Quantum Codes from Twisted Unitary t-Groups

Eric Kubischta[*] and Ian Teixeira[†]

Joint Center for Quantum Information and Computer Science, NIST/University of Maryland, College Park, Maryland 20742, USA

(Received 5 March 2024; accepted 3 June 2024; published 17 July 2024)

We introduce twisted unitary t-groups, a generalization of unitary t-groups under a twisting by an irreducible representation. We then apply representation theoretic methods to the Knill-Laflamme error correction conditions to show that twisted unitary t-groups automatically correspond to quantum codes with distance $d = t + 1$. By construction these codes have many transversal gates, which naturally do not spread errors and thus are useful for fault tolerance.

DOI: 10.1103/PhysRevLett.133.030602

Introduction.—There is a rich history of connections between classical t-designs (both spherical and orthogonal) and classical information theory [1]. Similarly, there are many applications of quantum t-designs (both complex projective and unitary) to quantum information theory, including tomography [2,3], randomized benchmarking [4], cryptography [5], and chaos [6].

However, until now, no connection has been made between quantum t-designs and quantum error correcting codes, despite the fact that there are deep connections between classical t-designs and classical error-correcting codes, such as the theorem of Assmus and Matteson [1,7].

Among quantum t-designs, unitary t-designs are especially commonplace in the quantum information literature, and in the special case that a unitary t-design $\mathcal{G}$ forms a finite group it is called a *unitary t-group*. Unitary t-groups are well studied [8–11].

In forging a connection between quantum t-designs and quantum error correcting codes we first review unitary t-groups using tools from representation theory; similar techniques were introduced in [9–11]. We then define *twisted unitary t-groups* and argue that they are a natural generalization of unitary t-groups under a "twisting" by $\boldsymbol{\lambda}$, an irreducible representation (irrep) of $\mathcal{G}$. In the special case that $\boldsymbol{\lambda}$ is the trivial irrep $\mathbf{1}$, twisted unitary t-groups are equivalent to the regular notion of unitary t-groups.

Application.—Our main application of twisted unitary t-groups is in constructing quantum codes that naturally have many transversal logical gates. A logical gate for an n qudit quantum code is called transversal if it can be implemented as $U_1 \otimes \cdots \otimes U_n$, where each unitary U_i acts on a single physical qudit. As an application of twisted unitary t-groups we show that they induce quantum codes with distance $d = t + 1$, and that the corresponding quantum codes can have very large groups of transversal gates: for each $g \in \mathcal{G}$ the physical gate $g^{\otimes n}$ implements the logical gate $\boldsymbol{\lambda}(g)$. A logical gate implemented by the physical gate $g^{\otimes n}$ acts on each physical qudit separately and so does not spread errors between physical qudits, for this reason such gates are likely to be useful for fault tolerance.

We highlight our application via two examples. In our first example we show that the unitary 5-group 2I, the binary icosahedral subgroup of SU(2), forms a twisted unitary 2-group with respect to a particular two-dimensional irrep. This yields n-qubit codes for all odd $n \geq 7$ of distance $d = 3$ (meaning these codes can correct an arbitrary single error). Each of these codes implements all of 2I transversally. In our second example, we show that the unitary 3-group $\Sigma(360\phi)$, a maximal subgroup of SU(3) (and well studied in the high energy literature [12–14]), forms a twisted unitary 1-group with respect to two distinct three-dimensional irreps. These yield n-qutrit quantum codes of distance $d = 2$ for all $n \geq 5$ not divisible by 3. Each of these codes implements all of $\Sigma(360\phi)$ transversally. For both our examples an encoding circuit can be obtained using [15].

Motivation.—Since transversal gates do not propagate errors between physical qudits, and thus are often useful for fault tolerance, it is desirable to have as many transversal gates as possible. However the Eastin-Knill theorem [16] shows that a nontrivial ($d \geq 2$) code can have only finitely many transversal gates. So the best we can do is find codes whose transversal gates form a maximal finite subgroup. When a maximal group of transversal gates is achieved, for example the Clifford group, the next step is a fault tolerant implementation of a single gate τ outside of the group $\mathcal{G}$. The most popular method for implementing τ in a fault tolerant fashion is by using magic state distillation [17], however, this is considered expensive [18,19]. It is therefore crucial for fault tolerant gate synthesis to minimize the number of τ gates that are needed.

It was proven in [20] that 2I, together with a particular τ gate, is the *optimal* universal gate set for qubits in the sense that this gate set can quickly approximate any gate in SU(2) while minimizing the number of expensive τ gates that are needed. Therefore, our first example of 2I transversal codes is well motivated.

Why is the 2I universal gate set optimal? Unfortunately the work in [20] is for the qubit case and there is no rigorous proof generalizing it to qudits (although some work towards SU(3) has already been accomplished [21]). But one heuristic is that 2I is a unitary 5-group whereas every other subgroup of SU(2) is at most a unitary 3-group. This means 2I is more "spread out" than the other subgroups and so an approximation algorithm does not have to use as many τ gates in order to reach the more hidden recesses of SU(2). The largest unitary t-group in SU(3) is in fact $\Sigma(360\phi)$. It is a unitary 3-group whereas all other subgroups of SU(3) are at best unitary 2-groups. Thus if we apply the same logic as before, we expect that $\Sigma(360\phi)$ plays a role in the optimal universal gate set for qutrits, but more work needs to be done to rigorously prove this claim.

