Completeness for Prime-Dimensional Phase-Affine Circuits

Colin Blake
Inria Mocqua and Université de Lorraine, CNRS, LORIA, F-54000 Nancy, France

Equational reasoning about circuits is central in quantum software for validation, optimisation, and verification. For qubits, the CNOT-dihedral fragment supports efficient rewriting via phase polynomials and layered normal forms, yielding a complete and practically effective equational theory. In this work we generalise that CNOT-dihedral picture from qubits to prime-dimensional qudits. We present a compact PROP for reversible affine circuits over a prime field, with a strict symmetric monoidal semantics into the affine group and a Lafont-style affine normal form. We then adjoin finite-angle diagonal phase generators and organise them by polynomial degree, obtaining linear, quadratic (odd prime), and cubic (prime greater than 3) calculi. Using binomial-basis identities we derive uniform transport rules, establish unique phase-affine normal forms, and prove completeness: semantic equality coincides with derivable equality. This yields a prime-dimensional, phase-polynomial-aligned generalisation of the CNOT-dihedral equational theory.

1 Introduction

Quantum circuits are the standard low-level formalism for describing computations on quantum devices. In this model, wires represent quantum systems and gates represent elementary unitary updates. Beyond their foundational role, circuits are the main intermediate language used throughout quantum software stacks, from synthesis and compilation to optimisation, verification, and resource estimation. Many of these tasks reduce to reasoning about circuit equivalence, either to certify that a compilation pass preserves semantics, or to justify local program transformations such as gate cancellations and commutation-based reordering. From the diagrammatic side, complete rewrite systems are available for several key non-universal fragments, including stabiliser quantum mechanics in the qutrit setting and, more generally, in odd prime dimensions, as well as complete rule sets for multi-qutrit Clifford circuits [20, 6, 16, 14].

A large and practically central class of circuit optimisations is algebraic, relying on explicit normal forms and on rewrite rules that realise them. For qubit circuits, the paradigmatic example is the CNOT-dihedral fragment: circuits built from reversible affine updates and a finite-angle diagonal layer admit a phase-polynomial semantics and a layered normal form, which together support efficient reasoning and optimisation [2]. This phase-polynomial viewpoint is also the backbone of T-count and T-depth optimisation, parity network synthesis, and routing heuristics [3, 4, 1, 10, 19, 12]. The goal of this paper is to provide a prime-dimensional generalisation of this CNOT-dihedral presentation: we give compact diagrammatic axiomatisations, normal forms, and completeness theorems for analogous affine-plus-diagonal fragments over $\mathbb{F}_d$.

Higher-dimensional systems can offer both conceptual and quantitative advantages in fault-tolerant and near-term architectures, including improved magic state distillation protocols and potential circuit-size reductions [7, 21, 8]. Prime-dimensional qudits are especially convenient, since arithmetic over $\mathbb{F}_d$ provides a uniform language for reversible classical control, Pauli operators, and the discrete phases that arise in fragments of the Clifford hierarchy. These motivations have led to explicit synthesis and compilation approaches for multiqudit exact circuits in prime dimensions [11]. What has been missing

Submitted to:
QPL 2026

is a compact, complete, and fully diagrammatic equational theory that matches the algebra exploited by phase-polynomial compilation, in the same way that the CNOT-dihedral theory does for qubits [2, 5], and which complements existing complete calculi for stabiliser and Clifford fragments in odd prime dimensions [20, 6, 16, 14].

We develop such a theory for a family of prime-dimensional circuit fragments built from two ingredients. The first ingredient is an affine update of computational-basis labels $x \in \mathbb{F}_d^n$, namely an invertible affine transformation $x \mapsto Ax + b$. Such updates form the affine general linear group $\mathrm{GA}_n(\mathbb{F}_d)$, and they model the reversible classical part of many fault-tolerant and compilation-relevant gate sets. The second ingredient is a diagonal phase layer whose eigenvalues are dth roots of unity. Writing $\omega = e^{2\pi i/d}$, any diagonal unitary in our scope has the form $U_q |x\rangle = \omega^{q(x)} |x\rangle$ for a function $q : \mathbb{F}_d^n \to \mathbb{F}_d$, where only the induced function matters because $\omega^d = 1$. As in the qubit CNOT-dihedral setting, the interaction between the affine update and the diagonal layer is captured by substitution $q \mapsto q \circ g$, and this is the mechanism behind commutation-based optimisation [2]. We organise the diagonal fragments by the total degree of a representing polynomial, yielding linear, quadratic, and cubic phase fragments. This degree stratification both matches the structure exploited in phase-polynomial compilation and isolates the first points where new controlled-diagonal primitives become necessary [2, 11, 12].

The affine core of the paper is a compact presentation $\mathbf{Aff}_d$ for reversible affine circuits over $\mathbb{F}_d$, obtained by specialising Lafont's algebraic theory of circuits to prime fields [13]. The generators are the translation X, the shear CX, and the family of nonzero scalings M_x, together with the symmetric structure. We then adjoin diagonal generators that represent phase functions in a controlled way: a linear phase gate Z (exponent x), a quadratic phase gate S (exponent $\binom{x}{2}$) for odd d, and a cubic phase gate T (exponent $\binom{x}{3}$) for $d > 3$, as well as a scalar generator for global phases. These choices are designed so that the commutation and transport equations needed for layered normal forms are short, local, and uniform.

The semantic content of each fragment is captured by a strict symmetric monoidal groupoid whose morphisms are pairs (g, q), where $g \in \mathrm{GA}_n(\mathbb{F}_d)$ is an affine update and $q : \mathbb{F}_d^n \to \mathbb{F}_d$ is a phase function in the appropriate degree class. Composition is the semidirect-product law $(g_2, q_2) \circ (g_1, q_1) = (g_2 \circ g_1, q_1 + q_2 \circ g_1)$. This is the prime-dimensional analogue of the standard CNOT-dihedral semantics: affine gates update basis labels, diagonal gates contribute a phase evaluated on the current label, and commuting phases across affine gates realises substitution [2]. It also provides a direct bridge to compilation techniques based on phase polynomials and parity networks [3, 4, 19, 12].

The central technical result is completeness by layered normal forms, in direct analogy with the layered normal forms used for qubit CNOT-dihedral circuits [2]. For each fragment, we show that every circuit rewrites to a composite $A \circ D$ where A is an affine normal form and D is a single diagonal normal form layer. The diagonal layer is then rewritten into a fixed syntactic shape similar to the one from [2], while the affine layer is normalised using Lafont-style completeness for affine maps [13]. Uniqueness is proved semantically: a diagonal normal form is uniquely determined by its phase function, using uniqueness of binomial-basis expansions in degrees at most 1, 2, and 3 under the relevant assumptions on d. Combining existence and uniqueness yields a completeness theorem in the usual diagrammatic sense: two circuits are equal in the semantic model if and only if their equality is derivable from the corresponding axiom set.

The main contributions can be summarised as follows.

– For each prime d, we give a compact PROP presentation $\mathbf{Aff}_d$ for reversible affine transformations over $\mathbb{F}_d$, with an explicit interpretation into $\mathrm{GA}_n(\mathbb{F}_d)$ and a normalisation theorem based on Lafont's circuit theory [13].

– We give a prime-dimensional, phase-polynomial-aligned generalisation of the CNOT-dihedral presentation [2], in the form of three phase-extended PROPs $\mathbf{LinPhase}_d$, $\mathbf{QuadPhase}_d$ (for odd d), and $\mathbf{CubicPhase}_d$ (for $d > 3$), presented by small, local axiom sets governing the interaction of affine updates with linear, quadratic, and cubic diagonal phases.

– We establish existence and uniqueness of phase-affine normal forms in each fragment, and deduce completeness: semantic equality implies derivable equality in the corresponding equational theory.

The paper is organised as follows. Section 2 introduces the affine PROP $\mathbf{Aff}_d$, its semantic interpretation, and its affine normal forms. Section 3 extends this core with finite-angle diagonal generators and axiom sets for linear, quadratic, and cubic phases. A uniform normal-form argument then yields soundness, uniqueness, and completeness theorems for all fragments, providing a compact graphical calculus that matches the algebraic structure used in phase-polynomial compilation and multiqudit synthesis [11, 2, 12].

2 Affine circuits

Definition 1. *A* PROP *is a strict symmetric monoidal category* $\mathbf{C}$ *whose objects are the natural numbers. The tensor product on objects is addition and the tensor unit is* 0.

A morphism $D : n \to m$ is depicted as a string diagram with n input wires and m output wires. We compose $D_2 \circ D_1$ by plugging the outputs of D_1 into the inputs of D_2, and we form $D_1 \otimes D_2$ by placing diagrams in parallel on disjoint sets of wires.

The word strict *means that tensor products are associative and unital on the nose, both on objects and on morphisms. For example, we freely identify $(n+m)+k$ with $n+(m+k)$, and we write $D_1 \otimes D_2 \otimes D_3$ without inserting associators. This matches the usual circuit convention that regrouping parallel wires is not a computational step.*

The symmetric structure provides, for each n,m, an isomorphism $\sigma_{n,m} : n+m \to m+n$ exchanging the first n wires with the last m. From these swaps we obtain, for every permutation $\pi \in S_n$, a canonical symmetry $\sigma_\pi : n \to n$. Graphically, these are drawn as wire crossings, and the symmetric monoidal axioms ensure that diagrams may be deformed without changing the represented morphism, as long as the connectivity is preserved.

The PROP formalism is a convenient level of abstraction for circuit rewriting.

First, it packages sequential composition and parallel composition into a single algebraic structure, so that equational reasoning can be phrased as equalities of morphisms. Second, PROPs are designed for languages with a single wire type: an object n records only the number of wires, which is exactly what we need for qudit circuits where every system has dimension d. Third, strict symmetric monoidality gives a built-in notion of context: if two subcircuits are equal, then they remain equal after plugging them into any larger circuit, tensoring with additional wires, or permuting wires. This is the categorical counterpart of the informal principle that local rewrite rules can be applied anywhere in a circuit diagram.

A PROP can be presented by generators and equations. Concretely, one starts from the free PROP on the chosen generators and then quotients by the smallest congruence containing the stated equations, and closed under $\circ$, $\otimes$, and the symmetric structure.

For a ruleset Γ, we write $\Gamma \vdash D_1 = D_2$ for equality in this quotient. Equivalently, $\Gamma \vdash D_1 = D_2$ is the least relation containing Γ and closed under reflexivity, symmetry, transitivity, and congruence. In particular, if $\Gamma \vdash D_1 = D_1'$ and $\Gamma \vdash D_2 = D_2'$, then $\Gamma \vdash D_2 \circ D_1 = D_2' \circ D_1'$ (when types match) and $\Gamma \vdash D_1 \otimes D_2 = D_1' \otimes D_2'$. The same closure holds under wire permutations provided by the symmetric structure.

Definition 2. *Let* $\mathbf{C}$ *and* $\mathbf{D}$ *be PROPs. A* strict symmetric monoidal functor $F : \mathbf{C} \to \mathbf{D}$ *is a functor that preserves composition and tensor on the nose, and sends the symmetry maps of* $\mathbf{C}$ *to the corresponding symmetry maps of* $\mathbf{D}$*. Such functors provide the appropriate notion of semantics for presented circuit languages: they interpret generators as concrete gates and ensure that all derivable equations remain valid after interpretation.*

2.1 The semantic PROP of reversible affine maps

Fix a prime d. We write vectors in $\mathbb{F}_d^n$ as columns, and we write $\mathrm{GA}_n(\mathbb{F}_d)$ for the affine group of invertible affine maps $x \mapsto Ax + b$, with $A \in \mathrm{GL}_n(\mathbb{F}_d)$ and $b \in \mathbb{F}_d^n$.

Definition 3. *Let* $\mathbf{AffVect}^{\times}_{\mathbb{F}_d}$ *be the strict symmetric monoidal groupoid defined as follows. Objects are* $n \in \mathbb{N}$*. Morphisms satisfy* $\mathbf{AffVect}^{\times}_{\mathbb{F}_d}(n,n) = \mathrm{GA}_n(\mathbb{F}_d)$ *and* $\mathbf{AffVect}^{\times}_{\mathbb{F}_d}(n,m) = \varnothing$ *for* $n \neq m$*. Composition is given by* $(A_2, b_2) \circ (A_1, b_1) = (A_2A_1, A_2b_1 + b_2)$.

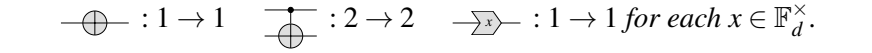
The tensor product on objects is $n \otimes m = n + m$*; on morphisms,* $(A_1, b_1) \otimes (A_2, b_2) = (A_1 \oplus A_2, b_1 \mid b_2)$*, where* $A_1 \oplus A_2$ *is block-diagonal and* $b_1 \mid b_2$ *is obtained by stacking* b_1 *above* b_2*. The symmetry* $\sigma_{n,m} : n + m \to n + m$ *is* $(P_{n,m}, 0)$*, where* $P_{n,m}$ *is the permutation matrix exchanging the first n and last m standard basis vectors.*

Remark 1. *For* $n = 0$*, we take* $\mathbb{F}_d^0$ *to be the singleton set. Then* $\mathrm{GA}_0(\mathbb{F}_d)$ *is the trivial group, and* $\mathbf{AffVect}^{\times}_{\mathbb{F}_d}(0,0)$ *has a single morphism.*

2.2 The diagrammatic PROP $\mathbf{Aff}_d$

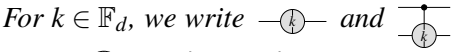
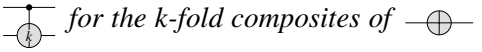
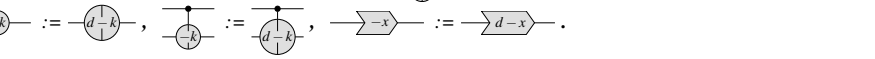
We use string diagrams with time flowing left to right. Wire permutations are provided by the symmetric monoidal structure (crossings).

Definition 4. *Let* $\mathbf{Aff}_d$ *be the PROP presented by the following generators:*



$: 1 \to 1 \quad : 2 \to 2 \quad : 1 \to 1$ *for each* $x \in \mathbb{F}_d^{\times}$.

We write $: 1 \to 1$ *for the identity wire,* $: 0 \to 0$ *for the identity on the tensor unit, and* $: 2 \to 2$ *for the symmetry on two wires. These generators satisfy the equations* Aff_d *displayed in Figure 1.*

Definition 5. *For* $k \in \mathbb{F}_d$*, we write*  *and*  *for the k-fold composites of* *and* *, we also write*  .

Definition 6. *In* $\mathbf{Aff}_d$ *define* .

Definition 7. *There is a strict symmetric monoidal functor* $[\![\cdot]\!]_{Aff} : \mathbf{Aff}_d \to \mathbf{AffVect}^{\times}_{\mathbb{F}_d}$*, identity on objects, uniquely determined on generators by*

$$[\![-]\!]_{Aff} = \left([1], [0]\right), \qquad [\![\text{⬚}]\!]_{Aff} = (I_0, 0), \qquad [\![-x-]\!]_{Aff} = \left([x], [0]\right),$$

$$[\![\text{⊕}]\!]_{Aff} = \left([1], [1]\right), \quad [\![\text{⊕•}]\!]_{Aff} = \left(\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix}\right), \quad [\![\text{×}]\!]_{Aff} = \left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix}\right).$$

The generators  ,  , and correspond respectively to Lafont's shear gates K_a (in particular K_1), scalings H_x, and the translation gate $\nu : x \mapsto x + 1$ in the Boolean case [13].

Lemma 1. *Every axiom in* Aff_d *holds under* $[\![\cdot]\!]_{Aff}$.

Lemma 2. *For every rule* $C = C'$ *in Lafont's presentation [13] of linear circuits (See Figure 5), one has* $\mathrm{Aff}_d \vdash C = C'$.

Proof. This is proved in Appendix A.1. □

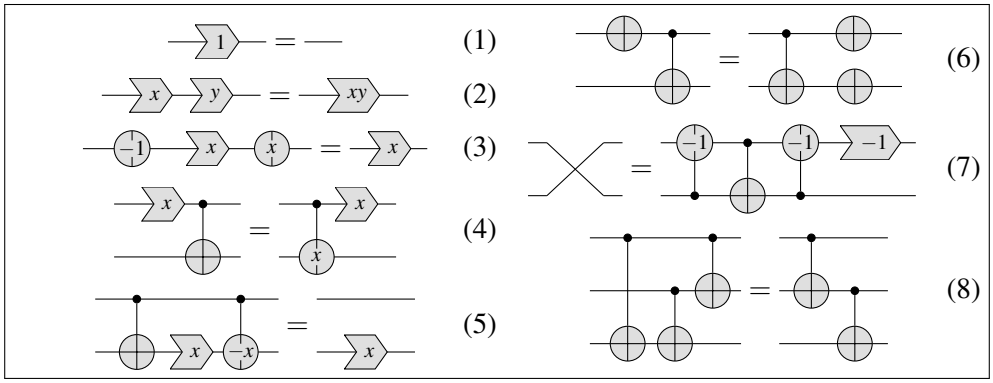
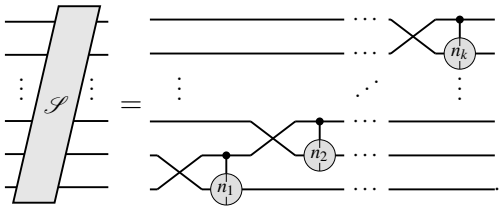


Figure 1: The ruleset Aff_d for circuits of affine transformations over $\mathbb{F}_d$.

2.3 Affine layers and normal forms

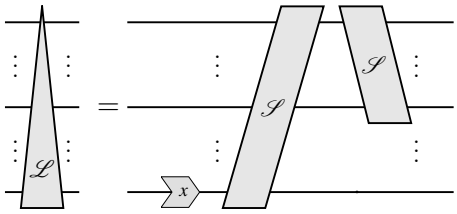
We use a layered normal form for affine circuits in the style of CNOT-dihedral normal forms: a linear layer built from  -stairs, diagonal scalings  , and permutations, followed by a translation column built from  -gates. This matches the decomposition of an affine map $x \mapsto Ax + b$ as a linear update $x \mapsto Ax$ followed by a translation $x \mapsto x + b$.

Definition 8 ([13])**.** *An ascending*  *-stair is a circuit of the form*

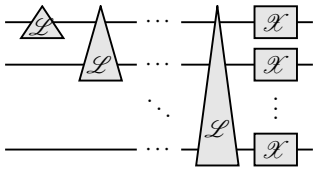


The descending  *-stair is defined analogously by the vertically reflected diagram.*

Definition 9 ([13])**.** *A ladder is a circuit of the form*

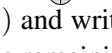


Definition 10 ([13])**.** *An affine normal form is a circuit of the form*



Lemma 3 ([13])**.** *For every $g \in \mathrm{GA}_n(\mathbb{F}_d)$, there exists a unique affine normal form circuit $\mathrm{NF}_{\mathrm{aff}}(g)$ such that $[\![\mathrm{NF}_{\mathrm{aff}}(g)]\!]_{Aff} = g$.*

Lemma 4. *For any affine circuit $A : n \to n$ in* $\mathbf{Aff}_d$*, if* $[\![A]\!]_{Aff} = g$ *then* $\mathrm{Aff}_d \vdash A = \mathrm{NF}_{\mathrm{aff}}(g)$.

Proof. Using the commutation axioms between translations and shears, rewrite A so that all occurrences of  are collected into a single translation column at the output side of the diagram. The remaining part is a linear circuit built from  ,  , and permutations.

Let $g = [\![A]\!]_{Aff} \in \mathrm{GA}_n(\mathbb{F}_d)$ and write $g(x) = Ax + b$. Under $[\![\cdot]\!]_{Aff}$, the collected translation column interprets as $x \mapsto x + b$, and the remaining linear circuit interprets as $x \mapsto Ax$. By Lafont's completeness for linear circuits, as imported via Lemma 2, the linear part rewrites to its unique linear normal form. Putting the two layers together yields $\mathrm{NF}_{\mathrm{aff}}(g)$, and hence $\mathrm{Aff}_d \vdash A = \mathrm{NF}_{\mathrm{aff}}(g)$. In Section B we also give an alternative proof of completeness for the affine presentation using group-theoretic arguments. □

Theorem 1. *For any affine circuits $A, A' : n \to n$ in* $\mathbf{Aff}_d$*, if* $[\![A]\!]_{Aff} = [\![B]\!]_{Aff}$ *then* $\mathrm{Aff}_d \vdash A = A'$.

Proof. Let $g = [\![A]\!]_{Aff} = [\![A']\!]_{Aff}$. By Lemma 4 we have $\mathrm{Aff}_d \vdash A = \mathrm{NF}_{\mathrm{aff}}(g)$ and $\mathrm{Aff}_d \vdash A' = \mathrm{NF}_{\mathrm{aff}}(g)$. By transitivity, $\mathrm{Aff}_d \vdash A = A'$. □

3 Finite-angle phase fragments

Fix a prime d. Let $\mathrm{Hilb}_d = \mathbb{C}^d$ with computational basis $\{|x\rangle \mid x \in \mathbb{F}_d\}$, and write $\omega = e^{2\pi i/d}$. This section extends the affine PROP $\mathbf{Aff}_d$ from Section 2 with diagonal gates whose eigenvalues are dth roots of unity. A diagonal gate on n wires is determined by a function $q : \mathbb{F}_d^n \to \mathbb{F}_d$ via $U_q |x\rangle = \omega^{q(x)} |x\rangle$. Since $\omega^d = 1$, exponents are taken in $\mathbb{F}_d$, and only the induced function q matters.

We organise our diagonal fragments by the maximal total degree of q: linear phases (degree at most 1), quadratic phases (degree at most 2), and cubic phases (degree at most 3). Quadratic phases are only considered when d is odd, and cubic phases only when $d > 3$. These assumptions ensure that the scalars 2 (and 6 in the cubic case) are invertible in $\mathbb{F}_d$, which is exactly what we need for the binomial basis below.

For each fragment we give two complementary descriptions. First, a semantic PROP of affine maps equipped with a phase polynomial. Second, a diagrammatic PROP extending $\mathbf{Aff}_d$ with diagonal generators and a compact axiom set. Completeness is proved by a uniform normal-form argument: every circuit rewrites to an affine layer followed by a single diagonal layer, and the diagonal layer is uniquely determined by its phase function.

3.1 Binomial polynomials over $\mathbb{F}_d$

For odd prime d, we use the binomial polynomial $\binom{x}{2} = x(x-1)/2 \in \mathbb{F}_d$. For prime $d > 3$, we also use $\binom{x}{3} = x(x-1)(x-2)/6 \in \mathbb{F}_d$. The point of these choices is that they satisfy simple finite-difference identities, matching the substitutions induced by commuting phases through translations $x \mapsto x+1$ and shears $(x,y) \mapsto (x, y+x)$. They also coincide with standard diagonal representatives of the first three levels of the qudit Clifford hierarchy: Z is Pauli, S is Clifford for odd d, and T lies in the third level for $d > 3$ [7, 11]. These properties make the transport equations of Section 3.5 short and uniform.

Lemma 5. *Assume d is an odd prime. For all $x, y, k \in \mathbb{F}_d$ one has*

$$\binom{x+1}{2} = \binom{x}{2} + x \quad (9) \qquad \binom{x+y}{2} = \binom{x}{2} + \binom{y}{2} + xy \quad (10) \qquad \binom{kx}{2} = k^2 \binom{x}{2} + \binom{k}{2} x \quad (11)$$

Lemma 6. *Assume $d > 3$ is prime. For all $x, y, k \in \mathbb{F}_d$ one has*

$$\binom{x+1}{3} = \binom{x}{3} + \binom{x}{2} \quad (12) \qquad \binom{x+y}{3} = \binom{x}{3} + \binom{y}{3} + \binom{x}{2}y + x\binom{y}{2} \quad (13)$$

$$\binom{kx}{3} = k^3\binom{x}{3} + 2k\binom{k}{2}\binom{x}{2} + \binom{k}{3}x \quad (14)$$

Lemma 7. *Assume d is an odd prime. For all $x, y \in \mathbb{F}_d$ one has*

$$x^2 = 2\binom{x}{2} + x \quad (15) \qquad x^2y = 2y\binom{x}{2} + xy \quad (16) \qquad xy^2 = 2x\binom{y}{2} + xy \quad (17)$$

If moreover $d > 3$, then also $x^3 = 6\binom{x}{3} + 6\binom{x}{2} + x$.

3.2 Semantic PROPs of affine maps with phase polynomials

For $n \in \mathbb{N}$, identify $\mathbb{F}_d^n$ with the computational basis of $\mathrm{Hilb}_d^{\otimes n}$ via $x \mapsto |x\rangle$. For $g \in \mathrm{GA}_n(\mathbb{F}_d)$ write $U_g|x\rangle = |g(x)\rangle$.

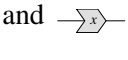
A morphism in our semantic phase PROPs consists of an affine update g together with a phase function q. Composition is the expected semidirect-product law: phases add, but the second phase must be evaluated on the intermediate basis label, hence the substitution $q_2 \circ g_1$. Tensor product is block sum on the affine part and addition on disjoint variables on the phase part.

Definition 11. *For $n \in \mathbb{N}$, let Lin_n, Quad_n and Cube_n be the sets of functions $q : \mathbb{F}_d^n \to \mathbb{F}_d$ representable by polynomials of total degree at most 1, 2, and 3, respectively.*

For $\mathscr{Q} \in \{\mathrm{Lin}, \mathrm{Quad}, \mathrm{Cube}\}$, define the strict symmetric monoidal groupoid $\mathbf{Qupit}_d^{\mathscr{Q}}$ as follows. Objects are natural numbers. Morphisms satisfy $\mathbf{Qupit}_d^{\mathscr{Q}}(n,n) = \{(g,q) \mid g \in \mathrm{GA}_n(\mathbb{F}_d),\ q \in \mathscr{Q}_n\}$ and $\mathbf{Qupit}_d^{\mathscr{Q}}(n,m) = \varnothing$ for $n \neq m$. A morphism (g,q) acts on basis states by $U_{g,q}|x\rangle = \omega^{q(x)}|g(x)\rangle$. Composition is $(g_2,q_2) \circ (g_1,q_1) = (g_2 \circ g_1, q_1 + q_2 \circ g_1)$. The tensor product is defined by block sum on affine parts and addition on disjoint variables. The symmetry permutes coordinates.

We write $\mathbf{Qupit}_d^{\mathrm{Lin}}$, $\mathbf{Qupit}_d^{\mathrm{Quad}}$, and $\mathbf{Qupit}_d^{\mathrm{Cube}}$ for the three choices.

3.3 Diagrammatic PROPs for finite-angle phases

We now introduce three diagrammatic PROPs extending $\mathbf{Aff}_d$. They share the affine generators  ,  , and  (for each parameter in $\mathbb{F}_d^\times$), and differ only by which diagonal primitives are adjoined.

Definition 12. *Let $\mathbf{LinPhase}_d$ be the PROP obtained from $\mathbf{Aff}_d$ by adjoining two generators  : $1 \to 1$ and  : $0 \to 0$, and imposing the additional relations displayed in Figure 2. We write  and  for the k-fold iterations of these generators.*

Definition 13. *Assume d is an odd prime. Let $\mathbf{QuadPhase}_d$ be the PROP obtained from $\mathbf{LinPhase}_d$ by adjoining the generator  : $1 \to 1$, and imposing the additional relations displayed in Figure 3. We write  for the k-fold iterations of this generator.*

Definition 14. *Assume $d > 3$ is prime. Let $\mathbf{CubicPhase}_d$ be the PROP obtained from $\mathbf{QuadPhase}_d$ by adjoining the generator  : $1 \to 1$, and imposing the additional relations listed in Figure 4. We write for the k-fold iteration of this generator.*

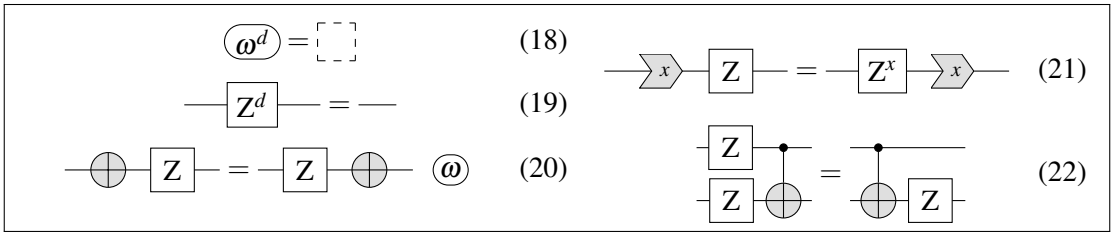


Figure 2: LinPhase$_d$ extends Aff$_d$. It presents the PROP **LinPhase**$_d$.

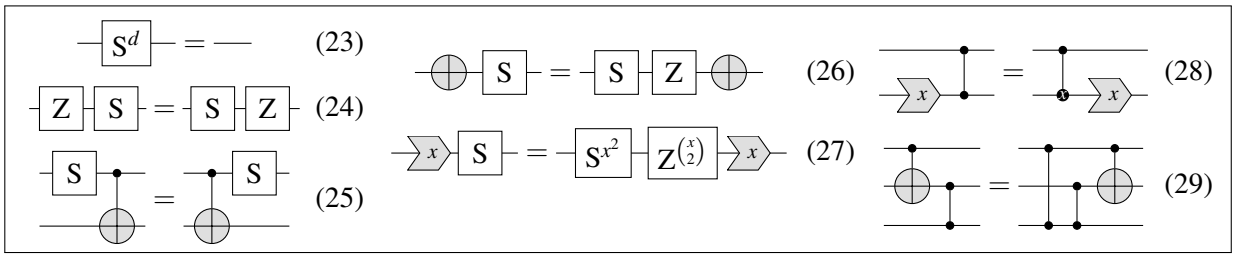


Figure 3: QuadPhase$_d$ extends LinPhase$_d$. It presents the PROP **QuadPhase**$_d$.

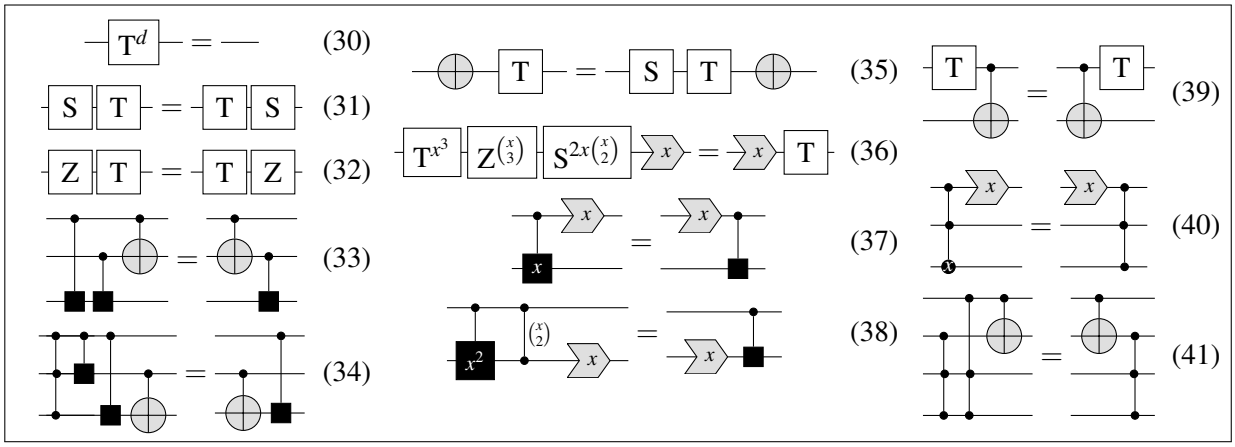
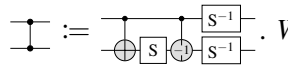
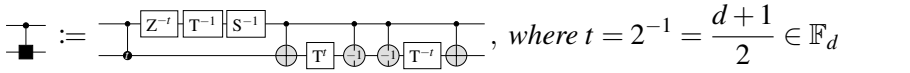
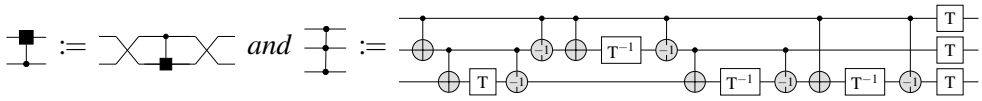


Figure 4: CubicPhase$_d$ extends QuadPhase$_d$. It presents the PROP **CubicPhase**$_d$.

Definition 15. *In* **QuadPhase**$_d$ *define the derived diagonal*  *. We write*  *or*  *for the k-fold iterate of this circuit.*

Definition 16. *In* **CubicPhase**$_d$ *define the derived diagonal shorthands*





We write  *and*  *for the k-fold iterate of these circuits.*

3.4 Interpretations and soundness

Each diagrammatic PROP comes with a canonical interpretation into its semantic counterpart, extending the affine interpretation by sending diagonal generators to the corresponding phase polynomials. Soundness reduces to checking that each diagrammatic axiom is an equality in $\mathbf{Qupit}_d^{\mathcal{Q}}$, that is, an equality of affine parts together with an identity of phase functions.

Definition 17. *There is a strict symmetric monoidal functor* $[\![\cdot]\!]_{Lin} : \mathbf{LinPhase}_d \to \mathbf{Qupit}_d^{\mathrm{Lin}}$ *which is identity on objects and is determined on generators by*

$$[\![\text{—}\oplus\text{—}]\!]_{Lin} = \big((a \mapsto a+1), 0\big), \quad [\![\text{—}\boxed{x}\text{—}]\!]_{Lin} = \big((a \mapsto xa), 0\big), \quad \left[\!\!\left[\begin{array}{c} \bullet \\ \oplus \end{array} \right]\!\!\right]_{Lin} = \big(((a,b) \mapsto (a, b+a)), 0\big),$$
$$[\![\text{—}\boxed{\mathrm{Z}}\text{—}]\!]_{Lin} = \big(\mathrm{id}, (x \mapsto x)\big), \qquad [\![\text{—}\circledcirc\text{—}]\!]_{Lin} = \big(\mathrm{id}_0, 1\big),$$

and sending symmetries to coordinate permutations.

Assume d is an odd prime. There is a strict symmetric monoidal functor $[\![\cdot]\!]_{Quad} : \mathbf{QuadPhase}_d \to \mathbf{Qupit}_d^{\mathrm{Quad}}$ *extending* $[\![\cdot]\!]_{Lin}$ *and sending* $[\![\text{—}\boxed{\mathrm{S}}\text{—}]\!]_{Quad} = (\mathrm{id}, (x \mapsto \binom{x}{2}))$.

Assume $d > 3$ is prime. There is a strict symmetric monoidal functor $[\![\cdot]\!]_{Cube} : \mathbf{CubicPhase}_d \to \mathbf{Qupit}_d^{\mathrm{Cube}}$ *extending* $[\![\cdot]\!]_{Quad}$ *and sending* $[\![\text{—}\boxed{\mathrm{T}}\text{—}]\!]_{Cube} = (\mathrm{id}, (x \mapsto \binom{x}{3}))$.

Lemma 8. *Under* $[\![\cdot]\!]_{Quad}$ *one has* $\left[\!\!\left[\begin{array}{c} \bullet \\ \bullet \end{array} \right]\!\!\right]_{Quad} = (\mathrm{id}, ((x,y) \mapsto xy))$.

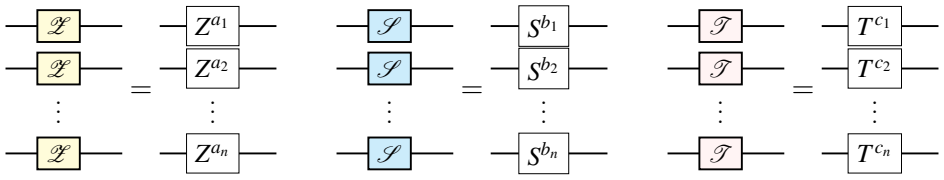
Under $[\![\cdot]\!]_{Cube}$ *one has* $\left[\!\!\left[\begin{array}{c} \bullet \\ \blacksquare \end{array} \right]\!\!\right]_{Cube} = (\mathrm{id}, ((x,y) \mapsto x\binom{y}{2}))$, $\left[\!\!\left[\begin{array}{c} \blacksquare \\ \bullet \end{array} \right]\!\!\right]_{Cube} = (\mathrm{id}, ((x,y) \mapsto y\binom{x}{2}))$, *and* $\left[\!\!\left[\begin{array}{c} \bullet \\ \bullet \\ \bullet \end{array} \right]\!\!\right]_{Cube} = (\mathrm{id}, ((x,y,z) \mapsto xyz))$.

Lemma 9. *Every axiom of* $\mathrm{LinPhase}_d$, $\mathrm{QuadPhase}_d$ *and* $\mathrm{CubicPhase}_d$ *holds respectively under* $[\![\cdot]\!]_{\mathrm{Lin}}$, $[\![\cdot]\!]_{\mathrm{Quad}}$ *and* $[\![\cdot]\!]_{\mathrm{Cube}}$.

3.5 Normal forms, uniqueness, and completeness

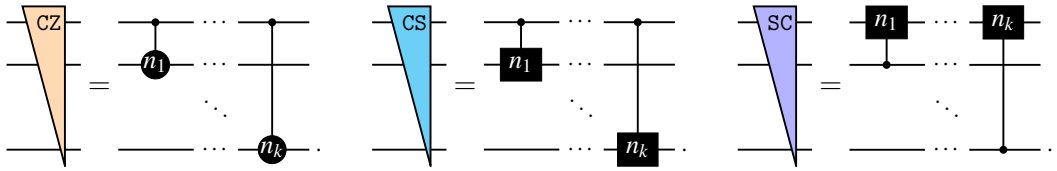
We now give normal forms for circuits in each fragment. Diagonal generators represent phase functions $q(x)$, while affine generators update the basis label $x \mapsto g(x)$. Commuting a diagonal gate past an affine gate therefore implements the substitution $q \mapsto q \circ g$. The transport equations in Table 2 implement these substitutions diagrammatically, allowing us to collect all diagonal generators into a single diagonal layer placed at the input side of the circuit. We then rewrite the diagonal layer into a fixed syntactic shape, and use affine completeness (Theorem 1) to normalise the remaining affine layer.

Definition 18. *A Z-column, S-column and T-column circuit is respectively a circuit of the form*



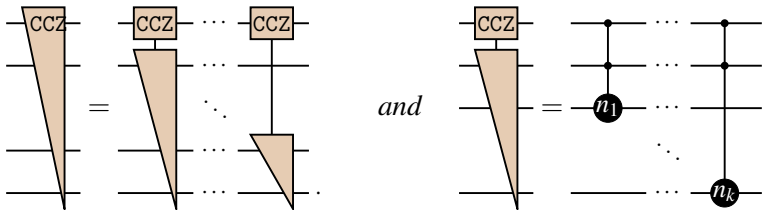
Exponents are taken in $\mathbb{F}_d$, so $a_i = 0$ denotes the identity on the ith wire.

Definition 19. *A CZ-descending stair, CS-descending stair and SC-descending stair is respectively a circuit of the form*



Each label $n_i \in \mathbb{F}_d$ denotes the n_i-fold iterate of the corresponding two-wire diagonal gate (taken modulo d).

