Phase (ring) homomorphisms

H. Miller-Bakewell

February 2, 2020

In this talk

- What is a phase ring homomorphism?

In this talk

- What is a phase ring homomorphism?
- Phase homomorphisms and semantics

In this talk

- What is a phase ring homomorphism?
- Phase homomorphisms and semantics
- Phase homomorphisms and proofs

In this talk

- What is a phase ring homomorphism?
- Phase homomorphisms and semantics
- Phase homomorphisms and proofs
- ZX

In this talk

- What is a phase ring homomorphism?
- Phase homomorphisms and semantics
- Phase homomorphisms and proofs
- ZX
- Galois Theory

In this talk

- What is a phase ring homomorphism?
- Phase homomorphisms and semantics
- Phase homomorphisms and proofs
- ZX
- Galois Theory
- Conclusion

Phase ring homomorphisms

In the languages ZW, ZH, RingZX, (SemiringZX?,) and RING

Phase ring homomorphisms

In the languages ZW, ZH, RingZX, (SemiringZX?,) and RING

Start with a non-trivial ring homomorphism $\phi : R \to S$

Phase ring homomorphisms

In the languages ZW, ZH, RingZX, (SemiringZX?,) and RING

Start with a non-trivial ring homomorphism $\phi : R \to S$

(Doesn't send everything to 0)

Phase ring homomorphisms

Given a non-trivial ring homomorphism $\phi : R \to S$

Phase ring homomorphisms

Given a non-trivial ring homomorphism $\phi : R \to S$

We get the map of matrices $\tilde{\phi} : R\text{-bit} \to S\text{-bit}$

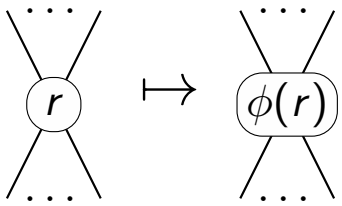
Phase ring homomorphisms

Given a non-trivial ring homomorphism $\phi : R \to S$

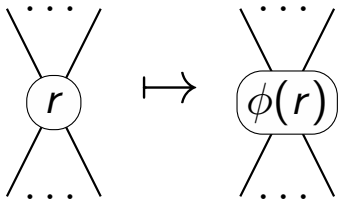
We get the map of matrices $\tilde{\phi} : R\text{-bit} \to S\text{-bit}$

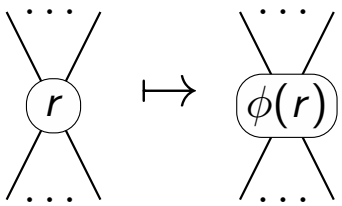
And the map of diagrams $\hat{\phi}$ acting on phases

Acting on phases

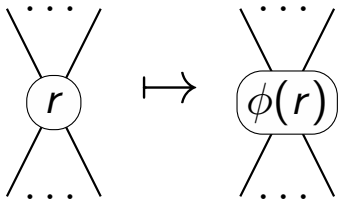
In RING, $\hat{\phi}$: 

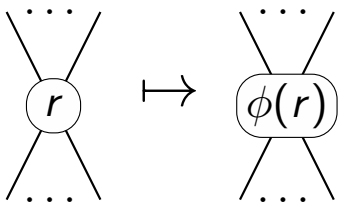
Acting on phases

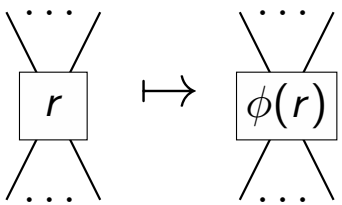
In RING, $\hat{\phi}$: 

In ZW, $\hat{\phi}$: 

Acting on phases

In RING, $\hat{\phi}$: 

In ZW, $\hat{\phi}$: 

In ZH, $\hat{\phi}$: 

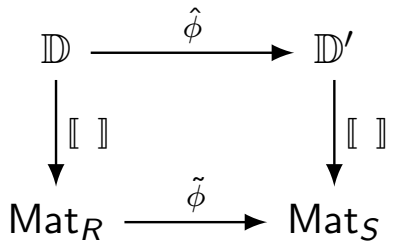
No ZX yet

We'll cover ZX later

Phase ring homomorphisms and semantics

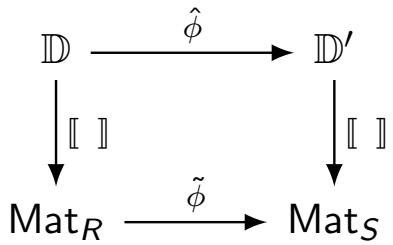
Semantics

The following diagram commutes for ZW, ZH, SemiringZX, RingZX and RING



Semantics

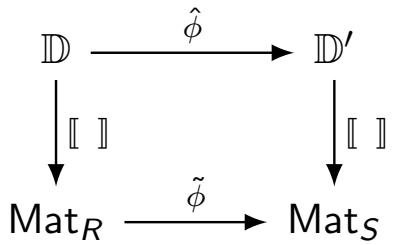
The following diagram commutes for ZW, ZH, SemiringZX, RingZX and RING



$$\left[\!\left[\ \hat{\phi}(\cdot)\ \right]\!\right] = \tilde{\phi}([\![\ \cdot\ ]\!])$$

Semantics

The following diagram commutes for ZW, ZH, SemiringZX, RingZX and RING



$$\left[\!\left[\hat{\phi}(\cdot) \right]\!\right] = \tilde{\phi}([\![\cdot]\!])$$

(Need to check the generators of each language)