Disclaimer.—The codes we find using our methods are in general nonadditive, meaning they are not equivalent to any stabilizer code. In particular this means that the standard fault tolerant methods of decoding and correcting errors for stabilizer codes [22] cannot be used. There are methods for decoding and correcting nonadditive codes, for example, one can just measure the error space projectors and then undo the error with an appropriate unitary, but also more advanced techniques exist [23–25]. However, the jury is still out regarding how fault tolerant those nonadditive decoding methods are (if at all). Our hope is that our work could be used to understand the structure of nonadditive codes in more detail and help spur new research toward fully fault tolerant nonadditive codes.

Review of unitary t-groups.—Let $\mathrm{U}(q)$ be the unitary group of degree q. A finite subgroup $\mathcal{G}$ of $\mathrm{U}(q)$ is called a *unitary t-group* [26] if

$$\frac{1}{|\mathcal{G}|}\sum_{U\in\mathcal{G}}(U\otimes U^*)^{\otimes t}=\int_{\mathrm{U}(q)}(U\otimes U^*)^{\otimes t}dU, \tag{1}$$

where the integral on the right is taken with respect to the unit-normalized Haar measure (if $\mathcal{G}$ is merely a finite subset rather than a finite subgroup then this is called a unitary t-design).

On the right-hand side, U is a $q\times q$ matrix in the **F**undamental (or defining) representation $\mathbf{F}$ of $\mathrm{U}(q)$. On the left hand side, U is a $q\times q$ matrix in the restricted representation of $\mathbf{F}$ to $\mathcal{G}$, denoted by $\mathbf{F}^{\downarrow}$ or $\mathbf{f}$ (sometimes called the *branching rules* in physics [27]). In our convention, we write representations with respect to $\mathrm{U}(q)$ using bold capital letters and we use the superscript $\downarrow$, or the corresponding bold lower-case letter, to denote the restriction to the finite subgroup $\mathcal{G}$. It follows that Eq. (1) is equivalent to

$$\frac{1}{|\mathcal{G}|}\sum_{g\in\mathcal{G}}(\mathbf{f}\otimes\mathbf{f}^*)^{\otimes t}(g)=\int_{\mathrm{U}(q)}(\mathbf{F}\otimes\mathbf{F}^*)^{\otimes t}(g)dg. \tag{2}$$

Here $\mathbf{F}^*$ is the dual representation of $\mathbf{F}$ given simply by the complex conjugate.

At this point we begin freely using concepts such as the character of a representation, inner product of characters, isotypic decomposition and isotypic projector, all of which are reviewed in the Supplemental Material [28].

Let $\mathbf{1}$ denote the trivial irrep for both $\mathrm{U}(q)$ and $\mathcal{G}$. The character of this irrep is 1 for all g. Thus we can multiply through by 1 on both sides to reveal that Eq. (2) is simply a projector equation:

$$\Pi_{\mathbf{1}}^{(\mathbf{f}\otimes\mathbf{f}^*)^{\otimes t}}=\Pi_{\mathbf{1}}^{(\mathbf{F}\otimes\mathbf{F}^*)^{\otimes t}}. \tag{3}$$

That is, a unitary t-group is such that the projector of the $\mathrm{U}(q)$-representation $(\mathbf{F}\otimes\mathbf{F}^*)^{\otimes t}$ onto the trivial irrep $\mathbf{1}$ must be the same as the projector of the $\mathcal{G}$-representation $(\mathbf{f}\otimes\mathbf{f}^*)^{\otimes t}$ onto the trivial irrep $\mathbf{1}$.

If we take the trace of both sides then we are counting the multiplicity of $\mathbf{1}$ in the isotypic decomposition of the tensor product via an inner product of characters. Because $\mathbf{f}$ is a branched version of $\mathbf{F}$, and the trivial irrep cannot branch further, the multiplicity on the left is greater than or equal to the multiplicity on the right. That is, *for any* subgroup $\mathcal{G}$ of $\mathrm{U}(q)$ we have

$$\langle 1,(ff^*)^t\rangle\geq\langle 1,(FF^*)^t\rangle. \tag{4}$$

And equality holds if and only if $\mathcal{G}$ is a unitary t-group. This is an inner product of characters where f and F denote the characters corresponding to the representations $\mathbf{f}$ and $\mathbf{F}$. We will continue to write the corresponding nonbold letters to represent characters.

Note that one can move characters within the inner product at the expense of a complex conjugation. Thus Eq. (4) says $\langle f^t,f^t\rangle\geq\langle F^t,F^t\rangle$, or $\|f^t\|\geq\|F^t\|$. Again equality holds if and only if $\mathcal{G}$ is a unitary t-group. Note that for a character f of a finite group it is standard to call $\langle f,f\rangle$ the *norm*, rather than call it the norm squared, and to denote it by $\|f\|\coloneqq\langle f,f\rangle$.