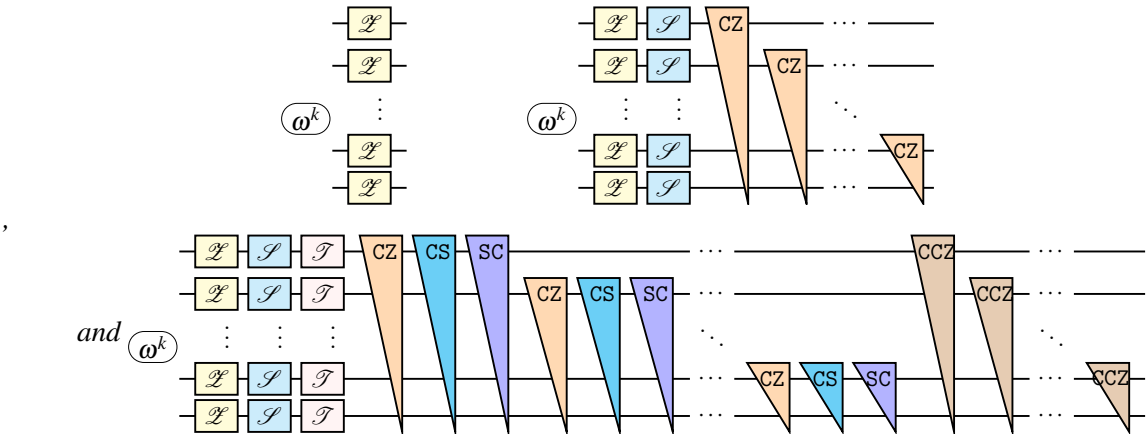
Definition 20. *A CCZ-descending stair is a circuit of the form*



Each label $n_i \in \mathbb{F}_d$ denotes the n_i-fold iterate of the corresponding three-wire diagonal gate (taken modulo d).

Definition 21.

Definition 22. *A linear phase normal form (in* $\mathbf{LinPhase}_d$*), a quadratic phase normal form (in* $\mathbf{QuadPhase}_d$*), and a cubic phase normal form (in* $\mathbf{CubicPhase}_d$*) are diagonal circuits of the respective shapes*



with all exponents taken in $\mathbb{F}_d$.

Remark 2. *In the qubit CNOT-dihedral fragment generated by $\{CNOT, T, X\}$, Amy et al. count the diagonal normal forms on n wires as $8 \cdot 8^{\binom{n}{1}} \cdot 4^{\binom{n}{2}} \cdot 2^{\binom{n}{3}} = 2^{3+3\binom{n}{1}+2\binom{n}{2}+\binom{n}{3}} = 2^{\binom{n+3}{2}+\binom{n+1}{3}}$ [2]. The different bases $8,4,2$ reflect the degree-dependent periodicities of the qubit phase-polynomial coefficients.*

In our prime-dimensional cubic fragment, every diagonal normal form is parametrised by coefficients in $\mathbb{F}_d$: one scalar coefficient (global phase), $3\binom{n}{1}$ one-wire coefficients (for Z, S, T), $3\binom{n}{2}$ two-wire coefficients (for CZ, CS, SC), and $\binom{n}{3}$ three-wire coefficients (for CCZ). It follows that the number of diagonal normal forms is $d^{1+3\binom{n}{1}+3\binom{n}{2}+\binom{n}{3}} = d^{\binom{n+3}{3}}$.

Lemma 10. *Fix $n \in \mathbb{N}$. For every circuit $C : n \to n$ in* $\mathbf{LinPhase}_d$ *(respectively in* $\mathbf{QuadPhase}_d$*, in* $\mathbf{CubicPhase}_d$*), there exist an affine normal form circuit $A : n \to n$ and a diagonal normal form circuit $D : n \to n$ (linear, respectively quadratic, cubic) such that* $\mathrm{LinPhase}_d \vdash C = A \circ D$ *(respectively* $\mathrm{QuadPhase}_d \vdash C = A \circ D$*,* $\mathrm{CubicPhase}_d \vdash C = A \circ D$*).*

Proof. We treat the three fragments uniformly. Using the transport equations of Table 2, rewrite C so that every diagonal generator occurs in a single diagonal layer on the input side. This yields a factorisation $C = C_{\mathrm{aff}} \circ C_{\mathrm{diag}}$ where C_{aff} is affine and C_{diag} is diagonal.

Rewrite C_{diag} into the corresponding diagonal normal form by commuting diagonal generators past each other and collecting like generators. In the quadratic and cubic fragments, the needed commutations are summarised in Table 1; in the linear fragment, only one-wire diagonals and scalars occur.

Finally, rewrite C_{aff} into affine normal form using Lemma 4. Since $\mathrm{Aff}_d \subseteq \mathrm{LinPhase}_d \subseteq \mathrm{QuadPhase}_d \subseteq \mathrm{CubicPhase}_d$, this normalisation is available in each fragment. Taking A and D to be the resulting normal forms yields the desired factorisation. □

Lemma 11. *Fix $n \in \mathbb{N}$. Let $D, D' : n \to n$ be diagonal normal form circuits in* $\mathbf{LinPhase}_d$ *(respectively in* $\mathbf{QuadPhase}_d$*, in* $\mathbf{CubicPhase}_d$*). If $[\![D]\!]_{Lin} = [\![D']\!]_{Lin}$ (respectively $[\![D]\!]_{Quad} = [\![D']\!]_{Quad}$, $[\![D]\!]_{Cub} = [\![D']\!]_{Cub}$) in the corresponding semantic PROP, then $D = D'$.*

Proof. In all three fragments, diagonality implies $[\![D]\!] = (\mathrm{id}, q)$ and $[\![D']\!] = (\mathrm{id}, q')$ for some phase functions q, q', hence $q = q'$.

In the linear fragment, q has a unique expansion $q(x) = c + \sum_i a_i x_i$ with $c, a_i \in \mathbb{F}_d$. In the quadratic fragment, q has a unique expansion $q(x) = c + \sum_i a_i x_i + \sum_i b_i \binom{x_i}{2} + \sum_{i<j} c_{ij} x_i x_j$. In the cubic fragment, q has a unique expansion in the degree-≤ 3 binomial basis generated by 1, x_i, $\binom{x_i}{2}$, $\binom{x_i}{3}$, $x_i x_j$, $x_i \binom{x_j}{2}$, and $x_i x_j x_k$ with distinct indices.

By construction, the corresponding diagonal normal form records exactly these coefficients as exponents on $\circledcirc$, the one-wire columns, and the two- and three-wire stair components. Therefore $q = q'$ forces equality of all recorded coefficients, hence $D = D'$. □

Lemma 12. *Fix $n \in \mathbb{N}$. Let $\mathscr{P} \in \{\mathbf{LinPhase}_d, \mathbf{QuadPhase}_d, \mathbf{CubicPhase}_d\}$, under the standing assumptions on d. If $A, A' : n \to n$ are affine normal form circuits (viewed as circuits in $\mathscr{P}$) and $[\![A]\!]_{Aff} = [\![A']\!]_{Aff}$ in $\mathrm{GA}_n(\mathbb{F}_d)$, then $A = A'$.*

Proof. Let $g = [\![A]\!]_{Aff} = [\![A']\!]_{Aff}$. By uniqueness of the affine normal form $\mathrm{NF}_{\mathrm{aff}}(g)$, we have $A = \mathrm{NF}_{\mathrm{aff}}(g) = A'$. □

Theorem 2. *Fix $n \in \mathbb{N}$. For any circuits $C, C' : n \to n$ in* $\mathbf{LinPhase}_d$ *(respectively in* $\mathbf{QuadPhase}_d$*, in* $\mathbf{CubicPhase}_d$*), if $[\![C]\!]_{Lin} = [\![C']\!]_{Lin}$ (respectively $[\![C]\!]_{Quad} = [\![C']\!]_{Quad}$, $[\![C]\!]_{Cub} = [\![C']\!]_{Cub}$) in the corresponding semantic PROP, then* $\mathrm{LinPhase}_d \vdash C = C'$ *(respectively* $\mathrm{QuadPhase}_d \vdash C = C'$*,* $\mathrm{CubicPhase}_d \vdash C = C'$*).*

Proof. We give the argument for $\mathbf{LinPhase}_d$; the quadratic and cubic cases are identical after replacing the diagonal normal forms and interpretations by the corresponding ones.

By Lemma 10, choose factorisations $\mathrm{LinPhase}_d \vdash C = A \circ D$ and $\mathrm{LinPhase}_d \vdash C' = A' \circ D'$ with A, A' affine normal forms and D, D' diagonal normal forms in $\mathbf{LinPhase}_d$. Applying $[\![\cdot]\!]_{Lin}$ and using functoriality yields $[\![C]\!]_{Lin} = [\![A \circ D]\!]_{Lin} = [\![A]\!]_{Lin} \circ [\![D]\!]_{Lin}$ and $[\![C']\!]_{Lin} = [\![A']\!]_{Lin} \circ [\![D']\!]_{Lin}$. Since $[\![A]\!]_{Lin} = ([\![A]\!]_{Aff}, 0)$ and $[\![D]\!]_{Lin} = (\mathrm{id}, q_D)$ for some q_D, we obtain $[\![C]\!]_{Lin} = ([\![A]\!]_{Aff}, q_D)$, and similarly $[\![C']\!]_{Lin} = ([\![A']\!]_{Aff}, q_{D'})$.

The hypothesis $[\![C]\!]_{Lin} = [\![C']\!]_{Lin}$ therefore implies $[\![A]\!]_{Aff} = [\![A']\!]_{Aff}$ and $q_D = q_{D'}$, hence $[\![D]\!]_{Lin} = [\![D']\!]_{Lin}$. By Lemmas 11 and 12, we conclude $A = A'$ and $D = D'$, and therefore $\mathrm{LinPhase}_d \vdash C = C'$. □

4 Conclusion

This paper develops a prime-dimensional diagrammatic calculus for a family of circuit fragments built from reversible affine updates and finite-angle diagonal phases. For each prime d, we introduced a compact PROP $\mathbf{Aff}_d$ for affine transformations over $\mathbb{F}_d$, together with a strict symmetric monoidal interpretation into $\mathrm{GA}_n(\mathbb{F}_d)$. Building on Lafont-style presentations of linear circuits, we proved that $\mathbf{Aff}_d$ admits affine normal forms and that the induced equational theory is sound and complete for reversible affine maps.

We then extended this affine core with diagonal generators aligned with phase-polynomial compilation. The resulting fragments $\mathbf{LinPhase}_d$, $\mathbf{QuadPhase}_d$ (for odd d), and $\mathbf{CubicPhase}_d$ (for primes $d > 3$) add uniform primitives for linear, quadratic, and cubic phase functions, together with short axioms governing their interaction with affine gates. In the semantic model, each fragment is interpreted in a strict symmetric monoidal groupoid of pairs (g, q), where $g \in \mathrm{GA}_n(\mathbb{F}_d)$ and q is a bounded-degree phase function, composed by the standard semidirect-product law $(g_2, q_2) \circ (g_1, q_1) = (g_2 \circ g_1, q_1 + q_2 \circ g_1)$.

The main technical result is completeness by layered normal forms. In each fragment, every circuit rewrites to a composite $A \circ D$ with A an affine normal form and D a single diagonal layer in a fixed syntactic shape. Uniqueness is proved semantically by identifying diagonal normal forms with unique binomial-basis expansions of the corresponding phase functions in degrees at most 1, 2, and 3 under the stated assumptions on d. Together, these results yield completeness theorems: two circuits are equal in the semantic model if and only if their equality is derivable from the diagrammatic axioms.

The resulting calculi give a prime-dimensional analogue of the CNOT-dihedral presentation and a fully diagrammatic interface to the structure underlying multiqudit phase-polynomial compilation. Several directions remain open.

– *Reducing generators for scalings.* For prime d, the multiplicative group $\mathbb{F}_d^\times$ is cyclic, so the family of generators  could be replaced by a smaller generating set, for example a single scaling for a primitive element g. Doing so would require revisiting the presentation so that the resulting axiomatisation remains compact and usable in rewrites, while keeping normalisation constructive.

– *Beyond prime dimensions.* Our development relies on arithmetic over $\mathbb{F}_d$ and, in the quadratic and cubic cases, on the invertibility of 2 and 6. Extending these calculi to prime-power dimensions $\mathbb{F}_{p^k}$ or to more general finite rings would broaden their applicability, but would also require new choices of generators and bases for phase functions, as well as a careful treatment of which finite-difference identities survive.

– *Higher degrees and refined phase hierarchies.* The degree stratification suggests a systematic extension to higher-degree phase polynomials, where generators corresponding to $\binom{x}{k}$ for $k \geq 4$ would naturally appear when $d > k$. Such extensions would also force a principled account of which additional controlled-diagonal primitives are required for closure under affine substitution, and how to keep the axiom sets local and uniform. Clarifying the analogue of refined-angle constructions, such as the qubit recipe for adding square-root phases, is particularly interesting in this higher-dimensional setting.

5 Acknowledgements

This work is supported by the Plan France 2030 through the PEPR integrated project EPiQ (ANR-22-PETQ-0007) and the HQI platform (ANR-22-PNCQ-0002); by the European Union through the MSCA Staff Exchanges project QCOMICAL (Grant Agreement ID: 101182520); and by the Maison du Quantique MaQuEst.

References

[1] Matthew Amy, Parsiad Azimzadeh & Michele Mosca (2018): *On the controlled-NOT complexity of controlled-NOT–phase circuits*. *Quantum Science and Technology* 4(1), p. 015002, doi:https://doi.org/10.1088/2058-9565/aad8ca. Available at http://dx.doi.org/10.1088/2058-9565/aad8ca.

[2] Matthew Amy, Jianxin Chen & Neil J. Ross (2018): *A Finite Presentation of CNOT-Dihedral Operators*. *Electronic Proceedings in Theoretical Computer Science* 266, p. 84–97, doi:https://doi.org/10.4204/eptcs.266.5. Available at http://dx.doi.org/10.4204/EPTCS.266.5.

[3] Matthew Amy, Dmitri Maslov & Michele Mosca (2014): *Polynomial-Time T-Depth Optimization of Clifford+T Circuits Via Matroid Partitioning*. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 33(10), p. 1476–1489, doi:https://doi.org/10.1109/tcad.2014.2341953. Available at http://dx.doi.org/10.1109/TCAD.2014.2341953.

[4] Matthew Amy & Michele Mosca (2019): *T-Count Optimization and Reed–Muller Codes*. *IEEE Transactions on Information Theory* 65(8), p. 4771–4784, doi:https://doi.org/10.1109/tit.2019.2906374. Available at http://dx.doi.org/10.1109/TIT.2019.2906374.

[5] Colin Blake (2026): *Simpler Presentations for Many Fragments of Quantum Circuits*. Available at https://arxiv.org/abs/2602.09874.

[6] Robert I. Booth & Titouan Carette (2022): *Complete ZX-calculi for the stabiliser fragment in odd prime dimensions*. *LIPIcs, Volume 241, MFCS 2022* 241, pp. 24:1–24:15, doi:https://doi.org/10.4230/LIPIcs.MFCS.2022.24. Available at http://arxiv.org/abs/2204.12531. ArXiv:2204.12531 [quant-ph].

[7] Earl T. Campbell, Hussain Anwar & Dan E. Browne (2012): *Magic-State Distillation in All Prime Dimensions Using Quantum Reed-Muller Codes*. *Physical Review X* 2(4), doi:https://doi.org/10.1103/physrevx.2.041021. Available at http://dx.doi.org/10.1103/PhysRevX.2.041021.

[8] Even Chiari, Wafa Makhlouf, Lucie Pepe, Emiel Koridon, Johanna Klein, Bruno Senjean, Benjamin Lasorne & Saad Yalouz (2025): *Ab Initio Polaritonic Chemistry on Diverse Quantum Computing Platforms: Qubit, Qudit, and Hybrid Qubit-Qumode Architectures*, doi:https://doi.org/10.48550/arXiv.2506.12504. Available at http://arxiv.org/abs/2506.12504. ArXiv:2506.12504 [quant-ph].

[9] Marston D. E. Conder, Edmund Robertson & Peter Williams (1992): *Presentations for 3-dimensional special linear groups over integer rings*. *Proceedings of the American Mathematical Society* 115(1), pp. 19–26, doi:https://doi.org/10.1090/S0002-9939-1992-1079696-5.

[10] Arianne Meijer-van de Griend & Ross Duncan (2023): *Architecture-Aware Synthesis of Phase Polynomials for NISQ Devices*. *Electronic Proceedings in Theoretical Computer Science* 394, p. 116–140, doi:https://doi.org/10.4204/eptcs.394.8. Available at http://dx.doi.org/10.4204/EPTCS.394.8.

[11] Luke E. Heyfron & Earl Campbell (2019): *A quantum compiler for qudits of prime dimension greater than 3*. Available at https://arxiv.org/abs/1902.05634.

[12] Korbinian Kottmann (2025): *Phase Polynomial Intermediate Representation*. https://pennylane.ai/compilation/phase-polynomial-intermediate-representation.

[13] Yves Lafont (2003): *Towards an algebraic theory of Boolean circuits*. Journal of Pure and Applied Algebra 184(2), pp. 257–310, doi:https://doi.org/https://doi.org/10.1016/S0022-4049(03)00069-0. Available at https://www.sciencedirect.com/science/article/pii/S0022404903000690.

[14] Sarah Meng Li, Michele Mosca, Neil J. Ross, John van de Wetering & Yuming Zhao (2025): *A Complete and Natural Rule Set for Multi-Qutrit Clifford Circuits*. Electronic Proceedings in Theoretical Computer Science 426, p. 23–78, doi:https://doi.org/10.4204/eptcs.426.2. Available at http://dx.doi.org/10.4204/EPTCS.426.2.

[15] Hideya Matsumoto (1969): *Sur les sous-groupes arithmétiques des groupes semi-simples déployés*. Annales scientifiques de l'École Normale Supérieure 4e série, 2(1), pp. 1–62, doi:https://doi.org/10.24033/asens.1174. Available at https://www.numdam.org/articles/10.24033/asens.1174/.

[16] Boldizsár Poór, Robert I. Booth, Titouan Carette, John van de Wetering & Lia Yeh (2023): *The Qupit Stabiliser ZX-travaganza: Simplified Axioms, Normal Forms and Graph-Theoretic Simplification*, doi:https://doi.org/10.4204/eptcs.384.13. Available at http://dx.doi.org/10.4204/EPTCS.384.13.

[17] Daniel Quillen (1972): *On the Cohomology and K-Theory of the General Linear Groups Over a Finite Field*. Annals of Mathematics 96(3), pp. 552–586. Available at http://www.jstor.org/stable/1970825.

[18] Robert Steinberg & Robert Steinberg (2016): *Lectures on Chevalley groups*. University lecture series volume 66, American Mathematical Society, Providence, Rhode Island. (Formerly: Mimeographed notes, Department of Math., Yale University, 1967/68.).

[19] Vivien Vandaele, Simon Martiel & Timothée Goubault de Brugière (2022): *Phase polynomials synthesis algorithms for NISQ architectures and beyond*. Quantum Science and Technology 7(4), p. 045027, doi:https://doi.org/10.1088/2058-9565/ac5a0e. Available at http://dx.doi.org/10.1088/2058-9565/ac5a0e.

[20] Quanlong Wang (2018): *Qutrit ZX-calculus is Complete for Stabilizer Quantum Mechanics*. Electronic Proceedings in Theoretical Computer Science 266, pp. 58–70, doi:https://doi.org/10.4204/EPTCS.266.3. Available at http://arxiv.org/abs/1803.00696. ArXiv:1803.00696 [quant-ph].

[21] Yuchen Wang, Zixuan Hu, Barry C. Sanders & Sabre Kais (2020): *Qudits and High-Dimensional Quantum Computing*. Frontiers in Physics 8, doi:https://doi.org/10.3389/fphy.2020.589504. Available at http://dx.doi.org/10.3389/fphy.2020.589504.

[22] Charles A. Weibel (2013): *The K-book: An Introduction to Algebraic K-Theory*. Graduate Studies in Mathematics 145, American Mathematical Society, Providence, RI, doi:https://doi.org/10.1090/gsm/145.

Appendix content

A Derivations

A.1 Derivations for the Affine fragment

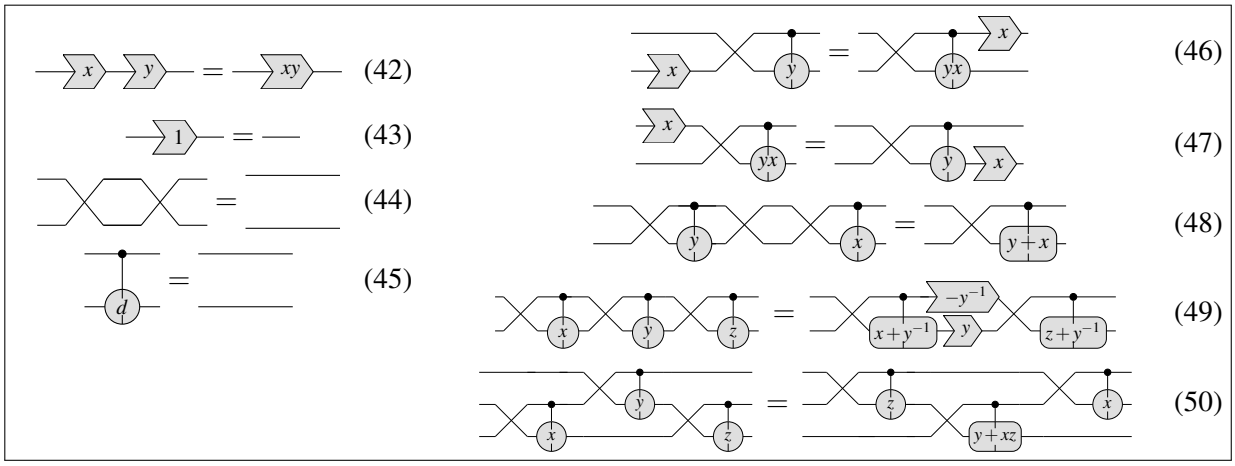


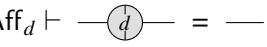
Figure 5: The ruleset [13] for circuits of linear transformations over $\mathrm{GL}(\mathbb{F}_d)$. We include Equation (45) because in Lafont's presentation the labels are in the field, which in $\mathbb{F}_d$ means taken modulo d.

Lemma 13. *For every rule $C = C'$ in Figure 5,* $\mathrm{Aff}_d \vdash C = C'$

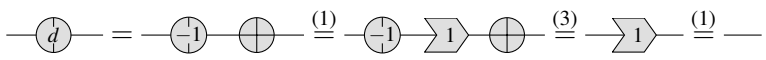
Proof. Let $C = C'$ be any equation in Figure 5. We show $\mathrm{Aff}_d \vdash C = C'$ by a case analysis on the equation.

1. For Equations (42) and (43), the statement is immediate: these equations appear verbatim among the axioms of Aff_d, namely Equations (1) and (2).
2. Equation Equation (46) is obtained from Equation (4) by closure of derivability under tensoring with identities, composition, and symmetries in a PROP.
3. Equation Equation (47) is derived in the same way from Lemma 17.
4. Equation Equation (44) is an instance of the symmetric monoidal axioms, since $\sigma_{1,1} \circ \sigma_{1,1} = \mathrm{id}_2$.
5. Equation Equation (48) holds by expanding the abbreviation  from Definition 5 and using associativity of composition.
6. Equation Equation (49) is proved using Lemma 22 and Lemma 16.
7. Equation Equation (50) follows from Lemma 19 together with the PROP laws.
8. Equation Equation (45) is proved in Lemma 16.

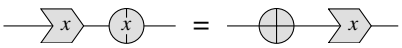
This covers all equations in Figure 5, hence every rule $C = C'$ in Lafont's presentation is derivable in Aff_d. □

Lemma 14. $\mathrm{Aff}_d \vdash$ 

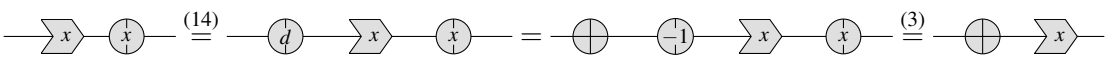
Proof.



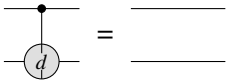
□

Lemma 15. $\forall x \in \mathbb{F}_d^\times$, $\mathsf{Aff}_d \vdash$ 

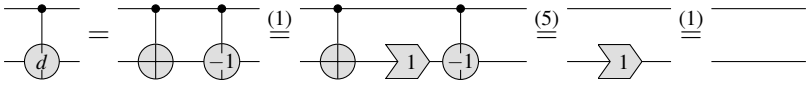
Proof.



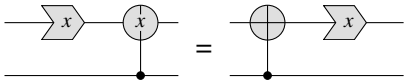
□

Lemma 16. $\mathsf{Aff}_d \vdash$ 

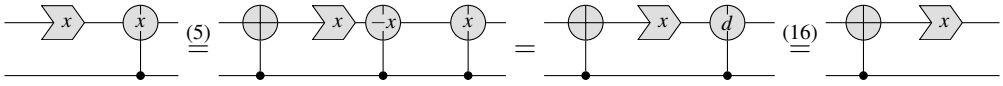
Proof.



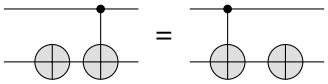
□

Lemma 17. $\forall x \in \mathbb{F}_d^\times$, $\mathsf{Aff}_d \vdash$ 

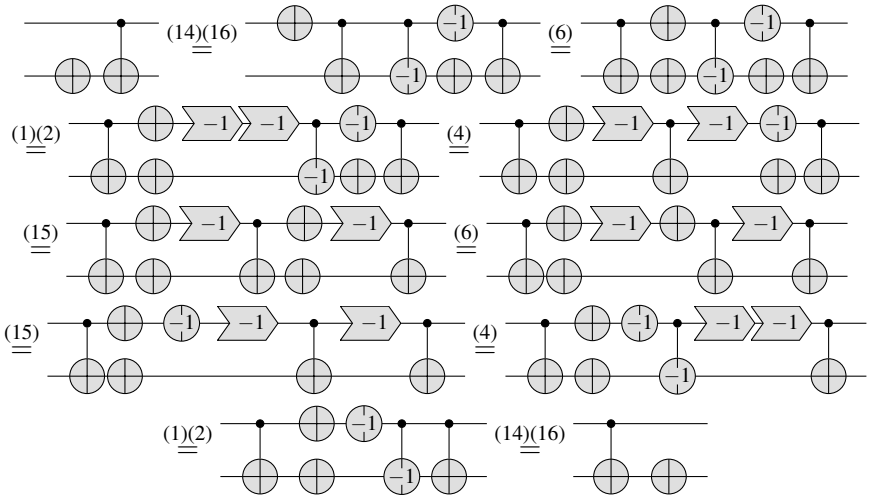
Proof.



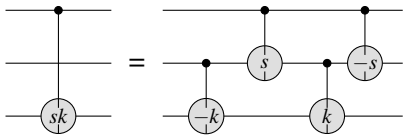
□

Lemma 18. $\mathsf{Aff}_d \vdash$ 

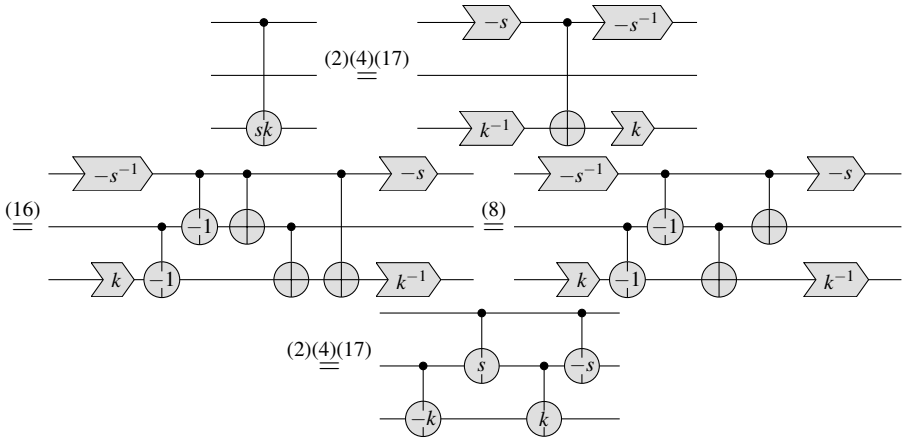
Proof.



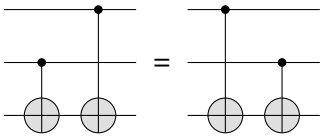
□

Lemma 19. $\forall s,k \in \mathbb{F}_d^\times$, $\mathsf{Aff}_d \vdash$ 

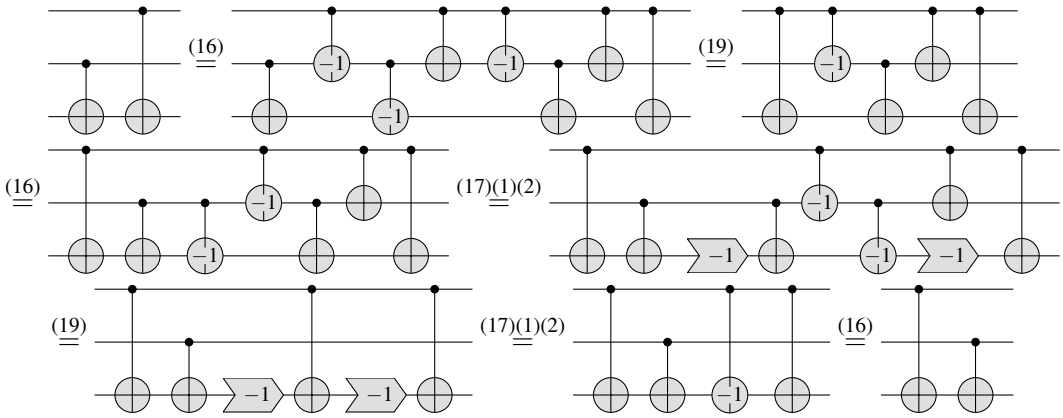
Proof.



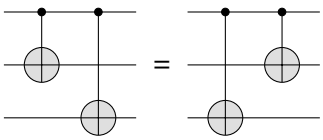
□

Lemma 20. $\mathsf{Aff}_d \vdash$ 

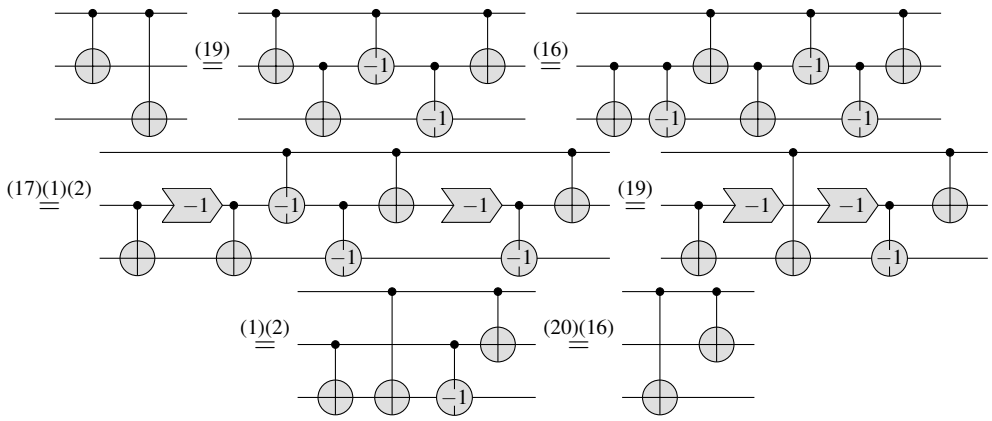
Proof.



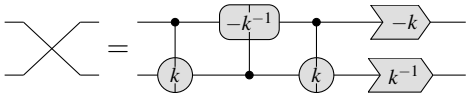
□

Lemma 21. $\mathsf{Aff}_d \vdash$ 

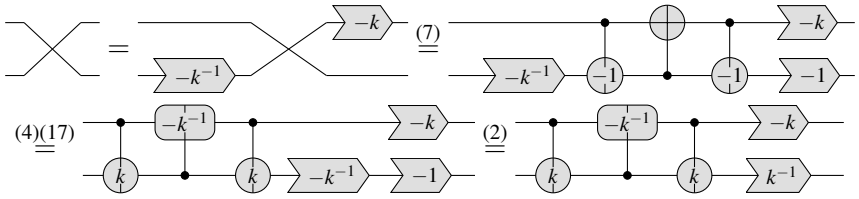
Proof.



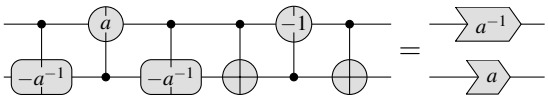
□

Lemma 22. $\forall k \in \mathbb{F}_d^\times$, $\mathsf{Aff}_d \vdash$ 

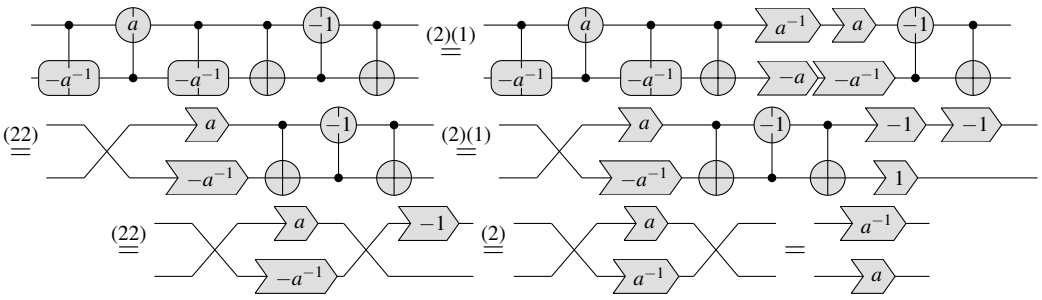
Proof.



□

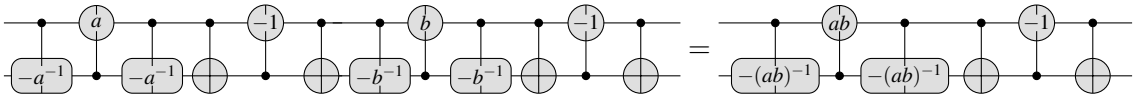
Lemma 23. $\forall a \in \mathbb{F}_d^\times$, $\mathsf{Aff}_d \vdash$ 

Proof.

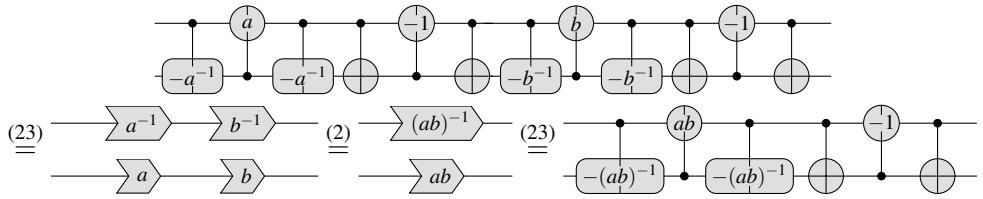


□

Lemma 24. $\forall a, b \in \mathbb{F}_d^\times$, $\mathsf{Aff}_d \vdash$

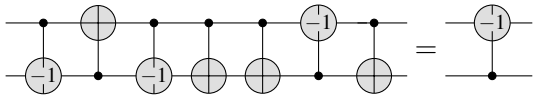


Proof.

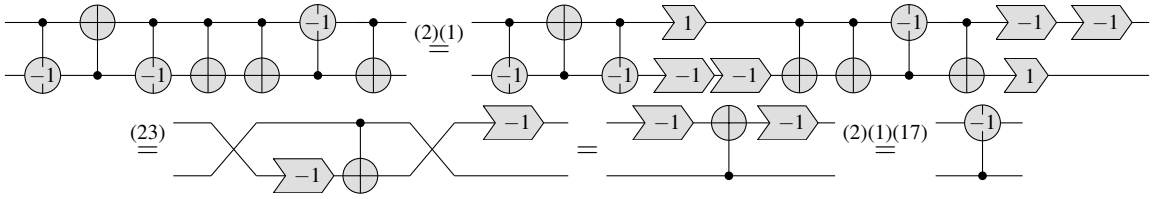


□

Lemma 25. $\mathsf{Aff}_d \vdash$



Proof.

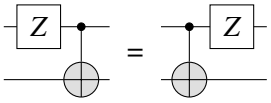


□

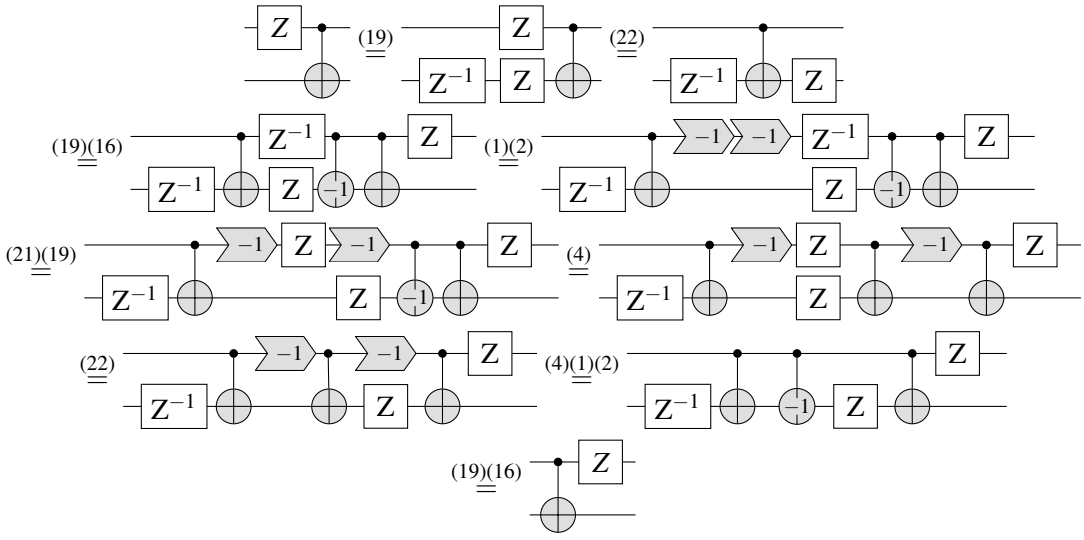
A.2 Derivations for the Phases fragments

A.2.1 The Z fragment

Lemma 26. $\mathrm{LinPhase}_d \vdash$

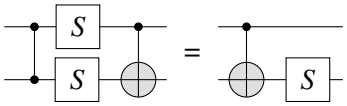


Proof.

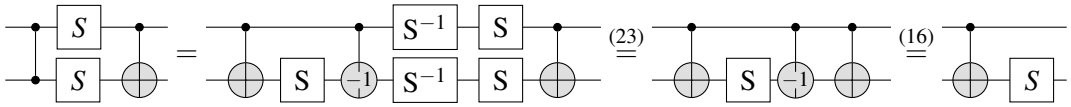


□

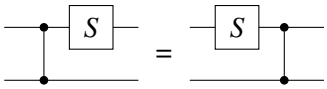
A.2.2 The S fragment

Lemma 27. *QuadPhase*$_d \vdash$ 

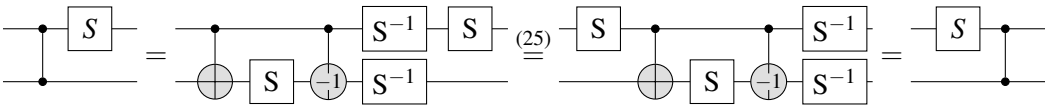
Proof.



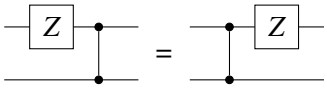
□

Lemma 28. *QuadPhase*$_d \vdash$ 

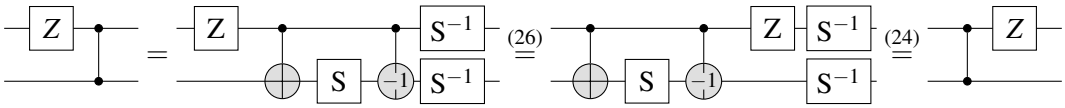
Proof.