Semantics

So if the equation $A = B$ is sound

Semantics

So if the equation $A = B$ is sound

Then the equation $\hat{\phi}A = \hat{\phi}B$ is also sound

Semantics

So if the equation $A = B$ is sound

Then the equation $\hat{\phi}A = \hat{\phi}B$ is also sound

$$[\![\hat{\phi}A]\!] = \tilde{\phi}\,[\![A]\!] = \tilde{\phi}\,[\![B]\!] = [\![\hat{\phi}B]\!]$$

Semantics

Theorem

Phase ring homomorphisms preserve soundness

$$\text{RING}_R \vDash A = B \qquad \Longrightarrow \qquad \text{RING}_S \vDash \hat{\phi} A = \hat{\phi} B$$

Example

$$R = S = \mathbb{Q}[i, \sqrt{2}]$$

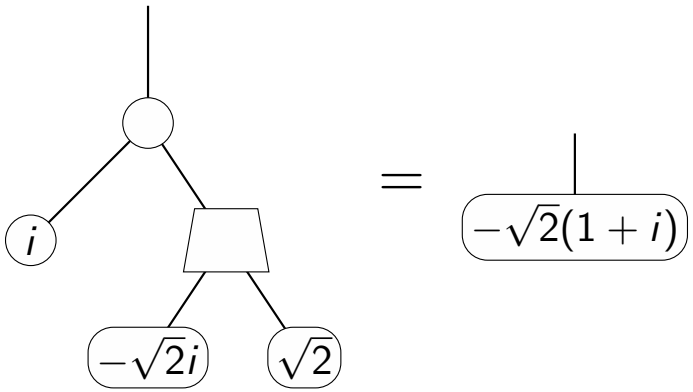
Example

$$R = S = \mathbb{Q}[i, \sqrt{2}]$$

$$\sigma : i \mapsto -i$$
$$\tau : \sqrt{2} \mapsto -\sqrt{2}$$

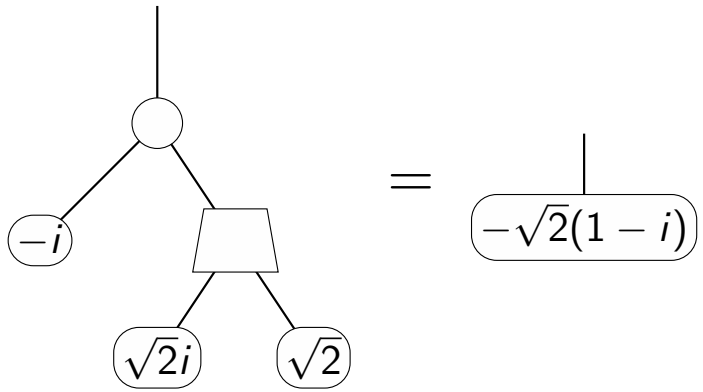
Example

The following $\mathrm{RING}_{\mathbb{Q}[i,\sqrt{2}]}$ equation is sound:



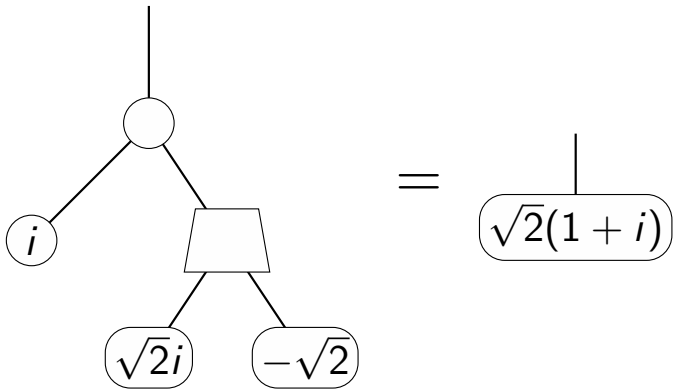
Example

$\hat{\sigma}$



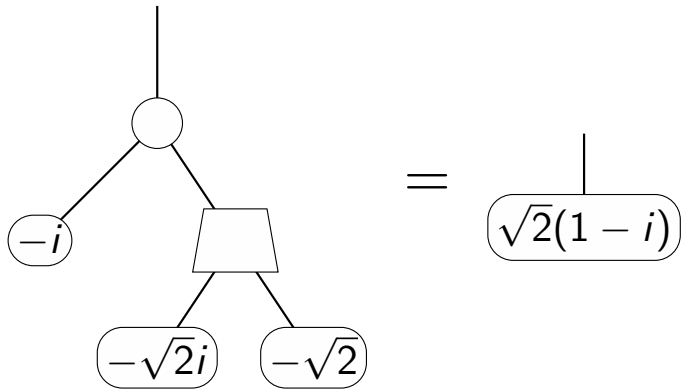
Example

$\hat{\tau}$



Example

$\hat{\sigma}\hat{\tau}$



Phase ring homomorphisms and proofs

Syntax

Given a proof in RING_R, ZW_R, $\mathrm{SemiringZX}_R$, RingZX_R, or ZH_R

$$A_1 = A_2 = \cdots = A_n$$

Syntax

Given a proof in RING_R, ZW_R, $\mathrm{SemiringZX}_R$, RingZX_R, or ZH_R

$$A_1 = A_2 = \cdots = A_n$$

Then the following is a proof, using the same proof steps, in RING_S, $\mathrm{SemiringZX}_S$, RingZX_S, ZW_S, or ZH_S

