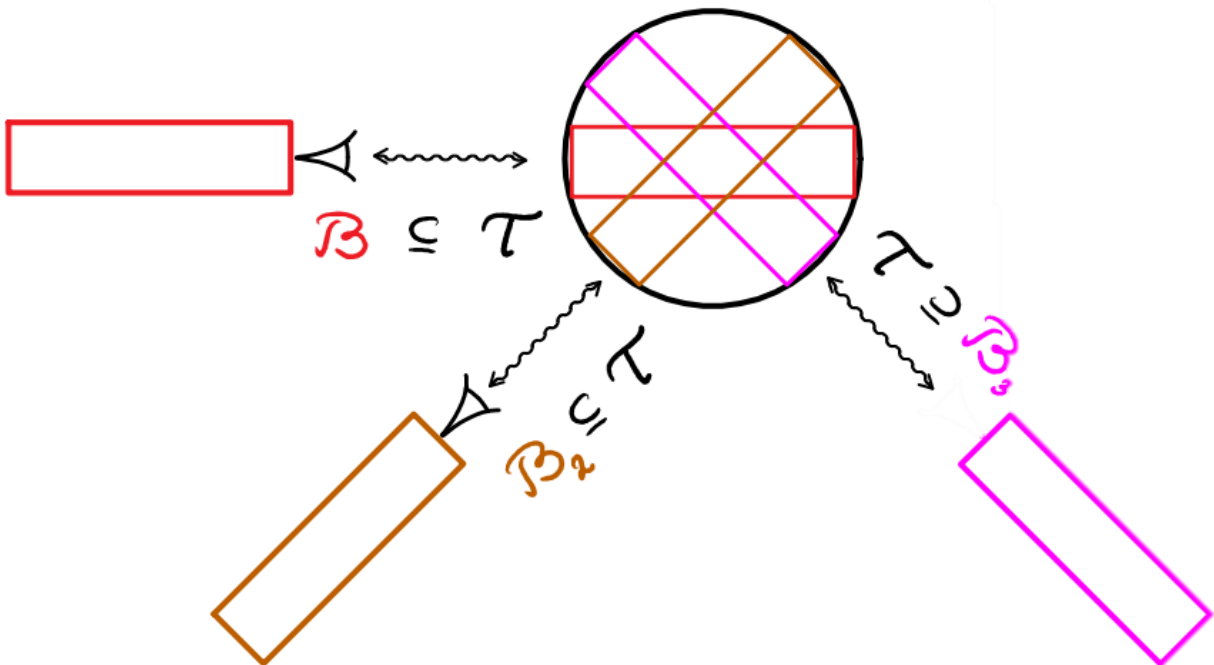


Самият процес на измерване представлява влагането на булевите събития, които съответстват на това измерване в орторешетката на всички квантови събития.

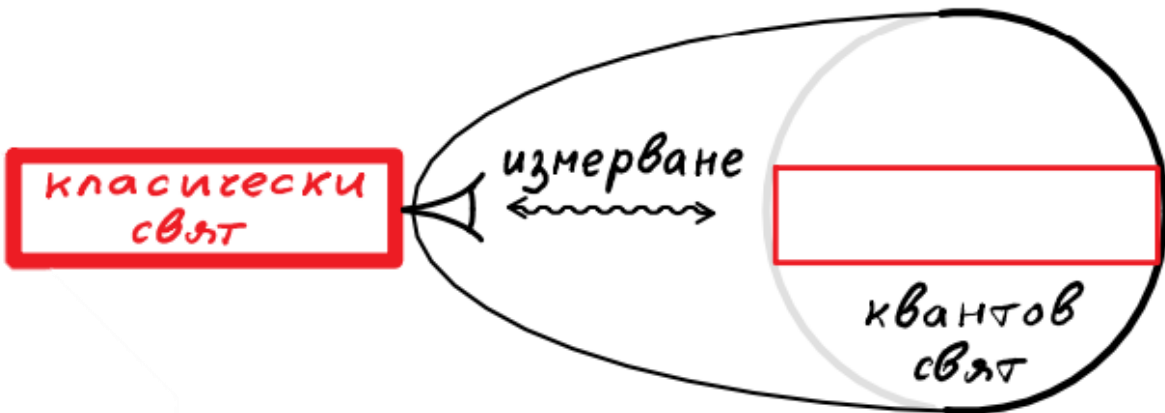
Орторешетката е частично подредено множество, което отговаря на определени свойства в булевата алгебра. По-конкретно, орторешетката е решетка, в която всеки елемент има допълнение и е в сила дистрибутивният закон.