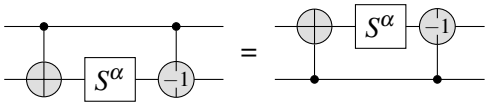
□

Lemma 29. *QuadPhase*$_d \vdash$ 

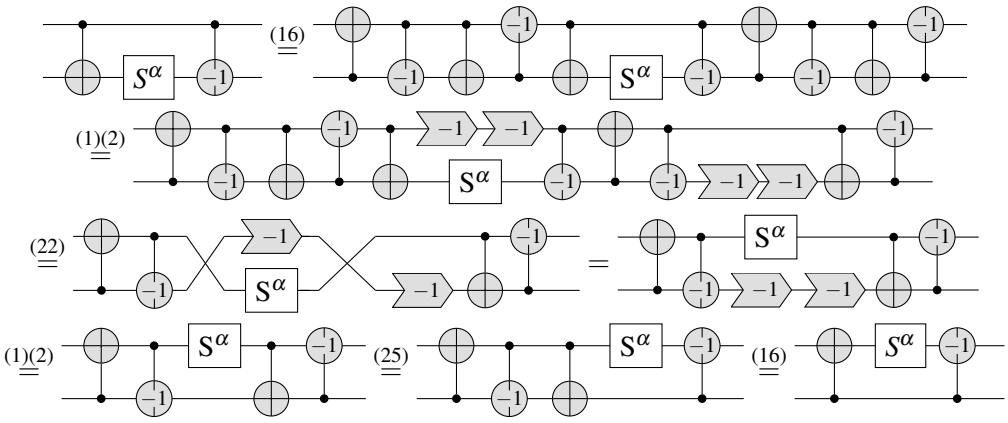
Proof.



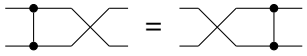
□

Lemma 30. *QuadPhase*$_d \vdash$ 

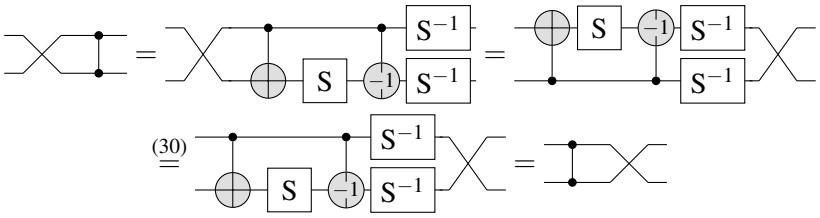
Proof.



□

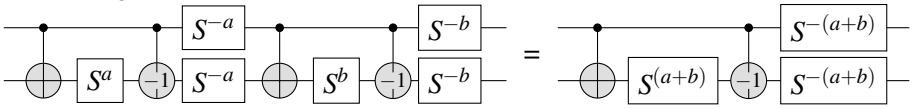
Lemma 31. *QuadPhase*$_d \vdash$ 

Proof.

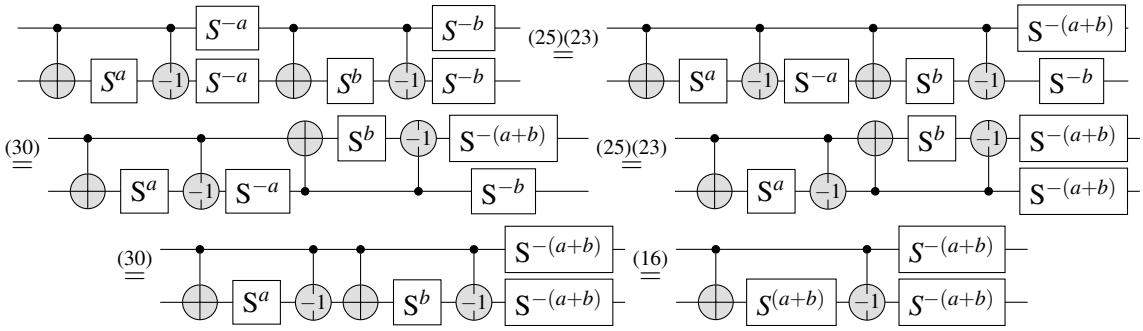


□

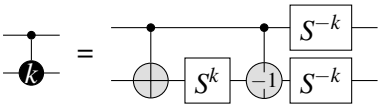
Lemma 32. *QuadPhase*$_d \vdash$

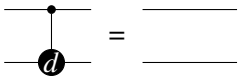


Proof.

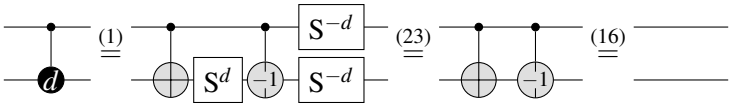


□

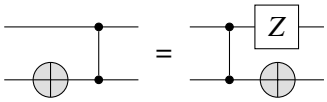
Corollary 1. *QuadPhase*$_d \vdash$ 

Lemma 33. *QuadPhase*$_d \vdash$ 

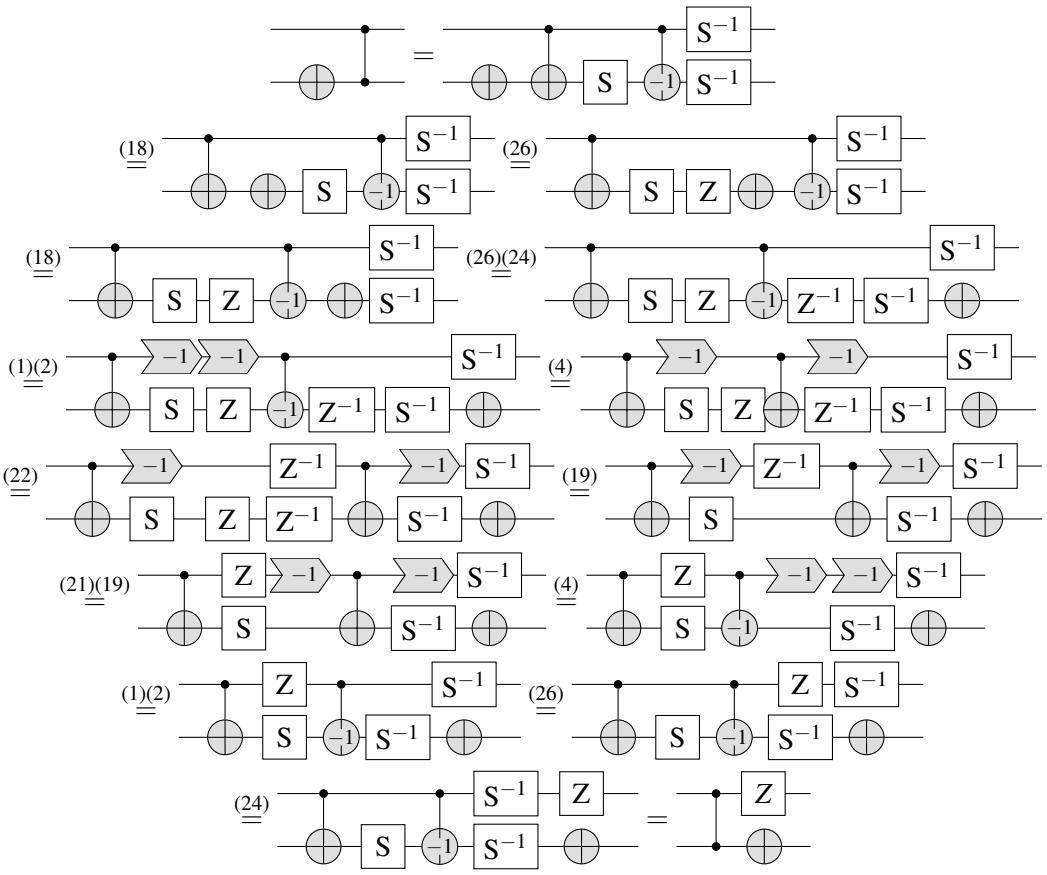
Proof.



□

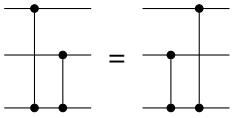
Lemma 34. *QuadPhase*$_d \vdash$ 

Proof.

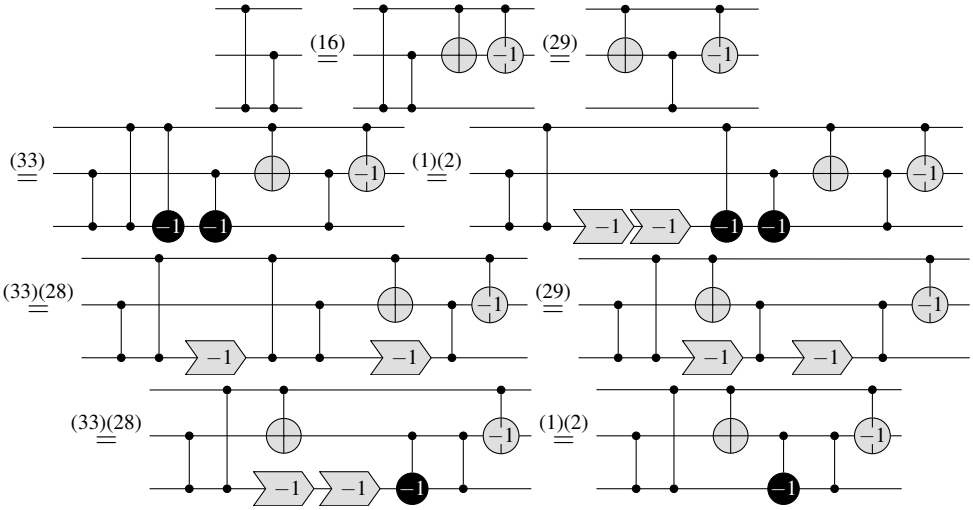


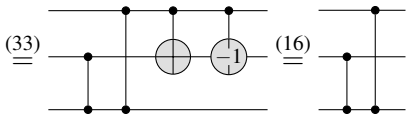
□

Lemma 35. *QuadPhase*$_d \vdash$

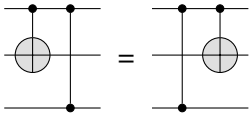


Proof.

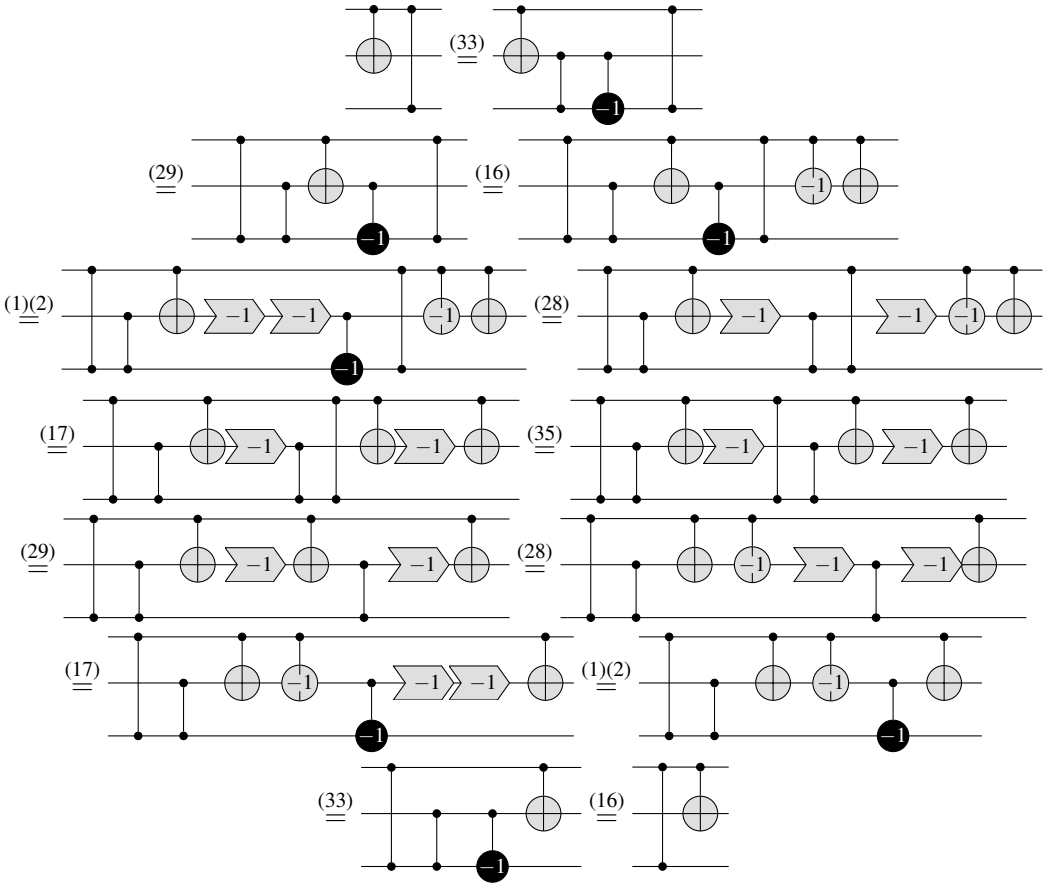




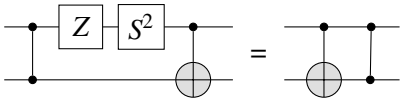
□

Lemma 36. *QuadPhase*$_d \vdash$  =

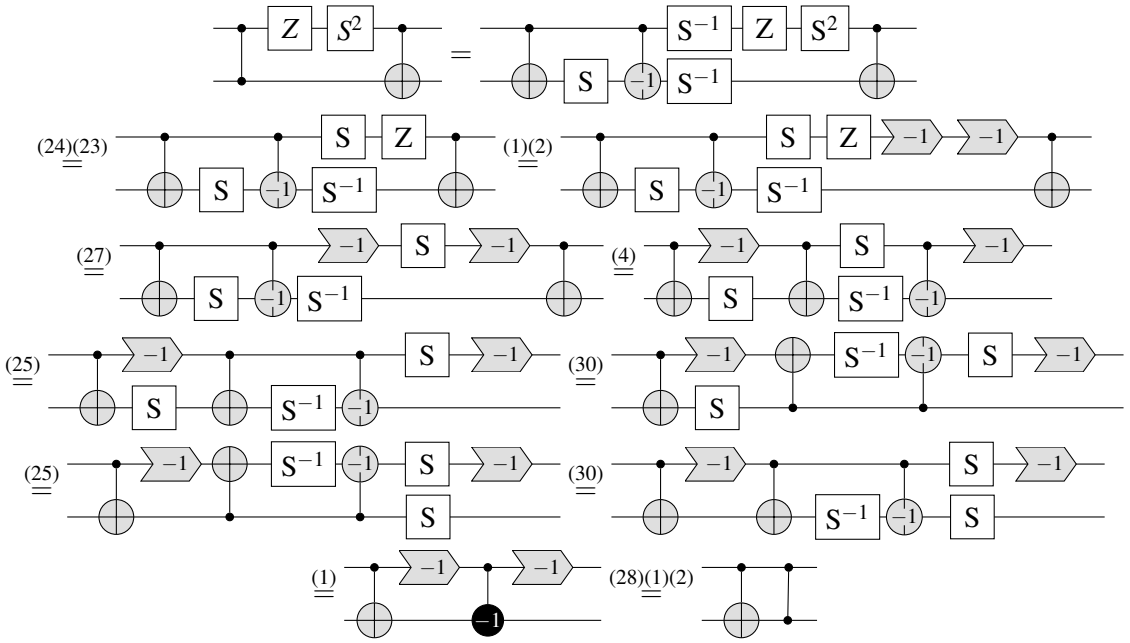
Proof.



□

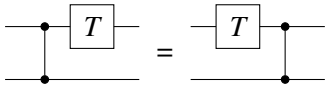
Lemma 37. *QuadPhase*$_d \vdash$  =

Proof.

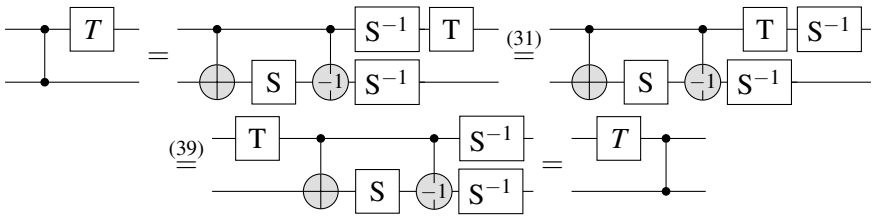


□

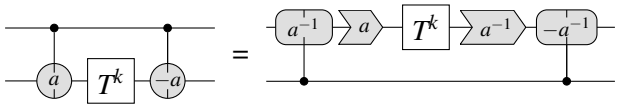
A.2.3 The T fragment

Lemma 38. *CubicPhase*$_d \vdash$  =

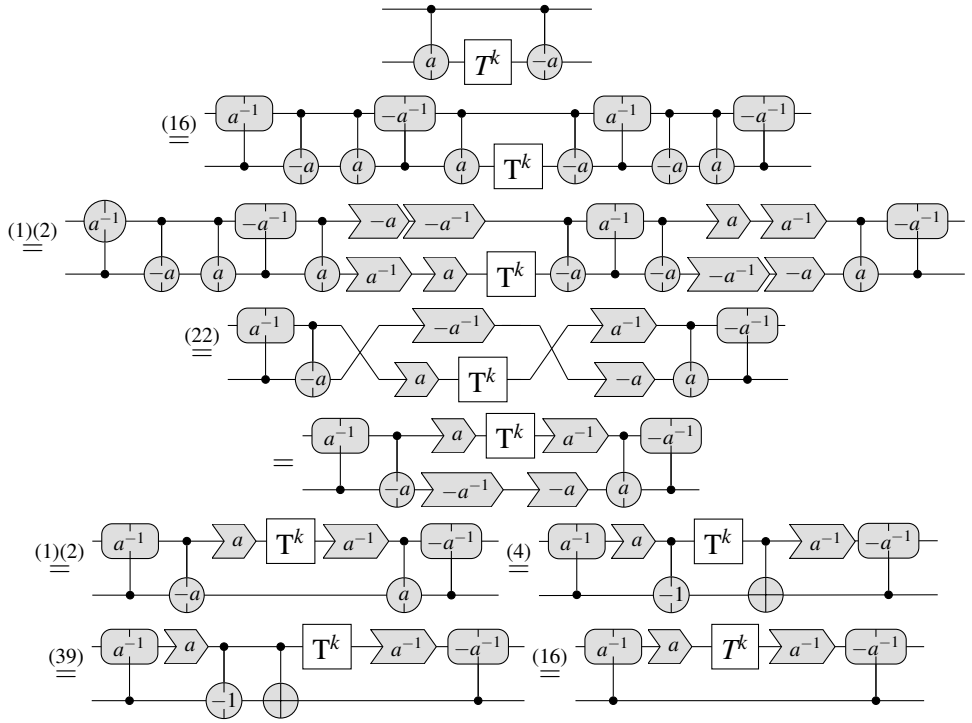
Proof.



□

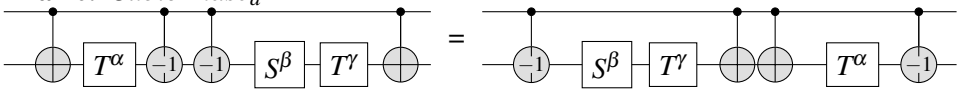
Lemma 39. *CubicPhase*$_d \vdash$  =

Proof.

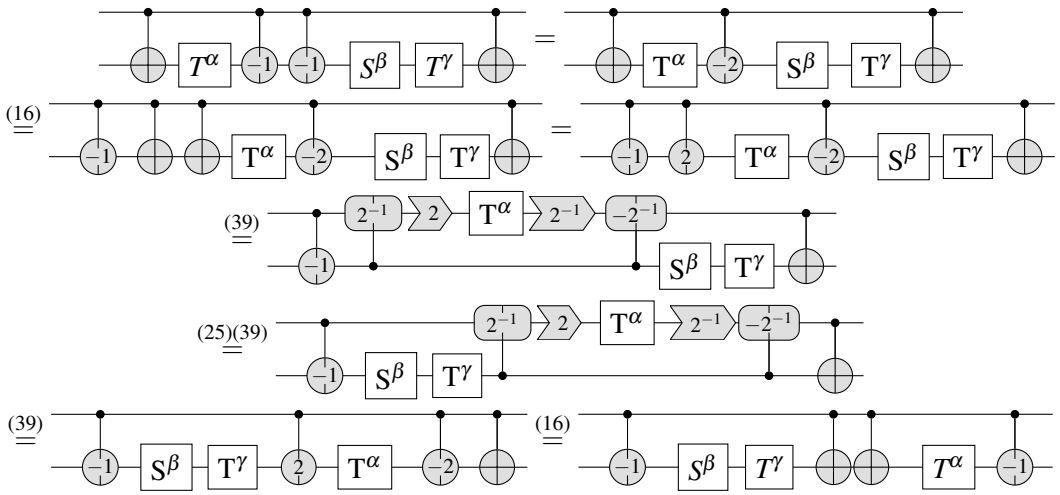


□

Lemma 40. *CubicPhase*$_d \vdash$

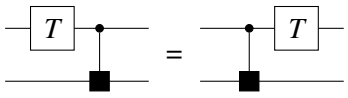


Proof.

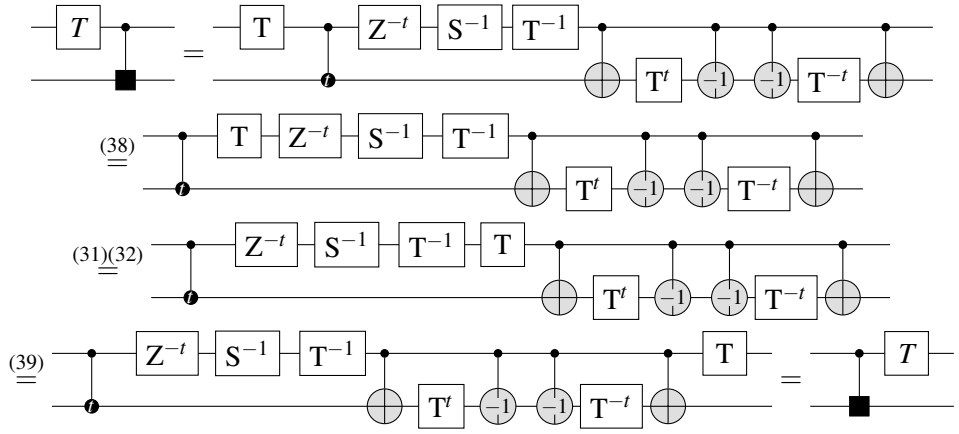


□

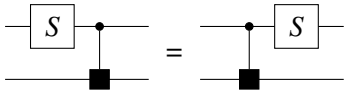
In the remainder of the T-fragment derivations, we use the convention $t = 2^{-1} \in \mathbb{F}_d$, since this is the parameter used in the definition of the derived gate  .

Lemma 41. *CubicPhase*$_d \vdash$ 

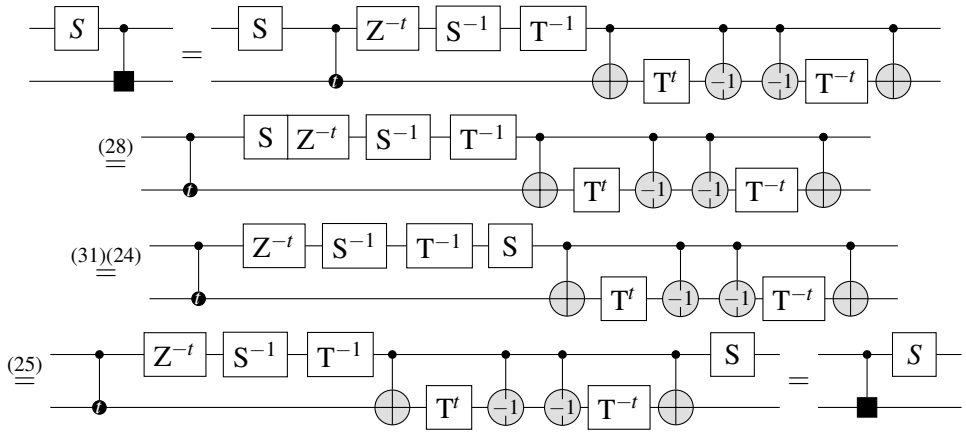
Proof.



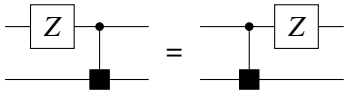
□

Lemma 42. *CubicPhase*$_d \vdash$ 

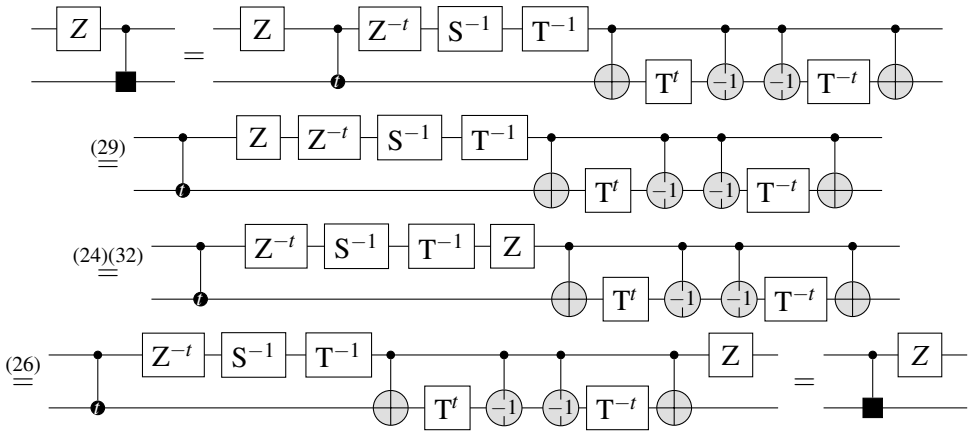
Proof.



□

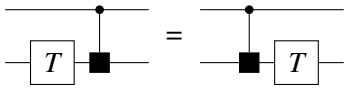
Lemma 43. *CubicPhase*$_d \vdash$ 

Proof.

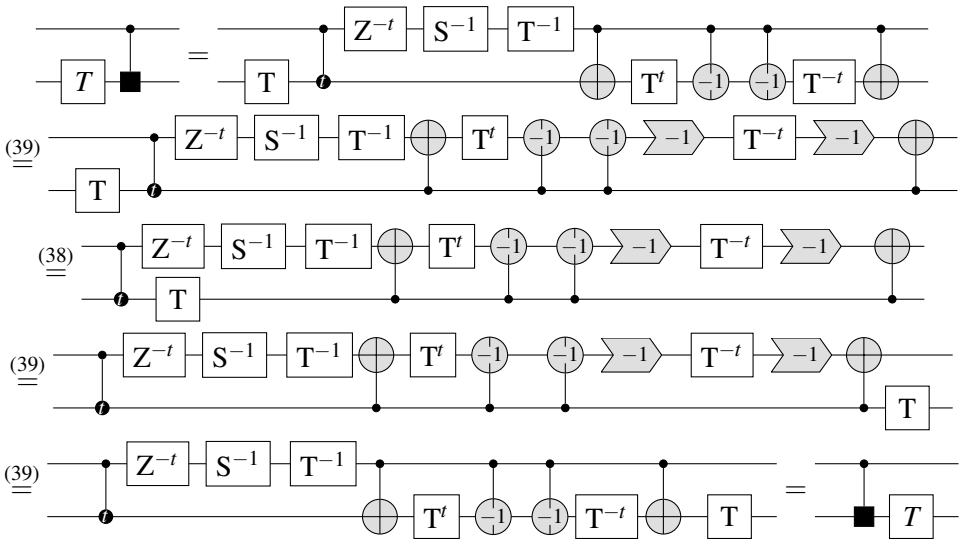


□

Lemma 44. *CubicPhase*$_d \vdash$

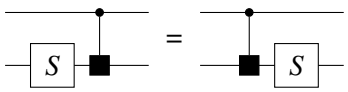


Proof.

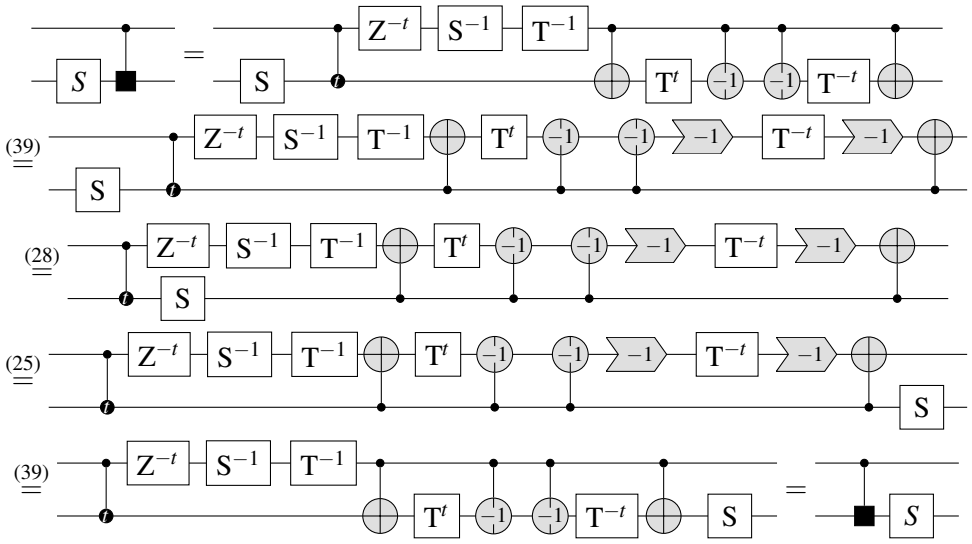


□

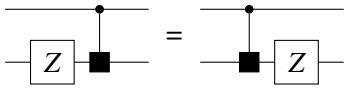
Lemma 45. *CubicPhase*$_d \vdash$



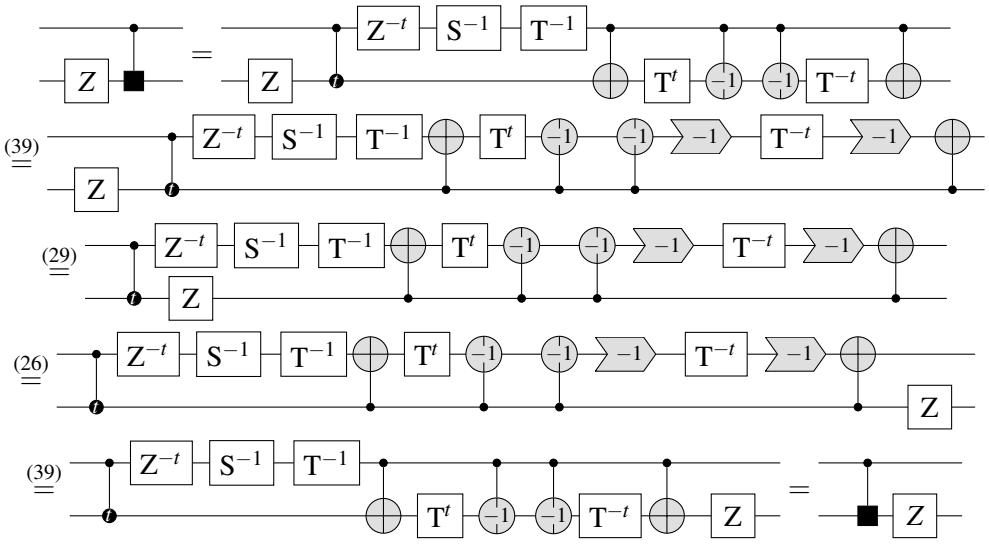
Proof.



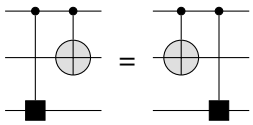
□

Lemma 46. *CubicPhase*$_d \vdash$ 

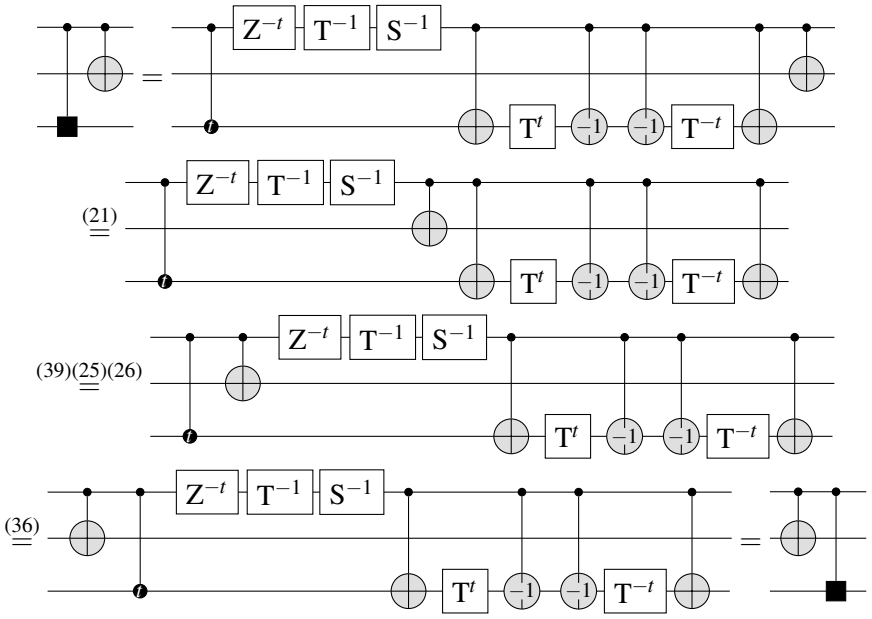
Proof.



□

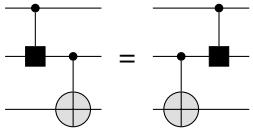
Lemma 47. *CubicPhase*$_d \vdash$ 

Proof.

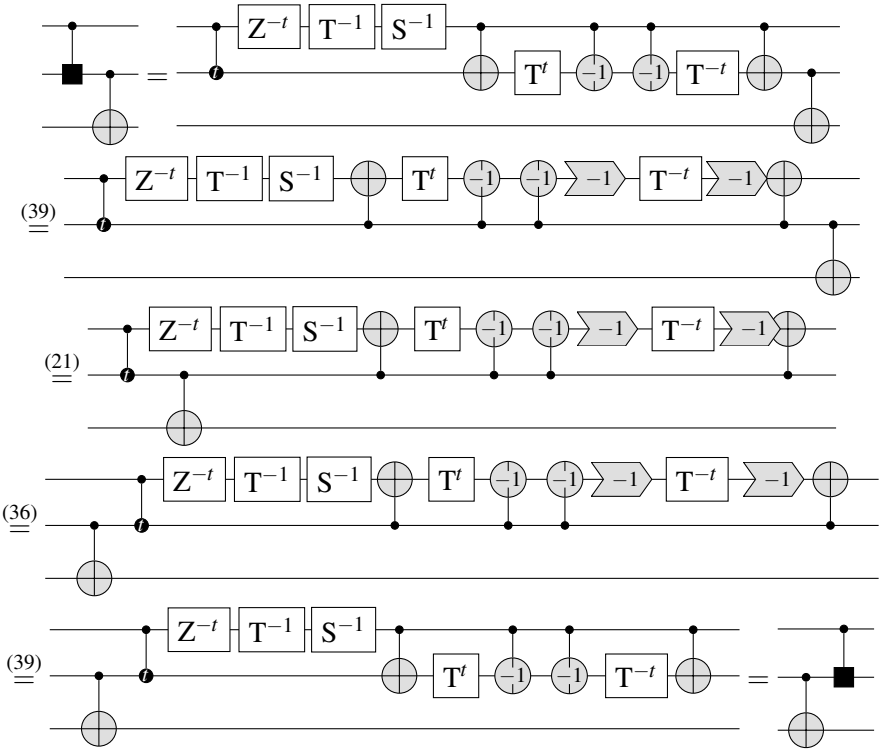


□

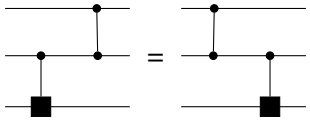
Lemma 48. *CubicPhase*$_d \vdash$



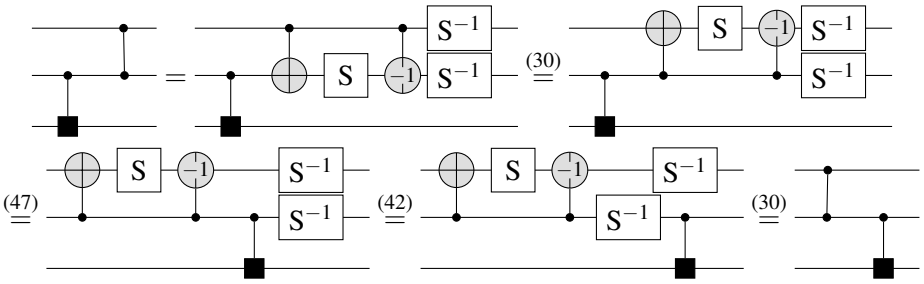
Proof.



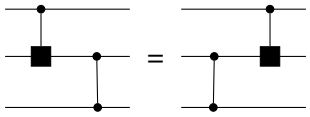
□

Lemma 49. *CubicPhase*$_d \vdash$ 

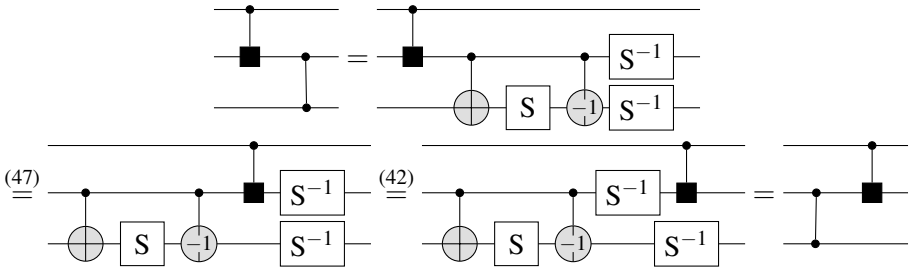
Proof.



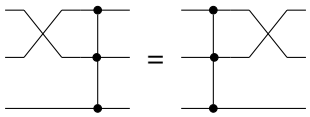
□

Lemma 50. *CubicPhase*$_d \vdash$ 

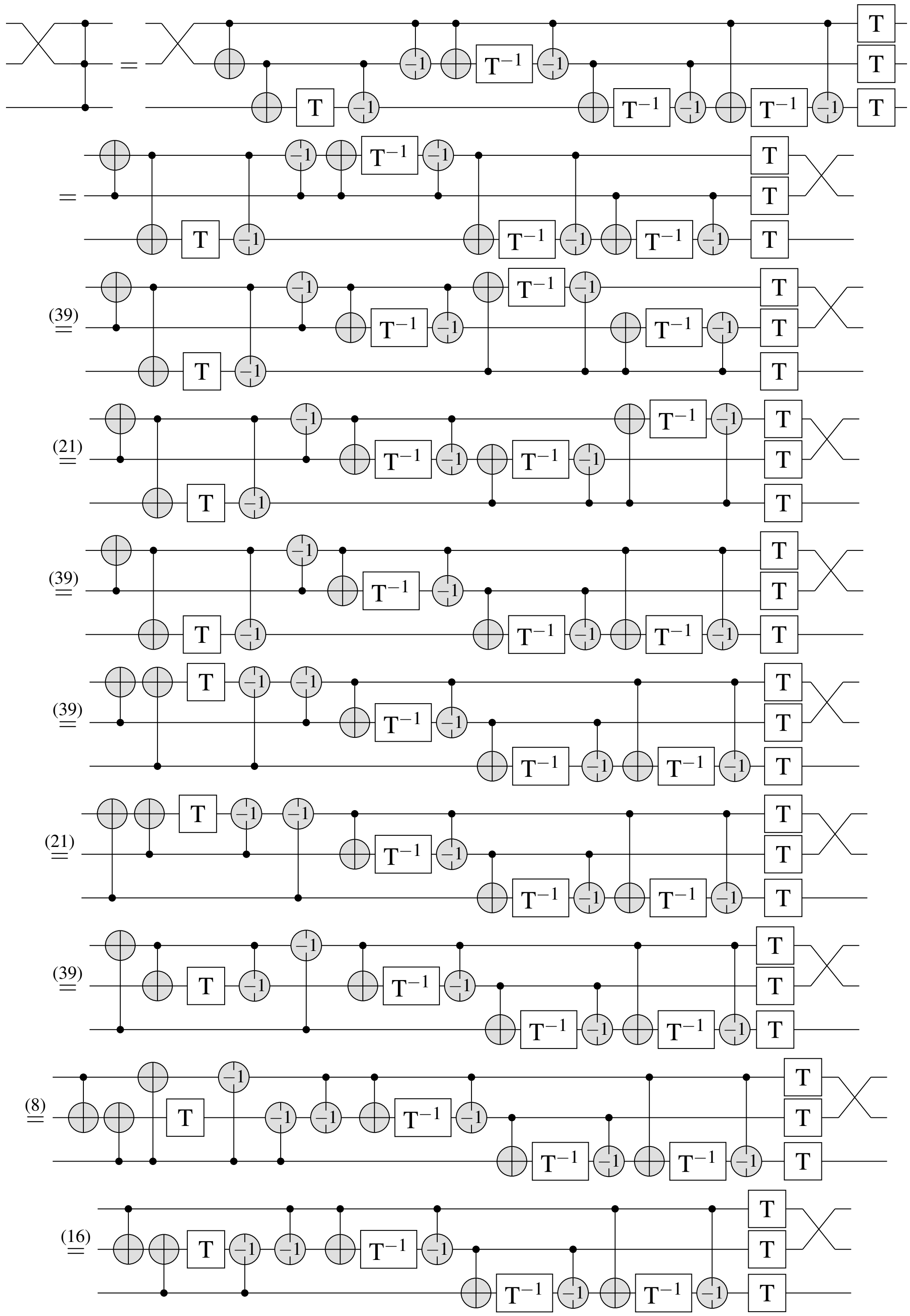
Proof.

