楽しい数学 第四夜

「同じ」を考える――「型の理論入門」

Vladimir Voevodsky
1966-2017

There is no such thing as Two Individuals indiscernible from each other.

Two Drops of Water, or Milk, viewed with a Microscope, will appear distinguishable from each other..

This is an Argument against Atoms; which are confuted, as well as a Vacuum, by the Principles of true Metaphysicks.

-- Leibniz

The univalent model satisfies a new axiom which is called the univalence axiom. It imposes the condition that the identity type between two types is naturally weakly equivalent to the type of weak equivalences between these types.

-- Voevodsky

Sooner or later computer proof assistants will become the norm, but the longer this process takes the more misery associated with mistakes and with unnecessary self-verification the practitioners of the field will have to endure.

-- Voevodsky

はじめに

- 「同じ」あるいは「同じではない」という判断は、知覚にとっても認識にとっても、最も基本的な判断の一つである。認識の対象が、自然であれ、人間であれ、あるいは、思惟が産み出す抽象的な概念であれ、その認識の土台には、対象の「同一性」についての判断があるように思う。
- 小論の第一部では、まず、日常の生活の中にも現れる「同じ」をめぐる問題を、いくつかのサンプルで考えてみようと思う。その後で、「哲学者」たちが、こうした問題をどのように考えていたのかを、きわめて簡単に振り返ろうと思う。
- 残念ながら、小論は、「同一性」についての、「哲学的」議論を紹介することを目的とはしていない。ただ、第一部での議論を通じて、日常の中にも、浅からぬ哲学への入り口が存在していることを意識することを楽しんでもらえれば嬉しいと思う。

はじめに

- 小論の第二部では、20世紀の科学が、すくなくとも自然認識の領域では、「同一性」概念の大きな変化を引き起こしたことを述べようと思う。
- 相対論は、宇宙規模の巨大な空間では、時間の「同時性」が成り立たないことを示し、量子論は、極めて微小な領域では、すべての物質と力は、「同じ」性質を持つ不断に変化する素粒子の運動として記述できることを示した。同時に、両者ともに、その法則性は、ある種の「不変性」として記述される。
- 物理的な「同一性」は、基本的には「情報」の「同一性」として表現されるのだが、この分野でも、量子情報理論の発展は、エンタングルメントや量子テレポーテーションといった、「同一性」にかかわる思いがけない知見を我々にもたらしている。

はじめに

- 小論の第三部は、数学での「同一性」にまつわる議論を、「型の理論」の成立と発展を中心に概観したものである。
- 「型の理論」は、20世紀初頭のラッセルに始まる。40年代のチャーチの「型付きラムダ計算」を経て、70年代には、マーティン・レフの「従属型理論」として発展してきた。その理論は、「関数型言語」の成立に大きな影響を与えた。
- 21世紀に入ってから、この分野は、ヴオェボドスキーの「ホモトピー型理論」の登場によって、大きな飛躍を遂げる。彼がこの理論の基礎に置いた “Univalent Axiom” は、「同一性」についての新しい原理に他ならない。それは、数学の基礎そのものについての新しい洞察を可能にするものであった。
- 彼が、この理論の展開をすべてコンピュータを使った証明支援システム上で行なったことは、特筆に値する。

Agenda
「同じ」を考える--「型の理論入門」

- **Part I**
  「同じ」について考えてみよう
- **Part II**
  物理学と同一性
- **Part III**
  数学と同一性　– 型の理論入門

Part I Agenda
「同じ」について考えてみよう

- 「同じ」について考えてみよう
- 哲学者たちが考えたこと
  - ユークリッド幾何学の公理
  - プラトンの「観念実在論」
  - 中世哲学 「普遍論争」
  - ライプニッツ 「不可識別者同一の原理」
  - ヘーゲル 「同一性と非同一性の同一性」
  - ヴィトゲンシュタイン
  - 般若心経

Part II Agenda
物理学と同一性

- 相対性理論と「同時性」
- 量子論と「同一性」
- エンタングルメント
- 量子情報理論と「同一性」

Part III Agenda
数学と同一性

- Leibniz -- 不可識別者同一の原理
- Russell -- 集合論の逆理と型の理論
- Church -- 型を持つラムダ計算
- Curry-Howard対応 --型付きラムダ計算と論理との対応
- Martin-Löf -- Dependent Type Theory
- Voevodsky -- Homotopy Type Theory

Part I

「同じ」について考えてみよう

君が、10年前にイメージした「三角形」は、いま
僕がイメージした「三角形」と同じだろうか？

君の10年と僕の10年は、同じ10年だろうか？

10年前の君と、いまの君は、同じだろうか？

君にとって君であること、
君のアイデンティティは何？

「性同一性障害」という考え方を、今はとらないのだが、それはなぜだろう？

未来の人工知能は、
人間と同じ何かを作り出すだろうか？

哲学者たちが考えたこと

ユークリッド幾何学の公理

1 同じものに等しいものはまた互いに等しい。
2 また、等しいものに等しいものが加えられれば全体は等しい。
3 また、等しいものから等しいものが引かれれば残りは等しい。
〔4 また、不等なものに等しいものが加えられれば全体は不等である。
5 また、同じものの2倍は互いに等しい。
6 また、同じものの半分は互いに等しい。〕
7 また、互いに重なり合うものは互いに等しい。
8 また、全体は部分より大きい。
〔9 また、2直線は面積を囲まない。〕

プラトンの「観念実在論」

「地下の洞窟に住んでいる人々を想像してみよう。明かりに向かって洞窟の幅いっぱいの通路が入口まで達している。人々は、子どもの頃から手足も首も縛られていて動くことができず、ずっと洞窟の奥を見ながら、振り返ることもできない。入口のはるか上方に火が燃えていて、人々をうしろから照らしている。火と人々のあいだに道があり、道に沿って低い壁が作られている。……壁に沿って、いろんな種類の道具、木や石などで作られた人間や動物の像が、壁の上に差し上げられながら運ばれていく。運んでいく人々のなかには、声を出すものもいれば、黙っているものもいる。」

「Republic: Book VII, 514a- 521d」
https://goo.gl/Fzv2XR

プラトンの「観念実在論」

- 「洞窟の喩え」で、影を生み出しているのは「形相（エイドス）Form」と呼ばれるものである。光・太陽にあたるのは「ロゴス」である。
- プラトンは、真実の実在の世界は、日常的に感覚される世界を超えたものであると考える。我々が、我々のまわりに感じるものは、その真実の世界の影に過ぎない。
- 我々の世界は、常に変化し、その変化を感覚で知るに過ぎない。真実の実在の世界は、我々の住む世界の他にある。
- その真実の世界は、変化することもなく永遠である。そこは感覚の世界ではなくイデア（観念）の世界であり、我々がこの地上で知っているものの、完全な形相が存在する世界である。
- 数学の対象（数や三角形）は、この形相の世界に存する。

中世哲学　普遍論争

□ 実在論

「アンセルムスなどの実在論者は、普遍概念は存在するとし、何ものかが明らかでない個物の基体存在物に、例えば「人間」の形相が付与されることで、すなわち「人間の普遍概念」が基体存在に加わることで、簡単に云えば、「人間の具体的存在」すなわち「個物としての人間」が成立するとした。このように、類の概念、すなわち普遍概念が実在するとする考えを、「実念論」または「実在論（Realismus）」と呼ぶ。」

https://goo.gl/XUrwWz

中世哲学　普遍論争

□ 唯名論

「これに対し、オッカムのウィリアムなどの唯名論者は、人間の類の概念、すなわち「人間の普遍概念」は形相的に実在するのではなく、古代のアリストテレスが考えたように、実在するのは具体的な個々の個物であるとした。つまり、人間のミケーレや犬のフェリスや柏の巨木が、個物（レース）として実在しているのである。このとき、「普遍概念」は、類を示す「名前（羅： nomen）」であり、名前は「言葉」として存在するが、類の概念、すなわち普遍概念としての形相的存在は実在しないとした。」

https://goo.gl/XUrwWz

ライプニッツ　不可識別者同一の原理

- 二つの個体で、互いに識別不能だというようなものは存在しない
- これらの偉大な原理、充足理由の原理と不可識別者同一の原理は、形而上学の状態を変える
- 二つのものが識別できないと考えることは、同じものが二つの名前のもとにあると考えることだ

- *Space is only an Order of things, as Time also is,*

"An Answer to Dr. CLARKE*'s Third Reply"*
https://goo.gl/7sgJPX

ヘーゲル　同一性と非同一性の同一性

- あるものが自己同一的であるというのは、それが同時に非同一的、すなわち自分自身と異なっている場合にのみ意味がある。同一性は、同一性と非同一性の同一性である。

「フィヒテとシェリングの哲学体系の差異」
https://goo.gl/UCiboL

ヴィトゲンシュタイン

- 大雑把にいえば、二つのものが同一だと言うのは無意味だ。一つのものが自分自身と同一だと言うのは、何も言ってないのに等しい。

「論理哲学論考」 5.5303

https://goo.gl/Zsf4Za

般若心経

- 色即是空
  「「色」は、宇宙に存在するすべての形ある物質や現象を意味し、「空」は、恒常な実体がないという意味。」
  日本語wiki https://goo.gl/6xR1wz

- 英訳では、「色」は、”Form”と訳されている。これは、プラトンの「形相」＝イデア と同じ言葉である。

  Form itself is emptiness; emptiness itself is form.

Part II

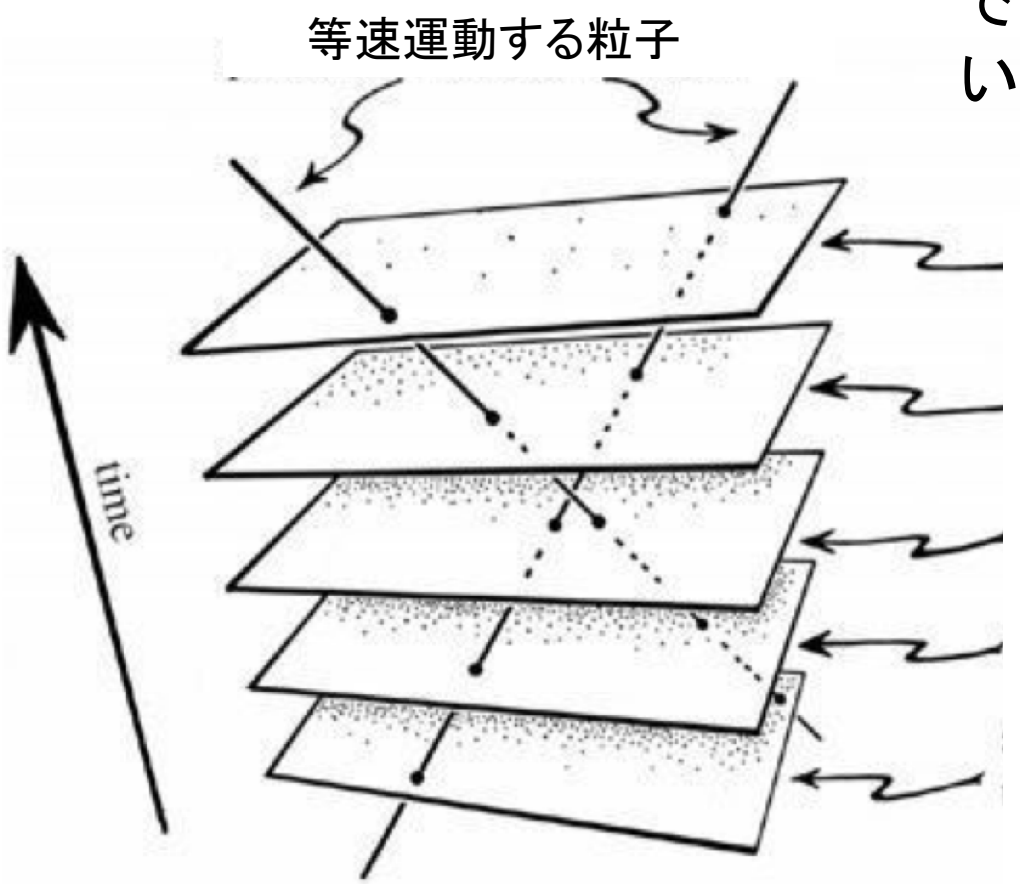
物理学と同一性 – 相対論と量子論

Part II Agenda
物理学と同一性

- 相対性理論と「同時性」
- 量子論と「同一性」
- エンタングルメント
- 量子情報理論と「同一性」

相対性理論と「同時性」

空間は、「同時刻の空間」で、平行にスライスされている。



あさって、正午の空間

明日、正午の空間

今日、正午の空間

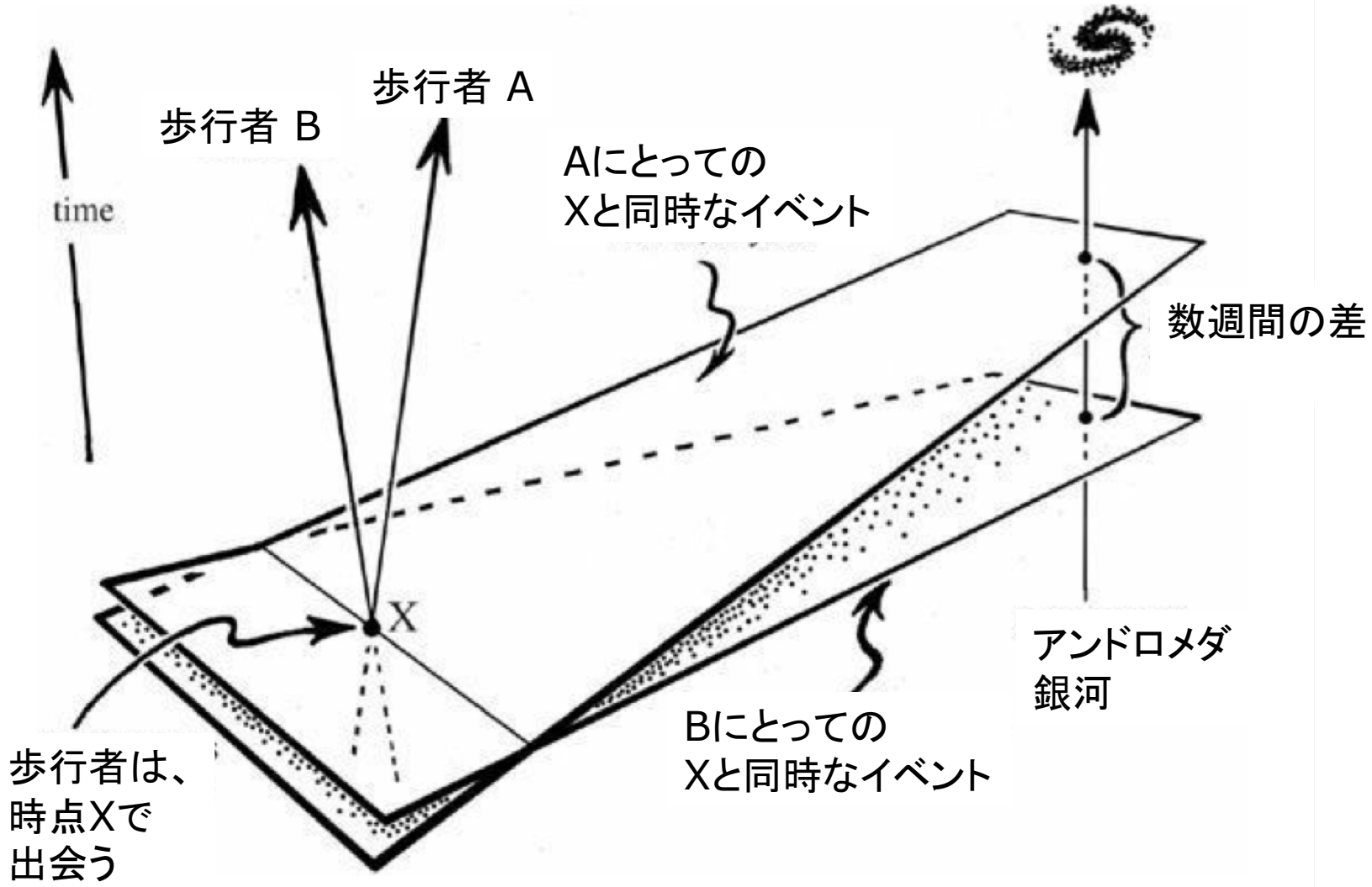
昨日、正午の空間

一昨日、正午の空間

ミンコフスキー以前の時空像

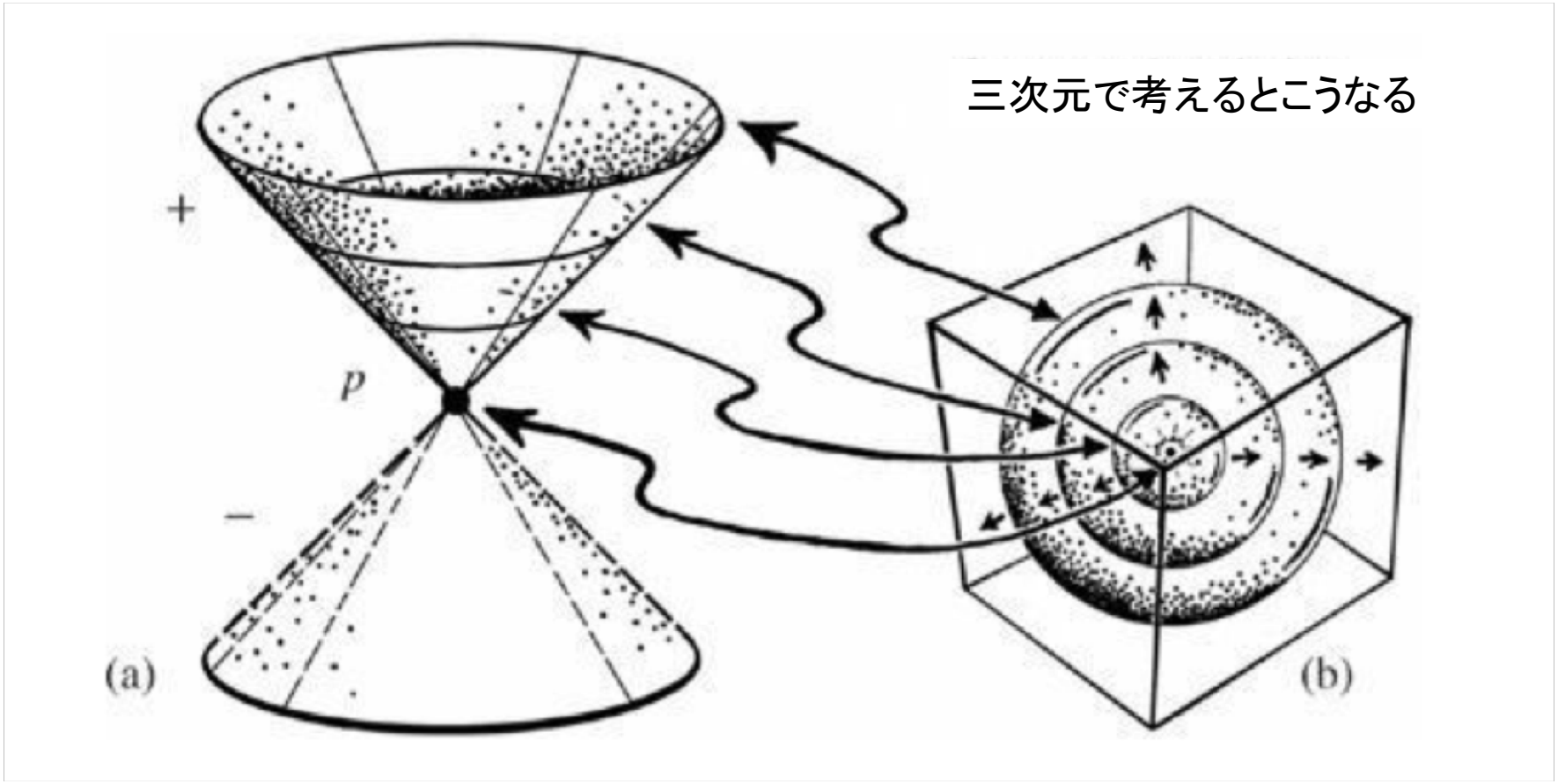
Penrose “Cycle of Time” https://goo.gl/RBYi5T