Ортографските решетки са важни в булевата алгебра, тъй като осигуряват математическа рамка за изучаване на структурата на логическите системи, като например тези, използвани в цифровите схеми и компютърното програмиране. Те са важни и при изучаването на квантовите изчисления, където се използват за моделиране на квантови операции и манипулиране на квантови битове (кюбити).

В класическата физика измерването е „безобидно“. Можем да игнорираме наблюдателя, но в квантовия свят, извличането на информация има неконтролируемо въздействие върху него, изпращайки го в различни състояния с различни вероятности.



Различните гледни точки представят различни квантови събития, които обаче са само една част от общото цяло. Понеже множеството на всички квантови събития (ортотрешетката) не е булева алгебра, не можем да я покрием с такава рамка, понеже има събития, които не изпълняват дистрибутивния закон и не могат да попаднат в нея.



Можем да присъединим към квантовото описание и измервателния прибор, както и самия измервателен процес. Винаги обаче ще остане класическата „проекция“, в която отчитаме резултата от измерването.

Има възможност за преплитане на измервателния уред с квантовия свят и тук възниква и въпросът, дали е нужно да въвеждаме изобщо „измерване“. По принцип, това е финален етап в квантово-теоретичното описание, след което то се „рестартира“ (прекръпява) съгласно проекционния постулат. Тоест акта на измерване прекръпява квантовата еволюция на системата и я рестартира. Ако го няма обаче този акт на измерване

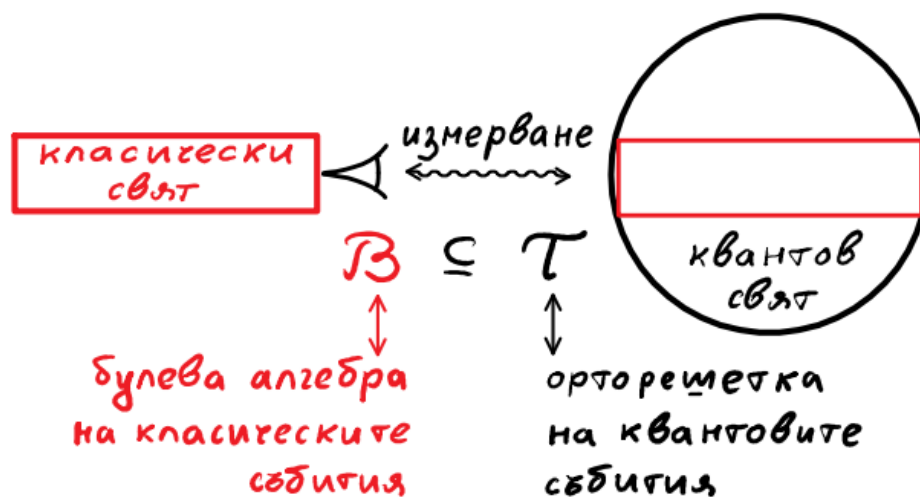
получаваме парадокси, като този с котката на Шрьодингер, която е в чисто състояние на суперпозиция на „жива“ и „умряла“.

Проблеми в областта:

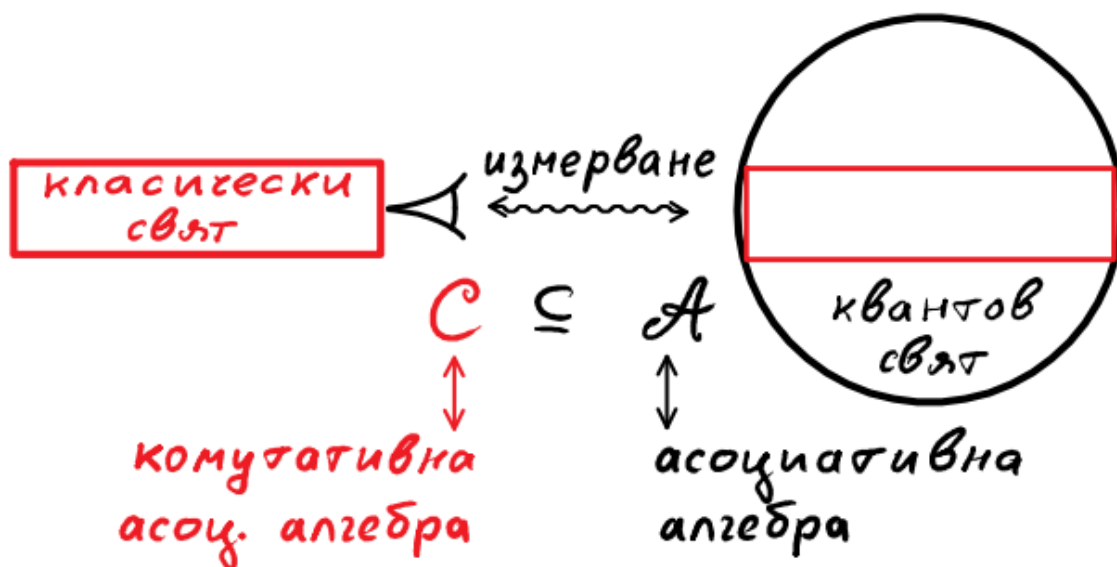
1. В „квантовата космология“: В затворените системи, като Вселената - като цяло, няма външен наблюдател. Днес обаче наблюдаваме класически макрообекти (хората, планетите, галактиките, звездите). Възниква въпросът как е станала проекцията и кой е бил в ролята на наблюдател. Трябва да е станало някакво измерване в някакъв момент, но не знаем кога е станал. Когато се е случило това, всички обекти са в ролята на котката на Шрьодингер, която може да я има в различни състояния, докато някой не установи какво всъщност се случва.
2. Квантовата гравитация: Тя не се покрива от квантовата теория, главно поради нововъведеното понятие за наблюдател. Постигането на такава теория изисква пространството и времето да се потопят в „квантовия свят“. Пространството и времето обаче са неотменна част и на „класическия свят“. По отношение на времето, ние имаме усещане за това кое е причина и кое е следствие. Ако това го потопим в „квантовия свят“, то тогава има известна вероятност причината и следствието да си сменят местата, тоест причината да е следствие и обратното. В някакъв смисъл причината и следствието съществуват в квантова суперпозиция. Затова ние не можем да си го представим как трябва да се случи това.

II. Теория на категориите

Квантовата теория се основава на водещата роля на „наблюдателя“: - в логическия подход страната на наблюдателя се определя от орторешетката на събитията. Тук експериментите и отделните класически гледни точки са булеви алгебри.



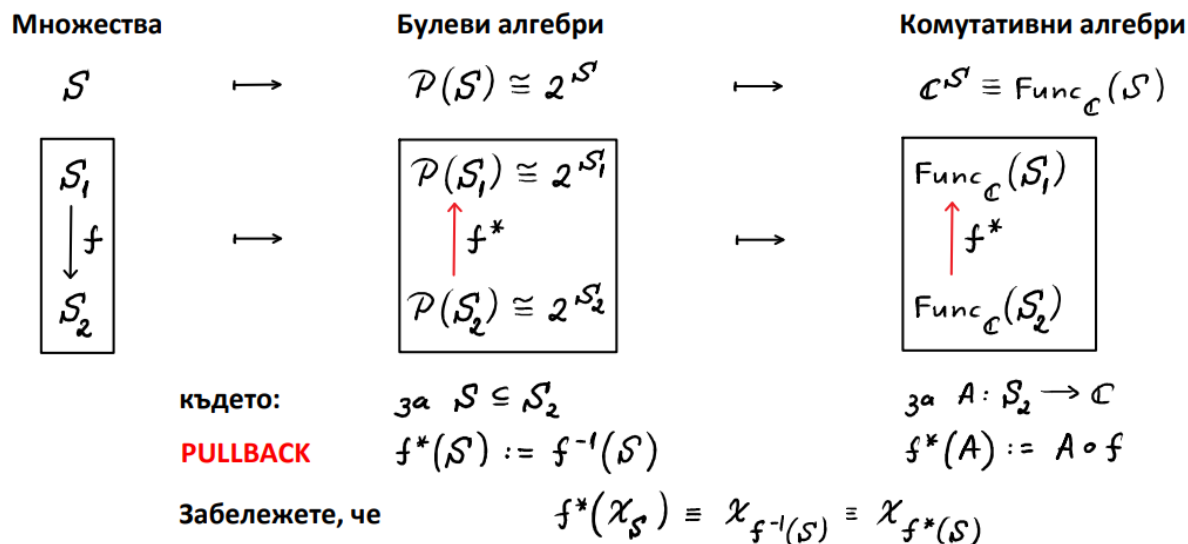
В алгебричния подход страната на наблюдателя се определя от алгебрата на наблюдаемите. Тук експериментите и отделните класически гледни точки са комутативни асоциативни алгебри.



