# Painless Quantum Benchmarking

Alejandro Ortega

29 April 2019

## 1 Introduction

Unitary designs are finite ensembles of unitary matrices that approximate the Haar distribution over the complex unitary group. As quantum algorithms and protocols increasingly require generating matrices uniformly distributed over the unitary group, the Haar measure provides a natural randomization measure that simplifies analysis of such protocols. However, sampling from the Haar measure is infeasible, hence the interest in finite unitary designs that approximate the measure. The unitary designs derived from the Kerdock Set are of interest in quantum benchmarking to support improvements to fidelity, and in wireless communication to develop algorithms that support multi-user detection for massive random access and neighbor discovery [2].

The unitary design associated with the Kerdock set is a representation of the projective linear group, and it was first constructed in [4] by different methods. The connection to Kerdock codes simplifies the description of this design. There are three types of generators, and the type associated with multiplication by field element, is the most challenging to implement efficiently. In this paper we approach implementation by making a connection to classical finite field arithmetic, and bound the gate complexity of multiplication by field element by the choice of irreducible polynomial.

### 1.1 Foundations of Quantum Mechanics

The mathematical foundation for fault-tolerant quantum computation is a group-theoretic framework centered on the Heisenberg-Weyl Group. Throughout, let $N = 2^m$ and denote the binary field by $\mathbb{F}_2$. The Heisenberg-Weyl Group $HW_N$ arises in physics as the Pauli Group, where it describes the possible state transitions in an $m$-qubit quantum system, and as the extraspecial group in mathematics, where it is the framework for orthogonal and symplectic geometry.

A single qubit is a 2-dimensional Hilbert space, where

$$e_0 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \qquad e_1 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

form a computational basis. A quantum state $\psi$ is a superposition of $e_0$ and $e_1$ such that $\psi = \alpha e_0 + \beta e_1$ for $\alpha, \beta \in \mathbb{C}$ satisfying the $|\alpha|^2 + |\beta|^2 = 1$. This condition on $\alpha$ and $\beta$ is known as the Born Rule.

Let $i \equiv \sqrt{-1}$. The Pauli matrices are

$$I_2, \quad X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad Y \equiv iXZ = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

where $I_2$ is the $2 \times 2$ identity matrix. An arbitrary quantum state can be written as linear combination of Pauli matrices and applied to the basis state $e_0$

$$\psi = (\alpha_0 I_2 + \alpha_1 X + i\alpha_2 Z + \alpha_3 Y)e_0$$

.

## 1.2 The Heisenberg-Weyl and Clifford Groups

The Heisenberg-Weyl Group is constructed as $m$-fold Kronecker products of the computational basis elements scaled by powers of $i$ [2]. Let $\otimes$ denote the usual Kronecker product. Suppose $a = (a_{m-1}, \ldots, a_1), b = (b_{m-1}, \ldots, b_1)$ are binary vectors in $\mathbb{F}_2^m$. Define the following operator as an $m$-fold Kronecker product

$$D(a, b) \equiv X^{a_{m-1}} Z^{b_{m-1}} \otimes \cdots \otimes X^{a_1} Z^{a_1}.$$

The Heisenberg-Weyl Group $HW_N$ consists of all scalar multiples of $m$-qubit Pauli matrices of the form $\omega D(a, b)$ for all $a, b \in \mathbb{F}_2^m$, where $\omega = i^c$ for $c = 1, 2, 3, 4$. The cardinality of $HW_N$ is $4N^2$.

The standard symplectic inner product [7] for $\mathbb{F}_2^{2m}$ is given by

$$\langle [a, b], [a', b'] \rangle_{\mathrm{S}} \equiv a'b^T + b'a^T = [a, b]\Omega[a', b']^T,$$

where the symplectic form is

$$\Omega = \begin{bmatrix} 0 & I_m \\ I_m & 0 \end{bmatrix}.$$

In general, a $2m \times 2m$ matrix $M$ with entries in $\mathbb{F}_2$ that satisfies $M\Omega M^T = \Omega$ is said to be a binary symplectic matrix.

Heisenberg-Weyl is a group with respect to matrix multiplication, where multiplication of the operator $D(a, b)$ satisfies

$$D(a, b)D(a', b') = (-1)^{a'b^T + b'a^T} D(a', b')D(a, b).$$

Hence, elements of the Heisenberg-Weyl group either commute or anti-commute, and commute if only if their symplectic inner product $\langle [a,b],[a',b'] \rangle_{\mathrm{S}} = 0$.

There exists an homomorphism $\phi : HW_N \to \mathbb{F}_2^{2m}$ defined by

$$\phi(\omega D(a,b)) \equiv [a,b] \ \forall \ \omega = i^c, \quad c = 1,2,3,4,$$

which allows elements of $HW_N$ to be represented as binary vectors in $\mathbb{F}_2^{2m}$, up to scalar multiplication. The kernel of this homomorphism is $\langle \omega I_N \rangle$.

The Clifford Group $\mathrm{Cliff}_N$ is the normalizer of $HW_N$ within the usual complex unitary group $\mathbb{U}_N$, and thus consists of all unitary matrices $g \in \mathbb{U}_N$ satisfying

$$\{g \mid gD(a,b)g^\dagger \in HW_N \text{ for all } D(a,b) \in HW_N\}$$

where $g^\dagger$ is the Hermitian transpose of $g$.

The Clifford Group is of interest because elements of $\mathrm{Cliff}_N$ are physical operators that act on quantum states, and thus correspond to quantum circuits. Clifford operators can be represented by $2m \times 2m$ binary symplectic matrices, providing an exponential reduction in size [7]. These symplectic matrices act as a binary control plane for the quantum computer. The group of symplectic $2m \times 2m$ binary matrices is called the symplectic group over $\mathbb{F}_2^{2m}$ and is denoted by $\mathrm{Sp}(2m, \mathbb{F}_2)$.