歩行者のスピードによって、「同時刻の空間」は、ことなる。



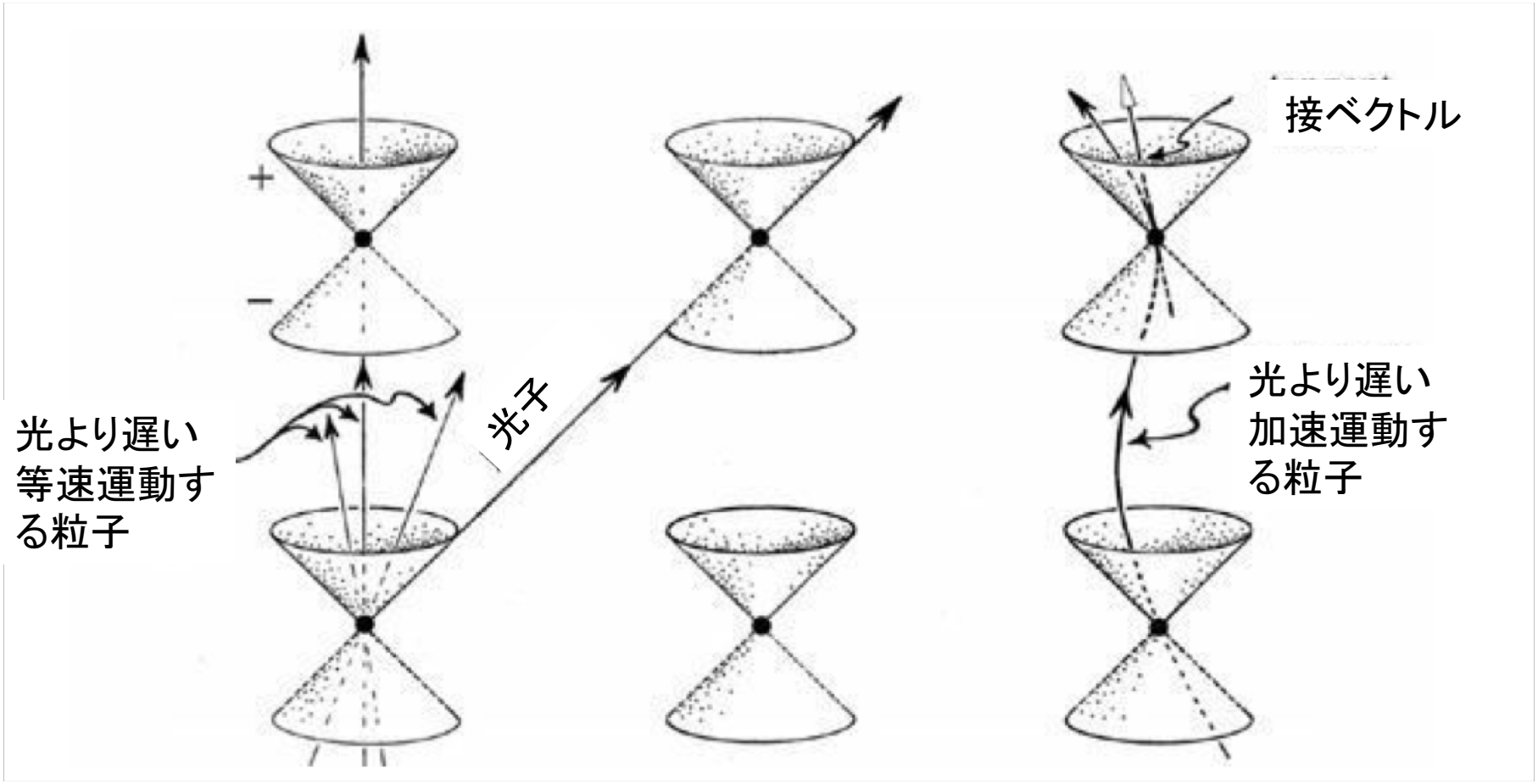
ミンコフスキー空間で二人の歩行者が出会う

Penrose “Cycle of Time” https://goo.gl/RBYi5T



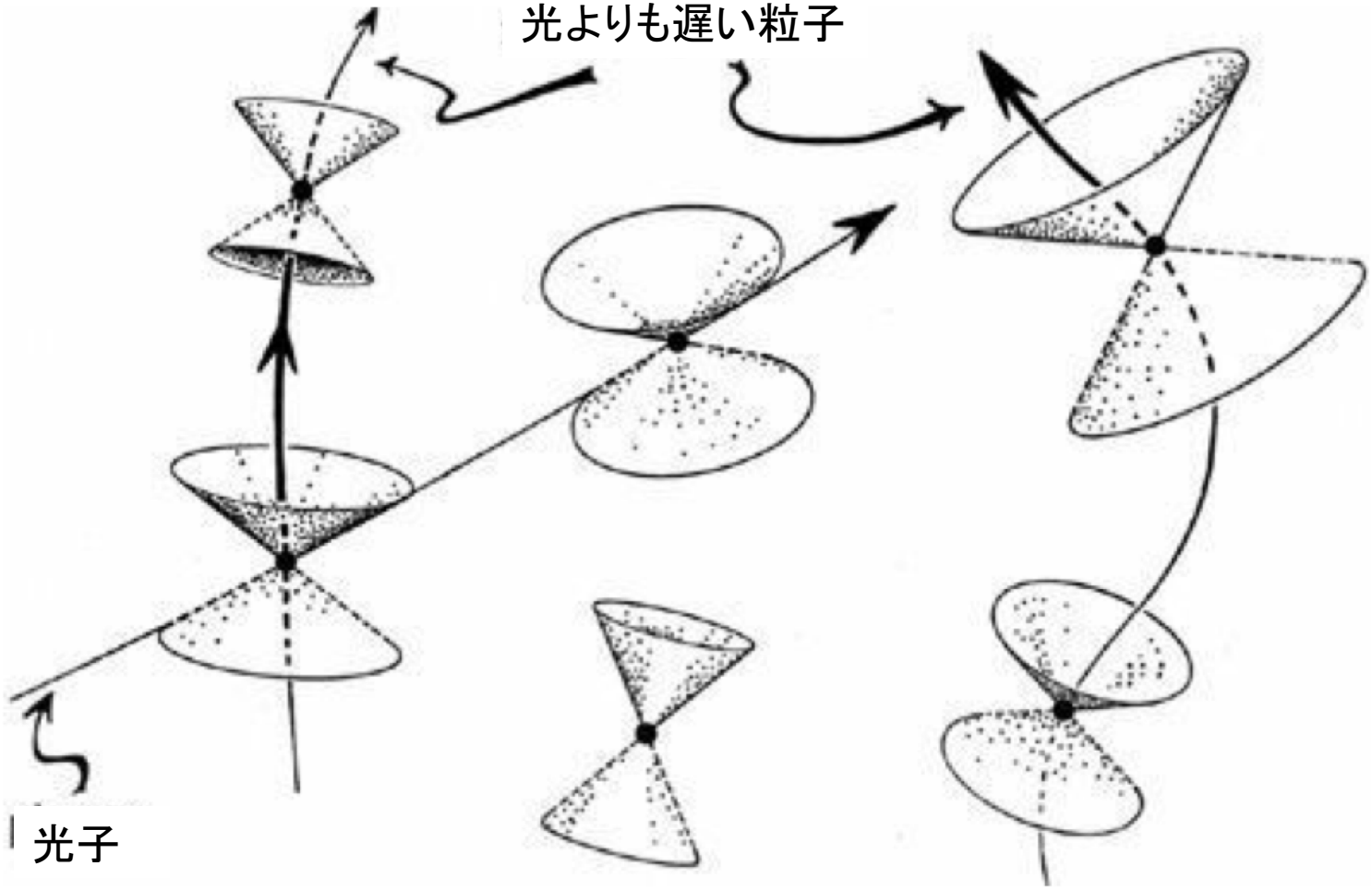
ミンコフスキー空間 pでの光円錐（Null cone）

Penrose “Cycle of Time” https://goo.gl/RBYi5T



ミンコフスキー空間の各点に
一様に置かれた光円錐（たいらな時空）
特殊相対論

アインシュタインは、時空の各点に時計を置いた



ミンコフスキー空間の各点に
非一様に置かれた光円錐（曲がった時空）
一般相対論

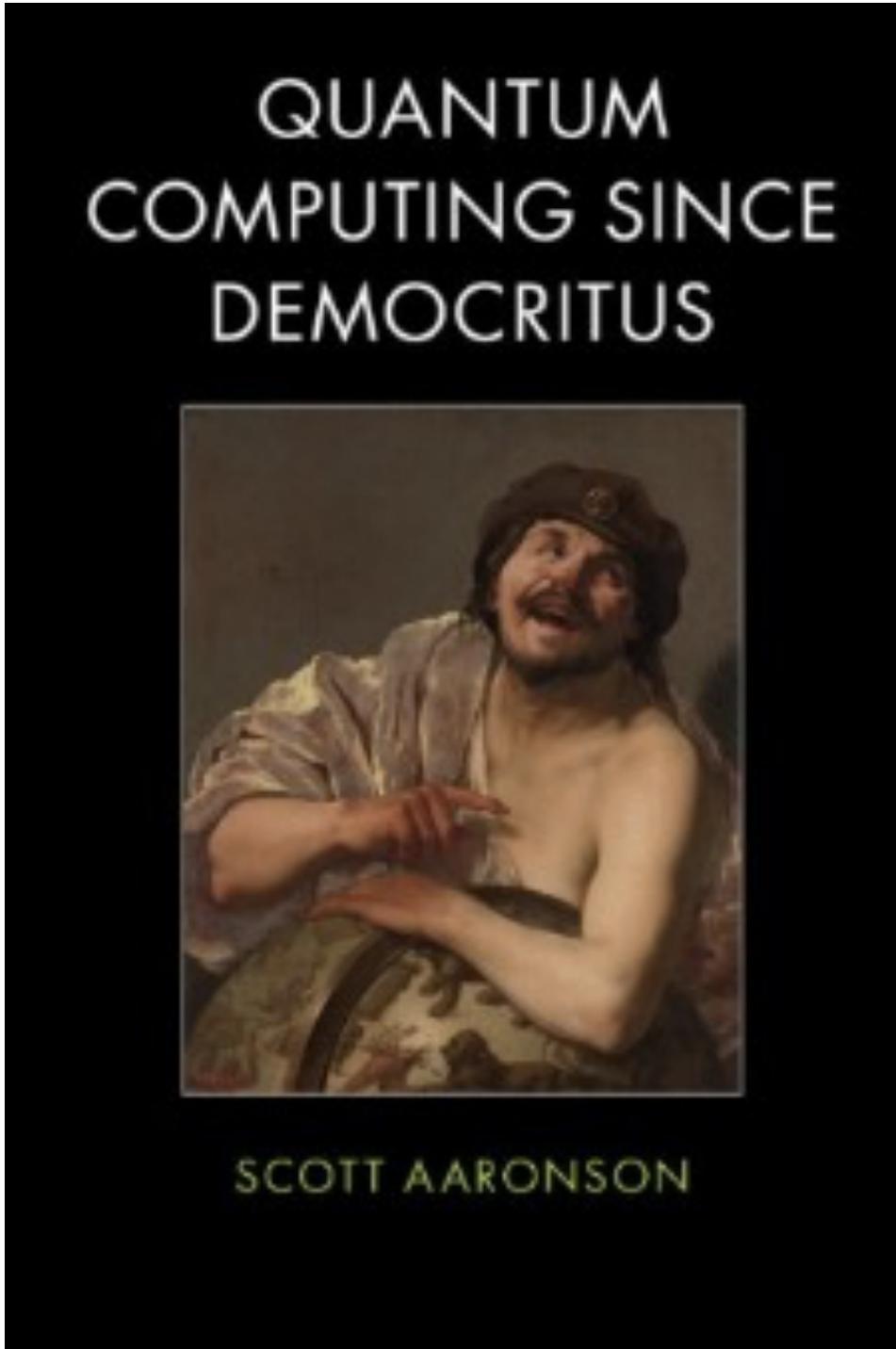
量子論と「同一性」

異端の学説　原子論

- 古代ギリシャで原子論を提唱したデモクリトスの著作を、プラトンは、全部、焼かせたという。
- 「しかし、そのこと〔粒子の偶然の衝突で宇宙が誕生したということ〕が起こりえたと考える者は、どうして次のことに考えが至らないのか、わたしは理解に苦しむ。すなわち、黄金製であれ何であれ、二十一種類のアルファベットの文字を数えきれないほど集めて何かある容器の中に投げ込み、それらを攪拌して地面に投げ出すと、たとえばエンニウスの『年代記』のように、読者にとってちゃんと読める形になって並ぶとはどうして考えないのか。もっとも、わたしは、幸運の助けを借りたとしても、たった一行の詩句さえまともにできるかどうか、いぶかしく思っているのだが。」 これは、3世紀のキケロの原子論批判。
- これは、「猿のタイプライター」の論理だ！

https://ja.wikipedia.org/wiki/無限の猿定理

Scott Aaronsonは、自書
“Quantum Computing Since Democritus”
「デモクリトス以来の量子コンピューティング」の表紙をデモクリトスで飾った



ライプニッツの不可識別性の議論は、原子論・真空に反対するための議論だった

There is no such thing as Two Individuals indiscernible from each other.

An Ingenious Gentleman of my Acquaintance, discoursing with me, in the presence of Her Electoral Highness the Princess Sophia, in the Garden of Herrenhausen; thought he could find two Leaves perfectly alike. The Princess defied him to do it, and he ran all over the Garden a long time to look for some; but it was to no purpose.

Two Drops of Water, or Milk, viewed with a Microscope, will appear distinguishable from each other..

This is an Argument against Atoms; which are confuted, as well as a Vacuum, by the Principles of true Metaphysicks.

-- Leibniz

19世紀でも、原子の存在は、疑われていた

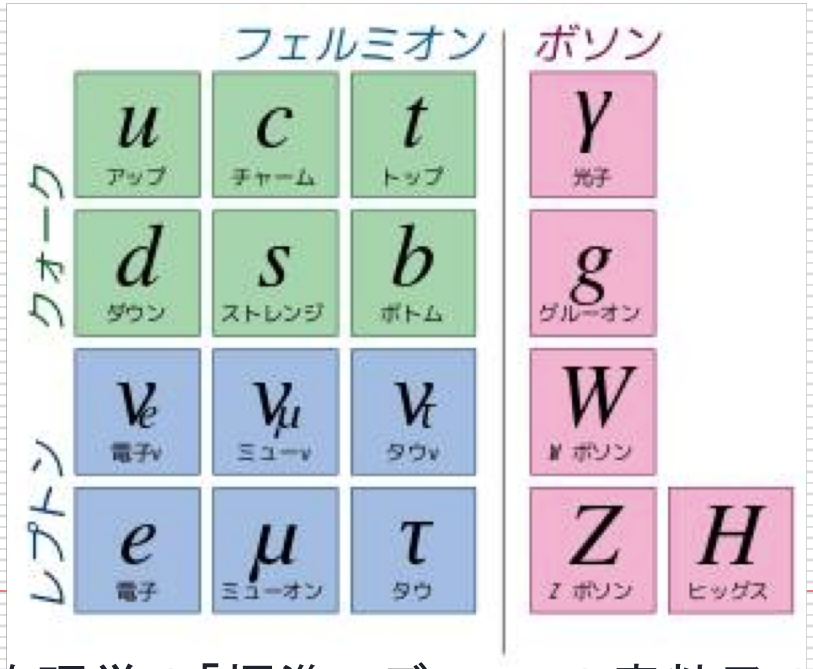
- ボルツマンは、日本でいえば、江戸時代末期に生まれ、明治維新の頃に論文を書いていると思っていい。
- ただ、原子論が、科学の世界で広いコンセンサスを得るのは（化学の世界では、原子論は、早くから受け入れられていたようなのだが）、1905年の、アインシュタインの「ブラウン運動」についての論文以降だった。
- 19世紀の物理学でも、「原子論」は「異端」の学説だったらしい。

ボルツマンの悲劇

- 19世紀の物理学者の双璧は、ボルツマンとマックスウェルだと思うが、二人のアカデミーでの人生は、はっきりと明暗を分けている。
- 紹介したサスキンドの発言は「悪い冗談」なのだが、ボルツマンの業績は、彼の生前には正当に評価されなかった。特に、当時の物理学会で大きな発言力を持っていたマッハとその取り巻きは、執拗にボルツマンの「原子論」を攻撃した。ボルツマンは、追い詰められ、次第に精神を病んでゆく。
- アインシュタインの画期的な論文「熱の分子論から要求される静止液体中の懸濁粒子の運動について」が出たのは、1905年5月である。ボルツマンも、この20代の若者の論文を読んだと思うのだが。
- 翌1906年、彼は、自ら命を絶つ。

素粒子論は、現代の原子論に他ならない

- 物理現象を、より基本的な要素の実在とその運動で説明しようというのは、現代物理学の基本的な態度である。ボルツマンらがその基礎を築いた統計力学の手法は、20世紀の量子力学を準備する。素粒子論というのは、現代の原子論に他ならない。



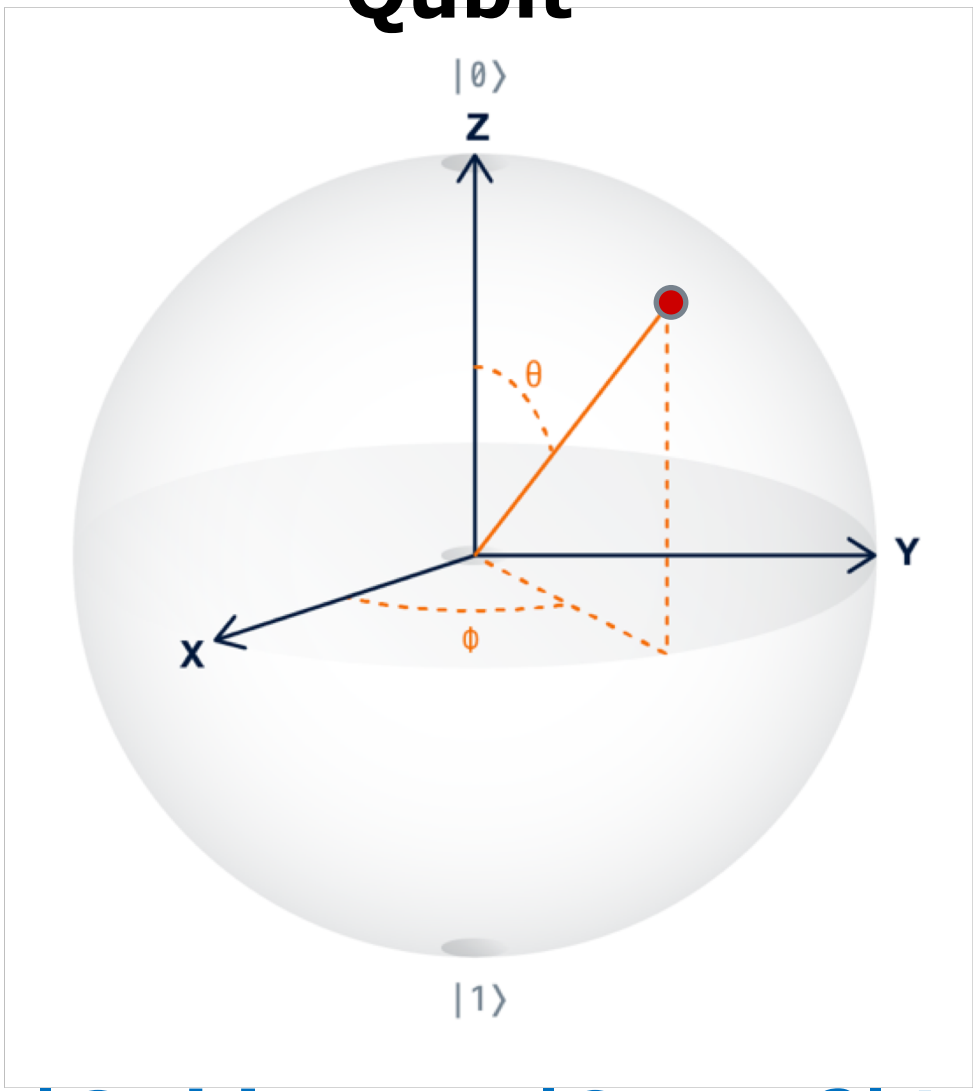
現代物理学の「標準モデル」での素粒子のリスト

量子の不可識別性
観測可能量と観測値

- 同じ状態にある量子は、たがいに区別できない。

- 量子の状態は、直接には、観測できない。
- 観測値が観測される確率は、正確に計算することができる。
- また、観測によって、系の状態は、観測前とは異なる状態に変化する。（重ね合わせは失われる。）