Страната на изследвания обект се задава със състоянието на системата. Състоянията на системата е всъщност какъв „вероятностен отклик“ дава изследваната система при нашите измервания. Оттук в частност следва, че състоянията са такива функции върху алгебрата на наблюдаемите, които след като се ограничат до всяка комутативна подалгебра могат да се интерпретират като средни стойности на наблюдаеми в класическа статистика.

Алгебричният подход може да се прилага и в класическия свят. Това се основава на следните „категорни“ еквивалентности:

Имаме съответствия между множества, булеви алгебри и комутативни алгебри. Те формират някакви категории, които можем да гледаме като типове (видове) на математически структури.



На S съпоставяме булевата алгебра на неговите подмножества 2^S . Тоест на всяко множество му съответства една булева алгебра, но на него му съответства и една комутативна алгебра, например алгебрата на всички функции с комплексни стойности върху това множество S .

Имаме такива съответствия между обектите в тези категории. Освен това се говори и за трансформации (морфизми) между обектите.

Ако имаме едно изображение $f: S_1 \rightarrow S_2$, то при преноса му в булеви и комутативни алгебри имаме нови изображения, които са в обратна посока.

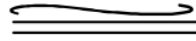
Тоест ако имаме подмножество на S_2 то се изтегля назад с ко-образа си. Това е морфизъм на орторешетки с 0-ла и 1-ца. Що се отнася до езика на функциите, изтеглянето е композиция с функцията.

Точното понятие за категория включва клас на обектите на категорията и клас на морфизмите на категорията. Горните съответствия между различни категории са примери за така наречените „функтори на категории“. Тези съответствия правят категориите еквивалентни.

Идеята на категорния подход е да се научим да работим категорно в „класическия свят“ и като сменим категорията да получим същите дефиниции и в „квантовия свят“.

Множества

FinSet



Комутативни алгебри

FinComAlg **opposite**

На тази еквивалентност (в малко по-общ вид) се основава „алгебричната геометрия“.

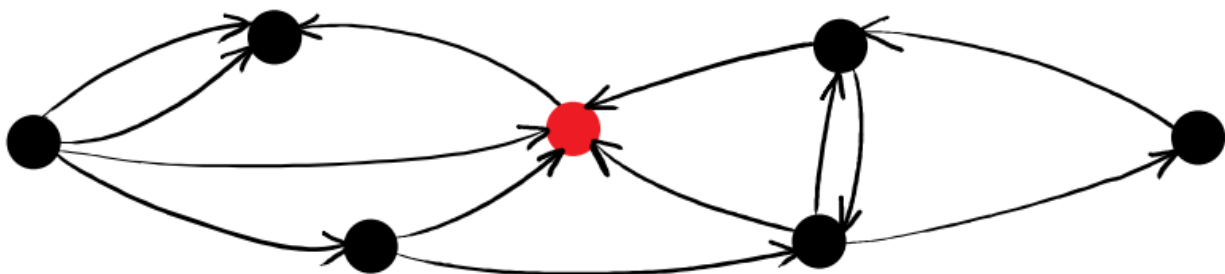
Ако заменим категорията на комутативните алгебри с некомутиативните - получаваме така наречената „некомутиативна геометрия“. Във физиката това съответства на преход към „квантовия свят“.

За съжаление, категорията на некомутиативните алгебри не е толкова богата, колкото категорията на множествата. В последните десетилетия има опити към квантовия свят да се приложи обобщен вариант на категорията на множествата, наречен „теория на топосите“.