Now notice that $(\mathbf{F}\otimes\mathbf{F}^*)^{\otimes t}$ is a reducible $\mathrm{U}(q)$ representation and can be decomposed as

$$(\mathbf{F}\otimes\mathbf{F}^*)^{\otimes t}=\bigoplus_{\mathbf{R}\in\mathcal{E}_t}(m_{\mathbf{R}})\mathbf{R}. \tag{5}$$

Here $\mathbf{R}$ is an ir<u>R</u>ep of $\mathrm{U}(q)$ and $\mathcal{E}_t$ is the set of all $\mathrm{U}(q)$ irreps that appear with nonzero multiplicity $m_{\mathbf{R}}$.

As an example of the notation consider U(2). Then using [31] we can compute

$$(\mathbf{2}\otimes\mathbf{2}^*)^{\otimes 1}=\mathbf{1}\oplus\mathbf{3}, \tag{6}$$

$$(\mathbf{2}\otimes\mathbf{2}^*)^{\otimes 2}=(2)\mathbf{1}\oplus(3)\mathbf{3}\oplus\mathbf{5}, \tag{7}$$

$$(\mathbf{2}\otimes\mathbf{2}^*)^{\otimes 3}=(5)\mathbf{1}\oplus(9)\mathbf{3}\oplus(5)\mathbf{5}\oplus\mathbf{7}. \tag{8}$$

Here (and elsewhere), parenthesis indicate multiplicity, for example, $(2)\mathbf{1}$ is shorthand for $\mathbf{1}\oplus\mathbf{1}$. Then we see that $\mathcal{E}_1=\{\mathbf{1},\mathbf{3}\},\mathcal{E}_2=\{\mathbf{1},\mathbf{3},\mathbf{5}\},\mathcal{E}_3=\{\mathbf{1},\mathbf{3},\mathbf{5},\mathbf{7}\}$. More generally for U(2), we have $\mathcal{E}_t=\{\mathbf{1},\mathbf{3},\mathbf{5},\ldots,(\mathbf{2t}+\mathbf{1})\}$.

Returning to the general case $\mathrm{U}(q)$, we can take Eq. (2) and insert the decomposition from Eq. (5) to obtain

$$\bigoplus_{\mathbf{R}\in\mathcal{E}_t}(m_{\mathbf{R}})\frac{1}{|\mathcal{G}|}\sum_{g\in\mathcal{G}}\mathbf{R}^{\downarrow}(g)=\bigoplus_{\mathbf{R}\in\mathcal{E}_t}(m_{\mathbf{R}})\int_{\mathrm{U}(q)}\mathbf{R}(g)dg. \tag{9}$$

Here $\mathbf{R}^{\downarrow}$ denotes the restriction of $\mathbf{R}$ to $\mathcal{G}$. Thus we see that $\mathcal{G}$ is a unitary t-group if and only if

$$\frac{1}{|\mathcal{G}|}\sum_{g\in\mathcal{G}}\mathbf{R}^{\downarrow}(g)=\int_{\mathrm{U}(q)}\mathbf{R}(g)dg\quad\forall\ \mathbf{R}\in\mathcal{E}_t. \tag{10}$$

Inserting the trivial character 1 into both sides, we see that this is an equality of projectors $\Pi_{\mathbf{1}}^{\mathbf{R}^{\downarrow}}=\Pi_{\mathbf{1}}^{\mathbf{R}}$ for all $\mathbf{R}\in\mathcal{E}_t$. However, notice that when $\mathbf{R}=\mathbf{1}$ this equality is trivially satisfied (because $\mathbf{1}^{\downarrow}=\mathbf{1}$). On the other hand, when $\mathbf{R}\neq\mathbf{1}$ the right-hand side is the zero matrix $\mathbf{0}$, that is,

$$\Pi_{\mathbf{1}}^{\mathbf{R}^{\downarrow}}=\mathbf{0}\quad\forall\ \mathbf{R}\in\mathcal{E}_t\colon\ \mathbf{R}\neq\mathbf{1}. \tag{11}$$

In a similar fashion as before we can take the trace of both sides to get that *for any* $\mathcal{G}$,

$$\langle 1,R^{\downarrow}\rangle\geq 0\quad\forall\ \mathbf{R}\in\mathcal{E}_t\colon\ \mathbf{R}\neq\mathbf{1}, \tag{12}$$

with equality if and only if $\mathcal{G}$ is a unitary t-group. As before $R^{\downarrow}$ is the character corresponding to the representation $\mathbf{R}^{\downarrow}$.

A summary of all the equivalent conditions derived above can be found in the Supplemental Material [28] but for our purposes, the most useful perspectives on unitary t-groups are the two we highlight below.

Lemma 1.—$\mathcal{G}\subset\mathrm{U}(q)$ is a unitary t-group if and only if either of the following equivalent conditions are satisfied:
(1) $\|f^t\|=\|F^t\|$,
(2) $\langle 1,R^{\downarrow}\rangle=0,\ \forall\ \mathbf{R}\in\mathcal{E}_t,\ \mathbf{R}\neq\mathbf{1}$.

For small t, we can compute $\|F^t\|$ to obtain even simpler criteria for identifying a unitary t-group (cf. [9]).