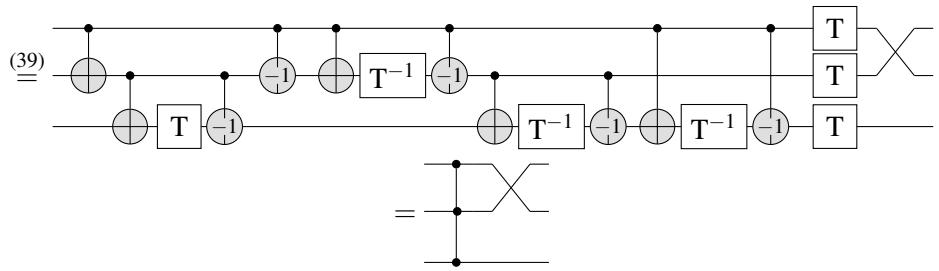


□

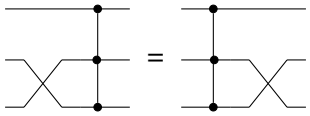
Lemma 51. *CubicPhase*$_d \vdash$ 

Proof.

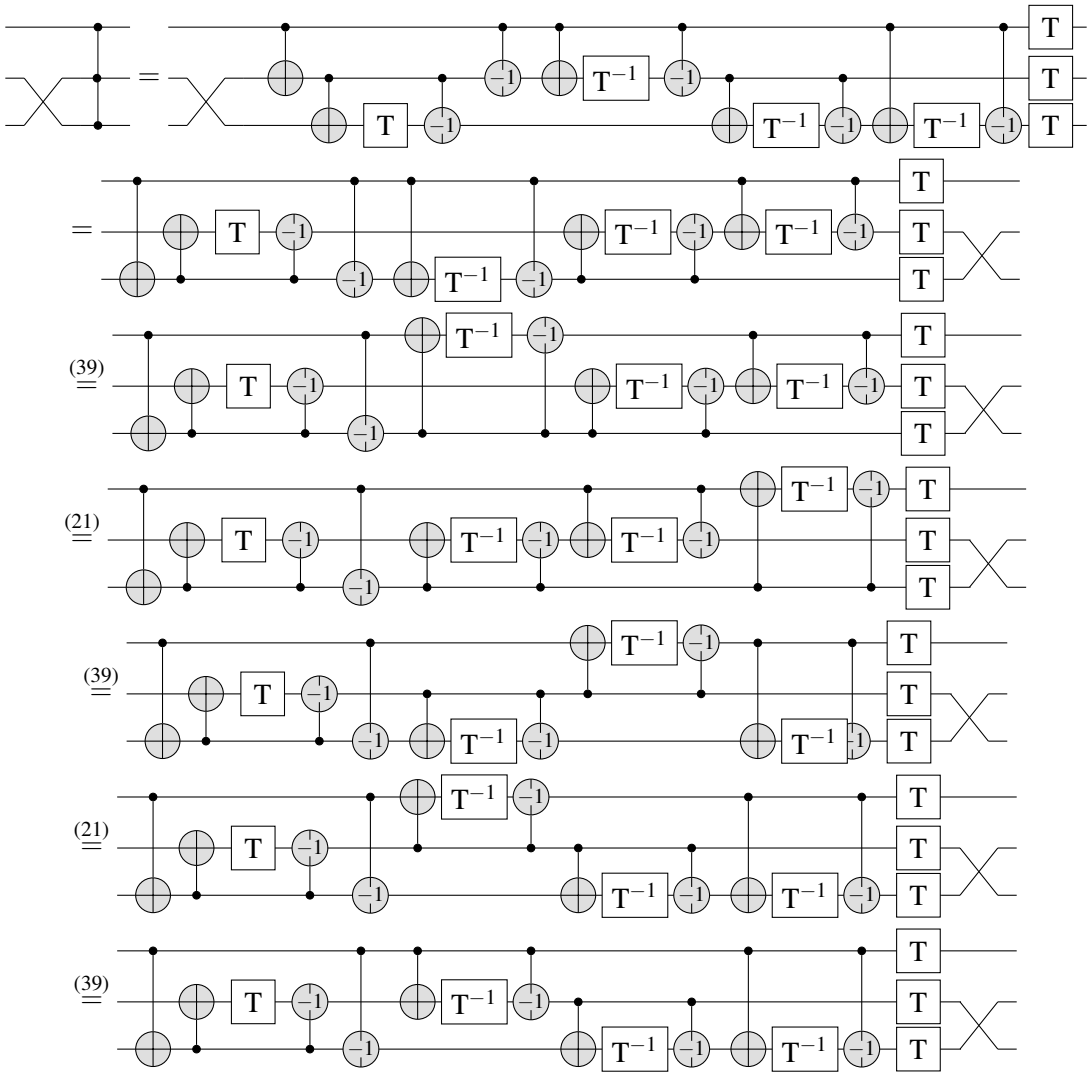


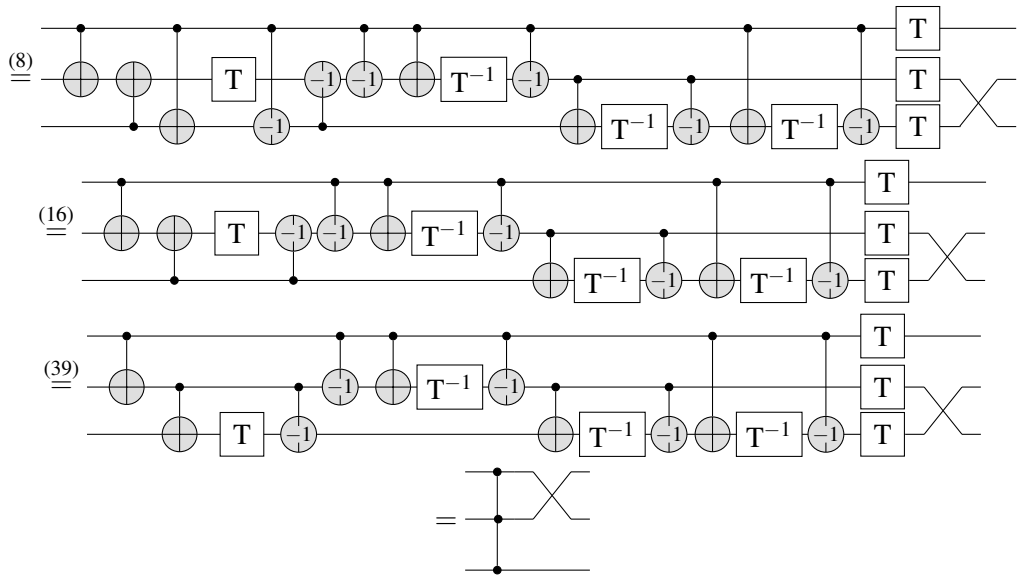


□

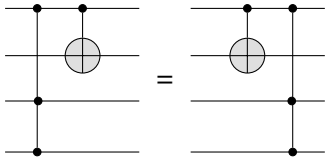
Lemma 52. *CubicPhase*$_d \vdash$  =

Proof.

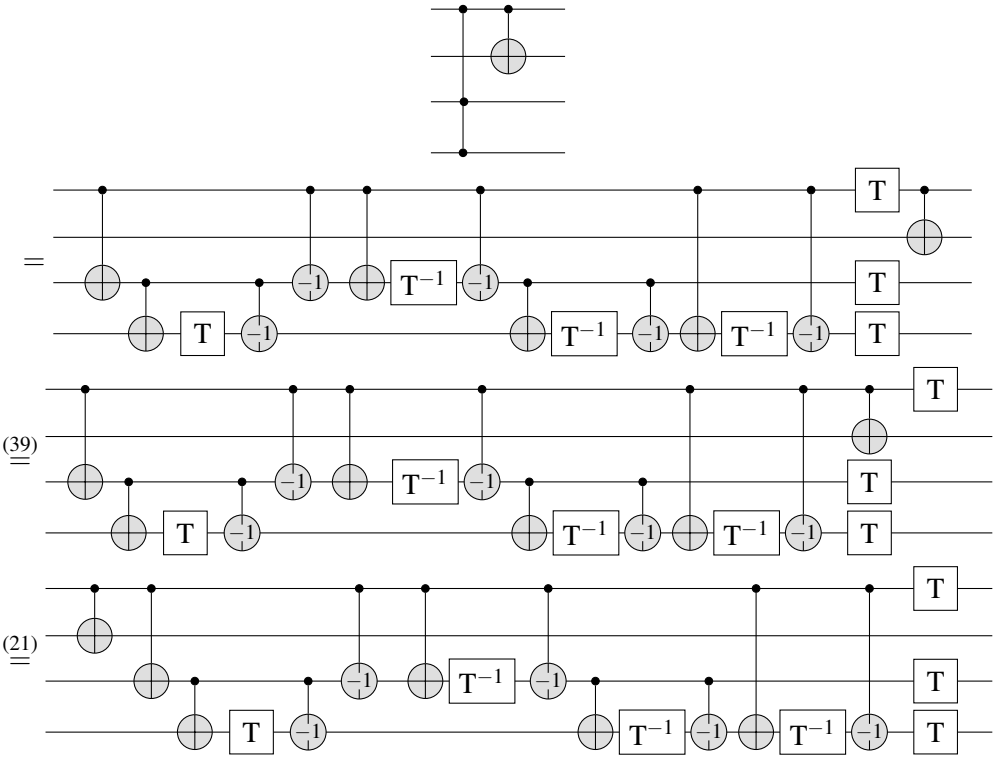


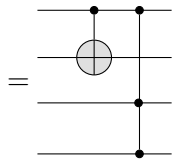


□

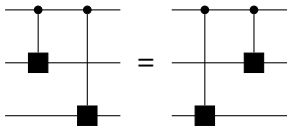
Lemma 53. *CubicPhase*$_d \vdash$ 

Proof.

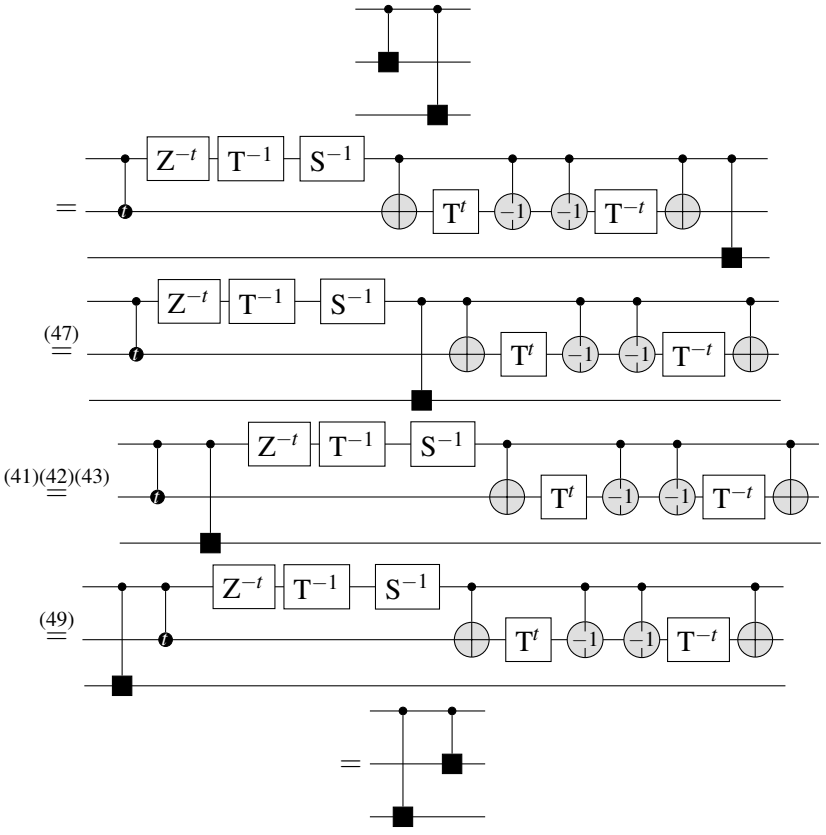




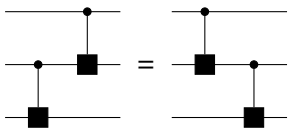
□

Lemma 54. *CubicPhase*$_d \vdash$ 

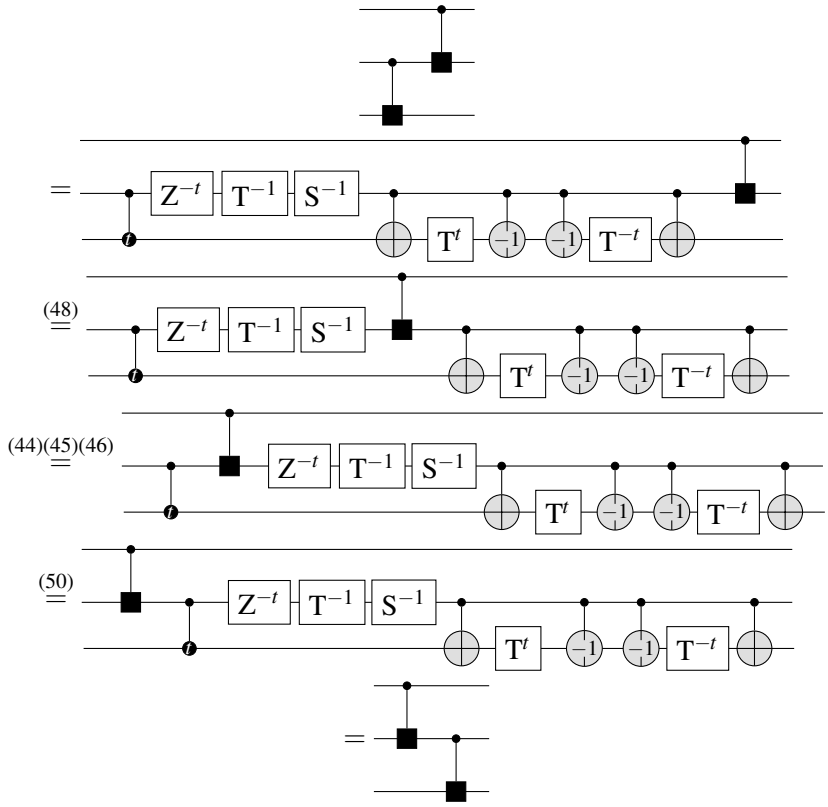
Proof.



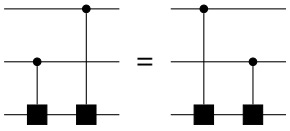
□

Lemma 55. *CubicPhase*$_d \vdash$ 

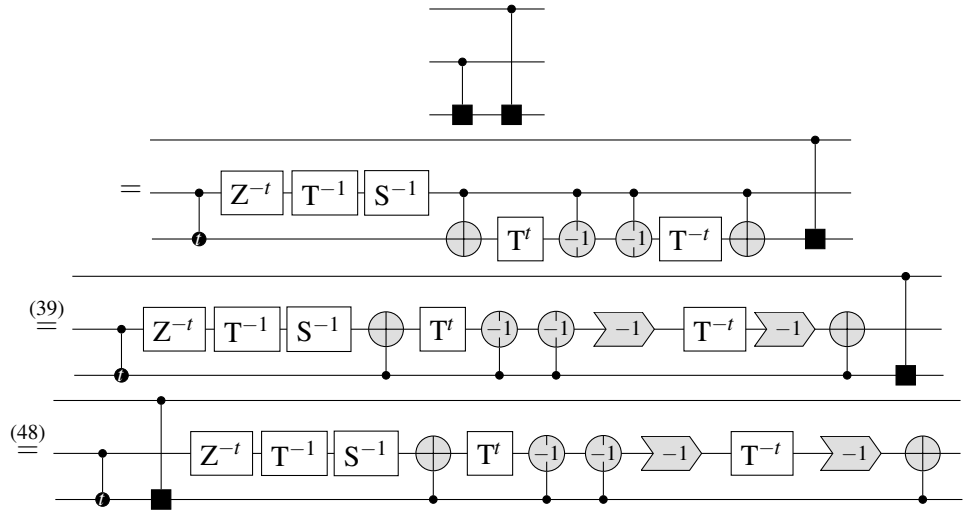
Proof.

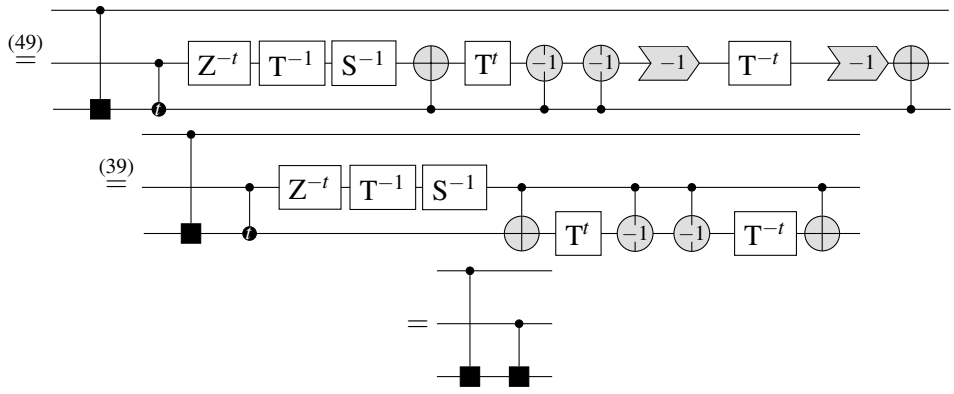


□

Lemma 56. *CubicPhase*$_d \vdash$ 

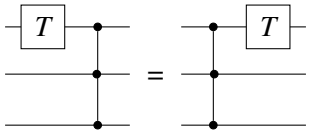
Proof.



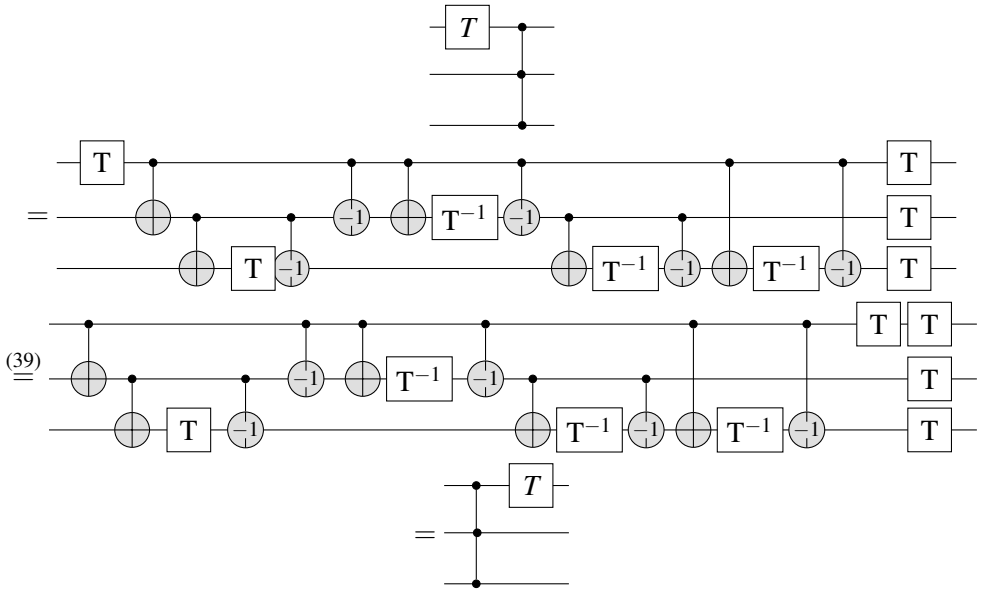


□

Lemma 57. *CubicPhase*$_d \vdash$

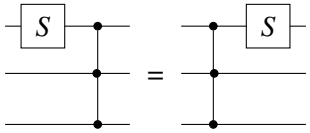


Proof.

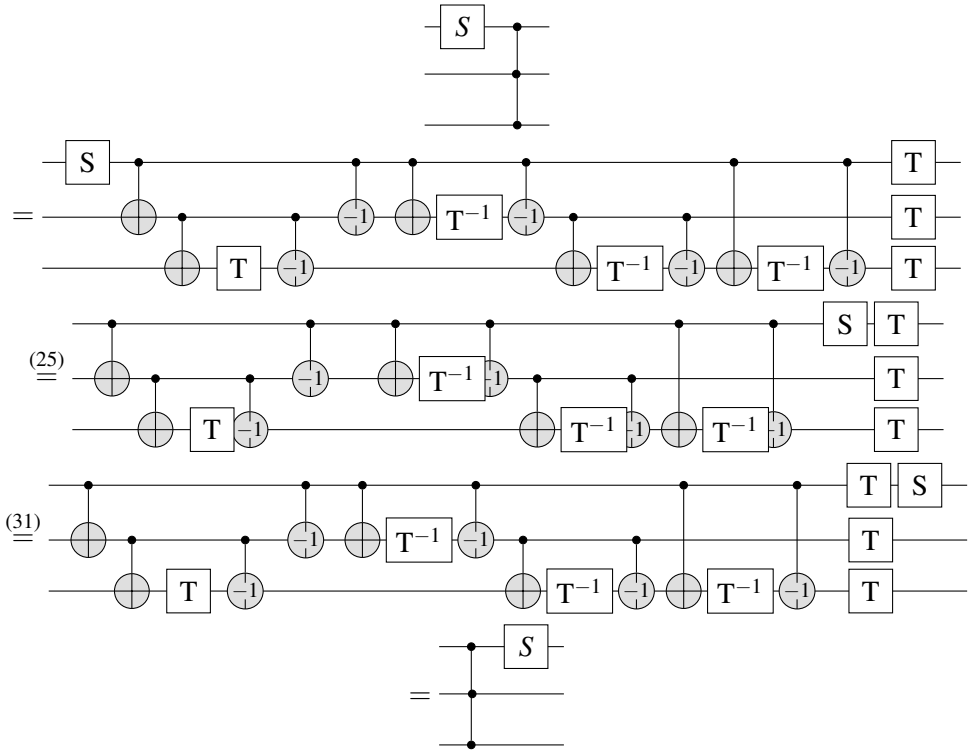


□

Lemma 58. *CubicPhase*$_d \vdash$

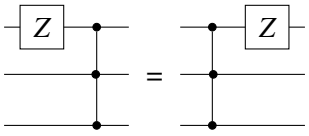


Proof.

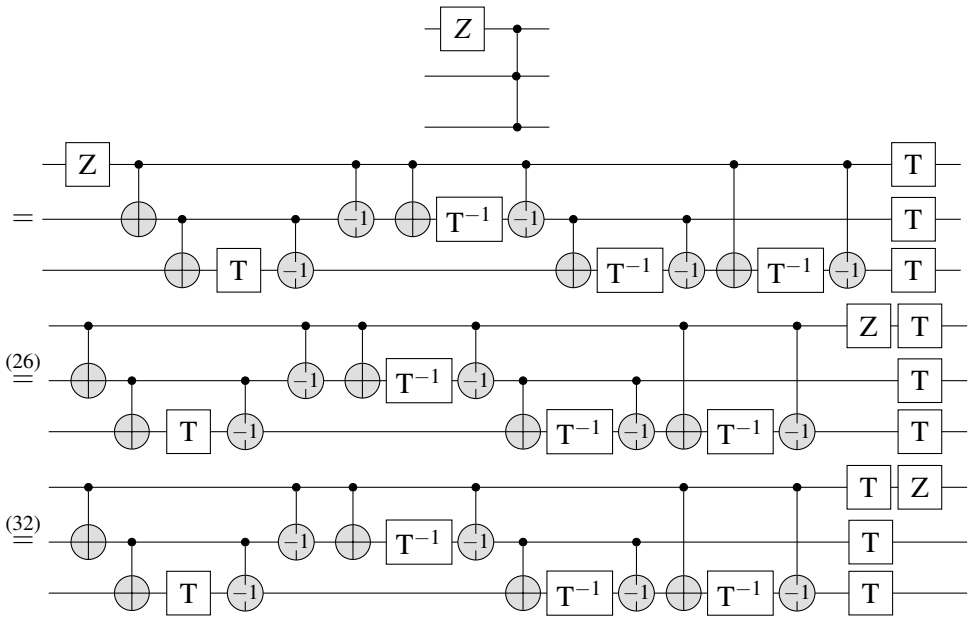


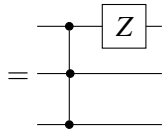
□

Lemma 59. *CubicPhase*$_d \vdash$

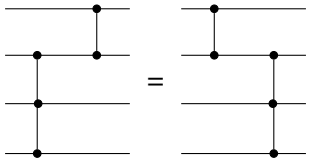


Proof.

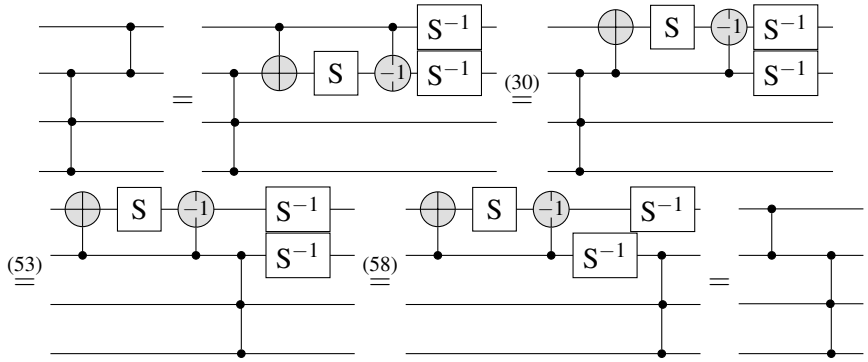




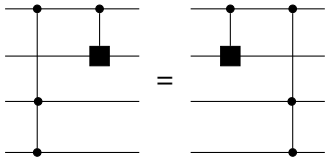
□

Lemma 60. *CubicPhase*$_d \vdash$ 

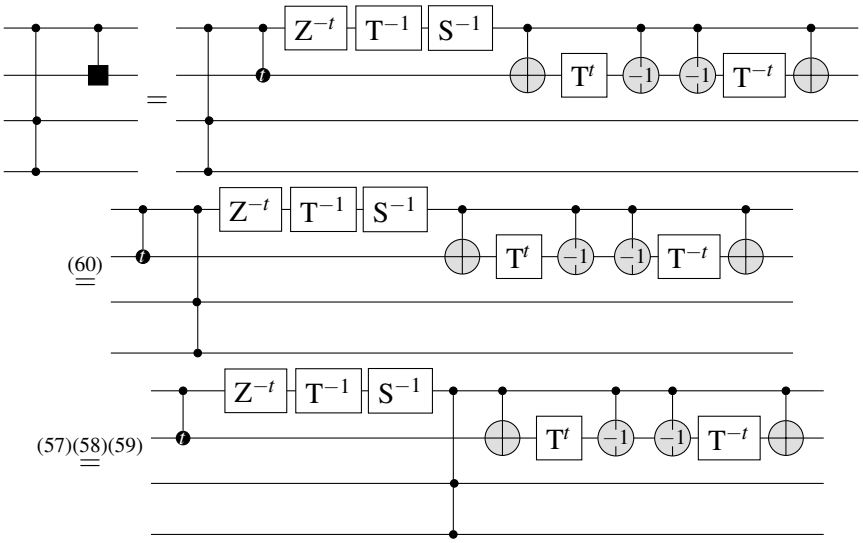
Proof.

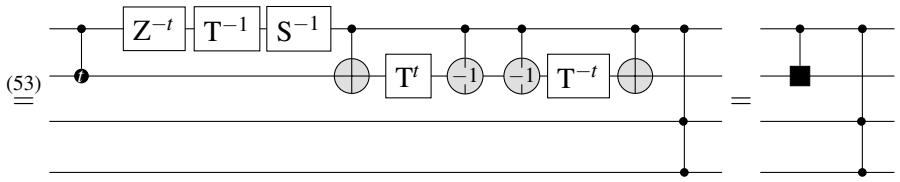


□

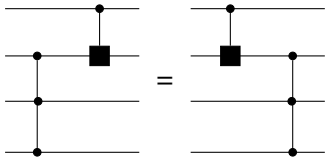
Lemma 61. *CubicPhase*$_d \vdash$ 

Proof.

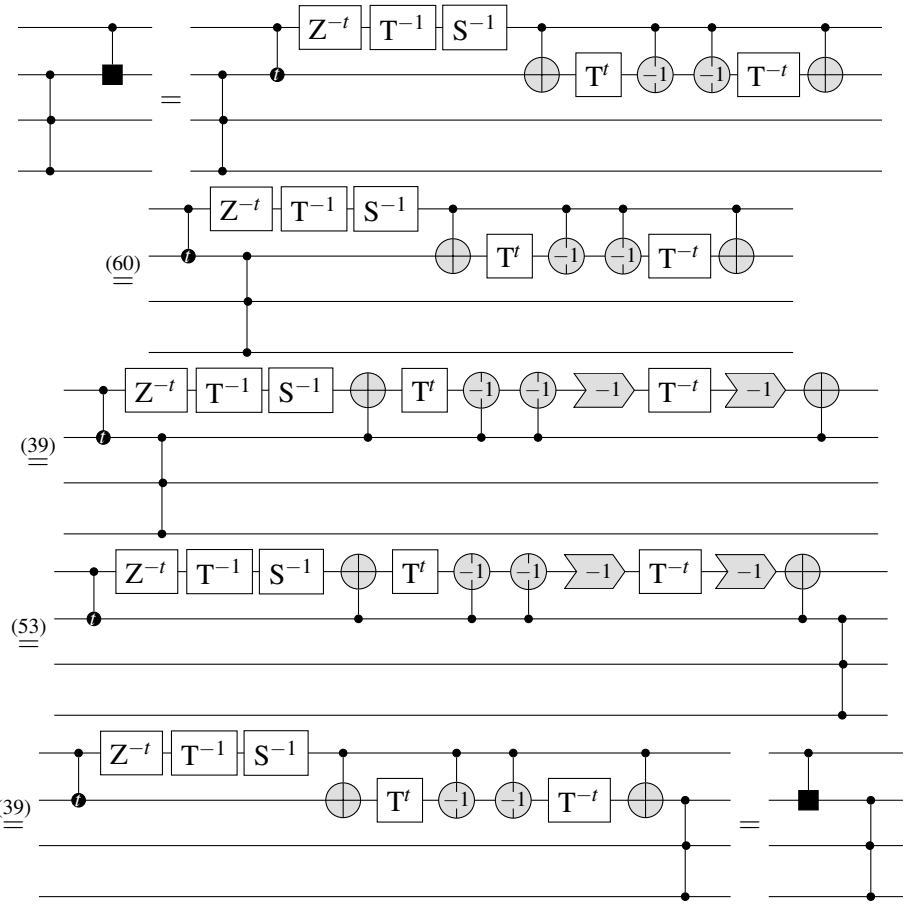




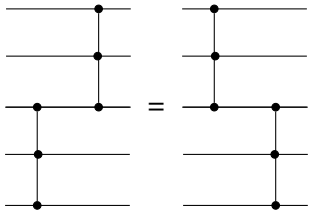
□

Lemma 62. *CubicPhase*$_d \vdash$ 

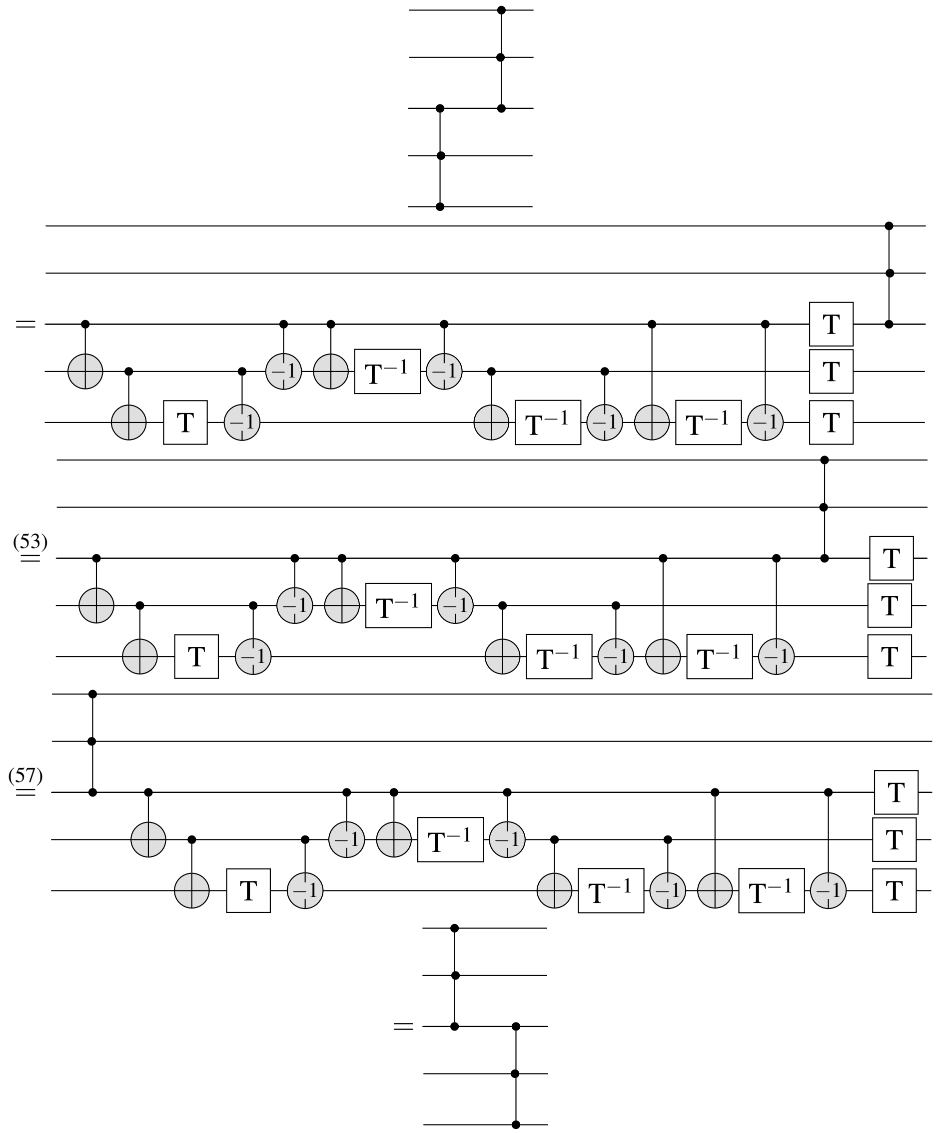
Proof.



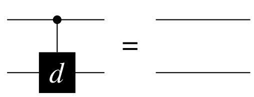
□

Lemma 63. *CubicPhase*$_d \vdash$ 

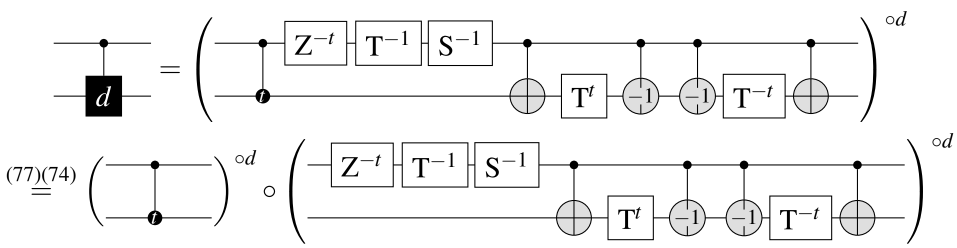
Proof.

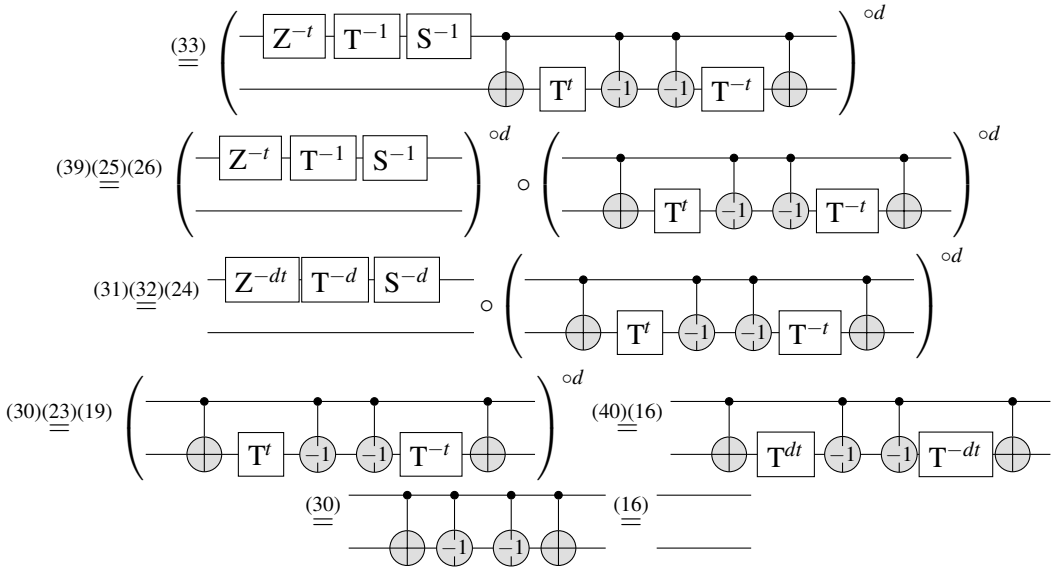


□

Lemma 64. *CubicPhase$_d$* $\vdash$ 

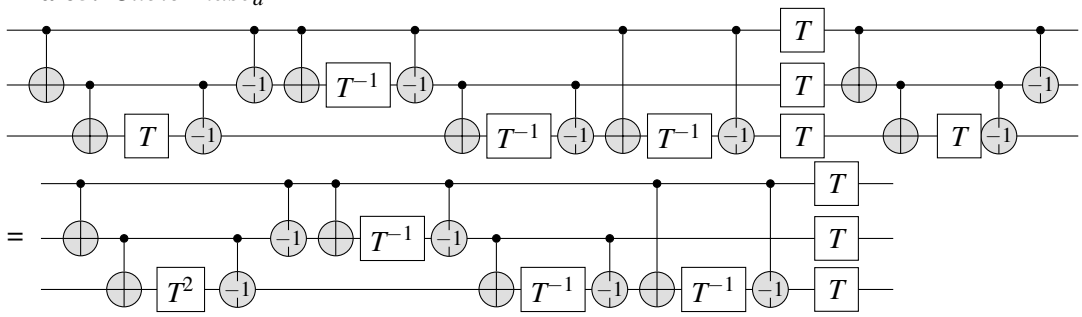
Proof.