Аксиоматична дефиниция на категория: Тя се състои от два класа обекти

1. обекти на категорията
2. стрелки на категорията
3. операция, която на всяка стрелка съпоставя два обекта: начало (domain) и край (codomain) на стрелката: $f: a \rightarrow b$
4. операция, която за всяка двойка от стрелки f и g със съвпадащи начало и край да имаме композиция: $f: a \rightarrow b, g: b \rightarrow c, g \circ f: a \rightarrow c$
5. на всеки един обект е съпоставена уникална стрелка, наречена единична стрелка, която е идентитета

Идейно, при категорния подход обектите с тяхната структура се задават не сами по себе си, а в отношението спрямо останалите обекти, посредством стрелките („трансформациите“) между тях.

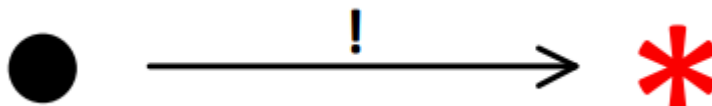


Аналогично, всяка стрелка се определя не сама себе си, а посредством структурата на абстрактните композиции между тях. Това води до понятието комутативна диаграма, което се използва за въвеждането на такива взаимоотношения между обектите. Това са графи, където стрелките са ребра, а върховете са обектите на категорията.

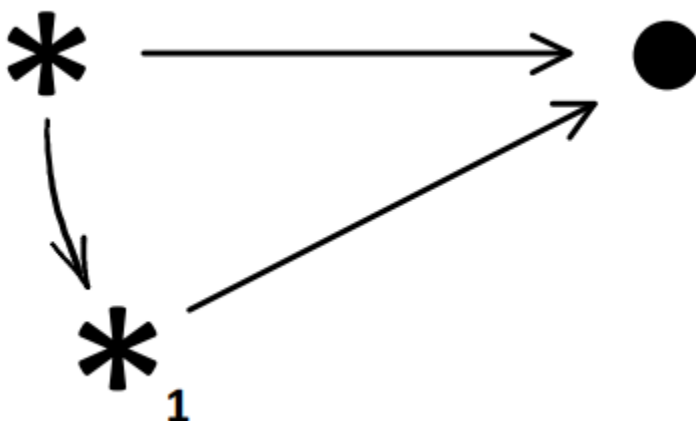
Някои примери:

- „синглетон“ (едно-елементно множество) има следната категорна характеристика: това е такъв обект, че за всеки друг обект съществува една-единствена стрелка към него.

Наричат се терминални обекти.



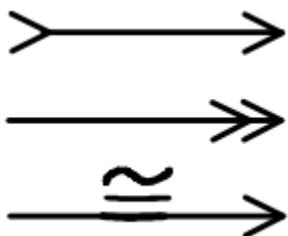
- „елемент“ на обект е всяка стрелка от терминален обект към него. По този начин ние посочваме вътре обекта. Ако имаме две такива стрелки, то те са един и същ елемент, ако има преход от единия обект към другия.



- моно-стрелки („инекции“): съкратимост от ляво („отзад“) при композиция - категорен аналог за понятието „инекция“. Една стрелка е моно-стрелка, ако винаги, когато се композира отляво дава един и същ резултат. $f: A \rightarrow B$; $g, h: X \rightarrow A$, Ако $f \circ g = f \circ h$, то $g = h$

- епи-стрелки („сюрекции“): съкратимост от дясно („отпред“) при композиция

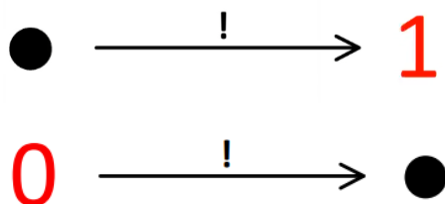
- изо-стрелки („биекции“): двустранна обратимост



- Внимание: в обща категория - изо \neq моно & епи (!!!); за топоси обаче това се доказва.