Lemma 2.—Suppose $\mathcal{G}\subset\mathrm{U}(q)$.
(1) $\mathcal{G}$ is a unitary 1-group $\Leftrightarrow\|f\|=1$ (i.e., $\mathbf{f}$ is irreducible),
(2) $\mathcal{G}$ is a unitary 2-group $\Leftrightarrow\|f^2\|=2$.

Proof.—The fundamental representation $\mathbf{F}$ of $\mathrm{U}(q)$ is irreducible, so $\|F\|=1$. It is well known that when $\mathbf{F}$ is the fundamental representation of $\mathrm{U}(q)$, then $\mathbf{F}\otimes\mathbf{F}^*=\mathbf{1}\oplus\mathbf{Ad}$ where $\mathbf{Ad}$ is the adjoint irrep of $\mathrm{SU}(q)$. Then $\|F^2\|=\|FF^*\|$ which can be evaluated as $\|1+Ad\|=2$ where Ad is the adjoint character. Note that we have used the irreducibility of $\mathbf{Ad}$ which is equivalent to the fact that $\mathrm{SU}(q)$ is a simple Lie group. ∎

Going further, $\mathcal{G}\subset\mathrm{U}(q)$ is a 3-group if and only if $\|f^3\|=6$, for $q\geq 3$, or $\|f^3\|=5$, for $q=2$ [9]. The classification of unitary t groups given in [32] shows that no t-groups exist for $t>3$, with the exception of the binary icosahedral subgroup 2I of U(2), which is the only unitary 4-group and the only unitary 5-group.

Twisted unitary t-groups.—In Eq. (2), the left hand side can be thought of as a sum with respect to the uniform weight $1/|\mathcal{G}|$. But more generally we can take the sum $\sum_{g\in\mathcal{G}}W(g)(\mathbf{f}\otimes\mathbf{f}^*)^{\otimes t}(g)$ with respect to any normalized weight W. If

$$\sum_{g\in\mathcal{G}}W(g)(\mathbf{f}\otimes\mathbf{f}^*)^{\otimes t}(g)=\int_{\mathrm{U}(q)}(\mathbf{F}\otimes\mathbf{F}^*)^{\otimes t}(g)dg, \tag{13}$$

it is standard to call $\mathcal{G}$ a *weighted t-group* [8].

Let $\boldsymbol{\lambda}$ be an irrep of $\mathcal{G}$ with corresponding character λ. Then there is a natural weight

$$W_{\boldsymbol{\lambda}}(g)=\frac{1}{|\mathcal{G}|}\lambda^*(g)\lambda(g)=\frac{1}{|\mathcal{G}|}|\lambda(g)|^2. \tag{14}$$

Note that because $\boldsymbol{\lambda}$ is irreducible then $W_{\boldsymbol{\lambda}}$ is normalized: $\sum_{g\in\mathcal{G}}W_{\boldsymbol{\lambda}}(g)=\|\lambda\|=1$. And when $\boldsymbol{\lambda}$ is one-dimensional then $W_{\boldsymbol{\lambda}}(g)=1/|\mathcal{G}|$ and so we recover the usual (unweighted) definition of unitary t-groups. When we use the weight $W_{\boldsymbol{\lambda}}$ we will call $\mathcal{G}$ a *twisted unitary t-group* with respect to $\boldsymbol{\lambda}$ or, equivalently, a $\boldsymbol{\lambda}$-twisted unitary t-group. We can adapt Lemma 1 to this scenario, for a proof see [28].

Lemma 3.—$\mathcal{G}\subset\mathrm{U}(q)$ is a $\boldsymbol{\lambda}$-twisted unitary t-group if and only if either of the following equivalent conditions are satisfied:
(1) $\|\lambda f^t\|=\|F^t\|$,
(2) $\langle\lambda^*\lambda,R^{\downarrow}\rangle=0,\ \forall\ \mathbf{R}\in\mathcal{E}_t,\ \mathbf{R}\neq\mathbf{1}$.

Notice that part (2) of Lemma 3 implies part (2) of Lemma 1, so every $\boldsymbol{\lambda}$-twisted unitary t-group is also a unitary t-group. To see this implication, it is enough to observe the tensor product of an irrep with its dual always contains a unique trivial subrepresentation, i.e., there is a unique way to write $\boldsymbol{\lambda}^*\otimes\boldsymbol{\lambda}=\mathbf{1}\oplus\boldsymbol{\xi}$ for some representation $\boldsymbol{\xi}$. Thus $\langle\lambda^*\lambda,R^{\downarrow}\rangle=\langle 1,R^{\downarrow}\rangle+\langle\xi,R^{\downarrow}\rangle$ and so $\langle\lambda^*\lambda,R^{\downarrow}\rangle=0$ implies $\langle 1,R^{\downarrow}\rangle=0$.

We can also adapt Lemma 2 to the $\boldsymbol{\lambda}$-twisted case.

Lemma 4.—Suppose $\mathcal{G}\subset\mathrm{U}(q)$. Let $\boldsymbol{\lambda}$ be an irrep of $\mathcal{G}$.
(1) $\mathcal{G}$ is a $\boldsymbol{\lambda}$-twisted unitary 1-group $\Leftrightarrow\|\lambda f\|=1$ (i.e., $\boldsymbol{\lambda}\otimes\mathbf{f}$ is irreducible),
(2) $\mathcal{G}$ is a $\boldsymbol{\lambda}$-twisted unitary 2-group $\Leftrightarrow\|\lambda f^2\|=2$.