Qubit

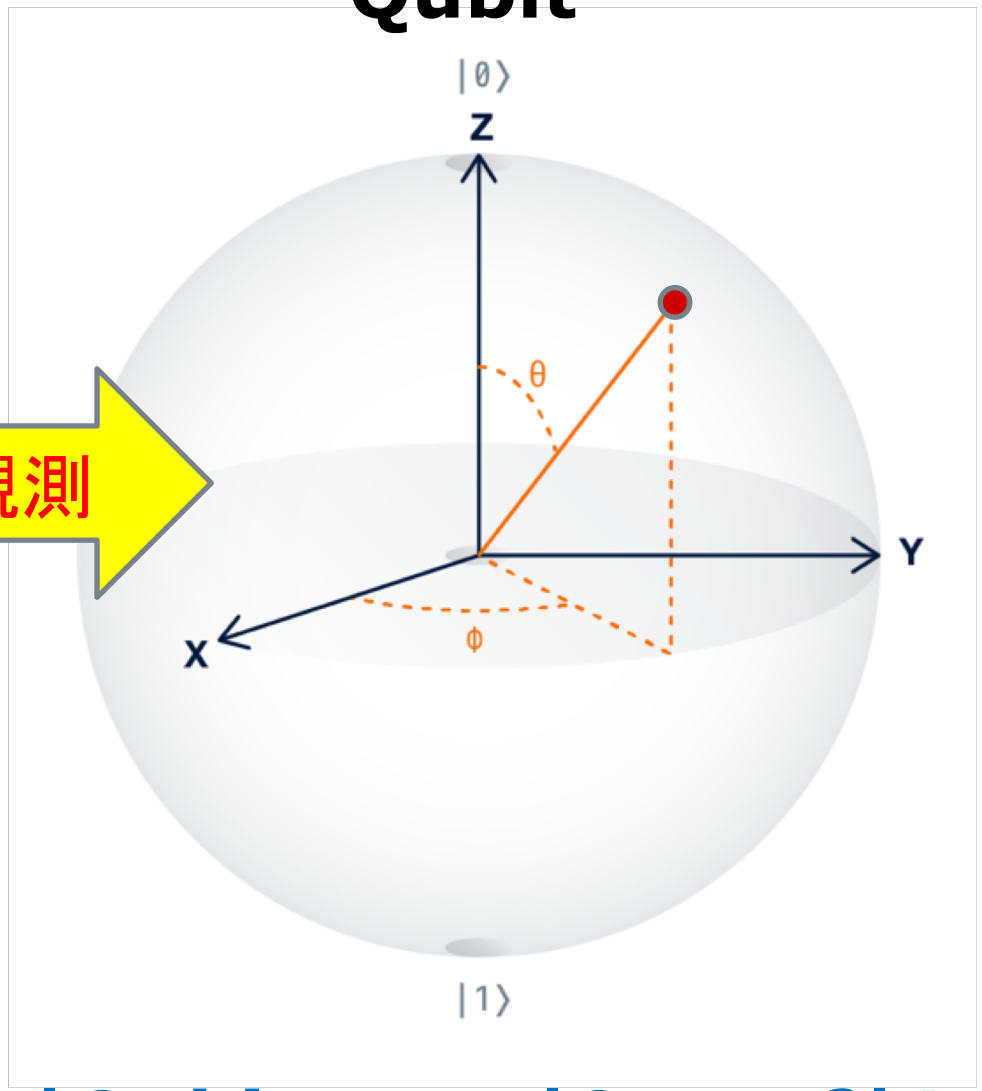


Qubitは、状態 |0>と状態 |1>の重ね合わせの状態を取る

|Qubit> = *α*|0> + *β*|1>

$$|\alpha|^2 + |\beta|^2 = 1 \; ; \quad \alpha, \beta \in \mathbb{C}$$

Qubit

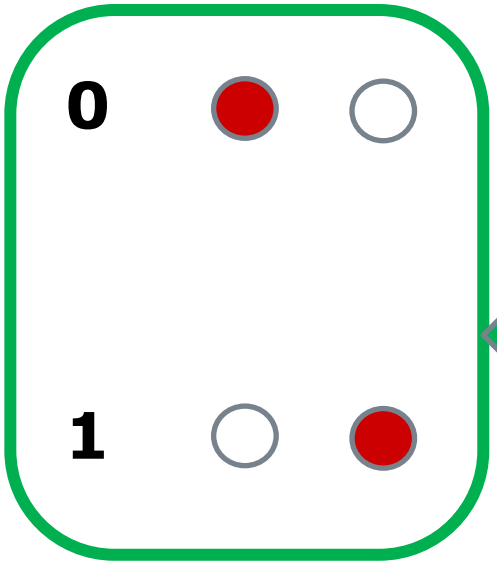


Qubitは、状態 |0>と状態 |1>の重ね合わせの状態を取る

$$|\mathrm{Qubit}\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$|\alpha|^2 + |\beta|^2 = 1\ ;\quad \alpha, \beta \in \mathbb{C}$$

観測を行うと、Qubitの
重ね合わせの状態は
失われ、0か1かの情報
が返る。



観測

観測値

Qubit

$\alpha|0\rangle + \beta|1\rangle$
の重ね合わせの
状態は、失われる

この時
0を得る確率は、$|\alpha|^2$で、
1を得る確率は、$|\beta|^2$で、
与えられる。

$\alpha^*\alpha + \beta^*\beta = 1 \; ; \quad \alpha, \beta \in \mathbb{C}$

フェルミオンとボソン

- 半整数 ±1/2, ±3/2,… のスピンを持つ量子をフェルミオン
  整数　±1, ±2, …のスピンを持つ量子をボソンという。
- クォークや電子やニュートリノはフェルミ粒子である。また、3つのクォークからなる陽子や中性子もフェルミ粒子である。一般に、「物質」を構成しているのは、フェルミオンである。
- 光子、ウィークボソン、グルーオン は、ボソンである。ボソンは、一般に、量子の間の相互作用を媒介する量子である。
- ボソンは、1つの体系内であっても同一の量子状態をいくつもの粒子がとることができる。
- 一方、2つ以上のフェルミ粒子は同一の量子状態を占めることはできない（「パウリの排他律」） 物質の安定性・同一性を担っているのは、一つには、このフェルミオンの性質による。

「保存量」の存在

- 一見すると、変転極まりなく、つかまえ難く見える量子の世界だが、変化を通じて変わらないものが存在する。それを「保存量」という。代表的な「保存量」は、エネルギーである。
- 「エネルギー保存則」は、「熱力学第一法則」とも呼ばれ、もっとも基本的な物理法則の一つである。

- エミー・ネーターは、系に連続的な対称性がある場合はそれに対応する保存則が存在することを発見した。

ゲージ不変性

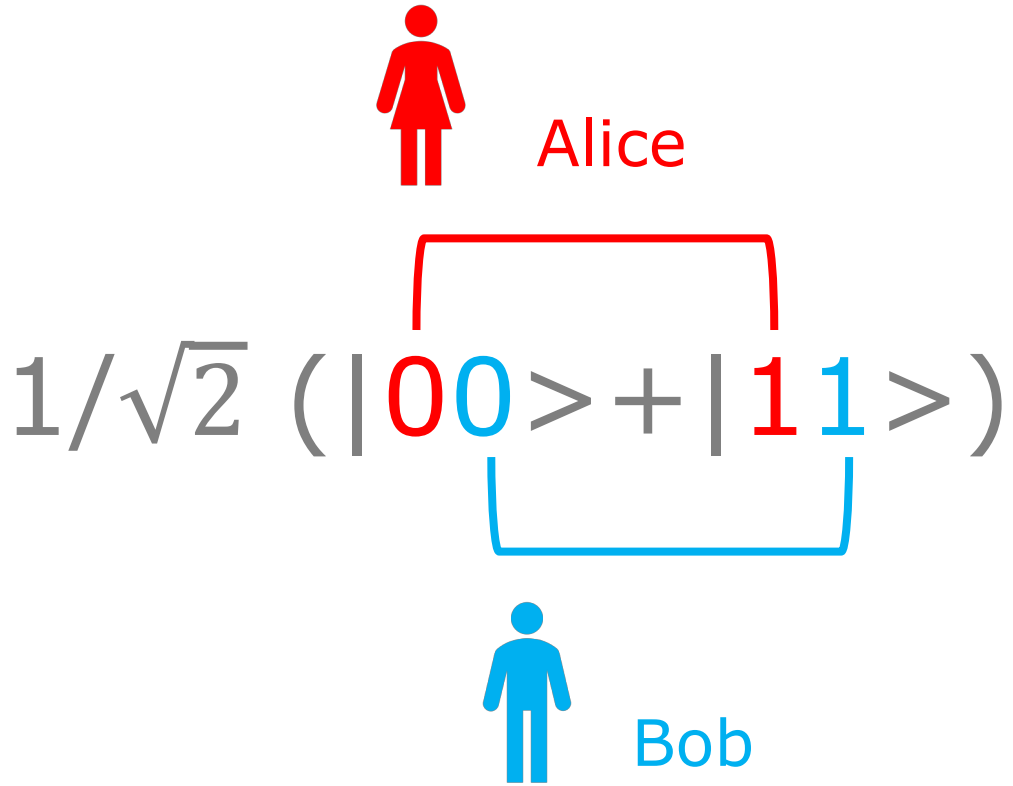
- マックスウェルの電磁方程式
  8つの方程式 → ヘビーサイド 4つの方程式
  →「ローレンツ ゲージ条件」 $\partial_u A^\mu = 0$
- アインシュタインの一般相対論と一般共変性
  「物理法則は座標変換のもとで同一の形式を保つ」
- ネーターの定理:「対称性が保存則を導く」
- ゲージ不変性
  「物理法則は、ある対称性変換群の下で不変なゲージ変換によって記述される」
  - 量子電磁気学は、U(1)対称性に基づく可換ゲージ理論
  - 場の量子論「標準理論」は、U(1) × SU(2) × SU(3) 対称性に基づく非可換ゲージ理論
  - 量子重力理論は？

エンタングルメント

Entanglement もつれ合い
二つの状態のテンソル積に分解できない状態

- 全ての Two qubitsの状態は、二つのqubitの状態のテンソル積に、分解できるだろうか？
- 次のTwo qubitの状態を考えよう。
  $1/\sqrt{2}$ (|00>+|11>)
  ところが、この状態は、二つのqubitのテンソル積では表現できないことが、次のようにしてわかる。
- $1/\sqrt{2}$ (|00>+|11>) が、(a|0>+b|1>)⊗(c|0>+d|1>) と二つの状態のテンソル積に分解できたとしよう。
  (a|0>+b|1>)⊗(c|0>+d|1>)
  = ac|00>+ad|01>+bc|10>+bd|11>
- 両辺の係数を比較すると、ad=bc=0となって、
  ac=bd=$1/\sqrt{2}$ となる a,b,c,d が存在しないことがわかる。
  こうした 2-qubitの状態を、「もつれ合い」と呼ぶ。

EPRペア：もつれ合った二つのqubit

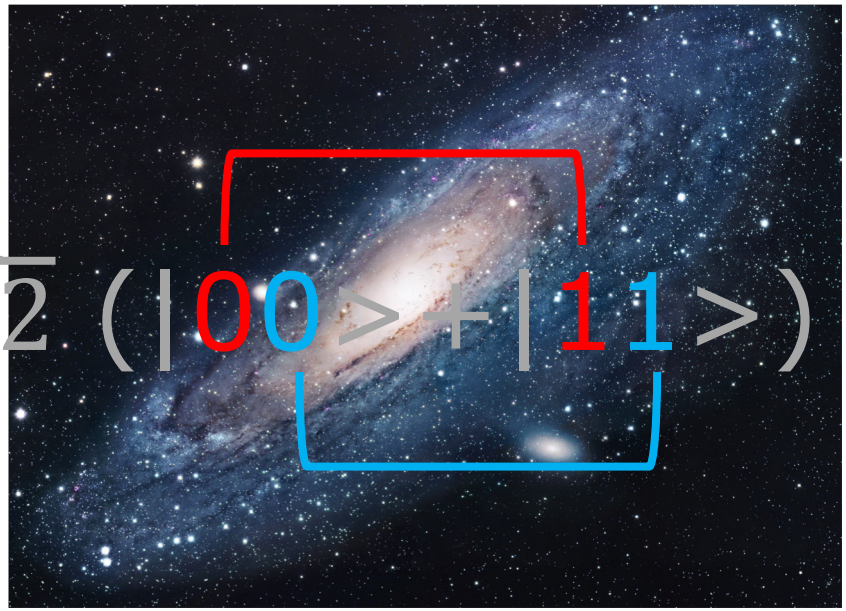


$1/\sqrt{2}$ (|00>+|11>) で表される状態は、二つのqubitの状態である。
一方のqubitをAliceが、他方のqubitをBobが持つことができる。
こうした、もつれ合った二つのqubitを、EPRペアと呼ぶ。

EPRペア：もつれ合った二つのqubit

Alice

$1/\sqrt{2}\ (|00>+|11>)$



Bob

$1/\sqrt{2}\ (|00>+|11>)$

Aliceが観察できるのは、$|00>+|11>$の第一bitで、
Bobが観察できるのは、$|00>+|11>$の第二bitである。
この関係は、両者がどんなに離れていても変わりない。

EPRペアのビットを観測する

Aliceが自分の持つEPRペア、$1/\sqrt{2}\ (|00>+|11>)$の最初のビットを観測したとしよう。それが1である確率は1/2で、0である確率は1/2である。

今、その結果が0であったとしよう。この観測の結果、新しい状態は、$|00>$に変わる。それは、第二ビットの観測が、0である確率が 1 であることを意味する。100% の確率で、Bobの持つ第二ビットの状態が0であることがわかる。

すなわち、Aliceが自分のqubitで状態0を観測するとすぐに、遠く離れたBobの持つqubitの状態が0であることがわかることになる。

最初の観測結果が1であったとしても、今度は、新しい状態が、$|11>$になるので、第二ビットの観察は、100%の確率で、1を返すことになる。

EPRペアのビットを観測する

Aliceの最初の観測結果が1であったとしよう。今度は、新しい状態が、|11>になるので、第二ビットの観察は、100%の確率で、1を返すことになる。

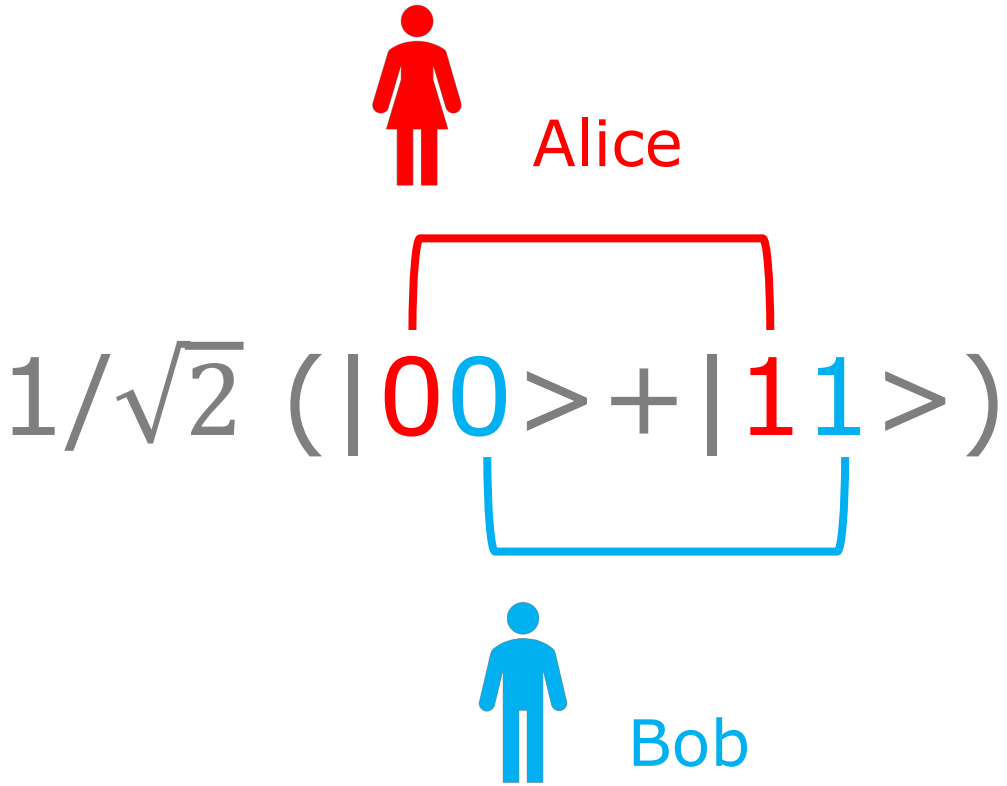
すなわち、Aliceが自分のqubitで状態1を観測するとすぐに、遠く離れたBobの持つqubitの状態が1であることがわかることになる。