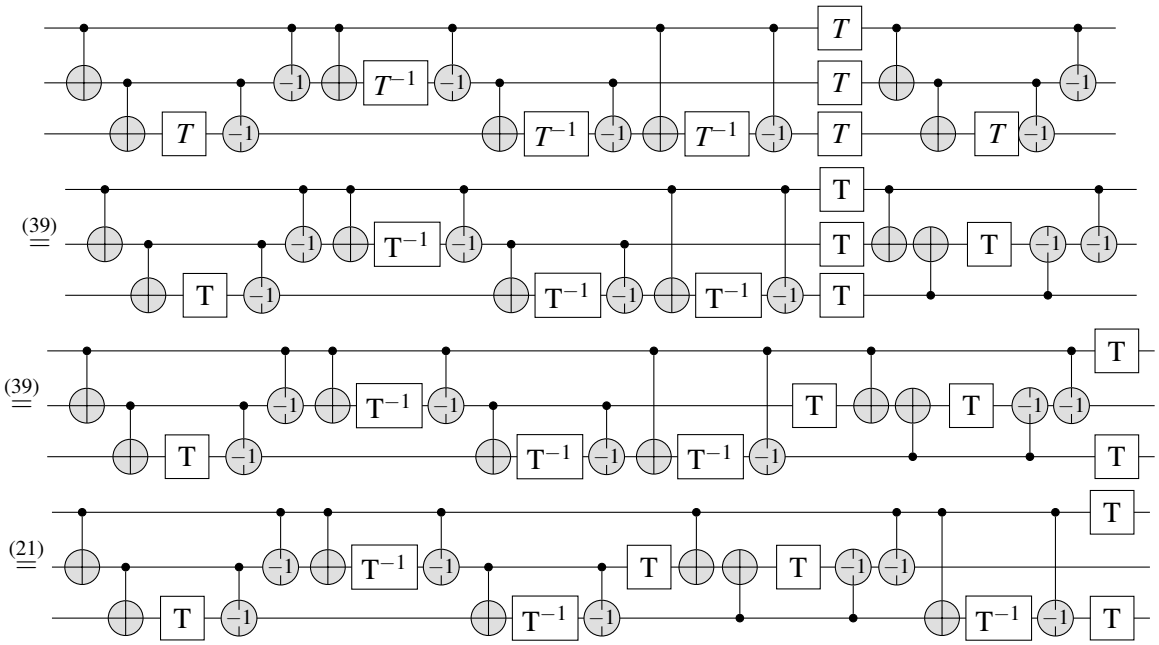


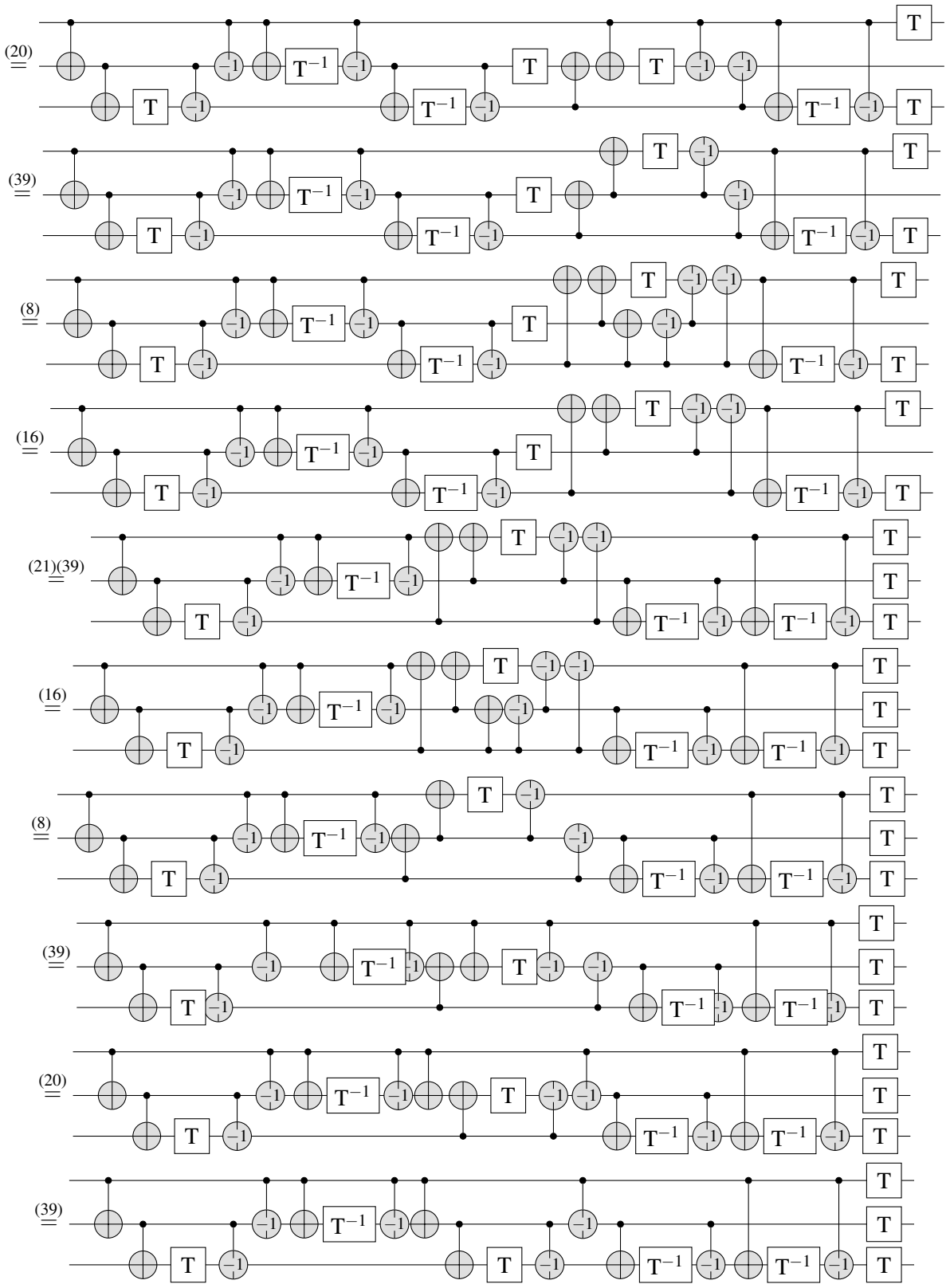
□

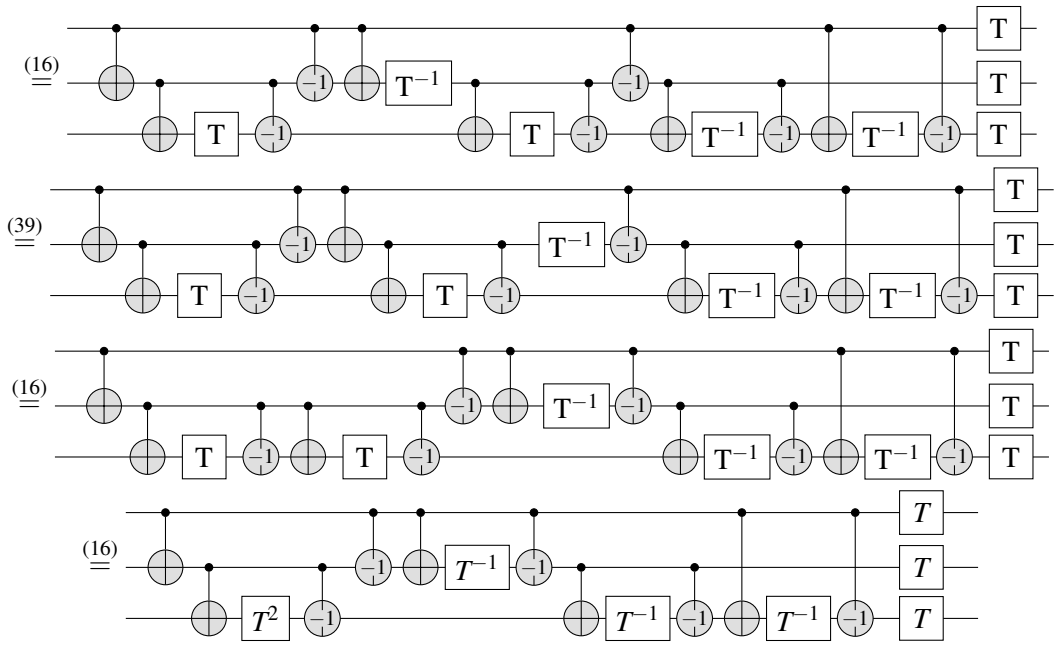
Lemma 65. *CubicPhase*$_d$ ⊢



Proof.

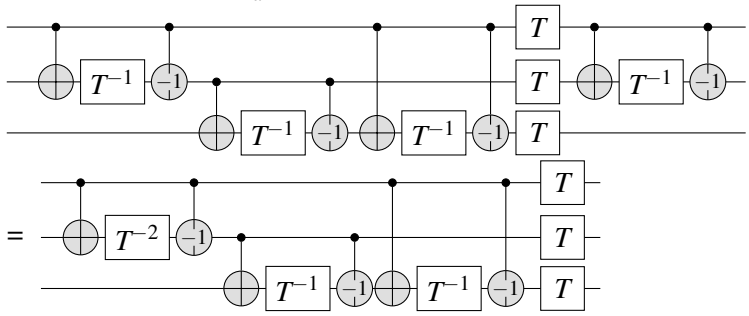



(20)
(39)
(8)
(16)
(21)(39)
(16)
(8)
(39)
(20)
(39)

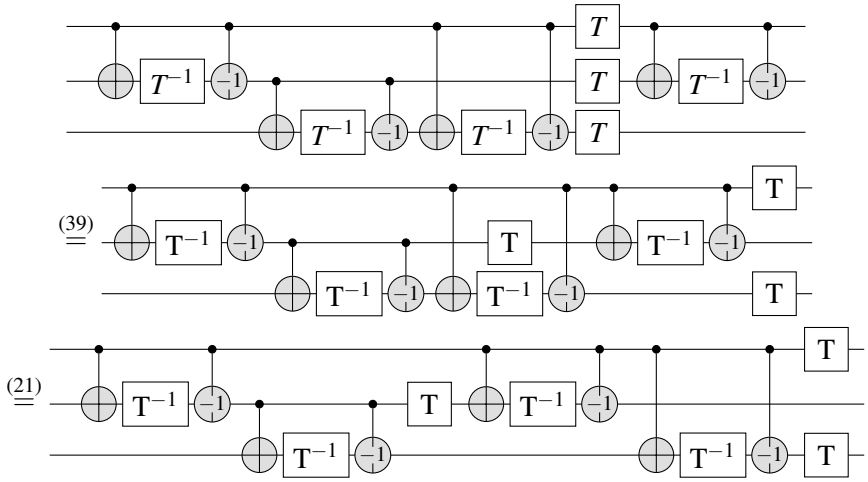


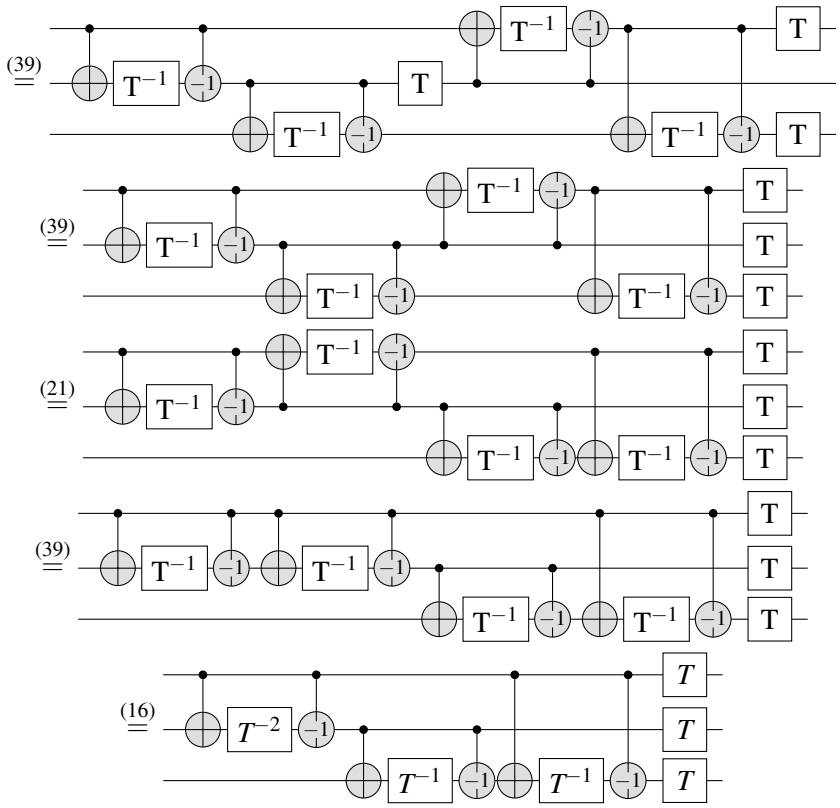
□

Lemma 66. *CubicPhase*$_d$ ⊢



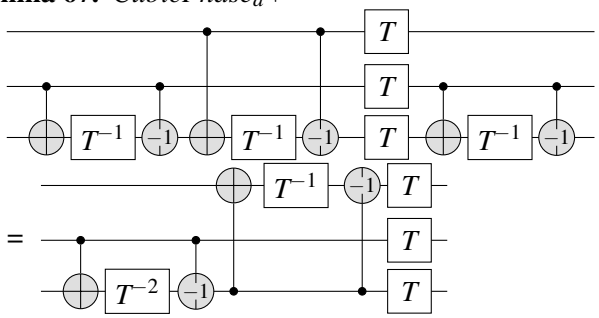
Proof.



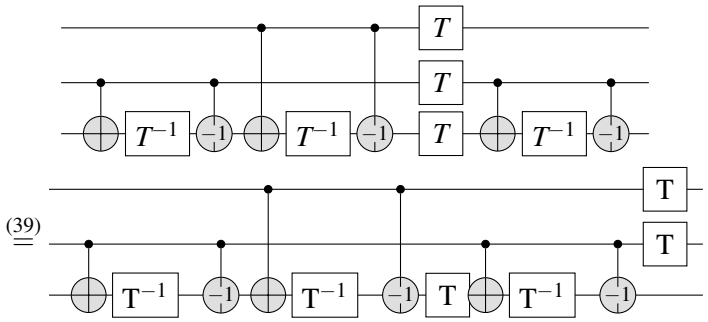


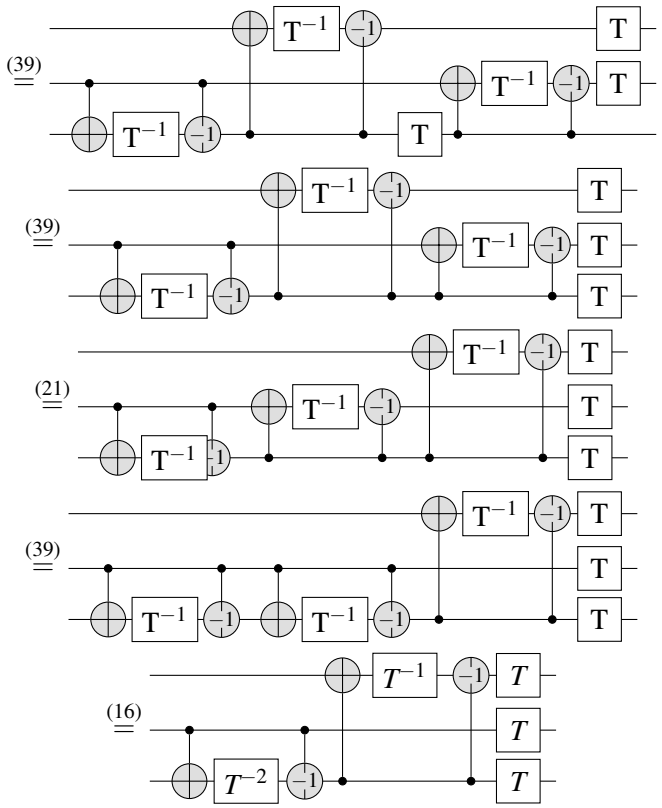
□

Lemma 67. *CubicPhase*$_d \vdash$

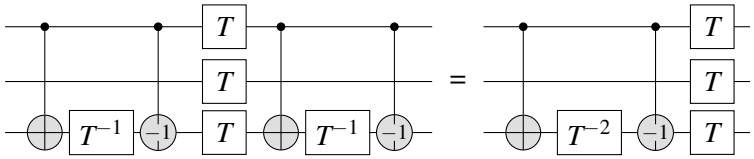


Proof.

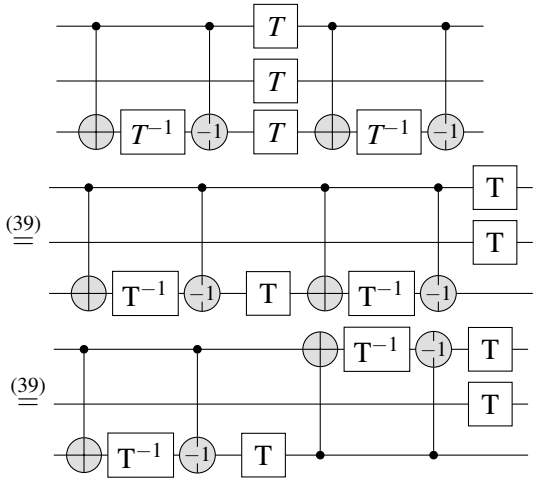


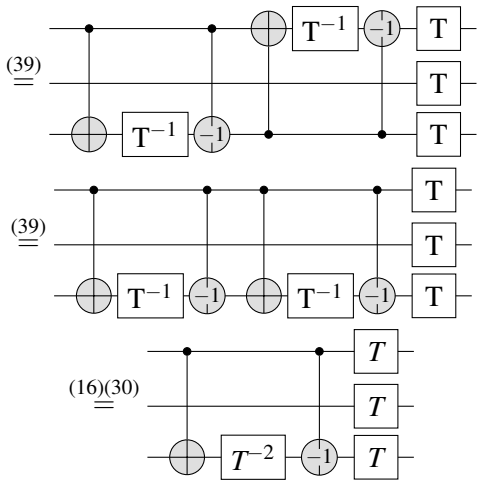


□

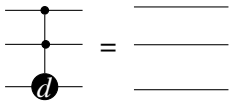
Lemma 68. *CubicPhase*$_d$ $\vdash$ 

Proof.

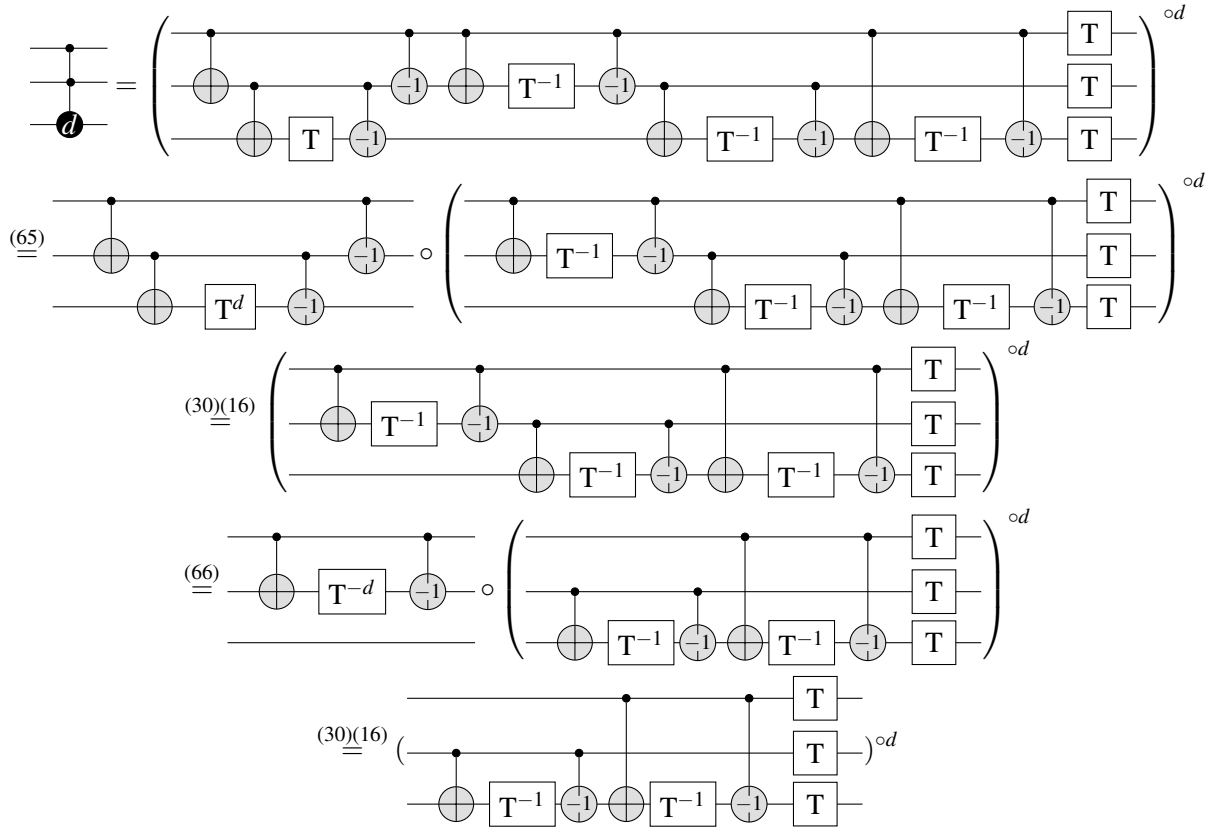


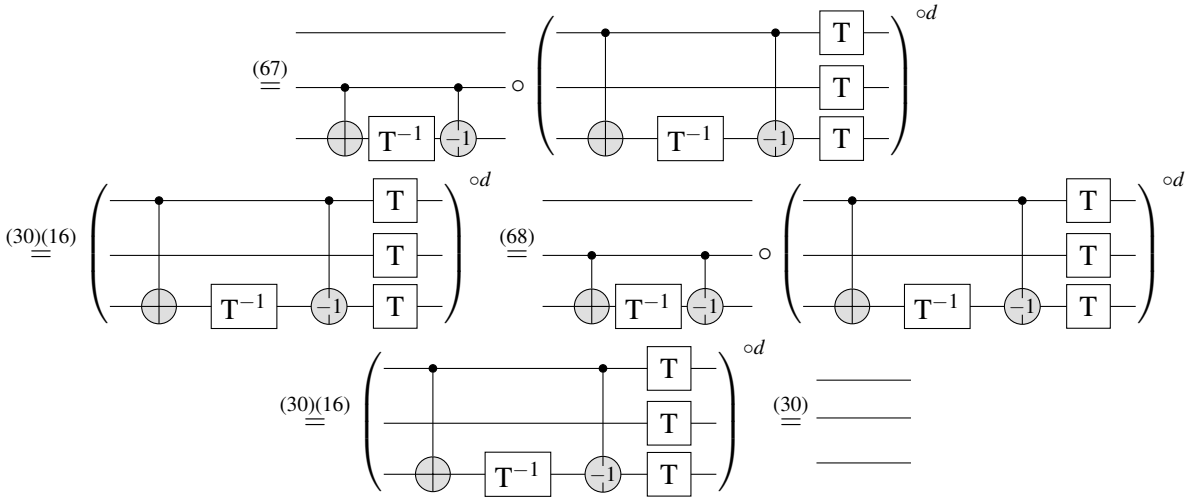


□

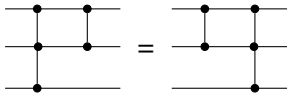
Lemma 69. *CubicPhase*$_d \vdash$ 

Proof.

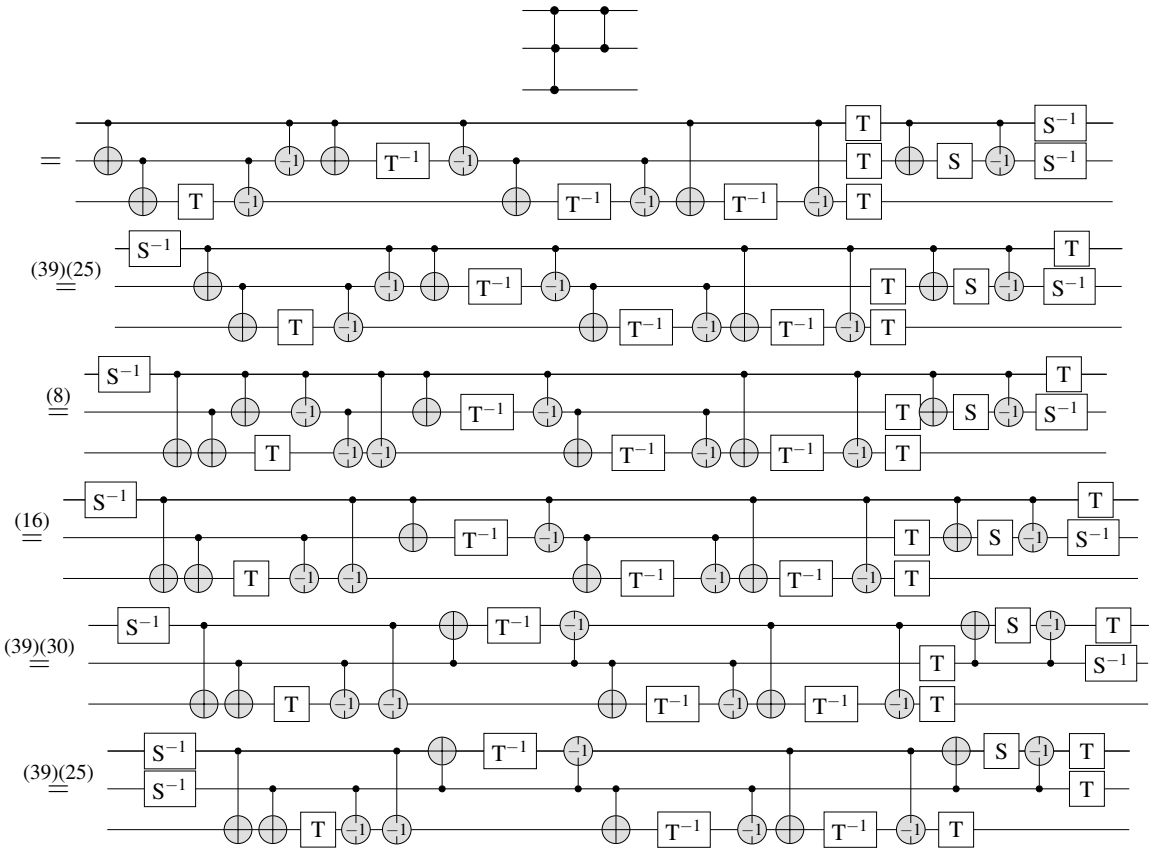


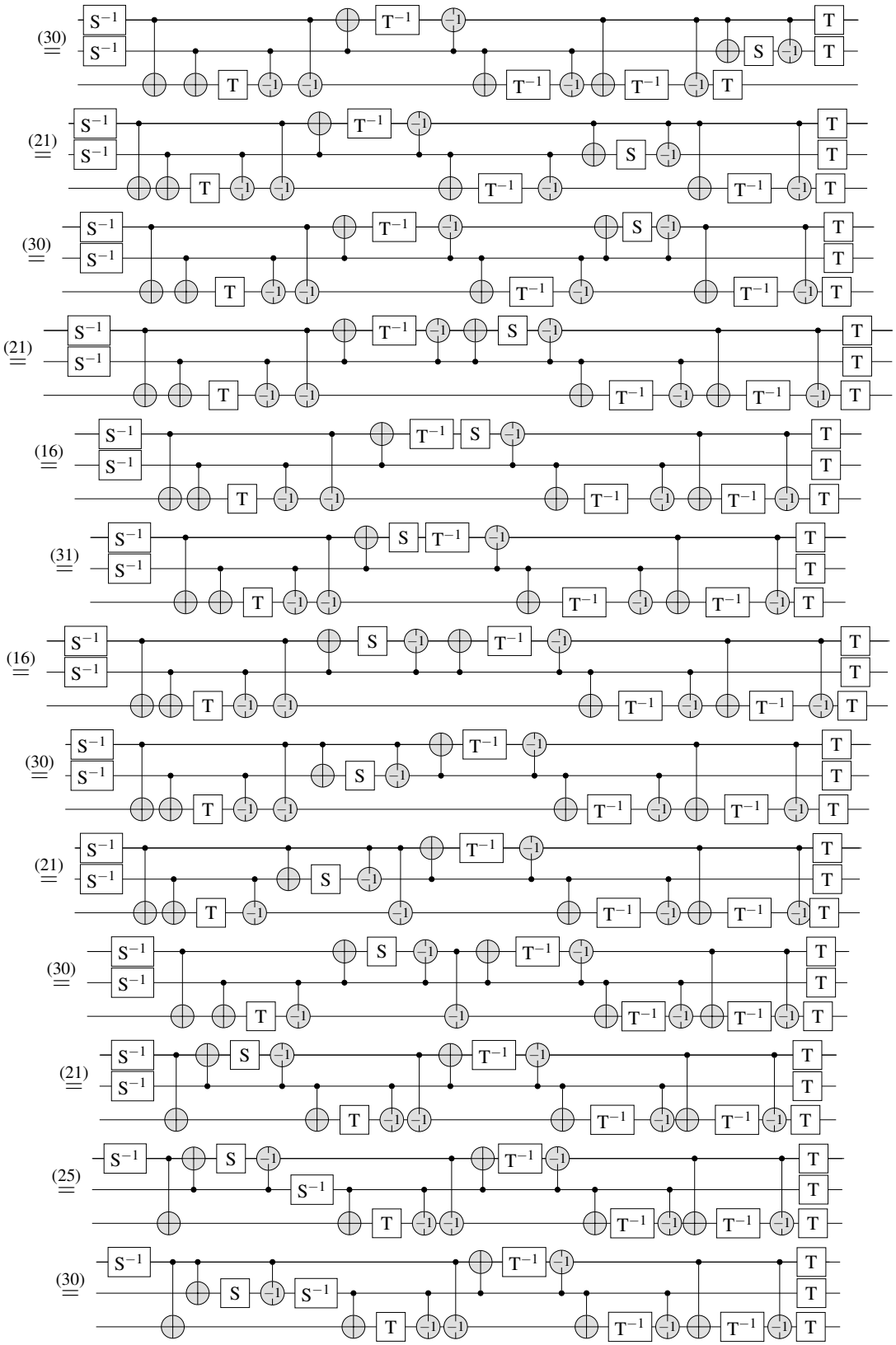


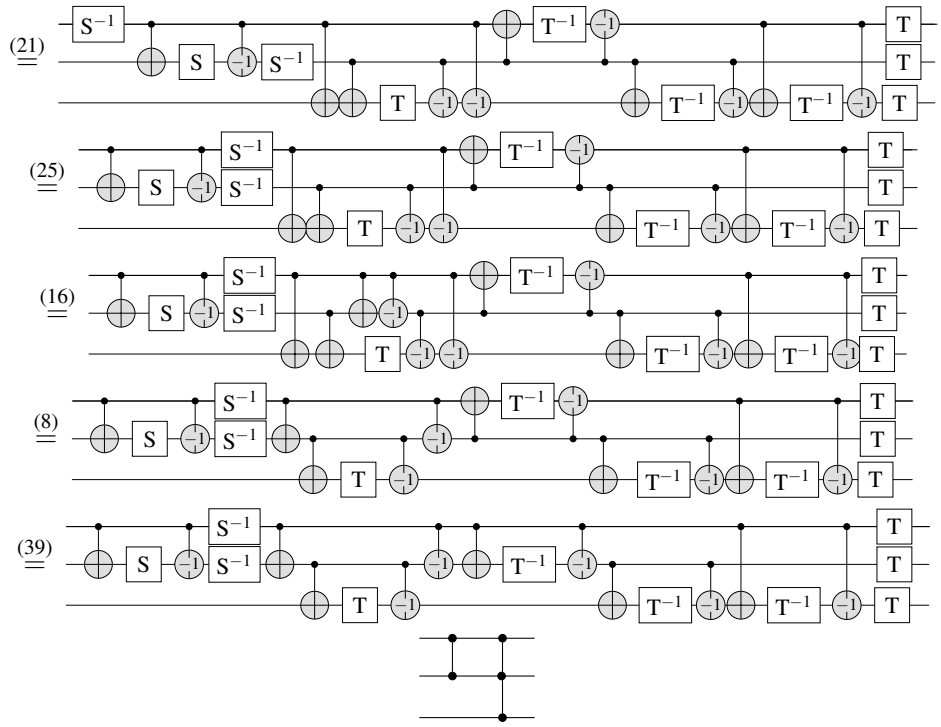
□

Lemma 70. *CubicPhase*$_d$ $\vdash$ 

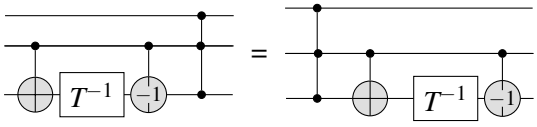
Proof.



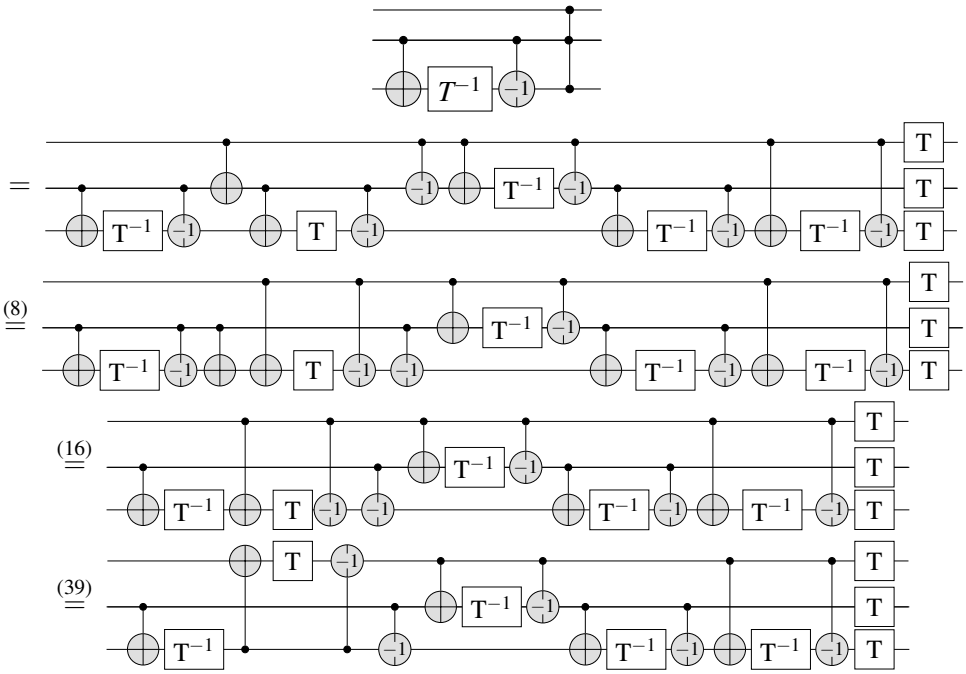

(30)
(21)
(30)
(21)
(16)
(31)
(16)
(30)
(21)
(30)
(21)
(25)
(30)

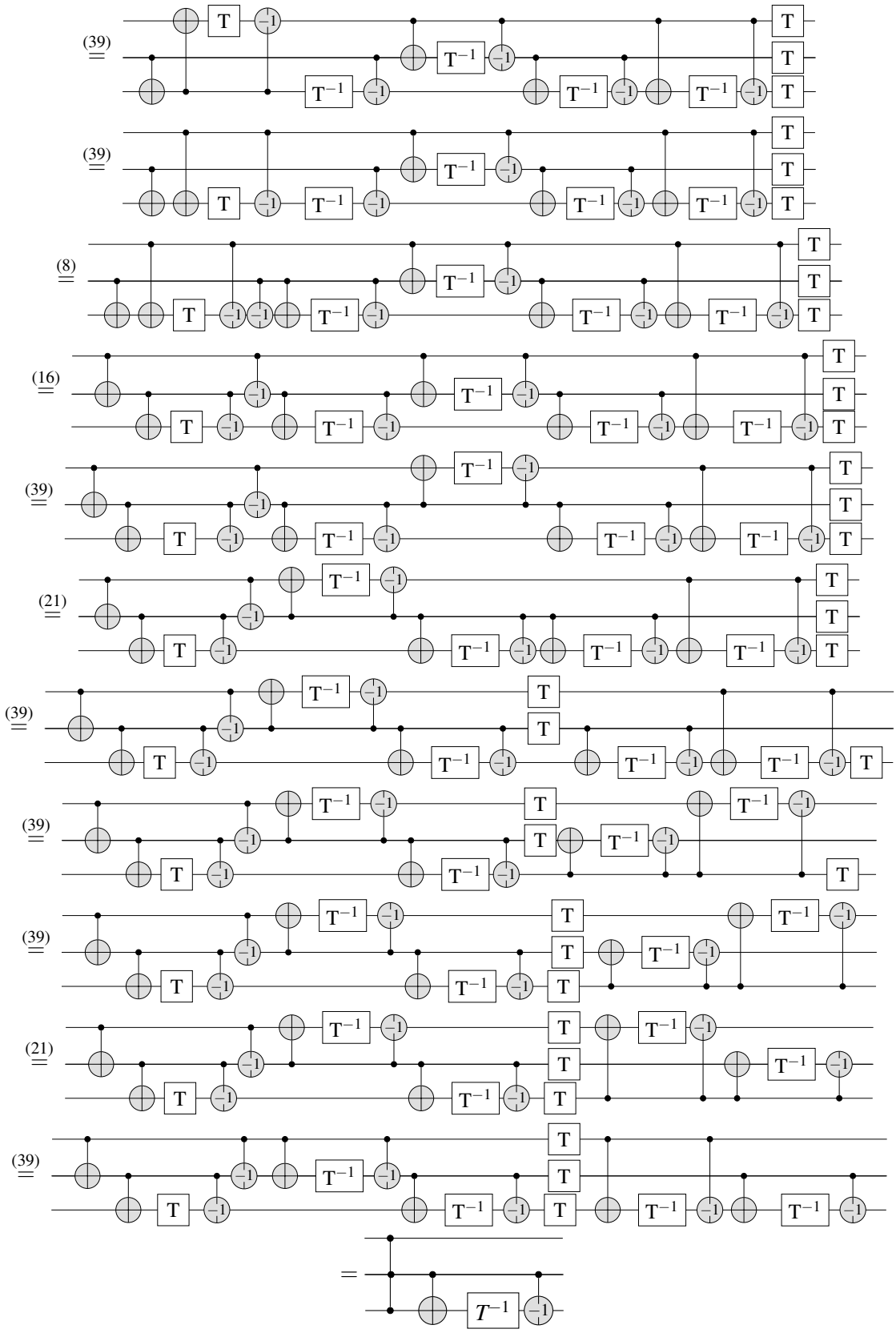


□

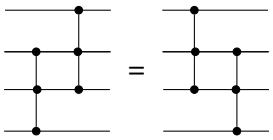
Lemma 71. *CubicPhase*$_d \vdash$ 

Proof.