This lemma is the reason we have dubbed these "twisted" unitary t-groups. The irrep $\boldsymbol{\lambda}$ latches onto the fundamental irrep $\mathbf{f}$ (or powers thereof) and *twists*. When $\boldsymbol{\lambda}$ is the trivial irrep $\mathbf{1}$ then no such twisting occurs and we reproduce the usual concept of unitary t-groups. A similar phenomenon can be found in twisted Gelfand pairs [33] and twisted wavefunctions from induced representations [34].

Quantum codes.—The Knill-Laflamme (KL) conditions [35] state that a quantum code has distance $d=t+1$

if and only if

$$\langle\psi|E|\phi\rangle = c_E\langle\psi|\phi\rangle, \tag{15}$$

for all errors E of weight t or less and all codewords $|\psi\rangle, |\phi\rangle$. In other words, we can correct $\lfloor t/2 \rfloor$ errors or detect t errors. Note that usually t denotes the number of errors that can be *corrected*, but in order for us to preserve the t in unitary t-design we had to resort to a convention where t denotes the number of errors that can be *detected*.

Consider a finite subgroup $\mathcal{G}$ of $\mathrm{U}(q)$. Suppose all codewords $|\psi\rangle$ transform in an irrep $\boldsymbol{\lambda}$ of $\mathcal{G}$ (where we think of lambda as the irrep of the logical codespace). In particular the codespace will have dimension $|\boldsymbol{\lambda}|$, the dimension of the irrep $\boldsymbol{\lambda}$. And suppose some error E transforms in a representation $\mathbf{R}$ of $\mathrm{U}(q)$, which branches to the representation $\mathbf{R}^{\downarrow}$ of $\mathcal{G}$. Then the tensor product $\langle\psi| \otimes E \otimes |\phi\rangle$ transforms in the representation $\boldsymbol{\lambda}^* \otimes \mathbf{R}^{\downarrow} \otimes \boldsymbol{\lambda}$ of $\mathcal{G}$. The contraction of any tensor is always an invariant, thus $\langle\psi|E|\phi\rangle$ is an invariant and so must transform in the trivial representation $\mathbf{1}$ or the null representation $\mathbf{0}$.

But if $\boldsymbol{\lambda}^* \otimes \mathbf{R}^{\downarrow} \otimes \boldsymbol{\lambda}$ does not contain a copy of the trivial representation 1 in its isotypic decomposition (i.e., $\langle 1, \lambda^* R^{\downarrow}\lambda\rangle = 0$), then the only option is that $\langle\psi|E|\phi\rangle = 0$ and thus the KL condition is satisfied for the error E. We have proven the following lemma.

Lemma 5.—Suppose a code transforms in an irrep $\boldsymbol{\lambda}$ of $\mathcal{G}$ and an error E transforms in an irrep $\mathbf{R}$ of $\mathrm{U}(q)$. If $\langle 1, \lambda^* R^{\downarrow}\lambda\rangle = 0$ then the KL conditions are automatically satisfied for the error E.

Notice that Lemma 5 does not apply to $\mathbf{R} = \mathbf{1}$ because $\langle 1, \lambda^* 1 \lambda\rangle = \|\lambda\| \neq 0$. However, in the $\mathbf{R} = \mathbf{1}$ case the KL conditions are also automatically satisfied. The idea is that if E transforms trivially with respect to $\mathcal{G}$ then E commutes with the action of $\mathcal{G}$ and thus, by Schur's lemma, E acts proportional to the identity on irreps of $\mathcal{G}$, i.e., $E|\phi\rangle = c_E|\phi\rangle$. Then $\langle\psi|E|\phi\rangle = c_E\langle\psi|\phi\rangle$. Note that here the KL condition may be satisfied in a degenerate manner, $c_E \neq 0$, whereas for the errors in Lemma 5 we always have $c_E = 0$. This proves the following lemma.

Lemma 6.—If a code transforms in an irrep $\boldsymbol{\lambda}$ of $\mathcal{G}$ and if an error E transforms in the trivial irrep $\mathbf{1}$ then the KL conditions are automatically satisfied for the error E.

Using these two lemmas we derive our main result.

Theorem 1.—If $\mathcal{G}$ is a $\boldsymbol{\lambda}$-twisted unitary t-group then every subspace of $\mathbf{f}^{\otimes n}$ that transforms in $\boldsymbol{\lambda}$ is a $|\boldsymbol{\lambda}|$-dimensional quantum code with distance $d \geq t+1$ and transversal gate group $\mathsf{G} = \boldsymbol{\lambda}(\mathcal{G})$.