$$\hat{\phi}A_1 = \hat{\phi}A_2 = \cdots = \hat{\phi}A_n$$

Syntax

First show, for each language, that $\hat{\phi}$ preserves rules

Syntax

First show, for each language, that $\hat{\phi}$ preserves rules

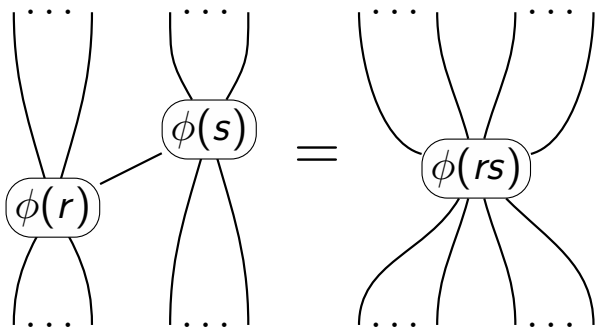
$L \longrightarrow\!\triangleright R$ a rule in RING_R

$\hat{\phi}L \longrightarrow\!\triangleright \hat{\phi}R$ a (restriction of a) rule in RING_S

(Just looking for problems with constants or side conditions)

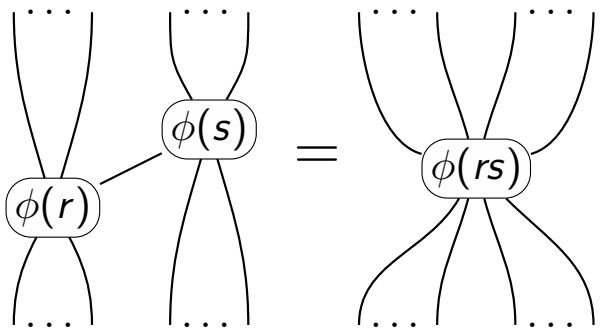
Example

An example of the spider fusion rule in ZW_R / RING_R under the action of $\hat{\phi}$:



Example

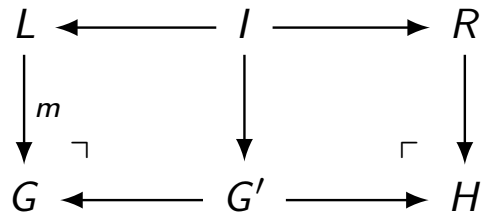
An example of the spider fusion rule in ZW_R / RING_R under the action of $\hat{\phi}$:



This is the white spider fusion rule in ZW_S / RING_S, but restricted to the image of ϕ

Syntax

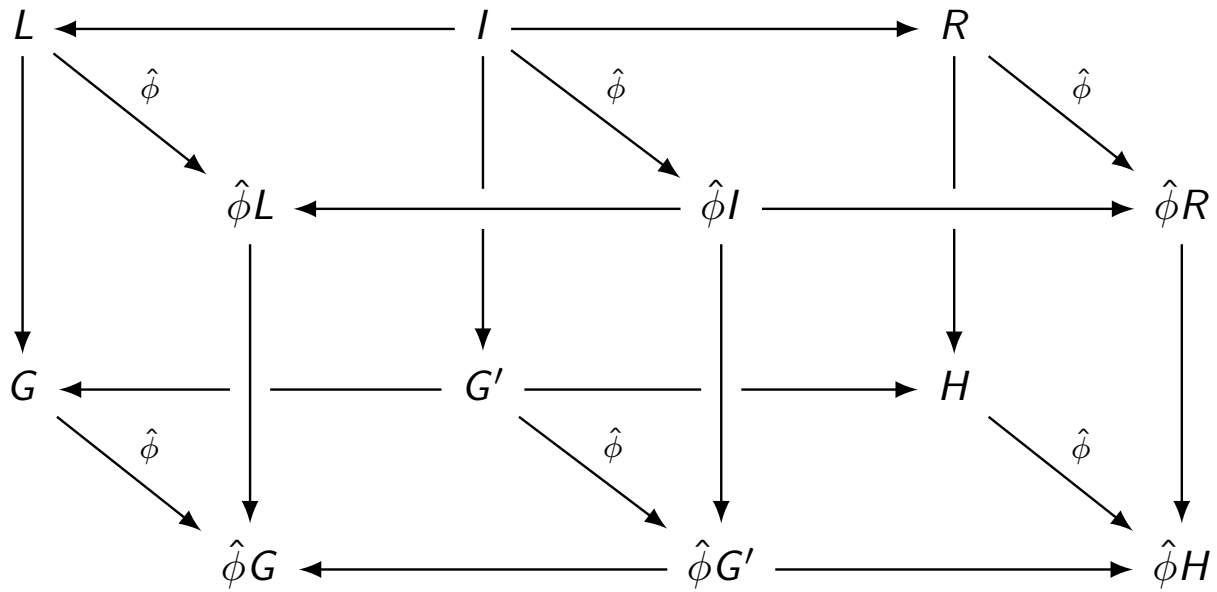
Recall that rule applications are actually double pushout diagrams



(This is the matching of L into G, and replacing L with R to get H)

Syntax

So show that the following double double pushout diagram commutes, and that the front rectangle is a double pushout diagram:



Syntax

So every rule application in the proof

$$A_1 = A_2 = \cdots = A_n$$

Is translated into a valid rule application in the proof

$$\hat{\phi} A_1 = \hat{\phi} A_2 = \cdots = \hat{\phi} A_n$$

Syntax

Theorem

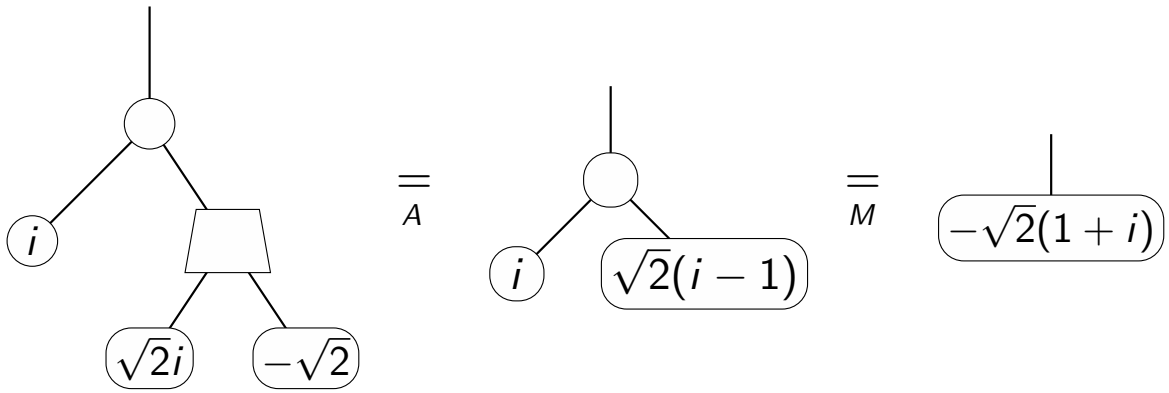
Phase ring homomorphisms preserve proofs

$$\text{RING}_R \vdash A = B \qquad \Longrightarrow \qquad \text{RING}_S \vdash \hat{\phi} A = \hat{\phi} B$$

Example

The $\mathrm{RING}_{\mathbb{Q}[i,\sqrt{2}]}$ proof

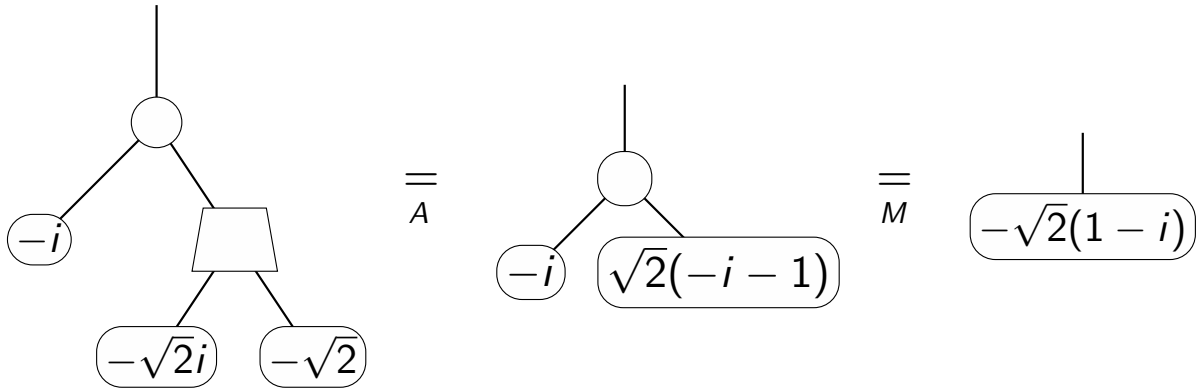
$$\mathrm{RING}_{\mathbb{C}} \vdash A = B$$



Example

Is translated using the field automorphism $\sigma : i \mapsto -i$

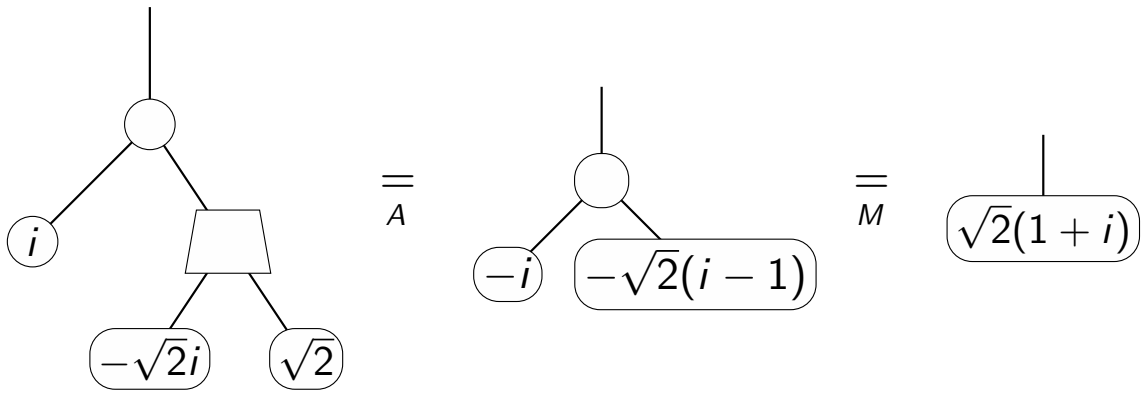
$$\mathrm{RING}_{\mathbb{C}} \vdash \hat{\sigma} A = \hat{\sigma} B$$