The elements of $\mathrm{Cliff}_N$ are called unitary automorphisms because they induce outer automorphisms of $HW_N$ by conjugation. The Inner automorphisms in $HW_N$ preserve every conjugacy class $\{\pm D(a,b)\}$ and $\{\pm iD(a,b)\}$.

## 1.3 Unitary Designs

Generating random matrices, randomly distributed over the unitary group $\mathbb{U}_N$ is a common feature of algorithms and protocols, and the Haar measure provides a natural randomization measure. However, sampling from the Haar measure is infeasible since the number of gates grows exponentially with the number of qubits, hence the interest in unitary $k$-designs. A unitary $k$-design is a finite ensemble of unitary matrices that approximates the Haar distribution.

Unitary designs are described in [5]; let $k$ be a positive integer. An ensemble is the set $\mathcal{E} = \{p_i, U_i\}_{i=1}^n$, where $p_i$ is the probability of selecting a unitary matrix $U_i$. $\mathcal{E}$ is a unitary $k$-design if for all linear operators $X \in (\mathbb{C}^{\mathbb{N}})^{\otimes k}$,

$$\sum_{(p,U)\in\mathcal{E}} pU^{\otimes k} X (U^\dagger)^{\otimes k} = \int_{\mathbb{U}_N} d\eta(U) U^{\otimes k} X (U^\dagger)^{\otimes k}$$

where $\eta(\cdot)$ denotes the Haar measure on the unitary group $\mathbb{U}_N$. The linear transformations on each side are called $k$-fold twirls [10]. A unitary $k$-design is defined by the property that an ensemble twirl coincides with the full unitary twirl.

The matrix $E(a,b)$ is defined as

$$E(a,b) \equiv i^{ab^T} D(a,b).$$

$E(a,b)$ is Hermitian since the matrices $D(a,b)$ are symmetric when $ab^T = 0$ and anti-symmetric when $ab^T = 1$. $E(a,b)$ satisfies $E(a,b)^2 = I_N$.

The automorphism induced by a Clifford element $g$ satisfies

$$gE(a,b)g^\dagger = \pm E([a,b]F_g)$$

where

$$F_g = \begin{bmatrix} A_g & B_g \\ C_g & D_g \end{bmatrix} \in \mathrm{Sp}(2m, \mathbb{F}_2).$$

Thus, the the symplectic property of $F_g$ is a consequence of the automorphism induced by $g$ respecting commutativity in $HW_N$ .

The graph $\Gamma_N$ is defined on vertices $\pm E(a,b)$ for all $[a,b] \neq 0$. An edge connects two vertices $\pm E(a,b)$ and $\pm E(a',b')$ if the corresponding Pauli matrices commute. To simplify notation, the matrix $\pm E(a,b)$ is identified by $[a,b]$.

A strongly regular graph is defined in [1], and has parameters $(n,t,\lambda,\mu)$. This graph has $n$ vertices each of degree $t$. The number of vertices joined to a pair of distinct vertices $x,y$ is either $\lambda$ or $\mu$, depending on whether $x,y$ are joined or not, respectively.

The graph $\Gamma_N$ is strongly regular with parameters

$$n = N-1, t = \frac{N^2}{2} - 2, \lambda = \frac{N^2}{4} - 3, \mu = \frac{N^2}{4} - 1.$$

The Clifford Group acts transitively on vertices, edges and non-edges of $\Gamma_N$, which is a well-known result in symplectic geometry.

Let $\mathcal{E} = \{p_i, U_i\}_{i=1}^n$ be an ensemble of Clifford elements. The ensemble is Pauli mixing if the induced distribution $(p_i, U_i E(a,b) U_i^\dagger)$ is uniform over all Hermitian Paulis [11]. The ensemble is Pauli 2-mixing if for every pair of distinct vertices

$$([a,b],[a',b'])$$

that are joined (resp. non-joined), the distribution over

$$(U_i E(a,b) U_i^\dagger, U_i E(a',b') U_i^\dagger)$$

is uniform over all edges(resp. non-edges).

Since Clifford is shown to act transitively on edges and non-edges of $\Gamma_N$, the Clifford Group forms a unitary 3-design.

| Circuit Element | Symplectic Matrix $F_g$ | Clifford Operator $g$ |
|---|---|---|
| Transversal Hadamard | $\Omega = \begin{bmatrix} 0 & I_m \\ I_m & 0 \end{bmatrix}$ | $H_N = H_2^{\otimes m}$ |
| Controlled-NOT (CNOT) | $L_Q = \begin{bmatrix} Q & 0 \\ 0 & Q^{-T} \end{bmatrix}$ | $l_Q : e_v \mapsto e_{vQ}$ |
| Controlled-$Z$ and Phase | $T_P = \begin{bmatrix} I_m & P \\ 0 & I_m \end{bmatrix}$; $P = P^T$ | $\mathrm{diag}\left(i^{xP_z x^T \bmod 4}\right)$ |
| Partial Hadamards | $G_k = \begin{bmatrix} L_{m-k} & U_k \\ U_k & L_{m-k} \end{bmatrix}$ | $g_k = H_{2^k} \otimes I_{2^{m-k}}$ |

Table 1: A generating set of symplectic matrices and their corresponding unitary operators. $e_v$ denotes the standard basis vector in $\mathbb{C}^N$. $H_{2^t}$ denotes the full Walsh-Hadamard matrix of size $2^t$.