Proof.—Recall that $\mathcal{E}_t$ is the set of all irreps in the isotypic decomposition of $(\mathbf{F} \otimes \mathbf{F}^*)^{\otimes t}$. So any error E of weight t or less can be decomposed as $E = \sum_{\mathbf{R} \in \mathcal{E}_t} E_{\mathbf{R}}$ where $E_{\mathbf{R}}$ is E projected onto the $\mathbf{R}$-isotypic subspace of $(\mathbf{F} \otimes \mathbf{F}^*)^{\otimes t}$. By Lemma 3 we have that $\langle \lambda^*\lambda, R^{\downarrow}\rangle = 0$, and equivalently $\langle 1, \lambda^* R^{\downarrow}\lambda\rangle = 0$, for every $\mathbf{R} \in \mathcal{E}_t$, $\mathbf{R} \neq \mathbf{1}$. So we can apply Lemma 5 to conclude that $\langle\psi|E_{\mathbf{R}}|\phi\rangle = 0$ for every $\mathbf{R} \in \mathcal{E}_t$, $\mathbf{R} \neq \mathbf{1}$. We are left with

$$\langle\psi|E|\phi\rangle = \sum_{\mathbf{R} \in \mathcal{E}_t} \langle\psi|E_{\mathbf{R}}|\phi\rangle = \langle\psi|E_{\mathbf{1}}|\phi\rangle = c_{E_{\mathbf{1}}}\langle\psi|\phi\rangle, \tag{16}$$

where the final equality follows from Lemma 6.

When $\boldsymbol{\lambda}$ is a subrepresentation of $\mathbf{f}^{\otimes n}$ then the transversal gate $\mathbf{f}^{\otimes n}(g) = g^{\otimes n}$ is a logical gate implementing $\boldsymbol{\lambda}(g)$ on the codespace. Thus all gates from $\mathsf{G} \coloneqq \boldsymbol{\lambda}(\mathcal{G})$, the image of the representation $\boldsymbol{\lambda}$, can be implemented transversally. ∎

In the two examples below, the way that we use this theorem is via Lemma 4. That is, we simply check if $\|\lambda f\| = 1$ or $\|\lambda f^2\| = 2$ to see if $\mathcal{G}$ is a $\boldsymbol{\lambda}$-twisted unitary 1-group or a $\boldsymbol{\lambda}$-twisted unitary 2-group, respectively. For higher orders of t, one must invoke Lemma 3 and use branching rules $\mathrm{U}(q){\downarrow}\mathcal{G}$ (see the Supplemental Material [28]).

A good heuristic when applying this theorem is to pick a "large" $\mathcal{G}$ inside of $\mathrm{U}(q)$ and pick a $\boldsymbol{\lambda}$ which is either faithful or almost faithful (i.e., the kernel of the representation $\boldsymbol{\lambda}$ should be small). That way the image $\mathsf{G} = \boldsymbol{\lambda}(\mathcal{G})$ is a very large transversal gate group. From this perspective, Theorem 1 is a method to construct *designer* quantum codes having a certain transversal gate group (cf. [36]).

Example 1: 2I qubit codes.—Let us apply our theorem to the binary icosahedral group $\mathcal{G} = 2\mathrm{I}$ in U(2), which is a unitary 5-group. The character table can be found in the Supplemental Material [28] which is taken directly from GAP [37] as `PerfectGroup(120)`. GAP labels the irreps as χ_i where i ranges between 1 and 9. There are two two-dimensional irreps, χ_2 and χ_3, and we will take $\mathbf{f} = \chi_2$ as our fundamental irrep.

Suppose our code transforms in the other two-dimensional irrep: $\boldsymbol{\lambda} = \chi_3$. Then one can check in GAP that $\|\lambda f\| = 1$ and $\|\lambda f^2\| = 2$ (we provide a code snippet in the Supplemental Material [28]). Using Lemma 4 we see that 2I is a χ_3-twisted unitary 2-group. So by Theorem 1, any subspace that transforms in χ_3 will be a code with distance $d = 3$ and will implement 2I transversally. This supersedes the codes found in [38].

As a canonical example, suppose we encode a qubit, transforming in χ_3, into an nth tensor power of qubits, transforming in $\chi_2^{\otimes n}$. In order for a code to be present, we need the multiplicity of χ_3 in $\chi_2^{\otimes n}$ to be at least 1, i.e., we need to find n such that $\langle \chi_3, \chi_2^n\rangle > 0$. The smallest code occurs when $n = 7$ and the multiplicity is $\langle \chi_3, (\chi_2)^7\rangle = 1$, meaning that this code is unique (for more on unique codes see the Supplemental Material [28]). Since χ_3 only occurs in odd tensor powers the next smallest code occurs when $n = 9$, and the multiplicity is 8. This means there is a $\mathbb{C}P^7$-moduli space worth of nonequivalent codes (see Supplemental Material [28]). Going further, there is a

$\mathbb{C}P^{43}$-moduli space of codes in $n = 11$ qubits and a $\mathbb{C}P^{208}$-moduli space of codes in $n = 13$ qubits. In fact there are χ_3 codes for all odd $n \geq 7$.

Example 2: $\Sigma(360\phi)$ *qutrit codes.*—As another example consider $\mathcal{G} = \Sigma(360\phi)$ in U(3), a unitary 3-group that appears in the high-energy physics literature [12–14]. The character table, a GAP code snippet, and branching rules can be found in the Supplemental Material [28]. The irrep $\chi_1 = \mathbf{1}$ is the trivial irrep and there are four different three-dimensional irreps, labeled χ_2, χ_3, χ_4, and χ_5. We will take the fundamental irrep to be $\mathbf{f} = \chi_2$.