Example

Or $\tau : \sqrt{2} \mapsto -\sqrt{2}$

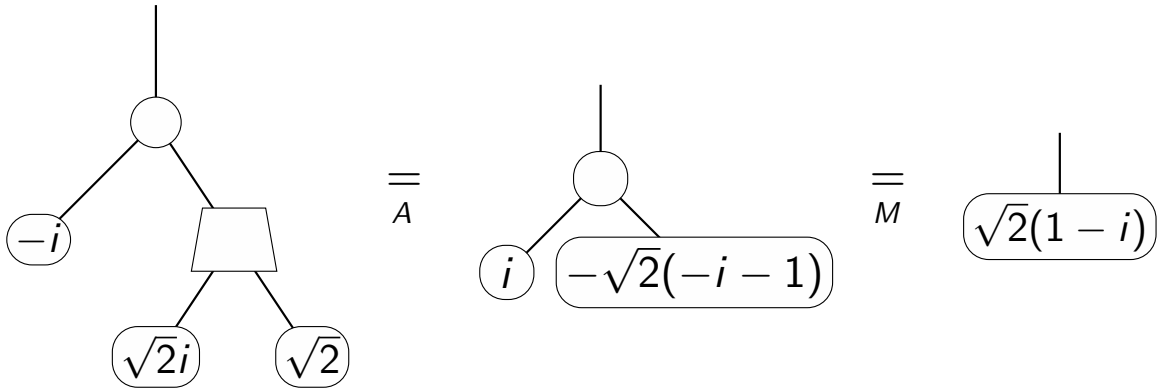
$$\mathrm{RING}_{\mathbb{C}} \vdash \hat{\tau} A = \hat{\tau} B$$



Example

Or $\sigma\tau : \sqrt{2} \mapsto -\sqrt{2}, i \mapsto -i$

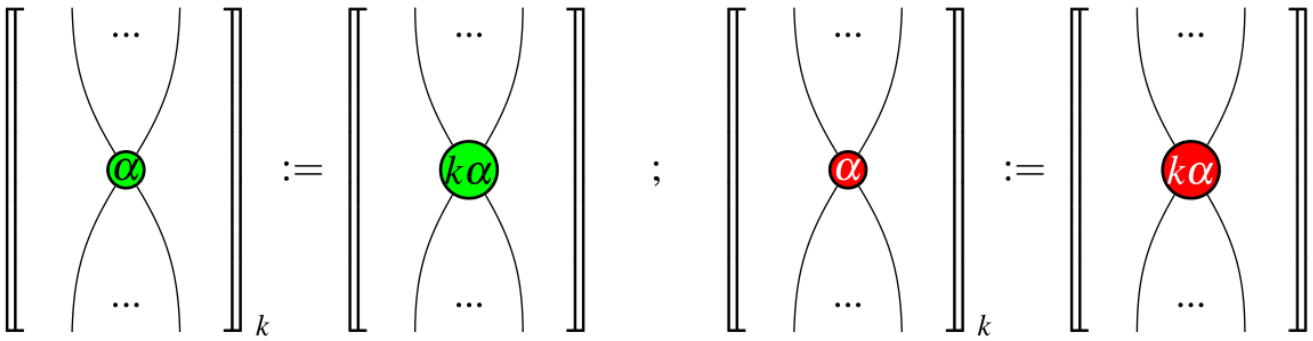
$$\mathrm{RING}_{\mathbb{C}} \vdash \hat{\sigma}\hat{\tau}A = \hat{\sigma}\hat{\tau}B$$



Do phase homomorphisms seem familiar?

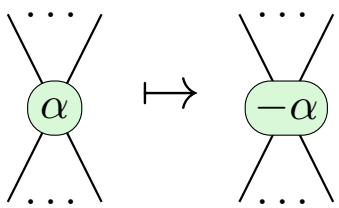
Incompleteness

Similar constructions were used for the incompleteness proofs (Schröder de Witt and Zamdzhiev, 2014)



Complex conjugation

Or complex conjugation in ZX



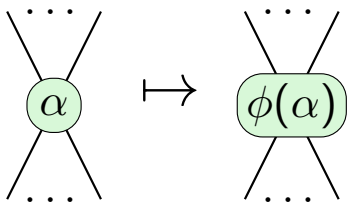
ZX

Phase group homomorphisms

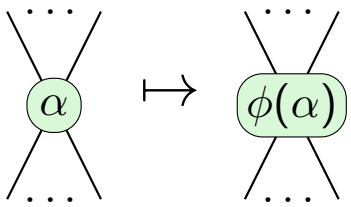
We can't lift a group homomorphism $\phi : G \to H$ directly to a ring homomorphism $R \to S$

But we can still make $\hat{\phi}$ on diagrams

Phase group homomorphisms

So take $\hat{\phi}$: 

Phase group homomorphisms

So take $\hat{\phi}$: 

and find $\tilde{\phi} : R \to S$ such that this diagram commutes

$$\begin{array}{ccc} \mathbb{D} & \xrightarrow{\hat{\phi}} & \mathbb{D}' \\ \downarrow{\scriptstyle [\![\ ]\!]} & & \downarrow{\scriptstyle [\![\ ]\!]} \\ \mathsf{Mat}_R & \xrightarrow{\tilde{\phi}} & \mathsf{Mat}_S \end{array}$$

Phase group homomorphisms

Just looking at endomorphisms and finite fragments of ZX:

Phase group homomorphisms

Just looking at endomorphisms and finite fragments of ZX:

The finite subgroups of $[0, 2\pi)$ under addition are cyclic of the form $< 2\pi/n >$

Phase group homomorphisms

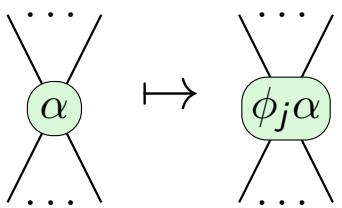
Just looking at endomorphisms and finite fragments of ZX:

The finite subgroups of $[0, 2\pi)$ under addition are cyclic of the form $< 2\pi/n >$

The group endomorphisms are of the form $\phi_j : 2\pi k/n \mapsto 2\pi jk/n$

Phase group homomorphisms

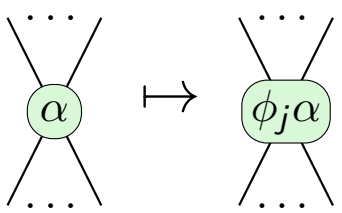
When does this diagram commute for Z spiders?



$$\begin{array}{ccc} \mathbb{D} & \xrightarrow{\hat{\phi}_j} & \mathbb{D}' \\ \downarrow [\![\ ]\!] & & \downarrow [\![\ ]\!] \\ \mathsf{Mat}_R & \xrightarrow{\tilde{\phi}_j} & \mathsf{Mat}_S \end{array}$$

Phase group homomorphisms

When does this diagram commute for Z spiders?

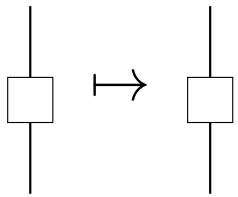


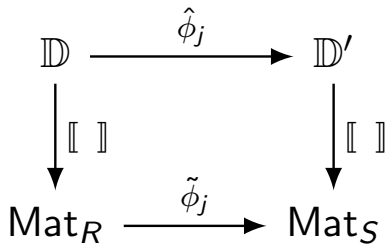
$$\begin{array}{ccc} \mathbb{D} & \xrightarrow{\hat{\phi}_j} & \mathbb{D}' \\ \downarrow [\![\ ]\!] & & \downarrow [\![\ ]\!] \\ \mathsf{Mat}_R & \xrightarrow{\tilde{\phi}_j} & \mathsf{Mat}_S \end{array}$$

$\tilde{\phi}_j$ is a ring homomorphism (so fixes 0, 1, etc.,) and $\tilde{\phi}_j : e^{i\alpha} \mapsto e^{ji\alpha}$

Phase group homomorphisms

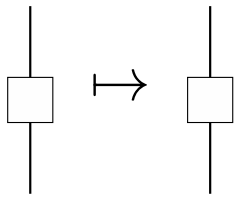
When does this diagram commute for Hadamard nodes?

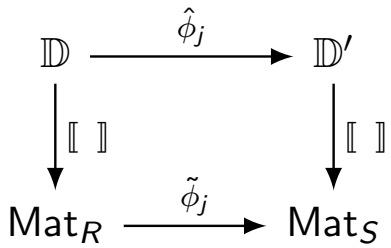




Phase group homomorphisms

When does this diagram commute for Hadamard nodes?





Only when $\tilde{\phi}$ fixes $\frac{1}{\sqrt{2}}$

Clifford+T Example

Group endo.	$\mathbb{Z}[\frac{1}{2}, i, \sqrt{2}]$ endo.	$\tilde{\phi}$?
ϕ_0	–	–
ϕ_1	Identity	Identity
ϕ_2	–	–
ϕ_3	τ	–
ϕ_4	–	–
ϕ_5	$\sigma\tau$	–
ϕ_6	–	–
ϕ_7	σ	Complex conjugation

Beyond Clifford+T

For a finite fragment of ZX that contains $\pi/4$, a group endomorphism ϕ_j lifts to a phase group homomorphism if and only if $j \equiv 1$ or 7 modulo 8

Beyond Clifford+T

Using the rules RZX from ‘A Generic Normal Form for ZX-Diagrams and Application to the Rational Angle Completeness’ (Jeandel, Perdrix, Vilmart, 2019)

Beyond Clifford+T

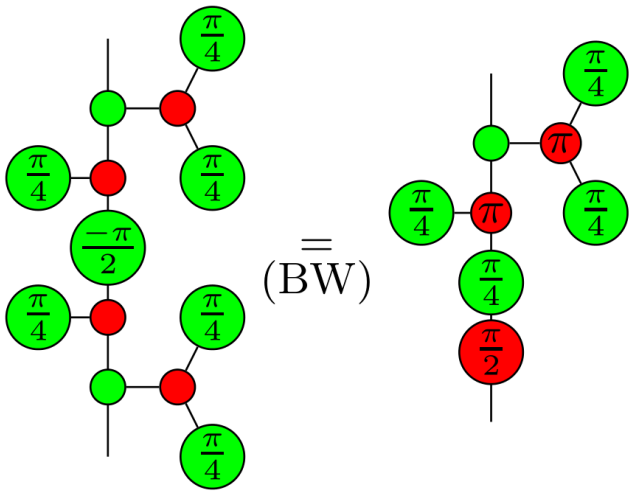
Using the rules RZX from 'A Generic Normal Form for ZX-Diagrams and Application to the Rational Angle Completeness' (Jeandel, Perdrix, Vilmart, 2019)

For a finite fragment of ZX that contains $\pi/4$, a group endomorphism ϕ_j lifts to an RZX-proof preserving map if and only if $j \equiv 1 \bmod 8$, i.e.

$$RZX \vdash A = B \quad \Longrightarrow \quad RZX \vdash \hat{\phi}_j A = \hat{\phi}_j B$$