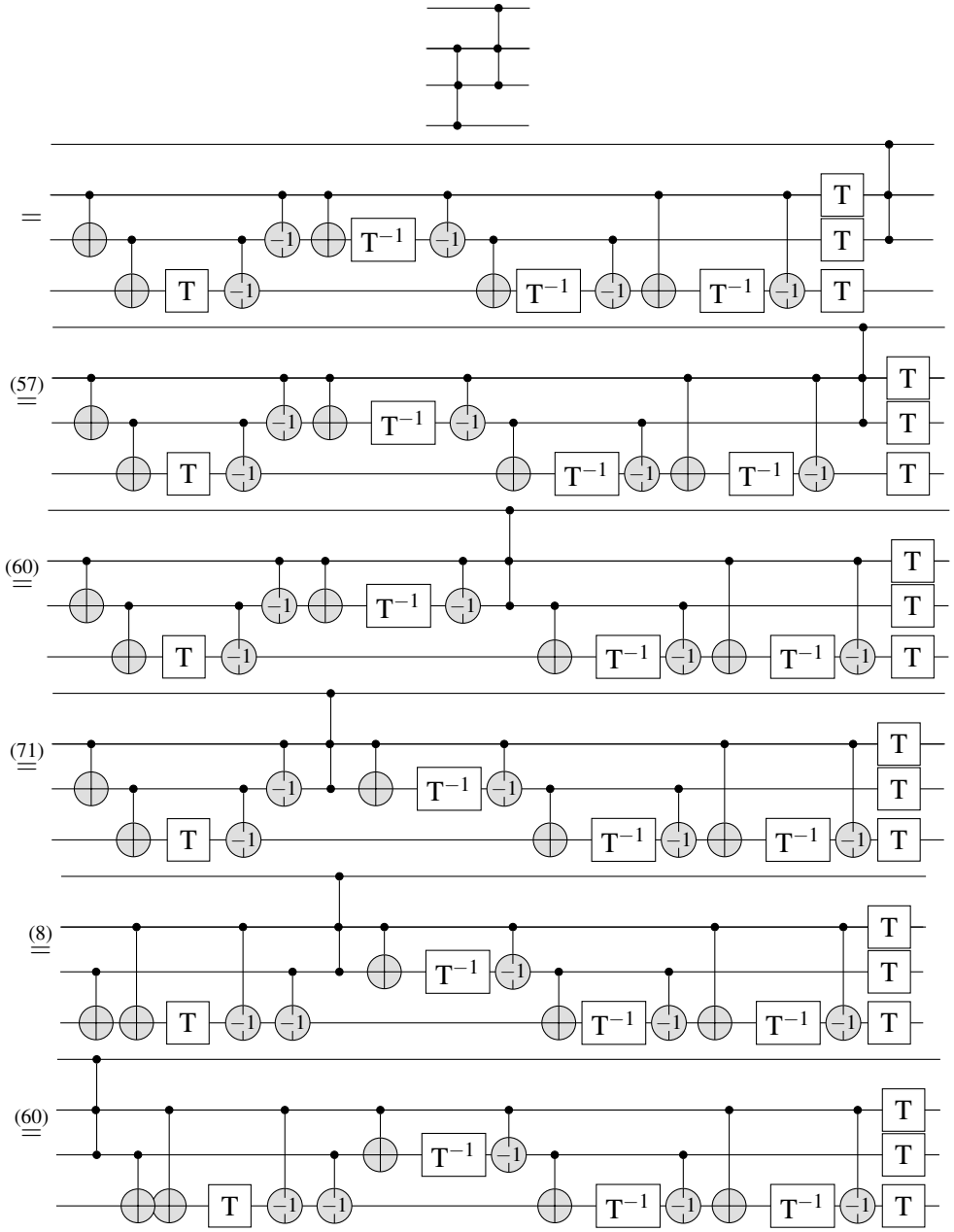


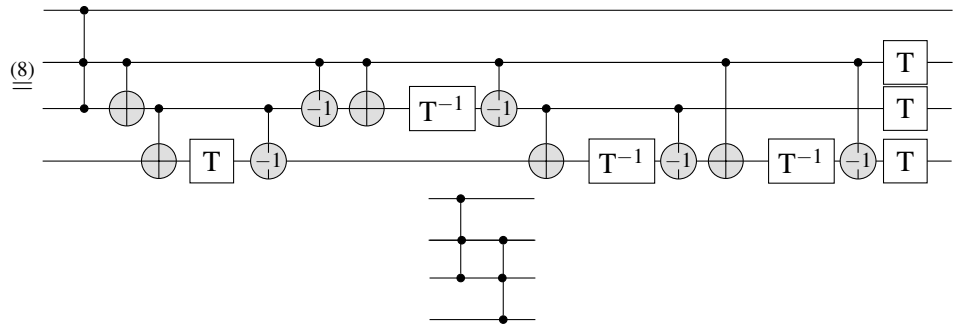

(39)
(39)
(8)
(16)
(39)
(21)
(39)
(39)
(39)
(21)
(39)
=
T^{-1}

□

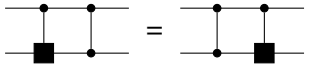
Lemma 72. *CubicPhase*$_d \vdash$  =

Proof.

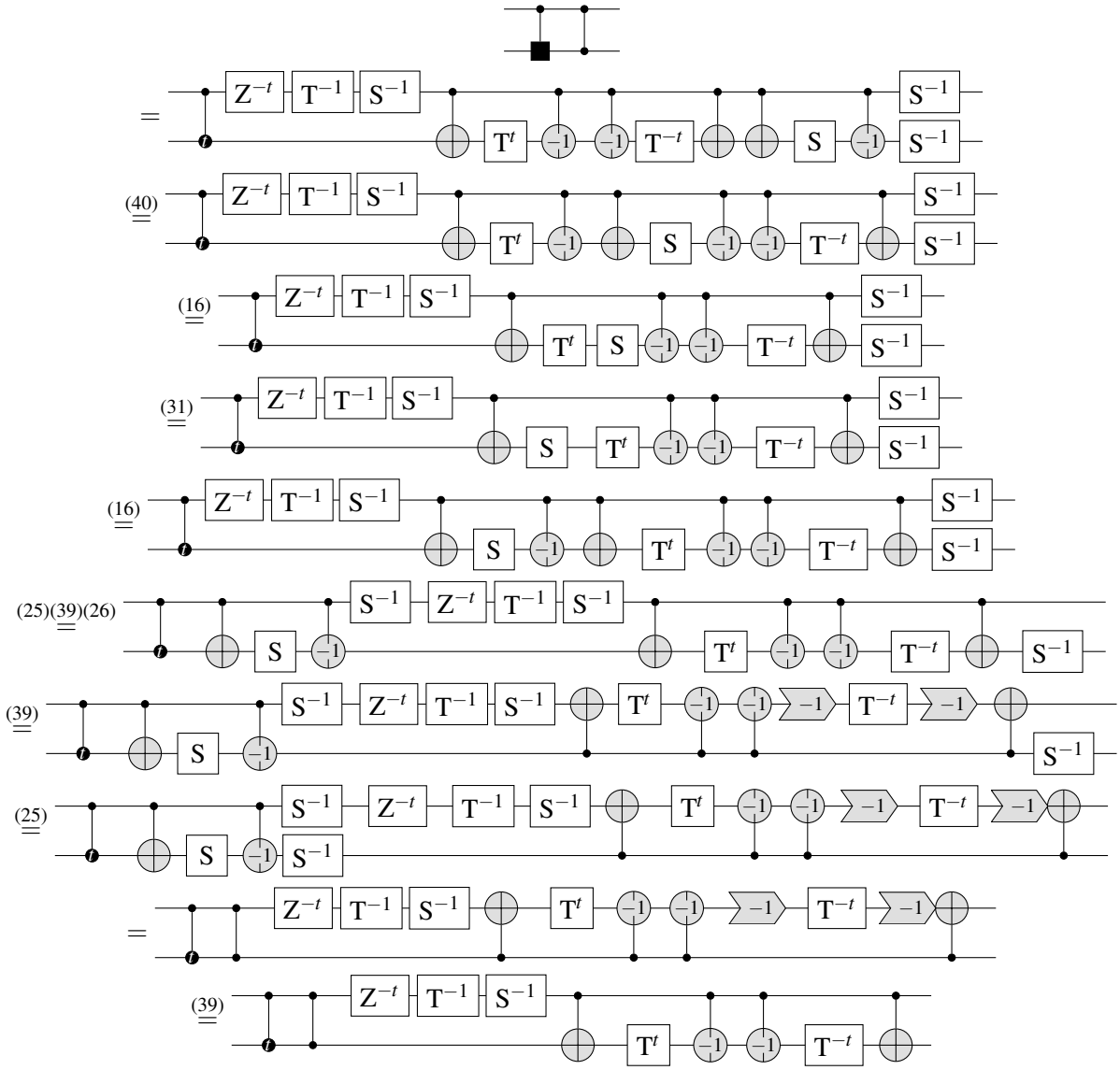


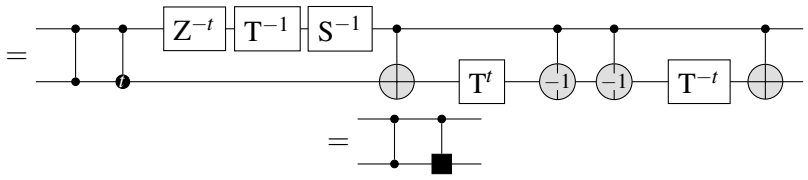


□

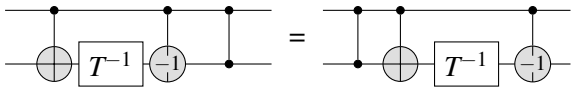
Lemma 73. *CubicPhase*$_d \vdash$ 

Proof.

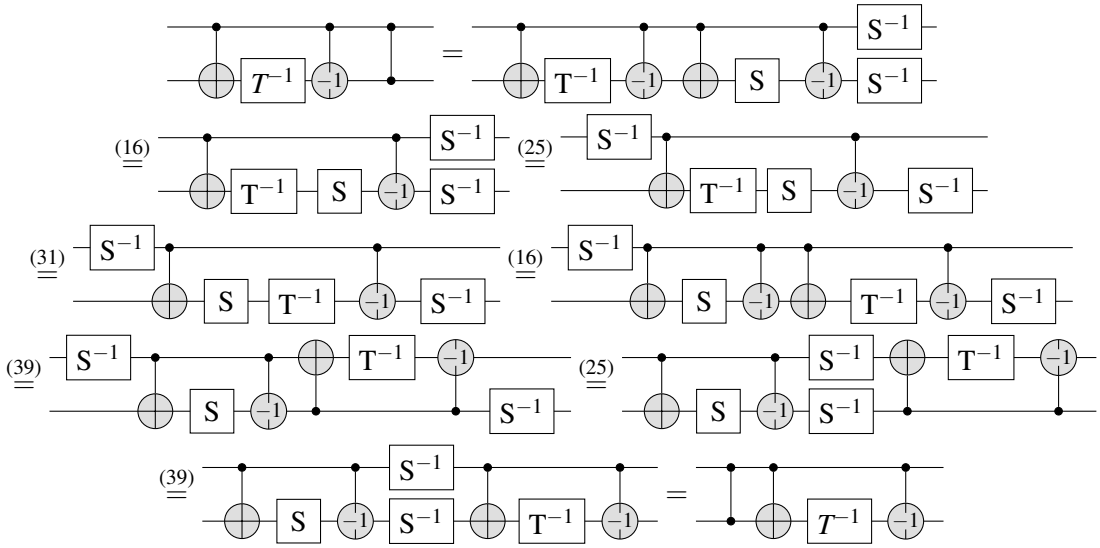




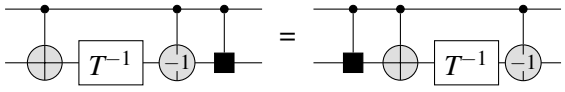
□

Lemma 74. *CubicPhase*$_d \vdash$ 

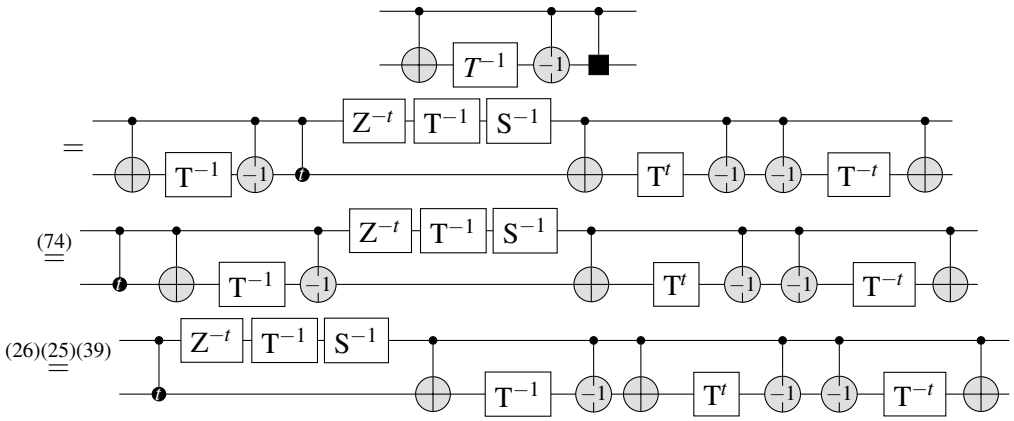
Proof.

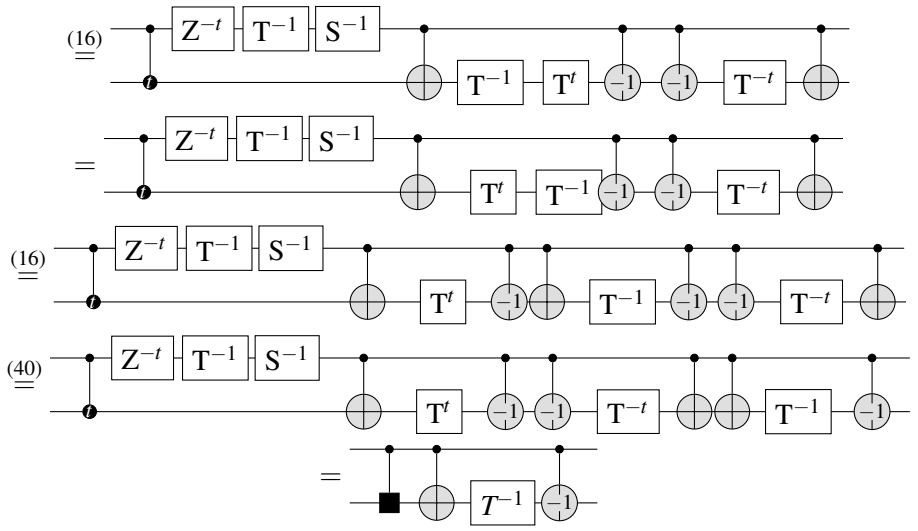


□

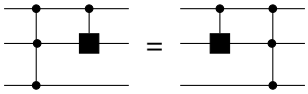
Lemma 75. *CubicPhase*$_d \vdash$ 

Proof.

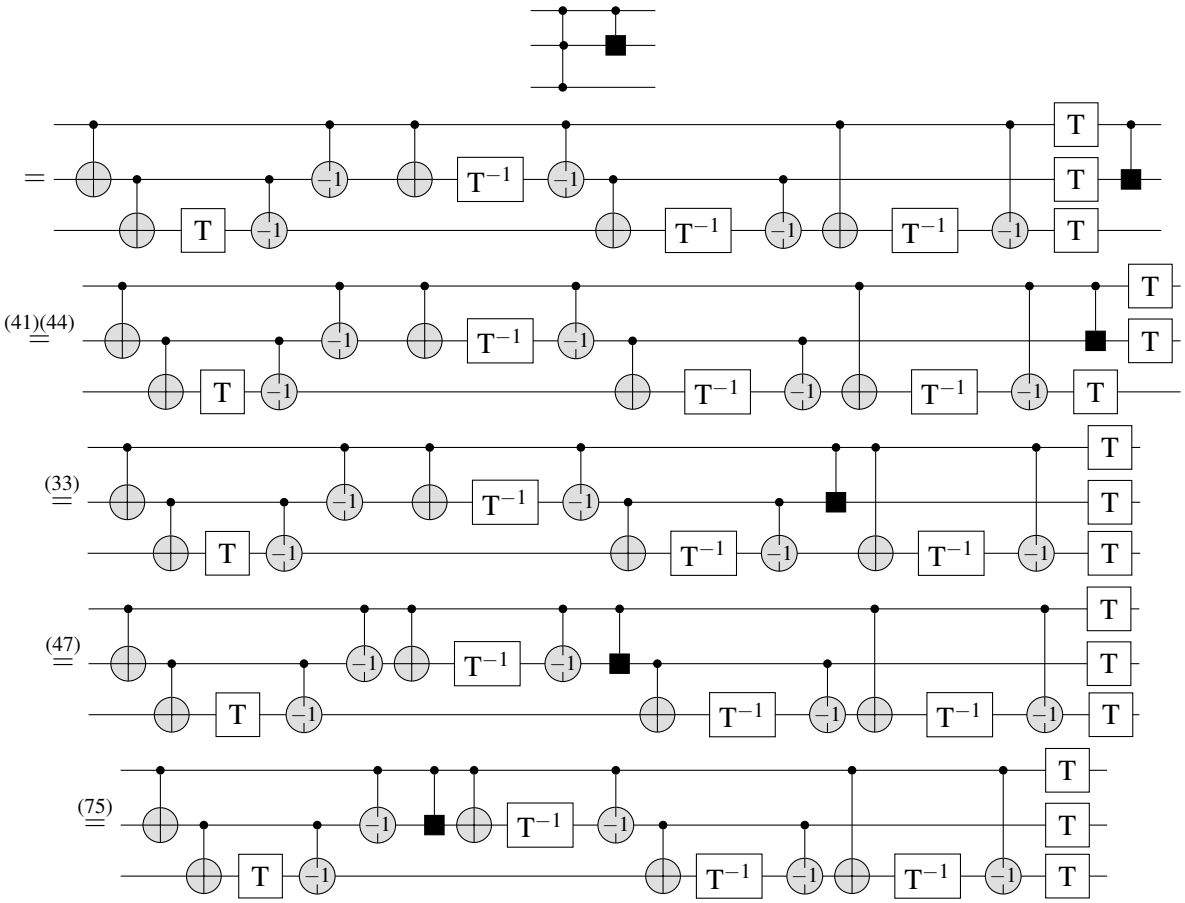


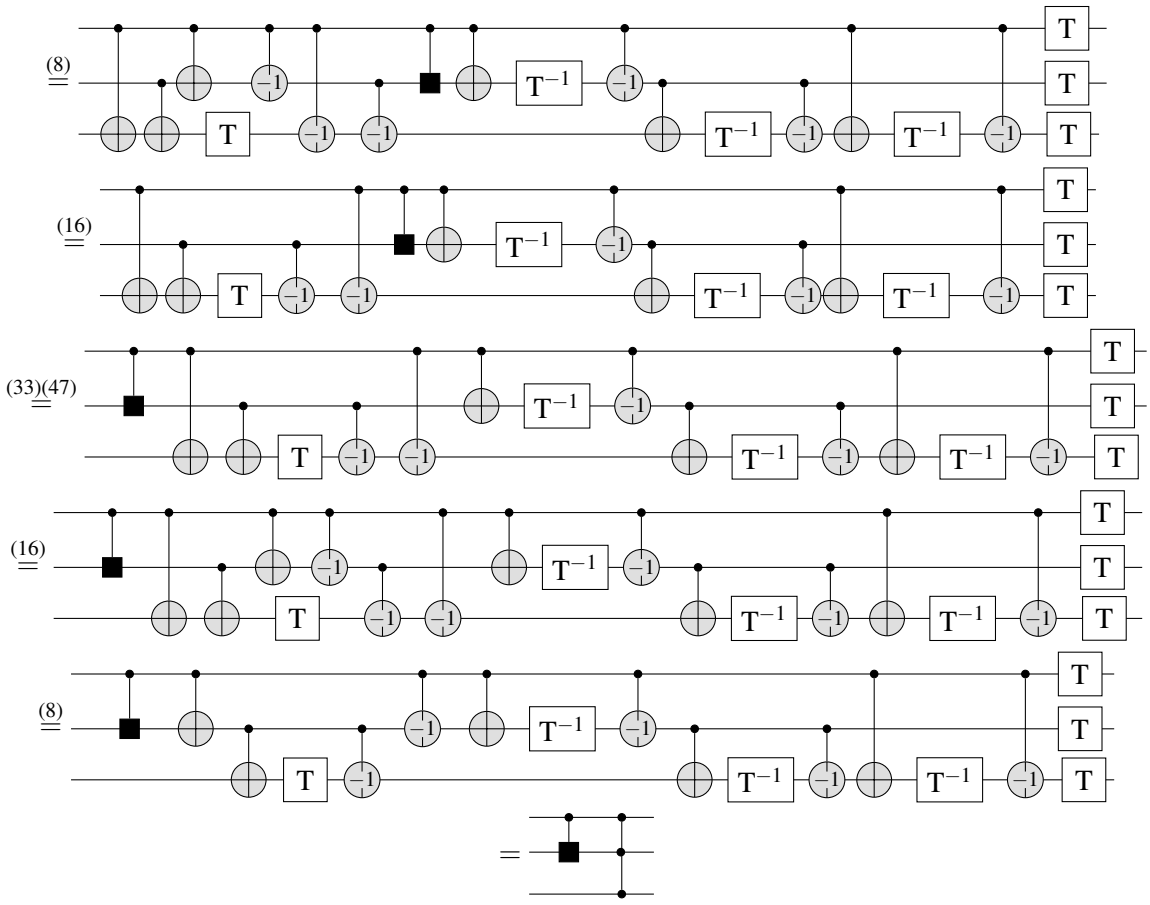


□

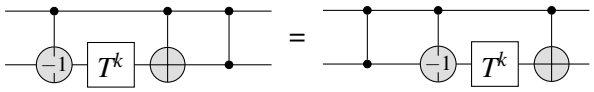
Lemma 76. *CubicPhase*$_d \vdash$ 

Proof.

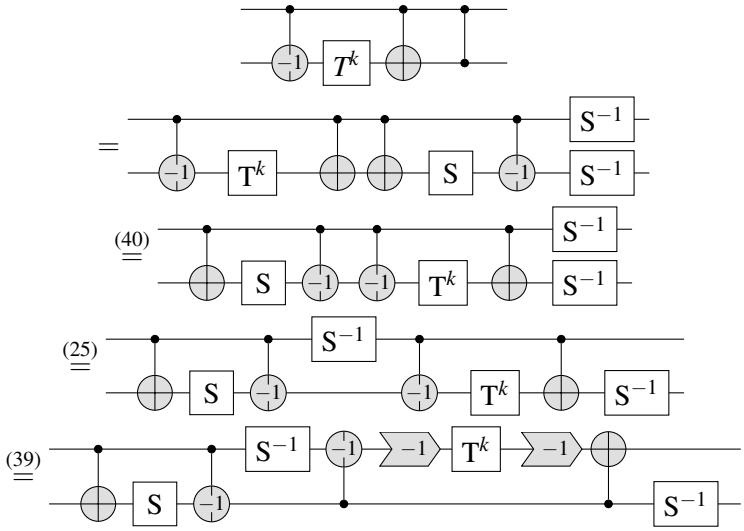


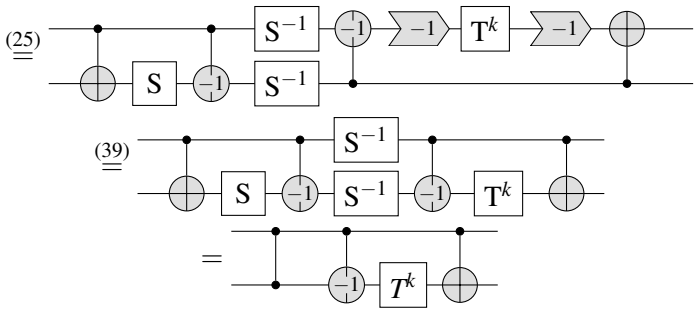


□

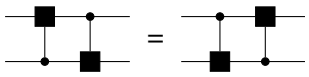
Lemma 77. *CubicPhase*$_d$ $\vdash$ 

Proof.

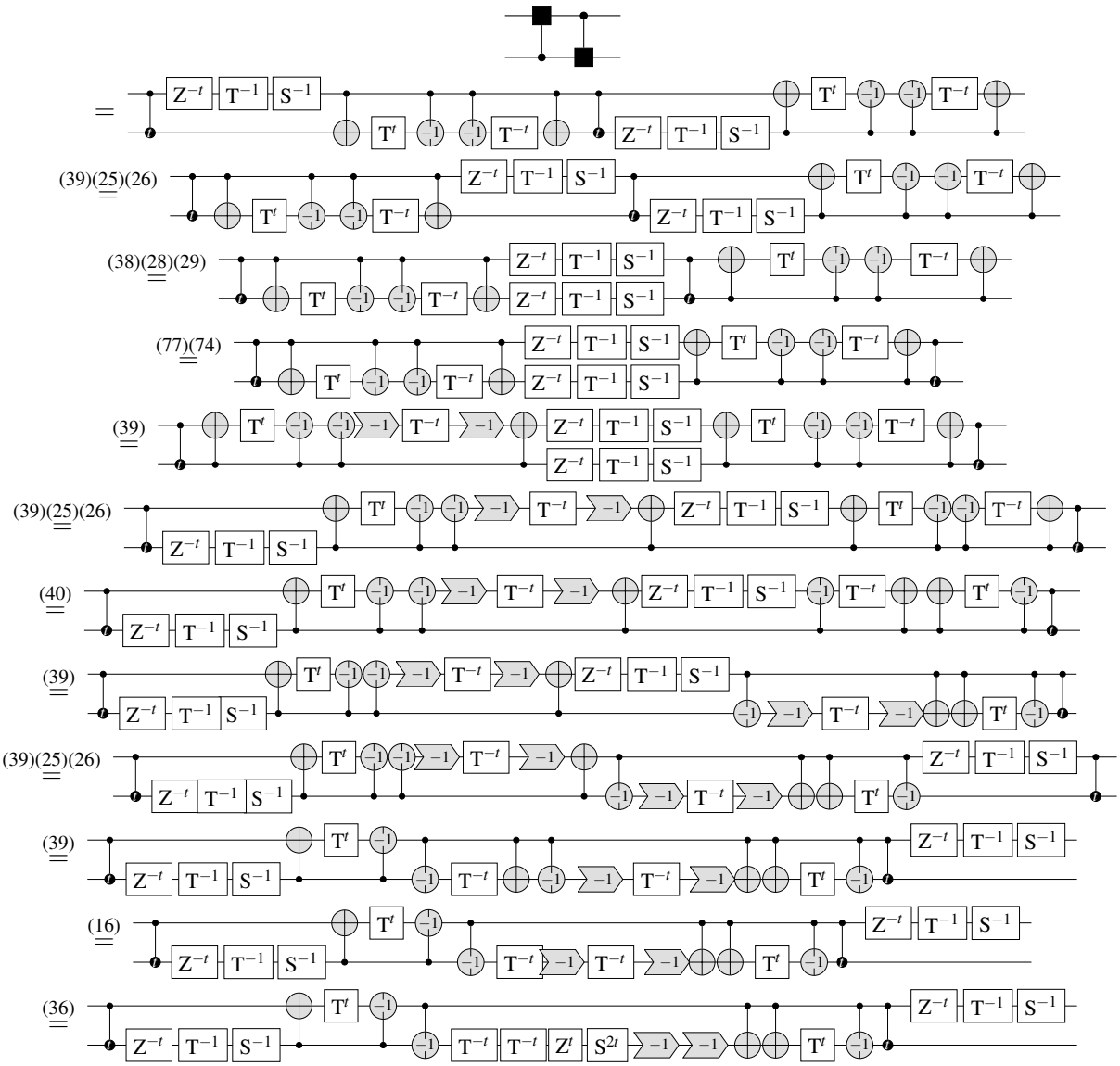


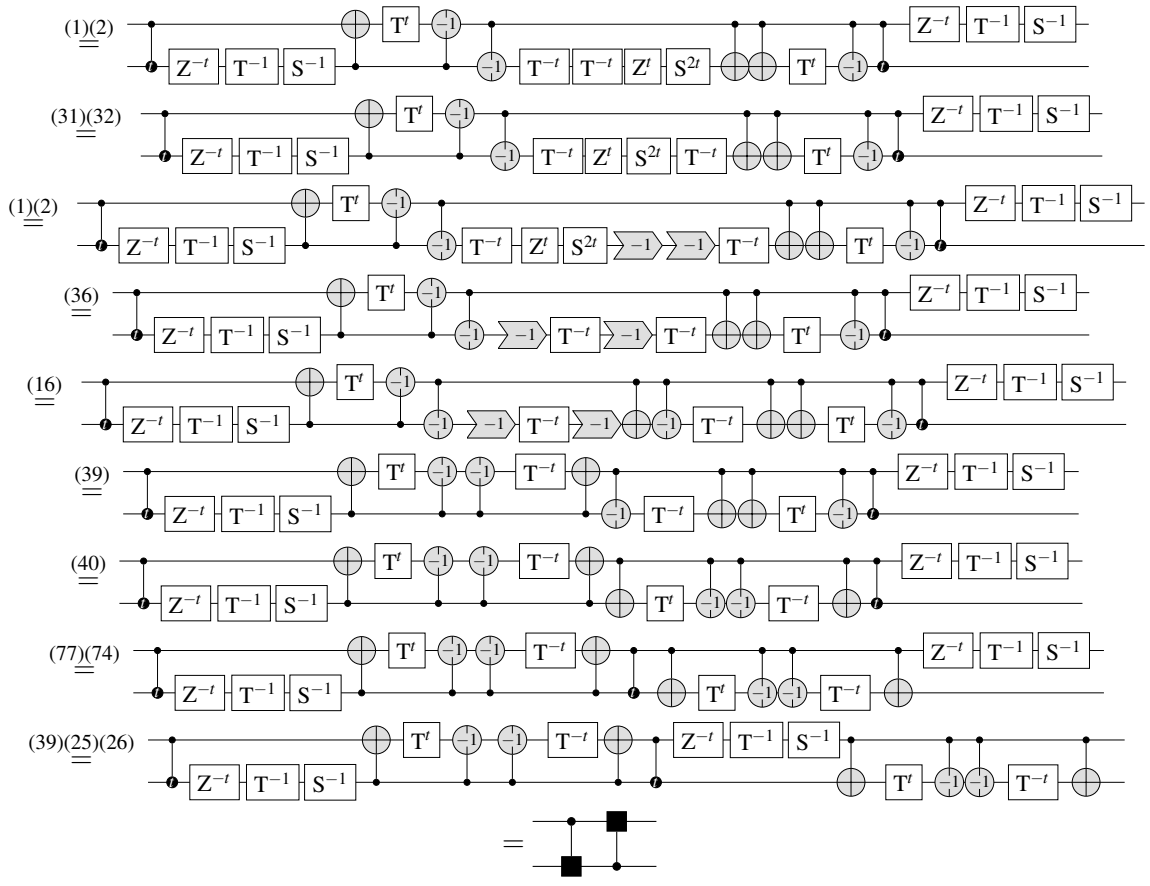


□

Lemma 78. *CubicPhase*$_d \vdash$ 

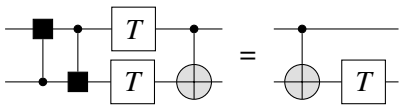
Proof.



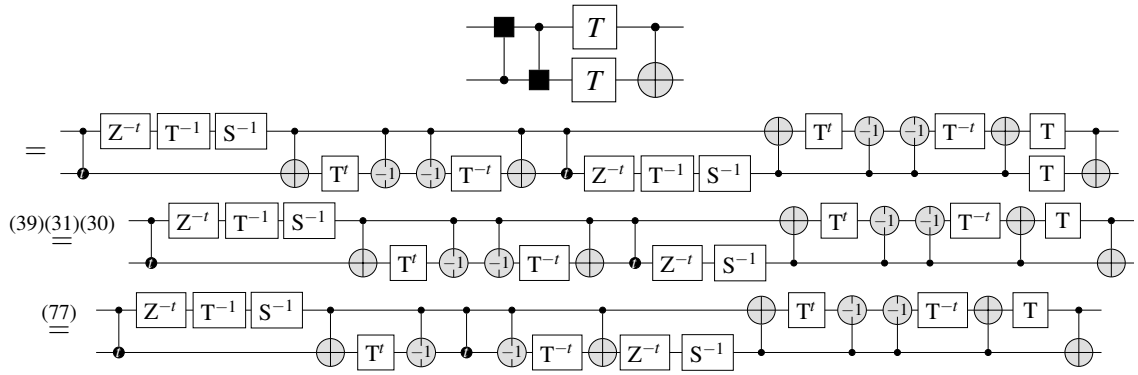


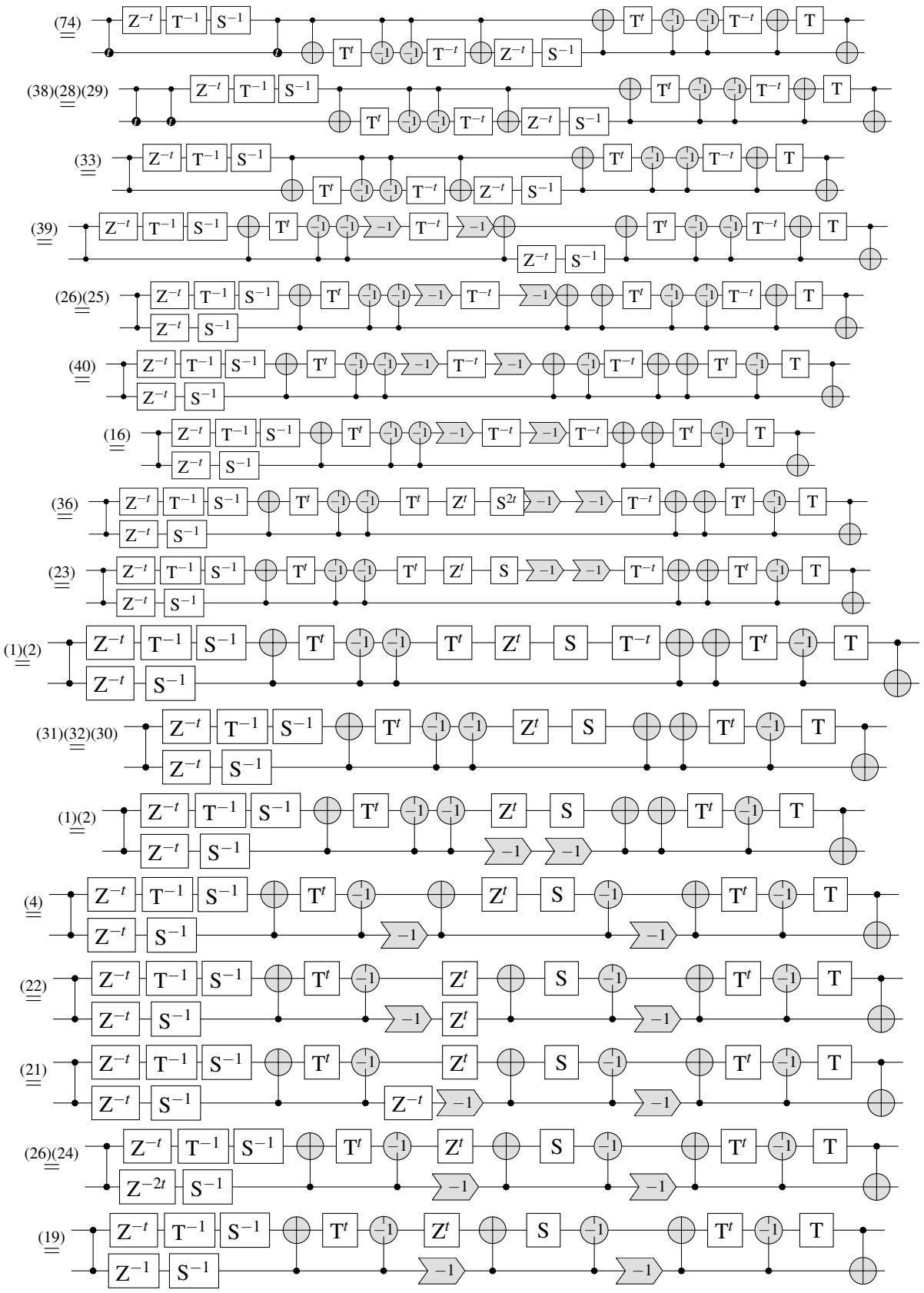
□

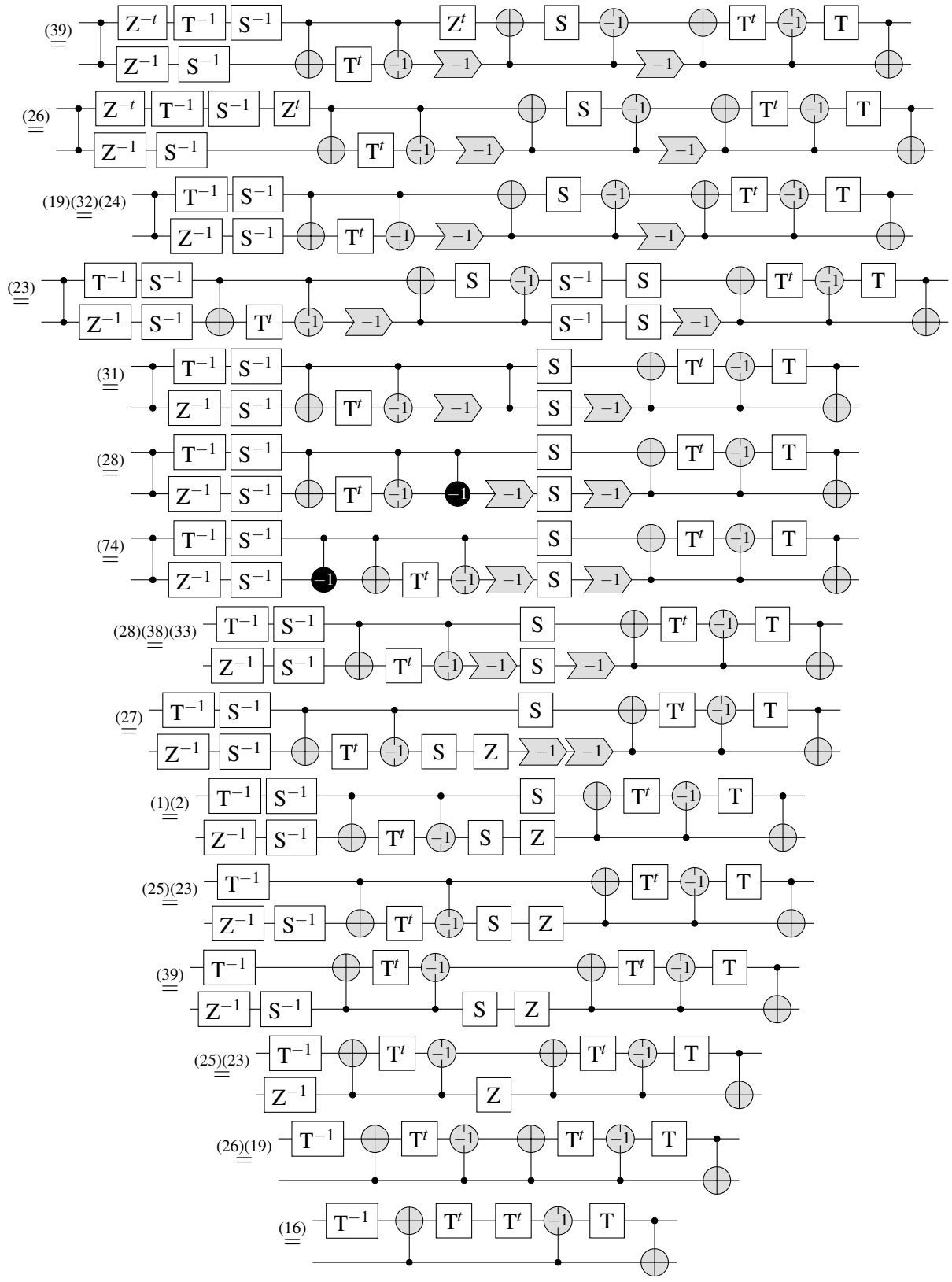
We have established all commutation relations between the diagonal generators recorded in Table 1. In the remainder of this appendix, we use these relations, together with their images under wire permutations and with disjoint-support instances given by the PROP laws, as admissible rewriting steps to reorder diagonal subcircuits without further mention.