## 1.4 The Kerdock Codes

The Kerdock codes are non-linear binary codes, where the exponentiated codewords are the eigenvectors of maximal commutative subgroups of $HW_N$ [3]. We will provide the framework for the construction of the Kerdock Set. The finite field $\mathbb{F}_{2^m}$ is constructed from the binary field $\mathbb{F}_2$ by adjoining the root $\alpha$ of an irreducible polynomial $p(x)$ of degree $m$. The field $\mathbb{F}_{2^m}$ consists of polynomials in $\alpha$ of degree at most $m-1$.

The *trace map* Tr: $\mathbb{F}_{2^m} \to \mathbb{F}_2$ is defined by

$$\mathrm{Tr}(x) = x + x^2 + x^{2^2} + \ldots + x^{2^{m-1}}.$$

The trace inner product $\langle x, y \rangle_{\mathrm{Tr}} = \mathrm{Tr}(xy)$ is a symmetric bilinear form, and thus there exists a binary symmetric matrix $W$ for which $\mathrm{Tr}(xy) = xWy^T$. This $m \times m$ matrix $W$ is defined over the primal basis, which consist of powers of $\alpha$:

$$W_{ij} = \mathrm{Tr}(\alpha^i \alpha^j) \quad i, j \in \{0, 1, \ldots, m-1\}.$$

Observe that this matrix $W$ is a Hankel matrix, since if $i + j = h + k$ then $\mathrm{Tr}(\alpha^i \alpha^j) = \mathrm{Tr}(\alpha^h \alpha^k)$.

Let the primitive irreducible polynomial be given by

$$p(x) = p_0 + p_1 x + p_2 x^2 + \ldots + p_{m-1} x^{m-1} + x^m.$$

Define the matrix $A$ by

$$A = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ & \vdots & & \ddots & 0 \\ 0 & 0 & 0 & \cdots & 1 \\ p_0 & p_1 & p_2 & \cdots & p_{m-1} \end{bmatrix}$$

which represents multiplication by the primitive element $\alpha$. Then multiplication by $z \in \mathbb{F}_{2^m}$ can be written as the linear transformation $xz = xA_z$, where $A_z = A^i$ for exactly $z = \alpha^i$, $i \in \{0, 1, \ldots, 2^m - 2\}$.

For $0 \leq r \leq (m-1)/2$ and for $z = (z_0, z_1, \ldots, z_r)$ the bilinear form $\mathrm{Tr}(zxy)$ is represented by the binary symmetric matrix

$$P_z = A_z W.$$

Then the Kerdock Set $P_K(m)$ consists of all such matrices $P_z$. Non-zero matrices in the Kerdock Set are non-singular.

Define $N$ mutually unbiased bases (MUBs) by

$$M_z \equiv t_{P_z} H_N = \mathrm{diag}\left(i^{x P_z x^T}\right) H_N, \quad z \in \mathbb{F}_{2^m}$$

where $[H_N]_{x,y} \equiv \frac{1}{\sqrt{N}}(-1)^{xy^T}$, for $x, y \in \mathbb{F}_2^m$, is the Walsh-Hadamard matrix of order $N$. Complete the mutually unbiased bases by appending $M_\infty \equiv I_N$. Hence, the set of Kerdock MUBs given by

$$\mathcal{B}_{\mathrm{K},m} \equiv \{I_N, M_z \mid z \in \mathbb{F}_{2^m}\}$$

is a maximal set of mutually unbiased bases. [3] showed that there is a systematic procedure to sample from the group $\mathcal{B}_{\mathrm{K},m}$ by taking advantage of the group's symmetry: by choosing $\alpha, \beta, \delta \in \mathbb{F}_{2^m}$ uniformly at random, a symmetry element can be constructed via

$$F_{\alpha,\beta,\delta} \equiv T_{A_\alpha W} \cdot L_{A_\beta} \cdot (\Omega L_{W^{-1}} \cdot T_{A_\delta W})$$

where $T$, $L$ and $\Omega$ are symplectic matrices given in Table 1. Note that the number of 1s in $Q$ and $P$ directly relates to number of gates involved in the circuit realizing the respective unitary operators [7]. The quantum gate complexity of symmetry elements in $\mathcal{B}_{\mathrm{K},m}$ is known for all components of the above product except for $L_{A_\beta}$; note that $A_\beta$ is equivalent to multiplication by random field element.

The implementation of the Kerdock design described in [4] had a quantum gate cost of $O(m \log m \log\log m)$, where $A_\beta$ was the most challenging element of the design, and many complicated assumptions were used to bound the gate complexity. Here, we will give a technique for generating $A_\beta$ that depends only on the choice of irreducible polynomial.

| Irreducible polynomial | Values of $m$ |
|---|---|
| $x^m + x + 1$ | 2, 3, 4, 6, 7, 9, 15, 22, 28, 30, 46, 60, 63, 127, 153, 172, 303, 471, 532, 865, 900 |

Table 2: Values of $m < 1000$ for which there exists an irreducible trinomial of the specified form

### 1.5 Irreducible Trinomials

Recall that $\mathbb{F}_{2^m}$ is created by adjoining the root of an irreducible polynomial. In [8] and [9], irreducible trinomials of the form $x^m + x + 1$ were shown to simplify classical bit-serial multipliers; in [6] we showed that these trinomials simplify the quantum circuit representation for multiplication by primitive element. However, trinomials are not necessarily irreducible for all fields $\mathbb{F}_{2^m}$. For example, $x^5 + x + 1$ is not irreducible over $\mathbb{F}_{32}$. In fact, $x^m + x + 1$ is irreducible for only 21 values for $m < 1000$. These values are given in Table 2. Thus, we will begin our discussion of multiplication by random field element by first considering only irreducible trinomials of the form $x^m + x + 1$, before discussing other trinomials.

## 2 Multiplication by Random Field Element

Throughout, let $N = 2^m$. Multiplication by random field element is the only element of the Kerdock design for which the quantum gate bound is not certain, hence the interest in an algorithm.