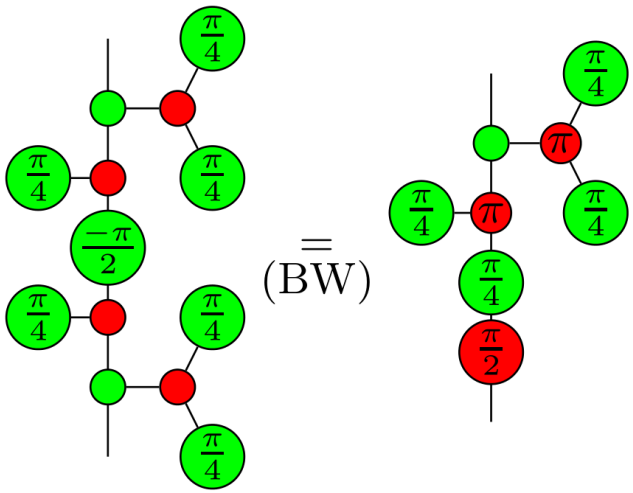
BW rule

Why not $j \equiv 7 \bmod 8$? Because the (BW) rule is part of RZX:



BW rule

Why not $j \equiv 7 \bmod 8$? Because the (BW) rule is part of RZX:



Which is not mapped by ϕ_7 to a rule in RZX (it's mapped to something sound, but not to a rule. Easy to repair.)

Galois Theory

Finite verification

Given a ZX, ZW, RING, RingZX, or ZH (but not SemiringZX) equation involving phase variables, we can verify that equation is sound by checking 'enough' values of that variable.

(Finite Verification for Infinite Families of Diagram Equations, 2019)

Finite verification

But we saw that phase homomorphisms generate new, sound equations from old

Finite verification

But we saw that phase homomorphisms generate new, sound equations from old

So by choosing the right value for our phase variables...

Finite verification

But we saw that phase homomorphisms generate new, sound equations from old

So by choosing the right value for our phase variables...

... we can generate 'enough' sound equations just from the phase homomorphisms

Galois groups

Given two fields $L \subset K$ the automorphisms of K that fix L form a group

Galois groups

Given two fields $L \subset K$ the automorphisms of K that fix L form a group

Under certain conditions we call this the Galois group, and it has desirable properties (like knowing how large it is)

Finite verification

Plan, working over qubits:

- Find a field L that contains every constant phase in our equation

Finite verification

Plan, working over qubits:

- Find a field L that contains every constant phase in our equation
- Construct a field extension K large enough for our purposes, ensuring K over L is Galois

Finite verification

Plan, working over qubits:

- Find a field L that contains every constant phase in our equation
- Construct a field extension K large enough for our purposes, ensuring K over L is Galois
- Choose suitable elements of that larger field as the values for our phase variables

Finite verification

Plan, working over qubits:

- Find a field L that contains every constant phase in our equation
- Construct a field extension K large enough for our purposes, ensuring K over L is Galois
- Choose suitable elements of that larger field as the values for our phase variables
- We get the Galois group of field automorphisms by construction

Finite verification

Plan, working over qubits:

- Find a field L that contains every constant phase in our equation
- Construct a field extension K large enough for our purposes, ensuring K over L is Galois
- Choose suitable elements of that larger field as the values for our phase variables
- We get the Galois group of field automorphisms by construction
- Because field automorphisms extend to phase ring homomorphisms, we have found a verifying set of equations

Finite verification

Plan, working over qubits:

- Find a field L that contains every constant phase in our equation
- Construct a field extension K large enough for our purposes, ensuring K over L is Galois
- Choose suitable elements of that larger field as the values for our phase variables
- We get the Galois group of field automorphisms by construction
- Because field automorphisms extend to phase ring homomorphisms, we have found a verifying set of equations
- Tweak all this to work with ZX

Single equation verification

For a $\mathrm{RING}_{\mathbb{C}}$, $\mathrm{ZW}_{\mathbb{C}}$, $\mathrm{RingZX}_{\mathbb{C}}$, or $\mathrm{ZH}_{\mathbb{C}}$ equation with phases that are polynomial in some phase variables, there exists a single verifying equation without any phase variables.

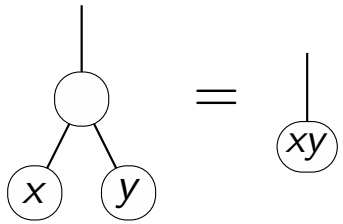
Single equation verification

For a $\mathrm{RING}_{\mathbb{C}}$, $\mathrm{ZW}_{\mathbb{C}}$, $\mathrm{RingZX}_{\mathbb{C}}$, or $\mathrm{ZH}_{\mathbb{C}}$ equation with phases that are polynomial in some phase variables, there exists a single verifying equation without any phase variables.

If we can put an upper bound on the degrees of the minimal polynomials of the phase constants then we can construct such an equation.

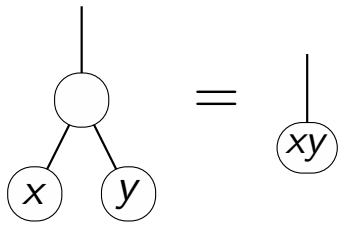
Example

Consider the $\mathrm{RING}_{\mathbb{C}[x,y]}$ equation



Example

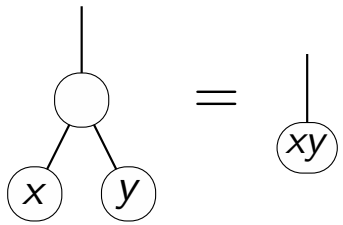
Consider the $\mathrm{RING}_{\mathbb{C}[x,y]}$ equation



By the earlier verification work we require sets A_x and A_y, with sizes $d_x \geq 2$ and $d_y \geq 2$.