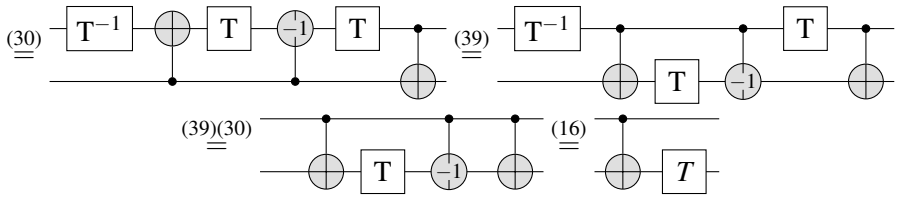
Lemma 79. *CubicPhase*$_d \vdash$ 

Proof.

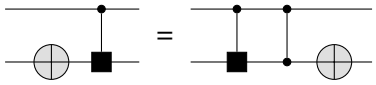



(74)
(38)(28)(29)
(33)
(39)
(26)(25)
(40)
(16)
(36)
(23)
(1)(2)
(31)(32)(30)
(1)(2)
(4)
(22)
(21)
(26)(24)
(19)

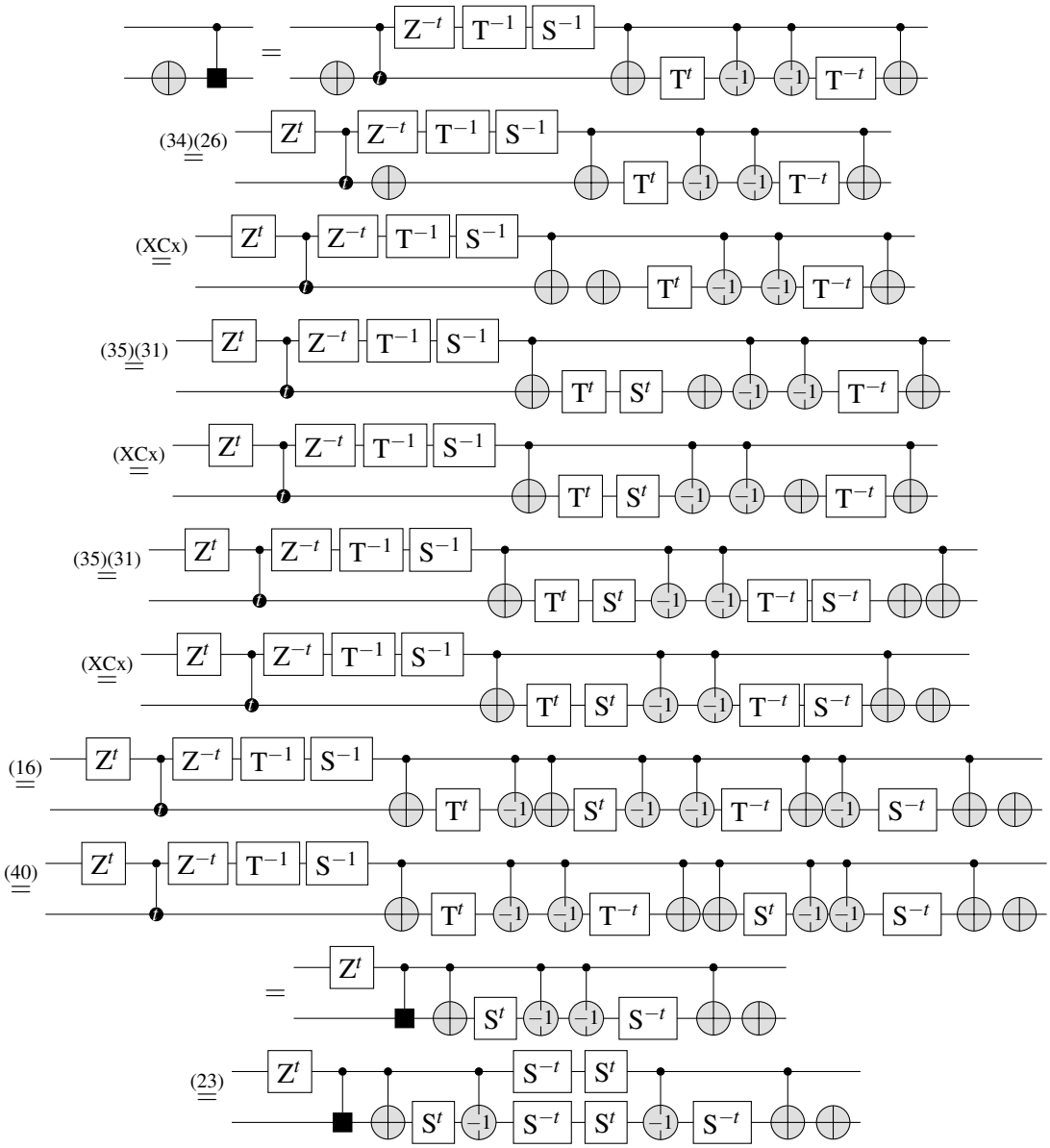

(39)
(26)
(19)(32)(24)
(23)
(31)
(28)
(74)
(28)(38)(33)
(27)
(1)(2)
(25)(23)
(39)
(25)(23)
(26)(19)
(16)

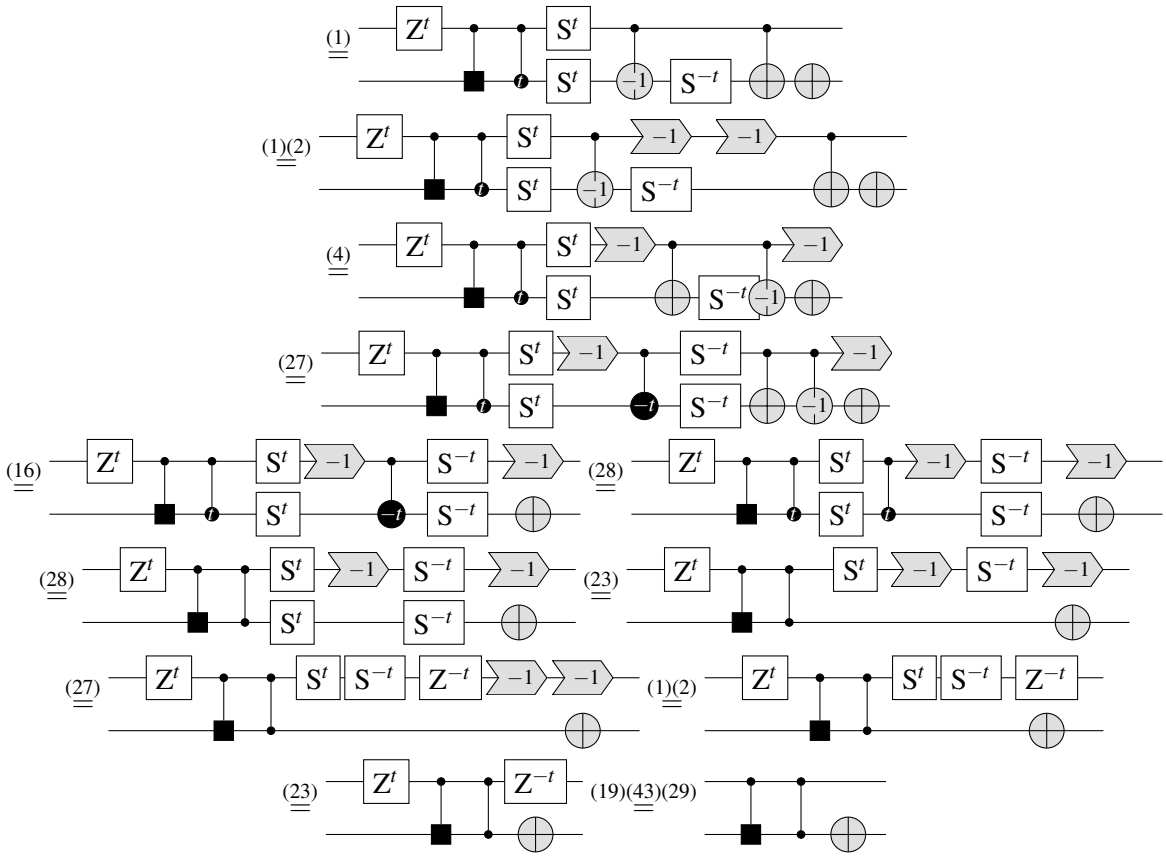


□

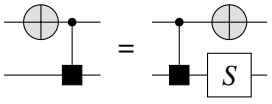
Lemma 80. *CubicPhase*$_d \vdash$ 

Proof.

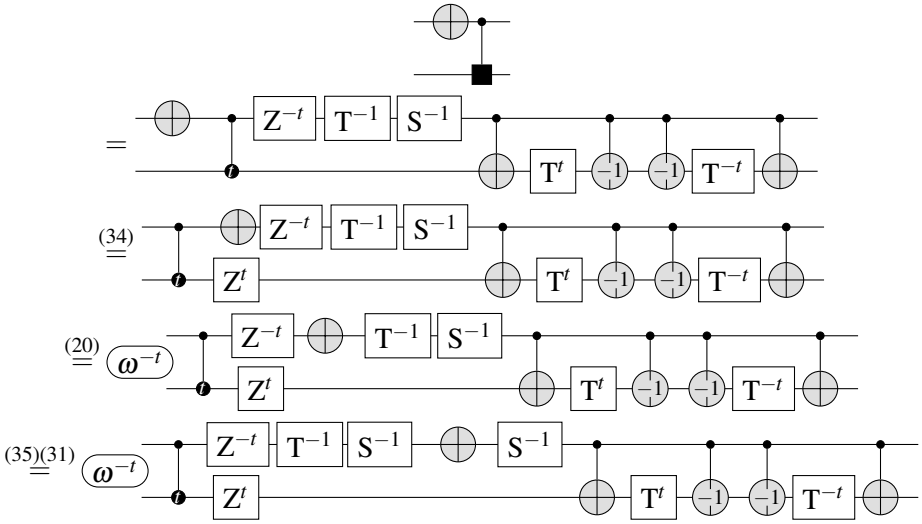


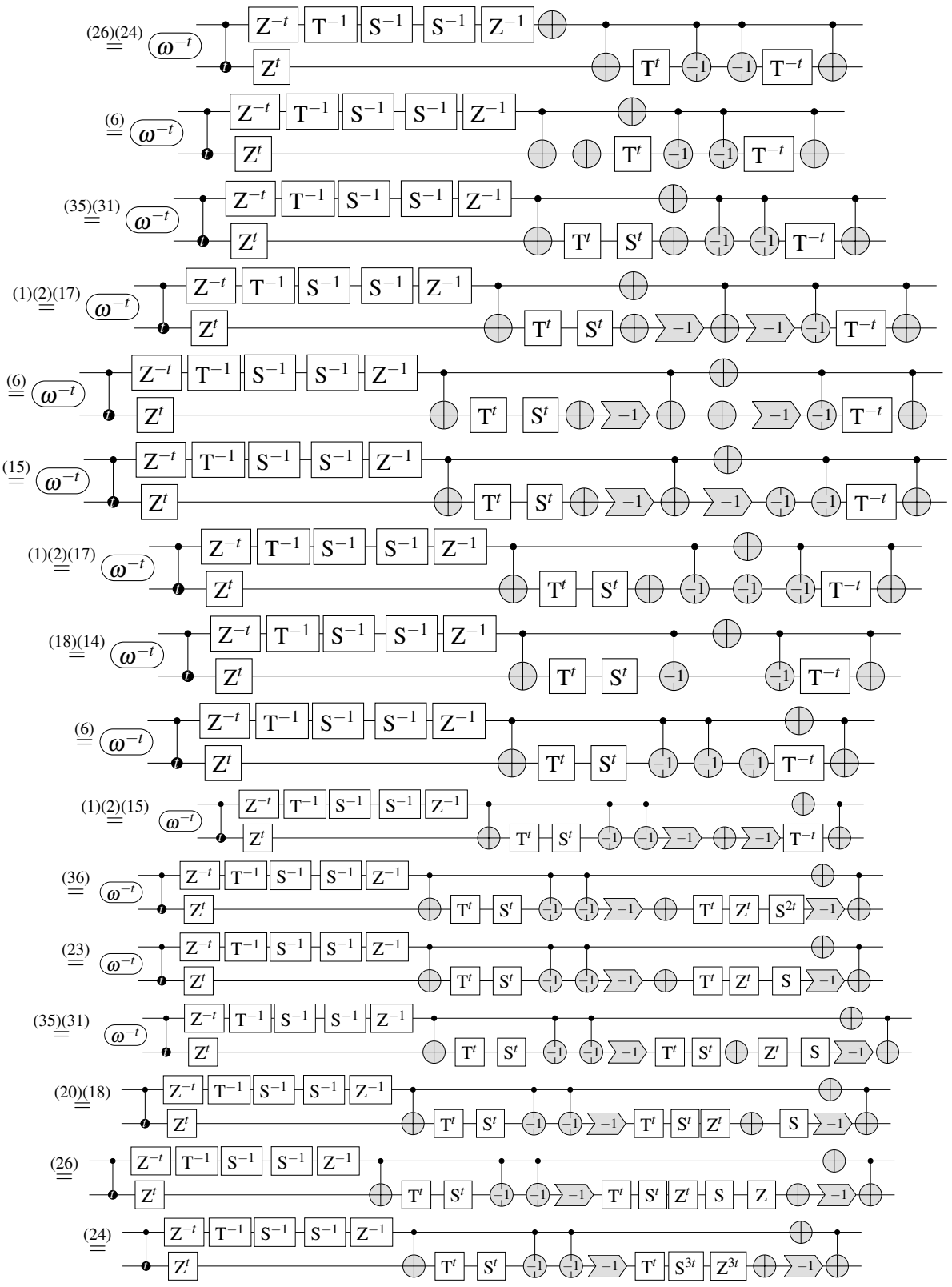


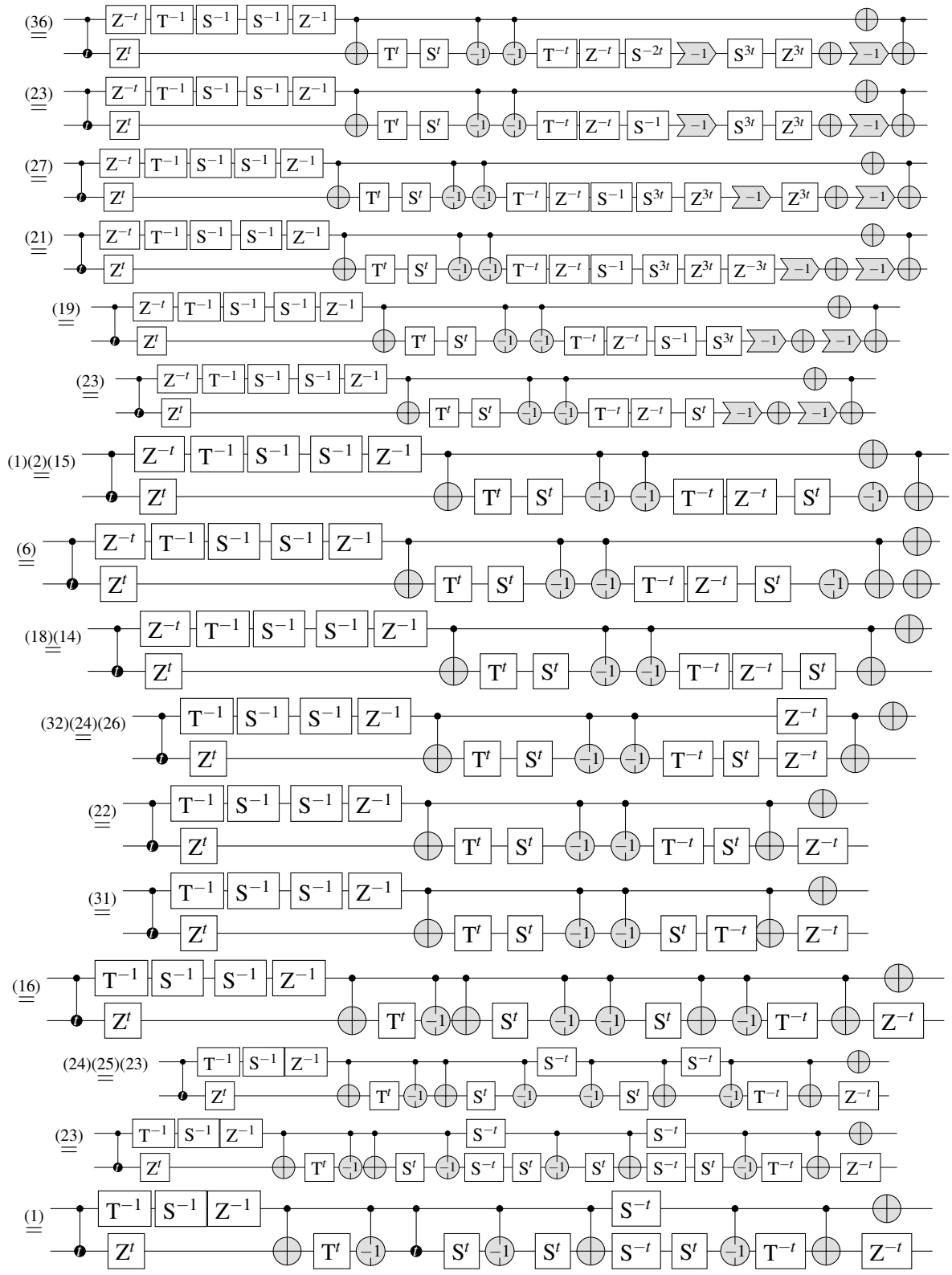
□

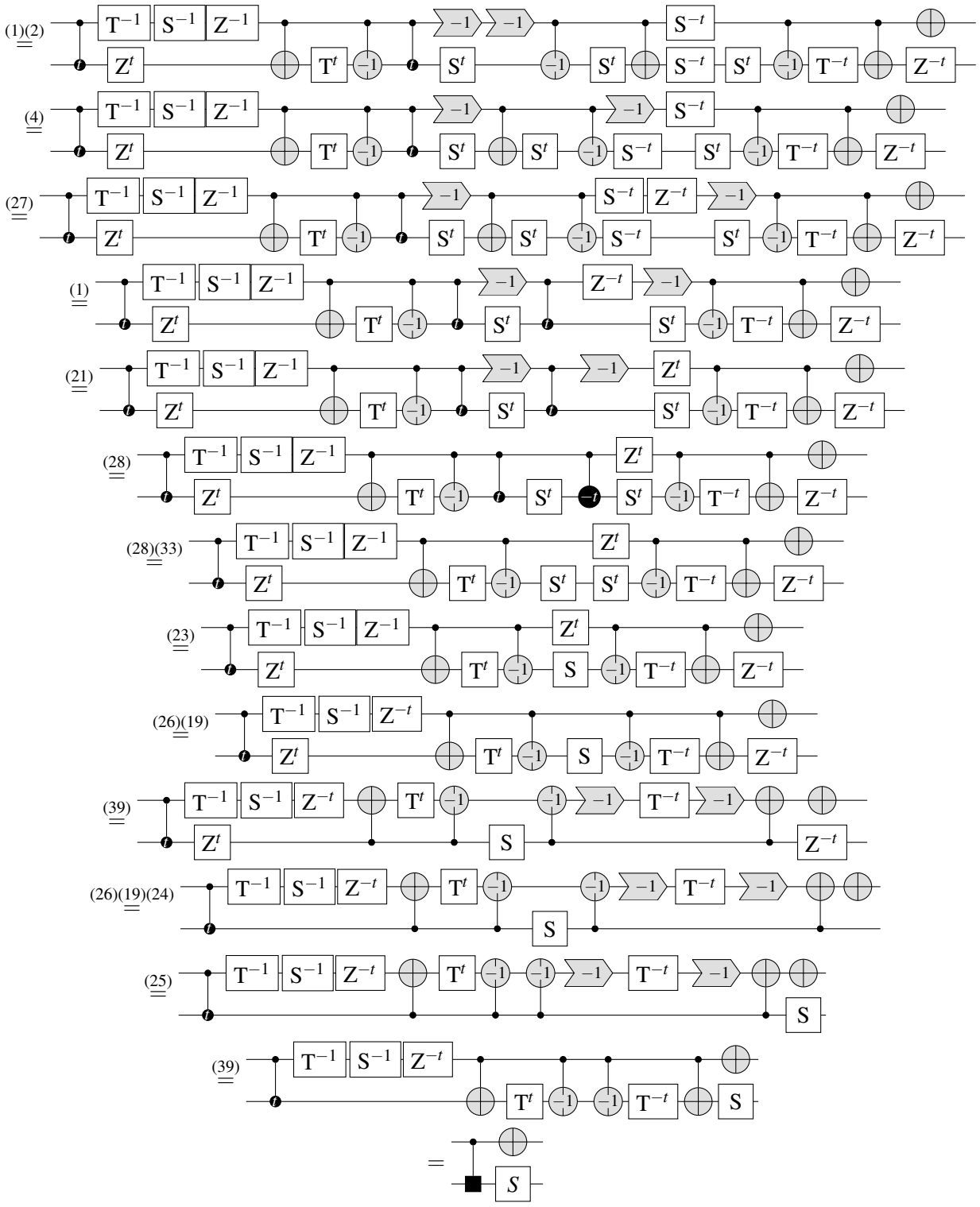
Lemma 81. *CubicPhase*$_d \vdash$ 

Proof.

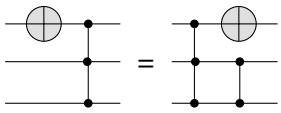



(26)(24)
(6)
(35)(31)
(1)(2)(17)
(6)
(15)
(1)(2)(17)
(18)(14)
(6)
(1)(2)(15)
(36)
(23)
(35)(31)
(20)(18)
(26)
(24)

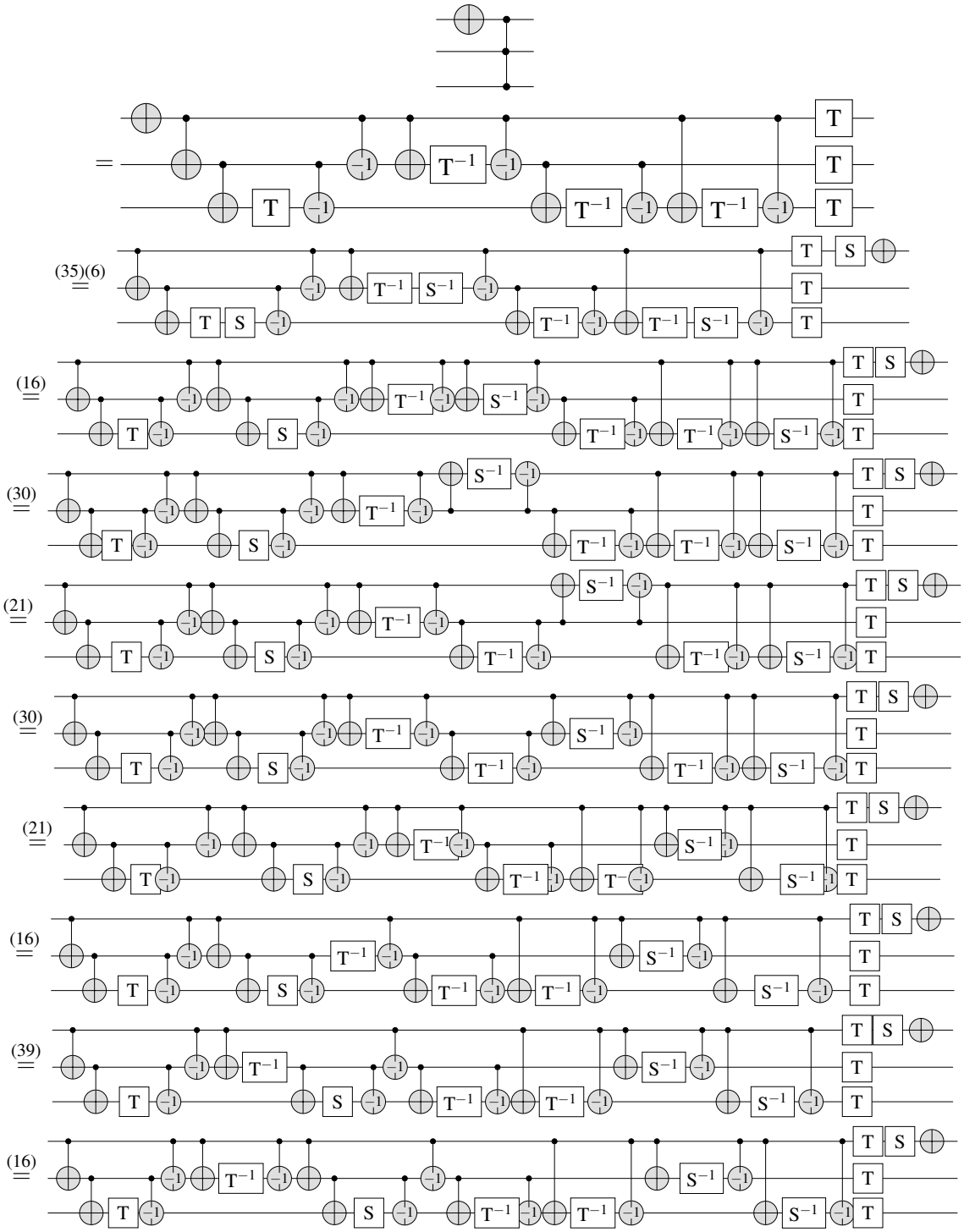

(36)
(23)
(27)
(21)
(19)
(23)
(1)(2)(15)
(6)
(18)(14)
(32)(24)(26)
(22)
(31)
(16)
(24)(25)(23)
(23)
(1)

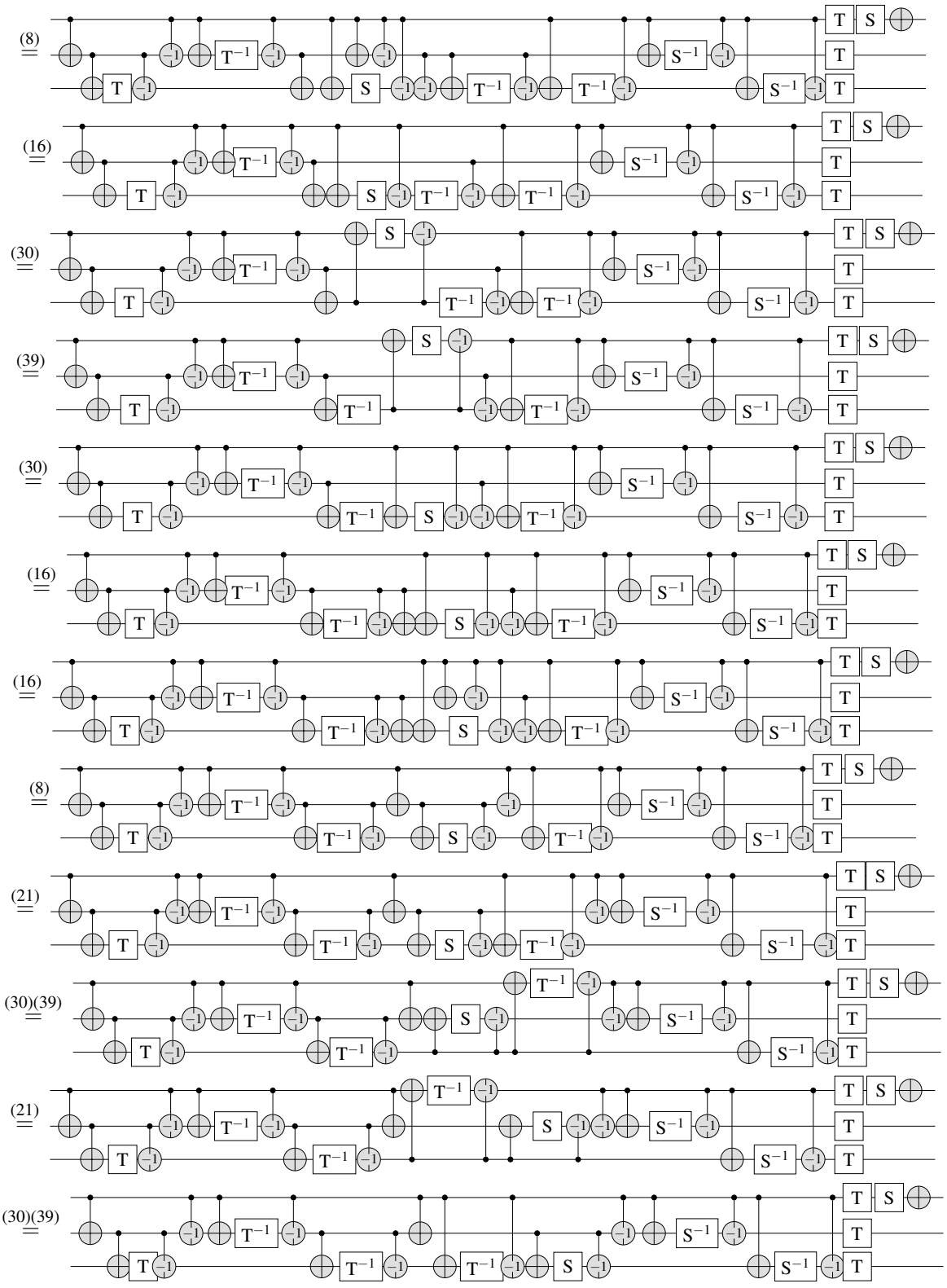

(1)(2)
(4)
(27)
(1)
(21)
(28)
(28)(33)
(23)
(26)(19)
(39)
(26)(19)(24)
(25)
(39)
=
S

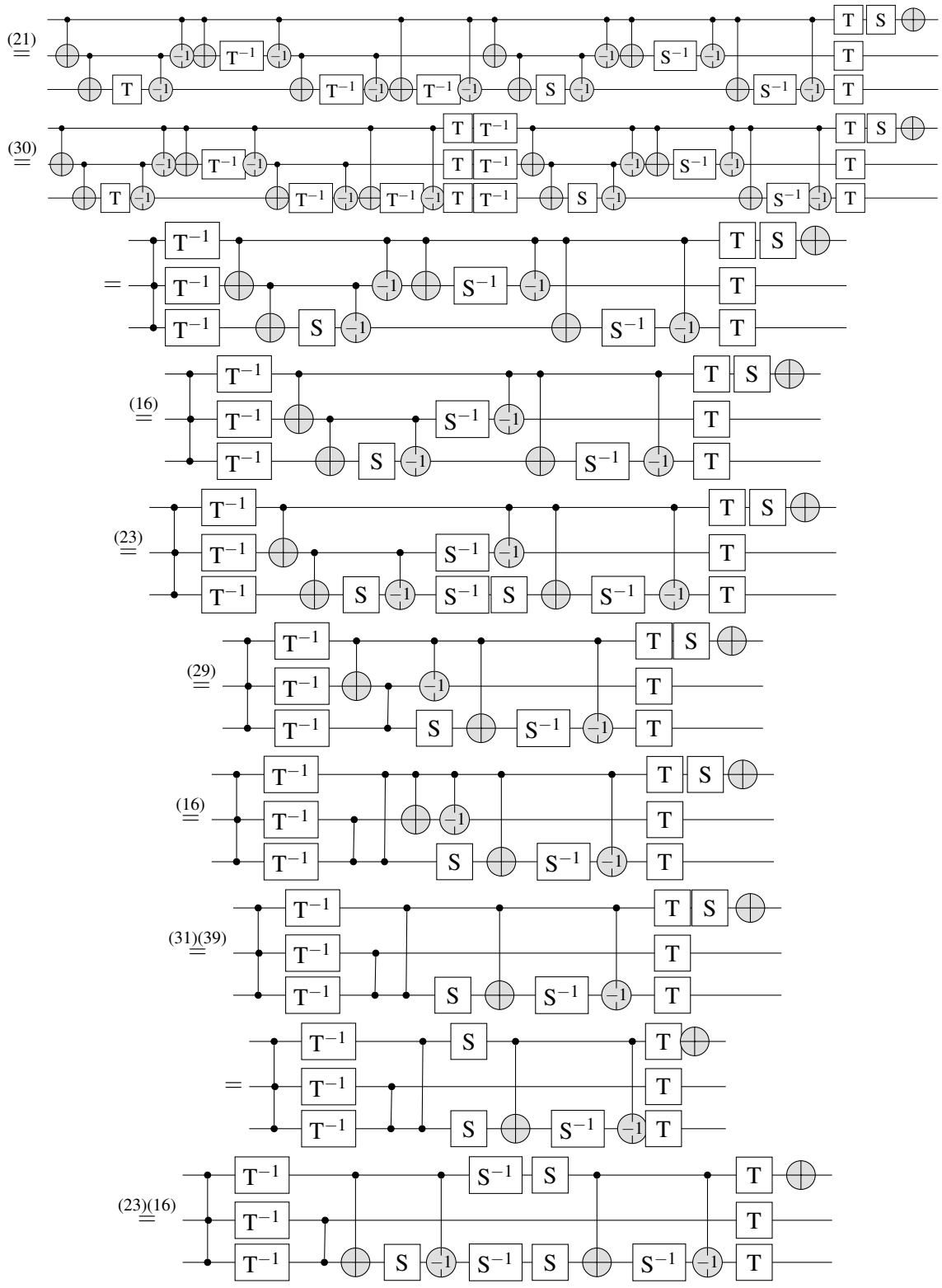
□

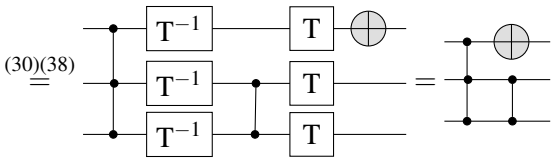
Lemma 82. *CubicPhase*$_d \vdash$  =

Proof.

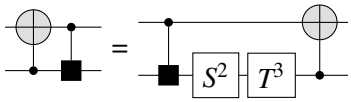



(8)
=
(16)
=
(30)
=
(39)
=
(30)
=
(16)
=
(16)
=
(8)
=
(21)
=
(30)(39)
=
(21)
=
(30)(39)
=

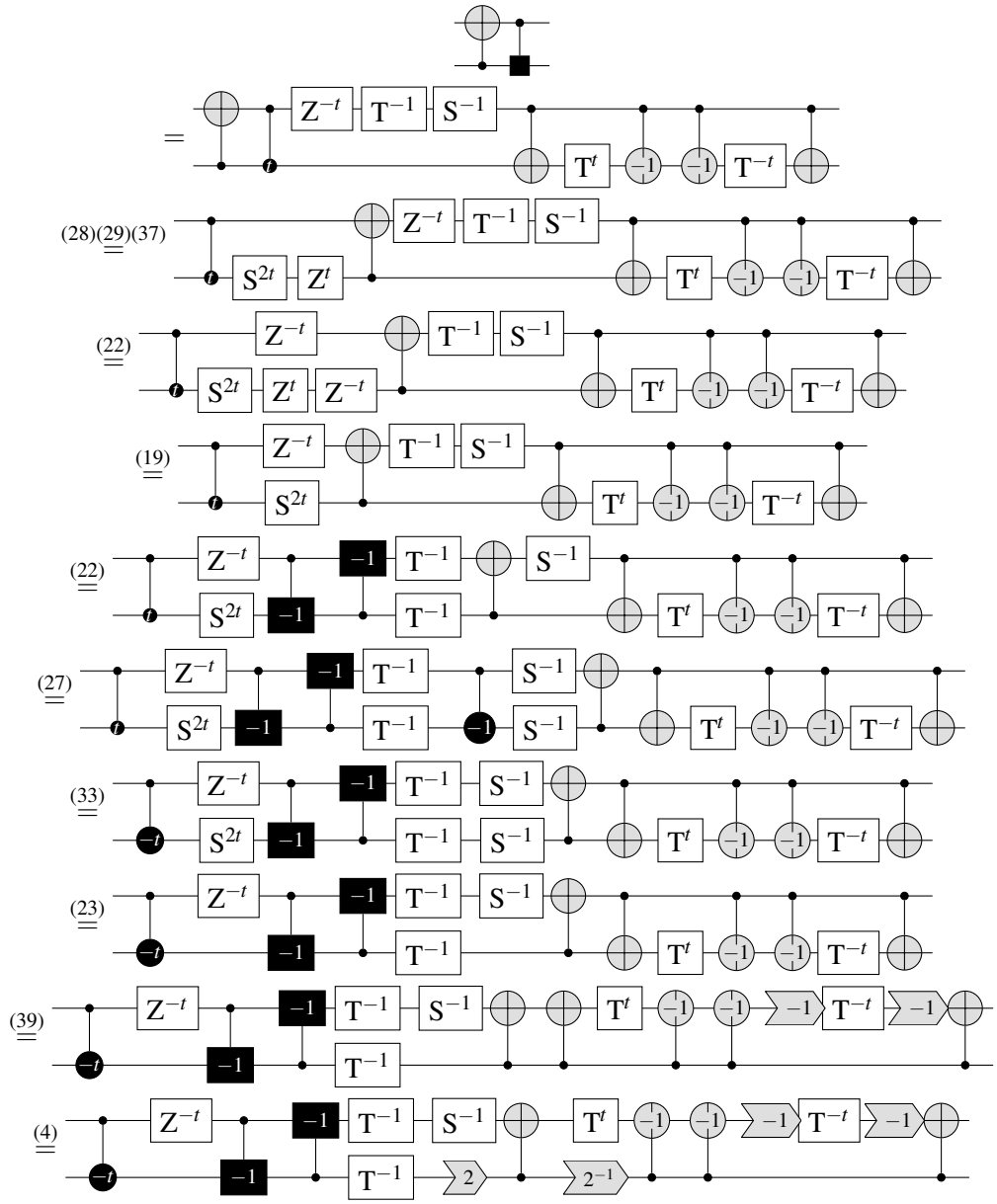

(21)
=
(30)
=
=
(16)
=
(23)
=
(29)
=
(16)
=
(31)(39)
=
=
(23)(16)
=

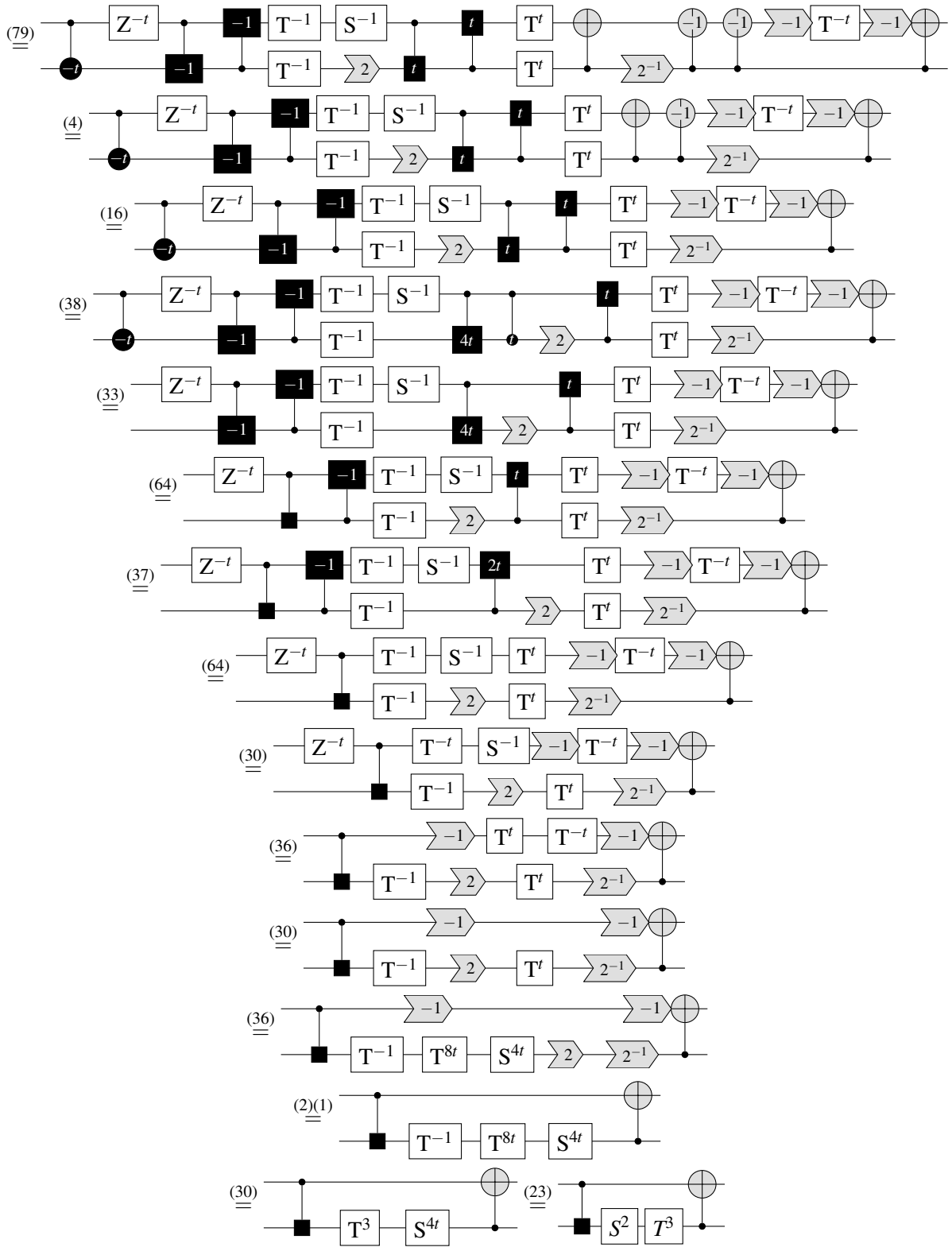


□

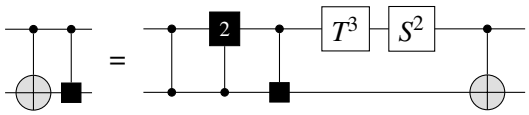
Lemma 83. *CubicPhase*$_d \vdash$ 

Proof.