Aliceの観測結果が、瞬時に、遠く離れたBobの観測結果に影響を与える？ これは、光のスピード以上で情報が伝わらないとする物理法則に矛盾しないか？

実際、アインシュタインは、こうした現象は「馬鹿げた遠隔作用」だと言った。

EPRペア：もつれ合った二つのqubit

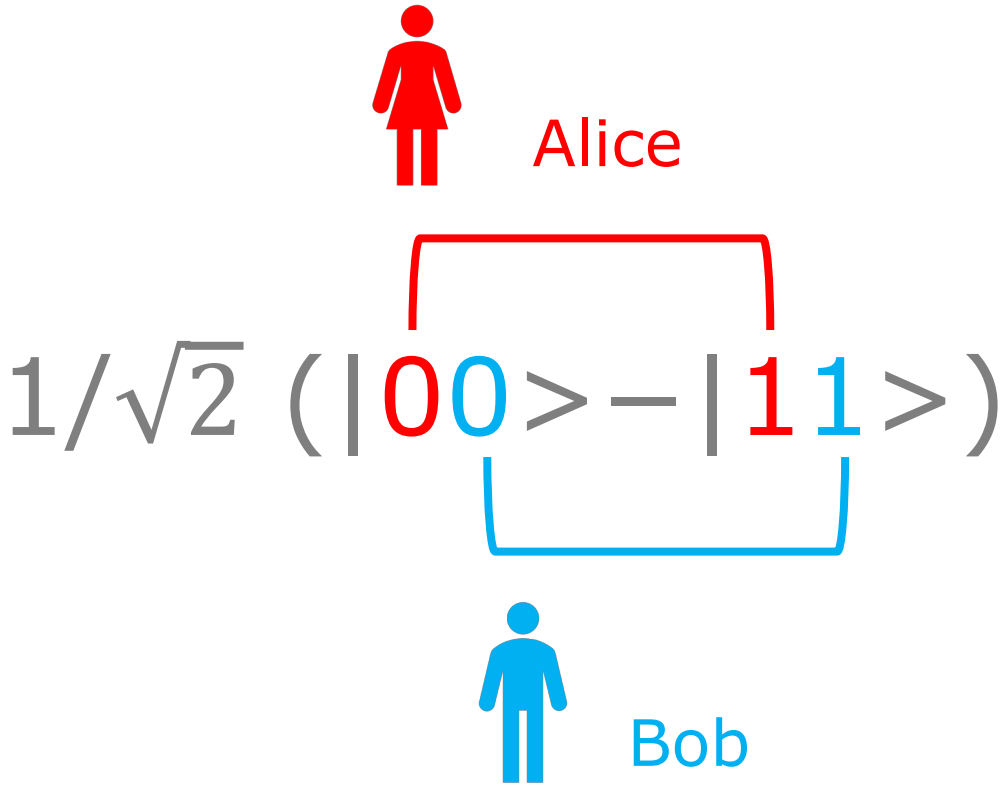
Φ^+



こうした性質を持つペアは、$1/\sqrt{2}$ (|00>+|11>) だけではない。

EPRペア：もつれ合った二つのqubit

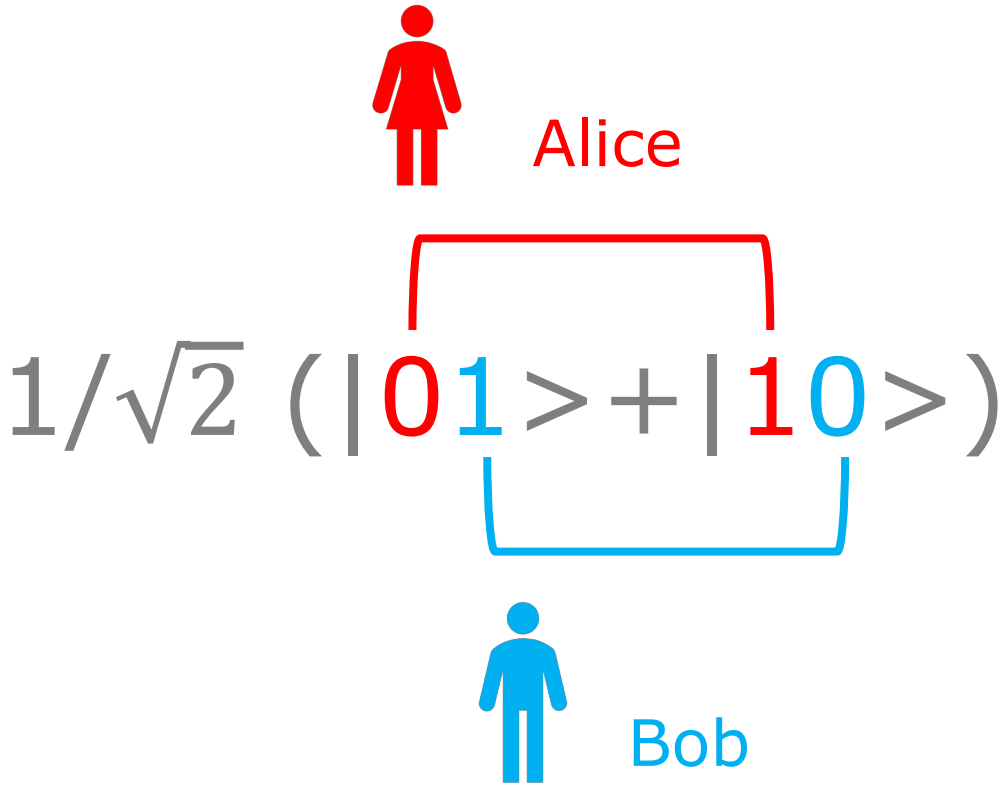
Φ^-



こうした性質を持つペアは、$1/\sqrt{2}\ (|00>+|11>)$ だけではない。

EPRペア：もつれ合った二つのqubit

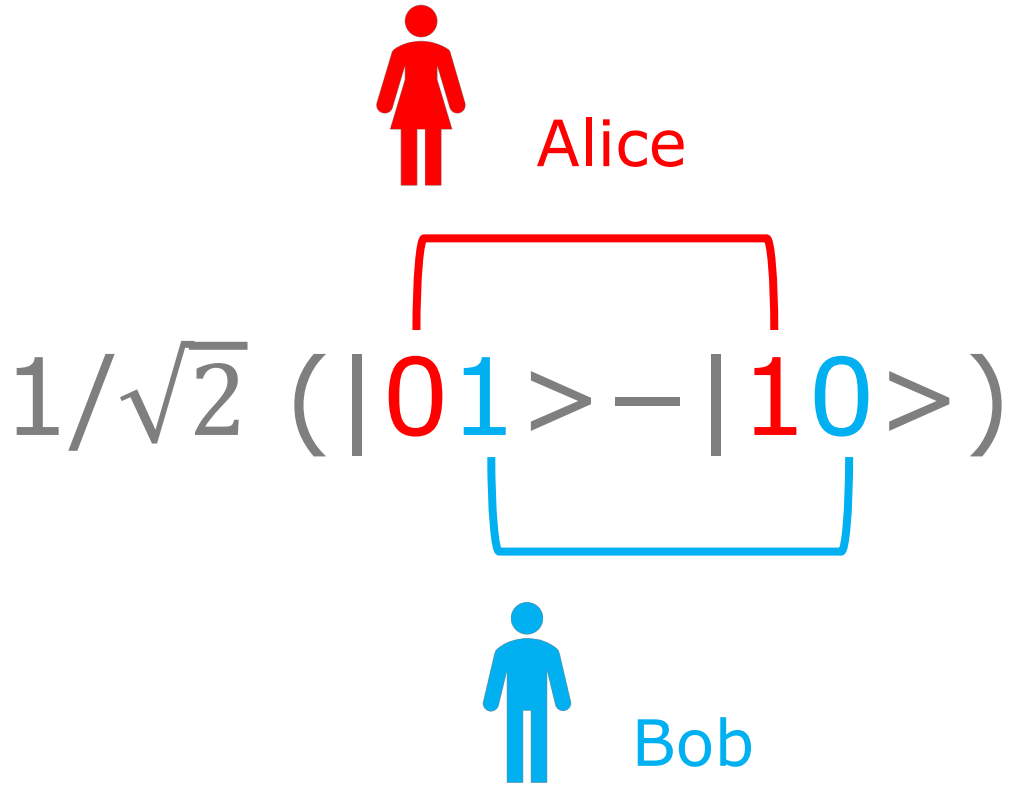
Ψ^+



こうした性質を持つペアは、$1/\sqrt{2}$ (|00>+|11>) だけではない。

EPRペア：もつれ合った二つのqubit

Ψ^-

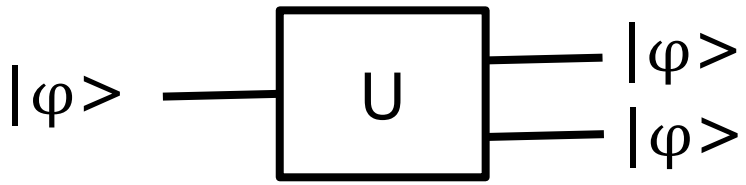


こうした性質を持つペアは、$1/\sqrt{2}\ (|00\rangle + |11\rangle)$ だけではない。

量子情報理論と「同一性」

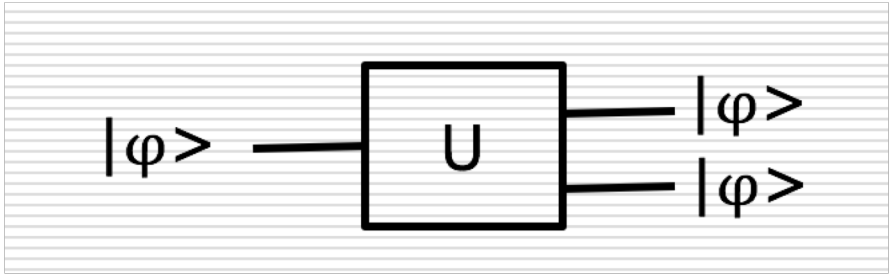
No Cloning 定理

- ある状態 $|\varphi\rangle=\alpha_0|0\rangle+\alpha_1|1\rangle$に対して、$|\varphi\rangle\otimes|\varphi\rangle$ すなわち自己のコピーをもう一つ生成する回路を考えよう。実は、量子ゲートの世界では、こうした基本的な操作ができないのだ。これを、No Cloning 定理と呼ぶ。以下、それを説明しよう。



こうした回路は存在しない！

No Cloning 定理の証明



- 先のような回路（ユニタリ変換U）が存在したとする。
  その回路は、一般のφだけでなく、|0>, |1> に対しても働くので、

$$U|0\rangle = |00\rangle$$
$$U|1\rangle = |11\rangle$$

- $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ とすれば、

$$U|\psi\rangle = \alpha U|0\rangle + \beta U|1\rangle = \alpha|00\rangle + \beta|11\rangle$$

- Uは、|ψ>もコピーできるはずなので、

$$U(|\psi\rangle) = |\psi\rangle|\psi\rangle = \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle$$

- しかし、この二つの条件を満たすα, βは、存在しない。

量子テレポーテーション

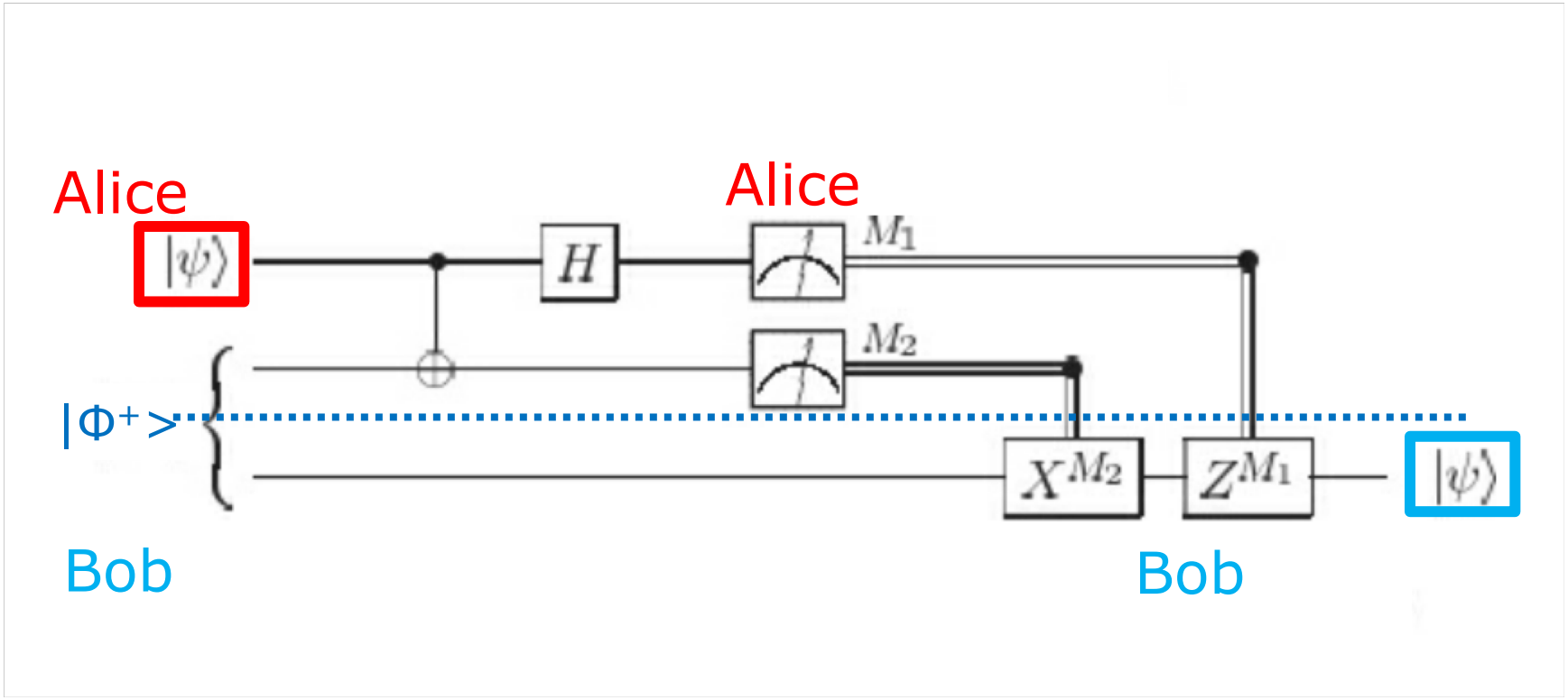
- AliceとBobは、ずいぶん昔にあっていたのだが、今は、遠くに離れて住んでいる。Aliceのミッションは受け取った量子の状態qubit $|\psi\rangle$をBobに送ることだった。彼女は、qubitの状態を知らない。さらに、Bobには、古典的な手段でしか情報を送れない。この時、Aliceは、このミッションを遂行できるだろうか？

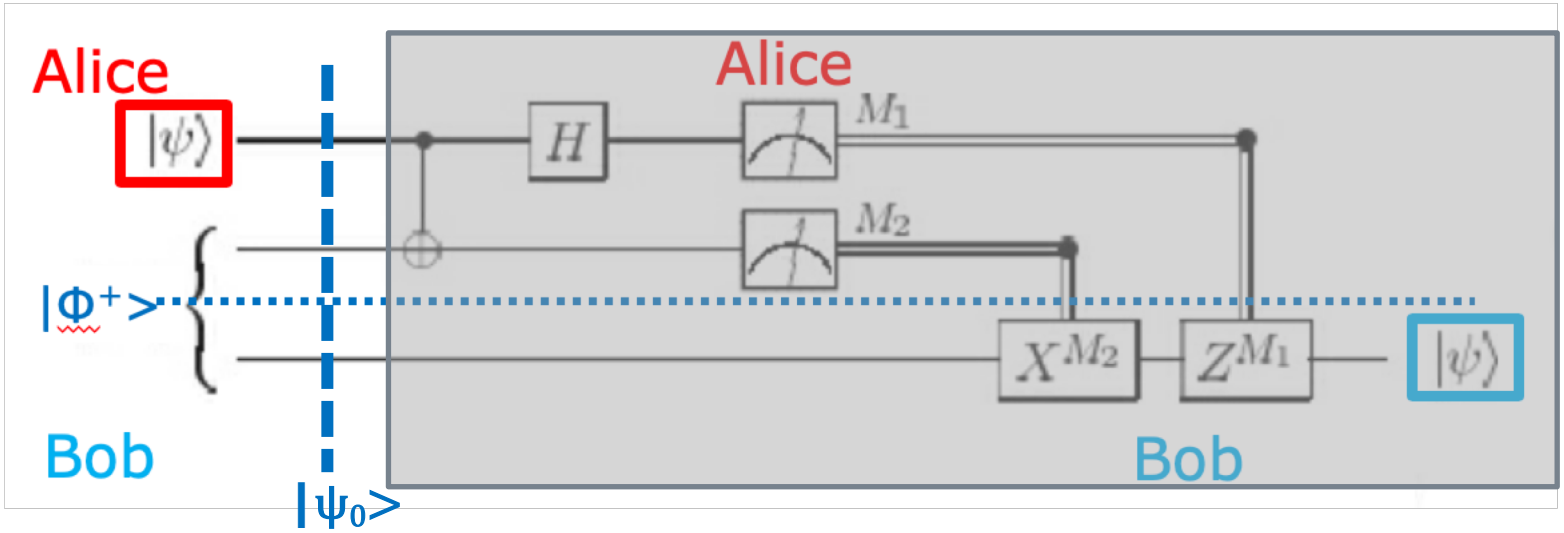
- 離れる前に、エンタングルしたEPRペアを共有していれば、このミッションは、実行可能である。これを、「量子テレポーテーション」という。

- 直感的には、Aliceはかなり分が悪いように見える彼女は、Bobに送らなければならないそのqubit $|\Psi\rangle$ の状態を知らないし、量子力学の法則は、たった一つのコピーを持っているだけの状態を決めることを妨げるだろう。もっと悪いことに、たとえ彼女が$|\Psi\rangle$の状態を知っていたとしても、 $|\Psi\rangle$の状態は、連続空間上に値をとるわけで、それを正確に記述するには、無限の量の古典情報が必要になる。それをBobに伝えるには無限の時間が必要になる。
- Aliceにとって幸いなことに、量子テレポーテーションは、エンタングルしたEPRペアを利用して、ほんの少しの古典的コミュニケーションの手間だけで、Bobに $|\Psi\rangle$ の状態を送ることを可能にするのである。

- Aliceは、彼女の持つEPRペアの片方に作用して、彼女が持つ二つのqubitを測定して、四つの可能な古典的結果 00, 01, 10, 11 を得る。
- 彼女は、この情報を、古典的な手段でBobに送る。
- Aliceの古典的なメッセージに基づいて、Bobは四つのうち一つの操作を選んで彼のEPRペアの片方に適応する。
- 驚くべきことに、それだけで、Bobはオリジナルの状態 $|\Psi\rangle$ を復元できるのである。

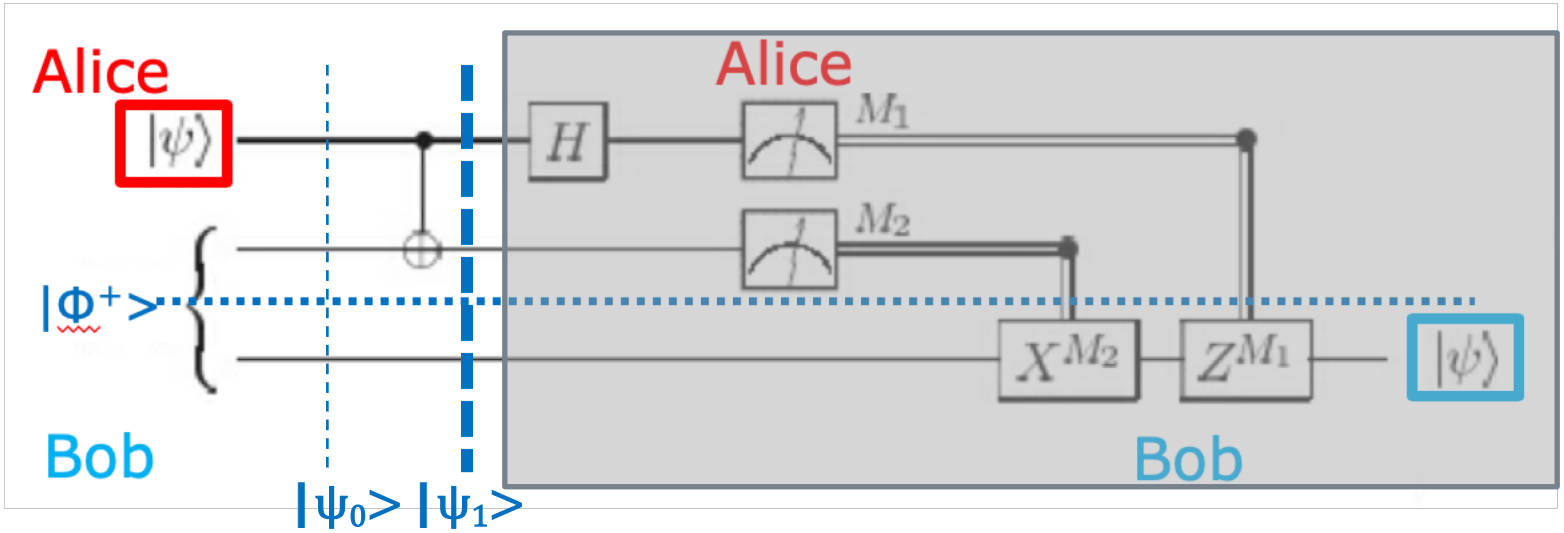
- Aliceの出力の測定に従って、Bobのqubitはこれらの四つの可能な状態をとる。もちろん、どの状態にあるかを知るためには、BobはAliceの測定の結果を知らされていなければならない。この事実によって、情報の伝達が光より速くなることは避けられることになる。いったんBobが測定の結果を知れば、Bobはその状態を、適当な量子ゲートを適応して「修正」して$|\Psi\rangle$を復活できる。
- 例えば、測定の結果が00であれば、Bobは何もする必要はない。測定が01の時には、Xゲートを適用すればいい。10ならZゲートを適用すればいい。もし、11ならば、最初にXゲートを、続いてZゲートを適用すればいい。


Alice
Alice
$|\psi\rangle$
H
M_1
M_2
$|\Phi^+\rangle$
X^{M_2}
Z^{M_1}
$|\psi\rangle$
Bob
Bob