Example

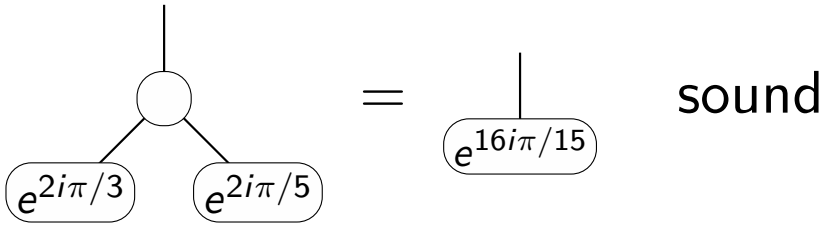
Consider the $\mathrm{RING}_{\mathbb{C}[x,y]}$ equation



By the earlier verification work we require sets A_x and A_y, with sizes $d_x \geq 2$ and $d_y \geq 2$.

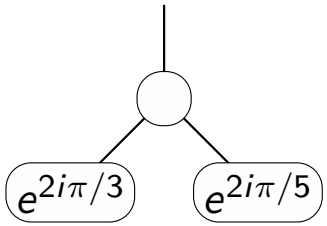
Choose $x = e^{2i\pi/3}$ and $y = e^{2i\pi/5}$,

Example

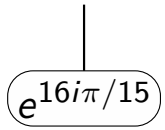


sound

Example

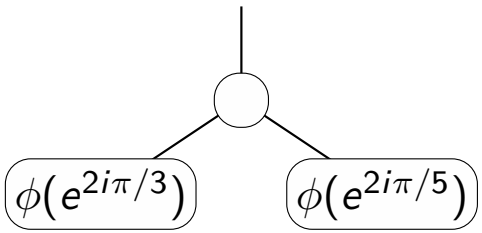


$=$

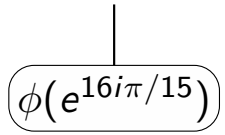


sound

$\Longrightarrow$



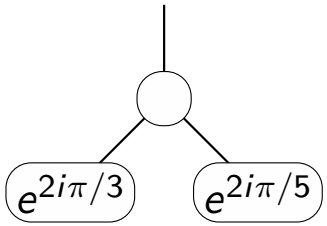
$=$



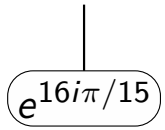
sound

$\forall \phi \in \mathsf{Gal}(\mathbb{Q}(\omega_3, \omega_5)/\mathbb{Q})$

Example

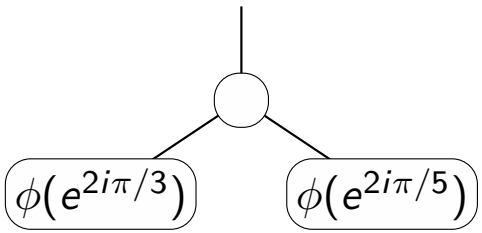


$=$

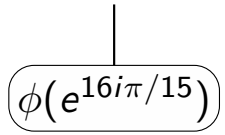


sound

$\Longrightarrow$



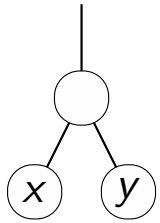
$=$



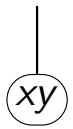
sound

$\forall \phi \in \mathsf{Gal}(\mathbb{Q}(\omega_3, \omega_5)/\mathbb{Q})$

$\Longrightarrow$



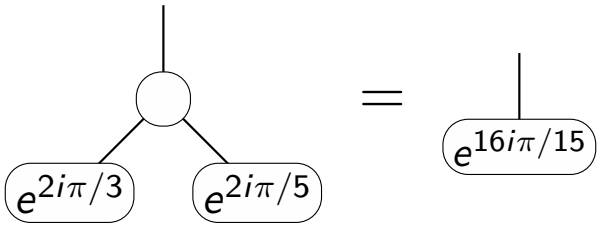
$=$



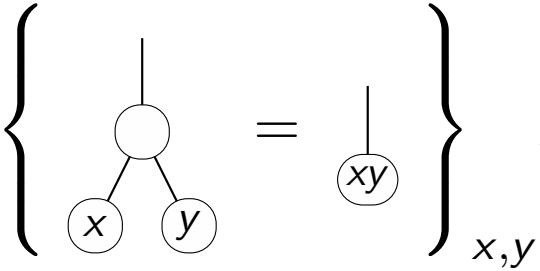
sound $\forall x, y \in \mathbb{C}$

Example

In other words:



implies and is implied by the equation



x, y phase variables

Conclusion

Conclusion

Depending on the language:

Conclusion

Depending on the language:

Phase homomorphisms preserve semantics and proofs

Conclusion

Depending on the language:

Phase homomorphisms preserve semantics and proofs

Over qubits you can verify phase variables with a single equation without any phase variables

Conclusion

Especially for equations with some phases that are not in $\mathbb{Q}$

Conclusion

Especially for equations with some phases that are not in $\mathbb{Q}$

Ask yourself what effect phase homomorphisms would have on it

Conclusion

Especially for equations with some phases that are not in $\mathbb{Q}$

Ask yourself what effect phase homomorphisms would have on it

Any phase that appears less often than its algebraic degree should* be a variable instead

Future work

What next?

Future work

What next?

- Classify phase homomorphisms for Universal ZX and ZQ

Future work

What next?

- Classify phase homomorphisms for Universal ZX and ZQ
- Other double double pushout diagrams

Thank you!