Suppose our code transforms as $\lambda = \chi_3$. Then one can check in GAP that $\|\chi_3\chi_2\| = 1$. Thus by Lemma 4, $\Sigma(360\phi)$ is a χ_3-twisted unitary 1-group. So by Theorem 1, any subspace that transforms in χ_3 will be a code with distance $d = 2$ and will implement $\Sigma(360\phi)$ transversally. Let us find a qutrit code transforming in χ_3 within a tensor product of n qutrits $\mathbf{f}^{\otimes n}$. Again we simply look for n such that $\langle \chi_3, \chi_2^n \rangle > 0$. Thus we have proven that there are codes in $n = 7, 10, 13, 16, 19, \ldots$, i.e., whenever $n \equiv 1 \mod 3$ for $n \geq 7$. The smallest code transforming in χ_3 encodes 1 qutrit into 7 qutrits, detects any single error, and transversally implements any gate from $\Sigma(360\phi)$.

However, unlike 2I, for $\Sigma(360\phi)$ there is also another good logical irrep. Let $\lambda = \chi_4$. One can check that $\Sigma(360\phi)$ is a χ_4-twisted unitary 1-group and there are codes whenever $n \equiv 2 \mod 3$ and $n \geq 5$. The smallest code here is actually better, it occurs when $n = 5$ and the multiplicity is $\langle \chi_4, (\chi_2)^5 \rangle = 1$, meaning that this code is unique (for more on the history of this code [39,40] and unique codes in general see the Supplemental Material [28]). All the codes in this family encode 1 qutrit into n qutrits and detect any single error while implementing $\Sigma(360\phi)$ transversally.

Conclusion.—This Letter establishes a novel and significant connection between quantum t-designs, specifically twisted unitary t-groups, and quantum error-correcting codes. By introducing twisted unitary t-groups, which generalize unitary t-groups through the incorporation of irreducible representations, we provide a framework for constructing quantum codes with many transversal gates, which naturally do not spread errors and thus are useful for fault tolerance. Two illustrative examples involving the unitary 5-group 2I in SU(2) and the unitary 3-group $\Sigma(360\phi)$ in SU(3) highlight the practicality and versatility of our approach, yielding n-qubit and n-qutrit quantum codes with impressive transversal gates. Both of these codes have transversal gate groups which are maximal, lacking only a single gate outside of the respective groups 2I and $\Sigma(360\phi)$ to achieve universality.

It is the hope of the authors that this work, on top of previous work on quantum error correcting codes outside the stabilizer framework [36,38,41–44], will spur a robust inquiry into quantum circuits to implement error correction, fault tolerant measurements, fault tolerant gates, and general fault tolerant circuit design, all for nonadditive codes.

We thank Markus Heinrich for first introducing us to unitary t-groups and we thank Michael Gullans and Victor V. Albert for helpful conversations regarding unitary t-designs and code finding. We thank Anthony Leverrier for thoroughly reviewing a previous version of the manuscript and finding an error. We also thank Brad Horner from Mathematics Stack Exchange for suggesting the proof in the last section of the Supplemental Material [28]. This research was supported in part by the MathQuantum RTG through the NSF RTG Grant No. DMS-2231533.

E. K. and I. T. contributed equally to this Letter.

[*]Contact author: erickub@umd.edu
[†]Contact author: igt@umd.edu

[1] J. H. Conway and S. N. J. A., *Sphere Packings, Lattices, and Groups* (World Publishing Corp., New York, 2008).
[2] A. J. Scott, Optimizing quantum process tomography with unitary 2-designs, J. Phys. A **41**, 055308 (2008).
[3] S. Kimmel and Y.-K. Liu, Phase retrieval using unitary 2-designs, in *Proceedings of the 2017 International Conference on Sampling Theory and Applications (SampTA)* (IEEE, New York, 2017).
[4] Y. Nakata, D. Zhao, T. Okuda, E. Bannai, Y. Suzuki, S. Tamiya, K. Heya, Z. Yan, K. Zuo, S. Tamate, Y. Tabuchi, and Y. Nakamura, Quantum circuits for exact unitary t designs and applications to higher-order randomized benchmarking, PRX Quantum **2**, 030339 (2021).
[5] A. Ambainis, J. Bouda, and A. Winter, Nonmalleable encryption of quantum information, J. Math. Phys. (N.Y.) **50**, 042106 (2009).
[6] D. A. Roberts and B. Yoshida, Chaos and complexity by design, J. High Energy Phys. 04 (2017) 121.
[7] E. Assmus and H. Mattson, New 5-designs, J. Comb. Theory Ser. A **6**, 122 (1969).
[8] A. Roy and A. J. Scott, Unitary designs and codes, Des. Codes Cryptogr. **53**, 13 (2009).
[9] D. Gross, K. Audenaert, and J. Eisert, Evenly distributed unitaries: On the structure of unitary designs, J. Math. Phys. (N.Y.) **48**, 052104 (2007).
[10] E. Bannai, M. Nakahara, D. Zhao, and Y. Zhu, On the explicit constructions of certain unitary t-designs, J. Phys. A **52**, 495301 (2019).
[11] E. Bannai, Y. Nakata, T. Okuda, and D. Zhao, Explicit construction of exact unitary designs, Adv. Math. **405**, 108457 (2022).
[12] W. Fairbairn, T. Fulton, and W. H. Klink, Finite and disconnected subgroups of SU3 and their application to the elementary-particle spectrum, J. Math. Phys. (N.Y.) **5**, 1038 (1964).
[13] P. O. Ludl, Comments on the classification of the finite subgroups of SU(3), J. Phys. A **44**, 255204 (2011).