Let $\mathbb{F}_{2^m}$ denote the finite field constructed from the binary field $\mathbb{F}_2$ by adjoining the root $\alpha$ of an irreducible polynomial $p(x)$ of degree $m$. Let the primitive irreducible polynomial be given by

$$p(x) = p_0 + p_1 x + p_2 x^2 + \ldots + p_{m-1} x^{m-1} + x^m.$$

Although any independent set of $m$ elements from $\mathbb{F}_{2^m}$ will suffice, the basis of the form $\{1, \alpha, \ldots, \alpha^{m-1}\}$ has useful properties and is known as the *primal basis*. Recall the matrix $A$ is defined by

$$A = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ & \vdots & & \ddots & 0 \\ 0 & 0 & 0 & \cdots & 1 \\ p_0 & p_1 & p_2 & \cdots & p_{m-1} \end{bmatrix}$$

which represents multiplication by the primitive element $\alpha$. At first, only irreducible polynomials of the form $p(x) = x^m + x + 1$—known as trinomials—will

be considered. In [6], we had shown that trinomials simplify the quantum circuit representation of the matrices in the bit-serial paradigm, and clearly $A$ is sparsest for a polynomial with three terms.

Suppose $x \in \mathbb{F}_{2^m}$ and let the basis expansion of $x$ be denoted by

$$x = \sum_{i=0}^{m-1} x_i \alpha_i \qquad x_i \in \{0, 1\}.$$

Define the binary row vectors $\mathbf{x}$ by

$$\mathbf{x} = [x_0, x_1, \ldots, x_{m-1}].$$

Henceforth, all $x \in \mathbb{F}_{2^m}$ will be identified by the binary row vector $\mathbf{x}$ of the appropriate basis expansion.

The *Frobenius map* $f$: $\mathbb{F}_{2^m} \mapsto \mathbb{F}_{2^m}$ is defined by $f(x) = x^2$. Consider the primal basis

$$\{1, \alpha, \ldots, \alpha^{m-1}\}$$

and its square

$$\{1, \alpha^2, \ldots, \alpha^{2(m-1)}\}.$$

Note that the latter set of $m$ elements forms a basis with respect to $\alpha^2$, and there similarly exists a basis for all $\alpha^{2^i}$ for $i = 0, \ldots, m-1$. Thus, there exists a change of basis matrix $F$ from $\alpha^{2^i} \mapsto \alpha^{2^{(i+1)}}$; since the Frobenius map is linear over $\mathbb{F}_2$, the change of basis matrix $F$ is fixed for all $i$.

To better illustrate this change of basis map, consider the case for $m = 6$ and the irreducible trinomial $p(x) = x^6 + x + 1$, and mapping from $\alpha^{2^0} = \alpha \mapsto \alpha^2$. Then the primal basis is

$$\{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5\}$$

and the $\alpha^2$ basis is

$$\{1, \alpha^2, \alpha^4, \alpha^6, \alpha^8, \alpha^{10}\}.$$

$x \in \mathbb{F}_{64}$ has a primal basis expansion $\mathbf{x} = [x_0, x_1, \ldots, x_5]$ such that

$$x = \sum_{i=0}^{5} x_i \alpha^i \qquad x_i \in \{0, 1\}.$$

Then applying $F$ to $\mathbf{x}$ results in a vector $\mathbf{x}' = [x'_0, x'_1, \ldots, x'_5]$, such that

$$x = \sum_{i=0}^{5} x'_i \alpha^{2i} \qquad x'_i \in \{0, 1\}$$

i.e. gives $x$ with respect to the $\alpha^2$ basis. To proceed we will equate

$$x_0 + x_1\alpha + x_2\alpha^2 + x_3\alpha^3 + x_4\alpha^4 + x_5\alpha^5$$

and

$$\begin{aligned}&x'_0 + x'_1\alpha^2 + x'_2\alpha^4 + x'_3\alpha^6 + x'_4\alpha^8 + x'_5\alpha^{10}\\ =&x'_0 + x'_1\alpha^2 + x'_2\alpha^4 + x'_3(\alpha+1) + x'_4(\alpha^3+\alpha^2) + x'_5(\alpha^5+\alpha^4)\end{aligned}$$

which results in the following system of equations

$$x_0 = x'_0 + x'_3, \qquad x_1 = x'_3 \tag{1}$$
$$x_2 = x'_1 + x'_4, \qquad x_3 = x'_4 \tag{2}$$
$$x_4 = x'_2 + x'_5, \qquad x_5 = x'_5. \tag{3}$$

After solving for $x'_0, x'_1$, and $x'_2$, we have

$$x'_0 = x_0 + x_1, \qquad x'_3 = x_1 \tag{4}$$
$$x'_1 = x_2 + x_3, \qquad x'_4 = x_3 \tag{5}$$
$$x'_2 = x_4 + x_5, \qquad x'_5 = x_5. \tag{6}$$

Thus, these equations give the columns of $F$ for $m = 6$:

$$F = \begin{bmatrix}1&0&0&0&0&0\\1&0&0&1&0&0\\0&1&0&0&0&0\\0&1&0&0&1&0\\0&0&1&0&0&0\\0&0&1&0&0&1\end{bmatrix}.$$

We will now prove $F$ has a specific form when the irreducible polynomial is a trinomial.

*Proof:* Let $N = 2^m$. Suppose the polynomial $x^m + x + 1$ is irreducible over $\mathbb{F}_N$. Then the primitive element $\alpha$ satisfies $\alpha^m = \alpha + 1$.