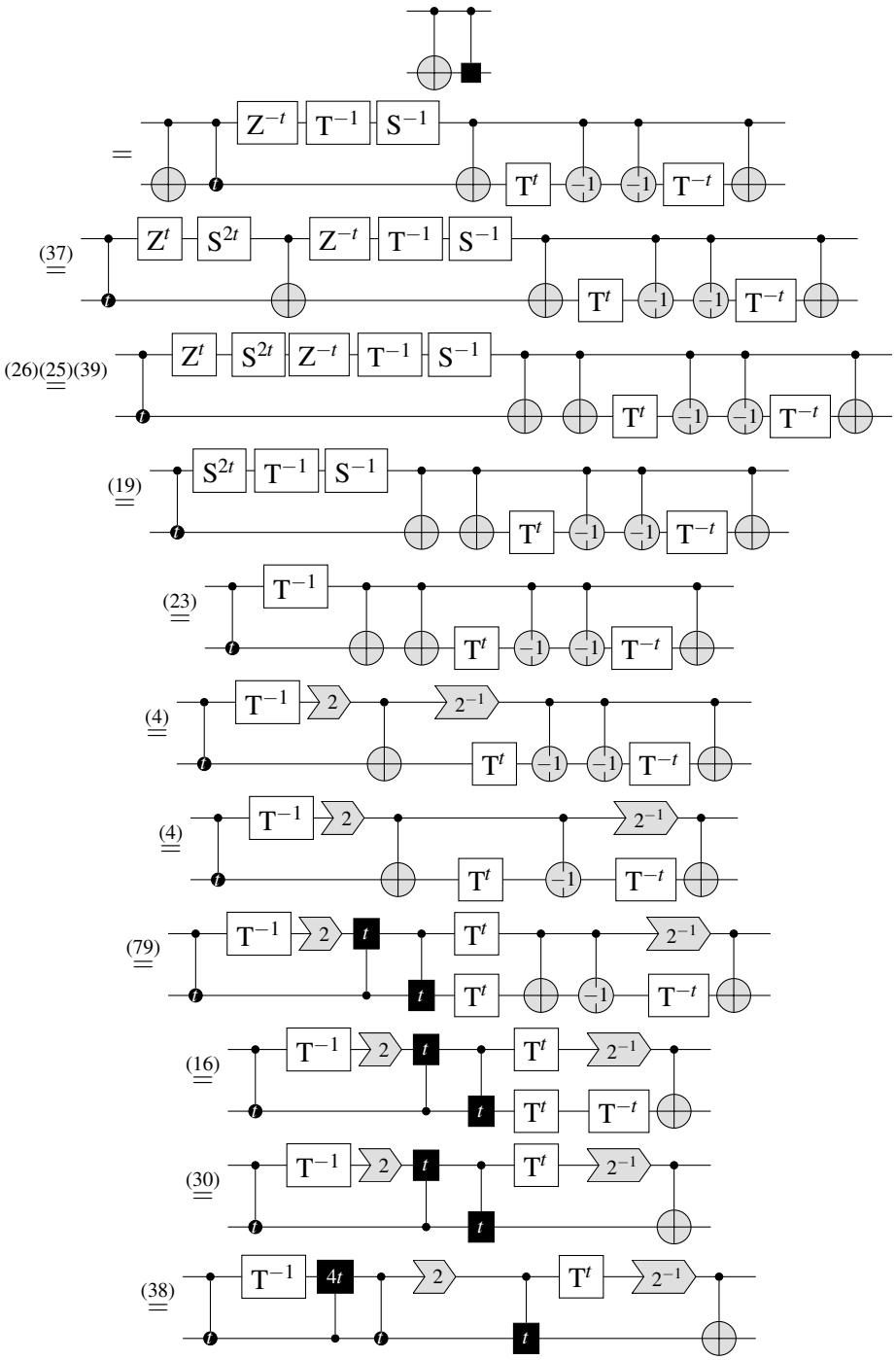


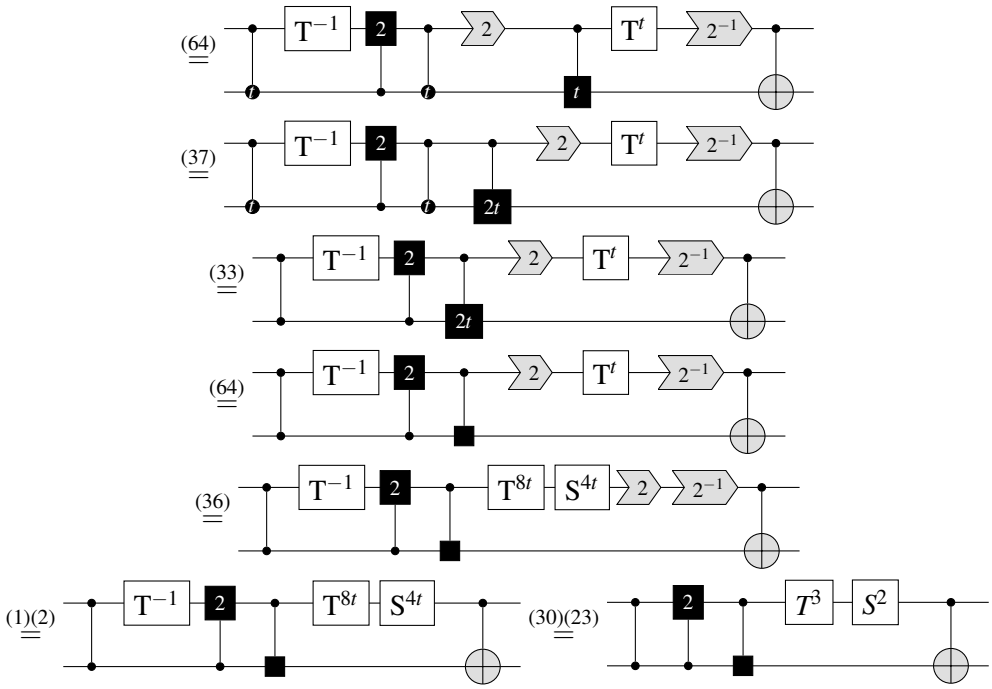

(79)
(4)
(16)
(38)
(33)
(64)
(37)
(64)
(30)
(36)
(30)
(36)
(2)(1)
(30)
(23)

□

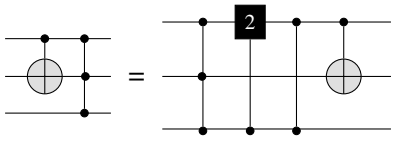
Lemma 84. *CubicPhase*$_d \vdash$ 

Proof.

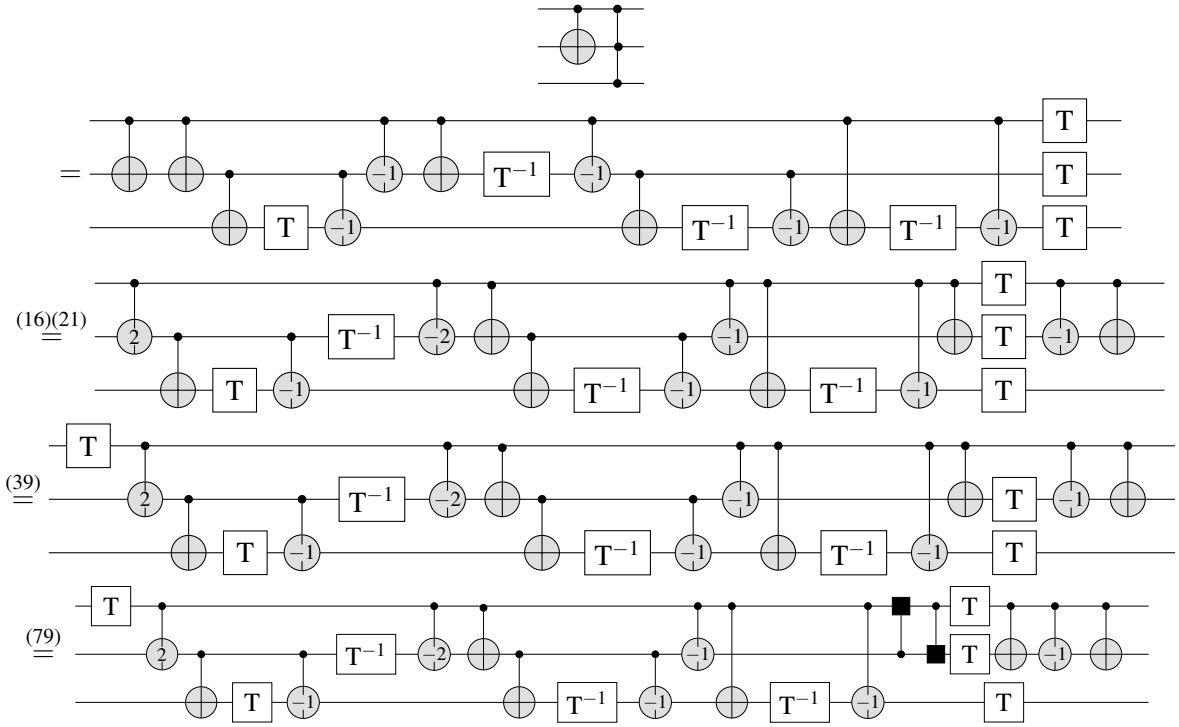


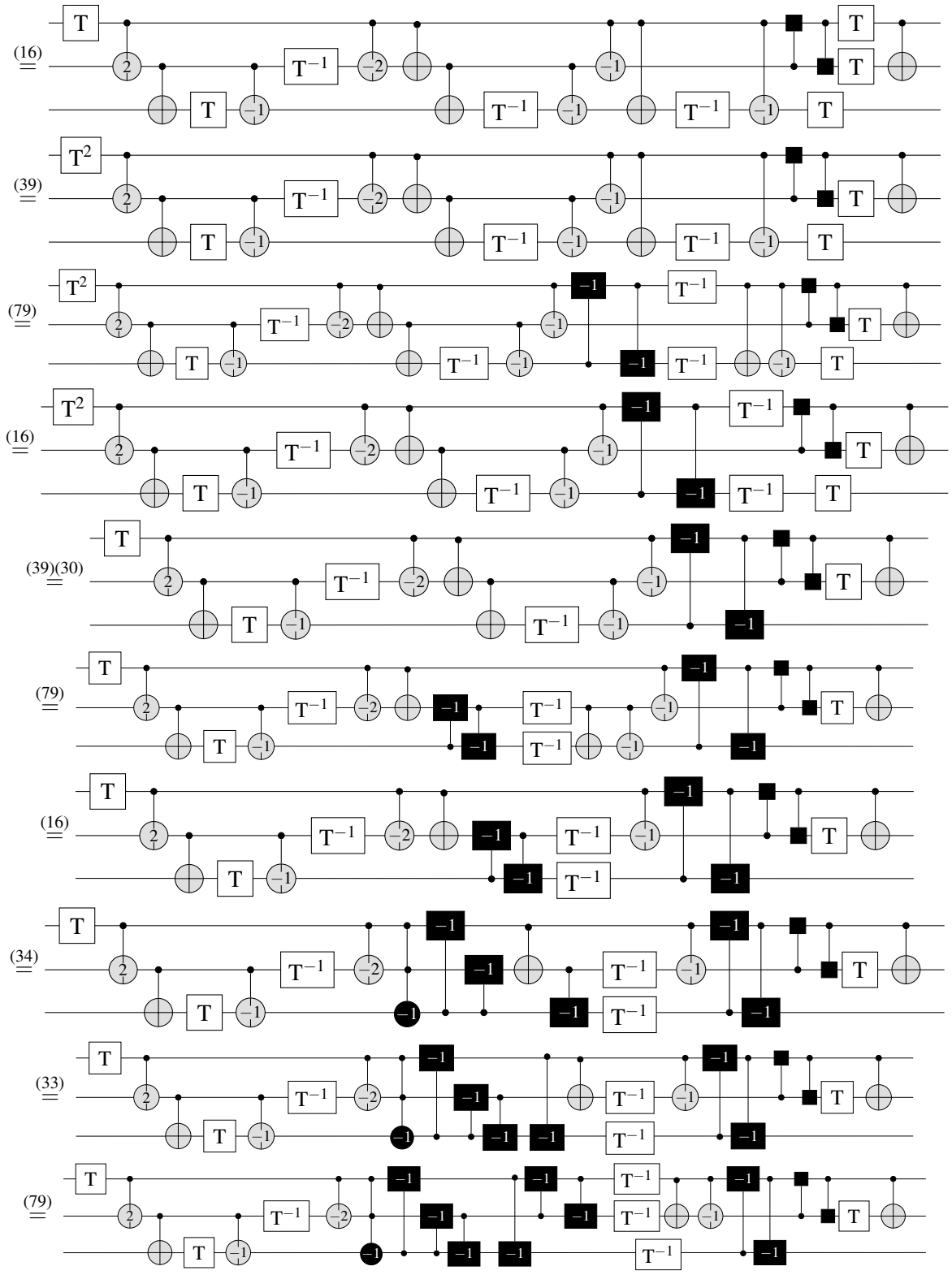


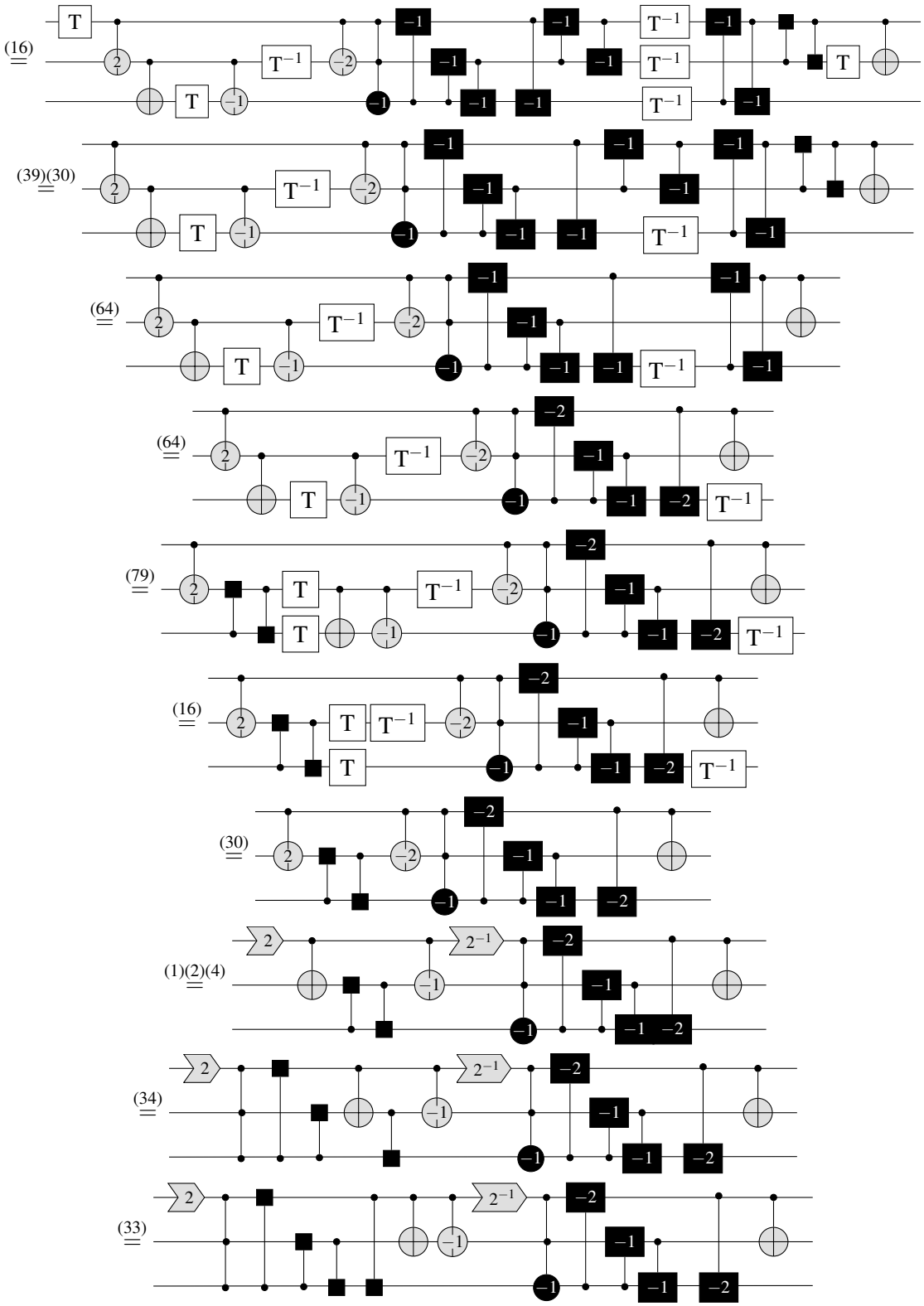
□

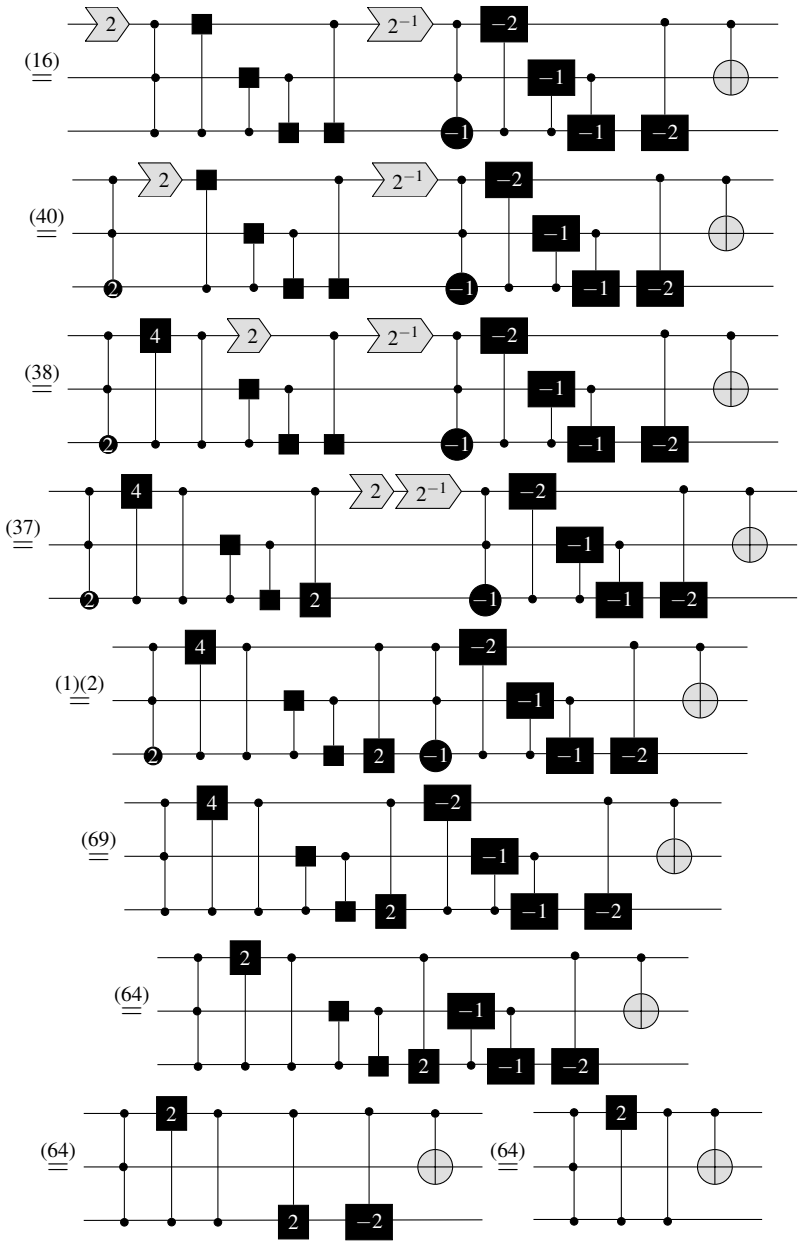
Lemma 85. *CubicPhase*$_d \vdash$ 

Proof.




(16)
(39)
(79)
(16)
(39)(30)
(79)
(16)
(34)
(33)
(79)


(16)
(39)(30)
(64)
(64)
(79)
(16)
(30)
(1)(2)(4)
(34)
(33)



□

B Group theoretic presentations for reversible linear and affine transformations in prime dimension d

This section is group-theoretic. Fix a prime d. We collect a single family of generators and relations that will later be read as circuit rules and diagrammatic axioms. From this list we obtain complete presentations of $\mathrm{SL}_n(\mathbb{F}_d)$, $\mathrm{GL}_n(\mathbb{F}_d)$, and $\mathrm{GA}_n(\mathbb{F}_d)$ by restricting generators and relations.

On computational basis labels $x \in \mathbb{F}_d^n$, an affine reversible circuit acts by $x \mapsto Ax+b$ with $A \in \mathrm{GL}_n(\mathbb{F}_d)$ and $b \in \mathbb{F}_d^n$. The linear part A lies in $\mathrm{SL}_n(\mathbb{F}_d)$ when $\det(A) = 1$, and in $\mathrm{GL}_n(\mathbb{F}_d)$ in general; adjoining

	Z	S	T				
Z	—	(24)	(32)	(29)	(43) (46)	(43) (46)	(59)
S		—	(31)	(28)	(42) (45)	(42) (45)	(58)
T			—	(38)	(41) (44)	(41) (44)	(57)
				(35)	(73) (50) (49)	(73) (50) (49)	(70) (60)
					(55) (56) (54)	(78) (55) (56) (54)	(61) (62) (76)
						(55) (56) (54)	(61) (62) (76)
							(63) (72)

Table 1: Diagonal commutations used to reorder a diagonal layer into normal form. Lower-triangular cases follow by symmetry / swapping the two sides, and disjoint-support cases follow from the PROP laws. For the CZ and CCZ we use the fact that we proved the symmetry of the circuit in (31), (51), (52) to reduce the number of cases to check.

	Z	S	T				
	(20)	(26)	(35)	(34)	(81) (80)	(81) (80)	(82)
	(22) (26)	(25) (27)	(39) (79)	(37) (29) (36)	(84) (83) (33) (34) (47) (48)	(84) (83) (33) (34) (47) (48)	(85) (41) (53)
x	(21)	(27)	(36)	(28)	(37) (38)	(37) (38)	(40)

Table 2: Transport equations used to commute diagonal generators past affine generators (so diagonal gates can be collected into a single layer). For the CZ and CCZ we use the fact that we proved the symmetry of the circuit in (31), (51), (52) to reduce the number of cases to check.

translations gives $\mathrm{GA}_n(\mathbb{F}_d) \cong \mathbb{F}_d^n \rtimes \mathrm{GL}_n(\mathbb{F}_d)$. When $d = 2$, one has $\mathbb{F}_2^\times = \{1\}$, hence $\mathrm{GL}_n(\mathbb{F}_2) = \mathrm{SL}_n(\mathbb{F}_2)$. For odd prime d, diagonal scalings must be included explicitly.

B.1 Conventions and notation

Identify $\mathbb{F}_d$ with $\mathbb{Z}/d\mathbb{Z}$, and write $\mathbb{F}_d^\times$ for its multiplicative group. Vectors in $\mathbb{F}_d^n$ are column vectors and matrices act on the left. Write I_n for the $n \times n$ identity matrix. For $1 \le i, j \le n$, let $e_{i,j}$ be the matrix unit with a single 1 in row i, column j.

Remark 3. *If g satisfies $g^d = \mathrm{id}$ and $t \in \mathbb{F}_d$, we write $g^t := g^{\tilde{t}}$ where $\tilde{t} \in \{0, \dots, d-1\}$ is the chosen integer representative. For $a, b \in \mathbb{F}_d$ one has $g^{a+b} = g^a g^b$ since exponents are computed modulo d. We still state relations of the form $g^d = \mathrm{id}$ explicitly, since this avoids bookkeeping when these are later translated into diagrammatic axioms.*

B.2 Generators in matrices

Definition 23. *For distinct indices $i \neq j$, let $\mathrm{CX}_{ij} \in \mathrm{GL}_n(\mathbb{F}_d)$ be the elementary transvection that sends $x_j \mapsto x_j + x_i$ and fixes x_k for $k \neq j$. Equivalently, $\mathrm{CX}_{ij} = I_n + e_{j,i}$.*

Definition 24. *For $k \in \mathbb{F}_d^\times$, let $\mathrm{M}_1(k) = \mathrm{diag}(k, 1, \dots, 1) \in \mathrm{GL}_n(\mathbb{F}_d)$.*

Definition 25. *For $1 \le i \le n$, let $X_i \in \mathrm{GA}_n(\mathbb{F}_d)$ be translation in the ith coordinate, $x_i \mapsto x_i + 1$, fixing the other coordinates. Equivalently, $X_i = (I_n, e_i)$ where e_i is the ith standard basis vector.*

B.3 A single list of relations

Fix $n \ge 1$. Let $\{x_{ij} \mid 1 \le i \neq j \le n\}$, $\{m(k) \mid k \in \mathbb{F}_d^\times\}$, and $\{t_i \mid 1 \le i \le n\}$ be abstract generators. All parameters t, u, b_i below are in $\mathbb{F}_d$, and all products ab, $k\ell$ are computed in $\mathbb{F}_d$.

Definition 26. *Write $\mathsf{R}_{\mathrm{SL}}(n,d)$ for the following relations on the generators x_{ij}:*

$$x_{ij}^d = \mathrm{id} \qquad (i \neq j), \tag{Stein1}$$

$$x_{ik}^{tu} x_{ij}^{t} x_{jk}^{u} = x_{jk}^{u} x_{ij}^{t} \qquad (i, j, k \text{ distinct}), \tag{Stein2}$$

$$x_{ij} x_{k\ell} = x_{k\ell} x_{ij} \qquad (i \neq \ell,\ j \neq k). \tag{Stein3}$$

When $n = 2$ we also impose the rank-1 relations as follows. For $a \in \mathbb{F}_d^\times$, define words

$$w(a) := x_{12}^{-a^{-1}} x_{21}^{a} x_{12}^{-a^{-1}}, \qquad h(a) := w(a)\, w(1)^{-1},$$

and impose

$$h(a)\, h(b) = h(ab) \qquad (a, b \in \mathbb{F}_d^\times), \tag{Torus}$$

$$w(1)\, x_{21}\, w(1)^{-1} = x_{12}^{-1}. \tag{Weyl}$$

Write $\mathsf{R}_{\mathrm{GL}}(n,d)$ for $\mathsf{R}_{\mathrm{SL}}(n,d)$ together with the relations involving $m(\cdot)$:

$$m(1) = \mathrm{id}, \tag{mult1}$$

$$m(k)\, m(\ell) = m(k\ell) \qquad (k, \ell \in \mathbb{F}_d^\times), \tag{multM}$$

$$m(x)\, x_{i1} = x_{i1}^{x}\, m(x) \qquad (i \neq 1,\ x \in \mathbb{F}_d^\times), \tag{MCx}$$

$$m(x)\, x_{1j}^{x} = x_{1j}\, m(x) \qquad (j \neq 1,\ x \in \mathbb{F}_d^\times), \tag{MxC}$$

$$m(x)\, x_{ij} = x_{ij}\, m(x) \qquad (1 \notin \{i, j\},\ x \in \mathbb{F}_d^\times). \tag{MCsep}$$

Write $\mathsf{R}_{\mathrm{GA}}(n,d)$ *for* $\mathsf{R}_{\mathrm{GL}}(n,d)$ *together with the relations involving* t_i*:*

$$t_i^d = \mathrm{id} \qquad (1 \le i \le n), \tag{Xd}$$
$$t_i t_j = t_j t_i \qquad (i \neq j), \tag{Xcom}$$
$$m(k)\, t_1 = t_1^k\, m(k) \qquad (k \in \mathbb{F}_d^\times), \tag{XM}$$
$$m(k)\, t_i = t_i\, m(k) \qquad (i \neq 1,\ k \in \mathbb{F}_d^\times), \tag{XMsep}$$
$$t_j x_{ij} = x_{ij} t_j \qquad (i \neq j), \tag{XCx}$$
$$x_{ij} t_i = t_i t_j x_{ij} \qquad (i \neq j), \tag{XxC}$$
$$t_s x_{ij} = x_{ij} t_s \qquad (s \notin \{i,j\}). \tag{XCxsep}$$

B.4 Three abstract groups and three comparison maps

Definition 27. *Let* $\mathrm{St}_n(\mathbb{F}_d)$ *be the group on generators* $\{x_{ij} \mid i \neq j\}$ *modulo* $\mathsf{R}_{\mathrm{SL}}(n,d)$*. Define* $\Phi^{\mathrm{SL}} : \mathrm{St}_n(\mathbb{F}_d) \to \mathrm{SL}_n(\mathbb{F}_d)$ *by* $\Phi^{\mathrm{SL}}(x_{ij}) = \mathrm{CX}_{ij}$*.*

Definition 28. *Let* G_n^{lin} *be the group on generators* $\{x_{ij} \mid i \neq j\} \cup \{m(k) \mid k \in \mathbb{F}_d^\times\}$ *modulo* $\mathsf{R}_{\mathrm{GL}}(n,d)$*. Define* $\Phi^{\mathrm{GL}} : G_n^{\mathrm{lin}} \to \mathrm{GL}_n(\mathbb{F}_d)$ *by* $\Phi^{\mathrm{GL}}(x_{ij}) = \mathrm{CX}_{ij}$ *and* $\Phi^{\mathrm{GL}}(m(k)) = \mathrm{M}_1(k)$*.*

Definition 29. *Let* G_n^{aff} *be the group on generators* $\{x_{ij} \mid i \neq j\} \cup \{m(k) \mid k \in \mathbb{F}_d^\times\} \cup \{t_i \mid 1 \le i \le n\}$ *modulo* $\mathsf{R}_{\mathrm{GA}}(n,d)$*. Define* $\Phi^{\mathrm{AGL}} : G_n^{\mathrm{aff}} \to \mathrm{GA}_n(\mathbb{F}_d)$ *by* $\Phi^{\mathrm{AGL}}(x_{ij}) = (\mathrm{CX}_{ij}, 0)$*,* $\Phi^{\mathrm{AGL}}(m(k)) = (\mathrm{M}_1(k), 0)$ *and* $\Phi^{\mathrm{AGL}}(t_i) = (I_n, e_i)$

B.5 Presentations

Theorem 3. *The homomorphism* Φ^{SL} *is an isomorphism.*

Proof. The defining relations $\mathsf{R}_{\mathrm{SL}}(n,d)$ hold in $\mathrm{SL}_n(\mathbb{F}_d)$, hence Φ^{SL} is well-defined. Its image contains all transvections CX_{ij}, hence contains $E_n(\mathbb{F}_d)$, and $E_n(\mathbb{F}_d) = \mathrm{SL}_n(\mathbb{F}_d)$ by [18, §7, p. 91], so Φ^{SL} is surjective.

The relations $\mathsf{R}_{\mathrm{SL}}(n,d)$ are the type-A_{n-1} Steinberg relations presenting the simply connected Chevalley group. By the Steinberg–Chevalley analysis, $\ker(\Phi^{\mathrm{SL}})$ is central and governed by $K_2(\mathbb{F}_d)$ [18, 15, §6, Thm. 8–9]. For a finite field, $K_2(\mathbb{F}_d) = 0$ by Quillen [17], hence $\ker(\Phi^{\mathrm{SL}}) = \{1\}$ and Φ^{SL} is injective. □

Theorem 4. *If* $n \ge 3$*, then* $\mathsf{R}_{\mathrm{SL}}(n,d)$ *may be taken to be just* (Stein1)–(Stein3)*, since* (Torus)–(Weyl) *follow from* (Stein1)–(Stein3) *in type* A_{n-1} *[18, §6, Thm. 9].*

Corollary 2. *The homomorphism* Φ^{GL} *is an isomorphism. In particular,* $\mathsf{R}_{\mathrm{GL}}(n,d)$ *presents* $\mathrm{GL}_n(\mathbb{F}_d)$*.*

Proof. Surjectivity: let $A \in \mathrm{GL}_n(\mathbb{F}_d)$ and set $x = \det(A)$. Then $S = \mathrm{diag}(x^{-1}, 1, \ldots, 1)A \in \mathrm{SL}_n(\mathbb{F}_d)$. By Theorem 3, S is a product of transvections, so $A = \Phi^{\mathrm{GL}}(m(x))\Phi^{\mathrm{GL}}(U)$ for some word U in the x_{ij}.

Injectivity: using (MCx)–(MCsep), commute all $m(\cdot)$ generators to the far left, and use (multM) to merge them, so every element of G_n^{lin} is represented by a word $m(x)U$ with U in the x_{ij}. If $\Phi^{\mathrm{GL}}(m(x)U) = I_n$, taking determinants gives $x = 1$, hence $\Phi^{\mathrm{SL}}(U) = I_n$. By Theorem 3, $U = \mathrm{id}$ in $\mathrm{St}_n(\mathbb{F}_d)$, hence $m(x)U = \mathrm{id}$ in G_n^{lin}. □

Corollary 3. *The homomorphism* Φ^{AGL} *is an isomorphism. In particular,* $\mathsf{R}_{\mathrm{GA}}(n,d)$ *presents* $\mathrm{GA}_n(\mathbb{F}_d)$*.*

Proof. Surjectivity: every $(A,b) \in \mathrm{GA}_n(\mathbb{F}_d)$ factors as $(I_n,b) \circ (A,0)$. Write $b = (b_1,\dots,b_n)$. Since $(I_n,b) = \Phi^{\mathrm{AGL}}(t_1^{b_1} \cdots t_n^{b_n})$ and $(A,0)$ lies in the image by Corollary 2, the map Φ^{AGL} is surjective.

Injectivity: using (XM)–(XCxsep), commute all t_i generators to the far left, collecting them with (Xd)–(Xcom) into a word $t_1^{b_1} \cdots t_n^{b_n} U$, where U is a word in $\{x_{ij}, m(k)\}$. If $\Phi^{\mathrm{AGL}}(t_1^{b_1} \cdots t_n^{b_n} U) = \mathrm{id}$, then $\Phi^{\mathrm{AGL}}(U) = (A,0)$ and $\Phi^{\mathrm{AGL}}(t_1^{b_1} \cdots t_n^{b_n}) = (I_n,b)$ satisfy $(A,b) = (I_n,0)$, hence $A = I_n$ and $b = 0$. By Corollary 2, $A = I_n$ forces $U = \mathrm{id}$. By (Xd)–(Xcom), $b = 0$ forces all $b_i = 0$, hence the translation word is id. □

B.6 Beyond finite fields: presentations over $\mathbb{Z}$ and other rings

While this appendix fixed a prime d, the Steinberg-type presentation used above fits into a more general pattern over coefficient rings. For a unital ring R and $n \geq 3$, one defines the Steinberg group $\mathrm{St}_n(R)$ on generators $x_{ij}(r)$ for $i \neq j$ and $r \in R$, subject to the usual Steinberg relations. The assignment $x_{ij}(r) \mapsto I_n + r e_{j,i}$ induces a surjection $\mathrm{St}_n(R) \twoheadrightarrow E_n(R)$ onto the elementary subgroup of $\mathrm{GL}_n(R)$, and its kernel is central and canonically identified with $K_2(R)$ [22]. In the finite-field case, $K_2(\mathbb{F}_d) = 0$, which is exactly why the relations above collapse to a presentation of $\mathrm{SL}_n(\mathbb{F}_d)$.

Over $R = \mathbb{Z}$, this kernel does not vanish. One has $K_2(\mathbb{Z}) \cong \mathbb{Z}/2$, and the nontrivial element may be represented by the Steinberg symbol $\{-1,-1\} = (x_{12}(1)x_{21}(-1)x_{12}(1))^4$, which generates $\ker(\mathrm{St}_n(\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{Z}))$ for all $n \geq 3$ [22]. Consequently, a Steinberg-style presentation yields $\mathrm{St}_n(\mathbb{Z})$; to obtain a presentation of $\mathrm{SL}_n(\mathbb{Z})$ one must add an additional relation killing this central element.

Finite presentations for $\mathrm{SL}_3(\mathbb{Z})$ and, more generally, for SL_3 over several rings of integers are worked out by Conder, Robertson and Williams [9]. These results suggest a route to extending our diagrammatic axiomatisations from prime fields to integer-linear and integer-affine fragments, by retaining the local Steinberg relations and adjoining a small number of additional axioms that account for the relevant K_2-kernel.

A related extension covers determinant-± 1 matrices. Starting from a presentation of $\mathrm{SL}_n(\mathbb{Z})$, one may adjoin a generator r representing a determinant -1 matrix such as $\mathrm{diag}(-1,1,\dots,1)$, together with relations describing its conjugation action on elementary transvections, to obtain a presentation of $\mathrm{SL}_n^{\pm}(\mathbb{Z}) = \mathrm{GL}_n(\mathbb{Z})$. Adding translations yields $\mathbb{Z}^n \rtimes \mathrm{GL}_n(\mathbb{Z})$; diagrammatically, this replaces the torsion relations $t_i^d = \mathrm{id}$ by infinite-order translation laws, while keeping the same semidirect-product interaction between translations and linear generators as in $\mathsf{R}_{\mathrm{GA}}(n,d)$.