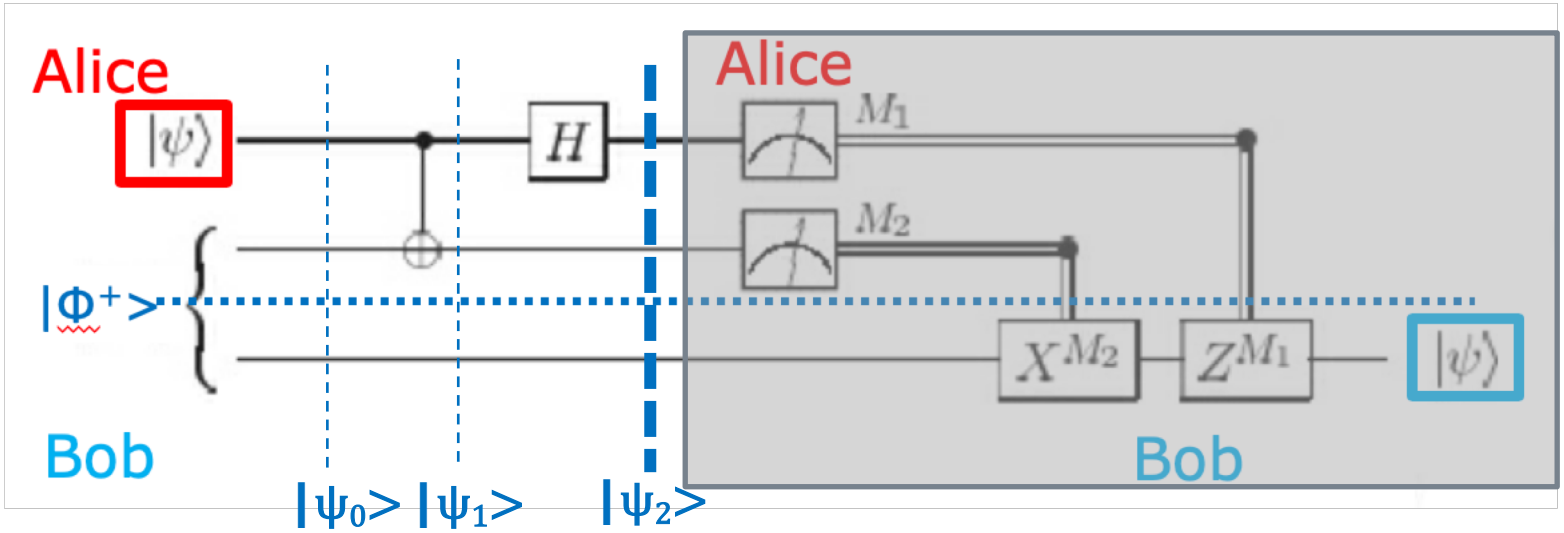
$|\psi\rangle = \alpha|0\rangle+\beta|1\rangle$, $|\Phi^+\rangle = 1/\sqrt{2}\,(|00\rangle + |11\rangle)$ とすると。

$$
\begin{aligned}
|\psi_0\rangle &= |\psi\rangle \otimes |\Phi^+\rangle \\
&= (\alpha|0\rangle+\beta|1\rangle) \otimes 1/\sqrt{2}\,(|00\rangle + |11\rangle) \\
&= 1/\sqrt{2}\,(\alpha|0\rangle \otimes(|00\rangle +|11\rangle)+\beta|1\rangle\otimes(|00\rangle + |11\rangle))
\end{aligned}
$$



$$|\psi_0\rangle = 1/\sqrt{2}\,(\alpha|0\rangle \otimes(|00\rangle + |11\rangle)+\beta|1\rangle\otimes(|00\rangle + |11\rangle))$$

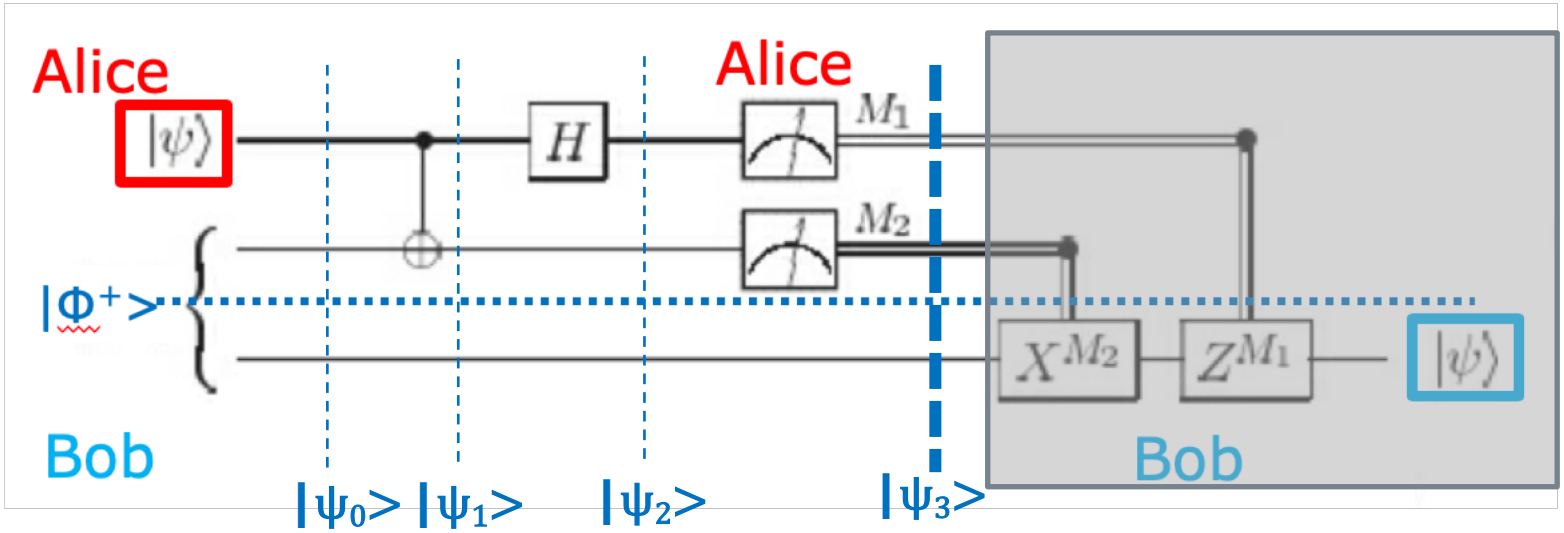
$$|\psi_1\rangle = 1/\sqrt{2}\,(\alpha|0\rangle \otimes(|00\rangle + |11\rangle)+\beta|1\rangle\otimes(|10\rangle + |01\rangle))$$



$$|\psi_0\rangle = 1/\sqrt{2}\,(\alpha|0\rangle \otimes(|00\rangle + |11\rangle) + \beta|1\rangle \otimes(|00\rangle + |11\rangle))$$

$$|\psi_1\rangle = 1/\sqrt{2}\,(\alpha|0\rangle \otimes(|00\rangle + |11\rangle) + \beta|1\rangle \otimes(|10\rangle + |01\rangle))$$

$$\begin{aligned}|\psi_2\rangle &= 1/\sqrt{2}\,(\alpha(|0\rangle+|1\rangle)\otimes(|00\rangle + |11\rangle) + \\ &\qquad \beta(|0\rangle-|1\rangle)\otimes(|10\rangle + |01\rangle)\,) \\ &= 1/\sqrt{2}\,(\alpha(|000\rangle+|011\rangle+|100\rangle+|111\rangle) + \\ &\qquad \beta(|010\rangle+|001\rangle-|110\rangle-|101)\,) \\ &= 1/\sqrt{2}\,(|00\rangle(\alpha|0\rangle+\beta|1\rangle)+|01\rangle(\alpha|1\rangle+\beta|0\rangle) + \\ &\qquad |10\rangle(\alpha|0\rangle-\beta|1\rangle)+|11\rangle\,(\alpha|1\rangle-\beta|0\rangle)\,)\end{aligned}$$

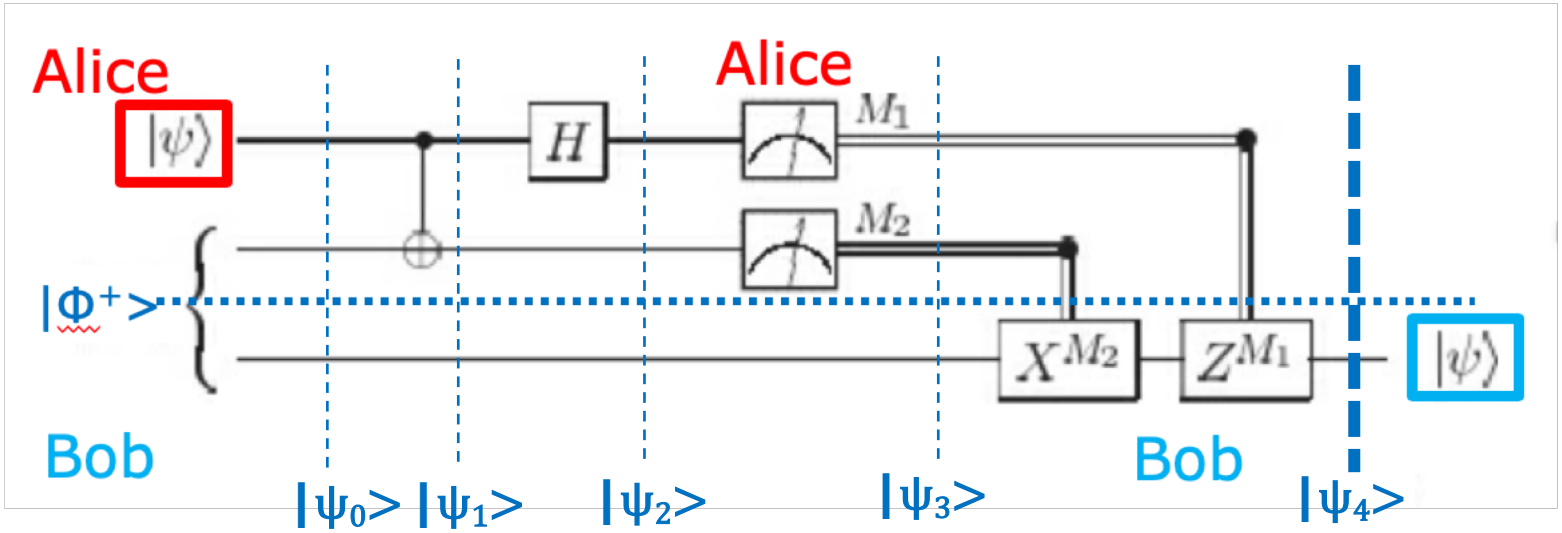


$$|\psi_0\rangle = 1/\sqrt{2}\,(\alpha|0\rangle \otimes(|00\rangle + |11\rangle) + \beta|1\rangle \otimes(|00\rangle + |11\rangle))$$

$$|\psi_1\rangle = 1/\sqrt{2}\,(\alpha|0\rangle \otimes(|00\rangle + |11\rangle) + \beta|1\rangle \otimes(|10\rangle + |01\rangle))$$

$$|\psi_2\rangle = 1/\sqrt{2}\,(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle\,(\alpha|1\rangle - \beta|0\rangle)\,)$$

$$|\psi_3(00)\rangle = (\alpha|0\rangle + \beta|1\rangle)$$
$$|\psi_3(01)\rangle = (\alpha|1\rangle + \beta|0\rangle)$$
$$|\psi_3(10)\rangle = (\alpha|0\rangle - \beta|1\rangle)$$
$$|\psi_3(11)\rangle = (\alpha|1\rangle - \beta|0\rangle)$$



$|\psi_3(00)\rangle = (\alpha|0\rangle+\beta|1\rangle)$
$|\psi_3(01)\rangle = (\alpha|1\rangle+\beta|0\rangle)$
$|\psi_3(10)\rangle = (\alpha|0\rangle-\beta|1\rangle)$
$|\psi_3(11)\rangle = (\alpha|1\rangle-\beta|0\rangle)$

$|\psi_4(00)\rangle = \psi_3(00)\rangle = (\alpha|0\rangle+\beta|1\rangle)$
$|\psi_4(01)\rangle = X\,|\psi_3(01)\rangle = X(\alpha|1\rangle+\beta|0\rangle)=(\alpha|0\rangle+\beta|1\rangle)$
$|\psi_4(10)\rangle = Z|\psi_3(10)\rangle = Z(\alpha|0\rangle-\beta|1\rangle)=(\alpha|0\rangle+\beta|1\rangle)$
$|\psi_4(11)\rangle = ZX|\psi_3(11)\rangle = ZX\,(\alpha|1\rangle-\beta|0\rangle)=(\alpha|0\rangle+\beta|1\rangle)$

$|\psi\rangle = \alpha|0\rangle+\beta|1\rangle$

いくつかの疑問について

- 第一。量子テレポーテーションは、光より早く量子状態を送ることができるのだろうか？
  これに対する答えは、明確にノーだ。テレポーテーションを実行するためには、Aliceは観測結果を、古典的な通信路で、Bobに送らなければならないのだから。

- 第二。量子テレポーテーションは、未知の量子状態のコピーを禁じたNo Cloning定理を破ることにならないか？
  これについても、答えはノーだ。Bobのもとで、量子状態は再現されるのだが、Aliceのもとにあったオリジナルの量子状態は、Aliceの観測によって、|0>か|1>かの状態に変わって、失われている。

Part III

数学と同一性 – 型の理論入門

Part III Agenda
数学と同一性

- Libniz -- 不可識別者同一の原理
- Russell -- 集合論の逆理と型の理論
- Church -- 型を持つラムダ計算
- Curry-Howard対応 --型付きラムダ計算と論理との対応
- Martin-Löf -- Dependent Type Theory
- Voevodsky -- Homotopy Type Theory

Libniz -- 不可識別者同一の原理

ライプニッツ

- 「不可識別者同一の原理」
  お互い区別できないものは同一である

- xについて真となる述語のすべてにおいて、その述語がyについても真となる時、その時に限り、xとyは等しい。

$$\forall F(Fx \leftrightarrow Fy) \rightarrow x=y.$$

- xとyが異なっているなら、xは持っているがyは持っていない少なくとも一つの性質がある。

ライプニッツ

1. **同一なものの不可識別性**
   すべての *x, y* について、*x*と*y*が同一なら、xとyはすべて同じ属性を持つ。

$$\forall x \, \forall y \, [x = y \rightarrow \forall P(Px \leftrightarrow Py)]$$

2. **不可識別なものの同一性**
   すべての *x, y* について、xとyがすべて同じ属性を持つならば、*x*と*y*は同一である。

$$\forall x \, \forall y \, [\forall P(Px \leftrightarrow Py) \rightarrow x = y]$$

「等号」のみたす性質 「同値関係」

1. 反射律　$x = x$
2. 対称律　$x = y$ なら $y = x$
3. 推移律　$x = y, y = z$ なら $x = z$

「等号」と同じ上の三つの性質を持つ「同値関係」 Rを考える。

1. Refl:　$\forall x.\ xRx$
2. Symm:　$\forall x,y.\ (xRy \rightarrow yRx)$
3. Trans:　$\forall x,y,z.\ (xRy \wedge yRz \rightarrow xRz)$

先のライプニッツの「不可識別性 (indiscernibility)」の 1. は、次のように表現される。

Indsc:　$\forall x,y.\ (xRy \rightarrow \forall P\ (Px \rightarrow Py))$

不可識別性から、対称律は導かれる

（証明） xRyが成り立っているとしよう。P(v)=vRyとする。

P(x)　(Pの定義と、xRyが成り立っていると言う前提から)
→ P(y)　(Indscから、xRy → ∀P (Px → Py) である）
→ yRx　(Pの定義から）

よって、xRy → yRx 対称律が成り立つ。

不可識別性から、推移律は導かれる

（証明） xRy, yRzが成り立っているとしよう。P(v)＝vRzとする。

　　yRz　（前提から）

→ Py　　(Pの定義から）

→ Px　　(xRyから、先に証明した対称律から、yRx。
　　Indiscから、yRx → ∀P (Py → Px) である ）

→ xRz　(Pの定義から）

よって、xRy, yRz → xRz で、推移律が成り立つ。

ただし、空な関係は、Indiscを満たすが、反射律を満たさない。

だから、不可識別性から反射律は導かれない。

Russell -- 集合論の逆理と型の理論

型の理論の歴史は古い。それは、Russellによる集合論のパラドックスの発見に端を発する100年以上前の理論にさかのぼる。

Fregeの公理

- Cantorの集合概念
  「集合とは、我々の直観あるいは思考の明確で異なった対象を一つの全体にした集まりである。
  その対象は、集合の要素と呼ばれる。」

- Fregeの定式化（Comprehension Axiom）
  ある述語Φについて$\Phi(x)$が成り立つ全ての要素xを集めた集合yが存在する。

$$\exists y \forall x [(x \in y) \Leftrightarrow \Phi(x)]$$

Russellの逆理

- 先のΦ(x)に、~(x∈x)を取ろう。
  このΦによって定義される集合をRとすれば、
  R={ x | ~(x∈x) }
  Rは、自分自身を要素として含まない全ての要素からなる集合になる。
- R∈Rだろうか？　この時、Rは自分自身を要素に含んでいるので、Rの要素ではない。だから、R∈Rならば~(R∈R)となって矛盾する。
- それでは、~(R∈R)だろうか？　この時、Rの定義から、このRはRの要素でなければならない。~(R∈R)ならばR∈Rとなって矛盾する。

Russellの矛盾の分析

- Russellは、定義されるべきクラス自身を含んだ、全てのクラスからなるクラスを考える自己参照的な定義、非述語的な定義(impredicative definition)が問題の原因だと考えた。
- 「全体は、その全体という言葉によってのみ定義される要素を含んではいけない。ある全体の全ての要素という言葉によってのみ定義されうるものは、その全体の要素にはなり得ない。」
- Russellは、対象と述語に型（degreeとorderからなる）を導入して、こうした述語の適用を排除しようとした。

Russellの型の理論

- 全ての個体は型 i を持つ。
- 述語 $P(x_1,x_2,\ldots x_n)$は、$x_1,x_2,\ldots x_n$ がそれぞれ持つ型 $i_1,i_2,\ldots i_n$に応じて、型 $(i_1,i_2,\ldots i_n)$ を持つ。
- ある型を持つ述語Pは、この型の階層構造の中で、その型以下の型を持つ個体に対してのみ適用出来る。
- 「全て」を表す全称記号は、その型以下の型を持つ個体の上を走る。

集合論の逆理に対する もうひとつのアプローチ

- Russellの型の理論とは、別のスタイルでの集合論の逆理に対する対応が、Zermelo–Fraenkelの公理的集合論（ZF）では、行われている。
- ZFでは、FregeのComprehension Axiomにかえて、次の公理が採用されている。

$$\exists y \forall x [(x \in y) \Leftrightarrow (x \in z) \wedge \Phi]$$

$$\exists y \forall x [(x \in y) \Leftrightarrow \Phi(x)]$$

集合論の逆理の発見の波紋
数学・論理学の基礎に対する反省

- 集合論での逆理の発見は、Russellの型の理論の導入、ZFによる集合論の公理化の動きとともに、数学・論理学の基礎に対する反省を活発なものにした。
- 疑われたのは次のような推論の正当性である。
  ~∀x~P(x) ==> ∃xP(x)
  「ある述語Pが成り立たないと全てのxについて言うことが否定できるなら、Pを満たすあるxが存在する。」 ここでは、あるものの存在が、存在しないと仮定すると矛盾することを示すことで証明されている。

直観主義・構成主義の登場

- こうした間接的な存在証明に疑いを持ち、こうしたものを論理から排除しようという動きが20世紀の初頭から生まれてくる。それが、直観主義・構成主義と呼ばれるものである。
- この立場では、P(x)を満たすあるxの存在は、P(a)が成り立つあるaを示すことで、始めて与えられることになる。
- この立場は、その後の数学・論理学に深い影響を与えた。現代のコンピュータ・サイエンスの基礎となっている型の理論も、後述するように、この立場に立っている。

Church -- 型を持つラムダ計算

現在のML, Haskellといった関数型言語は、
このChurchの型を持つラムダ計算に基礎をおいている。

λ計算の定義

- 次の三つのルールを利用して、λ式を(基本的には単純なものに)変換することをλ計算という。

1. α-conversion:
   抽象化に用いる変数の名前は、自由に変更出来る。例えば、
   $\lambda x.(x^2+1) \Rightarrow \lambda y.(y^2+1) \Rightarrow \lambda z.(z^2+1)$
2. β-reduction:
   代入による計算ルール　$(\lambda x.t)\ a \Rightarrow t[x:=a]$
3. η-conversion:
   $\lambda x.(f\ x) \Rightarrow f$
   xで抽象化されたf(x)は、fに等しいということ。

ラムダ計算への型の導入

- 型σから型τへの関数は、型 $\sigma \rightarrow \tau$ を持つ。
- あるλ式 eが型τを持つことを、$e : \tau$ と表す。
- α, β, ηの変換ルールは同じものとする