Let $\beta \in \mathbb{F}_N$. Then $\beta$ has a primal basis expansion

$$\beta = \sum_{i=0}^{m-1} \beta_i \alpha^i, \quad \beta_i \in \mathbb{F}_2.$$

With respect to matrix multiplication, this is equivalent to multiplying each coefficient $\beta_i$ with $e_i$, the basis vector with a one entry at the $i^{\text{th}}$ position. In other words, let $\beta$ be identified with its primal basis coefficient vector $[\beta_0, \ldots, \beta_{m-1}]$. Then clearly $\beta \cdot I_m$ keeps $\beta$ in the primal basis.

Recall that $F$ is the change of basis map from $\alpha^{2^i} \mapsto \alpha^{2^{(i+1)}}$ and is linear over $\mathbb{F}_N$. Then after applying $F$ to the primal basis expansion, we should have

$$\beta = \sum_{j=0}^{m-1} \beta'_j \alpha^{2j}, \quad \beta'_j \in \mathbb{F}_2$$

i.e., the vector $\beta' = \left[\beta'_0, \ldots, \beta'_{m-1}\right]$ is the expansion of $\beta$ in the $\alpha^2$ basis.

Then $F$ takes each coefficient $\beta_i$ of the primal basis and multiplies it by the vector $e'_i$ of the new basis $\alpha^2$, where $e'_i$ corresponds to the representation of $\alpha^i$ in the $\alpha^2$ basis. In other words,

$$\alpha^i = \sum_{j=0}^{m-1} \beta_j^{(i)} \alpha^{2j}, \quad \beta_j^{(i)} \in \mathbb{F}_2,$$

where $\beta^{(i)} = \left[\beta_0^{(i)}, \ldots, \beta_{m-1}^{(i)}\right]$ is the coefficient vector of the primal basis element $\alpha^i$ in the $\alpha^2$ basis, for $i = 0, \ldots, m-1$. Thus, $\beta^{(i)} \equiv e'_i$.

We will proceed by explicitly determining representation of basis elements of $\alpha^{2^i}$ in the $\alpha^{2^{i+1}}$ basis, enumerating the $e'_i$ and thus the rows of $F$. Consider the basis for $\alpha^{2^i}$

$$V = \left\{1, \alpha^{2^i}, \alpha^{2(2^i)}, \alpha^{3(2^i)}, \ldots, \alpha^{(m-1)(2^i)}\right\}$$

and $\alpha^{2^{(i+1)}}$

$$W = \left\{1, \alpha^{2^{(i+1)}}, \alpha^{2(2^{(i+1)})}, \alpha^{3(2^{(i+1)})}, \ldots, \alpha^{(m-1)(2^{(i+1)})}\right\}.$$

Thus, a basis element of $V$ is of the form $\alpha^{k \cdot 2^i}$ for $k = 0, \ldots, m-1$; similarly, a basis element of $W$ is of the form $\alpha^{j \cdot 2^{i+1}}$ for $j = 0, \ldots, m-1$. If $k$ is even, then

$$\alpha^{k \cdot 2^i} = \alpha^{\frac{k}{2} \cdot 2^{i+1}}.$$

Hence, the even rows of $F$ have a single 1 entry.

For the remaining basis elements of $V$ with $k$ odd, we will analyze the primitive element $\alpha$ in two separate cases.

First note that the primitive element satisfies $\alpha = \alpha^m + 1$. For even $m$, due to the linearity of the Frobenius map over $\mathbb{F}_{2^i}$, we have in general

$$\begin{aligned} \alpha^{2^i} &= 1 + \alpha^{2^i(m)}, \\ \alpha^{2^i} &= 1 + \alpha^{2^{i+1}(m/2)}. \end{aligned}$$

It is easy to verify that the odd-indexed elements are given by multiplying by factors of $\alpha^{2^{i+1}(h)}$

$$\alpha^{2^i(2h+1)} = \alpha^{2^{i+1}(h)} + \alpha^{2^{i+1}(h+m/2)}$$

for $h = 0, \ldots, (m-2)/2$.

For odd $m$, we consider $\alpha^2 = \alpha^{m+1} + \alpha \implies \alpha = \alpha^{m+1} + \alpha^2$, and thus in general

$$\begin{aligned} \alpha^{2^i} &= \alpha^{2^i(2)} + \alpha^{2^i(m+1)} \\ \alpha^{2^i} &= \alpha^{2^{i+1}} + \alpha^{2^{i+1}((m+1)/2)}. \end{aligned}$$

As for even $m$, the odd-indexed elements are given by multiplying by factors of $\alpha^{2^{i+1}(h)}$

$$\alpha^{2^i(2h+1)} = \alpha^{2^{i+1}(h+1)} + \alpha^{2^{i+1}(h+(m+1)/2)}$$

for $h = 0, \ldots, (m-3)/2$.

Thus for an irreducible trinomial, the change of basis map $F$ consists of two row types for $k = 0, \ldots m-1$:

1. For even $k$, the $k^{\text{th}}$ row has a single entry at position $k/2$.
2. For odd $k$, i.e. $k = 1 + 2h$ for some $0 \leq h < \lfloor (m-2)/2 \rfloor$, the $k^{\text{th}}$ row has
   (a) an entry at position $h$, and an entry at position $m/2 + h$ for even $m$.
   (b) an entry at position $h+1$, and an entry at position $(m+1)/2 + h$ for odd $m$.

where $k = 0, \ldots, m-1$.

□

It is easily verified that the case for $m = 6$ constructed explicitly earlier follows this form. A proof for generalized trinomials of the form $x^m + x^p + 1$ for $m$ odd is given in Section 3.

From the form of $F$, it is apparent that the right-most non-zero entry in any row has a unique position among all rows. In other words, the rows can be permuted such that $F$ is a triangular matrix. Then realizing F in a quantum circuit means the desired symplectic matrix is $L_F$, and hence the CNOT count follows. In fact, for a trinomial $F$ requires exactly $\lfloor m/2 \rfloor$ CNOT gates and is thus $O(m)$.