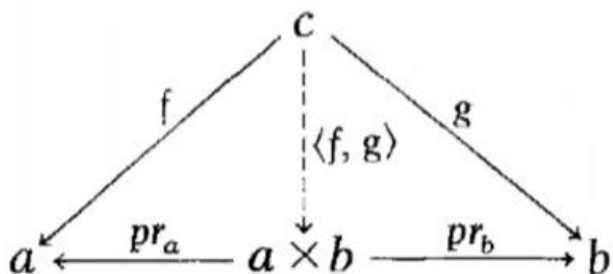
В теорията на категориите възниква следното понятие за „дуалност“. Това е обръщането на посоките на стрелките в една конструкция или определение. Например: моно и епи-стрелките са взаимно дуални обекти, а изо-стрелките са самодуални.

Дуалното понятие на терминален обект е понятието за „начален обект“ (обект „0“) Ако имаме понятието за терминален (краен) обект, означен с 1-ца, то като обърнем посоката на стрелката получаваме начален обект, от който във всеки друг обект има само една стрелка:



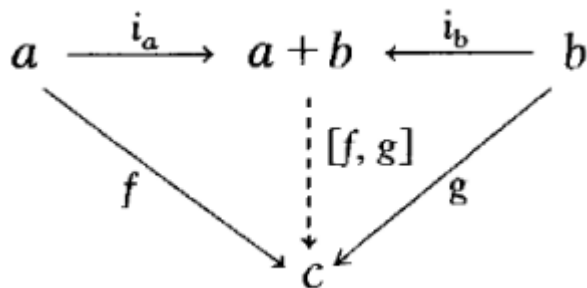
В категорията на множествата: Началният обект (0-ла) = \emptyset - празното множество.

- обект-произведение: В категорията на множествата, обектите-произведения са декартовите произведения на множества и те имат самостоятелен смисъл и в тяхната конструкция са „вградени“ изходните множества. От гледна точка на теория на категориите обектът-произведение няма нито самостоятелен смисъл и конструкция.



Обектите-произведения имат смисъл и еднозначност (с точност до единствен изоморфизъм) единствено, когато са взети заедно с „привързващите“ ги стрелки pr_a и pr_b .

- обект-ко-произведение: Дуалното понятие на произведението е ко-произведението:



В категорията на множествата ко-произведението е дизюнктивното обединение.

III. Квантово програмиране

Квантовото програмиране е бързо развиваща се област в пресечната точка на компютърните науки и квантовата механика. Тя включва разработването на софтуерни приложения, които използват уникалните свойства на квантовата механика, като суперпозиция и преплитане, за решаване на сложни проблеми по-ефективно от класическите компютри.

Едно от основните предизвикателства пред квантовото програмиране е присъщата на квантовите системи сложност, която бързо може да стане непосилна дори за малък брой кубити. Това е довело до разработването на рамки за квантово програмиране от високо ниво, които предоставят абстракции, опростяващи разработването на квантови алгоритми.

Въпреки предизвикателствата, квантовото програмиране има потенциала да революционизира много области, включително криптографията и машинното обучение. Например, доказано е, че квантовите компютри са в състояние да разбият много често използвани алгоритми за криптиране, като RSA, които разчитат на трудността на факторизацията на големи числа.

Квантовото функционално програмиране е сравнително нова област на изследване, която се стреми да приложи концепции от функционалното програмиране, като например ламбда-смятане, към квантовите изчисления. Във функционалното програмиране програмите се изграждат с помощта на функции, които приемат входни данни и произвеждат изходни данни, без странични ефекти или променливи. Това улеснява обосноваването на поведението на програмите и доказването на тяхната коректност.

По подобен начин в квантовото функционално програмиране квантовите схеми се конструират с помощта на квантови операции, които трансформират квантови състояния, без междинни измервания или класически контрол. Това позволява разработването на програми, които могат да бъдат по-лесно анализирани и оптимизирани и могат да се възползват от присъщия на квантовите системи паралелизъм и преплитане.

Ламбда-смятането, което е формална система за изразяване на функции и оценяване на изрази, е особено влиятелно в квантовото функционално програмиране. То може да се използва за описание на квантови вериги и операции по начин, който е удобен за формален анализ и оптимизация.

IV. Заключение

Квантовото функционално програмиране е все още сравнително зараждаща се област и има много отворени изследователски въпроси и предизвикателства, които трябва да бъдат разгледани. Въпреки това, тъй като квантовите изчисления продължават да се развиват и стават достъпни по-мощни квантови компютри, потенциалните приложения на квантовото функционално програмиране ще продължат да нарастват.