この表記の下で、λ式の型の定義を次のように行う。

1. 単純な変数 v_i は型を持つ。 $v_i : \tau$
2. $e_1 : (\sigma \rightarrow \tau)$で、$e_2 : \sigma$ なら、$(e_1\ e_2) : \tau$
3. $x : \sigma$ で $e : \tau$ なら、$(\lambda x_\sigma.e) : (\sigma \rightarrow \tau)$

型のないラムダ計算と単純な型を持つラムダ計算の違い

- 型のないλ計算で成り立つ性質の大部分は、型を持つλ計算でも成り立つ。
- ただ、両者のあいだには違いもある。
  型のないλ計算では、任意のλ式に対して任意のλ式の適用を許していたが、型を持つλ計算では、λ式の適用に型による制限が入っている。
- 型を持つラムダ計算では、$x_\sigma x_\sigma$という適用は許されない。許されるのは、$x_{\sigma\to\tau}\, x_\sigma$という型を持つλ式どうしの適用のみである。例えば、$\Omega := (\lambda x.xx)\,(\lambda x.xx)$ は、型を持つラムダ計算では許されないλ式である。

単純な型を持つラムダ計算の特徴

- 単純な型を持つラムダ計算は、こうした点では、型を持たないラムダ計算より表現力が弱いにもかかわらず、次のような重要な特徴を持つ。

- 単純な型を持つラムダ計算では、変換による計算は、必ず停止する。

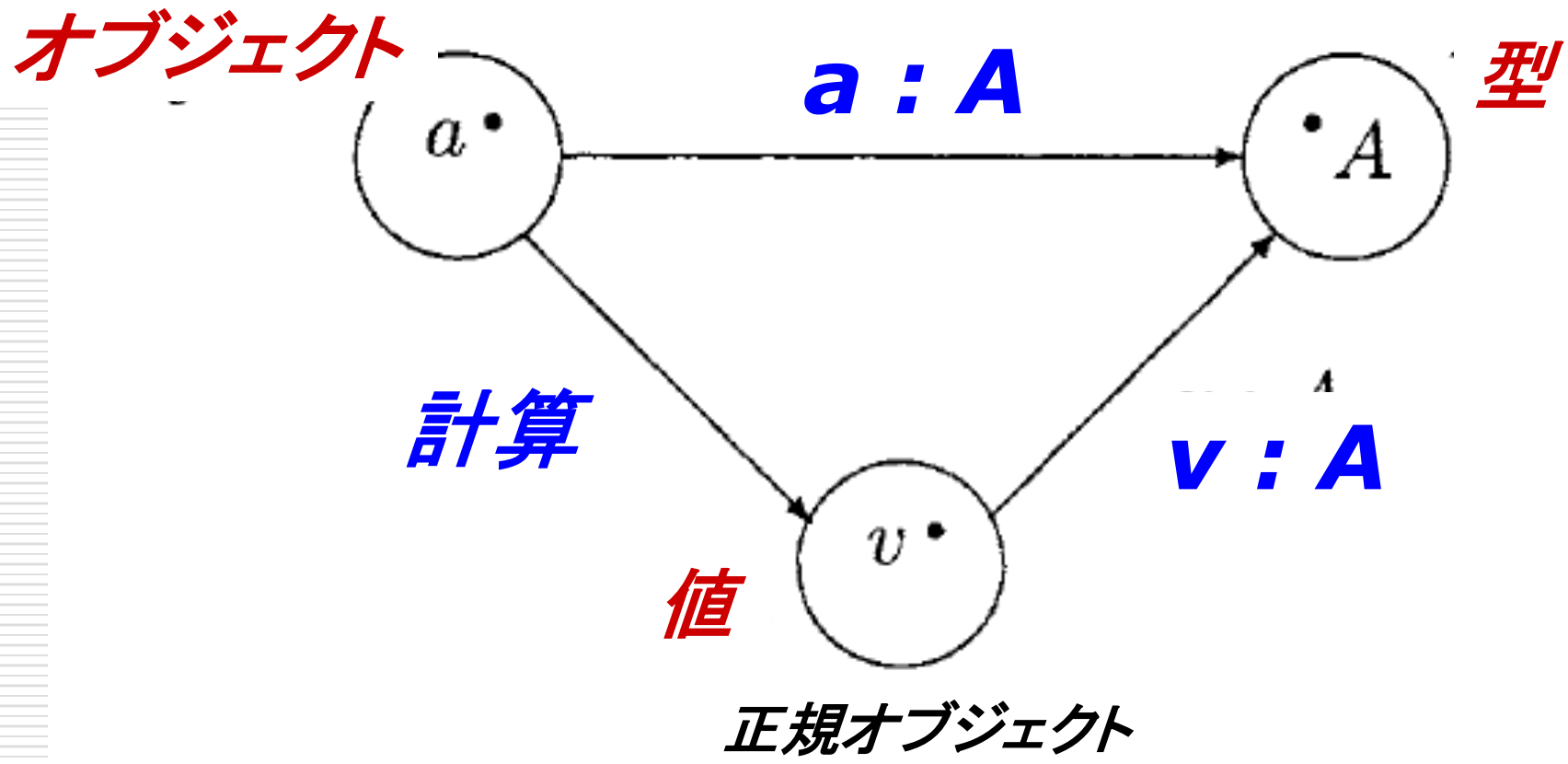
型を持つラムダ計算での計算

- あるオブジェクト aがある型 Aを持つという判断を、 ***a : A*** と表わそう。
- 型を持つラムダ計算の理論では、計算は、次の形をしている。
- 関数 ***λx:A.b[x]*** を、型Aに属するオブジェクトaを適用して ***b[a]***を得る。
- 計算の下で、全てのオブジェクトはユニークな値を持つ。また、計算で等しいオブジェクトは、同一の値を持つ。

型を持つラムダ計算での正規のオブジェクトとその値

- ある型に属するオブジェクトは、型の計算ルールによって、値が求まるなら、正規オブジェクトと呼ばれる。
- 例えば、１ ＋ １ は、自然数の型に属するが正規ではない。２ は、正規のオブジェクトである。
- ある型 A の正規オブジェクト v は、それ以上計算ルールの適用が出来ず、それ自身を値として持つ。
  この時、***v : A*** と書く。

型、オブジェクト、値



Curry-Howard対応
型付きラムダ計算と論理との対応

ラムダ計算に対する関心が、ふたたび活発化するのは、20年近くたった1960年代からだと思う。理由ははっきりしている。コンピュータが現実に動き出したからである。この時期の代表的な成果は、HowardのCurry-Howard対応の研究である。

Curry-Howard対応

- Curry-Howard対応は、「型の理論」の最も重要な発見の一つである。
- Curry-Howard対応は、論理と型の理論との間の、驚くべき対応関係を明らかにした。
  すなわち、論理における命題は、型の理論の型に対応し、論理における証明は、型の理論でのある型の要素に対応する。
- Curry-Howard対応は、“Proposition as Type” “Proof as Term” の頭文字をとって、PATと呼ばれることがある。

Curryの発見

- 既に1934年に、Curryは、型付を持つラムダ計算と直観主義論理とのあいだに、対応関係があることを発見していたという。
- ここでは、型を持つラムダ計算の型に登場する矢印 -> が、論理式で、「A ならば B」の含意を意味する “A -> B” の中に出てくる矢印 -> との間に、対応関係があることが大きな役割を果たす。

Curry, Haskell (1934), "Functionality in Combinatory Logic”
http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1076489/pdf/pnas01751-0022.pdf

Howardによる発展

- Howardは、このCurryの発見を、さらに深く考えた。
- 1969年の彼の論文のタイトルが示すように、
  論理式は型付きラムダ計算の型と見なすことが出来るのである。ただし、彼のこの論文が公開されたのは、1980年になってからのことらしい。

Howard,Williams (1980)
"The formulae-as-types notion of construction”
http://www.cs.cmu.edu/~crary/819-f09/Howard80.pdf

“Propositions as Types”
“Proofs as Terms”

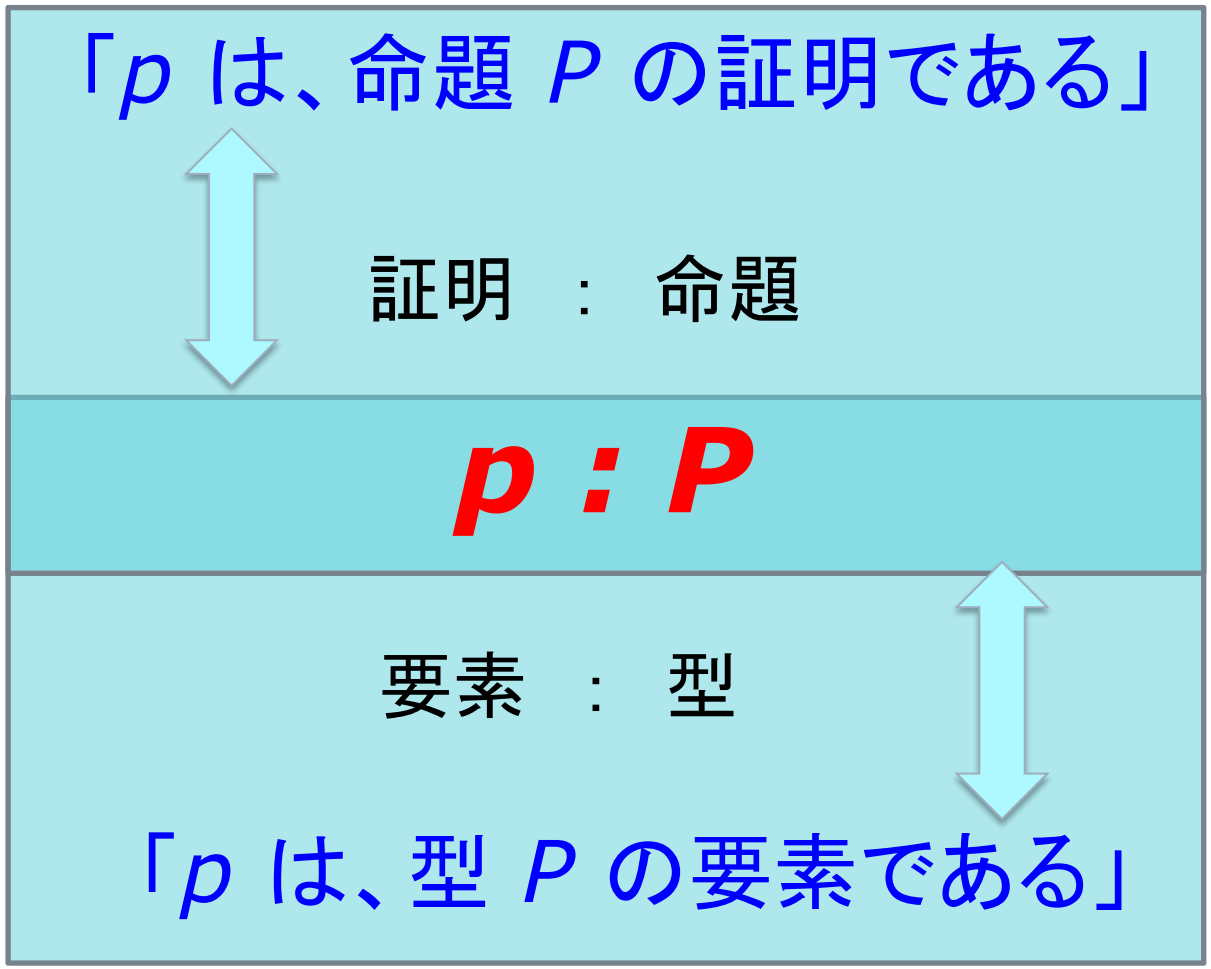
- Howardの洞察は、”Propositions as Types”, “Proofs as Terms” (これを、PATというらしい)として、次にみるMartin-Löfの型の理論に大きな影響を与えた。
- 同時に、Curry-Howard対応は、型付きラムダ計算をプログラムと見なせば、”Proof as Program”としても解釈出来る。
- こうした観点は、今日のCoq等の証明支援言語の理論的基礎になっている。

型と命題、証明と要素の「双対性」

- 型の理論の、中心的な概念は、型と命題、証明と要素の「双対性」である。
- p が命題 P の証明であることを、$p : P$ と表してみよう。
- この「p が命題 P の証明である」という判断を表す $p : P$ は、「p は、型 P の要素である」という判断を表していると見なすことが出来るし、また、逆の見方も出来るのである。

Curry-Howard対応

型と命題、要素と証明の「双対性」



Curry-Howardの対応関係をどう証明するか？

- ここでは、Simon Thompsonのやり方を紹介する。

- まず、***p : P*** が「*p* が命題 *P* の証明である」という判断を表すとして、そうした判断が従うべきルールを形式的に記述する。
- ついで、***p : P*** が「*p* が型 *P* の要素である」という判断を表すとして、そうした判断が従うべきルールを形式的に記述する。
- そうすると、前者と後者の形式的記述が、その解釈は別にして、まったく同じものであることが分かる。

Martin-Löf
Dependent Type Theory

現在の「型の理論」の基本が出来上がるのは、1980年代になってからである。その中心人物は、Martin-Löfである。

現在のCoq, Agdaという証明支援システムは、彼のDependent Typeの理論に基礎付けられている。

論理式の意味を考える

Due to Per Martin-Lof

"ON THE MEANINGS OF THE LOGICAL CONSTANTS AND THE JUSTIFICATIONS OF THE LOGICAL LAWS"

http://docenti.lett.unisi.it/files/4/1/1/6/martinlof4.pdf

論理式の意味？

- $A \wedge B$ ： AかつB
- $A \vee B$ ： AまたはB
- $A \rightarrow B$ ： AならばB
- $\sim A$ ： Aではない
- $\forall x P(x)$： 全てのxについてP(x)
- $\exists x P(x)$： あるxが存在してP(x)

⊢ A の意味

- 「Aは真である。」

- 「私は「Aは真である」ことを知っている。」

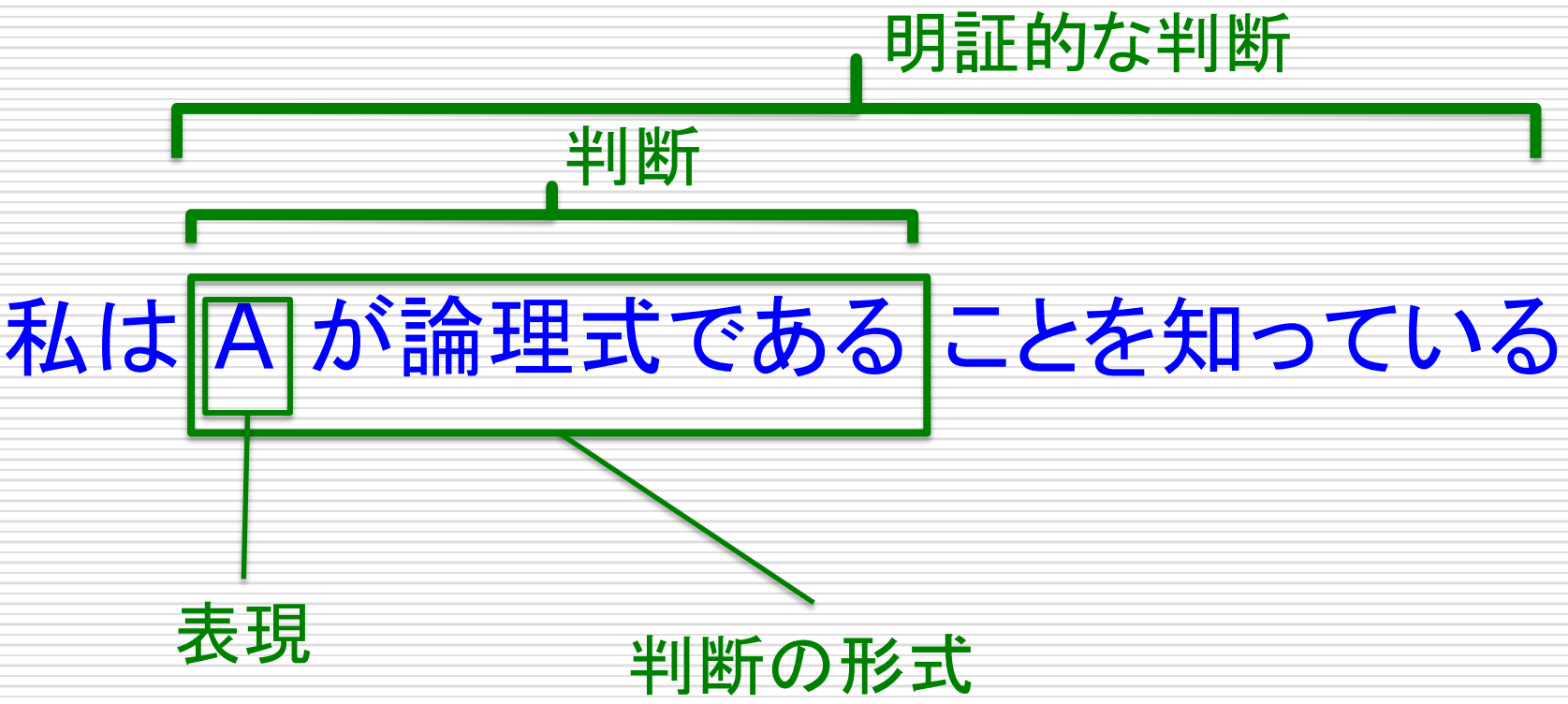
対象　　行為

私は「Aは真である」ことを知っている。

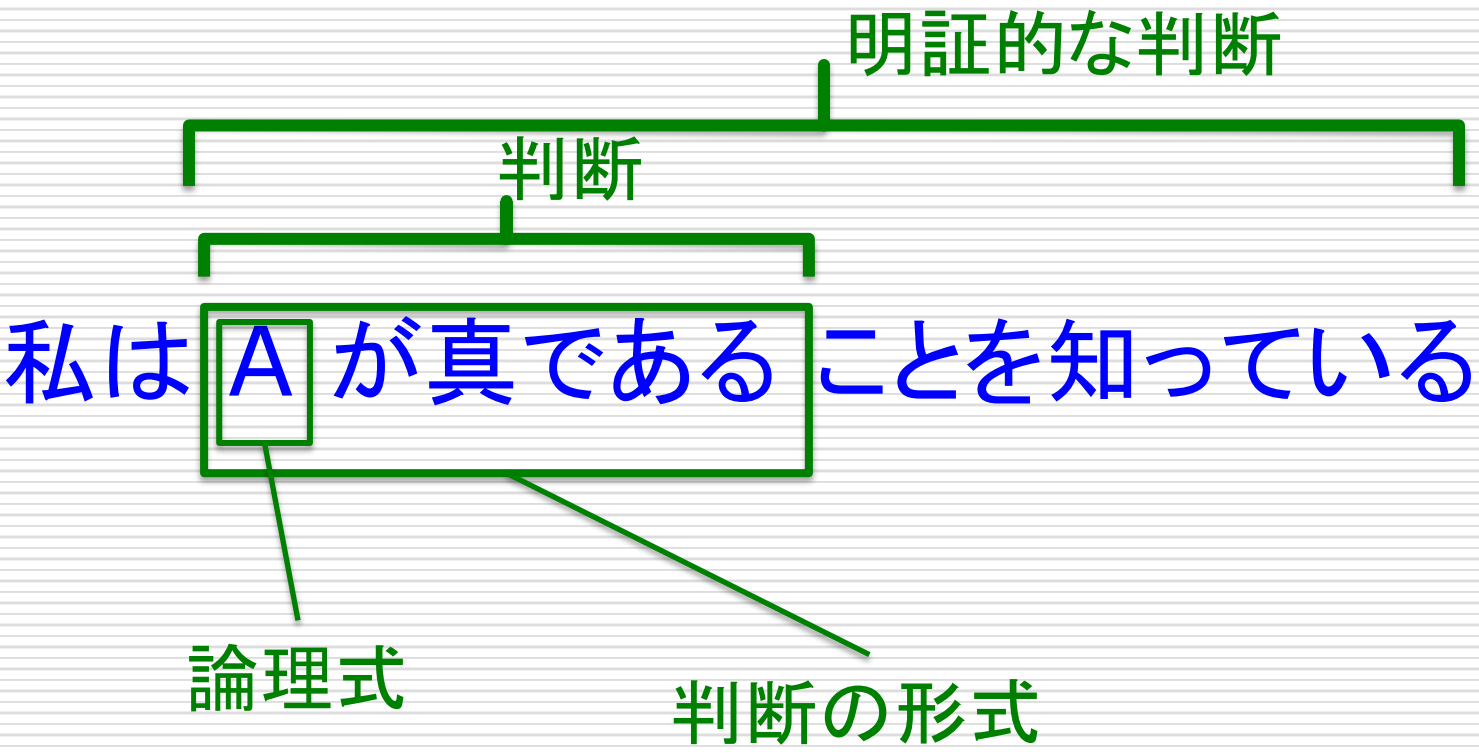
ただ、その前に、知っていることがある。

- 「私は「Aは論理式である」ことを知っている。」

論理式の表現･構成についての判断の構造



論理式の正しさについての判断の構造



判断と命題

- 判断の概念は、常に、命題の概念に先立つ。
- 判断における論理的帰結の概念は、命題における含意より先に、説明されなければならない。

証明とは何か？

- 証明とは、判断を明証なものにするもの。
- 証明すること＝知ること＝理解して把握すること
- 知るようになる＝知識を得ること
- 証明と知識は、同じもの

証明について考える

Due to Per Martin-Lof

“Intuitionistic Type Theory”