We will now proceed with an algorithm for multiplication by random field element. Consider multiplication by $\gamma \in \mathbb{F}_{2^m}$, where $\gamma = \alpha^l$ for arbitrary $0 \leq l < 2^m$. Express $l$ in its base 2 expansion,

$$l = \sum_{i=0}^{m-1} l_i 2^i$$

Then $l$ can be represented as the binary vector $[l_0, l_1, \ldots, l_{m-1}]$.

In an iterative process for $i = 0, \ldots, m-1$, the algorithm proceeds as follows:

1. Implement multiplication by $\alpha^{2^i}$ in the $\alpha^{2^i}$ basis as $M_\beta$ for $\beta = \alpha^{2^i}$ if the corresponding $l_i$ is non-zero.
2. Implement the change of basis map from $\alpha^{2^i} \mapsto \alpha^{2^{(i+1)}}$

The algorithm is detailed in Algorithm 1.

Note that if we are in the $\alpha^{2^i}$ basis, then multiplication by $\alpha^{2^i}$ is performed by the matrix $A$, and hence $M_\beta$ is fixed as the matrix $A$. Henceforth $M_\beta$ will be

**Algorithm 1** Algorithm for multiplication by random field element

**Input:** $l \neq \mathbf{0} \in \mathbb{F}^m$ i.e. $l = [l_0, l_1, \ldots, l_{m-1}]$, $m \in \mathbb{N}$
**Output:** $R$, i.e. $M_\gamma$ `the matrix for multiplication by` $\gamma = \alpha^l$

```
A ← matrix implementing multiplication by primitive element
F ← change of basis map from α^(2^i) ↦ α^(2^(i+1))
R ← I_m
for i = 0, ..., m − 1:
    if l_i ≠ 0:
        R ← R · A
    R ← R · F
return R
```

referred to simply as $A$. From the construction of $A$, it can be easily verified that $A$ is a single permutation and CNOT gate, and therefore $A$ consists of 3 CNOT gates and thus an $O(1)$ gate complexity.

Similarly, the change of basis map is simply the matrix $F$. Note that applying the basis conversion matrix $F$ $m$-times results in a basis with respect to $\alpha^{2^m}$, which of course is simply $\alpha$; hence, after $m$ iterations the final matrix is again in the primal basis. Recall that $F$ was shown to have a complexity of $\lfloor m/2 \rfloor$ when the irreducible polynomial is a trinomial.

Since this algorithm consists of $m$ iterations multiplying matrices with 3 CNOT gates and $\lfloor m/2 \rfloor$ CNOT gates, the entire complexity is $m^2/2 + 3m$ and thus is $O(m^2)$ with respect to the number of qubits.

Of course, this is a larger complexity than the near-linear complexity reported by [4], and it is apparent the worst case complexity corresponds to $\alpha^{m-1}$. While there are optimizations for certain $\gamma \in \mathbb{F}_N$, such as by multiplying by $F^{-1}$, the worst case complexity for $\alpha^{m-1}$ is still $O(m^2)$.

## 2.1 Example for $\mathbb{F}_8$

Consider $m = 3$ and the corresponding finite field $\mathbb{F}_8$ constructed with the root $\alpha$ of the irreducible polynomial $p(x) = x^3 + x + 1$. Then $\alpha$ is a primitive root satisfying $\alpha^3 = \alpha + 1$.

Then multiplication by primitive element is given by

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

The Frobenius change of basis map is given by

$$F = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

Then the permutations $\pi_{(231)}$ and $\pi_{(132)}$ render the matrices $A$ and $F$ as triangular, respectively. The quantum circuit diagrams are given in Figures 1 and 2 in Appendix A.1.

### 2.2 Example for $\mathbb{F}_{64}$

Consider $m = 6$ and the corresponding finite field $\mathbb{F}_{64}$ constructed with the root $\alpha$ of the irreducible polynomial $p(x) = x^6 + x + 1$. Then $\alpha$ is a primitive root satisfying $\alpha^6 = \alpha + 1$.

Then multiplication by primitive element is given by

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

The Frobenius change of basis map is given by

$$F = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Then the permutations $\pi_0 = \pi_{(234561)}$ and $\pi_1 = \pi_{(142536)}$ render the matrices $A$ and $F$ as triangular, respectively. The quantum circuit diagrams are given in Figures 3 and 4 in in Appendix A.2.

## 3 Quantum Gate Complexity For a General Trinomial

We will conclude by calculating the quantum gate complexity of the change of basis map $F$ for additional trinomials.

*Proof:* Let $N = 2^m$ for $m$ odd. Suppose the polynomial $x^m + x^p + 1$ is irreducible over $\mathbb{F}_N$. Then the primitive element $\alpha$ satisfies $\alpha^m = \alpha^p + 1$. If $p$ is even proceed with $\alpha^{-1}$; since $m$ is odd, $\alpha^{-1}$ is equivalent to the primitive element of the irreducible polynomial $x^m + x^{m-p} + 1$, which is subsequently guaranteed to be irreducible over $\mathbb{F}_N$ since $x^m + x^p + 1$ is irreducible. That is, if $p$ is even instead proceed with the primitive element for $x^m + x^{m-p} + 1$.

Recall $F$ is the change of basis map from $\alpha^{2^i} \mapsto \alpha^{2^{(i+1)}}$ and that we are trying to enumerate the rows of $F$.