[14] A. Merle and R. Zwicky, Explicit and spontaneous breaking of SU(3) into its finite subgroups, J. High Energy Phys. 02 (2012) 128.

[15] A. Denys and A. Leverrier, Multimode bosonic cat codes with an easily implementable universal gate set, arXiv:2306.11621.

[16] B. Eastin and E. Knill, Restrictions on transversal encoded quantum gate sets, Phys. Rev. Lett. **102**, 110502 (2009).

[17] S. Bravyi and A. Kitaev, Universal quantum computation with ideal Clifford gates and noisy ancillas, Phys. Rev. A **71**, 022316 (2005).

[18] J. Haah, M. B. Hastings, D. Poulin, and D. Wecker, Magic state distillation with low space overhead and optimal asymptotic input count, Quantum **1**, 31 (2017).

[19] D. Litinski, Magic state distillation: Not as costly as you think, Quantum **3**, 205 (2019).

[20] O. Parzanchevski and P. Sarnak, Super-golden-gates for $PU(2)$, Adv. Math. **327**, 869 (2018).

[21] S. Evra and O. Parzanchevski, Ramanujan complexes and golden gates in PU(3), Geom. Funct. Anal. **32**, 193 (2022).

[22] D. Gottesman, Stabilizer codes and quantum error correction, arXiv:quant-ph/9705052.

[23] Y. Ouyang and G. K. Brennen, Finite-round quantum error correction on symmetric quantum sensors, arXiv:2212.06285.

[24] Y. Ouyang, Robust projective measurements through measuring code-inspired observables, arXiv:2402.04093.

[25] Y. Li, Codeword stabilized quantum codes and their error correction, Ph.D. thesis, UC Riverside, 2010.

[26] A. A. Mele, Introduction to haar measure tools in quantum information: A beginner's tutorial, arXiv:2307.08956.

[27] D. J. Rowe, M. J. Carvalho, and J. Repka, Dual pairing of symmetry and dynamical groups in physics, Rev. Mod. Phys. **84**, 711 (2012).

[28] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.133.030602 which includes Refs. [29,30], for more detailed calculations.

[29] H. Pollatsek and M. B. Ruskai, Permutationally invariant codes for quantum error correction, Linear Algebra Appl. **392**, 255 (2004).

[30] J. A. Gross, Designing codes around interactions: The case of a spin, Phys. Rev. Lett. **127**, 010504 (2021).

[31] R. Feger, T. W. Kephart, and R. J. Saskowski, LIEART2.0—a mathematica application for lie algebras and representation theory, Comput. Phys. Commun. **257**, 107490 (2020).

[32] E. Bannai, G. Navarro, N. Rizo, and P. H. Tiep, Unitary t-groups, J. Math. Soc. Jpn. **72**, 909 (2020).

[33] J. R. Stembridge, On Schur's Q-functions and the primitive idempotents of a commutative Hecke algebra, Journal of Algebraic Combinatorics **1**, 71 (1992).

[34] C. J. Isham, Topological and Global Aspects of Quantum Theory, in *Les Houches Summer School on Theoretical Physics: Relativity, Groups and Topology* (North-Holland Physics Pub Amsterdam, Netherlands, 1983), pp. 1059–1290.

[35] E. Knill, R. Laflamme, and L. Viola, Theory of quantum error correction for general noise, Phys. Rev. Lett. **84**, 2525 (2000).

[36] E. Kubischta and I. Teixeira, The not-so-secret fourth parameter of quantum codes, arXiv:2310.17652.

[37] GAP, GAP—Groups, Algorithms, and Programming, Version 4.12.0, https://www.gap-system.org (2018).

[38] E. Kubischta and I. Teixeira, Family of quantum codes with exotic transversal gates, Phys. Rev. Lett. **131**, 240601 (2023).

[39] I. Teixeira, Finding the 5 qutrit $\Sigma(360\phi)$ code (private communication).

[40] V. V. Albert, Finding the 5 qutrit $\Sigma(360\phi)$ code (private communication).

[41] E. M. Rains, R. H. Hardin, P. W. Shor, and N. J. A. Sloane, A nonadditive quantum code, Phys. Rev. Lett. **79**, 953 (1997).

[42] S. Yu, Q. Chen, C. H. Lai, and C. H. Oh, Nonadditive quantum error-correcting code, Phys. Rev. Lett. **101**, 090501 (2008).

[43] Y. Ouyang, Permutation-invariant quantum codes, Phys. Rev. A **90**, 062317 (2014).

[44] A. Aydin, M. A. Alekseyev, and A. Barg, A family of permutationally invariant quantum codes, Quantum **8**, 1321 (2024).