Bibliopolis 1980

https://goo.gl/WUjzTE

証明の解釈

- Kolmogorovは、命題 a → bの証明に、「命題 aの証明を命題 bの証明に変換する方法を構築すること」という解釈を与えた。
- このことは、a → bの証明を、aの証明からbの証明への関数と見ることが出来るということを意味する。
- このことは、同時に、命題をその証明と同一視出来ることを示唆する。
- 型はこうした証明の集まりを表現し、そうした証明の一つは、対応する型の、一つの項と見なすことが出来る。

命題の証明は、何から構成されるか？

⊥	なし
A ∧ B	Aの証明とBの証明の両方
A ∨ B	Aの証明、あるいは、Bの証明
A → B	Aの証明からBの証明を導く方法
(∀x)B(x)	任意のaに対してB(a)の証明を与える方法
(∃x)B(x)	あるaに対するB(a)の証明

命題の証明は、何から構成されるか？
形式的に

⊥	none
A ∧ B	Aの証明であるaと、 Bの証明であるbのペア**(a,b)**
A ∨ B	Aの証明である**i(a)**、あるいは、 Bの証明である**j(b)**
A → B	Aの証明であるaに対して、 Bの証明b(a)を与える**(λx)b(x)**
(∀x)B(x)	任意のaに対して Bの証明b(a)を与える**(λx)b(x)**
(∃x)B(x)	あるaと、B(a)の証明であるbのペア **(a,b)**

Dependent Type Theory

“INTUITIONISTIC TYPE THEORY”

Martin-Löf

1984年

http://archive-pml.github.io/martin-lof/pdfs/Bibliopolis-Book-1984.pdf

型の命題への拡張

- Churchの単純な型を持つラムダ計算の体系は、基本的には、型A, 型Bに対して、型 A → Bで表現される関数型の型しか持たない。
- それに対して、Martin-Löfは、論理的な命題にも、自然なスタイルで型を定義した。例えば、Aが型であり、Bが型であれば、A∧BもA→BもA∨Bも型であるというように。もちろん、それぞれは異なる型である。詳しくは後述する。
- ある aが型Aを持つ時、***a : A*** で表す。

同一性への型の付与

- Martin-Löf は、式 a = b にも型を与える。

  $a =_A b : Id(A\ a\ b)$

  型 Id(A a b) を持つ式は、a と b は等しいという意味を持つ。
- $a =_A b$ のAは、型Aの中での同一性であることを表している。すなわち、a : A で b : Aで、かつa = bの時にはじめて、$a =_A b$ は型Id(A a b)
  を持つ。
- ここでは式の同一性について述べたが、式の同一性と型の同一性は、異なるものである。

Martin-Löf の同一性の型の構成

E1: すべての型Xと、そのすべての要素 a, b について、
a = b という型が存在する。

E2: すべての型Xと、そのすべての要素aについて、
型 a = a の要素である refl(a)が存在する。（”refl”
は、”reflexivilty” である）

E3:すべての型Xと、そのすべての要素aと、型 a = bに属するe
について型X上のパラメータbに従属する型の族P(b, e)が与えら
れた時、f(b, e) : P(b, e) である型P(b,e)の要素f(b,e)をす
べて定義するためには、P(a, refl(a))の一つの要素 pを与えれ
ば十分である。この結果得られる関数fは、次の単一の定義で完
全に定義されたとみなすことができる。
f(a, refl(a)) := p

型の理論の記述

- Martin-Löfの型の理論は、次のことを示す、四つの形式で記述される。

1. ある対象aが、型であること
   $a : Type$
2. ある表現式 aが、型 αの要素であること
   $a : \alpha$
3. 二つの表現式が、同じ型の内部で、等しいこと
   $a = b : \alpha$
4. 二つの型が、等しいこと
   $\alpha = \beta \ : Type$

Dependent Type

- これまで、A∧B, A → B, A∨B といった、元になる型 A, B を指定すると新しい型が決まるといったスタイルで型を導入してきた。
- これとは異なる次のようなスタイル、型Aそのものではなく型Aに属する要素 a：Aに応じて新しい型 B(a)が変化するような型の導入が可能である。
- 例えば、実数R上のn次元のベクトル Vec(R,n)とn+1次元のベクトルVec(R,n+1)は、別の型を持つのだが、これは nに応じて型が変わると考えることが出来る。

Dependent Type

- こうした型をDependent Typeと呼び、次のように表す。
  $\Pi(x:A).B(x)$
- Dependent Typeは、ある型Aの値aにディペンドして変化する型である。
- 先の例のベクトルの型は、次のように表される。
  $\Pi(x:N).Vec(R,n)$
  これは、全てのnについてVec(R,n)を考えることに対応している。
- 型の理論では、全称記号は、Dependent Typeとして導入される。

Dependent TypeとPolymorphism

- Dependent Typeの例を、もう一つあげよう。
  n次元のベクトルは、自然数 N、整数 Z、実数 R、複素数 C上でも定義出来る。
  { N, Z, R, C }：T とする時、次のように定義される Dependent Typeを考えよう。
  $$\Pi(x : T)\mathrm{Vec}(x,n)$$
- これは、次元nは同じだが、定義された領域が異なる別の型 Vec(N,n),Vec(Z,n),Vec(R,n), Vec(C,n)を考えることに相当する。
- こうして、Polymorphicな関数は、Dependent Typeとして表現されることが分かる。

Inductive Type

- 型の理論では、基本的な定数と関数から、新しい型を帰納的に定義することが出来る。こうした型をInductive Type（帰納的型）と呼ぶ。
- 次は、そうした帰納的な定義の例である。
  ここでは、自然数の型natが、ゼロを意味する定数Oとsuccesser関数を表す関数Sで、帰納的に定義されている。

```
Inductive nat : Type :=
  | 0 : nat
  | S : nat -> nat.
```

関数型言語の基礎としての型の理論

- Martin-Löfの型の理論は、型を持つラムダ計算の拡張として、ML, Haskell等の現在の関数型言語に理論的基礎を与えた。
- 同時に、それは、Curry-Howard対応によって、Coq, Agda等の証明システムの理論的な基礎をも与えることになった。

Voevodsky
Homotopy Type Theory

新しい型の理論 HoTT

- Homotopy Type Theory (HoTT) は、数学者 Voevodsky が中心となって構築した、新しい型の理論である。
- HoTTは、数学の一分野であるホモトピー論やホモロジー代数と、論理学・計算機科学の一分野である型の理論とのあいだに、深い結びつきがあるという発見に端を発している。
- ここで取り上げられている型の理論は、Martin-LöfのDependent Type Theoryである。

HoTTでの *a : A* の解釈

- 論理＝数学的には、a：A には、様々な解釈がある。ここでは、他の解釈と比較して、HoTTでの a：A の解釈を見てみよう。

1. 集合論: Russellの立場
   Aは集合であり、aはその要素である。
2. 構成主義: Kolmogorovの立場
   Aは問題であり、aはその解決である
3. PAT: Curry & Howardの立場
   Aは命題であり、aはその証明である。
4. HoTT: Voevodskyの立場
   Aは空間であり、aはその点である。

Univalent TheoryとCoq

- Voevodskyは、HoTTを武器に、Univalent Theoryという数学の新しい基礎付け・再構成を始めている。興味深いのは、彼が、こうした理論展開を、数学論文ではなく、Coqのプログラムの形でGitHubで公開していることである。
  https://github.com/vladimirias/Foundations/
- 次の論文は、型の理論やHoTTにあまりなじみのない一般の数学者向けの、Voevodskyの理論 Coqライブラリーの解説である。
  http://arxiv.org/pdf/1210.5658v1.pdf

Univalent Foundation

“Structuralism, Invariance, and Univalence”

Steve Awodey

2014年

https://www.andrew.cmu.edu/user/awodey/preprints/siu.pdf

構造主義の原理

- 「同型な対象は同一である」
  “Isomorphic objects are identical. “
  これを「構造主義の原理 The Principle of Structuralism 」として、PSで表そう。

例

- コーシー列で定義された「実数$_{Cauchy}$」も、デディキンドの切断で定義された「実数$_{Dedekind}$」も同型である。解析的には、二つの実数は、同じものである。
- 単位区間 [0,1]は、区間 [0,2]と位相同型である。トポロジー的には、この二つの空間は、同じものである。

弱い形の構造主義の原理

- この原理は、実践的には有用なのだが、集合論的には、正しくない。先の二つの例でも、集合としては、二つは同じものではない。
- 「同一性 Identical」を、もっと弱い形で表現してみよう。

  「AとBが同型ならば、関係するすべての性質Pについて、P(A)が成り立つなら、P(B)が成り立つ。」

  AとBが同型であることを、$A \cong B$ と表そう。
  この弱い形の原理をPS’としよう。
- 確かに、PS’の主張は、PSより弱い。しかし、「関係するすべての性質」というのは、何を指しているのだろう？

同型について

- 二つのものが同型であるというのは、どういうことだろう？
  すぐに思いつくのは、次の定義である。
  以下、AとBが同型であることを、$A \cong B$で表す。

$$A \cong B \iff \text{AとBは同じ構造を持つ}$$

- ただし、これは、「同じ構造を持つ」ということの定義であって、
  「同型」の定義ではない。

カテゴリー論での同型の定義

- カテゴリー論では、次の条件を満たす時に、AとBは同型であるといわれる。

  構造を保存するような写像 f, gがあって、
  $f: A \to B$ と $g: B \to A$ が、$f \circ g = 1_A$, $g \circ f = 1_B$を満たす。

構造的性質と不変性

- ある性質P(X)は、次の性質を満たす時、不変であるという。

$$A \cong B \ \& \ P(A) \Longrightarrow P(B)$$

- この不変性は、この同型に関しての不変性で、構造的性質ともいわれる。

- 「もし、$A \cong B$ で、P(X)が構造的性質で P(A)が成り立つなら、P(B)が成り立つ」

- この性質は、実践的には役に立つのだが、同型について何が構造的性質かは、この定義は何も語っていない。

構成的型の理論と、Curry-Howard対応

- 構成的型の理論では、基本的なオブジェクト、すなわち、個物の型 Xは、次のものである。

$$0,\ 1,\ A+B,\ A\times B,\ A\to B,\ \Sigma_{x:A}B(x),\ \Pi_{x:A}B(x),\ \mathsf{Id}_A(x,y).$$

- そして、それらは次の論理的な命題に対応している。

$$\bot,\ \top,\ A\vee B,\ A\wedge B,\ A\Rightarrow B,\ \exists x:A.\ B(x),\ \forall x:A.\ B(x),\ x=_A y.$$

- こうした対応は、Curry-Howard対応、あるいは、“Propositions-as-Types” と呼ばれる。

$$\text{proof} : \text{Proposition} \quad \approx \quad \text{term} : \text{Type}$$

- すなわち、ある命題の証明は、対応する型の項になる。

不変性の原理

- 型の理論は、オブジェクトのすべての定義可能な性質は、不変であるという重要な性質を持っている。
- もし、Pが、ある基本的な型の上で定義可能なら、次の推論は演繹可能である。

$$\frac{A \cong B \qquad P(A)}{P(B)}$$

- これを、型の理論の不変性の原理という。すなわち、

  すべての定義可能な性質は、同型のもとで不変である。

オブジェクトの同一性（Identity）

- オブジェクトAとBが、同一であるというのはどういうことだろうか？
- 型の理論では、同一性を、ライプニッツの法則で定義する。

$$A = B \;:=\; \forall P.\; P(A) \Rightarrow P(B),$$

- この同一性は、AとBが共通に属する同じ型 Xの項の同一性である。$\forall P.$は、X上のすべての性質の型である$\mathcal{P}(X)$上（Pの部分集合である）を走る。
- だから、正確には、先の式は次のようになる。

$$A =_X B \;:=\; \forall P : \mathcal{P}(X).\; P(A) \Rightarrow P(B),$$

- これは、オブジェクトの間の同一性を示すもので、型Xと型Yの同一性を表すものではない。

型の同一性

- 構成的型の理論には、すべての型Xの項について、基本的な同一性の関係 $\mathbf{Id}_X(a, b)$が存在するので、項の同一性については、次の推論規則が成り立つ。

$$\frac{\mathsf{Id}_X(a,b) \qquad P(a)}{P(b)}$$

- それでは、型の同一性については、どのような推論が可能だろうか？　それには、すべての型のUniverseであるUを追加すればいい。

$$\frac{\mathsf{Id}_U(A,B) \qquad P(A)}{P(B)}$$

型の同一性と同型

- 型の同一性の推論の仕方はそれでいいとして、型の同一性と同型の関係はどうなるのか考えてみよう。
- Uを追加する前に、定義可能なすべての性質は不変であることを見てきた。すなわち、

$$\frac{A \cong B \qquad P(A)}{P(B)}$$

不変性の原理

- もしも、Uを含んだPについても、この推論が成り立つのなら、

$$P(X) := \mathsf{Id}_U(A, X),$$

と置けば、$\mathsf{Id}_U(A, A)$ から、次の構造主義の原理を導くことができる。

$$A \cong B \;\Rightarrow\; \mathsf{Id}_U(A, B)$$

- すなわち、型の理論では、不変性の原理は、構造主義の原理を含意する。

- 簡単に言えば、Universeを持つ拡張された型の理論でも、すべての定義可能な性質は、同型不変である。この時、特別のオブジェクトは、同一のものになる。

- こうしたことは、本当に可能なのだろうか？

「… である」の意味するもの
型と命題の同一視　Curry-Howard対応

- 型の理論では、すべての命題がある型（すなわち、その命題の証明の型）に対応する。そして、すべての型は、命題（すなわち、その型が項を持つという命題）とみなすことができる。
- 例えば、A ≅ Bという命題には、AとBとの同型の型 $\mathsf{Iso}(A, B)$ が対応する。（以下で X ≈ Yは、「XとYは対応する」を表す）

  $$\text{“}A \cong B\text{”} \approx \mathsf{Iso}(A, B)$$

  同様に、$\mathsf{Id}_U(A, B)$ という型には、AとBは同一の型であるという命題 $A =_U B$ が対応する。

  $$\text{“}A =_U B\text{”} \approx \mathsf{Id}_U(A, B).$$

- 以下では、型の理論の慣例（ Curry-Howard対応）に従って、型と命題を同一視することにする。

A ≅ B と $A =_U B$

- 同型関係は、反射的なので、次のような写像があることを示すことができる。

$$(A =_U B) \to (A \cong B),$$

- もし、AとBが集合なら、後述のUnivalence Axiomを使えば、この写像自身が、同型であることを示すことができる。

$$(A =_U B) \cong (A \cong B).$$

- これは、次のような写像が存在することを意味する。

$$(A \cong B) \to (A =_U B)$$

これは、「同型なものは、同じものである」という、構造主義の原理である。

等価性　Equivalence

- Voevodsky は、射 f：A → B が、equivalent「等価である」という概念に、次のような単純で統一的な定義を与えた。

1. もし、AとB が集合であるなら、それは集合間の全単射（一対一対応のこと）である。
2. もし、AとB が命題であるなら、それは命題間の論理的等価性である。
3. もし、AとB がgroupoids であるなら、それはgroupoid間のカテゴリー的等価性である。

Voevodskyの Univalence Axiom

- Voevodskyの Univalence Axiom は、先のA, Bが集合の場合の $(A =_U B) \cong (A \cong B).$ をもっと一般的な形で述べたものである。

- $$(A =_U B) \simeq (A \simeq B),$$

  すなわち、「二つのものの同一性は、二つのものの等価性と等価である」

Univalence Axiomから導かれるもの

- 構造主義の原理
  - 二つの同型な集合は等しい
  - 二つの同型な代数的構造は等しい
- 統価原理 Univalence Axiom
  - 二つの (カテゴリー的に) 等価なgroupoid は等しい
  - 二つの等価なカテゴリーは等しい
- ライプニッツの原理
  - aとbが等しいなら、aのすべての性質は、bの性質でもある

用語と訳語、概念の整理

「同じ」に関連した用語と記号

- 同一　Ident　　“ = ”　　同一性　Identity
- 同型　Isomorphic　“ ≅ ”　　同型性　Isomorphy
- 等価　Equivalent　“ ≃ ”　　等価性　Equivalent

「同じ」に関連した用語と記号

- 同一　Ident　　“ = ”　　同一性　Identity
- 同型　Isomorphic　“ ≅ ”　　同型性　Isomorphy
- 等価　Equivalent　“ ≃ ”　　等価性　Equivalence

- 対応関係　　“ ≈ ”
- ホモトピー同値　　“ ～ ”

「同じ」に関連した原理

- ライプニッツの原理

  「 *A*と*B*が同一なら、AとBはすべて同じ性質を持つ。」

$$A = B \;:=\; \forall P.\; P(A) \Rightarrow P(B),$$

- 構造主義の原理

  「同型な対象は同一である」

$$A \cong B \;\Rightarrow\; \mathsf{Id}_U(A, B)$$

- 不変性の原理

  「すべての定義可能な性質は、同型のもとで不変である」

$$\frac{A \cong B \qquad P(A)}{P(B)}$$

「同じ」に関連した原理

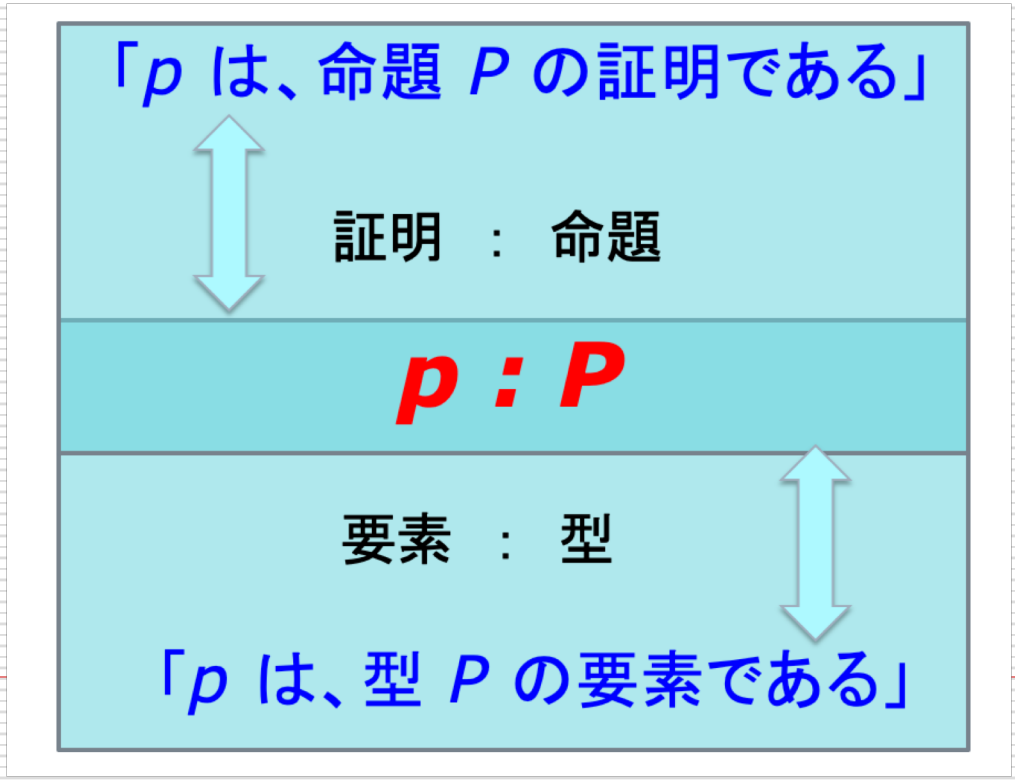
- Voevodskyの統価公理（ Univalence Axiom ）

「二つのものの同一性は、二つのものの等価性と等価である」

$$(A =_U B) \simeq (A \simeq B),$$

Curry-Howard 対応

- 型の理論では、すべての命題がある型（すなわち、その命題の証明の型）に対応する。そして、すべての型は、命題（すなわち、その型が項を持つという命題）とみなすことができる。