Consider the basis for $\alpha^{2^i}$

$$V = \left\{1, \alpha^{2^i}, \alpha^{2(2^i)}, \alpha^{3(2^i)}, \ldots, \alpha^{(m-1)(2^i)}\right\}$$

and $\alpha^{2^{(i+1)}}$

$$W = \left\{1, \alpha^{2^{(i+1)}}, \alpha^{2(2^{(i+1)})}, \alpha^{3(2^{(i+1)})}, \ldots, \alpha^{(m-1)(2^{(i+1)})}\right\}.$$

Thus, a basis element of $V$ is of the form $\alpha^{k \cdot 2^i}$ for $k = 0, \ldots, m-1$; similarly, a basis element of $W$ is of the form $\alpha^{j \cdot 2^{i+1}}$ for $j = 0, \ldots, m-1$. If $k$ is even, then

$$\alpha^{k \cdot 2^i} = \alpha^{\frac{k}{2} \cdot 2^{i+1}}.$$

Hence, the even rows of $F$ have a single 1 entry.

For the remaining basis elements of $V$ with $k$ odd, we will analyze the primitive element $\alpha$.

First note that the primitive element satisfies $\alpha^m = \alpha^p + 1$, p odd.

Since $m$ is odd, we consider

$$\begin{aligned}
\alpha^{m+1} &= \alpha^{p+1} + \alpha \\
\alpha &= \alpha^{m+1} + \alpha^{p+1} \\
\alpha &= \alpha^{2 \cdot (m+1)/2} + \alpha^{2 \cdot (p+1)/2} \implies \\
\alpha^{2^i} &= \alpha^{2^{i+1} \cdot (m+1)/2} + \alpha^{2^{i+1} \cdot (p+1)/2}
\end{aligned}$$

and thus in general the odd-indexed elements are given by

$$\alpha^{2^i(2h+1)} = \alpha^{2^{i+1}((p+1)/2+h)} + \alpha^{2^{i+1}(h+(m+1)/2)}$$

for $h = 0, \ldots, (m-3)/2$.

Thus for an irreducible trinomial of the form $x^m + x^p + 1$ for $m$ odd, the change of basis map $F$ consists of two row types for $k = 0, \ldots m-1$:

1. For even $k$, the $k^{\text{th}}$ row has a single entry at position $k/2$.

2. For odd $k$, i.e. $k = 1 + 2h$ for some $0 \leq h < (m-3)/2$, the $k^{\text{th}}$ row has an entry at position $(p+1)/2 + h$, and an entry at position $(m+1)/2 + h$

where $k = 0, \ldots, m-1$.

□

Consider polynomials of the form $x^m + x^p + 1$. We have already discussed the case for $p = 1$ and for $m$ odd. Note that if both $m$ and $p$ are even, the polynomial is reducible since it is a square; hence this case is non-existent. The remaining case is for $m$ even and $p$ odd. If $p = m-1$, then we can proceed with the primitive element $\alpha^{-1}$, which corresponds to the $p = 1$ case. Then the final case under consideration is $m$ even, $p$ odd such that $1 < p < m-1$. Note that in this scenario we can have irreducible polynomials that are not primitive, such as the polynomial $x^6 + x^3 + 1$ for $\mathbb{F}_{64}$. This case is more complicated than those previously discussed, and is subject to further research to determine if their exists a standard form for $F$. Thus, our algorithm works for all finite fields in which there exists an irreducible trinomial of the form $x^m + x^p + 1$ for $p = 1$, or for $m$ odd; this provides a simple construction of the Kerdock design for quantum benchmarking with $O(m^2)$ complexity for the multiplication by field element operation that depends solely on the choice of irreducible polynomial.

## 3.1 Example for $\mathbb{F}_{32}$

We conclude with an illustrative example for $\mathbb{F}_{32}$. Note that $x^5 + x + 1$ is not irreducible. Consider $m = 5$ and the corresponding finite field $\mathbb{F}_{32}$ constructed with the root $\alpha$ of the irreducible polynomial $p(x) = x^5 + x^3 + 1$. Then $\alpha$ is a primitive root satisfying $\alpha^5 = \alpha^3 + 1$.

Then multiplication by primitive element is given by

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

The Frobenius change of basis map is given by

$$F = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

Then the permutations $\pi_0 = \pi_{(23451)}$ and $\pi_1 = \pi_{(14253)}$ render the matrices $A$ and $F$ as triangular, respectively. The quantum circuit diagrams are given in Figures 5 and 6 in in Appendix A.3.

# References


[1] Peter Jephson Cameron, Jacobus Hendricus Van Lint, and Peter J Cameron. *Designs, graphs, codes and their links*, volume 3. Cambridge University Press Cambridge, 1991.

[2] Trung Can. The heisenberg-weyl group, finite symplectic geometry and their applications, 2018. Bachelor's Senior Thesis, Duke University, USA, 2018.

[3] Trung Can, Narayanan Rengaswamy, Robert Calderbank, and Henry D Pfister. Kerdock codes determine unitary 2-designs. *arXiv preprint arXiv:1904.07842*, 2019. `https://arxiv.org/abs/1904.07842`.

[4] Richard Cleve, Debbie Leung, Li Liu, and Chunhao Wang. Near-linear constructions of exact unitary 2-designs. *arXiv preprint arXiv:1501.04592*, 2015. `https://arxiv.org/abs/1501.04592`.

[5] Richard A. Low. *Pseudo-randomness and Learning in Quantum Computation*. PhD thesis, PhD Thesis, University of Bristol, UK, 2010, 2010. `https://arxiv.org/abs/1006.5227`.

[6] Alejandro Ortega. Simplifying quantum circuits using classical bit-serial multipliers, 2018.

[7] Narayanan Rengaswamy, Robert Calderbank, Henry D Pfister, and Swanand Kadhe. Synthesis of logical clifford operators via symplectic geometry. In *2018 IEEE International Symposium on Information Theory (ISIT)*, pages 791–795. IEEE, 2018. `http://arxiv.org/abs/1803.06987`.