Homotopy Type Theory

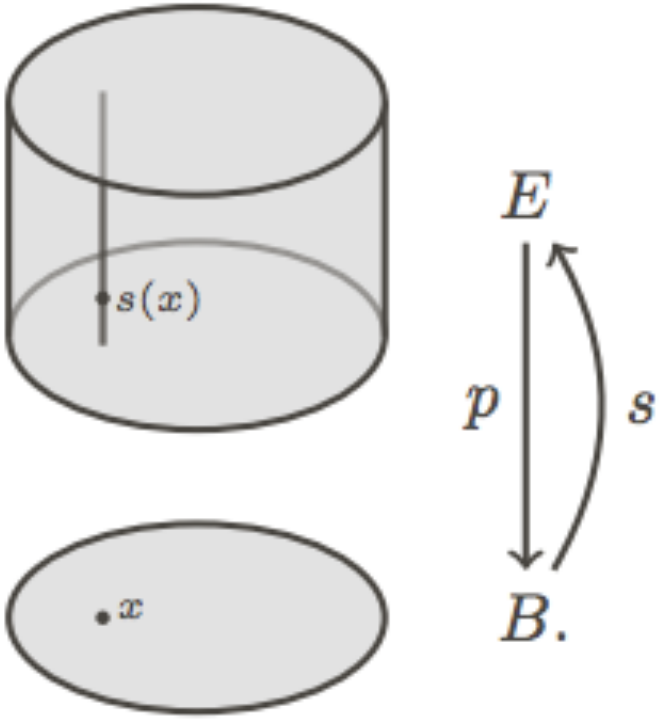
"The HoTT Book"

https://homotopytypetheory.org/book/

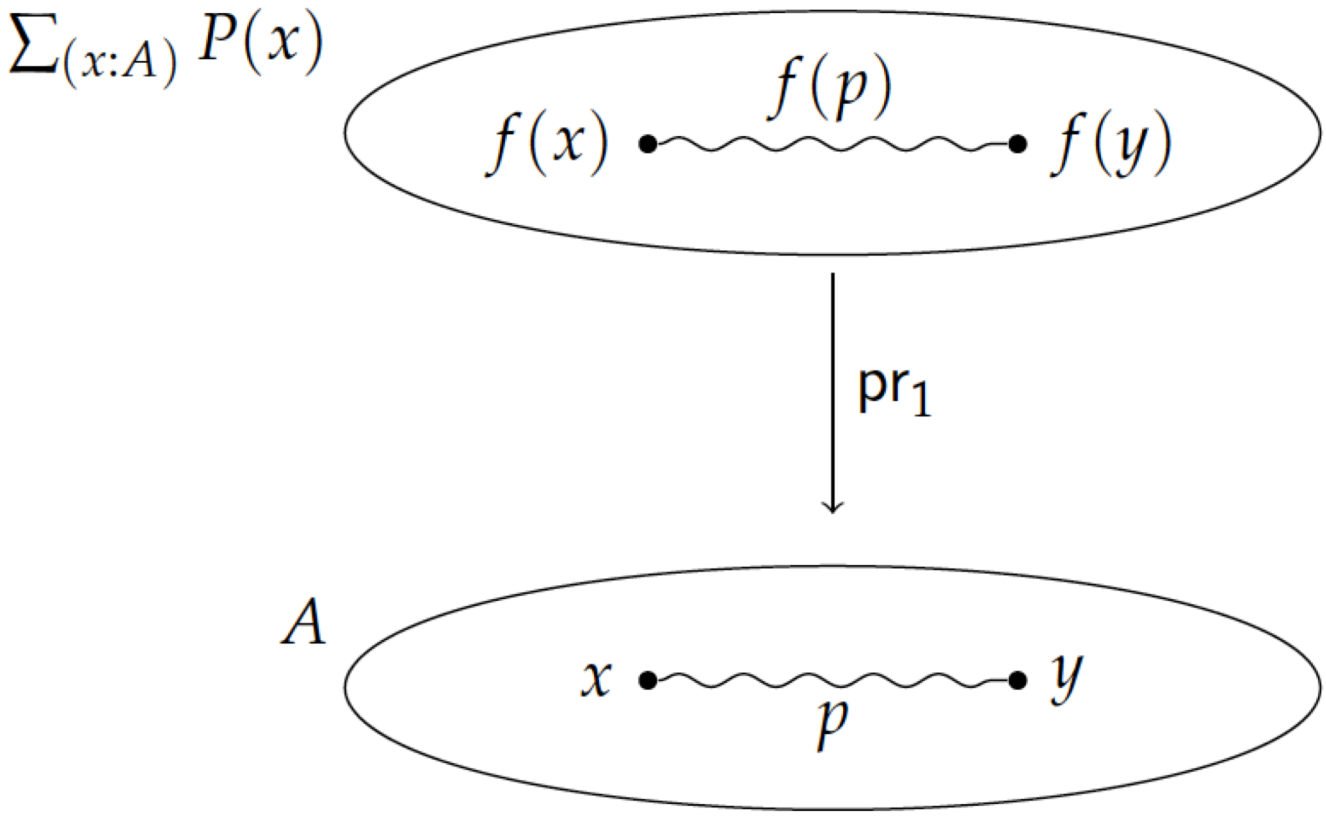
HoTTでのDependent Typeの解釈

$(E_x)_{x \in B}$

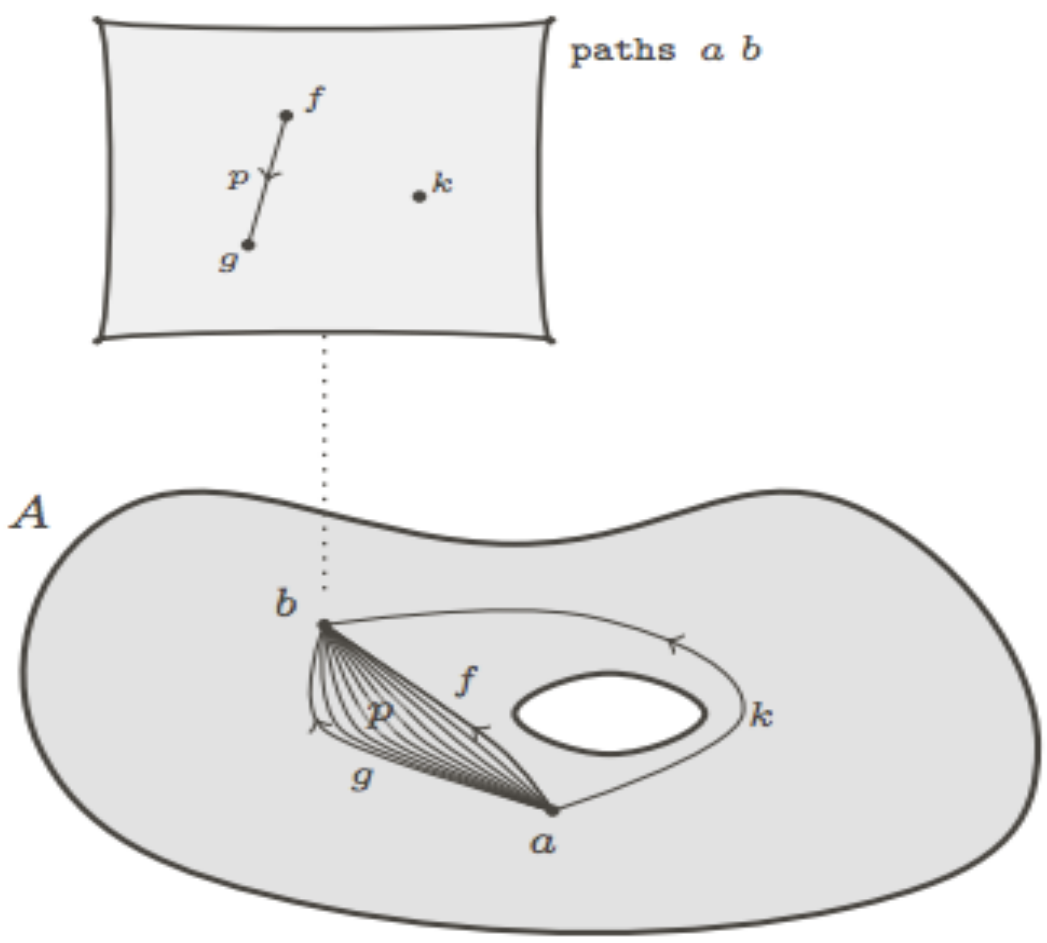
Bの値で、
パラメータ
ー化されたE



type theory		*homotopy theory*
$(x : B)$	$E(x)$	$p : E \to B$ is a fibration over B
$(x : B)$	$s(x) : E(x)$	s is a section of p


$\sum_{(x:A)} P(x)$
$f(p)$
$f(x)$
$f(y)$
pr_1
A
x
y
p

HoTTでの同一性の解釈



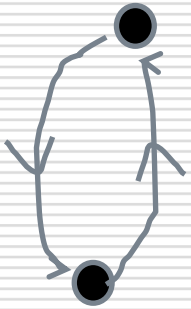
空間Aの中で、
点aと点bをつなぐ「道」がある時、
aとbは、同じものと見なす。
「道」自体は、連続的に変化しうる。
その同一性は、
homotopyが
与える

Equality	Homotopy	∞-Groupoid
reflexivity	constant path	identity morphism
symmetry	inversion of paths	inverse morphism
transitivity	concatenation of paths	composition of morphisms

reflexivity

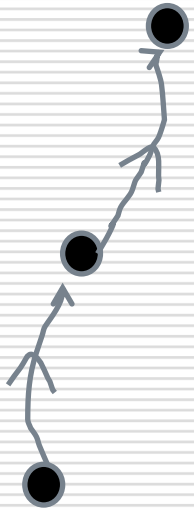
a = a

symmetry



a = b → b = a

transitivity

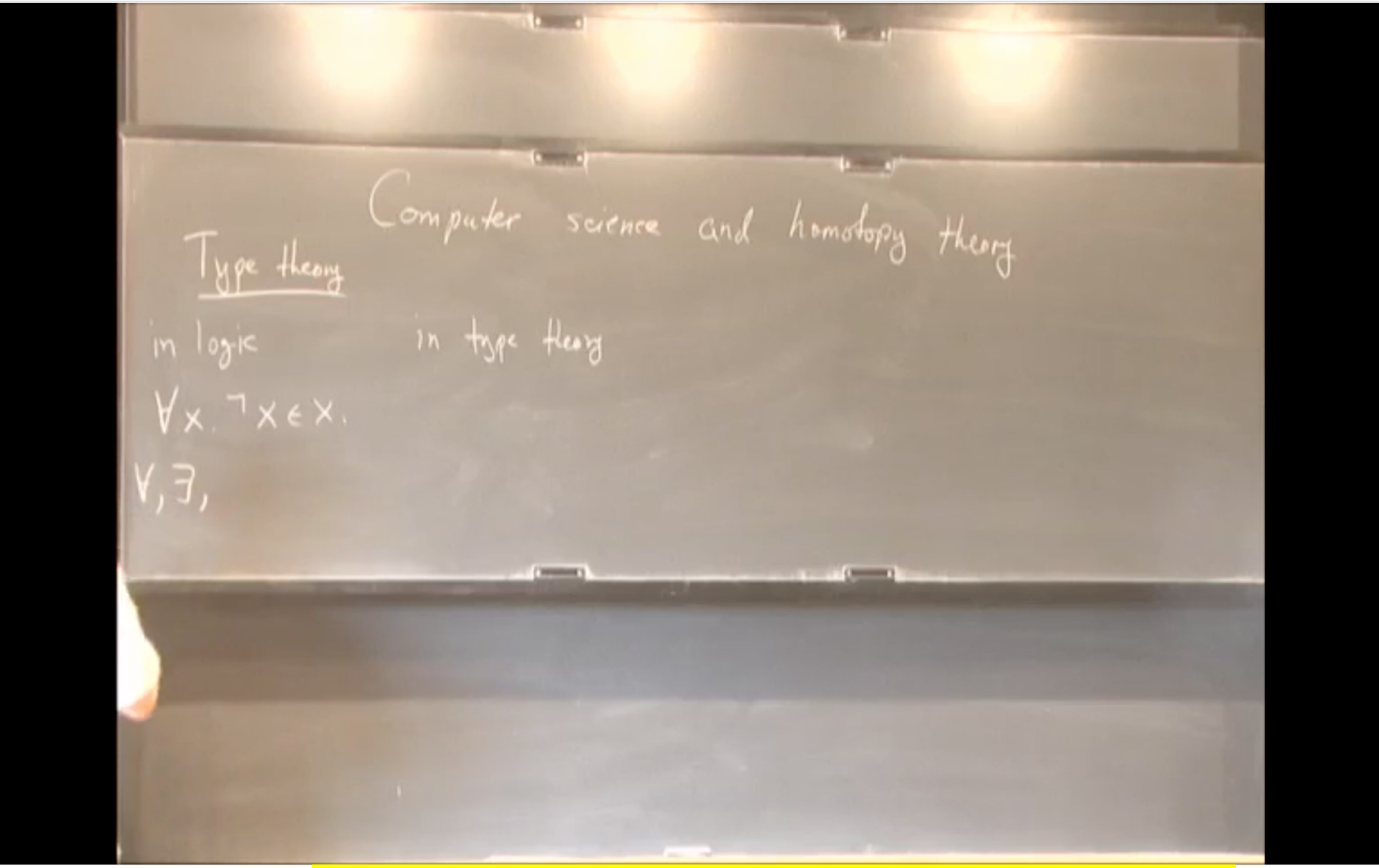


a = b & b = c → a = c

Voevodskyと数学でのコンピュータの利用

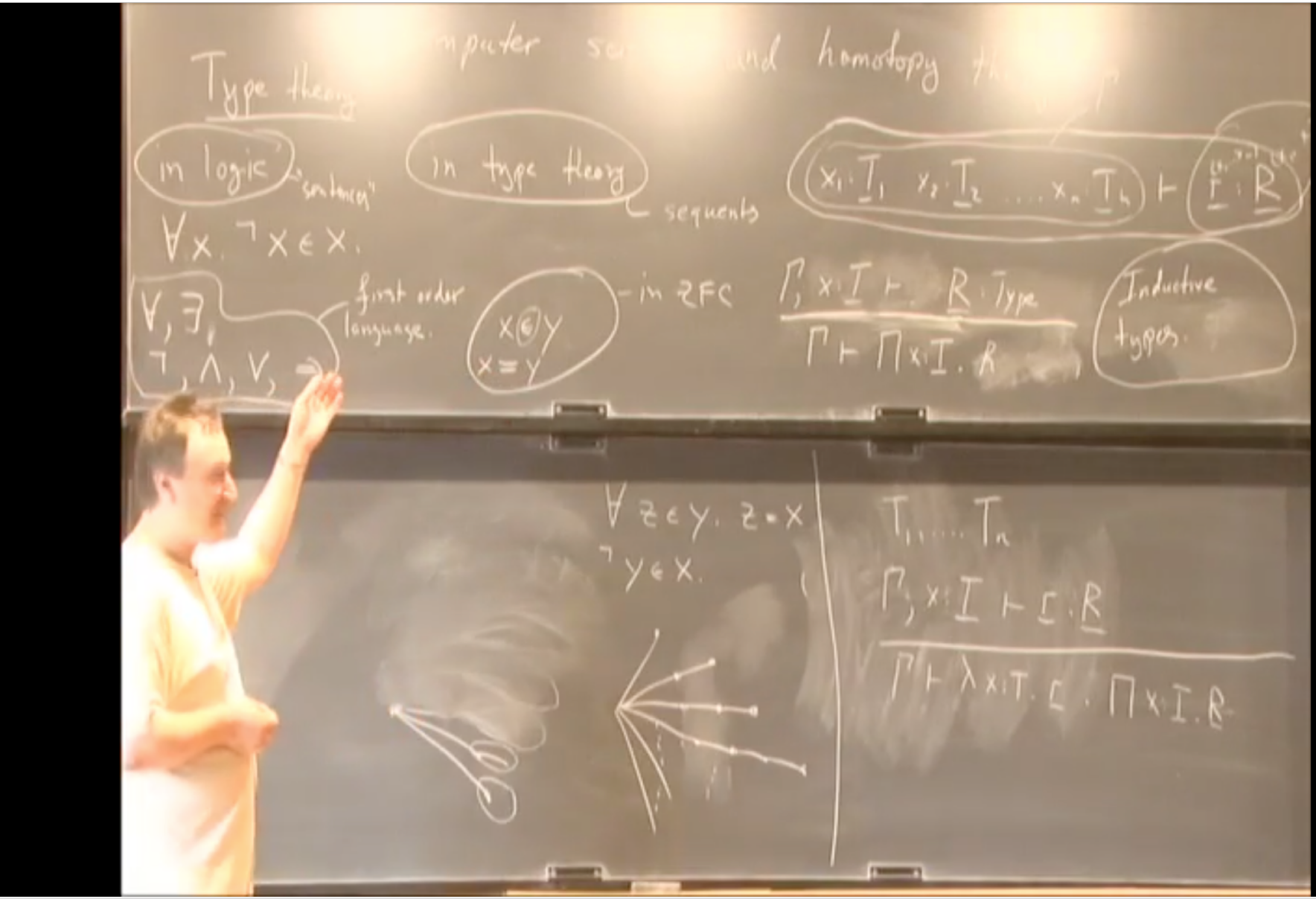
- 昨年亡くなったVoevodskyは、Milner予想、Bloch-Kato予想を解くなど、代数幾何でグロタンディックが進もうとした道で、大きな業績を残した。Voevodskyの最後の仕事は、数学の基礎とコンピュータに関係していた。
- 彼は、数学の証明に、コンピュータを使うべきだと主張した最初の数学者の一人で、また、そのためのコンピュータによる証明支援システムのライブラリーUniMthを開発した。
- GitHub: https://github.com/UniMath/UniMath
- 2016年9月の講演 "UniMath - a library of mathematics formalized in the univalent style" https://goo.gl/3sJr1M

Computer Science and Homotopy Type



https://www.youtube.com/watch?v=UvDeVqzcw4k

Computer Science and Homotopy Type



https://www.youtube.com/watch?v=UvDeVqzcw4k

Voevodskyの経験

- 2000年頃、彼は1993年に自分が発表した論文の重要な補題が間違っていたことに気づく。でも、その頃には、その論文は広く出回っていて、多くの数学者がその証明を「信じて」いた。彼が、その間違った補題なしでも、論文の結論が正しいことを証明できたのは、2006年になってからだった。
- 別のこともあった。1998年に共著で彼が発表した論文の証明に対して、「正しくない」という批判が出される。結論的には、彼は、正しかったのだが、彼が、最終的に、自分が正しいことを確信できたのは、2013年になってからだった。
- （このあたりの経緯は、"The Origins and Motivations of Univalent Foundations" https://goo.gl/LW2Wcq に、詳しく触れられている。）

21世紀の数学の形式

- ヴォヴォスキーは、考える。「数学が、累積的（accumulative）な性格を持つのなら、もしも、そこに誤りが紛れ込むと、それも、累積する可能性がある。」
- ワイルズのフェルマーの定理の1993年の証明には、誤りがあった。それが修正されたのは、1995年のことだ。どんどん複雑化して高度化する数学の「証明」の正しさをチェックするのは難しい。数学者の「証明」が正しいという保証はないのだ！
- ヴォヴォスキーは、数学の証明は、コンピュータでチェックできるプログラムの形を取るべきだと主張し、実際に、それを実行してみせた。
- この流れは、21世紀の数学の形式を、大きく変えていくだろう。