[8] Douglas R. Stinson. On bit-serial multiplication and dual bases in gf($(2^m)$). *IEEE transactions on information theory*, 37(6):1733–1736, 1991.

[9] Muzhong Wang and Ian F Blake. Bit serial multiplication in finite fields. *SIAM Journal on Discrete Mathematics*, 3(1):140–148, 1990.

[10] John Watrous. *The theory of quantum information*. Cambridge University Press, 2018.

[11] Zak Webb. The clifford group forms a unitary 3-design. *arXiv preprint arXiv:1510.02769*, 2015. `https://arxiv.org/abs/1510.02769`.

# Appendices

## A Quantum Circuit Diagrams

### A.1 Circuits for $\mathbb{F}_8$

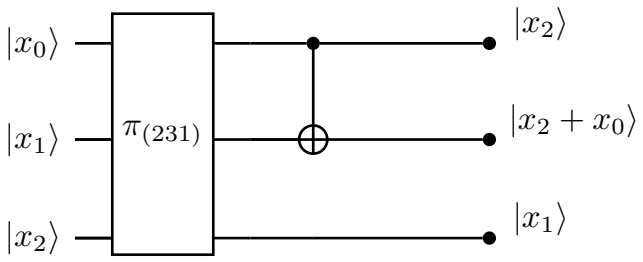


Figure 1: The quantum circuit diagram for $A$, multiplication by $\alpha$ where $\alpha$ satisfies $\alpha^3 = \alpha + 1$.

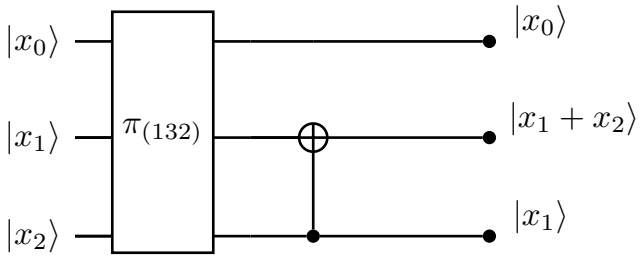


Figure 2: The quantum circuit diagram for the change of basis map $F$ where $\alpha$ satisfies $\alpha^3 = \alpha + 1$.

## A.2 Circuits for $\mathbb{F}_{64}$

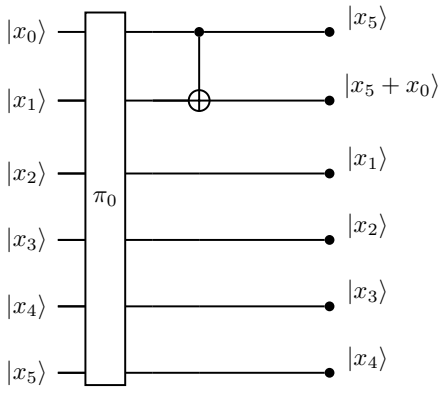


Figure 3: The quantum circuit diagram for $A$, multiplication by $\alpha$ where $\alpha$ satisfies $\alpha^6 = \alpha + 1$.

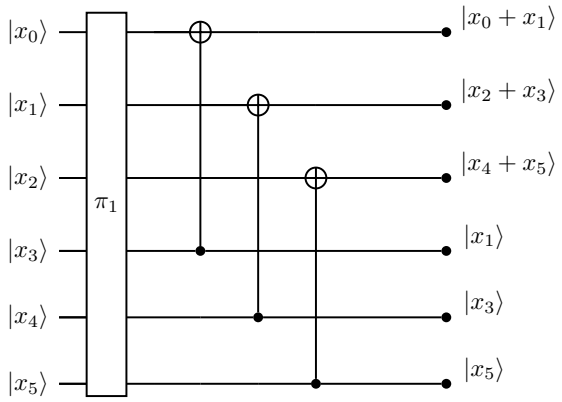


Figure 4: The quantum circuit diagram for the change of basis map $F$ where $\alpha$ satisfies $\alpha^6 = \alpha + 1$.

## A.3 Circuits for $\mathbb{F}_{32}$

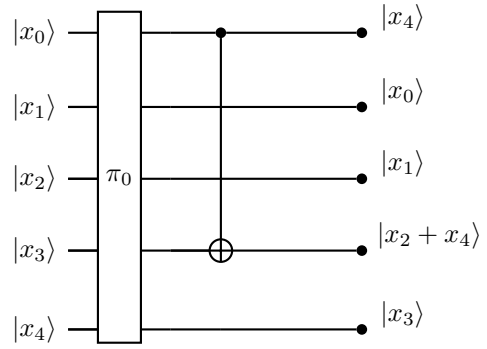


Figure 5: The quantum circuit diagram for $A$, multiplication by $\alpha$ where $\alpha$ satisfies $\alpha^5 = \alpha^3 + 1$.

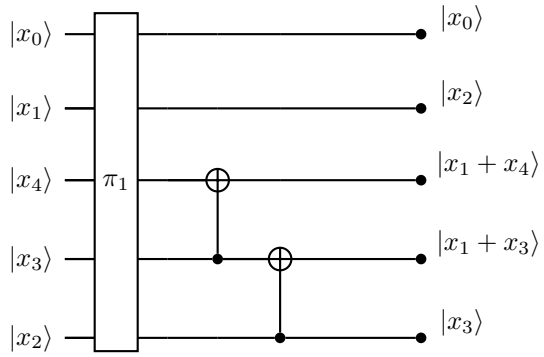


Figure 6: The quantum circuit diagram for the change of basis map $F$ where $\alpha$ satisfies $\alpha^5 = \alpha^3 + 1$.